تكوين واجهات FTD في وضع زوج الخط

المحتويات

المقدمة

يصف هذا المستند تكوين واجهة زوج مضمنة على جهاز الدفاع عن تهديد FirePOWER (FTD) والتحقق منها وتشغيلها.

المتطلبات الأساسية

المتطلبات

هناك ما من متطلب خاص ل هذا وثيقة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Firepower 4150 FTD (الرمز 6.1.0.x و 6.3.x)
- مركز إدارة Firepower (FMC) (الرمز 6.1.0.x و 6.3.x)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

هذا وثيقة يستطيع أيضا كنت استعملت مع هذا جهاز وبرمجية صيغة:

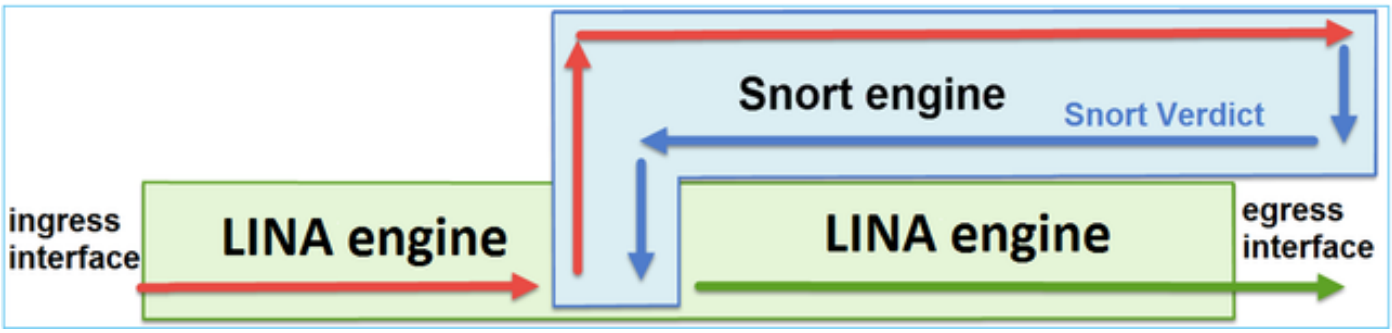
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100 و FPR4100 و FPR9300
- VMware (ESXi)، خدمات أمازون ويب (AWS)، الجهاز الافتراضي المستند إلى Kernel (KVM)
- رمز برنامج FTD الإصدار 6.2.x والإصدارات الأحدث

معلومات أساسية

FTD عبارة عن صورة برنامج موحّد تتكون من محركين رئيسيين:

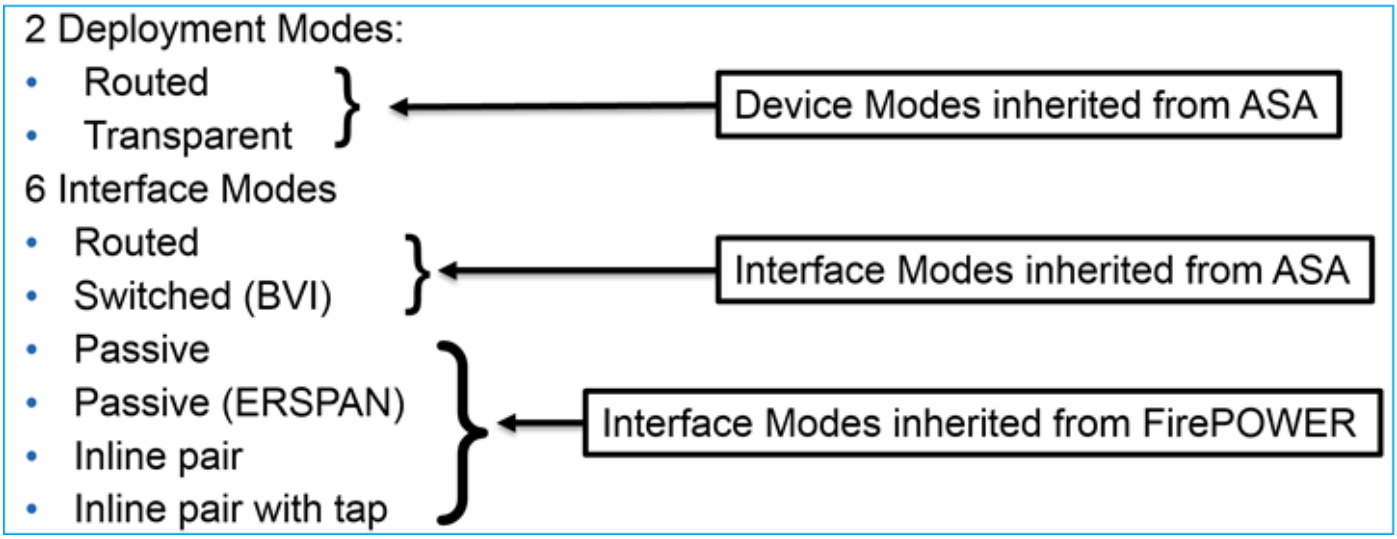
- محرك LINA
- محرك Snort

يوضح هذا الشكل كيفية تفاعل المحركين:



- تدخل الحزمة إلى واجهة الدخول ويتم التعامل معها بواسطة محرك LINA
- وإذا كانت سياسة FTD مطلوبة، فيتم فحص الحزمة بواسطة محرك Snort
- يرجع محرك الشخير حكما للحزمة
- يقوم محرك LINA بإسقاط الحزمة أو إعادة توجيهها بناءً على قرار Snort

يوفر برنامج الإرسال فائق السرعة (FTD) وضعي نشر وستة أوضاع واجهة كما هو موضح في الصورة:



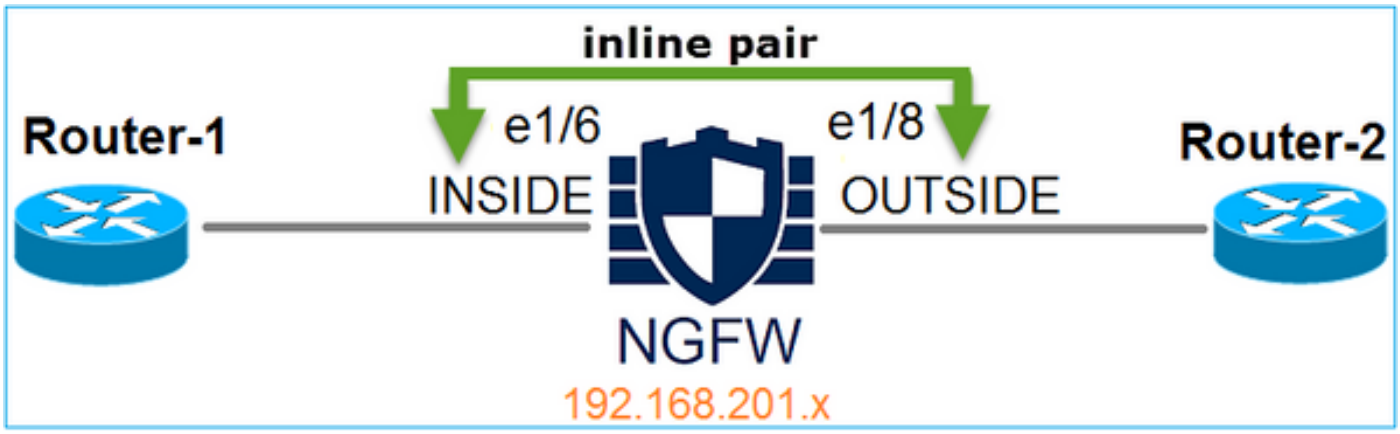
ملاحظة: يمكنك مزج أوضاع الواجهة على جهاز FTD واحد.

وفيما يلي نظرة عامة عالية المستوى على مختلف أوضاع نشر برنامج الإرسال فائق السرعة (FTD) والواجهة:

وضع واجهة FTD	وضع نشر FTD	الوصف	يمكن إسقاط حركة المرور
موجه	موجه	فحوصات كاملة لمحرك LINA و Snort-engine	نعم
محول	شفاف	فحوصات كاملة لمحرك LINA و Snort-engine	نعم
زوج مضمن	موجه أو شفاف	فحص محرك LINA الجزئي ومحرك الشخر بالكامل	نعم
زوج مضمن مع TAP	موجه أو شفاف	فحص محرك LINA الجزئي ومحرك الشخر بالكامل	ال
خامل	موجه أو شفاف	فحص محرك LINA الجزئي ومحرك الشخر بالكامل	ال
خامل (ERSPAN)	موجه	فحص محرك LINA الجزئي ومحرك الشخر بالكامل	ال

تكوين واجهة الزوج المضمنة على FTD

الرسم التخطيطي للشبكة



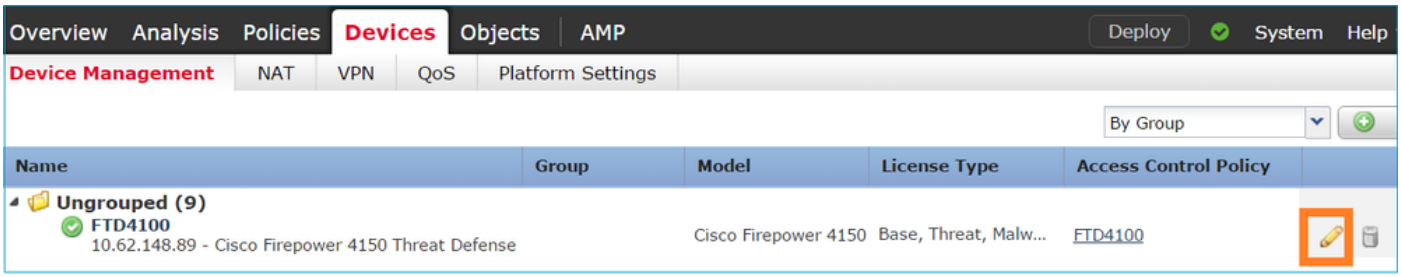
المتطلبات

قم بتكوين الواجهات المادية E1/6 و E1/8 في وضع الزوج الداخلي وفقا لهذه المتطلبات:

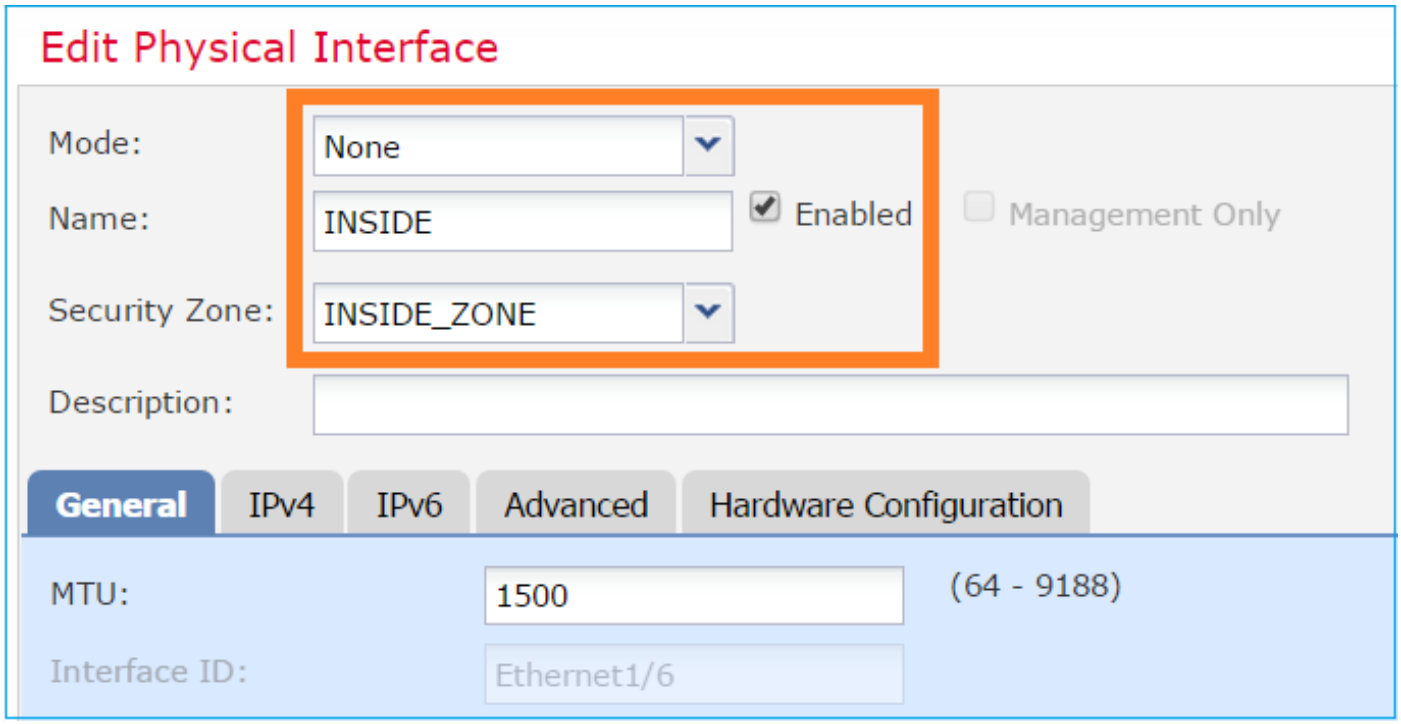
الواجهة	E1/6	E1/8
الاسم	داخل	خارج
المنطقة الأمنية	Inside_zone	Outside_Zone
اسم المجموعة المضمنة	زوج خط-1	
مجموعة MTU مضمنة	1500	
FailSafe	ممكن	
نشر حالة الارتباط	ممكن	

الحل

الخطوة 1. انتقل إلى الأجهزة > إدارة الأجهزة من أجل التكوين على الواجهات الفردية، وحدد الجهاز المناسب وحدد تحرير كما هو موضح في الصورة.

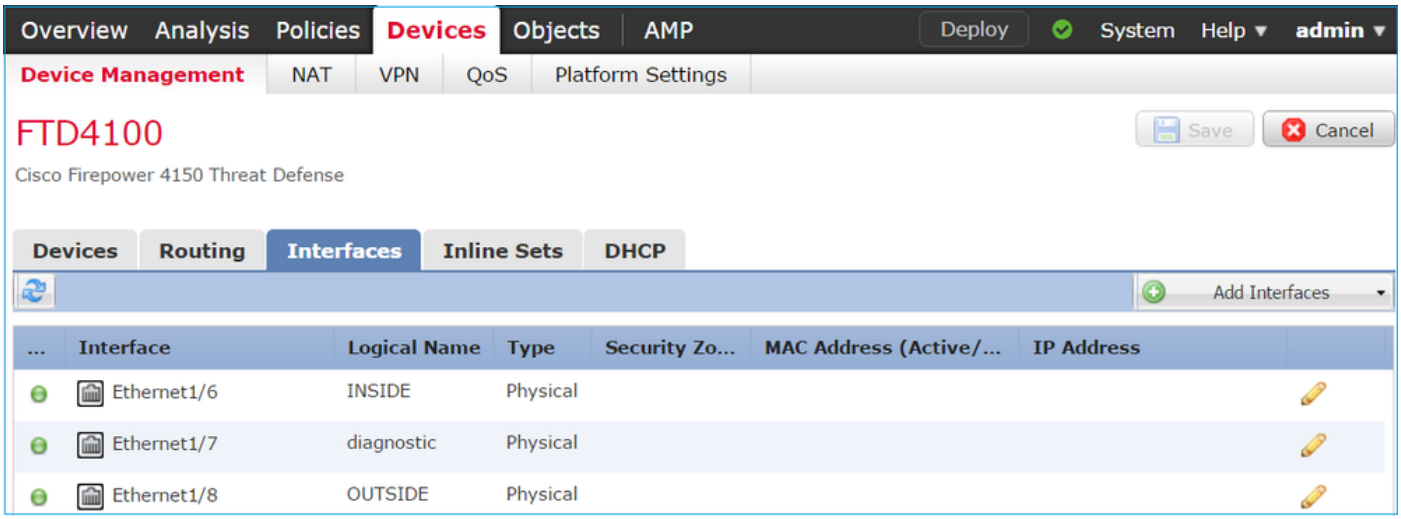


بعد ذلك، قم بتعيين الاسم والتأشير ممكن للواجهة كما هو موضح في الصورة.



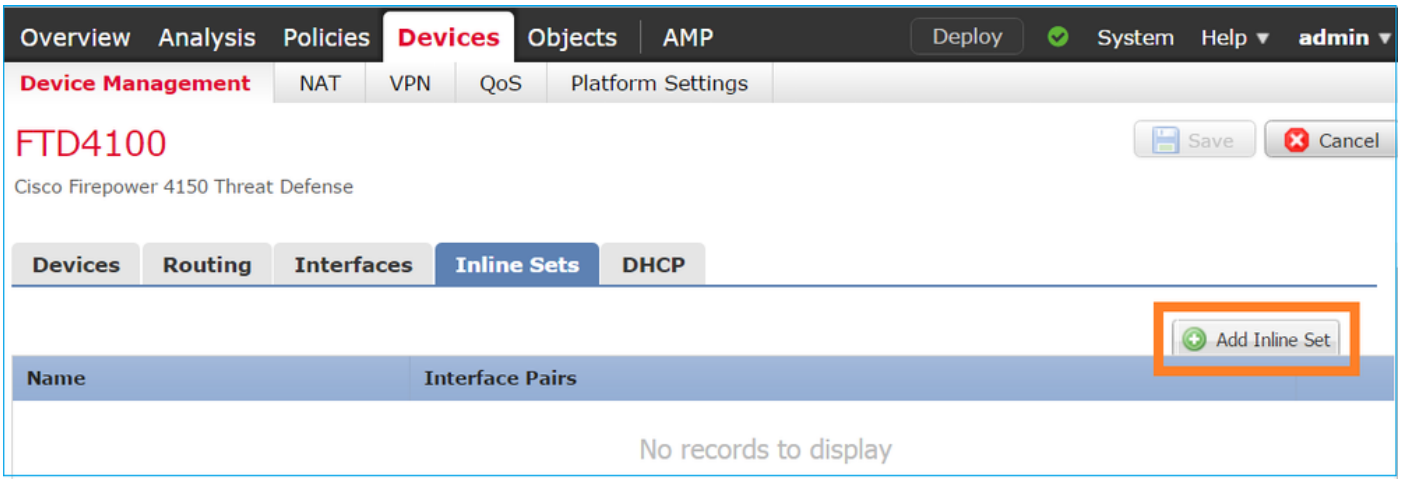
ملاحظة: الاسم هو اسم الواجهة.

بالمثل للواجهة Ethernet1/8. النتيجة النهائية كما هو موضح في الصورة.

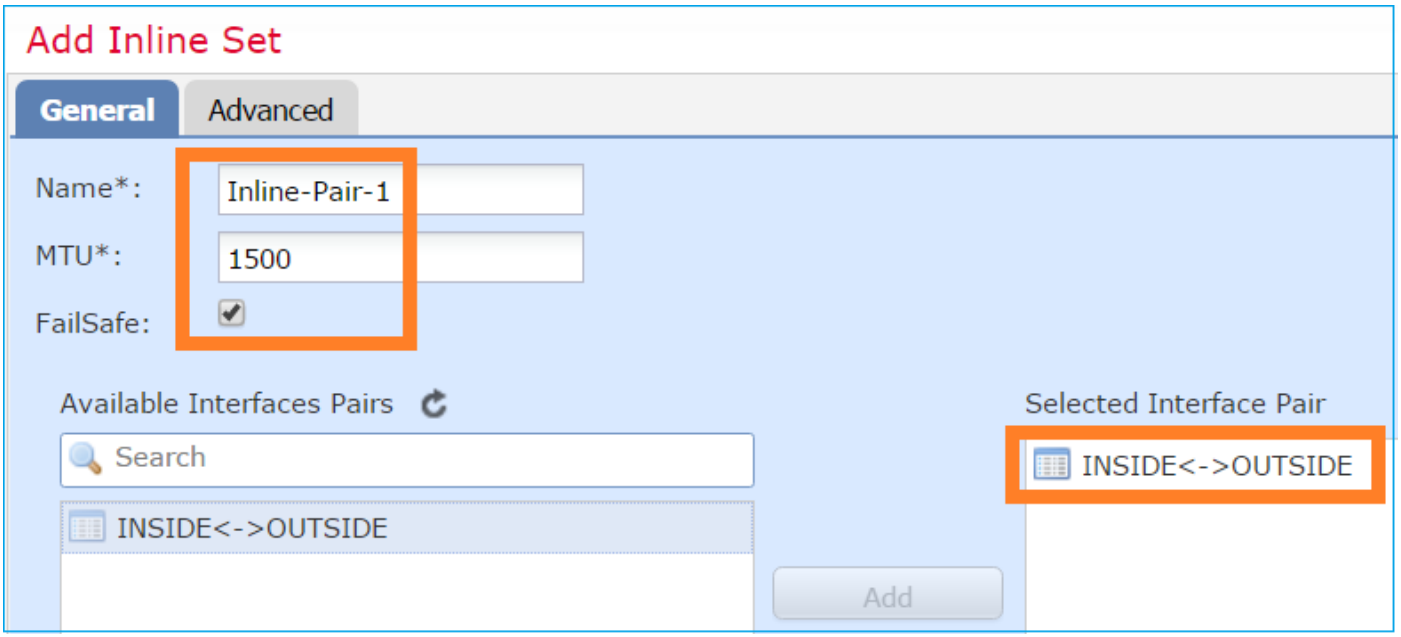


الخطوة 2. قم بتكوين الزوج المضمن.

انتقل إلى مجموعات في السطر > إضافة مجموعة في السطر كما هو موضح في الصورة.

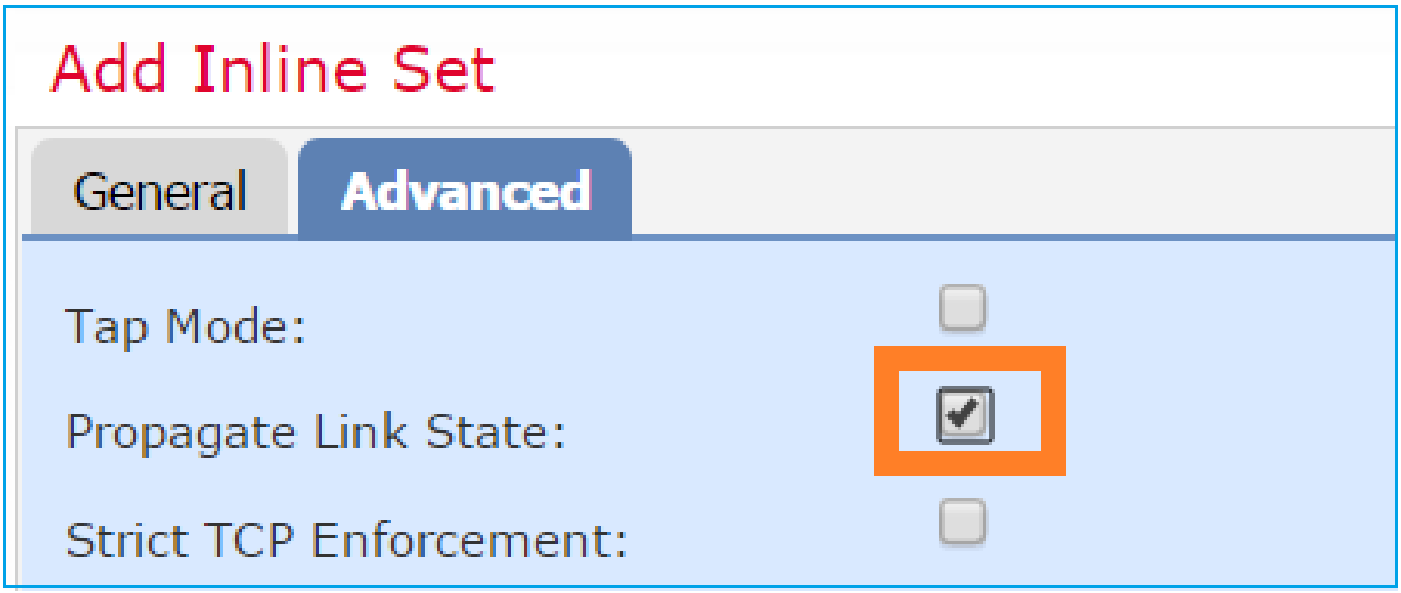


الخطوة 3. قم بتكوين الإعدادات العامة وفقا للمتطلبات كما هو موضح في الصورة.



ملاحظة: يسمح FailedSafe لحركة المرور بالمرور عبر الزوج المضمن الذي لم يتم فحصه في حالة امتلاء المخازن المؤقتة للواجهة (عادة ما ترى عندما يكون الجهاز محملا فوق طاقته أو أن محرك snort محمل فوق طاقته). تم تخصيص حجم مخزن الواجهة المؤقت بشكل ديناميكي.

الخطوة 4. قم بتمكين خيار حالة انتشار الارتباط في الإعدادات المتقدمة كما هو موضح في الصورة.



يعمل نشر حالة الارتباط تلقائيا على إسقاط الواجهة الثانية في زوج الواجهة المضمنة عند تعطل إحدى الواجهات في مجموعة الخطوط الداخلية.

الخطوة 5. حفظ التغييرات والنشر.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تحقق من تكوين الزوج المضمنة من واجهة سطر الأوامر (CLI) الخاصة ب FTD.

الحل

قم بتسجيل الدخول إلى CLI (واجهة سطر الأوامر) في FTD وتحقق من تكوين الزوج الداخلي:

```
> show inline-set

Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
  Tap mode is off
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/8 "OUTSIDE"
      Current-Status: UP
    Bridge Group ID: 509
>
```

ملاحظة: معرف مجموعة الجسر قيمة مختلفة عن 0. إذا كان وضع الضغط قيد التشغيل، فسيكون 0

معلومات الواجهة والاسم:

```
<#root>

>

show nameif

Interface                   Name                        Security
Ethernet1/6                 INSIDE                      0

Ethernet1/7                 diagnostic                  0
Ethernet1/8                 OUTSIDE                     0

>
```

دقق القارن وضع:

```
<#root>

> show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           169.254.1.1     YES unset  up                    up

Ethernet1/6                unassigned      YES unset  up                    up
Ethernet1/7                unassigned      YES unset  up                    up

Ethernet1/8                unassigned      YES unset  up                    up
```

التحقق من معلومات الواجهة المادية:

```
<#root>

>

show interface e1/6
```

```
Interface Ethernet1/6 "INSIDE", is up, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.770e, MTU 1500


IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


        IP address unassigned
  Traffic Statistics for "INSIDE":
        468 packets input, 47627 bytes
        12 packets output, 4750 bytes
        1 packets dropped
      1 minute input rate 0 pkts/sec,  200 bytes/sec
      1 minute output rate 0 pkts/sec,  7 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  96 bytes/sec
      5 minute output rate 0 pkts/sec,  8 bytes/sec
      5 minute drop rate, 0 pkts/sec
>

show interface e1/8


Interface Ethernet1/8 "OUTSIDE", is up, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.774d, MTU 1500


IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        12 packets input, 4486 bytes
        470 packets output, 54089 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  7 bytes/sec
      1 minute output rate 0 pkts/sec,  212 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  7 bytes/sec
      5 minute output rate 0 pkts/sec,  106 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

التحقق من عملية واجهة زوج الخطوط المضمنة لـ FTD

يغطي هذا القسم عمليات التحقق من الصحة هذه للتحقق من عملية "الزوج الداخلي":

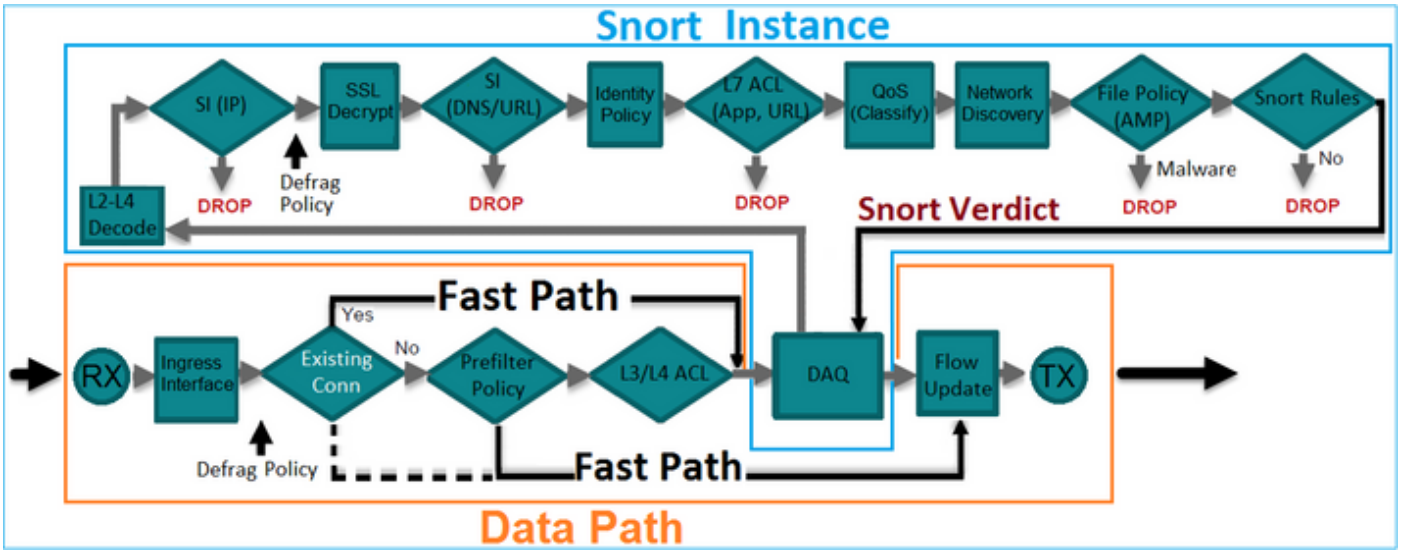
- التحقق 1. مع إستخدام ربط-tracer

- التحقق 2. تمكين الالتقاط باستخدام التتبع وإرسال حزمة TCP Sync/Acknowledge (SYN/ACK) من خلال الزوج الداخلي
- التحقق 3. مراقبة حركة مرور FTD باستخدام تصحيح أخطاء محرك جدار الحماية
- التحقق 4. التحقق من وظيفة نشر حالة الارتباط
- التحقق 5. تكوين ترجمة عنوان الشبكة الثابتة (NAT)

الحل

نظرة عامة على البنية

عندما تعمل 2 واجهات FTD في وضع زوج خط داخلي، تتم معالجة الحزمة كما هو موضح في الصورة.

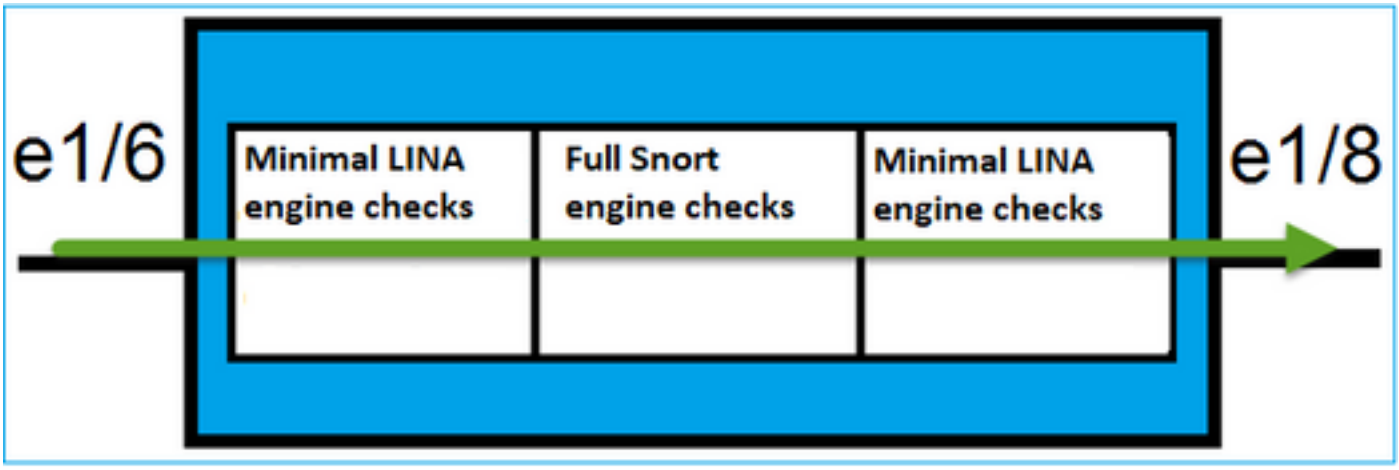


ملاحظة: يمكن أن تكون الواجهات المادية فقط أعضاء في مجموعة زوج مضمن

النظرية الأساسية

- عند تكوين زوج مضمن 2 يتم ربط الواجهات المادية داخليا
- تشبه إلى حد كبير النظام الكلاسيكي لمنع التطفل (IPS)
- متوفر في أوضاع النشر الموجهة أو الشفافة
- ال تتوفر معظم ميزات محرك LINA (NAT، التوجيه وما إلى ذلك) للتدفقات التي تمر عبر زوج في السطر
- يمكن إسقاط حركة مرور النقل
- يتم تطبيق بعض فحوصات محرك LINA مع فحوصات محرك الشخير بالكامل

يمكن عرض النقطة الأخيرة كما هو موضح في الصورة:



التحقق 1. مع إستخدام Packet-tracer

مخرجات الحزمة-tracer التي تحاكي الحزمة التي تجتاز الزوج في السطر مع النقاط المهمة المبرزة:

<#root>

>

packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80

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

Phase: 2

Type: NGIPS-MODE

Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services is be applied

Phase: 3

Type: ACCESS-LIST

Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet is sent to snort for additional processing where a verdict is reached

Phase: 4

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface
Result: ALLOW
Config:

Additional Information:

Ingress interface INSIDE is in NGIPS inline mode.

Egress interface OUTSIDE is determined by inline-set configuration

Phase: 5

Type: FLOW-CREATION

Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 106, packet dispatched to next module

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: allow

>

التحقق 2. إرسال حزم TCP syn/ACK من خلال جوز الخطية

يمكنك إنشاء حزم TCP SYN/ACK باستخدام الحزمة التي تنتحل الأداة المساعدة مثل Scapy.
تقوم هذه الصيغة بإنشاء 3 حزم باستخدام عالمات SYN/ACK الممكنة:

```
<#root>

root@KALI:~#

scapy

INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>

conf.iface='eth0'

>>>

packet = IP(dst="192.168.201.60")/TCP(flags="SA",dport=80)

>>>

syn_ack=[]

>>>

for i in range(0,3): # Send 3 packets

...

syn_ack.extend(packet)

...
>>>

send(syn_ack)
```

قم بتمكين هذا التقاط على واجهة سطر الأوامر (CLI) من FTD أو إرسال بعض حزم TCP SYN/ACK:

```
<#root>

>

capture CAPI interface INSIDE trace match ip host 192.168.201.60 any


>

capture CAPO interface OUTSIDE match ip host 192.168.201.60 any


>
```

بعد إرسال الحزم من خلال FTD، يمكنك رؤية اتصال تم إنشاؤه:

```
<#root>

>

show conn detail


1 in use, 34 most used
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,


 b - TCP state-bypass or nailed,


       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media,

N - inspected by Snort

, n - GUP
       O - responder data, P - inside back connection,
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow


TCP Inline-Pair-1:OUTSIDE(OUTSIDE): 192.168.201.60/80 Inline-Pair-1:INSIDE(INSIDE): 192.168.201.50/20,




flags b N

, idle 13s, uptime 13s, timeout 1h0m, bytes 0

>
```

ملاحظة: علامة b - يقوم ASA التقليدي بإسقاط حزمة SYN/ACK غير مطلوبة ما لم يتم تمكين تجاوز حالة TCP. يقوم FTD في وضع "زوج الخط الداخلي" بمعالجة اتصال TCP في وضع تجاوز حالة TCP ولا تسقط حزم TCP التي لا تنتمي إلى الاتصالات الموجودة بالفعل.

ملاحظة: علامة N - يتم فحص الحزمة بواسطة محرك تشفير FTD.

تثبت عمليات الالتقاط ذلك، نظرا لأنه يمكنك رؤية الحزم الثلاثة التي تجتاز FTD:

<#root>

>

show capture CAPI

3 packets captured

   1: 15:27:54.327146   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   2: 15:27:54.330000   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   3: 15:27:54.332517   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
3 packets shown
>

تخرج 3 حزم من جهاز FTD:

<#root>

>

show capture CAPO

3 packets captured

   1: 15:27:54.327299   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

```
ack

 0 win 8192
   2: 15:27:54.330030       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   3: 15:27:54.332548       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
3 packets shown
>
```

مع التتبع الخاص بالحزمة الالتقاط الأولى يكشف بعض المعلومات الإضافية مثل الحكم على محرك الشيري:

```
<#root>

>

show capture CAPI packet-number 1 trace


3 packets captured

   1: 15:27:54.327146       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE

Additional Information:
This packet is sent to snort for additional processing where a verdict is reached

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface

Result: ALLOW
Config:
Additional Information:

Ingress interface INSIDE is in NGIPS inline mode.
Egress interface OUTSIDE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 282, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT

Subtype:
Result: ALLOW
Config:
Additional Information:

Application: 'SNORT Inspect'

Phase: 8
Type: SNORT

Subtype:

Result: ALLOW

Config:

```
Additional Information:
Snort Verdict: (pass-packet) allow this packet


Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
Action: allow


1 packet shown
>
```

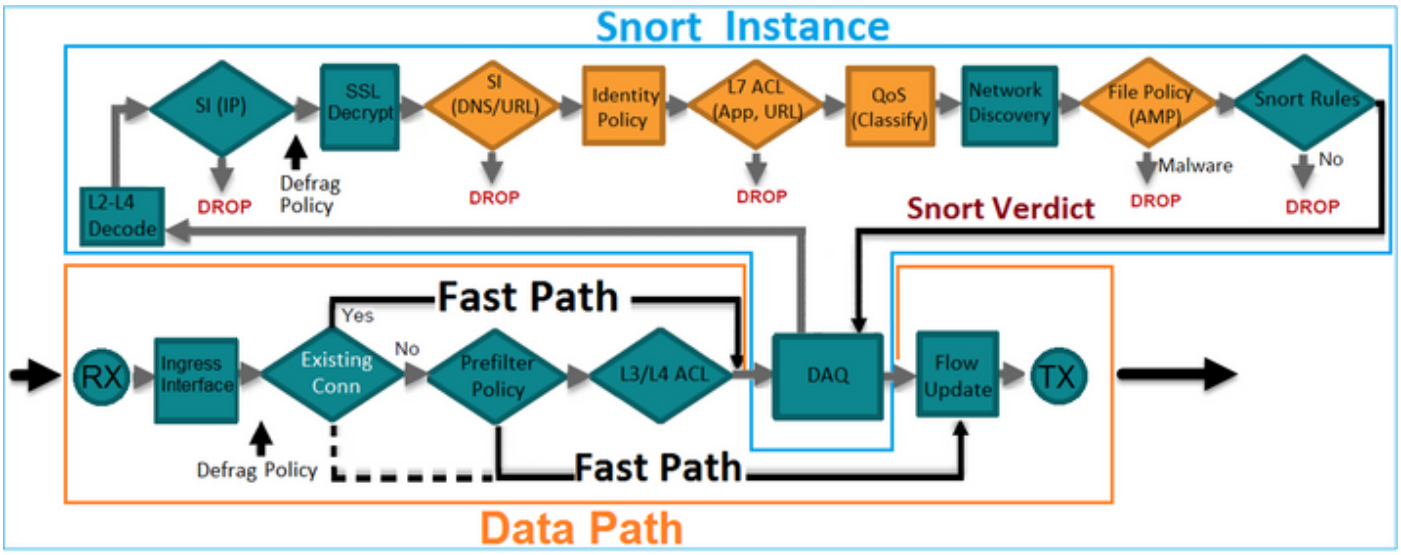
باستخدام تتبع الحزمة الثانية التي تم القبض عليها يظهر أن الحزمة تطابق الاتصال الحالي لذلك فإنها تتجاوز التحقق من قائمة التحكم في الوصول، ولكن ام يزال يتم فحصه بواسطة محرك snort:

```
<#root>

>

show capture CAPI packet-number 2 trace


3 packets captured

   2: 15:27:54.330000       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
```

```
Config:
Implicit Rule
Additional Information:
MAC Access list


Phase: 3
Type: FLOW-LOOKUP
Subtype:ing
Result: ALLOW
Config:
Additional Information:
Found flow with id 282, using current flow



Phase: 4
Type: EXTERNAL-INSPECT

Subtype:
Result: ALLOW
Config:

Additional Information:
Application: 'SNORT Inspect'



Phase: 5
Type: SNORT

Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet


Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
Action: allow


1 packet shown
>
```

التحقق 3. تصحيح أخطاء محرك دارا الحماية لحركة المرور المسموح بها

يتم تشغيل تصحيح أخطاء محرك دارا الحماية قبل مكونات معينة لمحرك تشفير FTD مثل نهج التحكم في الوصول كما هو موضح في الصورة:



عند إرسال حزم TCP syn/ACK من خلال الزوج الداخلي، يمكنك أن ترى في إخراج تصحيح الأخطاء:

<#root>

>

system support firewall-engine-debug

Please specify an IP protocol:

tcp

Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:

192.168.201.60

Please specify a server port:

80

Monitoring firewall engine debug messages

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 New session

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 using HW or preset rule order 3, id 268438528 action A

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 allow action

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 Deleting session

التحقق 4. التحقق من نشر حالة الارتباط

قم بتمكين سجل المخزن المؤقت على FTD وإيقاف تشغيل switchport المتصل بواجهة E1/6.
على CLI ل FTD يجب أن ترى أن الاقتباس التالي:

```
<#root>

>

show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           169.254.1.1     YES unset  up                    up

Ethernet1/6                unassigned      YES unset  down                  down

Ethernet1/7                unassigned      YES unset  up                    up

Ethernet1/8                unassigned      YES unset  administratively down up

>
```

عرض سجلات FTD:

```
<#root>

>

show log

Jan 03 2017 15:53:19: %ASA-4-411002:

Line protocol on Interface Ethernet1/6, changed state to down

Jan 03 2017 15:53:19: %ASA-4-411004:

Interface OUTSIDE, changed state to administratively down

Jan 03 2017 15:53:19: %ASA-4-411004:

Interface Ethernet1/8, changed state to administratively down

Jan 03 2017 15:53:19: %ASA-4-812005:

Link-State-Propagation activated on inline-pair due to failure of interface Ethernet1/6(INSIDE) bringing

>
```

تظهر حالة المجموعة الداخلية حالة أعضاء الواجهة 2:

```
<#root>

>

show inline-set



Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
  Tap mode is off

 Propagate-link-state option is on


  hardware-bypass mode is disabled

Interface-Pair[1]:


    Interface: Ethernet1/6 "INSIDE"


      Current-Status: Down(Propagate-Link-State-Activated)


    Interface: Ethernet1/8 "OUTSIDE"


      Current-Status: Down(Down-By-Propagate-Link-State)

    Bridge Group ID: 509
>
```

لاحظ الفرق في حالة الواجهات المزدوجة:

```
<#root>

>

show interface e1/6



Interface Ethernet1/6 "INSIDE", is down, line protocol is down


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.770e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
```

```
  Propagate-Link-State-Activated


        IP address unassigned
  Traffic Statistics for "INSIDE":
        3393 packets input, 234923 bytes
        120 packets output, 49174 bytes
        1 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  6 bytes/sec
      5 minute output rate 0 pkts/sec,  3 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

وبالنسبة لواجهة Ethernet1/8:

```
<#root>

>

show interface e1/8


Interface Ethernet1/8 "OUTSIDE", is administratively down, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.774d, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


Down-By-Propagate-Link-State


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        120 packets input, 46664 bytes
        3391 packets output, 298455 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  3 bytes/sec
      5 minute output rate 0 pkts/sec,  8 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

بعد أن يعين أنت ال switchport ال FTD سجل عرض:

```
<#root>

>
```

```
show log

...
Jan 03 2017 15:59:35: %ASA-4-411001:
Line protocol on Interface Ethernet1/6, changed state to up

Jan 03 2017 15:59:35: %ASA-4-411003:
Interface Ethernet1/8, changed state to administratively up

Jan 03 2017 15:59:35: %ASA-4-411003:
Interface OUTSIDE, changed state to administratively up

Jan 03 2017 15:59:35: %ASA-4-812006:
Link-State-Propagation de-activated on inline-pair due to recovery of interface Ethernet1/6(INSIDE) brir

>
```

التحقق 5. تكوين NAT الثابت

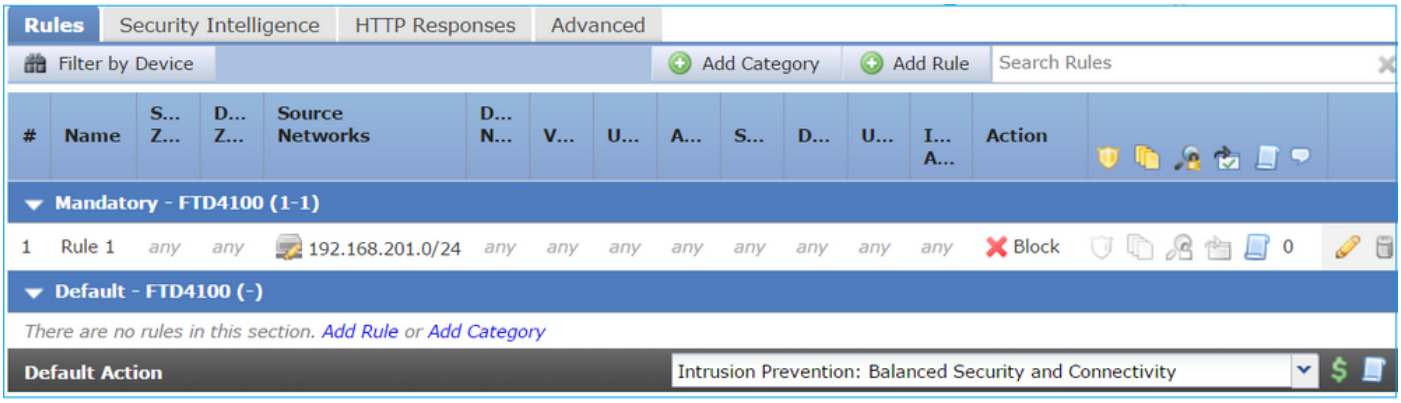
الحل

NAT غير مدعوم للواجهات التي تعمل في الأوضاع الداخلية أو المس الداخلي أو الخاملة:

https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Network_Address_Translation__NAT__for_Threat_Defense.html

حظر الحزمة على وضع واجهة زوج الخطوط الداخلية

قم بإنشاء قاعدة حظر، وأرسل حركة مرور البيانات من خلال زوج FTD الداخلي، وراقب السلوك كما هو موضح في الصورة.



الحل

قم بتمكين الالتقاط باستخدام التتبع وأرسل حزم SYN/ACK من خلال زوج FTD الداخلي. تم

حظر حركة المرور:

<#root>

>

show capture

capture CAPI type raw-data trace interface INSIDE

[Capturing - 210 bytes]

  match ip host 192.168.201.60 any
capture CAPO type raw-data interface OUTSIDE

[Capturing - 0 bytes]

  match ip host 192.168.201.60 any

مع التتبع، تظهر الحزمة:

<#root>

>

show capture CAPI packet-number 1 trace

3 packets captured

   1: 16:12:55.785085

192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW
Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: DROP

Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log fl
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1

Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up

Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule

1 packet shown

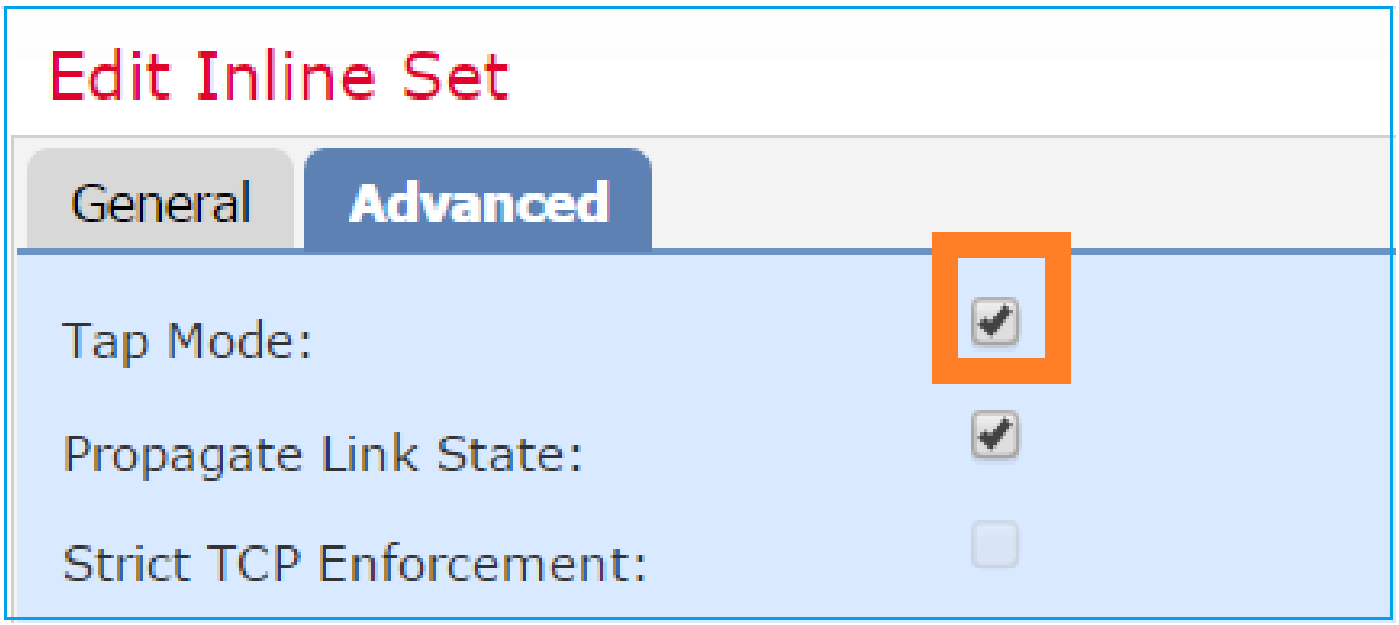
في هذا التتبع، يمكن ملاحظة أن الحزمة تم إسقاطها من قبل محرك FTD LINA ولم يتم إعادة توجيهها إلى محرك snort الخاص ب FTD.

تكوين وضع الزوج المضمن باستخدام TAP

قم بتمكين وضع الضغط على الزوج الداخلي.

الحل

انتقل إلى الأجهزة > إدارة الأجهزة > المجموعات المضمنة > تحرير المجموعة المضمنة > خيارات متقدمة وتمكين وضع الضغط كما هو موضح في الصورة.



التحقق

<#root>

>

show inline-set

```
Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
```

Tap mode is on

```
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/8 "OUTSIDE"
```

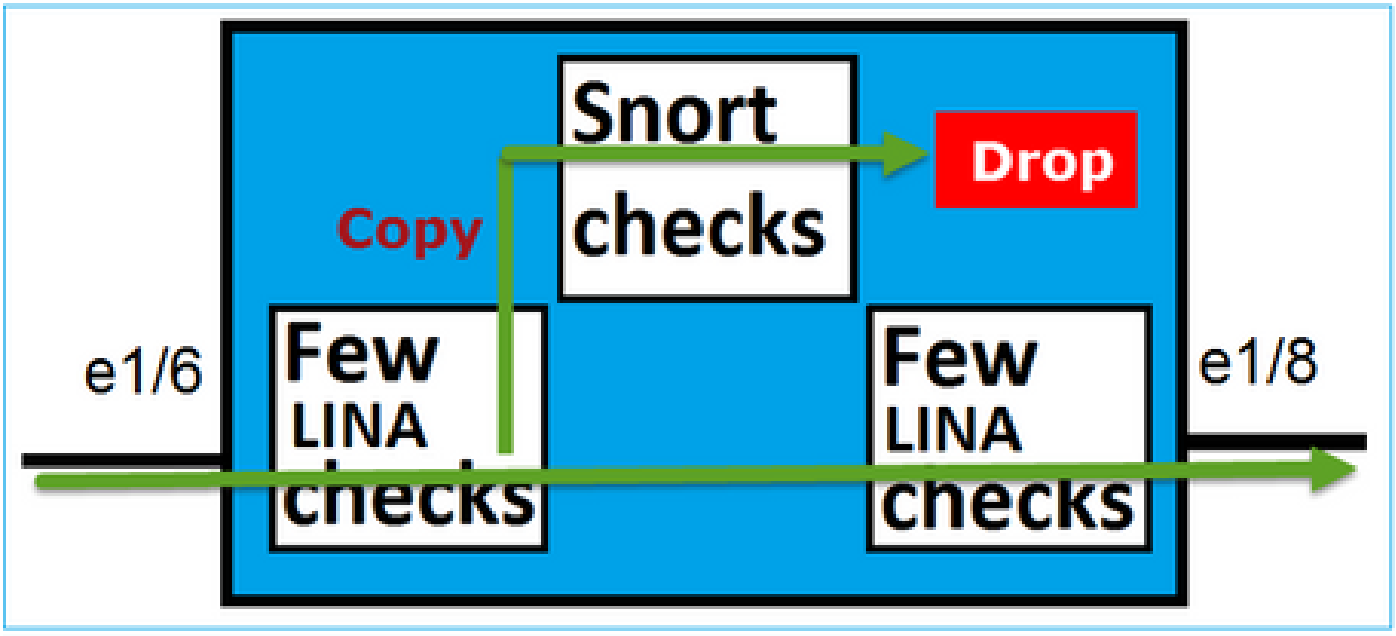
```
      Current-Status: UP
    Bridge Group ID: 0
>
```

التحقق من زوج FTD الداخلي باستخدام عملية واجهة TAP

النظرية الأساسية

- عند تكوين زوج خطي باستخدام TAP 2، يتم ربط الواجهات المادية داخليا
- ويتوفر في أوضاع النشر الموجهة أو الشفافة
- لا تتوفر معظم ميزات محرك LINA (NAT، التوجيه وما إلى ذلك) للتدفقات التي تمر عبر الزوج الداخلي
- لا يمكن إسقاط حركة المرور الفعلية
- يتم تطبيق بعض عمليات التحقق من محرك LINA مع التحقق الكامل من محرك Snort لنسخة من حركة المرور الفعلية

النقطة الأخيرة هي كما هو موضح في الصورة:



لا يقوم الزوج المضمن مع وضع الضغط بإسقاط حركة مرور النقل. باستخدام تتبع حزمة، فإنه يؤكد ما يلي:

<#root>

>

show capture CAPI packet-number 2 trace

```
3 packets captured
```

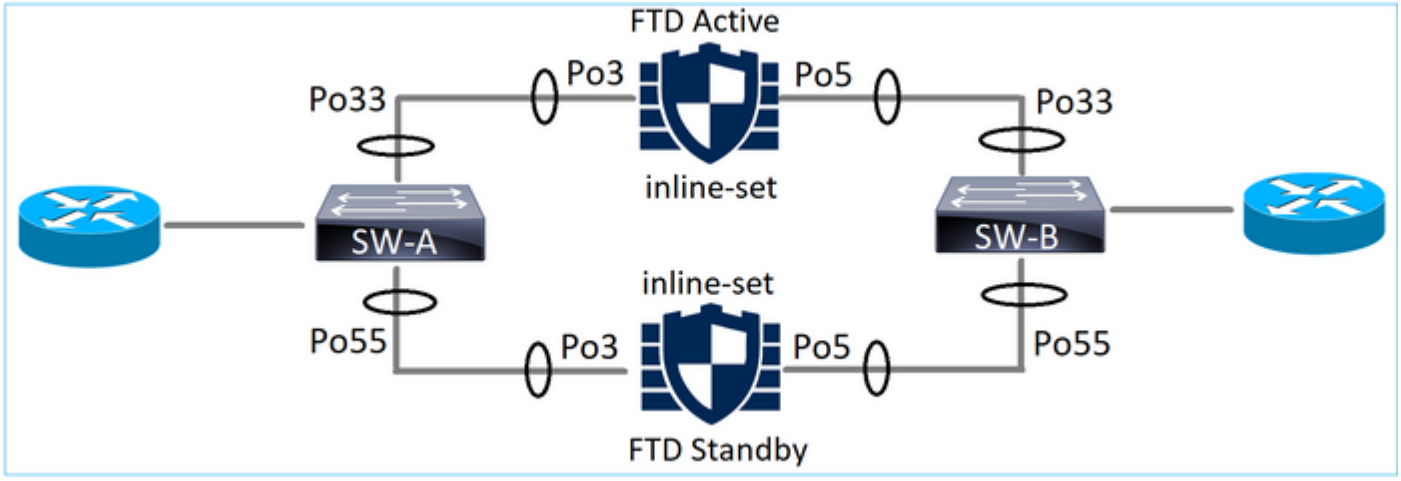
```
   2: 13:34:30.685084       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list


Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode

Result: ALLOW
Config:
Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied



Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: WOULD HAVE DROPPED

Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log fl
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up

Action: Access-list would have dropped, but packet forwarded due to inline-tap


1 packet shown
>
```

زوج خطي و EtherChannel

أنت يستطيع شكلت داخل زوج مع EtherChannel بطريقتين:

1. تم إنهاء EtherChannel على FTD
2. يمر EtherChannel من خلال FTD (يتطلب FXOS رمز 2.3.1.3 ومتأخر)

تم إنهاء EtherChannel على FTD



EtherChannels على SW-A:

<#root>

SW-A#

show etherchannel summary | i Po33|Po55

```
33      Po33(SU)         LACP      Gi3/11(P)
35      Po35(SU)         LACP      Gi2/33(P)
```

EtherChannels على SW-B:

<#root>

SW-B#

show etherchannel summary | i Po33|Po55

```
33      Po33(SU)         LACP        Gi1/0/3(P)
55      Po55(SU)         LACP        Gi1/0/4(P)
```

تتم إعادة توجيه حركة المرور من خلال FTD النشط القائم على معرفة عنوان MAC:

<#root>

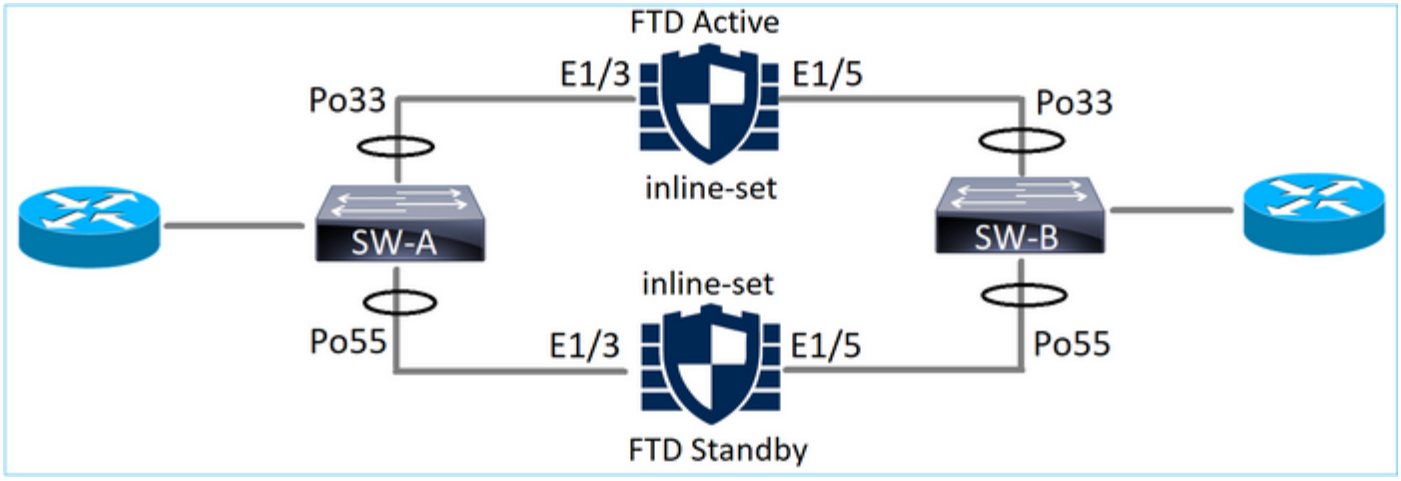
```
SW-B#
 show mac address-table address 0017.dfd6.ec00

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC
Po33

Total Mac Addresses for this criterion: 1
```

المجموعة المضمنة على FTD:

```
<#root>

FTD#

show inline-set


Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled


Interface-Pair[1]:
    Interface: Port-channel3 "INSIDE"
      Current-Status: UP
    Interface: Port-channel5 "OUTSIDE"
      Current-Status: UP

    Bridge Group ID: 775
```

ملاحظة: في حالة حدوث تجاوز فشل في برنامج الإرسال فائق السرعة (FTD)، يعتمد انقطاع حركة مرور البيانات بشكل رئيسي على الوقت الذي يستغرقه في المحولات لتعلم عنوان MAC الخاص بالنظير البعيد.

EtherChannel من خلال FTD



EtherChannels على SW-A:

<#root>

SW-A#

show etherchannel summary | i Po33|Po55

```
33     Po33(SU)         LACP      Gi3/11(P)
55     Po55(SD)         LACP      Gi3/7
```

(I)

يتم حظر حزم LACP من خلال FTD للاستعداد:

<#root>

FTD#

capture ASP type asp-drop fo-standby

FTD#

show capture ASP | i 0180.c200.0002

```
  29: 15:28:32.658123       a0f8.4991.ba03 0180.c200.0002 0x8809 Length: 124
  70: 15:28:47.248262       f0f7.556a.11e2 0180.c200.0002 0x8809 Length: 124
```

EtherChannels على SW-B:

<#root>

SW-B#

show etherchannel summary | i Po33|Po55

```
33     Po33(SU)         LACP        Gi1/0/3(P)
```

```
55     Po55(SD)        LACP        Gi1/0/4
(s)
```

تتم إعادة توجيه حركة المرور من خلال FTD النشط القائم على معرفة عنوان MAC:

<#root>

```
SW-B#
 show mac address-table address 0017.dfd6.ec00
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC
Po33
Total Mac Addresses for this criterion: 1
```

المجموعة المضمنة على FTD:

<#root>

```
FTD#
show inline-set


Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled

Interface-Pair[1]:

    Interface: Ethernet1/3 "INSIDE"

      Current-Status: UP

    Interface: Ethernet1/5 "OUTSIDE"
```

```
Current-Status: UP

Bridge Group ID: 519
```

تحذير: في هذا السيناريو في حالة حدوث تجاوز فشل في برنامج الإرسال فائق السرعة (FTD)، يعتمد وقت التقارب بشكل رئيسي على تفاوض LACP في برنامج EtherChannel وعلى الوقت الذي يتم فيه قطع الاتصال يمكن أن يكون أطول من ذلك. في حالة أن EtherChannel يكون أسلوب على (ال LACP) بعد ذلك يعتمد وقت التقارب على كام عنوان يعلم.

استكشاف الأخطاء وإصلاحها

هناك حاليا ما من معلومة خاص يتوفر ل هذا تشكيل.

المقارنة: زوج مضمن مقابل زوج مضمن باستخدام TAP

	زوج مضمن	زوج مضمن مع TAP
إظهار المجموعة الداخلية	> إظهار المجموعة الداخلية زوج خط داخلي-1 داخل المجموعة وحدة الحد الأقصى للنقل (MTU) هي 1500 بايت وضع الأمان في حالة الفشل قيد التشغيل/التنشيط تم إيقاف تشغيل وضع تأمين الفشل تم إيقاف تشغيل وضع الضغط خيار Propagate-link-state قيد التشغيل تم تعطيل وضع تجاوز الجهاز زوج الواجهة[1]: الواجهة: Ethernet1/6 "Inside" الحالة الحالية: لأعلى الواجهة: إيثرنت 1/8 "خارجي" الحالة الحالية: لأعلى معرف مجموعة الجسر: 509 >	> إظهار المجموعة الداخلية زوج خط داخلي-1 داخل المجموعة وحدة الحد الأقصى للنقل (MTU) هي 1500 بايت وضع الأمان في حالة الفشل قيد التشغيل/التنشيط تم إيقاف تشغيل وضع تأمين الفشل وضع الضغط قيد التشغيل خيار Propagate-link-state قيد التشغيل تم تعطيل وضع تجاوز الجهاز زوج الواجهة[1]: الواجهة: Ethernet1/6 "Inside" الحالة الحالية: لأعلى الواجهة: إيثرنت 1/8 "خارجي" الحالة الحالية: لأعلى معرف مجموعة الجسر: 0 >

show interface	> إظهار الواجهة e1/6 < واجهة إيثرنت 1/6 "INSIDE"، قيد التشغيل، بروتوكول الخط قيد التشغيل الأجهزة هي EtherSVI و BW سرعة 1000 ميجابت في الثانية و LY سرعة 1000 usec عنوان MAC، الإصدار 5897.bdb9.770e، MTU 1500 وضع واجهة IPS: مضمن، مضمن: مزدوج خطي-1 عنوان IP غير معين إحصائيات حركة المرور ل "Inside": إدخال الحزم 3957، 264913 بايت إخراج 144 حزمة، 58664 بايت تم إسقاط 4 حزم معدل إدخال يبلغ دقيقة واحدة 0 pkts/ثانية و 26 بايت/ثانية معدل إخراج يبلغ دقيقة واحدة 0 pkts/ثانية و 7 بايت/ثانية معدل الإنزال لمدة دقيقة واحدة، 0 كيلو بايت/ثانية 5 دقائق معدل الإدخال 0 بيكات/ثانية، 28 بايت/ثانية معدل إخراج يبلغ 5 دقائق 0 كيلو بايت/ثانية و 9 بايت/ثانية 5 دقائق معدل الإنزال، 0 بيكات/ثانية > إظهار الواجهة e1/8 واجهة إيثرنت 1/8 "خارجي"، قيد التشغيل، بروتوكول الخط قيد التشغيل الأجهزة هي EtherSVI و BW سرعة 1000 ميجابت في الثانية و LY سرعة 1000 usec عنوان MAC 5897.bdb9.774d، MTU 1500 وضع واجهة IPS: مضمن، مضمن: مزدوج خطي-1 عنوان IP غير معين إحصائيات حركة المرور ل "خارجي": إدخال 144 حزمة، 55634 بايت إخراج الحزم 3954، 339987 بايت تم إسقاط 0 حزم معدل إدخال يبلغ دقيقة واحدة 0	> إظهار الواجهة e1/6 < واجهة إيثرنت 1/6 "INSIDE"، قيد التشغيل، بروتوكول الخط قيد التشغيل الأجهزة هي EtherSVI و BW سرعة 1000 ميجابت في الثانية و LY سرعة 1000 usec عنوان MAC، الإصدار 5897.bdb9.770e، MTU 1500 وضع واجهة IPS: الضغط داخل 1-داخلي خط زوج: داخلية مجموعة، المرسل عنوان IP غير معين إحصائيات حركة المرور ل "Inside": إدخال 24 حزمة، 1378 بايت إخراج 0 حزم، 0 بايت تم إسقاط 24 حزمة معدل إدخال يبلغ دقيقة واحدة 0 pkts/ثانية و 0 بايت/ثانية معدل إخراج يبلغ دقيقة واحدة 0 pkts/ثانية، و 0 بايت/ثانية معدل الإنزال لمدة دقيقة واحدة، 0 كيلو بايت/ثانية 5 دقائق معدل الإدخال 0 بيكات/ثانية، 0 بايت/ثانية معدل إخراج يبلغ 5 دقائق 0 كيلو بايت/ثانية، و 0 بايت/ثانية 5 دقائق معدل الإنزال، 0 بيكات/ثانية > إظهار الواجهة e1/8 واجهة إيثرنت 1/8 "خارجي"، قيد التشغيل، بروتوكول الخط قيد التشغيل الأجهزة هي EtherSVI و BW سرعة 1000 ميجابت في الثانية و LY سرعة 1000 usec عنوان MAC 5897.bdb9.774d، MTU 1500 وضع واجهة IPS: الضغط داخل 1-داخلي خط زوج: داخلية مجموعة، المرسل عنوان IP غير معين إحصائيات حركة المرور ل "خارجي": إدخال حزمة واحدة، 441 بايت إخراج 0 حزم، 0 بايت تم إسقاط حزمة واحدة معدل إدخال يبلغ دقيقة واحدة 0

	pkts/ةيناث و 7 ةيناث/تياب 0 ةدحاو ةقيقد غلبي جارخإ لدعم pkts/ةيناث و 37 ةيناث/تياب 0 ،ةدحاو ةقيقد ةدمل لازنإلا لدعم ةيناث/تياب وليك 0 لاخدإلا لدعم قئاقد 5 بيكات/ةيناث، 8 ةيناث/تياب وليك 0 قئاقد 5 غلبي جارخإ لدعم يف تياب 39 و ةيناثلا يف تياب ةيناثلا 0 ،لازنإلا لدعم قئاقد 5 بيكات/ةيناث >	pkts/ةيناث و 0 ةيناث/تياب 0 ةدحاو ةقيقد غلبي جارخإ لدعم pkts/ةيناث، و 0 ةيناث/تياب 0 ،ةدحاو ةقيقد ةدمل لازنإلا لدعم ةيناث/تياب وليك 0 لاخدإلا لدعم قئاقد 5 بيكات/ةيناث، 0 ةيناث/تياب وليك 0 قئاقد 5 غلبي جارخإ لدعم تياب/ةيناث، و 0 ةيناث/تياب 0 ،لازنإلا لدعم قئاقد 5 بيكات/ةيناث >
ةجلاعم ةمزحلا مادختساب ةدعاق رظحلا	> راهظإ طاقتلالا عبتت ةمزح CAPI مقر 1 مت طاقتلا 3 مزح 1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) Ack 0 win 8192 ةلحرملا: 1 عونلا: طاقتلالا عونلا يعرفلا: ةجيتنلا: حامسلا نيوكتلا: تامولعم ةيفاضإ: ةمئاق لوصولا ىلإ MAC ةلحرملا: 2 عونلا: ةمئاق لوصولا عونلا يعرفلا: ةجيتنلا: حامسلا نيوكتلا: ةدعاق ةينمض تامولعم ةيفاضإ: ةمئاق لوصولا ىلإ MAC ةلحرملا: 3 عونلا: NGIPS-mode عونلا يعرفلا: ngips-mode ةجيتنلا: حامسلا نيوكتلا: تامولعم ةيفاضإ: اهنيوكت مت ةهجاو ىلع قفدتلا فرعت	> راهظإ طاقتلالا عبتت ةمزح CAPI مقر 1 مت طاقتلا 3 مزح 1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192 ةلحرملا: 1 عونلا: طاقتلالا عونلا يعرفلا: ةجيتنلا: حامسلا نيوكتلا: تامولعم ةيفاضإ: ةمئاق لوصولا ىلإ MAC ةلحرملا: 2 عونلا: ةمئاق لوصولا عونلا يعرفلا: ةجيتنلا: حامسلا نيوكتلا: ةدعاق ةينمض تامولعم ةيفاضإ: ةمئاق لوصولا ىلإ MAC ةلحرملا: 3 عونلا: NGIPS-mode عونلا يعرفلا: ngips-mode ةجيتنلا: حامسلا نيوكتلا: تامولعم ةيفاضإ: اهنيوكت مت ةهجاو ىلع قفدتلا فرعت عضول NGIPS متو قيبطت تامدخ

	لوضع NGIPS وتم تطبيق خدمات NGIPS المرحلة: 4 النوع: قائمة الوصول النوع الفرعي: السجل النتيجة: إسقاط التكوين: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ رفض متقدم IP 192.168.201.0 255.255.255.0 أي قاعدة-id 268441600 سجل الأحداث flow-start access-list CSM_FW_ACL_ ملاحظة rule-id 268441600: سياسة الوصول: FTD4100 - إلزامية/1 access-list csm_fw_acl_ ملاحظة rule-id 268441600: قاعدة L4: القاعدة 1 معلومات إضافية: النتيجة: واجهة الإدخال: من الداخل حالة الإدخال: لأعلى حالة خط الإدخال: للأعلى الإجراء: drop سبب الإسقاط: يتم رفض تدفق (acl-drop) بواسطة القاعدة التي تم تكوينها تم عرض حزمة واحدة >	NGIPS المرحلة: 4 النوع: قائمة الوصول النوع الفرعي: السجل النتيجة: قد تكون سقطت التكوين: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ رفض متقدم IP 192.168.201.0 255.255.255.0 أي قاعدة-id 268441600 سجل الأحداث flow-start access-list CSM_FW_ACL_ ملاحظة rule-id 268441600: سياسة الوصول: FTD4100 - إلزامية/1 access-list csm_fw_acl_ ملاحظة rule-id 268441600: قاعدة L4: القاعدة 1 معلومات إضافية: النتيجة: واجهة الإدخال: من الداخل حالة الإدخال: لأعلى حالة خط الإدخال: للأعلى الإجراء: كانت قائمة الوصول ستسقط، ولكن تمت إعادة توجيهه بسبب حزمة الضغط الداخلي تم عرض حزمة واحدة >

ملخص

- عندما تستخدم وضع الزوج الداخلي، فإن الحزمة تنتقل بشكل رئيسي من خلال محرك FTD
- تتم معالجة إتصالات TCP في وضع تجاوز حالة TCP
- من وجهة نظر FTD LINA Engine، يتم تطبيق سياسة قائمة التحكم في الوصول (ACL)
- عندما يكون وضع الزوج الداخلي قيد الاستخدام، يمكن حظر الحزم نظرا لأنها تتم معالجتها في السطر
- عند تمكين وضع الضغط، يتم فحص نسخة من الحزمة وإسقاطها داخليا بينما تمر حركة المرور الفعلية عبر FTD غير المعدل

معلومات ذات صلة

- جدار الحماية من الجيل التالي من Cisco Firepower
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).