Configurazione delle interfacce FTD in modalità Inline-Pair

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati
- Prodotti correlati

Premesse

Configura interfaccia a coppia inline su FTD

- Esempio di rete

Verifica

Verifica funzionamento interfaccia a coppia inline FTD

- Teoria base
- Verifica 1. Con l'uso di Packet-Tracer
- Verifica 2. Invio dei pacchetti TCP SYN/ACK tramite una coppia inline
- Verifica 3. Debug Del Motore Firewall Per Il Traffico Autorizzato
- Verifica 4. Verifica della propagazione dello stato del collegamento
- Verifica 5. Configurare un NAT statico
- Caso di studio: traffico asimmetrico attraverso set inline

Blocca pacchetto in modalità interfaccia a coppia inline

Configura La Modalità Inline Pair Con Tap

Verifica coppia inline FTD con funzionamento interfaccia tap

Coppia inline ed Etherchannel

- Etherchannel terminato su FTD
- Etherchannel tramite FTD

Risoluzione dei problemi

Confronto: Doppino inline e coppia inline con tap

Riepilogo

Introduzione

In questo documento viene descritta la configurazione, la verifica e il funzionamento di un'interfaccia a coppia inline su un accessorio Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower 4112 FTD (codice 7.x)
- Firepower Management Center (FMC) (codice 7.x)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

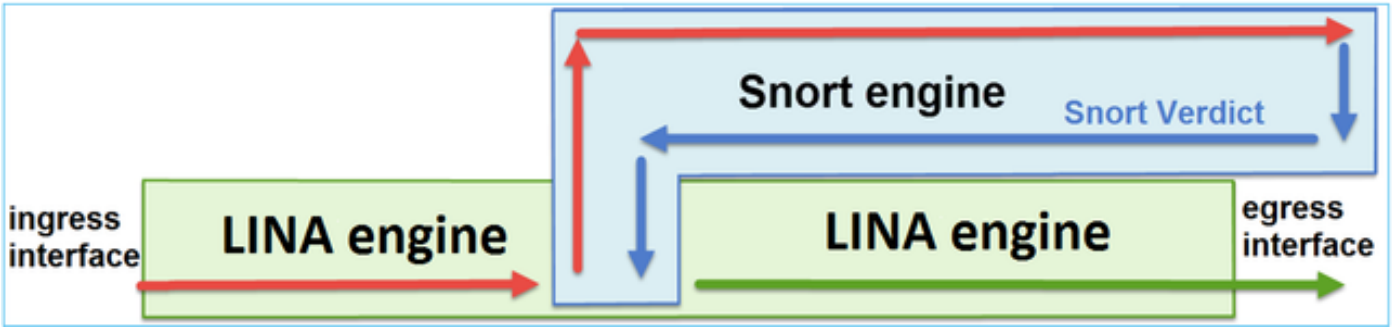
- FPR1000, FPR2100, FPR4100, FPR9300
- Secure Firewall serie 3100 e 4200
- vFTD
- Codice software FTD 6.2.x e versioni successive

Premesse

FTD è un'immagine software unificata costituita da 2 motori principali:

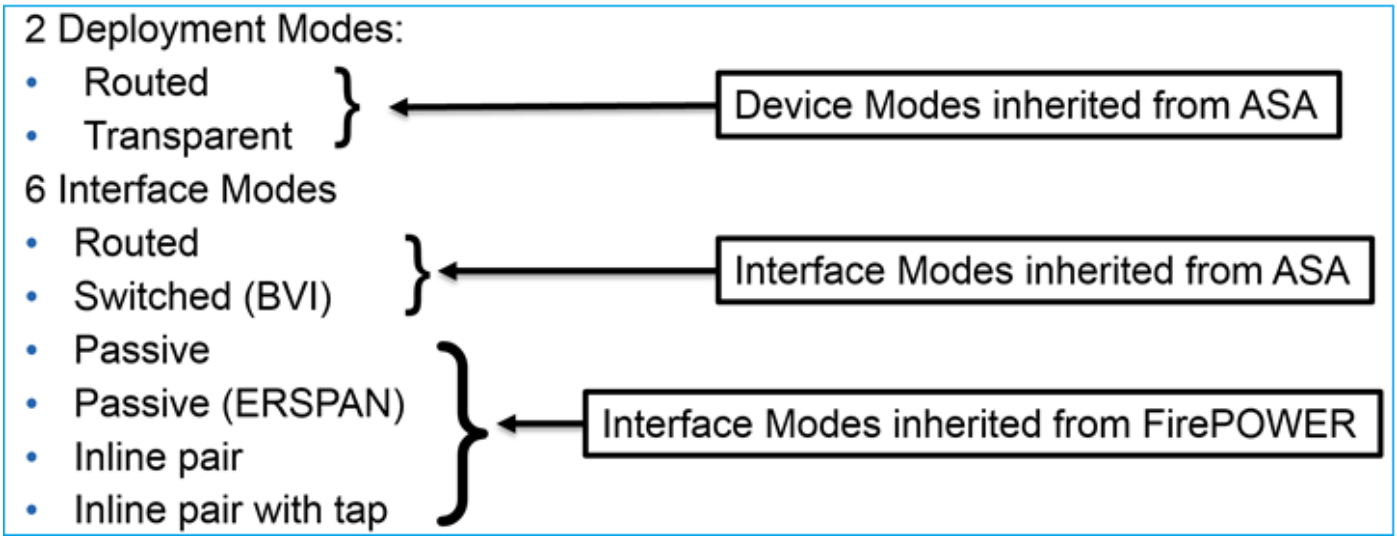
1. Motore LINA
2. Motore Snort

Questa figura mostra il rapporto tra i 2 motori:



- Il pacchetto entra dall'interfaccia di ingresso e viene gestito dal motore LINA.
- Se richiesto dalla policy FTD, il pacchetto viene ispezionato dal motore Snort.
- Il motore Snort restituisce un verdetto per il pacchetto.
- In base a questo verdetto, il motore LINA elimina il pacchetto o lo inoltra.

FTD fornisce due modalità di distribuzione e sei modalità di interfaccia, come mostrato nell'immagine:



Nota: È possibile utilizzare diverse modalità di interfaccia su un unico accessorio FTD.

Di seguito è riportata una panoramica di alto livello delle diverse modalità di distribuzione FTD e interfaccia:

Modalità interfaccia FTD	Modalità di distribuzione FTD	Descrizione	Il traffico può essere interrotto
Stesura	Stesura	Controlli completi dei motori LINA e Snort.	Sì
Commutato	Trasparente	Controlli completi dei motori LINA e Snort.	Sì
Coppia inline	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort.	Sì
Coppia inline con tap	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort.	No
Passive	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort.	No
Passivo	Stesura	Controlli parziali del motore LINA	No

(ERSPAN)		e completi del motore Snort.	

Configura interfaccia a coppia inline su FTD

Esempio di rete

Requisito

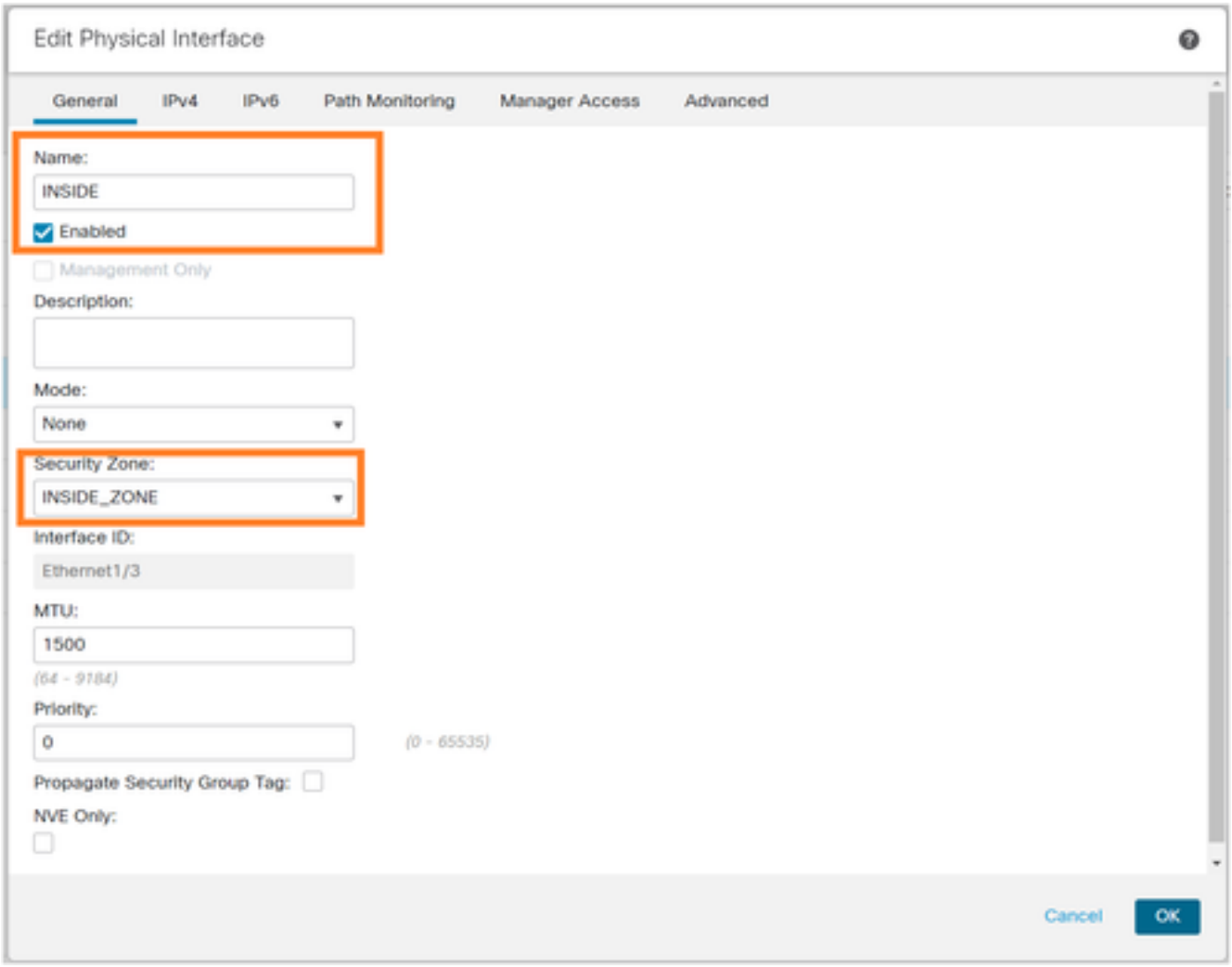
Configurare le interfacce fisiche e1/3 ed e1/4 in modalità Inline Pair come indicato nei seguenti requisiti:

Interfaccia	e1/3	e1/4
Nome	INTERNO	ESTERNO
Area di sicurezza	AREA_INTERNA	AREA_ESTERNA
Nome set inline	Inline-Pair-1	
MTU impostata inline	1500	
Propaga stato collegamento	Attivato	

Soluzione

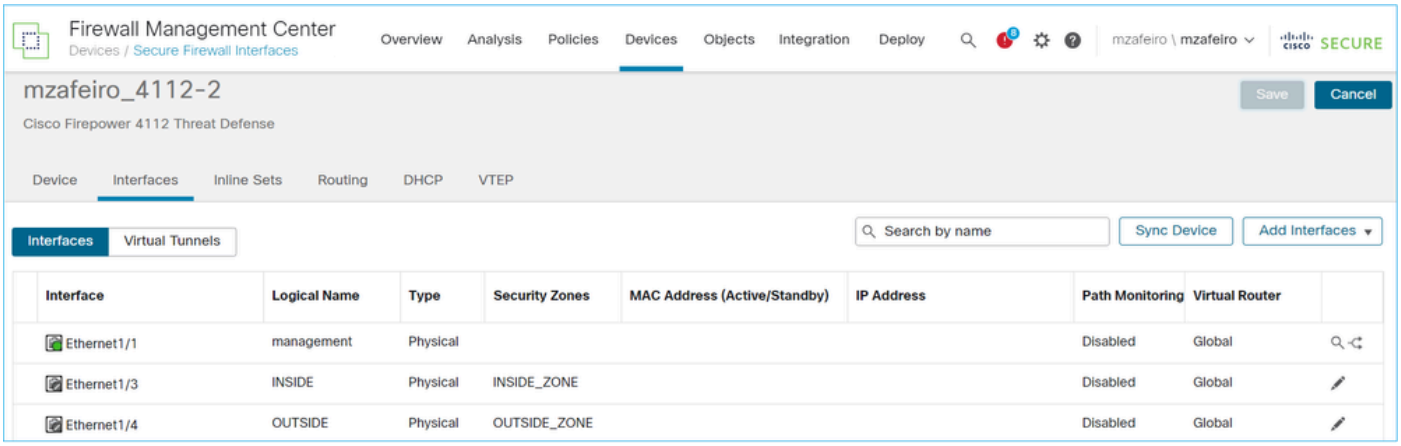
Passaggio 1. Per configurare le singole interfacce, passare a Dispositivi > Gestione dispositivi, selezionare il dispositivo appropriato e selezionare Modifica:

Quindi, specificare Name e selezionare Enabled (Abilitato) per l'interfaccia, come mostrato nell'immagine.



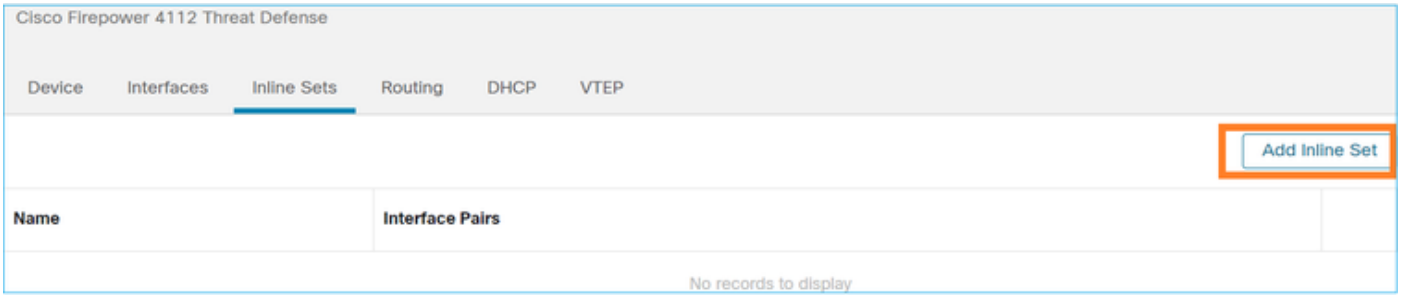
Nota: Name è il nome dell'interfaccia.

Analogamente, per l'interfaccia Ethernet1/4. Viene mostrato il risultato finale:

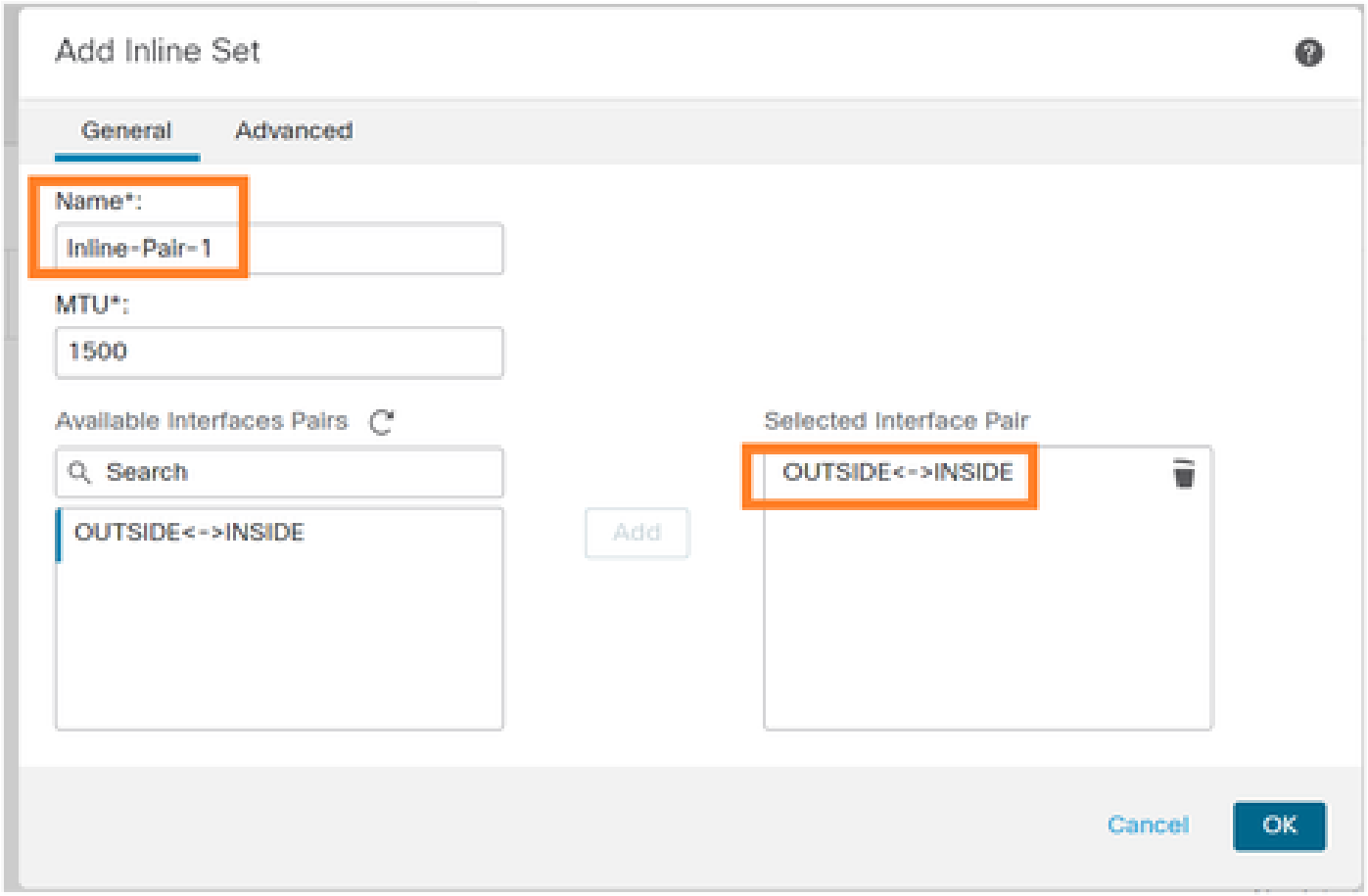


Passaggio 2. Configurare la coppia inline.

Passate a Insiemi in linea (Inline Sets) > Aggiungi insieme in linea (Add Inline Set) come mostrato nell'immagine.



Passaggio 3. Configurare le impostazioni generali in base ai requisiti come mostrato nell'immagine.



Passaggio 4. Abilitare l'opzione Propaga stato collegamento nelle Impostazioni avanzate come mostrato nell'immagine.

La propagazione dello stato del collegamento riduce automaticamente la seconda interfaccia nella coppia di interfacce inline quando una delle interfacce nel set inline diventa inattiva.

Passaggio 5. Salvare le modifiche e distribuire.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Verificare la configurazione della coppia inline dalla CLI FTD.

Soluzione

Accedere alla CLI FTD e verificare la configurazione della coppia inline:

<#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
```

Nota: L'ID gruppo bridge è un valore diverso da 0. Se Modalità tocco è attiva, il valore è 0.

Informazioni sull'interfaccia e sul nome:

<#root>

```
firepower#

show nameif


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

Verificare lo stato dell'interfaccia:

<#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
```

Verificare le informazioni sull'interfaccia fisica:

<#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
```

Verifica funzionamento interfaccia a coppia inline FTD

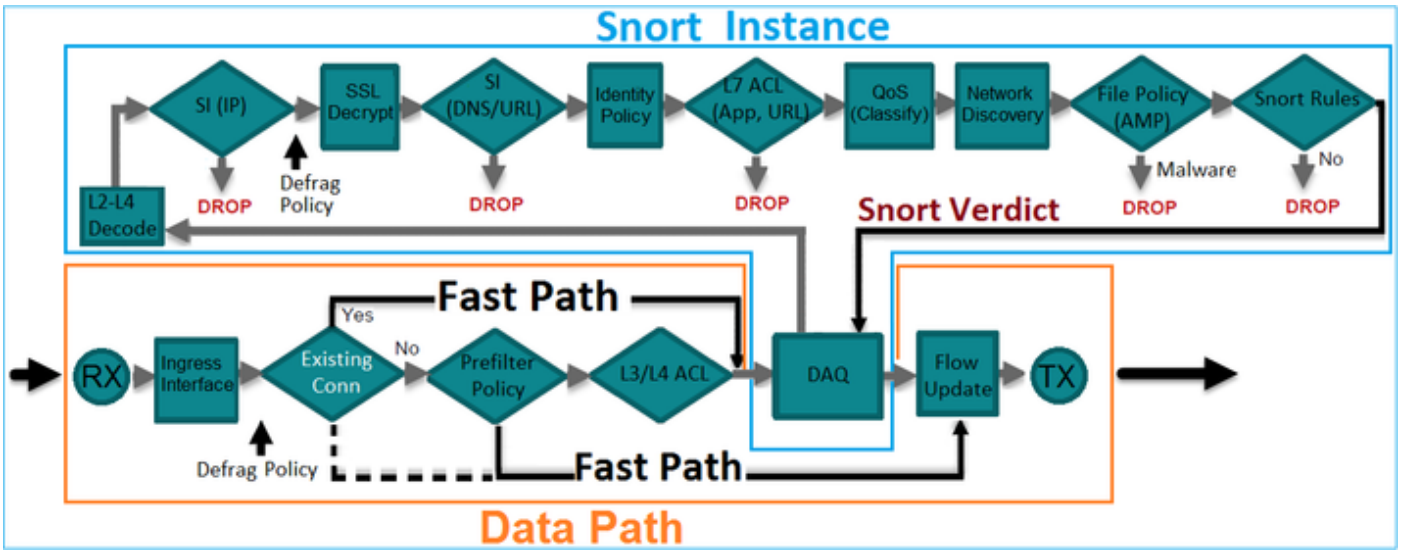
In questa sezione vengono illustrati i controlli di verifica per verificare il funzionamento di Inline Pair:

- Verifica 1. Con l'uso di packet-tracer.
- Verifica 2. Abilita l'acquisizione con traccia e invia un pacchetto di sincronizzazione/conferma TCP (SYN/ACK) tramite la coppia inline.
- Verifica 3. Monitoraggio del traffico FTD con l'utilizzo del debug del motore del firewall
- Verifica 4. Verificare la funzionalità di propagazione dello stato del collegamento.
- Verifica 5. Configurare NAT (Static Network Address Translation).

Soluzione

Panoramica dell'architettura

Quando due interfacce FTD funzionano in modalità Inline-pair, viene gestito un pacchetto, come mostrato nell'immagine.

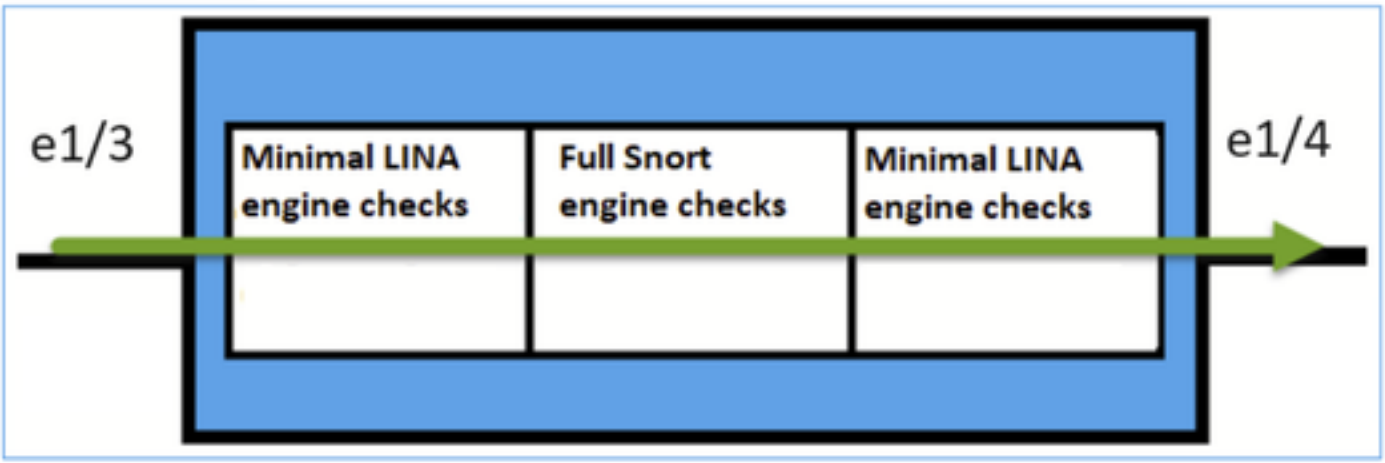


Nota: Solo le interfacce fisiche possono essere membri di un set di coppie inline.

Teoria base

- Quando si configura una coppia inline 2 fisica, le interfacce vengono collegate internamente.
- Molto simile al classico IPS (Intrusion Prevention System) in linea.
- Disponibile in modalità di distribuzione instradata o trasparente.
- La maggior parte delle funzionalità del motore LINA (NAT, Routing e così via) non è disponibile per i flussi che passano attraverso una coppia inline.
- Il traffico di transito può essere scartato.
- Alcuni controlli del motore LINA vengono applicati insieme a controlli completi del motore Snort.

L'ultimo punto può essere visualizzato come mostrato nell'immagine:



Verifica 1. Con l'uso di Packet-Tracer

L'output packet-tracer che emula un pacchetto che attraversa la coppia inline con i punti importanti

evidenziati:

<#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
```

Verifica 2. Invio dei pacchetti TCP SYN/ACK tramite una coppia inline

È possibile generare pacchetti TCP SYN/ACK con l'uso di un pacchetto che crea un'utilità come Scapy. Questa sintassi genera 3 pacchetti con flag SYN/ACK abilitati:

<#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)
```

Abilitare questa acquisizione sulla CLI FTD e inviare alcuni pacchetti 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
```

Le clip mostrano che i pacchetti SYN/ACK 3 attraversano l'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
```

La traccia del primo pacchetto di acquisizione rivela alcune informazioni aggiuntive come il verdetto del motore Snort:

<#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
```

La traccia del secondo pacchetto acquisito mostra che il pacchetto corrisponde a una connessione corrente, quindi ignora il controllo ACL, ma viene comunque ispezionato dal motore Snort:

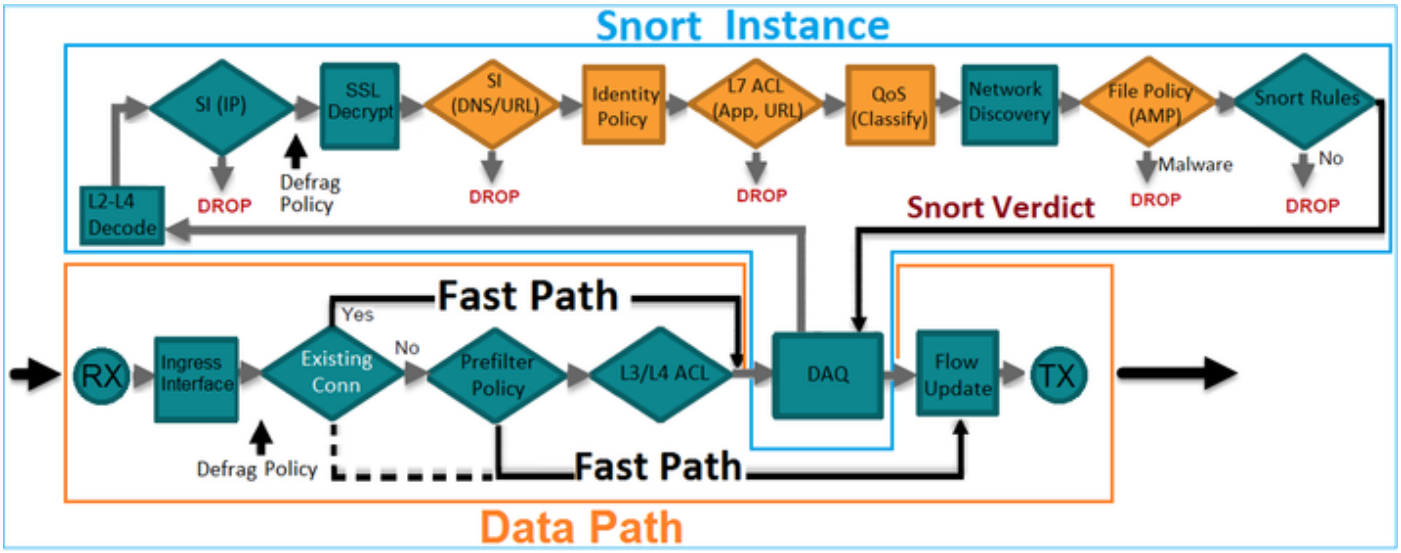
<#root>

```
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
```

Verifica 3. Debug Del Motore Firewall Per Il Traffico Autorizzato

Il debug del motore del firewall viene eseguito su componenti specifici del motore dello snort FTD, ad esempio i criteri di controllo dell'accesso, come mostrato nell'immagine:



Quando si inviano i pacchetti TCP SYN/ACK tramite Inline Pair, è possibile vedere nell'output del comando debug:

<#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
```

Verifica 4. Verifica della propagazione dello stato del collegamento

Abilitare il buffer log su FTD e chiudere la porta dello switch collegata all'interfaccia e1/4. Dalla CLI di FTD, è necessario notare che entrambe le interfacce sono disabilitate:

<#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
```

I log FTD mostrano:

<#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
```

Lo stato inline-set mostra lo stato dei due membri dell'interfaccia:

<#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
```

Si noti la differenza nello stato delle due interfacce:

<#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
```

Dopo aver riattivato la porta dello switch, nei log FTD vengono visualizzati:

<#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
```

Verifica 5. Configurare un NAT statico

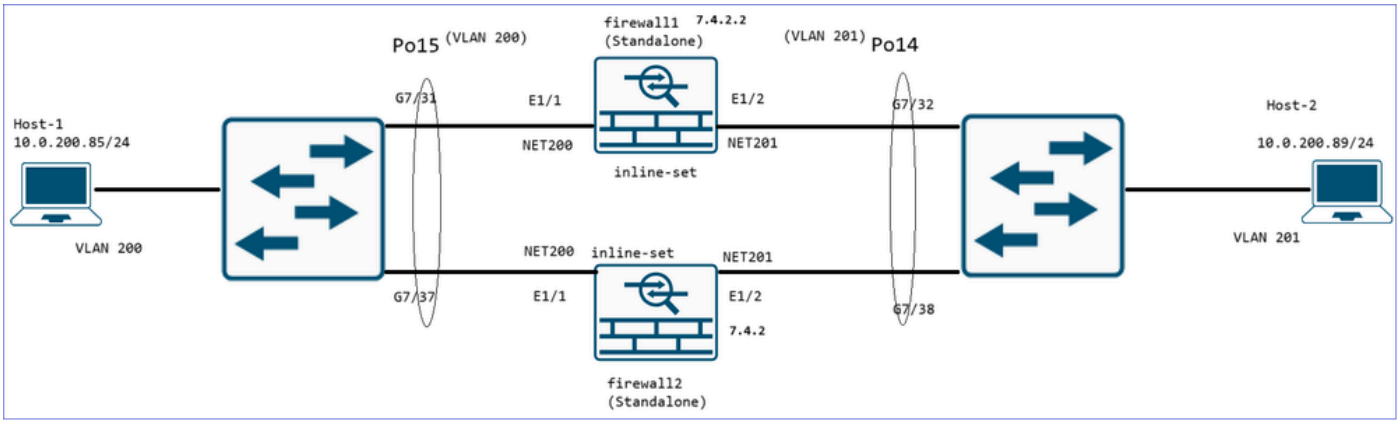
Soluzione

NAT non è supportato per le interfacce che operano in modalità inline, inline tap o passive:

[Guida alla configurazione di Firepower Management Center, versione 6.0.1]

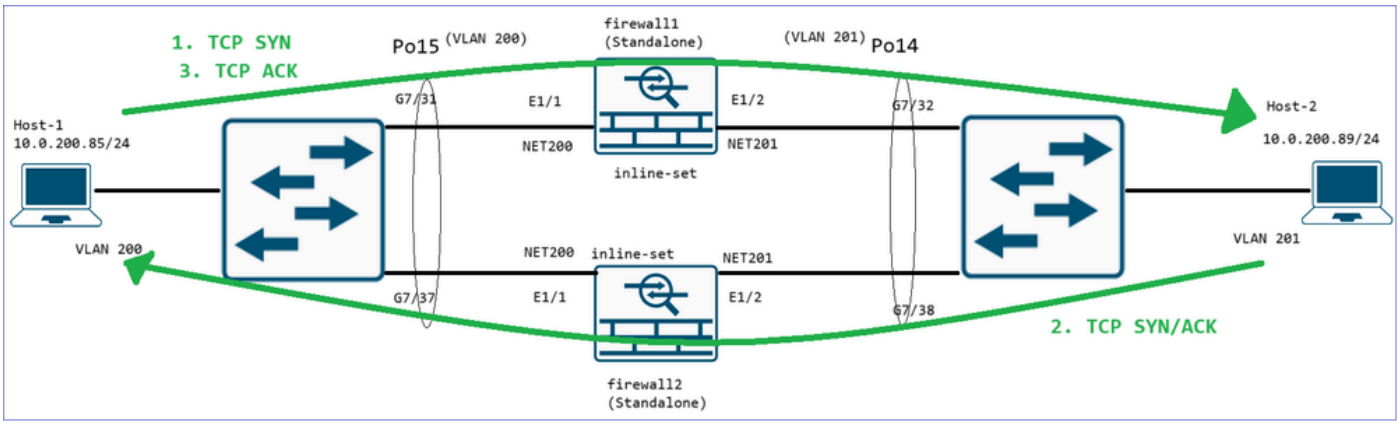
Caso di studio: traffico asimmetrico attraverso set inline

Considerare questo scenario:



I due firewall funzionano in modalità standalone (possono anche eseguire versioni software diverse), ma gestiscono il traffico proveniente dalle stesse interfacce porta-canale.

In questo caso, il traffico può essere asimmetrico a causa dell'algoritmo di bilanciamento del carico del canale della porta:



1. L'host 1 (10.0.200.85) invia una SYN TCP verso l'host 2 (10.0.200.89). Questo pacchetto attraversa il firewall1.
2. L'host 2 (10.0.200.89) invia un messaggio TCP SYN/ACK verso l'host 2 (10.0.200.85). Questo pacchetto attraversa il firewall 2.
3. L'handshake TCP a 3 vie viene completato con l'host 1 che invia un ACK TCP verso l'host 2. Questo pacchetto attraversa il firewall 1.

Dal punto di vista dell'host 1, la connessione è stata stabilita correttamente:

<#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]
```

L'acquisizione dei pacchetti sul firewall1 mostra solo il traffico dall'host 1 all'host 2:

<#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
```

Il contenuto dell'acquisizione:

<#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
...
```

L'acquisizione dei pacchetti sul firewall2 mostra solo il traffico dall'host 2 all'host 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
...
```

I syslog sul firewall1 mostrano che il pacchetto TCP SYN ha creato una connessione TCP di bypass dello stato:

<#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)
```

Sul firewall2, il pacchetto TCP SYN/ACK ha anche creato una connessione TCP di bypass dello stato:

<#root>

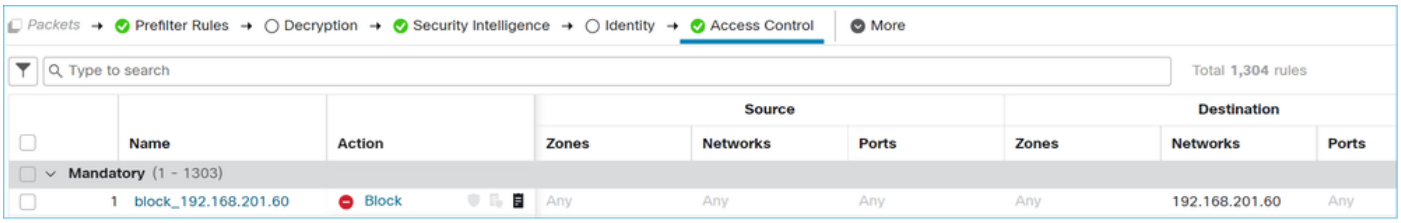
```
FTD1010-12#

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)
```

Considerazioni principali

- Il traffico asimmetrico funziona attraverso un set inline di dispositivi firewall diversi poiché entrambi i dispositivi gestiscono la connessione TCP in modalità TCP di ignoramento dello stato.
- Notare che il bypass dello stato TCP non è configurato manualmente sui firewall, ma è il risultato dell'operazione dell'interfaccia inline-set.

Blocca pacchetto in modalità interfaccia a coppia inline

Creare una regola di blocco, inviare il traffico attraverso la coppia inline FTD e osservare il comportamento, come mostrato nell'immagine.



Soluzione

Abilita l'acquisizione con trace e invia i pacchetti SYN/ACK tramite la coppia inline FTD. Il traffico è bloccato:

<#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
```

Nella traccia, si può vedere che il pacchetto è stato scartato dal motore LINA FTD e non è stato inoltrato al motore Snort 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
```

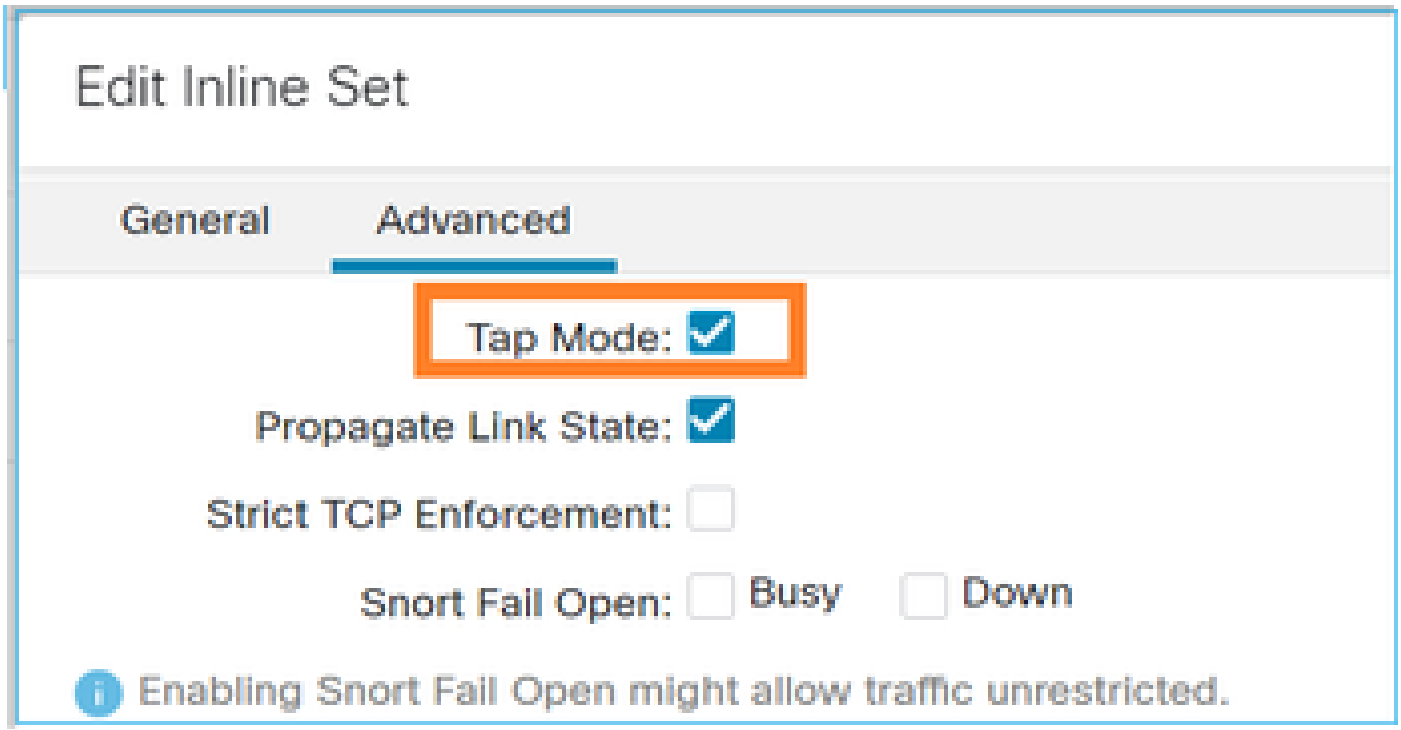
```
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 10126 ns
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

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
```

Configura La Modalità Inline Pair Con Tap

Abilitare la modalità Tap sulla coppia inline.

Soluzione

Passare a Dispositivi > Gestione periferiche > Insiemi in linea > Modifica insieme in linea > Avanzate e attivare la modalità maschiatura, come mostrato nell'immagine.



Verifica

<#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
```

Verifica coppia inline FTD con funzionamento interfaccia tap

Teoria base

- Quando si configura una coppia inline con tap, le interfacce fisiche vengono collegate internamente tramite bridge.
- È disponibile in modalità di distribuzione instradata o trasparente.
- La maggior parte delle funzionalità del motore LINA (NAT, Routing e così via) non sono disponibili per i flussi che passano attraverso la coppia in linea.
- Impossibile eliminare il traffico effettivo.
- Alcuni controlli del motore LINA vengono applicati insieme a controlli completi del motore Snort su una copia del traffico effettivo.

L'opzione Inline Pair with Tap Mode (Accoppia inline con modalità tap) non elimina il traffico di transito. Con la traccia di un pacchetto conferma questo:

<#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
```

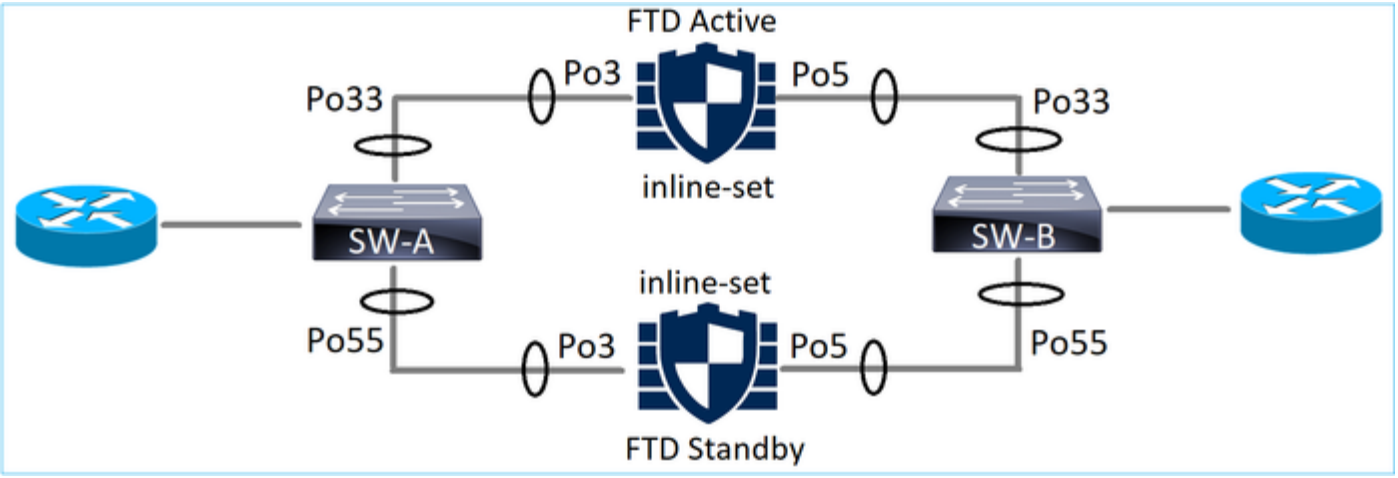
```
Subtype: log
Result: WOULD HAVE DROPPED

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
>
```

Coppia inline ed Etherchannel

È possibile configurare una coppia inline con etherchannel in 2 modi:

1. Etherchannel terminato su FTD.
2. Etherchannel passa attraverso il FTD (richiede il codice FXOS 2.3.1.3 e versioni successive).

Etherchannel terminato su FTD



Etherchannel su 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)
```

Etherchannel su 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)
```

Il traffico viene inoltrato tramite l'FTD attivo in base all'apprendimento dell'indirizzo 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
```

Il set in linea su FTD:

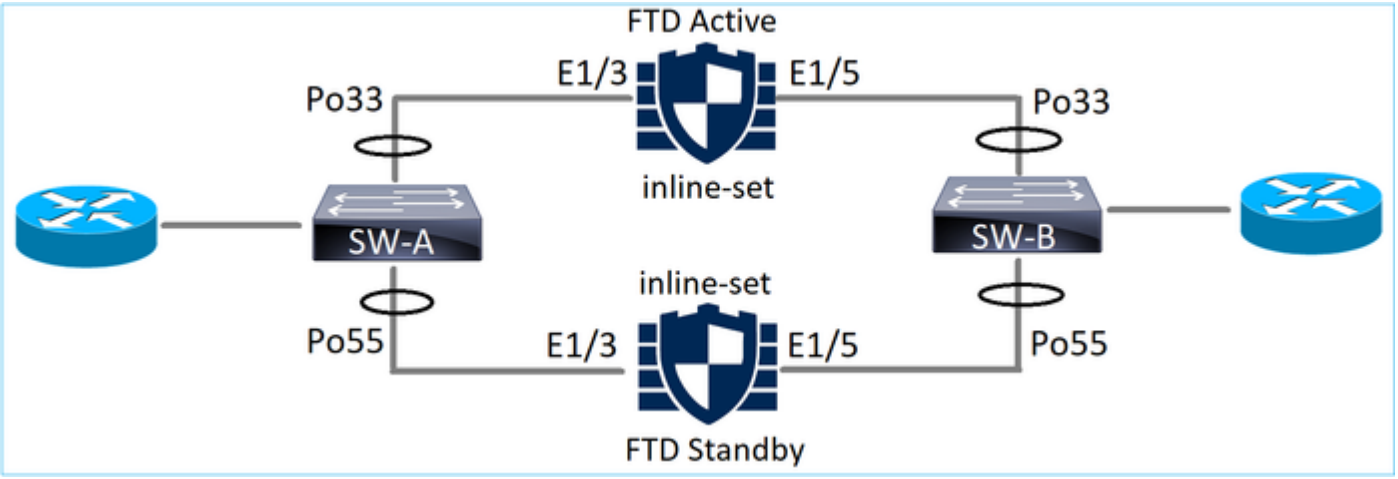
<#root>

```
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
```

Nota: In caso di evento di failover FTD, l'interruzione del traffico dipende principalmente dal tempo impiegato dagli switch per conoscere l'indirizzo MAC del peer remoto.

Etherchannel tramite FTD



Etherchannel su 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)
```

I pacchetti LACP attraverso l'FTD standby sono bloccati:

<#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
```

Etherchannel su 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)
```

Il traffico viene inoltrato tramite l'FTD attivo in base all'apprendimento dell'indirizzo 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
```

Il set in linea su 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
```

⚠ Attenzione: In questo scenario, nel caso di un evento di failover FTD, il tempo di convergenza dipende principalmente dalla negoziazione LACP Etherchannel e dal tempo necessario per l'interruzione, che può essere molto più lungo. Se la modalità Etherchannel è impostata su ON (nessun LACP), il tempo di convergenza dipende dall'apprendimento dell'indirizzo MAC.

Risoluzione dei problemi

Nessuna informazione specifica disponibile per questa configurazione.

Confronto: Doppino inline e coppia inline con tap

	Coppia inline	Coppia inline con tap
show inline-set	> show inline-set Inline-set Inline-Pair-1 Mtu è 1500 byte La modalità Failsafe è attivata/attivata La modalità di protezione da errori è disattivata Modalità maschiatura disattivata Opzione Propagate-link-state attivata	> show inline-set Inline-set Inline-Pair-1 Mtu è 1500 byte La modalità Failsafe è attivata/attivata La modalità di protezione da errori è disattivata Modalità tocco attivata Opzione Propagate-link-state attivata

	la modalità di bypass dell'hardware è disabilitata Interface-Pair[1]: Interfaccia: Ethernet 1/6 "INTERNA" Current-Status: ATTIVO Interfaccia: Ethernet 1/8 "ESTERNO" Current-Status: ATTIVO ID gruppo bridge: 509 >	la modalità di bypass dell'hardware è disabilitata Interface-Pair[1]: Interfaccia: Ethernet 1/6 "INTERNA" Current-Status: ATTIVO Interfaccia: Ethernet 1/8 "ESTERNO" Current-Status: ATTIVO ID gruppo bridge: 0 >
show interface	> show interface e1/6 Interfaccia Ethernet1/6 "INSIDE", attiva, protocollo di linea attivo L'hardware è EtherSVI, BW 1000 Mbps, DLY 1000 usec Indirizzo MAC 5897.bdb9.770e, MTU 1500 Modalità interfaccia IPS: inline, Inline-Set: Inline-Pair-1 Indirizzo IP non assegnato Statistiche sul traffico per "INSIDE": Ingresso pacchetti 3957, 264913 byte 144 pacchetti in uscita, 5864 byte 4 pacchetti ignorati Velocità di ingresso di 1 minuto 0 pkt/sec, 26 byte/sec Velocità di uscita di 1 minuto 0 pkt/sec, 7 byte/sec cadute di 1 minuto, 0 pkt/sec Velocità di ingresso di 5 minuti 0 pkt/sec, 28 byte/sec Velocità di uscita di 5 minuti 0 pkt/sec, 9 byte/sec cadute di 5 minuti, 0 pkt/sec > show interface e1/8 Interface Ethernet1/8 "OUTSIDE", è attivo, il protocollo di linea è attivo L'hardware è EtherSVI, BW 1000 Mbps, DLY 1000 usec Indirizzo MAC 5897.bdb9.774d, MTU 1500 Modalità interfaccia IPS: inline, Inline-Set: Inline-Pair-1	> show interface e1/6 Interfaccia Ethernet1/6 "INSIDE", attiva, protocollo di linea attivo L'hardware è EtherSVI, BW 1000 Mbps, DLY 1000 usec Indirizzo MAC 5897.bdb9.770e, MTU 1500 Modalità interfaccia IPS: tocco in linea, Inline-Set: Inline-Pair-1 Indirizzo IP non assegnato Statistiche sul traffico per "INSIDE": 24 pacchetti di input, 1378 byte 0 pacchetti di output, 0 byte 24 pacchetti ignorati Velocità di input di 1 minuto: 0 pkt/sec, 0 byte/sec Velocità di uscita di 1 minuto 0 pkt/sec, 0 byte/sec cadute di 1 minuto, 0 pkt/sec Velocità di ingresso di 5 minuti 0 pkt/sec, 0 byte/sec Velocità di uscita di 5 minuti 0 pkt/sec, 0 byte/sec cadute di 5 minuti, 0 pkt/sec > show interface e1/8 Interface Ethernet1/8 "OUTSIDE", è attivo, il protocollo di linea è attivo L'hardware è EtherSVI, BW 1000 Mbps, DLY 1000 usec Indirizzo MAC 5897.bdb9.774d, MTU 1500 Modalità interfaccia IPS: tocco in linea, Inline-Set: Inline-Pair-1 Indirizzo IP non assegnato

	Indirizzo IP non assegnato Statistiche traffico per "ALL'ESTERNO": 144 pacchetti in ingresso, 55634 byte 3954 pacchetti in uscita, 39987 byte 0 pacchetti ignorati Velocità di ingresso di 1 minuto 0 pkt/sec, 7 byte/sec Velocità di uscita di 1 minuto 0 pkt/sec, 37 byte/sec cadute di 1 minuto, 0 pkt/sec Velocità di ingresso di 5 minuti 0 pkt/sec, 8 byte/sec Velocità di uscita di 5 minuti 0 pkt/sec, 39 byte/sec cadute di 5 minuti, 0 pkt/sec >	Statistiche traffico per "ALL'ESTERNO": 1 pacchetto di input, 441 byte 0 pacchetti di output, 0 byte 1 pacchetto scartato Velocità di input di 1 minuto: 0 pkt/sec, 0 byte/sec Velocità di uscita di 1 minuto 0 pkt/sec, 0 byte/sec cadute di 1 minuto, 0 pkt/sec Velocità di ingresso di 5 minuti 0 pkt/sec, 0 byte/sec Velocità di uscita di 5 minuti 0 pkt/sec, 0 byte/sec cadute di 5 minuti, 0 pkt/sec >
Per gestire il pacchetto con la regola di blocco	> show capture CAPI packet-number 1 trace 3 pacchetti acquisiti 1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192 Fase: 1 Tipo: ACQUISIRE Sottotipo: Risultato: Allow (Autorizza) Config: Ulteriori informazioni: Elenco accessi MAC Fase: 2 Tipo: ACCESS-LIST Sottotipo: Risultato: Allow (Autorizza) Config: Regola implicita Ulteriori informazioni: Elenco accessi MAC Fase: 3 Tipo: MODALITÀ NGIPS	> show capture CAPI packet-number 1 trace 3 pacchetti acquisiti 1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192 Fase: 1 Tipo: ACQUISIRE Sottotipo: Risultato: Allow (Autorizza) Config: Ulteriori informazioni: Elenco accessi MAC Fase: 2 Tipo: ACCESS-LIST Sottotipo: Risultato: Allow (Autorizza) Config: Regola implicita Ulteriori informazioni: Elenco accessi MAC Fase: 3 Tipo: MODALITÀ NGIPS Sottotipo: modalità ngips

	Sottotipo: modalità ngips Risultato: Allow (Autorizza) Config: Ulteriori informazioni: Il flusso in ingresso è un'interfaccia configurata per la modalità NGIPS e vengono applicati i servizi NGIPS Fase: 4 Tipo: ACCESS-LIST Sottotipo: registro Risultato: DROP Config: access-group CSM_FW_ACL_ globale access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-start access-list CSM_FW_ACL_ note rule-id 268441600: CRITERI DI ACCESSO: FTD4100 - Obbligatorio/1 access-list CSM_FW_ACL_ note rule-id 268441600: REGOLA L4: Regola 1 Ulteriori informazioni: Risultato: interfaccia di ingresso: INTERNO stato-input: attivo stato della linea di ingresso: attivo Azione: drop Motivo di rilascio: (acl-drop) Flusso negato dalla regola configurata 1 pacchetto visualizzato >	Risultato: Allow (Autorizza) Config: Ulteriori informazioni: Il flusso in ingresso è un'interfaccia configurata per la modalità NGIPS e vengono applicati i servizi NGIPS Fase: 4 Tipo: ACCESS-LIST Sottotipo: registro Risultato: SAREBBE CADUTO Config: access-group CSM_FW_ACL_ globale access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-start access-list CSM_FW_ACL_ note rule-id 268441600: CRITERI DI ACCESSO: FTD4100 - Obbligatorio/1 access-list CSM_FW_ACL_ note rule-id 268441600: REGOLA L4: Regola 1 Ulteriori informazioni: Risultato: interfaccia di ingresso: INTERNO stato-input: attivo stato della linea di ingresso: attivo Azione: L'elenco degli accessi sarebbe stato scartato, ma il pacchetto sarebbe stato inoltrato a causa della connessione in linea 1 pacchetto visualizzato >

Riepilogo

- Quando si usa la modalità Inline Pair, il pacchetto passa principalmente attraverso il motore Snort FTD.
- Le connessioni TCP vengono gestite in modalità TCP state-bypass.
- Dal punto di vista di un motore LINA FTD, viene applicato un criterio ACL.
- Quando è in uso la modalità Inline Pair, i pacchetti possono essere bloccati perché vengono elaborati in linea.
- Quando la modalità tap è abilitata, una copia del pacchetto viene ispezionata e scartata

internamente, mentre il traffico effettivo attraversa l'FTD senza modifiche.

Informazioni correlate

- Cisco Firepower NGFW
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione
Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).