

يطلع احوال صاير رورملا ةكرح عا طخا فاشكتسا CSF ل (CLI) رماوالا رطس ةهجاو

تايوت حمل

[قم دقمل](#)

[قيساسالا تابلطتم](#)

[تابلطتم](#)

[قم دختسملا تانوكملا](#)

[قلصل تاذ تاجتتملا](#)

[قمهم تامولعم](#)

[قيساسا تامولعم](#)

[قلكشملا](#)

[راسملا نع شحبل: 1 ةوطخل](#)

[Packet-Tracer لي غشت: 2 ةوطخل](#)

[طاقتل لي غشت: 3 ةوطخل](#)

[ماظنلا معد عبتت لي غشت: 4 ةوطخل](#)

[قحصل نم ققحتلا](#)

[احوال صاير عا طخا فاشكتسا](#)

[قلصل تاذ تامولعم](#)

قم دقمل

Cisco نم نم آلا ةيامل رادجل (CLI) رماوالا رطس ةهجاو مادختسا ةيفيك دنتسملا اذه حضوي
كولسو مزحلا قفدتو هي جوتلا نم ققحتلا لالخنم احوال صاير رورملا ةكرح عا طخا فاشكتسال
ةجذمنلا.

قيساسالا تابلطتم

دنتسملا اذهل ةصاخ تابلطتم دجوتال

تابلطتم

ةيلالاتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

- نئاكل ني نوكتو Firepower (FMC) ةرادا زكرم تاسايس

- Cisco نم (CSF) نم آلا ةيماحل راج هيچوتو ةهجال قطنم
- اهلصاو ةيماحل راج ءاطخأ فاشكتساو مزحل صحف ميهافم

ةمدختسملا تانوكملا

يف ممدختسملا زاهجل موقى CSF ل ةغيص زاهجو ةيچمرب صاخ ىلإ ةقيثو اذه دىقي ال 7.6.5. زمزلا لىغشتب دنتسمل

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل ءاشنإ مت تناك اذا. (يضايرتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال ةيجمج تادب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا دىق كتكبش

ةلصللا تاذ تاجتنملا

ةغيص ةيچمربو زاهج اذه عم تلمعتسا تنك اضيأ عيطتسي ةقيثو اذه

- (FMC) نم آلا ةيماحل راج ةرادا زكرم
- Cisco نم (CSF) نم آلا ةيماحل راج
- Firepower دىدهتل ةيعافدلا (CLI) رماوالا رطس ةهجاو تاودأ

ةمهم تامولعم

وأ ةركاذلا وأ (CPU) ةيزكرمل ةجلالعمل ةدحو مادختسا نم اعفترم ىوتسم زاهجل هجاوي ام دنع مقافت ىلإ اهلصاو ءاطخأ فاشكتسا رماو اذيفنت يدؤي نأ نكمي ،جارخا/الاخدا ةدحو يف ةعباتملا مث ،الو اهلحو دراوملا كالهتسا ةلاح يف قيقيحتلاب ىصوي .ءادال ضافخنا نأ نكمي امم ،ةيفاضا ماظن دراوم صيخشلا رماو كالهتست .رورملا ةكرح ةلكشم صيخش دادرستالا ةدم ةلاطاو رفوتلا ىدم يف يفاضا ضافخنا ىلإ يدؤي

ةيساسا تامولعم

راسملا ديكأت لالخن نم CSF ىلع اهلصاو رورملا ةكرح ءاطخأ فاشكتسا أدبي ام ابلاغ ،ةهجاو راسملا طيخت مهف درجمب .ةيماحل راج ربع ةمزل هكلست نأ بجي يذلا يقطنملا اذه ذيفنت نكميو .يلعفل ةمزل قفدتب عقوتملا راسملا ةنراقم يه ةيلاتلا ةوطخل نإف عبتتو مزحل طاقتل او-tracer ةمزح قيبطت ةكاحم وراسملا ثحب تايلمع مادختساب ءارجلال ةكبشلل كرحم

ةيؤرلا نم ةفلتخم ةقبط ءادأ لك رفوت

- .ةهجاوالا ةيوهو ةمزحلا هيحوت راسم show route دكؤي
- و (ACL) لوصولا يف مكحتلا ةمئاق تارارق ددحيو رورملا ةكرح قفدت Packet-tracer يكاحي
- .ةهجاوالا NAT
- .ةيامحلا رادج زاتجت يتلا ةرشابملا تانايبلا رورم ةكرح صحف طاقتلا مزح
- ةقلعتملا لتكلل ةرشابم ريغ ةقيرطب رارقلا ذاختا ةيلمع ماظنلا معد عبتت ضرعي
- .شيتفتلا ثادحأ وأ تاسايسلاب

يتح ،رورملا ةكرح طاقتلا لبق مزحلا عبتت ةحص نم ققحتلاو هيحوتلاب أدبا :حيملت لبق نيحيحص لوصولا يف مكحتلا تارارقو عقوتملا راسملا ناك اذا ام ديكأت كنكمي .ةرشابملا رورملا ةكرح ليلحت

ةلكشملا

ذخأت ةمزحلا تناك اذا ام ديدحت لوؤسملا ىلع بجيو ،عقوتم وه امك رورملا ةكرح قفدت لمعي ال جهنلا صحف ناك اذا امو ،هضفري وأ لاصتالاب حمسي ةيامحلا رادج ناك اذا امو ،حيحصلا راسملا رورملا ةكرح عنمي لفطتلا وأ

راسملا نع شحبالا :1 ةوطخلا

.ةهجولاوردصملا IP نيوانعب ةطبترملا ةيقطنملا ةهجاوالا ءامسأ ددحو هيحوتلا راسم ددح كذل ،اهحالصإو ءاطخألا فاشكتسأ رماوأ مظعم لبق نم ةبولطم ةيقطنملا ةهجاوالا ءامسأ .اهحالصإو ءاطخألا فاشكتسأ لمع ريس يف ىلوالا ةوطخلا هذه نوكت نأ بجي

IP: ناونع ةهجولاوردصملا رمألا ليغشتب مق

show route <IP>

في رعت يضارثفالا راسملا ىلع دمتعت يتلا تنرتنإلا ىلإ ةهجوملا رورملا ةكرح بلطتت ةوطخلا هذه ذيفنت لالخنم يققطنملا ةهجاوالا مسا ديدحت نكمي .ةيقطنملا جورخلا ةهجاو

show route 0.0.0.0

جارخالا لاثم

FTD1# show route 192.168.0.11

Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

 directly connected, via Inside
Route metric is 0, traffic share count is 1

FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

 128.107.0.1, via Outside
Route metric is 0, traffic share count is 1

جراخ نراق جرخم لاو لخاد نراق لخدم يقطنم لا، لاثم اذه يف

 تاهجاو لال خ نم رورم لا ةكرح هيچوت (NAT) ةكبشلا ناو نع ةمچرت ديعت نا نكمي :ريذحت
ةكرح قفدت NAT تاسايس قباطت ام دنع هيچوت لا لودج هيل ري شي امم ةفلتخم
كيدل NAT نيوكت نا نم ققحت، اهاحالصاو لاصتالا عاطاخا فاشكتسا دنع .رورم لا
عقوتم لا رورم لا ةكرح راسم عم قفاوتي

 CLI عاطاخا فاشكتسا رماوا يف ةيقطنم لا ةهجاو لا ءامسا مادختسا متي :حيملت
لبقتسم لا يف هيل عوچرلل يقطنم لا مسالا عطاخالم عاجرلا .اهحالصاو

Packet-Tracer لي غشت 2: ةوطخلا

دعاست .نعم رورم ةكرح قفدتل ةيhamحل رادج مييقت ةيفيك ةاااحمل packet-tracer مدختسا
اذا امو، NAT ةسايس قيبطت متي ناك اذا امو، اهامدختسا متي تاهجاو لا ي اديكات يف ةادالا هذه
اهضفرت وا رورم لا ةكرح بجمست (ACL) لوصولا يف مكحتلا ةمئاق تناك

هذه رمالا ةغايص مدختسا

packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destination port>

لأثام رمأ

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

نوكو و. ةاكاحملا ءانثأ اهب حومسم اهنأ وعقوتملا راسملا عبتت ةمزحلا نأ ديكأتل جارخإل عجار
و NAT وأ هي جوتلاب ةقلعتم ةلكشملا تناك اذا ام ديدحت ىلإ جاتحت ام دنع اديفم عارجل اذه
ةرشابملا ةمزحلا ليلحت في طارخنالا لبق ةسايسلا ةقباطم

ةهجاو في ةاكاحملا ةمزحلا نقح في packet-tracer في transmit ةيساسألا ةملاكلا ببستت
ةاكاحمك عاقبل نم الدب ةياملال رادج ةجلاعم لحارم عيجم زايح نم اهنكمي امم ، لوخدلا

لأثام رمأ

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

طاقاتلا ليغشت : 3 ةوطخل

فلتخت . ةياملال رادج ربع اهرورم ءانثأ ةرشابملا رورملا ةكرح صرحفل مزحلا طاقاتلا مدختسأ
قباطت نأ بجي يلاتلابو ةيلعف رورم ةكرح طقتلت اهنأ Packet-tracer نم ةمزحلا طاقاتلا
اطشن طاقاتلا هي في نوكي يذلا تقولا في ةياملال رادج زاتجي يذلا يقيقحلا قفدتلا
لاصتالا يبناج الك قثوت ، هاجتالا ةيئانث مزحلا طاقاتلا تايلمع

تايلمع نيوكتب مق ، اهالصلو رورملا ةكرح عاطخأ فاشكتسأ تاهوي رانيس مظعمل ةبسنلاب
ةيلاتلا طاقاتلا

- ردصملا بئاج ةهجاو ىلع لصت ياتلا رورملا ةكرح ضبق ىلع — لخدملا طاقاتلا
- ةهجولا بئاج نم ةهجاو ىلع جورخل دنع رورملا ةكرح ضبق ىلع — جرخملا طاقاتلا
- قباطتو ةياملال رادج ةطساوب اهطاقسا متي ياتلا مزحلا ىلع — ASP Drop طاقاتلا
اهنيوكت مت ياتلا ريياعملا

ماعم طاقاتلا ةغايص

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

لخدم طاقاتلا ىلع لأثام

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

جرحم ال طاقنتل ىلع لاثم

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

طاقس ال ASP طاقنتل لاثم

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

عاجرال او مامألل رورم ال ةكرح نم لك طاقنتل نكمي هنا ينعي امم، هاجت ال يئانث مزحل طاقنتل
يتل تارارق ال ضرع ةيناكم عبتت ال ةزيم حيتت. ةدحمل ةقباطم ال ريياعم ىل ادا نسا
ةلعلف ال رورم ال ةكرح ىلع ةيامل راج اهذختي



سيل، IP ردصم مچرتي ل طاقنتل لمعتسي نأ بجي جرحم ال، نوکي nat متي ن: ريذحت
جحص لكشب رورم ةكرح post-NAT ل ضبق ىلع نأ، لصلأل ردصم ال

ماظنل معد عبتت ليغشت: 4 ةوطخل

رورم ةكرح قفدتل ىلعفل تقولا في Snort صحف ةيلمع ضرعل ماظنل معد عبتت مدختسأ
ةمئاقل حامسل ةدعاق عم رورم ال ةكرح قباطت امذن ع صاخ لكشب اديفم اذه نوکي و. ني عم
تاطاقتل رهظت. جهنل صحف ةطساوب امرظح متي لازي ال نكلو لوصول في مكحتل
ةفرعمل ةيؤر ةيناكم رفوي ماظنل معد بقعت نكلو، ةمزح رظح مت هنا مزحلل ةيسايقل
ىقلتني هنا ينعي امم، هاجت ال يئانث ماظنل معد عبتت. ةقيرطال هذبه ةمزحلل ةجلاعم ببس
مه ال ةادأل ىل IPs ةفاضل هب متي يذل بيترتل نأ ينعي اذه. نينبناجل ال كم نم رورم ةكرح

تابل اطملل ةباجتسال او رمال اذه ليغشتب مق

> system support trace

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

وَأ URL ناو نع وأ قيبطتال دعاوق ةئيبال مدختست ام دنع صاخ لكشب ةديفم ةأدأل هذه نوكت
دعب تازيما هذه مبيقت متي .لفطتال جهن وأ تافلما جهن وأ ةيوهال إلإ ةدنتسمال دعاوقال
مكحتال ةسايس ةطساوب ةمزحلاب حامسلا نكمي كذل ،لوصولا يف مكحتال ةمئاق ةقباطم
رخشال صحف ةطساوب اهرطح متي لازي ال نكلو لوصولا يف

ف.ورعم ريغ ددحمال ردصمال ذفنم ناك اذا اغراف ليمعلا ذفنم كرت نكمي :ةطحال م

ةحصلال نم ققحتال

ماظنل معد عبتتو ،مزحلا طاقنالو ،مزحلا عبتت ةكاحمو ،راسمال شحب نم تاجرخلما مدختسأ
راسمال كلست ةمزحلا تناك اذا ام ديدحت وه فدهالو .رورمال ةكرح قفدت كولس ديكأتل اع
ادانتسا هعنمي رخشال ناك اذا امو ،هيفني وأ كلذب حمسي ةيامحل رادج ناك اذا امو ،حيحصلال
قمعأ صحف إلا

يجزومن لكشب اهالحاصلو عاطخال فاشكتسال لماكل قفدتال دكؤي

- ةيقطنمال جورخلو لوخدل تاهجاو راسمال شحب رهظي
- ةسايسال مبيقتو دوصقمال هيحوتال ةداعإ راسم Packet-tracer دكؤت
- عقوقتم وه امك رداغتو لصت رورمال ةكرح تناك اذا ام ةمزحلا طاقنال تايلمع دكؤت
- ةلتكال ثودح يف ببستي رخشال وأ جهنال صحف ناك اذا ام ماظنل معد عبتت دكؤي

اهالحاصلو عاطخال فاشكتسا

ةيلاتال قطانمال عجار ،رورمال ةكرح ةلكشم رمتست ام دنع

- ةعقوقتمال ةهجولو ردصمال تاهجاو قباطي راسمال شحب ناك اذا ام ققحت
- ةلحرم nat وأ ACL ال يف ركني نوكي رورمال ةكرحال جاتنإ يدبي packet-tracer ال اذا ام تققد
- كرتي ةيامحل رادج إلإ لصي نوكي رورمال ةكرح نأ ضبق إلع طبرجورخو لخدمال تعجار
حيحص نراقال إلع
- رورمال ةكرح طاقساب موقبي ةيامحل رادج ناك اذا ام ديكأتل ASP طاقسال طاقنال مدختسأ
ايلخاد
- رارق دعب رورمال ةكرح رطح موقي Snort ناك اذا ام ديدحتل ماظنل معد عبتت مدختسأ
(ACL) لوصولا يف مكحتال ةمئاق لحامسلا

ةلص تاذا تاملولعم

- [اهحل الصاوة ك ب ش ل ا ع ا ط خ ا ف اش ك ت س ال FirePOWER ة ي ام ح ر ا د ج ط ا ق ت ل ا ل ي ل ح ت](#)
- [م ز ح ل ا ع ب ت ت و FirePOWER د ي د ه ت ن ع ع ا ف د ل ا ط ا ق ت ل ا م ا د خ ت س ا](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا