

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

تايوتحملا

[ةمدقملا](#)

[ةيساسالاب لطلتتلا](#)

[تابلطتلا](#)

[ةمدختسملاتانوكملا](#)

[ةيساسا تامولعم](#)

[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 فصبي (PBR) ةسايساللا ىل دن تسمللا هيوتلا في

ةيساسالاب لطلتتلا

تابلطتلا

تاحتنملا هذبه ةفرعم كي دل نوكت ناب Cisco يصوت:

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

ةمدختسملاتانوكملا

ةيلاللا ةيداملا تانوكملا وجماربال تارادصلا ىل دن تسمللا اذه في ةدراولا تامولعملا دن تست:

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

ةصاخ ةيلمعم ةئيب في ةدووملا ةزهجالا نم دن تسمللا اذه في ةدراولا تامولعملا ءاشنإ 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

آسياس أامول عم

لاجملا مسا تانئاك مادختساب HTTP ريغ رورم ةكرح ىلع يفصي ي فTD حمسي ال ،ايلا ح
Cisco [CSCuz98322](#) نم ااطخأل احيصت فرعم يف روكذم وه امك (FQDN) لمالكاب لهؤملا

تاكبشلا ةيفصت نكمي ،كلذ عمو ،آسياسأال ASA ةمظنا ىلع ةمعدم ةفيظولا هذه
FTD ىلع طقف تاقيبطتلاو

هذه مادختساب PBR نيوكتل ةعسوملا لوصول ةمئاق ىلإ FQDN نئاك ةفاضل كنكمي
ةقيرطلا.

نيوكتلا

ةجالح بسح FQDN تانئاك عاشناب مق 1. ةوطخلا

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

Cancel

Save

ةكبشلا نئاك ةمئاق 1. ةروصولا

> لوصول ةمئاق > نئاكلا ةرادا > تانئاكلا تحت ةعسوم لوصول ةمئاق عاشناب 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)

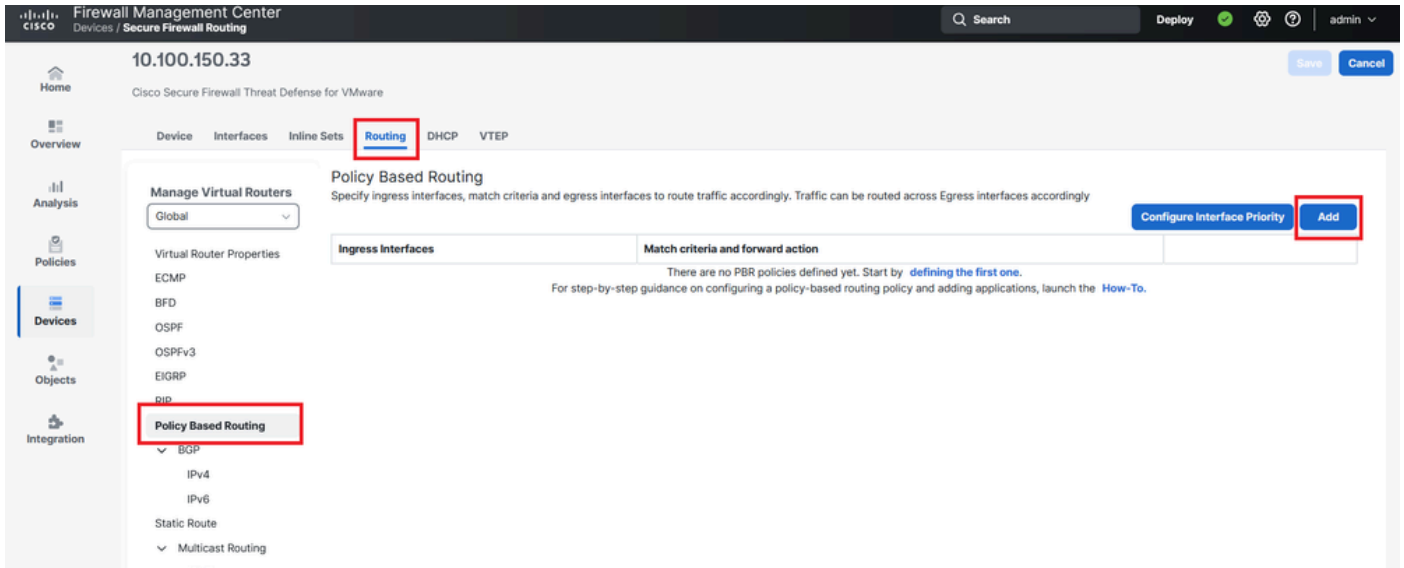
Enter an IP address Add

Enter an IP address Add

Cancel Save

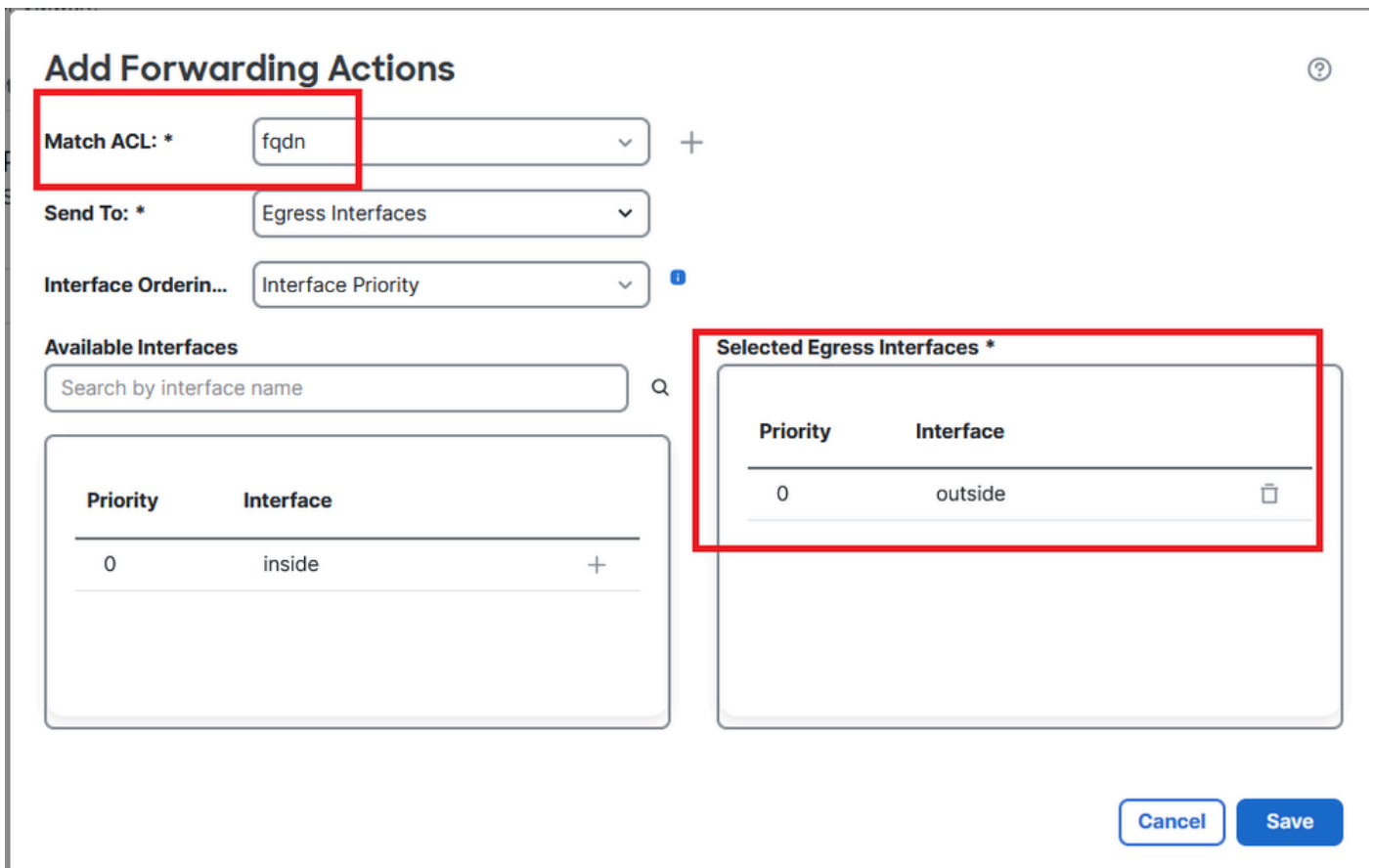
ةديءل ةسوملا لوصول ةمئاق ةءاق ةمئاق 3. ةروصل

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



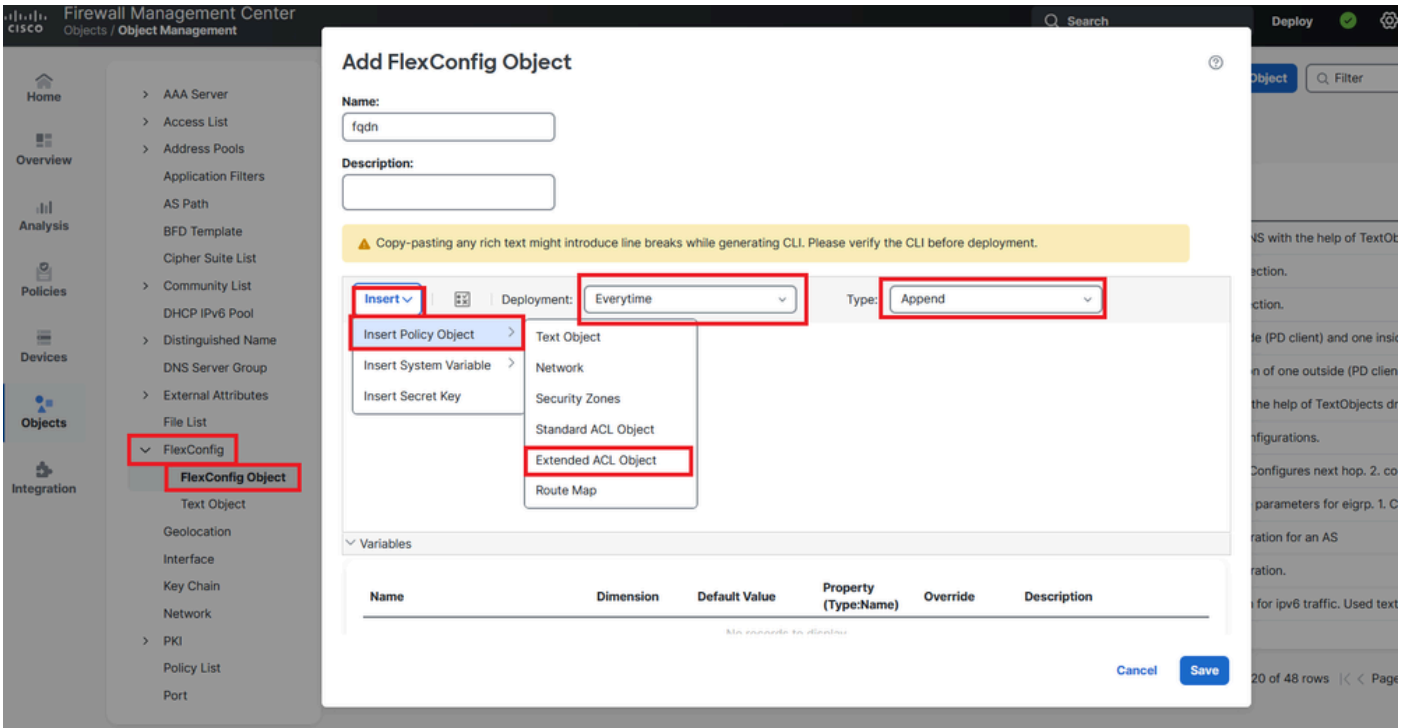
6. PBR ةمئاق ةروصل

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



7. لوصول ي ف مكحتال ةمئاق ديحت ةمئاقو PBR ةهجاو ةروصل

ديج نئاك عاشناب مقو نئاك > FlexConfig > نئال ةرادا > تانئاك لىل لقتنا 7 ةوطخلال.



FlexConfig نئىك نىوكت ەمئاق 8. ەروصل

ەمستب مقو، ەسوملا (ACL) لوصولا ي ف مكحتلا ەمئاق نئاك > چاردا ددح. ەوطخلا متت. اقبسم اهئاشناب تمق يتلا ەسوملا (ACL) لوصولا ي ف مكحتلا ەمئاق ددحوري غتملا. ەمدختسأ يذلا مسالاب ري غتملا ەفاضل.

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

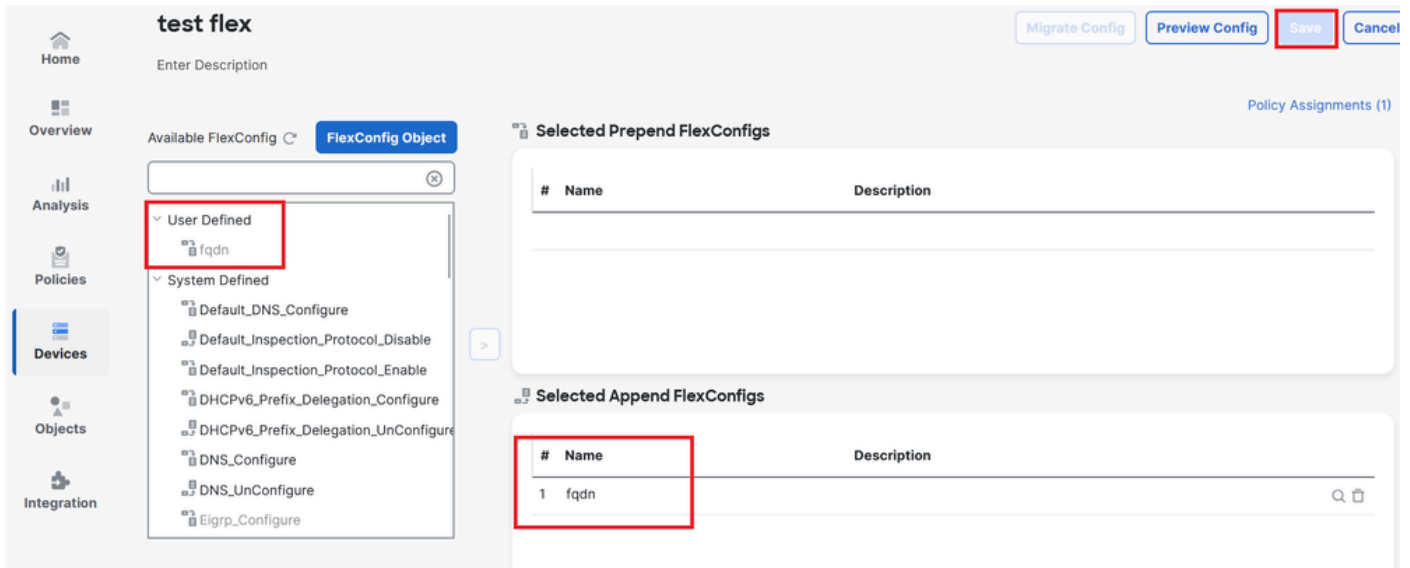
The screenshot shows the Cisco FlexConfig web interface. On the left is a vertical sidebar with icons and labels for: Home, Overview, Analysis, Policies, Devices (highlighted with a red box), Objects, and Integration. The main content area is titled 'Devices' and has a close button (X) in the top right. It is organized into a grid of categories: 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, FlexConfig (with a blue checkmark and highlighted by a red box), 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 دي دج FlexConfig جهن ءاشن اب مق .12 ةوطخال

اه و اشن و ا ة دي دج FlexConfig ة سايس 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 يتوتحي ةمدختسمل.

```
<#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 ةيفاضإلأ ةءاقلاو ءءرم لل مدءءسملا فيضملا ءلع لوصولأ ةمئاق يوتءء اهتفضأ ل FlexConfig. ءالء 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
```

ةلءرم PBR لآ ءبرض ءنأ ققءي نأ رءصمك نراق لءءملا نم tracer ءبء ءلمء ءبء ءسئي 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#
```

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

فقدن لحي ال

حلاص ريغ فيضملا مسالوح ةلاسرىلع لصحت، FQDN لاصتا رابتخا ةلواحم 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.

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومجم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء ان اعيمج يف نيمدختسمل معدى وتحم ميدقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف ان ةظحال مچري. ةصاخل متهتل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتهال ةمچرتل عم لاعل او
ىل اءاد عوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيل وئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزيلچنل دن تسمل