

# Configureer in Routed Mode interfaces voor firepower Threat Defence

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configureer een Routed Interface en een Subinterface](#)

[Stap 1. De logische interface configureren](#)

[Stap 2. De fysieke interface configureren](#)

[FTD Routed Interface-handeling](#)

[FTD Routed Interface - Overzicht](#)

[Verifiëren](#)

[Packet overtrekken op FTD Routed Interface](#)

[Gerelateerde informatie](#)

## Inleiding

In dit document worden de configuratie, verificatie en werking van een inline paarinterface op een FTD-apparaat (Firepower Threat Defence) beschreven.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten voor dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA 5512-X - FTD-code 6.1.0.x
- Firepower Management Center (FMC) - code 6.1.0.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

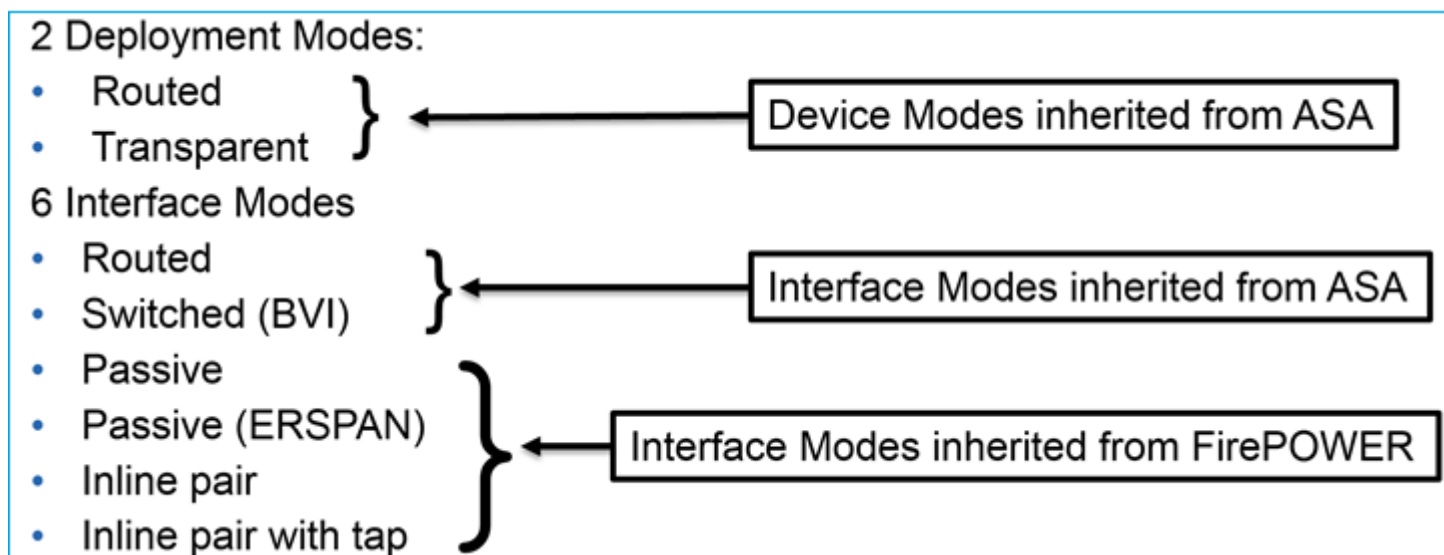
### Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR210, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- FTD-softwarecode 6.2.x en hoger

## Achtergrondinformatie

De Firepower Threat Defence (FTD) biedt twee implementatiemodi en zes interfacemodi zoals in deze afbeelding:



**Opmerking:** u kunt interfacemodi op één FTD-apparaat combineren.

Overzicht op hoog niveau van de verschillende FTD-implementaties en interfacemodi:

FTD-interface wijze	FTD-implementatiemodus	Beschrijving	Verkeer kan worden gedropt
Verstuurd	Verstuurd	Volledige LINA-motor en snelmotorcontroles	Ja
Switched	Doorzichtig	Volledige LINA-motor en snelmotorcontroles	Ja
Inline paar	Routed of Transparent	Gedeeltelijke LINA-motor en volledige snormotorcontroles	Ja

Inline paar met tap	Routed of Transparent	Gedeeltelijke LINA-motor en volledige snortmotorcontroles	Nee
passief	Routed of Transparent	Gedeeltelijke LINA-motor en volledige snortmotorcontroles	Nee
Passief (ERSPAN)	Verstuurd	Gedeeltelijke LINA-motor en volledige snortmotorcontroles	Nee

## Configureren

### Netwerkdigram



### Configureer een Routed Interface en een Subinterface

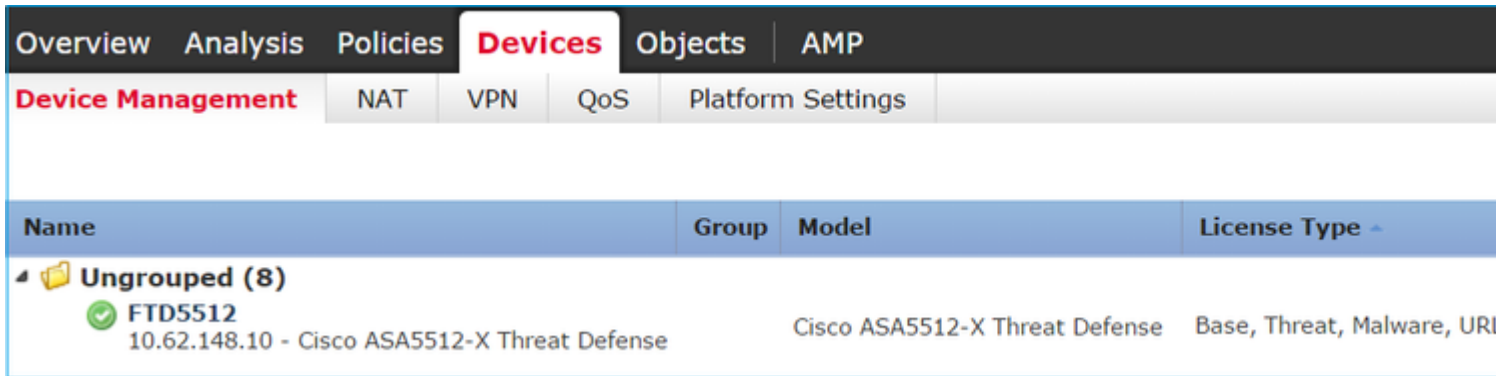
Configureer subinterface G0/0.201 en interface G0/1 volgens deze vereisten:

<b>Interface</b>	G0/0,201	G0/1
<b>Name</b>	BINNENKANT	BUITEN
<b>Security zone</b>	BINNEN_ZONE	BUITEN_ZONE
<b>Beschrijving</b>	INTERN	EXTERN
<b>Subinterface-ID</b>	201	-
<b>VLAN-id</b>	201	-
<b>IPv4</b>	192.168.201.1/24	192.168.202.1/24
<b>Duplex/Snelheid</b>	Auto	Auto

### Oplossing

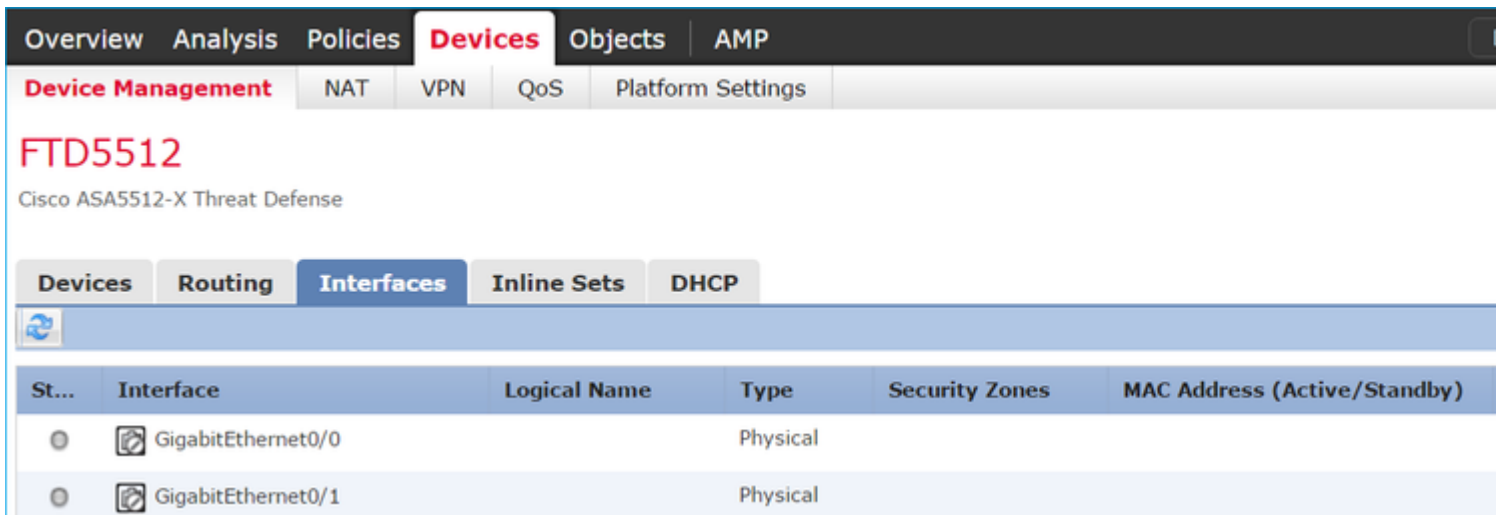
## Stap 1. De logische interface configureren

Navigeer naar **Apparaten > Apparaatbeheer**, selecteer het juiste apparaat en selecteer het pictogram **Bewerken**:



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, UR

Selecteer **Interfaces toevoegen > Subinterface**:



St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)
<input type="radio"/>	GigabitEthernet0/0		Physical		
<input type="radio"/>	GigabitEthernet0/1		Physical		

Configureer de subinterface-instellingen volgens de vereisten:

### 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)

IP-instellingen voor interfaces:

### 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

Specificeer onder de fysieke interface (Gigabit Ethernet0/0) de instellingen Duplex en Snelheid:

General IPv4 IPv6 Advanced **Hardware Configuration**

Duplex:  ▼

Speed:  ▼

Schakel de fysieke interface in (G0/0 in dit geval):

### Edit Physical Interface

Mode:  ▼

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

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

MTU:  (64 - 9198)

Interface ID:

## Stap 2. De fysieke interface configureren

Bewerk de Gigabit Ethernet0/1 fysieke interface volgens de vereisten:

### Edit Physical Interface

Mode:  ▼

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

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

IP Type:  ▼

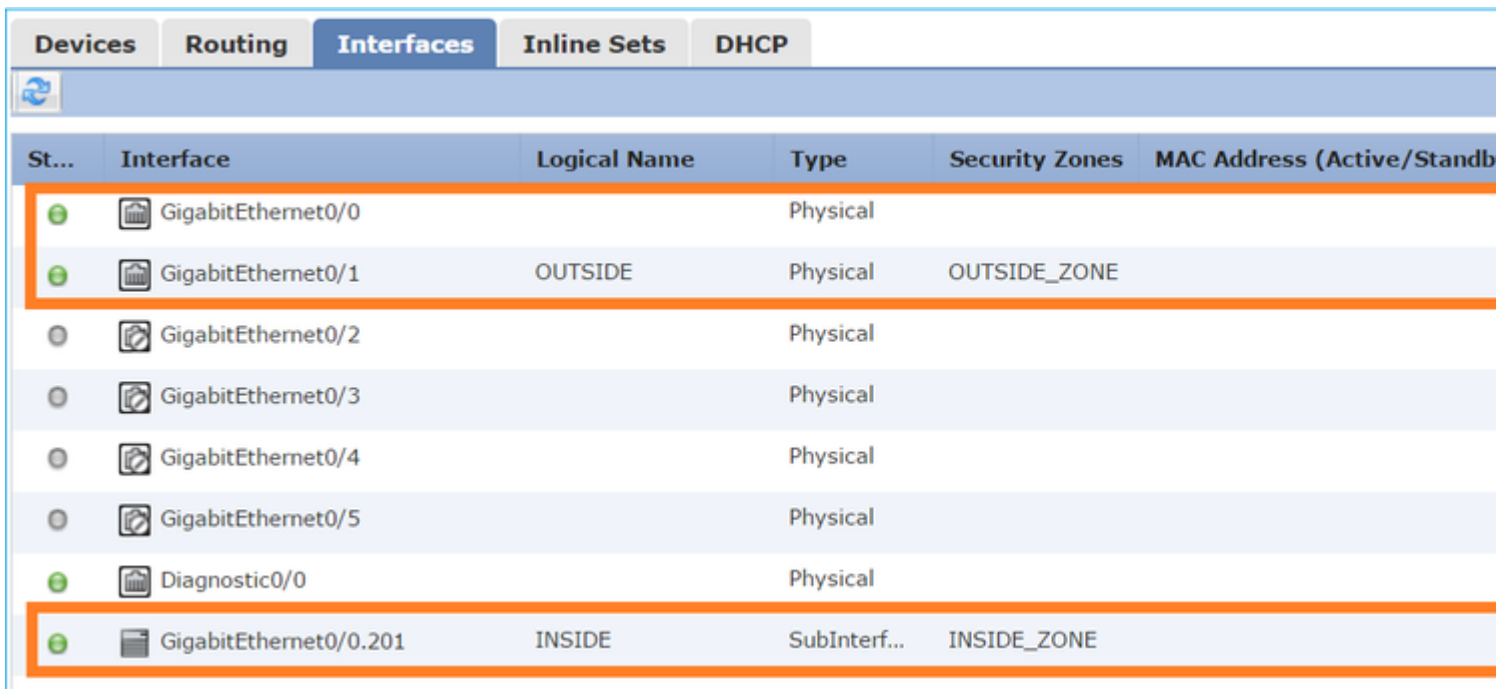
IP Address:  eg. 1.1.1.1/255.255.255.228

- Voor Routed interface is de Modus: **Geen**
- De naam is gelijk aan de **naam** van de ASA-interface
- Op FTD hebben alle interfaces veiligheidsniveau = 0
- **Hetzelfde veiligheidsverkeer** is niet van toepassing op FTD. Verkeer tussen FTD-interfaces (inter) en (intra) is standaard toegestaan

Selecteer **Opslaan** en **implementeren**.

## Verificatie

Van de VCC GUI:



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	

Van de 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

Correlatie tussen FMC GUI en FTD CLI:

```
<#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
>
```

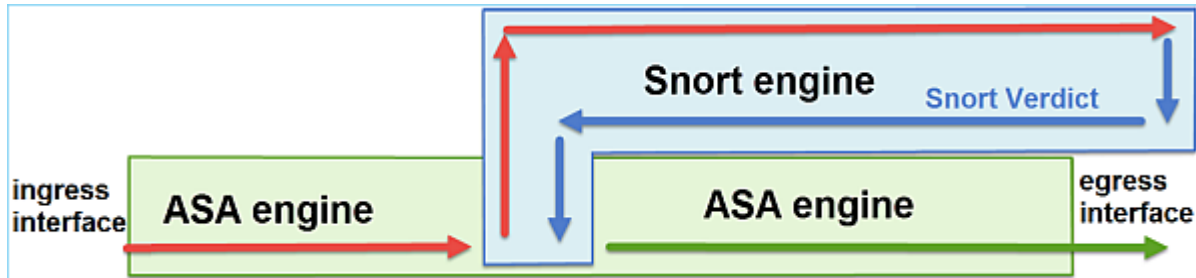
## FTD Routed Interface-handeling

Controleer de FTD-pakketstroom wanneer Routed interfaces in gebruik zijn.

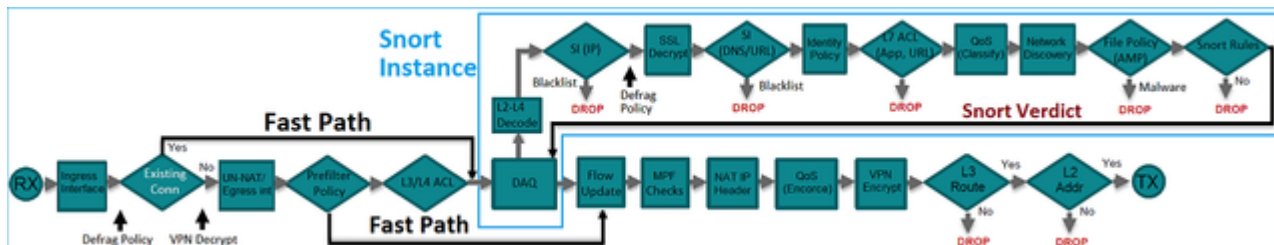
## Oplossing

### FTD Architecturaal overzicht

Een overzicht op hoog niveau van het FTD-gegevensvlak:



Dit beeld toont enkele controles die binnen elke motor plaatsvinden:



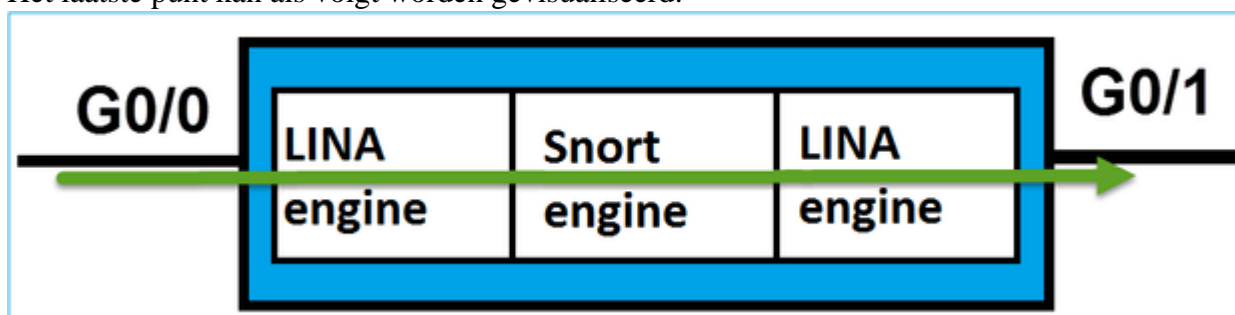
### Belangrijkste punten

- De controles aan de onderkant komen overeen met de FTD LINA engine Data Path
- De controles in het blauwe vak komen overeen met de FTD Snort engine instantie

### FTD Routed Interface - Overzicht

- Alleen beschikbaar in **Routed** Implementation
- Traditionele **L3 firewall-implementation**
- Een of meer fysieke of logische (VLAN) routeerbare interfaces
- Maakt het mogelijk functies zoals NAT of Dynamic Routing protocollen te configureren
- De pakketten worden door:sturen gebaseerd op **Route Lookup** en de volgende hop wordt opgelost gebaseerd op **ARP Lookup**
- Feitelijk verkeer **kan worden gedropt**
- **Volledige LINA motorcontroles** worden uitgevoerd samen met **volledige Snort-motorcontroles**.

Het laatste punt kan als volgt worden gevisualiseerd:



# Verifiëren

## Packet overtrekken op FTD Routed Interface

### Netwerkdigram



Gebruik packet-tracer met de volgende parameters om het toegepaste beleid te zien:

<b>Invoerinterface</b>	BINNENKANT
<b>Protocol/service</b>	TCP-poort 80
<b>Bron-IP</b>	192.168.201.100
<b>Bestemmings-IP</b>	192.168.202.100

### Oplossing

Wanneer een Routed interface wordt gebruikt, wordt het pakket op dezelfde manier verwerkt als een klassieke ASA Routed interface. Controles zoals Route Lookup, Modular Policy Framework (MPF), NAT, ARP lookup etc vinden plaats in de LINA engine Data Path. Bovendien, als het Toegangsbeheerbeleid dit vereist, wordt het pakket geïnspecteerd door de Snort-engine (een van de Snort-instanties) waar een vonnis wordt gegenereerd en teruggestuurd naar de LINA-engine:

```
<#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

>

---

**Opmerking:** in fase 4 wordt het pakket gecontroleerd op een TCP-kaart met de naam UM\_STATIC\_TCP\_MAP. Dit is de standaard TCP Map op 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
```

!

>

## Gerelateerde informatie

- [Cisco Firepower Threat Defence Configuration Guide voor Firepower Device Manager, versie 6.1](#)
- [Firepower Threat Defense installeren en upgraden op ASA 550x-X apparaten](#)
- [Cisco Secure Firewall-bescherming tegen bedreigingen](#)
- [Cisco technische ondersteuning en downloads](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.