

اهبې ترتو IP ىل لوصولا مئوق نيوكت

تايوت حمل

قم دق م

قېساس انا تابل ط م

تابل ط م

قم دخت س م ا تان و م

تاجال ط ص ا

قېساس ا تامول عم

(ACL) لوصولا ىف مكحت ل مئوق مئوق

قنق

(ACL) لوصولا ىف مكحت ل مئوق مئوق صىخت

(ACL) لوصولا ىف مكحت ل مئوق مئوق قنق

لئاس رل او ذفان م ا عاون ا دى دخت

(ACL) لوصولا ىف مكحت ل مئوق مئوق قى ب ط

قنق و ل او ر دص م ا و ر داص ل او دراو ل او چراخ ل او ل خا د ل ا دى دخت

(ACL) لوصولا ىف مكحت ل مئوق مئوق رى دخت

اهجال ص او عا ط خ ا ل فاش ك ت س ا

IP ىل لوصولا ىف مكحت ل مئوق مئوق عاون ا

قنق ب ش ل ل ل ط ي ط خ ت ل م س ر ل ا

قېساس ا ق ل ل لوصولا ىف مكحت ل مئوق مئوق

قنق س و م ل لوصولا ىف مكحت ل مئوق مئوق

IP

ICMP

TCP

UDP

(قېكې مئوق د ل ا (ACL) لوصولا ىف مكحت ل مئوق مئوق) خات ف م ل او ل ق ل ل ا

IP ىل ا ق م س م ل ا (ACL) لوصولا ىف مكحت ل مئوق مئوق

قېساس ك ع ل ا (ACL) لوصولا ىف مكحت ل مئوق مئوق

تق و ل ا تاقاطن مادخت س ا ب تق و ل ا ىل ا ق د ن ت س م ل ا (ACL) لوصولا ىف مكحت ل مئوق مئوق

ا ه ل ع ق ي ل ع ت ل ا م ت ي ت ل ا IP ىل ا (ACL) لوصولا ىف مكحت ل مئوق مئوق تال خا د ا

ق ا ي س ل ا ىل ا د ن ت س م ل ا لوصولا ىف مكحت ل مئوق مئوق

قنق داص م ل ل ل و

Turbo نم (ACL) لوصولا ىف مكحت ل مئوق مئوق

تق و ل ا ىل ا ق د ن ت س م ل ا ق ن و م ل ا (ACL) لوصولا ىف مكحت ل مئوق مئوق

(ACL) لوصولا ب مكحت ل مئوق مئوق ل ا ب ق ت س ا

قېساس ا ل ا ق ن ب ل ا ق ي ا م ح ل (ACL) لوصولا ىف مكحت ل مئوق مئوق

قنق ا ع ل ا (ACL) لوصولا ىف مكحت ل مئوق مئوق

قنق ص ت ا ذ تامول عم

قم دق م

فيكو IP ىل (ACLs) لوصولو في مكحتلا مئوقو نم ةفلتخم اعاونأ دنتسمل اذه فصوي ةكبشلا رورم ةكرح ةيفصت اهنكمي.

ةيساسال تابلطتملا

تابلطتملا

اهتشقانم تمت يتي لهافملا رفوتت. دنتسمل اذهل ةصاخ ةيساسا تابلطتم دجوت ال ةمئاق في ةزيم لك نمض كلذ ةظحالم متتو. ثحلأا و Cisco IOS® Software 8.3 جمارب تارادصا في لوصول.

ةمدختسمل تانوكملا

هذه ضعب رفوتت (ACL) لوصولو في مكحتلا مئوقو نم ةفلتخم اعاونأ دنتسمل اذه لوانتي تارادصا في هميدقت مت رخآال اهضعبو 8.3 رادصال، Cisco IOS جمانربلا تارادصا ذنم رصانعل اعون لك ةشققانم في كلذ ةظحالم متتو. ةقحلال جماربلا


ةصاخ ةيلعم ةئيب في ةدوجوملا ةزهجال نم دنتسمل اذه في ةدراول تامولعمل اعاشنإ مت تناك اذإ. (يضارتفا) حوسمم نيوكتب دنتسمل اذه في ةمدختسمل ةزهجال اعيمج تادب رمأ يال لمحتملا ريثأتلل كمهف نم دكأتف، ليغشتلا ديقت كتكبش

تاحالطصالا


تاحالطصا لوح تامولعمل نم ديزم ىلع لوصولل [ةينقتلا Cisco حئاصن تاحالطصا](#) عجار تادننتسمل.

ةيساسا تامولعمل

IP ىل (ACLs) لوصولو في مكحتلا مئوقل اهب نكمي يتي ةيفيكل دنتسمل اذه حضوي تازيملا رفوتتو ACL IP اعونأل ةزجوم فاصوا ىلع يوتحي امك. ةكبشلا رورم ةكرح ةيفصت ةكبش في مادختسالل لاثمو.

 ىلع [RFC 1918 يوتحي](#). ةفورعمل ذفانملا نم ةنيعم دادعأ ىلع [RFC 1700](#) يوتحي: ةظحالم ةداع اهتيرؤر مدع بجي يتي ال IP نيوانعو ةصاخلا تنرتنإلا تاكبشل ناوعلا صيصخت تنرتنإلا ىلع.

 ةيلخادلا تامولعمل ىل لوصولو نيلجسمل Cisco في مدختسمل طقف نكمي: ةظحالم.

 ىل رورملا ةكرح ديدحتل اضيا (ACL) لوصولو في مكحتلا مئوق مادختسا نكمي: ةظحالم IP اهل سيل يتي تالالوكوتوربلا ةيفصت وأ اهريفشت وأ (NAT) ةكبشلا ناوع ةمچرت دنتسمل اذه قاطن جراخ فئاظولا هذهل ةشققانم دجوت. AppleTalk و IPX.

ACL) لوصولي ف مكحتل ةمئاق ميهافم

ةعنقأ

بجي ام ديحتل IP لوصولاب مكحتل ةمئاق في IP نيوانع عم ةعنقأل مادختسا متي تاهجاولا لىل IP نيوانع نيوكت لجأ نم 255 ةميقب ةعنقأل أدبت. هضفر بجي امو هب حامسلا عم 10.165.202.129 IP ناوع، لاثملا لىبس لىل، رسيأل بانجال لىل ةريكبلا ميقلل نوكتو لاثملا لىبس لىل، سكالل يه IP لوصولاب مكحتل ةمئاق ةعنقأ. 255.255.255.224 ةانق ةميق ميستقت متي ام دنع. لذب فرح ةانق وأ يسكع ةانق أنايحأ اذه ىمسي. 0.0.0.255 ةانق بجي يتل نيوانعلا تب تادحو جئاتنلا ددحت، (داحأل او رافصأل) ةيئانث ميقل لىل ةانقلا قباطت) نيوانعلا تب تادحو ةاعارم بجي هنأ لىل 0 ريشي. رورملا ةكرح ةجالعم دنع اهتاعارم ركبأ لكشب موهفملا لودجال اذه حرشي. ةانقلا في 1 متهت ال؛ (مات

ةانقلا لىل لاثم	
10.1.1.0 (اهتجالعم متتس يتل رورملا ةكرح) ةكبشلا ناوع	
0.0.0.255	ةانقلا
00001010.00000001.00000001.00000000	(ةيئانثلا ميقللاب) ةكبشلا ناوع
00000000.00000000.00000000.11111111	(ةيئانثلا ميقللاب) ةانق

ثالثلا تاعومجملا قباطت بجي هنأ ىرت نأ كنكمي، ةيئانثلا ميقللاب ةانقلا لىل أدانتسا ددحمل ةيئانثلا ميقللاب ةكبشلا ناوع عم أمامت (ةينامثلا ةمظنأل) لىل وأل، لكذل. (11111111). متهت ال ماقرأل نم ةريخأل ةعومجملا. (00001010.00000001.00000001). ثرتكي ال ريخأل ينامثلا ماطنلا نأ امب. 10.1.1. ب أدبت يتل رورملا تاكرح لك قباطت. 10.1.1.255 لىل 10.1.1.1 نم ةكبشلا نيوانع ةجالعم متت، ةانقلا اذه مادختساب، لكذل (10.1.1.x).

لوصولاب مكحتل ةمئاقل سوكعمل ةانقلا ديحتل 255.255.255.255 نم يداعال ةانقلا حرطا يداع ةانقب 172.16.1.0 ةكبشلا ناوع لىل سوكعمل ةانقلا ديحت متي، لاثملا اذه في. (ACL) 255.255.255.0.

- 255.255.255.255 - 255.255.255.0 = 0.0.0.255 (سوكعمل ةانقلا) (يداعال ةانقلا)

(ACL) لوصولي ف مكحتل ةمئاق تالداعم ظحال

- ي. 0.0.0.0/255.255.255.255 لىل فرح/ردصملا ينع ي.
- 10.1.1.2 فيضملا هسفن وه 10.1.1.2/0.0.0.0 لىل فرح/ردصملا.

(ACL) لوصولي ف مكحتل ةمئاق صيخلت

لىل. تبثا لوط يذ نيودتك ةي عرفلا ةكبشلا ةعنقأ ليثمت اضيأ نكمي: ةظحالم 192.168.10.0/24 لىل 192.168.10.0، لاثملا لىبس

ةمئاق نيوسحتل ةدحاو ةكبش في تاكبشلا نم ةعومجم صيخلت ةي في ةمئاقلا هذه فرصت. تاكبشلا لىل رابتعالا في عض. (ACL) لوصولي ف مكحتل

192.168.32.0/24
 192.168.33.0/24
 192.168.34.0/24
 192.168.35.0/24
 192.168.36.0/24
 192.168.37.0/24
 192.168.38.0/24
 192.168.39.0/24

ةيفيكل حرش وه لودجلا اذه .ةكبش لكل اهسفن يه ينامث ماظن رخآو ناينامث ناماظن لوأ
 ةدحاو ةكبش يف اهصيخلت

لودجلا اذه يف حضورم وه امك ةقباسلا تاكبش لل ثلاثلا ينامثلا ماظنلا ةباتك نكمي
 تب لكل ناوعلا ةميقو تب ينامث ماظن حضورم لىا لسارمو

يرشع	128	64	32	16	8	4	2	1
32	0	0	1	0	0	0	0	0
33	0	0	1	0	0	0	0	1
34	0	0	1	0	0	0	1	0
35	0	0	1	0	0	0	1	1
36	0	0	1	0	0	1	0	0
37	0	0	1	0	0	1	0	1
38	0	0	1	0	0	1	1	0
39	0	0	1	0	0	1	1	1
	M	M	M	M	M	D	D	D

ةقباسلا ينامثلا تاكبشلا صيخلت نكمي ف ،تقباطت لىلوالا سمخلا تبال تادحو نأ امب
 ةينامثلا تاعومجم لاعيجم .(192.168.32.0 255.255.248.0 وأ 192.168.32.0/21) ةدحاو ةكبش يف
 ةكبشلا تاقاطنبة لصل تاذ صفخنم لبيترتلا تاذ ةثالثلا تبال تادحو نم ةنكمم ل
 تمق اذا .ةكبشلا هذهل حمسي يذلا (ACL) لوصولا يف مكحت ةمئاق رمالا اذه ددحي .ةينعم ل
 0.0.7.255 حتني هناف ،255.255.255.255 نم (يداعلا عانقلا) 255.255.248.0 حرطب

<#root>

```
access-list acl_permit permit ip 192.168.32.0 0.0.7.255
```

حيضوتلا نم ديزمل تاكبشلا نم ةعومجم ل هذه يف ركف

192.168.146.0/24
 192.168.147.0/24
 192.168.148.0/24
 192.168.149.0/24

ةيفيكل حرش وه لودجال اذه .ةكبش لكل اهسفن يه ينامث ماظن رخاؤ ناينامث ناماظن لوا اهصيخلت

لودجال اذه يف حضورم وه امك ةقباسلا تاكبش لل ثلاثلا ينامثلا ماظنلا ةباتك نكمي ، تب لكل ناونعلا ةميقو تب ينامث ماظن حضورم ل لسارمو

يرشع	128	64	32	16	8	4	2	1
146	1	0	0	1	0	0	0	1
147	1	0	0	1	0	0	0	1
148	1	0	0	1	0	1	0	0
149	1	0	0	1	0	1	0	1
	M	M	M	M	M	?	?	?

مت اذ .ةدحاو ةكبش يف تاكبش لل كلت صيخلت كنكمي ال ،قباسلا لاثملا فالخب ةهباشتم تب تادحو سمخ كانه نأل 192.168.144.0/21 حبصت اهنإف ،ةدحاو ةكبش ل اهصيخلت نم ةعومجم 192.168.144.0/21 ةصخلملا ةكبش ل هذه ي طغت .ثلاثلا ينامثلا ماظنلا يف 192.168.144.0 ، تاكبش ل هذه ني نم 192.168.151.0 لىا 192.168.144.0 نم تاكبش ل عبرأل ةدحملا ةمئاقلا يف ةجردم تسي ل 192.168.151.0 و 192.168.150.0 و 192.168.145.0 و 192.168.144.0 نكمي .يندا دحك ني تصخلم ني تاكبش لىا جاتحت ،ةدحملا تاكبش لة ي طغت لجا نم . تاكبش نيتكبش ل ني تاه يف ةدحملا عبرأل تاكبش ل صيخلت

- تبلا تادحو عيمج قباطت ، 192.168.147.x و 192.168.146.x تاكبش ل ةبس نلاب (أ و 192.168.146.0/23 يلى امك اذه ةباتك نكمي .متهت ال يهو ،ةريخأ ل اناثتساب 192.168.146.0 255.255.254.0).
- تبلا تادحو عيمج قباطت ، 192.168.149.x و 192.168.148.x تاكبش ل ةبس نلاب (أ و 192.168.148.0/23 يلى امك اذه ةباتك نكمي .متهت ال يهو ،ةريخأ ل اناثتساب 192.168.148.0 255.255.254.0).

ةقباسلا تاكبش ل ةصخلم (ACL) لوصولا يف مكحت ةمئاق جارخا ل اذه دحى

<#root>

!--- This command is used to allow access access for devices with IP
!--- addresses in the range from 192.168.146.0 to 192.168.147.254.

access-list 10 permit 192.168.146.0 0.0.1.255

<#root>

!--- This command is used to allow access access for devices with IP
!--- addresses in the range from 192.168.148.0 to 192.168.149.254

access-list 10 permit 192.168.148.0 0.0.1.255

ACL) لوصولي ف مكحتل مئوق ةجلع

أدانتسا (ACL) لوصولاب مكحتل مئوق تالخداب ةجوملإ إلإ ةدراول رورملا ةكرح ةنراقم مت ةمئاقلا ةياهن إلإ ةديجل تارابعلا ةفاضإ متت. ةجوملإ يف تالخدإل راركت بيترت إلإ دن ع تاقباطت يأل ع رثعُي مل إذا. قباطت هي دل حبصي يتح ثحبلا يف ةجوملإ رممتسي كي دل نوكي نأ بجي، ببسلا اذل. رورملا ةكرح ضفرت متي، ةمئاقلا ةياهن إلإ ةجوملإ لوصولي نمض ضفرك انه. ةمئاقلا إلعأ يف رركتم لكشب اهيلإ لوصولا متي يتل تالخدإل ةيدألا (ACL) لوصولا يف مكحتل مئوق موقت نأ نكمي. اهب حومسملا ريغ رورملا ةكرح نوكي نأ بجي. رورملا تاكل عي مج ضفرب طقف دحاو ضفرب لخدإ إلع يتحت يتل لخدإل ةكرح نم متيسف إلو لوصولا يف مكحت مئوق يف لقالا إلع ةدحاو حامس ةرابع كي دل ريثأتلا امهل (101 و 102) (ACL) لوصولا يف مكحتل مئوق نم ناعونلا ناذه. اهلماكب رورملا هسفن.

<#root>

```
!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected.
```

```
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

<#root>

```
!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected.
```

```
access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 102 deny ip any any
```

نمضت ي IP نأل إلوألا ةثالثل تالخدإل إلإ جاتحت ال. فاك ريخألا لخدإل، يتل للاثملا يف يف مكحتل لئاسر لوكوتوربو (UDP) مدختسملا تانايب طاطخم لوكوتوربو و TCP لوكوتوربو (ICMP) تنرتنإل.

<#root>

```
!--- This command is used to permit Telnet traffic
!--- from machine 10.1.1.2 to machine 172.16.1.1.
```

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

<#root>

!--- This command is used to permit tcp traffic from
!--- 10.1.1.2 host machine to 172.16.1.1 host machine.

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1
```

<#root>

!--- This command is used to permit udp traffic from
!--- 10.1.1.2 host machine to 172.16.1.1 host machine.

```
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1
```

<#root>

!--- This command is used to permit ip traffic from
!--- 10.1.1.0 network to 172.16.1.10 network.

```
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

لئاسرلواو ذفانملا عاونأ ديدحت

اضيأ كنكمي نكلو، ةهوجلواو (ACL) لوصولا ي ف مكحت ةمئاق ردصم ديدحت طقف كنكمي ال
[أديج أردصم RFC 1700](#) دعي. ىرخألا تاملعملواو ICMP لوكوتورب لئاسرول ذفانملا عاونأ ديدحت
RFC 792 ي ف ICMP لوكوتورب لئاسر عاونأ حرش متي. [ةفورعملل ذفانملا بة صاخلا تامولعملل](#)
792 .

ىلع لوصولل a؟ مدختست له. ةفورعملل ذفانملا ضع ب ىلع ي ف صوصن ضرع ةجوملل نكمي
ةدعاسملا.

<#root>

```
access-list 102 permit tcp host 10.1.1.1 host 172.16.1.1 eq ?
```

bgp	Border Gateway Protocol (179)
chargen	Character generator (19)
cmd	Remote commands (rcmd, 514)

ي ف ةلوهس رثكأ ميقي ىلإ ةيمقرلا ميقرلا ليوحتب أضيأ ةجوملا موقبي، نيوكتلا ءانثأ
ليوحتب ةجوملا مايقي ي ف ببستيو، ICMP ةلاسرعون مقرر بتكت ثيح لاثم اذه. مادختسال
مسا ىلإ مقررلا

<#root>

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 14
```

ح بصري

<#root>

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 timestamp-reply
```

(ACL) لوصولي ف مكحتال مئوق قي بطت

نوكي ال، نكلو. دعب اهقي بطت متي الو (ACL) لوصولي ف مكحتال مئوق ديحت كنكمي نم. هجولم اهجاو يلع اهقي بطت متي يتح ريثأت ي (ACL) لوصولي ف مكحتال مئوق ردمل برقأل اهجاو يلع (ACL) لوصولي ف مكحتال مئوق قي بطت ديجال تاسرامل اهجاو يلع ردمل نم رورملا كرح رظح ةلواحم دنع، لاثملا اذه ي ف حضوم وه امك. رورملا كرح مئوق نم ال دب A هجولم اب E0 يلع ةدراو (ACL) لوصولي ف مكحتال مئوق قي بطت كنكمي ي اةياهن ي ف اي نمض adeny ip any يلع لوصولي ف مئوق يوتحت C. هجولم اب E1 يلع ةرداص متي، ةحارص هب احومسم نكي مل اذو DHCP بلطب ةطبترم رورملا كرح تناك اذو. لوصولي ف مئوق ردمل ال ناوع نوكي، IP ي ف DHCP بلطب يلع رظنت ام دنع هنال رورملا كرح طاقس s=0.0.0.0 ردمل ال ناوع نأ طحال. (Ethernet1/0)، d=255.255.255.255، len 604، rcvd 2 UDP src=68، dst=67. كليلع بجي، كليلع 67. اهجاو او 68 وه ردمل ذف نم 255.255.255.255 وه اهجاو ناوع و 0.0.0.0 وه كرح طاقس متيس هنأ وأ كب ةصاخل لوصولي ف مئوق ي ف رورملا كرح نم عونلا اذهب حامسلا ةرابعل اةياهن ي ف ينمضلا ضفرل ببسب رورملا.

حيرص لكشب UDP رورم كرحب حامسلا اضيأ بجي، UDP رورم كرح رمت يكل: ةطحال م (ACL) لوصولي ف مكحتال مئوق ةطساوب.



اهجاو ردمل او رداصل او دراو او جراخالو لخال ديحت

كرح ةنراقم نكمي. عجارمك اهجاو ردمل او جورخالو لوخدل تاحل لطمم هجولم مدختسي نوناقل قي بطت ي ف اطباض تنك اذو. عيرسلا قي رطلال يلع رورملا كرحب هجولم يلع رورملا ةنحاشل ردمل نإف، كرويوي ن يلع دناليرام نم لقتنت ةنحاش فاقيا تدرأو اينافل سنب ي ف اينافل سنب دودح يلع قي رطلال زجاج قي بطت نكمي. كرويوي يه ةنحاشل اهجوو، دناليرام وه (لخاد) اينافل سنب-دناليرام دودح وأ (جراخ) كرويوي.

يناعمل اهه اهل تاحل لطمم اهه نإف، هجولم يلع ريشت ام دنع.

- ناكل وه ردمل. اهجاو رداغتو هجولم لخال نم لعلاب تمت يتل رورملا كرح — جراخ هيلع بهذي يذل ناكل يه اهجاو، هجولم نم رخأل بانجال يلع، هيلع ناكل يذل.

- ناكمل او ره ردصملا . ءجوملا ربع لقتنت م ءهجاولا ىلا لصت يتلا رورملا ءكرح — لءاد ءجوملا نم رءال بانءال ىلع ، هـىلـل بهـذي يـذـلـا نـاـكـمـلـا يـه ءهـجـولـا و هـىـلـع نـاـك يـذـلـا .
- ءمانربلا ققءتـي ، ءمزح ءجوملا لبقـتـسـي امـدـنـع ، ءءراو لوصول ءمئـاق تـنـاـك اذـا — ءراولـا اذـا . قـبـاطـت نـع اءـءـحـب لوصول ءمئـاق بـءـصـاـءـل رـيـءـيـءـمـلـا تـارـابـع نـم Cisco IOS software نـاـف ، ءـمـزـحـلـا ضـفـرـمـت اذـا . ءـمـزـحـلـا ءـلـعـمـ يـف ءـمـانـرـبـلـا رـمـتـسـي ، اـهـب ءـومـسـم ءـمـزـحـلـا تـنـاـك ءـمـزـحـلـا لـهـاـءـتـي ءـمـانـرـبـلـا .
- ىلا اهـءـوـيـو ءـمـزـح ءـمـانـرـبـلـا لـبـقـتـسـي نـا ءـعـب ، ءـرـءـاص لوصول ءمئـاق تـنـاـك اذـا — رءاصـلـا نـع اءـءـحـب لوصول ءمئـاق لـرـيـءـيـءـمـلـا تـارـابـع نـم ءـمـانـرـبـلـا قـقـءـتـي ، ءـرـءـاصـلـا ءـهـجـاـولـا نـاـف ، ءـمـزـحـلـا ضـفـرـمـت اذـا . ءـمـزـحـلـا ءـمـانـرـبـلـا لـسـرـي ، اـهـب ءـومـسـم ءـمـزـحـلـا تـنـاـك اذـا . قـبـاطـت ءـمـزـحـلـا لـهـاـءـتـي ءـمـانـرـبـلـا .

مـتـي يـتـلـا ءـهـجـاـولـا نـم ءـزـج ىـلـع رءـصـم ىـلـع لءـاـءـلـل (ACL) لوصولاب مكـءـلـا ءـمئـاق يـوتـءـت مكـءـلـا ءـمئـاق يـوتـءـت . اـهـىـلـع اـهـقـيـبـطـت مـتـي يـتـلـا ءـهـجـاـولـا ءـراـء ءـهـجـوـو هـىـلـع اـهـقـيـبـطـت ءـهـجـوـو هـىـلـع اـهـقـيـبـطـت مـتـي يـتـلـا رـيـءـمـلـا ءـهـجـاـوـيـا نـم ءـزـج ىـلـع رءـصـم ىـلـع ءـراـءـلـل (ACL) لوصولاب اـهـىـلـع اـهـقـيـبـطـت مـتـي يـتـلـا ءـهـجـاـولـا ءـراـء .

(ACL) لوصول يـف مكـءـلـا ءـمئـاق رـيـءـت

ىـلـع . اءـصـاـء اءـمـاـءـهـا بـلـطـتـت اـهـنـاـف ، (ACL) لوصول يـف مكـءـلـا ءـمئـاق رـيـءـتـب مـوـقـت امـدـنـع ءـمـقـرـمـلـا (ACL) لوصول يـف مكـءـلـا ءـمئـاق نـم نـيـعـم رطـس فءـءـ يـونـت تـنـك اذـا ، لـاـءـمـلـا لـيـبـس لـمـاـكـلـاب لوصول يـف مكـءـلـا ءـمئـاق فءـء مـتـي سـف ، اـنـه ءـضـوم وـه امـك ءـءـوـجـومـلـا .

<#root>

```
!--- The access-list 101 denies icmp from any to any network
!--- but permits IP traffic from any to any network.
```

```
router#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#
access-list 101 deny icmp any any
router(config)#
access-list 101 permit ip any any
router(config)#
^Z

router#
show access-list

Extended IP access list 101
  deny icmp any any
  permit ip any any
router#
```

```

*Mar  9 00:43:12.784: %SYS-5-CONFIG_I: Configured from console by console

router#
configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#

no access-list 101 deny icmp any any

router(config)#
^Z

router#

show access-list

router#
*Mar  9 00:43:29.832: %SYS-5-CONFIG_I: Configured from console by console

```

في مكدحتل المئوق ريححتل Notepad لثم صوصن ررحم وأ TFTP م داخ ىل ةجومل ني وكت خسن
ةجومل ىل ةرخ ةرم ني وكتل خسن او تاريغت ي ءارج اب مق م ث. ةم ق رمل (ACL) لوصول

ك. لذ م اي ق ل ا ض ي ا كن ك م ي

<#root>

```

router#
configure terminal

Enter configuration commands, one per line.
router(config)#

ip access-list extended test

!--- Permits IP traffic from 10.2.2.2 host machine to 10.3.3.3 host machine.

router(config-ext-nacl)#
permit ip host 10.2.2.2 host 10.3.3.3

!--- Permits www traffic from 10.1.1.1 host machine to 10.5.5.5 host machine.

router(config-ext-nacl)#
permit tcp host 10.1.1.1 host 10.5.5.5 eq www

!--- Permits icmp traffic from any to any network.

router(config-ext-nacl)#
permit icmp any any

!--- Permits dns traffic from 10.6.6.6 host machine to 10.10.10.0 network.

```

```

router(config-ext-nacl)#
permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain

router(config-ext-nacl)#^Z
1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-1

router#
show access-list

Extended IP access list test
  permit ip host 10.2.2.2 host 10.3.3.3
  permit tcp host 10.1.1.1 host 10.5.5.5 eq www
  permit icmp any any
  permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain

```

ىل افاضا ةي اءارء مءىو (ACL) لوصول اب مكءءءا ةمءءاق نم فءءءا ءءل مع ءى ءلازا مءءء (ACL) لوصول اب مكءءءا ةمءءاق ةءاهن

<#root>

```

router#
configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
router(config)#
ip access-list extended test

!--- ACL entry deleted.

router(config-ext-nacl)#
no permit icmp any any

!--- ACL entry added.

router(config-ext-nacl)#
permit gre host 10.4.4.4 host 10.8.8.8

router(config-ext-nacl)#
^Z

1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-1

router#
show access-list

Extended IP access list test
  permit ip host 10.2.2.2 host 10.3.3.3
  permit tcp host 10.1.1.1 host 10.5.5.5 eq www
  permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
  permit gre host 10.4.4.4 host 10.8.8.8

```

لوصول اب مكحتلا مئاوق ىلإ (ACL) لوصول اب مكحتلا ةمئاوق طوطخ ةفاضإ اضيأ كنكمي نيوكتل نم ةنيع هذو. Cisco IOS في لسلست مقرب ةمقرم وأ ةسايق ةمقرم (ACL):

ةقيرطالا هذو ةعسوملا (ACL) لوصولا في مكحتلا ةمئاوق نيوكت:

```
<#root>
```

```
Router(config)#  
access-list 101 permit tcp any any  
  
Router(config)#  
access-list 101 permit udp any any  
  
Router(config)#  
access-list 101 permit icmp any any  
  
Router(config)#  
exit  
Router#
```

مأقرألا رهظت امك. (ACL) لوصولا في مكحتلا ةمئاوق تالخدإ ضرعل show access-list رمألا ردصأ انه 30 و 20 و 10 لثم ةيلسلستلا.

```
<#root>
```

```
Router#  
show access-list  
  
Extended IP access list 101  
 10 permit tcp any any  
 20 permit udp any any  
 30 permit icmp any any
```

5. لسلستلا مقربلا 101 لوصولا ةمئاوق صاخلا لاخدإلا فإصأ.

1: لاثم

```
<#root>
```

```
Router#  
configure terminal  
  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#  
  
ip access-list extended 101  
  
Router(config-ext-nacl)#
```

```
5 deny tcp any any eq telnet
Router(config-ext-nacl)#
exit
Router(config)#
exit
Router#
```

مقررلاب ةصاخلا (ACL) لوصولا يف مكحتلا ةمئاق ةفاضإ متت ، show access-list جارخا يف
101 لوصولا ةمئاق ىلا لوالا لاخدإلا هرابت عاب 5 ىلس لسلا

<#root>

```
Router#
show access-list
Extended IP access list 101
5 deny tcp any any eq telnet
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
Router#
```

2: لاثم

<#root>

```
internetrouter#
show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.16.2.9
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any
internetrouter#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
internetrouter(config)#
ip access-list extended 101
internetrouter(config-ext-nacl)#
18 per tcp any host 172.16.2.11
internetrouter(config-ext-nacl)#
```

^Z

```
internetrouter#  
show access-lists  
Extended IP access list 101  
 10 permit tcp any any  
 15 permit tcp any host 172.16.2.9  
 18 permit tcp any host 172.16.2.11  
 20 permit udp host 172.16.1.21 any  
 30 permit udp host 172.16.1.22 any  
internetrouter#
```

ةقيرطاللا هذبة ةيسايقلا لوصوللا ةمئاق نيوكت كنكمي ،لثملابو

<#root>

```
internetrouter(config)#  
access-list 2 permit 172.16.1.2  
internetrouter(config)#  
access-list 2 permit 172.16.1.10  
internetrouter(config)#  
access-list 2 permit 172.16.1.11
```

```
internetrouter#  
show access-lists  
Standard IP access list 2  
 30 permit 172.16.1.11  
 20 permit 172.16.1.10  
 10 permit 172.16.1.2
```

```
internetrouter(config)#  
ip access-list standard 2  
internetrouter(config-std-nacl)#  
25 per 172.16.1.7  
internetrouter(config-std-nacl)#  
15 per 172.16.1.16
```

```
internetrouter#  
show access-lists  
Standard IP access list 2  
15 permit 172.16.1.16  
 30 permit 172.16.1.11
```

```
20 permit 172.16.1.10
```

```
25 permit 172.16.1.7
```

```
10 permit 172.16.1.2
```

الاجراء في ضي Cisco IOS نأ في ةسي ايقلا لوصول ةمئاق في في سيئرلا فالخال نم كي
ي لس لس ت مقر يلع سي لو، IP ناون عل عبات بي تر تب

IP ناون عب حامس لة في في ك، لاثم ل ل ي بس يلع، ةفل تخم لال اخل اء ل ل اءم ل اءه ح ضوي
(10.10.10.0) تاك بشل ل وأ (192.168.100.0).

```
<#root>
```

```
internetrouter#
```

```
show access-lists
```

```
Standard IP access list 19  
 10 permit 192.168.100.0  
 15 permit 10.10.10.0, wildcard bits 0.0.0.255  
 19 permit 10.101.110.0, wildcard bits 0.0.0.255  
 25 deny any
```

IP 172.22.1.1 ناون عب حامس ل ل 2 لوصول ةمئاق في في لال اءل اء فاضاب مق

```
<#root>
```

```
internetrouter(config)#
```

```
ip access-list standard 2
```

```
internetrouter(config-std-nacl)#
```

```
18 permit 172.22.1.1
```

نم آل دب دءم لال IP ناون عل ةي ول وائل اءاع ل لء نم ةمئاق لال يلع أ في في لال اءل اءه فاضا مءت
ءك بشل ل.

```
<#root>
```


```
internetrouter#
```

```
show access-lists
```

```
Standard IP access list 19  
 10 permit 192.168.100.0
```

```
18 permit 172.22.1.1
```

```
15 permit 10.10.10.0, wildcard bits 0.0.0.255
19 permit 10.101.110.0, wildcard bits 0.0.0.255
25 deny any
```

 Security نامأل زاخ يف ةم و عدم ريغ ةق باسلا (ACL) لوصولا يف مكحتلا مئاقوق: ةظحالما Appliance ةيامح رادج لثم ASA/PIX.

ري فشتلا طئارخ ىلع اهق يبطت دنع لوصولا مئاقوق ريغيغتل تاداشرا.

- تفضأ اذا . ري فشتلا ةطيخ ةلازال ةجالح الف ، ةيلالح لوصولو ةمئاق نيوكت ىلإ تفضأ اذا . لوبقمو موعدم اذهف ، ري فشتلا ةطيخ ةلازالا نود ةرشابم اهليل.
- هفدح وأ ةيلالح لوصولو مئاقوق نم لوصولو ةمئاق لاخدا لي دعت ىلإ ةجالح تنك اذا . عارجاب مق ، ري فشتلا ةطيخ ةلازالا دعب . ةهجاوالا نم ري فشتلا ةطيخ ةلازالا كي لعل بجي يف عارجاب تمق اذا . ري فشتلا ةطيخ ةفاضلا دعأو لوصولو ةمئاق ىلعل تاريغيغتل اعيمج نكميو موعدم ريغ اذهف ، ري فشتلا ةطيخ ةلازالا نود لوصولو ةمئاق فدح لثم تاريغيغتل . عقوقتم ريغ كولس ىلإ يدوي نأ .

اهحال صا وءاطخال فاشكتسا

ةهجاو نم (ACL) لوصولا يف مكحتلا ةمئاق ةلازالا يننكمي فيك


اذه يف حضورم وه امك ، no in front of the access-group رمالا لخدا و نيوكتلا عضو ىلإ لقتنا . ةهجاو نم (ACL) لوصولا يف مكحتلا ةمئاق ةلازالا ، لاثملا

<#root>

```
interface <interface-name>
no ip access-group <acl-number> {in|out}
```

رورملا ةكرح ضفر متي ام دنع لع فأ اذام

ةمئاق دي دحت لواح وأ ةمئاقلا قطنم ةساردب مقف ، تارايزلا نم ةيغلل ري بكد دع ضفر مت اذا . ةمئاق لاخدا حضورم مزللل اءادعت show ip access-lists رمالا رفو . اهق يبطت و عسوأ ةي فاضا ةي اهن يف لجسلا ةي اساسألا ةم لكلا رهطت . هيلل لوصولو مت يذلا (ACL) لوصولو يف مكحتلا ناك اذا امو لوصولو يف مكحتلا ةمئاق مقرة يدرفل (ACL) لوصولو يف مكحتلا ةمئاق تالاخدا . ذفنم لابل ةصخال تامولعمل ىلإ ةفاضلا اب ، اهضفر وأ ةمزللل حامسلا مت دق .

 جم انرب نم 11.2 رادصإلا يف لجسلا لاخدا لاجسلا لاخدا ةي اساسألا ةم لكلا دجوت : ةظحالما Cisco IOS نم 11.1 رادصإلا ىلإ ةدنتس ملام جماربلا ضعب يفو ، ثدخال تارادصإلا او Cisco IOS ةم لكلا هذه مدقألا جم انربلا معدي ال . ةمدخللا دوزم قوسل اصي صخ اهؤاشنإ مت يتلا IOS ردملا MAC ناو نعو لاخدا ةهجاو ةي سيئرلا ةم لكلا هذه مادختسا نمضتت . ةي سيئرلا كل ذق بطن ي امثي .

Cisco؟ جوم مدختست يتال مزلال وتسم ىلع اطاخال احيحصت يننكمي فيك

ف مكحتال مئاوق دوجو مدع نم دكأت، ادبال لبق. اطاخال احيحصت ةيلمع ارجال اذه حرشي لطم ريغ عيرسال ليوحتال كذا نأو ACL كانه نأو، أيلاح ةقبطم (ACL) لوصول

✎ مئاوق مدختسا. ةمحدزم رورم ةكره ب ماظن اطاخال احيحصت دنع ديدشال رذال خوت: ةظالم قفدتو ةيلمعال نم دكأت. ةنيعم رورم ةكره اطاخال احيحصت ل (ACL) لوصول في مكحت رورم ةكره.

1. ةبولطمال تانايبال طاقتال لجأ نم access-list رمأل مدختسأ.

ناونع وأ 10.2.6.6 ةهجال ناونع ىلع تانايبال طاقتال نييعة متي، لاثمال اذه في 10.2.6.6 رصمالم.

```
<#root>
```

```
access-list 101 permit ip any host 10.2.6.6  
access-list 101 permit ip host 10.2.6.6 any
```

2. مل اذا طقف لىلوال مزلال ىرتس. ةنيعمال تاهجال ىلع عيرسال ليوحتال ليطعتب مق. عيرسال ليوحتال ليطعت متي.

```
<#root>
```

```
configure terminal  
interface
```

```
no ip route-cache
```

3. أطخ لئاسرو debug رمأل ضرعل نيكمتال عضو في terminal monitor رمأل مدختسا. ةيلجال ةسلجال وةيفرطال ةطحملل ماظنل.

4. احيحصت ةيلمع ادبال debug ip packet 101 detail وأ debug ip packet 101 رمأل مدختسأ. اطاخال.

5. فاقيل interface configuration رمأو نيكمتال عضو في no debug all رمأل ذيفنتب مق. اطاخال احيحصت ةيلمع.

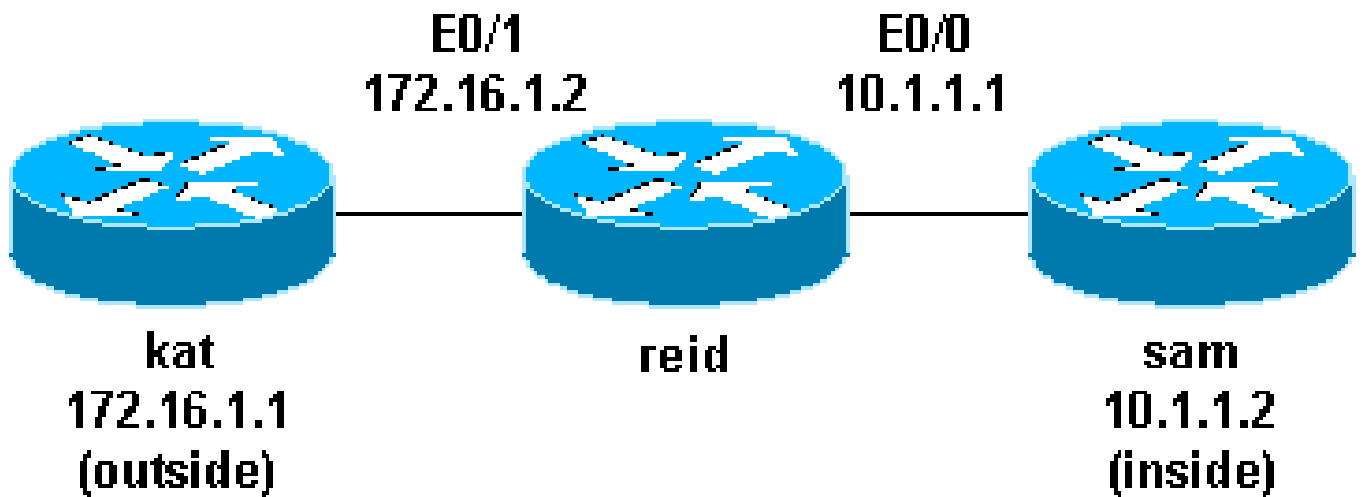
6. ت.ق.وم.ال.ن.ي.ز.خ.ت.ال.ة.ر.ك.ا.ذ.ل.ي.غ.ش.ت.ة.د.ا.ع.ا.ب.م.ق.

```
<#root>  
configure terminal  
interface  
  
ip route-cache
```

IP إلى لوصول في مكحتال مئاق عاوناً

(ACL) لوصول في مكحتال مئاق عاوناً دن تسمل نم مسقلا اذه فصي

ةكبش لل يطيطختال مسرلا



ةيسايقل لوصول في مكحتال مئاق

ركبم تقو إلى اهخيرات دوعي. ACL عاوناً مدقأ يه ةيسايقل (ACL) لوصول في مكحتال مئاق
(ACL) لوصول في مكحتال مئاق مكحتت. 8.3 رادصلال، Cisco IOS Software جمانرب لثم
مت يتال نيوانع إلى IP مزحل ردمال ناوع ةنراقم لالخنم رورملا ةكرح في ةيسايقل
(ACL) لوصول في مكحتال مئاق في انهنيوكت.

ةيسايقل (ACL) لوصول في مكحتال مئاق لرمألا ةغايص قيسنت وه اذه

<#root>

```
access-list <access-list-number> {permit|deny} {host|source source-wildcard|any}
```

في 99 إلى 1 نم عيشي أ access-list-number نوكي نأ نكمي، جماربل تارادصل عي مج ي في (ACL) لوصولي في مكحتل مئوق أدبت، 12.0.1 رادصلإا، Cisco IOS Software جمانربلإا عي فاضلإا ماقرالإا هذه لراشوي. (1999 إلى 1300 نم) عي فاضلإا ماقرالإا مادختسا في عي سايقلا عمئوقلا مسا مادختسال عي ناكم 11.2 رادصلإا، Cisco IOS Software. عسوملإا IP مئوقب عي سايقلا (ACL) لوصولي في مكحتل مئوق ي في.

فرحأ فذح نكمي. يأ هنا لعل 0.0.0.0/255.255.255.255 ردم لذب فرح/ردصم دادعإ ديحت نكمي 10.1.1.2 هسفن فيضملإا وه 0.0.0.0 10.1.1.2 فيضملإا، كلذل رافصأ اهلك تناك إذل لذبلا.

جماربل تارادصل ي في (رداصل وأ إدراول) عهاولي لعل اهقي ببطب بجي، ACL عمئوق ديحت دعب وأ جراخلل اهنأ عي سايقلا عمئوق ديحت متي مل امدنع يضارتفالا دادعإلا وه جورخل ناك، عقباسلا عهاولل جماربل تارادصل ي في هاجتالا ديحت بجي. لخلادل

<#root>

```
interface <interface-name>
```

```
ip access-group number {in|out}
```

رورملا كرح لك رطل عي سايق (ACL) لوصولي في مكحتل عمئوق مادختسا لعل لاثم اذه 10.1.1.x ردمل نم إدراول كلت اناثتساب

<#root>

```
interface Ethernet0/0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
ip access-group 1 in
```

```
!
```

```
access-list 1 permit 10.1.1.0 0.0.0.255
```

عسوملإا لوصولي في مكحتل مئوق

مئوق مكحتت 8.3 رادصلإا، Cisco IOS Software جمانربلإا ي في عدتمملا ACL مئوق مي دقت مت عهول او ردمل نيوانع نراقم لال خ نم رورملا كرح ي في عسوملإا (ACL) لوصولي في مكحتل (ACL) لوصولي في مكحتل عمئوق ي في اهنويوكت مت يتل نيوانعلا لىلإ IP مزحل

ني مضت متي. عسوملإا (ACL) لوصولي في مكحتل عمئوقل رمألا عي صقي سنت وه اذه. عحاسملا تارابتعال انه طوطخلال

IP

<#root>

access-list

access-list-number

[dynamic

dynamic-name

[timeout

minutes

]]

{deny|permit}

protocol source source-wildcard destination destination-wildcard

[precedence

precedence

]

[tos

tos

] [log|log-input] [time-range

time-range-name

]

ICMP

<#root>

access-list

access-list-number

[dynamic

dynamic-name

[timeout

minutes

]]

{deny|permit} icmp

source source-wildcard destination destination-wildcard

[icmp-type [icmp-code] |icmp-message]

[precedence

precedence

] [tos

tos

```
] [log|log-input]
    [time-range
time-range-name
]
```

TCP

<#root>

access-list

access-list-number

[dynamic

dynamic-name

[timeout

minutes

]]

{deny|permit} tcp

source source-wildcard

[operator [

port

]]

destination destination-wildcard

[operator [

port

]]

[established] [precedence

precedence

] [tos

tos

]

[log|log-input] [time-range

time-range-name

]

UDP

```

<#root>
access-list
access-list-number
    [dynamic
dynamic-name
    [timeout
minutes
]]
    {deny|permit} udp
source source-wildcard
[operator [
port
]]
destination destination-wildcard
    [operator [
port
]]
    [precedence precedence] [tos
tos
] [log|log-input]
    [time-range
time-range-name
]

```

جمانربلا يف 199 إلى 100 نم access-list-number نوكي نأ نكمي، جماربل تارادصلإ عيمج يف يف ةعسوملا (ACL) لوصولا يف مكحتلا مئوق أدبت، 12.0.1 رادصلإ، Cisco IOS Software، IP مئوقب ةيفاضلا ماقرالآ هذه إلى راشي و. (2699 إلى 2000 نم) ةيفاضا ماقراً مادختسا مئوق يف ةمئاقلا مسا مادختسال ةيناكم 11.2 رادصلإ، Cisco IOS Software، ةعسوملا ةعسوملا (ACL) لوصولا يف مكحتلا

بجي، ACL ةمئاق ديدحت دعب. يأ اهنأ إلى ع 0.0.0.0/255.255.255.255 ةميق ديدحت نكمي وه جورخل ناك، ةقباسلا جماربل تارادصلإ يف. (ةرداصل وأ ةدراولا) ةهجاو لا يل ع اهق يبطت ديدحت بجي. لخدلل وأ جراخلل اهنأ ةيساساً ةمك ديدحت متي مل ام دنع يضارتفالا دادعإلا ةقحلالا جماربل تارادصلإ يف هاجتالا

```

<#root>
interface
<interface-name>
    ip access-group {

```


number | name

} {in|out}

يلع رورملا ةكرب حامسلل هذه ةعسوملا (ACL) لوصولا يف مكحتلا ةمئاق مادختسا متي عنمت امنيب جراخل نم لاصلتالا تارابتخا تارابتسا يقلتو (لخادلل يف) 10.1.1.x ةكبش عيمجل حمسي يذلاو، جراخل يف صاخشال نم اهيف بوغرمل ريغ لاصلتالا تارابتخا تاوصأ يخال رورملا ةكرب.

<#root>

```
interface Ethernet0/1
  ip address 172.16.1.2 255.255.255.0
  ip access-group 101 in
!
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 101 permit ip any 10.1.1.0 0.0.0.255
```

 ةفيظو لجأ نم لاصلتالا رابتخا، ةكبشلا ةرادا لثم، تاقببطلتلا ضعبل طلتت: ةظالم اهراطح متي يتلل ةدراول لاصلتالا تارابتخا ديقت كنكميف، لالحل وه اذه ناك اذا. ظافتح ةضوفرملا/اهب حومسمل IP نيوانع يف ةقد رثكأ نوكت نأ وأ

ةيكيماني دللا (ACL) لوصولا يف مكحتلا (مئاق) حاتفملاو لفلل

(ACL) لوصولا يف مكحتلا مئاق مساب اضيأ نيفورعملالو، حاتفملاو لفلل لالحل مت جم انرب يلع ةزيملا هذه دمتعت 11.1 رادصال، Cisco IOS Software جم انربلل يف، ةيكيماني دللا ةعسوملا (ACL) لوصولا يف مكحتلا مئاقو (ديعب وأ يلحم) ةقد اصلالو Telnet.

رطحل ةعسوم (ACL) لوصولا يف مكحتلا مئاق قيببطلت حاتفملاو لفلل نيوكت ادبي ةطساوب هجومل زاي تجا يف نوبغري نيذل ني مدختسملا رطح متي. هجومل ربع رورملا ةكرب متتو هجوملاب Telnet جم انرب عضوب اوموقي يتح ةعسوملا (ACL) لوصولا يف مكحتلا ةمئاق ةعسوم (ACL) لوصولا يف مكحتلا ةمئاق ةفاضلا متتو، Telnet لاصلتال عطقني مث. مهتقد اصم حمسي اذه. دوجوملا ةعسوملا (ACL) لوصولا يف مكحتلا ةمئاق لالحل ةيداح ةيكيماني دةنكمم ةقلطملاو ةلمخال راظتنال تارثف؛ ةنيعم ةينمز ةرتفل رورملا ةكرب.

ةيحلحمل ةقد اصلال مادختساب حاتفملاو لفلل نيوكتل رماولل ةغايص قيسنت وه اذه.

<#root>

username

<user-name>

password

<password>

```

!
interface
<interface-name>
  ip access-group {
number|name
} {in|out}

```

ىل اى كى م ا ن ي د ر م ا ل ا ا ذ ه ي ف ل ا خ د ا ل ا ة ي د ا ح ا ل ا (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ة ف ا ض ا م ت ت
ة ق د ا ص م ل ا د ع ب ة د و ج و م ل ا (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق .

```

<#root>
access-list
access-list-number
  dynamic
name
  {permit|deny} [protocol]
{
source source-wildcard
|any} {
destination destination-wildcard
|any}
[precedence
precedence
][tos
tos
][established] [log|log-input]
[
operator destination-port|destination port
]

line vty
<line_range>

  login local

```

ح ا ت ف م ل ا و ل ف ق ل ا ي ل ع ي س ا س ا ل ل ا ث م ا ذ ه .


```
<#root>
```

```
username test password 0 test
```

```
!--- Ten (minutes) is the idle timeout.
```

```
username test autocommand access-enable host timeout 10
```

```
!
```

```
interface Ethernet0/0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
ip access-group 101 in
```

```
!
```

```
access-list 101 permit tcp any host 10.1.1.1 eq telnet
```

```
!--- 15 (minutes) is the absolute timeout.
```

```
access-list 101 dynamic testlist timeout 15 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
!
```

```
line vty 0 4
```

```
login local
```

متمتة ائاق قيبطت متي، 10.1.1.1 بـ Telnet لاصتا اءارب 10.1.1.2 في مدختسملا مايق دع
مدختسملل نكميو، لاصتالا عطق لكد دع ب متي. ةيكيما نديلا (ACL) لوصولا في مكحتلا
172.16.1.x ةكبش للاقتنالا

IP لةامسُملا (ACL) لوصولا في مكحتلا مئاق

Cisco IOS جم انربلا في IP لةامسُملا (ACL) لوصولا في مكحتلا مئاق مي دقت مت
(ACL) لوصولا في مكحتلا مئاق ءامسُ اءاعاب حمسي اذهو. 11.2 رادصلا، Software
ماقرا نم الءب ةءسوملاو ةيسايقلا

IP لةامسُملا (ACL) لوصولا في مكحتلا مئاق لرم الة ءايس قيسنت وه اذه

```
<#root>
```

```
ip access-list {extended|standard} name
```

TCP لوكوتورب لىل لءم اذه

```
<#root>
```

```
{permit|deny} tcp source source-wildcard [operator [port]]
```

```
destination destination-wildcard [operator [port]] [established]
```

```
[precedence precedence] [tos tos] [log] [time-range time-range-name]
```

رورملا تاكرح لك رظحل ةامسُملا (ACL) لوصولاي ف مكحتلا ةمئاق مادختسا ىلع لاثم اذه
172.16.1.1 فيضملا ىلإ 10.1.1.2 فيضملا نم Telnet لاصتا ءانثتساب

```
<#root>
```

```
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip access-group in_to_out in
!
ip access-list extended in_to_out
  permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

ةيسكعلا (ACL) لوصولاي ف مكحتلا مئاق

Cisco IOS Software، جم انربلا في ةيسكعلا (ACL) لوصولاي ف مكحتلا مئاق مي دقت مت
آدانسا IP مزح ةيفصتب ةيسكعلا (ACL) لوصولاي ف مكحتلا مئاق حمست 11.3 رادصإل
رورملا ةكرحب حامسلل ماع لكشب اهمادختسا متي. ايلعلا ةقبطلا ةسلج تامولعم ىلإ
هجوملا لخاد أشنت يتلا تاسلجل ةباجتسا في ةدراولا رورملا ةكرح نم دحلاو ةرداصللا

لوصولاي ف مكحتلا مئاق عم طقف ةيسكعلا لوصولاي ف مكحتلا مئاق دي دحت نكمي
(ACL) لوصولاي ف مكحت مئاق مادختساب اهديدحت نكمي ال IP ىلإ ةامسُملا ةعسوملا (ACL)
لوكتوربلا ىرخألا (ACL) لوصولاي ف مكحتلا مئاق عم وا، ةيسايق وا ةمقرم IP ىلإ ةامسُم
مكحتلا مئاق عم بنج ىلإ اَبنج ةيسكعلا (ACL) لوصولاي ف مكحتلا مئاق مادختسا نكمي
ىرخألا ةتباطلاو ةيسايقللا ةعسوملا (ACL) لوصولاي ف

ةيسكعلا (ACL) لوصولاي ف مكحتلا مئاق رم اوأ فل تخملا ةغاياصللا يه هذو.

```
<#root>
```

```
interface
<interface-name>

  ip access-group {
number|name
} {in|out}
!
ip access-list extended
<name>

  permit
protocol

  any any reflect

name [timeoutseconds]

!
ip access-list extended
```

```
<name>
  evaluate
</name>
```

TCP رورم ةكرحل طقف حمسي امنيب، ةدراول او ةرداصل ال ICMP رورم ةكرحب حامسلا يلعل لاثم اذه
ىرخال رورملا تاكرحض فرمتي امنيب، لخدال نم تادب يتلا

```
<#root>
```

```
ip reflexive-list timeout 120
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group inboundfilters in
 ip access-group outboundfilters out
!
ip access-list extended inboundfilters
 permit icmp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
 evaluate tcptraffic

!--- This ties the reflexive ACL part of the outboundfilters ACL,
!--- called tcptraffic, to the inboundfilters ACL.

ip access-list extended outboundfilters
 permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 reflect tcptraffic
```

تاقاطن مادختساب تقولا لىل ةدنتسملا (ACL) لوصولا يف مكحتلا مئاوق
تقولا

Cisco IOS جمانربلا يف تقولا لىل ةدنتسملا (ACL) لوصولا يف مكحتلا مئاوق ميديقت مت
يف ةعسوملا (ACL) لوصولا يف مكحتلا مئاوق هبشت امنيب 12.0.1.T رادصلال،
ددحي ينمز قاطن عاشن امتي. تقولا لىل ةانب لوصولا يف مكحتلاب حمست اهناف، ةفيظولا
ةدنتسملا (ACL) لوصولا يف مكحتلا مئاوق ذيفنت لجأ نم عوبسأل او مويلا نم ةددم اتاقوا
ةطساوب هيلل ةراشال امتت مءامسأل دحأ بسح ينمزل قاطنلا ديدحت متي. تقولا لىل
لىل ينمزل قاطنلا دمتعي. اهسفن ةفيظولا لىل تقولا دويق صرف متي، كلذل. ةفيظو
نم ازم عم لصفأ لكشب لمعت ةزيملا نكلو، ةجوملا ةعاس مادختسا نكمي. ةجوملا ماطن ةعاس
(NTP) ةكبشلا تقولا لوكوتورب.

تقولا لىل ةدنتسملا (ACL) لوصولا يف مكحتلا مئاوق رماو ايه هذو.

```
<#root>
```

```
!--- Defines a named time range.
```

```
time-range time-range-name
```

!--- Defines the periodic times.

```
periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm
```

!--- Or, defines the absolute times.

```
absolute [start time date] [end time date]
```

!--- The time range used in the actual ACL.

```
ip access-list name|number
```

```
time-rangename_of_time-range
```

نېنثال ماية جيخراخله كيشل الى لخال نم Telnet لاصتاب حامسلا متي، لاثملا اذه في لمعل تاغاس لخال عمجل او اعبرال او

```
<#root>
```

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
 !
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range EVERYOTHERDAY
 !
time-range EVERYOTHERDAY
 periodic Monday Wednesday Friday 8:00 to 17:00
```

اهي لع قيلعتلا متي ال IP الى (ACL) لوصول في مكحتلا مئاوق تالخال

في اهي لع قيلعتلا متي ال IP الى (ACL) لوصول في مكحتلا مئاوق تالخال مي دقت مت لوصول في مكحتلا مئاوق تالعلي لعتل لعتت 12.0.2.T رادصل الى Cisco IOS Software، جامانربل او ايسايل ال IP الى (ACL) لوصول في مكحتلا مئاوق لاهم ادختسا نكمي ومهفلل لهسا ACL عة سومل.

قيلعتلا متي ال امسمل ال IP الى (ACL) لوصول في مكحتلا مئاوق رمة غايسيه هذه اهي لع.

```
<#root>
```

```
ip access-list {standard|extended} <access-list-name>
 remark remark
```

قيلعتلا مت يتلا ةمقرملا IP لى (ACL) لوصول في مكحتلا ةمئاق رما ةغايص يه هذه اهيع.

```
<#root>
```

```
access-list <access-list-number> remark remark
```

ةمقرملا (ACL) لوصول في مكحتلا ةمئاق نمض تاقيلعتلا لىل لاثم اذه

```
<#root>
```

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
!
access-list 101 remark permit_telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

قايصل لى دن تسمل لوصول في مكحتلا

Cisco IOS جم انربل في (CBAC) قايصل لى دن تسمل لوصول في مكحتلا لادام مت صحتفب CBAC موقوي Cisco IOS. ةيماح رادج تازيم ةومجم بلطتي و 12.0.5.T رادصلال Software، تاسلجل اهترادو ةلاجل تامولعم فاشتك لجا نم ةيماحلا رادج ربع لقتنت يتلا رورملا ةكرح لوصول مئاق في ةتقوم تاحتف ءاشن لجا نم هذه ةلاجل تامولعم مادختسا متي TCP و UDP. ةكرح حامسلل رورملا ةكرح ءدب قفدت هاجت في ip صحتف مئاق نيوكتب مق. ةيماحلا رادجل تاشن يتلا تاسلجل او، اهب حومسمل ةسلجلل ةيفاضال تانايبلا تالاصتا و ةدئاعلا رورملا ككذب مايقلا لجا نم، ةيحمملا ةيلخادلا ةكبشلا لخد نم.

(CBAC) قايصل لى دن تسمل لوصول في مكحتلا ةصاخلا ةغايصل يه هذه

```
<#root>
```

```
ip inspect name inspection-name protocol [timeoutseconds]
```

مكحتلا ةمئاق موقت ام ةداعو. ةرداصلال رورملا ةكرح صحتف لجا نم CBAC مادختسا لىل لاثم اذه نودب ICMP لوكوتورب فالخب ةدئاعلا رورملا ةكرح رظحب 111 ةسوملا (ACL) لوصول في ةدئاعلا رورملا ةكرحل CBAC تاحتف بوقت.

```
<#root>
```

```
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw tcp timeout 3600
```

```

ip inspect name myfw udp timeout 3600
ip inspect name myfw tftp timeout 3600
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group 111 in
 ip inspect myfw out
!
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 111 permit icmp any 10.1.1.0 0.0.0.255

```

ةقداصملا ليكو

نأ بلطتي اذه 12.0.5 رادصإلا Cisco IOS Software، جم انربللا في ةقداصملا ليكو لاخذإ مت ةقداصملا ةقداصملا ليكو مادختسا متي Cisco IOS ةيامح رادج تازيم ةعومجم كيذل نوكتي ةءاع مه رطح متي نيذلا نيمدختسملل نكمي. امهيليكل وأ، ني رداصللا وأ ني دراووال نيمدختسملا ةيامحلا رادج لالخنم لاقتنالا ل حفصتم بلج (ACL) لوصوللا في مكحتلا مئاوق يدحإ ةطساوب مئاوقل ةيفاضا تالخذإ ريرمتب مداخلا موقوي. RADIUS وأ TACACS+ مداخيلع ةقداصملاو ةقداصملا دعب رورم لاب نيمدختسملل حامس لل ةجوملا يلا (ACL) لوصوللا في مكحتلا

(ACL) لوصوللا في مكحتلا مئاوق) حاتفملاو لفقلا لالاثامم ةقداصملا ليكو دعئى ت: افالاتخاللا يه هذه. (ةيكيما ني دلا

- ليغشت متي. ةجوملاب Telnet جم انرب لا صتا ةطساوب حاتفملاو لفقلا ليغشت متي ةجوملا لالخنم HTTP ةطساوب ةقداصملا ليكو.
- آيچراخا مداخ ةقداصملا ليكو مدختسي نأ بجي.
- لفقلا نكمي. ةددعتم ةيكيما ني د مئاوق ةفاضلا ةجالعم ةقداصملا ليكو ليغشت متي. طقف ةدحاو ةفاضلا حاتفملاو
- لفقلا يوتحي. ةلماخ ةلهم سيل نكلو ةقلطم ةلهمب ةقداصملا ليكو عتمت متي. امهيليكل يلع حاتفملاو

ةقلعتم ةلثما يلع لوصوللا Cisco نم ةلماكتملا جم انربلا نيوكت تاميلعت باتك يلا عجرا ةقداصملا ليكوب.

Turbo نم (ACL) لوصوللا في مكحتلا مئاوق

رادصإلا Cisco IOS Software، جم انربلا في Turbo نم (ACL) لوصوللا في مكحتلا مئاوق لاخذإ مت ةيساسالا ةمظنالاو 7500 و7200 ةيساسالا ةمظنالا يلع طقف اهيلي لع روثلعل متي و 12.1.5.T ةجالعم لجا نم Turbo نم (ACL) لوصوللا في مكحتلا مئاوق ةزيم ميمصت مت. ةروطتملا يرخالا ةجوملا عادأ ني سحتل ربكأ ةءافكب (ACL) لوصوللا في مكحتلا مئاوق

يلع لالاثم اذه Turbo نم (ACL) لوصوللا في مكحتلا مئاوقل access-list compiled رمالا مدختسا آيچمرب ةلوحم (ACL) لوصوللا في مكحتلا مئاوق

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq ftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq syslog
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq tftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq ntp
```

global رمأل مدختسا، ةعّسومل وأ ةيسايقل (ACL) لوصول في مكحتل ةمئاق ديحت دعب
configuration نم حجمربل ليوحتل ءارج نم

<#root>

!--- Tells the router to compile.

```
access-list compiled
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
```

!--- Applies to the interface.

```
ip access-group 101 in
```

(ACL) لوصول في مكحتل ةمئاق لوح تايئاصح | show access-list compiled رمأل حضوي

تقول الى ةدنتسمل ةعزومل (ACL) لوصول في مكحتل ةمئاق

Cisco جم انربل في تقول الى ةدنتسمل ةعزومل (ACL) لوصول في مكحتل ةمئاق لادخا مت
ةعزومل (ACL) لوصول في مكحتل ةمئاق ذيفنت لجا نم 12.2.2.T رادصل،
ةزيم لادخا لبق. اهب VPN ني كمت مت يتل 7500 ةلسلس تاهجوم يلع تقول الى ةدنتسمل
في مكحتل ةمئاق نك مل، تقول الى ةدنتسمل ةعزومل (ACL) لوصول في مكحتل ةمئاق
نم 7500 ةلسلس تاهجوم لاطب يلع ةم ودم تقول الى ةدنتسمل (ACL) لوصول
تفرصت دق ف، تقول الى ةدنتسمل (ACL) لوصول في مكحتل ةمئاق ني وكت مت اذا
في مكحتل ةمئاق مادختساب طخ ةقاطب يلع ةهجاو ني وكت مت اذا. ةيداع ACL ةمئاق اهنأ يلع
متي مل ةهجاو الى اهل يوحت مت يتل مزحل ان ف، تقول الى ةدنتسمل (ACL) لوصول
اهتجالع لجا نم هي جوتل جلاع م الى اهي جوت ةداع تم نكلو لاطب لال خ نم اه عيزوت

لحال وه امك اهسفن يه تقول الى ةدنتسمل ةعزومل ACL ةمئاق ةصاخل ةغايصل دعت
لئاسر ةلحج قلع تي امي ف رمأل ةفاض عم تقول الى ةدنتسمل ACL ةمئاق ل ةبس نلاب
لاطب ةقاطب و هي جوتل جلاع م ني ب (IPC) جلاع م ني ب لاصلت ال

<#root>

```
debug time-range ipc
show time-range ipc
```

ACL) لوصول اب مكحتل مئوق لابقتسا

تاهوم ىلع نامألا ةدايزل ةملتسُملا (ACL) لوصول اب يف مكحتل مئوق مادختسا متي صاخلا (GRP) gigabit route processor هي جوتلا جلام ةيامح لالخ نم Cisco نم 12000 ةلسلسلا يف مكحتل مئوق ةفاضلا تمت. ةلمتحملا ةراضلاو ةرورضلا ريغ رورملا ةكرح نم ةجوملاب Cisco IOS جمانربلا رادصلا ةنايصللا ديقت نع صاخ لزانتك ةملتسُملا (ACL) لوصول مئوق [مالتسا: GSR ىلا](#) عجرا. 12.0(22)S رادصلا يف اهجم دو 12.0.21S2 رادصلا، Cisco Software، تامولعمل نم ديزم ىلع لوصول [لوصول اب يف مكحتل](#).

ةيساسألا ةينبلا ةيامحل (ACL) لوصول اب يف مكحتل مئوق

رطاخم ليلقتل ةيتحتللا ةينبلا ةصاخلا (ACL) لوصول اب يف مكحتل مئوق مادختسا متي اهب حرصملا رورملا ةكرحل حيرص نذا لالخ نم ةيتحتللا ةينبلا ىلع رشابملا موجهلا ةيلاعف و ىلا عجرا. ىرخألا ةرباعلا رورملا ةكرح عيمجل خامسلا عم ةيتحتللا ةينبلا تادعم ىلا طقف لوصول [ةيساسألا ةينبلا ةيامحل لوصول اب يف مكحتل مئوق: ةيساسألا كتقبط ةيامح](#) تامولعمل نم ديزم ىلع.

ةرباعلا (ACL) لوصول اب يف مكحتل مئوق

اهنألا ةكبشلا نامأ ةدايز لجأ نم ةرباعلا (ACL) لوصول اب يف مكحتل مئوق مادختسا متي [مكحتل مئوق](#) ىلا عجرا. كتاكبش وأ كتكبش ىلا طقف ةبولطملا رورملا ةكرح حوضوحتت تامولعمل نم ديزم ىلع لوصول [Edge يف ةيفصتلا: ةرباعلا لوصول اب يف](#).

ةلص تاذ تامولعمل

- [عئاش لكشب ةمدختسُملا IP ىلا \(ACL\) لوصول اب يف مكحتل مئوق نيوكت](#)
- [RFC 1700](#)
- [RFC 1918](#)
- [لوصول مئوق معد ةحفص](#)
- [Cisco IOS ةيامح رادج](#)
- [Cisco Systems - تادنتسمل او ينقتلا معدلا](#)

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 ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل