

# في مكحتلا ةمئاق ىلع FQDN نئاك نيوكت FMC ىلع PBR ةعسوملا لوصول

## تايوتحملا

[ةمدقملا](#)

[ةيساسالاب لطلتتلا](#)

[تابلطلتتلا](#)

[ةمدختسملاتانوكملا](#)

[ةيساساتاملولعم](#)

[نيوكتلا](#)

[ةحصلا نم ققحتلا](#)

[ةعئاشلا تالكشمللا](#)

[ةيناث رشن ةيلمع دعب لمعلا نغ PBR فقوت](#)

[FQDN لجيلال](#)

## ةمدقملا

مادختسالل (ACL) ةعسوملا لوصول ةمئاق في FQDN نئاك نيوكت ءارج دن تسمللا اذه فصي (PBR) ةسايساللا ىل دن تسمللا هيوتللا في

## ةيساسالاب لطلتتلا

### تابلطلتتلا

تاحتنملا هذبه ةفرعم كي دل نوكت ناب Cisco يصوت:

- FMC) نم آلا ةياملال رادج ةرادا زكرم
- (FTD) ةياملال رادج ديدهت نغ نم آلا عافدلا
- رآ ي ب

### ةمدختسملاتانوكملا

ةيلاللا ةيداملاتانوكملا او جماربلا تارادصلا ىل دن تسمللا اذه في ةدراولا تامولعمللا دن تست:

- 7.6.0 رادصلا VMware ل Firepower ديدهت دض عافدلا
- 7.6.0 رادصلا VMware ل نم آلا ةياملال رادج ةرادا زكرم

ةصاخ ةيلمعم ةئيب في ةدوچوملا ةزهجالا نم دن تسمللا اذه في ةدراولا تامولعمللا ءاشنلا مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دن تسمللا اذه في ةمدختسمللا ةزهجالا عيمج تادب رما يال لمحتملا ريثا تلل كمهف نم دكأتف، ليغشتلا دي قكتك بش

## ةيساسأ تامولعم

لاجملا مسا تانئاك مادختساب HTTP ريغ رورم ةكرح ىلع يفصيفي FTD حمسي ال، ايلاح  
Cisco [CSCuz98322](#) نم اءاطأل اءصت فرعم يف روكذم وه امك (FQDN) لمكلا ل لهؤملا

تاكبشلا ةيفصت نكمي، كلذعمو، ةيساسأ ال ASA ةمظنا ىلع ةمعدم ةفيظولا هذه  
FTD ىلع طقف تاقيبطتلاو

هذه مادختساب PBR نيوكتل ةعسوملا لوصول ةمئاق ىل فQDN نئاك ةفاضل كنكمي  
ةقيرطلا.

## نيوكتلا

ةءاحلا بسح FQDN تانئاك ءاشناب مق 1. ةوطخلا

### Edit Network Object



Name

Description

Network

Host  Range  Network

FQDN

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

Cancel

Save

ةكبشلا نئاك ةمئاق 1. ةروصولا

> لوصول ةمئاق > نئاكلا ةرادا > تانئاكلا تحت ةعسوم لوصول ةمئاق ءاشناب مق 2. ةوطخلا

## ة.سوم

> AAA Server

▼ Access List

Extended

Standard

> Address Pools

Application Filters

AS Path

BFD Template

Cipher Suite List

> Community 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 traf 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		

Add Extended Access List

Filter

## عسوملا لوصول ةمئاق ةمئاق 2. ةروصل

ءارج دنع هنيوكتب تمق يذلا FQDN نئاك ةيؤر كنكمي ال هنا طحال، ةديج ةءاق ةفاضا دنع ةهءول او رءصملا ديءتل ةكبشلا تانئاك لىل ءشءب.

### Edit Extended Access List Entry

Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Network Port Application Users Security Group Tag

Available Networks (+)

Source Networks (0)

Destination Networks (0)

Enter an IP address Add

Enter an IP address Add

Cancel Save

## ةديءل ةسوملا لوصول ةمئاق ةءاق ةمئاق 3. ةروصل

ف مكءل ةمئاق ءاشنإ مءي ءيءب اهلا لوصول نكمي ال ةءاق ءاشنإب مق 3. ةوطءلا PBR نيوكتل اهرفاوءو ةسوملا (ACL) لوصول.

## Add Extended Access List Entry



**Action:**

**Logging:**

**Log Level:**

**Log Interval:**  
 Sec.

**Network** | Port | Application | Users | Security Group Tag

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

اهيلا لوصول نكمي ال يتلا لوصول عمئاق ءءاق نيوك 4 ءروصل

كب صاخال FTD فءءسء (ACP) لوصول ي ف مكءءلا ءن ءل ءءاق ءاشن بءي 4 ءوطلال ءل FQDN ءئك رشن ب (FMC) لءهلا ءراءا ي ف مكءءلا ءءو موءق FQDN ءئك ماءءءساب FlexConfig ءئك لالء نم هيل ءوءرلا لءنكمي ءءء FTD

1 Add Rule

Name:  Action:  Logging:  Time Range:  Rule Enabled:

Insert:  Intrusion Policy:  Variable Set:  File Policy:

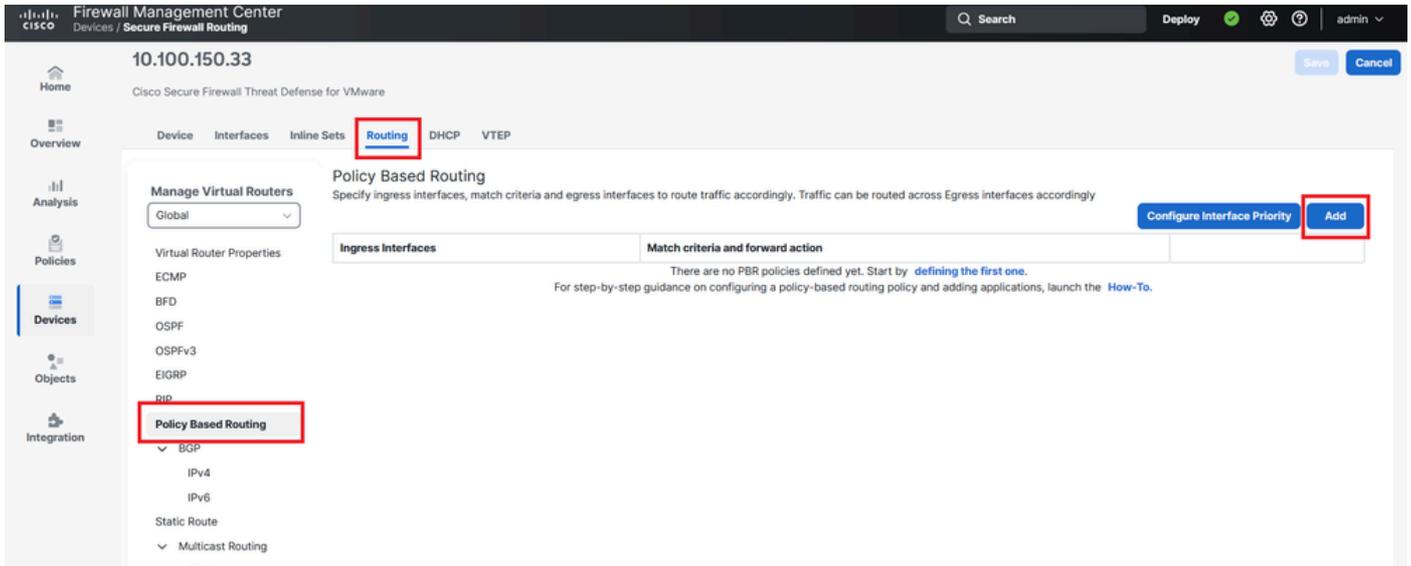
**Networks (2)** | Ports | Applications | Users | URLs | Dynamic Attributes | VLAN Tags

Showing 15 out of 15

Networks	Geolocations	Selected Sources: 1	Selected Destinations and Applications: 1
<input type="checkbox"/> any (Network Group)	0.0.0.0/0::/0	<input type="button" value="NET"/> 1 Object cisco.com	<input type="button" value="NET"/> 1 Object cisco.com
<input type="checkbox"/> any-ipv4 (Network Object)	0.0.0.0/0		
<input type="checkbox"/> any-ipv6 (Host Object)	::/0		
<input checked="" type="checkbox"/> cisco.com (Network FQDN Object)	cisco.com		
<input type="checkbox"/> IPv4-Benchmark-Tests (Network Object)	198.18.0.0/15		

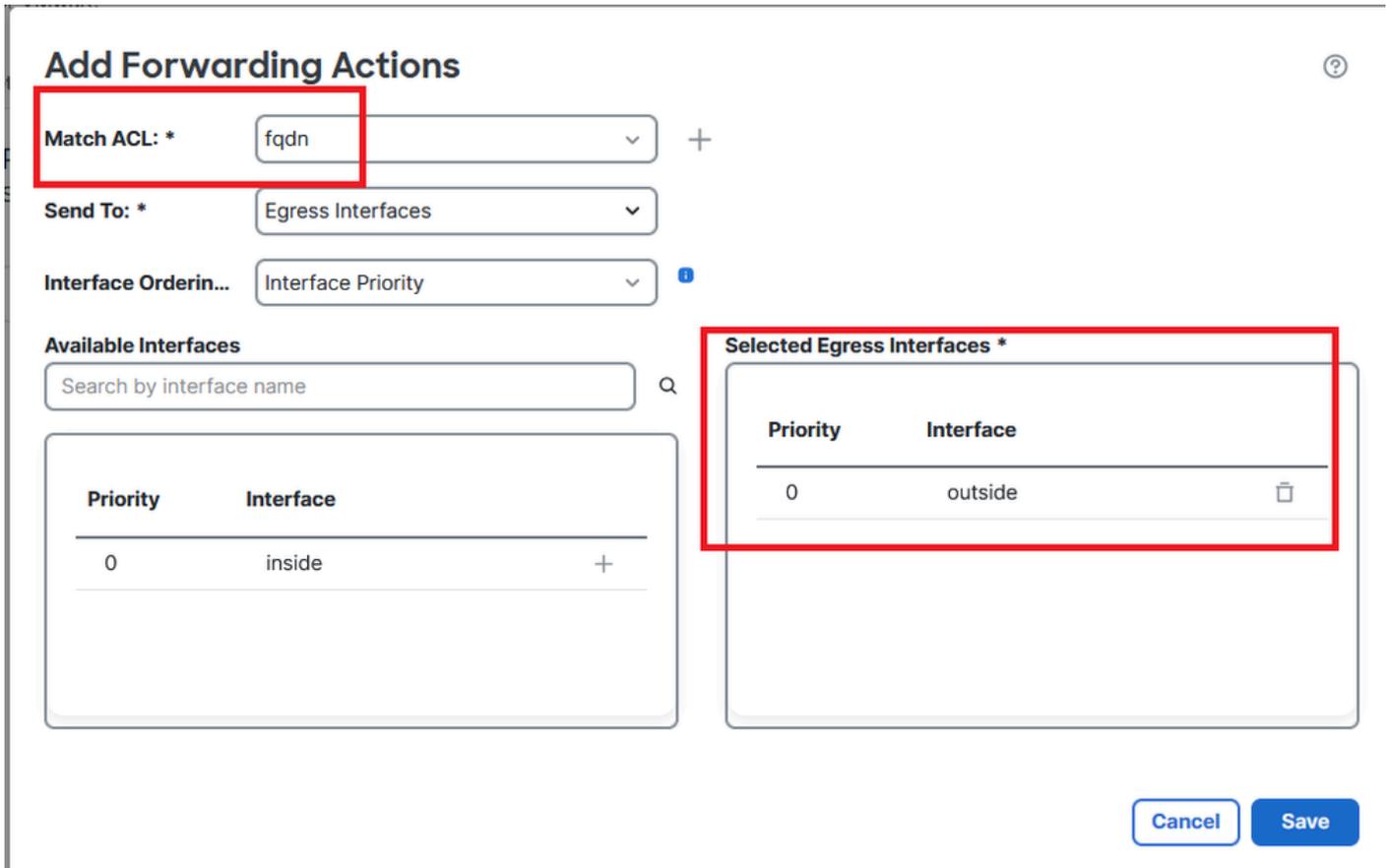
ءروصل FQDN ءئك عم ACP ءءاق 5 ءروصل

ءل ءءءناو هءءوء بءوءءلا ءمال ءءو زاهءا ءراءا > ءزهءال ءل ءءء FTD ءل ءءءنا 5 ءوطلال ءسائسلا ءل ءءءسملا هءءوءلا مسق



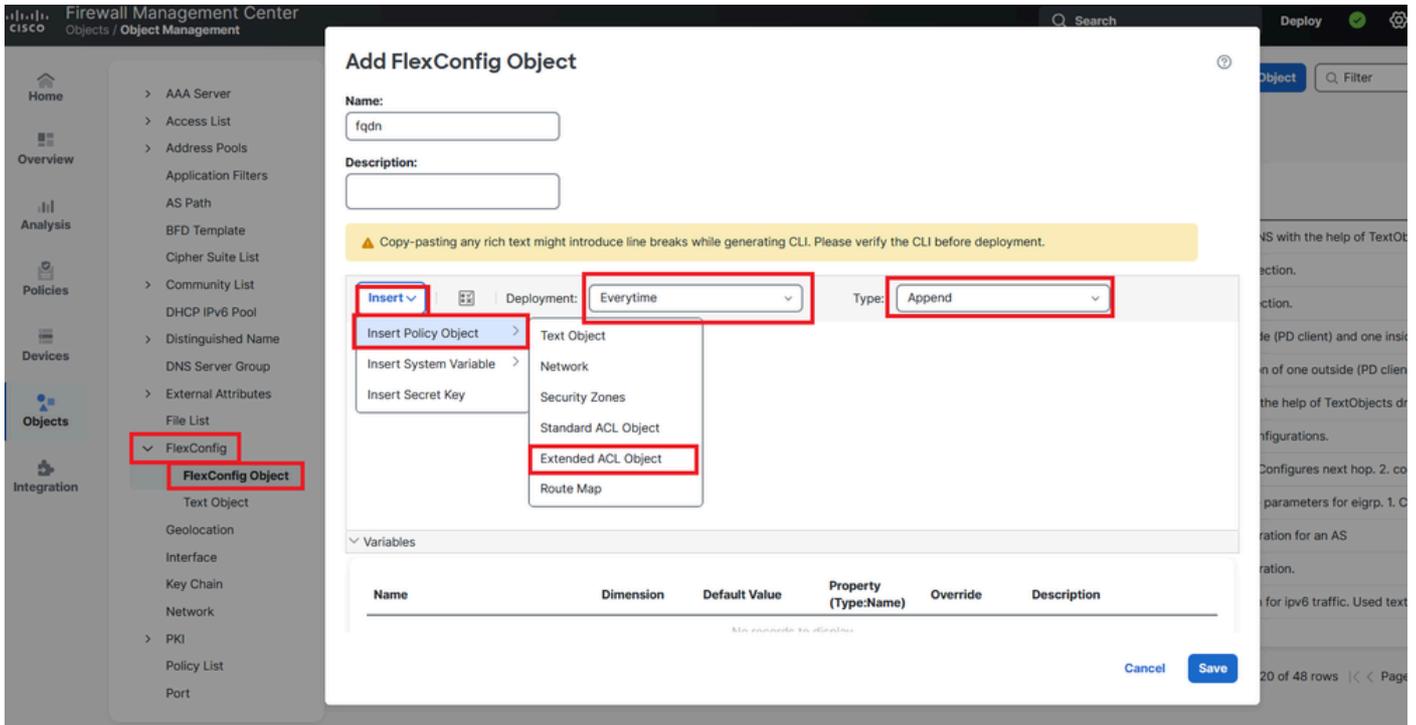
## 6. PBR ةمئاق ةروصل

م ت يتال (ACL) لوصول في مكحتال ةمئاق مادختساب ةهجاو لىع PBR نيوكت ب مق 6 ةوطخلال اهرشن مت و اقباس اهنىوكت.



## 7. لوصول في مكحتال ةمئاق ديحت ةمئاقو PBR ةهجاو 7 ةروصل

ديج نئك عاشناب مقو نئك > FlexConfig > نئال ةرادا > تانئك لىل لقتنا 7 ةوطخلال.



## FlexConfig نئىك نىوكت ەمئاق 8. ەروصل

ەمستب مقو، ەسوملا (ACL) لوصولا ي ف مكحتلا ەمئاق نئاك > چاردا ددح 8. ەوطخلا متت. اقبسم ەئاشناب تمق يتلا ەسوملا (ACL) لوصولا ي ف مكحتلا ەمئاق ددحور ي غتملا. ەمدختسأ يذلا مسالاب ري غتملا ەفاضلا.

# Insert Extended Access List Object Variable



**Variable Name:**  
fqdnacl

**Description:**

**Available Objects**

Search

fqdn

**Selected Object**  
fqdn

Add

Cancel Save

FlexConfig نئائك ل ريغتم لءاشنإ 9 ةروصل

ءصاخلا (ACL) لوصولا يف مكحتلا ةمئاقل هديرت FQDN نئاك لك ل رطسلا اذه لخدأ 9 ةوطخل  
بك.

```
<#root>
```

```
access-li $
```

```
extended permit ip any object
```

ةفاضل > ةرم لك لك كب صاخال FlexConfig نئلك ظفحا .10 ةوطخال

FlexConfig > ةزهجال نمض FlexConfig جهن ةمئاق ىل لقتنا.11 ةوطخال

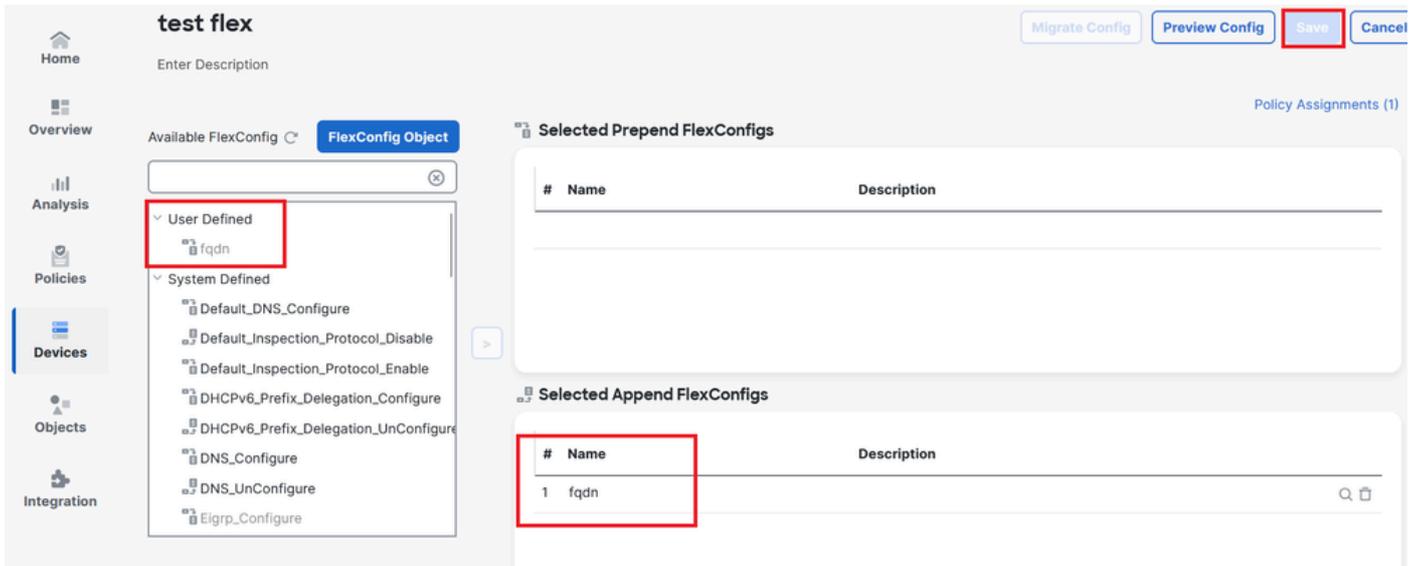
The screenshot shows the Cisco FlexConfig web interface. On the left is a vertical sidebar with navigation icons and labels: Home, Overview, Analysis, Policies, Devices (highlighted with a red box), Objects, and Integration. The main content area is titled 'Devices' and features a grid of management options. The 'FlexConfig' option is highlighted with a red box and has a blue checkmark next to it. Other options include Device Management, VPN, Troubleshoot, Template Management, Site To Site, File Download, NAT, Remote Access, Threat Defense CLI, QoS, Dynamic Access Policy, Packet Tracer, Platform Settings, Packet Capture, Snort 3 Profiling, Certificates, Troubleshooting Logs, Upgrade, Threat Defense Upgrade, and Chassis Upgrade.

FlexConfig جهن ةمئاق راسم .10 ةروصلال

كب صاخال FTD ل لعفلاب هن يي عت مت جهن ددح و ا ديج FlexConfig جهن ءاشن اب مق .12 ةوطخال

اه و اشن اب و ا ةديج FlexConfig ةسايس ريرحت .11 ةروصلال

رشن و ظفحا و ، جهن لال ىل FlexConfig نئلك فضا .13 ةوطخال



FlexConfig ةسايس لىل FlexConfig نئاك ةفاضل 12. ةروصل

## ةحصلال نم ققحتلال

اهؤاشنإ مت يتل راسملا ةطيرخ عم ةسايسل راسم ك ب ةصاخلا لوخذلا ةهجاو نمضتت ايئاقلت.

```
<#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
```

ةهجولا ةهجاو مادختساب ةددحملا (ACL) لوصولاي فم كحتلا ةمئاق لىل راسملا ططخم يوتحي ةمدختسملا.

```
<#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
```

اهتفضاً يتلأ في فاضإلأ ءءاق لآو ءءرم لآ مءءءسم لآ في ضم لآ لء لوصولآ ءمئاق يءءءء  
م FlexConfig لآ لء نم

```
<#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
```

ءلءرم PBR لآ ءءرض ءنأ ققءي نأ رءصمك نراق لءءم لآ نم tracer طءر ءلمء ءءطءسي ءنأ

```
<#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
```

## ةعئاشلا تال كشملا

ةيناث رشن ةيلمع دعب لمعلا نع PBR فقوت

FQDN نئاك ةدعاق ىلع يوتحت لازت ال لوصول ةمئاق تناك اذا ام ققحتلا عاجرلا

انه دعتمل ةدعاقلا ىرت نأ كنكمي، ةلاحلا هذه يف

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

قيبطت متي. AllTime and type: Append: رشن هنا ىلع FlexConfig نئاك دادع نم ققحت  
ةيلبقتسمل رشنلا تايلمع ىلع ةرم لك يف ةدعاقلا

## حلحلا FQDN

حلحلا ريغ فيضمل مسالوح ةلاسرىلع لصحت، FQDN لاصتا رابتخا ةلواح دنع

```
<#root>
```

```
firepower#
```

```
ping cisco.com
```

^

ERROR: % Invalid Hostname

ةومجم ىلع اهېلا لوصولا نكمې DNS مداوخ كېدل نوکې نأ بچې DNS نېوكت نم ققحت اهېلا لوصولا ىلع ەرداق لاجملا ثحب تاهجاو نوكت نأ بچېو، كب ەصاخلا مداوخلا

<#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.

