

اهحال صا و رورم لا ة كرح ءاطخا فاشكتسا FTD ىلع LINA لوكوتورب صحف ببسب

تايوتحملا

[ةمدقملا](#)

[ةيساسالا تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[ةيضارتفالا تانوكملا](#)

[MPF لوكوتورب صحف ببسب مزحلا طاقسا تاي لمع ىلع فرعتلا](#)

[ةعئاشلا طاقسا لا اطح لئاسر](#)

[Sun ل RPC صحف طاقسا لا اطم](#)

[SQL*NET Inspection Drop ل اطم](#)

[ICMP صحف طاقسا لا اطم](#)

[SIP صحف طاقسا لا اطم](#)

[اهحال صا و ءاطخالا فاشكتسا](#)

[اهلي طعت و اةدحمل ل LINA MPF تاقى بطت صحف تاي لمع نيكم تة فيكي](#)

[FlexConfig ربع نيوكملا](#)

[FTD ل \(CLI\) رما و اطرس ةهجاو مادختساب نيوكملا](#)

[ةحصلا نم ققحتلا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ةسايسلا راطال LINA لوكوتورب صحف ناك اذا ام دي دحت ةي فيكي دنتسملا اذه حضوي
ةعرسللا قئاف لاسرالا جم انرب" في تانايبلا رورم ة كرح طاقسا ب موقى (MPF) ةي طمنلا
(FTD) نم نم آلا Cisco".

ةيساسالا تابلطتملا

ةيلاللا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- Cisco نم (FTD) ةيامحل راج دي دعت نع نم آلا عافدلا
- Cisco نم (FMC) نم آلا ةيامحل راج ري دم زكرم

ةمدختسملا تانوكملا

ةيلاللا ةي داملا تانوكملا و جم اربلا تارادصا ىل دنتسملا اذه في ةدراولا تامولعمل دنتست

- Cisco Virtual Secure Firewall Threat Defense (FTD)، 7.4.2 رادصا
- Cisco، 7.4.2 رادصا، Cisco نم يره اظلا (FMC) نم آلا ةيامحل راج ري دم زكرم

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجال نم دنتسملا اذه ي ف ةدراول تامولعمل عاشنإ م ت
تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجال ا عيمج ت ادب
رما ي آل لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا دي ق ك تكبش

ةيساسأ تامولعم

ةنونع تامولعم جم دب موقت ي تل تامدخلل ةيامح راج ي ف ةبولطم شيتفتل تاكرحم نوكت
ةني عمل ذفانملا يل ع ةيوناتل تاونقل حتفت ي تل وأ م دختسملا تانايب ةم زح ي ف IP
يكي ماني د لكشب

لالخ نم ةكبشل ل وخذ نم ةراضل رورملا ةكرح عنم ي ف لوكوتوربل صحف دعاسي نأ نكمي
وأ قي بطتل لا ا اذانتسا اهلي دعت وأ تانايبلا رورم ةكرح رظحو ةكبشل مزح يوتحم صحف
مدختسملا لوكوتوربل
نيكمت متي .ةيلامجال ا ةيجاتنإلا يل ع رثؤت نأ نكمملا نم صحفلا تاكرحم نإف اذهل ةجيتنو
ةجاج كانه نوكت دقو ،يضا رتفا لكشب ةيامحل راج يل ع ةعئاشل صحفلا تاكرحم نم دي دعل
ةكبشل بسح ىرخأ تاكرحم نيكمتل هيل

ةيضا رتفال تانيوكتلا

صفح رورم ةكرح لك قباطت ةساي س FTD LINA نيوكت نمضتي ،يضا رتفا لكشب
ةيضا رتفال قي بطتل

(ةيملع ةساي س) نراق لك يل ع رورم ةكرحل يل ع شيتفتل قبطي

ذفانملا لا ا تانايبلا رورم ةكرح ةيضا رتفال قي بطتل صحف رورم ةكرح نمضتت
ديرت تنك اذا كلذل ،طقف ةدحاو ةماع ةساي س قي بطت كنكمي .لوكوتوربل لكل ةيضا رتفال
وأ ،ةيساي ق ريغ ذفانم يل ع صحف قي بطتل ،لاثملا ليل بس يل ع ،ةماعلا ةساي سل ريغي
ةساي سل ريحت لا ا اما جاتحت ،يضا رتفا لكشب اهنكمت متي مل صحف تايلمع ةفاضل
ةديج ةساي س قي بطت واهلي طعت وأ ةيضا رتفال

لالخ نم (CLI) رماوأل رطس ةهجاو ،LINA يل ع show running-config policy-map رمال ليغشتب مق
تامولعمل يل ع لوصحلل diagnostic-cli ماطنل معد

```
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 sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class_snmp
inspect snmp
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

لوگوتورب صحف ببسب مزحل طاقسإ تاي لمع ىلع فرعتل MPF

رادج ىلى لىة نىعملا (ACP) لوصولو ىف مكحتلا ةسايس عم رورملا ةكرح قفاوت دنع ىتح كولسل ارظن تالاصتالاهانإب شىتفتلا ةيلمع موقت، ةنىعم تاهو ىرانيس ىف، ةيامحل رايعم وأ ميمصت دامتعا مدع ببسب وأ، ةيامحل رادج ةطساوب هلابقتسإ مت نىعم رورم ةكرح شىتفتلل دح وأ قىببطت.

ىه ةديفملا ةيلمعلا نوكت، اءالصلو رورملا ةكرح ءاطءا فاشكتسأ ءانثأ

- ةكرح اهنم قفدتت ىتلا تاهءاولا ىلع ىلعفل تقولو طاقتل تالچس نىيىعتب مق رمألا، (ءورءالو لوءللا تاهءاو) رورملا

```
firepower# capture
```

```
[interface
```

```
][match
```

```
[port
```

```
]
```

[port

]]

رايخلل X مزلحلا مقرب ةصاخلا عبتتلا ليصافت ني مضت كنكمي ،تاطقلا مادختساب
عم نكلو ، packet-tracer رمأ لعفي امك ،الاصتالا ذخأ ةلحرم بسح جئاتنلا ةلحرم رفوت نأ بجي و
يلعفل تقولا في رورم ةكرح اهنأ نمضت رايخل اذه .

firepower# show capture

packet number X trace detail

- طاقتلالاعون ضرعي ،(ASP) يلعفل تقولا في عيرسلا نامألا راسم طاقسإ طبض
بابسألاب ةمئاق كانه ، ASP ةطساوب اهطاقسإ مت يتلا تالاصتالا وأ مزلحلا asp-drop
:رمألا ،دنتسملل ةلصللا تاذ تاطابتلالا في اهيلع روثلعل كنكمي يتلا

firepower# capture

[type

] [interface

][match

[port

]

[port

]]

لحارم يف حامسلا ةجيتن ةظحالم نكمي شيح ،لوكوتوربلا صحف طاقسإ تايلمع لهاجت نكمي تالجس مادختساب طاقسإلا ببس نم امئاد ققحتلا مهملا نم ،ببسل اذهلو .Packet-tracer
يلعفل تقولا يف طاقتلالا

ةعئاشلا طاقسإلا أطخ لئاسر

ةدعاسم لل ءاطخألا حيحصت ضارغلأ (ASP) عيرسل نامألا راسم طاقسإ مادختسا متي ام ابلاغ مزحل هذه ضرعل show asp drop رمألا مادختسا متي .اهخالصإو ةكبشل ءاطخأ فاشكتسا يف نأ نكمي يتلاو ،طاقسإلا تايلمع بابسا يف يورفوي امم ،اهطاقسإ مت يتلا تالاصتالا وأ لوصول ةدعاق صفر تالاح وأ صحفل لشف تالاح وأ NAT لشف تالاح لثم لكاشم نمضتت

ASP طاقسإ تالاح لوح ةيسيئرلا طاقنلا:

- ني مضتلا لثم ،ةيدرفلا مزحلأاب ةطبترم طاقسإ تايلمع هذهو :تاراطإلا طاقسإ تايلمع فيضملا ىلا راسم دجوي ال وأ حيحصل ريغ
- اهضفر متي يتلا تاقفدتلا لثم ،تالاصتالاب ةطبترم هذهو :قفدتلا طوقس تالاح NAT لشف تالاح وأ لوصول دعاقو ةطساوب
- تاجرخل ريغتني نأ نكمي وحيحصت لل لوألا ماقملا يف رمألا :مادختسالا

ءاطخأل فاشكتسأ ءانثأ اهتءءاوم كنكمي ةلثمأ يه طاقسأل بابسأ وأ هءه أطحل لئاسر مدختسمال شيتفتل لوكوتورب بسح لجؤت نأ نكمي .اهحالصاو

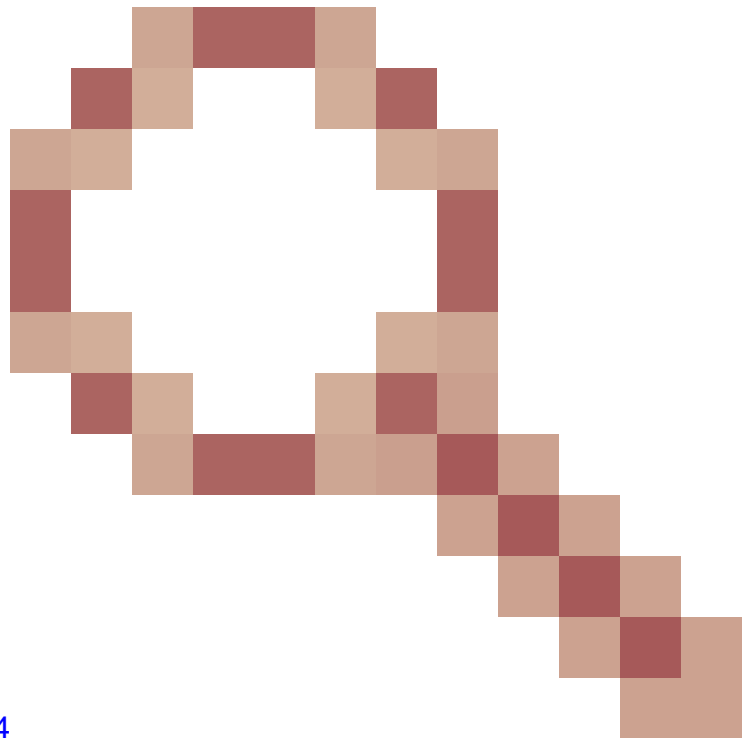
Sun ل RPC صحف طاقسأل لاثم

اذا، Geneve ةطساوب فلغي RPC رورم ةكرح ،AWS رشن ي ف عارذلا يداحأ FTDv ل ويرانيس اذه ل.اصلتال سمشلل RPC صحف نيكمتم

طبر رخآ ةياغك 111 ءانيم لمعتسي Sun RCP ،شيتفت Sun RPC ل تارطق ASP جاتنإل يدبي امك جارخال ي ف طاقسأل بابس .ةياغك 6081 لمعتسي يأ ءانيم ةلسبك ةيلمع Geneve نوكي "حلص رواجت دجوي ال" وه هتطحالم كنكمي

```
firepower# show capture asp-drop
```

```
...
8: 16:23:02.462958 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
9: 16:23:09.769338 10.0.0.5.780 > 172.16.0.3.111: P 1795131583:1795131679(96) ack 526534108 win 29200 D
10: 16:23:10.148658 172.16.0.3.111 > 10.0.0.5.780: . ack 4026726685 win 26880 Drop-reason: (no-adjacency)
11: 16:23:10.463004 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
12: 16:23:26.462729 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
13: 16:23:27.548692 10.79.67.11.60855 > 10.79.67.4.6081: udp 176 [GENEVE segment-id 0 payload-length 13
```



Cisco [CSCwj00074](#) نم ءاطخأل حيحصت فرعم

[SunRPC](#) صحف نيكمتم عم رواجتل مدع عم رورملا ةكرح طاقساب عارذلا يداحأ FTDv ليكوموقي

ناونع نأل LINA كرحم نم ASP ي ف "حيحصلا ريغ رواجتال" اهنأ يلع رورملا ةكرح طاقسإ متي نم (SYN/ACK) ةيناثلا ةمزحل ادعب رافصألأب ةأجف هؤلم متي ةهوجل او ردصم MAC هاجتإل ةيثالث ءحفاصملا

ASP: طاقس إ ب بس

رواجتال مدع: م سال

ح ي ص ل رواجتال مدع

جارخا رواجت ه ي دل د ع ي مل دوجوم ق ف د ت ي ل ع ة مزح نامأل زا ه ج ل ب ق ت س ي ا م د ن ع د ا د ع ل ا ا ذ ه د ي ا ز ت ي ه ي ج و ت ر ي ي غ ت ث د ح ا ذ ا و ا ل و ص و ل ل ة ل ب ا ق ة ي ل ل ا ت ل ة و ط خ ل د ع ت م ل ا ذ ا ك ل ذ ث د ح ي ن ا ن ك م ي . ح ل ا ص ة . ة ي ك ي م ا ن ي د ه ي ج و ت ة ي ي ب ي ف ص ا خ ل ك ش ب

SunRPC ص ح ف ل ي ط ع ت : ل ح ل

SQL*NET Inspection Drop ل ا ث م

SQL*Net ص ح ف ن ي ك م ت م ت ا ذ ا ، AWS ر ش ن ي ف ع ا ر ذ ل ا ي د ا ح ا ل ي ك و ل ل FTDv ل و ي ر ا ن ي س ل ا ا ذ ه Geneve. ة ط س ا و ب ة ف ل غ م ل ر و ر م ل ة ك ر ح ط ا ق س ا م ت ي

(م ق ر ط ب ر ه س ف ن ل ا ت ظ ح ا ل ع ي ط ت س ي ت ن ا) ج م د م ض ب ق ي ل ع ط ب ر ل ل ا ج ا ت ن ا ل ا

ه ح و ك 1521 ذ ف ن م SQL*Net م د خ ت س ي ، ASP-Drop ة مزح ط ا ق ت ل ا ن ي م ص ت م ت ي م ل : ل و ا ل ر ط س ل ا 6081 ء ا ن ي م ة ل س ب ك ة ي ل م ع ل م ع ت س ي Gen ، LINA ي ل ع asp-drop ن ر ا ق VNI : ي ن ا ث ل ر ط س ل ا ة ي ا غ ك

"tcp-buffer-مه ت ظ ح ا ل ع ي ط ت س ي ت ن ا ن ا م ب ، ج ا ت ن ا ل ا ي ف ف ل ت خ م ط ا ق س ا ب ب س ن ا ن ث ا ك ا ن ه timeout" و "tcp-not-syn"

95 2024-12-14 07:55:58.771764 172.16.0.14 10.0.8.2 TCP 251 53905 → 1521 [PSH, ACK] Seq=95: 07:55:58.771764 10.7.0.3.64056 > 10.7.2.5.6081: udp 209 [GENEVE segment-id 0 payload-length 169] Drop-

96 2024-12-14 07:55:58.771780 172.16.0.14 10.0.8.2 TCP 1514 [TCP Out-Of-Order] 53905 → 1521 [ACK] 96: 07:55:58.771780 10.7.0.3.64056 > 10.7.2.5.6081: udp 1472 [GENEVE segment-id 0 payload-length 1432] Drop-

99 2024-12-14 07:55:58.997049 172.16.0.14 10.0.8.2 TCP 308 53903 → 1521 [PSH, ACK] Seq=1 Ack=1 99: 07:55:58.997049 10.7.0.3.64056 > 10.7.2.5.6081: udp 266 [GENEVE segment-id 0 payload-length 226] Drop-

100 2024-12-14 07:55:58.997079 172.16.0.14 10.0.8.2 TCP 1514 [TCP Out-Of-Order] 53903 → 1521 [ACK] 100: 07:55:58.997079 10.7.0.3.64056 > 10.7.2.5.6081: udp 1472 [GENEVE segment-id 0 payload-length 1432] Drop-

ASP: طاقس إ ب بس

tcp-buffer-timeout م سال

ا ه ت ي ح ا ل ص ت ه ت ن ا ي ت ل TCP ة مزح ل ت ق و م ل ن ز خ م ل ة ل ه م

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

ت ا ي ص و ت ل ا

ي ف ي ع ي ب ط ر م ا و ه و ة ك ب ش ل ا ي ف م ا ح د ز ا ل ا ب ب س ب ة ي ل ل ا ت ل ا ة ع ق و ت م ل TCP ة مزح ل ص ت ل ا

مزمحل لاسرل ففرطلل ففضممل فف TCP لاسرل ةءاعل ةلل آءل ء نأ بءل .ةلوءشم ةكبش
ةسلءلل رمل ءل نأ نكمملو.

مسلال: tcp-not-syn

syn ءسلل للوال TCP ةمزل

لصل ءمل رل ءرءم رل ء لاصل ءا نمل للوال ةمزلال SYN رل ء ةمزل فقل ءل

ةلصولل:

لاصل ءا قلال ءل لعلاب ماق ءق زاهلل نوكمل امءنل ءل ء ءلء ءلء نكممل ءل ءلءال ففرطلل ف
ضعب . ءانالل لاسرل ففرءسلو ءلء ءلءال نأ ءلءل مءالل وأ لملءلل لازل الو
ءلءل . 'ءلءل' وأ 'ءلءل' ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل
زاهلل ضرءل نأ نكممل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل
ببسل للءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل

ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل
ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل
ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل
ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل

ICMP صءل ءاقسل لءل

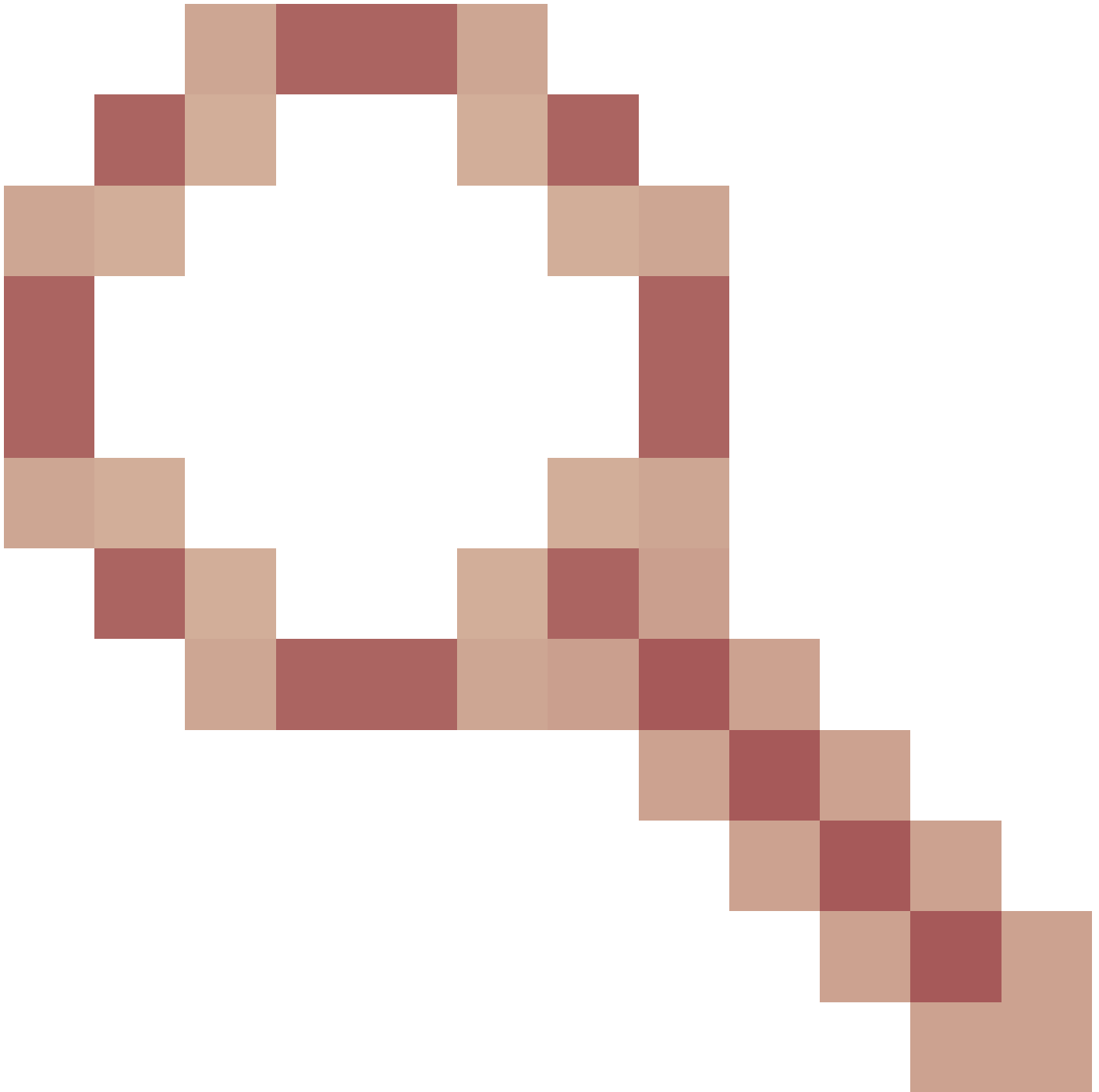
FTD ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل

ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل
ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل
ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل ءلءل

firepower#show cap asp-drop

1: 19:47:09.293136 10.0.5.8 > 10.50.0.53 icmp: echo reply Drop-reason: (inspect-icmp-seq-num-not-match

Cisco ءلءل ءلءل ءلءل [CSCvb92417](#)



["inspection-icmp-seq-num-not-match" بېس عم ICMP دودر بېرمال ىل ASA ةومجم طقس](#)

ASP: طاقس بېس

قباطم ريغ inspection-icmp-seq-num: مسال

ICMP: صف مقر ةقباطم مت مل

ICMP Echo ىل درلا ةلاسري في لسلستل مقرلا قباطتي ال ام دنع دادعل اذه ةدايز بجي
لاصتال سفن ىل اقبس م زاهجل ربع ترم يتل ICMP ىص ةلاسري ا عم

نم رثكأ وانا نانا لكانه نوكي نا نكمي: ةومجمال ماظن ةئيبي في ICMP صف لي طعت: لجال
فذل ريخأت دوجو ةطحال م مت. نيلثامتم ريغ ICMP رورم ةكرحو ةومجمال ماظن في FTD
رابتخا قفدت فيظنت لبق ةعرب قجاللا لاصتال رابتخا لاسرا متي، ICMP قفدت
ةيلاتم لاصتال رابتخا مزل دق شحي نا نكمي، ةلحال هذه في. قباسل لاصتال

SIP طاقس لاثم

دنع لاصتال عطق م ت م ث ، طقف قئاق د س م خ تامل اكمل تقرغتسا ، ويرانيسلا اذه يف تالاصتال SIP طقف طقسى نأ نكمي ، RTP مادختسا .
ةمالع ينعت ، VoIP رورم ةكرجل ةهجاولا ىلع ةمزجل طاقتل جارخا يف ةظحالما كنكمي امكو .
تقولو كلذ يف ةقلغم ةيفتاهل ةملاكمل نأ SIP رورم ةكرج يف BYE .

1	2023-10-13 18:39:03.421456	10.6.6.66	172.16.3.77	SIP/SDP	1055	Request: INVITE sip:1
2	2023-10-13 18:39:03.448325	172.16.3.77	10.6.6.66	SIP	497	Status: 100 Trying
3	2023-10-13 18:39:03.525424	172.16.3.77	10.6.6.66	SIP	687	Status: 401 Unauthorized
4	2023-10-13 18:39:03.525943	10.6.6.66	172.16.3.77	SIP	425	Request: ACK sip:123456789
5	2023-10-13 18:39:03.527331	10.6.6.66	172.16.3.77	SIP/SDP	1343	Request: INVITE sip:1
6	2023-10-13 18:39:03.553544	172.16.3.77	10.6.6.66	SIP	497	Status: 100 Trying
7	2023-10-13 18:39:05.902815	172.16.3.77	10.6.6.66	SIP/SDP	992	Status: 183 Session Pr
8	2023-10-13 18:39:06.091822	172.16.3.77	10.6.6.66	SIP/SDP	967	Status: 180 Ringing
9	2023-10-13 18:39:13.114435	172.16.3.77	10.6.6.66	SIP/SDP	1063	Status: 200 OK (INVIT
10	2023-10-13 18:39:13.115899	10.6.6.66	172.16.3.77	SIP	560	Request: ACK sip:55663399
11	2023-10-13 18:40:29.206593	172.16.3.77	10.6.6.66	SIP	642	Request: UPDATE sip:FD3a5
12	2023-10-13 18:40:29.207630	10.6.6.66	172.16.3.77	SIP	659	Status: 200 OK (UPDATE)
13	2023-10-13 18:41:09.940854	10.6.6.66	172.16.3.77	SIP	684	Request: BYE sip:33445566
14	2023-10-13 18:41:10.003066	172.16.3.77	10.6.6.66	SIP	659	Status: 200 OK (BYE)

ءانيم دحاو طقف عم تكرت ip ل ، برض لمعتسي يا ip ططخي syslog ل يدبي ، رخآ لاثم اذه يف نإ . رسيأ عيزوت ىل بجاو SIP failed ، ءانيم هسفن ل ىلع تطقس ةسلج SIP لاو رفوتي .
ليصوتال تطقس عيطتسي شيتفت SIP لامعتسا يف برض نوكي .

لوصول ببسب IP/port ىل IP/port نم UDP لاصتا ءاشن ىل رداق ريغ : ASP طاقس ببس
ةداع - ببسلا ، صحفلا كرحم ةطساوب هؤاهن مت "و x" وهو فيضم لكل PAT ذفنم ةلتك دح ىل
"دومبني ةداع ةمدخل" نيوك ىل ادانتسا نييعتال

```
Nov 18 2019 10:19:34: %FTD-6-607001: Pre-allocate SIP Via UDP secondary channel for 3111:10.11.0.13/5060
Nov 18 2019 10:19:35: %FTD-6-302022: Built backup stub TCP connection for identity:172.16.2.20/2325 (17
Nov 18 2019 10:19:38: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:38: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
Nov 18 2019 10:19:39: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:39: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
```

ASP طاقس ببس

نمازتمال ريغ راطتنال ةمئاق دح :مسالا
ن: نمازتمال ريغ نيمازتمال راطتنال ةمئاق دح زواجت مت
ةلواحم دنع 1000 غلبي ىصقأ دح نمازتم ريغ نيمازتم لمع راطتنال ةمئاق لكل نوكي نأ بجي
ةمزجل طاقس ببس ، لمعل راطتنال ةمئاق ىل SIP مزح نم ديزمل لاسرا
ةيصوتال :

نكمي ويلصلال نيمازتمال سفن SIP مزجل نوكي ام دنع . طقف SIP رورم ةكرج طاقس نكمي
ىل كلذ دؤي نأ نكمي ، نمازتمال ريغ لفقلا ب ةصاخلا هسفن راطتنال ةمئاق يف اهعضو

مزمح تناك اذإ . طئاسولا عيمج جلاع يي ذلأ وه طقف يداألأ جلاع مأل نأل ارطن ، لتكأل فازنتسإ نم ازتم ريغ ني مأت راطت نا عمئاق مجح زواجتي ام دنع راطت ناأ عمئاق يي ف نوكت نأ لواحت SIP . عمزأل طاقسإ بج يي ، دحلأ

sp راركت ناو نع : مسالا

راركتل ناو نع :

م تي . اهسفن يه قفدت يي هجولأو ردصمأل نيوانع نوكت ام دنع دادعأل اذه دي ازتي نأ يي عي بطأل نم هنأ ثيح ، ناو نعأل عيصوصخ ني كم ت اه يي م تي يي تأل SIP تاقفدت داع بتسإ هجولأو ردصمأل ناو نع سفن تاقفدتل ك لتل نو كي .

عيصوتل :

عم طبر زاهجأل ملتسي ام دنع دحاو . دادعأل اذه دي زي نأ نكم يي ام دنع نال ملتحم نا طرش كانه nat ل ام دنع عي نا ثلأو . (DoS) عم دخلأ صفر موجه عون اذه لثم يي . عيأغلأ يواس ت ناو نع ردصمأل عيأغلأ نأ يواس يي نأ ردصم ناو نع nat زاهجأل نم لي كش ت

قلغم- دلأو : مسالا

يي لصألأ قفدتل قالغلأ مت :

يلع . يي عرفأل قفدتل قالغلأ اض يي أ م تي ، يوناث قفدتل يي لصألأ قفدتل قالغلأ م تي ام دنع اهانأ دنع ددحمأل ببسأل اذهل (يوناث قفدت) FTP تانا يي ب قفدت قالغلأ نكم يي ، لاثمأل لي بس م تي ام دنع اض يي ببسأل اذه حيضوت م تي و . هب صاخأل (يي لصألأ قفدتل) مكحتل قفدت . هب صاخأل مكحتل قفدتل عي بطت ع طساوب (يي صخشأل في رع تأل مقر بقث) يوناث قفدت قالغلأ مكحتل (SIP صحف كرحم موق يي نأ بج يي ، "ني مضتأل" ع لاسر مالتسإ دنع ، لاثمأل لي بس يي ل (يونا ثلأ قفدتل) ع لبا قمأل SIP RTP تاقفدت قالغلأ ب (قي بطتأل يي

لوكوتوربأل يي لع دوي قأل ببسب . SIP صحف لي طعت : لحلأ

- تافل مأل لقنو واض يي بأل عحوللأ معد م تي أل . طقف ع شدر دلأ ع زي م SIP صحف معد يي . موع دم ريغ 5.0 RTC ل يمع . تاق يي بطتأل ع كراشم و
- أل عي طتسي انا يي م نودب يي لخاد IP ناو نع يي لع يوتحي SIP ناو نع يي ، برض ما دختسإ دنع نأ تنأ دي ري نأ . ج راخ ت برست تنك عي طتسي يي لخاد ناو نعأل يي لاتلأبو ت م جرت نو كي . برض نم أل دب nat ت لكش ، برست اذه ب ن جتي ،
- عي ضا رت فألأ صحفأل ع طي رخ ما دختسا ب يي ضا رت فألأ لكش ب SIP صحف ني كم ت م تي : نم ضتت يي تلأو
 - * نكم م : SIP لوكوتورب رب ع (IM) عي روفأل ع لسا رملأ تادادت ما .
 - * اتطقسأ : SIP ذفنم يي لع SIP ريغ رورم ع كرح .
 - * ل طعم : عي اهانلأ ع طقنو مداخلل IP نيوانع ع افخإ .
 - * ل طعم : SIP ريغ URI تا يولوأو عا نقلأ جم ان رب را دصإ .
 - * نكم م : 0 نم ربكأ هجولأ يي لا تاو طخلأ ددع نأ نم دكأت .
 - * ضرورفم ريغ : RTP قفاوت .
 - * سألألأ ع حص نم ققحتلأو ع لالألأ نم ققحتلأ عا رجا مدع : SIP قفاوت .

اهحال صإو عا طخالأ فاشكتسا

LINA لوكوتورب صحفب ع قلعت مأل رورمأل ع كرح عا طخالأ فاشكتسأل ع حرت قمأل رمأوالأ ضعب هزه ا هحال صإو MPF .

- ەنكمم ل LINA MPF صحف تاي لم عمل ەمدخلال ەن تاي ئا صرح| ضرع ەمدخلال ەن راھظ|

```
firepower# show service-policy
```

Global policy:

Service-policy: global_policy

Class-map: inspection_default

Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: skinny, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: sip, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: icmp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: icmp error, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Class-map: class_snmp

Inspect: snmp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0

Class-map: class-default

Default Queueing Set connection policy: drop 0

Set connection advanced-options: UM_STATIC_TCP_MAP

Retransmission drops: 0

TCP checksum drops : 0

Exceeded MSS drops : 0

SYN with data drops: 0

Invalid ACK drops : 0

SYN-ACK with data drops: 0

Out-of-order (OoO) packets : 0

OoO no buffer drops: 0

OoO buffer timeout drops : 0

SEQ past window drops: 0

Reserved bit cleared: 0

Reserved bit drops : 0

IP TTL modified : 0

Urgent flag cleared: 0

Window varied resets: 0

TCP-options:

Selective ACK cleared: 0

Timestamp cleared : 0

Window scale cleared : 0

Other options cleared: 0

Other options drops: 0

http: تاي ئا صرح| show service-policy inspection http رمأل ن م ج تانل ا ج ذوم نل ا ذه حضوي

```
firepower# show service-policy inspect http
```

Global policy:

Service-policy: global_policy

Class-map: inspection_default

Inspect: http http, packet 1916, drop 0, reset-drop 0

protocol violations

```

packet 0
class http_any (match-any)
  Match: request method get, 638 packets
  Match: request method put, 10 packets
  Match: request method post, 0 packets
  Match: request method connect, 0 packets
log, packet 648

```

- صحفلل ةهجاو لا ىل ع ASP-Drop طاقا لا نىي عت

Syntax
#Capture

```
type asp-drop
```

```
match
```

for example
 #Capture asp type asp-drop all match ip any any
 #Capture asp type asp-drop all match ip any host x.x.x.x
 #Capture asp type asp-drop all match ip host x.x.x.x host x.x.x.x

ةدحما ل LINA MPF اقاىب ط صا ف اىل م ع نى ك م ة فى ك اهل ط ع ت و ا

عاف دلا " فى MPF LINA قىب ط صا ف اىل م ع لى ط ع ت و ا نى ك م ت ل ةا م ل ا اراى خ لا ي ه هذ ه
 ن م ن م ا ل ا ة ا م ل ا ر ا د ج دى د ه ت د ص
 Cisco".

- اذ ه و FMC م د خ ت س م ة ه جا و لى لى ل و و س م ل ل و ص و لى لى ا ج ا ت ح ت FlexConfig ر ب ع نى و ك ت ل ا
 نى و ك ت ل ا فى م ئ ا د رى غ ت ل ا .
- سى ل رى غ ت ل ا اذ ه و FTD CLI لى لى ل و و س م ل ل و ص و لى لى ا ج ا ت ح ت FTD لى لى ر ب ع نى و ك ت ل ا

نيوكتال ازالا متت ،ةديج رشن ةيلمع وأ ديهمت ةداع ةيلمع تثدح اذا ،امئاد

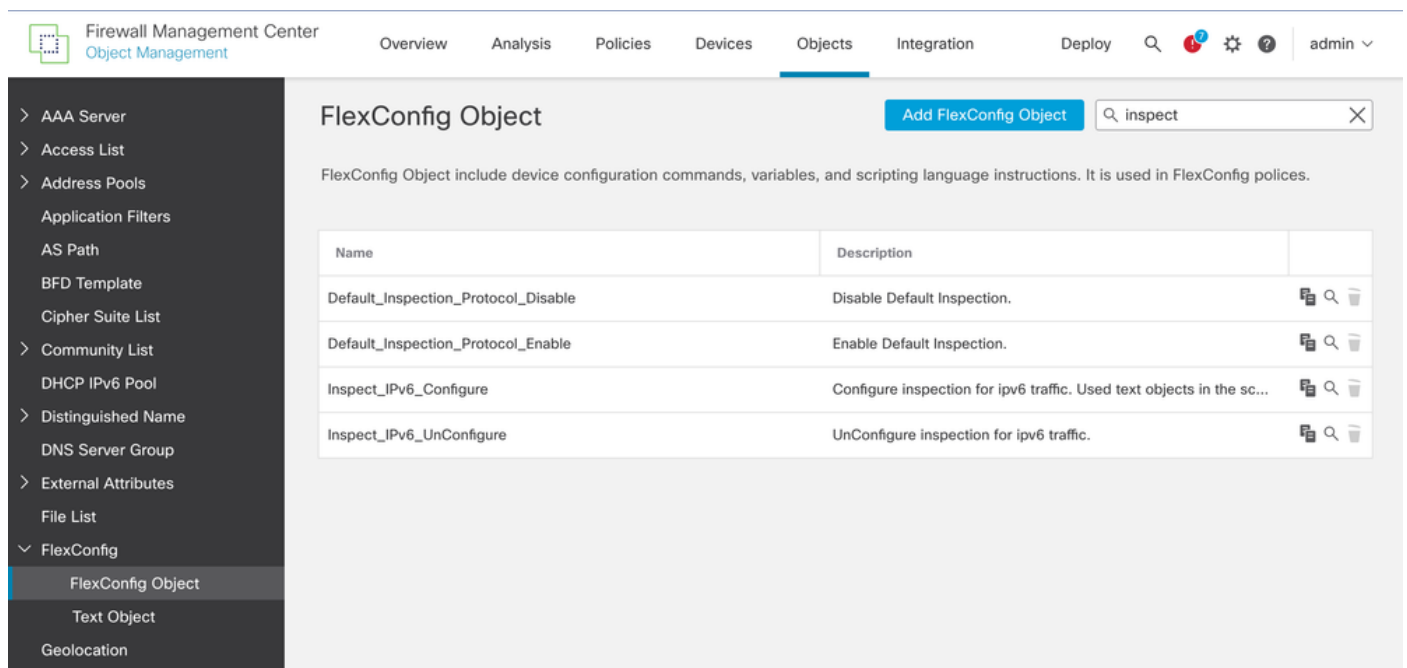
FlexConfig ربع نيوكتال

عم ةقفاوتم الـ ASA الى ةدنتسم الـ تازيمل نيوكتال ريخألا ذالم لل ةقيرط يه FlexConfig ةرادإلا زكرم يه ف نيوكتال لل ةلباق ريغ اهنكلو ديهتال نع عافدلا

مدختسم ةهجاو ربع FlexConfig لىل عمئاد لكشب هنيكمت وأ صحتل لىل نيوكتال نوكتي طقف ةنيعم رورم ةكرحل وأ ماع لكشب هقيبطت نكميو، FMC

1. ةوطخل

FlexConfig > FlexConfig Object > Object Management > Objects الى لقتنا ،FMC مدختسم ةهجاو لىل ةيضايرتفالال لوكوتورب الـ صحت تانئاك ةمئاق لىل روثعلا كنكمي كانهو، Object



Name	Description	
Default_Inspection_Protocol_Disable	Disable Default Inspection.	  
Default_Inspection_Protocol_Enable	Enable Default Inspection.	  
Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in the sc...	  
Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.	  

ةيضايرتفالال FlexConfig لوكوتورب صحت تانئاك

2. ةوطخل

FlexConfig نئاك ءاشن كنكمي ،ددحم لوكوتورب صحت لىل طعتل

FlexConfig نئاك ةفاضإ > FlexConfig Object > FlexConfig > نئاك الـ ةرادإ > تانئاك الـ الى لقتنا global_policy نم SIP صحت لىل طعتل ةغايصلال نوكت نأ بجي ،لاثمل اذه يه

```
policy-map global_policy
class inspection_default
no inspect sip
```

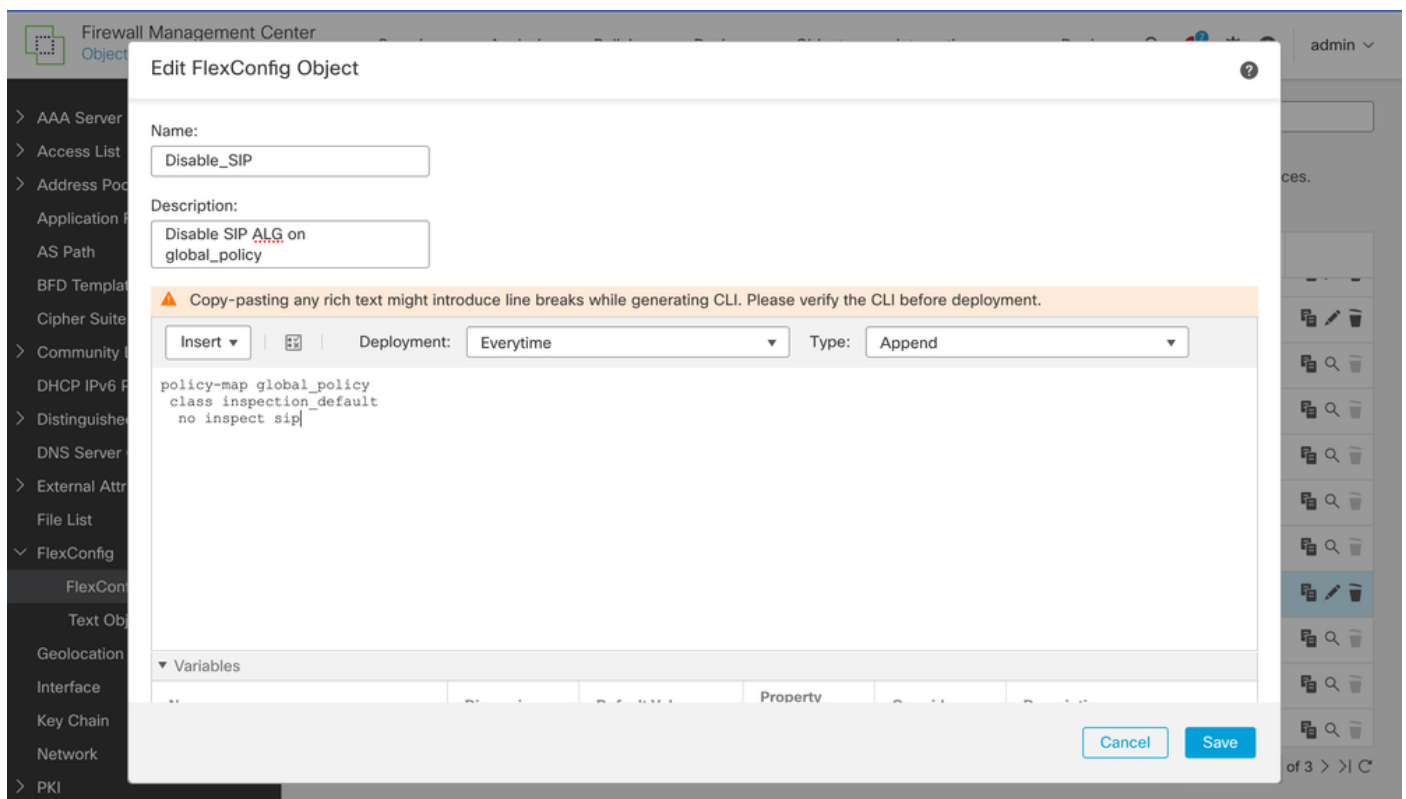
هتباتك ورشننلا ددرت رايخا كنكمي FlexConfig، نئاك نيوكت دنع

رشننلا

- تانئاك لثم ماظننلا ةطساوب اهترادا متت تانئاك ىل ريشي FlexConfig نئاكلا ناك اذا تاثيري دحت رشن رذعت، ال او تقو لك رتخاف، (ACL) لوصولي ف مكحتنلا ةمئاق و ا ةكبشلا تانئاكلا.
- دع ب. نيوكت حسم وه نئاكلا ي ف هب موقت يذلا ديجولاي عيشلا ناك اذا Once مدختسا يلات رشننلا دع ب FlexConfig جهن نم نئاكلا ةلازاب مق، كلذ

عونلا

- يتل تاننيوكتلا ةياهن ي ف نئاكلا ي ف ةدوجوملا رماوالا عضو متي (يضايرتفالا) قاحل ا تاريغت م مدختست تنك اذا قاحل ا م مدختست نأ بجي. ةرادال زكرم جهن نم اهواشن م تناك اذا. اهترادا متت تانئاك نم اهديلوت مت تانئاك ىل ريشي تالو، ةسايسلا نئاك رايخلا اذه دحت نأ بجي، نئاكلا ي ف ةددحملا لك لت عم لخادتت رخا جهنل ةدلوملا رماوالا. انام رثكال رايخلا وه اذه. كب ةصاخلا رماوالا لادبتسا متي ال ثيحب
- مت يتل تاننيوكتلا ةيادب ي ف نئاكلا ي ف ةدوجوملا رماوالا عضو متي. قبسمل دادعلا اعالا و ا حسمب موقت يتل رماوالا دادعلا ةداع م مدختست تنأ. ةرادال زكرم جهن نم اهواشن ا ام نيوكت



global_policy يضايرتفالا دادعلا نم دحاو لوكوتورب لي طعتل نئاك عاشنا

3. ةوطخلا

LINA ىل ني عمل FlexConfig جهن ي ف تانئاكلا ةفاضلا

لكاشم عم ةياملال رادج ىلع ةقبطم ال FlexConfig ةسايس ددح FlexConfig > ةزهجال ىل لقتنا طاقسال

default_inspection_protocol_disable نئال ددح،ماع لكشب صحتل تايلمع ةفاك لي طعتل يف قرزال مهسلال قوف رقنا م،ماظنل ةطساوب ةفرعالم FlexConfig تائاك نمض FlexConfig جهن ىل ةفاضل فصتلم

Firewall Management Center
Flexconfig Policy Editor

OverviewAnalysisPoliciesDevicesObjectsIntegrationDeploy

admin

Protocol_Inspection

Enter Description

Migrate ConfigPreview ConfigSaveCancel

Policy Assignments (1)

Available FlexConfig

FlexConfig Object

User Defined

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

Selected Prepend FlexConfigs

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

Selected Append FlexConfigs

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

لوكونوربل صحتل ماظنل لبق نم فرعالم نئال ددح

4. ةوطخل

نيوكتال ظفح سئالو،ةححصال تاعبرمل يف هروهظ نم دكأت،رايخال اذه ديدحت درجمب هلوعم يرسيل هرشنو

Firewall Management Center

Flexconfig Policy Editor

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

Protocol_Inspection

Enter Description

Migrate Config

Preview Config

Save

Cancel

Policy Assignments (1)

Available FlexConfig

FlexConfig Object

User Defined

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

Selected Prepend FlexConfigs

#	Name	Description
1	Default_Inspection_Protocol_Disable	Disable Default Inspection.

Selected Append FlexConfigs

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

لم اكمل اب لوكونتورب الصفحة ليطعتل ددحمل نئالك

5. ةوطخل

نم ةفرعمل ةمئاقلل نم اقبس م ءاشن مت يذل نئالك دح ، دحاو لوكونتورب صفحه ليطعتل .
تاعبرمل نبب دوجومل مهسلل مادختساب جهنللىل هتفاضل مقو مدختسمل لبق

Firewall Management Center

Flexconfig Policy Editor

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

Protocol_Inspection

Enter Description

You have unsaved changes

Migrate Config

Preview Config

Save

Cancel

Policy Assignments (1)

Available FlexConfig

FlexConfig Object

User Defined

System Defined

ACL-ControlPlane

ACL_OUTSIDE_CONTROL_PLANE

Adjust-TCP-MSS

AnyConnect_FlexObject

Disable_SIP

enable-threat-detection-ravpn

Username_Logging_Enable

Default_DNS_Configure

Default_Inspection_Protocol_Disable

Default_Inspection_Protocol_Enable

DHCPv6_Prefix_Delegation_Configure

Selected Prepend FlexConfigs

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

Selected Append FlexConfigs

#	Name	Description
1	Disable_SIP	Disable SIP ALG on global_policy

global_policy نم دحاو لوكونتورب صفحه ليطعتل اذه دح

6. ةوطخل

نيوكتل ظفح س ن ت الو، ةحيصل تاع برمل ي ف هروهظ نم دكأت، رايل ا اذه دي دحت درجم ب هلو ع ف م يرسل هرشن و.

FTD ل (CLI) رماوأل رطس ةهجاو مادختساب نيوكتل

ناك اذا ام رابتخال FTD ب ةصاخال (CLI) رماوأل رطس ةهجاو نم اروف ل حل ا اذه قي ب طت نكمي ةيلمع ثودح ةلاح ي ف نيوكتل ريغت ظفح متي ال، كلذ عمو. رورمل ةكرح يل ع رثوي صاخال ةديج رشن ةيلمع وا دي همت ةداع.

Clish. عضو ي ف FTD ب ةصاخال (CLI) رماوأل رطس ةهجاو نم رمال ا ذيفنت بجي

```
> configure inspection
```

```
disable
```

```
for example
```

```
> configure inspection SIP disable
```

ةحصل نم ققحتل

show running-config policy-map. رمال ا ذيفنت ب مق، لوكوتوربل ليطعت ةيلاعف نم ققحتل ل تالوكوتوربل ةمئاق ي ف رهظي دعي مل ه نأل SIP صاخال ليطعت متي، لاثم ا اذه ي ف ةيضارفال.

```
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
```

```
eof 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 netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class_snmp
  inspect snmp
class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
firepower#
```

ةلص تاذا تامولعم

Cisco Systems - تادنتس مل او ينقتلا معدلا

- [شيتفت لوكوتورب ةقبط قيبطتلا عم أدبي لصحي](#)
- [ةيساسلا تنرتنالا تالوكوتورب صحف](#)
- [show asp drop رمألا مادختسا](#)

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 ا 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