

Konfigurieren von Firepower Threat Defense-Schnittstellen im Routing-Modus

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Verwandte Produkte](#)
- [Hintergrundinformationen](#)
- [Konfigurieren](#)
- [Netzwerkdiagramm](#)
- [Konfigurieren einer gerouteten Schnittstelle und einer Subschnittstelle](#)
- [Schritt 1: Konfigurieren der logischen Schnittstelle](#)
- [Schritt 2: Konfigurieren der physischen Schnittstelle](#)
- [FTD Routed Interface-Betrieb](#)
- [FTD Routed Interface - Übersicht](#)
- [Überprüfung](#)
- [Verfolgen eines Pakets auf einer FTD-gerouteten Schnittstelle](#)
- [Zugehörige Informationen](#)

Einleitung

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

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine spezifischen Anforderungen.

Verwendete Komponenten

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

- ASA5512-X - FTD-Code 6.1.0.x
- FirePOWER Management Center (FMC) - Code 6.1.0.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 möglichen Auswirkungen aller Befehle kennen.

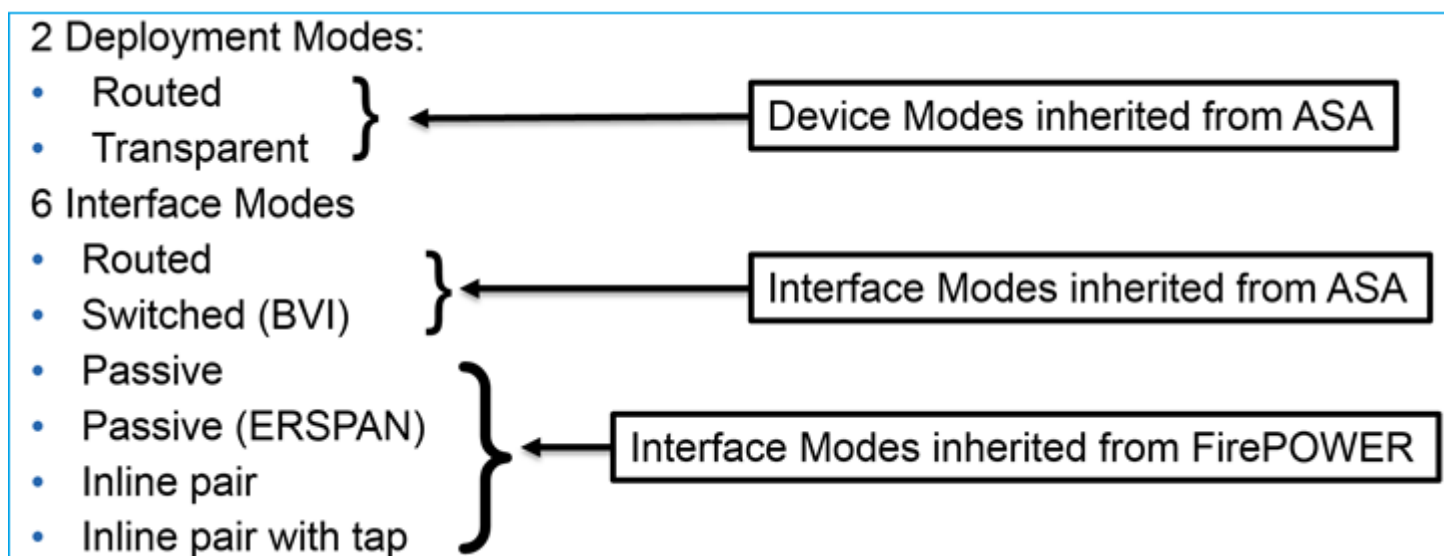
Verwandte Produkte

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

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR 2100, FPR 4100, FPR 9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- FTD-Softwarecode 6.2.x und höher

Hintergrundinformationen

Die Firepower Threat Defense (FTD) bietet zwei Bereitstellungsmodi und sechs Schnittstellenmodi, wie in diesem Bild gezeigt:



Hinweis: Sie können die Schnittstellenmodi auf einer FTD-Einheit kombinieren.

Überblick über die verschiedenen FTD-Bereitstellungs- und Schnittstellenmodi:

FTD-Schnittstelle Modus	FTD-Bereitstellungsmodus	Beschreibung	Datenverkehr kann verworfen werden
Geroutet	Geroutet	Vollständige LINA-Engine- und Snort-Engine-Prüfungen	Ja
Geschaltet	Transparent	Vollständige LINA-Engine- und Snort-Engine-Prüfungen	Ja

Inline-Paar	Geroutet oder transparent	Partielle LINA-Engine- und vollständige Snort-Engine-Prüfungen	Ja
Inline-Paar mit Tap	Geroutet oder transparent	Partielle LINA-Engine- und vollständige Snort-Engine-Prüfungen	Nein
Passive	Geroutet oder transparent	Partielle LINA-Engine- und vollständige Snort-Engine-Prüfungen	Nein
Passiv (ERSPAN)	Geroutet	Partielle LINA-Engine- und vollständige Snort-Engine-Prüfungen	Nein

Konfigurieren

Netzwerkdiagramm



Konfigurieren einer gerouteten Schnittstelle und einer Subschnittstelle

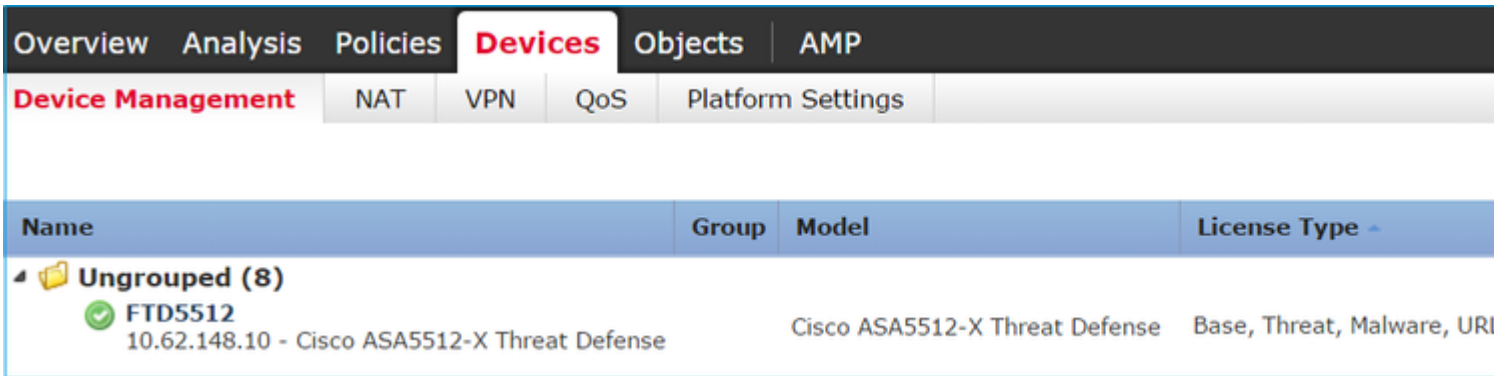
Konfigurieren Sie die Subschnittstelle G0/0.201 und die Schnittstelle G0/1 wie folgt:

Schnittstelle	G0/0,201	G0/1
Name	INNEN	AUSSEN
Sicherheitszone	INNENBEREICH	EXTERNE_ZONE
Beschreibung	INTERN	EXTERN
Subschnittstellen-ID	201	-
VLAN-ID	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
Duplex/Geschwindigkeit	Auto (automatisch)	Auto (automatisch)

Lösung

Schritt 1: Konfigurieren der logischen Schnittstelle

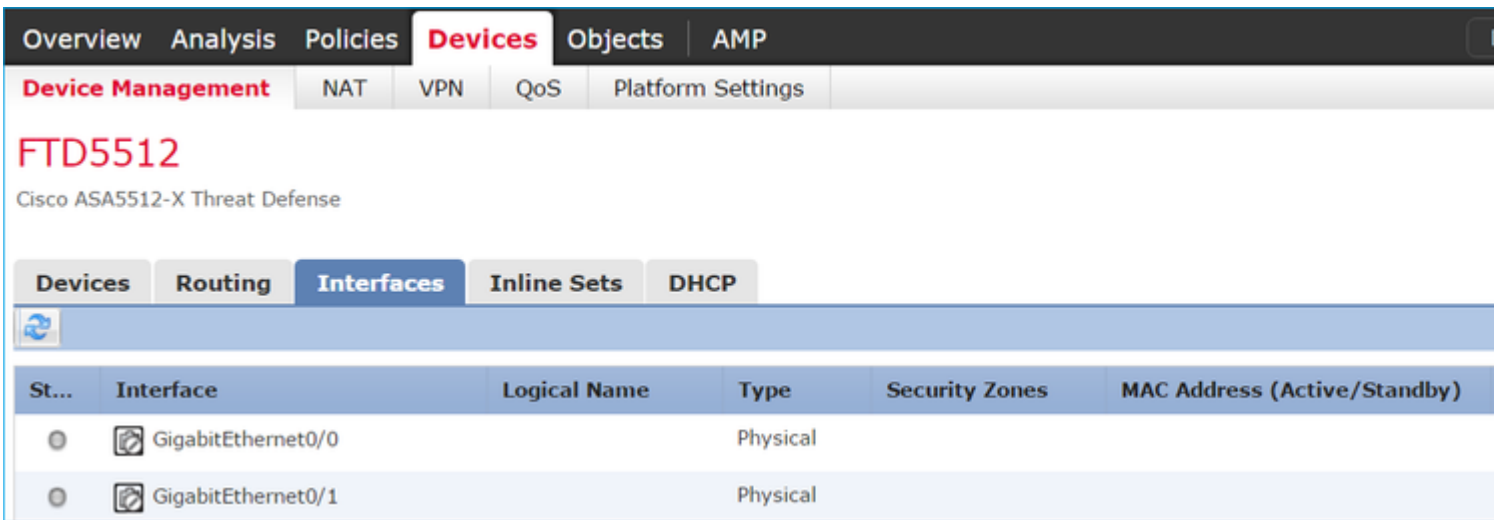
Navigieren Sie zu **Devices (Geräte) > Device Management (Geräteverwaltung)**, wählen Sie das entsprechende Gerät aus, und wählen Sie das Symbol **Edit (Bearbeiten)** aus:



The screenshot shows the Cisco FMC interface with the 'Devices' tab selected. Under 'Device Management', there are sub-tabs for NAT, VPN, QoS, and Platform Settings. A table lists devices under the 'Ungrouped (8)' category. The device 'FTD5512' is highlighted, with details: IP 10.62.148.10, Model Cisco ASA5512-X Threat Defense, and License Type Base, Threat, Malware, URL.

Name	Group	Model	License Type
Ungrouped (8)			
FTD5512 10.62.148.10 - Cisco ASA5512-X Threat Defense		Cisco ASA5512-X Threat Defense	Base, Threat, Malware, URL

Wählen Sie **Schnittstellen hinzufügen > Subchnittstelle** aus:



The screenshot shows the configuration page for device 'FTD5512'. The 'Interfaces' tab is selected, showing a table of interfaces. Two physical interfaces are listed: GigabitEthernet0/0 and GigabitEthernet0/1.

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)
	GigabitEthernet0/0		Physical		
	GigabitEthernet0/1		Physical		

Konfigurieren Sie die Subschnittstelleneinstellungen wie folgt:

Add Sub Interface

Name: Enabled Management Only
Security Zone:
Description:

General

IPv4

IPv6

Advanced

MTU: (64 - 9198)
Interface *: Enabled
Sub-Interface ID *: (1 - 4294967295)
VLAN ID: (1 - 4094)

Schnittstellen-IP-Einstellungen:

Add Sub Interface

Name: Enabled Management Only
Security Zone:
Description:

General

IPv4

IPv6

Advanced

IP Type:
IP Address: eg. 1.1.1.1/255.255.255.228

Geben Sie unter der physischen Schnittstelle (GigabitEthernet0/0) die Duplex- und Geschwindigkeitseinstellungen an:

General

IPv4

IPv6

Advanced

Hardware Configuration

Duplex:
Speed:

Aktivieren Sie die physische Schnittstelle (in diesem Fall G0/0):

Edit Physical Interface

Mode: ▼

Name: Enabled Management Only

Security Zone: ▼

Description:

General IPv4 IPv6 Advanced Hardware Configuration

MTU: (64 - 9198)

Interface ID:

Schritt 2: Konfigurieren der physischen Schnittstelle

Bearbeiten Sie die physische GigabitEthernet0/1-Schnittstelle gemäß den Anforderungen:

Edit Physical Interface

Mode: ▼

Name: Enabled Management Only

Security Zone: ▼

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▼

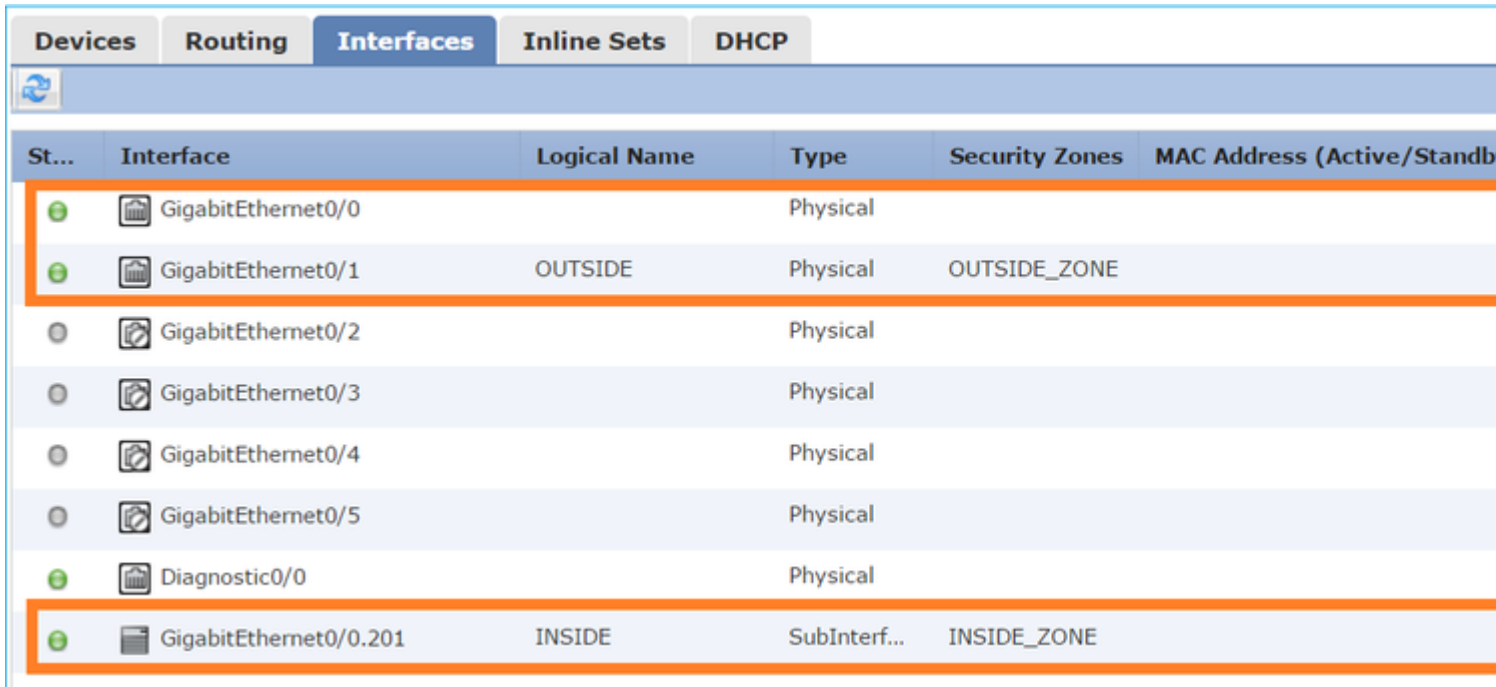
IP Address: eg. 1.1.1.1/255.255.255.228

- Für geroutete Schnittstellen lautet der Modus: **Keine**
- Der Name entspricht dem ASA-Schnittstellennamen **if**
- Bei FTD haben alle Schnittstellen die Sicherheitsstufe = 0.
- **Der gleiche Sicherheitsdatenverkehr** gilt nicht für FTD. Datenverkehr zwischen FTD-Schnittstellen (inter) und (intra) ist standardmäßig zulässig

Wählen Sie **Speichern** und **Bereitstellen**.

Verifizierung

Über die grafische Benutzeroberfläche des FMC:



St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standb
+	GigabitEthernet0/0		Physical		
+	GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE_ZONE	
○	GigabitEthernet0/2		Physical		
○	GigabitEthernet0/3		Physical		
○	GigabitEthernet0/4		Physical		
○	GigabitEthernet0/5		Physical		
+	Diagnostic0/0		Physical		
+	GigabitEthernet0/0.201	INSIDE	SubInterf...	INSIDE_ZONE	

Aus der FTD-CLI:

```
<#root>
```

```
>
```

```
show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/0.201	192.168.201.1	YES	manual	up	up
GigabitEthernet0/1	192.168.202.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down
GigabitEthernet0/4	unassigned	YES	unset	administratively down	down
GigabitEthernet0/5	unassigned	YES	unset	administratively down	down
Internal-Control0/0	127.0.1.1	YES	unset	up	up
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
Management0/0	unassigned	YES	unset	up	up

```
<#root>
```

>

show ip

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

FMC-GUI- und FTD-CLI-Korrelation:

Edit Sub Interface

Name: Enabled Management Only

Security Zone: ▾

Description:

General **IPv4** IPv6 Advanced

IP Type: ▾

IP Address: eg. 1.1.1.1/255.255.255.0

> show running-config
!
interface GigabitEthernet0/0.201
description INTERNAL
vlan 201
nameif INSIDE
cts manual
propagate sgt
policy static sgt
security-level 0
ip address 192.168.201.1/24

<#root>

>

show interface g0/0.201

Interface GigabitEthernet0/0.201

"

INSIDE

",

is up, line protocol is up

Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

VLAN identifier 201

Description: INTERNAL

MAC address a89d.21ce.fdea, MTU 1500

IP address 192.168.201.1, subnet mask 255.255.255.0

```
Traffic Statistics for "INSIDE":
  1 packets input, 28 bytes
  1 packets output, 28 bytes
  0 packets dropped
```

>

show interface g0/1

Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up

Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)

Input flow control is unsupported, output flow control is off

Description: EXTERNAL

MAC address a89d.21ce.fde7, MTU 1500

IP address 192.168.202.1, subnet mask 255.255.255.0

```
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  1 packets output, 64 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 12 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (511/511)
  output queue (blocks free curr/low): hardware (511/511)
```

Traffic Statistics for "OUTSIDE":

```
  0 packets input, 0 bytes
  0 packets output, 0 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, 0 bytes/sec
  5 minute output rate 0 pkts/sec, 0 bytes/sec
  5 minute drop rate, 0 pkts/sec
```

>

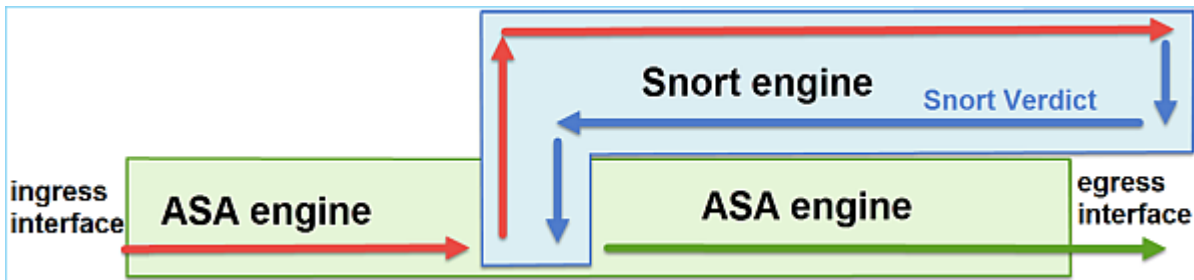
FTD Routed Interface-Betrieb

Überprüfen des FTD-Paketflusses bei Verwendung von gerouteten Schnittstellen

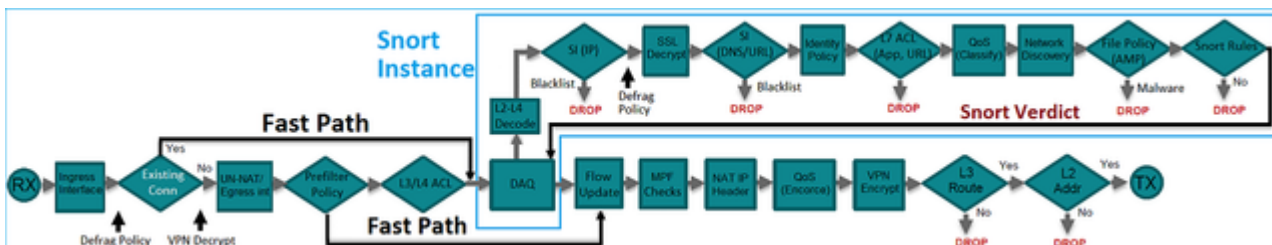
Lösung

FTD - Architekturübersicht

Überblick über die FTD-Datenebene:



Dieses Bild zeigt einige der Überprüfungen, die innerhalb der einzelnen Motoren stattfinden:



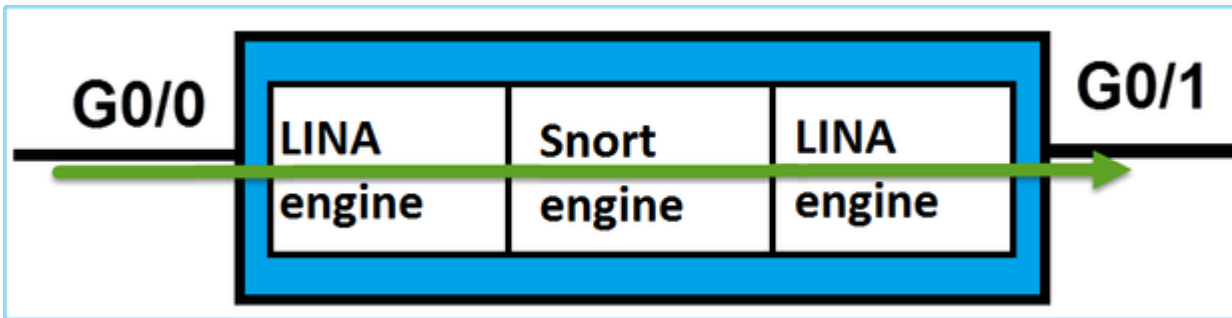
Wichtigste Punkte

- Die untersten Prüfungen entsprechen der FTD LINA-Engine Data Path
- Die Prüfungen im blauen Feld entsprechen der FTD Snort Engine-Instanz.

FTD Routed Interface - Übersicht

- Nur bei **gerouteter** Bereitstellung verfügbar
- Herkömmliche **L3-Firewall-Bereitstellung**
- Eine oder mehrere physische oder logische (VLAN) routbare Schnittstellen
- Konfiguration von Funktionen wie NAT oder dynamischen Routing-Protokollen
- Pakete werden basierend auf der **Routensuche** weitergeleitet und der nächste Hop wird basierend auf der **ARP-Suche** aufgelöst.
- Tatsächlicher Datenverkehr **kann fallen gelassen werden**
- **Vollständige LINA-Engine-Prüfungen** werden zusammen mit **vollständigen Snort-Engine-Prüfungen** angewendet

Der letzte Punkt lässt sich wie folgt darstellen:



Überprüfung

Verfolgen eines Pakets auf einer FTD-gerouteten Schnittstelle

Netzwerkdiagramm



Verwenden Sie den Packet-Tracer mit den folgenden Parametern, um die angewendeten Richtlinien anzuzeigen:

Eingangsschnittstelle	INNEN
Protokoll/Service	TCP-Port 80
Quell-IP	192.168.201.100
Ziel-IP	192.168.202.100

Lösung

Bei Verwendung einer gerouteten Schnittstelle wird das Paket ähnlich wie eine klassische ASA-geroutete Schnittstelle verarbeitet. Prüfungen wie Routensuche, MPF (Modular Policy Framework), NAT, ARP-Suche usw. erfolgen im Datenpfad der LINA-Engine. Wenn die Zugriffskontrollrichtlinie dies erfordert, wird das

Paket außerdem von der Snort-Engine (einer der Snort-Instanzen) überprüft, wo ein Verdict generiert und an die LINA-Engine zurückgegeben wird:

<#root>

>

packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80

Phase: 1

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 192.168.202.100 using egress ifc OUTSIDE

Phase: 2

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 268437505

access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 - Default/1

access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 11336, packet dispatched to next module

Result:

input-interface: INSIDE

input-status: up
input-line-status: up

output-interface: OUTSIDE

output-status: up
output-line-status: up
Action: allow

>

Hinweis: In Phase 4 wird das Paket mit einer TCP-Zuordnung namens UM_STATIC_TCP_MAP abgeglichen. Dies ist die Standard-TCP-Zuordnung auf FTD.

<#root>

firepower#

show run all tcp-map

```
!  
tcp-map UM_STATIC_TCP_MAP  
  no check-retransmission  
  no checksum-verification  
  exceed-mss allow  
  queue-limit 0 timeout 4  
  reserved-bits allow  
  syn-data allow  
  synack-data drop  
  invalid-ack drop  
  seq-past-window drop  
  tcp-options range 6 7 allow  
  tcp-options range 9 18 allow  
  tcp-options range 20 255 allow  
  tcp-options selective-ack allow  
  tcp-options timestamp allow  
  tcp-options window-scale allow  
  tcp-options mss allow  
  tcp-options md5 clear  
  ttl-evasion-protection  
  urgent-flag allow  
  window-variation allow-connection  
!
```

>

Zugehörige Informationen

- [Cisco Firepower Threat Defense - Konfigurationsleitfaden für Firepower Device Manager, Version](#)

6.1

- [Installation und Upgrade von Firepower Threat Defense auf ASA 55xx-X-Geräten](#)
- [Cisco Secure Firewall - Schutz vor Bedrohungen](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.