

Konfigurieren von FTD-Schnittstellen im Inline-Pair-Modus

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren der Inline-Paare-Schnittstelle in FTD](#)

[Netzwerkdiagramm](#)

[Überprüfung](#)

[Überprüfen des Betriebs der FTD-Inline-Schnittstelle](#)

[Grundlegende Theorie](#)

[Überprüfung 1. Mit Packet-Tracer](#)

[Überprüfung 2. Senden von TCP-SYN/ACK-Paketen über Inline-Paar](#)

[Überprüfung 3. Firewall-Engine-Debug für zulässigen Datenverkehr](#)

[Überprüfung 4. Überprüfen der Link-State-Übertragung](#)

[Überprüfung 5. Konfigurieren der statischen NAT](#)

[Blockieren von Paketen im Inline-Paare-Schnittstellenmodus](#)

[Inline-Paarmodus mit TapP konfigurieren](#)

[Überprüfung des FTD-Inline-Paars mit Tap-Interface-Operation](#)

[Inline-Paar und Etherchannel](#)

[Etherchannel wird über FTD terminiert](#)

[Etherchannel über FTD](#)

[Fehlerbehebung](#)

[Vergleich: Inline-Paar und Inline-Paar mit Tasten](#)

[Zusammenfassung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt die Konfiguration, Verifizierung und den Hintergrundbetrieb einer Inline-Paare-Schnittstelle auf einer FirePOWER Threat Defense (FTD)-Appliance.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Firepower 4150 FTD (Code 6.1.0.x und 6.3.x)
- FirePOWER Management Center (FMC) (Code 6.1.0.x und 6.3.x)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Verwandte Produkte

Dieses Dokument kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

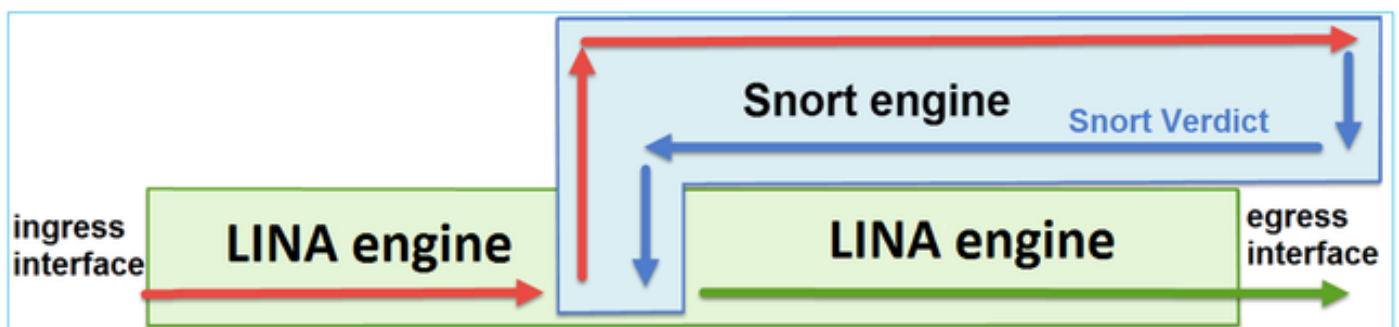
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-basiertes Virtual Machine (KVM)
- FTD Software Code 6.2.x oder höher

Hintergrundinformationen

FTD ist ein einheitliches Software-Image, das aus zwei Hauptmodulen besteht:

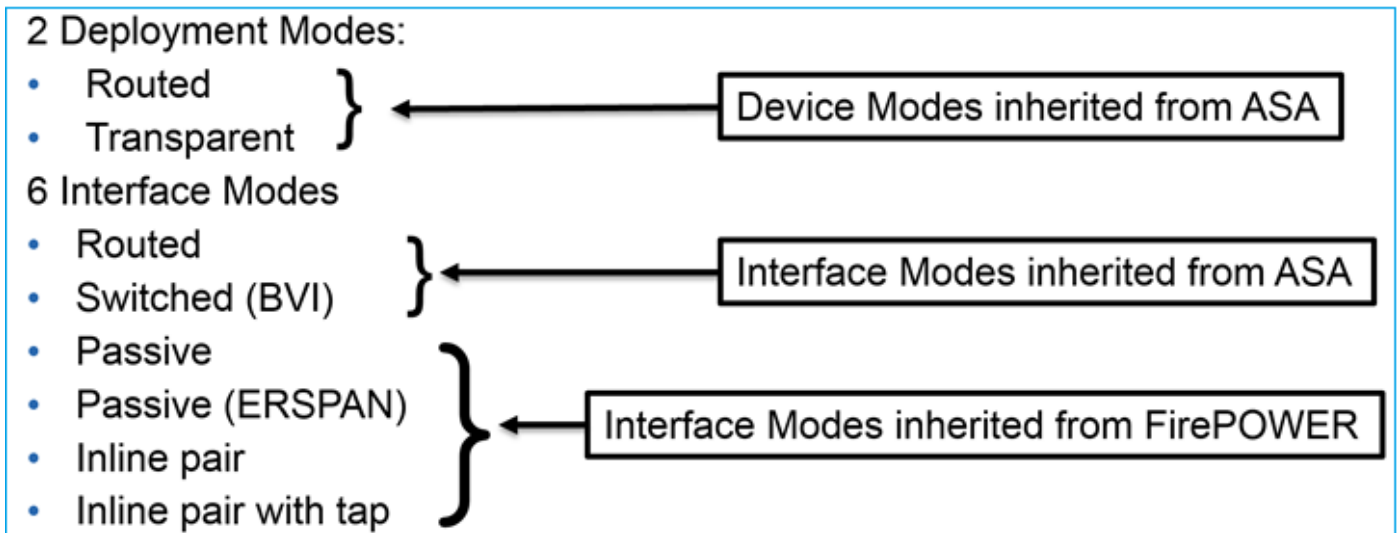
- LINA-Engine
- Snort-Engine

Diese Abbildung zeigt die Interaktion der beiden Engines:



- Ein Paket geht in die Eingangs-Schnittstelle ein, und es wird von der LINA-Engine behandelt
- Wenn die FTD-Richtlinie dies vorschreibt, wird das Paket von der Snort Engine geprüft
- Die Snort-Engine gibt ein Urteil für das Paket zurück.
- Die LINA-Engine verwirft oder leitet das Paket basierend auf dem Urteil von Snort weiter.

FTD stellt zwei Bereitstellungsmodi und sechs Schnittstellenmodi bereit, wie im Bild gezeigt:



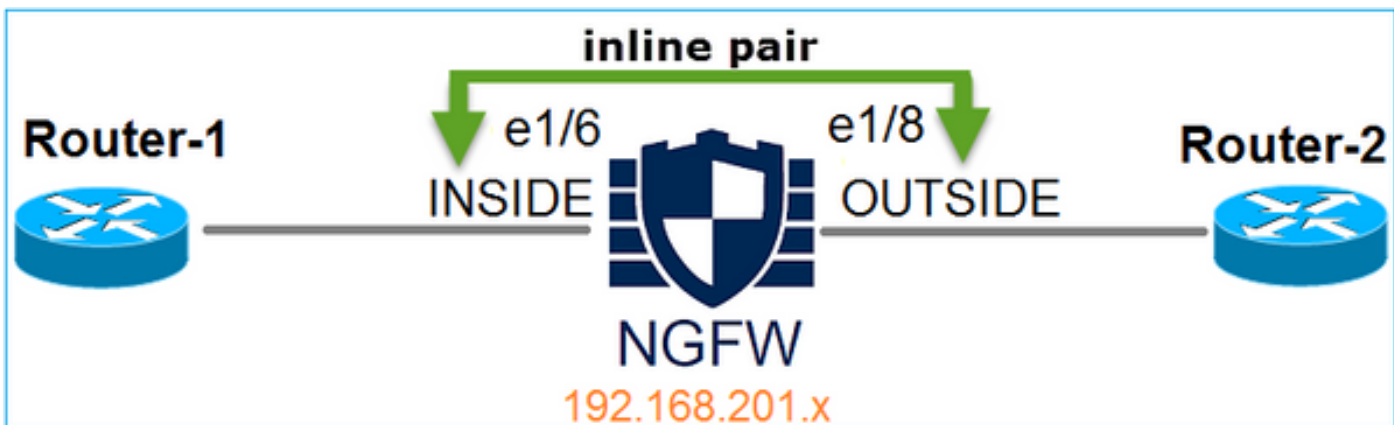
Hinweis: Sie können Schnittstellenmodi auf einer einzigen FTD-Appliance kombinieren.

Im Folgenden finden Sie eine allgemeine Übersicht über die verschiedenen Bereitstellungs- und Schnittstellenmodi der FTD:

FTD-Schnittstellenmodus	FTD-Bereitstellungsmodus	Beschreibung	Datenverkehr kann verworfen werden
Geroutet	Geroutet	Vollständige LINA-Engine- und Snort-Engine-Prüfungen	Ja
Switched	Transparent	Vollständige LINA-Engine- und Snort-Engine-Prüfungen	Ja
Inline-Paar	Geroutet oder transparent	Teilweise LINA-Engine- und vollständige Snort-Engine-Prüfungen	Ja
Inline-Paar mit Tasten	Geroutet oder transparent	Teilweise LINA-Engine- und vollständige Snort-Engine-Prüfungen	Nein
Passiv	Geroutet oder transparent	Teilweise LINA-Engine- und vollständige Snort-Engine-Prüfungen	Nein
Passiv (ERSPAN)	Geroutet	Teilweise LINA-Engine- und vollständige Snort-Engine-Prüfungen	Nein

Konfigurieren der Inline-Paare-Schnittstelle in FTD

Netzwerkdiagramm



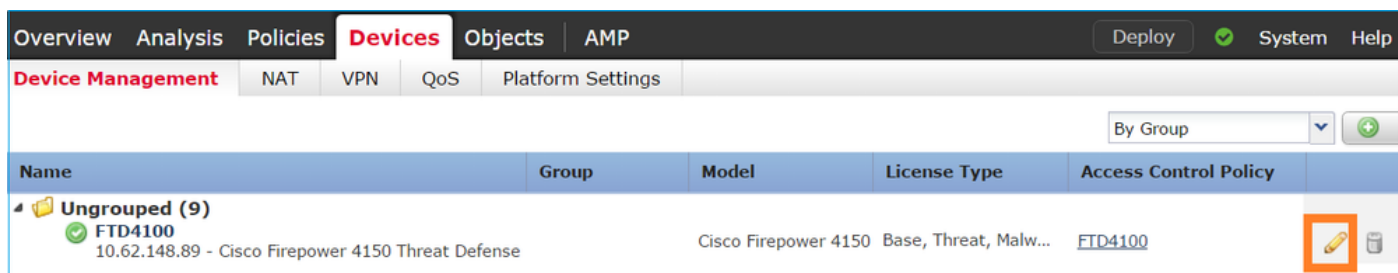
Anforderung

Konfigurieren Sie die physischen Schnittstellen e1/6 und e1/8 im Inline-Paare-Modus gemäß den folgenden Anforderungen:

Schnittstelle	E1/6	E1/8
Name	INNEN	AUSSEN
Sicherheitszone	INSIDE_ZONE	AUSSENBEREICH
Name des Inline-Satzes	Inline-Paar-1	
Inline-Set-MTU	1500	
FailSafe	Aktiviert	
Propagierter Link-Status	Aktiviert	

Lösung

Schritt 1: Um die Konfiguration für die einzelnen Schnittstellen durchzuführen, navigieren Sie zu **Devices > Device Management (Geräte > Gerätemanagement)**, wählen Sie das entsprechende Gerät aus, und wählen Sie **Edit (Bearbeiten)** aus, wie im Bild gezeigt.



Geben Sie als Nächstes den **Namen** und die Option **Aktiviert** für die Schnittstelle an, wie im Bild gezeigt.

Edit Physical Interface

Mode:

Name: Enabled Management Only

Security Zone:

Description:

General | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU: (64 - 9188)

Interface ID:

Hinweis: Der Name ist der Name der Schnittstelle.

Ähnlich bei Schnittstelle Ethernet1/8. Das Endergebnis ist wie im Bild dargestellt.

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			

Schritt 2: Konfigurieren Sie das Inline-Paar.

Navigieren Sie zu **Inlinesätze** > **Inlinesatz hinzufügen**, wie im Bild gezeigt.

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

Device Management NAT VPN QoS Platform Settings Save Cancel

FTD4100

Cisco Firepower 4150 Threat Defense

Devices Routing Interfaces **Inline Sets** DHCP

Name	Interface Pairs
No records to display	

Add Inline Set

Schritt 3: Konfigurieren Sie die allgemeinen Einstellungen gemäß den im Bild angezeigten Anforderungen.

Add Inline Set

General Advanced

Name*: Inline-Pair-1

MTU*: 1500

FailSafe:

Available Interfaces Pairs

- INSIDE<->OUTSIDE

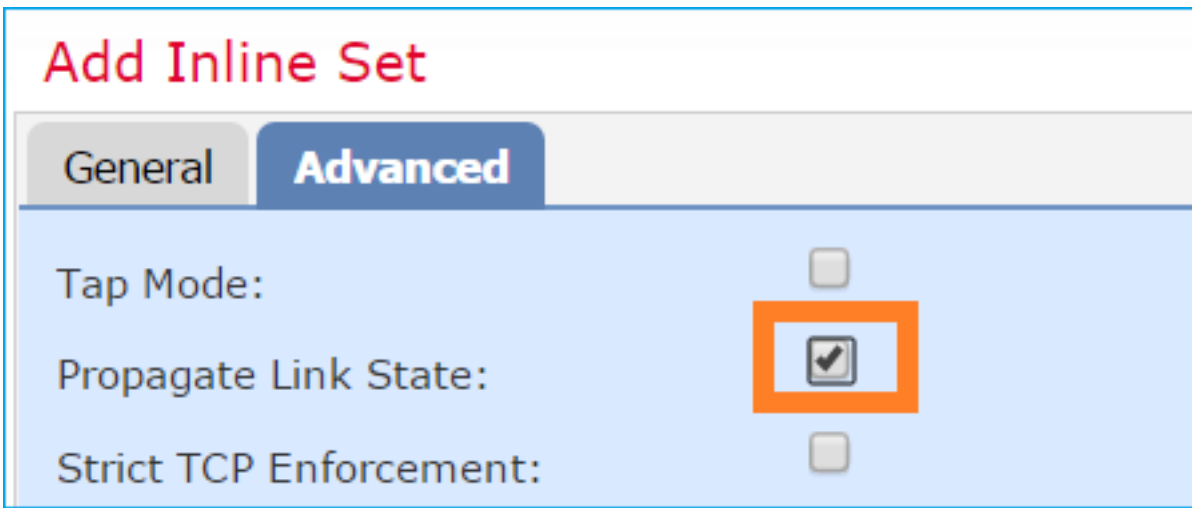
Selected Interface Pair

INSIDE<->OUTSIDE

Add

Hinweis: Failsafe ermöglicht, dass der Datenverkehr das Inline-Paar ungeprüft durchläuft, wenn die Schnittstellen-Puffer voll sind (normalerweise sichtbar, wenn das Gerät überladen oder die Snort-Engine überladen ist). Die Puffergröße der Schnittstelle wird dynamisch zugewiesen.

Schritt 4: Aktivieren Sie die Option **Propagate Link State** (Propagate Link-Status) in den erweiterten Einstellungen, wie im Bild gezeigt.



Durch die Übertragung des Verbindungsstatus wird die zweite Schnittstelle im Inline-Schnittstellenpaar automatisch deaktiviert, wenn eine der Schnittstellen im Inline-Set ausfällt.

Schritt 5: **Speichern** der Änderungen und **Bereitstellen**.

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen Sie die Inline-Paare-Konfiguration aus der FTD-CLI.

Lösung

Melden Sie sich bei der FTD-CLI an, und überprüfen Sie die Inline-Paare-Konfiguration:

```
> 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
>
```

Hinweis: Die Bridge-Gruppen-ID ist ein Wert, der sich von 0 unterscheidet. Wenn der Tap-Modus aktiviert ist, ist er 0.

Schnittstellen- und Namensinformationen:

> show nameif

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

>

Überprüfen Sie den Schnittstellenstatus:

> 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

Überprüfen Sie die Informationen zur physischen Schnittstelle:

> 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

>

Überprüfen des Betriebs der FTD-Inline-Schnittstelle

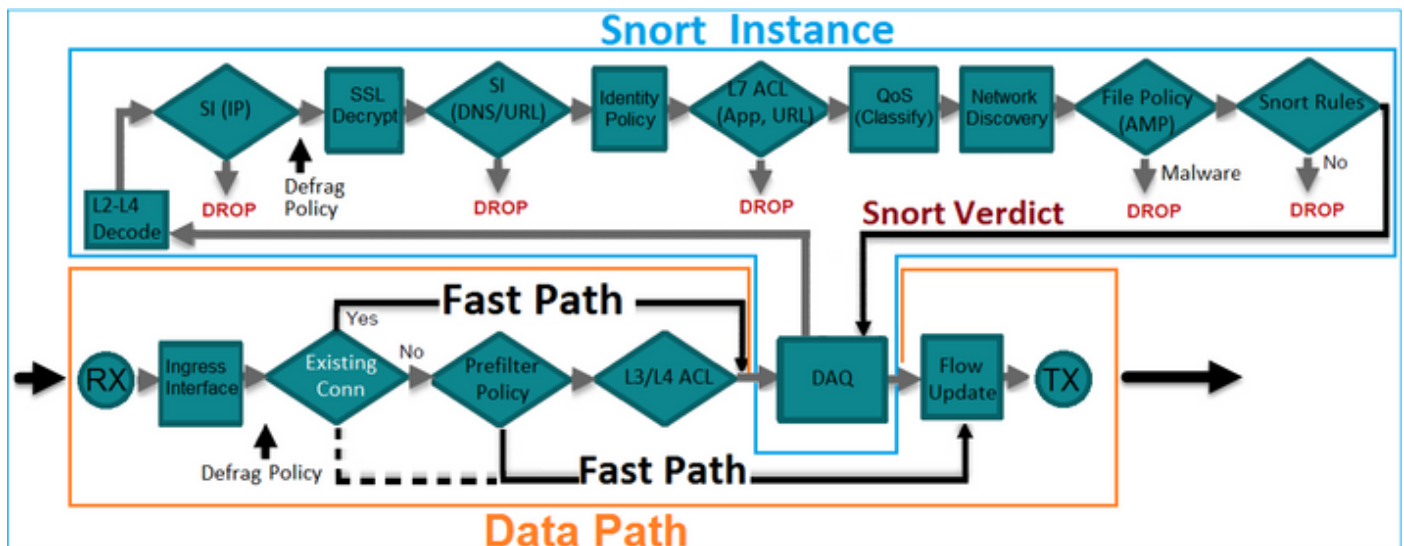
In diesem Abschnitt werden die folgenden Überprüfungen erläutert, um die Inline-Paare-Operation zu überprüfen:

- Überprüfung 1. Mit Packet-Tracer
- Überprüfung 2. Aktivieren der Erfassung mit Trace und Senden eines TCP-Pakets zur Synchronisierung/Bestätigung (SYN/ACK) über das Inline-Paar
- Überprüfung 3. Überwachung von FTD-Datenverkehr mithilfe von Firewall-Engine-Debugging
- Überprüfung 4. Überprüfen der Link-State-Weiterleitungsfunktion
- Überprüfung 5. Konfigurieren der NAT (Static Network Address Translation)

Lösung

Architekturübersicht

Wenn zwei FTD-Schnittstellen im Inline-Pair-Modus arbeiten, wird ein Paket wie im Bild gezeigt behandelt.

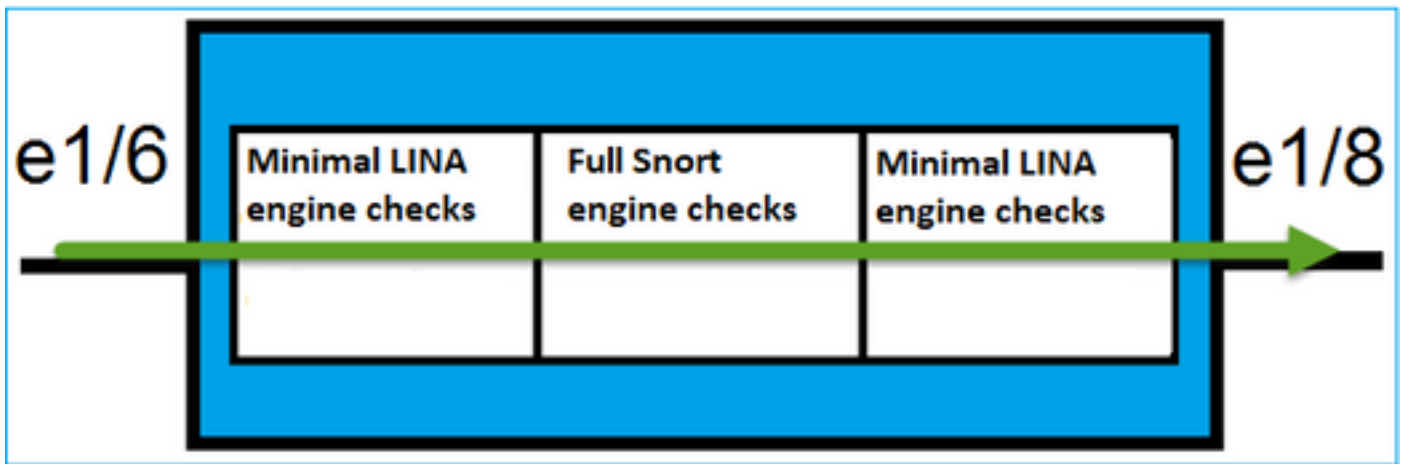


Hinweis: Nur physische Schnittstellen können einem Inline-Paarsatz angehören.

Grundlegende Theorie

- Wenn Sie ein Inline-Paar konfigurieren, werden physische Schnittstellen 2 intern überbrückt
- Sehr ähnlich wie klassisches Inline Intrusion Prevention System (IPS)
- Verfügbar im Bereitstellungsmodus Routed oder Transparent
- Die meisten LINA-Engine-Funktionen (NAT, Routing usw.) sind für Datenflüsse, die ein Inline-Paar durchlaufen, nicht verfügbar
- Transitverkehr kann verworfen werden
- Es werden einige LINA-Engine-Prüfungen und vollständige Snort Engine-Prüfungen angewendet.

Der letzte Punkt kann visualisiert werden, wie im Bild gezeigt:



Überprüfung 1. Mit Packet-Tracer

Die Packet-Tracer-Ausgabe, die ein Paket emuliert, das das Inline-Paar passiert, wobei die wichtigsten Punkte hervorgehoben werden:

```
> 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

>

Überprüfung 2. Senden von TCP-SYN/ACK-Paketen über Inline-Paar

Sie können TCP-SYN/ACK-Pakete mithilfe eines Pakets generieren, das ein Dienstprogramm wie Scapy erstellt. Diese Syntax generiert 3 Pakete mit aktivierten SYN/ACK-Flags:

```
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)
```

Aktivieren Sie diese Erfassung über FTD-CLI, und senden Sie einige TCP-SYN/ACK-Pakete:

```
> 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
>
```

Nachdem Sie die Pakete über FTD gesendet haben, wird eine Verbindung angezeigt, die erstellt wurde:

```
> 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
```

>

Hinweis: b-Flag - Eine klassische ASA würde ein unerwünschtes SYN/ACK-Paket verwerfen, wenn der TCP-State-Bypass nicht aktiviert wurde. Eine FTD-Schnittstelle im Inline-Pair-Modus verarbeitet eine TCP-Verbindung im TCP-Zustandsumgehungsmodus und verwirft keine TCP-Pakete, die nicht zu den bereits vorhandenen Verbindungen gehören.

Hinweis: N-Markierung - Das Paket wird von der FTD Snort Engine geprüft.

Die Aufzeichnungen belegen dies, da Sie die drei Pakete sehen können, die die FTD passieren:

```
> 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 Pakete verlassen das FTD-Gerät:

```
> 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
```

>

Mit Trace des ersten Erfassungspakets werden einige zusätzliche Informationen angezeigt, z. B. das Snort Engine-Urteil:

```
> 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
>
```

Der Trace des zweiten aufgezeichneten Pakets zeigt, dass das Paket mit einer vorhandenen Verbindung übereinstimmt, sodass es die ACL-Prüfung umgeht, aber trotzdem von der Snort-Engine überprüft wird:

```
> 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

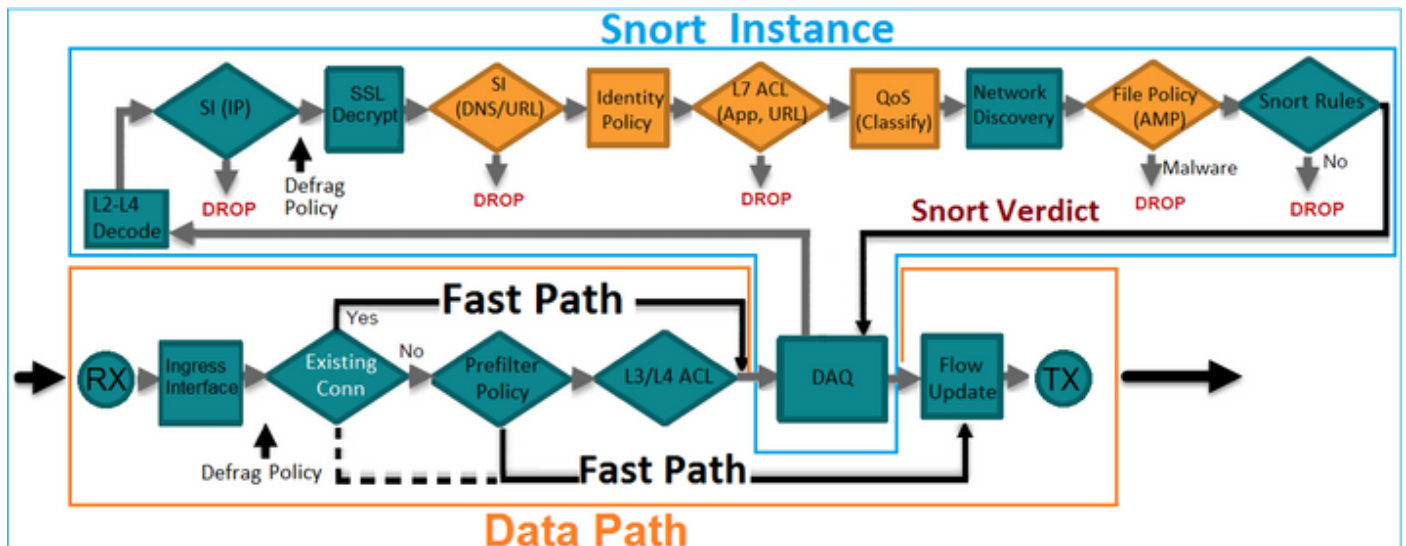
Result:
 input-interface: OUTSIDE
 input-status: up
 input-line-status: up
 Action: allow

1 packet shown

>

Überprüfung 3. Firewall-Engine-Debug für zulässigen Datenverkehr

Firewall-Engine-Debugging wird für bestimmte Komponenten der FTD Snort Engine ausgeführt, wie die Zugriffskontrollrichtlinie, wie im Bild gezeigt:



Wenn Sie die TCP-SYN/ACK-Pakete über das Inline-Paar senden, sehen Sie in der Debug-Ausgabe:

```
> 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

```

Überprüfung 4. Überprüfen der Link-State-Übertragung

Aktivieren Sie die Pufferprotokollierung auf FTD, und schalten Sie den mit der e1/6-Schnittstelle verbundenen Switch-Port aus. Bei FTD CLI sind beide Schnittstellen ausgefallen:

```

> 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
>

```

Die FTD-Protokolle werden angezeigt:

```

> 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)
>

```

Der Inline-Set-Status zeigt den Status der beiden Schnittstellenmember an:

```

> 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
>

```

Beachten Sie den Unterschied im Status der beiden Schnittstellen:


```

> 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
>

```

Und für die Ethernet1/8-Schnittstelle:

```

> 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
>

```

Nachdem Sie den Switch-Port erneut aktiviert haben, werden folgende FTD-Protokolle angezeigt:

```

> 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)
>

```

Überprüfung 5. Konfigurieren der statischen NAT

Lösung

NAT wird für Schnittstellen, die im Inline-, Inline-Tap- oder passiven Modus betrieben werden, nicht unterstützt:

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

Blockieren von Paketen im Inline-Paare-Schnittstellenmodus

Erstellen Sie eine Blockregel, senden Sie Datenverkehr über das FTD Inline-Paar, und beobachten Sie das Verhalten wie im Bild gezeigt.

#	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	0
▼ Default - FTD4100 (-)														
There are no rules in this section. Add Rule or Add Category														
Default Action												Intrusion Prevention: Balanced Security and Connectivity		

Lösung

Aktivieren Sie die Erfassung mit Ablaufverfolgung, und senden Sie die SYN/ACK-Pakete über das FTD-Inline-Paar. Der Datenverkehr wird blockiert:

```
> 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
```

Mit der Ablaufverfolgung zeigt ein Paket Folgendes an:

```
> 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

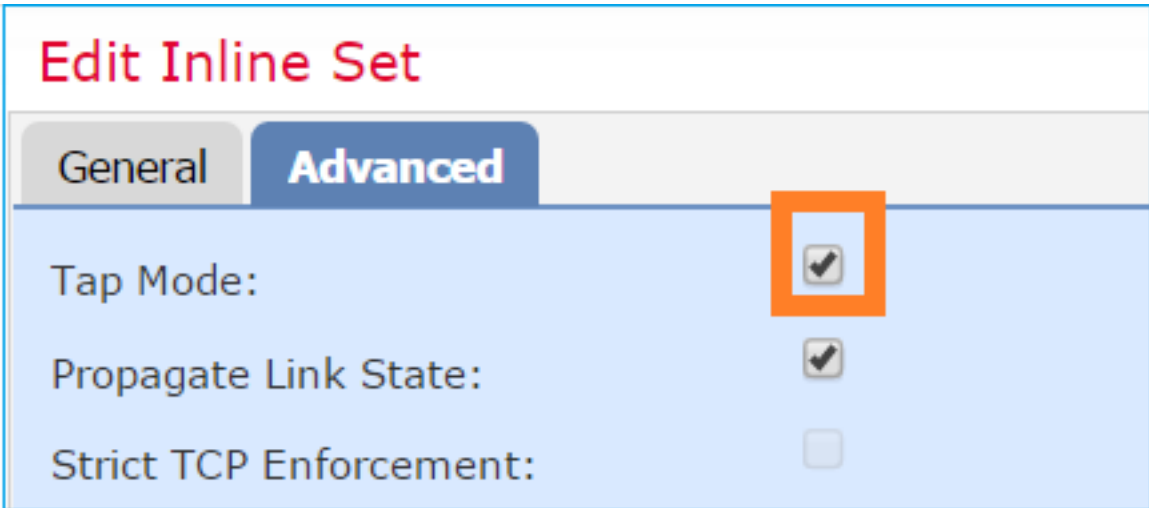
In dieser Spur ist zu erkennen, dass das Paket von der FTD LINA Engine verworfen und nicht an die FTD Snort Engine weitergeleitet wurde.

Inline-Paarmodus mit TapP konfigurieren

Aktivieren Sie den Tap-Modus im Inline-Paar.

Lösung

Navigieren Sie zu **Geräte > Gerätemanagement > Inlinesätze > Inlinesatz bearbeiten > Erweitert**, und aktivieren Sie **den** im Bild angezeigten **Modus**.



The screenshot shows a web interface for editing an inline set. The title is 'Edit Inline Set' in red. There are two tabs: 'General' and 'Advanced', with 'Advanced' selected. Under the 'Advanced' tab, there are three settings:

- Tap Mode:** This setting is checked, and the checkbox is highlighted with an orange square.
- Propagate Link State:** This setting is also checked.
- Strict TCP Enforcement:** This setting is unchecked.

Überprüfung

```
> 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
```

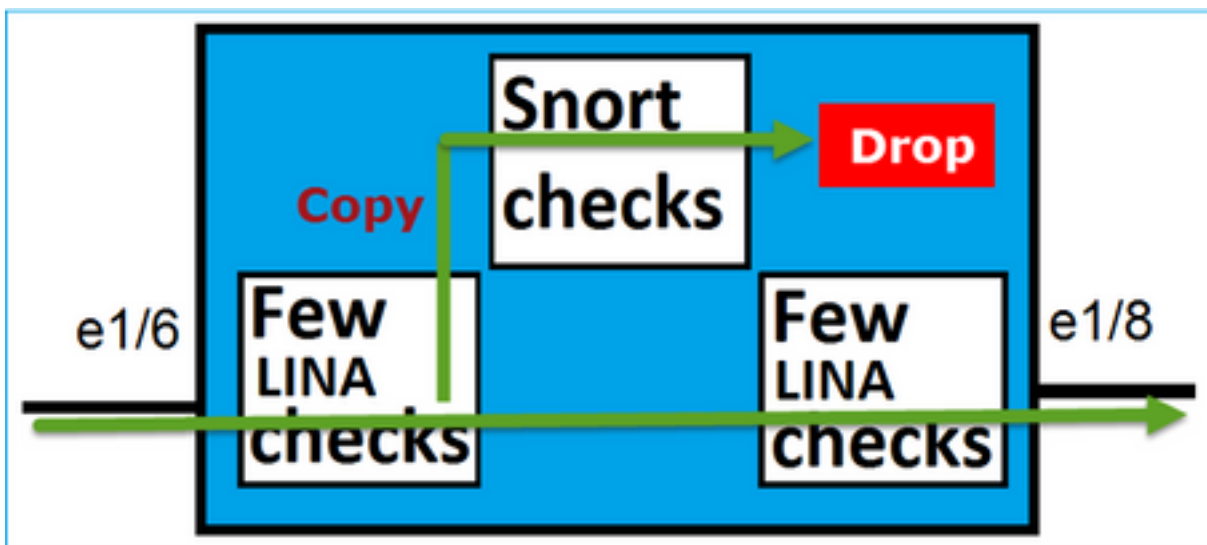
```
>
```

Überprüfung des FTD-Inline-Paars mit Tap-Interface-Operation

Grundlegende Theorie

- Wenn Sie ein Inline-Paar mit Tap 2 konfigurieren, werden physische Schnittstellen intern überbrückt
- Es ist im Routed- oder Transparent Deployment-Modus verfügbar
- Die meisten LINA-Engine-Funktionen (NAT, Routing usw.) sind für Datenflüsse, die das Inline-Paar durchlaufen, nicht verfügbar
- Tatsächlicher Datenverkehr kann nicht verworfen werden
- Es werden einige LINA-Engine-Überprüfungen angewendet, zusammen mit vollständigen Snort Engine-Prüfungen für eine Kopie des tatsächlichen Datenverkehrs.

Der letzte Punkt ist, wie im Bild gezeigt:



Das Inline-Paar mit dem Tap-Modus verwirft den Transitverkehr nicht. Mit der Nachverfolgung eines Pakets wird Folgendes bestätigt:

```
> 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
```

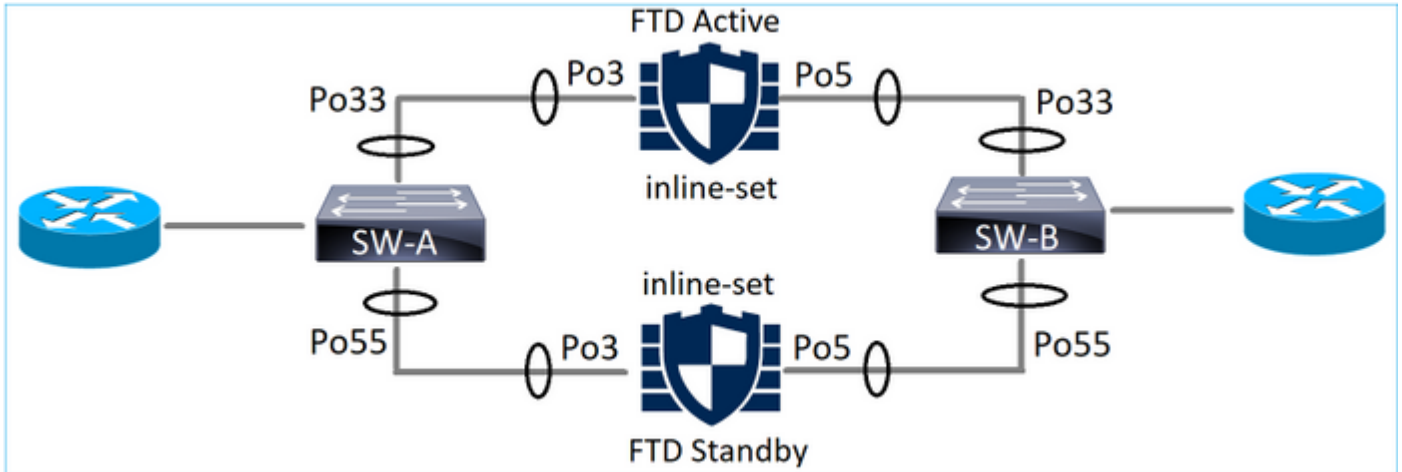
```
>
```

Inline-Paar und Etherchannel

Sie haben zwei Möglichkeiten, ein Inline-Paar mit einem EtherChannel zu konfigurieren:

1. Etherchannel wird über FTD terminiert
2. Etherchannel über FTD (erfordert FXOS-Code 2.3.1.3 und höher)

Etherchannel wird über FTD terminiert



EtherChannels auf 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 auf 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)
```

Der Datenverkehr wird über die aktive FTD weitergeleitet, basierend auf dem MAC-Adresslernen:

```
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
```

Die Inline-Einstellung für 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]:

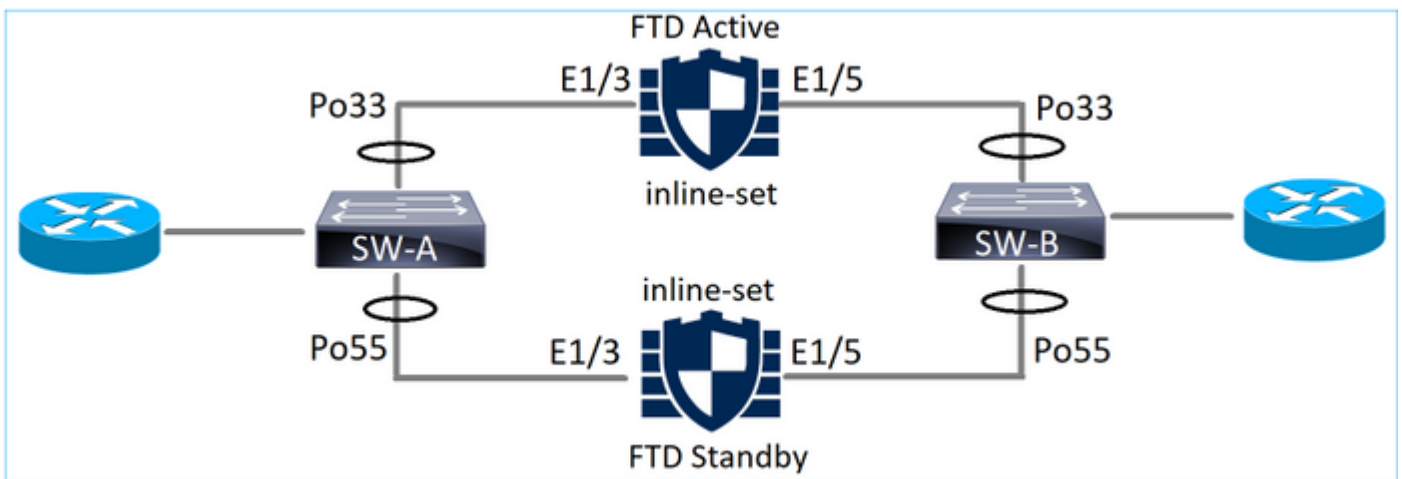
```

Interface: Port-channel3 "INSIDE"
Current-Status: UP
Interface: Port-channel5 "OUTSIDE"
Current-Status: UP
Bridge Group ID: 775

```

Hinweis: Bei einem FTD-Failover hängt der Datenverkehrsausfall hauptsächlich von der Zeit ab, die die Switches benötigen, um die MAC-Adresse des Remote-Peers zu ermitteln.

Etherchannel über FTD



EtherChannels auf SW-A:

```

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

```

Die LACP-Pakete, die das Standby-FTD durchlaufen, werden blockiert:

```

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 auf 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)

```

Der Datenverkehr wird über die aktive FTD weitergeleitet, basierend auf dem MAC-Adresslernen:

```
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
```

Die Inline-Einstellung für 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
```

Vorsicht: In diesem Szenario hängt die Konvergenzzeit bei einem FTD-Failover-Ereignis hauptsächlich von der Etherchannel-LACP-Aushandlung ab und kann je nach Dauer des Ausfalls etwas länger dauern. Wenn der Etherchannel-Modus eingeschaltet ist (kein LACP), hängt die Konvergenzzeit vom Lernen der MAC-Adresse ab.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Vergleich: Inline-Paar und Inline-Paar mit Tasten

	Inline-Paar	Inline-Paar mit Tap
Inline-Satz anzeigen	<pre>> Inline-Satz anzeigen Inline-Set Inline-Paar-1 MTU beträgt 1.500 Byte Der Failsafe-Modus ist aktiviert/aktiviert. Der ausgefallene Modus ist deaktiviert. Der Tap-Modus ist deaktiviert. Option "Propagate-Link-State" ist aktiviert Der Hardware-Umgehungsmodus ist deaktiviert. Schnittstellenpaar[1]: Schnittstelle: Ethernet1/6 "INSIDE" Aktueller Status: UP Schnittstelle: Ethernet1/8 "AUSSEN" Aktueller Status: UP Bridge-Gruppen-ID: 509 ></pre>	<pre>> Inline-Satz anzeigen Inline-Set Inline-Paar-1 MTU beträgt 1.500 Byte Der Failsafe-Modus ist aktiviert/aktiviert. Der ausgefallene Modus ist deaktiviert. Tap-Modus ist aktiviert. Option "Propagate-Link-State" ist aktiviert Der Hardware-Umgehungsmodus ist deaktiviert. Schnittstellenpaar[1]: Schnittstelle: Ethernet1/6 "INSIDE" Aktueller Status: UP Schnittstelle: Ethernet1/8 "AUSSEN" Aktueller Status: UP Bridge-Gruppen-ID: 0 ></pre>
Anzeigeschnittstelle	<pre>> Schnittstelle e1/6 anzeigen Schnittstelle Ethernet1/6 "INSIDE", ist aktiv, Leitungsprotokoll ist aktiv Hardware ist EtherSVI, BW 1000 Mbit/s, DLY 1000 µs MAC-Adresse 5897.bdb9.770e, MTU 1500 IPS-Schnittstellenmodus: Inline, Inline-Set: Inline-Paar-1</pre>	<pre>> Schnittstelle e1/6 anzeigen Schnittstelle Ethernet1/6 "INSIDE", ist aktiv, Leitungsprotokoll ist aktiv Hardware ist EtherSVI, BW 1000 Mbit/s, DLY 1000 µs MAC-Adresse 5897.bdb9.770e, MTU 1500 IPS-Schnittstellenmodus: Inline-Tap, Inline-Set: Inline-Paar-1</pre>

IP-Adresse nicht zugewiesen
Datenverkehrsstatistiken für "INSIDE":
3.957 Paketen-Eingang, 26.4913 Byte
Ausgabe von 144 Paketen, 58664 Byte
4 Pakete verworfen
Eine Minute Eingangsrate 0 Pkte/s, 26 Byte/s
Eine Minute Ausgangsrate 0 Pkte/s, 7 Byte/s
Verlustrate von 1 Minute, 0 Pkte/s
5-Minuten-Eingangsrate 0 Pkte/s, 28 Byte/s
5-Minuten-Ausgaberate 0 Pkte/s, 9 Byte/s
5-Minuten-Verlustrate, 0 Pkte/s

>Schnittstelle e1/8 anzeigen

Schnittstelle Ethernet1/8 "OUTSIDE", ist aktiv, Leitungsprotokoll ist aktiv
Hardware ist EtherSVI, BW 1000 Mbit/s, DLY 1000 µs

MAC-Adresse 5897.bdb9.774d, MTU 1500
IPS-Schnittstellenmodus: **Inline**, Inline-Set: Inline-Paar-1
IP-Adresse nicht zugewiesen

Datenverkehrsstatistiken für "AUSSEN":

Eingabe von 144 Paketen, 55634 Byte
3954 Pakete Ausgabe, 339987 Byte
0 Pakete verworfen
Eine Minute Eingangsrate 0 Pkte/s, 7 Byte/s
Eine Minute Ausgangsrate 0 Pkte/s, 37 Byte/s
Verlustrate von 1 Minute, 0 Pkte/s
5-Minuten-Eingangsrate 0 Pkte/s, 8 Byte/s
5 Minuten Ausgangsrate 0 Pkte/s, 39 Byte/s
5-Minuten-Verlustrate, 0 Pkte/s

>

> CAPI Packet-Number 1 Trace für die CAPI-Erfassung anzeigen

3 erfasste Pakete

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
Typ: ERFASSEN
Untertyp:
Ergebnis: ZULASSEN
Konfiguration:
Zusätzliche Informationen:
MAC-Zugriffsliste

Phase: 2
Typ: ZUGRIFFSLISTE
Untertyp:
Ergebnis: ZULASSEN
Konfiguration:
Implizite Regel
Zusätzliche Informationen:
MAC-Zugriffsliste

Phase: 3
Typ: NGIPS-MODUS
Untertyp: NGIPS-Modus
Ergebnis: ZULASSEN
Konfiguration:

Zusätzliche Informationen:
Der eingehende Datenfluss, eine für den NGIPS-Modus konfigurierte Schnittstelle und NGIPS-Services werden angewendet.

Phase: 4
Typ: ZUGRIFFSLISTE
Untertyp: Protokoll
Ergebnis: VERLOREN
Konfiguration:

Zugriffsgruppe CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced deny ip 192.168.201.0 255.255.255.0 any
regel-id 268441600 event-log flow-start
access-list CSM_FW_ACL_Hinweis zur Regel-ID 268441600:
ZUGRIFFSRICHTLINIE: FTD4100 - Obligatorisch/1
access-list CSM_FW_ACL_Hinweis zur Regel-ID 268441600: L4-REGEL: Regel 1
Zusätzliche Informationen:

Ergebnis:
Eingabeschnittstelle: INNEN
Eingabestatus: hochfahren
Eingabezeilenstatus: hochfahren
Aktion: Tropfen
Gründe für Verwerfen: (acl-drop) Fluss wird durch konfigurierte Regel abgelehnt

1 Paket angezeigt
>

IP-Adresse nicht zugewiesen
Datenverkehrsstatistiken für "INSIDE":
Eingabe von 24 Paketen, 1378 Byte
0 Paketausgabe, 0 Byte
24 Pakete verworfen
Eine Minute Eingangsrate 0 Pkte/s, 0 Byte/s
Eine Minute Ausgangsrate 0 Pkte/s, 0 Byte/s
Verlustrate von 1 Minute, 0 Pkte/s
5-Minuten-Eingangsrate 0 Pkte/s, 0 Byte/s
5-Minuten-Ausgaberate 0 Pkte/s, 0 Byte/s
5-Minuten-Verlustrate, 0 Pkte/s

>Schnittstelle e1/8 anzeigen

Schnittstelle Ethernet1/8 "OUTSIDE", ist aktiv, Leitungsprotokoll ist aktiv
Hardware ist EtherSVI, BW 1000 Mbit/s, DLY 1000 µs

MAC-Adresse 5897.bdb9.774d, MTU 1500
IPS-Schnittstellenmodus: **Inline-Tap**, Inline-Set: Inline-Paar-1
IP-Adresse nicht zugewiesen

Datenverkehrsstatistiken für "AUSSEN":

1 Paketeingabe, 441 Byte
0 Paketausgabe, 0 Byte
1 Paket verworfen
Eine Minute Eingangsrate 0 Pkte/s, 0 Byte/s
Eine Minute Ausgangsrate 0 Pkte/s, 0 Byte/s
Verlustrate von 1 Minute, 0 Pkte/s
5-Minuten-Eingangsrate 0 Pkte/s, 0 Byte/s
5-Minuten-Ausgaberate 0 Pkte/s, 0 Byte/s
5-Minuten-Verlustrate, 0 Pkte/s

>

> CAPI Packet-Number 1 Trace für die CAPI-Erfassung anzeigen

3 erfasste Pakete

1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) geo 8192

Phase: 1
Typ: ERFASSEN
Untertyp:
Ergebnis: ZULASSEN
Konfiguration:
Zusätzliche Informationen:
MAC-Zugriffsliste

Phase: 2
Typ: ZUGRIFFSLISTE
Untertyp:
Ergebnis: ZULASSEN
Konfiguration:
Implizite Regel
Zusätzliche Informationen:
MAC-Zugriffsliste

Phase: 3
Typ: NGIPS-MODUS
Untertyp: NGIPS-Modus
Ergebnis: ZULASSEN
Konfiguration:

Zusätzliche Informationen:
Der eingehende Datenfluss, eine für den NGIPS-Modus konfigurierte Schnittstelle und NGIPS-Services werden angewendet.

Phase: 4
Typ: ZUGRIFFSLISTE
Untertyp: Protokoll
Ergebnis: HÄTTE ABGEBROCHEN
Konfiguration:

Zugriffsgruppe CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced deny ip 192.168.201.0 255.255.255.0 any
regel-id 268441600 event-log flow-start
access-list CSM_FW_ACL_Hinweis zur Regel-ID 268441600:
ZUGRIFFSRICHTLINIE: FTD4100 - Obligatorisch/1
access-list CSM_FW_ACL_Hinweis zur Regel-ID 268441600: L4-REGEL: Regel 1
Zusätzliche Informationen:

Ergebnis:
Eingabeschnittstelle: INNEN
Eingabestatus: hochfahren
Eingabezeilenstatus: hochfahren
Aktion: Die Zugriffsliste wäre verloren gegangen, aber das Paket wurde auf Inline-Tap weitergeleitet.

1 Paket angezeigt
>

So
behandeln
Sie Paket mit
Blockregel

Zusammenfassung

- Wenn Sie den Inline-Pair-Modus verwenden, durchläuft das Paket hauptsächlich die FTD-Snort-Engine.

- TCP-Verbindungen werden im TCP-Zustandsumgehungsmodus behandelt.
- Aus Sicht der FTD LINA Engine wird eine ACL-Richtlinie angewendet
- Wenn Inline-Paare verwendet werden, können Pakete blockiert werden, da sie inline verarbeitet werden
- Wenn der Tap-Modus aktiviert ist, wird eine Kopie des Pakets intern überprüft und verworfen, während der tatsächliche Datenverkehr unverändert über FTD läuft.

Zugehörige Informationen

- [Cisco FirePOWER NGFW](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)