# Configurar a defesa da ameaça da potência de fogo conecta no modo dos Inline-pares

## Índice

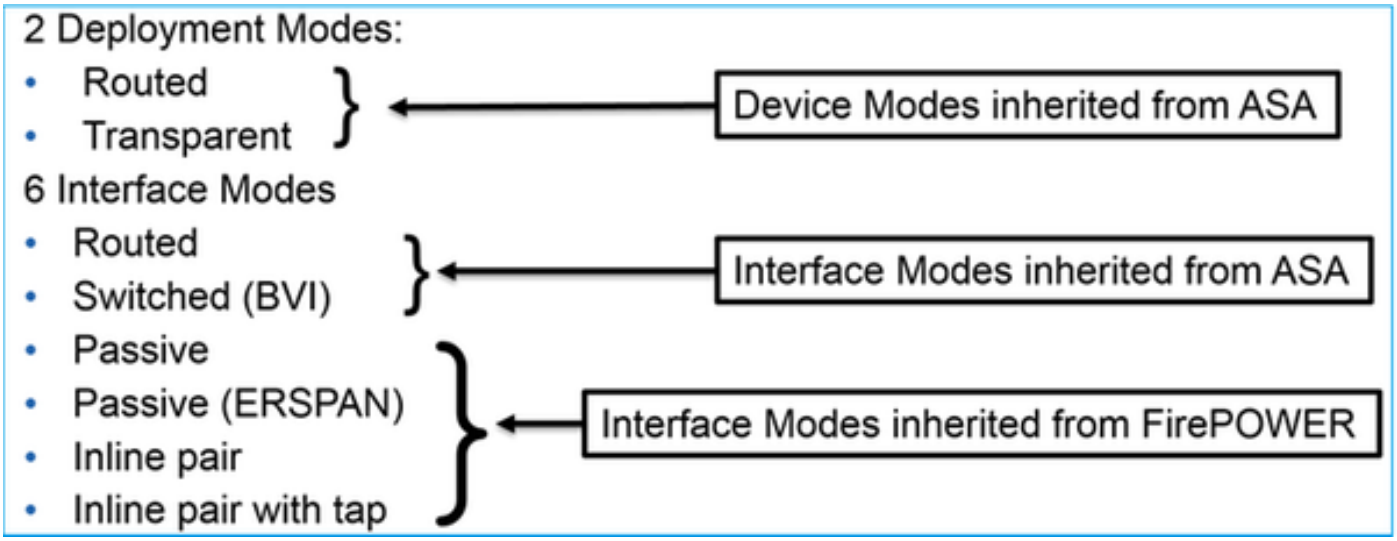


## Introdução

A defesa da ameaça da potência de fogo (FTD) é uma imagem do software unificada que possa ser instalada nas seguintes Plataformas:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Serviços de Web das Amazonas (AW)
- KVM
- Módulo de roteador ISR

FTD fornece 2 modos do desenvolvimento e modos da relação 6




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 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 torneira | Roteado ou transparente | ASA-motor parcial e verificações completas do Snort-motor | Não |
| 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 |

## Objetivo

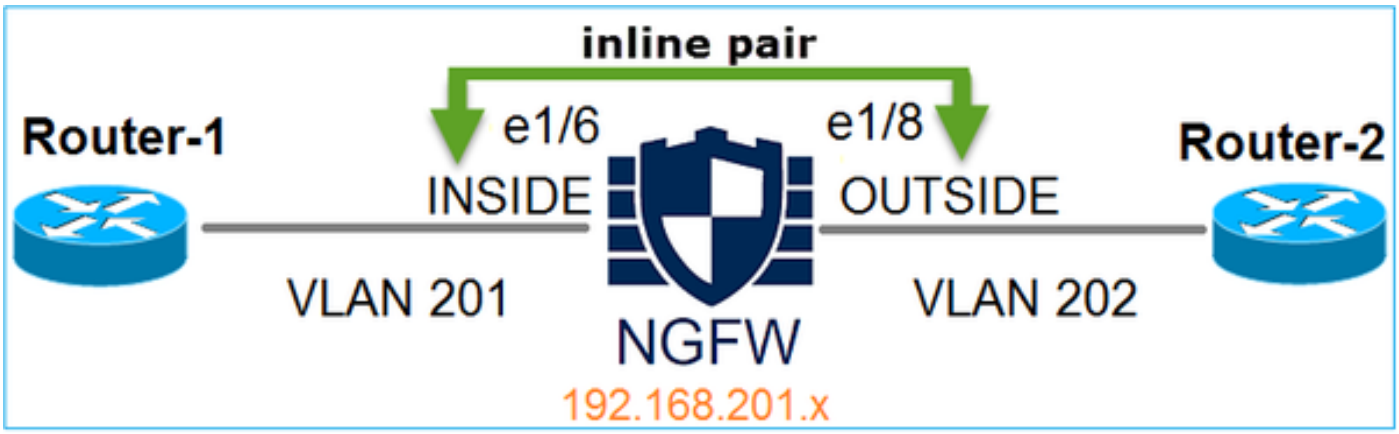
O objetivo deste documento está a:

- Demonstre a configuração e a operação de Inline-pares FTD conecta

## Componentes usados

- Código sendo executado 6.1.0.x da potência de fogo 4150 FTD
- Centro de gerenciamento da potência de fogo (FMC) 6.1.0.x sendo executado

### Topologia




## Configurando uma relação Inline dos pares em FTD

### Exigência

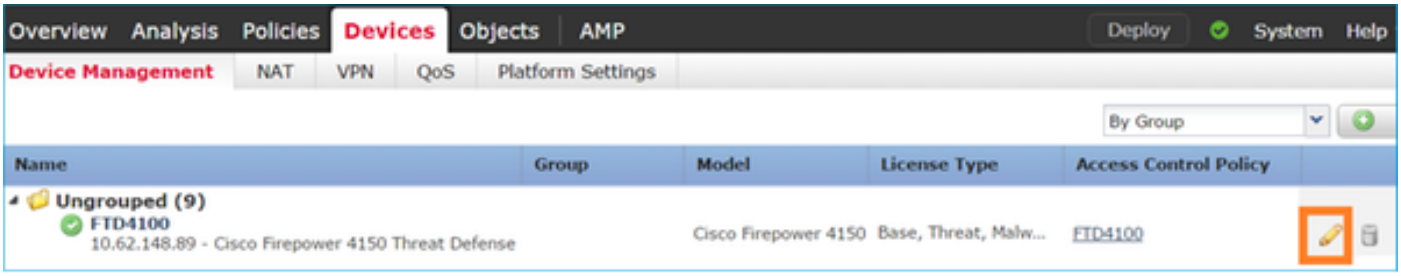
Configurar as interfaces física e1/6 e e1/8 no modo Inline dos pares por seguintes exigências:

| | | |
|---|---|---|
| **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 | |
| **À prova de falhas** | Habilitado | |
| **Estado do link da propagação** | Habilitado | |

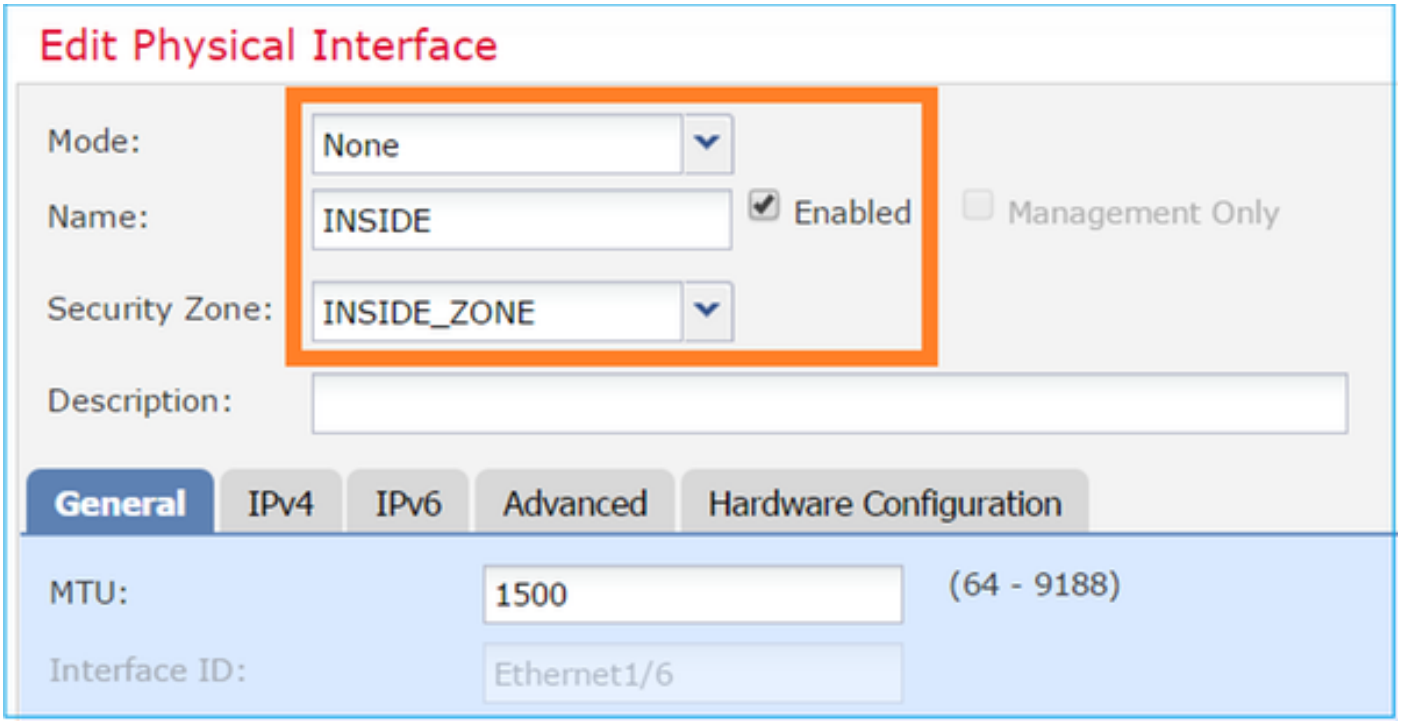
### Solução

#### Etapa 1? Configurando as interfaces individuais

Navegue aos **dispositivos > ao Gerenciamento de dispositivos,** selecione o dispositivo apropriado e clique sobre o ícone **Edit**:

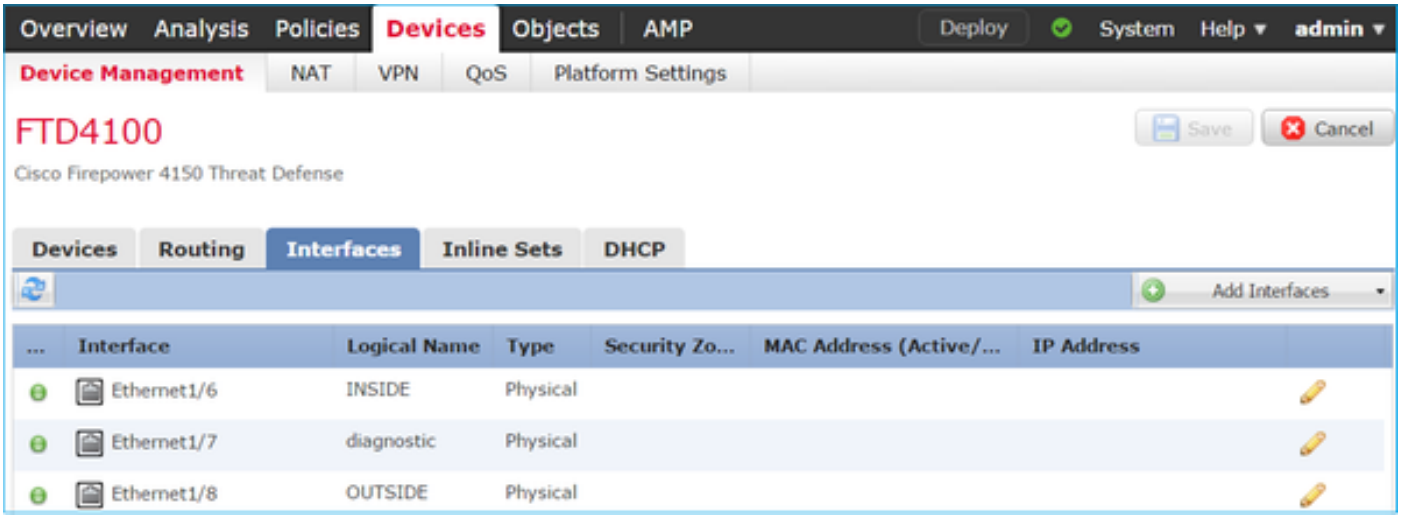



Especifique o nome e permita a relação:



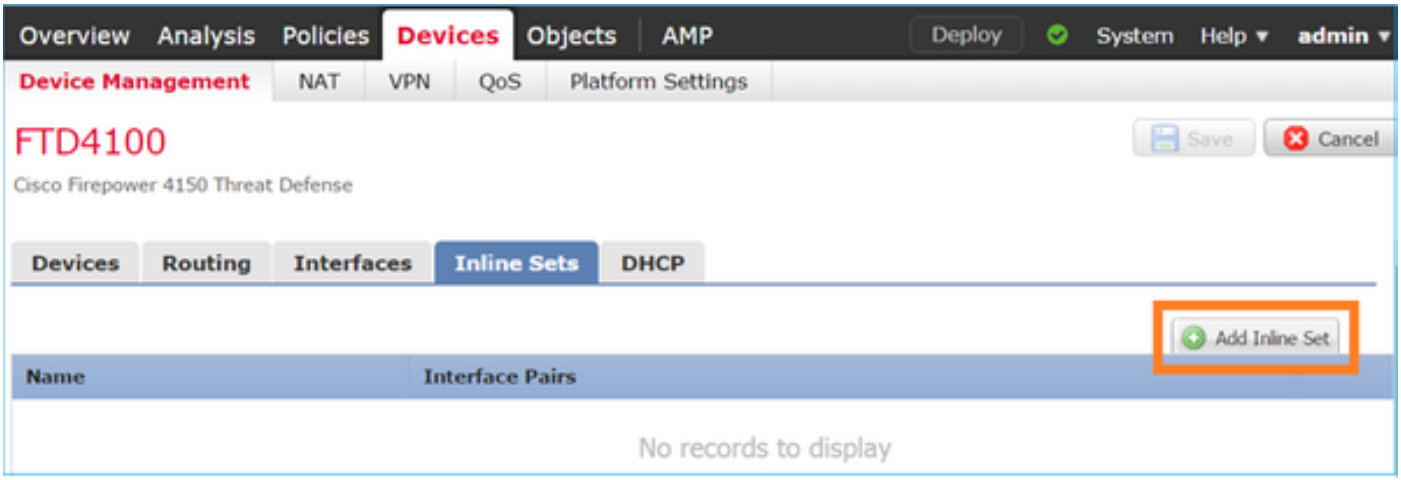

**O nome** será o **nameif da** relação

Similarmente para a relação Ethernet1/8. O resultado final:

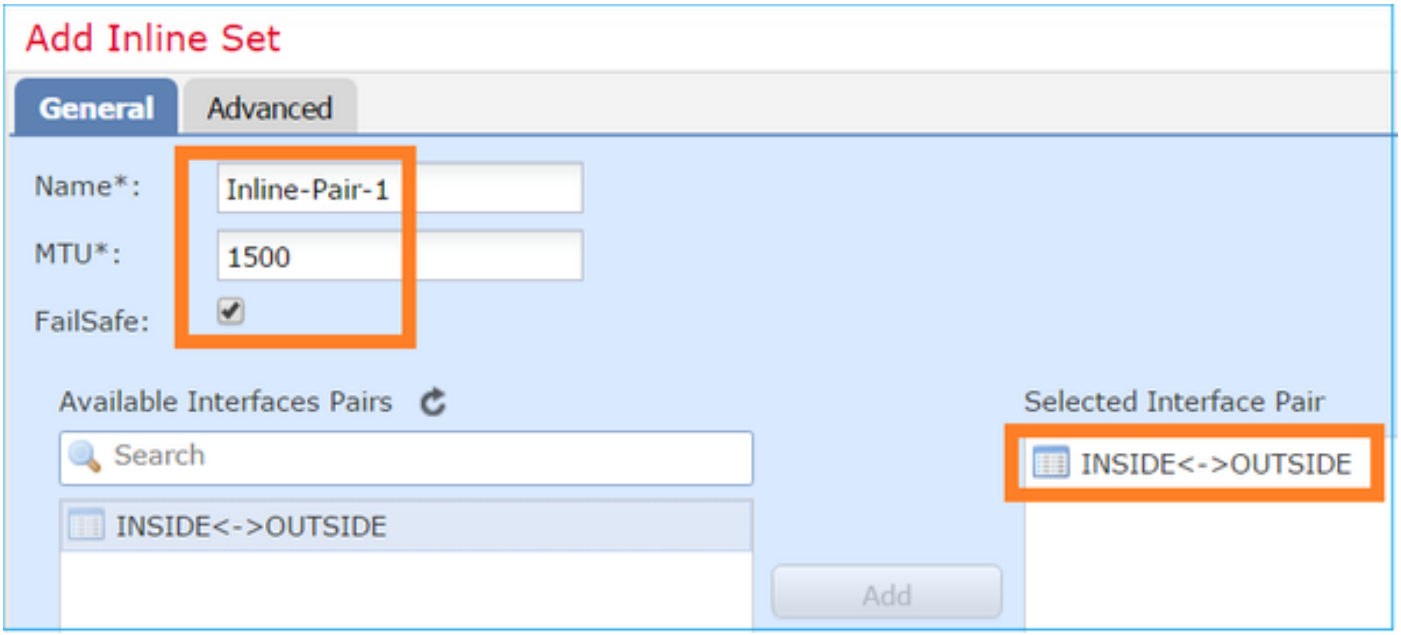


### Etapa 2? Configurando os pares Inline

Navegue à aba **Inline dos grupos** e clique sobre **Add ajustado Inline**:

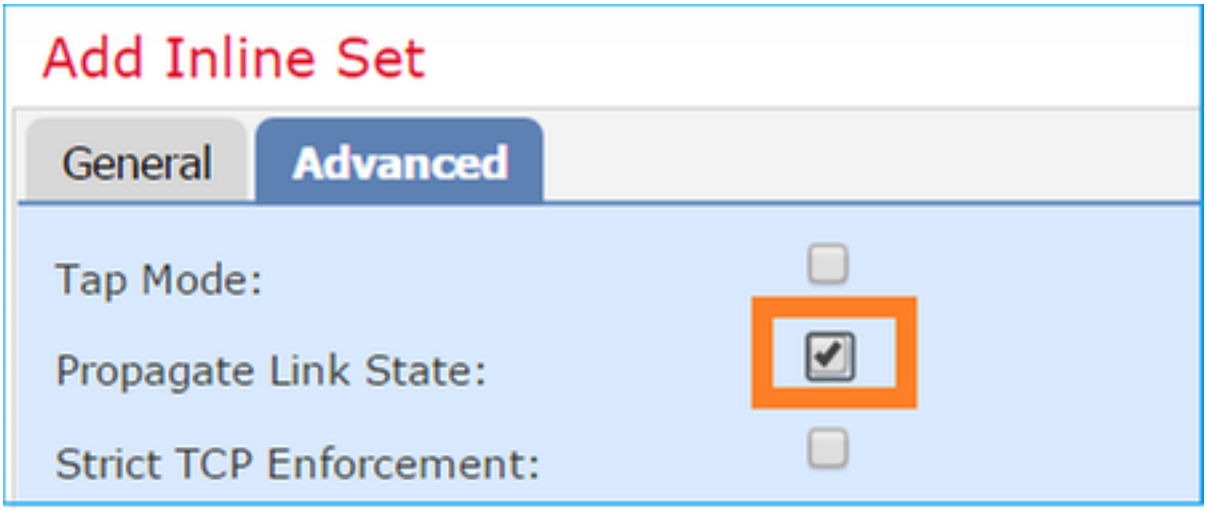



Configurar os ajustes por exigências:




**À prova de falhas** permite que o tráfego passe com os pares inline uninspected caso que os bufferes 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.

Permita? **Propague o estado do link**? opção:




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.

**Salvar as** mudanças e **distribua-as**

## Verificando a configuração da interface Inline dos pares

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
>
```

Verificando 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
```

Verificando 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
>
```

# Verificando a operação Inline da relação dos pares FTD

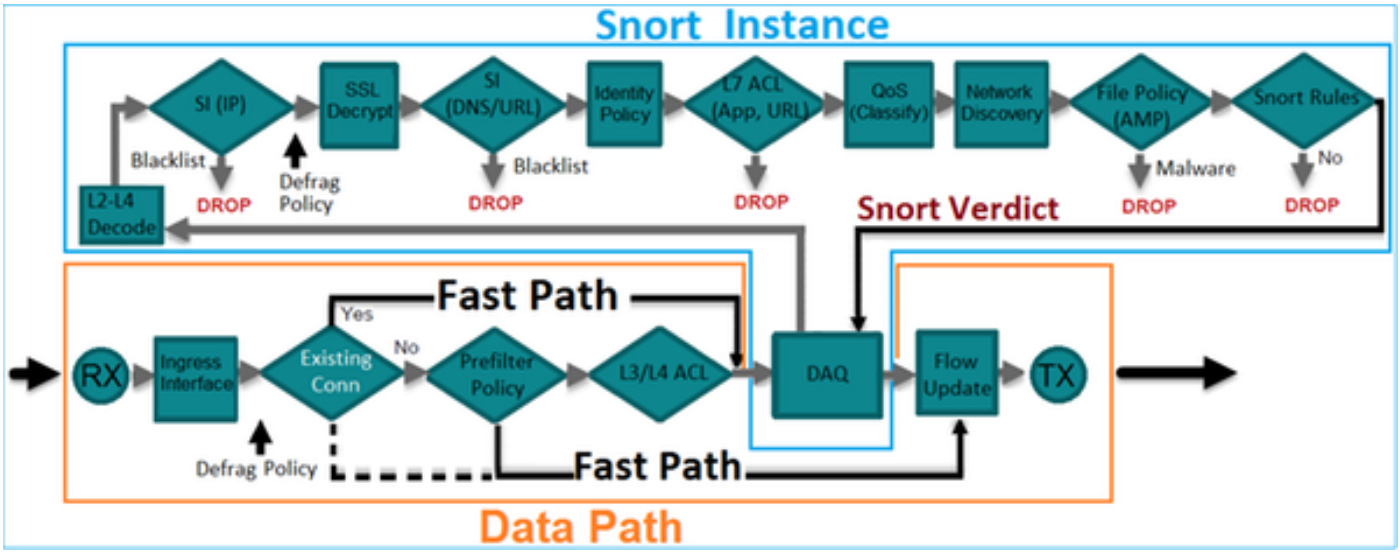
Esta seção cobre as seguintes verificações da verificação a fim verificar a operação Inline dos pares:

- Verificação 1? Usando o pacote-projétil luminoso
- Verificação 2? Permitindo a captação com traço e emissão de um pacote TCP SYN/ACK com os pares Inline
- Verificação 3? Monitorando o tráfego FTD que usa o motor do Firewall debugar
- Verificação 4? Verificando a funcionalidade da propagação do link-state
- Verificação 5? Configurando o NAT estático

### Solução

### Visão geral arquitetural

Quando 2 relações FTD se operam no modo dos Inline-pares um pacote está segurado como segue:



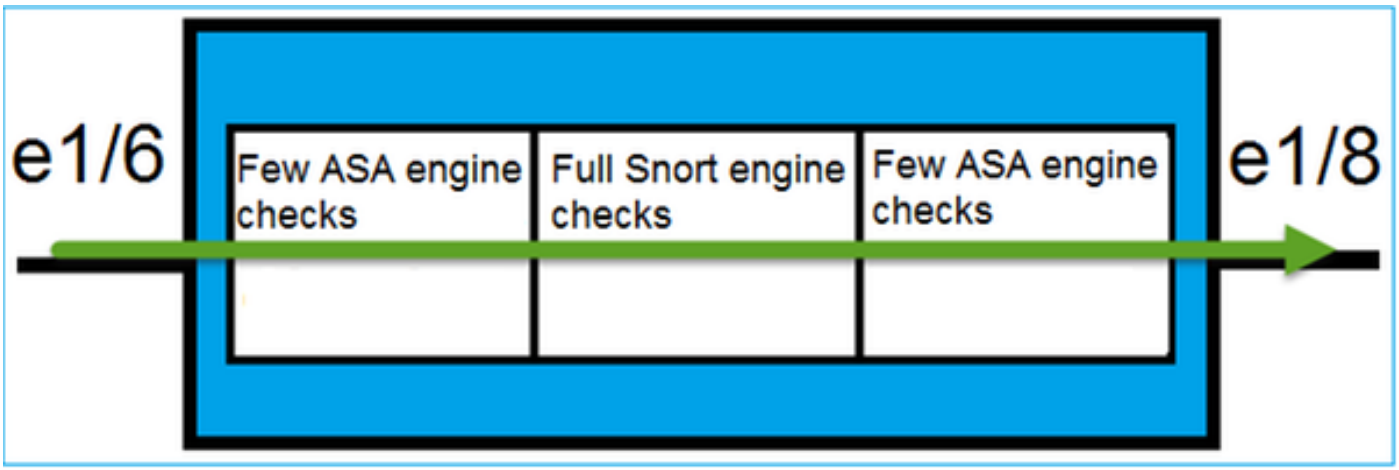

Nota: Somente as interfaces física podem ser membros de um par Inline ajustado

### Teoria básica

- Ao configurar um par Inline 2 interfaces física são construídas uma ponte sobre internamente
- Muito similar ao **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 os fluxos que vão com um par Inline
- O tráfego de trânsito **pode ser deixado cair**
- **Poucas** verificações do **motor ASA** são aplicadas junto com verificações **completas do motor do Snort**

O último ponto pode ser visualizado como segue:




## Verificação 1? Usando o pacote-projétil luminoso

Éaqui o pacote-projétil luminoso output emulando um pacote que atravessa os pares inline com os pontos interessantes 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

>
```

## Verificação 2? Enviando pacotes TCP SYN/ACK com os pares Inline

Você pode gerar pacotes TCP SYN/ACK usando uma utilidade crafting do pacote como Scapy. A seguinte sintaxe gerará 3 pacotes com as bandeiras SYN/ACK permitidas:

```
root@KALI:~# scapyINFO: 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 a seguinte captação 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
>
```

Após a emissão 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

>
```

- **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 e em um doesn do estado-desvio TCP? pacotes de TCP da gota t que don? t pertence às conexões existentes
- **Bandeira N:** O pacote será inspecionado pelo motor do Snort FTD

As captações provam o acima desde que você pode ver os 3 pacotes atravessar 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 retiram 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
>
```

Seguir o primeiro pacote da captação revela alguma informação adicional como a sentença do motor do Snort:

```
> show capture CAPI packet-number 1 trace3 packets captured 1: 15:27:54.327146 192.168.201.50.20
```

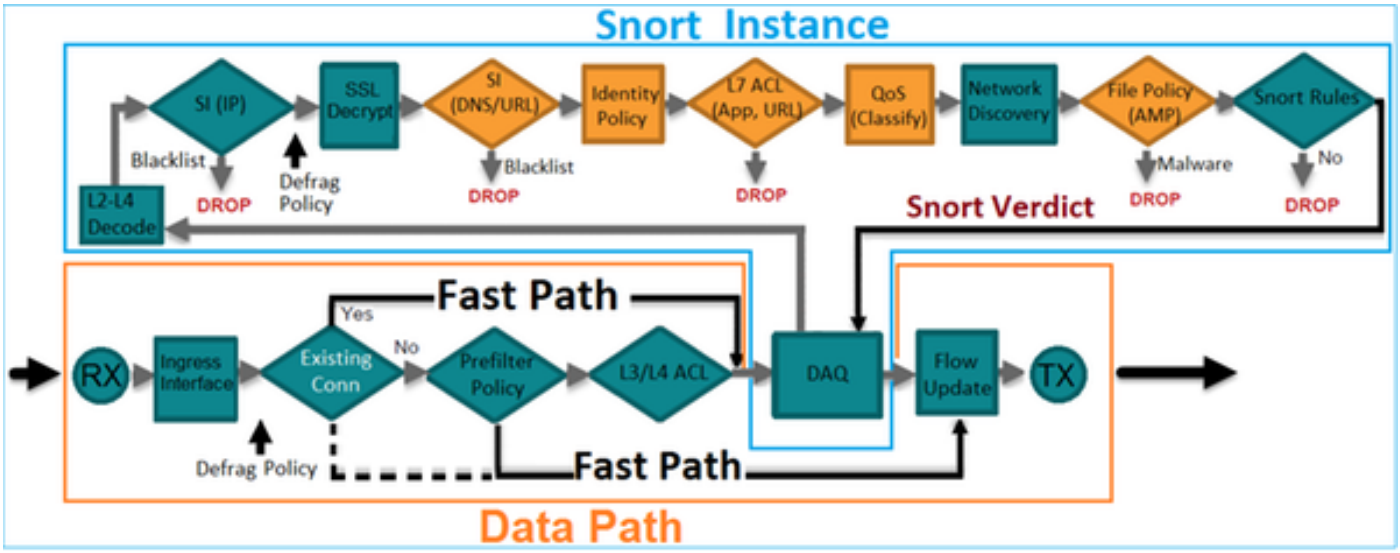
> 192.168.201.60.80: **S** 0:0(0) **ack** 0 win 8192Phase: 1Type: CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result: ALLOWConfig:Implicit RuleAdditional Information:MAC Access list**Phase: 3Type: NGIPS-MODESubtype: ngips-modeResult: ALLOWConfig:Additional Information:The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied**Phase: 4Type: ACCESS-LISTSubtype: logResult: ALLOWConfig:access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1access-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 reachedPhase: 5Type: NGIPS-EGRESS-INTERFACE-LOOKUPSubtype: Resolve Egress InterfaceResult: ALLOWConfig:Additional Information:Ingress interface INSIDE is in NGIPS inline mode.Egress interface OUTSIDE is determined by inline-set configuration**Phase: 6Type: FLOW-CREATIONSubtype:Result: ALLOWConfig:Additional Information:New flow created with id 282, packet dispatched to next module**Phase: 7Type: EXTERNAL-INSPECT**Subtype:Result: ALLOWConfig:Additional Information:**Application: 'SNORT Inspect'Phase: 8Type: SNORT**Subtype:**Result: ALLOW**Config:**Additional Information:Snort Verdict: (pass-packet) allow this packet**Phase: 9Type: CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access listResult:input-interface: OUTSIDEinput-status: upinput-line-status: upAction: allow1 packet shown>

Seguir o 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 8192Phase: 1Type: CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result: ALLOWConfig:Implicit RuleAdditional Information:MAC Access list**Phase: 3Type: FLOW-LOOKUPSubtype:Result: ALLOWConfig:Additional Information:Found flow with id 282, using existing flowPhase: 4Type: EXTERNAL-INSPECT**Subtype:Result: ALLOWConfig:**Additional Information:Application: 'SNORT Inspect'Phase: 5Type: SNORTSubtype:Result: ALLOWConfig:Additional Information:Snort Verdict: (pass-packet) allow this packet**Phase: 6Type: CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access listResult:input-interface: OUTSIDEinput-status: upinput-line-status: upAction: allow1 packet shown>

## Verificação 3? O motor do Firewall debuga 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:




Quando enviá-lo aos pacotes TCP SYN/ACK com os pares Inline puder 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
```

## Verificação 4? Verificando 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
>
```

Após re-ter permitido o switchport a mostra dos logs FTD:

```
> 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)
>
```

### Verificação 5? Configurando o NAT estático

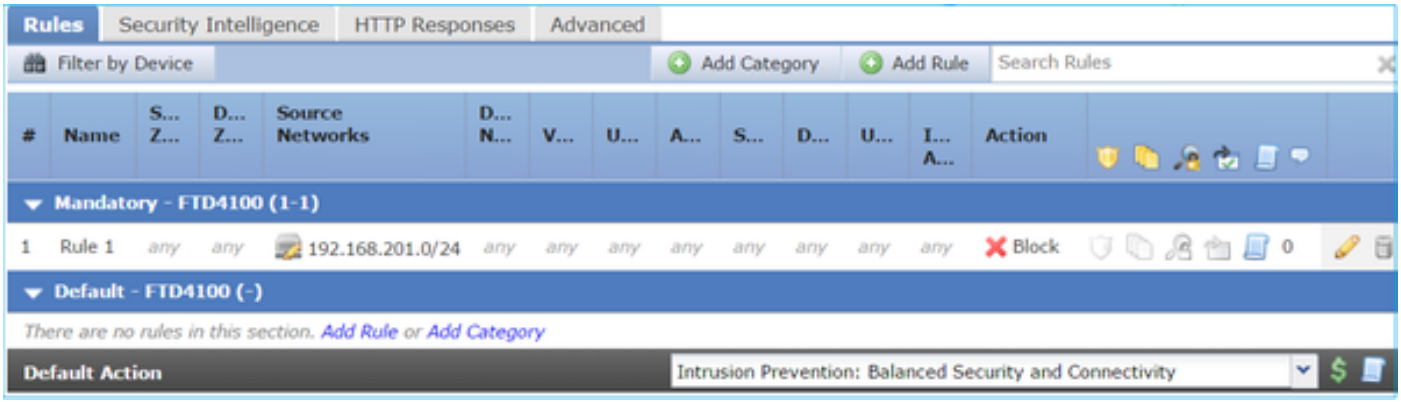
#### Solução

O NAT não é apoiado para as relações que operam 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

## Obstruindo um pacote no modo Inline da relação dos pares

Crie uma regra de bloqueio como o seguinte, envie o tráfego com os pares Inline FTD e observe o comportamento:




## Solução

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

```
> show capturecapture CAPI type raw-data trace interface INSIDE [Capturing - 210 bytes] match ip host 192.168.201.60 anycapture CAPO type raw-data interface OUTSIDE [Capturing - 0 bytes] match ip host 192.168.201.60 any
```

Seguir 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 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
```

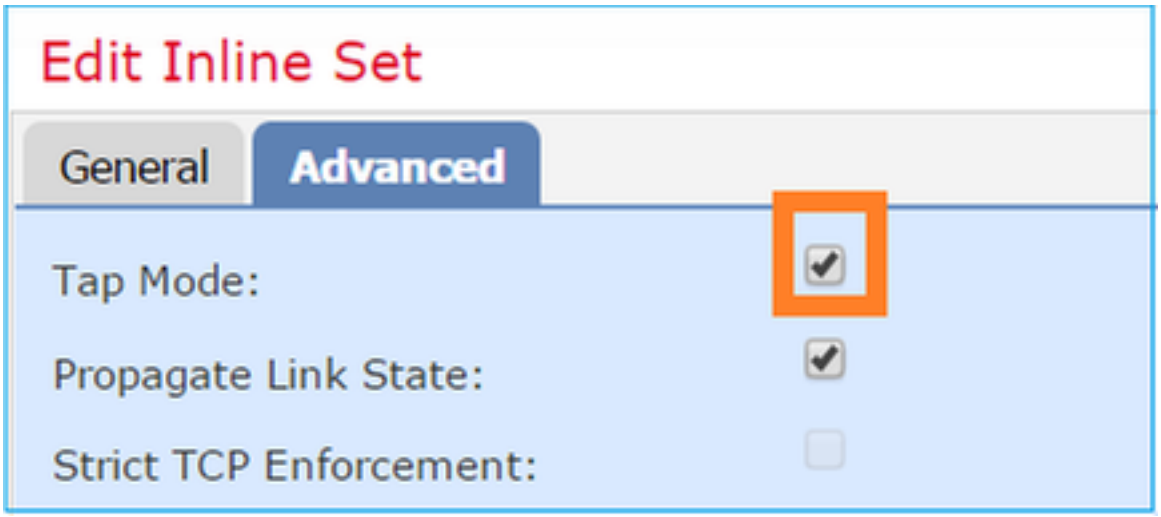
No traço acima pode-se ver que o pacote esteve deixado cair pelo motor FTD ASA e não enviado ao motor do Snort FTD.

# Configurando 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**, edite os pares Inline, clique sobre o **guia avançada** e permita o **modo da torneira**:



### Verificação

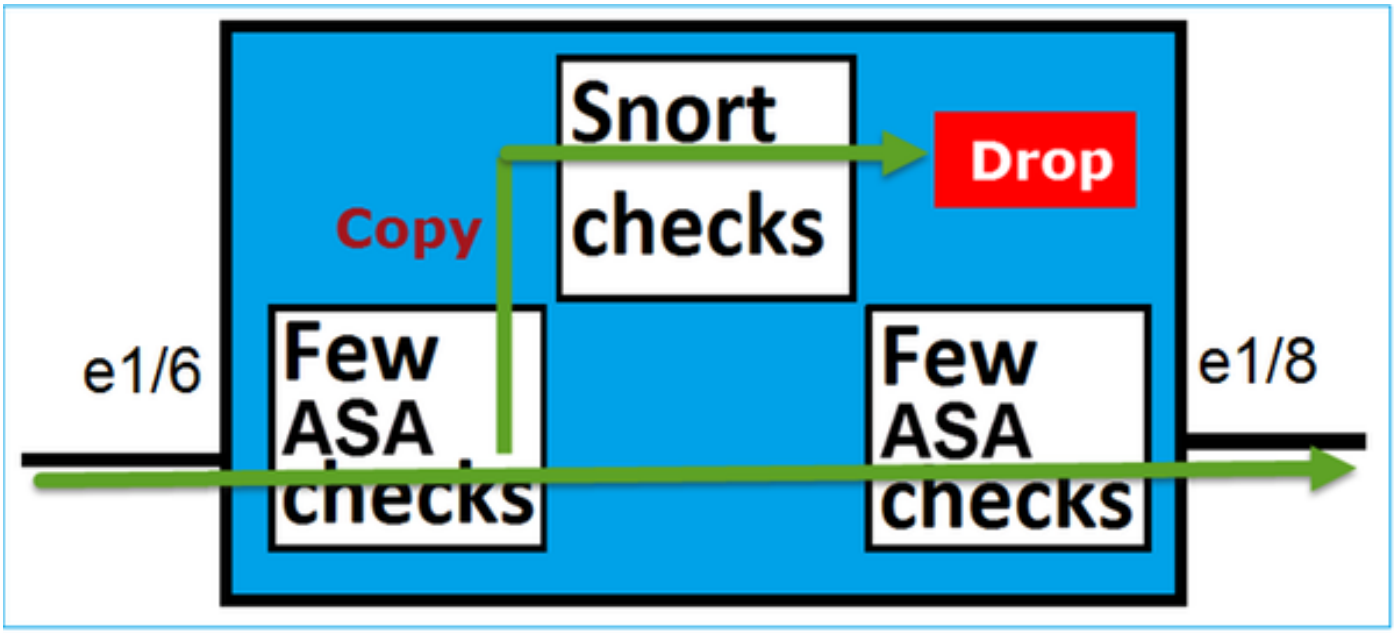
```
> show inline-setInline-set Inline-Pair-1 Mtu is 1500 bytes Failsafe mode is on/activated
Failsecure mode is off Tap mode is on Propagate-link-state option is on hardware-bypass mode is
disabled Interface-Pair[1]: Interface: Ethernet1/6 "INSIDE" Current-Status: UP Interface:
Ethernet1/8 "OUTSIDE"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

## Verificando os pares Inline FTD com operação da relação da torneira

### Teoria básica

- Ao configurar um par Inline com interfaces física da torneira 2 são construídos uma ponte sobre internamente
- 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 os fluxos que vão com 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 pode ser visualizado como segue:



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

```
> show capture CAPI packet-number 2 trace3 packets captured 2: 13:34:30.685084 192.168.201.50.20
> 192.168.201.60.80: S 0:0(0) win 8192Phase: 1Type: CAPTURESubtype:Result:
ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result:
ALLOWConfig:Implicit RuleAdditional Information:MAC Access listPhase: 3Type: NGIPS-MODESubtype:
ngips-modeResult: ALLOWConfig:Additional Information:The flow ingressed an interface configured
for NGIPS mode and NGIPS services will be appliedPhase: 4Type: ACCESS-LISTSubtype: logResult:
WOULD HAVE DROPPEDConfig:access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced deny ip
192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-startaccess-list CSM_FW_ACL_
remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1access-list CSM_FW_ACL_ remark
rule-id 268441600: L4 RULE: Rule 1Additional Information:Result:input-interface: INSIDEinput-
status: upinput-line-status: upAction: Access-list would have dropped,but packet forwarded due
to inline-tap1 packet shown
>
```

# Comparação: Pares Inline contra pares Inline com torneira

| | Pares Inline | Pares Inline com torneira |
|---|---|---|
| mostre o inline-grupo | >mostre o inline-grupo<br><br>Inline-grupo Inline-Pair-1<br>O MTU é 1500 bytes<br>O modo à prova de falhas é on/activated<br>O modo de Failsecure está<br>O modo da torneira está<br>a opção do Propagação-link-estado está ligada<br>o modo do hardware-desvio é desabilitado<br>Interface-Pair[1]:<br>Interface: Ethernet1/6 “INTERIOR”<br>Status atual: PARA CIMA<br>Interface: Ethernet1/8 “PARTE EXTERNA”<br>Status atual: PARA CIMA<br>Grupo de bridge ID: 509 | > mostre o inline-grupo<br><br>Inline-grupo Inline-Pair-1<br>O MTU é 1500 bytes<br>O modo à prova de falhas é on/activated<br>O modo de Failsecure está<br>O modo da torneira está ligada<br>a opção do Propagação-link-estado está ligada<br>o modo do hardware-desvio é desabilitad<br>Interface-Pair[1]:<br>Interface: Ethernet1/6 “INTERIOR”<br>Status atual: PARA CIMA<br>Interface: Ethernet1/8 “PARTE EXTERN<br>Status atual: PARA CIMA<br>Grupo de bridge ID: 0 |
| show interface | ><br>>mostre a relação e1/6<br>Conecte Ethernet1/6 “INTERIOR”, esteja acima, protocolo de linha está acima<br>O hardware é EtherSVI, 1000 Mbps de BW, usec DLY 1000<br>MAC address 5897.bdb9.770e, MTU 1500<br>IPS Relação-MODE: inline, Inline-grupo: Inline-Pair-1<br>Endereço IP de Um ou Mais Servidores Cisco ICM NT unassigned<br>Estatísticas de tráfego para o “INTERIOR”:<br>entrada de 3957 pacotes, 264913 bytes<br>saída de 144 pacotes, 58664 bytes<br>4 pacotes deixados cair<br>1 pacotes minutos da taxa de entrada | ><br>>mostre a relação e1/6<br>Conecte Ethernet1/6 “INTERIOR”, esteja acima, protocolo de linha está acima<br>O hardware é EtherSVI, 1000 Mbps de B usec DLY 1000<br>MAC address 5897.bdb9.770e, MTU<br>IPS Relação-MODE: inline-torneira, I grupo: Inline-Pair-1<br>Endereço IP de Um ou Mais Servidor Cisco ICM NT unassigned<br>Estatísticas de tráfego para o “INTERIOR<br>24 entradas dos pacotes, 1378 bytes<br>0 saídas dos pacotes, bytes 0<br>24 pacotes deixados cair<br>1 pacotes minutos da taxa de entrada |

| | | |
|---|---|---|
| | 0/segundo, 26 bytes/segundo<br>1 pacotes da taxa de saídas por minuto 0/segundo, 7 bytes/segundo<br>1 taxa minuto da gota, 0 pacotes/segundo<br>pacotes da taxa de entrada 0 do minuto 5/segundo, 28 bytes/segundo<br>pacotes da taxa de saídas por minuto 5 0/segundo, 9 bytes/segundo<br>taxa da gota do minuto 5, 0 pacotes/segundo<br>**> mostre a relação e1/8**<br>Conecte Ethernet1/8 “PARTE EXTERNA”, esteja acima, protocolo de linha está acima<br>O hardware é EtherSVI, 1000 Mbps de BW, usec DLY 1000<br>MAC address 5897.bdb9.774d, MTU 1500<br>IPS Relação-MODE: **inline**, Inline-grupo: Inline-Pair-1<br>Endereço IP de Um ou Mais Servidores Cisco ICM NT unassigned<br>Estatísticas de tráfego para a “PARTE EXTERNA”:<br>entrada de 144 pacotes, 55634 bytes<br>saída de 3954 pacotes, 339987 bytes<br>pacotes 0 deixados cair<br>1 pacotes minutos da taxa de entrada 0/segundo, 7 bytes/segundo<br>1 pacotes da taxa de saídas por minuto 0/segundo, 37 bytes/segundo<br>1 taxa minuto da gota, 0 pacotes/segundo<br>pacotes da taxa de entrada 0 do minuto 5/segundo, 8 bytes/segundo<br>pacotes da taxa de saídas por minuto 5 0/segundo, 39 bytes/segundo<br>taxa da gota do minuto 5, 0 pacotes/segundo<br>**>**<br>**>mostre a pacote-número da captação CAPI 1 traço**<br><br>3 pacotes capturados<br><br>1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: Vitória 8192 S 0:0(0) ack 0<br>Fase: 1<br>Digite: CAPTAÇÃO<br>Subtipo:<br>Resultado: RESERVE<br>Configuração:<br>Informações adicionais:<br>Lista de acessos MAC<br><br>Fase: 2 | 0/segundo, 0 bytes/segundo<br>1 pacotes da taxa de saídas por minut 0/segundo, 0 bytes/segundo<br>1 taxa minuto da gota, 0 pacotes/segu<br>pacotes da taxa de entrada 0 do minut 5/segundo, 0 bytes/segundo<br>pacotes da taxa de saídas por minuto 0/segundo, 0 bytes/segundo<br>taxa da gota do minuto 5, 0 pacotes/segundo<br>**> mostre a relação e1/8**<br>Conecte Ethernet1/8 “PARTE EXTERNA”, esteja acim<br>O hardware é EtherSVI, 1000 Mbps de B usec DLY 1000<br>MAC address 5897.bdb9.774d, MTU<br>IPS Relação-MODE: **inline-torneira**, I grupo: Inline-Pair-1<br>Endereço IP de Um ou Mais Servidor Cisco ICM NT unassigned<br>Estatísticas de tráfego para a “PARTE EXTERNA”:<br>1 entrada dos pacotes, 441 bytes<br>0 saídas dos pacotes, bytes 0<br>pacotes 1 deixados cair<br>1 pacotes minutos da taxa de entrada 0/segundo, 0 bytes/segundo<br>1 pacotes da taxa de saídas por minut 0/segundo, 0 bytes/segundo<br>1 taxa minuto da gota, 0 pacotes/segu<br>pacotes da taxa de entrada 0 do minut 5/segundo, 0 bytes/segundo<br>pacotes da taxa de saídas por minuto 0/segundo, 0 bytes/segundo<br>taxa da gota do minuto 5, 0 pacotes/segundo<br>**>**<br>**> mostre a pacote-número da captação CA traço**<br><br>3 pacotes capturados<br><br>1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: Vitória 8192 S 0:0(0)<br>Fase: 1<br>Digite: CAPTAÇÃO<br>Subtipo:<br>Resultado: RESERVE<br>Configuração:<br>Informações adicionais:<br>Lista de acessos MAC<br><br>Fase: 2 |
| Pacote que segura com **regra de bloqueio** | | |

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 ingressed 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
>

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 ingressed 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_ avança
nega a IP 192.168.201.0 255.255.255.0 to
fluxo-início do log de eventos regra-identificação 268441600
regra-identificação 268441600 da observa
da lista de acesso CSM_FW_ACL_: POLÍ
DE ACESSO: FTD4100 - Mandatory/1
regra-identificação 268441600 da observa
da lista de acesso CSM_FW_ACL_: REGR
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 pacote**

1 pacote mostrado
>

## Resumo

- Ao usar 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 está sendo aplicada
- Quando o modo Inline dos pares está em uns pacotes do uso pode ser obstruído desde que são processados inline
- Quando o modo da torneira está permitido uma cópia do pacote está inspecionada e deixada cair internamente quando o tráfego real atravessar FTD unmodified

## Documentos relacionados

Potência de fogo NGFW de Cisco