

مكحتل مئوقو ةكبشلا ناووع ةمچرت نيوكت ASA ةيامح رادج ىلع (ACL) لوصولا يف

تايوتحمل

[ةمدقملا](#)

[ةيساس الابلطتلا](#)

[تابلطتلا](#)

[ةمدختس مئانوكملا](#)

[ةيساس ا تامولعم](#)

[ةماع قرظن](#)

[فادهال](#)

[لوصولا يف مكحتلا ةمئاق ىلع ةماع قرظن](#)

[NAT ىلع ةماع قرظن](#)

[نيوكتلا](#)

[مادختس الاعدب](#)

[ططخلا](#)

[تنترت الابلطتلا بهذي نأ فيضم حمسي نأ nat تليكش 1. ةوطخلا](#)

[تنترت الابلطتلا مديوللا لوصولا ل NAT نيوكت 2. ةوطخلا](#)

[ACL ىلا لوصولا يف مكحتلا مئاقو نيوكت 3. ةوطخلا](#)

[ةمس عبتتتي طبرلا عم ليكشت رابتخلا 4. ةوطخلا](#)

[ةحصللا نم ققحتلا](#)

[اهجالص او عاخذ ال افاشكتسا](#)

[بارقلا](#)

ةمدقملا

يف مكحتل مئاقو (NAT) ةكبشلا ناووع ةمچرت نيوكت ةيفيكت دنتس مئانوك اذه حضوي
ASA ةيامح رادج ىلع (ACL) لوصولا

ةيساس الابلطتلا

تابلطتلا

دنتس مئانوك اذهل ةصاخ تابلطتلا دجوت ال

ةمدختس مئانوكملا

ASA زمر لغشي يذلا ASA 5510 ةيامح رادج ىلا دنتس مئانوك اذه يف ةدراولا تامولعملا دنتست
9.1(1) رادصالا

ةصاخ ةي لمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ م تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف ، ليغشتلا ديقتك تكبش

ةيساسأ تامولعم

للا لوصول يف مكحتلا مئوق نيوكت ةيفيكل ارشابمو اطيسب الاثم دنتسمل اذه فص ي هتباتك تمت دقل . دراولا كلكذو رداصلا لاصتالاب حامسلل ASA ةيامح راجل عىل ACLs و NAT ASA زمر ليغشتب ةنراقم 5510 (ASA) فيكتلل لباقلا نامال زاه ةيامح راجل مادختساب نإ . رخآ ASA ةيامح راجل ماطن يال عىل ةلوهسب رمال اذه قيبتت نكمي نكلو ، (1) 9.1 رداصلا جاتحت تنأ ، يعيبط نراق نم ال دب VLANs لمعتسي يال ، ASA 5505 لثم ةصنم تنأ لمعتسي بسانم بسح عون نراقلا ريغي نأ

ةماع ةرظن

فادهال

حامسلل ةمزالل ACL و NAT تانيوكت يه ام يف رظنلا نكمي ، اذه نيوكتلا لاثم يف لاصتالاب حامسلو ، ASA ةيامح راجل DMZ ةقطنملا يف بيولا مداخىل دراولا لوصولاب نيفدهك اذه صيختل نكميو . DMZ و ةيلخادلا ةفيضملا ةزهجال نم رداصلا

1. تنرتنإلاب رداصلا DMZ لاصتالاب لخدالاب ني دوجوملا نيفيضملااب حامسل .
2. IP ناوئعب DMZ عىل بيو مداخىل لوصولاب تنرتنإل عىل نيفيضملااب حامسل . 192.168.1.100.

زاجياب دنتسمل اذه رمي ، نيفدهال نيذه قيقتحتل اهلامك بچي يتلا تاوطخلا ذي فننت لباق ASA زمر نم ثدخال تارداصلا عىل NAT و (ACL) لوصولا يف مكحتلا مئوق لمع ةقيرط عىل (ثدخال تارداصلا او 8.3 رداصلا).

لوصولا يف مكحتلا ةمئاق عىل ةماع ةرظن

يه (راصتخالل لوصولا يف مكحتلا مئوق و لوصولا مئوق) لوصولا يف مكحتلا مئوق لكشبو . ةضوفرم و اهب حومسم رورملا ةكرح ناك اذا ام ASA ةيامح راجل اهب دح ييتلا ةقيرطلا عىل نامأ يوتسم عىل لقا نامأ يوتسم نم رمت ييتلا رورملا ةكرح صفر متي ، يضا رتفا ةهجاو عىل اهقيبطت متي (ACL) لوصولا يف مكحت ةمئاق ةطساوب عارجلا اذه زواجت نكمي . نراق نمأ لفسأ عىل نامأ رورم ةكرح ، يضا رتفا ، ASA ل حامسي ، اضيأ . هذه لقال نامال (ACL) لوصولا يف مكحتلا ةمئاق مادختساب كولسل اذه زواجت اضيأ نكمي .

ةمزح و لاصتالاب ةنراقمب ASA ماق ، (مدقال تارداصلا او 8.2) ASA زمر نم ةقباسلا تارداصلا يف ينعمب . ال و ةمزحلا ةمجرت عاغل نود ةهجاو عىل (ACL) لوصولا يف مكحتلا ةمئاق لباقم ةدراو كلت طاقتلا ديرت تنك ول امك ةمزحلل (ACL) لوصولا يف مكحتلا ةمئاق حمست نأ بچي ، رخآ لباق ةمزحلا كلتل ASA ةمجرت متت ال ، ثدخال زمرلاو 8.3 رداصلا يف . ةهجاو عىل ةمزحلا اذهو ، زمر رخأتمو 8.3 ل نأ ينعي اذه . ةهجاو ل (ACLs) لوصولا يف مكحتلا مئوق نم ققحتلا IP مچرتي فيضملا الوحمسي IP يقيقتح فيضملا عىل رورم ةكرح ، ةقيثو

[ةلسلس نم رماوالا رطس ةهجاو نيوكت ليلىد : 2 باتكلا يف لوصولا دعاقو نيوكت](#) مسق عجار

لوصولها في مكنحتل مئوق لوح تامولعمل نم ديزم يلعل لوصحلل [9.1 رادصلال، Cisco ASA](#).

NAT يلعل ةماع ةرطن

Auto NAT (Object NAT) ب نيفورعمل نيعون لئ مسقت دعب اميفو 8.3 ةغيص يف ASA لئ لعل nat ةكبش فيرعت نمض تللكش، nat نئك، نانثال نم لوالا. (NAT نيترم) يودي NAT و (Object NAT) ةقيرطل ةيساسال تازيملا يدح. دنتمسلا اذو يف اقحال كلذل لعل لاثم ريفوت متي. نئك لهسا وه اذو. تاضراعتل بنجتل ةلعمل دعاقو بلطب ايئاقلت ASA موقو نأ يو هذو NAT ال عيطتسي تنأ، الثم. ببحت لئكشت يف دح يتأي ةلوهسلا هذو عم نكلو، nat لئ لكش nat، ينال لعل عم عيطتسي تنأ نأ امب طبرلا يف ةيغال لعل سسؤي رارق ةمجت لعلج تللكش طوطخلل نوكت نأ بلطتي وه نأ ريغ، هتباقن يف ةوق رثكأ وه يودي nat لئ. يودي nat ةجيتنو، NAT عون اذو دقعي اذو. جحصلا كولسلل ققحي نأ نكمي ثيحب جحصلا بيترتلل اذو. اذو نيوكتل للاثم يف همادختسا نكمي ال كلذل

ل [9.1، دشرم لئكشت CLI ةيماح رادج cisco ASA sery 2: باتك](#) نم مسق [nat لوح ةمولعمل](#) تيأر NAT لوح ةمولعمل ريثك.

نيوكتل

مادختسال ادب

لئ صوت متي. ةكبش لعل عطاقم ةثالشب ةلصتم تاهجاو ثالث وه ةيساسال ASA نيوكت دادع لئ صوت مت. 0 نامأ يوتسمب ايچراخ هتيمست متي و Ethernet0/0 ةهجاوب ISP ةكبش عطاقم DMZ، عطاقم 100 نامأ يوتسمب لخالاب اهتيمست مت و 0/1 تنرثيالاب ةيخالاب ةكبش لعل 50 غلب ي نامأ يوتسمب DMZ هيلعل قلطي و Ethernet0/2 ب لصتم، بيولا مداخ دجوي ثيحب

ان: للاثم لئ IP نيوانعو ةهجاوال نيوكت رهظي

```
interface Ethernet0/0
  nameif outside
  security-level 0
  ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
  nameif inside
  security-level 100
  ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
  nameif dmz
  security-level 50
  ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

ل لخدم ريصقتل وهو، 192.168.0.1 ناو نعل عم تتبث لئ لئ ASA لئ نأ تيأر عيطتسي تنأ انه نم هيلعل لوصحلل مت يذل IP ناو نعل مادختساب ةيچراخلل ASA ةهجاو نيوكت مت. فيضم لئ لئ لئ ISP. اذو ةباوب نوكت نأ ةللالل ةوطخلل تبثي يذل، ناكلما يف فيضارتفا راسم كانه ISP.

اذه ىلى لثامم لىكشت اذه ودبى:

```
object network inside-subnet
 subnet 192.168.0.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
object network dmz-subnet
 subnet 192.168.1.0 255.255.255.0
 nat (dmz,outside) dynamic interface
```

(show run) رمألا تاجرخم مادختساب) ةطقنلا هذه يف هلىغشت ىراجل نىوكتلا ىلى ترظن اذا ىلى طقف لوألا عزجلا رىشى .جارجلا نم نىئزج ىلى مسقم نىكلا فىرعت نأ ىرت نأ كنىمى مسقلا رهظى امنىب ،(كلذ ىلى امو ،IP ناووع ،ةىعرفلا ةكبشلا/فىضملا) نىكلا فى وه ام قىباسلا جارجلا فى لوألا لاجدالا تذخأ اذا .نىكلا كلذب ةطبترملا NAT ةدعاق ىناثلا

نم 192.168.0.0/24 ةىعرفلا ةكبشلا زایتج قىباطت ىتلا ةفىضملا ةزهجال نوكت ام دنع ةىجراخلا ةهجال ىلى اىكىمانىد اهتمرت دىرت تنأف ،ةىجراخلا ةهجال ىلى ةىلجدلا ةهجال

تنرتنالا نم بىولا مداخ ىلى لوصول NAT نىوكت 2. ةوطخلا

ىلى لوصول DMZ تاهجاو لجدالاب نىدوجوملا نىفىضملا ناكما بىبصأ نأ دعب نألا ىلى لوصول نم تنرتنالا ىلع نومدختسملا نكىمتى ىتح نىوكتلا لىدعت كىمزلى ،تنرتنالا نكىمتى شىب داعدالا داعدامتى ،لاثملا اذه فى .80 TCP ذفنم ىلع انب صاخلا بىولا مداخ IP ناووع وهو ،ISP هرفوى ىذلا رخآ IP ناووع لاصتالا نم تنرتنالا ىلع نودوجوملا صاخشألا نكىمى ،نىوكتلا اذه مادختساب .198.51.100.101 مدختسأ ،لاثملا لىبس ىلع .هكلمن فىاضا ىلى لوصول لالا نم DMZ بىو مداخ ىلى لوصول تنرتنالا ىلع نىمدختسملا لىل مجرتى نأ نكىمى ،ةمهمللا هذلل نىكلا ل NAT مدختسأ .80 مقرر TCP ذفنم ىلع 198.51.100.101 ذفنم ىلع 198.51.100.101 لثم ودبىل (192.168.1.100) بىولا مداخ ىلع 80 TCP ذفنم ASA دعاوق فىرعتب مقونىك فىرعتب مق ،اقباس هلعف مت ام عم لثملاب .جراخلا نم 80 مقرر TCP اذه ةمجرت نكىمى ىذلا IP لىلثمتل نا نىكلا فىرعتب مق ،اضىأ .نىكلا كلذل ةمجرتلا هىلى فىضملا

اذه ىلى لثامم لىكشت اذه ودبى:

```
object network webserver-external-ip
 host 198.51.100.101
!
object network webserver
 host 192.168.1.100
 nat (dmz,outside) static webserver-external-ip service tcp www www
```

لاثملا اذه فى هذه NAT ةدعاق هىنعت ام صىخلتلاو

نم sourced لىصوت ةعطق DMZ لىل 192.168.1.100 ناووعلا قىباطى نأ فىضم قلىخى ام دنع TCP نوکى نأ مجرتى نأ دىرت تنأ ،ىجراخلا نراقلا جراخ بهذى لىصوت نأو (WWW) 80 عانىم TCP

198.51.100.101 نوكي نأ ناوونع نأ مچرتيوي جراخ نراقلا ىلع (WWW) 80 ءانيم

ىلإ ل دعم بيورورم ةكرح نأ ريغ، "www) 80 ءانيم TCP نم sourced"... اليلق بيورغ ودي اذه
كذلذ ةجيتن. اهتعببط يف هاجتإلا ةيئانث NAT دعاوقلا هذه نأ مهفن نأ مهمل نم. 80 ءانيم
ةيقتنم رثكأ تحبصأ ةجيتنلاو. ةلمجال هذه ةغايص ةداعإل تاملكلا بلق كنكمي

(www) 80 ءانيم TCP ةياغ ىلع 198.51.100.101 ىلإ لاصتا جراخلا ىلع فيضم قلاخي ام دنع
تنك عيقتسي ءانيم ةهجو لاو 192.168.1.100 نوكي نأ ناوونع ةياغلا تمجرت عيقتسي تنأ
DMZ ل نم هتلسرأو (www) 80 ءانيم TCP.

مئاوق دادعإ كمزلي، كلذ دع ب. ةقيرطالا هذبه هتغايص متت ام دنع رثكأ ايقطنم اذه نوكيوي
(ACL) لوصولا يف مكحتلا

ACL ىلإ لوصولا يف مكحتلا مئاوق نيوكت 3. ةوطخلا

ASA ىلع لوصولا يف مكحتلا مئاوق كل حمست، ركذت. بيورق ليكشت اذه ةياهنو تلكتش nat
ي: يلي امك وهو يضارثفالا نامألا كولس زواجت ب

- نامأ ةهجاو ىلإ اهلاق تنا دنع لقأ نامأ ةهجاو نم لقتنت يتلا رورملا ةكرح ضمفرتي
ىلع.
- نامأ ةهجاو ىلإ اهلاق تنا دنع ىلع نامأ ةهجاو نم لقتنت يتلا رورملا ةكرح حامسلا متي
لقأ.

هذه رورملا ةكرح لمعت، نيوكتلا ىلإ (ACL) لوصولا يف مكحت مئاوق ية فاضا نودب كذلذ
لثملا يف:

- ني فيضم لاب لاصتالا (100 نامألا ىوتسم) لخادلا يف ني دوجوملا ني فيضم ل نكمي
(50 نامألا ىوتسم) DMZ ةقطنملا يف
- ني فيضم لاب لاصتالا (100 نامألا ىوتسم) لخادلا يف ني دوجوملا ني فيضم ل نكمي
(0 نامألا ىوتسم) جراخلا يف ني دوجوملا
- (50 نامألا ىوتسم) حالسلا نم ةدرجملا ةقطنملا يف ني دوجوملا ني فيضم ل نكمي
(0 نامألا ىوتسم) جراخلا يف ني دوجوملا ني فيضم لاب لاصتالا

هذه رورملا ةكرح ضمفرتي، كلذ عمو

- ني فيضم لاب لاصتالا (0 نامألا ىوتسم) جراخلا يف ني دوجوملا ني فيضم ل نكمي ال
(100 نامألا ىوتسم) لخادلا يف ني دوجوملا
- ني فيضم لاب لاصتالا (0 نامألا ىوتسم) جراخلا يف ني دوجوملا ني فيضم ل نكمي ال
(50 نامألا ىوتسم) DMZ ىلع
- لاصتالا (50 نامألا ىوتسم) DMZ ةقطنملا يف ني دوجوملا ني فيضم ل نكمي ال
(100 نامألا ىوتسم) لخادلا ب ني دوجوملا ني فيضم لاب

ي، لال اهن نيوكت عم ASA ةطساوب اهضمفرتي DMZ ةكبش ىلإ جراخلا نم رورملا ةكرح نأل
في NAT نيوكت نم مغرلاب بيولا مداخ ىلإ لوصولا تنرتنإلا ىلع ني مدختسم ل نكمي ال
نأ بجي، ثدحألا زمراو 8.3 يف. جهرصر لكشب هذه رورملا ةكرح حامسلا ىلإ جاتحت 2. ةوطخلا
اذه. مچرتملا IP سيولو لوصولا يف مكحتلا ةمئاق يف ني فيضم ل قيقحلا IP مدختست
ةكرح سيولو 192.168.1.100 ىلإ ةهجوملا رورملا ةكرح حامسلا ىلإ جاتحت نيوكتلا نأ ينع
مادختسا نكمي، ةطاسبلا لجأ نم. 80 ذفنملا ىلع 198.51.100.101 ىلإ ةهجوملا رورملا

لكشبة هجاوول لوصول في مكنحتلا عمئاق في رورملا كرحب حامسلا كيلع بجيو لوعفملا حيرص.

عمس عبتتي طب رلا عم ليكشت رابتخا. 4 ةوطخل

مادختسا يه قيرط لهسا. لمعي هنا نم دكأتلل هرابتخا كمزلي، نيوكتلا لامكإ مت دقو نألا نم اذه رابتخا عجلصم، كذا عمو. (كتكبش يه هذه تناك اذا) ةيلعفل ةفيضملا تائيبل ي رابتخال مزحلل بقعت ةادأ مدختسا، ASA تاودأ نم ديزملا فاشكتسا ورمأوالا رطس ةهجاو اهئاظأا حيصت ةينامإو اهتفداصم تمت لكاشم.

راسم يلا ةمزحلا هذه لاخداو تاملعمل نم ةلسلس يلا اذانتسا ةمزح ةاكاحمب tracer ةمزح لمعت مت اذا ةيقيقحلا ةايحلا ةمزح اهمدختست نأ نكمي يتلا ةقيرطلل لثامم، ةهجاوالتا نايب تايلمعل او تاققحتلا نم يصح يال ددع لالخنم ةمزحلا هذه عابتا متي. كلسلا نم اهطاقتلا. ةجيتنلا ةظحال مب ةمزحلا عبتت موقيو، ةيامحلا رادج ربع اهرورم دنع اهب مايقلا متي يتلا ةيامحلا رادج رمالا اذه دشري. تنرتنالا يلع فيضم يلا جرخي يذلا يلاخادلا فيضملا ةاكاحم يلا:

ردصملا ذفنم يلع 192.168.0.125 IP ناووع نم ةيلخادلا هجاوالا في ةدراولا TCP ةمزح يكاخي 80 ذفنملا يلع 203.0.113.1 IP ناووع يلا ةهجوملا 12345.

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80
```

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 0.0.0.0 0.0.0.0 outside
```

```
Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
 nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345
```

```
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
```


Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

تايللمع عيمج تزواجت اهنأ ينعي امم، اهب حومسم رورملا ةكرح نأ يه ةيئاهنلا ةجيتنلا تمجرت ةمزحلا نأ طحال جراخ، جورخال ةهجاونم اهلاسرا متو نيوكتل ي ACL و NAT نم ققحتلا ةمجرت متت. اهليل لوصولا مت يتلا ةدعاقلا رهظت ةلحرملا كلت ليصافتو 3 ةلحرملا ي نيوكتل للاقو 198.51.100.100 ىل يكيما نيدي لكشب 192.168.0.125 فيضملا

ىل عني فيضملا نكمي، ركذت. بيولا مداخل ىل تنرتنإل نم لاصلتال لهليغشتب مق، نآلا ةرم. ةجراخال ةهجاولا ىل 198.51.100.101 ب لاصلتال اب بيولا مداخل ىل لوصولا تنرتنإل ىل يلاتال رمالا مجرتي، ىخ:

ردصملا ذفنم ىل 192.0.2.123 IP ناو نع نم ةجراخال ةهجاولا ي ةدراولا TCP ةمزح يكي احي 80 ذفنملا ىل 198.51.100.101 IP ناو نع ىل ةهجوملا 12345

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80
```

Phase: 1

Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:

New flow created with id 3, packet dispatched to next module

```
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

،اديچ نيوكتلا ودبي ،لوصولو ي ف مكحتلا مئوق بحس .حومسم طبرلا نأ ةجيتنلا ،ىرخأ ةرم ،يچراخال IP مادختساب اذه بيولا مداخ لىل لوصولو (جراخ) تنرتنالا لىل ع نيمدختسملل نكمي و .

ةحصلال نم ققحتلا

ةمزلال بقعت ةزيم مادختساب نيوكتلا رابتخا - 4 ةوطخال ي ف ققحتلا تاءارجا نيضت متي .

اهحالص او ءاطخال فاشكتسا

اهحالص او نيوكتلا اذه ءاطخا فاشكتسا ةيفيكي لىل ع رفوتي ةدحم تامولعم نم ام ايلاح كانه .

رارقال

ي ف لاثملا فيفيكت نكمي .ةمهم نم بعص لكل ذ nat يساسا متي نأ ASA نم ليكشتلا سيلي لاثم ي ف ةمدختسمل ذفانملاو IP نيوانع ريغتت تمق اذا دحم وييرانيسل دنتسمل اذه لىل ASA ةبسنلاب اذهل اءاشم ،هجمد دنع ،اذهل يئاهنلا ASA نيوكت ودبي و .تانويكتلا 5510:

```
ASA Version 9.1(1)
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
 subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
 subnet 192.168.1.0 255.255.255.0
object network webserver
```

```

host 192.168.1.100
object network webserver-external-ip
  host 198.51.100.101
object network dns-server
  host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
  nat (inside,outside) dynamic interface
object network dmz-subnet
  nat (dmz,outside) dynamic interface
object network webserver
  nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1

```

ب لصتم ج راخ) اق ب سم حضورم وه امك تاه ج اول ل ل صوت عم ، ل ا ث م ل ل ل ب س ل ع ، ASA 5505 في
Ethernet0/0، ب لصتم DMZ و Ethernet0/1 ب لصتم ل خاد ، Ethernet0/2):

```

ASA Version 9.1(1)
!
interface Ethernet0/0
  description Connected to Outside Segment
  switchport access vlan 2
!
interface Ethernet0/1
  description Connected to Inside Segment
  switchport access vlan 1
!
interface Ethernet0/2
  description Connected to DMZ Segment
  switchport access vlan 3
!
interface Vlan2
  nameif outside
  security-level 0
  ip address 198.51.100.100 255.255.255.0
!
interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
  nameif dmz
  security-level 50
  ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
  subnet 192.168.0.0 255.255.255.0

```

```
object network dmz-subnet
 subnet 192.168.1.0 255.255.255.0
object network webserver
 host 192.168.1.100
object network webserver-external-ip
 host 198.51.100.101
object network dns-server
 host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
 nat (inside,outside) dynamic interface
object network dmz-subnet
 nat (dmz,outside) dynamic interface
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ل ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة يرش ب ل و
م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل چ ن ا ل ا دن ت س م ل ا