FMCのPBR用の拡張ACLでのFQDNオブジェクトの設定

内容

はじめに

このドキュメントでは、ポリシーベースルーティング(PBR)で使用する拡張アクセスリスト(ACL)にFQDNオブジェクトを設定する手順について説明します。

前提条件

要件

次の製品に関する知識があることが推奨されます。

- セキュアファイアウォール管理センター(FMC)
- セキュアファイアウォール脅威対策(FTD)
- PBR

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VMware向けFirepower Threat Defenseバージョン7.6.0
- Secure Firewall Management Center for VMwareバージョン7.6.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

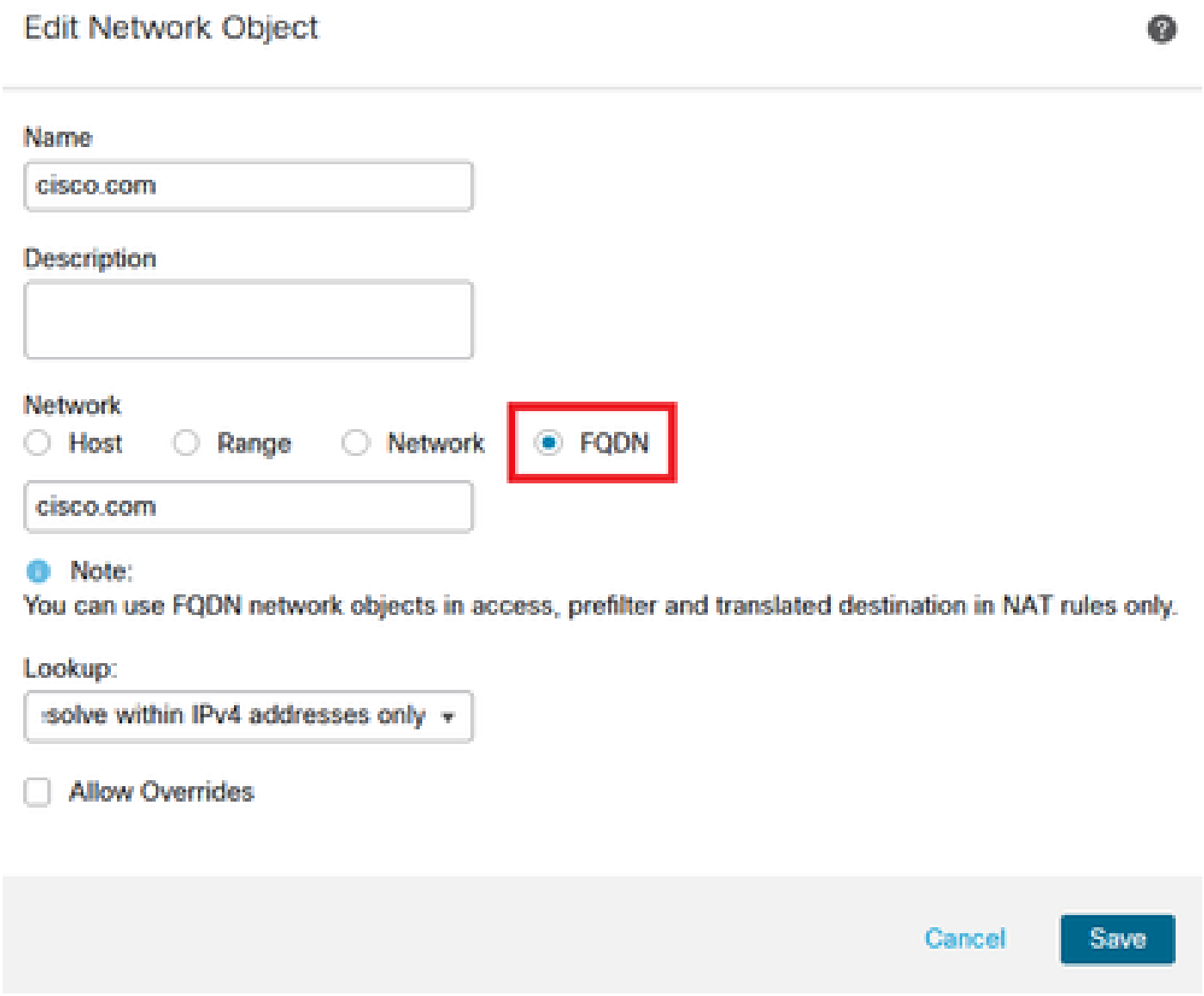
現在、FTDでは、Cisco Bug ID CSCuz98322で説明されているように、完全修飾ドメイン名(FQDN)オブジェクトを使用して非HTTPトラフィックをフィルタリングすることはできません。

この機能はASAプラットフォームでサポートされていますが、FTDでフィルタリングできるのはネットワークとアプリケーションだけです。

拡張アクセスリストにFQDNオブジェクトを追加して、この方法でPBRを設定できます。

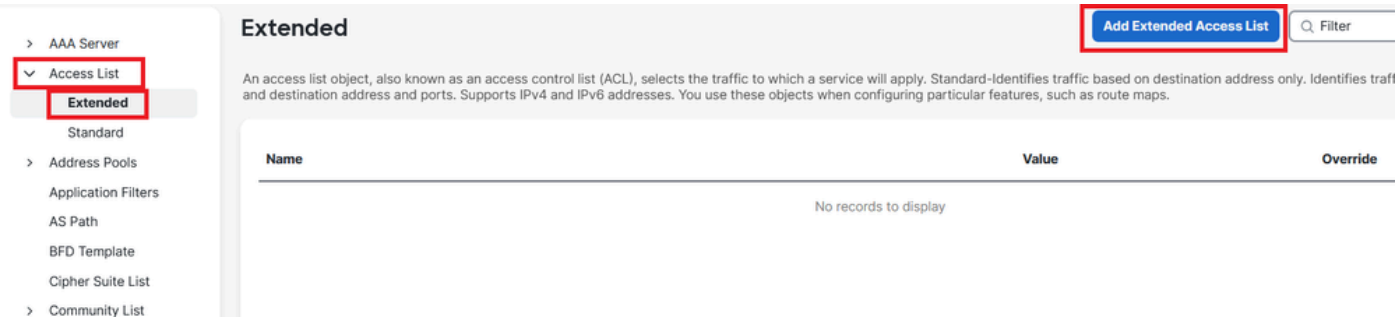
設定

ステップ 1：必要に応じてFQDNオブジェクトを作成します。



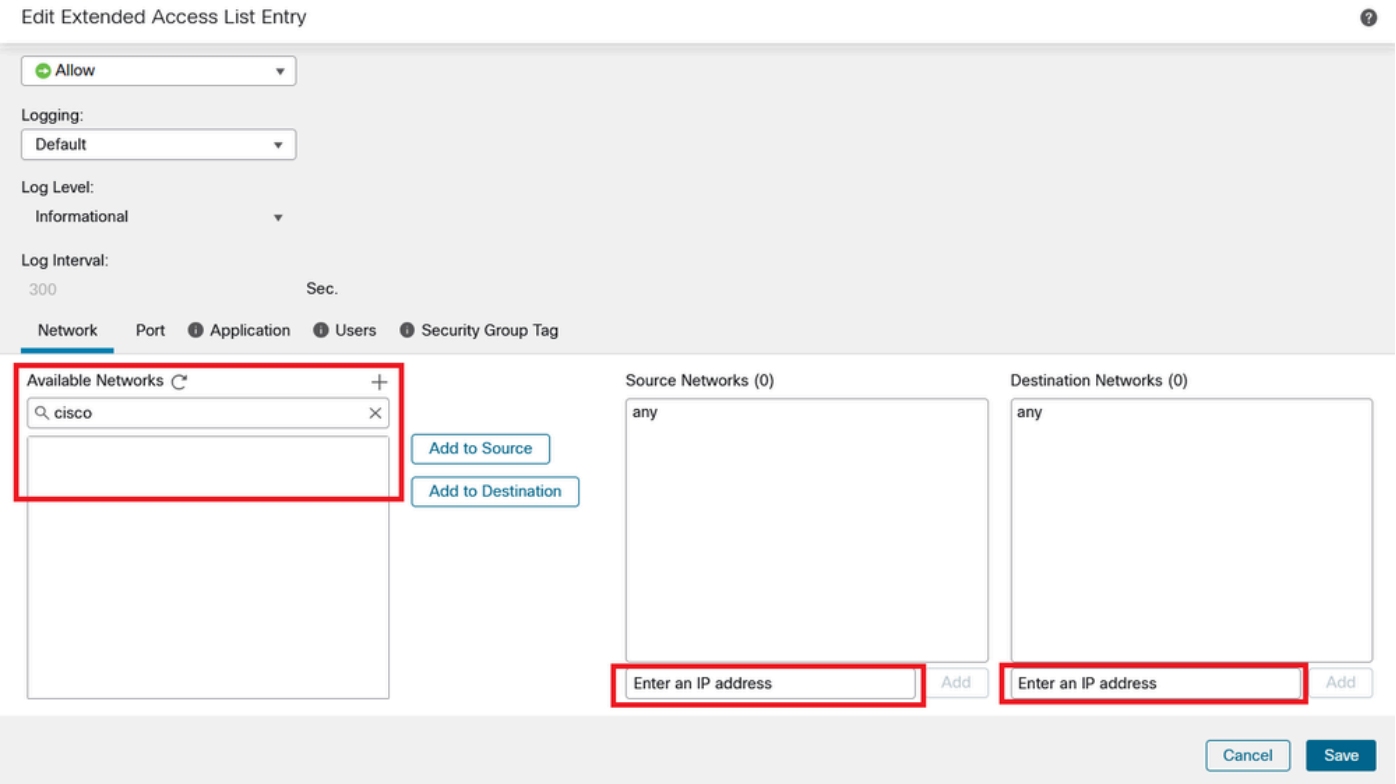
画像 1.Network Objectメニュー

ステップ 2：Objects > Object Management > Access List > Extendedの順に選択して、拡張アクセスリストを作成します。



画像 2.拡張アクセスリストメニュー

新しいルールを追加する場合は、ネットワークオブジェクトで送信元と宛先を選択する検索を実行するときに設定したFQDNオブジェクトが表示されないことに注意してください。



画像 3.新しい拡張アクセスリストルールメニュー

ステップ 3：ヒットできないルールを作成して、拡張ACLを作成し、PBR設定に使用できるようにします。

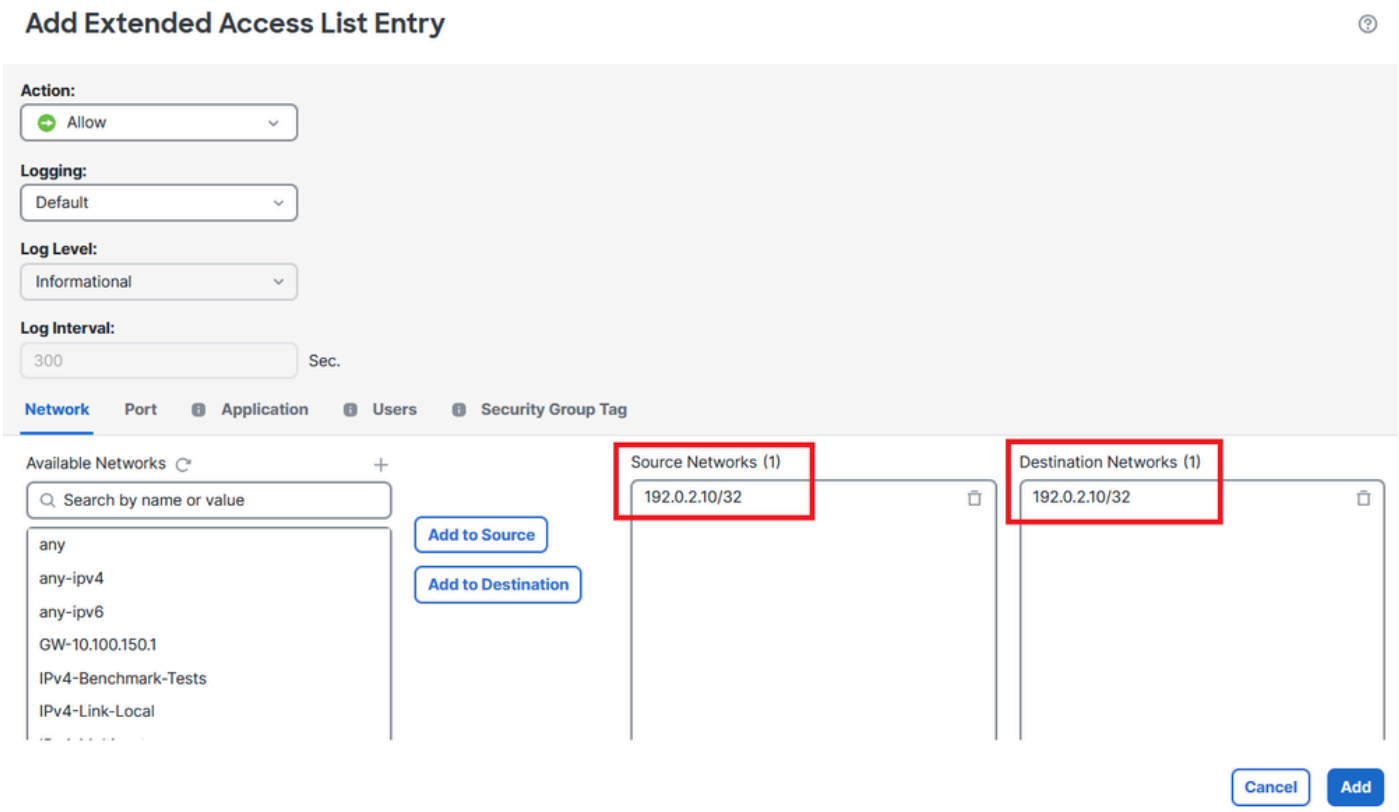


図 4.ヒットできないアクセスリストルールの設定

ステップ 4：FQDNオブジェクトを使用してFTDを対象とするアクセスコントロールポリシー(ACP)でルールを作成する必要があります。FMCはFQDNオブジェクトをFTDに導入するため、FlexConfigオブジェクトを介して参照できます。

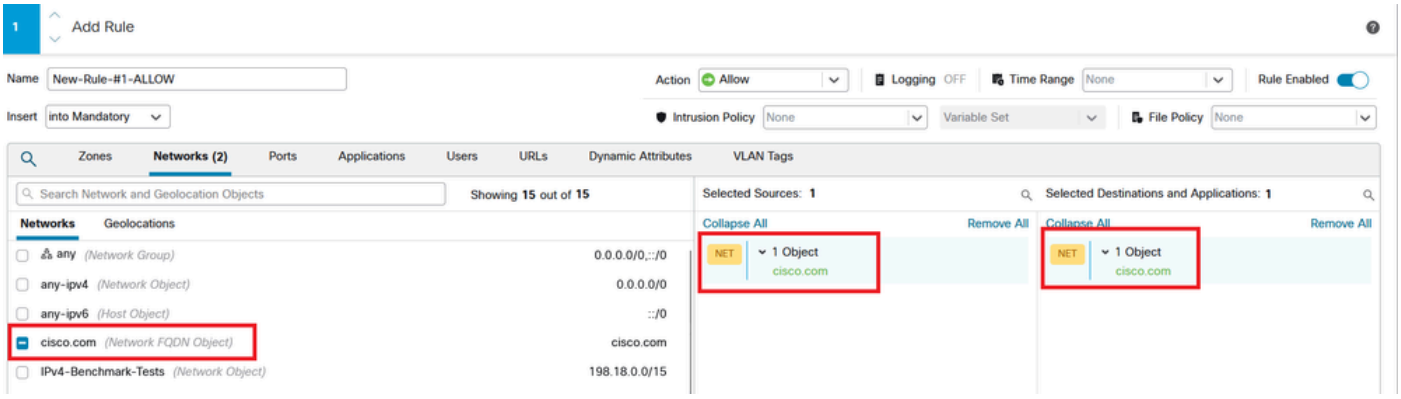


図 5.FQDNオブジェクトを含むACPルール

ステップ 5：Devices > Device ManagementでFTDに移動し、Routingタブを選択して、Policy Based Routingセクションに移動します。

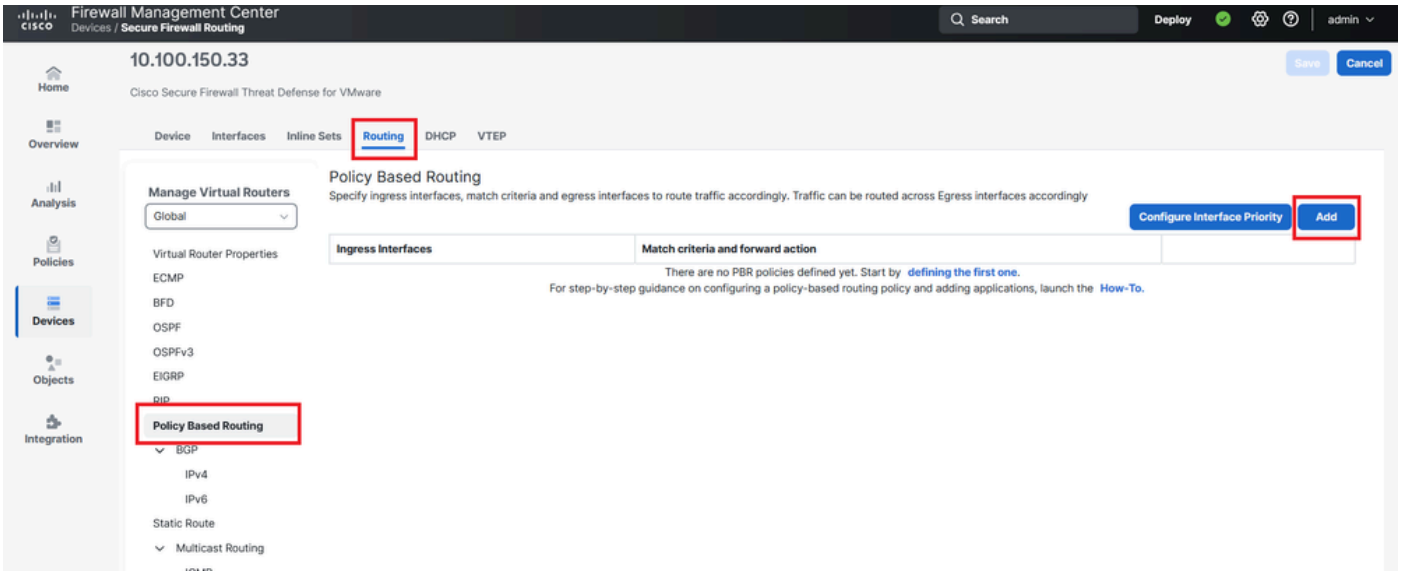


図 6.PBRメニュー

手順 6：以前に設定したACLを使用してインターフェイスにPBRを設定し、展開します。

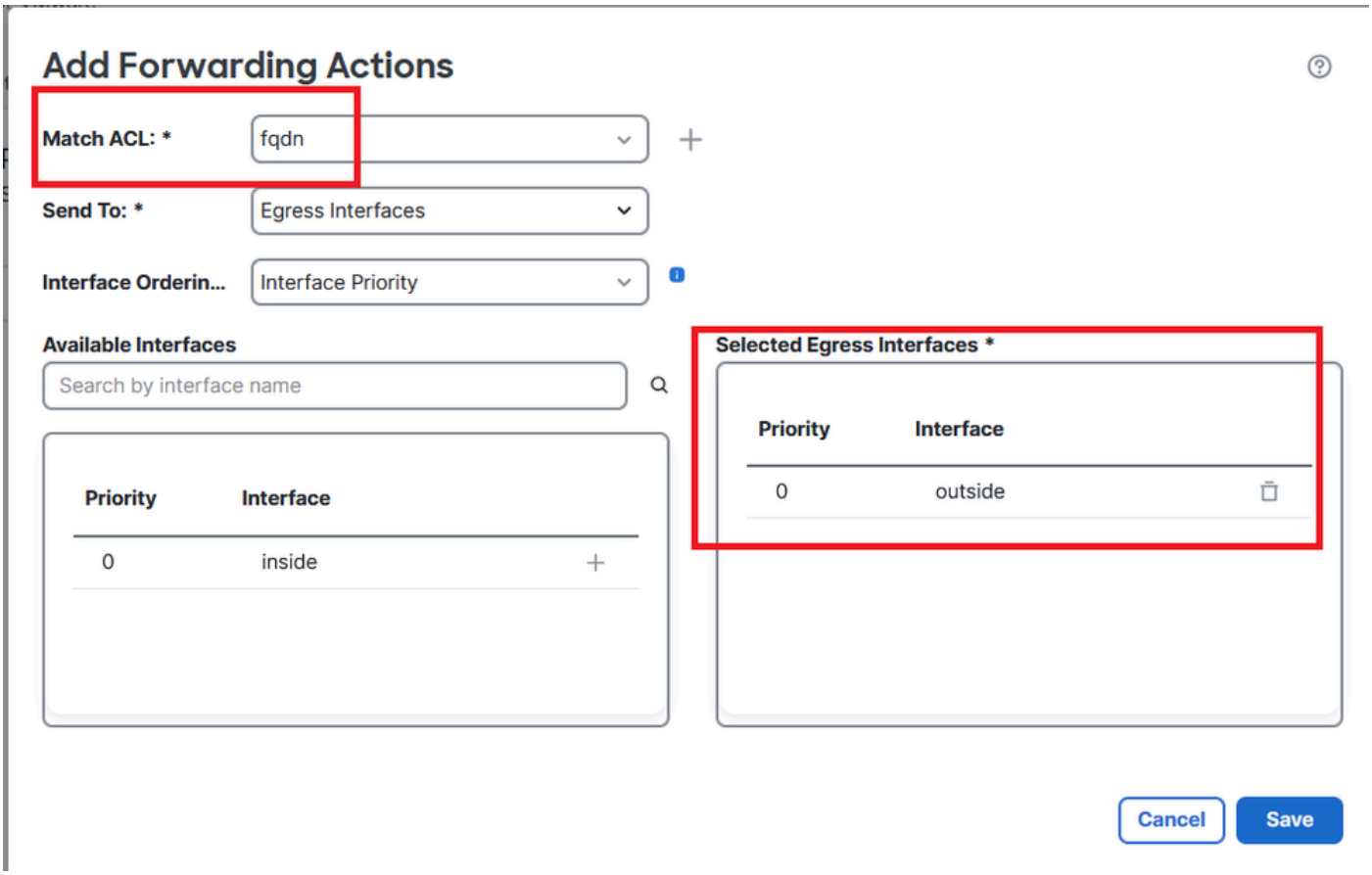


図 7.PBRインターフェイスとACL選択メニュー

手順 7：Objects > Object Management > FlexConfig > Objectの順に選択し、新しいオブジェクトを作成します。

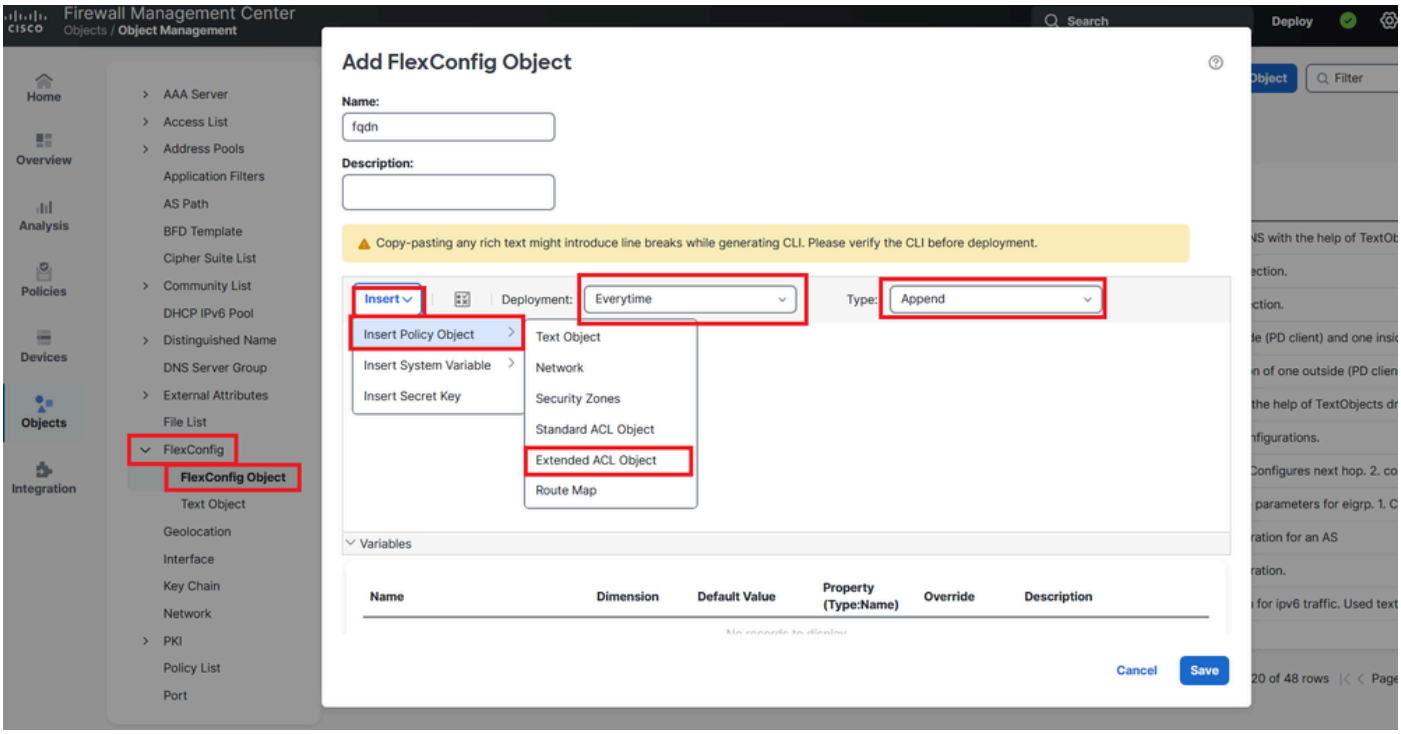


図 8.FlexConfigオブジェクト設定メニュー

ステップ 8：Insert > Extended ACL Objectの順に選択し、変数に名前を付け、前に作成した拡張ACLを選択します。変数が使用した名前で追加されます。

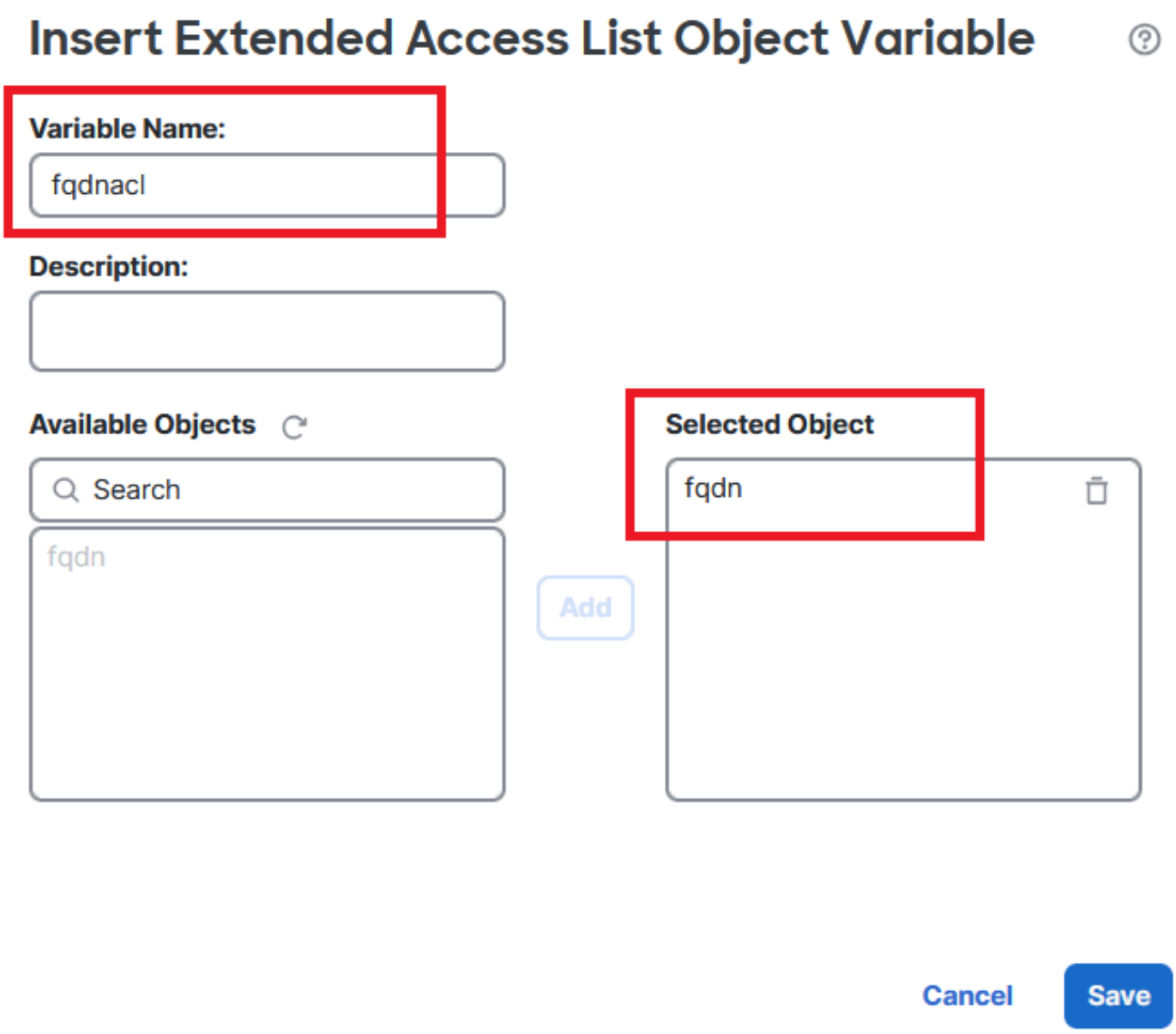


図 9.FlexConfigオブジェクトの変数の作成

ステップ 9：ACLに追加する各FQDNオブジェクトに対して、この行を入力します。

<#root>

```
access-li $
```

```
extended permit ip any object
```

ステップ 10：FlexConfigオブジェクトをEverytime > Appendとして保存します。

ステップ11:Devices > FlexConfigの下にあるFlexConfig Policyメニューに移動します。

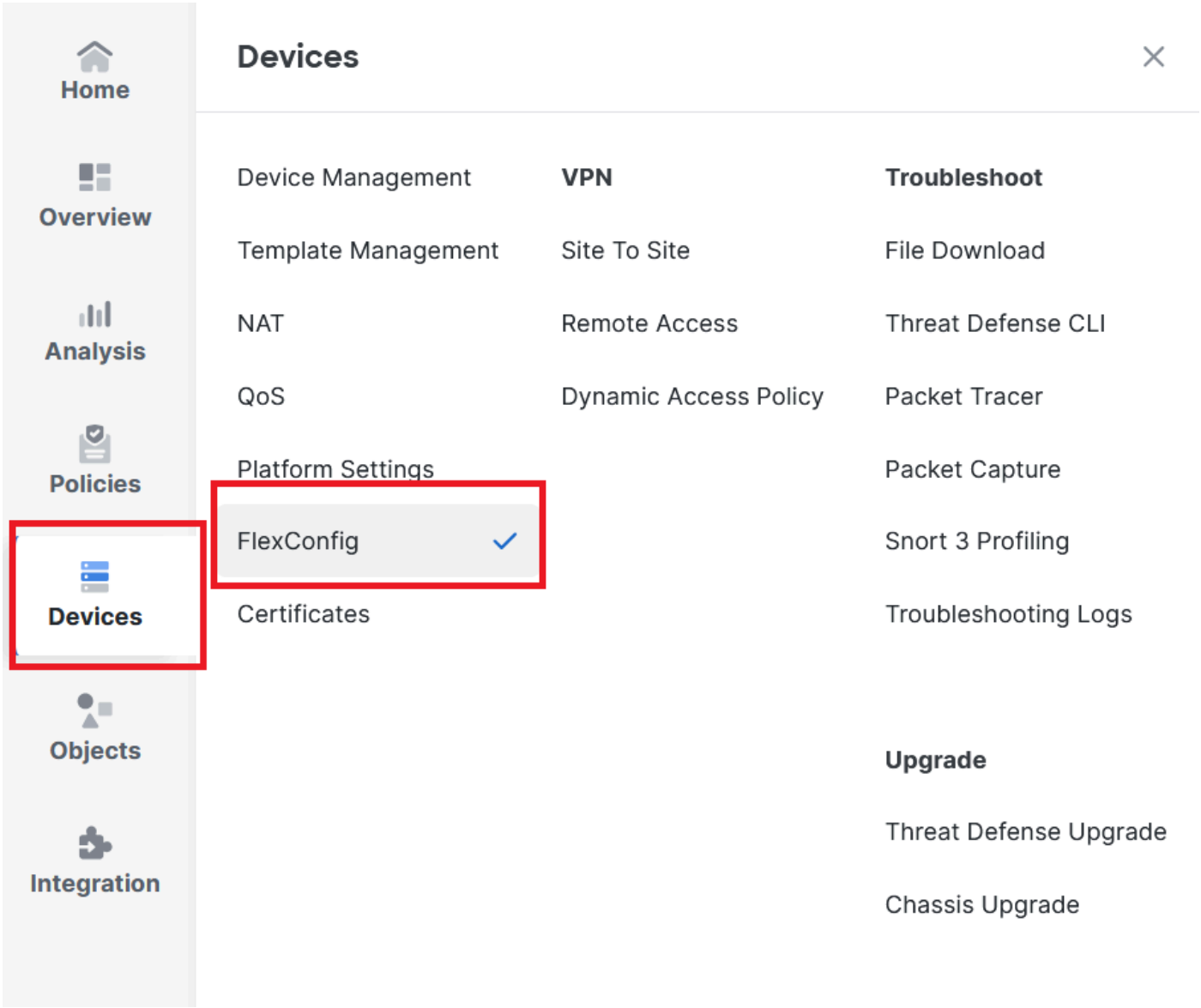


図 10.FlexConfigポリシーメニューへのパス

ステップ 12新しいFlexConfigポリシーを作成するか、FTDにすでに割り当てられているポリシーを選択します。

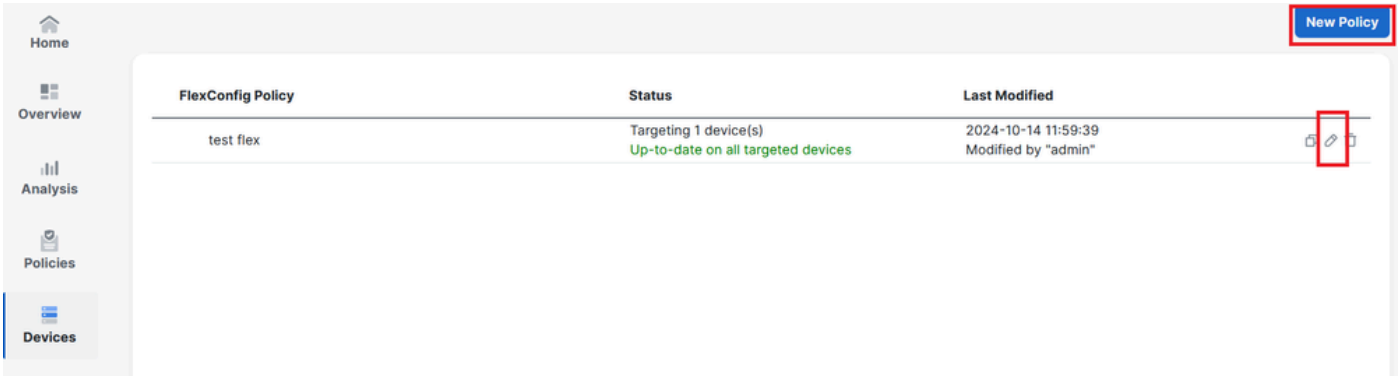


図 11.新しいFlexConfigポリシーの編集または作成

ステップ 13FlexConfigオブジェクトをポリシーに追加し、保存して展開します。

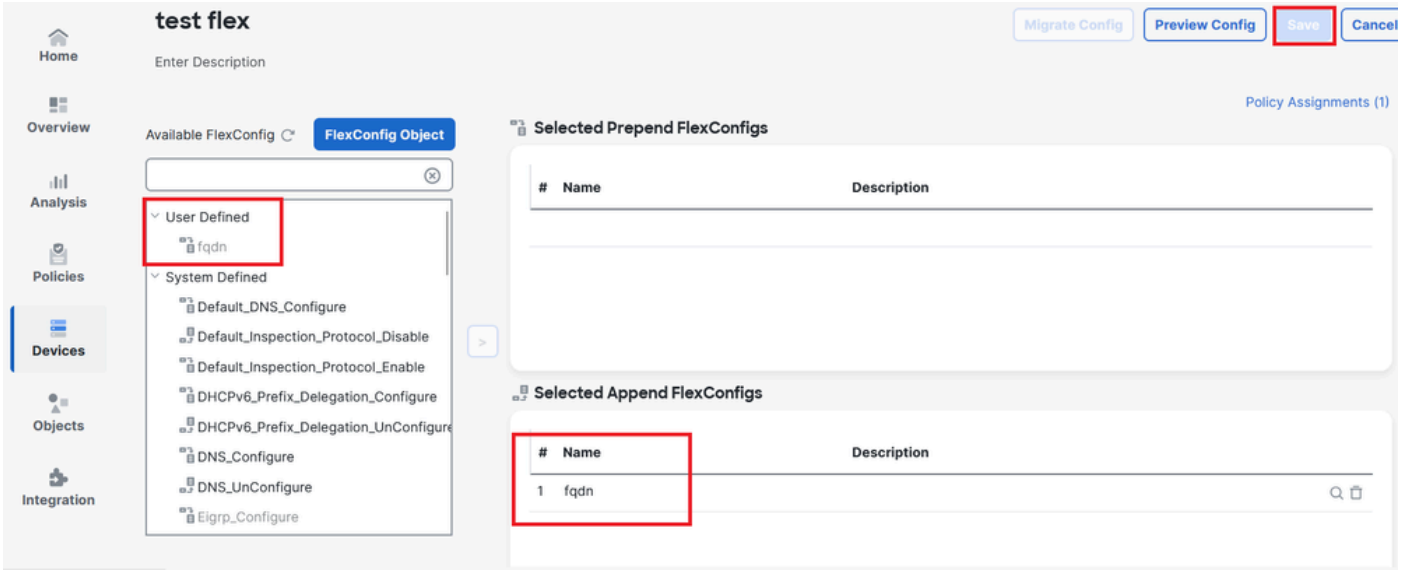


図 12.FlexConfigオブジェクトをFlexConfigポリシーに追加

確認

入力インターフェイスには、自動生成されたルートマップを持つポリシールートがあります。

<#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

ルートマップには、使用されている宛先インターフェイスを持つ選択されたACLが含まれています。

```
<#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
```

アクセスリストには、参照用のホストと、FlexConfigを使用して追加した追加ルールが含まれています。

```
<#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
```

送信元として入力インターフェイスからパケットトレーサを実行して、PBRフェーズに到達したことを確認できます。

```
<#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
```

一般的な問題

2回目の導入の後でPBRが動作しなくなる

アクセスリストにまだFQDNオブジェクトルールが含まれているかどうかを確認してください。

この場合、ルールがもはやここにないことを確認できます。

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

FlexConfigオブジェクトがDeployment: Everytime およびType: Appendとして設定されていることを確認します。このルールは、今後の展開で毎回適用されます。

FQDNが解決されない

FQDNにpingを実行しようとすると、無効なホスト名に関するメッセージが表示されます。

```
<#root>

firepower#

ping cisco.com

                ^

ERROR: % Invalid Hostname
```

DNS設定を確認します。到達可能なDNSサーバがサーバグループに存在し、ドメインルックアップインターフェイスがそれらに到達できる必要があります。

```
<#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.
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。