在具有Rest API的FDM上配置基於時間的訪問控 制規則

Ħ	目錄		
<u>簡</u> 2	<u>寄介</u>		
必要	<u>※要條件</u>		
	<u>需求</u>		
	<u>採用元件</u>		
<u>背</u>	皆景資訊		
<u>設</u>	<u>设定</u>		
驗	<u>魚證</u>		

簡介

本文描述如何在FDM使用Rest API管理的FTD上配置和驗證基於時間的訪問控制規則。

必要條件

需求

思科建議您瞭解以下主題:

- 安全防火牆威脅防禦(FTD)
- Firepower裝置管理(FDM)
- 具象狀態傳輸應用程式設計介面(REST API)知識
- 存取控制清單(ACL)

採用元件

本檔案中的資訊是根據FTD 7.1.0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。

背景資訊

FTD API版本6.6.0和更新版本支援根據時間進行限制的訪問控制規則。

使用FTD API,您可以建立時間範圍對象(指定一次性或循環時間範圍),並將這些對象應用於訪問控制規則。使用時間範圍,您可以將訪問控制規則應用於一天中的某些時間或某些時間段的流量 ,以便為網路使用提供靈活性。不能使用FDM建立或應用時間範圍,FDM也不會顯示訪問控制規則 是否應用了時間範圍。

步驟 1.按一下高級選項(「kebab」選單)以開啟FDM API資源管理器。

Firepower Devic	ce Manager	Monitoring	Policies (Dbjects Devic	ce: firepower			>	(2)	Explorer	ninistrator ~
🔊 Se	curity Polic	ies									
- D	\rightarrow \bigcirc SSL De	ecryption \rightarrow ()	Identity \rightarrow ()	Security Intelligence	e -> 🕑 NA	Acces	is Control \rightarrow	Intrusion			
						Ŧ	Filter			¢ [*]	()
		SOURCE			DESTINATION						
# NA	ME AC	CTION ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
					There are no a	access rules yet.					
				S	tart by creating t	he first access rule.					
					CREATE A	CCESS RULE					
Default A	Acces	s Control 😑 Block									

圖1.FDM Web使用者介面。

步驟 2.選擇類別AccessPolicy以顯示不同的API呼叫。

cisco.	Firepower Devic	ce Manager	Monitoring	Policies	Objects	Device: firepower		\triangleright			adm Adn	in inistrator	Ň
FTD RES	ST API ←	document You can te	tation for the resource	e. ds and resou	rces through th	nis page. When you fill in paramete	ers and click the Try it Out! but	tton, you inte	eract direct	ly with the syst	em. GET calls r	etrieve re	al information.
API Explor	rer	POST call /operation	s create real objects. hal/deploy resource in	PUT calls mon	odify existing o nent group. Alt	bjects. DELETE calls remove real of hough some changes, such as to	objects. However, most change the management IP address ar	es do not be nd other syst	come activ tem-level o	e until you dep hanges, do not	oy them using require deploy	the POST ment, it i	r is safer to do a
Error Catal	log	deployme	nt after you make any	y configuratio	n changes.		-						
		The REST API uses OAuth 2.0 to validate access. Use the resources under the Token group to get a password-granted or custom access token, to refresh a token, or to revoke a token. You must include a valid access token in the Authorization: Bearer header on any HTTPS request from your API client.											
		Before usi	ing the REST API, you	u need to finis	sh the device in	itial setup. You can complete the	device initial setup either throu	ugh UI or thro	ough Initial	Provision API.			
		You can a	lso refer to this page	for a list of A	PI custom erro	r codes. (Additional errors might e	exist.)						
		NOTE: The purpose of the API Explorer is to help you learn the API. Testing calls through the API Explorer requires the creation of access locks that might inte that you use the API Explorer on a non-production device.							at might interfe	terfere with regular operation. We recommend			
		Cisco mai otherwise	kes no guarantee that improve the API bas	t the API vers ed on user fe	ion included or edback.	this Firepower Threat Device (the	e "API") will be compatible with	h future relea	ases. Cisco	o, at any time in	its sole discre	tion, may	modify, enhance or
		AAASe	tting							Show,	Hide List Op	erations	Expand Operations
		ASPath	List							Show/	Hide List Op	erations	Expand Operations
		Access	Policy							Show/	Hide List Op	erations	Expand Operations
		Active	DirectoryRealm							Show/	Hide List Op	erations	Expand Operations
		Activel	JserSessions							Show/	Hide List Op	erations	Expand Operations
		AnyCo	nnectClientPro	file						Show/	Hide List Op	erations	Expand Operations
		AnyCo	nnectPackageF	ile						Show/	Hide List Op	erations	Expand Operations

圖2.API Explorer Web使用者介面。

步驟 3.運行GET呼叫以獲取訪問策略ID。

Acces	sPolicy	Show/Hide	List Operations	Expand Operations
GET	/policy/accesspolicies/{parentId}/accessrules			
POST	/policy/accesspolicies/{parentId}/accessrules			
DELETE	/policy/accesspolicies/{parentId}/accessrules/{objId}			
GET	/policy/accesspolicies/{parentld}/accessrules/{objld}			
PUT	/policy/accesspolicies/{parentld}/accessrules/{objld}			
GET	/policy/accesspolicies			
GET	/policy/accesspolicies/{objld}			

圖3.訪問策略類別。

步驟 4.您必須點選TRY IT OUT!才能檢索API響應。

Firepower Device Man	ager Monitoring Policies Objects Device: firepower	S₂ (♣) (∅) (?) (€) administrator
FTD REST API 🔶	"message": "string", "internal_error_code":)	•
API Explorer		
Error Catalog		<i>k</i>
	520 Model Example Valu f "status_code": 0, "status_code": 0, "stat	•
	TRY/FOUT ott /policy/accesspolicies/(objid)	
	Put /policy/accesspolicies/{objid}	

圖4.TRY IT OUT!運行API呼叫的按鈕。

步驟 5.將資料從JSON響應正文複製到記事本。以後,您必須使用訪問控制策略ID。

Firepower Device Mana	jer Monitoring Policies Objects Device: firepower	\triangleright	0	?	•	admin Administrator	×
FTD REST API ←	TRY IT OUTI				le.		
Error Catalog	Curl curl -X GETheader 'Accept: application/json' 'https://10.88.243.61:44370/api/fdm/v6/policy/accesspolicies Request URL						
	https://10.88.243.61:44370/api/fdm/v6/policy/accesspolicies Response Body						
	<pre>"hitCount": { "hitCount": 0, "firstHitTimeStamp": "", "lastHitTimeStamp": "", "lastFHitTimeStamp": "",</pre>						Ŷ
	<pre>"type": "hitcount" }, "type": "accessdefaultaction"), "sslPolicy": null, "certVisibilityEnabled": false,</pre>						
	<pre>"networkAnalysisPolicy": null, "advancedSettings": { "dnsReputationEnforcementEnabled": true, "type": "advancedSettings" .</pre>						
	"id": "72865bc-c557-43fe-bcf-96b79b3475b3", "identityPolicySetting": null, "securityIntelligence": null, "type": "accesspolicy",						

步驟 6.在API資源管理器上查詢並開啟TimeRange類別以顯示不同的API呼叫。

Firepower Device Mar	hager Monitoring Policies Objects Device: firepower	6.	0	?	•	admin Administrato	ŕ
FTD REST API ←	StandardAccessList			Show	/Hide	List Operations	Expand Operations
	StandardCommunityList			Show	/Hide	List Operations	Expand Operations
API Explorer	SyslogServer			Show	/Hide	List Operations	Expand Operations
Error Catalog	SystemInformation			Show	/Hide	List Operations	Expand Operations
	Telemetry			Show	/Hide	List Operations	Expand Operations
	TestDirectory			Show	/Hide	List Operations	Expand Operations
	TestIdentityServicesEngineConnectivity			Show	/Hide	List Operations	Expand Operations
	TestIdentitySource			Show	/Hide	List Operations	Expand Operations
	TimeRange			Show	/Hide	List Operations	Expand Operations
	TimeZoneObjects			Show	/Hide	List Operations	Expand Operations
	TimeZoneSettings			Show	/Hide	List Operations	Expand Operations
	TimeZones			Show	/Hide	List Operations	Expand Operations
	Token			Show	/Hide	List Operations	Expand Operations
	TrafficInterruptionReasons			Show	/Hide	List Operations	Expand Operations
	TrafficUser			Show	/Hide	List Operations	Expand Operations
	TrafficUserGroup			Show	/Links	List Operations	Evnand Operations

圖6.時間範圍類別。

步驟 7.使用POST API呼叫,建立任意多個TimeRange對象。

Firepower Device Ma	nager Monitoring Policies Objects Device: firepo	wer		admin Administrator
	TimeRange			Show/Hide List Operations Expand Operations
TD RESTAPI	GET /object/timeranges			
API Explorer	Post /object/timeranges			
Fror Catalog	Implementation Notes This API call is not allowed on the standby unit in an HA pair. Response Class (Status 200)			
	Model Example Value			
	<pre>"effectiveEndOateTime": "string", "recurrenceList": [{ "days": ["nou"], "recurrenceType": "OxILY_INTERVAL", "dallyStartTime": "oxILN_INTERVAL", "dallyStartTime": "string", "rangeStartTime": "string",</pre>			•
	Response Content Type application/json Parameters			
	Parameter Value body (required)	Description Para body	meter Type Data	Model Example Value

圖7.時間範圍POST呼叫。

在此處找到幾個格式示JSON例,以建立兩個不同的TimeRange對象。

對象1:

<#root>

```
"name": "
range-obj-1
",
"recurrenceList": [
    {
      "days": [
        "MON",
        "TUE",
        "WED",
        "THU",
        "FRI"
      ],
      "recurrenceType": "DAILY_INTERVAL",
      "dailyStartTime": "
00:00
۳,
      "dailyEndTime": "
23:50
```

", "type": "recurrence" }], "type": "timerangeobject" }

對象2:

<#root>

{

"name": "

```
range-obj-2
```

```
",

"recurrenceList": [

{

"days": [

"MON"

],

"recurrenceType": "DAILY_INTERVAL",

"dailyStartTime": "
```

12:00

", "dailyEndTime": "

13:00

```
",
"type": "recurrence"
}
```

], "type": "timerangeobject", }

◆ 注意:請記得按TRY IT OUT! 鍵以運行API呼叫。

步驟 8.運行調用GET,以獲取TimeRange對象ID。

Firepower Device Manager	Monitoring Policies Objects Device: firepower	\odot	e admin Administrator	
FTD REST API 🔶	https://10.88.243.61:44370/api/fdm/v6/object/timeranges			-
API Explorer	tesponse Body			
Error Catalog	<pre>"effectiveEndDateTime: "Never End", "eccurrenceList": [("days": ["DUT, "TUT, "NEU", "THU", "FEU", "THU", "FEU", "ABUT, "FRI"], "necurrenceType": "DAILY_INTERVAL", "dailyStartIme": "00:00", "dailyStartIme": "00:00", "dailyEndTime": "23:50", "timeRangeObjectId": 3, "timeRangeObjectId": 3, "id": "TimeenageObject", "links": ("dailyStartImenageObject", "linkstite</pre>			
	Response Code			
	tesponse Headers ("accept-ranges": "bytes",			

圖8.從時間範圍獲取GET響應。

步驟 9.按一下Deploy「OK」按鈕以驗證並應用您的變更。

CISCO. Firepow	er Devic	e Manager	囧 Monitoring	Ø Policies	:≛⊒: Objects	Device: firepower	Adminin Adminin	strator		
FTD REST API	~	Firepov	Firepower Threat Defense REST API							
API Explorer		The followi	ng is a list of resou	rces you can u	se for program	matic access to the device using t	e Firepower Threat Defense REST API. The resources are organized into groups of re	elated resources. Click a		
Error Catalog		group nam documenta	e to see the availab tion for the resourc	le methods an e.	d resources. Cli	ick a method/resource within a gr	up to see detailed information. Within a method/resource, click the Model link under	Response Class to see		
		You can tes POST calls /operationa deploymen	t the various metho create real objects I/deploy resource i t after you make an	ods and resour . PUT calls mo in the Deploym y configuration	ces through this dify existing obj ent group. Altho changes.	s page. When you fill in parameter jects. DELETE calls remove real of ough some changes, such as to th	and click the Try it Out! button, you interact directly with the system. GET calls retrie ects. However, most changes do not become active until you deploy them using the management IP address and other system-level changes, do not require deployment	eve real information. POST nt, it is safer to do a		
		The DECT				······				

圖9.API資源管理器中提供了「部署」按鈕。

步驟 10.驗證您剛剛建立的配置,然後按一下 DEPLOY NOW.

	Last Deployment Completed Successfully			
	Deployed Version (19.Jul 2023 06:32 PM)	Pending Version		ND
•			_	A
	- - - -	recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 00:00 recurrenceList.dailyEndTime: 23:50 effectiveStartDateTime: Started effectiveEndDateTime: Never End timePerseDistatti .		
	-	name: range-obj-1		
Ð	- - timerangeobject Added: <i>range-obj-2</i>	name: range-obj-1	5	
Ð	- - timerangeobject Added: <i>range-obj-2</i> - - - - - -	recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:00 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 name: range-obj-2		
Ð	- - timerangeobject Added: range-obj-2 - - - - -	recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:00 effectiveEndDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 name: range-obj-2		•

圖10.FDM掛起更改視窗。

步驟 11.查詢類AccessPolicy,然後開啟POST呼叫,以便建立基於時間的訪問控制規則。

cisco. Firepower Devi	ice Manager Monitoring Policies Objects Device: firepower Device: firepower
FTD REST API +	Cisco makes no guarantee that the API version included on this Firepower Threat Device (the "API") will be compatible with future releases. Cisco, at any time in its sole discretion, may modify, enhance or otherwise improve the API based on user feedback.
API Explorer	AAASetting Show/Hide List Operations Expand Operations
Error Catalog	ASPathList Show/Hide List Operations Expand Operations
	AccessPolicy Show/Hide List Operations Expand Operations
	GET /policy/accesspolicies/{parentId}/accessrules
	post /policy/accesspolicies/{parentid}/accessrules
	DELETE /policy/accesspolicies/{parentld}/accessrules/{objid}
	cer /policy/accesspolicies/{parentld}/accessrules/{objld}
	policy/accesspolicies/{parentld}/accessrules/{objld}
	art /policy/accesspolicies
	GET /policy/accesspolicies/{objld}
	/policy/accesspolicies/{objld}
	ActiveDirectoryRealm Show/Hide List Operations Expand Operations
	ActiveUserSessions Show/Hide List Operations Expand Operations
	AnyConnectClientProfile Show/Hide List Operations Expand Operations

圖11.訪問策略POST呼叫。

在此處找到JSON一個格式示例,以建立允許流量從內部區域流向外部區域的基於時間的ACL。

確保使用正確的時間範圍對象ID。

```
{
  "name": "test_time_range_2",
  "sourceZones": [
    {
          "name": "inside_zone",
          "id": "90c377e0-b3e5-11e5-8db8-651556da7898",
          "type": "securityzone"
    }
  ],
  "destinationZones": [
    {
      "name": "outside_zone",
      "id": "b1af33e1-b3e5-11e5-8db8-afdc0be5453e",
      "type": "securityzone"
    }
  ],
  "ruleAction": "PERMIT",
  "eventLogAction": "
LOG_FLOW_END
  "timeRangeObjects": [
    {
    "id": "
718e6b5c-2697-11ee-a5a7-57e37203b186
...
    "type": "timerangeobject",
```

```
"type": "timerangeobject"
"name": "Time-test2"
}
],
"type": "accessrule"
}
```

Signature State Sta

步驟 12.部署更改以應用新的基於時間的ACL。Pending Changes提示必須顯示步驟10中所用的時 間範圍對象。

iger (admin Administrator
https://10.	Pending Changes		
Response E	Last Deployment Completed Successfully 19 Jul 2023 07:05 PM. See Deployment History		
{ "versio	Deployed Version (19 Jul 2023 07:05 PM)	Pending Version	C LEGEND
"name": "ruleId	Access Rule Added: test_time_range		· ·
"source { "ve		<pre>logFiles: false eventLogAction: LOG_FLOW_END rule1d: 268435460 nume: test time range</pre>	
"id "ty }	timeRangeObjects: - sourceZones:	range-obj-2	
], "destin	- destinationZones: -	inside_zone outside zone	
"ve "na "id	Access Policy Edited: NGFW-Access-Policy		
,)	More actions $$	CANCEL	DEPLOY NOW
Response (
200			

圖12.「FDM掛起更改」視窗顯示新規則。

第13步(可選)。如果要編輯ACL,可以使用調用PUT,並編輯時間範圍ID。

CISCO. Firepower Device Manag	ger Monito	ring Policies	Objects	Device: firepo	wer		(ک	2) ()	•	admin Administrator	~
	GET /policy/acce	sspolicies/{parent	d}/accessru	iles/{objld}								
FTD REST API ←	PUT /policy/acce	sspolicies/{parent	d}/accessru	iles/{objld}								
API Explorer												
Error Catalog	Implementation I This API call is not a Response Class Model Examp	Notes allowed on the stand (Status 200) le Value	by unit in an H	HA pair.								
	"name": "s }], "sourcelletwork { "id": "str "type": "s "version": "name": "s }],	tring" s": [ing", tring", "string", tring"										•
	Response Content	Type application/json	~									
	Parameter	Value			Description	Param	neter Type	Data Typ	2e			
	parentId	(required)				path		string				
	objId	(required)				path		string				

圖13.訪問策略PUT呼叫。

在此處查詢JSON「格式」示例為了編輯時間範圍,可以使用呼叫收集這些時間範圍IDGET。

<#root>

```
{
    "version": "flya3jw7wvqg7",
    "name": "test_time_range",
    "ruleId": 268435460,
    "sourceZones": [
    {
        "version": "lypkhscmwq4bq",
        "name": "inside_zone",
    }
}
```

```
"id": "90c377e0-b3e5-11e5-8db8-651556da7898",
"type": "securityzone"
}
],
"destinationZones": [
{
"version": "pytctz6vvfb3i",
"name": "outside_zone",
"id": "b1af33e1-b3e5-11e5-8db8-afdc0be5453e",
"type": "securityzone"
}
],
"sourceNetworks": [],
"destinationNetworks": [],
"sourcePorts": [],
"destinationPorts": [],
"ruleAction": "PERMIT",
"eventLogAction": "LOG_FLOW_END",
"identitySources": [],
"users": [],
"embeddedAppFilter": null,
"urlFilter": null,
"intrusionPolicy": null,
"filePolicy": null,
"logFiles": false,
"syslogServer": null,
"destinationDynamicObjects": [],
"sourceDynamicObjects": [],
"timeRangeObjects": [
{
"version": "i3iohbd5iufol",
"name": "range-obj-1",
"id": "
718e6b5c-2697-11ee-a5a7-57e37203b186
۳,
"type": "timerangeobject"
}
],
"id": "0f2e8f56-269b-11ee-a5a7-6f90451d6efd",
"type": "accessrule"
}
```

步驟 14.部署和驗證您的更改。

ager I	Р	ending Changes		0 X	2 Communistrator
"ve "na "id "ty }	0	Last Deployment Completed Successfully 19 Jul 2023 07:19 PM. See Deployment History			
], "14", "		Deployed Version (19 Jul 2023 07:19 PM)	Pending Version	C LEGEND	
"type": "links" "self	0	Access Rule Edited: test_time_range		Â	-11ee-a5a7-8de2389540a7"
}	0	Access Rule Added: test_time_range_2			
3		-	<pre>logFiles: false eventLogAction: LOG_FLOW_END</pre>		
Response (-	ruleId: 268435461		
200		-	name: test_time_range_2		
		-	range-obj-1		
Response F		sourceZones:			
7		-	inside_zone		
accept-r		destinationZones:			
"connecti		-	outside_zone		
"content- "date": " "expires" "keep-ali "pragma":	0	Access Policy Edited: NGFW-Access-Policy			
"server": "strict-t "transfer "vary": " "x-conter	N	MORE ACTIONS ~	CANCEL	DEPLOY NOW	
x-frame- "x-xss-pro }	tect:	ion": "1; mode-blóck"			

圖14.「FDM掛起更改」視窗顯示對象的更改。

驗證

1.運行命令show time-range,以驗證時間範圍對象的狀態。

<#root>

>

show time-range

time-range entry:

```
range-obj-1
```

(

active

)

```
periodic weekdays 0:00 to 23:50 time-range entry:
```

```
range-obj-2
```

(

```
inactive
```

)

periodic Monday 12:00 to 13:00

<#root>

>

show access-control-config

```
========[ NGFW-Access-Policy ]=============
Description :
=======[ Default Action ]============
Default Action : Block
Logging Configuration
DC : Enabled
Beginning : Disabled
End : Disabled
Rule Hits : 0
Variable Set : Object missing: 76fa83ea-c972-11e2-8be8-8e45bb1343c0
===[ Security Intelligence - Network Whitelist ]====
===[ Security Intelligence - Network Blacklist ]====
Logging Configuration : Disabled
DC : Disabled
=====[ Security Intelligence - URL Whitelist ]======
=====[ Security Intelligence - URL Blacklist ]======
Logging Configuration : Disabled
DC : Disabled
=====[ Rule Set: admin_category (Built-in) ]=======
=====[ Rule Set: standard_category (Built-in) ]=====
-----[ Rule: test_time_range ]------
Action :
Allow
Source ISE Metadata :
Source Zones : inside_zone
Destination Zones : outside_zone
Users
URLs
Logging Configuration
DC : Enabled
Beginning : Disabled
End : Enabled
Files : Disabled
Safe Search : No
Rule Hits : 0
Variable Set : Object missing: 76fa83ea-c972-11e2-8be8-8e45bb1343c0
Time Range :
range-obj-1
Daily Interval
StartTime : 00:00
EndTime : 23:50
Days : Monday, Tuesday, Wednesday, Thursday, Friday
```

3.運行System Support Trace調試,以確認流量是否達到正確的規則。

<#root>

> system support trace

Enable firewall-engine-debug too? [n]: y Please specify an IP protocol: tcp Please specify a client IP address: Please specify a client port: Please specify a server IP address: Please specify a server port: 443 Monitoring packet tracer and firewall debug messages

10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 New firewall session 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 app event with app id no change, url no chang 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Starting with minimum 1, 'test_time_range', a 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1

match rule order 1, 'test_time_range', action Allow

10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 MidRecovery data sent for rule id: 268435460, 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1

allow action

10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Packet 1930048: TCP *****S*, 07/20-18:05:06. 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Session: new snort session 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 AppID: service: (0), client: (0), payload: (0 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Firewall: starting rule matching, zone 2 -> 1 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1

Firewall: allow rule, 'test_time_range', allow

10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Policies: Network 0, Inspection 0, Detection 10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Verdict:

pass

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)。