Configura oggetto FQDN in ACL esteso per PBR in FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Problemi comuni](#)

- [PBR interrompe il funzionamento dopo una seconda distribuzione](#)
- [FQDN non risolto](#)

Introduzione

In questo documento viene descritta la procedura per configurare un oggetto FQDN in un elenco degli accessi esteso (ACL) da utilizzare in Policy Based Routing (PBR).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti prodotti:

- Centro gestione firewall protetto (FMC)
- Secure Firewall Threat Defense (FTD)
- PBR

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower Threat Defense per VMware versione 7.6.0
- Secure Firewall Management Center per VMware versione 7.6.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Al momento, l'FTD non consente il filtro sul traffico non HTTP utilizzando oggetti FQDN (Fully Qualified Domain Name), come indicato sull'ID bug Cisco CSCuz98322.

Questa funzionalità è supportata sulle piattaforme ASA, tuttavia, solo le reti e le applicazioni possono essere filtrate con FTD.

È possibile aggiungere un oggetto FQDN a un elenco degli accessi estesi per configurare PBR utilizzando questo metodo.

Configurazione

Passaggio 1. Creare gli oggetti FQDN in base alle esigenze.

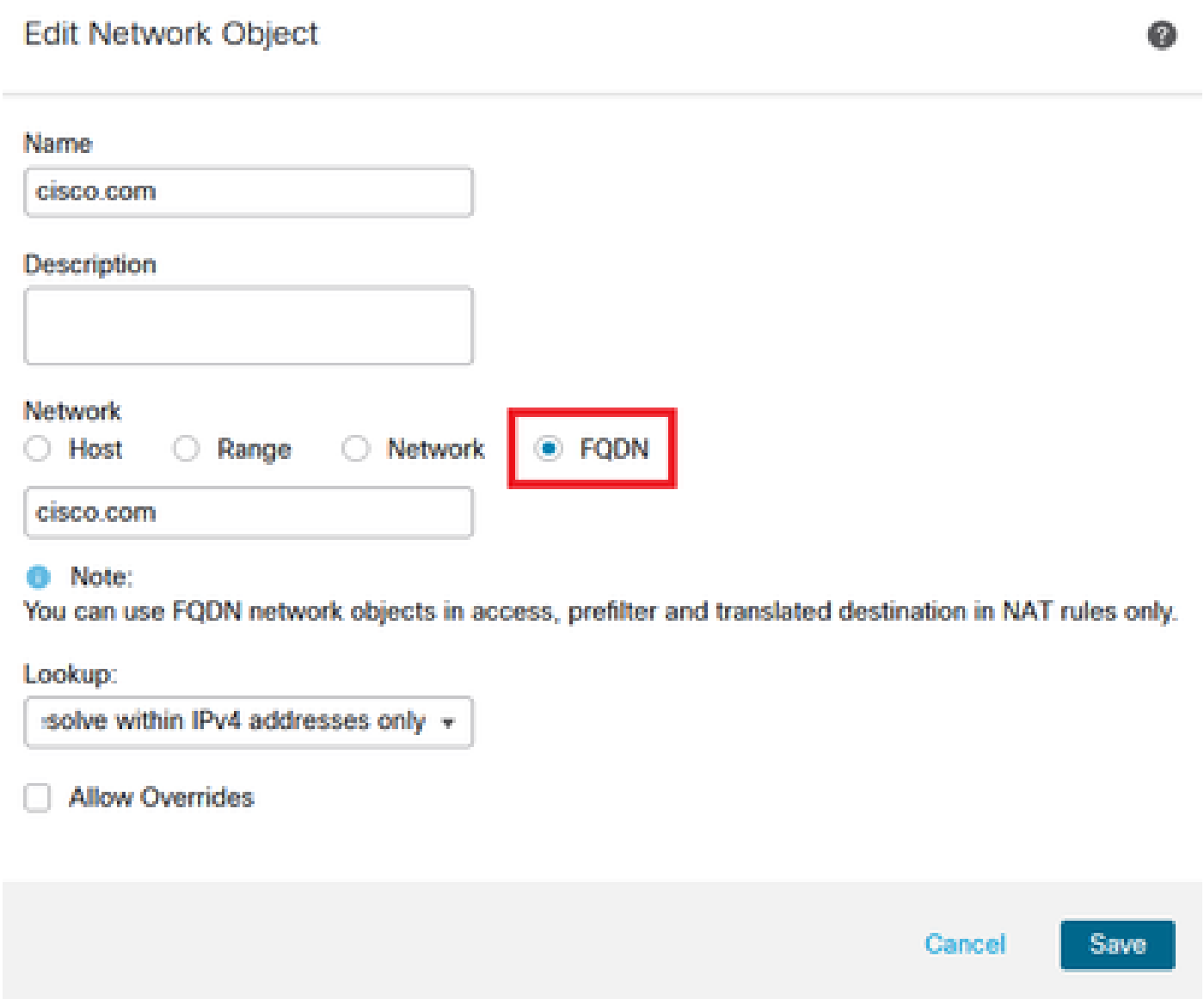

Immagine 1. Menu Oggetto di rete

Passaggio 2. Creare un elenco degli accessi esteso in Oggetti > Gestione oggetti > Elenco

accessi > Esteso.

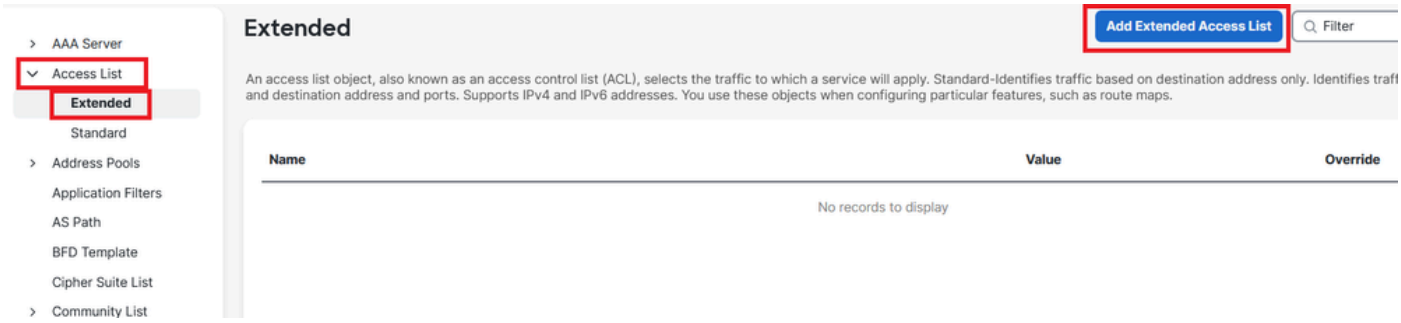

Immagine 2. Menu elenco accessi estesi

Quando si aggiunge una nuova regola, si noti che non è possibile visualizzare l'oggetto FQDN configurato durante una ricerca negli oggetti di rete per selezionare l'origine e la destinazione.

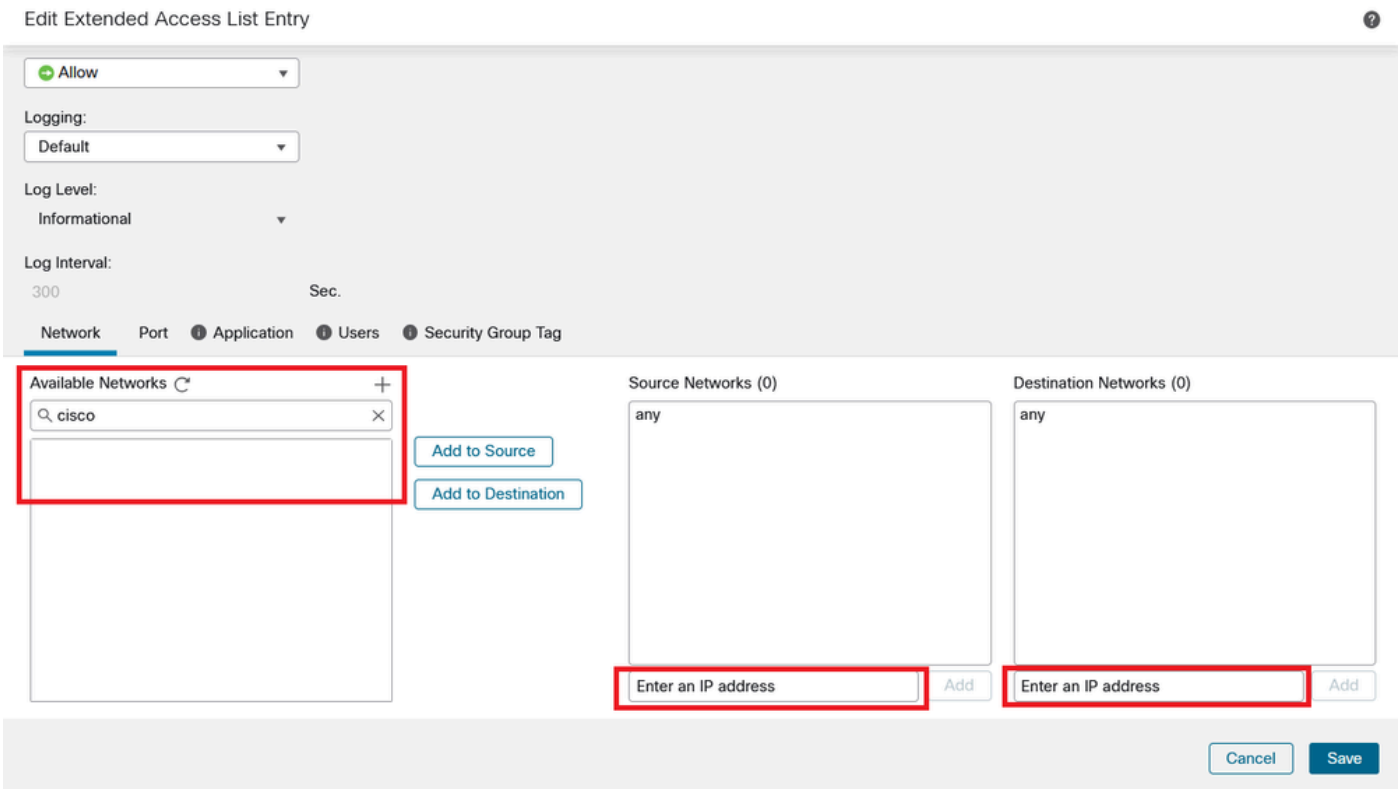

Immagine 3. Menu Nuova regola elenco accessi estesi

Passaggio 3. Creare una regola che non possa essere trovata, in modo che l'ACL esteso venga creato e sia disponibile per la configurazione PBR.

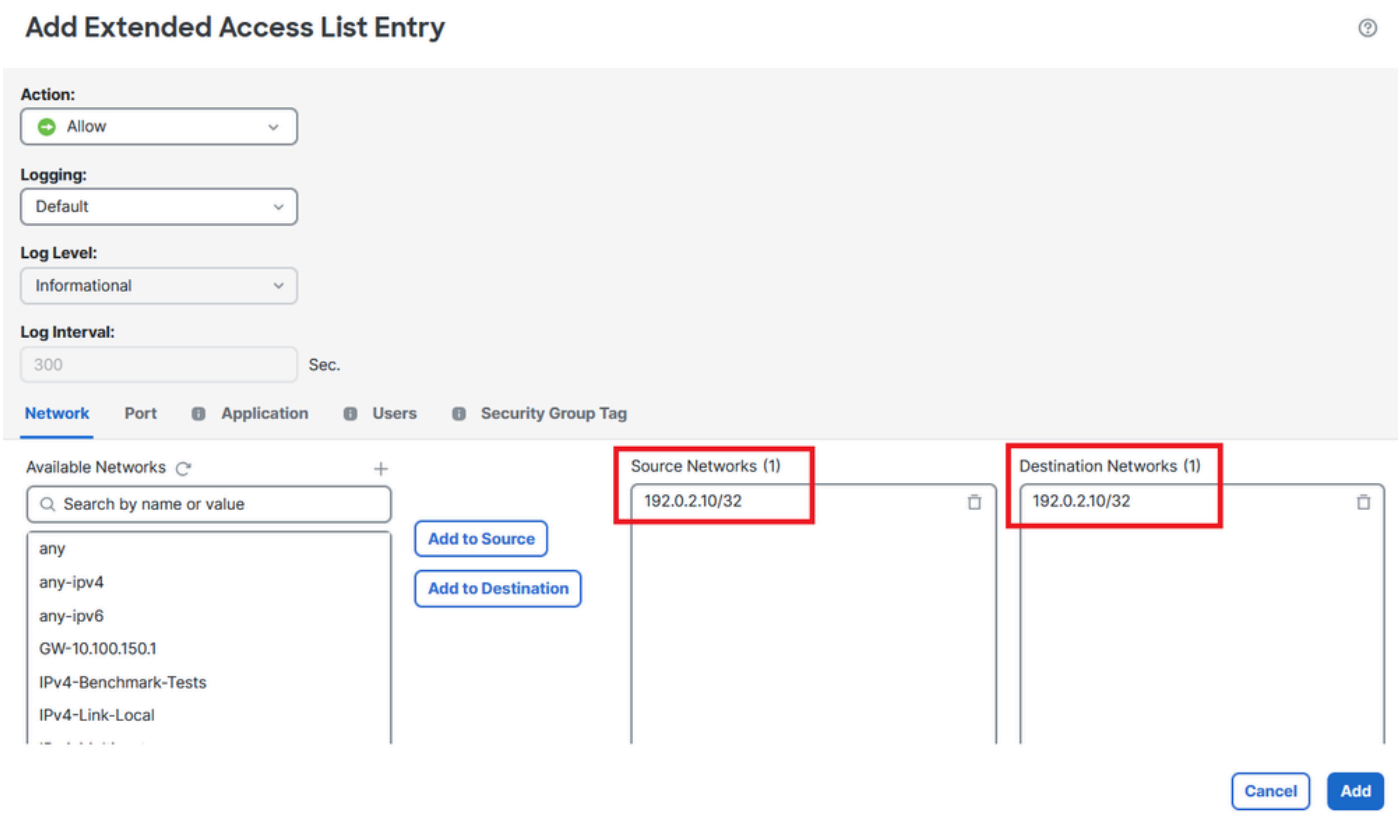

Immagine 4. Impossibile trovare la configurazione della regola dell'elenco accessi

Passaggio 4. È necessario creare una regola in Access-Control Policy (ACP) destinata all'FTD con l'oggetto FQDN. Il FMC distribuisce l'oggetto FQDN nell'FTD in modo che sia possibile farvi riferimento tramite un oggetto FlexConfig.

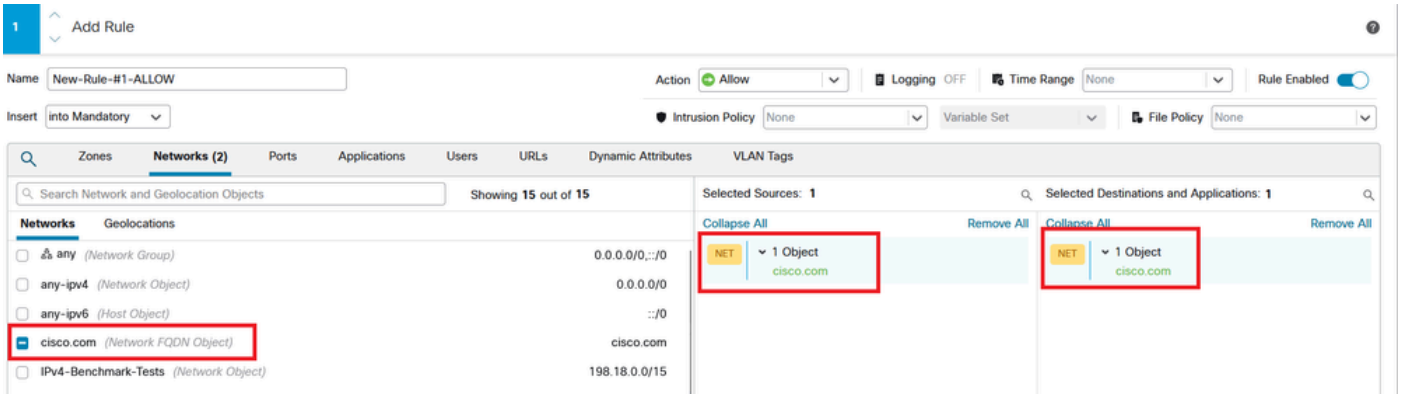

Immagine 5. Regola del provider di servizi di audioconferenza con oggetto FQDN

Passaggio 5. Passare a FTD su Dispositivi > Gestione dispositivi e selezionare la scheda Instradamento, quindi passare alla sezione Instradamento basato su policy.

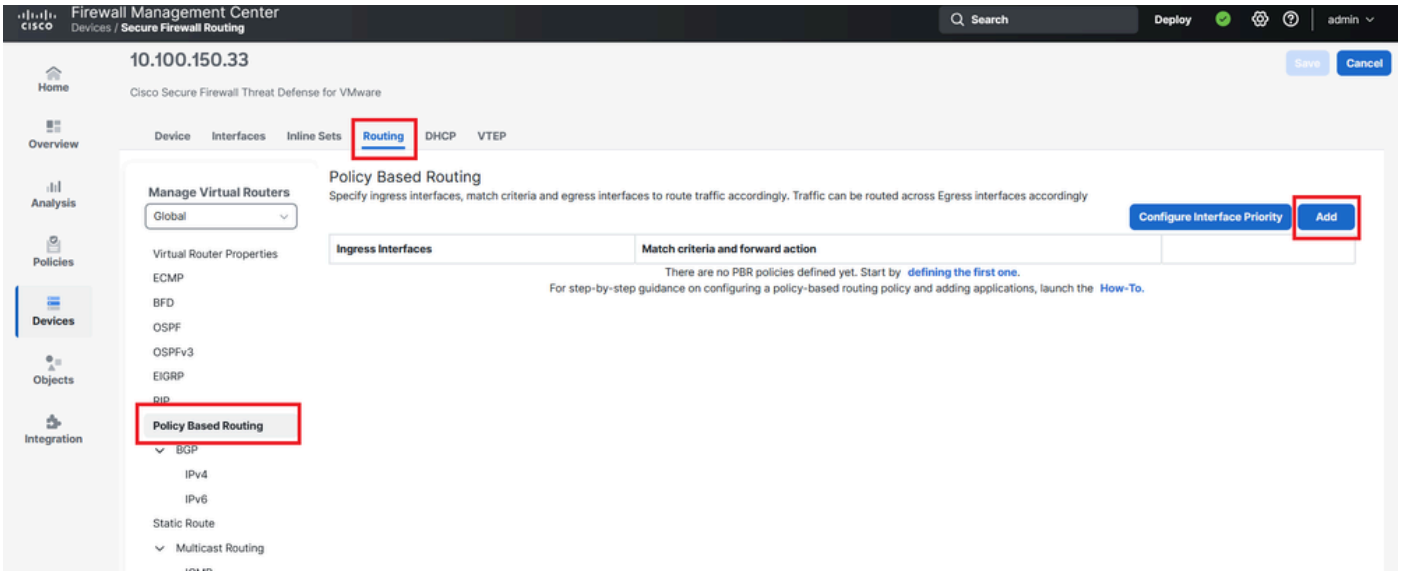

Immagine 6. Menu PBR

Passaggio 6. Configurare il PBR su un'interfaccia utilizzando l'ACL configurato in precedenza e distribuirlo.

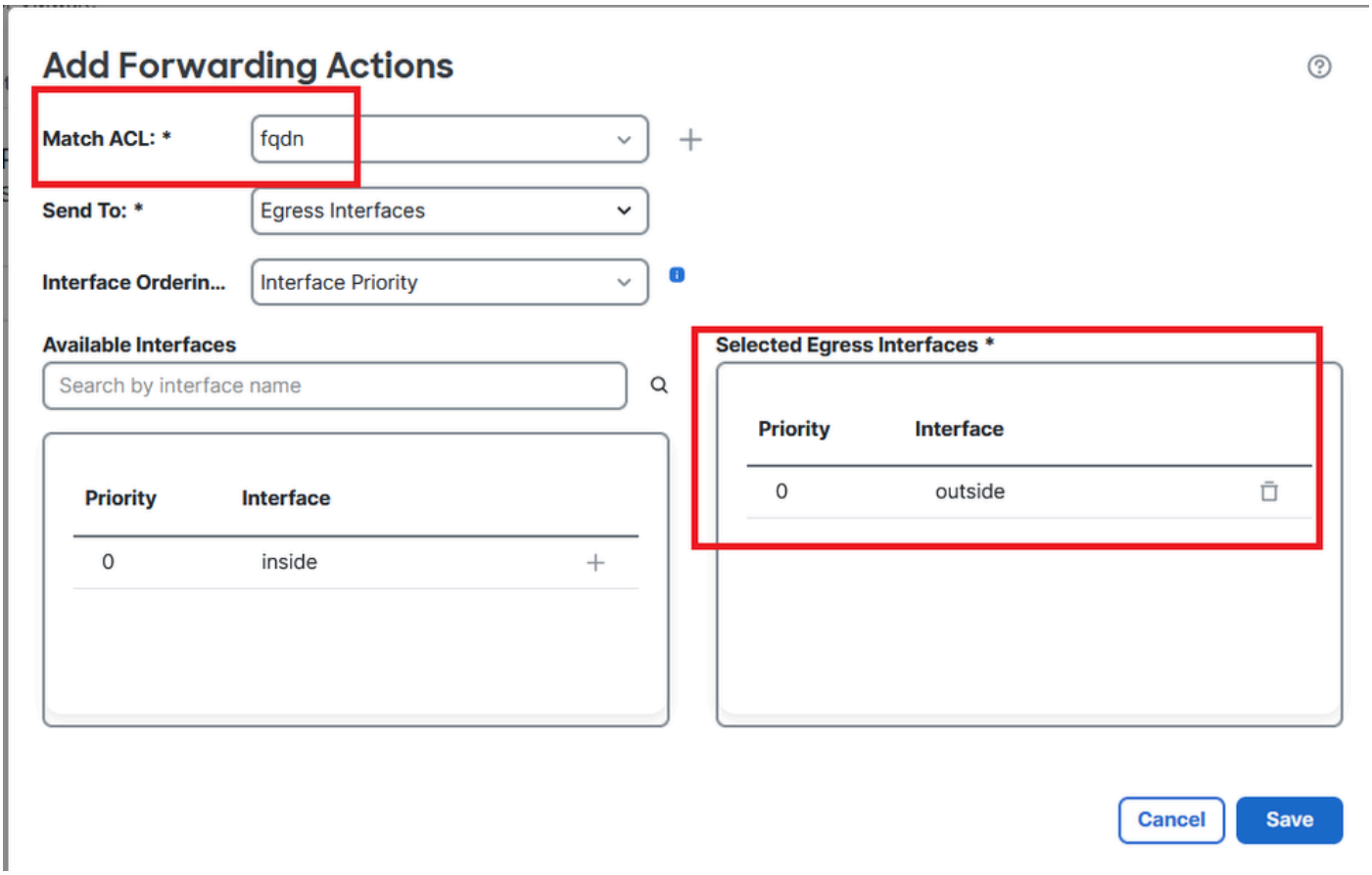

Immagine 7. Interfaccia PBR e menu di selezione ACL

Passaggio 7. Passare a Oggetti > Gestione oggetti > FlexConfig > Oggetto e creare un nuovo oggetto.

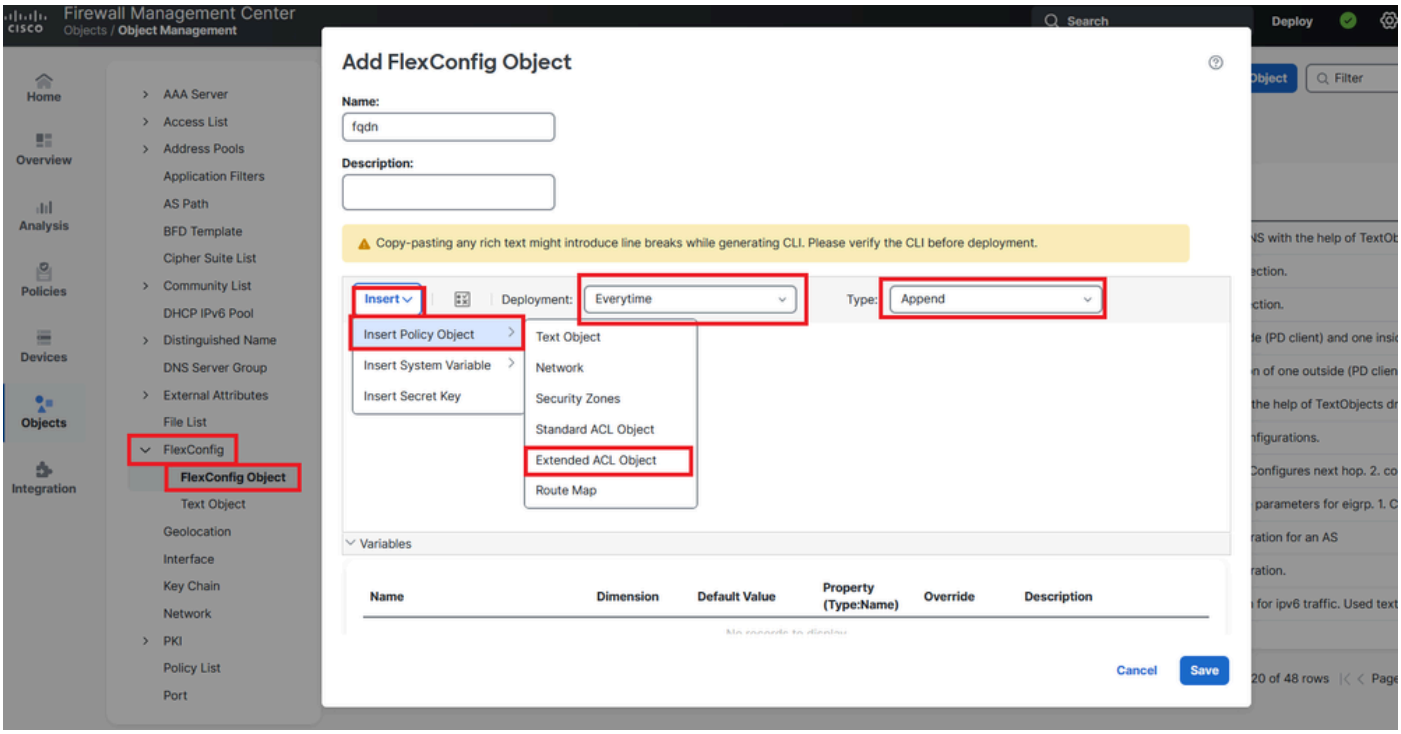

Immagine 8. Menu Configurazione oggetto FlexConfig

Passaggio 8. Selezionare Inserisci > Oggetto ACL esteso, assegnare un nome alla variabile e selezionare l'ACL esteso creato in precedenza. La variabile viene aggiunta con il nome utilizzato.

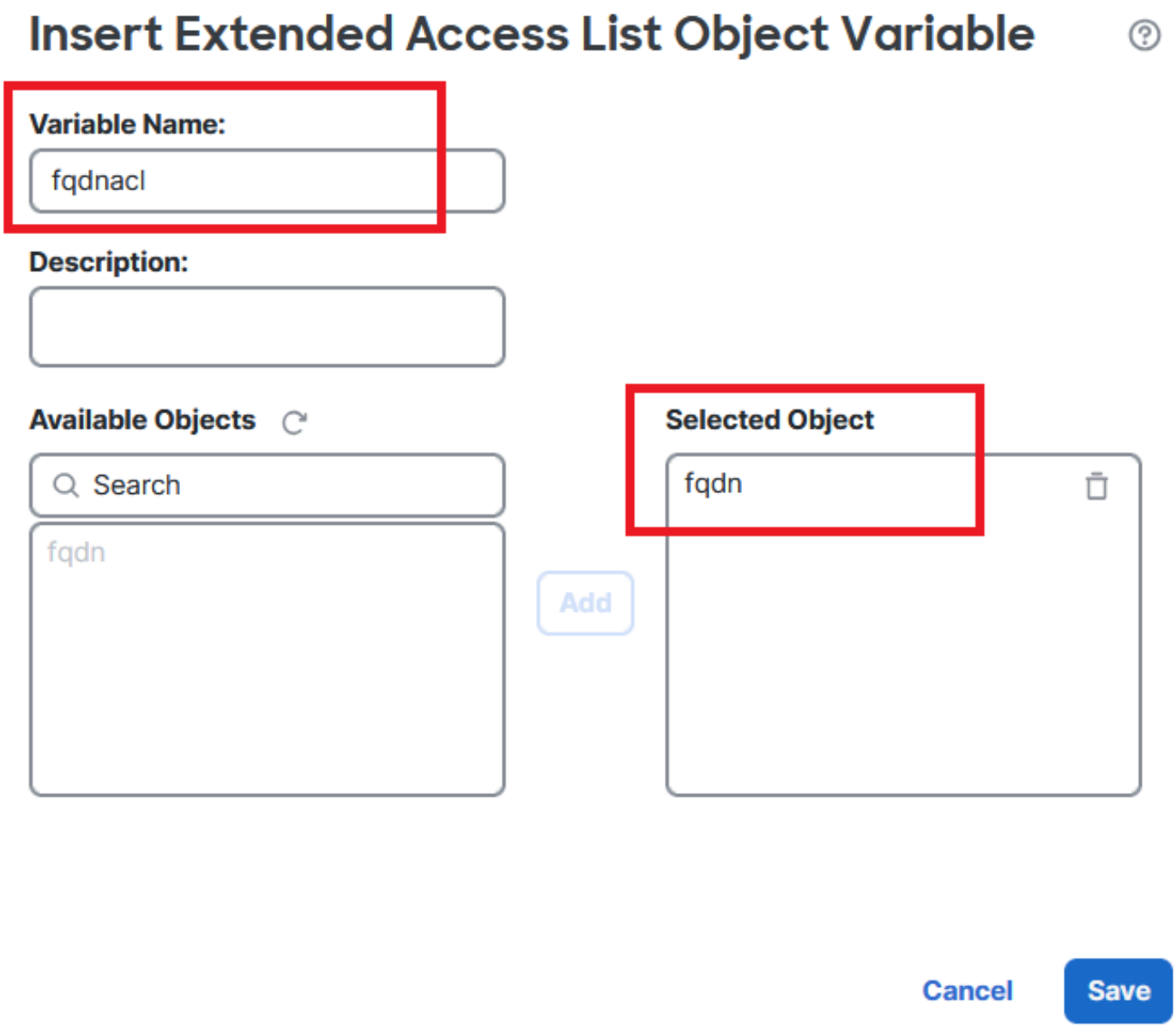

Immagine 9. Creazione di variabili per l'oggetto FlexConfig

Passaggio 9. Immettere questa riga per ogni oggetto FQDN che si desidera includere nell'ACL.

<#root>

```
access-li $
```

```
extended permit ip any object
```

Passaggio 10. Salvare l'oggetto FlexConfig come Everytime > Append.

Passaggio 11. Passare al menu FlexConfig Policy in Devices > FlexConfig.

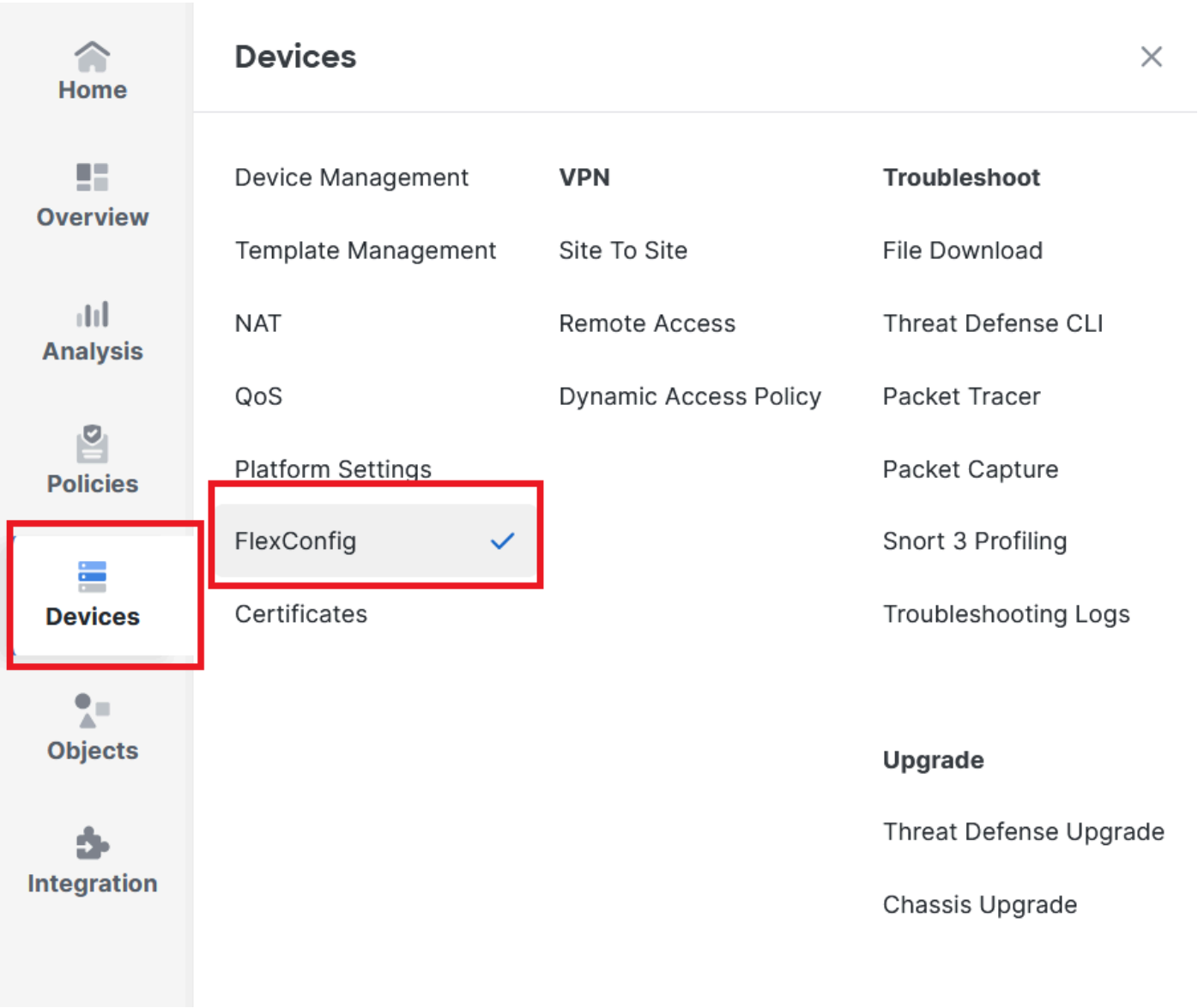

Immagine 10. Percorso del menu criteri di FlexConfig

Passaggio 12. Creare un nuovo criterio FlexConfig o selezionare un criterio già assegnato al FTD.

Immagine 11. Modifica o crea un nuovo criterio FlexConfig

Passaggio 13. Aggiungere l'oggetto FlexConfig al criterio, salvare e distribuire.

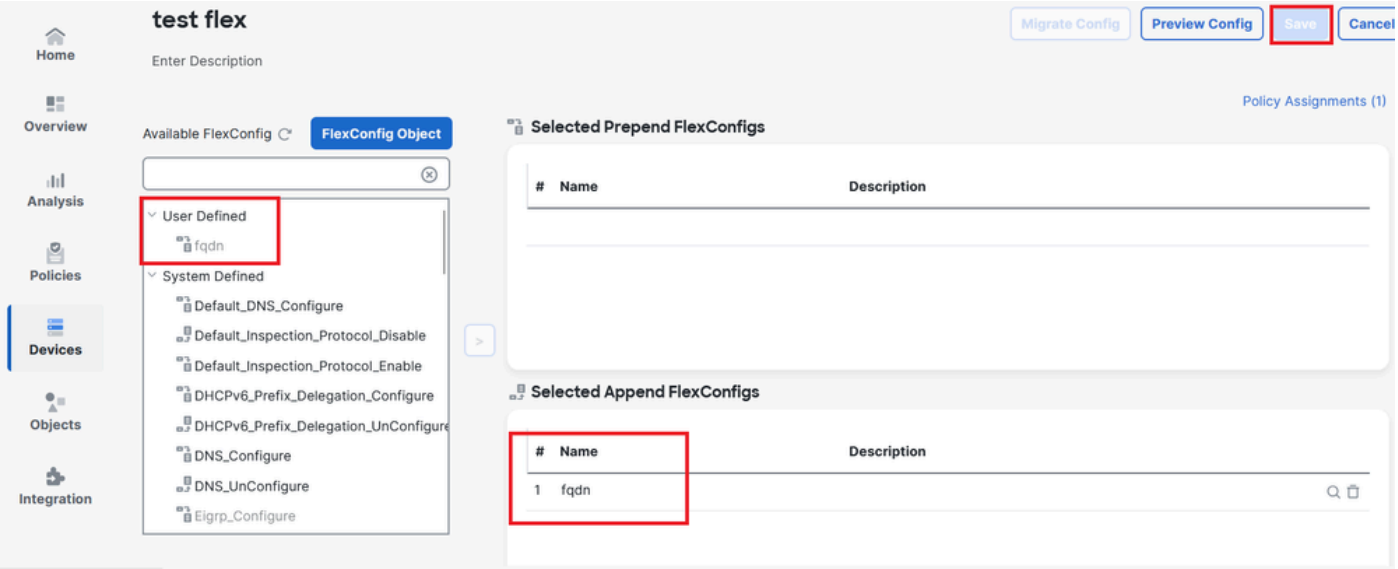

Immagine 12. Oggetto FlexConfig aggiunto nei criteri FlexConfig

Verifica

L'interfaccia in entrata dispone di route-map generata automaticamente con policy-route-map.

<#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

La route-map contiene l'ACL selezionato con l'interfaccia di destinazione utilizzata.

<#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

L'elenco degli accessi contiene l'host utilizzato come riferimento e la regola aggiuntiva aggiunta tramite FlexConfig.

```
<#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
```

È possibile eseguire un tracer dei pacchetti dall'interfaccia in entrata come origine per verificare di aver raggiunto la fase PBR.

```
<#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
```

Problemi comuni

PBR interrompe il funzionamento dopo una seconda distribuzione

Verificare se l'elenco degli accessi contiene ancora la regola dell'oggetto FQDN.

In questo caso, è possibile vedere che la regola non è più presente.

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

Verificare che l'oggetto FlexConfig sia impostato come Deployment: Everytime e Type: Append. La regola viene applicata ogni volta alle distribuzioni future.

FQDN non risolto

Quando si tenta di eseguire il ping dell'FQDN, viene visualizzato un messaggio relativo a un nome host non valido.

```
<#root>
firepower#
ping cisco.com
                ^
ERROR: % Invalid Hostname
```

Verificare la configurazione DNS. È necessario che nel gruppo di server siano presenti server DNS raggiungibili e che le interfacce di ricerca del dominio siano in grado di raggiungerli.

<#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.
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).