

# Configurar relações FTD no modo dos Inline-pares

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar a relação Inline dos pares em FTD](#)

[Diagrama de Rede](#)

[Verifique a operação Inline da relação dos pares FTD](#)

[Teoria básica](#)

[Verificação 1. Com o uso do Pacote-projétil luminoso](#)

[A verificação 2. envia pacotes TCP SYN/ACK com os pares Inline](#)

[O motor do Firewall da verificação 3. debuga para o tráfego permitido](#)

[A verificação 4. verifica a propagação do link-state](#)

[A verificação 5. configura o NAT estático](#)

[O bloquear pacote em pares Inline conecta o modo](#)

[Configurar o modo Inline dos pares com torneira](#)

[Verifique pares Inline FTD com operação da relação da torneira](#)

[Comparação: Pares Inline contra pares Inline com torneira](#)

[Resumo](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve a configuração, a verificação e a operação de fundo de uma relação Inline dos pares em um dispositivo da defesa da ameaça da potência de fogo (FTD).

## Pré-requisitos

### Requisitos

Não há umas exigências específicas para este documento.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Potência de fogo 4150 que executa o código 6.1.0.x FTD

- Centro de gerenciamento da potência de fogo (FMC) que executa 6.1.0.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

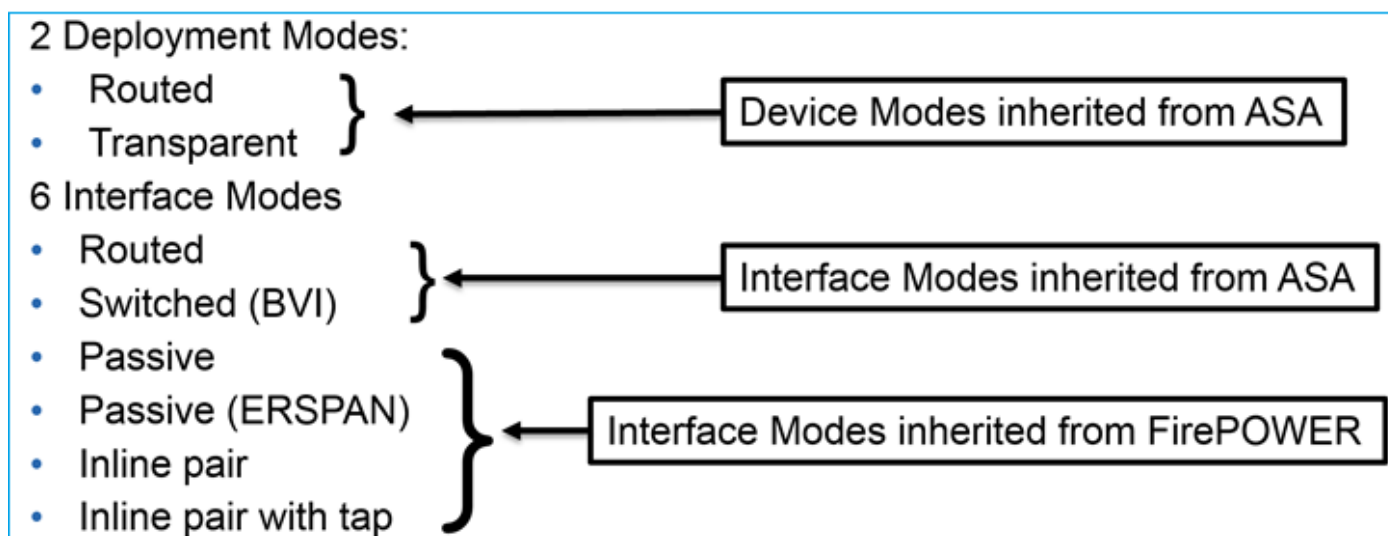
## Produtos Relacionados

Este documento pode igualmente ser usado com estes versão de 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), serviços de Web das Amazonas (AW), teclado/vídeo/rato (KVM)
- Código de software 6.2.x FTD e mais tarde

## Informações de Apoio

FTD fornece dois modos do desenvolvimento e seis modos da relação segundo as indicações da imagem:



Nota: Você pode misturar modos da relação em um dispositivo do sigle FTD.

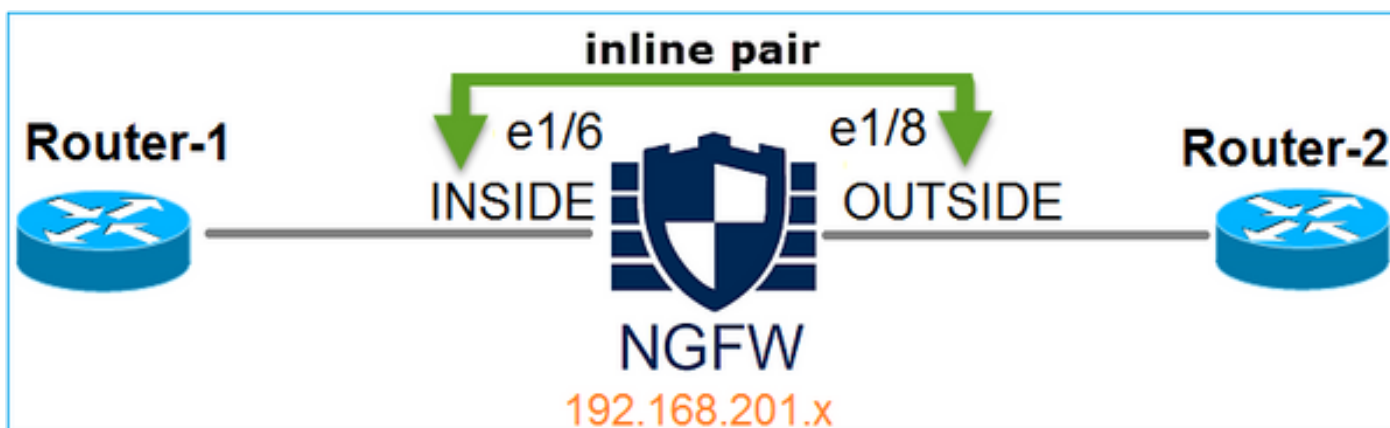
Está aqui uma visão geral de alto nível dos vários modos do desenvolvimento e da relação FTD:

Modo da relação FTD	Modo do desenvolvimento o FTD	Descrição	O tráfego pode ser deixado cair
Roteado	Roteado	ASA-motor e verificações completos do Snort-motor	Sim
Comutado	Transparente	ASA-motor e verificações completos do Snort-motor	Sim
Pares Inline	Roteado ou transparente	ASA-motor parcial e verificações completas do Snort-motor	Sim
Pares Inline com	Roteado ou	ASA-motor parcial e verificações	Não

torneira	transparente	completas do Snort-motor	
Passivo	Roteado ou transparente	ASA-motor parcial e verificações completas do Snort-motor	Não
Voz passiva (ERSPAN)	Roteado	ASA-motor parcial e verificações completas do Snort-motor	Não

## Configurar a relação Inline dos pares em FTD

### Diagrama de Rede



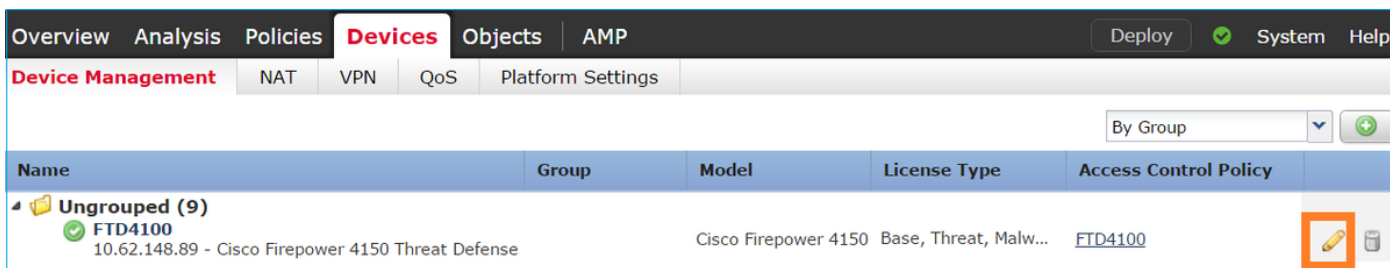
### Exigência

Configurar as interfaces física e1/6 e e1/8 no modo Inline dos pares conforme estas exigências:

Interface	e1/6	e1/8
Nome	INTERNA	EXTERNA
Zona de Segurança	INSIDE_ZONE	OUTSIDE_ZONE
Nome de conjunto Inline	Inline-Pair-1	
Grupo Inline MTU	1500	
Àprova de falhas	Habilitado	
Estado do link da propagação	Habilitado	

### Solução

Etapa 1. A fim configurar às interfaces individuais, para navegar aos **dispositivos** > ao **Gerenciamento de dispositivos**, para seleccionar o dispositivo apropriado e ao clique **edite** segundo as indicações da imagem.



Em seguida, especifique o **nome** e o tiquetaque **permitidos** para a relação segundo as indicações da imagem.

## Edit Physical Interface

Mode:

Name:   Enabled  Management Only

Security Zone:

Description:

**General** | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU:  (64 - 9188)

Interface ID:

Nota: O nome é o o nameif da relação.

Similarmente para a relação Ethernet1/8. O resultado final é segundo as indicações da imagem.

Overview Analysis Policies **Devices** Objects AMP   System Help **admin**

**Device Management** NAT VPN QoS Platform Settings

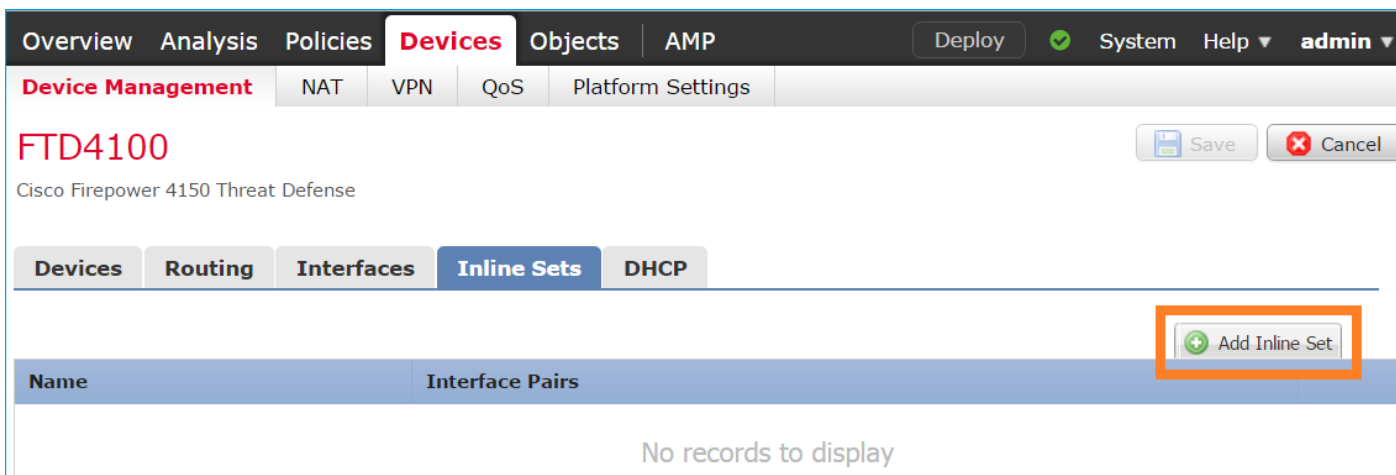
**FTD4100**  
Cisco Firepower 4150 Threat Defense

**Devices** Routing **Interfaces** Inline Sets DHCP  Add Interfaces

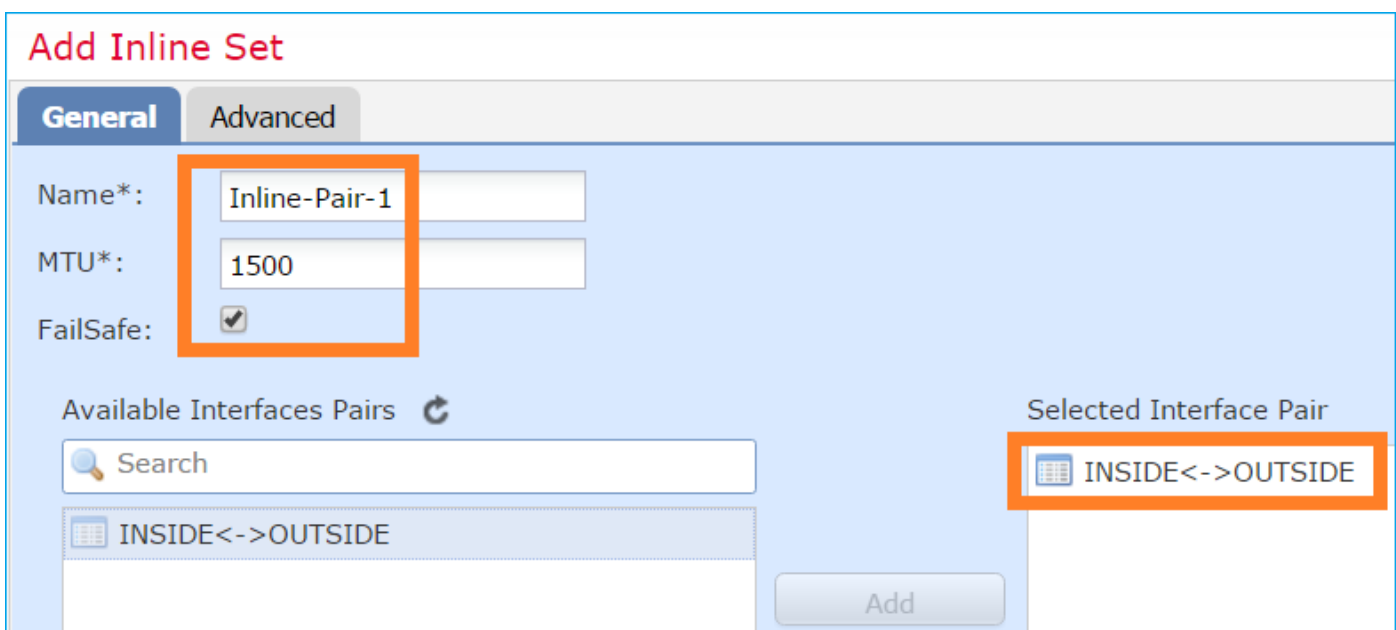
...	Interface	Logical Name	Type	Security Zo...	MAC Address (Active/...	IP Address
<input checked="" type="checkbox"/>	Ethernet1/6	INSIDE	Physical			
<input checked="" type="checkbox"/>	Ethernet1/7	diagnostic	Physical			
<input checked="" type="checkbox"/>	Ethernet1/8	OUTSIDE	Physical			

Etapa 2. Configurar os pares Inline.

Navegue ao > Add Inline dos grupos ajustado Inline segundo as indicações da imagem.

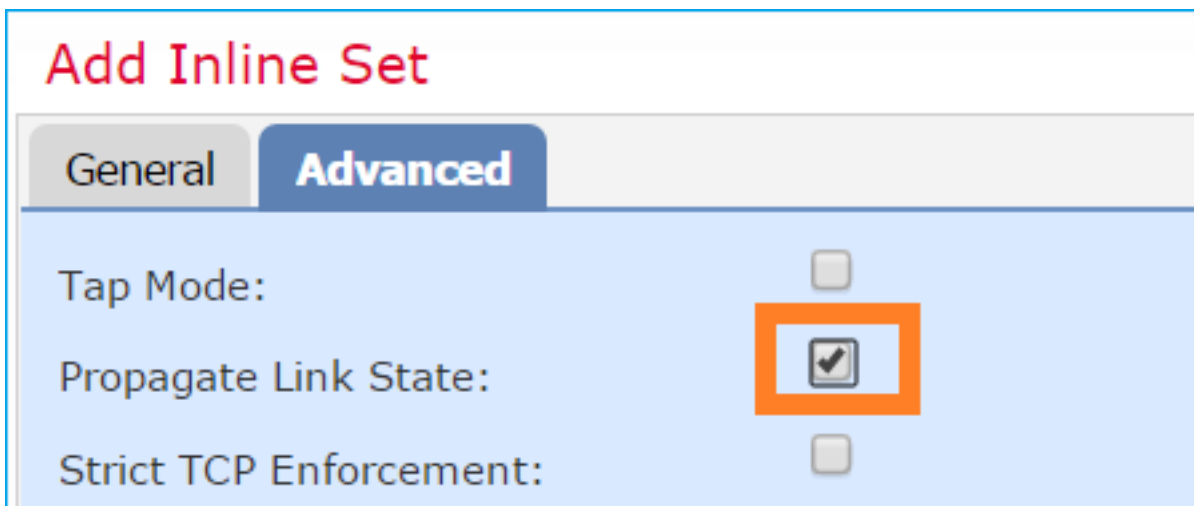


Etapa 3. Configurar os ajustes gerais conforme as exigências segundo as indicações da imagem.



Nota: À prova de falhas permite que o tráfego passe com os pares inline uninspected caso que os buffers da relação estão completos (visto tipicamente quando o dispositivo é sobrecarregado ou o motor do Snort está sobrecarregado). O tamanho de buffer da relação é atribuído dinamicamente.

Etapa 4. Permita a opção do **estado do link da propagação nos ajustes avançados** segundo as indicações da imagem.



A propagação do estado do link derruba automaticamente a segunda relação nos pares inline da relação quando uma das relações no grupo inline vai para baixo.

Etapa 5. **Salvar as mudanças e distribua-as.**

### Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique a configuração Inline dos pares do FTD CLI.

### Solução

Entre a FTD CLI e verifique a configuração Inline dos 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
>
```

Nota: O grupo de bridge ID é um valor diferente do que 0. Se o modo da torneira está em então é 0

Relação e informação de nome:

```
> show nameif
```

Interface	Name	Security
-----------	------	----------

```

Ethernet1/6          INSIDE          0
Ethernet1/7          diagnostic      0
Ethernet1/8          OUTSIDE        0
>

```

Verifique o status da interface:

```

> 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 a informação da interface 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 a operação Inline da relação dos pares FTD

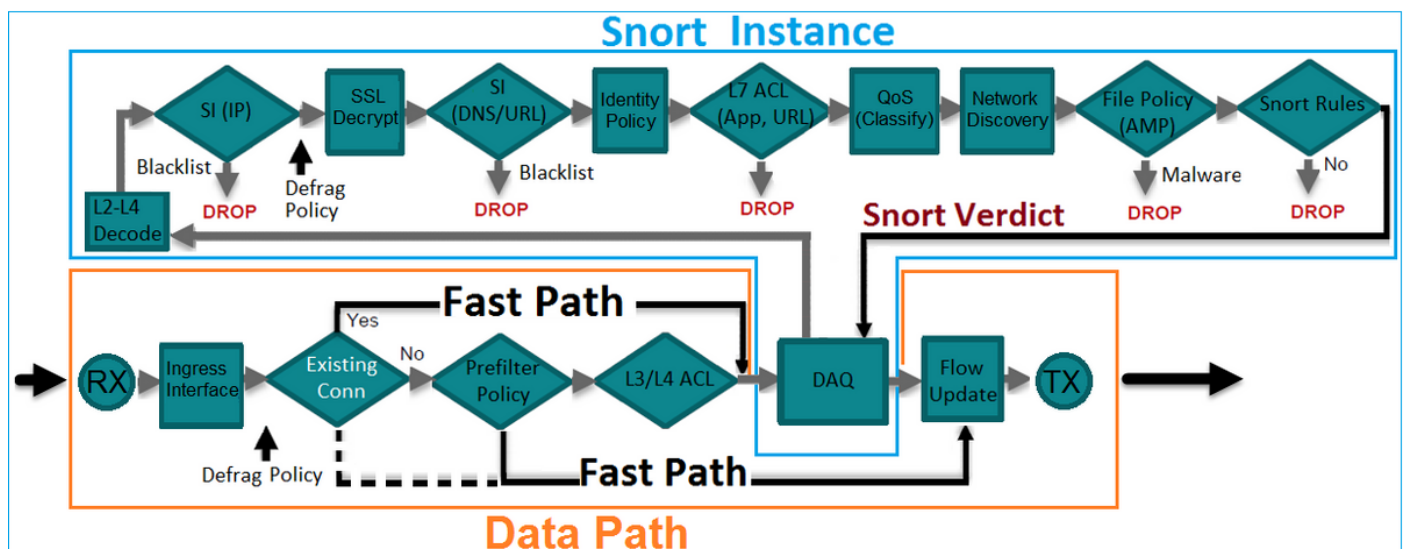
Esta seção cobre estas verificações da verificação a fim verificar a operação Inline dos pares:

- Verificação 1. Com o uso do pacote-projétil luminoso.
- A verificação 2. permite a captação com traço e envia um sincronizar TCP/reconhece o pacote (SYN/ACK) com os pares Inline.
- O tráfego do monitor FTD da verificação 3. com o uso do motor do Firewall debuga.
- A verificação 4. verifica a funcionalidade da propagação do link-state.
- A verificação 5. configura a tradução de endereço da rede estática (NAT).

## Solução

Visão geral arquitetural

Quando 2 relações FTD se operam no modo dos Inline-pares um pacote está segurado segundo as indicações da imagem.

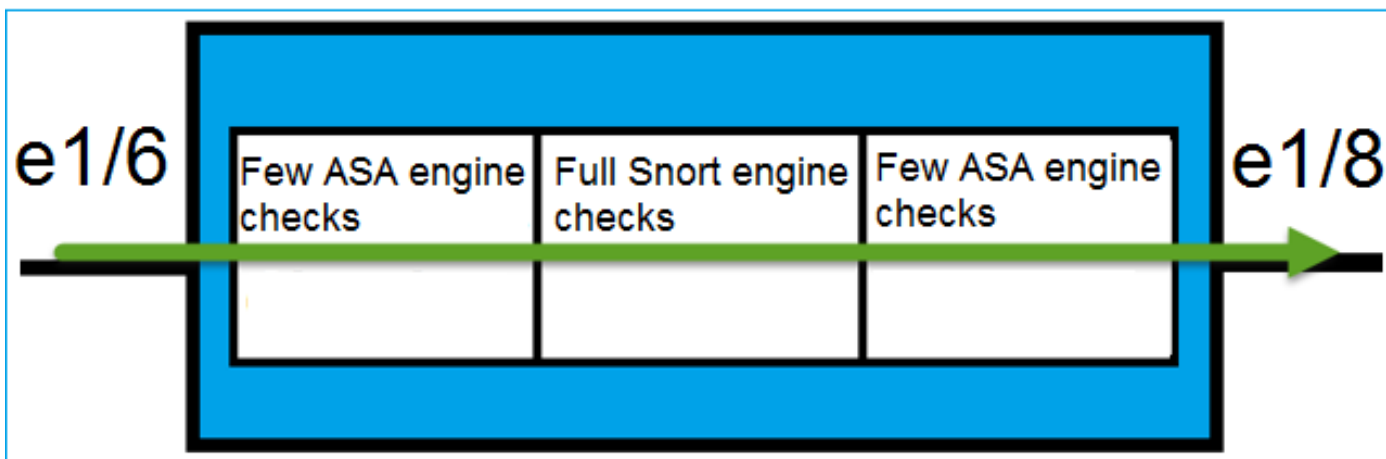


Nota: Somente as interfaces física podem ser membros de um par Inline ajustado

## Teoria básica

- Quando você configura um par Inline 2 interfaces física está construído uma ponte sobre internamente
  - Muito similar ao Intrusion Prevention System (IPS) inline clássico
  - Disponível em modos roteados ou transparentes do desenvolvimento
  - A maioria das características do motor ASA (NAT, roteamento, L3/L4 ACL etc.) não estão disponíveis para fluxos que atravessam um par Inline
  - O tráfego de trânsito pode ser deixado cair
  - Poucas verificações adaptáveis do motor da ferramenta de segurança (ASA) são aplicadas junto com verificações completas do motor do Snort
- O último ponto pode ser visualizado segundo as indicações da imagem.





## Verificação 1. Com o uso do Pacote-projétil luminoso

Está aqui o pacote-projétil luminoso output que emula um pacote que atravesse os pares inline com os pontos importantes destacados:

```
> 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

>

## A verificação 2. envia pacotes TCP SYN/ACK com os pares Inline

Você pode gerar pacotes TCP SYN/ACK com o uso de um pacote esse os serviços de serviço público como Scapy. Esta sintaxe gerencie 3 pacotes com as bandeiras SYN/ACK permitidas:

```
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)
```

Permita esta captura em FTD CLI e envie poucos pacotes 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
>
```

Depois que você envia os pacotes com o FTD você pode ver uma conexão que seja criada:

```
> 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:** bandeira b - Um ASA clássico deixaria cair um pacote espontâneo SYN/ACK a menos que o estado-desvio TCP fosse permitido. Uma relação FTD no modo Inline dos pares segura uma conexão de TCP em um modo do estado-desvio TCP e não deixa cair os pacotes de TCP que não pertencem às conexões que já existem.

**Nota:** A bandeira N o pacote é inspecionada pelo motor do Snort FTD.

As captações provam esta, desde que você pode ver os 3 pacotes que atravessa o 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 pacotes que retira o 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
```

>

Com o traço de primeira captação o pacote revela alguma informação adicional como a sentença do motor do 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
>
```

Com o traço do segundo pacote capturado mostra que o pacote combina uma conexão existente assim que contorneia a verificação ACL, mas é inspecionado ainda pelo motor do 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

```

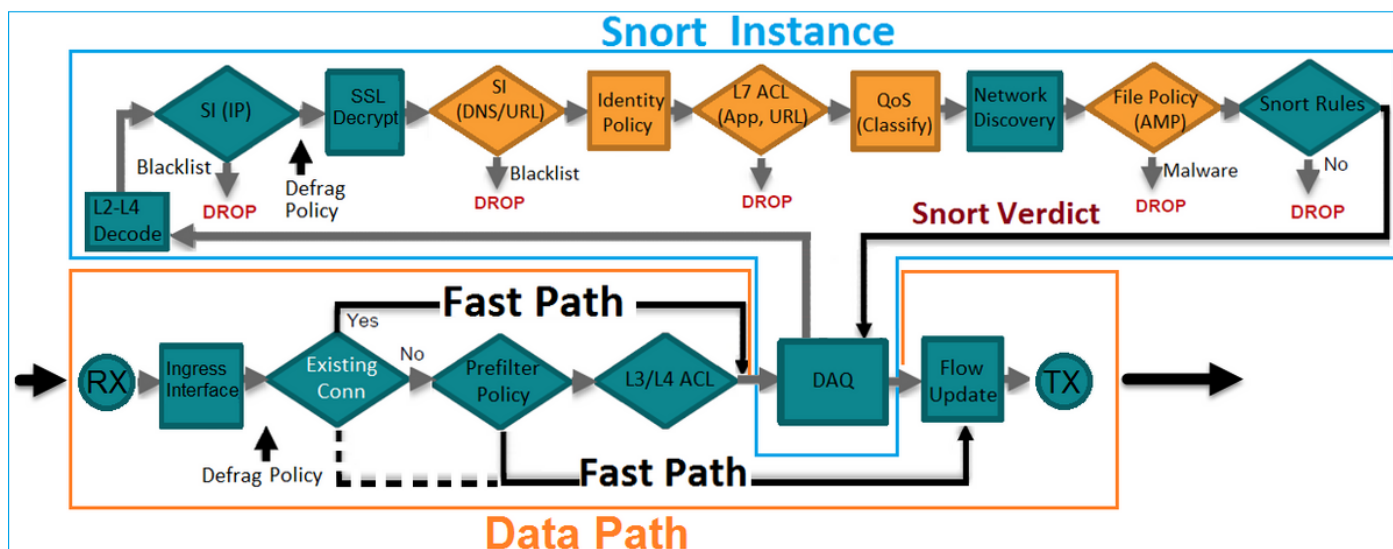
```

1 packet shown
>

```

### O motor do Firewall da verificação 3. debug para o tráfego permitido

O motor do Firewall debuga corridas contra componentes específicos do motor do Snort FTD como a política do controle de acesso segundo as indicações da imagem:



Quando você envia os pacotes TCP SYN/ACK com os pares Inline você pode ver no resultado do debug:

```
> 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

```

### A verificação 4. verifica a propagação do link-state

Permita o buffer que entra FTD e parada programada o switchport conectado à relação e1/6. Em FTD CLI você deve ver que ambas as relações foram para baixo:

```

> 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
>

```

A mostra dos logs 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)
>

```

O estado do inline-grupo mostra o estado dos 2 membros da relação:

```

> 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
>

```

Note a diferença no estado das 2 relações:

```

> 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 para a relação 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

```

>  
Depois que você re-permite o switchport os logs FTD mostram:

```

> 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)
>

```

## A verificação 5. configura o NAT estático

### Solução

O NAT não é apoiado para relações que opera dentro a torneira inline, inline ou os modos passivos:

<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>

## Bloquear pacote no modo Inline da relação dos pares

Crie uma regra de bloqueio, envie o tráfego com os pares Inline FTD e observe o comportamento segundo as indicações da imagem.

Rules													Security Intelligence	HTTP Responses	Advanced	
Filter by Device													+ Add Category	+ Add Rule	Search Rules	
#	Name	S... Z...	D... Z...	Source Networks	D... N...	V...	U...	A...	S...	D...	U...	I... A...	Action			
▼ Mandatory - FTD4100 (1-1)																
1	Rule 1	any	any	192.168.201.0/24	any	any	any	any	any	any	any	any	Block			
▼ Default - FTD4100 (-)																
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>																
Default Action													Intrusion Prevention: Balanced Security and Connectivity			

### Solução



Permita a captação com traço e envie os pacotes SYN/ACK com os pares Inline FTD. O tráfego é obstruído:

```
> 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
```

Com o traço, um pacote 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 ingresses 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

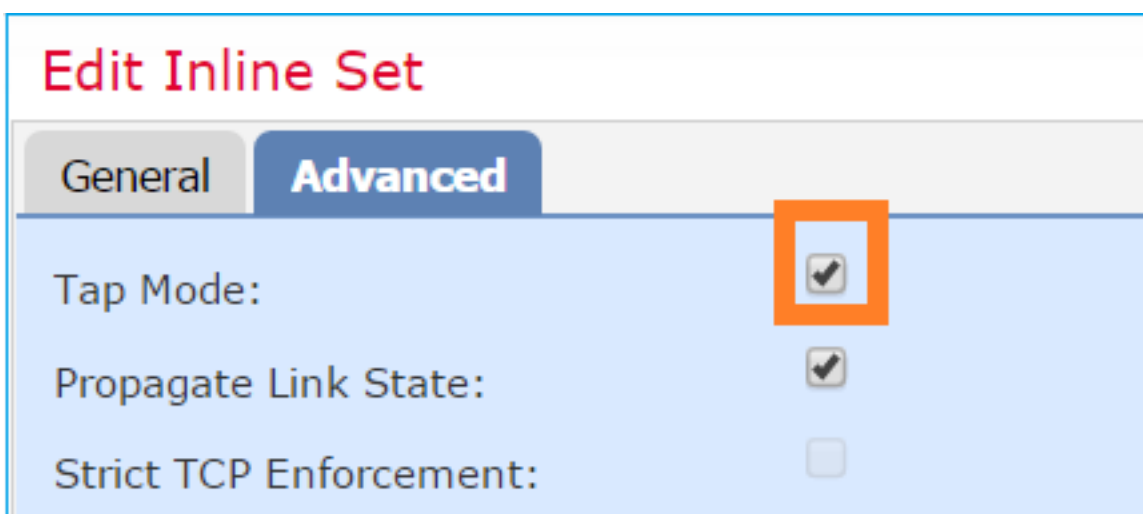
Neste traço, pode-se ver que o pacote esteve deixado cair pelo motor FTD ASA e não enviado ao motor do Snort FTD.

## Configurar o modo Inline dos pares com torneira

Permita o modo da torneira nos pares Inline.

### Solução

Navegue aos **dispositivos** > ao **Gerenciamento de dispositivos** > **Inline grupos** > **editam o grupo Inline** > **avançou** e permitem o **modo da torneira** segundo as indicações da imagem.



### Verificação

```
> show inline-set
```

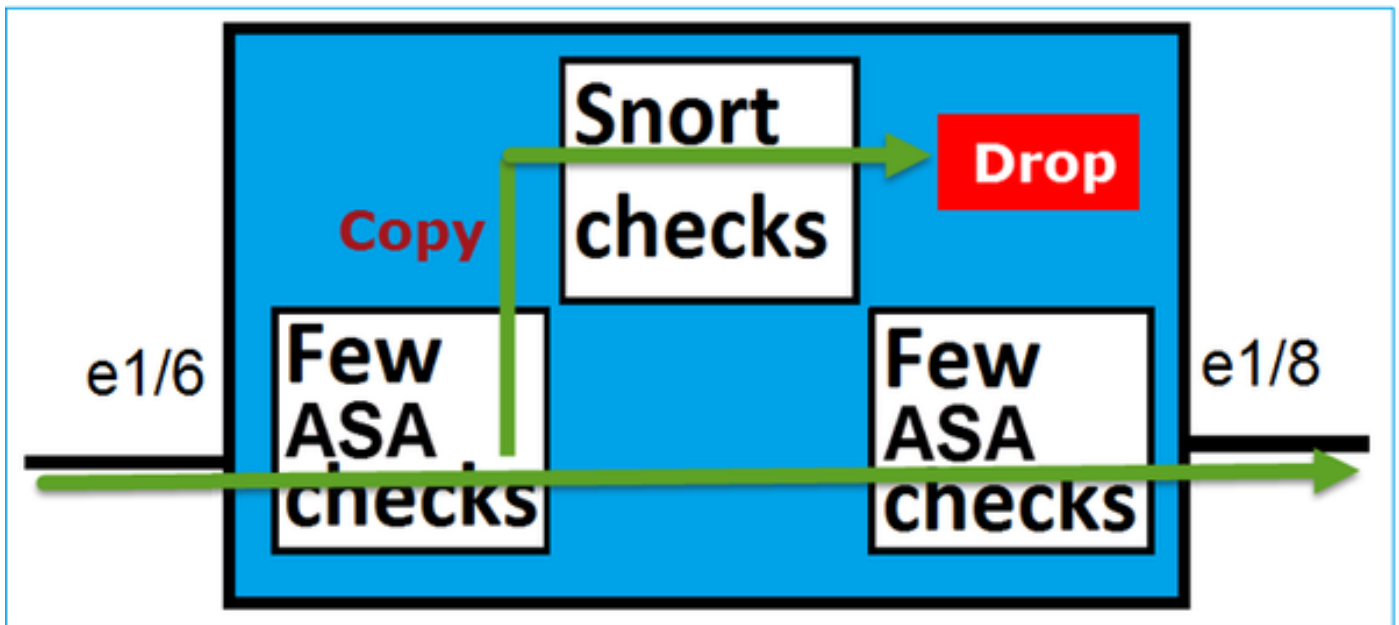
```
Inline-set Inline-Pair-1
Mtu is 1500 bytes
Failsafe mode is on/activated
Failsecure mode is off
Tap mode is on
Propagate-link-state option is on
hardware-bypass mode is disabled
Interface-Pair[1]:
  Interface: Ethernet1/6 "INSIDE"
  Current-Status: UP
  Interface: Ethernet1/8 "OUTSIDE"
  Current-Status: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

## Verifique pares Inline FTD com operação da relação da torneira

Teoria básica

- Quando você configura um par Inline com torneira 2, as interfaces física estão construídas uma ponte sobre internamente
- Está disponível em modos roteados ou transparentes do desenvolvimento
- A maioria das características do motor ASA (NAT, roteamento, L3/L4 ACL etc.) não estão disponíveis para fluxos que atravessam os pares Inline
- O tráfego real não pode ser deixado cair
- Poucas verificações do motor ASA são aplicadas junto com verificações completas do motor do Snort a uma cópia do tráfego real

O último ponto é segundo as indicações da imagem.



O par Inline com modo da torneira não deixa cair o tráfego de trânsito. Com o traço de um pacote confirma este:

```
> 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 ingresssed 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

>

## Comparação: Pares Inline contra pares Inline com torneira

### Pares Inline

> mostre o inline-grupo

Inline-grupo Inline-Pair-1  
O MTU é 1500 bytes  
O modo à prova de falhas é on/activated  
O modo de Failsecure está  
**O modo da torneira está**  
a opção do Propagação-link-estado está ligada  
o modo do hardware-desvio é desabilitado  
Interface-Pair[1]:  
Interface: Ethernet1/6 "INTERIOR"  
Status atual: PARA CIMA  
Interface: Ethernet1/8 "PARTE EXTERNA"  
Status atual: PARA CIMA  
**Grupo de bridge ID: 509**

>

> mostre a relação e1/6

Conecte Ethernet1/6 "INTERIOR", esteja acima, protocolo de linha está acima  
O hardware é EtherSVI, 1000 Mbps de BW, usec DLY 1000  
MAC address 5897.bdb9.770e, MTU 1500  
IPS Relação-MODE: **inline**, Inline-grupo: Inline-Pair-1  
Endereço IP de Um ou Mais Servidores Cisco ICM NT unassigned  
Estatísticas de tráfego para o "INTERIOR":  
entrada de 3957 pacotes, 264913 bytes  
saída de 144 pacotes, 58664 bytes  
4 pacotes deixados cair  
1 pacotes minutos da taxa de entrada 0/segundo, 26 bytes/segundo  
1 pacotes da taxa de saídas por minuto 0/segundo, 7 bytes/segundo  
1 taxa minuto da gota, 0 pacotes/segundo  
pacotes da taxa de entrada 0 do minuto 5/segundo, 28 bytes/segundo  
pacotes da taxa de saídas por minuto 5 0/segundo, 9 bytes/segundo  
taxa da gota do minuto 5, 0 pacotes/segundo

> mostre a relação e1/8

Conecte Ethernet1/8 "PARTE EXTERNA", esteja acima, protocolo de linha está acima  
O hardware é EtherSVI, 1000 Mbps de BW, usec DLY 1000  
MAC address 5897.bdb9.774d, MTU 1500  
IPS Relação-MODE: **inline**, Inline-grupo: Inline-Pair-1  
Endereço IP de Um ou Mais Servidores Cisco ICM NT unassigned  
Estatísticas de tráfego para a "PARTE EXTERNA":  
entrada de 144 pacotes, 55634 bytes  
saída de 3954 pacotes, 339987 bytes  
pacotes 0 deixados cair  
1 pacotes minutos da taxa de entrada 0/segundo, 7 bytes/segundo  
1 pacotes da taxa de saídas por minuto 0/segundo, 37 bytes/segundo  
1 taxa minuto da gota, 0 pacotes/segundo  
pacotes da taxa de entrada 0 do minuto 5/segundo, 8 bytes/segundo

### Pares Inline com torneira

> mostre o inline-grupo

Inline-grupo Inline-Pair-1  
O MTU é 1500 bytes  
O modo à prova de falhas é on/activated  
O modo de Failsecure está  
**O modo da torneira está ligada**  
a opção do Propagação-link-estado está ligada  
o modo do hardware-desvio é desabilitado  
Interface-Pair[1]:  
Interface: Ethernet1/6 "INTERIOR"  
Status atual: PARA CIMA  
Interface: Ethernet1/8 "PARTE EXTERNA"  
Status atual: PARA CIMA  
**Grupo de bridge ID: 0**

>

> mostre a relação e1/6

Conecte Ethernet1/6 "INTERIOR", esteja acima, protocolo de linha está acima  
O hardware é EtherSVI, 1000 Mbps de BW, usec DLY 1000  
MAC address 5897.bdb9.770e, MTU 1500  
IPS Relação-MODE: **inline-torneira**, Inline-grupo: Inline-Pair-1  
Endereço IP de Um ou Mais Servidores Cisco ICM NT unassigned  
Estatísticas de tráfego para o "INTERIOR":  
24 entradas dos pacotes, 1378 bytes  
0 saídas dos pacotes, bytes 0  
24 pacotes deixados cair  
1 pacotes minutos da taxa de entrada 0/segundo, 0 bytes/segundo  
1 pacotes da taxa de saídas por minuto 0/segundo, 0 bytes/segundo  
1 taxa minuto da gota, 0 pacotes/segundo  
pacotes da taxa de entrada 0 do minuto 5/segundo, 0 bytes/segundo  
pacotes da taxa de saídas por minuto 5 0/segundo, 0 bytes/segundo  
taxa da gota do minuto 5, 0 pacotes/segundo

> mostre a relação e1/8

Conecte Ethernet1/8 "PARTE EXTERNA", esteja acima, protocolo de linha está acima  
O hardware é EtherSVI, 1000 Mbps de BW, usec DLY 1000  
MAC address 5897.bdb9.774d, MTU 1500  
IPS Relação-MODE: **inline-torneira**, Inline-grupo: Inline-Pair-1  
Endereço IP de Um ou Mais Servidores Cisco ICM NT unassigned  
Estatísticas de tráfego para a "PARTE EXTERNA":  
1 entrada dos pacotes, 441 bytes  
0 saídas dos pacotes, bytes 0  
pacotes 1 deixados cair  
1 pacotes minutos da taxa de entrada 0/segundo, 0 bytes/segundo  
1 pacotes da taxa de saídas por minuto 0/segundo, 0 bytes/segundo  
1 taxa minuto da gota, 0 pacotes/segundo  
pacotes da taxa de entrada 0 do minuto 5/segundo, 0 bytes/segundo

mostre o  
inline-grupo

show  
interface

```

pacotes da taxa de saídas por minuto 5 0/segundo, 39 bytes/segundo
taxa da gota do minuto 5, 0 pacotes/segundo
>
> mostre a pacote-número da captação CAPI 1 traço

3 pacotes capturados

1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: Vitória 8192 S 0:0(0)
ack 0
Fase: 1
Digite: CAPTAÇÃO
Subtipo:
Resultado: RESERVE
Configuração:
Informações adicionais:
Lista de acessos MAC

Fase: 2
Digite: LISTA DE ACESSO
Subtipo:
Resultado: RESERVE
Configuração:
Regra implícita
Informações adicionais:
Lista de acessos MAC

Fase: 3
Digite: NGIPS-MODE
Subtipo: ngips-MODE
Resultado: RESERVE
Configuração:
Informações adicionais:
O fluxo ingressou uma relação configurada para o modo NGIPS e os serviços
NGIPS serão aplicados

Fase: 4
Digite: LISTA DE ACESSO
Subtipo: log
Resultado: GOTA
Configuração:
acesso-grupo CSM_FW_ACL_ global
a lista de acesso CSM_FW_ACL_ avançada nega a IP 192.168.201.0 255.255.255.0
todo o fluxo-início do log de eventos regra-identificação 268441600
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_:
POLÍTICA DE ACESSO: FTD4100 - Mandatory/1
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_:
REGRA L4: Regra 1
Informações adicionais:

Resultado:
interface de entrada: INTERNA
entrada-estado: up
entrada-linha-estado: up
Ação: gota
Gota-razão: o fluxo (da ACL-gota) é negado pela regra configurada

1 pacote mostrado
>

```

```

pacotes da taxa de saídas por minuto 5 0/segundo, 0 bytes/segundo
taxa da gota do minuto 5, 0 pacotes/segundo
>
> mostre a pacote-número da captação CAPI 1 traço

3 pacotes capturados

1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: Vitória 8192 S 0:0(0)
ack 0
Fase: 1
Digite: CAPTAÇÃO
Subtipo:
Resultado: RESERVE
Configuração:
Informações adicionais:
Lista de acessos MAC

Fase: 2
Digite: LISTA DE ACESSO
Subtipo:
Resultado: RESERVE
Configuração:
Regra implícita
Informações adicionais:
Lista de acessos MAC

Fase: 3
Digite: NGIPS-MODE
Subtipo: ngips-MODE
Resultado: RESERVE
Configuração:
Informações adicionais:
O fluxo ingressou uma relação configurada para o modo NGIPS e os serviços
NGIPS serão aplicados

Fase: 4
Digite: LISTA DE ACESSO
Subtipo: log
Resultado: DEIXARIA CAIR
Configuração:
acesso-grupo CSM_FW_ACL_ global
a lista de acesso CSM_FW_ACL_ avançada nega a IP 192.168.201.0 255.255.255.0
todo o fluxo-início do log de eventos regra-identificação 268441600
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_:
POLÍTICA DE ACESSO: FTD4100 - Mandatory/1
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_:
REGRA L4: Regra 1
Informações adicionais:

Resultado:
interface de entrada: INTERNA
entrada-estado: up
entrada-linha-estado: up
Ação: A lista de acesso deixaria cair, mas inline-torneira devida enviada para
ser processada

1 pacote mostrado
>

```

Para segurar o pacote com regra de bloqueio

## Resumo

- Quando você usa o modo Inline dos pares, o pacote atravessa principalmente o motor do Snort FTD
- As conexões de TCP são seguradas em um modo do estado-desvio TCP
- De um ponto de vista do motor FTD ASA, uma política ACL é aplicada
- Quando o modo Inline dos pares está no uso, os pacotes podem ser obstruídos desde que são processados inline
- Quando o modo da torneira é permitido, uma cópia do pacote está inspecionada e deixada cair internamente quando o tráfego real atravessar FTD unmodified

## Informações Relacionadas

- [Potência de fogo NGFW de Cisco](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)