

Interfaces de la configuración FTD en el modo de los En línea-pares

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Interfaz en línea de los pares de la configuración en FTD](#)

[Diagrama de la red](#)

[Verificación](#)

[Verifique la operación en línea de la interfaz de los pares FTD](#)

[Teoría Básica](#)

[Verificación 1. Con el uso del Paquete-trazalíneas](#)

[La verificación 2. envía los paquetes TCP SYN/ACK con los pares en línea](#)

[Debug del motor del Firewall de la verificación 3. para el tráfico permitido](#)

[La verificación 4. verifica la propagación del link-state](#)

[NAT estático de la configuración de la verificación 5.](#)

[Bloquear paquete en el modo en línea de la interfaz de los pares](#)

[Modo en línea de los pares de la configuración con el golpecito](#)

[Verifique los pares en línea FTD con la operación de la interfaz del golpecito](#)

[Troubleshooting](#)

[Comparación: Pares en línea contra los pares en línea con el golpecito](#)

[Resumen](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración, la verificación y la operación de fondo de una interfaz en línea de los pares en un dispositivo de la defensa de la amenaza de FirePOWER (FTD).

Prerequisites

Requisitos

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 que funciona con el código 6.1.0.x FTD
- Centro de administración de FirePOWER (FMC) que ejecuta 6.1.0.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

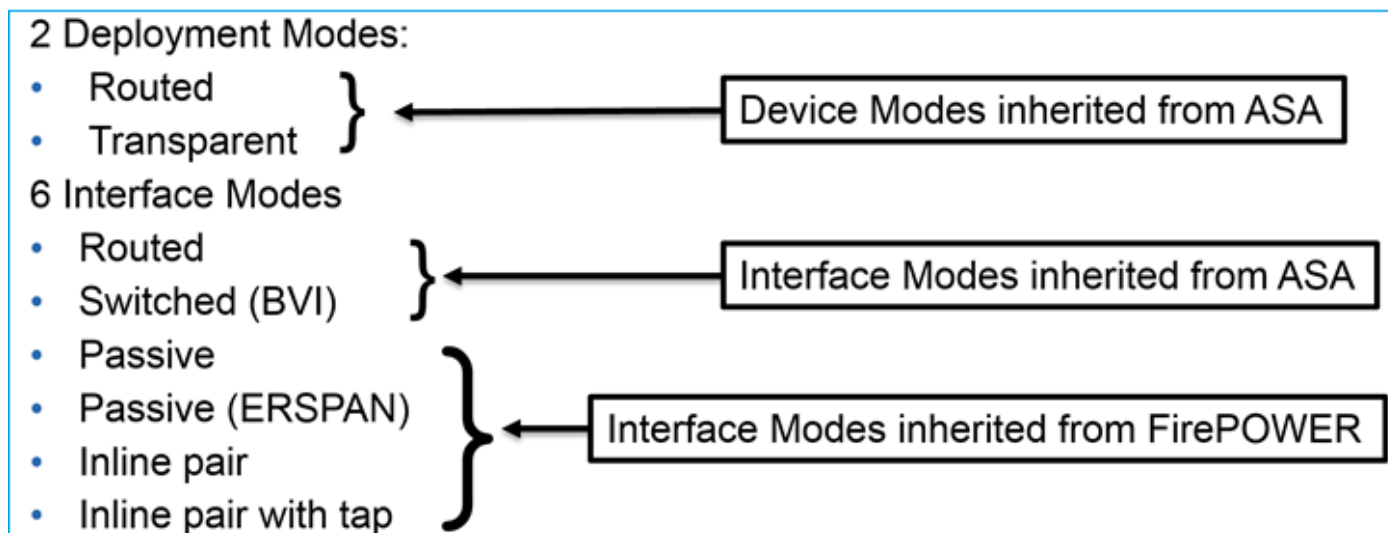
Productos Relacionados

Este documento se puede también utilizar 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), servicios web del Amazonas (AWS), teclado/vídeo/ratón (KVM)
- Código del software 6.2.x FTD y posterior

Antecedentes

FTD proporciona dos modos del despliegue y seis modos de la interfaz tal y como se muestra en de la imagen:



Note: Usted puede mezclar los modos de la interfaz en un dispositivo del siglo FTD.

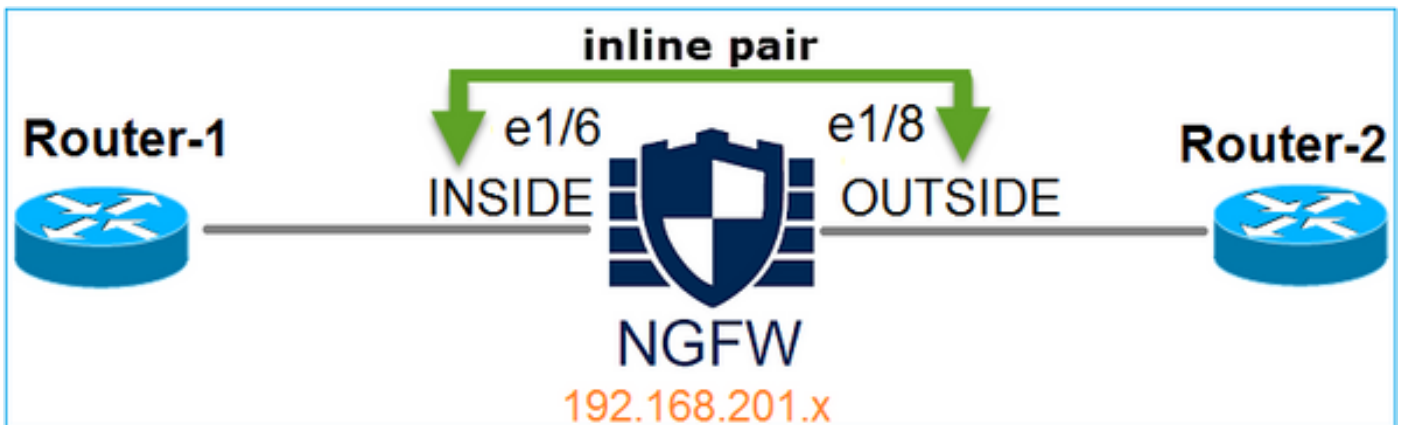
Aquí está una descripción general de alto nivel de los diversos modos del despliegue y de la interfaz FTD:

Modo de la interfaz FTD	Modo del despliegue FTD	Descripción	El tráfico puede ser caído
Ruteado	Ruteado	ASA-motor y controles completos del Snort-motor	Yes
Conmutado	Transparente	ASA-motor y controles completos	Yes

Pares en línea	Ruteado o transparente	del Snort-motor ASA-motor parcial y controles completos del Snort-motor	Yes
Pares en línea con el golpecito	Ruteado o transparente	ASA-motor parcial y controles completos del Snort-motor	No
Pasivo	Ruteado o transparente	ASA-motor parcial y controles completos del Snort-motor	No
Voz pasiva (ERSPAN)	Ruteado	ASA-motor parcial y controles completos del Snort-motor	No

Interfaz en línea de los pares de la configuración en FTD

Diagrama de la red



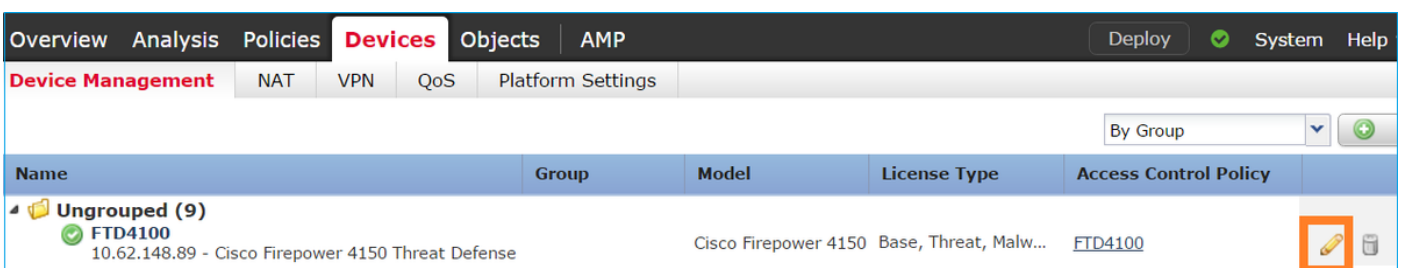
Requisito

Configure las interfaces físicas e1/6 y e1/8 en el modo en línea de los pares 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	
Conjunto en línea MTU	1500	
A prueba de averías	Habilitado	
Estado del link de la propagación	Habilitado	

Solución

Paso 1. Para configurar a las interfaces individuales, navegar a los **dispositivos** > a la **Administración de dispositivos**, seleccionar el dispositivo apropiado y al tecleo **edite** tal y como se muestra en de la imagen.



Después, especifique el **nombre** y haga tictac **habilitado** para la interfaz tal y como se muestra en de la imagen.

Edit Physical Interface

Mode:

Name: Enabled Management Only

Security Zone:

Description:

General | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU: (64 - 9188)

Interface ID:

Note: El nombre es el nameif de la interfaz.

Semejantemente para la interfaz Ethernet1/8. El resultado final está tal y como se muestra en de la imagen.

Overview | Analysis | Políticas | **Devices** | Objects | AMP | Deploy | System | Help | admin

Device Management | NAT | VPN | QoS | Platform Settings

FTD4100

Cisco Firepower 4150 Threat Defense

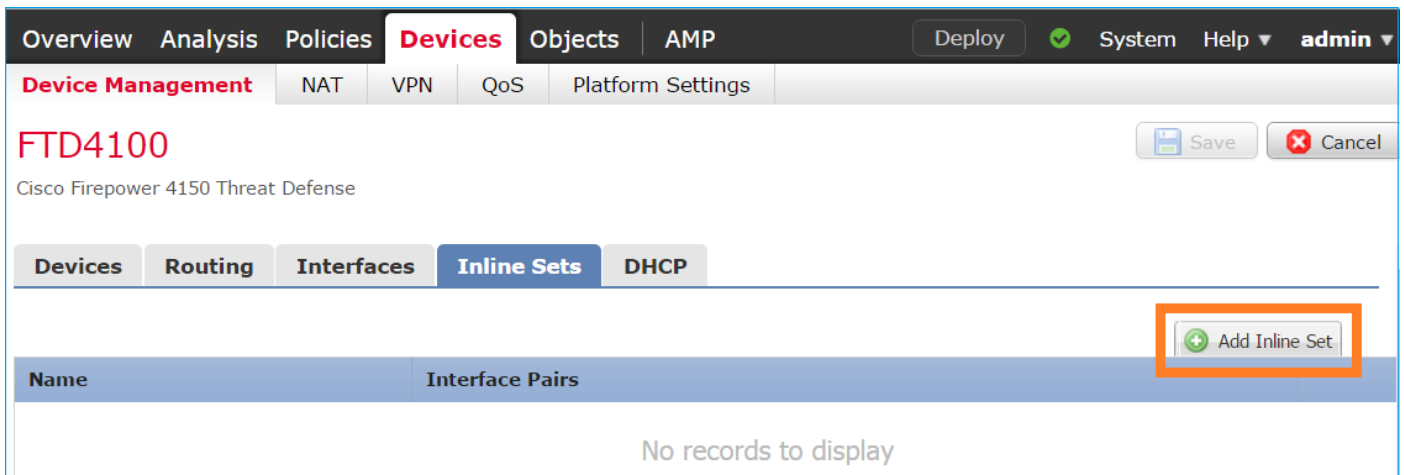
Devices | Routing | **Interfaces** | Inline Sets | DHCP

+ Add Interfaces

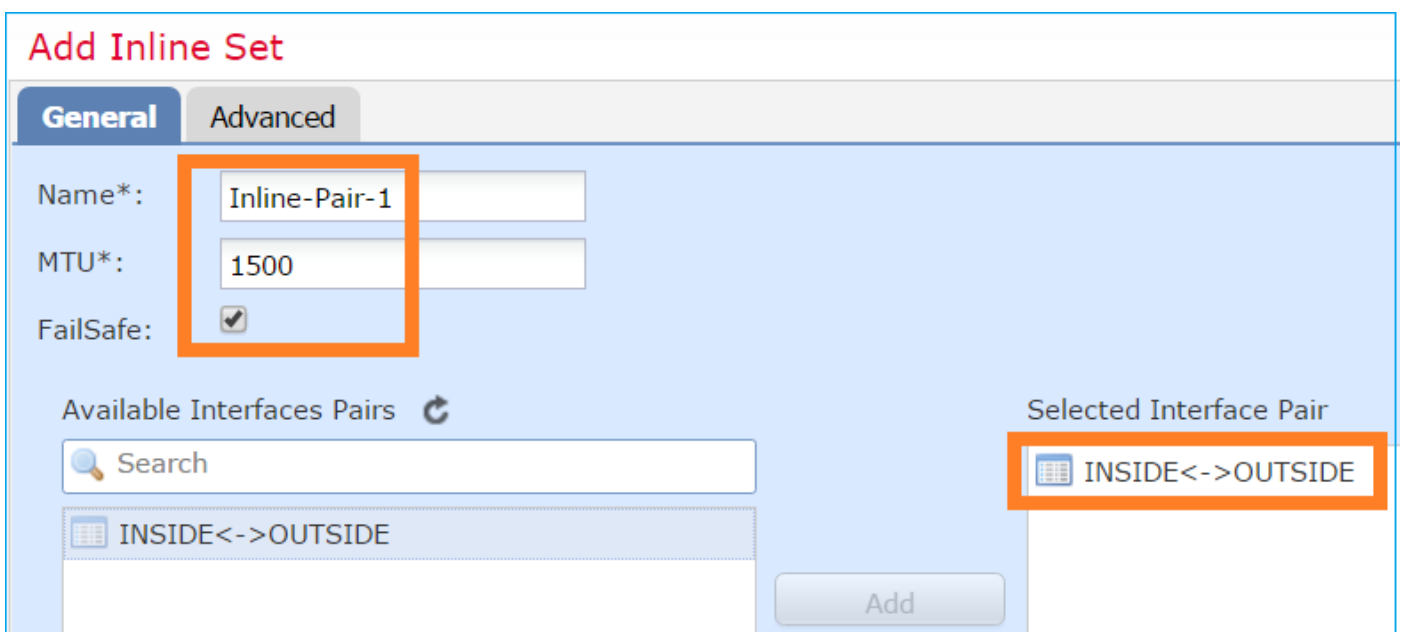
...	Interface	Logical Name	Type	Security Zo...	MAC Address (Active/...	IP Address
+	Ethernet1/6	INSIDE	Physical			
+	Ethernet1/7	diagnostic	Physical			
+	Ethernet1/8	OUTSIDE	Physical			

Paso 2. Configure los pares en línea.

Navigate a los **conjuntos en línea** > **Add en línea fijados** tal y como se muestra en de la imagen.

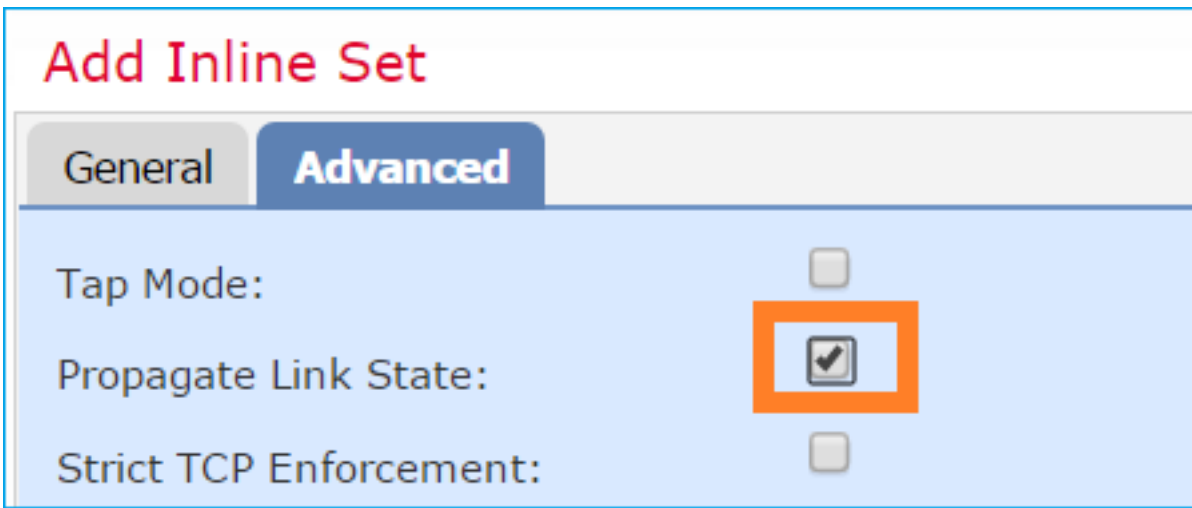


Paso 3. Configure las opciones generales según los requisitos tal y como se muestra en de la imagen.



Note: A prueba de averías permite que el tráfico pase con los pares en línea sin inspeccionar en caso de que los buffers de la interfaz sean llenos (visto típicamente cuando se sobrecarga el dispositivo o se sobrecarga el motor del Snort). El tamaño de almacén intermedio de la interfaz se afecta un aparato dinámicamente.

Paso 4. Opción del **estado del link de la propagación del** permiso en las configuraciones avanzadas tal y como se muestra en de la imagen.



La propagación del estado del link derriba automáticamente la segunda interfaz en los pares en línea de la interfaz cuando va una de las interfaces en el conjunto en línea abajo.

Paso 5. **Salve los cambios y despliegúelos.**

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Verifique la configuración en línea de los pares del FTD CLI.

Solución

Inicie sesión a FTD CLI y verifique la configuración en línea de los pares:

```
> 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
>
```

Note: El ID de grupo del Bridge es un valor diferente que 0. Si el modo tap está en entonces es 0

Interfaz y información de nombre:

> show nameif

Interface	Name	Security
Ethernet1/6	INSIDE	0
Ethernet1/7	diagnostic	0
Ethernet1/8	OUTSIDE	0

>

Verifique el estatus 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

>

Verifique la operación en línea de la interfaz de los pares FTD

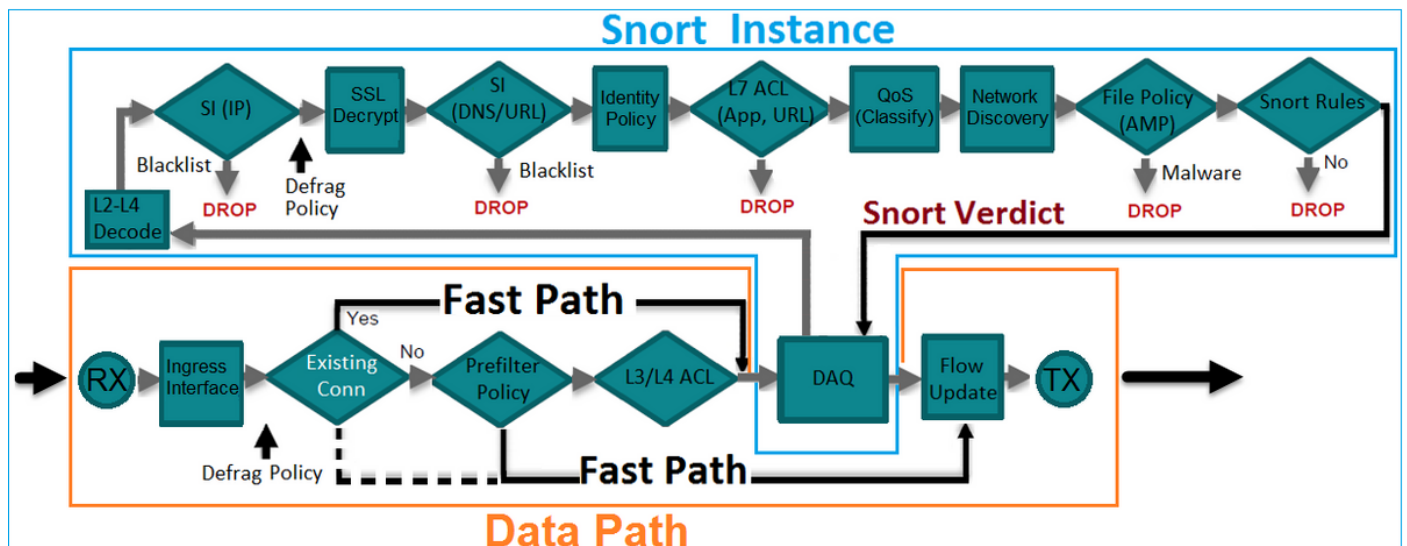
Esta sección cubre estos controles de la verificación para verificar la operación en línea de los pares:

- Verificación 1. Con el uso del paquete-trazalíneas.
- La captura del permiso de la verificación 2. con la traza y envía un TCP sincroniza/reconoce el paquete (SYN/ACK) con los pares en línea.
- Tráfico del monitor FTD de la verificación 3. con el uso del debug del motor del Firewall.
- La verificación 4. verifica las funciones de la propagación del link-state.
- Traducción de dirección de red estática (NAT) de la configuración de la verificación 5.

Solución

Descripción general de la arquitectura

Cuando 2 interfaces FTD actúan en el modo de los En línea-pares un paquete se maneja tal y como se muestra en de la imagen.

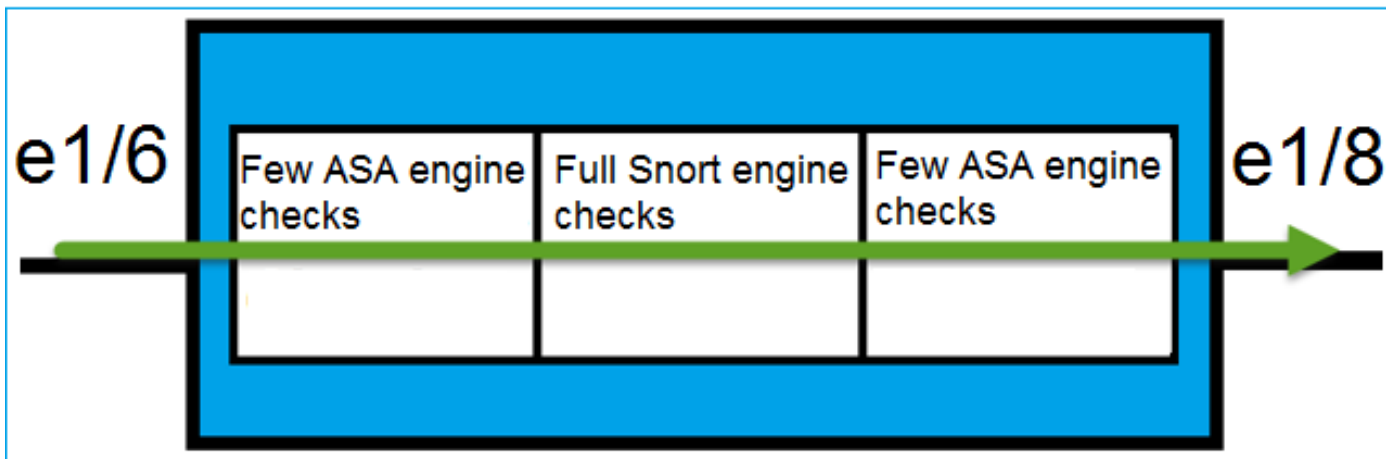


Note: Solamente las interfaces físicas pueden ser miembros de un par en línea fijado

Teoría Básica

- Cuando usted configura un par en línea 2 interfaces físicas internamente se interliga
- Muy similar al Sistema de prevención de intrusiones (IPS) en línea clásico
- Disponible en los modos ruteados o transparentes del despliegue
- La mayor parte de las características del motor ASA (NAT, encaminamiento, L3/L4 ACL etc) no están disponibles para los flujos que pasa con un par en línea
- El tráfico de tránsito puede ser caído
- Pocos controles adaptantes del motor del dispositivo de seguridad (ASA) son aplicados junto con los controles completos del motor del Snort

La punta más reciente se puede visualizar tal y como se muestra en de la imagen.



Verificación 1. Con el uso del Paquete-trazalíneas

El paquete-trazalíneas hizo salir que emula a un paquete que atraviese los pares 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

>

La verificación 2. envía los paquetes TCP SYN/ACK con los pares en línea

Usted puede generar los paquetes TCP SYN/ACK con el uso de un paquete ese los artes utilitarios como Scapy. Este sintaxis genera 3 paquetes con los 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 FTD CLI y envíe pocos 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 que usted envíe los paquetes con el FTD usted puede ver una conexión que fue creada:

```
> 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
```

>

Note: indicador b - Un ASA clásico caería un paquete no solicitado SYN/ACK a menos que estado-puente TCP fuera habilitado. Una interfaz FTD en el modo en línea de los pares maneja una conexión TCP en un modo de estado-puente TCP y no cae los paquetes TCP que no pertenecen a las conexiones que existen ya.

Note: El indicador N el paquete es examinado por el motor del Snort FTD.

Las capturas prueban esto, puesto que usted 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 el 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 la traza de la primera captura el paquete revela una cierta información adicional como el veredicto del motor del 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 la traza del segundo paquete capturado muestra que el paquete hace juego una conexión existente así que desvía el control ACL, pero todavía es examinado por el motor del 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

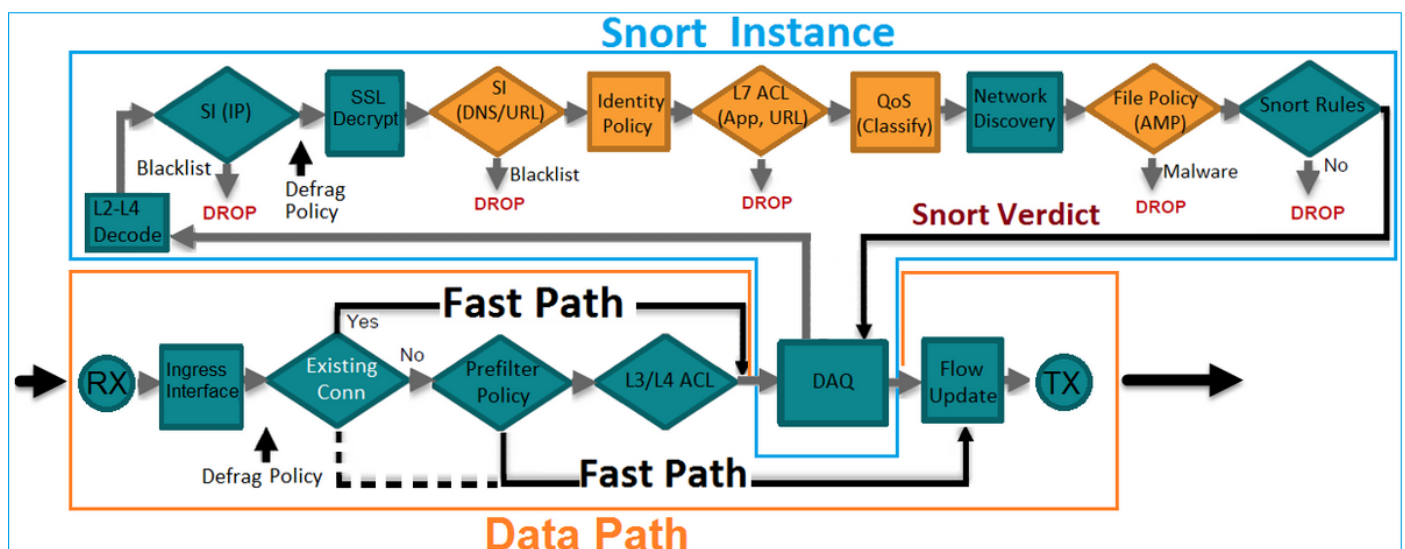
Action: allow

1 packet shown

>

Debug del motor del Firewall de la verificación 3. para el tráfico permitido

Funcionamientos del debug del motor del Firewall contra los componentes específicos del motor del Snort FTD como la directiva del control de acceso tal y como se muestra en de la imagen:



Cuando usted envía los paquetes TCP SYN/ACK con los pares en línea usted puede ver en la salida de los debugs:

```
> 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
```

La verificación 4. verifica la propagación del link-state

Habilite el buffer que abre una sesión FTD y apague el switchport conectado con la interfaz e1/6. En FTD CLI usted debe ver que fueron ambas interfaces abajo:

```
> 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
>
```

La demostración de los registros FTD:

```
> 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 estatus del en línea-conjunto 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 estatus 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 que usted vuelva a permitir 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)
>

```

NAT estático de la configuración de la verificación 5.

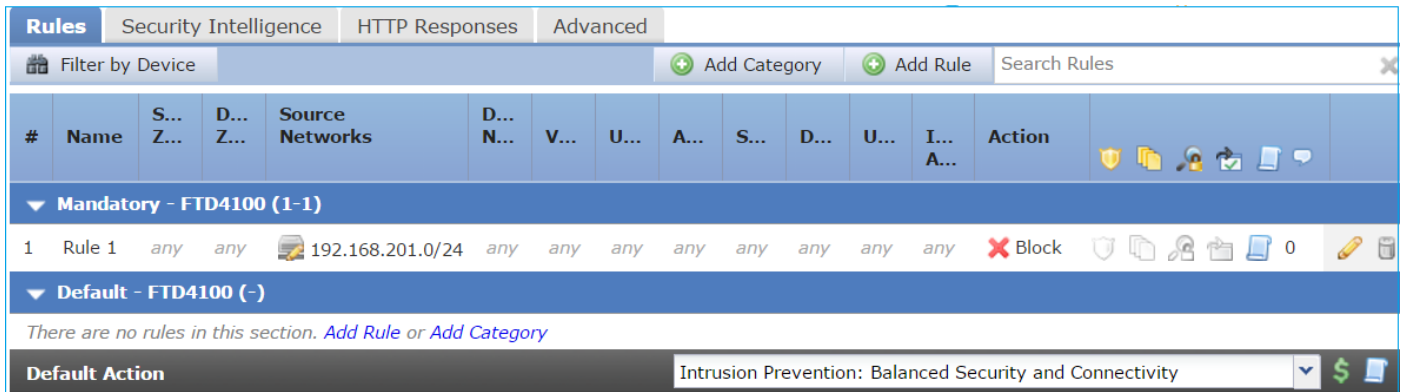
Solución

El NAT no se soporta para las interfaces que actúa adentro el golpecito o a los modos pasivos en línea, en línea:

<http://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config->

Bloquear paquete en el modo en línea de la interfaz de los pares

Cree una regla de bloques, envíe el tráfico con los pares en línea FTD y observe el comportamiento tal y como se muestra en de la imagen.



Solución

Habilite la captura con la traza y envíe los paquetes SYN/ACK con los pares en línea FTD. Se bloquea el tráfico:

```
> 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 traza, 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

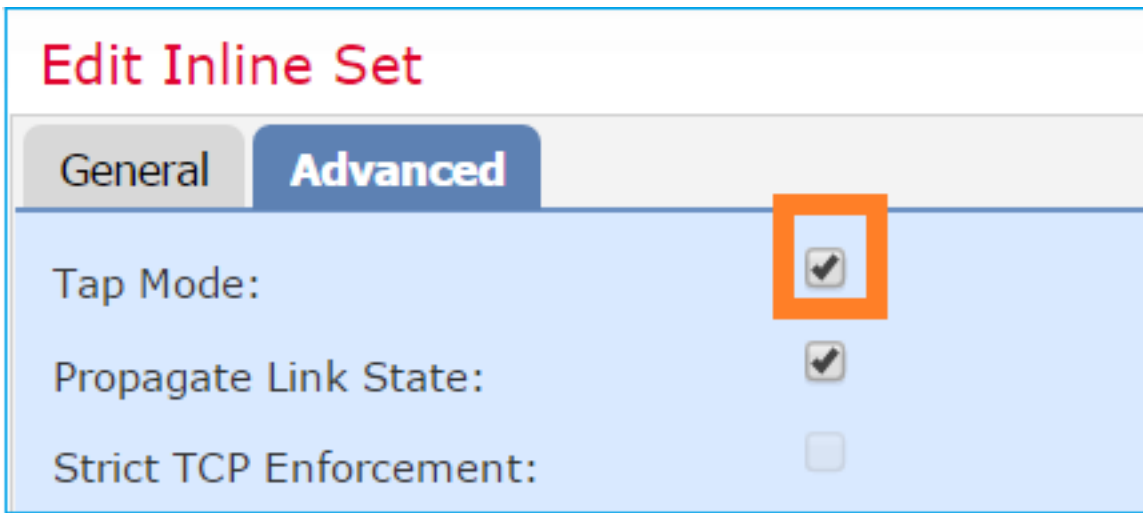
En esta traza, puede ser visto que el paquete fue caído por el motor FTD ASA y no remitido al motor del Snort FTD.

Modo en línea de los pares de la configuración con el golpecito

Modo tap del permiso en los pares en línea.

Solución

Navegue a los dispositivos > a la Administración de dispositivos > en línea los conjuntos > editan el conjunto en línea > avanzó y habilitan el modo tap tal y como se muestra en de la imagen.



Verificación

```
> show inline-set
```

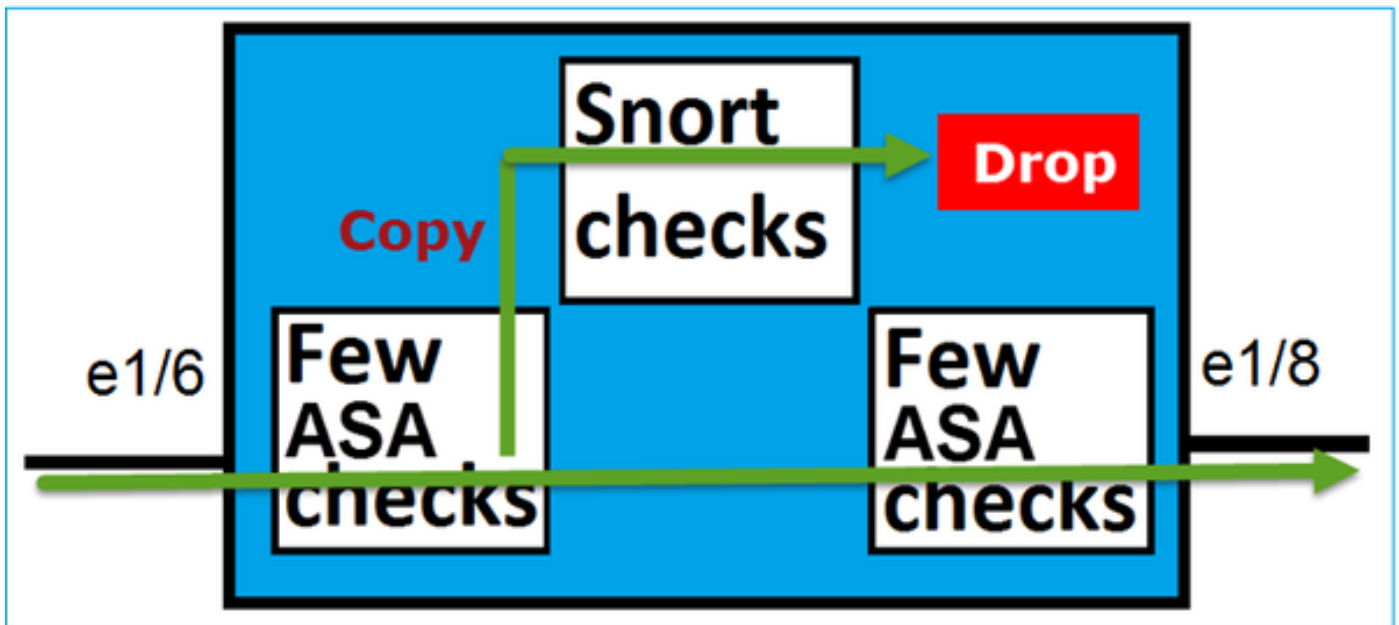
```
Inline-set Inline-Pair-1
Mtu is 1500 bytes
Failsafe mode is on/activated
Failsecure mode is off
Tap mode is on
Propagate-link-state option is on
hardware-bypass mode is disabled
Interface-Pair[1]:
  Interface: Ethernet1/6 "INSIDE"
  Current-Status: UP
  Interface: Ethernet1/8 "OUTSIDE"
  Current-Status: UP
  Bridge Group ID: 0
>
```

Verifique los pares en línea FTD con la operación de la interfaz del golpecito

Teoría básica

- Cuando usted configura un par en línea con el golpecito 2, las interfaces físicas internamente se interligan
- Está disponible en los modos ruteados o transparentes del despliegue
- La mayor parte de las características del motor ASA (NAT, encaminamiento, L3/L4 ACL etc) no están disponibles para los flujos que pasa con los pares en línea
- El tráfico real no puede ser caído
- Pocos controles del motor ASA son aplicados junto con los controles completos del motor del Snort a una copia del tráfico real

La punta más reciente está tal y como se muestra en de la imagen.



El par en línea con el modo del golpecito no cae el tráfico de tránsito. Con la traza 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
>
```

Troubleshooting

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

Comparación: Pares en línea contra los pares en línea con el golpecito

	Pares en línea	Pares en línea con el golpecito
	>muestre el en línea-conjunto	> muestre el en línea-conjunto
muestre el en línea-conjunto	<pre>En línea-conjunto Inline-Pair-1 El MTU es 1500 bytes El modo a prueba de averías es on/activated El modo de Failsecure está apagado El modo tap está apagado la opción del Propagación-link-estado está prendido se inhabilita el modo de hardware-puente Interface-Pair[1]: Interfaz: Ethernet1/6 "INTERIOR" Estado actual: EN FUNCIONAMIENTO Interfaz: Ethernet1/8 "EXTERIOR" Estado actual: EN FUNCIONAMIENTO ID de grupo del Bridge: 509</pre>	<pre>En línea-conjunto Inline-Pair-1 El MTU es 1500 bytes El modo a prueba de averías es on/activated El modo de Failsecure está apagado El modo tap está prendido la opción del Propagación-link-estado está prendido se inhabilita el modo de hardware-puente Interface-Pair[1]: Interfaz: Ethernet1/6 "INTERIOR" Estado actual: EN FUNCIONAMIENTO Interfaz: Ethernet1/8 "EXTERIOR" Estado actual: EN FUNCIONAMIENTO ID de grupo del Bridge: 0</pre>
	> muestre la interfaz e1/6	> muestre la interfaz e1/6
	<pre>Interconecte Ethernet1/6 "INTERIOR", está para arriba, Line Protocol está para arriba El hardware es EtherSVI, 1000 Mbps de BW, usec DLY 1000 Dirección MAC 5897.bdb9.770e, MTU 1500 IPS Interfaz-MODE: en línea, En línea-conjunto: Inline-Pair-1 Dirección IP no asignada Estadísticas de tráfico para el "INTERIOR": entrada de 3957 paquetes, 264913 bytes salida de 144 paquetes, 58664 bytes 4 paquetes caídos 1 pkts minucioso/sec de la velocidad de entrada 0, 26 bytes/sec 1 pkts/sec de la tarifa de salida de minuto 0, 7 bytes/sec 1 tarifa minuciosa del descenso, 0 pkts/sec 5 pkts minuciosos/sec de la velocidad de entrada 0, 28 bytes/sec 5 pkts/sec de la tarifa de salida de minuto 0, 9 bytes/sec 5 tarifas minuciosas del descenso, 0 pkts/sec</pre>	<pre>Interconecte Ethernet1/6 "INTERIOR", está para arriba, Line Protocol está arriba El hardware es EtherSVI, 1000 Mbps de BW, usec DLY 1000 Dirección MAC 5897.bdb9.770e, MTU 1500 IPS Interfaz-MODE: en línea-golpecito, En línea-conjunto: Inline-Pair-1 Dirección IP no asignada Estadísticas de tráfico para el "INTERIOR": 24 entradas de los paquetes, 1378 bytes 0 salidas de los paquetes, bytes 0 24 paquetes caídos 1 pkts minucioso/sec de la velocidad de entrada 0, 0 bytes/sec 1 pkts/sec de la tarifa de salida de minuto 0, 0 bytes/sec 1 tarifa minuciosa del descenso, 0 pkts/sec 5 pkts minuciosos/sec de la velocidad de entrada 0, 0 bytes/sec 5 pkts/sec de la tarifa de salida de minuto 0, 0 bytes/sec 5 tarifas minuciosas del descenso, 0 pkts/sec</pre>
show interface	> muestre la interfaz e1/8	> muestre la interfaz e1/8
	<pre>Interconecte Ethernet1/8 "EXTERIOR", está para arriba, Line Protocol está para arriba El hardware es EtherSVI, 1000 Mbps de BW, usec DLY 1000 Dirección MAC 5897.bdb9.774d, MTU 1500 IPS Interfaz-MODE: en línea, En línea-conjunto: Inline-Pair-1 Dirección IP no asignada Estadísticas de tráfico para el "EXTERIOR": entrada de 144 paquetes, 55634 bytes salida de 3954 paquetes, 339987 bytes paquetes 0 caídos 1 pkts minucioso/sec de la velocidad de entrada 0, 7 bytes/sec 1 pkts/sec de la tarifa de salida de minuto 0, 37 bytes/sec 1 tarifa minuciosa del descenso, 0 pkts/sec 5 pkts minuciosos/sec de la velocidad de entrada 0, 8 bytes/sec 5 pkts/sec de la tarifa de salida de minuto 0, 39 bytes/sec 5 tarifas minuciosas del descenso, 0 pkts/sec</pre>	<pre>Interconecte Ethernet1/8 "EXTERIOR", está para arriba, Line Protocol está arriba El hardware es EtherSVI, 1000 Mbps de BW, usec DLY 1000 Dirección MAC 5897.bdb9.774d, MTU 1500 IPS Interfaz-MODE: en línea-golpecito, En línea-conjunto: Inline-Pair-1 Dirección IP no asignada Estadísticas de tráfico para el "EXTERIOR": 1 entrada de los paquetes, 441 bytes 0 salidas de los paquetes, bytes 0 paquetes 1 caídos 1 pkts minucioso/sec de la velocidad de entrada 0, 0 bytes/sec 1 pkts/sec de la tarifa de salida de minuto 0, 0 bytes/sec 1 tarifa minuciosa del descenso, 0 pkts/sec 5 pkts minuciosos/sec de la velocidad de entrada 0, 0 bytes/sec 5 pkts/sec de la tarifa de salida de minuto 0, 0 bytes/sec 5 tarifas minuciosas del descenso, 0 pkts/sec</pre>
Para manejar	> muestre a paquete-número de la captura CAPI 1 traza	> muestre a paquete-número de la captura CAPI 1 traza

3 paquetes capturados

1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: Triunfo 8192 S 0:0(0)
ack 0
Fase: 1
Tipo: CAPTURA
Subtipo:
Resultado: PERMITA
Config:
Información adicional:
Lista de acceso MAC

Fase: 2
Tipo: LISTA DE ACCESO
Subtipo:
Resultado: PERMITA
Config:
Regla implícita
Información adicional:
Lista de acceso MAC

Fase: 3
Tipo: NGIPS-MODE
Subtipo: ngips-MODE
Resultado: PERMITA
Config:
Información adicional:
El flujo ingresado una interfaz configurada para el modo NGIPS y los servicios NGIPS serán aplicados

Fase: 4
Tipo: LISTA DE ACCESO
Subtipo: registro
Resultado: DESCENSO
Config:
acceso-grupo CSM_FW_ACL_ global
la lista de acceso CSM_FW_ACL_ avanzada niega a IP 192.168.201.0
255.255.255.0 cualquier flujo-principio del registro de acontecimientos regla-
identificación 268441600
regla-identificación 268441600 de la observación de la lista de acceso
CSM_FW_ACL_: POLÍTICA DE ACCESO: FTD4100 - Mandatory/1
regla-identificación 268441600 de la observación de la lista de acceso
CSM_FW_ACL_: REGLA L4: Regla 1
Información adicional:

Resultado:
interfaz de entrada: DENTRO
entrada-estatus: en funcionamiento
entrada-línea-estatus: en funcionamiento
Acción: descenso
Descenso-razón: el flujo (del ACL-descenso) es negado por la regla configurada

1 paquete mostrado
>

3 paquetes capturados

1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: Triunfo 8192 S 0:0(0)
Fase: 1
Tipo: CAPTURA
Subtipo:
Resultado: PERMITA
Config:
Información adicional:
Lista de acceso MAC

Fase: 2
Tipo: LISTA DE ACCESO
Subtipo:
Resultado: PERMITA
Config:
Regla implícita
Información adicional:
Lista de acceso MAC

Fase: 3
Tipo: NGIPS-MODE
Subtipo: ngips-MODE
Resultado: PERMITA
Config:
Información adicional:
El flujo ingresado una interfaz configurada para el modo NGIPS y los servicios NGIPS serán aplicados

Fase: 4
Tipo: LISTA DE ACCESO
Subtipo: registro
Resultado: HABRÍA CAÍDO
Config:
acceso-grupo CSM_FW_ACL_ global
la lista de acceso CSM_FW_ACL_ avanzada niega a IP 192.168.201.0
255.255.255.0 cualquier flujo-principio del registro de acontecimientos regla-
identificación 268441600
regla-identificación 268441600 de la observación de la lista de acceso
CSM_FW_ACL_: POLÍTICA DE ACCESO: FTD4100 - Mandatory/1
regla-identificación 268441600 de la observación de la lista de acceso
CSM_FW_ACL_: REGLA L4: Regla 1
Información adicional:

Resultado:
interfaz de entrada: DENTRO
entrada-estatus: en funcionamiento
entrada-línea-estatus: en funcionamiento
Acción: La lista de acceso habría caído, solamente en línea-golpecito debido a un paquete remitido paquete

1 paquete mostrado
>

el paquete
con la regla
de bloques

Resumen

- Cuando usted utiliza el modo en línea de los pares, el paquete pasa principalmente a través del motor del Snort FTD.
- Las conexiones TCP se manejan en un modo de estado-puente TCP.
- Desde un punto de vista del motor FTD ASA, una directiva ACL es aplicada.
- Cuando el modo en línea de los pares es funcionando, los paquetes pueden ser bloqueados puesto que se procesan en línea.
- Cuando se habilita el modo tap, una copia del paquete se examina y se cae internamente mientras que el tráfico real pasa con FTD sin modificar.

Información Relacionada

- [Cisco FirePOWER NGFW](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)