Configure FQDN Object on Extended ACL for PBR on FMC

Contents

Introduction

This document describes the procedure to configure a FQDN object in an extended Access-list (ACL) for use in Policy Based Routing (PBR).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these products:

- Secure Firewall Management Center (FMC)
- Secure Firewall Threat Defense (FTD)
- PBR

Components Used

The information in this document is based on these software and hardware versions:

- Firepower Threat Defense for VMware version 7.6.0
- Secure Firewall Management Center for VMware version 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

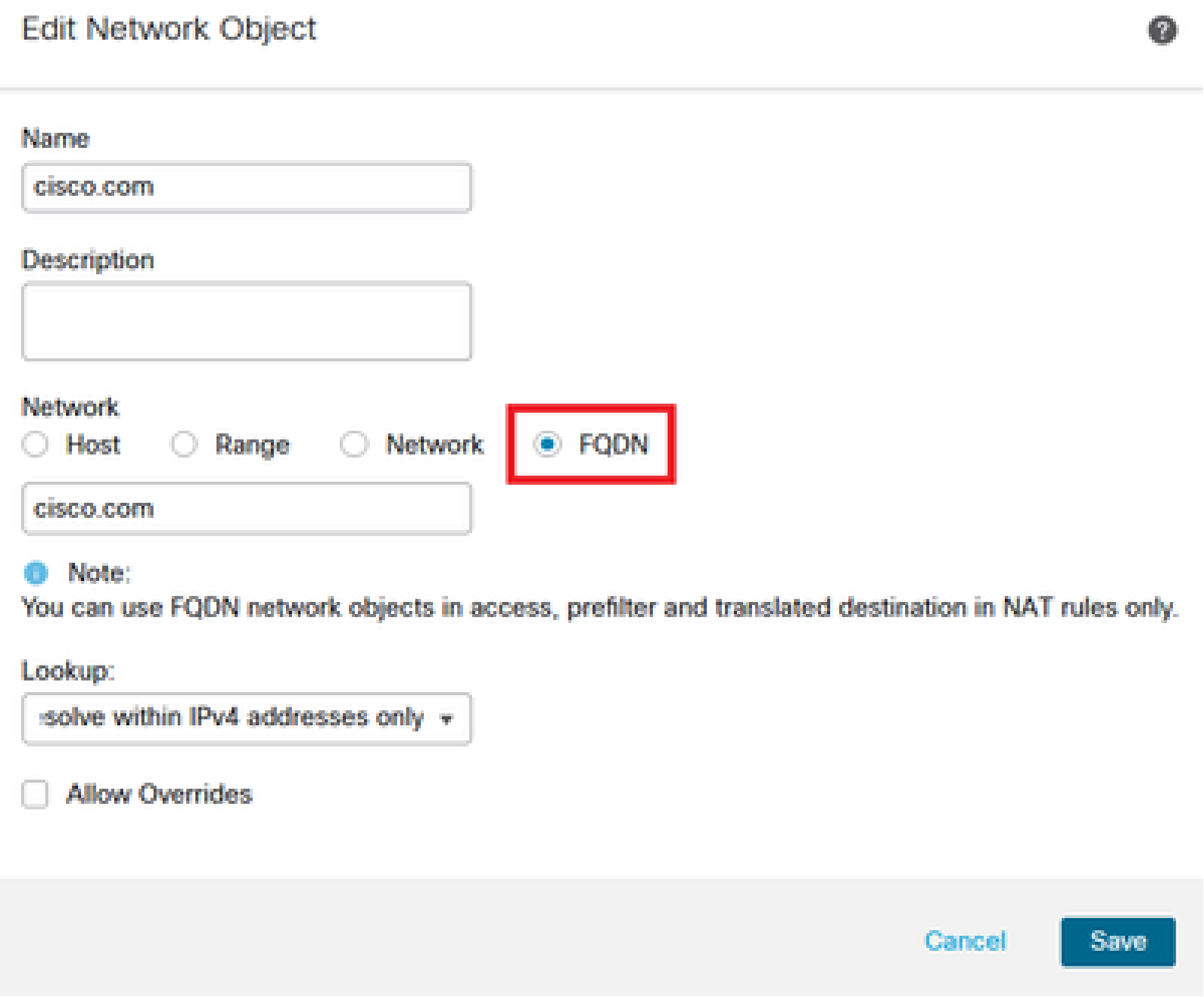
Currently, FTD does not allow filtering on non-HTTP traffic using Fully Qualified Domain Name (FQDN) objects as mentioned on Cisco bug ID CSCuz98322.

This functionality is supported on ASA platforms, however, only networks and applications can be filtered on FTD.

You can add a FQDN object to an extended access-list to configure PBR using this method.

Configure

Step 1. Create FQDN objects as needed.



Edit Network Object

Name: cisco.com

Description:

Network: ○ Host ○ Range ○ Network ● FQDN

cisco.com

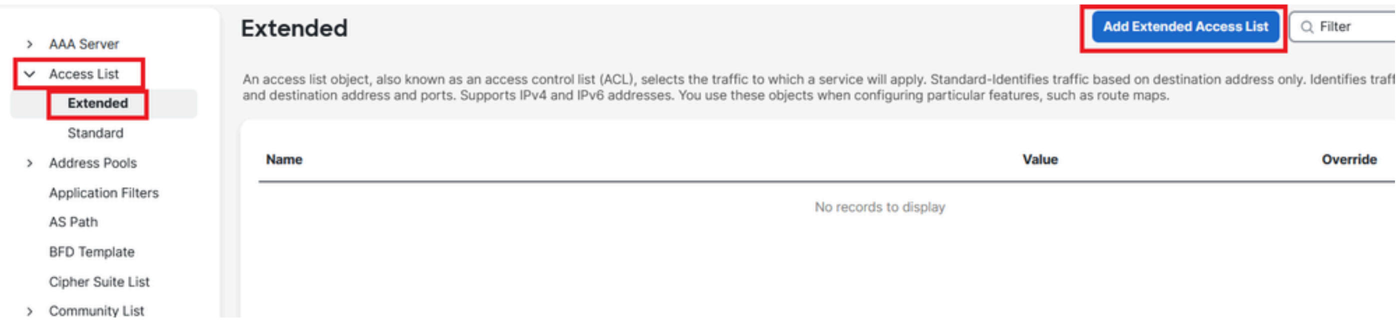
Note:
You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Lookup: solve within IPv4 addresses only

□ Allow Overrides

Image 1. Network Object Menu

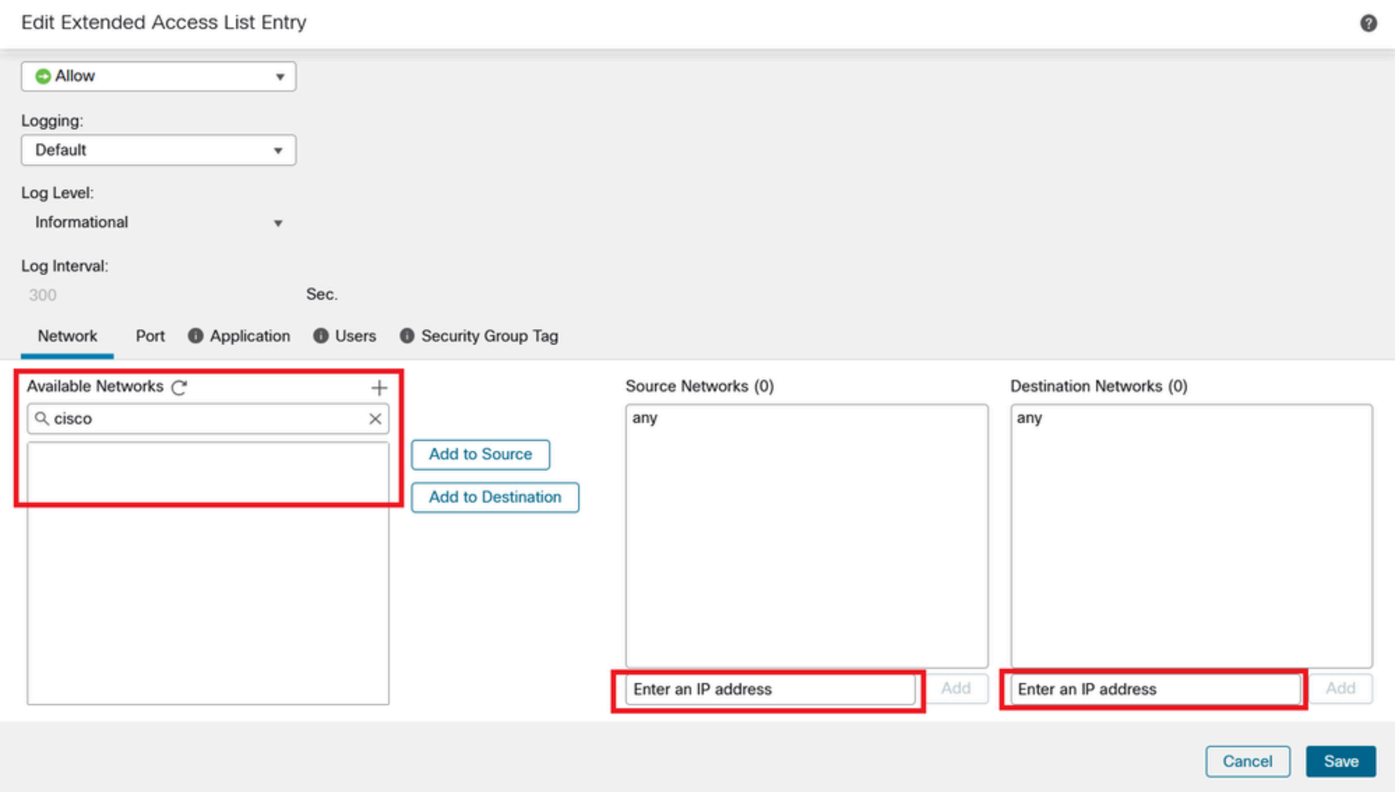
Step 2. Create an extended access-list under **Objects** > **Object Management** > **Access List** > **Extended**.



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.

Image 2. Extended Access List Menu

When you add a new rule, notice that you cannot see the FQDN object you configured when doing a search on the Network Objects to select source and destination.



Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

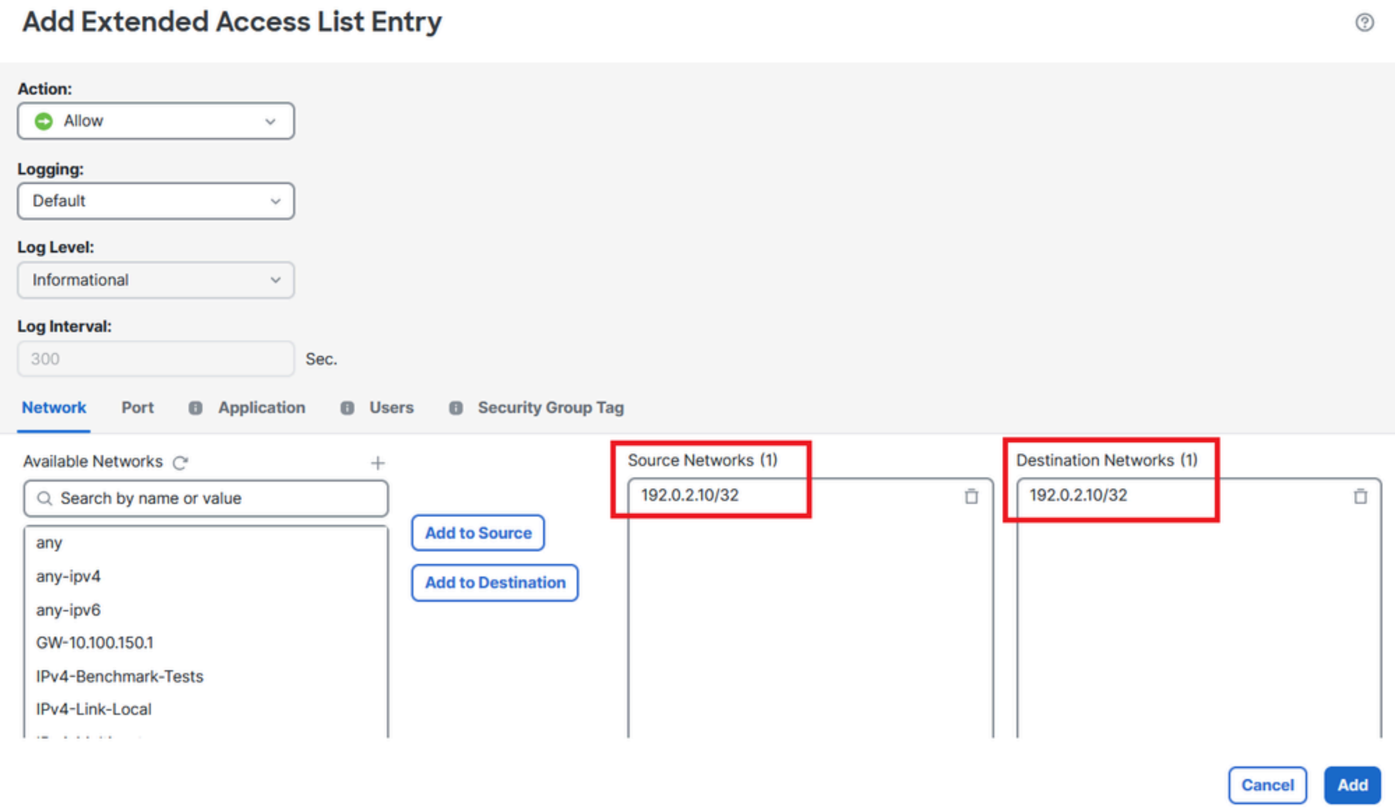
cisco

any

any

Image 3. New Extended Access List Rule Menu

Step 3. Create a rule that cannot be hit so the extended ACL is created and available for PBR configuration.



Add Extended Access List Entry

Action: Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Available Networks

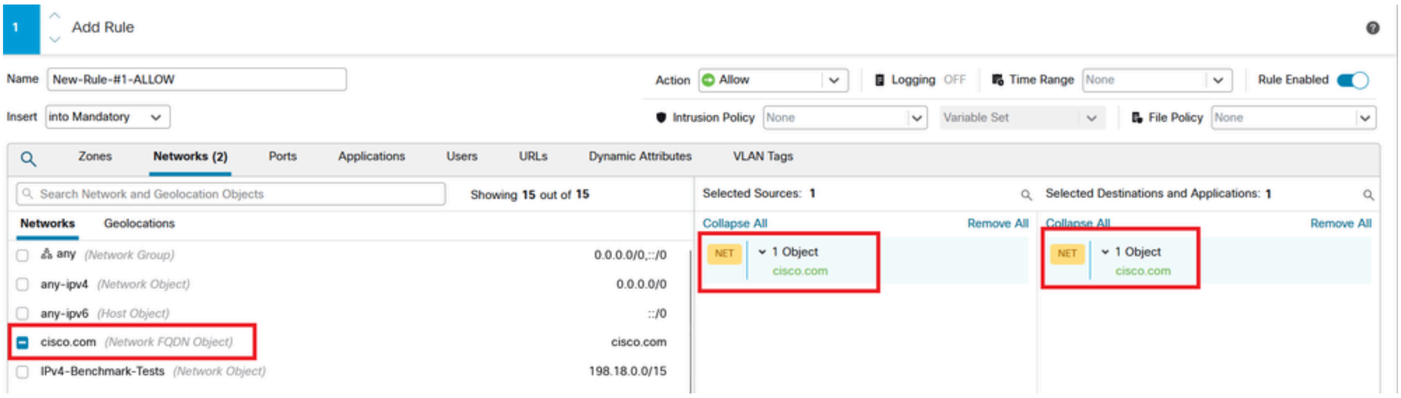
- any
- any-ipv4
- any-ipv6
- GW-10.100.150.1
- IPv4-Benchmark-Tests
- IPv4-Link-Local

Source Networks (1): 192.0.2.10/32

Destination Networks (1): 192.0.2.10/32

Image 4. Access List Rule Configuration that Cannot Be Hit

Step **4.** You need to create a rule on the Access-Control Policy (ACP) targeting your FTD with the FQDN object. The FMC deploys the FQDN object to the FTD so you can reference it through a FlexConfig object.



1 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

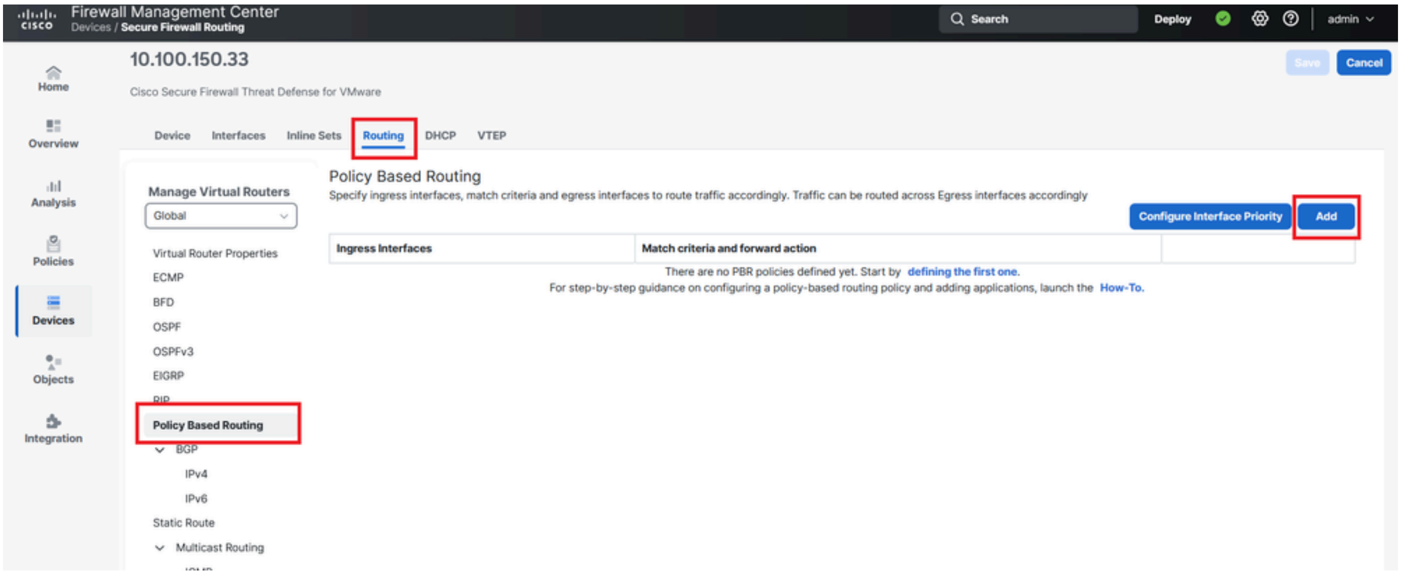
□	any (Network Group)	0.0.0.0/0,::/0
□	any-ipv4 (Network Object)	0.0.0.0/0
□	any-ipv6 (Host Object)	::/0
■	cisco.com (Network FQDN Object)	cisco.com
□	IPv4-Benchmark-Tests (Network Object)	198.18.0.0/15

Selected Sources: 1 — NET 1 Object cisco.com

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

Image 5. ACP Rule with FQDN Object

Step 5. Navigate to the FTD on **Devices** > **Device Management** and select the **Routing** tab and navigate to **Policy Based Routing** section.



10.100.150.33

Cisco Secure Firewall Threat Defense for VMware

Policy Based Routing

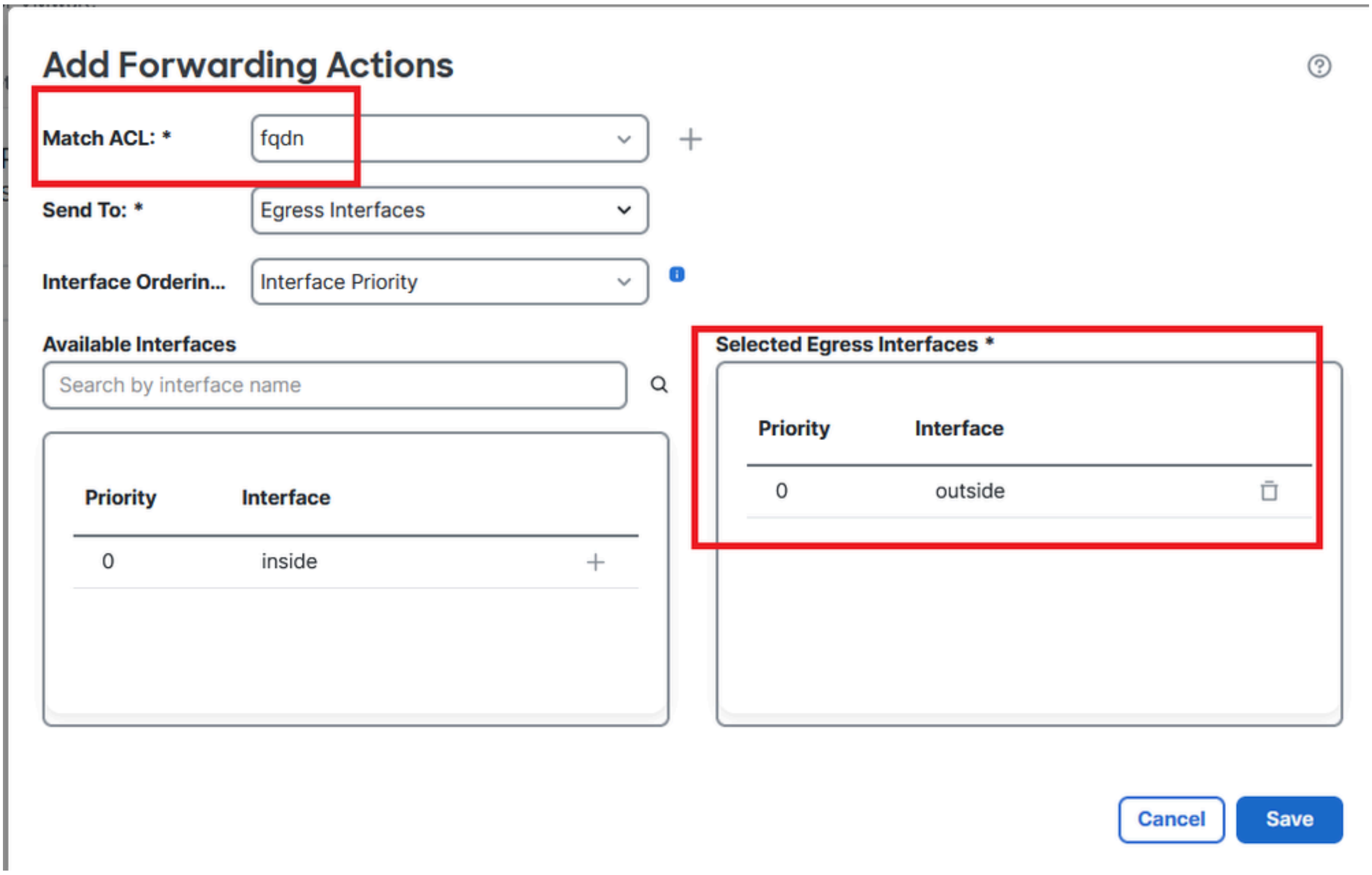
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

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.

Image 6. PBR Menu

Step 6. Configure the **PBR** on an interface using the ACL configured earlier and deploy.



Add Forwarding Actions

Match ACL: * fqdn

Send To: * Egress Interfaces

Interface Orderin... Interface Priority

Available Interfaces

Search by interface name

Priority	Interface
0	inside

Selected Egress Interfaces *

Priority	Interface
0	outside

Image 7. PBR Interface and ACL Selection Menu

Step 7. Navigate to **Objects** > **Object Management** > **FlexConfig** > **Object** and create a **new object**.

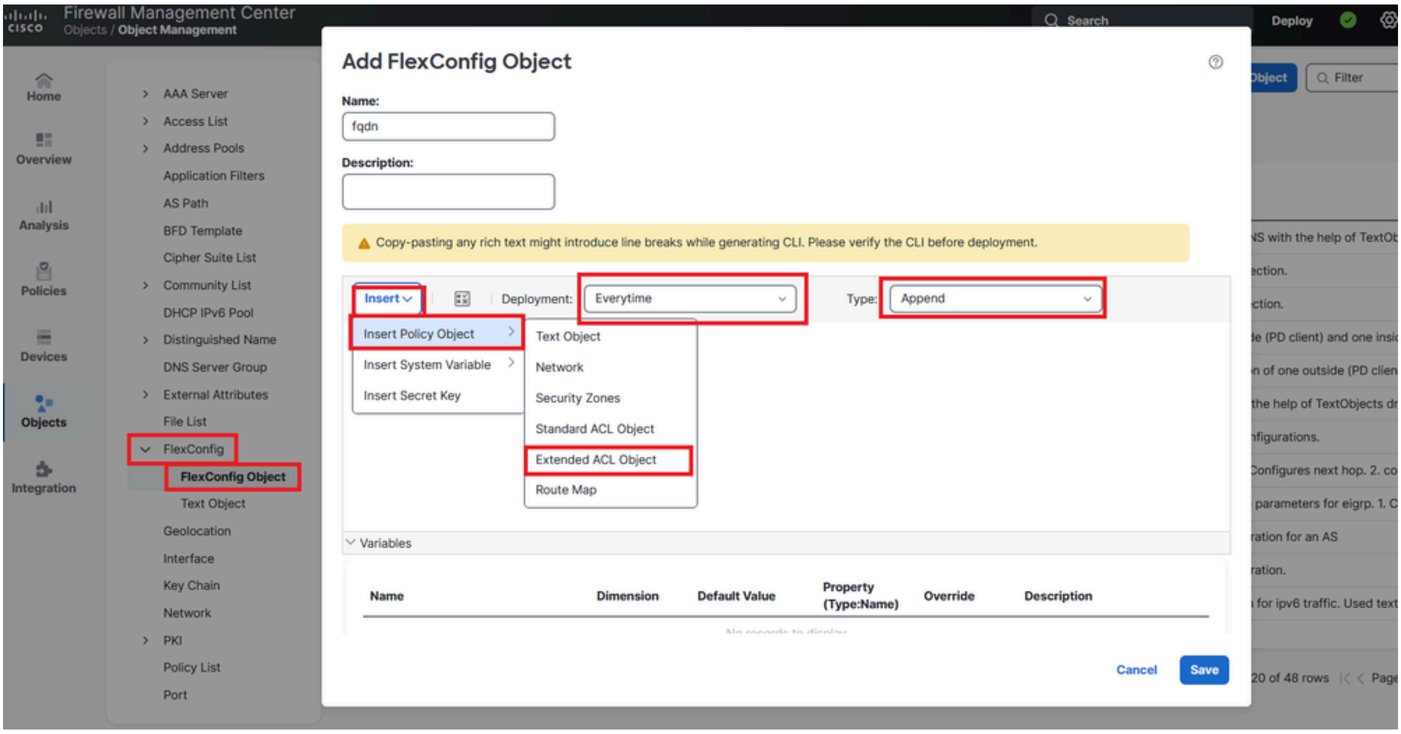
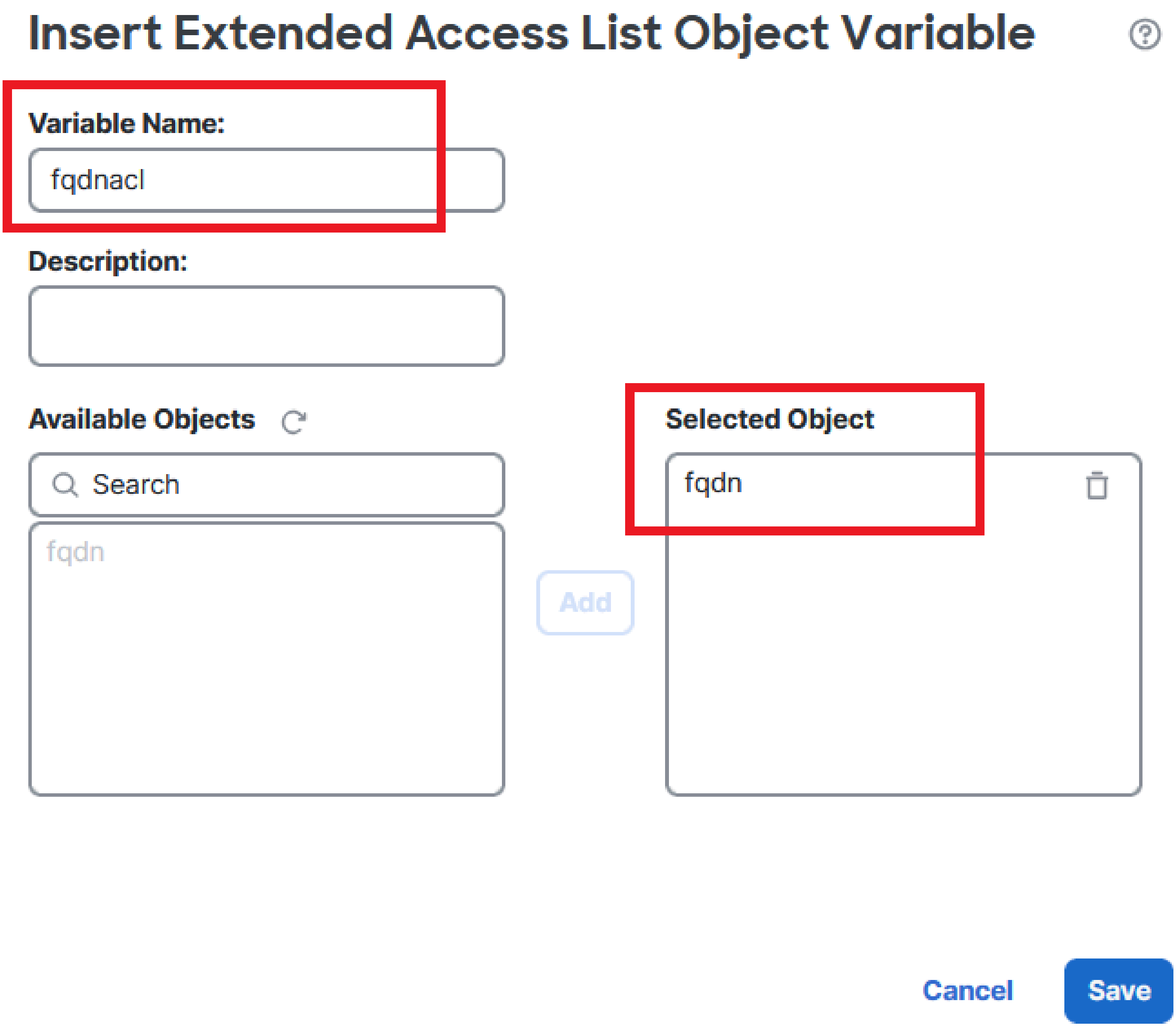


Image 8. FlexConfig Object Configuration Menu

Step 8. Select **Insert** > **Extended ACL Object**, name your **variable** and select your **extended ACL** you created earlier. The variable is added with the name you used.



Insert Extended Access List Object Variable

Variable Name: fqdnacl

Description:

Available Objects

Selected Object: fqdn

Image 9. Variable Creation for FlexConfig Object

Step 9. Enter this line for each FQDN object you want to your ACL.

<#root>

```
access-li $<your_ACL_variable> extended permit ip any object <your_FQDN_object_name>
```

Step 10. Save your **FlexConfig Object** as **Everytime** > **Append**.

Step 11.Navigate to the **FlexConfig Policy** menu under **Devices** > **FlexConfig**.

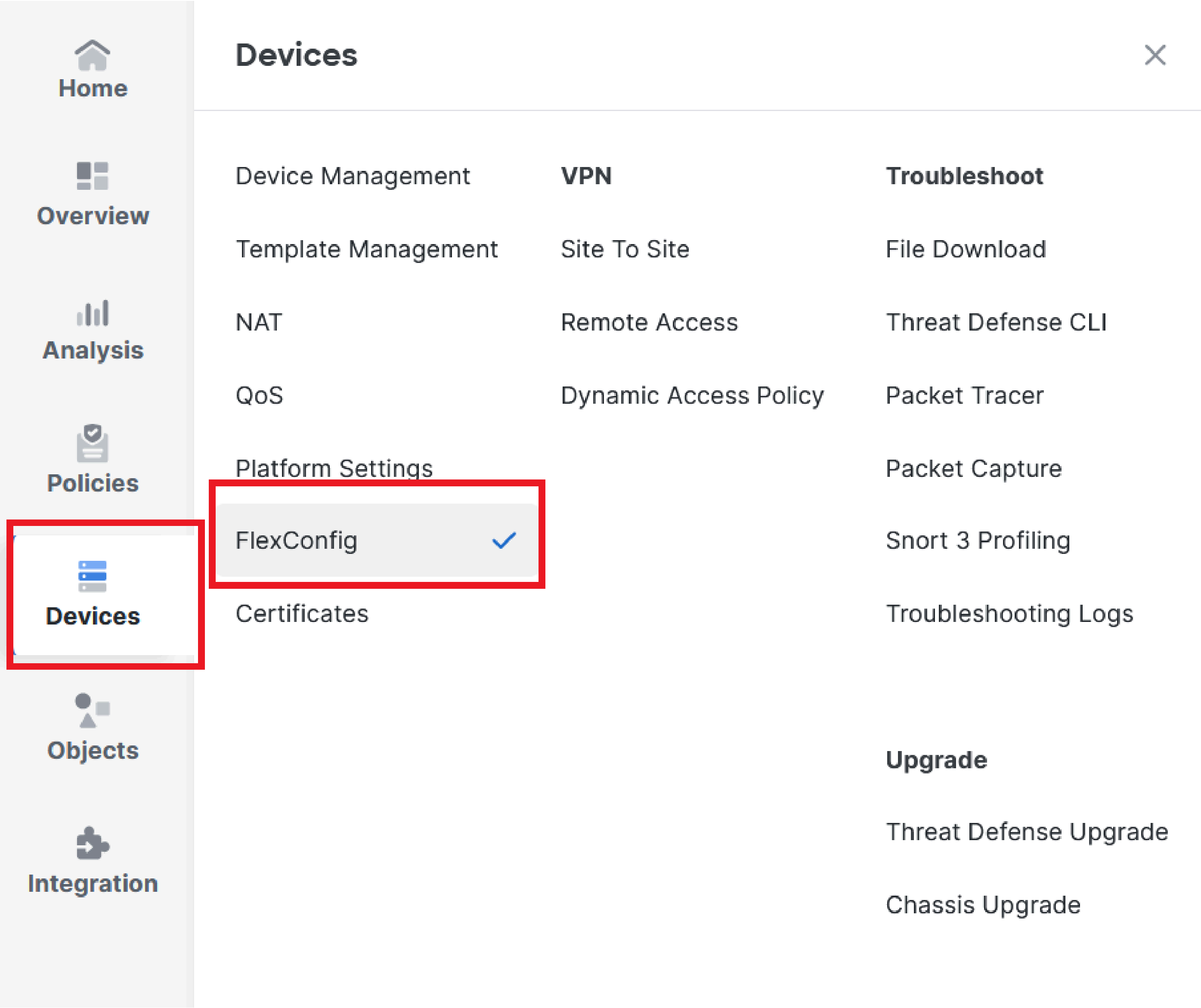


Image 10. Path to FlexConfig Policy Menu

Step 12. Create a new **FlexConfig Policy** or select a **Policy** already assigned to your FTD.

Image 11. Edit or Create a New FlexConfig Policy

Step 13. Add your **FlexConfig object** to the Policy, **save** and **deploy**.

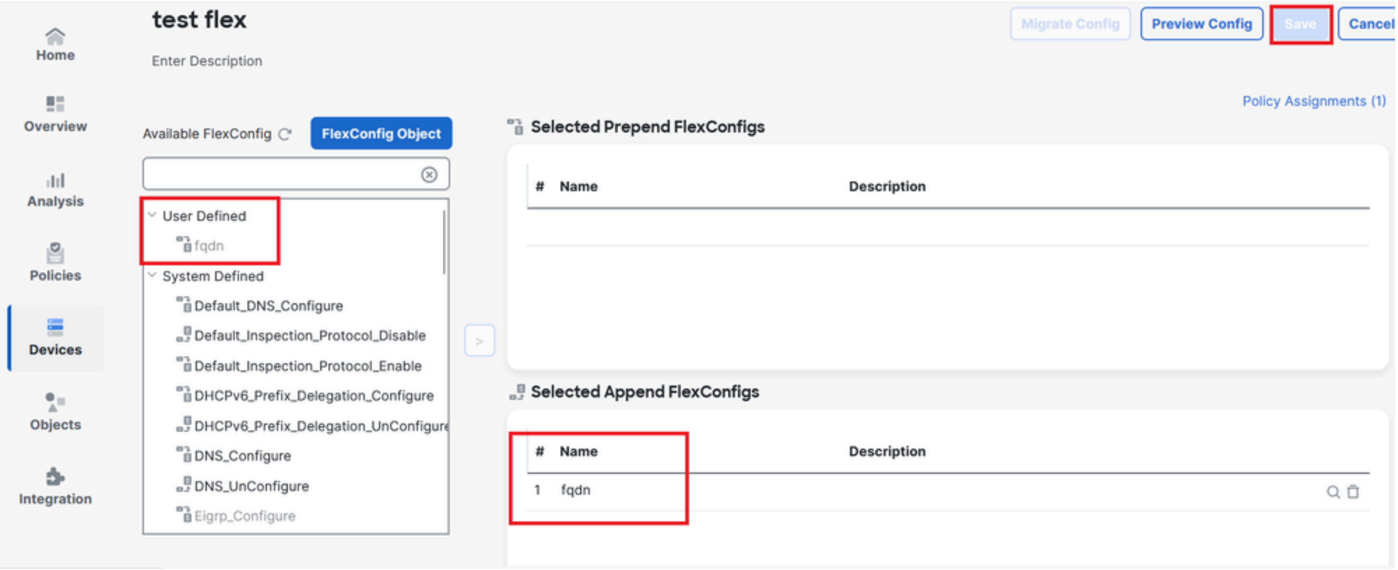


Image 12. Added FlexConfig Object into FlexConfig Policy

Verify

Your ingress interface has the policy-route with auto-generated 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
```

The route-map contains the selected ACL with the used destination interface.

<#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
```

Your access list contains the host used for reference and the additional rule you added through 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
```

You can do a packet tracer from the ingress interface as a source to verify you hit the PBR phase.

<#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
```

Common Issues

PBR Stops Working After a Second Deployment

Please verify if the access-list still contains the FQDN object rule.

In this case, you can see the rule is no longer here.

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

Verify that the FlexConfig Object is set up as **Deployment: Everytime** and **Type: Append**. The rule is applied every time on future deployments.

FQDN does not Resolve

When you attempt to ping the FQDN, you get a message about invalid hostname.

<#root>

```
firepower#

ping cisco.com


                ^

ERROR: % Invalid Hostname
```

Verify DNS configuration. You must have reachable DNS servers on your server group, and the domain-lookup interfaces must be able to reach them.

<#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.
```