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

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- Firepower 4112 FTD (رمز 7.x)
- مركز إدارة Firepower (FMC) (رمز 7.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:

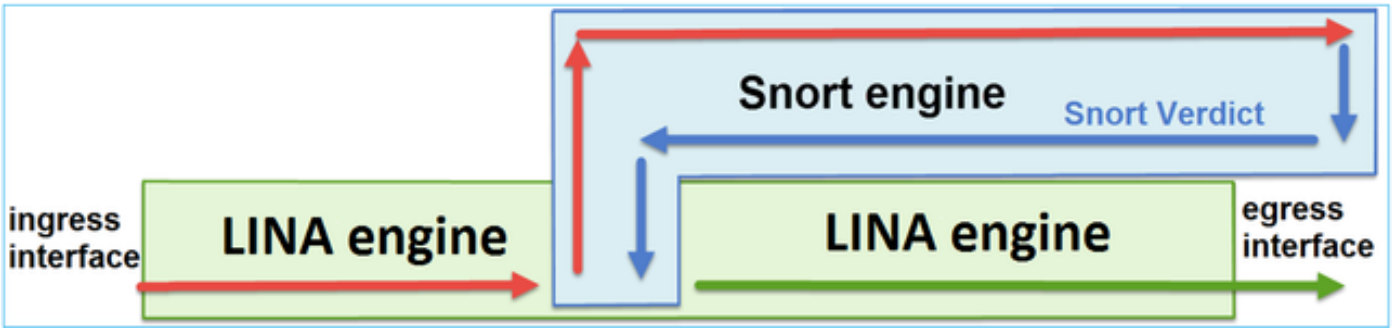
- FPR1000, FPR2100, FPR4100, FPR9300
- Secure Firewall 3100 و 4200 Series
- vFTD
- رمز برنامج FTD الإصدار 6.2.x والإصدارات الأحدث

معلومات أساسية

FTD عبارة عن صورة برنامج موحّد تتكون من محركين رئيسيين:

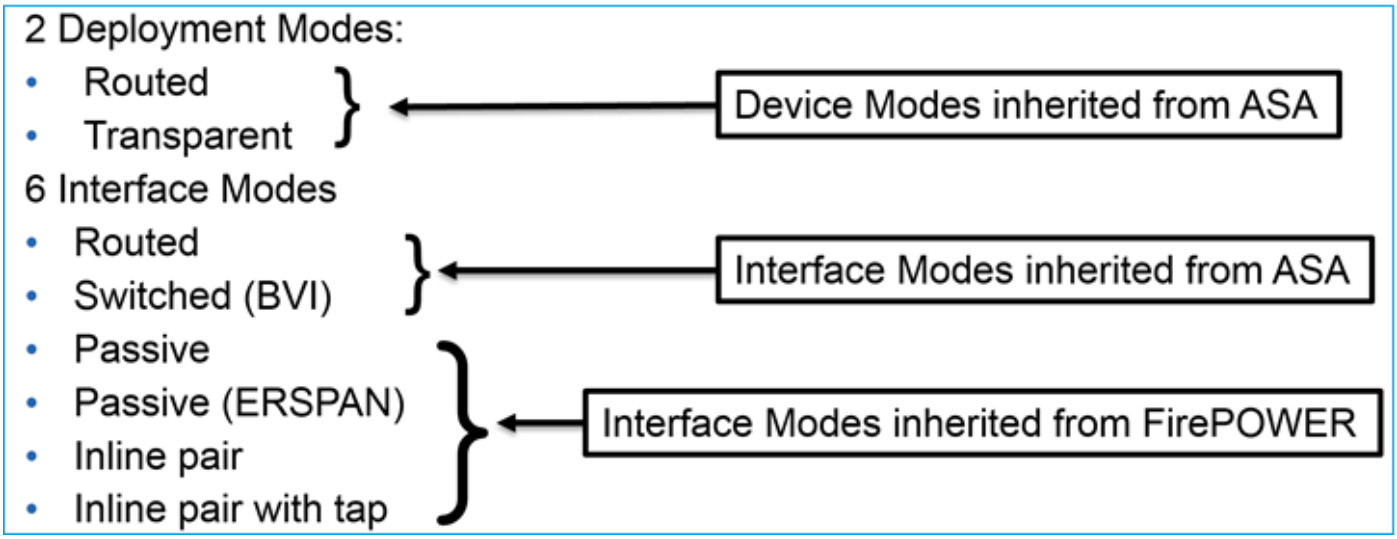
1. محرك LINA
2. محرك Snort

يوضح هذا الشكل كيفية تفاعل المحركين:



- تدخل الحزمة إلى واجهة الدخول ويتم التعامل معها بواسطة محرك LINA.
- إذا كان مطلوبا من قبل سياسة FTD، يتم فحص الحزمة بواسطة محرك snort.
- يرجع محرك الشخير حكما للحزمة.
- يقوم محرك LINA بإسقاط الحزمة أو إعادة توجيهها بناءً على قرار Snort.

يوفر FTD وضعي نشر وسته 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	تحققات كاملة لمحرك LINA و Snort-engine.	نعم
محول	شفاف	تحققات كاملة لمحرك LINA و Snort-engine.	نعم
زوج مضمن	موجه أو شفاف	فحص محرك LINA الجزئي وفحص محرك الشبكة بالكامل.	نعم
زوج مضمن مع TAP	موجه أو شفاف	فحص محرك LINA الجزئي وفحص محرك الشبكة بالكامل.	لا
خامل	موجه أو شفاف	فحص محرك LINA الجزئي وفحص محرك الشبكة بالكامل.	لا
خامل (ERSPAN)	موجه	فحص محرك LINA الجزئي وفحص محرك الشبكة بالكامل.	لا

تكوين واجهة الزوج المضمنة على FTD

الرسم التخطيطي للشبكة

المتطلبات

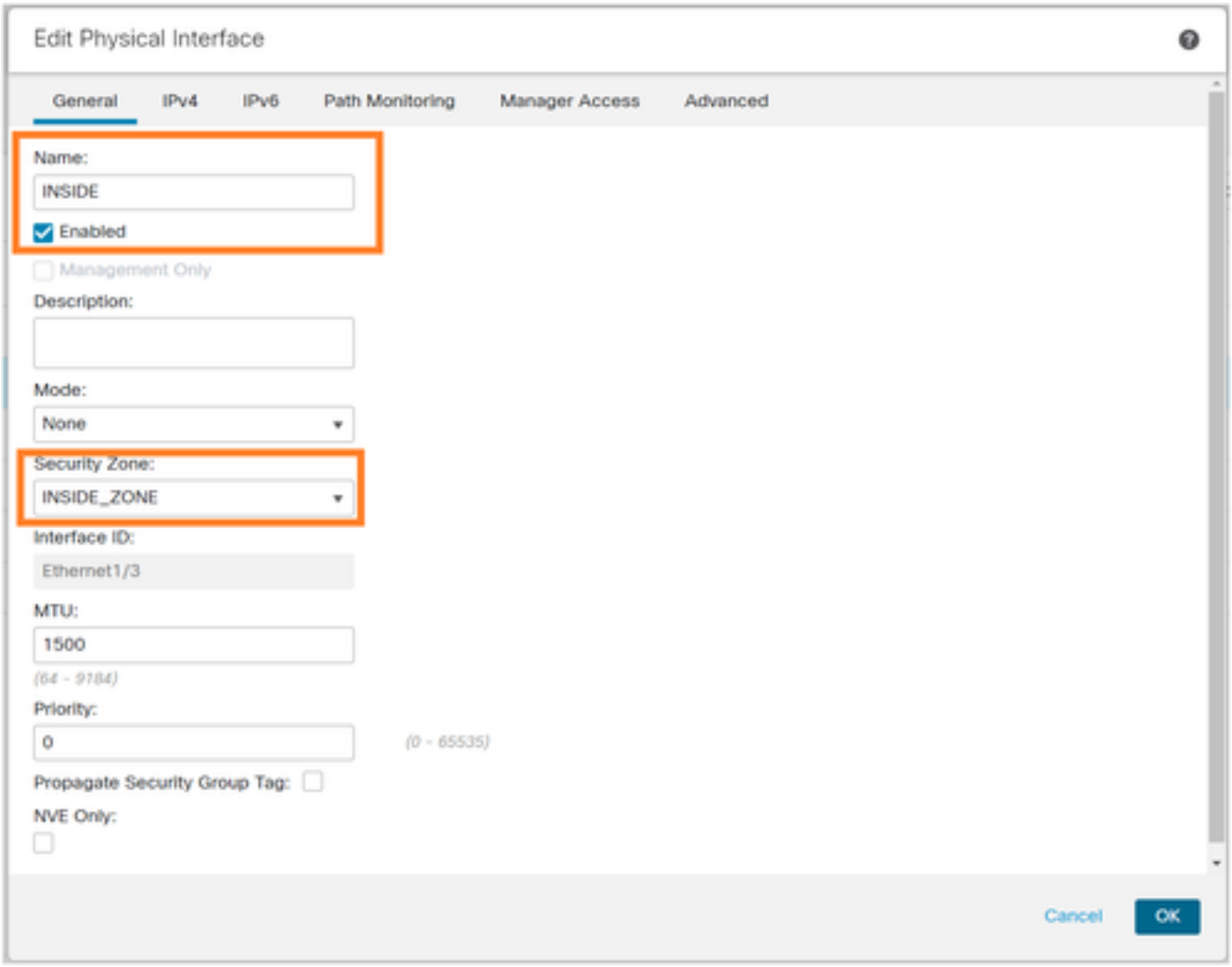
قم بتكوين الواجهات المادية E1/3 و E1/4 في وضع الزوج الداخلي وفقا لهذه المتطلبات:

الواجهة	E1/3	E1/4
الاسم	داخل	خارج
المنطقة الأمنية	Inside_zone	Outside_Zone
اسم المجموعة المضمنة	زوج خطي-1	
مجموعة MTU مضمنة	1500	
نشر حالة الارتباط	ممكن	

الحل

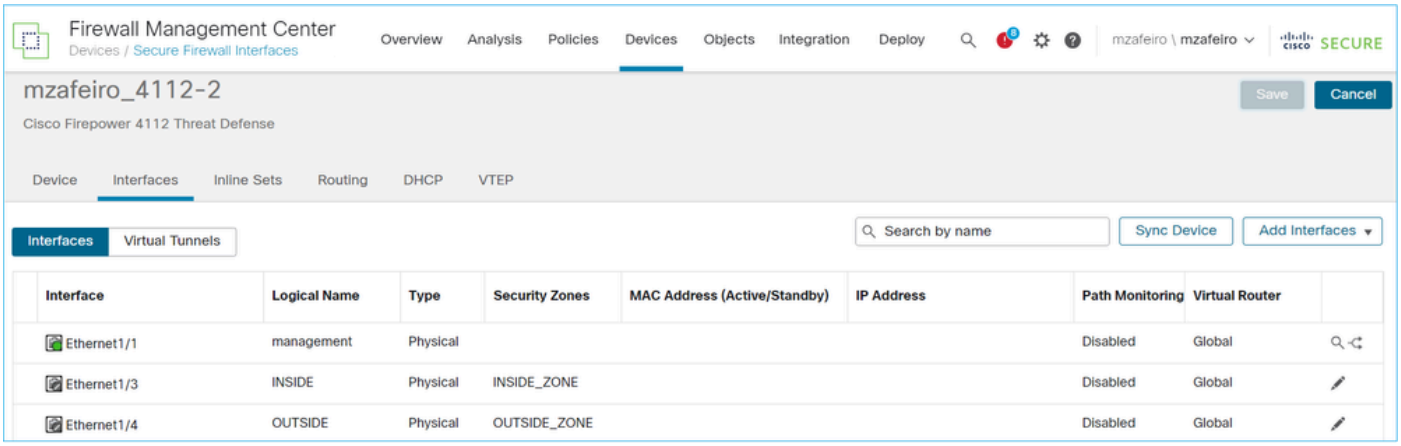
الخطوة 1. من أجل التكوين إلى الواجهات الفردية، انتقل إلى الأجهزة > إدارة الأجهزة، وحدد الجهاز المناسب وحدد تحرير:

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



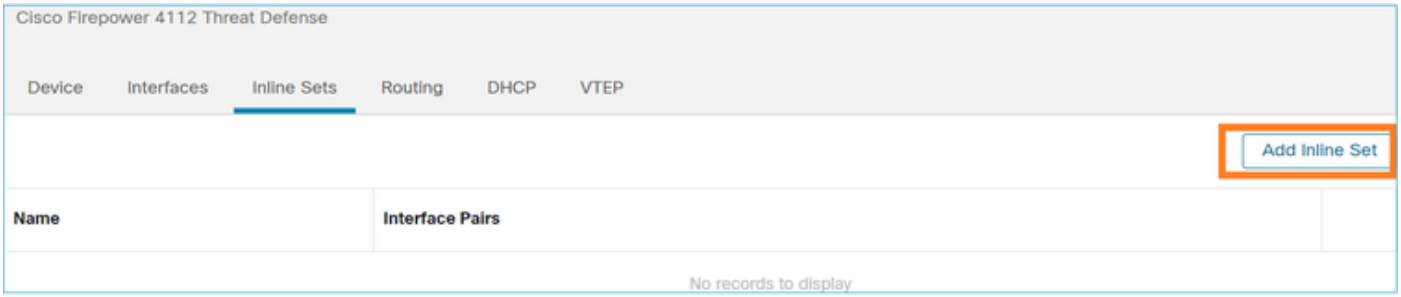
ملاحظة: الاسم هو اسم الواجهة.

وبالمثل، واجهة إيثرنت 1/4. يتم عرض النتيجة النهائية:

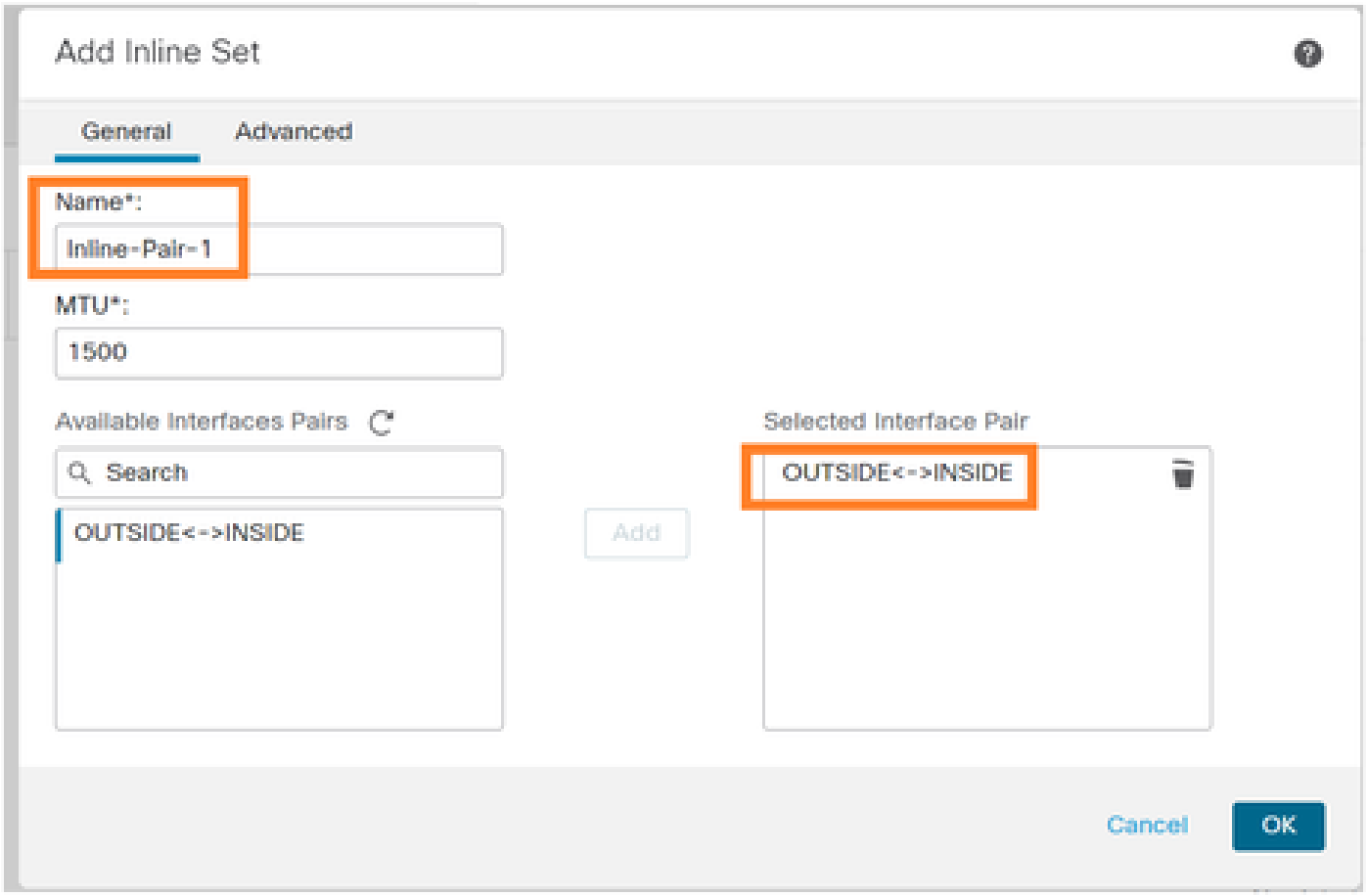


الخطوة 2. قم بتكوين الزوج المضمن.

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.



الخطوة 4. قم بتمكين خيار حالة إرتباط النشر 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. احفظ التغييرات وقم بالنشر.

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:

```
<#root>

firepower#

show inline-set


Inline-set Inline-Pair-1
  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 on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
      Current-Status: UP
    Interface: Ethernet1/3 "INSIDE"
```

```
  Current-Status: UP
Bridge Group ID: 507
```

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

معلومات الواجهة والاسم:

<#root>

```
firepower#
```

show nameif

```
Interface       Name            Security
Ethernet1/1     management       0
Ethernet1/3     INSIDE           0
Ethernet1/4     OUTSIDE          0
```

دقق القارن وضع:

<#root>

```
firepower#
```

show interface ip brief

```
Interface             IP-Address    OK? Method Status Protocol
Internal-Control0/0   unassigned    YES unset  up     up
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
Internal-Data0/3      unassigned    YES unset  up     up
Internal-Data0/4      unassigned    YES unset  down   up
Ethernet1/1           203.0.113.130 YES unset  up     up
Ethernet1/3           unassigned    YES unset  up     up
Ethernet1/4           unassigned    YES unset  up     up
```

التحقق من معلومات الواجهة المادية:

<#root>

```
firepower#
show interface e1/3


Interface Ethernet1/3 "INSIDE", is up, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
           MAC address ac4a.670e.641e, MTU 1500


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


           IP address unassigned
  Traffic Statistics for "INSIDE":
           170 packets input, 12241 bytes
            41 packets output, 7881 bytes
             9 packets dropped
      1 minute input rate 0 pkts/sec, 37 bytes/sec
      1 minute output rate 0 pkts/sec, 19 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec, 34 bytes/sec
      5 minute output rate 0 pkts/sec, 23 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

التحقق من عملية واجهة زوج الخطوط المضمنة لـ FTD

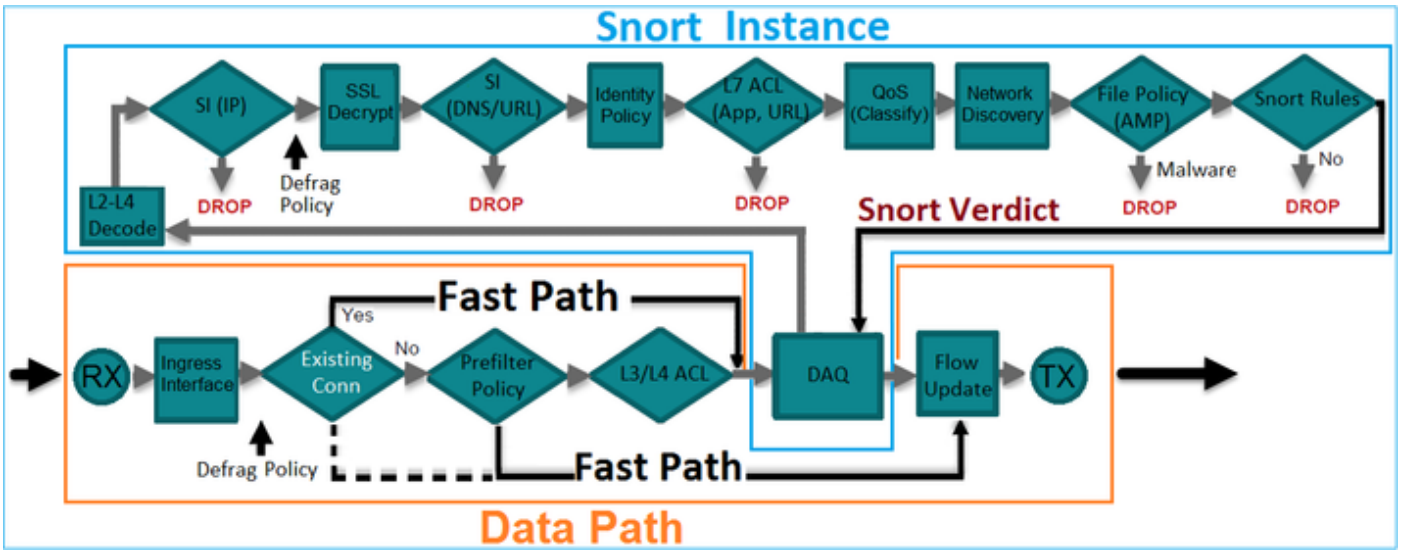
يغطي هذا القسم عمليات التحقق من الصحة هذه للتحقق من عملية "الزوج الداخلي":

- التحقق 1. باستخدام أداة تتبع الحزم.
- التحقق 2. قم بتمكين الالتقاط باستخدام التتبع وأرسل حزمة مزامنة/إقرار TCP (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.
- تدقيق 5. يشكل شبكة عنوان ترجمة (NAT) ساكن إستاتيكي.

الحل

نظرة عامة على البنية

عند تشغيل واجهتي FTD في وضع زوج خطي، تتم معالجة الحزمة، كما هو موضح في الصورة.

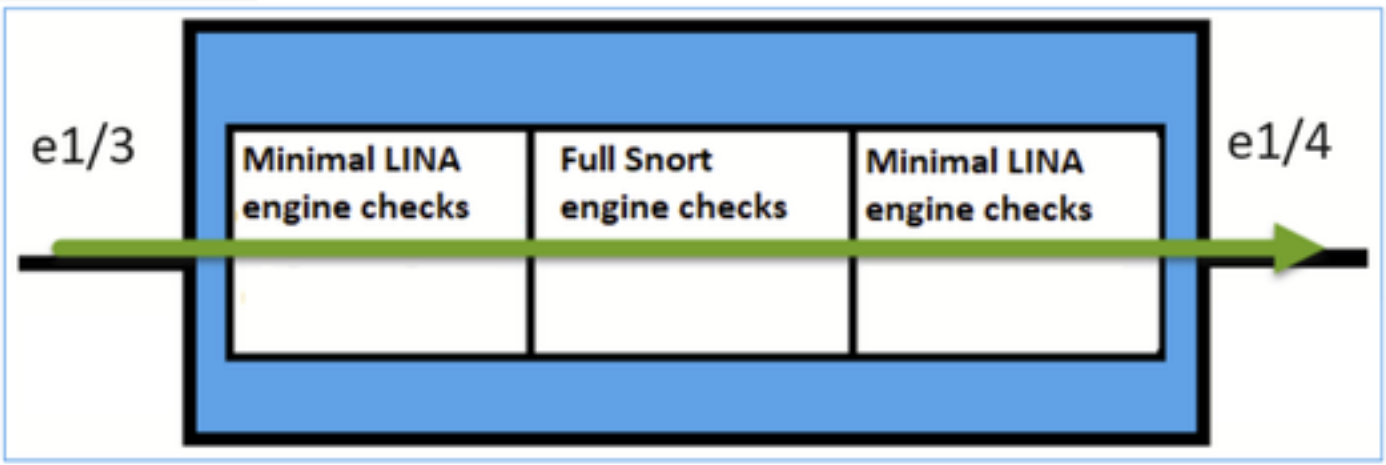


ملاحظة: يمكن أن تكون الواجهات المادية فقط أعضاء في مجموعة زوج مضمن.

النظرية الأساسية

- عند تكوين زوج مضمن 2 مادي، يتم ربط الواجهات 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. باستخدام Packet-tracer

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

<#root>

firepower#

packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80

Phase: 1

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW

Elapsed time: 11834 ns

Config:

Additional Information:

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

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 11834 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.201.50 host 192.168.202.50 rule-id 268451044
access-list CSM_FW_ACL_ remark rule-id 268451044: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451044: L7 RULE: New-Rule-#1303-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Elapsed time: 2440 ns

Config:

Additional Information:

Ingress interface INSIDE is in NGIPS inline mode.

Egress interface OUTSIDE is determined by inline-set configuration

Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 68320 ns
Config:
Additional Information:
New flow created with id 1801, packet dispatched to next module

Phase: 5
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 18056 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 6
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 13668 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Phase: 7
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 67770 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268451044
Additional Information:
Starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt:
Matched rule ids 268451044 - Allow

Phase: 8
Type: SNORT
Subtype: appid
Result: ALLOW

```
Elapsed time: 11002 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:
```

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface: OUTSIDE(vrfid:0)

output-status: up

output-line-status: up

Action: allow

```
Time Taken: 204924 ns
```

التحقق 2. إرسال حزم TCP SYN/ACK من خلال زوج خطي

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

<#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 هذه القاعدة على واجهة سطر الأوامر (CLI) من FTD وأرسل بعض حزم TCP SYN/ACK:

```
<#root>

firepower#

capture CAPI interface INSIDE trace match ip host 192.168.201.60 any


firepower#

capture CAPO interface OUTSIDE match ip host 192.168.201.60 any
```

توضح عمليات التقاط أن حزم SYN/ACK الثلاثة تجتاز FTD:

```
<#root>

firepower#

show capture CAPI


3 packets captured

1: 09:20:18.206440 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
2: 09:20:18.208180 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3: 09:20:18.210026 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
firepower#

show capture CAPO


3 packets captured

1: 09:20:18.206684 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
2: 09:20:18.208210 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3: 09:20:18.210056 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
```

يكشف تتبع حزمة الالتقاط الأولى عن بعض المعلومات الإضافية مثل الحكم على محرك الشير:

<#root>

firepower#

show capture CAPI packet-number 1 trace

3 packets captured

1: 09:20:18.206440 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 5978 ns
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5978 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.201.50 object-group FMC_INLINE_dst_rule_2684510
access-list CSM_FW_ACL_ remark rule-id 268451044: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451044: L7 RULE: New-Rule-#1303-ALLOW
object-group network FMC_INLINE_dst_rule_268451044
network-object 192.168.202.50 255.255.255.255
network-object 192.168.201.60 255.255.255.255
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 1952 ns
Config:
Additional Information:
Ingress interface INSIDE is in NGIPS inline mode.
Egress interface OUTSIDE is determined by inline-set configuration

Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 45872 ns
Config:
Additional Information:
New flow created with id 1953, packet dispatched to next module

Phase: 5

Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 18544 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 6
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 25182 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Phase: 7

Type: SNORT

Subtype: firewall

Result: ALLOW

Elapsed time: 50924 ns

Config:

Network 0, Inspection 0, Detection 0, Rule ID 268451044

Additional Information:

Starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0

Matched rule ids 268451044 - Allow

Phase: 8
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 17722 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

```
Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 172152 ns


1 packet shown
```

يظهر تتبع الحزمة الملتقطة الثانية أن الحزمة تطابق اتصال حالي حتى تتجاوز التحقق من قائمة التحكم بالوصول (ACL)، ولكن ام يزال يتم فحصه بواسطة محرك snort:

<#root>

firepower#

show capture CAPI packet-number 2 trace

```
3 packets captured

2: 09:20:18.208180 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 1952 ns
Config:
Additional Information:
```

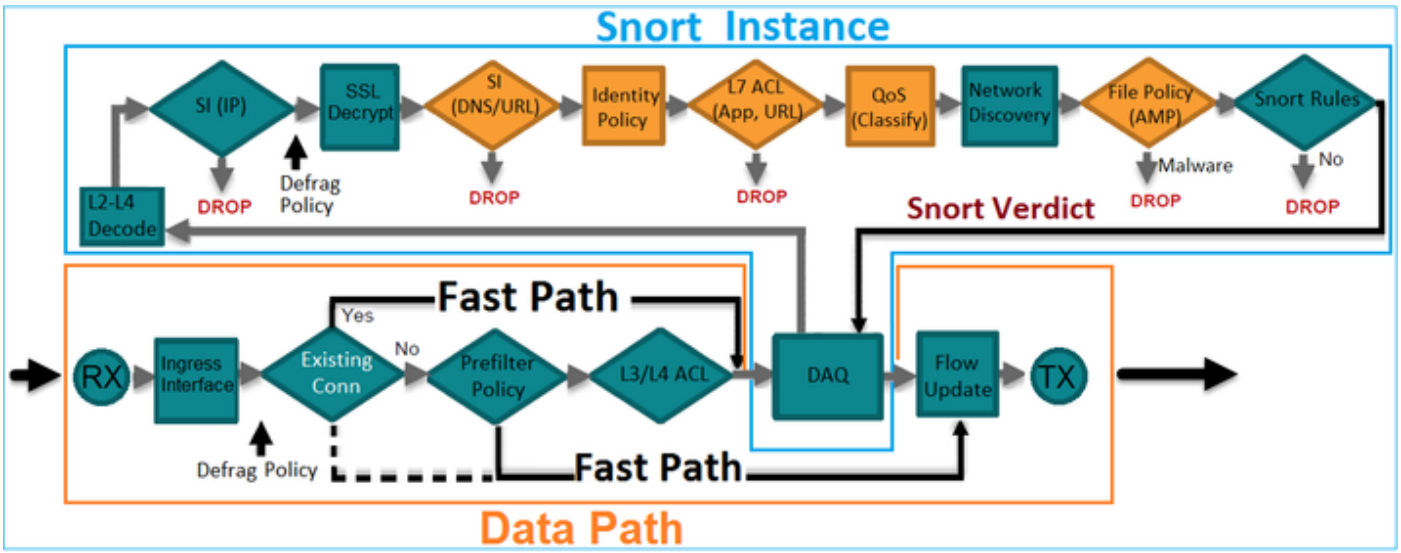
Found flow with id 1953, using existing flow

```
Phase: 2
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 7320 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 3
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 1860 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:
```

```
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow
Time Taken: 11132 ns


1 packet shown
```

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

يتم تشغيل تصحيح أخطاء محرك جدار الحماية مقابل 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 E1/4.
على واجهة سطر أوامر (CLI) واجهة سطر الأوامر (FTD)، يجب أن ترى أن كل الواجهات قد سقطت:

<#root>

```
firepower#

show interface ip brief

Interface              IP-Address    OK? Method Status     Protocol
Internal-Control0/0    unassigned    YES unset  up         up
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
Internal-Data0/3       unassigned    YES unset  up         up
Internal-Data0/4       unassigned    YES unset  down       up
Ethernet1/1            203.0.113.130 YES unset  up         up
Ethernet1/3            unassigned    YES unset  admin down down

Ethernet1/4            unassigned    YES unset  down       down
```

تظهر سجلات FTD:

<#root>

```
firepower#

show log

...
```

May 28 2024 07:35:10: %FTD-4-411002: Line protocol on Interface Ethernet1/4, changed state to down

May 28 2024 07:35:10: %FTD-4-411004: Interface INSIDE, changed state to administratively down

May 28 2024 07:35:10: %FTD-4-411004: Interface Ethernet1/3, changed state to administratively down

May 28 2024 07:35:10: %FTD-4-812005: Link-State-Propagation activated on inline-pair due to failure of i

May 28 2024 07:35:10: %FTD-4-411002: Line protocol on Interface Ethernet1/3, changed state to down

2: تظهر حالة المجموعة الداخلية حالة أعضاء الواجهة

<#root>

firepower#

show inline-set

Inline-set Inline-Pair-1
  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 on

  hardware-bypass mode is disabled
    Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"

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

    Interface: Ethernet1/3 "INSIDE"

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

Bridge Group ID: 507

لاحظ الفرق في حالة الواجهات الثانية:

<#root>

firepower#

```
 show interface e1/3


Interface Ethernet1/3 "INSIDE", is admin down, line protocol is down


  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        MAC address ac4a.670e.641e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


Administrative-Down-By-Propagate-Link-State


        IP address unassigned
  Traffic Statistics for "INSIDE":
        2400 packets input, 165873 bytes
        1822 packets output, 178850 bytes
        17 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,  32 bytes/sec
      5 minute output rate 0 pkts/sec,  57 bytes/sec
      5 minute drop rate, 0 pkts/sec
firepower#
show interface e1/4


Interface Ethernet1/4 "OUTSIDE", is down, line protocol is down


  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        MAC address ac4a.670e.640e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
        Propagate-Link-State-Activated


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        1893 packets input, 158046 bytes
        2386 packets output, 213997 bytes
        67 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,  51 bytes/sec
      5 minute output rate 0 pkts/sec,  39 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

بعد إعادة تمكين switchport، تظهر سجلات FTD:

```
<#root>

May 28 2024 07:38:04: %FTD-4-411001: Line protocol on Interface Ethernet1/4, changed state to up
```

```
May 28 2024 07:38:04: %FTD-4-411003: Interface Ethernet1/3, changed state to administratively up

May 28 2024 07:38:04: %FTD-4-411003: Interface INSIDE, changed state to administratively up

May 28 2024 07:38:04: %FTD-4-812006: Link-State-Propagation de-activated on inline-pair due to recovery

May 28 2024 07:38:05: %FTD-4-411002: Line protocol on Interface Ethernet1/4, changed state to down
```

تدقيق 5. يشكل NAT ساكن إستاتيكي

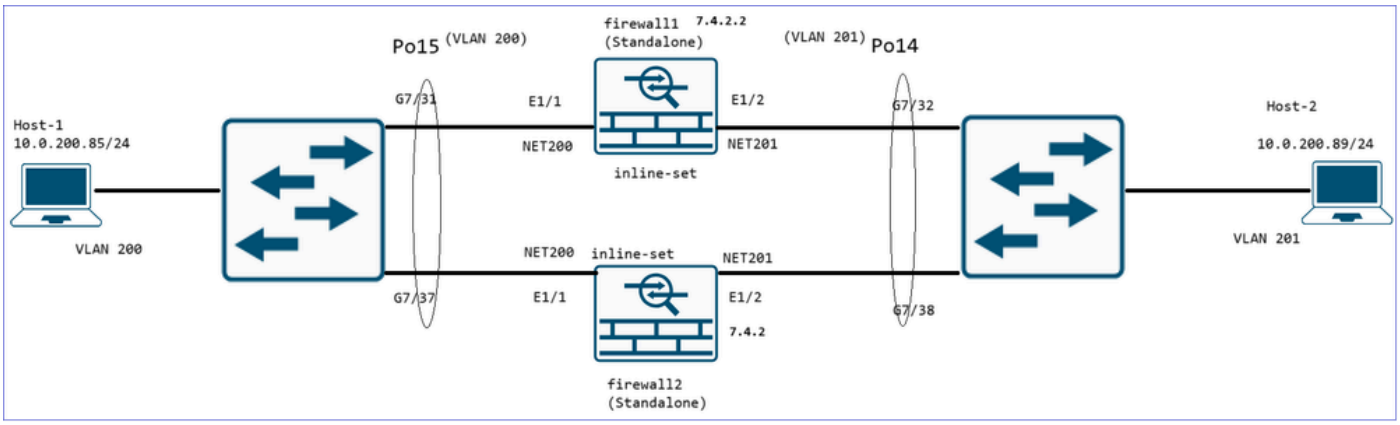
الحل

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

دليل تكوين Firepower Management Center، الإصدار 6.0.1

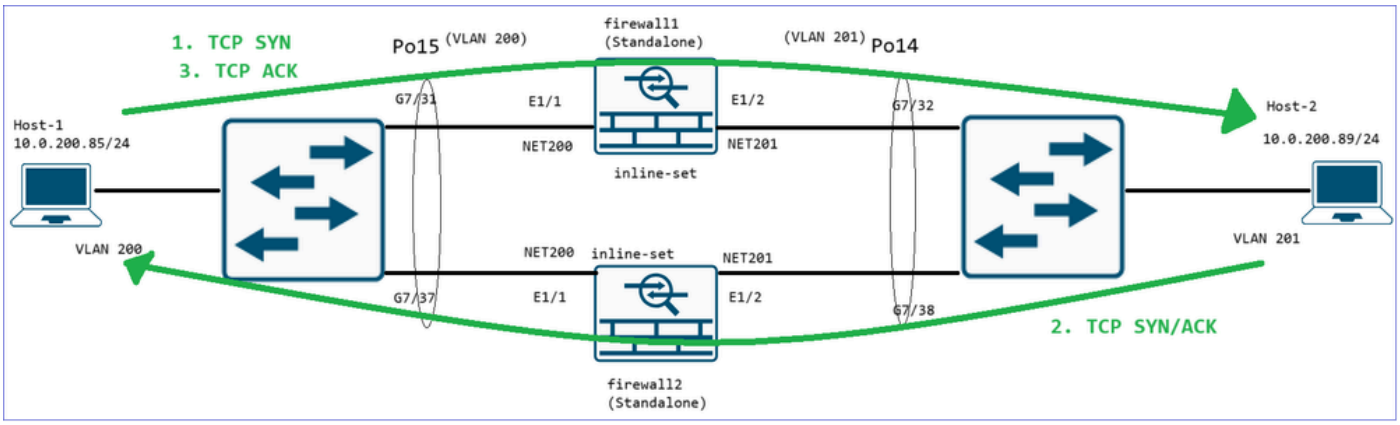
دراسة حالة - حركة المرور غير المتماثلة عبر مجموعات الخطوط الداخلية

تأمل في هذا السيناريو:



يعمل جدران الحماية في الوضع المستقل (حتى أنهم يشغلون إصدارات برامج مختلفة)، ولكنهم يتعاملون مع حركة مرور البيانات من نفس واجهات قناة المنفذ.

في هذه الحالة، أنت يستطيع يتلقى حركة مرور غير متماثل بسبب قناة ميناء موازنة خوارزمية:



1. المضيف-1 (10.0.200.85) يرسل نظام TCP نحو المضيف-2 (10.0.200.89). جدار حماية إجتياز الحزمة هذا 1.
2. المضيف-2 (10.0.200.89) يرسل TCP SYN/ACK نحو المضيف-2 (10.0.200.85). جدار الحماية الخاص بتجاوز الحزمة 2.
3. اكتملت مصافحة TCP الثلاثية الإتجاه مع المضيف-1 الذي يرسل TCP ACK نحو المضيف-2. جدار حماية إجتياز الحزمة هذا 1.

من وجهة نظر المضيف-1، تم إنشاء الاتصال بنجاح:

<#root>

```
root@kali:/ #
```

wget -O - http://10.0.200.89/10K

```
--2025-05-06 08:20:28--  http://10.0.200.89/10K
Connecting to 10.0.200.89:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10240 (10K)
Saving to: ‘STDOUT’
-                                                   100%[=============================================================
2025-05-06 08:20:28 (99.8 MB/s) - written to stdout [10240/10240]
```

يظهر التقاط الحزمة على جدار الحماية 1 فقط حركة مرور من المضيف1 إلى المضيف2:

<#root>

```
firepower#
```

show capture

```
capture CAPI type raw-data trace interface NET200 [Capturing - 875 bytes]
  match ip host 10.0.200.85 host 10.0.200.89
capture CAPO type raw-data trace interface NET201 [Capturing - 875 bytes]
  match ip host 10.0.200.85 host 10.0.200.89
```

محتويات االلتقاط:

```
<#root>

firepower#

show capture CAPI



9 packets captured

   1: 12:21:14.161689       10.0.200.85.44806 > 10.0.200.89.80:

S

1877376557:1877376557(0) win 64240 <mss 1460,sackOK,timestamp 2133104674 0,nop,wscale 7>
   2: 12:21:14.162924       10.0.200.85.44806 > 10.0.200.89.80: .

ack

 3274105192 win 502 <nop,nop,timestamp 2133104676 1658009126>
   3: 12:21:14.163077       10.0.200.85.44806 > 10.0.200.89.80: P 1877376558:1877376687(129) ack 327410
   4: 12:21:14.164801       10.0.200.85.44806 > 10.0.200.89.80: . ack 3274106640 win 501 <nop,nop,times
   5: 12:21:14.164908       10.0.200.85.44806 > 10.0.200.89.80: . ack 3274108088 win 494
...
```

يظهر التقاط الحزمة على جدار الحماية 2 فقط حركة مرور من المضيف2 إلى المضيف 1:

```
<#root>

FTD1010-12#

show capture CAPI



11 packets captured

   1: 12:21:14.198949       10.0.200.89.80 > 10.0.200.85.44806:

S

 3274105191:3274105191(0)

ack

 1877376558 win 65160 <mss 1460,sackOK,timestamp 1658009126 2133104674,nop,wscale 7>
   2: 12:21:14.200001       10.0.200.89.80 > 10.0.200.85.44806: . ack 1877376687 win 509 <nop,nop,times
   3: 12:21:14.200825       10.0.200.89.80 > 10.0.200.85.44806: . 3274105192:3274106640(1448) ack 18773
   4: 12:21:14.200947       10.0.200.89.80 > 10.0.200.85.44806: . 3274106640:3274108088(1448) ack 18773
   5: 12:21:14.200963       10.0.200.89.80 > 10.0.200.85.44806: . 3274108088:3274109536(1448) ack 18773
   6: 12:21:14.200978       10.0.200.89.80 > 10.0.200.85.44806: . 3274109536:3274110984(1448) ack 18773
   7: 12:21:14.200993       10.0.200.89.80 > 10.0.200.85.44806: P 3274110984:3274112432(1448) ack
...
```

تظهر Syslog على جدار الحماية 1 أن حزمة TCP syn قامت بإنشاء اتصال تجاوز حالة TCP:

```
<#root>

firepower#

show logging

...
May 06 2025 12:21:14: %FTD-6-302303:

Built TCP state-bypass connection

 106977 from NET200:10.0.200.85/44806 (10.0.200.85/44806) to NET201:10.0.200.89/80 (10.0.200.89/80)
```

على جدار الحماية 2، قامت حزمة TCP SYN/ACK أيضا بإنشاء اتصال تجاوز حالة TCP:

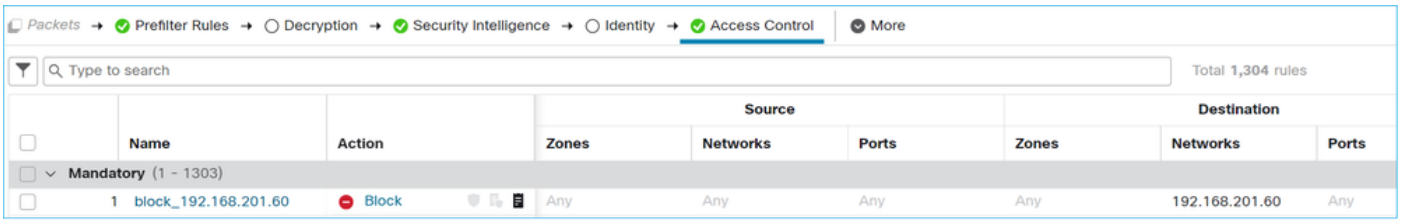
```
<#root>

FTD1010-12#

show logging

...
May 06 2025 12:21:14: %FTD-6-302303:

Built TCP state-bypass

connection

 325 from NET201:10.0.200.89/80 (10.0.200.89/80) to NET200:10.0.200.85/44806 (10.0.200.85/44806)
```

النقاط الرئيسية

- تعمل حركة المرور غير المتماثلة من خلال مجموعة داخلية من أجهزة جدار الحماية المختلفة نظرا لأن كل الجهازين يعالجان اتصال TCP في وضع تجاوز حالة TCP.
- لاحظ أنه لم يتم تكوين تجاوز حالة TCP يدويا على جدران الحماية، ولكنه تتيجة لعملية واجهة مجموعة الأسطر.

حظر الحزمة على وضع واجهة زوج الخطوط الداخلية

قم بإنشاء قاعدة حظر، وأرسل حركة المرور عبر 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>

firepower#

show capture


capture CAPI type raw-data trace interface INSIDE

[Capturing - 270 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
```

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

```
<#root>

firepower#

show capture CAPI packet-number 1 trace


4 packets captured

   1: 09:41:54.562547       192.168.201.50.59144 > 192.168.201.60.80: S 3817586151:3817586151(0) win 64
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 10126 ns
```

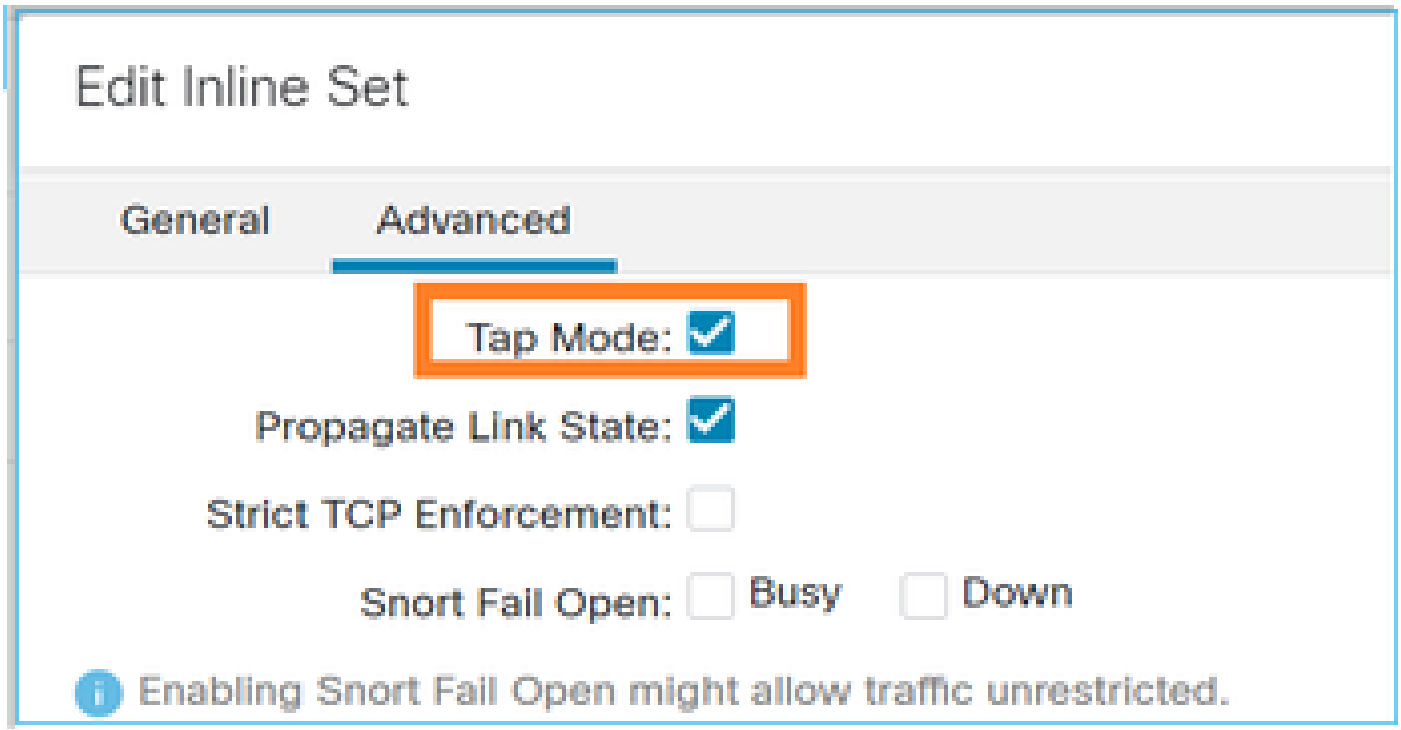
```
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Elapsed time: 10126 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any host 192.168.201.60 rule-id 268451045 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268451045: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451045: L4 RULE: block_192.168.201.60
Additional Information:

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: drop

Time Taken: 20252 ns

1 packet shown
```

تكوين وضع الزوج المضمن باستخدام TAP

قم بتمكين وضع الضغط على الزوج الداخلي.

الحل

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



التحقق

<#root>

```
firepower#
```

show inline-set

```
Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Fail-open for snort down is off
  Fail-open for snort busy is off
```

Tap mode is on

```
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
      Current-Status: UP
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP
```

Bridge Group ID: 0

التحقق من زوج FTD الداخلي باستخدام عملية واجهة TAP

النظرية الأساسية

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

يقوم الزوج المضمن مع وضع الضغط بإسقاط حركة مرور النقل. باستخدام تتبع حزمة، فإنه يؤدي 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
```

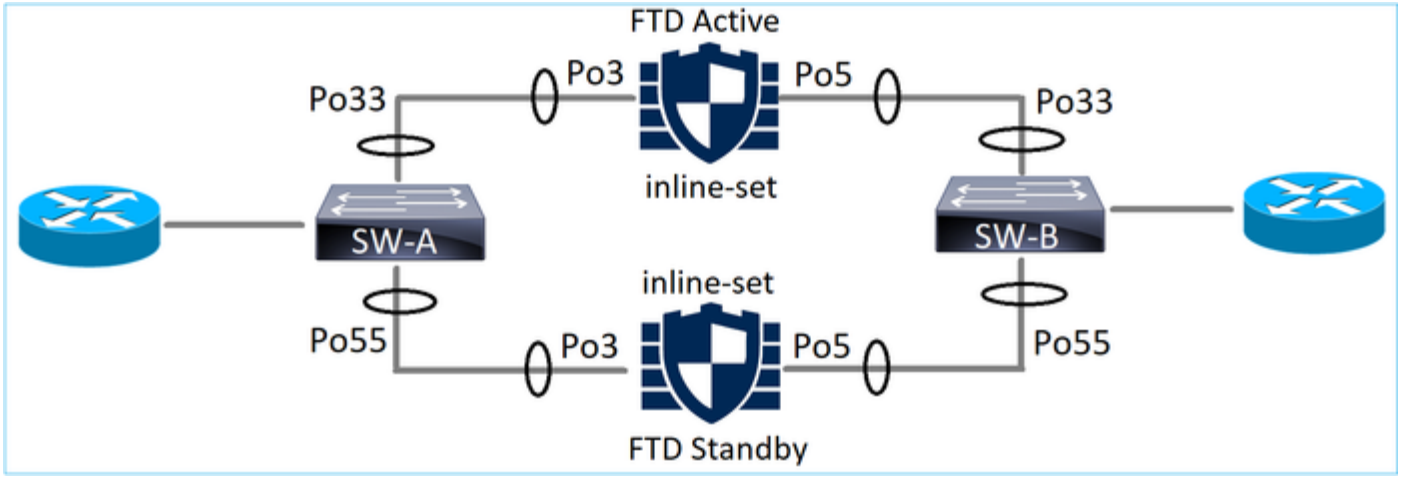
```
Result: WOULD HAVE DROPPED

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     Po55(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:

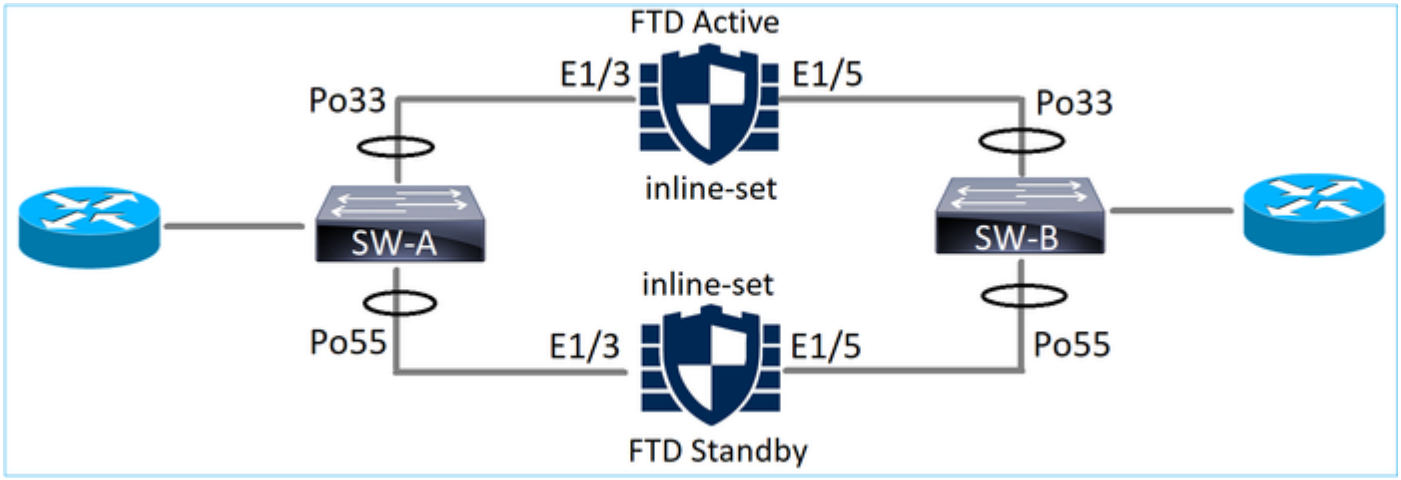
<#root>

```
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 حدث تجاوز فشل في برنامج الإرسال فائق السرعة (FTD)، يعتمد انقطاع حركة المرور بشكل رئيسي على الوقت الذي تستغرقه المحولات لتعلم عنوان MAC للنظير 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 عبر قناة EtherChannel، وعلى الوقت الذي يتم فيه قطع الاتصال، والذي يمكن أن يكون أطول من ذلك. في حالة تشغيل وضع EtherChannel (لا LACP)، بعد ذلك يعتمد وقت التقارب على يعلم عنوان MAC.

استكشاف الأخطاء وإصلاحها

هناك حاليا ما من معلومة خاص يتوفر ل هذا تشكيل.

المقارنة: الزوج المضمن مقابل الزوج المضمن باستخدام TAP

	زوج مضمن	زوج مضمن مع TAP
إظهار المجموعة الداخلية	> إظهار المجموعة الداخلية مجموعة الداخل 1-داخلي خط زوج وحدة الحد الأقصى للنقل (MTU) هي 1500 بايت وضع الأمان في حالة الفشل قيد التشغيل/التنشيط تم إيقاف تشغيل وضع تأمين الفشل	> إظهار المجموعة الداخلية مجموعة الداخل 1-داخلي خط زوج وحدة الحد الأقصى للنقل (MTU) هي 1500 بايت وضع الأمان في حالة الفشل قيد التشغيل/التنشيط تم إيقاف تشغيل وضع تأمين الفشل

	مت إيقاف تشغيل وضع الضغط خيار Propagate-link-state ديق التشغيل مت تعطيل وضع تجاوز الجهاز زوج الواجهة[1]: الواجهة: إيثرنت 1/6 "داخل" الحالة الحالية: يعمل الواجهة: إيثرنت 1/8 "خارج" الحالة الحالية: يعمل عدد فرع مجموعة السجل: 509 >	وضع الضغط ديق التشغيل خيار Propagate-link-state ديق التشغيل مت تعطيل وضع تجاوز الجهاز زوج الواجهة[1]: الواجهة: إيثرنت 1/6 "داخل" الحالة الحالية: يعمل الواجهة: إيثرنت 1/8 "خارج" الحالة الحالية: يعمل عدد فرع مجموعة السجل: 0 >
show interface	> إظهار الواجهة e1/6 واجهة إيثرنت 1/6 "INSIDE"، ديق التشغيل، بروتوكول الخط ديق 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: مضمنة، مضمنة: زوج خطي-1 عنوان IP غير معين إحصائيات حركة المرور ل "Inside": إدخال الحزم 3957، 264913 بايت إخراج 144 حزمة، 58664 بايت مت إسقاط 4 حزم معدل الإدخال يبلغ دقيقة واحدة 0 pkts/ثانية و 26 بايت/ثانية معدل الإخراج يبلغ دقيقة واحدة 0 pkts/ثانية و 7 بايت/ثانية معدل الإنزال لمدة دقيقة واحدة، 0 كيلو بايت/ثانية 0 الإدخال معدل دقائق 5 بايت/ثانية، 28 بايت/ثانية كيلو 0 دقائق 5 يبلغ إخراج معدل بايت/ثانية و 9 بايت/ثانية 0 ،الإنزال معدل دقائق 5 بايت/ثانية > إظهار الواجهة e1/8 واجهة إيثرنت 1/8 "خارجي"، ديق التشغيل، بروتوكول الخط ديق التشغيل	> إظهار الواجهة e1/6 واجهة إيثرنت 1/6 "INSIDE"، ديق التشغيل، بروتوكول الخط ديق 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 الداخلي، مجموعة داخلية: زوج خطي-1 عنوان IP غير معين إحصائيات حركة المرور ل "Inside": إدخال 24 حزمة، 1378 بايت إخراج 0 حزم، 0 بايت مت إسقاط 24 حزمة معدل الإدخال يبلغ دقيقة واحدة 0 pkts/ثانية و 0 بايت/ثانية معدل الإخراج يبلغ دقيقة واحدة 0 pkts/ثانية، و 0 بايت/ثانية معدل الإنزال لمدة دقيقة واحدة، 0 كيلو بايت/ثانية 0 الإدخال معدل دقائق 5 بايت/ثانية، 0 بايت/ثانية كيلو 0 دقائق 5 يبلغ إخراج معدل بايت/ثانية، و 0 بايت/ثانية 0 ،الإنزال معدل دقائق 5 بايت/ثانية > إظهار الواجهة e1/8 واجهة إيثرنت 1/8 "خارجي"، ديق التشغيل، بروتوكول الخط ديق التشغيل

	الأجهزة هي EtherSVI و BW ةعرس 1000 ميجاجت يف الثانية و LY ةعرس 1000 usec عنوان MAC 5897.bdb9.774d، MTU 1500 وضع ةهجاو IPS: مضمنة، مضمنة: زوج خطي-1 عنوان IP غير معين إحصائيات حركة المرور ل "خارجي": إدخال 144 حزمة، 55634 بايت إخراج المزحل 3954، 339987 بايت تم إسقاط 0 حزم معدل الإدخال يبلغ دقيقة واحدة 0 pkts/ثانية و 7 بايت/ثانية معدل الإخراج يبلغ دقيقة واحدة 0 pkts/ثانية و 37 بايت/ثانية معدل الإنزال لمدة دقيقة واحدة، 0 كيلو بايت/ثانية معدل الإدخال لـ 5 دقائق 0 بيكات/ثانية، 8 بايت/ثانية معدل الإخراج يبلغ 5 دقائق 0 كيلو بايت في الثانية و 39 بايت في الثانية معدل الإنزال لـ 5 دقائق، 0 بيكات/ثانية >	الأجهزة هي EtherSVI و BW ةعرس 1000 ميجاجت يف الثانية و LY ةعرس 1000 usec عنوان MAC 5897.bdb9.774d، MTU 1500 وضع ةهجاو IPS: الضغط الداخلي، مجموعة داخلية: زوج خطي-1 عنوان IP غير معين إحصائيات حركة المرور ل "خارجي": إدخال حزمة واحدة، 441 بايت إخراج 0 حزم، 0 بايت تم إسقاط حزمة واحدة معدل الإدخال يبلغ دقيقة واحدة 0 pkts/ثانية و 0 بايت/ثانية معدل الإخراج يبلغ دقيقة واحدة 0 pkts/ثانية، و 0 بايت/ثانية معدل الإنزال لمدة دقيقة واحدة، 0 كيلو بايت/ثانية معدل الإدخال لـ 5 دقائق 0 بيكات/ثانية، 0 بايت/ثانية معدل الإخراج يبلغ 5 دقائق 0 كيلو بايت/ثانية، و 0 بايت/ثانية معدل الإنزال لـ 5 دقائق، 0 بيكات/ثانية >
المعالجة المزحة باستخدام قاعدة الحظر	> إظهار التقاط تتبع حزمة CAPI رقم 1 تم التقاط 3 حزمة 1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: s 0:0(0) كات 0 ويين 8192 المرحلة: 1 النوع: أسر النوع الفرعي: النتيجة: سماح التكوين: معلومات إضافية: قائمة الوصول إلى MAC المرحلة: 2 النوع: قائمة الوصول النوع الفرعي:	> إظهار التقاط تتبع حزمة CAPI رقم 1 تم التقاط 3 حزمة 1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: فوز س 0:0(0) 8192 المرحلة: 1 النوع: أسر النوع الفرعي: النتيجة: سماح التكوين: معلومات إضافية: قائمة الوصول إلى MAC المرحلة: 2 النوع: قائمة الوصول النوع الفرعي: النتيجة: سماح

	النتيجة: سماح التكوين: قاعدة مضمنة معلومات إضافية: قائمة الوصول إلى MAC المرحلة: 3 النوع: وضع NGIPS النوع الفرعي: وضع NGIPS النتيجة: سماح التكوين: معلومات إضافية: تعرف التدفق على واجهة تم تكوينها لوضع NGIPS وتم تطبيق خدمات NGIPS المرحلة: 4 النوع: قائمة الوصول النوع الفرعي: سجل النتيجة: قطرة 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: وصول: FTD4100 - من إزالي/1 access-list CSM_FW_ACL_ ملاحظة rule- id 268441600: قاعدة L4: القاعدة 1 معلومات إضافية: النتيجة: واجهة الإدخال: داخل حالة الإدخال: معي حالة خط الإدخال: معي الإجراء: قطرة سبب الإسقاط: (ACL-drop) تم رفض التدفق بواسطة القاعدة التي تم تكوينها تم عرض حزمة واحدة >	التكوين: قاعدة مضمنة معلومات إضافية: قائمة الوصول إلى MAC المرحلة: 3 النوع: وضع NGIPS النوع الفرعي: وضع NGIPS النتيجة: سماح التكوين: معلومات إضافية: تعرف التدفق على واجهة تم تكوينها لوضع NGIPS وتم تطبيق خدمات NGIPS المرحلة: 4 النوع: قائمة الوصول النوع الفرعي: سجل النتيجة: كان سياسة 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: وصول: FTD4100 - من إزالي/1 access-list CSM_FW_ACL_ ملاحظة rule- id 268441600: قاعدة L4: القاعدة 1 معلومات إضافية: النتيجة: واجهة الإدخال: داخل حالة الإدخال: معي حالة خط الإدخال: معي الإجراء: قطرة مكن إسقاط كان الوصول، ولكن تمت إعادة توجيه الحزمة بسبب الضغط الداخلي تم عرض حزمة واحدة >

ملخص

- عندما تستخدم وضع الوزج في السطر، تمر الحزمة بشكل رئيسي من خلال محرك نخر 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 الوزج 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 معدلة.

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).