在FMC的PBR的擴展ACL上配置FQDN對象

目錄

簡介

本檔案介紹在延伸存取清單(ACL)中設定FQDN物件以用於原則型路由(PBR)的程式。

必要條件

需求

思科建議您瞭解以下產品：

- 安全防火牆管理中心(FMC)
- 安全防火牆威脅防禦(FTD)
- PBR

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 適用於VMware的Firepower威脅防禦7.6.0版
- 適用於VMware的安全防火牆管理中心7.6.0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

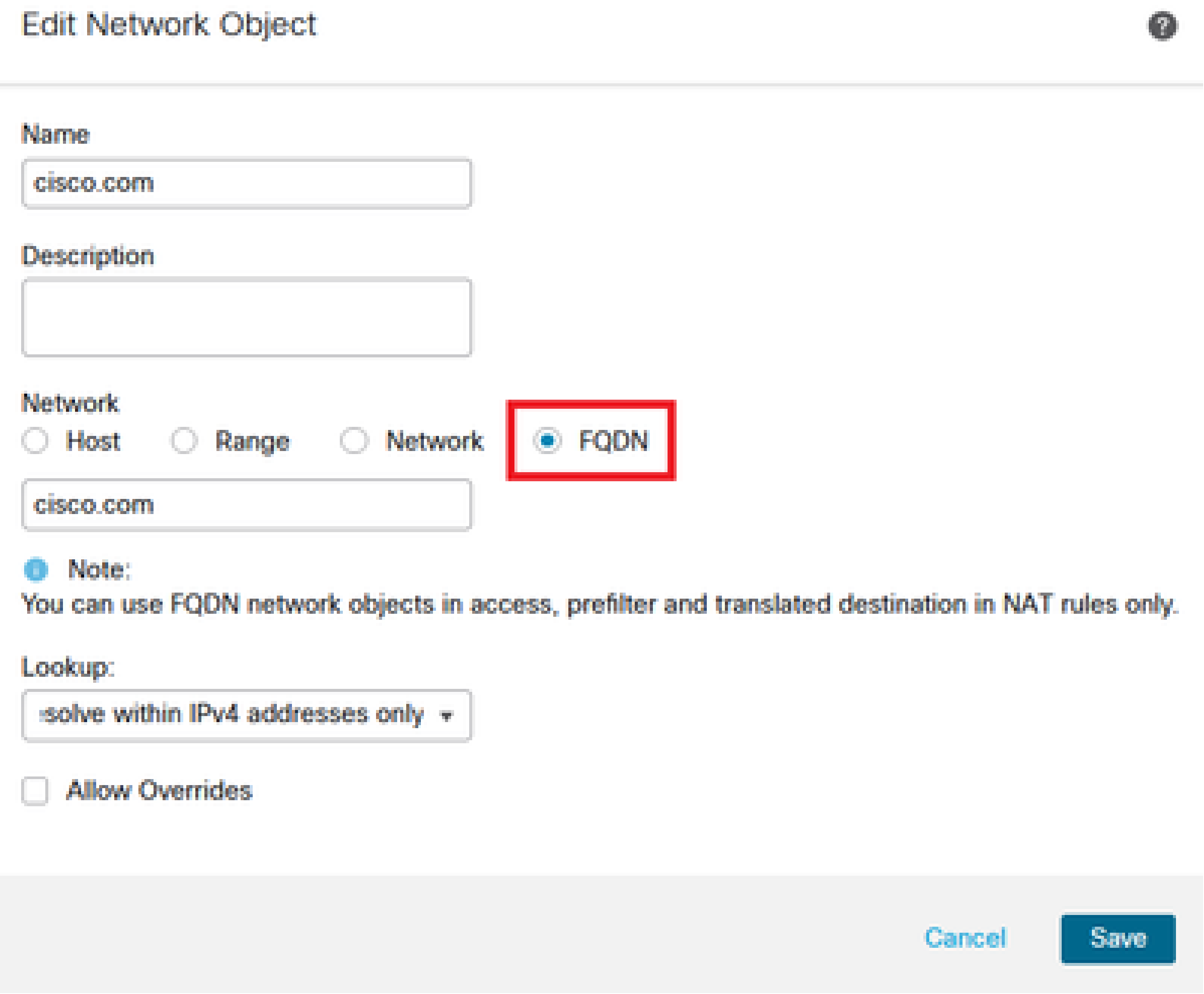
目前，FTD不允許使用思科錯誤ID CSCuz98322上提到的完整網域名稱(FQDN)物件在非HTTP流量上進行過濾。

ASA平台支援此功能，但是，在FTD上只能過濾網路和應用。

您可以使用此方法將FQDN對象增加到擴展訪問清單以配置PBR。

設定

步驟 1.根據需要建立FQDN對象。



Edit Network Object

Name: cisco.com

Description:

Network: ○ Host ○ Range ○ Network ● FQDN

cisco.com

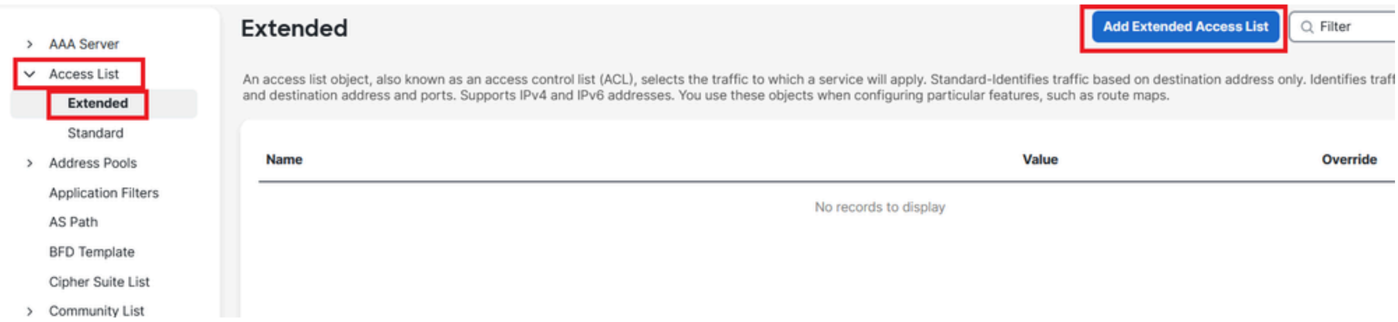
Note:
You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Lookup: solve within IPv4 addresses only

□ Allow Overrides

圖1.網路物件功能表

步驟 2.在Objects > Object Management > Access List > Extended下建立擴展訪問清單。



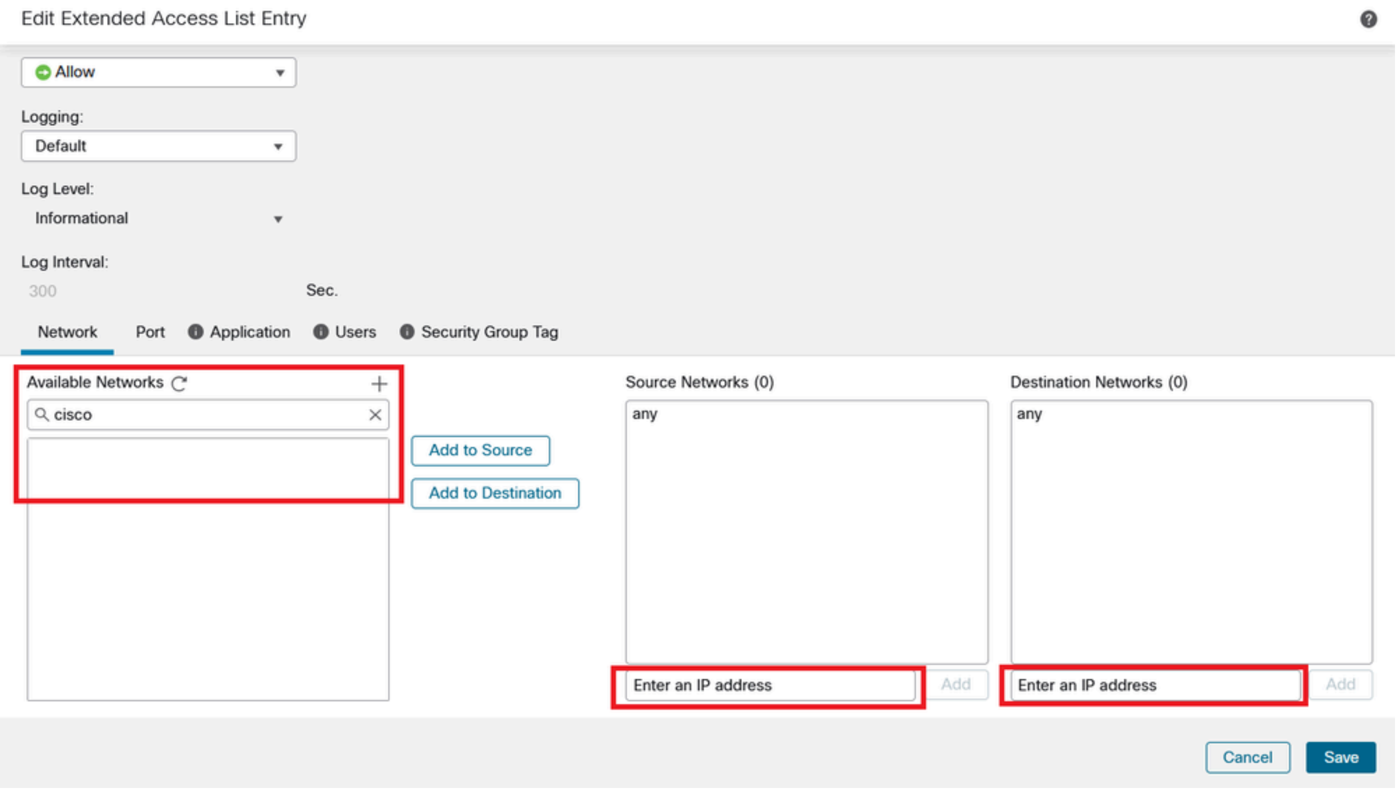
Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traff
and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

Name	Value	Override
No records to display		

圖2.擴展訪問清單選單

增加新規則時，請注意在搜尋網路對象以選擇源和目標時看不到配置的FQDN對象。



Edit Extended Access List Entry

Allow

Logging:
Default

Log Level:
Informational

Log Interval:
300 Sec.

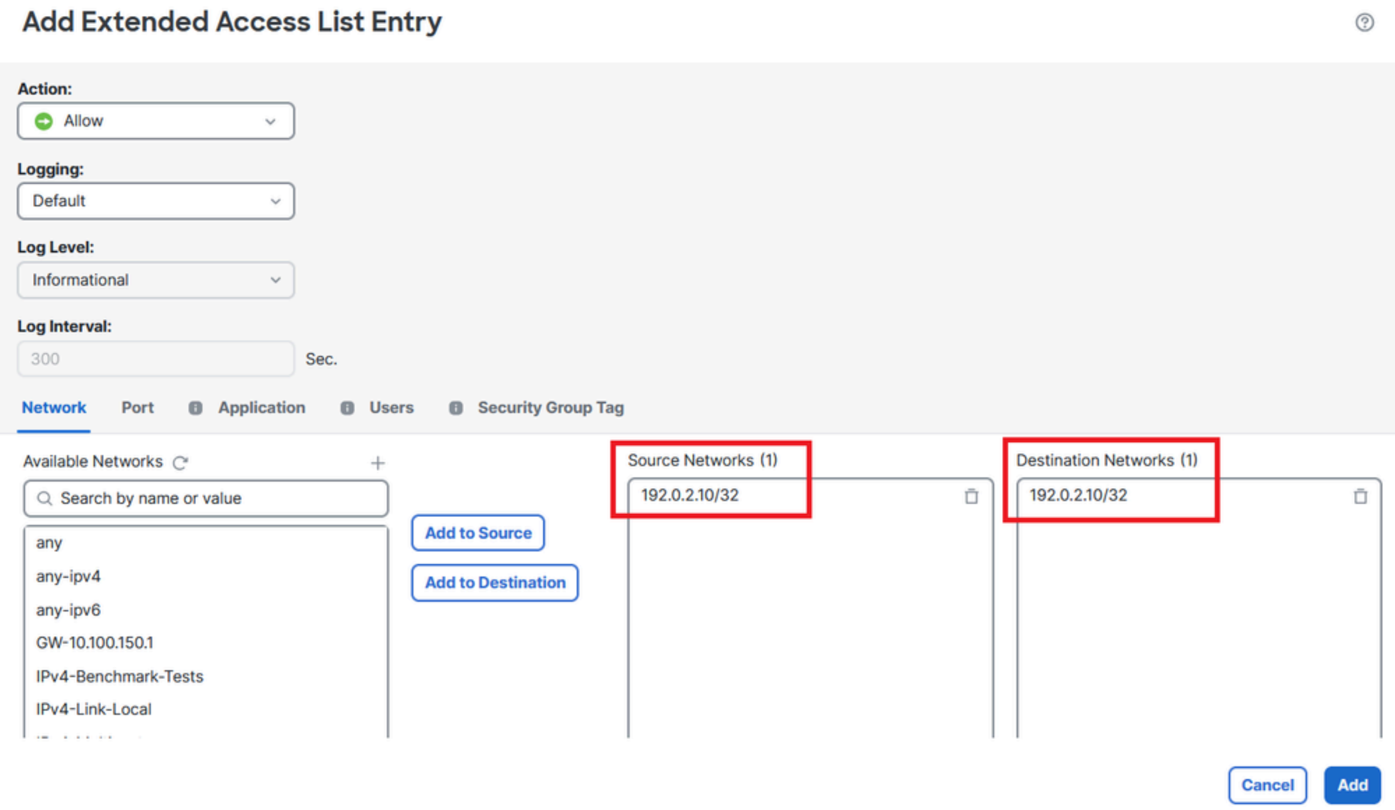
Available Networks
cisco

Source Networks (0)
any

Destination Networks (0)
any

圖3.新建擴展訪問清單規則選單

步驟 3.建立無法命中的規則，以便建立擴展ACL並可用於PBR配置。



Add Extended Access List Entry

Action: Allow

Logging: Default

Log Level: Informational

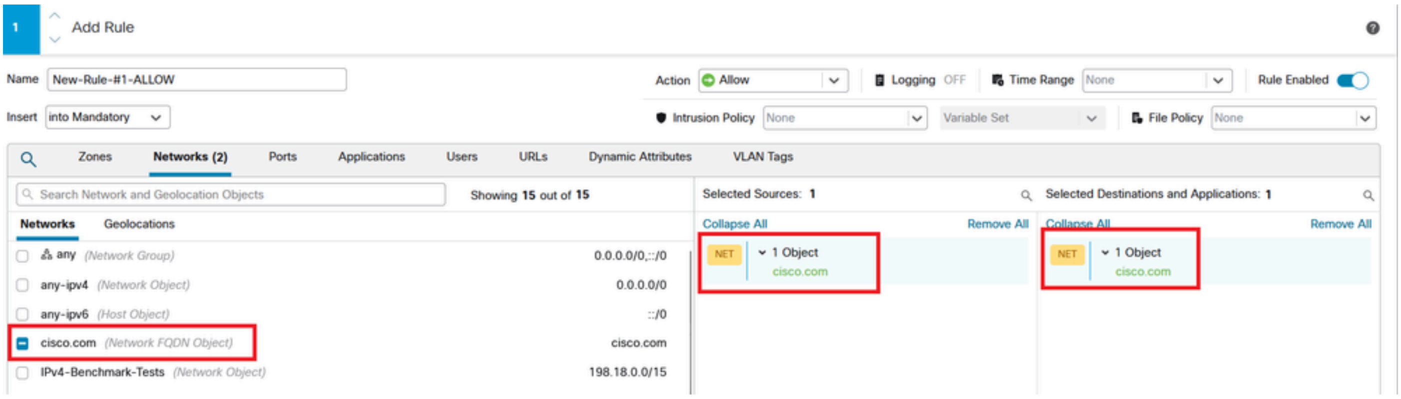
Log Interval: 300 Sec.

Source Networks (1): 192.0.2.10/32

Destination Networks (1): 192.0.2.10/32

圖4.無法命中的訪問清單規則配置

步驟 4.您需要在以FQDN物件為FTD目標的存取控制原則(ACP)上建立規則。FMC會將FQDN物件部署到FTD，以便您可以透過FlexConfig物件來參考它。



Add Rule

Name: New-Rule-#1-ALLOW

Insert: into Mandatory

Action: Allow

Logging: OFF

Time Range: None

Rule Enabled

Intrusion Policy: None

Variable Set

File Policy: None

Showing 15 out of 15

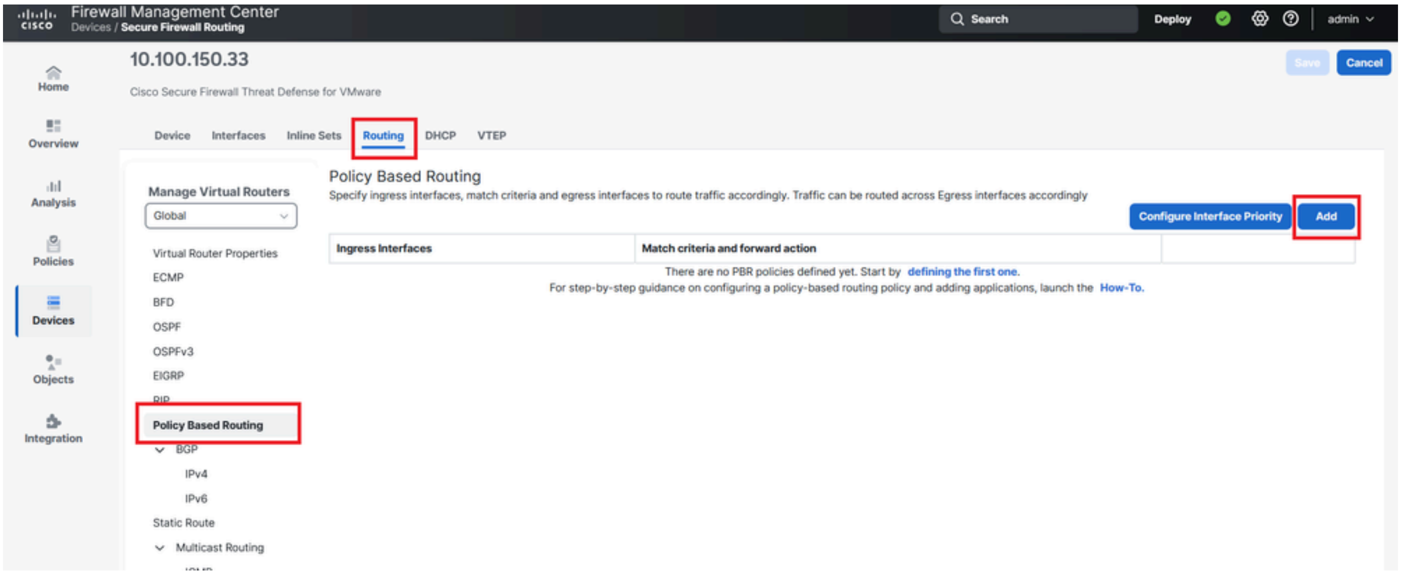
□	any (Network Group)	0.0.0.0/0,::/0
□	any-ipv4 (Network Object)	0.0.0.0/0
□	any-ipv6 (Host Object)	::/0
☑	cisco.com (Network FQDN Object)	cisco.com
□	IPv4-Benchmark-Tests (Network Object)	198.18.0.0/15

Selected Sources: 1 — 1 Object: cisco.com

Selected Destinations and Applications: 1 — 1 Object: cisco.com

圖5.具有FQDN物件的ACP規則

步驟 5.導覽至Devices > Device Management上的FTD，然後選擇Routing索引標籤，然後導覽至Policy Based Routing區段。



10.100.150.33

Cisco Secure Firewall Threat Defense for VMware

Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

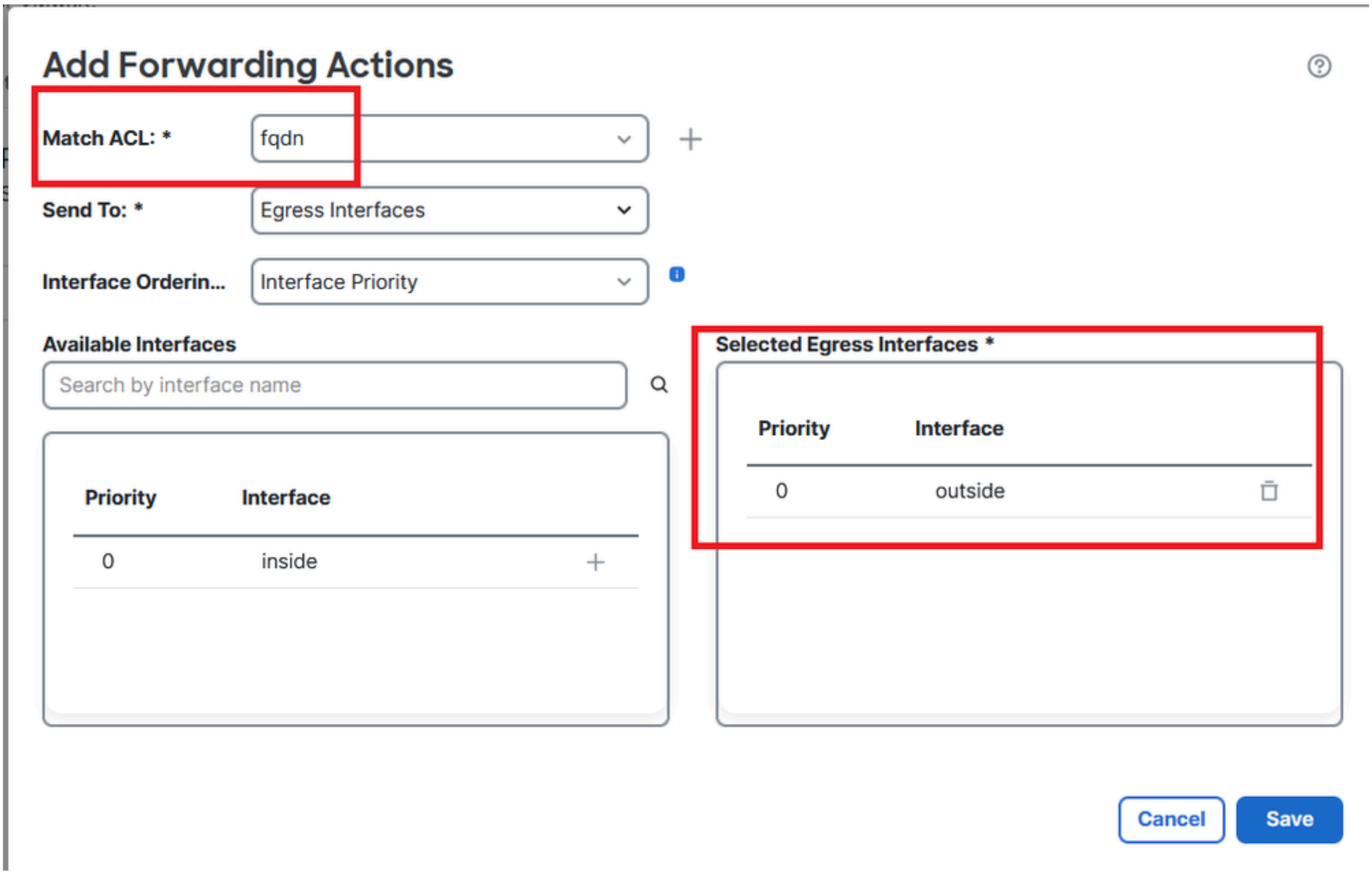
Ingress Interfaces	Match criteria and forward action

There are no PBR policies defined yet. Start by defining the first one.

For step-by-step guidance on configuring a policy-based routing policy and adding applications, launch the How-To.

圖6.PBR選單

步驟 6.使用之前配置的ACL在介面上配置PBR並進行部署。



Add Forwarding Actions

Match ACL: * fqdn

Send To: * Egress Interfaces

Interface Orderin... Interface Priority

Available Interfaces

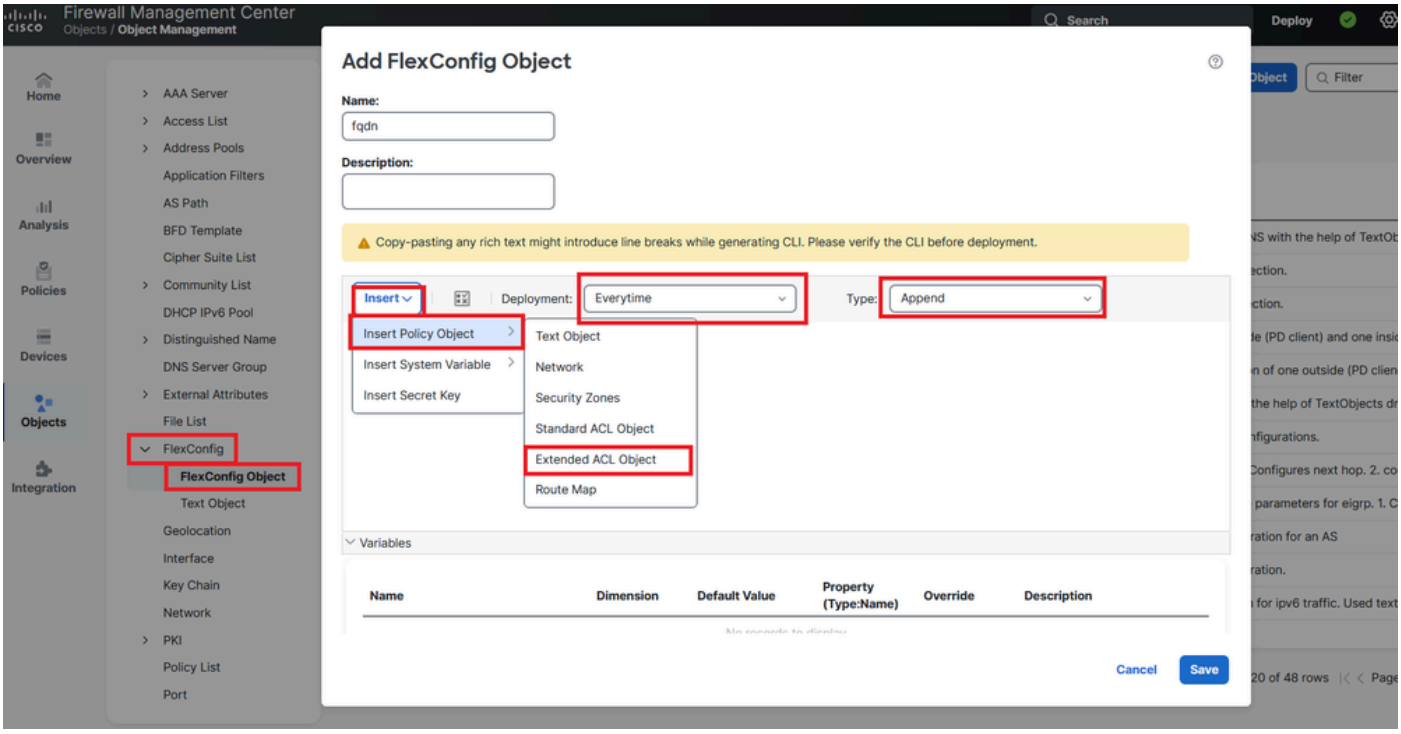
Priority	Interface
0	inside

Selected Egress Interfaces *

Priority	Interface
0	outside

圖7.PBR介面和ACL選擇選單

步驟 7.導航到對象>對象管理> FlexConfig >對象並建立新對象。



Add FlexConfig Object

Name: fqdn

Description:

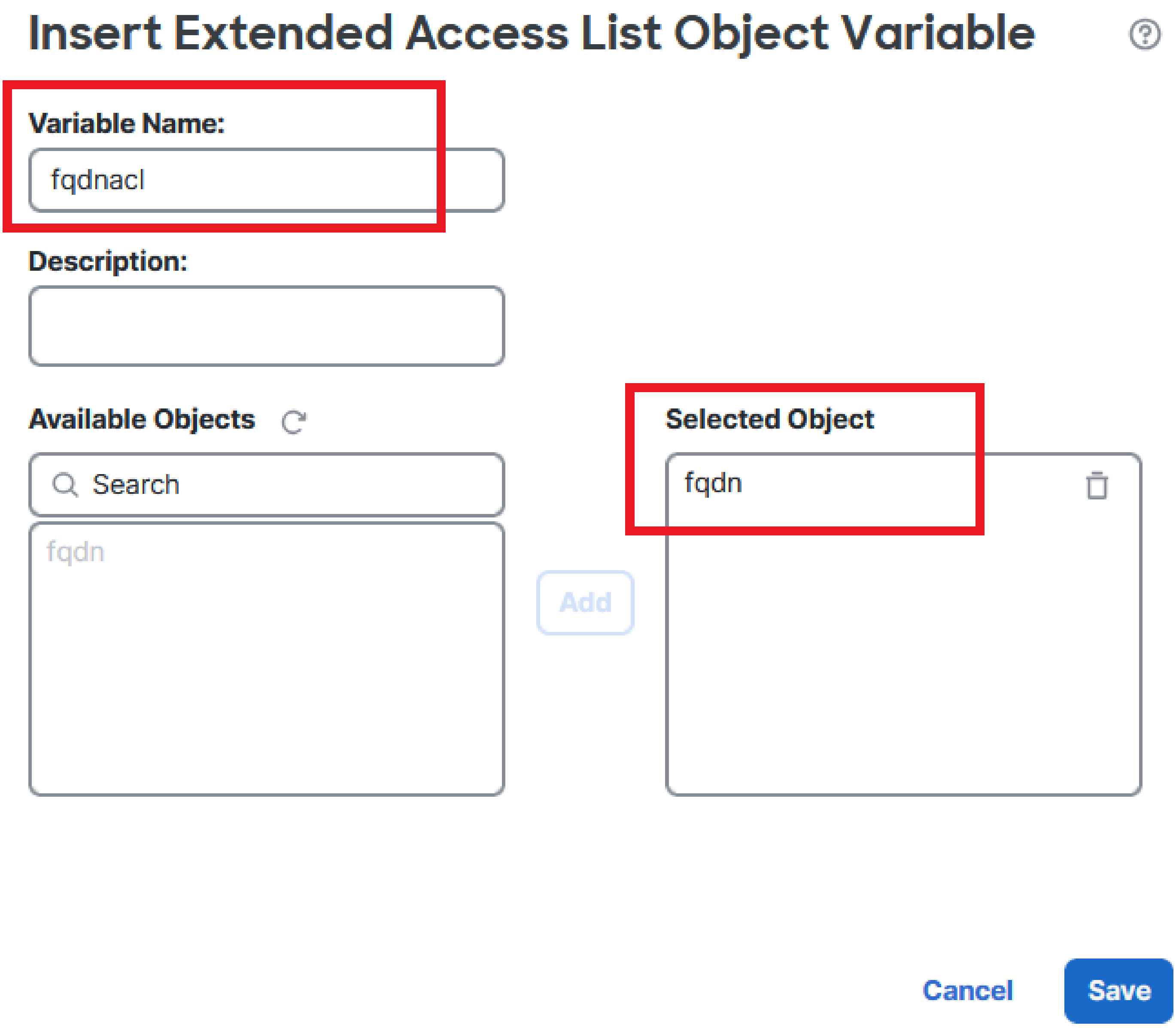
Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Everytime

Type: Append

圖8.FlexConfig物件組態功能表

步驟 8.選擇Insert > Extended ACL Object，命名變數並選擇之前建立的擴展ACL。該變數會以您使用的名稱加入。



Insert Extended Access List Object Variable

Variable Name: fqdnacl

Description:

Available Objects: fqdn

Selected Object: fqdn

圖9.FlexConfig物件的變數建立

步驟 9.為要用於ACL的每個FQDN對象輸入此行。

```
<#root>
access-li $




      extended permit ip any object
```

步驟 10.將FlexConfig對象儲存為Everytime > Append。

第11步：導航到Devices > FlexConfig下的FlexConfig Policy選單。

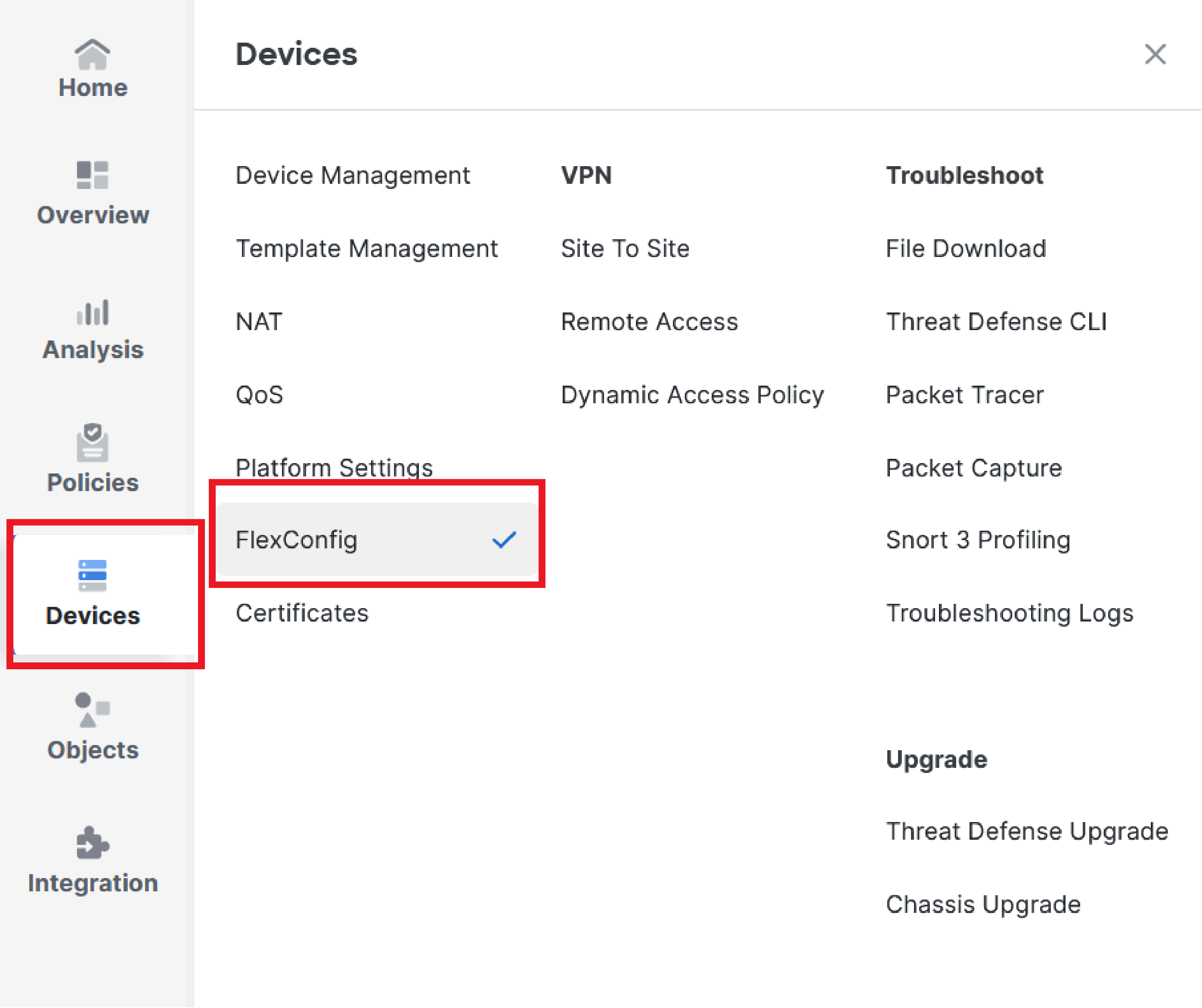
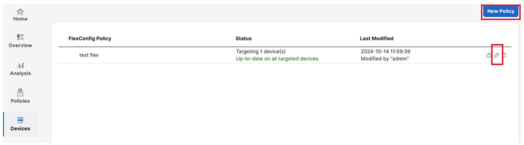


圖10.FlexConfig策略選單的路徑

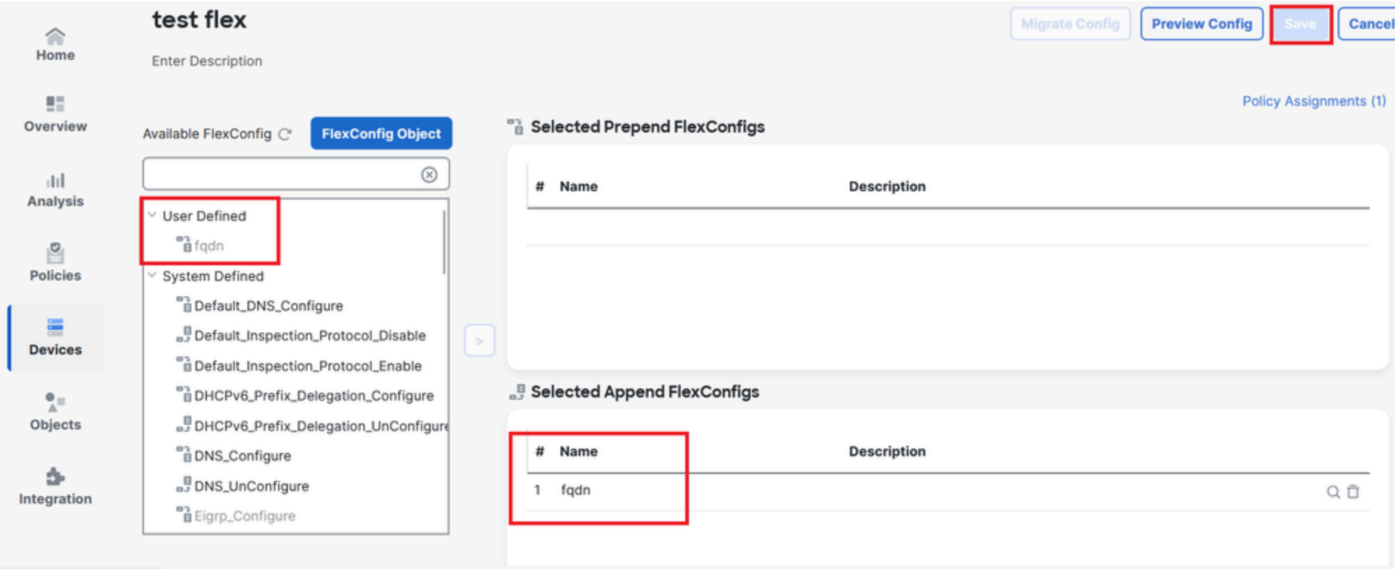
步驟 12.建立新的FlexConfig策略或選擇已分配給FTD的策略。



FlexConfig Policy	Status	Last Modified
test flex	Targeting 1 device(s) Up-to-date on all targeted devices	2024-10-14 11:59:39 Modified by "admin"

圖11.編輯或建立新的FlexConfig策略

步驟 13.將FlexConfig對象增加到策略，儲存和部署。



Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	fqdn	

圖12.已將FlexConfig對象增加到FlexConfig策略中

驗證

您的輸入介面具有帶有自動生成的路由對映的策略路由。

<#root>

```
firepower#

show run interface gi0/0


!
interface GigabitEthernet0/0
 nameif inside
 security-level 0
 ip address 10.100.151.2 255.255.255.0

policy-route route-map FMC_GENERATED_PBR_1727116778384
```

路由對映包含具有已使用目標介面的選定ACL。

<#root>

```
firepower#

show run route-map FMC_GENERATED_PBR_1727116778384


!
route-map FMC_GENERATED_PBR_1727116778384 permit 5

match ip address fqdn


set adaptive-interface cost outside
```

您的訪問清單包含用於參考的主機以及透過FlexConfig增加的其他規則。

```
<#root>

firepower#

show run access-list fqdn

access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10

access-list fqdn extended permit ip any object cisco.com
```

您可以從入口介面執行Packet Tracer作為源，以驗證您是否進入PBR階段。

```
<#root>

firepower#

packet-tracer input inside tcp 10.100.150.1 12345 fqdn cisco.com 443


Mapping FQDN cisco.com to IP address 72.163.4.161


[...]
Phase: 3

Type: PBR-LOOKUP


Subtype: policy-route
Result: ALLOW
Elapsed time: 1137 ns

Config:


route-map FMC_GENERATED_PBR_1727116778384 permit 5


 match ip address fqdn


 set adaptive-interface cost outside


Additional Information:


 Matched route-map FMC_GENERATED_PBR_1727116778384, sequence 5, permit


 Found next-hop 10.100.150.1 using egress ifc outside
```

```
[...]
Result:

input-interface: inside(vrfid:0)


input-status: up
input-line-status: up

output-interface: outside(vrfid:0)


output-status: up
output-line-status: up
Action: allow
Time Taken: 140047752 ns
```

常見問題

PBR在第二次部署後停止工作

請驗證訪問清單是否仍包含FQDN對象規則。

在這種情況下，您可以看到規則已不存在。

```
firepower# show run access-list fqdn
access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10
firepower#
```

驗證FlexConfig對象是否設定為Deployment： Everytime和Type： Append。該規則每次都應用於未來的部署。

FQDN未解析

嘗試對FQDN執行ping操作時，會收到有關主機名無效的消息。

```
<#root>

firepower#

ping cisco.com


                ^

ERROR: % Invalid Hostname
```

驗證DNS配置。您的伺服器組上必須有可訪問的DNS伺服器，並且域名查詢介面必須能夠訪問它們

。

<#root>

```
firepower#

show run dns


dns domain-lookup outside


DNS server-group DefaultDNS
DNS server-group dns

name-server 208.67.222.222



name-server 208.67.220.220


dns-group dns

firepower#

ping 208.67.222.222


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 208.67.222.222, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 170/202/280 ms
firepower#

ping cisco.com


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 72.163.4.161, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/140/190 ms.
```

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）。