

# TCP ةلأح زواجت ننيوكت ننيكمت ةيفيك: FTD FlexConfig ةسايس مادختساب

## تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ننيوكتلا](#)

[ةعسوملا لوصول ةمئاق نئاك ننيوكت 1. ةوطخلا](#)

[FlexConfig نئاك ننيوكت 2. ةوطخلا](#)

[FTD لىلا FlexConfig ةسايس ننيغت 3. ةوطخلا](#)

[ققحتلا](#)

[اهخالص او ءاطخألا فاشكتسا](#)

[ةلص تاذاطاور](#)

## ةمدقملا

(TCP) لاسرإلا يف مكحتلا لوكوتورب ةلأح زواجت ةزيم ذيفنت ةيفيك دنتسملا اذه حضوي مادختساب (FMC) FirePOWER ةرادا زكرم ربع (FTD) FirePOWER ديدهت نع عافدلا ةزهجأ لىع 6.3.0 ل ةقباسلا تارادصإلا يف FlexConfig ةسايس.

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيذل نوكت ناب Cisco ي صوت:

- FirePOWER ةرادا زكرم ةفرعم.
- نارينلا ةوق ديدهت دض عافدلاب ةصاخلا ةيساسألا ةفرعملا.
- TCP ةلأح زواجت ةزيم م هف.

### ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا او جماربال تارادصإلا دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- 6.2.3 رادصإلا، Firepower (FTD) ديدهت دض عافدلا.
- 6.2.3 رادصإلا، Firepower (FMC) ةرادا زكرم.

## ةيساسأ تامولعم

دنع ةدعاسملا رفويو (ASA) فيكتلل لباقلا نامألا زاهج نم ةثوروم ةزيم TCP ةلأح زواجت دعى

TCP عي بطت تازيم لال خ نم اما اه اطاق سا نكمي يتل ا ه ا ل ص او رورم ا ة ك ر ح ا ط خ ا ف ا ش ك ت س ا .  
ت ا ق ي ب ط ت ل ل ة ن ي ع م ص ح ف ت ا ي ل م ع و ل ث ا م ت م ل ر ي غ ه ي ج و ت ل ا ط و ر ش و .

دع ب FlexConfig تانئ ا ك ف ذ ح ب ي ص و ي . 6.3.0 FMC ء د ب ر ا د ص ا ي ل ع ا ه ت ع ي ب ط ب ة م و ع د م ة ز ي م ل ا ه ذ ه  
ة ي ف ي ك ل و ح ت ا م و ل ع م ل ا ن م د ي ز م ل . ل و ا ل ر ش ن ل ل ا ب ق FMC ي ل ن ي و ك ت ل ل ا ذ ه ل ق ن و ة ي ق ر ت ل ل  
ا ذ ه [ن ي و ك ت ل ل ا ل ي ل د](#) ي ل ل ل ق ت ن ا ، ث د ح ا ر ا د ص ا و ا 6.3.0 ر ا د ص ا ل ا ي ف TCP ة ل ا ح ز و ا ج ت ن ي و ك ت

س ي ل ن ك ل و ، ت ا ز ي م ل ا ض ع ب ذ ي ف ن ت ل ASA ن ي و ك ت ر م ا و ا Firepower د ي د ه ت ن ع ع ا ف د ل ا م د خ ت س ي  
ن م ا ل د ب و . FirePOWER د ي د ه ت ن ع ع ا ف د ل ا ن ي و ك ت ر م ا و ا ن م ة د ي ر ف ة ع و م ج م د ج و ت ا ل . ت ا ز ي م ل ا ع ي م ج  
ة ر ش ا ب م ا ه م ع د م ت ي م ل ي ت ل ا ت ا ز ي م ل ا ن ي و ك ت ب ك ل ح ا م س ل ل ي ه FlexConfig ن م ة ط ق ن ل ل ا ف ، ك ل ذ  
ه ت ا د ا د ع ا و Firepower ة ر ا د ا ز ك ر م ج ه ن ل ل ا ل خ ن م د ع ب

و ا ه ا ح ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا ض ا ر غ ا ل ط ق ف TCP ة ل ا ح ز و ا ج ت م ا د خ ت س ا ب ج ي : **ة ط ح ا ل م**  
ت ا ز ي م ل ي ط ع ت ي ل ا ة ز ي م ل ا ه ذ ه م ا د خ ت س ا ي د و ي . ل ث ا م ت م ل ر ي غ ه ي ج و ت ل ل ا ل ح ن ك م ي ا ل ا م د ن ع  
ج ح ص ل ك ش ب ا ه ذ ي ف ن ت م ت ي م ل ا ذ ا ت ا ل ا ص ت ا ل ا د د ع ا ف ت ر ا ي ل ل ي د و ي د ق و ة د د ع ت م ن ا م

د ش ر م ل ي ك ش ت cisco ASA 5500 sery ل و [ASA 5500 sery ل ا ي ل ع ة م س ي ب ن ا ج ي ر ج م ة ل و د TCP](#) ل ا  
ASA، ي ف ا ه ذ ي ف ن ت و ا ة م س ز و ا ج ت ة ل و د TCP ل و ح ر ي ث ك ت ف ر ع in order to ت ل ج ا

## ن ي و ك ت ل ل ا

FlexConfig ة س ا ي س ل ا ل خ ن م FMC ي ل ع TCP ة ل ا ح ز و ا ج ت ن ي و ك ت ة ي ف ي ك م س ق ل ا ا ذ ه ف ص ي

### ة ع س و م ل ا ل و ص و ل ا ة م ئ ا ق ن ئ ا ك ن ي و ك ت . 1 ة و ط خ ل ا

ي ل ع و ، ت ا ن ئ ا ك ل ل ا ة ر ا د ا > ت ا ن ئ ا ك ل ل ا ي ل ل ل ق ت ن ا ، FMC ي ل ع ة ع س و م ل ا ل و ص و ل ا ة م ئ ا ق ا ش ن ا ل  
ClickAdd ل ة ع س و م ل ا ل و ص و ل ا ة م ئ ا ق . ع س و م د د ح ل و ص و ل ا ة م ئ ا ق ت ح ت ، ي ر س ي ل ا ة م ئ ا ق ل ل ا

The screenshot shows the Palo Alto Networks management console interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. Below this, there are tabs for 'Object Management' and 'Intrusion Rules'. A red arrow points to the 'Add Extended Access List' button in the top right corner. On the left side, there is a tree view of configuration objects. Under 'Security Intelligence', 'Network Lists and Feeds' is expanded, and 'Access List' is selected. A red circle highlights 'Access List', and another red arrow points to it from the right. Below 'Access List', 'Standard' and 'Extended' options are visible.

TCP\_Bypass م س ا ل ا ن و ك ي ، ل ا ث م ل ا ا ذ ه ي ف . ة ب و ل ط م ل ا ة م ي ق ل ا ب " م س ا ل ا " ل ق ح ة ئ ب ع ت ب م ق  
ر ز ف ي ض ي ة ق ط ق ط

## New Extended Access List Object

Name:

Entries (0)

| Sequence              | Action | Source | Source Port | Destination | Destination Port |
|-----------------------|--------|--------|-------------|-------------|------------------|
| No records to display |        |        |             |             |                  |

Allow Overrides:

ة فرعم ة كبش م ادختس ا نكمي . 'حامسلا' هنا يلع ة دعاقلا هذبه صاخلا اارجالا نيوكت بجي قباطت ، لاثملا اذه في . ةهجوو ردصم لكل ديدج ة كبش نئاك عاشن ا نكمي و ا ماظنلا ة طساوب قي بطتل لاصتالا اذه نوكي شي ح 2 فيضملا الى 1 فيضملا م IP رورم ة كرح لوصولا ة مئاق UDP و TCP ذف نم ة قباطملا اي رايتخ ا ذف نملا بيوبت ة مالع م ادختس ا نكمي . TCP ة لاج زواجت ة . عباتملا ل ة فاضا رزلا قوف رقنا . ني عم

## Add Extended Access List Entry

Action:

Logging:

Log Level:

Log Interval:  Sec.

**Network** Port

Available Networks

- any
- any-ipv4
- any-ipv6
- FMC
- Host1
- Host2
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

Source Networks (1)

- Host1

Destination Networks (1)

- Host2

ظفح يلع رقنا ، ةهجوو او ردصملا ة فيضملا تائيبللا و ا تاكبشلا دي دحت درجم

## Edit Extended Access List Object

Name:

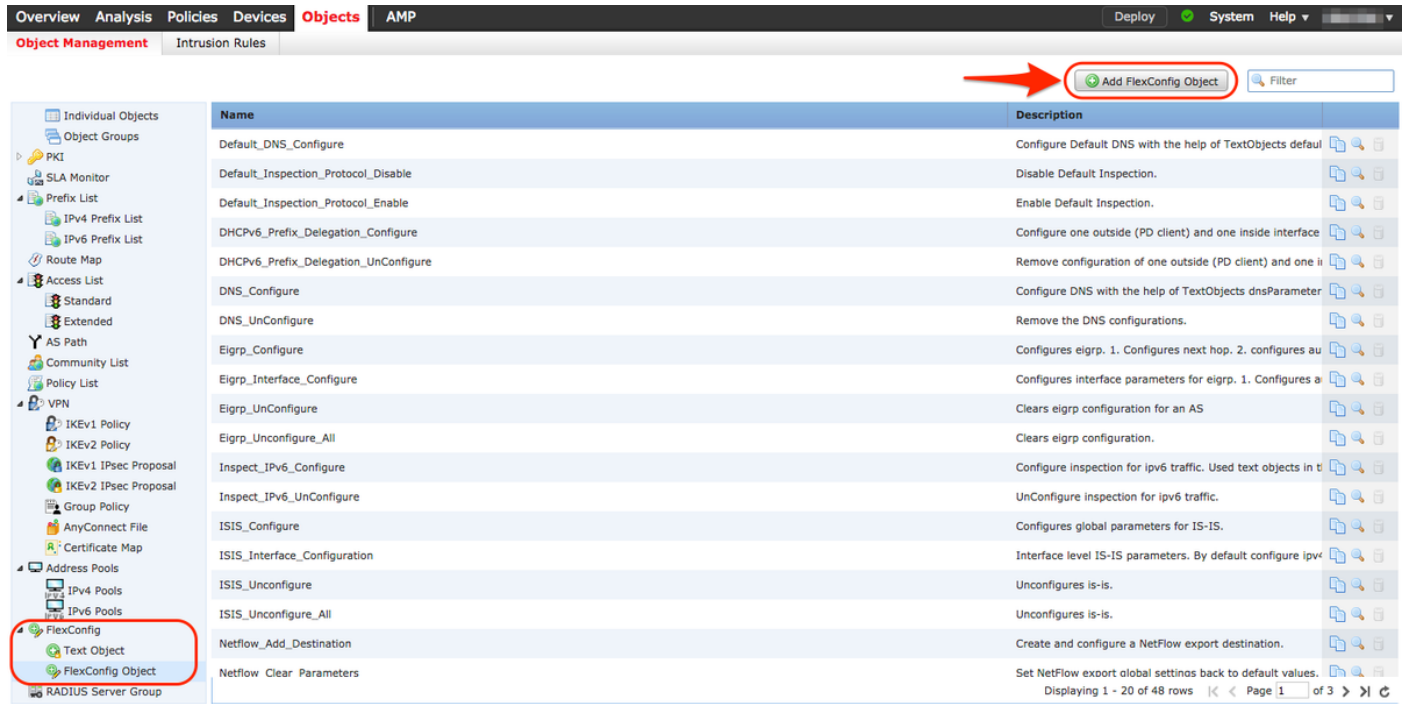
Entries (1)

| Sequence | Action | Source | Source Port | Destination | Destination Port |
|----------|--------|--------|-------------|-------------|------------------|
| 1        | Allow  | Host1  | Any         | Host2       | Any              |

Allow Overrides:

## FlexConfig نئىك نىوكت 2. ةوطخلال

ةفاضل رزى لىع رقن او FlexConfig Object > FlexConfig > نئىكلا ةرادل > تانئىكلا لىل لىلق تانئىك FlexConfig.



The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Objects' tab is active, and the 'Object Management' sub-tab is selected. In the top right corner, there is a button labeled 'Add FlexConfig Object' with a green plus icon, which is highlighted by a red arrow. Below the navigation bar, there is a table with columns 'Name' and 'Description'. The table lists various configuration objects, including 'Default\_DNS\_Configure', 'Default\_Inspection\_Protocol\_Disable', 'Default\_Inspection\_Protocol\_Enable', 'DHCPv6\_Prefix\_Delegation\_Configure', 'DHCPv6\_Prefix\_Delegation\_UnConfigure', 'DNS\_Configure', 'DNS\_UnConfigure', 'Eigrp\_Configure', 'Eigrp\_Interface\_Configure', 'Eigrp\_UnConfigure', 'Eigrp\_Unconfigure\_All', 'Inspect\_IPv6\_Configure', 'Inspect\_IPv6\_UnConfigure', 'ISIS\_Configure', 'ISIS\_Interface\_Configuration', 'ISIS\_Unconfigure', 'ISIS\_Unconfigure\_All', 'Netflow\_Add\_Destination', and 'Netflow\_Clear\_Parameters'. The 'FlexConfig' category is highlighted in the left sidebar, and the 'FlexConfig Object' option is also highlighted. The bottom of the table shows 'Displaying 1 - 20 of 48 rows' and 'Page 1 of 3'.

اذه قباطتي نأ مزلي ال. لوصول ةمئاق لثم TCP\_Bypass لاثملا اذهل نئىكلا مسالى مسي لوصول ةمئاق مسالى.

ةوسوملا لوصول ي ف مكحتلا ةمئاق نئىك > جهن نئىك جاردا دح.

## Add FlexConfig Object

Name:

Description:

Deployment:  Type:

Insert

- Insert Policy Object
- Insert System Variable
- Insert Secret Key

- Text Object
- Network
- Security Zones
- Standard ACL Object
- Extended ACL Object**
- Route Map

Variables

| Name                  | Dimension | Default Value | Property (Ty... | Override | Description |
|-----------------------|-----------|---------------|-----------------|----------|-------------|
| No records to display |           |               |                 |          |             |

Save Cancel

ءانثأ نيوكتلا اذه ىلع ظافحلاب حمسي اذهو . "ةرم لك" راىخلا رايختإ نم دكأت :ةظحالم ىرخألا ةيقرتلل اورشنللا تايلمع

نبيعتب مقو ةحاتملا تانئلكلا مسق نم 1 ةوطخلا يف اهؤاشنإ مت يتيلا لوصولا ةمئاق دح TCP\_Bypass مسإ ريغتتم لا ،لاثم اذه يف . ةفاضل رزلا قوف رونا ،لكذ دعب . ريغتتم مسأ

ظفح قوف رونا

## Insert Extended Access List Object Variable



Variable Name:

Description:

Available Objects

TCP\_Bypass

Selected Object

TCP\_Bypass

نېمضتېب موقوچاردا رزلا لفسا غرافال لقلحلا يف ةيلاتلا نيوكتلا طوطخ ةفاضاب مق ظحال *match access-list* نيوكت رطس يف (**\$TCP\_Bypass**) اقبس م هفيرت مت يذلا ريغتملا اذى عبتى ريغتملا نأ فيرتى لىل دعاسى اذى. ريغتملا مسال قباس \$ زم رنا

```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

ناك اذا. ةيخراخال ةهجال لىل اهقېببط متى و ةسايس ةطيخ عاشنإ متى، لاثملا اذى يف ةئف ةطيخ قېببط نكمى، ةيملال ةمدخلال ةسايس نم عزك TCP ةلاح زواجت نيوكت مزلي *tcp\_bypass* لىل *global\_policy*.

ءاهت نالا دن ع ظفح لىل رقنا.

## Add FlexConfig Object

Name:

Description:

Deployment:  Type:

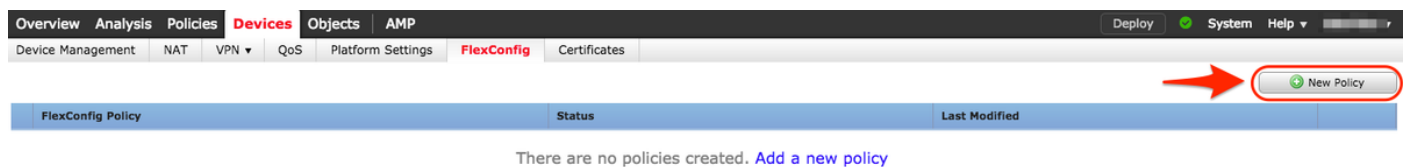
```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

**Variables**

| Name                  | Dimension | Default Value | Property (Ty... | Override | Description |
|-----------------------|-----------|---------------|-----------------|----------|-------------|
| No records to display |           |               |                 |          |             |

### FTD ىل FlexConfig ةسايس نييعت 3. ةوطخلا

هؤاشنإ مت چهن كانه نكي مل ام) ةديج ةسايس ئشنأ FlexConfig > ةزهجالا ىل لقتنا FelxConfig چهن ىمسي، لاثملا اذه في. (FTD سفن ىل هنييعت مت ورخأ ضرغل لعفلاپ ل TCP\_Bypass ديجال



FTD زاھج FlexConfig TCP\_Bypass ةسايس صيصختب مق.

## New Policy



Name:

Description:

**Targeted Devices**

Select devices to which you want to apply this policy.

**Available Devices**

FTD

**Selected Devices**

FTD

فرعم مسقلا تحت 2 ةوطخلا يف هؤاشنإ مت يذلا TCP\_Bypass ىمسمل FlexConfig نئاك دح جهنلا ىلإ نئال اذه ةفاضل مهسلا قوف رقن او مدختسمل لبق نم

Overview Analysis Policies **Devices** Objects AMP Deploy System Help

Device Management NAT VPN QoS Platform Settings **FlexConfig** Certificates

**TCP\_Bypass** TCP State Bypass

You have unsaved changes

Policy Assignments (1)

**Available FlexConfig** FlexConfig Object

- User Defined
  - TCP\_Bypass
- System Defined
  - Default\_DNS\_Configure
  - Default\_Inspection\_Protocol\_Disable
  - Default\_Inspection\_Protocol\_Enable
  - DHCPv6\_Prefix\_Delegation\_Configure
  - DHCPv6\_Prefix\_Delegation\_UnConfigure
  - DNS\_Configure
  - DNS\_UnConfigure
  - Eigrp\_Configure
  - Eigrp\_Interface\_Configure
  - Eigrp\_UnConfigure
  - Eigrp\_Unconfigure\_All
  - Inspect\_IPv6\_Configure
  - Inspect\_IPv6\_UnConfigure
  - ISIS\_Configure
  - ISIS\_Interface\_Configuration
  - ISIS\_UnConfigure
  - ISIS\_Unconfigure\_All
  - Netflow\_Add\_Destination
  - Netflow\_Clear\_Parameters

**Selected Prepend FlexConfigs**

| # | Name | Description |
|---|------|-------------|
|---|------|-------------|

**Selected Append FlexConfigs**

| # | Name       | Description      |
|---|------------|------------------|
| 1 | TCP_Bypass | TCP State Bypass |

،رشنلاو تاريخيغتل ظفح



| ✓ | Device   | Group | Current Version     |
|---|--|-------|---------------------|
| ✓ | FTD  |       | 2017-08-18 01:06 AM |
|   | <ul style="list-style-type: none"> <li>✓ Nat Policy: NAT-Lab</li> <li>✓ NGFW Settings: Platform_Lab</li> <li>⚙ FlexConfig Policy: TCP_Bypass</li> <li>✓ Access Control Policy: Policy_FTD</li> <li>✓ --- Intrusion Policy: Balanced Security and Connectivity</li> <li>✓ --- DNS Policy: Default DNS Policy</li> <li>✓ --- Prefilter Policy: Default Prefilter Policy</li> <li>✓ Network Discovery</li> <li>✓ Device Configuration(<a href="#">Details</a>)</li> </ul> |       |                     |

Selected devices: 1

Deploy

Cancel

## ققحتلا

system support diagnostic-cli مألرم أمدختساو م كحتلا ةدحو وأ SSH لال خ نم FTD لى لوصولاب مق cli.

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
firepower# show access-list TCP_Bypass
```

```
access-list TCP_Bypass; 1 elements; name hash: 0xec2b41eb
```

```
access-list TCP_Bypass line 1 extended permit object-group ProxySG_ExtendedACL_34359739205
```

```
object Host1 object Host2 log informational interval 300 (hitcnt=0) 0x42940b0e
```

```
access-list TCP_Bypass line 1 extended permit ip host 1.1.1.1 host 1.1.1.2 log informational
```

```
interval 300 (hitcnt=0) 0x769561fc
```

```
firepower# show running-config class-map
```

```
!
```

```
class-map inspection_default
```

```
match default-inspection-traffic
```

```
class-map tcp_bypass
```

```
match access-list TCP_Bypass
```

```
!
```

```
firepower# show running-config policy-map
```

```
!
```

```
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
router-alert action allow
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
!
```

## اهحال صا و عاطخ ال فاشكت سا

ةدع اسم رم او ال هذه نع جت ني ، ا ه حال صا و ة زي مل ا هذه عاطخ ا فاشكت سا

### - show conn [detail]

Shows connection information. Detailed information uses flags to indicate special connection characteristics.

For example, the "b" flag indicates traffic subject to TCP State Bypass

### - show service-policy

Shows service policy statistics, including Dead Connection Detection (DCD) statistics

## ةلص تا ذ ط باور

[https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa\\_91\\_firewall\\_configuration/conns\\_connlimits.html](https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_configuration/conns_connlimits.html)

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118995-configure-asa-00.html>

[https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configuration-guide-v62/flexconfig\\_policies.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configuration-guide-v62/flexconfig_policies.html)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل