Configurazione delle interfacce FTD in modalità Inline-Pair

Sommario

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 4150 FTD (codice 6.1.0.x e 6.3.x)
- Firepower Management Center (FMC) (codice 6.1.0.x e 6.3.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:

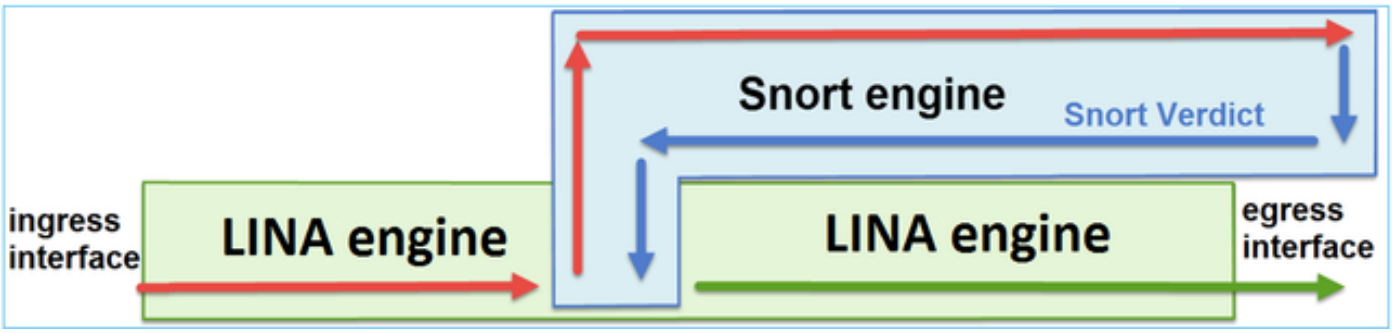
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- Codice software FTD 6.2.x e versioni successive

Premesse

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

- Motore LINA
- Motore Snort

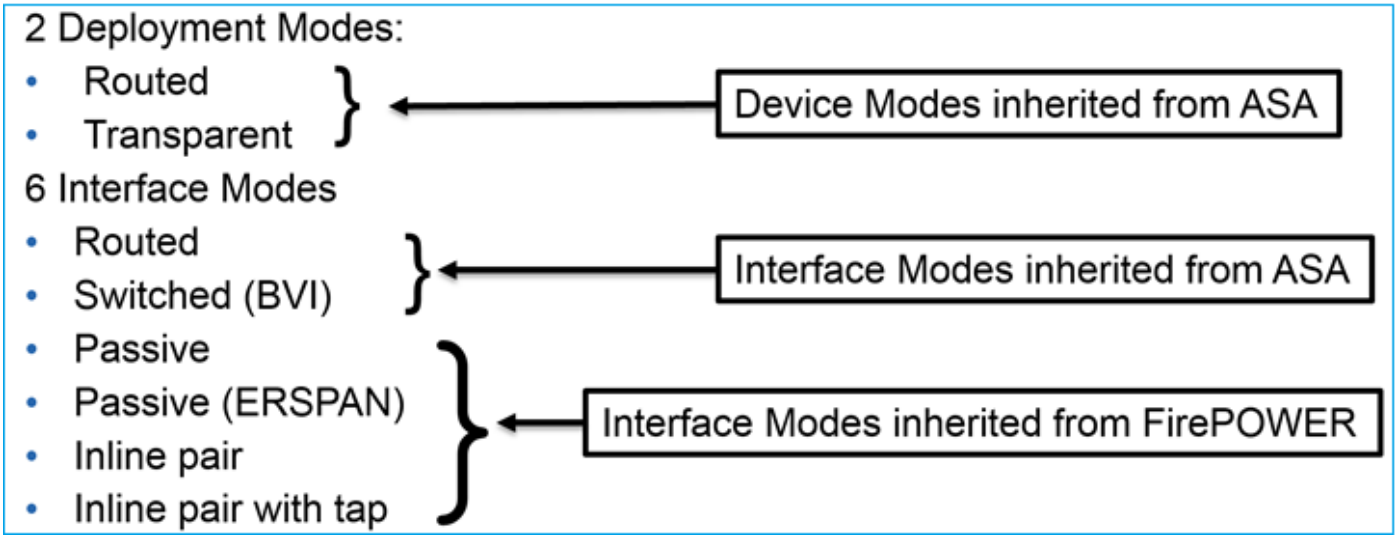
Questa figura mostra il rapporto tra i 2 motori:



- 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 più modalità di interfaccia su un unico accessorio FTD.

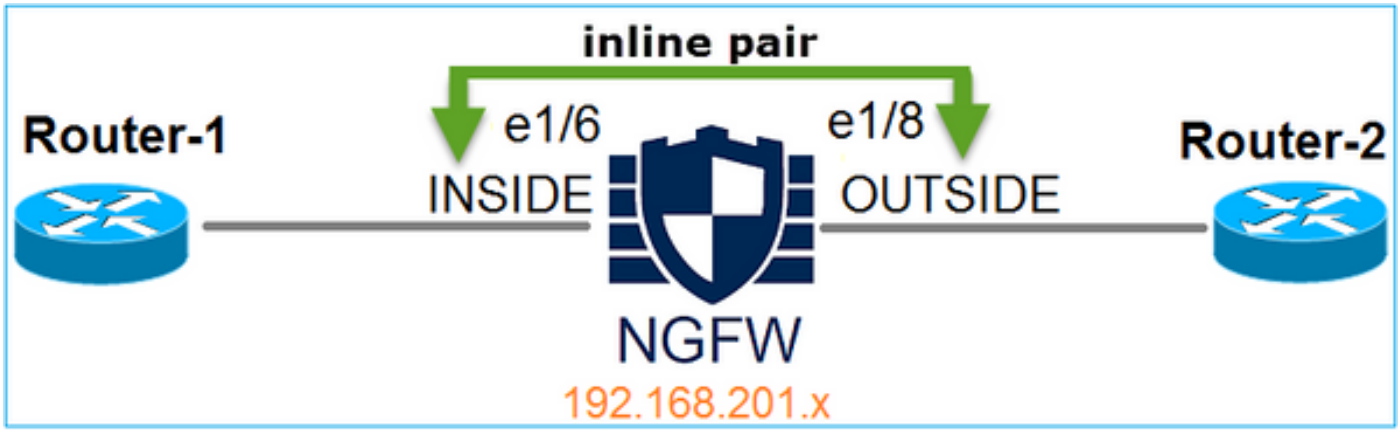
Di seguito è riportata una panoramica di alto livello delle diverse modalità di distribuzione FTD e interfaccia:

Modalità interfaccia FTD	Modalità di distribuzione FTD	Descrizione	Il traffico può essere interrotto
Stesura	Stesura	Controlli completi del motore LINA e del motore Snort	Sì
Commutato	Trasparente	Controlli completi del motore LINA e del motore 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
Passivo	Routed o	Controlli parziali del motore LINA	No

	Transparent	e completi del motore Snort	
Passivo (ERSPAN)	Stesura	Controlli parziali del motore LINA e completi del motore Snort	No

Configura interfaccia a coppia inline su FTD

Esempio di rete



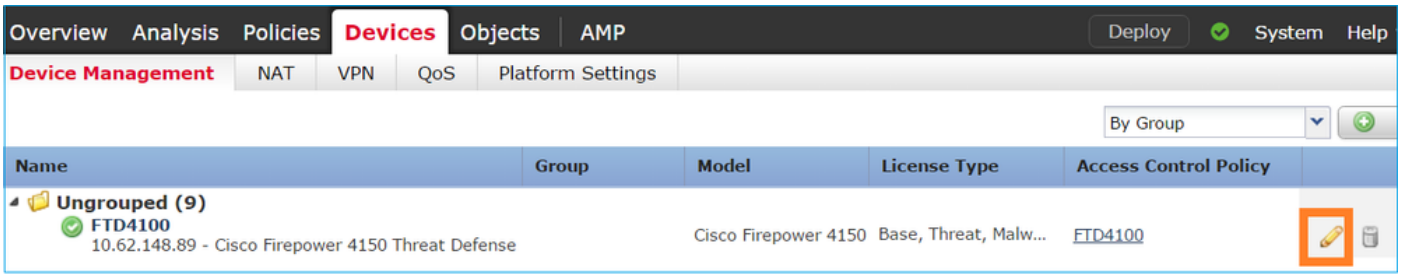
Requisito

Configurare le interfacce fisiche e1/6 e e1/8 in modalità Inline Pair come indicato nei seguenti requisiti:

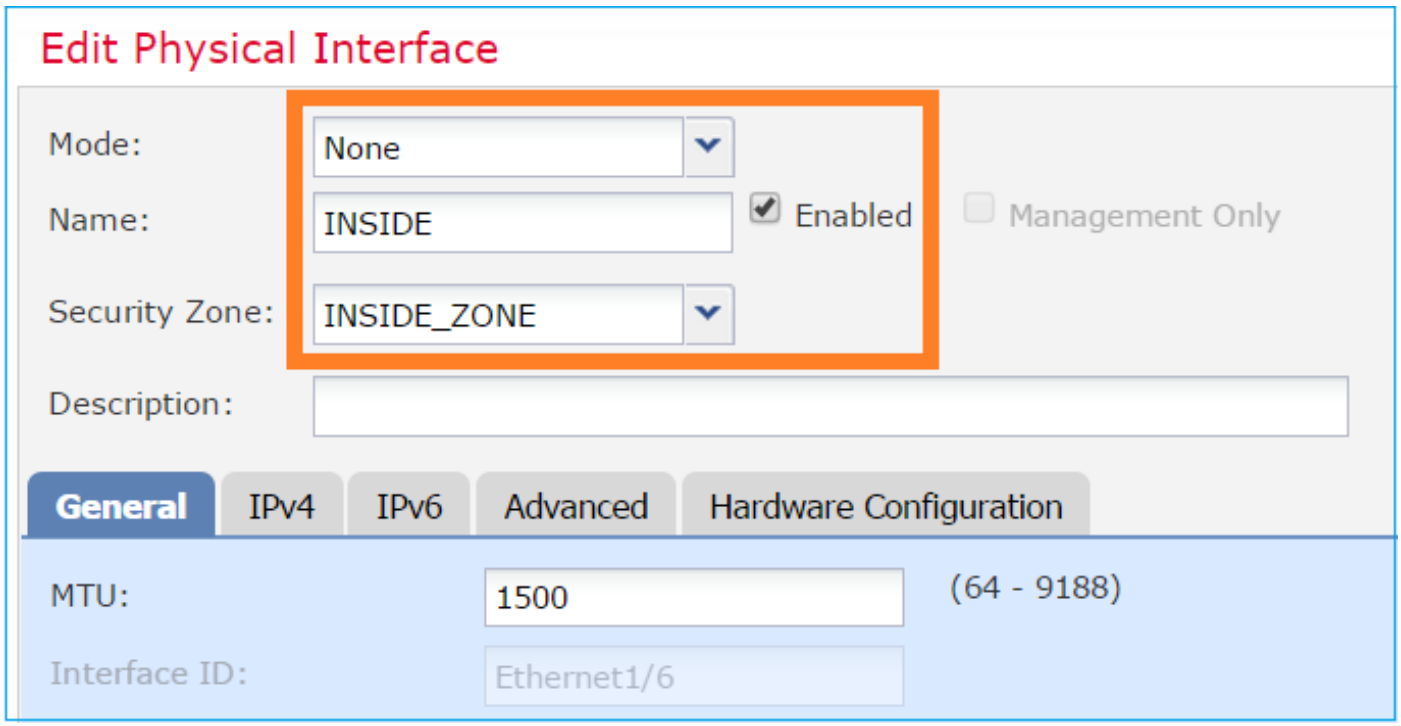
Interfaccia	e1/6	e1/8
Nome	INTERNO	ESTERNO
Area di sicurezza	AREA_INTERNA	AREA_ESTERNA
Nome set inline	Inline-Pair-1	
MTU impostata inline	1500	
FailSafe	Attivato	
Propaga stato collegamento	Attivato	

Soluzione

Passaggio 1. Per configurare le singole interfacce, selezionare Dispositivi > Gestione dispositivi, selezionare il dispositivo appropriato e selezionare Modifica, come mostrato nell'immagine.

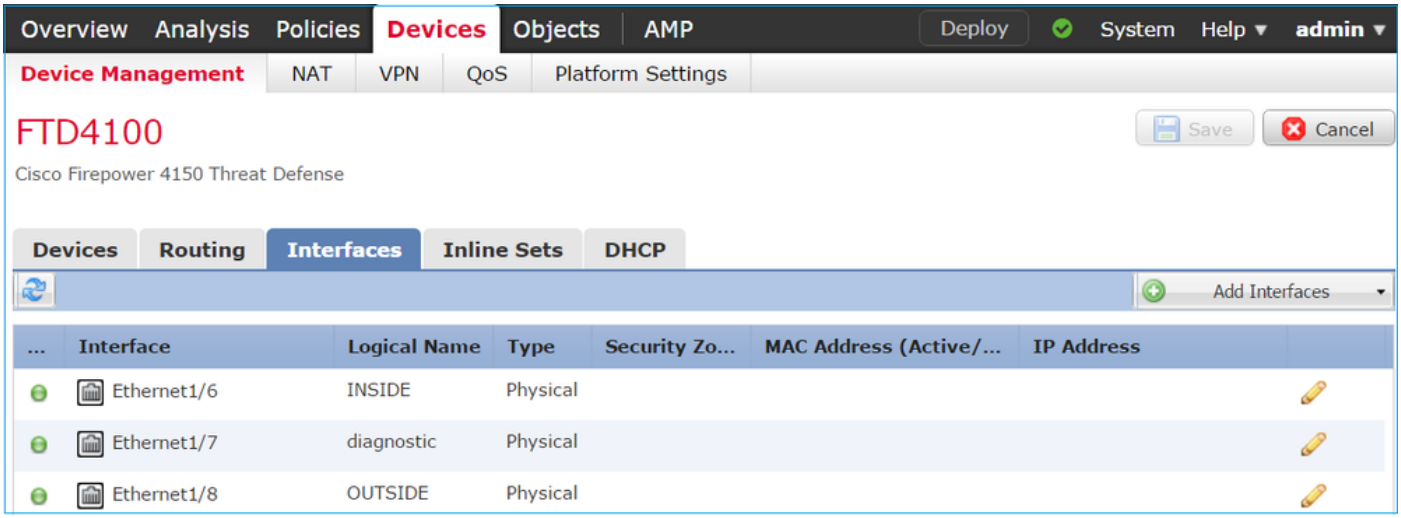


Quindi, specificare Name e Tick Enabled (Nome e Tick attivati) per l'interfaccia, come mostrato nell'immagine.



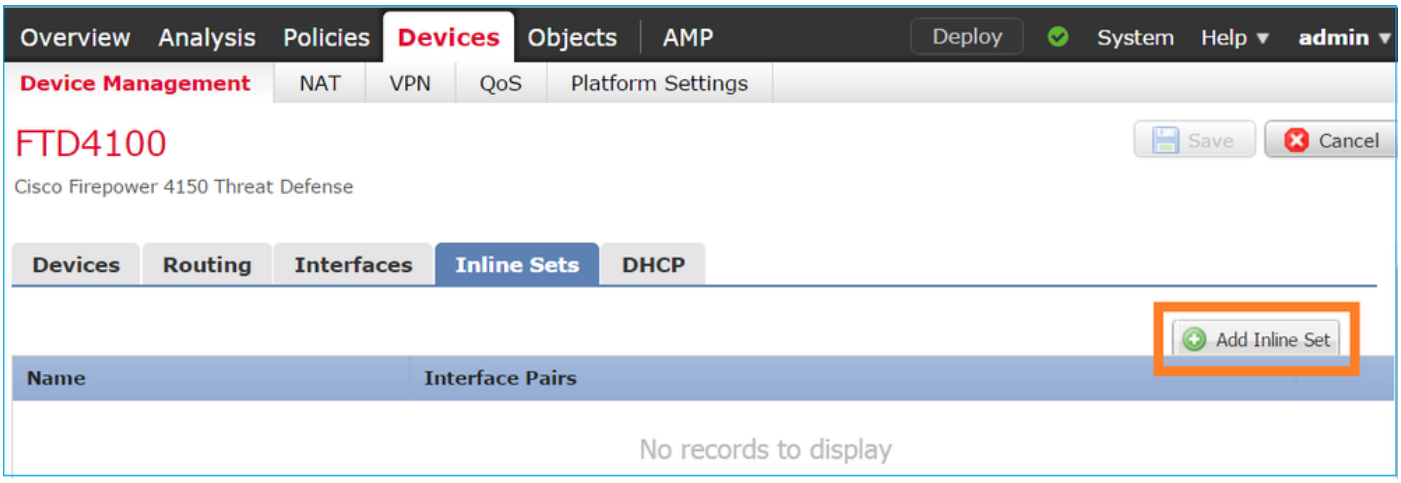
Nota: Name è il nome dell'interfaccia.

Analogamente, all'interfaccia Ethernet1/8. Il risultato finale è quello mostrato nell'immagine.

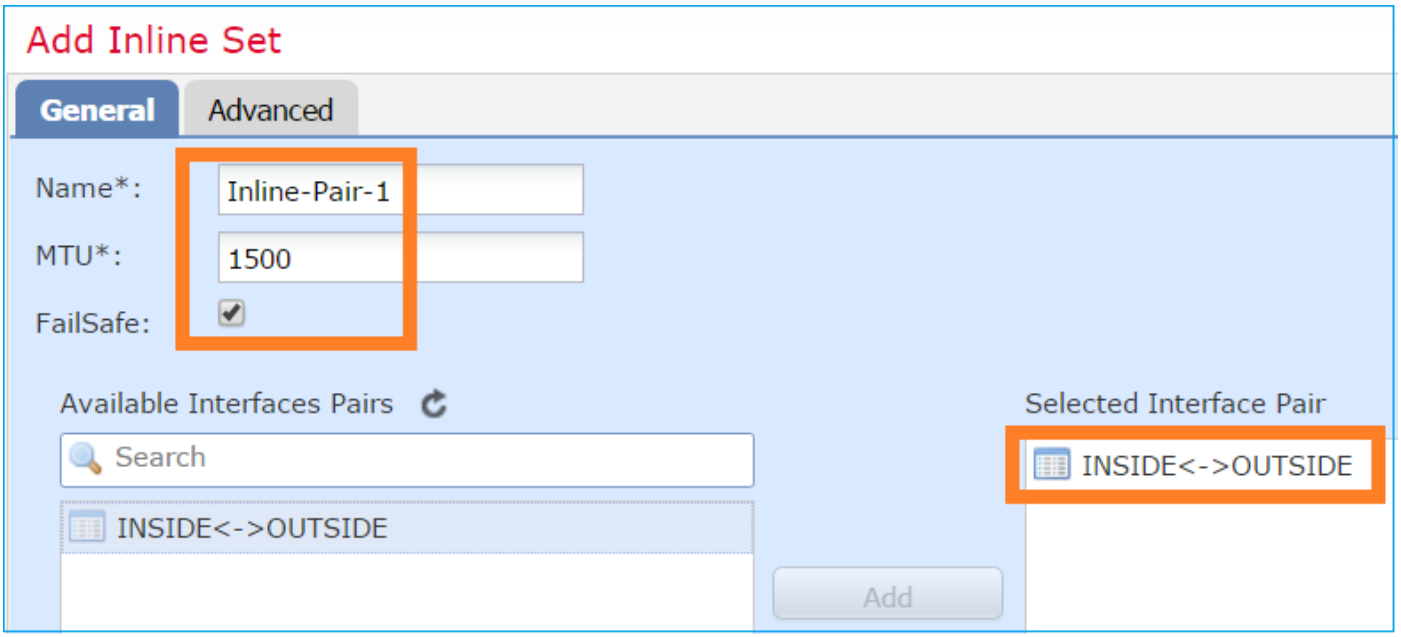


Passaggio 2. Configurare la coppia inline.

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

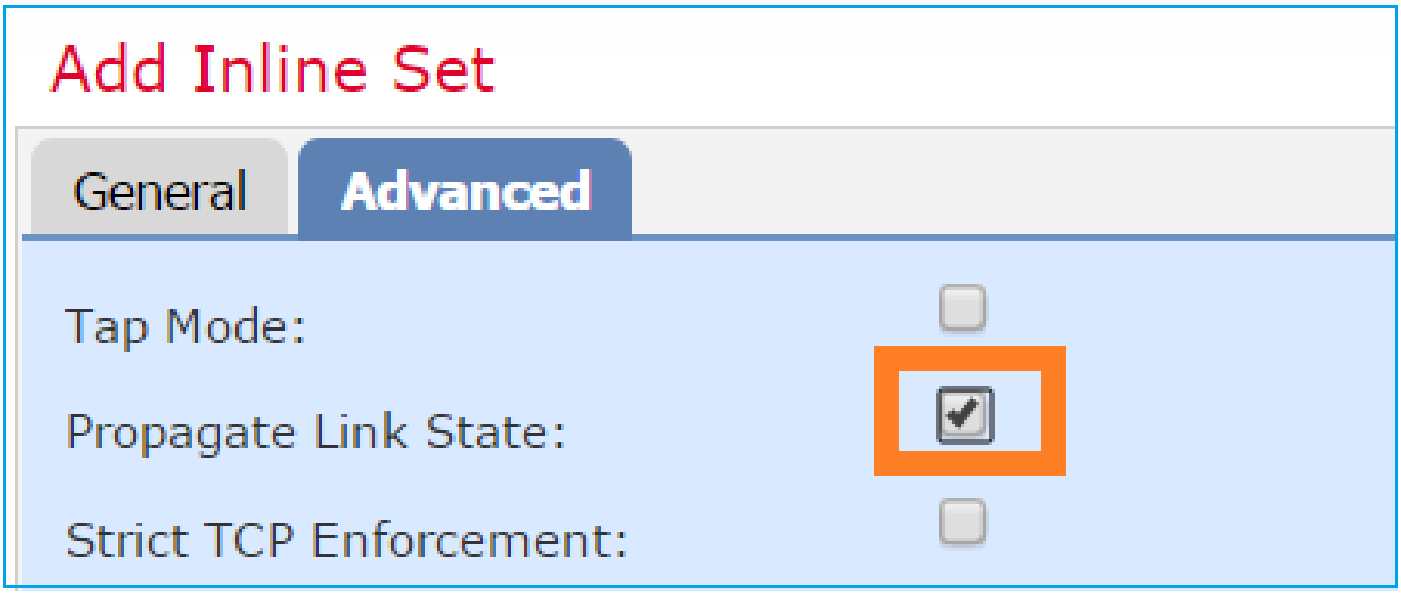


Passaggio 3. Configurare le impostazioni generali in base ai requisiti, come mostrato nell'immagine.



Nota: Failsafe consente il passaggio del traffico attraverso la coppia inline senza essere ispezionata nel caso in cui i buffer dell'interfaccia siano pieni (in genere rilevati quando il dispositivo è sovraccarico o il motore Snort è sovraccarico). Le dimensioni del buffer dell'interfaccia vengono allocate dinamicamente.

Passaggio 4. Abilitare l'opzione Propagate Link State (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:

```
> 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
>
```

Nota: l'ID del gruppo di bridge è un valore diverso da 0. Se la modalità maschiatura è attiva, è 0

Informazioni sull'interfaccia e sul nome:

```
<#root>

>

show nameif

Interface                   Name                    Security
Ethernet1/6                 INSIDE                    0

Ethernet1/7                 diagnostic                0
Ethernet1/8                 OUTSIDE                   0

>
```

Verificare lo stato dell'interfaccia:

```
<#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
```

Verificare le informazioni sull'interfaccia fisica:

```
<#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
>
```

Verifica funzionamento interfaccia a coppia inline FTD

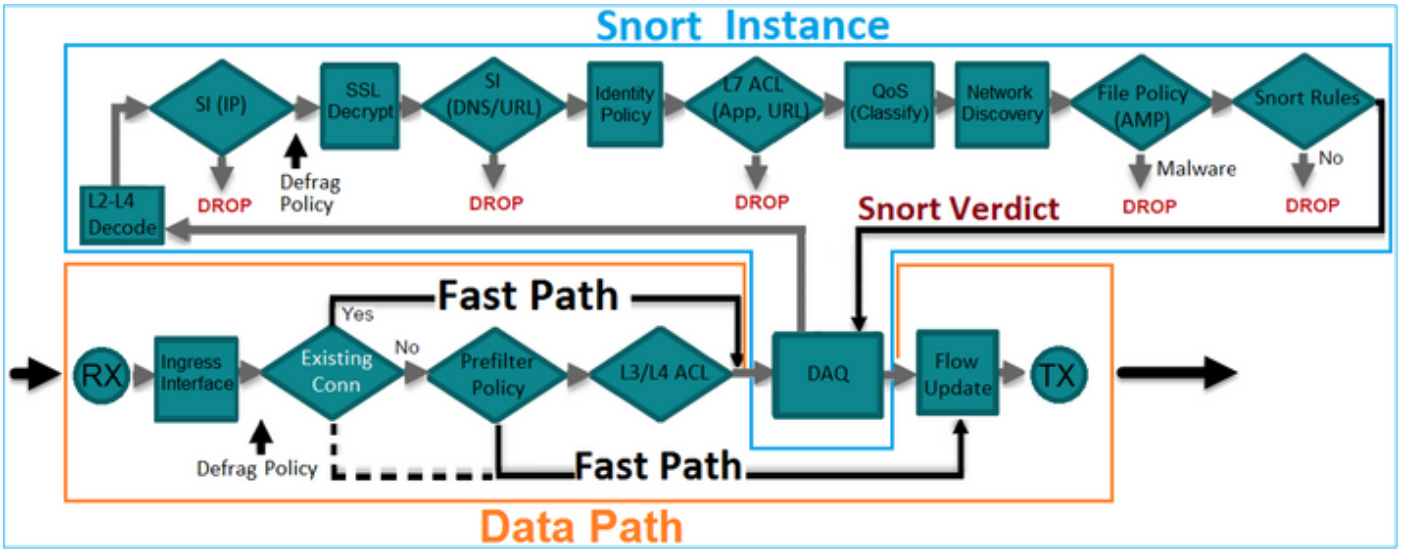
In questa sezione vengono illustrati i controlli di verifica per verificare il funzionamento di Inline Pair:

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

Soluzione

Panoramica dell'architettura

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

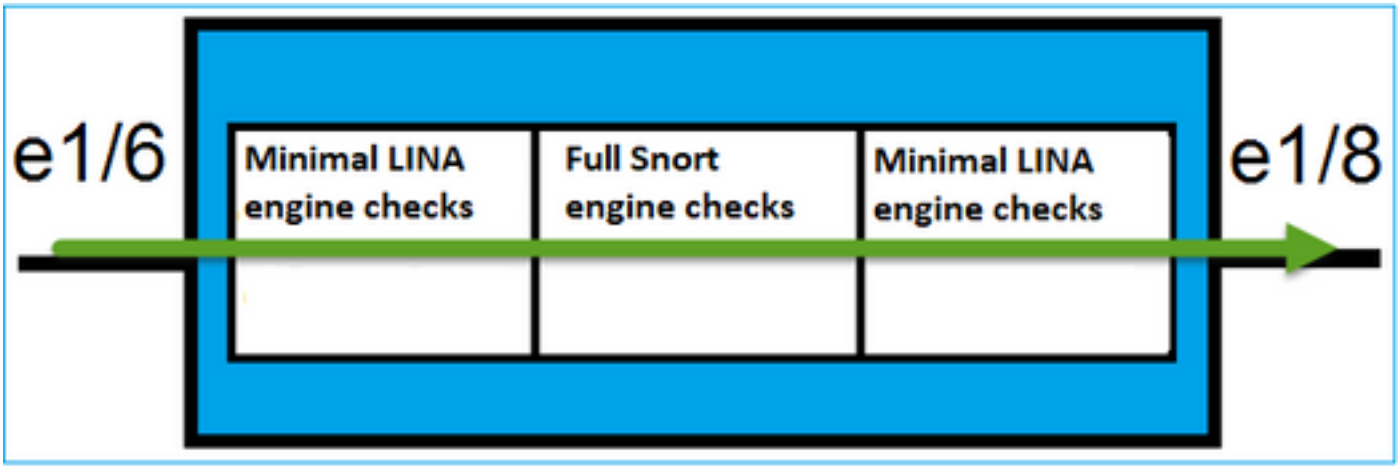


Nota: solo le interfacce fisiche possono essere membri di un set di coppie inline

Teoria base

- Quando si configura una coppia inline 2, le interfacce fisiche 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 ai 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>

>

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

>

Verifica 2. Invia pacchetti TCP SYN/ACK tramite 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>

>

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


>
```

Dopo aver inviato i pacchetti tramite l'FTD, è possibile vedere una connessione che è stata creata:

```
<#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

>
```

Nota: b flag: un'appliance ASA classica rifiuta un pacchetto SYN/ACK non richiesto a meno che non sia stato abilitato il bypass dello stato TCP. Un'interfaccia FTD in modalità Inline Pair gestisce una connessione TCP in modalità di bypass dello stato TCP e non elimina i pacchetti TCP che non appartengono alle connessioni già esistenti.

Nota: flag N - Il pacchetto viene ispezionato dal motore Snort FTD.

Le clip lo provano, dal momento che si possono vedere i 3 pacchetti che attraversano l'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
>

3 pacchetti escono dal dispositivo 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
>
```

Con la traccia del primo pacchetto di acquisizione rivelano alcune informazioni aggiuntive come il verdetto del motore Snort:

<#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
>
```

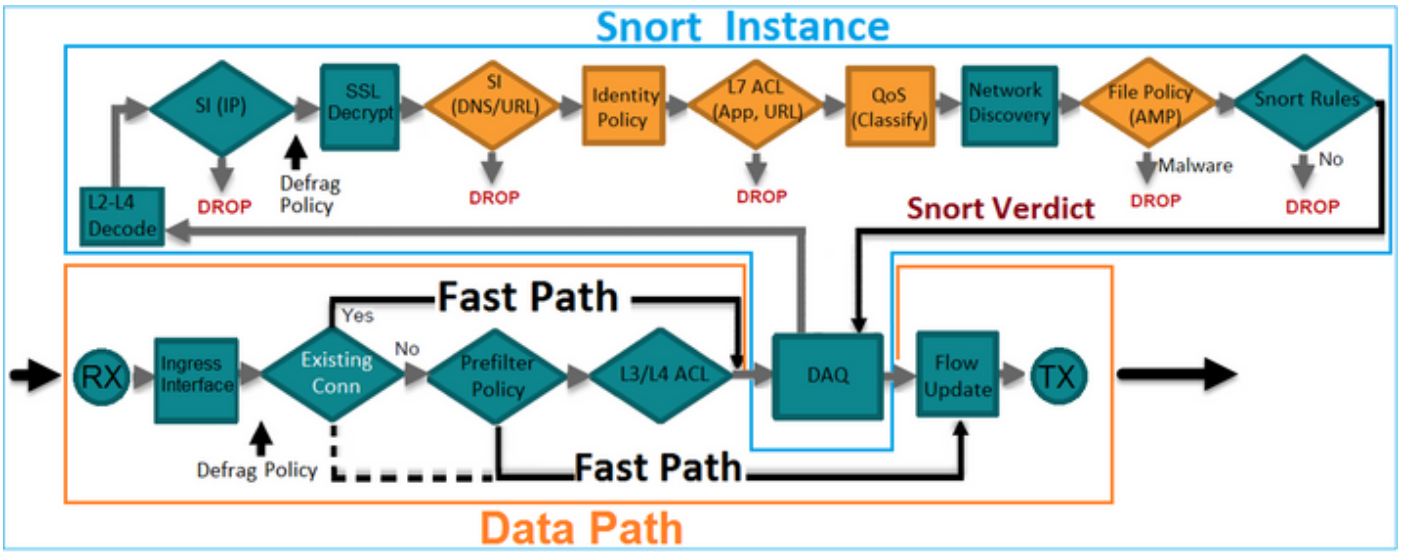
Quando la traccia del secondo pacchetto acquisito mostra che il pacchetto corrisponde a una connessione corrente, quindi ignora il controllo ACL, ma viene comunque ispezionato dal motore Snort:

```
<#root>

>

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
>
```

Verifica 3. Debug Del Motore Firewall Per Il Traffico Consentito

Il debug del motore del firewall viene eseguito su componenti specifici del motore dello snort FTD come 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 e1/6. Dalla CLI del FTD è necessario notare che entrambe le interfacce sono disabilitate:

```
<#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


>
```

I log FTD mostrano:

```
<#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
>
```

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

```
<#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
>
```

Si noti la differenza nello stato delle due interfacce:

```
<#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
>
```

E per l'interfaccia 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
>
```

Dopo aver riattivato switchport, i log FTD mostrano:

```
<#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

>
```

Verifica 5. Configurazione NAT statico

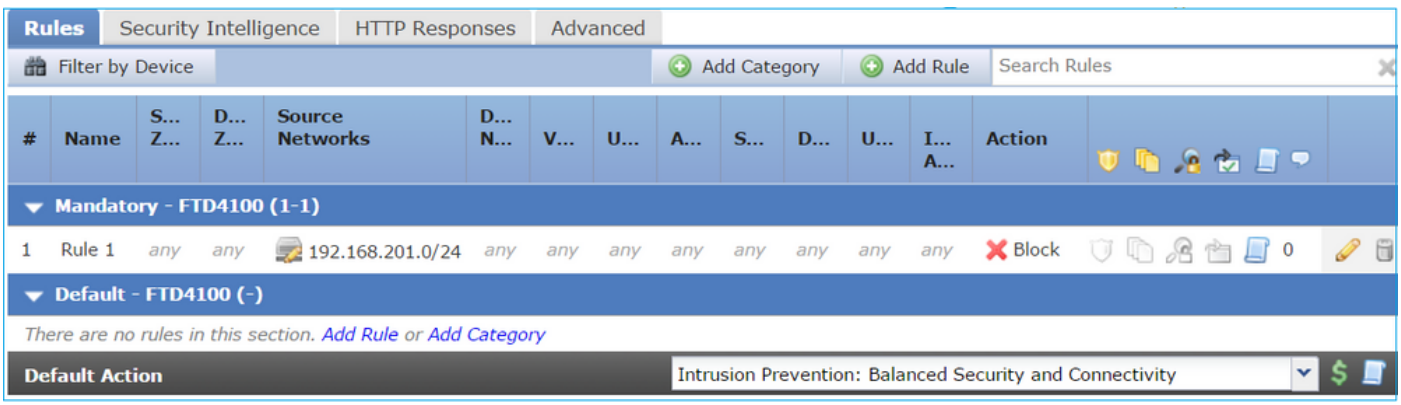
Soluzione

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

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

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>

>

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

Con la traccia, un pacchetto rivela:

<#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

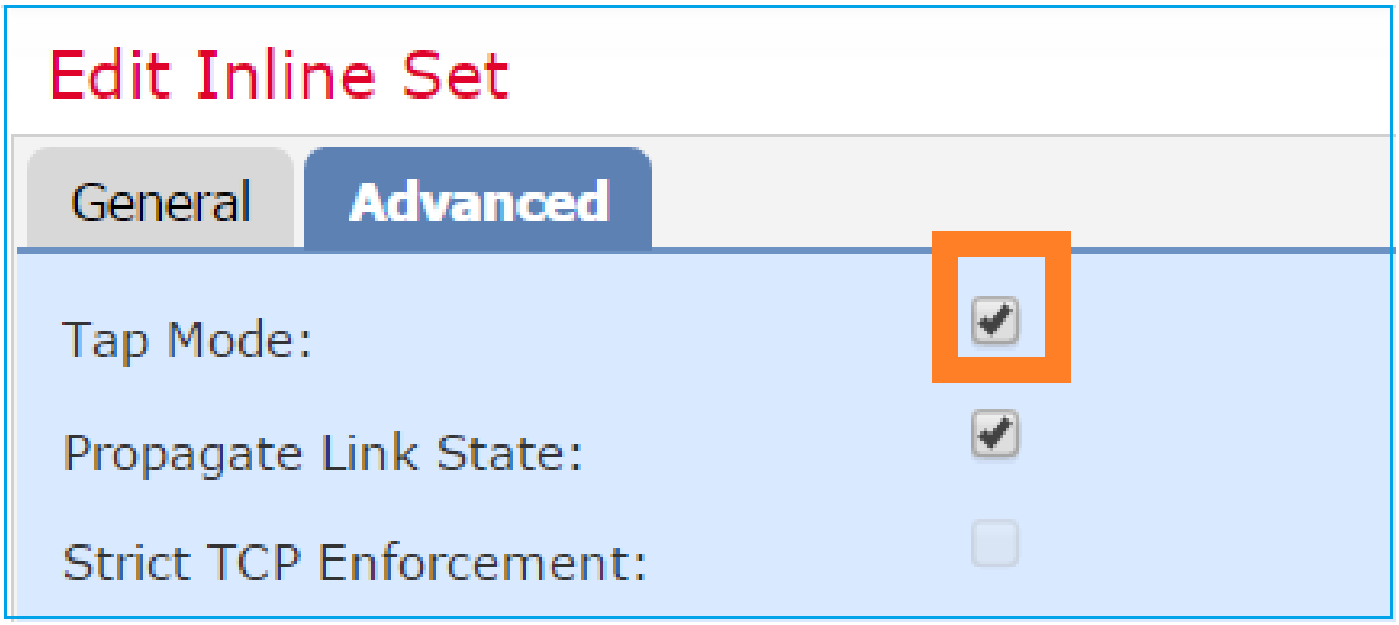
In questa traccia, si può vedere che il pacchetto è stato scartato dal motore LINA FTD e non è stato inoltrato al motore Snort FTD.

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>

>

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]:
```

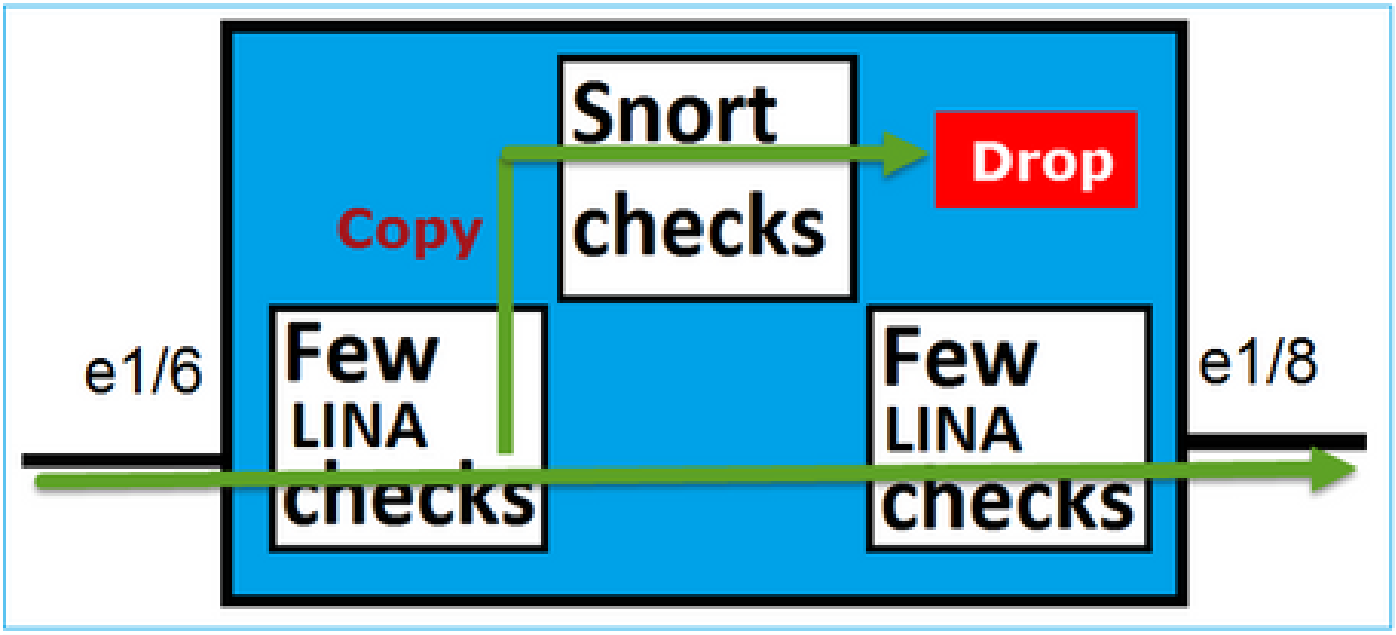
```
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/8 "OUTSIDE"
      Current-Status: UP
    Bridge Group ID: 0
>
```

Verifica coppia inline FTD con funzionamento interfaccia tap

Teoria base

- Quando si configura una coppia inline con il tap 2, le interfacce fisiche vengono collegate internamente
- È 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 la coppia inline
- Impossibile eliminare il traffico effettivo
- Alcuni controlli del motore LINA vengono applicati insieme ai controlli completi del motore Snort su una copia del traffico effettivo

L'ultimo punto è come mostrato nell'immagine:



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

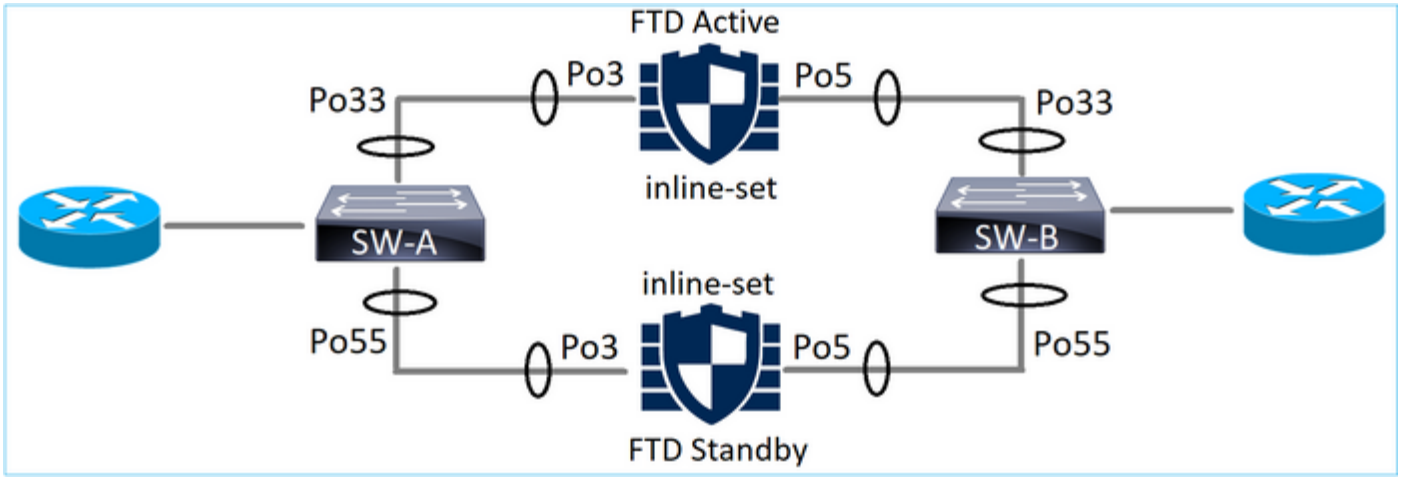
```
1 packet shown
>
```

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     Po35(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

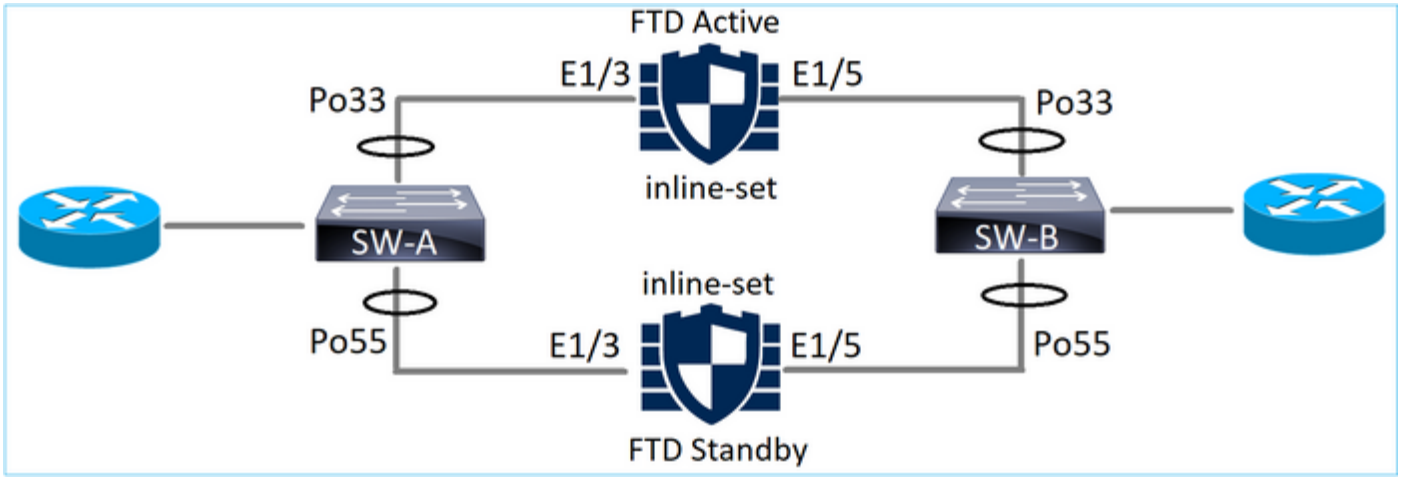
```
Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
```

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 necessario sugli 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 il tempo necessario per l'interruzione può essere più lungo. Se la modalità Etherchannel è impostata su ON (senza LACP), il tempo di convergenza dipende dall'apprendimento dell'indirizzo MAC.

Risoluzione dei problemi

Nessuna informazione specifica disponibile per questa configurazione.

Confronto: coppia 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
	  la modalità di bypass dell'hardware è disabilitata
	  Interface-Pair[1]:
	  Interfaccia: Ethernet1/6 "INSIDE"
	  Current-Status: SU
	  Interfaccia: Ethernet 1/8 "OUTSIDE"
	  Current-Status: SU
	  ID gruppo bridge: 509
	>
		> 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: Ethernet1/6 "INSIDE"
		  Current-Status: SU
		  Interfaccia: Ethernet 1/8 "OUTSIDE"
		  Current-Status: SU
		  ID gruppo bridge: 0
		
		>

show	> show interface e1/6	> show interface e1/6

interface	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 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	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-tap, 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: inline-tap, Inline-set: Inline-Pair-1 Indirizzo IP non assegnato 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, 8 byte/sec Velocità di uscita di 5 minuti 0 pkt/sec, 39 byte/sec cadute di 5 minuti, 0 pkt/sec >	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: ACQUISIZIONE Sottotipo: Risultato: ALLOW Config: Ulteriori informazioni: Elenco accessi MAC Fase: 2 Tipo: ACCESS-LIST Sottotipo: Risultato: ALLOW Config: Regola implicita Ulteriori informazioni: Elenco accessi MAC Fase: 3 Tipo: MODALITÀ NGIPS Sottotipo: modalità ngips Risultato: ALLOW 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: log Risultato: DROP	> 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: ACQUISIZIONE Sottotipo: Risultato: ALLOW Config: Ulteriori informazioni: Elenco accessi MAC Fase: 2 Tipo: ACCESS-LIST Sottotipo: Risultato: ALLOW Config: Regola implicita Ulteriori informazioni: Elenco accessi MAC Fase: 3 Tipo: MODALITÀ NGIPS Sottotipo: modalità ngips Risultato: ALLOW 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: log Risultato: ELIMINATO Config:

	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: ACCESS POLICY: FTD4100 - Obbligatorio/1 access-list CSM_FW_ACL_ note rule-id 268441600: L4 RULE: Rule 1 Ulteriori informazioni: Risultato: interfaccia di ingresso: INSIDE input-status: attivo stato della linea di ingresso: su Azione: eliminare Motivo dell'eliminazione: flusso (acl-drop) negato dalla regola configurata 1 pacchetto visualizzato >	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: ACCESS POLICY: FTD4100 - Obbligatorio/1 access-list CSM_FW_ACL_ note rule-id 268441600: L4 RULE: Rule 1 Ulteriori informazioni: Risultato: interfaccia di ingresso: INSIDE input-status: attivo stato della linea di ingresso: su Azione: l'elenco degli accessi sarebbe stato ignorato, ma il pacchetto sarebbe stato inoltrato a causa di un tocco 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).