Configuración de Interfaces FTD en el Modo de Par en Línea

Contenido

Introducción

Este documento describe la configuración, verificación y funcionamiento en segundo plano de una interfaz de par en línea en un dispositivo Firepower Threat Defense (FTD).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firepower 4150 FTD (código 6.1.0.x y 6.3.x)
- Firepower Management Center (FMC) (código 6.1.0.x y 6.3.x)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

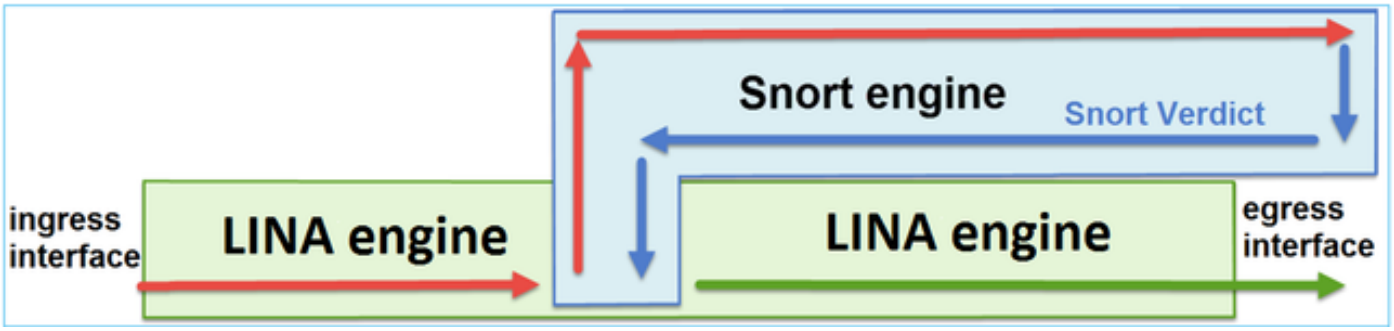
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), máquina virtual basada en kernel (KVM)
- Código de software FTD 6.2.x y posterior

Antecedentes

FTD es una imagen de software unificada que consta de 2 motores principales:

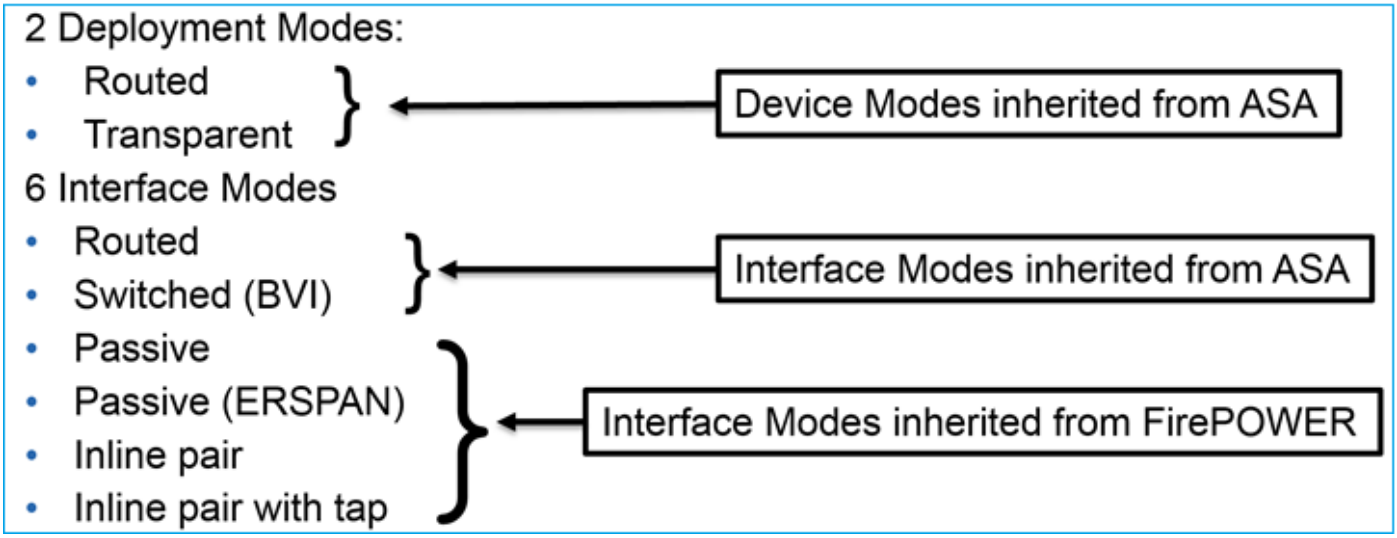
- Motor LINA
- Motor Snort

Esta figura muestra cómo interactúan los 2 motores:



- Un paquete ingresa a la interfaz de ingreso y es manejado por el motor LINA.
- Si lo requiere la política de FTD, el paquete es inspeccionado por el motor Snort.
- El motor Snort devuelve un veredicto para el paquete
- El motor LINA descarta o reenvía el paquete según el veredicto de Snort.

FTD proporciona dos modos de implementación y seis modos de interfaz, como se muestra en la imagen:



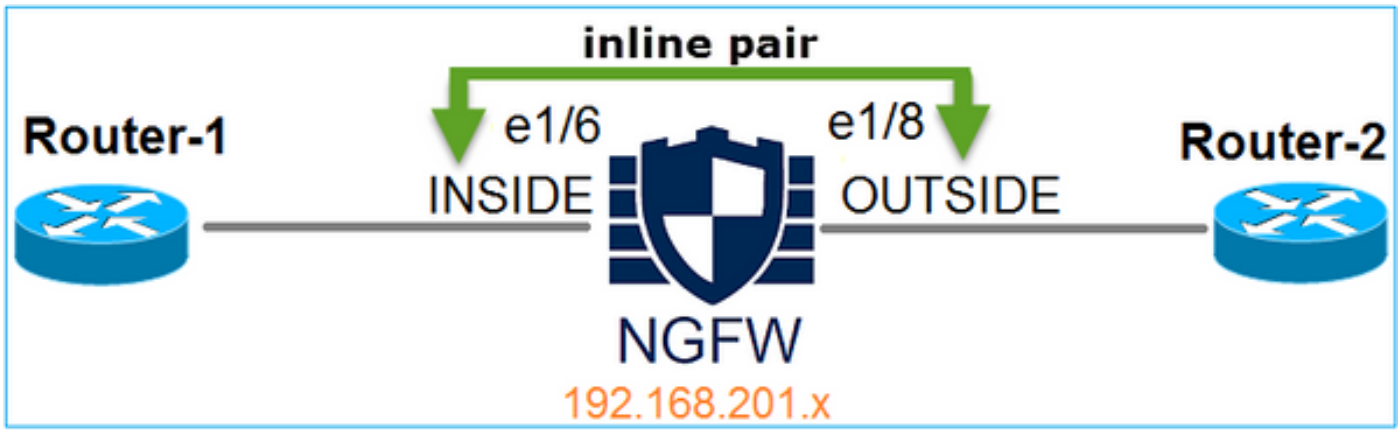
Nota: Puede combinar modos de interfaz en un único dispositivo FTD.

A continuación se ofrece una descripción general de alto nivel de los diversos modos de implementación e interfaz de FTD:

modo de interfaz FTD	Modo de implementación FTD	Descripción	El tráfico se puede descartar
Enrutado	Enrutado	Comprobaciones completas del motor LINA y del motor Snort	Yes
Conmutado	Transparente	Comprobaciones completas del motor LINA y del motor Snort	Yes
Pareja en línea	Ruteado o transparente	Comprobaciones parciales del motor LINA y del motor Snort	Yes
Vinculación en línea con pulsación	Ruteado o transparente	Comprobaciones parciales del motor LINA y del motor Snort	No
Pasivo	Ruteado o transparente	Comprobaciones parciales del motor LINA y del motor Snort	No
Pasivo (ERSPAN)	Enrutado	Comprobaciones parciales del motor LINA y del motor Snort	No

Configuración de la Interfaz de Par en Línea en FTD

Diagrama de la red



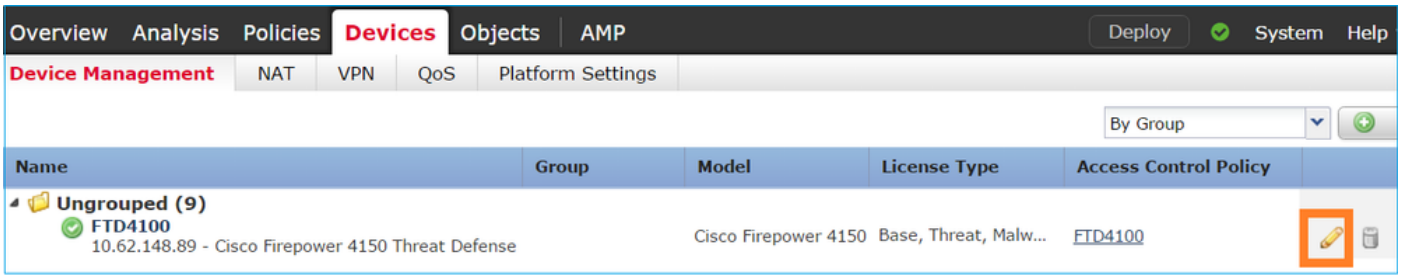
Requisito

Configure las interfaces físicas e1/6 y e1/8 en el modo de par en línea según estos requisitos:

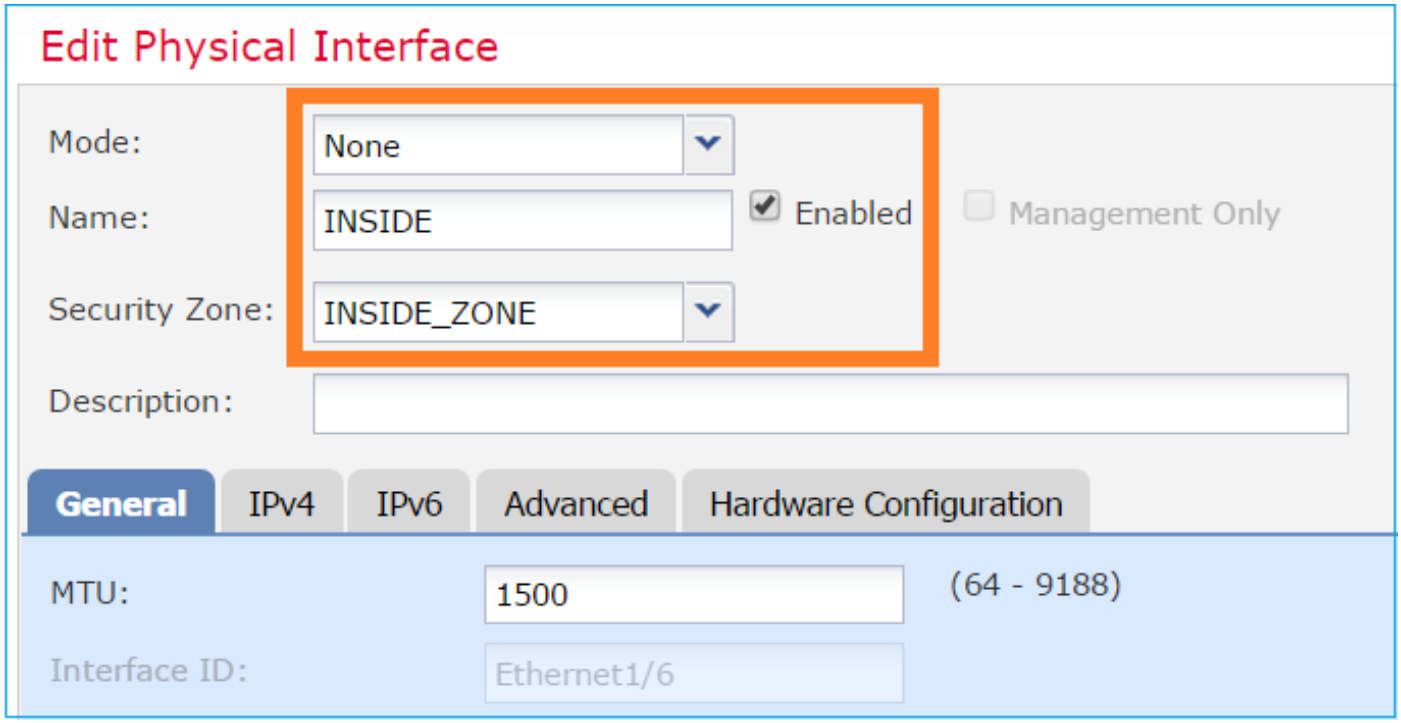
Interfaz	E1/6	E1/8
Nombre	DENTRO	FUERA
Zona de seguridad	INSIDE_ZONE	OUTSIDE_ZONE
Nombre del conjunto en línea	Inline-Pair-1	
MTU de conjunto en línea	1500	
FalloSeguro	Habilitado	
Propagación del estado del link	Habilitado	

Solución

Paso 1. Para configurar a las interfaces individuales, Navegue a **Dispositivos > Administración de dispositivos,** seleccione el dispositivo apropiado y seleccione **Editar** como se muestra en la imagen.

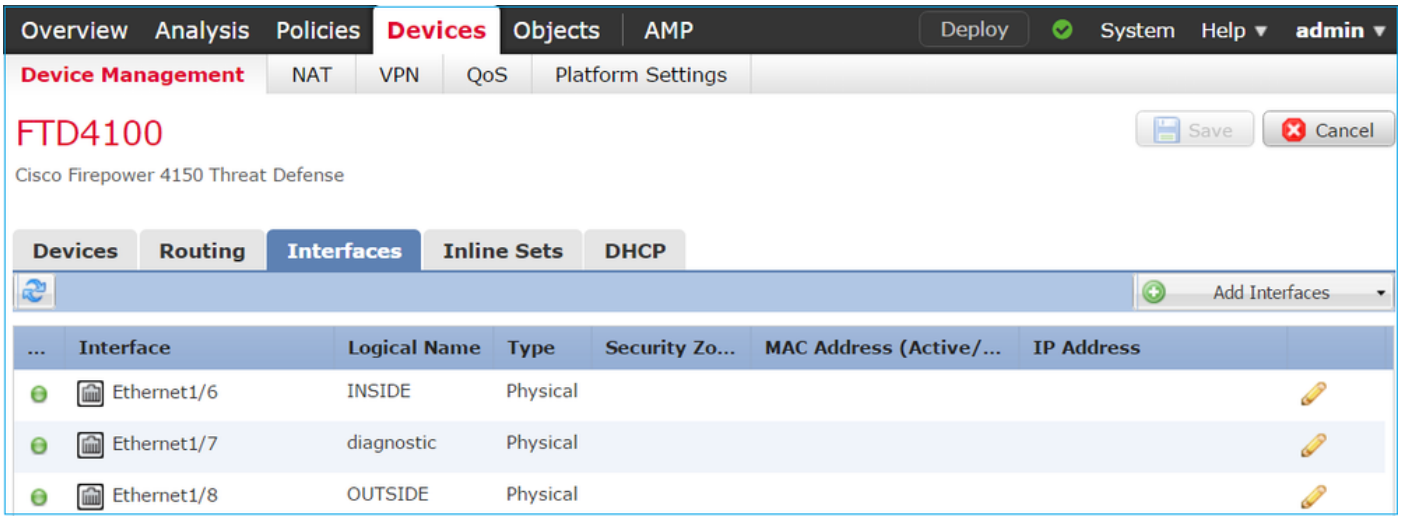


A continuación, especifique el **nombre** y marque **habilitado** para la interfaz como se muestra en la imagen.



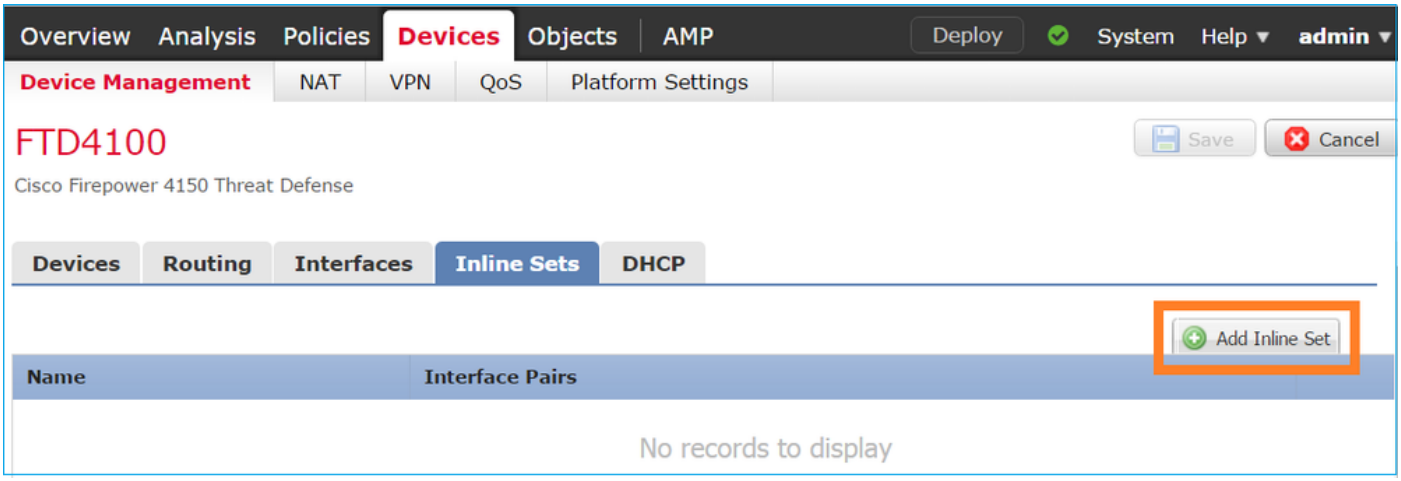
Nota: El nombre es el nombre de la interfaz.

De manera similar para la interfaz Ethernet1/8. El resultado final es como se muestra en la imagen.

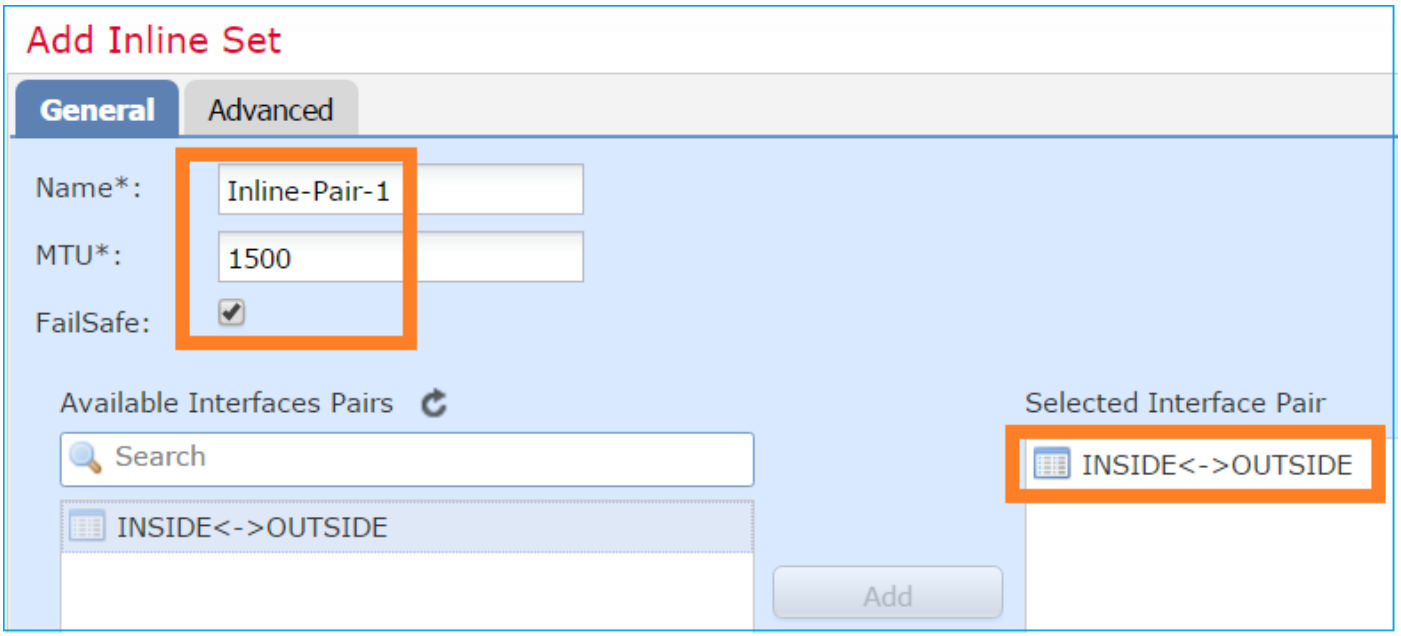


Paso 2. Configure el par en línea.

Navegue hasta **Conjuntos en línea > Agregar conjunto en línea** como se muestra en la imagen.

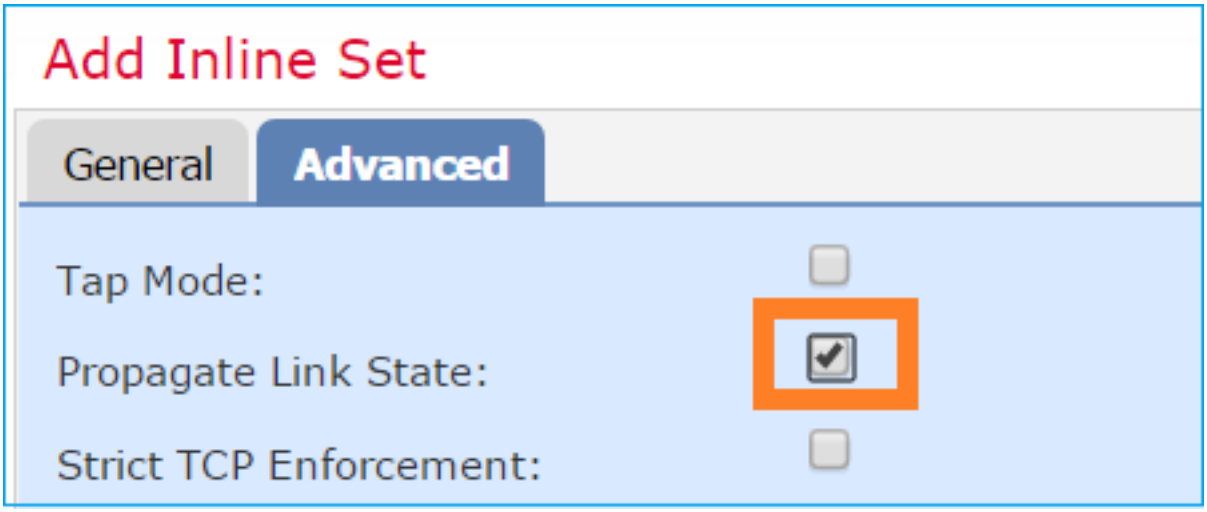


Paso 3. Configure los parámetros generales según los requisitos que se muestran en la imagen.



Nota: failsafe permite que el tráfico pase a través del par en línea sin inspeccionar en caso de que las memorias intermedias de la interfaz estén llenas (normalmente cuando el dispositivo está sobrecargado o el motor Snort está sobrecargado). El tamaño del búfer de la interfaz se asigna dinámicamente.

Paso 4. Habilite la opción **Propagate Link State** en Advanced Settings como se muestra en la imagen.



La propagación del estado de link desactiva automáticamente la segunda interfaz en el par de interfaz en línea cuando una de las interfaces en el conjunto en línea se desactiva.

Paso 5. **Guarde** los cambios y **implemente**.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Verifique la configuración del par en línea desde la CLI de FTD.

Solución

Inicie sesión en la CLI de FTD y verifique la configuración del par en línea:

```
> 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:** El ID de grupo de puentes es un valor diferente de 0. Si el modo de pulsación está activado, es 0

Información de nombre e interfaz:

```
> show nameif
Interface                Name                    Security
Ethernet1/6              INSIDE                    0
Ethernet1/7              diagnostic                0
Ethernet1/8              OUTSIDE                   0
>
```

Verifique el estado de la interfaz:

```
> 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
```

Verifique la información de la interfaz física:

```
> 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
>
```

Verificación de la Operación de Interfaz de Par de Línea FTD

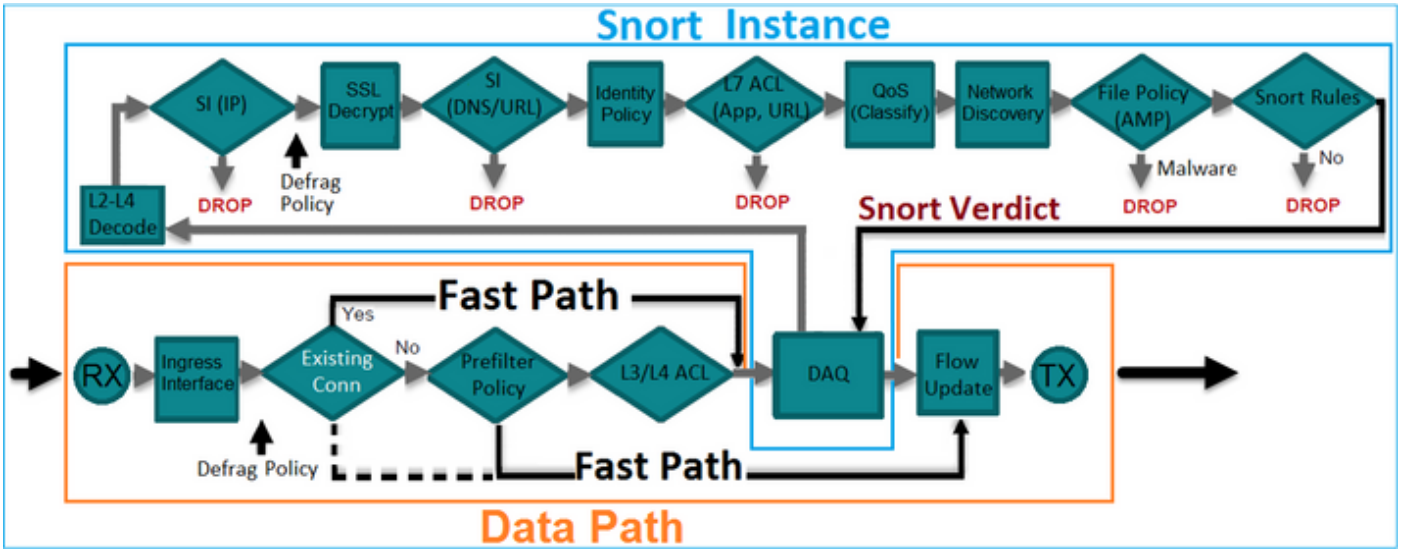
Esta sección cubre estas verificaciones de verificación para verificar la operación del par en línea:

- Verificación 1. Con el uso de packet-tracer
- Verificación 2. Habilitar la captura con seguimiento y enviar un paquete TCP de sincronización/reconocimiento (SYN/ACK) a través del par en línea
- Verificación 3. Supervise el tráfico FTD con el uso de la depuración del motor de firewall
- Verificación 4. Verifique la funcionalidad de Propagación de Link-State
- Verificación 5. Configuración de la traducción estática de direcciones de red (NAT)

Solución

Descripción general de la arquitectura

Cuando 2 interfaces FTD funcionan en el modo de par en línea, se maneja un paquete como se muestra en la imagen.

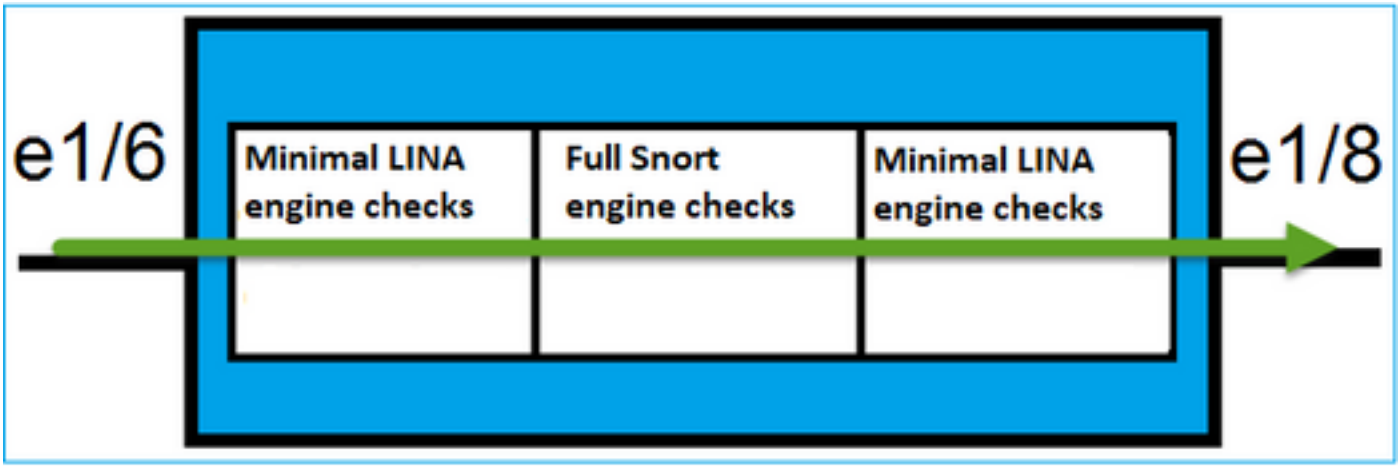


Nota: Sólo las interfaces físicas pueden ser miembros de un conjunto de pares en línea

Teoría Básica

- Cuando configura un par en línea 2, las interfaces físicas se puentean internamente
- Muy similar al clásico sistema de prevención de intrusiones en línea (IPS)
- Disponible en los modos de implementación enrutada o transparente
- La mayoría de las funciones del motor LINA (NAT, routing, etc.) no están disponibles para los flujos que pasan por un par en línea
- El tráfico de tránsito se puede descartar
- Se aplican algunas comprobaciones del motor LINA junto con comprobaciones completas del motor Snort

El último punto se puede visualizar como se muestra en la imagen:



Verificación 1. Con el Uso de Packet-Tracer

La salida packet-tracer que emula un paquete que atraviesa el par en línea con los puntos importantes resaltados:

```
> 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 will 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 will be sent to snort for additional processing where a verdict will be 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

>
```

Verificación 2. Enviar paquetes TCP SYN/ACK a través de un par en línea

Puede generar paquetes TCP SYN/ACK con el uso de un paquete que crea una utilidad como Scapy. Esta sintaxis genera 3 paquetes con indicadores SYN/ACK habilitados:

```
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)
```

Habilite esta captura en la CLI de FTD y envíe algunos paquetes TCP SYN/ACK:

```
> 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
>
```

Después de enviar los paquetes a través del FTD, puede ver una conexión que se creó:

```
> 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: un ASA clásico descartaría un paquete SYN/ACK no solicitado a menos que se habilitara la omisión de estado TCP. Una interfaz FTD en modo de par en línea maneja una conexión TCP en modo de omisión de estado TCP y no descarta paquetes TCP que no pertenecen a las conexiones que ya existen.

Nota: Indicador N - El paquete es inspeccionado por el motor FTD Snort.

Las capturas lo demuestran, ya que puede ver los 3 paquetes que atraviesan el FTD:

```
> 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 paquetes salen del dispositivo FTD:

```
> 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 el Seguimiento del primer paquete de captura se revela información adicional como el veredicto del motor Snort:

```
> 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 will be 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 will be sent to snort for additional processing where a verdict will be 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
>
```

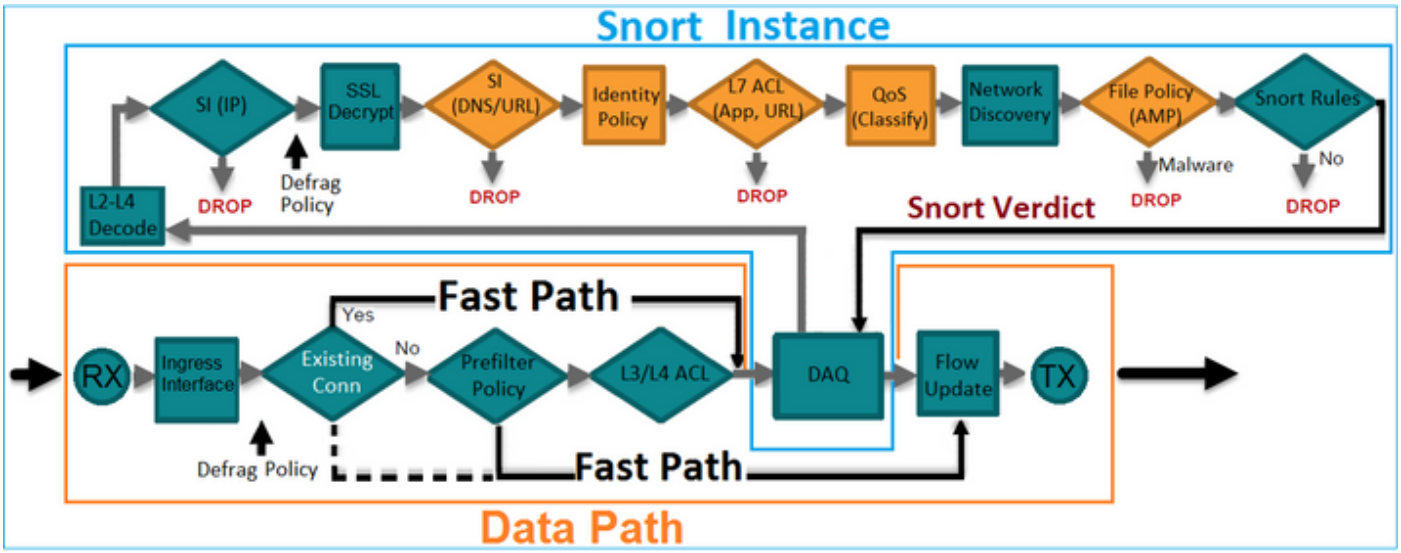
Con el Seguimiento del segundo paquete capturado, se muestra que el paquete coincide con una conexión existente, por lo que omite la verificación ACL, pero aún es inspeccionado por el motor Snort:

```
> 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 existing 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
>
```

Verificación 3. Depuración del motor de firewall para tráfico permitido

La depuración del motor de firewall se ejecuta con componentes específicos del motor de Snort de FTD, como la política de control de acceso, como se muestra en la imagen:



Cuando envía los paquetes TCP SYN/ACK a través del Par en línea, puede ver en el resultado de la depuración:

```
> 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 Allow and prefilter rule 0
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
```

Verificación 4. Verificar Propagación de Link-State

Habilite el registro del búfer en FTD y cierre el switchport conectado a la interfaz e1/6. En la CLI de FTD, debe ver que ambas interfaces se desactivaron:

```
> 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
>
```

Los registros de FTD muestran:

```
> show logging

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 down pair interface Ethernet1/8(OUTSIDE)
>
```

El estado del conjunto en línea muestra el estado de los 2 miembros de la interfaz:

```
> 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
>
```

Observe la diferencia en el estado de las 2 interfaces:

```
> 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
>
```

Y para la interfaz Ethernet1/8:

```
> 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
>
```

Después de volver a habilitar el switchport, los registros FTD muestran:

```
> show logging
...
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) bringing up pair interface Ethernet1/8(OUTSIDE)
>
```

Verificación 5. Configuración de NAT estática

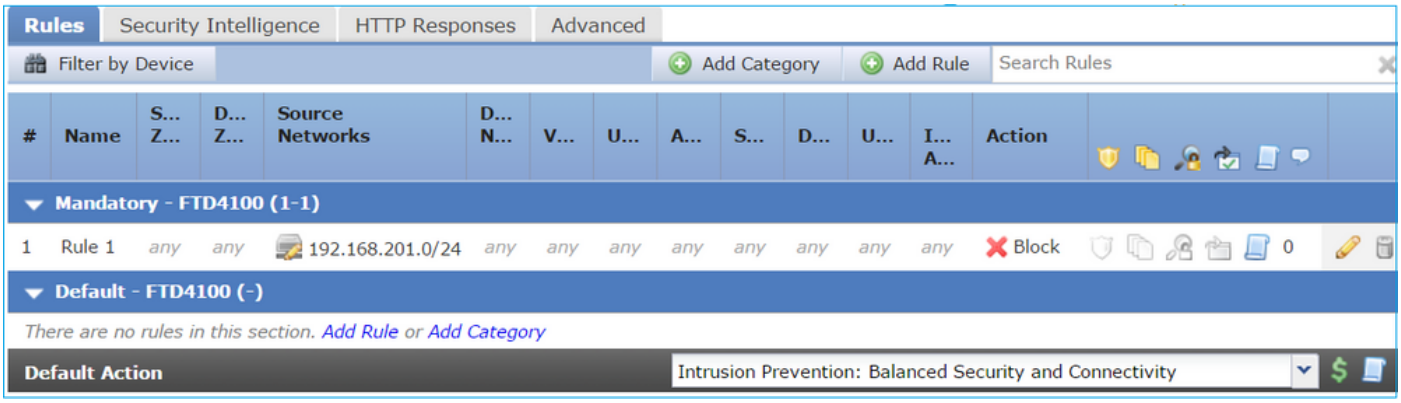
Solución

La NAT no se soporta para las interfaces que funcionan en los modos en línea, de pulsación en línea o pasivo:

http://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

Block Packet on Inline Pair Interface Mode

Cree una regla de bloqueo, envíe tráfico a través del Par de línea de FTD y observe el comportamiento como se muestra en la imagen.



Solución

Habilite la captura con seguimiento y envíe los paquetes SYN/ACK a través del Par en línea FTD. El tráfico está bloqueado:

```
> 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 el seguimiento, un paquete revela:

```
> 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 will be 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 flow-start
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
```

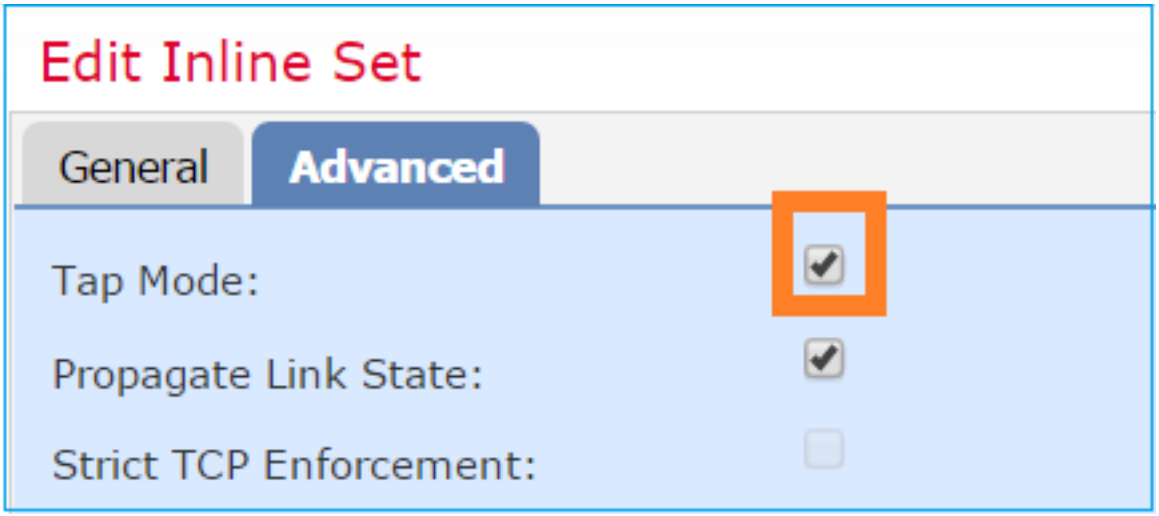
En este seguimiento, se puede ver que el paquete fue descartado por el motor FTD LINA y no fue reenviado al motor FTD Snort.

Configuración Del Modo De Par En Línea Con Tap

Active el modo Tap en el par en línea.

Solución

Navegue hasta **Dispositivos > Administración de dispositivos > Conjuntos en línea > Editar conjunto en línea > Avanzado** y active **Modo Tap como se muestra en la imagen.**



Verificación

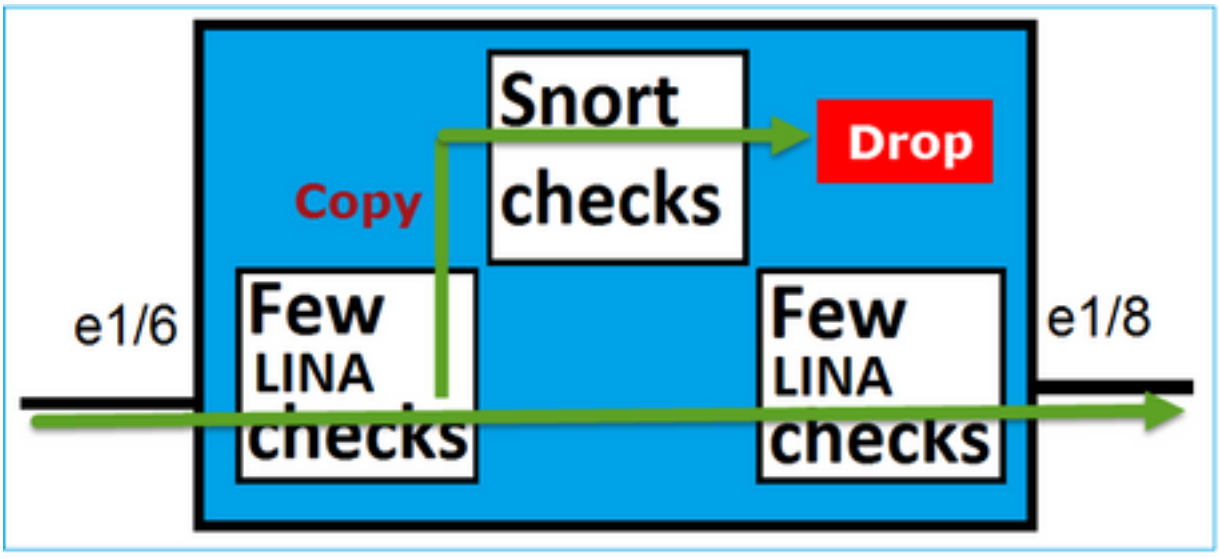
```
> show inline-set

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
>
```

Verificar El Par En Línea FTD Con La Operación De Interfaz Tap

Teoría Básica

- Cuando configura un par en línea con el Toque 2, las interfaces físicas se puentean internamente
- Está disponible en los modos de implementación enrutada o transparente
- La mayoría de las funciones del motor LINA (NAT, routing, etc.) no están disponibles para los flujos que atraviesan el par en línea
- El tráfico real no se puede descartar
- Se aplican algunas comprobaciones del motor LINA junto con comprobaciones completas del motor Snort a una copia del tráfico real

El último punto es como se muestra en la imagen:



El par en línea con el modo de pulsación no descarta el tráfico de tránsito. Con el seguimiento de un paquete, confirma esto:

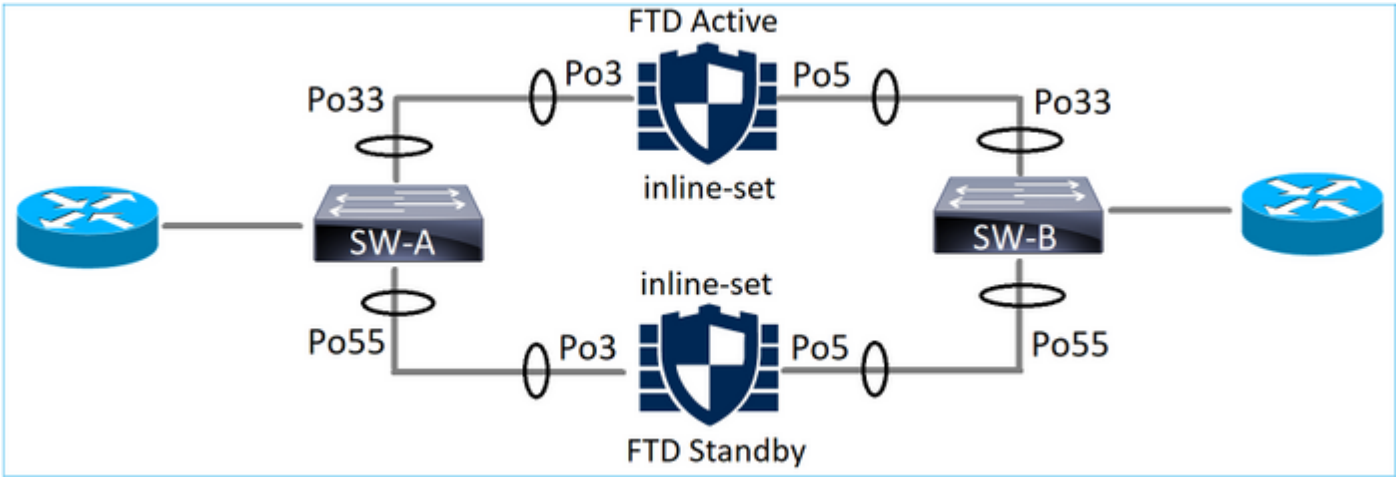
```
> show capture CAPI packet-number 2 trace

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 will be 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 flow-start
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
>
```

Par en línea y Etherchannel

Puede configurar el par en línea con etherchannel de 2 maneras:

1. Etherchannel finalizado en FTD
2. Etherchannel que pasa por el FTD (requiere código FXOS 2.3.1.3 y superior)

Etherchannel finalizado en FTD



Etherchannel en SW-A:

```
SW-A# show etherchannel summary | i Po33|Po55
33     Po33(SU)         LACP      Gi3/11(P)
35     Po35(SU)         LACP      Gi2/33(P)
```

Etherchannel en SW-B:

```
SW-B# show etherchannel summary | i Po33|Po55
33     Po33(SU)         LACP        Gi1/0/3(P)
55     Po55(SU)         LACP        Gi1/0/4(P)
```

El tráfico se reenvía a través del FTD activo basado en el aprendizaje de direcciones MAC:

```
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
```

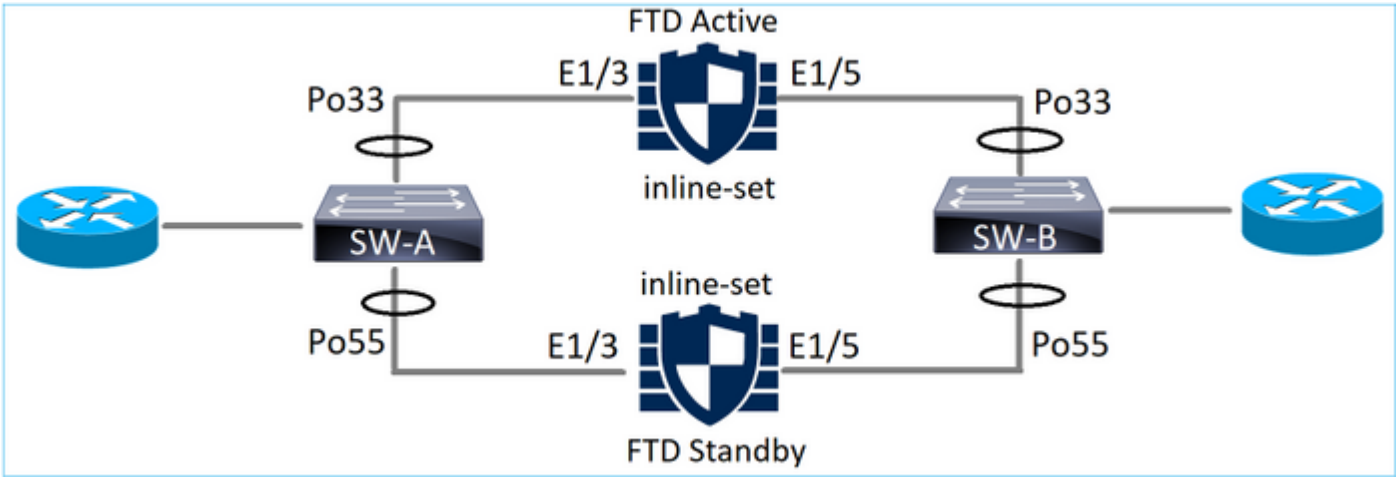
El conjunto en línea en FTD:

```
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: En el caso de un evento de failover de FTD, la interrupción del tráfico depende principalmente del tiempo que toma en los switches para aprender la dirección MAC del peer remoto.

Etherchannel a través de FTD



Etherchannel en SW-A:

```
SW-A# show etherchannel summary | i Po33|Po55
33     Po33(SU)         LACP      Gi3/11(P)
55     Po55(SD)         LACP      Gi3/7(I)
```

Los paquetes LACP que pasan a través del FTD en espera se bloquean:

```
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 en SW-B:

```
SW-B# show etherchannel summary | i Po33|Po55
33     Po33(SU)         LACP        Gi1/0/3(P)
55     Po55(SD)         LACP        Gi1/0/4(s)
```

El tráfico se reenvía a través del FTD activo basado en el aprendizaje de direcciones MAC:

```
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
```

El conjunto en línea en FTD:

```
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
```

> **Precaución:** En este escenario en el caso de un evento de failover de FTD, el tiempo de convergencia depende principalmente de la negociación de LACP de Etherchannel y dependiendo del tiempo que tome la interrupción puede ser bastante más largo. En caso de que el modo Etherchannel esté ON (sin LACP), el tiempo de convergencia dependerá del aprendizaje de la dirección MAC.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Comparación: Pareja en línea vs. Pareja en línea con pulsación

	Par en línea	Par en línea con pulsación
show inline-set	> show inline-set Inline-set Inline-Pair-1 Mtu es de 1500 bytes El modo de seguridad contra fallos está activado/activado El modo de seguridad fallida está desactivado **El modo de pulsación está desactivado** La opción Propagate-link-state está activada el modo de omisión de hardware está desactivado Par de interfaz[1]: Interfaz: Ethernet1/6 "DENTRO" Estado actual: EN FUNCIONAMIENTO Interfaz: Ethernet1/8 "EXTERIOR" Estado actual: EN FUNCIONAMIENTO **ID de grupo de puentes: 509**	> **show inline-set** Inline-set Inline-Pair-1 Mtu es de 1500 bytes El modo de seguridad contra fallos está activado/activado El modo de seguridad fallida está desactivado **El modo de pulsación está activado** La opción Propagate-link-state está activada el modo de omisión de hardware está desactivado Par de interfaz[1]: Interfaz: Ethernet1/6 "DENTRO" Estado actual: EN FUNCIONAMIENTO Interfaz: Ethernet1/8 "EXTERIOR" Estado actual: EN FUNCIONAMIENTO **ID de grupo de puentes: 0**
show interface	> > **show interface e1/6** La interfaz Ethernet1/6 "INSIDE", está activa, el protocolo de línea está activo El hardware es EtherSVI, BW 1000 Mbps, DLY 1000 usec Dirección MAC 5897.bdb9.770e, MTU 1500 Modo de interfaz IPS: **en línea**, en línea: Inline-Pair-1	> > **show interface e1/6** La interfaz Ethernet1/6 "INSIDE", está activa, el protocolo de línea está act El hardware es EtherSVI, BW 1000 Mbps, DLY 1000 usec Dirección MAC 5897.bdb9.770e, MTU 1500 Modo de interfaz IPS: **inline-tap**, Inline-Set: Inline-Pair-1

Para administrar paquetes con regla de bloqueo

```
      Dirección IP no asignada
 Estadísticas de tráfico para "INSIDE":
      entrada de paquetes 3957, 264913 bytes
      Salida de 144 paquetes, 58664 bytes
      4 paquetes descartados
    Velocidad de entrada de 1 minuto 0 pkts/seg, 26 bytes/seg
    Velocidad de salida de 1 minuto 0 pkts/seg, 7 bytes/seg
    velocidad de caída de 1 minuto, 0 pkts/s
    Velocidad de entrada de 5 minutos 0 pkts/seg, 28 bytes/seg
    Velocidad de salida de 5 minutos 0 pkts/s, 9 bytes/s
    Velocidad de caída de 5 minutos, 0 pkts/s
>show interface e1/8
La interfaz Ethernet1/8 "FUERA", está activa, el protocolo de línea está activo
 El hardware es EtherSVI, BW 1000 Mbps, DLY 1000 usec
      Dirección MAC 5897.bdb9.774d, MTU 1500
      Modo de interfaz IPS: en línea, en línea: Inline-Pair-1
      Dirección IP no asignada
 Estadísticas de tráfico para "FUERA":
      Entrada de 144 paquetes, 55634 bytes
      3954 paquetes de salida, 339987 bytes
      0 paquetes descartados
    Velocidad de entrada de 1 minuto 0 pkts/seg, 7 bytes/seg
    Velocidad de salida de 1 minuto 0 pkts/seg, 37 bytes/seg
    velocidad de caída de 1 minuto, 0 pkts/s
    Velocidad de entrada de 5 minutos 0 pkts/s, 8 bytes/s
    Velocidad de salida de 5 minutos 0 pkts/seg, 39 bytes/seg
    Velocidad de caída de 5 minutos, 0 pkts/s
>
> show capture CAPI packet-number 1 trace

3 paquetes capturados

  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: CAPTURA
Subtipo:
Resultado: PERMISO
Config:
Información adicional:
lista de acceso MAC

Fase: 2
Tipo: ACCESS-LIST
Subtipo:
Resultado: PERMISO
Config:
Regla implícita
Información adicional:
lista de acceso MAC

Fase: 3
Tipo: NGIPS-MODE
Subtipo: ngips-mode
Resultado: PERMISO
Config:
Información adicional:
Se aplicará el flujo ingresado a una interfaz configurada para el modo NGIPS y los
servicios NGIPS

Fase: 4
Tipo: ACCESS-LIST
Subtipo: registro
Resultado: DESCARTAR
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 flow-start
access-list CSM_FW_ACL_ remark rule-id 268441600: POLÍTICA DE ACCESO:
FTD4100 - Obligatorio/1
access-list CSM_FW_ACL_ remark rule-id 268441600: REGLA L4: Artículo 1
Información adicional:

Resultado:
interfaz de entrada: DENTRO
estado de entrada: en funcionamiento
input-line-status: en funcionamiento
Acción: caída
Motivo de caída: (acl-drop) La regla configurada niega el flujo


1 paquete mostrado
>
```

```
      Dirección IP no asignada
 Estadísticas de tráfico para "INSIDE":
      Entrada de 24 paquetes, 1378 bytes
      0 paquetes de salida, 0 bytes
      Se descartaron 24 paquetes
    Velocidad de entrada de 1 minuto 0 pkts/s, 0 bytes/s
    Velocidad de salida de 1 minuto 0 pkts/sec, 0 bytes/s
    velocidad de caída de 1 minuto, 0 pkts/s
    Velocidad de entrada de 5 minutos 0 pkts/s, 0 bytes/s
    Velocidad de salida de 5 minutos 0 pkts/s, 0 bytes/s
    Velocidad de caída de 5 minutos, 0 pkts/s
>show interface e1/8
La interfaz Ethernet1/8 "FUERA", está activa, el protocolo de línea está act
 El hardware es EtherSVI, BW 1000 Mbps, DLY 1000 usec
      Dirección MAC 5897.bdb9.774d, MTU 1500
      Modo de interfaz IPS: inline-tap, Inline-Set: Inline-Pair-1
      Dirección IP no asignada
 Estadísticas de tráfico para "FUERA":
      Entrada de 1 paquete, 441 bytes
      0 paquetes de salida, 0 bytes
      1 paquetes descartados
    Velocidad de entrada de 1 minuto 0 pkts/s, 0 bytes/s
    Velocidad de salida de 1 minuto 0 pkts/sec, 0 bytes/s
    velocidad de caída de 1 minuto, 0 pkts/s
    Velocidad de entrada de 5 minutos 0 pkts/s, 0 bytes/s
    Velocidad de salida de 5 minutos 0 pkts/s, 0 bytes/s
    Velocidad de caída de 5 minutos, 0 pkts/s
>

> show capture CAPI packet-number 1 trace

3 paquetes capturados

  1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win
Fase: 1
Tipo: CAPTURA
Subtipo:
Resultado: PERMISO
Config:
Información adicional:
lista de acceso MAC

Fase: 2
Tipo: ACCESS-LIST
Subtipo:
Resultado: PERMISO
Config:
Regla implícita
Información adicional:
lista de acceso MAC

Fase: 3
Tipo: NGIPS-MODE
Subtipo: ngips-mode
Resultado: PERMISO
Config:
Información adicional:
Se aplicará el flujo ingresado a una interfaz configurada para el modo NGIP
servicios NGIPS

Fase: 4
Tipo: ACCESS-LIST
Subtipo: registro
Resultado: HUBIERA ABANDONADO
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.
id 268441600 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268441600: POLÍTICA DE ACC
FTD4100 - Obligatorio/1
access-list CSM_FW_ACL_ remark rule-id 268441600: REGLA L4: Artículo
Información adicional:

Resultado:
interfaz de entrada: DENTRO
estado de entrada: en funcionamiento
input-line-status: en funcionamiento
Acción: La lista de acceso se habría descartado, pero el paquete se ha ree
debido a inline-tap


1 paquete mostrado
>
```

Summary

- Cuando utiliza el modo Par en línea, el paquete pasa principalmente a través del motor Snort FTD

- Las conexiones TCP se manejan en un modo de omisión de estado TCP
- Desde el punto de vista de un motor FTD LINA, se aplica una política ACL
- Cuando el modo de par en línea está en uso, los paquetes se pueden bloquear porque se procesan en línea
- Cuando se habilita el modo de pulsación, una copia del paquete se inspecciona y se descarta internamente mientras el tráfico real pasa a través de FTD sin modificar

Información Relacionada

- NGFW Cisco Firepower
- Soporte Técnico y Documentación - Cisco Systems