# Configurar interfaces FTD no modo de par em linha

## Contents



## Introduction

Este documento descreve a configuração, a verificação e a operação em segundo plano de uma Interface de Par em Linha em um dispositivo Firepower Threat Defense (FTD).

## Prerequisites

### Requirements

Não há requisitos específicos para este documento.

### Componentes Utilizados

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

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

### Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

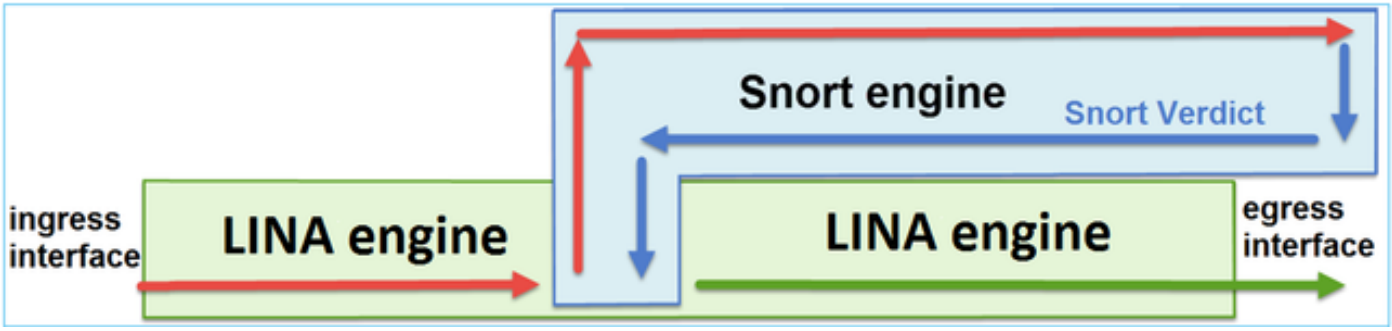
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- Código de software FTD 6.2.x e posterior

## Informações de Apoio

O FTD é uma imagem de software unificada que consiste em dois mecanismos principais:

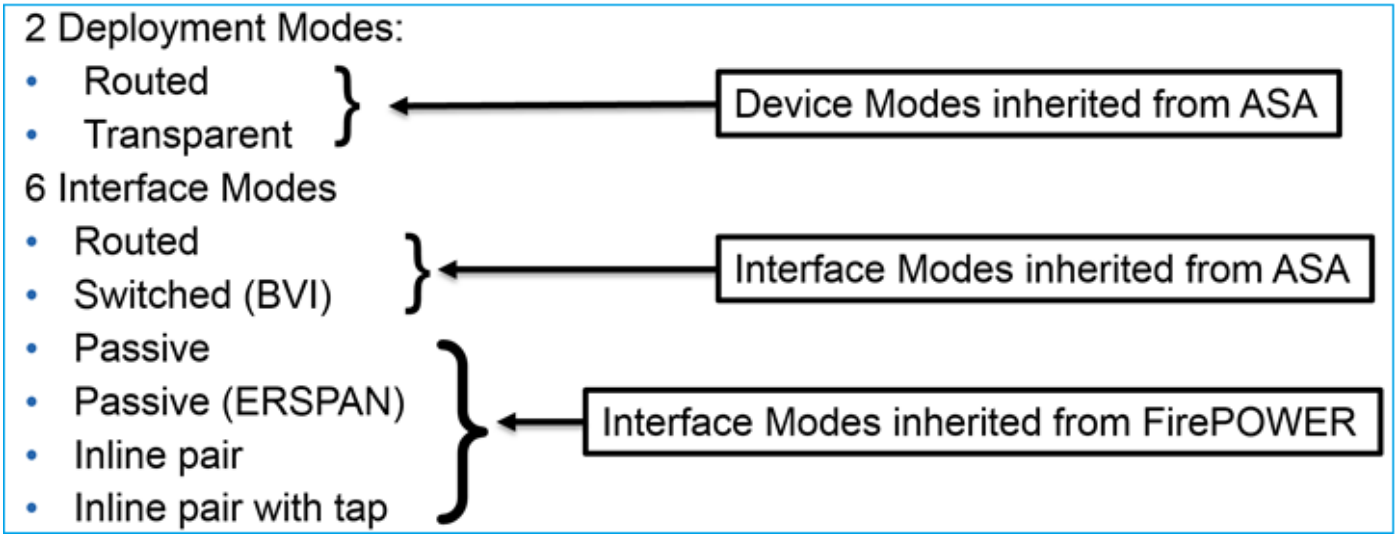
- Mecanismo LINA
- Mecanismo Snort

Esta figura mostra como os dois mecanismos interagem:




- Um pacote é inserido na interface de entrada e tratado pelo mecanismo LINA
- Se exigido pela política do FTD, o pacote será inspecionado pelo mecanismo Snort
- O mecanismo Snort retorna um veredito para o pacote
- O mecanismo LINA descarta ou encaminha o pacote de acordo com a conclusão do Snort

O FTD fornece dois modos de implantação e seis modos de interface, como mostrado na imagem:



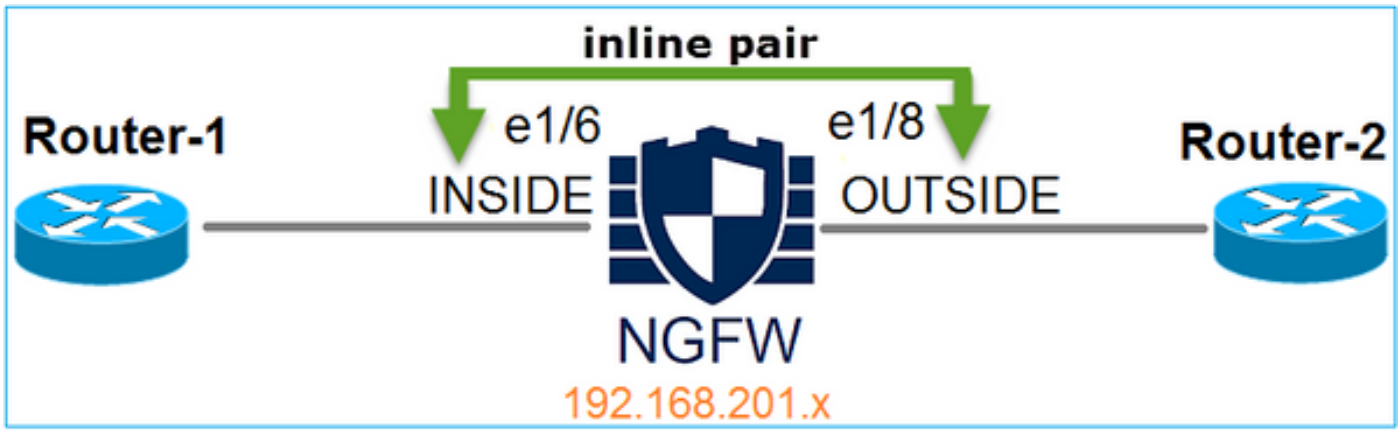

**Note**: Você pode combinar modos de interface em um único dispositivo FTD.

Aqui está uma visão geral de alto nível dos vários modos de implantação e interface do FTD:

| modo de interface FTD | modo de Implantação FTD | Descrição | O tráfego pode ser descartado |
|---|---|---|---|
| Roteado | Roteado | Verificações completas do mecanismo LINA e do mecanismo Snort | Yes |
| Comutado | Transparente | Verificações completas do mecanismo LINA e do mecanismo Snort | Yes |
| Par em linha | Roteado ou Transparente | Verificações parciais do mecanismo LINA e do mecanismo Snort completo | Yes |
| Par em linha com torneira | Roteado ou Transparente | Verificações parciais do mecanismo LINA e do mecanismo Snort completo | No |
| Passivo | Roteado ou Transparente | Verificações parciais do mecanismo LINA e do mecanismo Snort completo | No |
| Passivo (ERSPAN) | Roteado | Verificações parciais do mecanismo LINA e do mecanismo Snort completo | No |

# Configurar a interface do par em linha no FTD

## Diagrama de Rede



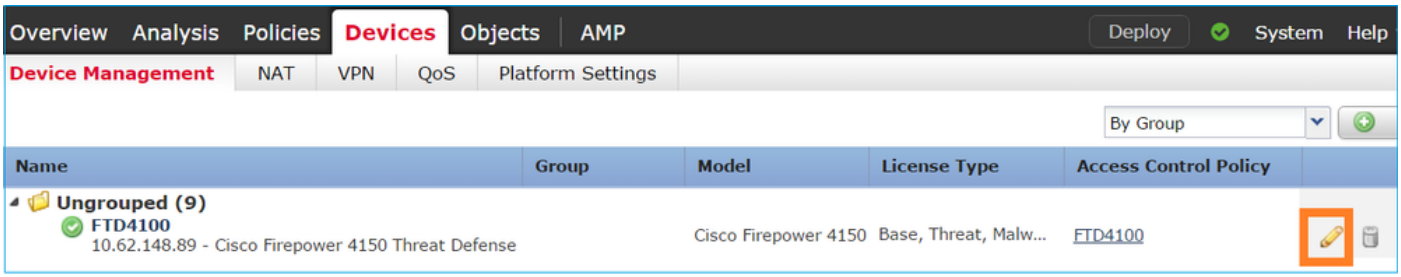

## Requisito

Configure as interfaces físicas e1/6 e e1/8 no modo Par em Linha de acordo com estes requisitos:

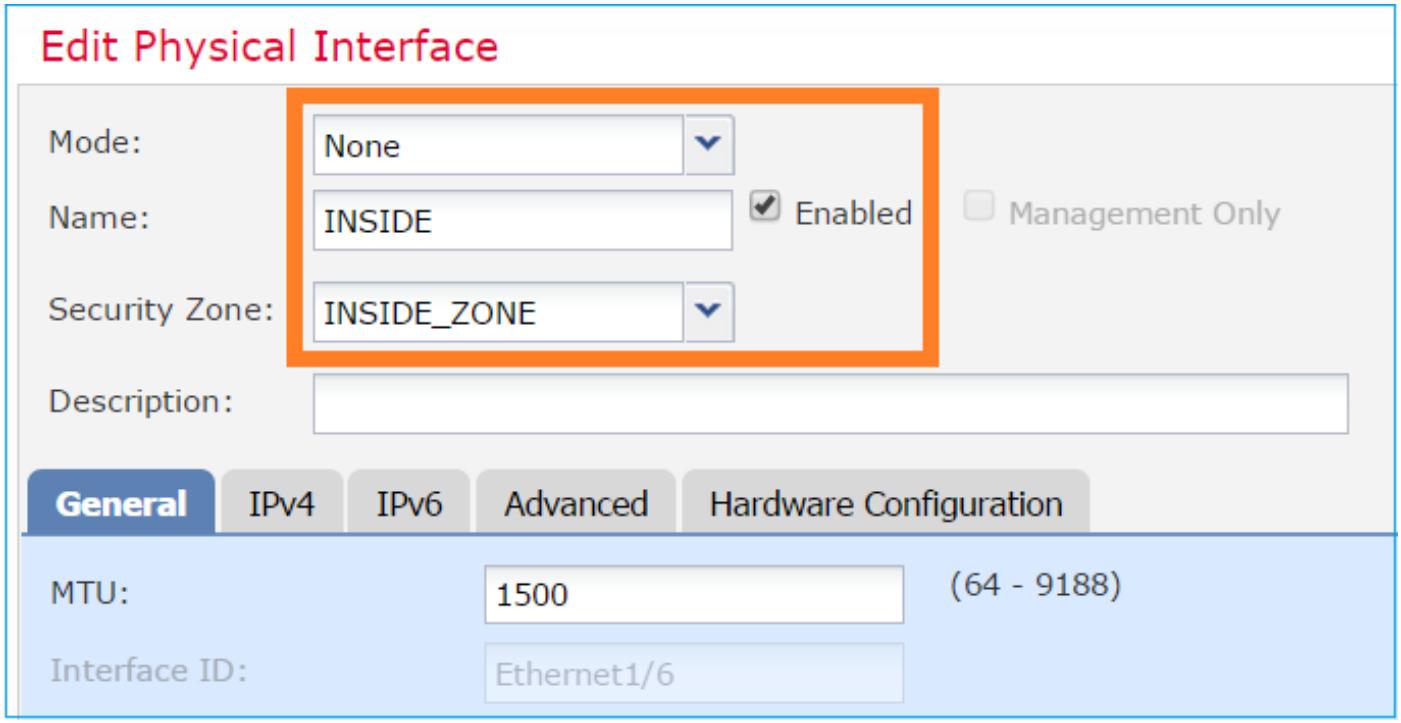
| | | |
|---|---|---|
| Interface | e1/6 | e1/8 |
| Nome | INTERNA | EXTERNA |
| Zona de segurança | INSIDE_ZONE | OUTSIDE_ZONE |
| Nome do conjunto em linha | Par em linha-1 | |
| MTU do conjunto em linha | 1500 | |
| FailSafe | Habilitado | |
| Propagar estado do link | Habilitado | |

## Solução

Etapa 1. Para configurar as interfaces individuais, navegue até **Dispositivos > Gerenciamento de dispositivos,** selecione o dispositivo apropriado e selecione **Editar** conforme mostrado na imagem.

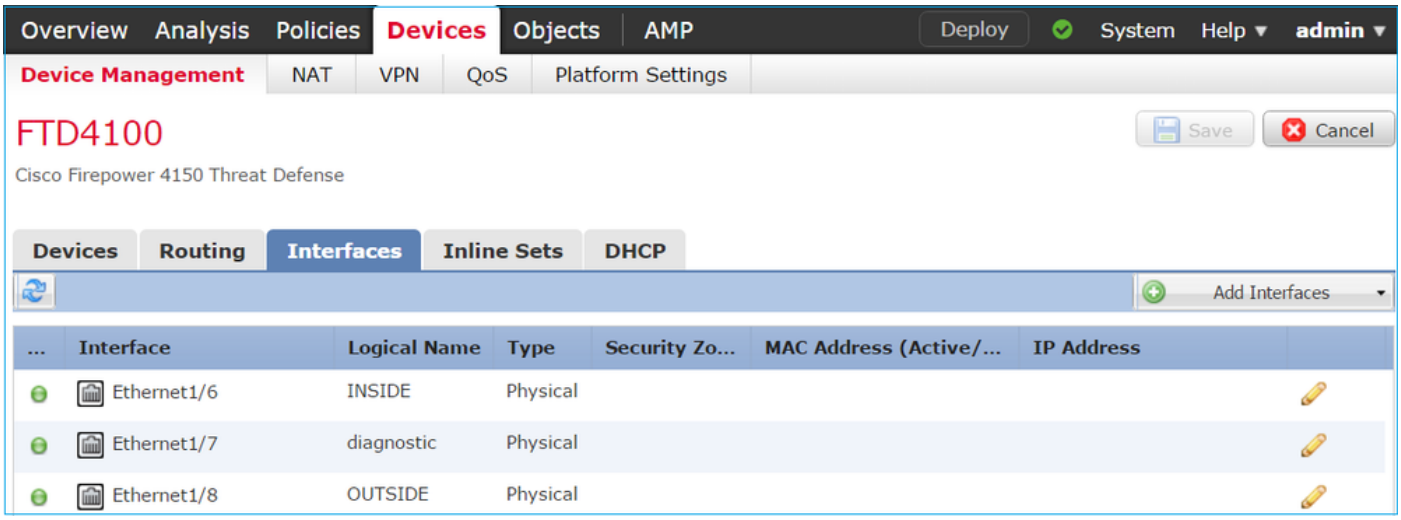



Em seguida, especifique **nome** e tique **habilitado** para a interface, como mostrado na imagem.



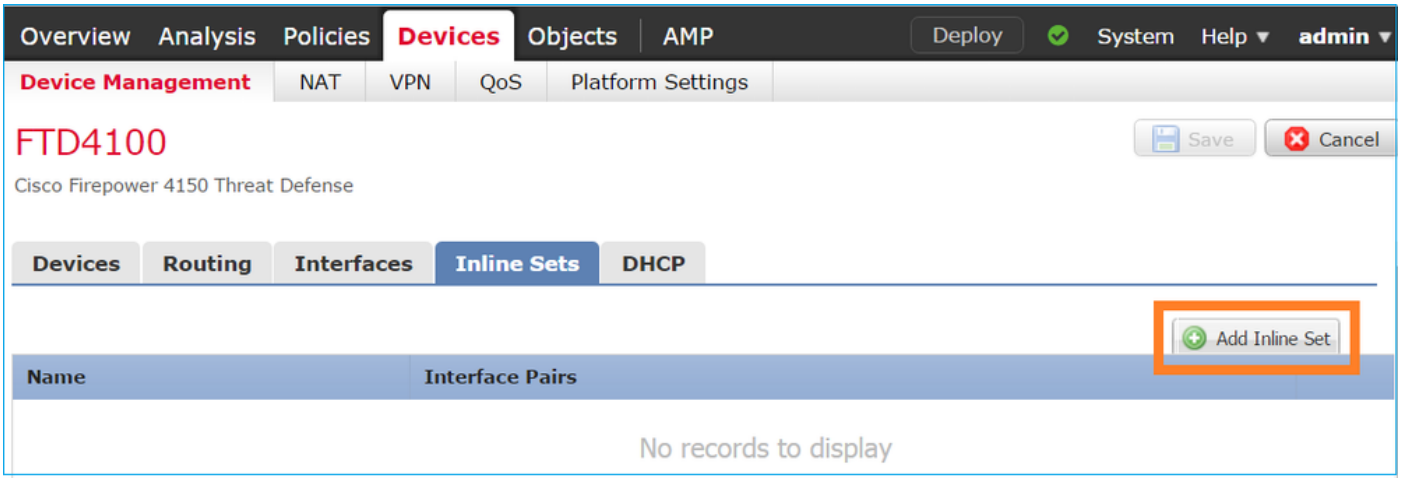

**Note**: O nome é o nome da interface.

Da mesma forma para a interface Ethernet1/8. O resultado final é como mostrado na imagem.

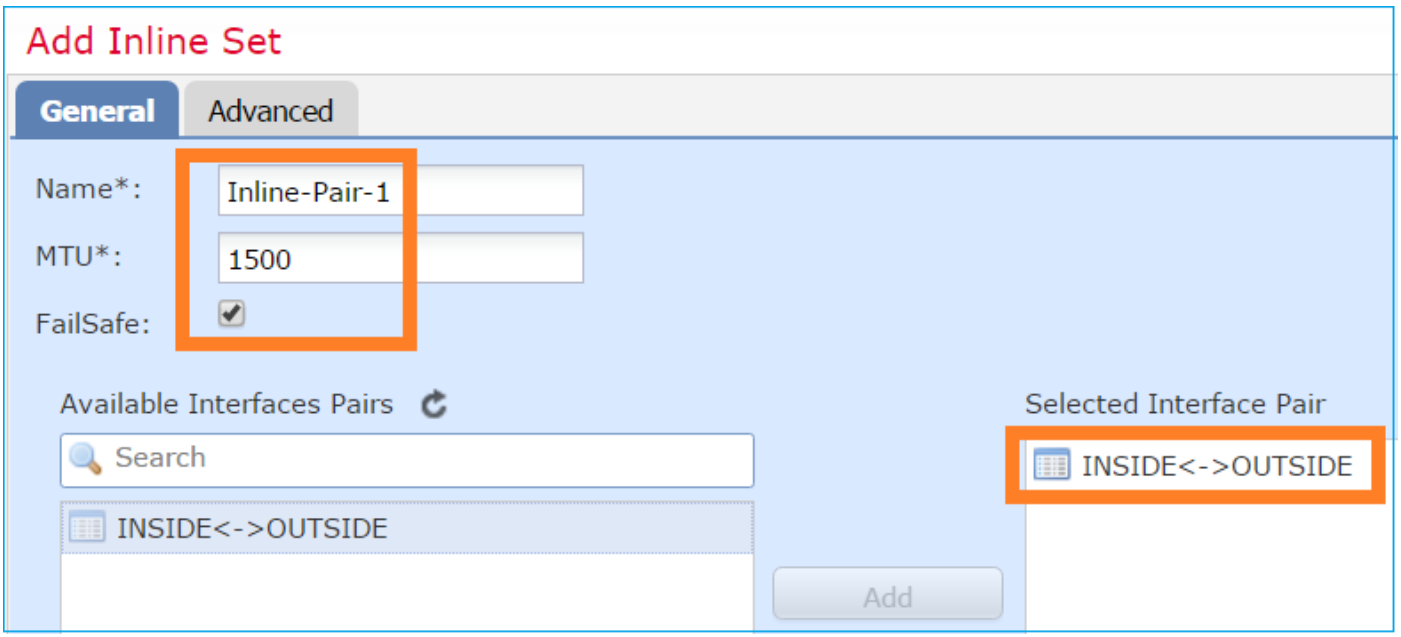



Etapa 2. Configure o par em linha.

Navegue até **Conjuntos em linha > Adicionar conjunto em linha** conforme mostrado na imagem.

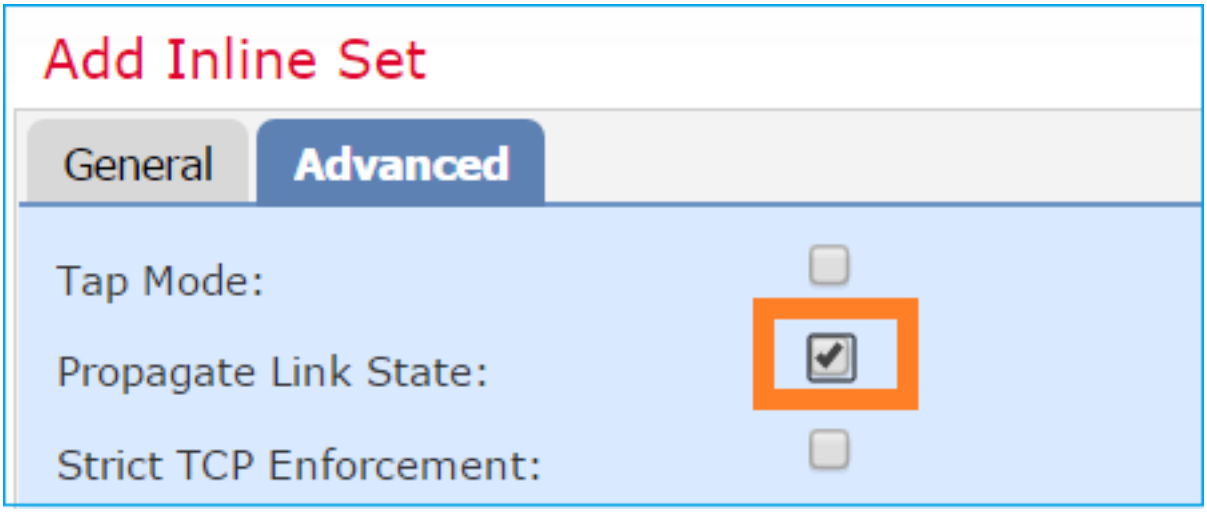



Etapa 3. Defina as configurações gerais de acordo com os requisitos conforme mostrado na imagem.




**Note**: Failsafe permite que o tráfego passe pelo par em linha não inspecionado caso os buffers da interface estejam cheios (normalmente visto quando o dispositivo está sobrecarregado ou o mecanismo Snort está sobrecarregado). O tamanho do buffer da interface é alocado dinamicamente.

Etapa 4. Ative a opção **Propagate Link State** nas Configurações avançadas, conforme mostrado na imagem.




A propagação de estado do link ativa automaticamente a segunda interface no par de interface em linha quando uma das interfaces no conjunto em linha fica inativa.

Etapa 5. **Salve** as alterações e **implemente**.

# Verificar

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

Verifique a configuração do par em linha da CLI do FTD.

**Solução**

Faça login na CLI do FTD e verifique a configuração do par em linha:

```
> 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**: O ID do grupo de bridge é um valor diferente de 0. Se o modo Toque estiver ativado, ele será 0

Informações de interface e 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 as informações 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
>
```

# Verificar a operação da interface em linha FTD

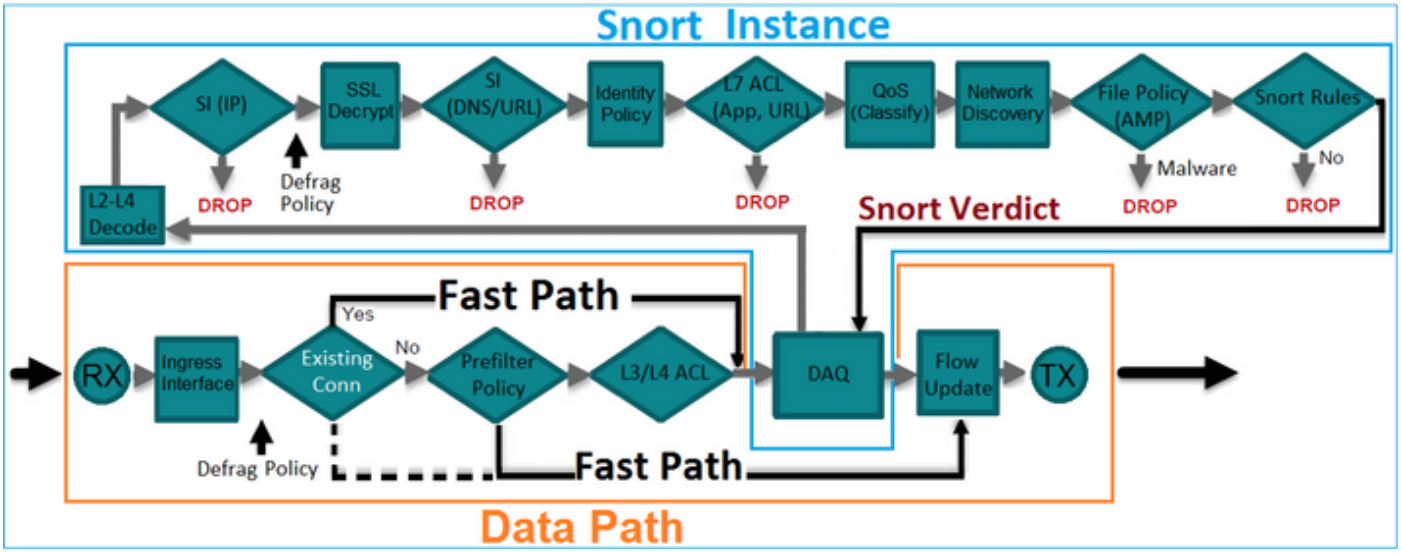
Esta seção abrange estas verificações para verificar a operação do par em linha:

- Verificação 1. Com o uso do packet-tracer
- Verificação 2. Habilitar captura com rastreamento e enviar um pacote de sincronização/confirmação (SYN/ACK) de TCP através do par em linha
- Verificação 3. Monitorar o tráfego FTD com o uso da depuração do mecanismo de firewall
- Verificação 4. Verificar a funcionalidade de Propagação de Link-State
- Verificação 5. Configurar a Conversão de Endereço de Rede Estático (NAT - Static Network Address Translation)

### Solução

Visão geral da arquitetura

Quando 2 interfaces FTD operam no modo Par em linha, um pacote é tratado como mostrado na imagem.

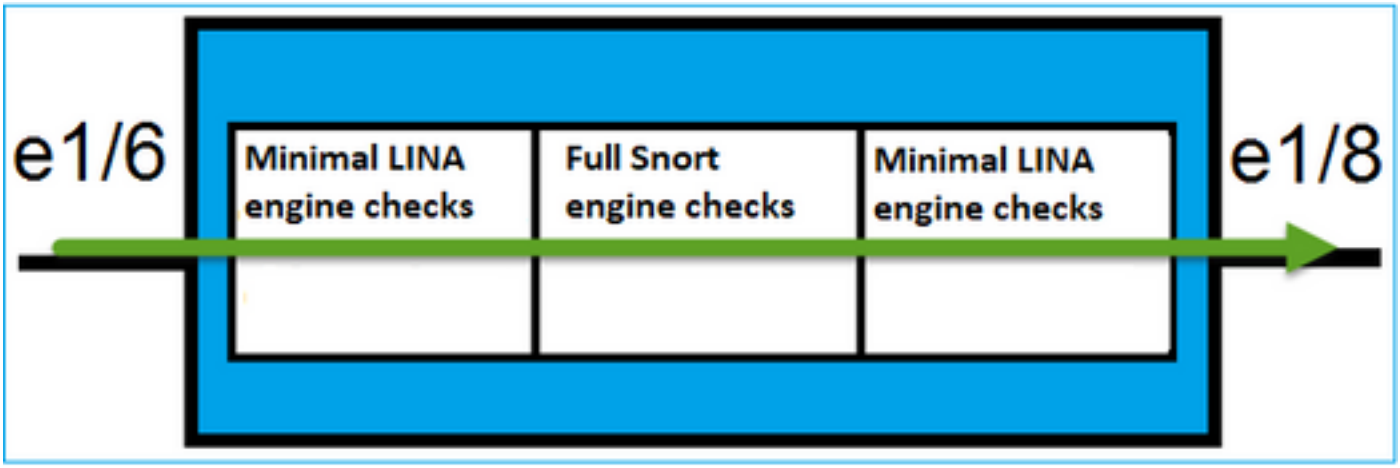



**Note**: Somente as interfaces físicas podem ser membros de um conjunto de pares em linha

## Teoria básica

- Quando você configura um par em linha 2, as interfaces físicas são ligadas internamente
- Muito semelhante ao sistema clássico de prevenção de intrusão em linha (IPS)
- Disponível nos modos de implantação roteada ou transparente
- A maioria dos recursos do mecanismo LINA (NAT, roteamento etc.) não está disponível para fluxos que passam por um par em linha
- O tráfego de trânsito pode ser descartado
- Algumas verificações do mecanismo LINA são aplicadas juntamente com verificações completas do mecanismo Snort

O último ponto pode ser visualizado como mostrado na imagem:




## Verificação 1. Com o uso do Packet Tracer

A saída do packet-tracer que emula um pacote que atravessa o par em linha 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

>
```

## Verificação 2. Enviar pacotes TCP SYN/ACK através de pares em linha

Você pode gerar pacotes TCP SYN/ACK com o uso de um utilitário de pacote que cria como Scapy. Esta sintaxe gera 3 pacotes com sinalizadores SYN/ACK ativados:

```
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)
```

Ative essa captura na CLI do FTD e envie alguns 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 de enviar os pacotes pelo FTD, você pode ver uma conexão que foi 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

>
```

**Note**: b flag - Um ASA clássico descartaria um pacote SYN/ACK não solicitado, a menos que o desvio de estado do TCP estivesse ativado. Uma interface FTD no modo Par em Linha trata uma conexão TCP em um modo de desvio de estado TCP e não descarta pacotes TCP que não pertencem às conexões que já existem.

**Observação:** flag N - O pacote é inspecionado pelo mecanismo Snort FTD.

As capturas comprovam isso, já que você pode ver os 3 pacotes que atravessam 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 saem do 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 Rastreamento do primeiro pacote de captura revela algumas informações adicionais, como o veredito do Snort engine:

```
> 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
>
```

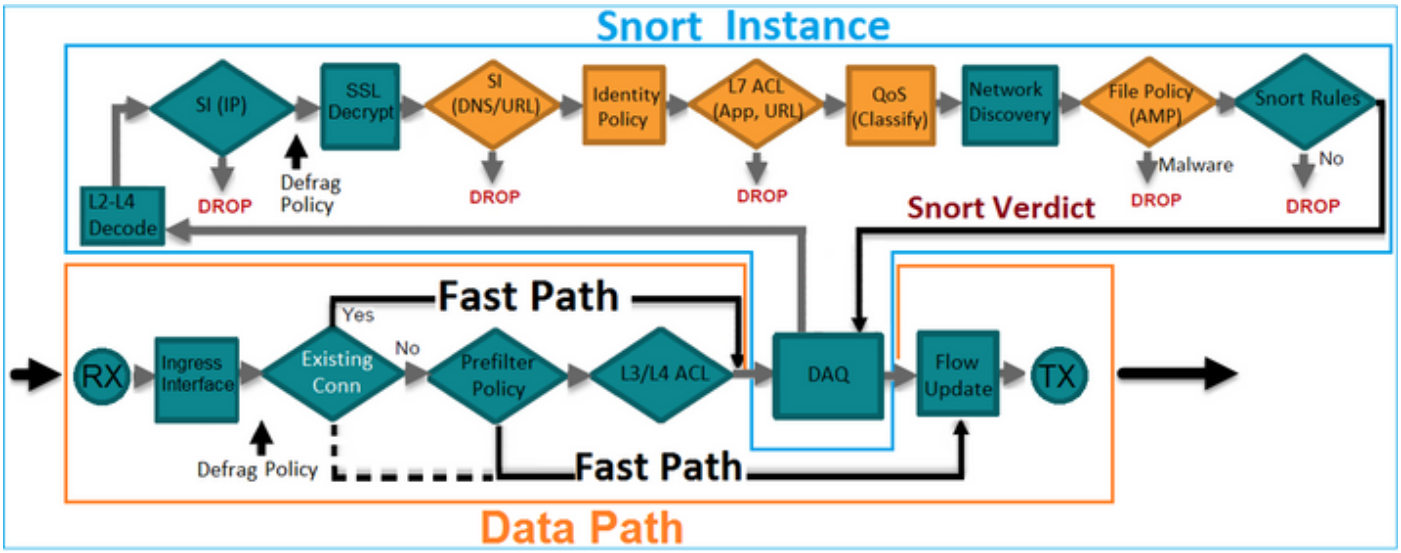
Com o Rastreamento do segundo pacote capturado mostra que o pacote corresponde a uma conexão existente, portanto, ele ignora a verificação da ACL, mas ainda é inspecionado pelo mecanismo Snort:

```
> 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
>
```

## Verificação 3. Depuração Do Firewall Engine Para Tráfego Permitido

A depuração do mecanismo de firewall é executada em relação a componentes específicos do FTD Snort Engine, como a Política de controle de acesso, como mostrado na imagem:




Quando você envia os pacotes TCP SYN/ACK através do Par em Linha, você pode ver na saída de depuração:

```
> 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. Verificar a propagação de estado do link

Ative o registro em buffer no FTD e desligue a porta de switch conectada à interface e1/6. Na CLI do FTD, você deve ver que ambas as interfaces foram desativadas:

```
> 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
>
```

Os registros FTD mostram:

```
> 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 status inline-set mostra o estado dos 2 membros da interface:

```
> 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 a diferença no status das 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
>
```

E para a interface 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 de reativar a porta do switch, os registros 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)
>
```

## Verificação 5. Configurar NAT estático

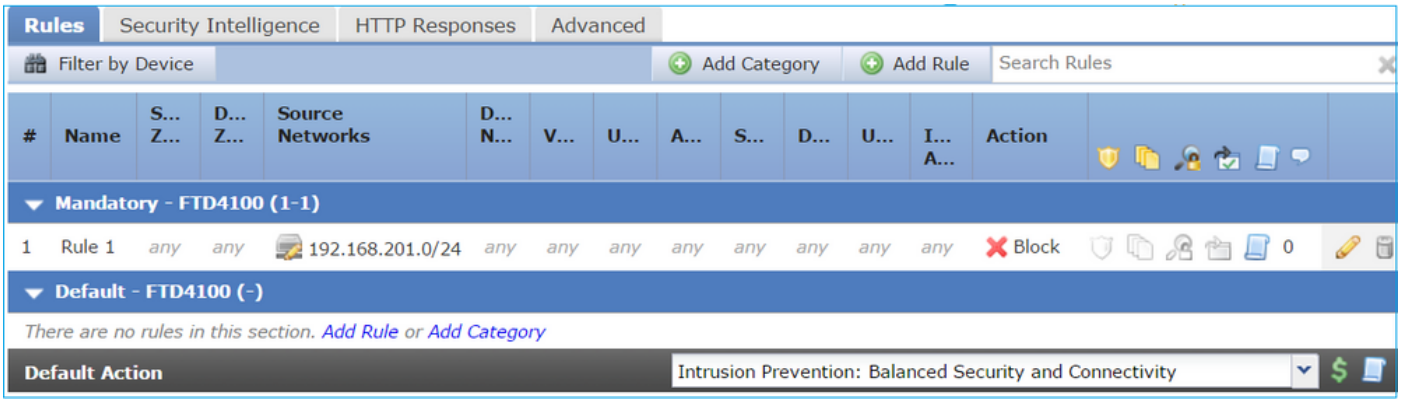
### Solução

O NAT não é suportado para interfaces que operam em modos inline, inline tap ou passivo:

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 de interface de par em linha

Crie uma regra de bloqueio, envie tráfego através do Par em linha FTD e observe o comportamento como mostrado na imagem.




## Solução

Ative a captura com rastreamento e envie os pacotes SYN/ACK através do Par em linha FTD. O tráfego está bloqueado:

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

Com o rastreamento, 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
```

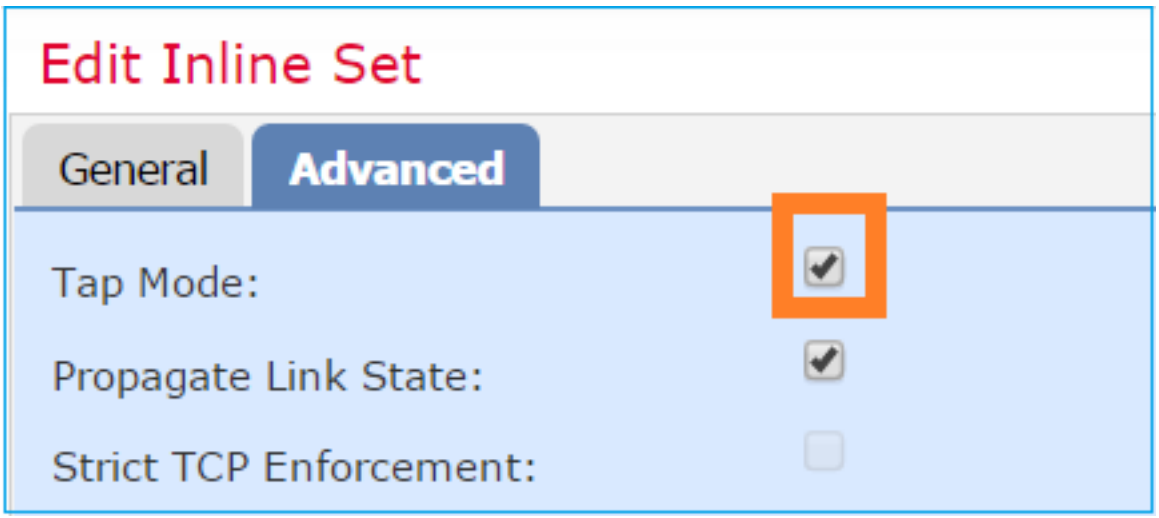
Nesse rastreamento, pode-se ver que o pacote foi descartado pelo mecanismo de LINA do FTD e não foi encaminhado ao mecanismo de Snort do FTD.

# Configurar o modo de par em linha com o toque

Ative o modo Toque no par em linha.

### Solução

Navegue até **Dispositivos > Gerenciamento de dispositivos > Conjuntos em linha > Editar conjunto em linha > Avançado** e habilite o **modo Toque** como mostrado na imagem.



### Verificação

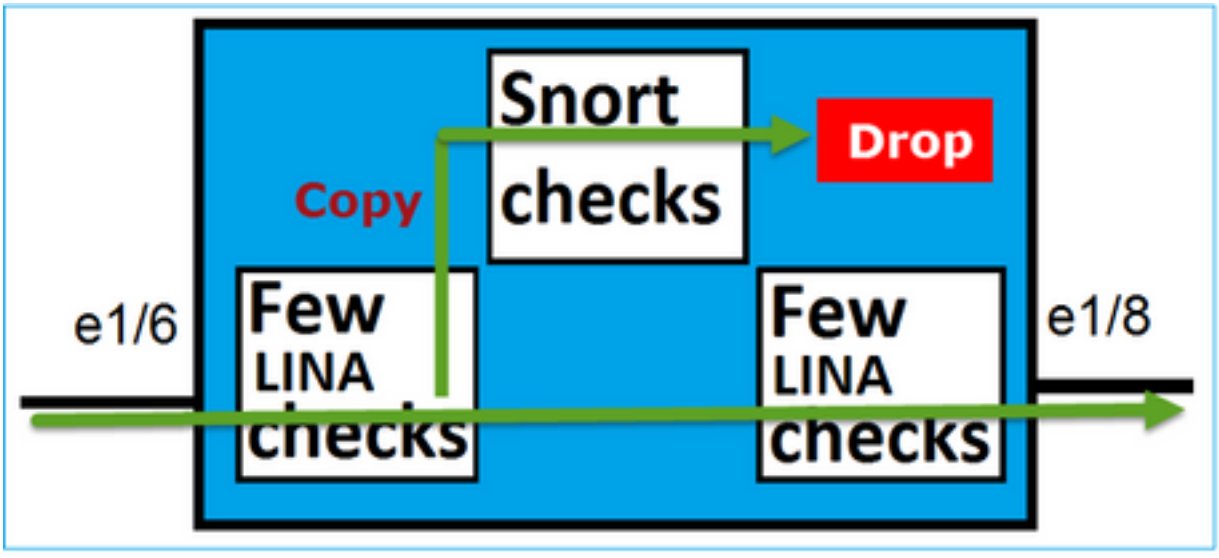
```
> show inline-set

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
>
```

## Verificar o par em linha FTD com a operação da interface da torneira

Teoria básica

- Quando você configura um par em linha com a Tap 2, as interfaces físicas são ligadas internamente
- Ele está disponível nos modos de implantação roteada ou transparente
- A maioria dos recursos do mecanismo LINA (NAT, roteamento etc.) não está disponível para fluxos que passam pelo par em linha
- O tráfego real não pode ser descartado
- Algumas verificações do mecanismo LINA são aplicadas juntamente com verificações completas do mecanismo Snort para uma cópia do tráfego real

O último ponto é como mostrado na imagem:



O par em linha com modo de toque não descarta o tráfego em trânsito. Com o rastreamento de um pacote, ele confirma isso:

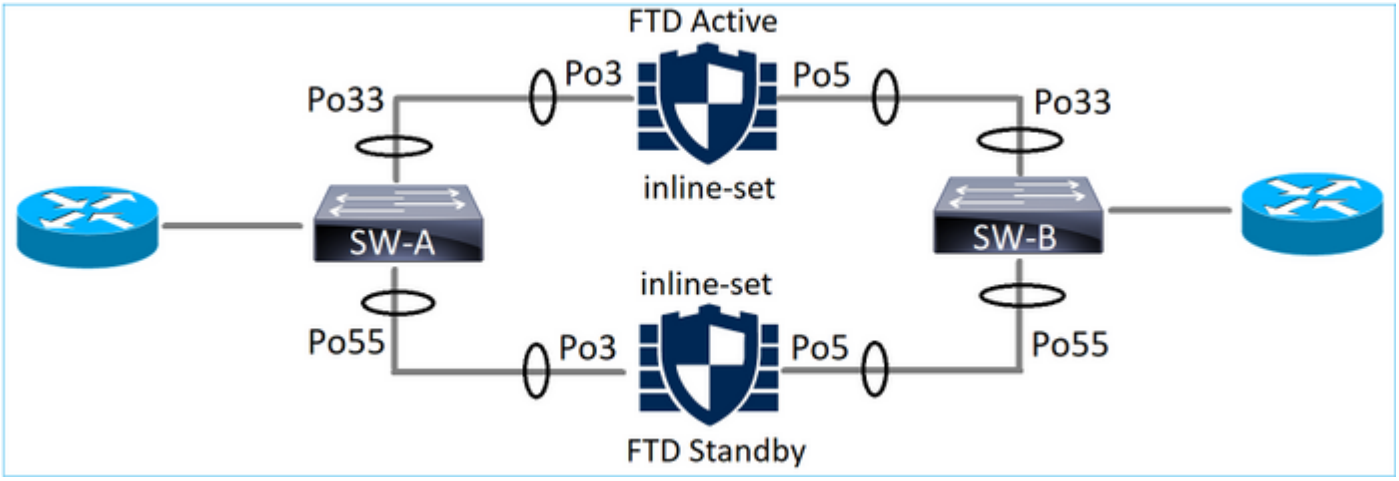
```
> show capture CAPI packet-number 2 trace

3 packets captured

   2: 13:34:30.685084       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: WOULD HAVE DROPPED
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: Access-list would have dropped, but packet forwarded due to inline-tap


1 packet shown
>
```

# Par em linha e Etherchannel

Você pode configurar o par em linha com etherchannel de duas maneiras:

1. Etherchannel terminado no FTD
2. Etherchannel passando pelo FTD (requer código FXOS 2.3.1.3 e superior)

## Etherchannel terminado no FTD




Etherchannels no SW-A:

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

Etherchannels no SW-B:

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

O tráfego está sendo encaminhado através do FTD ativo com base no aprendizado de endereço MAC:

```
SW-B# show mac address-table address 0017.dfd6.ec00
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC     Po33
Total Mac Addresses for this criterion: 1
```

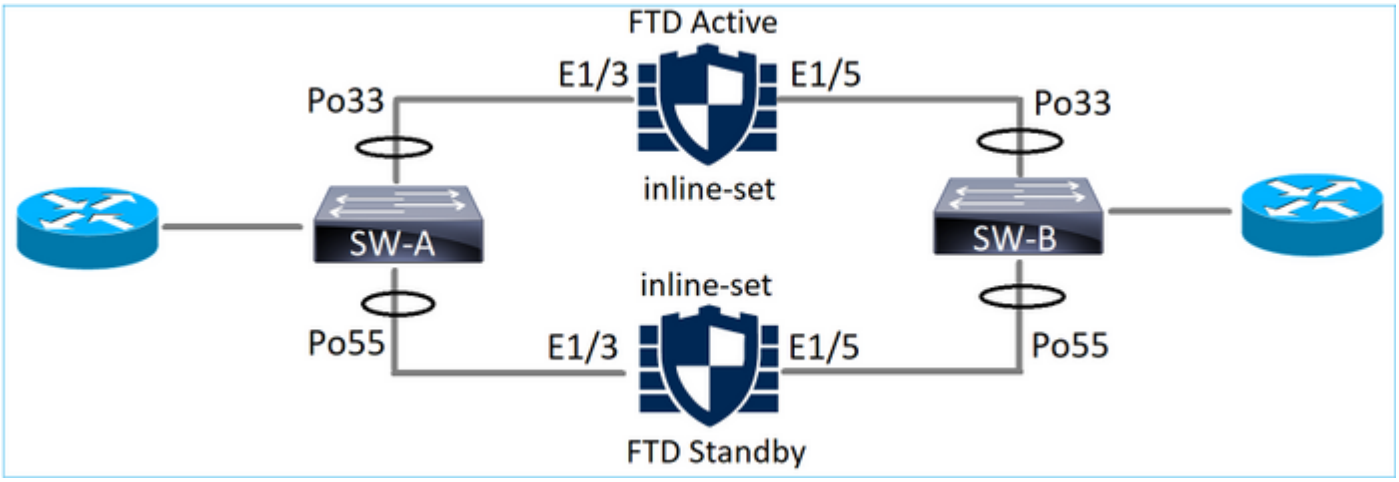
O conjunto em linha no FTD:

```
FTD# show inline-set

Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
```

```
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Port-channel3 "INSIDE"
      Current-Status: UP
    Interface: Port-channel5 "OUTSIDE"
      Current-Status: UP
    Bridge Group ID: 775
```

**Note**: No caso de um evento de failover FTD, a interrupção do tráfego depende principalmente do tempo que os switches levam para aprender o endereço MAC do peer remoto.

## Etherchannel através do FTD




Etherchannels no SW-A:

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

Os pacotes LACP que passam pelo FTD em standby são bloqueados:

```
FTD# capture ASP type asp-drop fo-standby
FTD# show capture ASP | i 0180.c200.0002
  29: 15:28:32.658123       a0f8.4991.ba03 0180.c200.0002 0x8809 Length: 124
  70: 15:28:47.248262       f0f7.556a.11e2 0180.c200.0002 0x8809 Length: 124
```

Etherchannels no SW-B:

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

O tráfego está sendo encaminhado através do FTD ativo com base no aprendizado de endereço MAC:

```
SW-B# show mac address-table address 0017.dfd6.ec00
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC     Po33
Total Mac Addresses for this criterion: 1
```

O conjunto em linha no FTD:

```
FTD# show inline-set

Inline-set SET1
 Mtu is 1500 bytes
 Fail-open for snort down is on
 Fail-open for snort busy is off
 Tap mode is off
 Propagate-link-state option is off
 hardware-bypass mode is disabled
 Interface-Pair[1]:
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/5 "OUTSIDE"
      Current-Status: UP
   Bridge Group ID: 519
```

**Caution**: Neste cenário, no caso de um evento de failover do FTD, o tempo de convergência depende principalmente da negociação do Etherchannel LACP e, dependendo do tempo que leva, a interrupção pode ser bem maior. Caso o modo Etherchannel esteja ON (sem LACP), o tempo de convergência depende do aprendizado do endereço MAC.

# Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

# Comparação: Par em linha vs Par em linha com toque

| | Par em linha | Par embutido com toque |
|---|---|---|
| show inline-set | > show inline-set<br><br>Inline-Pair-1 em linha definida<br>Mtu é 1500 bytes<br>O modo Failsafe está ativado/ativado<br>O modo de failover está desativado<br>**O modo Toque está desativado**<br>A opção Propagate-Link-State está ativada<br>o modo de desvio de hardware está desativado<br>Par da interface[1]:<br>Interface: Ethernet1/6 "DENTRO"<br>Status atual: PARA CIMA<br>Interface: Ethernet1/8 "FORA"<br>Status atual: PARA CIMA<br>**ID do grupo de bridge: 509** | > **show inline-set**<br><br>Inline-Pair-1 em linha definida<br>Mtu é 1500 bytes<br>O modo Failsafe está ativado/ativado<br>O modo de failover está desativado<br>**O modo Toque está ativado**<br>A opção Propagate-Link-State está ativada<br>o modo de desvio de hardware está desativado<br>Par da interface[1]:<br>Interface: Ethernet1/6 "DENTRO"<br>Status atual: PARA CIMA<br>Interface: Ethernet1/8 "FORA"<br>Status atual: PARA CIMA<br>**ID do grupo de bridge: 0** |
| show interface | ><br>> **show interface e1/6**<br>Interface Ethernet1/6 "INSIDE", está ativa, protocolo de linha está ativo<br>O hardware é EtherSVI, BW 1000 Mbps, DLY 1000 usec<br>Endereço MAC 5897.bdb9.770e, MTU 1500<br>Modo de interface IPS: **em linha**, definido em linha: Par em linha-1 | ><br>> **show interface e1/6**<br>Interface Ethernet1/6 "INSIDE", está ativa, protocolo de linha está ativo<br>O hardware é EtherSVI, BW 1000 Mbps, DLY 1000 usec<br>Endereço MAC 5897.bdb9.770e, MTU 1500<br>Modo de interface IPS: **inline-tap**, Inline-Set: Par em linha-1 |

Para tratar o pacote com a regra de bloqueio

```
    Endereço IP não atribuído
 Estatísticas de tráfego para "DENTRO":
    3957 pacotes de entrada, 264913 bytes
    Saída de 144 pacotes, 58664 bytes
    4 pacotes descartados
   Taxa de entrada de 1 minuto 0 pkts/seg, 26 bytes/seg
   Taxa de saída de 1 minuto 0 pkts/seg, 7 bytes/seg
   Taxa de queda de 1 minuto, 0 pkts/seg
   Taxa de entrada de 5 minutos 0 pkts/seg, 28 bytes/seg
   Taxa de saída de 5 minutos 0 pkts/seg, 9 bytes/seg
   Taxa de queda de 5 minutos, 0 pkts/seg
>show interface e1/8
Interface Ethernet1/8 "EXTERNA", está ativa, protocolo de linha está ativo
 O hardware é EtherSVI, BW 1000 Mbps, DLY 1000 usec
    Endereço MAC 5897.bdb9.774d, MTU 1500
    Modo de interface IPS: em linha, definido em linha: Par em linha-1
    Endereço IP não atribuído
 Estatísticas de tráfego para "FORA":
    144 pacotes de entrada, 55634 bytes
    3954 saída de pacotes, 339987 bytes
    0 pacotes descartados
   Taxa de entrada de 1 minuto 0 pkts/seg, 7 bytes/seg
   Taxa de saída de 1 minuto 0 pkts/seg, 37 bytes/seg
   Taxa de queda de 1 minuto, 0 pkts/seg
   Taxa de entrada de 5 minutos 0 pkts/seg, 8 bytes/seg
   Taxa de saída de 5 minutos 0 pkts/seg, 39 bytes/seg
   Taxa de queda de 5 minutos, 0 pkts/seg
>
> show capture CAPI packet-number 1 trace

3 pacotes capturados

  1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win
8192
Fase: 1
Digite: CAPTURA
Subtipo:
Resultado: PERMISSÃO
Config:
Informações adicionais:
Lista de acesso MAC

Fase: 2
Digite: ACCESS-LIST
Subtipo:
Resultado: PERMISSÃO
Config:
Regra implícita
Informações adicionais:
Lista de acesso MAC

Fase: 3
Digite: MODO NGIPS
Subtipo: ngips-mode
Resultado: PERMISSÃO
Config:
Informações adicionais:
O fluxo incorporado em uma interface configurada para o modo NGIPS e os serviços
NGIPS serão aplicados

Fase: 4
Digite: ACCESS-LIST
Subtipo: registro
Resultado: SOLTAR
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 rule-id 268441600: POLÍTICA DE ACESSO:
FTD4100 - Obrigatório/1
access-list CSM_FW_ACL_ remark rule rule-id 268441600: REGRA L4: Regra 1
Informações adicionais:

Resultado:
interface de entrada: INTERNA
estado de entrada: up
status da linha de entrada: up
Ação: queda
Razão da queda: (acl-drop) O fluxo é negado pela regra configurada


1 pacote mostrado
>
```

```
    Endereço IP não atribuído
 Estatísticas de tráfego para "DENTRO":
    entrada de 24 pacotes, 1378 bytes
    0 saída de pacotes, 0 bytes
    24 pacotes descartados
   Taxa de entrada de 1 minuto 0 pkts/seg, 0 bytes/seg
   Taxa de saída de 1 minuto 0 pkts/seg, 0 bytes/seg
   Taxa de queda de 1 minuto, 0 pkts/seg
   Taxa de entrada de 5 minutos 0 pkts/seg, 0 bytes/seg
   Taxa de saída de 5 minutos 0 pkts/seg, 0 bytes/seg
   Taxa de queda de 5 minutos, 0 pkts/seg
>show interface e1/8
Interface Ethernet1/8 "EXTERNA", está ativa, protocolo de linha está ativo
 O hardware é EtherSVI, BW 1000 Mbps, DLY 1000 usec
    Endereço MAC 5897.bdb9.774d, MTU 1500
    Modo de interface IPS: inline-tap, Inline-Set: Par em linha-1
    Endereço IP não atribuído
 Estatísticas de tráfego para "FORA":
    1 entrada de pacotes, 441 bytes
    0 saída de pacotes, 0 bytes
    1 pacote descartado
   Taxa de entrada de 1 minuto 0 pkts/seg, 0 bytes/seg
   Taxa de saída de 1 minuto 0 pkts/seg, 0 bytes/seg
   Taxa de queda de 1 minuto, 0 pkts/seg
   Taxa de entrada de 5 minutos 0 pkts/seg, 0 bytes/seg
   Taxa de saída de 5 minutos 0 pkts/seg, 0 bytes/seg
   Taxa de queda de 5 minutos, 0 pkts/seg
>

> show capture CAPI packet-number 1 trace

3 pacotes capturados

  1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win
Fase: 1
Digite: CAPTURA
Subtipo:
Resultado: PERMISSÃO
Config:
Informações adicionais:
Lista de acesso MAC

Fase: 2
Digite: ACCESS-LIST
Subtipo:
Resultado: PERMISSÃO
Config:
Regra implícita
Informações adicionais:
Lista de acesso MAC

Fase: 3
Digite: MODO NGIPS
Subtipo: ngips-mode
Resultado: PERMISSÃO
Config:
Informações adicionais:
O fluxo incorporado em uma interface configurada para o modo NGIPS e o
NGIPS serão aplicados

Fase: 4
Digite: ACCESS-LIST
Subtipo: registro
Resultado: TERIA CAÍDO
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.
id 268441600 event-log flow-start
access-list CSM_FW_ACL_ remark rule rule-id 268441600: POLÍTICA DE A
FTD4100 - Obrigatório/1
access-list CSM_FW_ACL_ remark rule rule-id 268441600: REGRA L4: Re
Informações adicionais:

Resultado:
interface de entrada: INTERNA
estado de entrada: up
status da linha de entrada: up
Ação: A lista de acesso teria sido descartada, mas o pacote foi encaminha
ao toque em linha


1 pacote mostrado
>
```

# Summary

- Quando você usa o modo Par em linha, o pacote passa principalmente pelo mecanismo de Snort FTD

- As conexões TCP são tratadas em um modo de desvio de estado TCP
- De um ponto de vista do mecanismo do FTD LINA, uma política de ACL é aplicada
- Quando o modo de par em linha está em uso, os pacotes podem ser bloqueados, pois são processados em linha
- Quando o modo de toque está ativado, uma cópia do pacote é inspecionada e removida internamente enquanto o tráfego real passa por FTD não modificado

## Informações Relacionadas

- NGFW do Cisco Firepower
- Suporte Técnico e Documentação - Cisco Systems