

Probleemoplossing voor routing van firepower Threat Defence

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[FTD-mechanismen voor pakketdoorsturen](#)
[Kernpunt](#)
[Data-plane \(LINA\) routinggedrag](#)
[Belangrijkste punten](#)
[FTD Regeling van werkzaamheden](#)
[Configureren](#)
[Case 1 - Forwarding gebaseerd op Connection Lookup](#)
[Zwevende time-out](#)
[Time-out voor conn-holddown](#)
[Case 2 - Forwarding gebaseerd op NAT Lookup](#)
[Case 3 - Forwarding op basis van beleidsgebaseerde routing \(PBR\)](#)
[Case 4 - Forwarding op basis van Global Routing Lookup](#)
[Null0-interface](#)
[Equal Cost Multi-Path \(ECMP\)](#)
[FTD-beheerplan](#)
[FTD LINA diagnostische interfacerouting](#)

Inleiding

Dit document beschrijft hoe Firepower Threat Defence (FTD) pakketten doorstuurt en verschillende routingconcepten implementeert.

Voorwaarden

Vereisten

- Basiskennis over routing

Gebruikte componenten

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

- Cisco Firepower 41x Threat Defense versie 7.1.x
- Firepower Management Center (FMC) versie 7.1.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

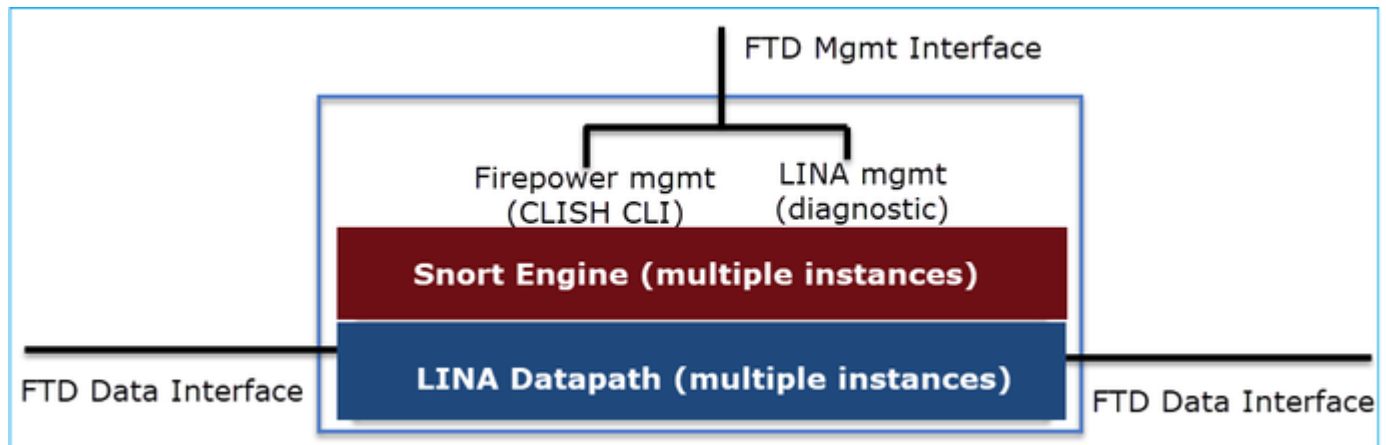
uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

FTD-mechanismen voor pakketdoorsturen

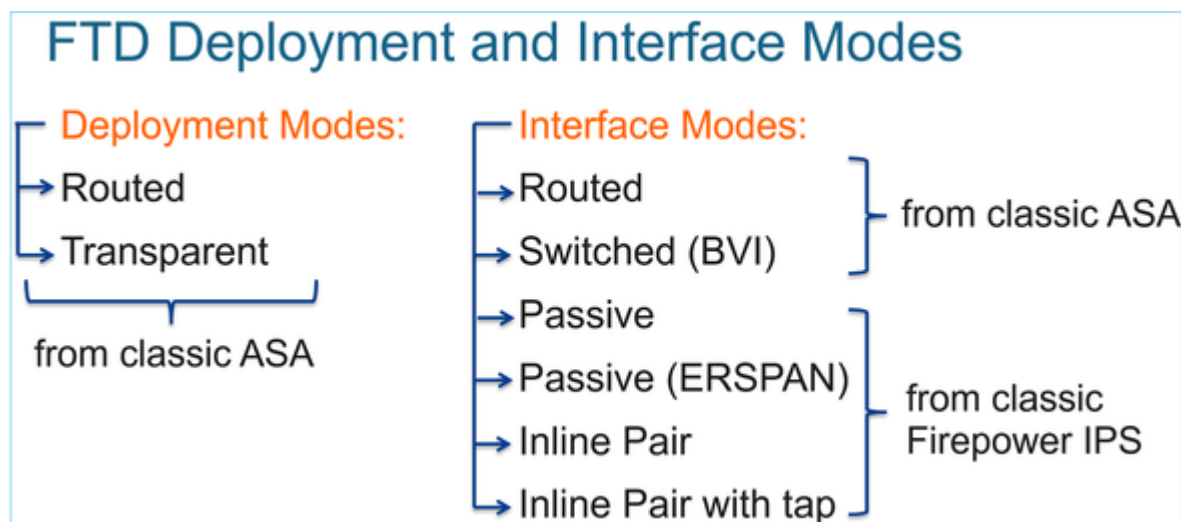
FTD is een unified software-image die bestaat uit twee hoofd-engines:

- Datapath-motor (LINA)
- Snort-engine



De Datapath en de Snort Engine zijn de belangrijkste onderdelen van het FTD dataplane.

Het FTD Data Plane Forwarding mechanisme is afhankelijk van de interfacemodus. Het volgende beeld vat de verschillende interfacemodi samen samen met de FTD plaatsingswijzen:



De tabel vat samen hoe de FTD forwards pakketten in het gegevensvlak op basis van de interfacemodus. De verzendingsmechanismen worden vermeld in volgorde van voorkeur:

FTD Deployment mode	FTD Interface mode	Forwarding Mechanism
Routed	Routed	Packet forwarding based on the following order: 1. Connection lookup 2. Nat lookup (xlate) 3. Policy Based Routing (PBR) 4. Global routing table lookup
Routed or Transparent	Switched (BVI)	1. NAT lookup 2. Destination MAC Address L2 Lookup*
Routed or Transparent	Inline Pair	The packet will be forwarded based on the pair configuration.
Routed or Transparent	Inline Pair with Tap	The original packet will be forwarded based on the pair configuration. The copy of the packet will be dropped internally
Routed or Transparent	Passive	The packet is dropped internally
Routed	Passive (ERSPAN)	The packet is dropped internally

* Een FTD in Transparent modus doet in bepaalde situaties een Route Lookup:

MAC Address vs. Route Lookups

For traffic within a bridge group, the outgoing interface of a packet is determined by performing a destination MAC address lookup instead of a route lookup.

Route lookups, however, are necessary for the following situations:

- Traffic originating on the Firepower Threat Defense device—Add a default/static route on the Firepower Threat Defense device for traffic destined for a remote network where a syslog server, for example, is located.
- Voice over IP (VoIP) and TFTP traffic, and the endpoint is at least one hop away—Add a static route on the Firepower Threat Defense device for traffic destined for the remote endpoint so that secondary connections are successful. The Firepower Threat Defense device creates a temporary "pinhole" in the access control policy to allow the secondary connection; and because the connection might use a different set of IP addresses than the primary connection, the Firepower Threat Defense device needs to perform a route lookup to install the pinhole on the correct interface.

Affected applications include:

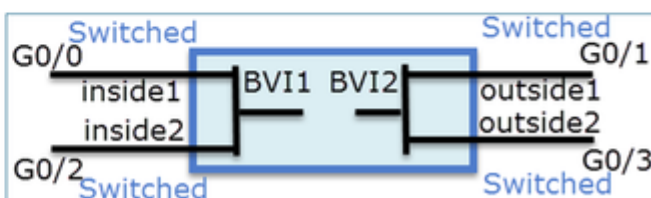
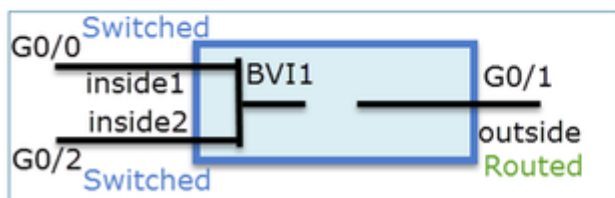
- H.323
- RTSP
- SIP
- Skinny (SCCP)
- SQL*Net
- SunRPC
- TFTP
- Traffic at least one hop away for which the Firepower Threat Defense device performs NAT—Configure a static route on the Firepower Threat Defense device for traffic destined for the remote network. You also need a static route on the upstream router for traffic destined for the mapped addresses to be sent to the Firepower Threat Defense device.

Raadpleeg de [VCC-handleiding](#) voor meer informatie.

Vanaf de 6.2.x-versie ondersteunt de FTD geïntegreerde routing en bridging (IRB):

FTD Integrated Routing and Bridging (IRB)

- Available as from 6.2.x
- Allows an FTD in **Routed mode** to have multiple interfaces (up to 64) to be part of the **same VLAN** and perform L2 switching between them
- BVI-to-Routed or BVI-to-BVI Routing is allowed



BVI-verificatieopdrachten:

Verification commands

```
firepower# show bridge-group
```

```
firepower# show ip
```

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	VLAN1576_G0-0	203.0.113.1	255.255.255.0	manual
GigabitEthernet0/1	VLAN1577_G0-1	192.168.1.15	255.255.255.0	manual
GigabitEthernet0/2	VLAN1576_G0-2	203.0.113.1	255.255.255.0	manual
GigabitEthernet0/4.100	SUB1	203.0.113.1	255.255.255.0	manual
BVI1	LAN	203.0.113.1	255.255.255.0	manual
BVI2	LAN2	192.168.1.15	255.255.255.0	manual

- BVI nameif is used in L3 Routing configuration

```
firepower# show run route
```

```
route LAN 1.1.1.0 255.255.255.0 203.0.113.5 1
```

- BVI member nameif is used in policies like NAT configuration

```
firepower# show run nat
```

```
nat (VLAN1576_G0-0,VLAN1577_G0-1) source dynamic any interface  
nat (VLAN1576_G0-2,VLAN1577_G0-1) source dynamic any interface
```

Kernpunt

Voor Routed Interfaces of BVI's (IRB) is het pakketdoorsturen gebaseerd op deze volgorde:

- Opzoeken verbinding
- NAT-lookup (bestemming-NAT, ook bekend als UN-NAT)
- Op beleid gebaseerde routing (PBR)
- Wereldwijde raadpleging van routingstabel

En bron-NAT dan?

De bron-NAT wordt gecontroleerd na de wereldwijde raadpleging voor routing.

De rest van dit document concentreert zich op de Routed interface-modus.

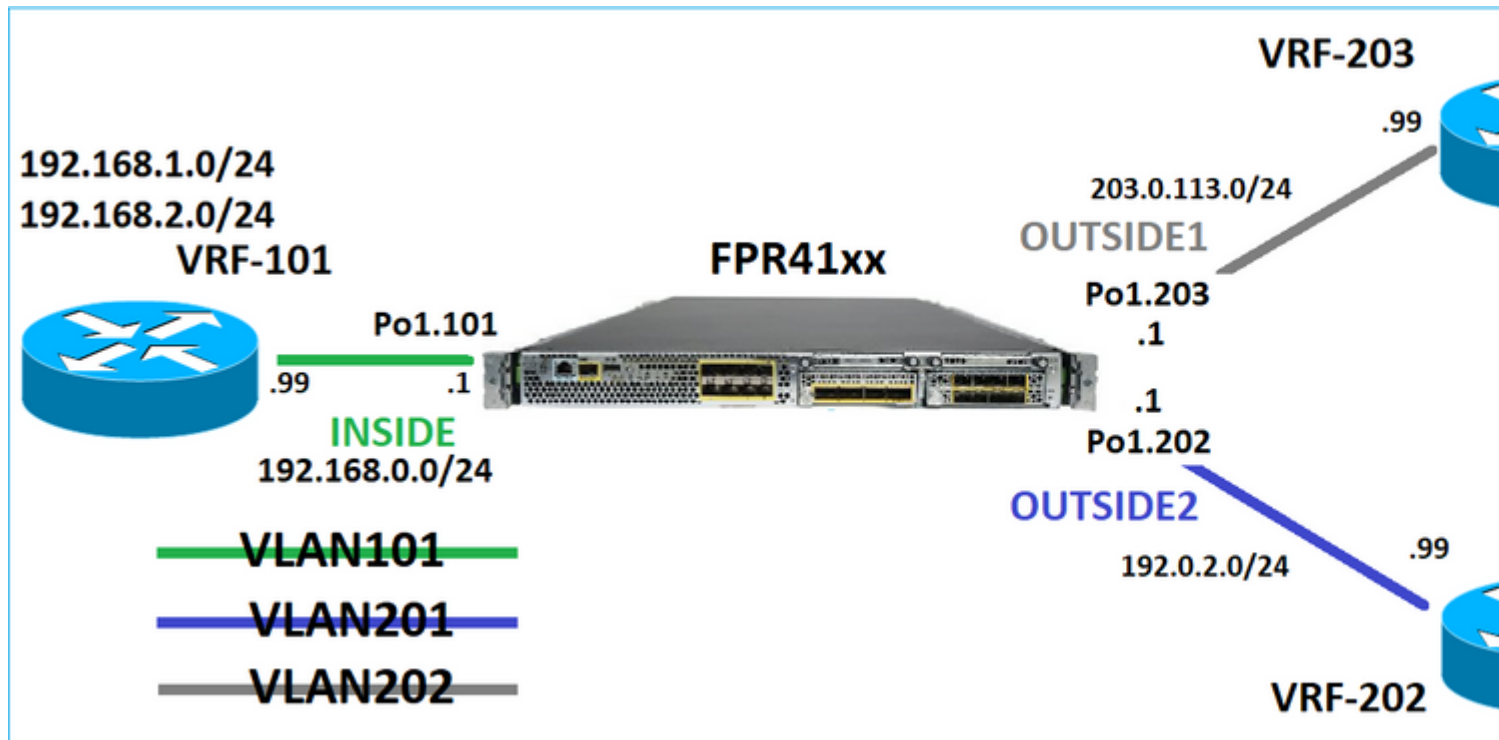
Data-plane (LINA) routinggedrag

In routed interface mode FTD LINA voorwaarts de pakketten in 2 fasen:

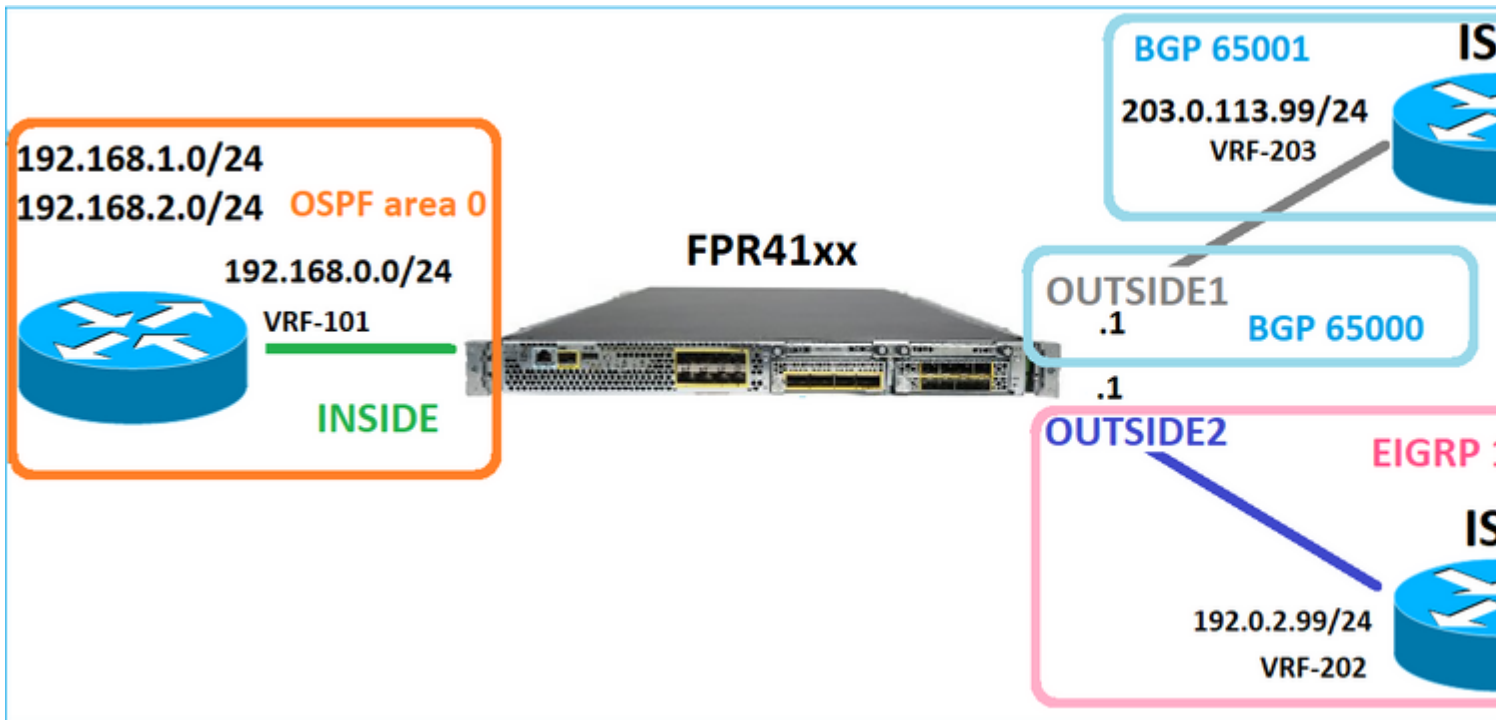
Fase 1 - bepaling van uitgaande interface

Fase 2 - selectie van volgende hop

Bekijk de volgende topologie:



En dit routeontwerp:



De FTD-routerconfiguratie:

```
firepower# show run router
router ospf 1
network 192.168.0.0 255.255.255.0 area 0
log-adj-changes
!
router bgp 65000
bgp log-neighbor-changes
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 203.0.113.99 remote-as 65001
neighbor 203.0.113.99 ebgp-multihop 255
neighbor 203.0.113.99 transport path-mtu-discovery disable
neighbor 203.0.113.99 activate
no auto-summary
no synchronization
exit-address-family
!
router eigrp 1
no default-information in
no default-information out
no eigrp log-neighbor-warnings
no eigrp log-neighbor-changes
network 192.0.2.0 255.255.255.0
!
firepower# show run route
route OUTSIDE2 198.51.100.0 255.255.255.248 192.0.2.99 1
```

De FTD Routing Information Base (RIB) - besturingsplane:

```
firepower# show route | begin Gate
```

Gateway of last resort is not set

```
C 192.0.2.0 255.255.255.0 is directly connected, OUTSIDE2
L 192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
C 192.168.0.0 255.255.255.0 is directly connected, INSIDE
L 192.168.0.1 255.255.255.255 is directly connected, INSIDE
O 192.168.1.1 255.255.255.255
[110/11] via 192.168.0.99, 01:11:25, INSIDE
O 192.168.2.1 255.255.255.255
[110/11] via 192.168.0.99, 01:11:15, INSIDE
S 198.51.100.0 255.255.255.248 [1/0] via 192.0.2.99, OUTSIDE2
D 198.51.100.8 255.255.255.248
[90/130816] via 192.0.2.99, 01:08:11, OUTSIDE2
D 198.51.100.16 255.255.255.248
[90/130816] via 192.0.2.99, 01:08:04, OUTSIDE2
B 198.51.100.24 255.255.255.248 [20/0] via 203.0.113.99, 00:28:29
B 198.51.100.32 255.255.255.248 [20/0] via 203.0.113.99, 00:28:16
C 203.0.113.0 255.255.255.0 is directly connected, OUTSIDE1
L 203.0.113.1 255.255.255.255 is directly connected, OUTSIDE1
```

De corresponderende FTD Accelerated Security Path (ASP) Routing Table - Data Plane:

```
firepower# show asp table routing
route table timestamp: 91
in 169.254.1.1 255.255.255.255 identity
in 192.168.0.1 255.255.255.255 identity
in 192.0.2.1 255.255.255.255 identity
in 192.168.1.1 255.255.255.255 via 192.168.0.99, INSIDE
in 192.168.2.1 255.255.255.255 via 192.168.0.99, INSIDE
in 203.0.113.1 255.255.255.255 identity
in 169.254.1.0 255.255.255.248 nlp_int_tap
in 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
in 198.51.100.8 255.255.255.248 via 192.0.2.99, OUTSIDE2
in 198.51.100.16 255.255.255.248 via 192.0.2.99, OUTSIDE2
in 198.51.100.24 255.255.255.248 via 203.0.113.99 (unresolved, timestamp: 89)
in 198.51.100.32 255.255.255.248 via 203.0.113.99 (unresolved, timestamp: 90)
in 192.168.0.0 255.255.255.0 INSIDE
in 192.0.2.0 255.255.255.0 OUTSIDE2
in 203.0.113.0 255.255.255.0 OUTSIDE1
in ff02::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff01:3 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff00:1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fe80::200:ff:fe01:3 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fd00:0:0:1:: ffff:ffff:ffff:ffff:: nlp_int_tap
out 255.255.255.255 255.255.255.255 OUTSIDE1
out 203.0.113.1 255.255.255.255 OUTSIDE1
out 203.0.113.0 255.255.255.0 OUTSIDE1
out 224.0.0.0 240.0.0.0 OUTSIDE1
out 255.255.255.255 255.255.255.255 OUTSIDE2
out 192.0.2.1 255.255.255.255 OUTSIDE2
out 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.8 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.16 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 192.0.2.0 255.255.255.0 OUTSIDE2
out 224.0.0.0 240.0.0.0 OUTSIDE2
out 255.255.255.255 255.255.255.255 INSIDE
out 192.168.0.1 255.255.255.255 INSIDE
```

```
out 192.168.1.1 255.255.255.255 via 192.168.0.99, INSIDE
out 192.168.2.1 255.255.255.255 via 192.168.0.99, INSIDE
out 192.168.0.0 255.255.255.0 INSIDE
out 224.0.0.0 240.0.0.0 INSIDE
out 255.255.255.255 255.255.255.255 cmi_mgmt_int_tap
out 224.0.0.0 240.0.0.0 cmi_mgmt_int_tap
out 255.255.255.255 255.255.255.255 ha_ctl_nlp_int_tap
out 224.0.0.0 240.0.0.0 ha_ctl_nlp_int_tap
out 255.255.255.255 255.255.255.255 ccl_ha_nlp_int_tap
out 224.0.0.0 240.0.0.0 ccl_ha_nlp_int_tap
out 255.255.255.255 255.255.255.255 nlp_int_tap
out 169.254.1.1 255.255.255.255 nlp_int_tap
out 169.254.1.0 255.255.255.248 nlp_int_tap
out 224.0.0.0 240.0.0.0 nlp_int_tap
out fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff nlp_int_tap
out fd00:0:0:1:: ffff:ffff:ffff:ffff:: nlp_int_tap
out fe80:: ffc0:: nlp_int_tap
out ff00:: ff00:: nlp_int_tap
out 0.0.0.0 0.0.0.0 via 0.0.0.0, identity
out :: : via 0.0.0.0, identity
```

Belangrijkste punten

De FTD (op een manier die vergelijkbaar is met een adaptieve security applicatie - ASA) bepaalt eerst de exit (uitloop) interface van een pakket (daarvoor bekijkt hij de 'in'-vermeldingen van de ASP-routeringstabel). Dan voor de bepaalde interface, probeert het om de volgende-hop te vinden (voor dat, bekijkt het de "uit"ingangen van het ASPIS dat lijst verplettert). Voorbeeld:

```
firepower# show asp table routing | include in.*198.51.100.0
in 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
firepower#
firepower# show asp table routing | include out.*OUTSIDE2
out 255.255.255.255 255.255.255.255 OUTSIDE2
out 192.0.2.1 255.255.255.255 OUTSIDE2
out 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.8 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.16 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 192.0.2.0 255.255.255.0 OUTSIDE2
out 224.0.0.0 240.0.0.0 OUTSIDE2
```

Tot slot, voor de opgeloste volgende-hop controleert LINA het ARP geheim voorgeheugen een geldige nabijheid.

Het FTD packet-tracer tool bevestigt dit proces:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.1 8 0 198.51.100.1

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 7582 ns
Config:
```


Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 8474 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 5017 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433
access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: mzafeiro_empty - Default
access-list CSM_FW_ACL_ remark rule-id 268434433: 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: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 5017 ns
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: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 5017 ns
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 5017 ns
Config:
Additional Information:

Phase: 7
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Elapsed time: 57534 ns
Config:

```
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect icmp
service-policy global_policy global
Additional Information:
```

```
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Elapsed time: 3122 ns
Config:
Additional Information:
```

```
Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 29882 ns
Config:
Additional Information:
```

```
Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 446 ns
Config:
Additional Information:
```

```
Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 20962 ns
Config:
Additional Information:
New flow created with id 178, packet dispatched to next module
```

```
Phase: 12
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 20070 ns
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Elapsed time: 870592 ns
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Snort id 1, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
```

Phase: 14
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 6244 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1784 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 5 reference 1

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 1046760 ns

De FTD ARP-tabel zoals deze wordt weergegeven in het besturingsplane:

```
firepower# show arp
OUTSIDE1 203.0.113.99 4c4e.35fc.fcd8 3051
OUTSIDE2 192.0.2.99 4c4e.35fc.fcd8 5171
```

U kunt de ARP-resolutie als volgt forceren:

```
firepower# ping 192.168.0.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.99, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
firepower# show arp
INSIDE 192.168.0.99 4c4e.35fc.fcd8 45
OUTSIDE1 203.0.113.99 4c4e.35fc.fcd8 32
OUTSIDE2 192.0.2.99 4c4e.35fc.fcd8 1
```

De FTD ARP-tabel wordt weergegeven in het gegevensplane:

```

firepower# show asp table arp

Context: single_vf, Interface: OUTSIDE1
203.0.113.99 Active 4c4e.35fc.fcd8 hits 2 reference 1

Context: single_vf, Interface: OUTSIDE2
192.0.2.99 Active 4c4e.35fc.fcd8 hits 5 reference 0

Context: single_vf, Interface: INSIDE
192.168.0.99 Active 4c4e.35fc.fcd8 hits 5 reference 0

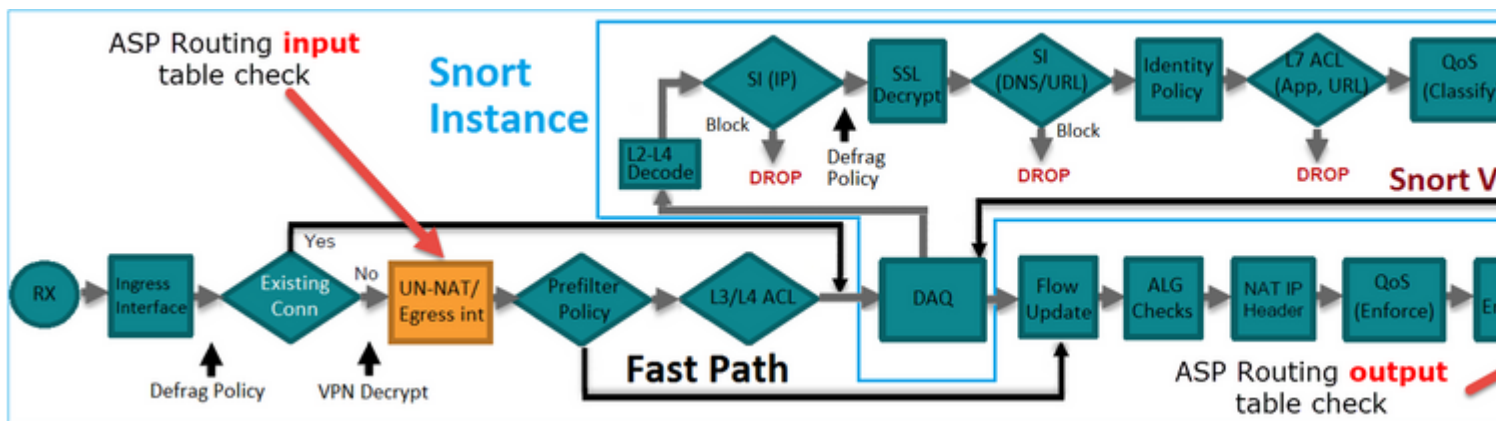
Context: single_vf, Interface: identity
:: Active 0000.0000.0000 hits 0 reference 0
0.0.0.0 Active 0000.0000.0000 hits 848 reference 0

Last clearing of hits counters: Never

```

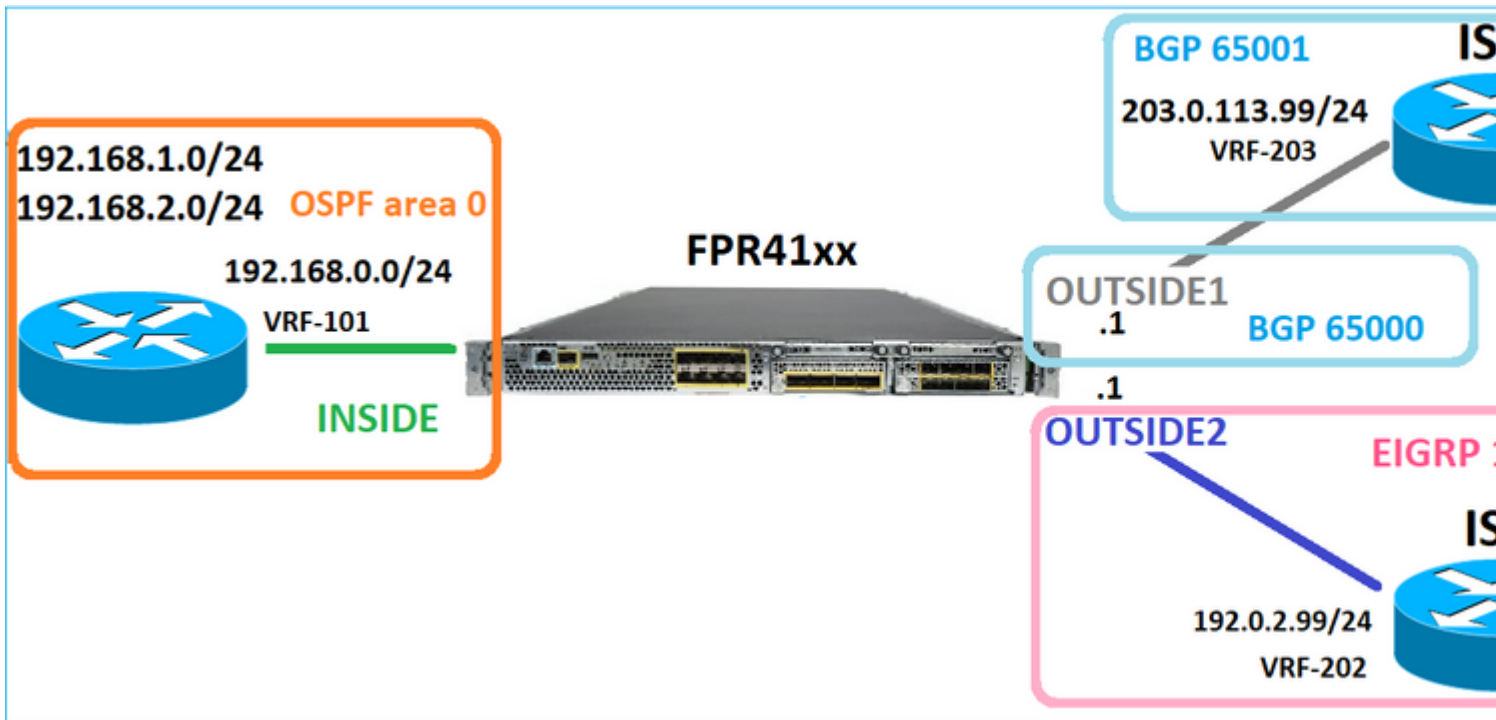
FTD Regeling van werkzaamheden

De afbeelding toont de volgorde van de bewerkingen en waar de controles voor de invoer en uitvoer van ASP-routing worden uitgevoerd:



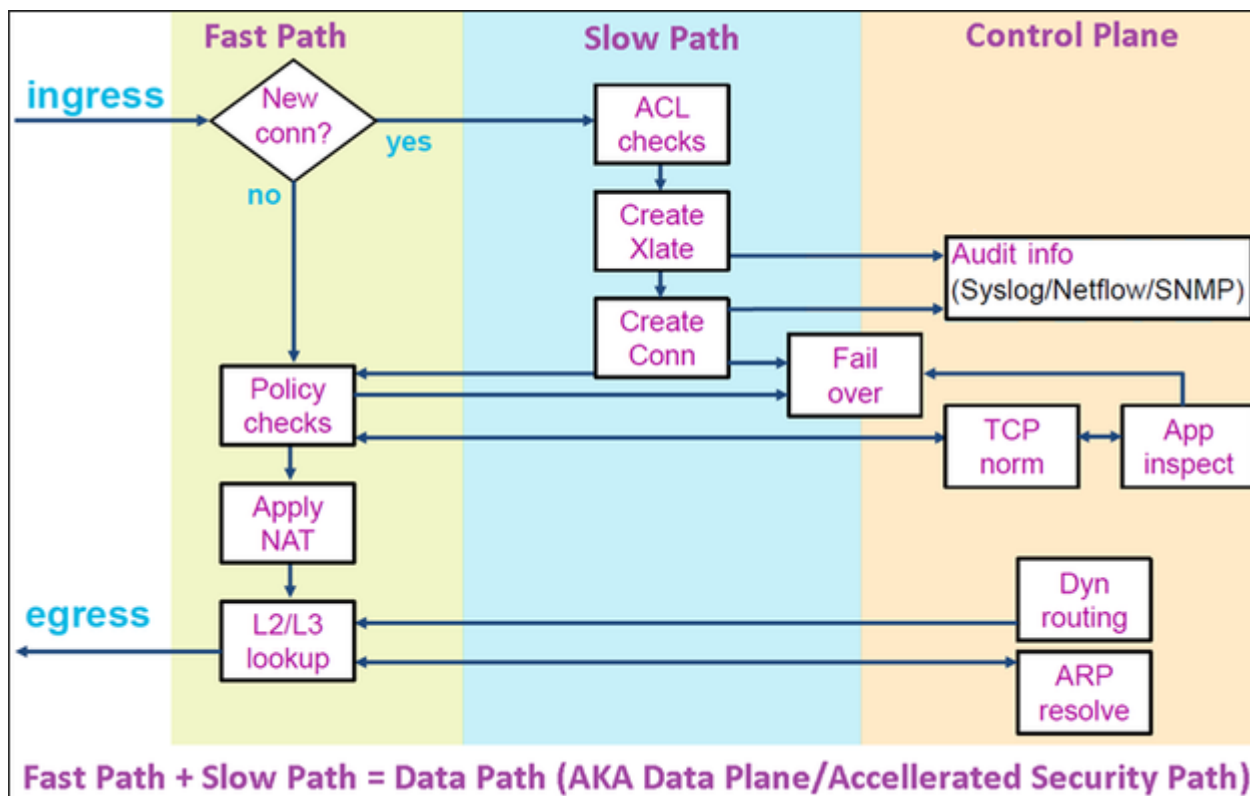
Configureren

Case 1 - Forwarding gebaseerd op Connection Lookup



Zoals reeds vermeld, is de belangrijkste component van de FTD LINA Engine het Datapath-proces (meerdere instanties gebaseerd op het aantal apparaatkernen). Bovendien bestaat de Datapath (ook bekend als Accelerated Security Path - ASP) uit 2 paden:

1. Slow Path = Verantwoordelijk voor nieuwe verbindingsonderneming (deze vult het Fast Path in).
2. Fast Path = behandelt pakketten die tot bestaande verbindingen behoren.



- Opdrachten zoals route tonen en arp tonen de inhoud van het besturingsplane.
- Aan de andere kant tonen opdrachten zoals asp-tabel routing en asp tabel arp de inhoud van ASP (Datapath) wat is wat daadwerkelijk wordt toegepast.

Opname met spoor inschakelen op FTD INSIDE-interface:

```
firepower# capture CAPI trace detail interface INSIDE match ip host 192.168.1.1 host 198.51.100.1
```

Een Telnet-sessie openen via de FTD:

```
Router1# telnet 198.51.100.1 /vrf VRF-101 /source-interface lo1
Trying 198.51.100.1 ... Open
```

De FTD legt vast hoe de pakketten vanaf het begin van de verbinding worden getoond (de 3-voudige TCP-handdruk wordt opgenomen):

```
firepower# show capture CAPI
```

26 packets captured

```
1: 10:50:38.407190 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: S 1306692135:1306692135(0) wi
2: 10:50:38.408929 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: S 1412677784:1412677784(0) ac
3: 10:50:38.409265 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: . ack 1412677785 win 4128
4: 10:50:38.409433 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: P 1306692136:1306692154(18) a
5: 10:50:38.409845 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: . ack 1412677785 win 4128
6: 10:50:38.410135 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: . ack 1306692154 win 4110
7: 10:50:38.411355 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: P 1412677785:1412677797(12) a
8: 10:50:38.413049 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: P 1306692154:1306692157(3) ac
9: 10:50:38.413140 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: P 1306692157:1306692166(9) ac
10: 10:50:38.414071 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: . 1412677797:1412678322(525)
...
```

Traceer het eerste pakket (TCP/SYN). Dit pakket gaat door de FTD LINA Slow Path en in dit geval wordt een Global Routing lookup gedaan:

```
firepower# show capture CAPI packet-number 1 trace
```

26 packets captured

```
1: 10:50:38.407190 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: S 1306692135:1306692135(0)
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 4683 ns
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x1505f1d17940, priority=13, domain=capture, deny=false
```

hits=1783, user_data=0x1505f2096910, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=INSIDE, output_ifc=any

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 4683 ns

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x1502a7ba4d40, priority=1, domain=permit, deny=false

hits=28, user_data=0x0, cs_id=0x0, l3_type=0x8

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0100.0000.0000

input_ifc=INSIDE, output_ifc=any

Phase: 3

Type: INPUT-ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Elapsed time: 5798 ns

Config:

Additional Information:

Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Elapsed time: 3010 ns

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433

access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: mzafeiro_empty - Default

access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE

Additional Information:

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

Forward Flow based lookup yields rule:

in id=0x1505f1e2e980, priority=12, domain=permit, deny=false

hits=4, user_data=0x15024a56b940, cs_id=0x0, use_real_addr, flags=0x0, protocol=0

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any,, dscp=0x0, nsg_id=none

input_ifc=any, output_ifc=any

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Elapsed time: 3010 ns

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:

Forward Flow based lookup yields rule:

in id=0x1505f1f18bc0, priority=7, domain=conn-set, deny=false
hits=4, user_data=0x1505f1f13f70, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=INSIDE(vrfid:0), output_ifc=any

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Elapsed time: 3010 ns

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x15052e96b150, priority=0, domain=nat-per-session, deny=false
hits=125, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Elapsed time: 3010 ns

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x1502a7bacde0, priority=0, domain=inspect-ip-options, deny=true
hits=19, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=INSIDE(vrfid:0), output_ifc=any

Phase: 8

Type: NAT

Subtype: per-session

Result: ALLOW

Elapsed time: 52182 ns

Config:

Additional Information:

Reverse Flow based lookup yields rule:

in id=0x15052e96b150, priority=0, domain=nat-per-session, deny=false
hits=127, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any

Phase: 9

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Elapsed time: 892 ns

Config:

Additional Information:

Reverse Flow based lookup yields rule:

in id=0x1502a7f9b460, priority=0, domain=inspect-ip-options, deny=true
hits=38, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=OUTSIDE2(vrfid:0), output_ifc=any

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 25422 ns
Config:
Additional Information:
New flow created with id 244, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 11
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 36126 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 12
Type: SNORT
Subtype:
Result: ALLOW
Elapsed time: 564636 ns
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 182318660
Session: new snort session
AppID: service unknown (0), application unknown (0)
Snort id 28, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Phase: 13
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 7136 ns
Config:
Additional Information:

Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 14

Type: ADJACENCY-LOOKUP

Subtype: Resolve Nexthop IP address to MAC

Result: ALLOW

Elapsed time: 2230 ns

Config:

Additional Information:

Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2

Adjacency :Active

MAC address 4c4e.35fc.fcd8 hits 10 reference 1

Phase: 15

Type: CAPTURE

Subtype:

Result: ALLOW

Elapsed time: 5352 ns

Config:

Additional Information:

Forward Flow based lookup yields rule:

out id=0x150521389870, priority=13, domain=capture, deny=false

hits=1788, user_data=0x1505f1d2b630, cs_id=0x0, l3_type=0x0

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0000.0000.0000

input_ifc=OUTSIDE2, output_ifc=any

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface: OUTSIDE2(vrfid:0)

output-status: up

output-line-status: up

Action: allow

Time Taken: 721180 ns

1 packet shown

firepower#

Overtrek een ander toegangspakket uit dezelfde stroom. Het pakket dat een actieve verbinding aanpast:

firepower# show capture CAPI packet-number 3 trace

33 packets captured

3: 10:50:38.409265 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: . ack 1412677785 win 4128

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Elapsed time: 2676 ns

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x1505f1d17940, priority=13, domain=capture, deny=false

hits=105083, user_data=0x1505f2096910, cs_id=0x0, l3_type=0x0

src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=INSIDE, output_ifc=any

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 2676 ns

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x1502a7ba4d40, priority=1, domain=permit, deny=false

hits=45, user_data=0x0, cs_id=0x0, l3_type=0x8

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0100.0000.0000

input_ifc=INSIDE, output_ifc=any

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Elapsed time: 1338 ns

Config:

Additional Information:

Found flow with id 2552, using existing flow

Module information for forward flow ...

snp_fp_inspect_ip_options

snp_fp_tcp_normalizer

snp_fp_snort

snp_fp_translate

snp_fp_tcp_normalizer

snp_fp_adjacency

snp_fp_fragment

snp_ifc_stat

Module information for reverse flow ...

snp_fp_inspect_ip_options

snp_fp_tcp_normalizer

snp_fp_translate

snp_fp_snort

snp_fp_tcp_normalizer

snp_fp_adjacency

snp_fp_fragment

snp_ifc_stat

Phase: 4

Type: EXTERNAL-INSPECT

Subtype:

Result: ALLOW

Elapsed time: 16502 ns

Config:

Additional Information:

Application: 'SNORT Inspect'

Phase: 5

Type: SNORT

Subtype:

Result: ALLOW

Elapsed time: 12934 ns

Config:

Additional Information:

Snort Trace:

Packet: TCP, ACK, seq 1306692136, ack 1412677785
AppID: service unknown (0), application unknown (0)
Snort id 19, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Result:

input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow
Time Taken: 36126 ns

1 packet shown
firepower#

Zwevende time-out

Het probleem

Tijdelijke instabiliteit van routes kan langdurige (olifant) UDP-verbindingen via de FTD veroorzaken die via verschillende FTD-interfaces tot stand worden gebracht dan gewenst.

De oplossing

Om dit te verhelpen, stelt u de drijvende-kommawaarde in voor de time-out in op een andere waarde dan de standaard die is uitgeschakeld:



FTD4100-1

Enter Description

- ARP Inspection
- Banner
- DNS
- External Authentication
- Fragment Settings
- HTTP Access
- ICMP Access
- SSH Access
- SMTP Server
- SNMP
- SSL
- Syslog
- Timeouts**
- Time Synchronization
- Time Zone
- UCAPL/CC Compliance

Console Timeout*	<input type="text" value="0"/>	(0 - 1440 mins)	?
Translation Slot(xlate)	Default	3:00:00	(3:0:0 or 0:1:0 - 1193:0:0)
Connection(Conn)	Default	1:00:00	(0:0:0 or 0:5:0 - 1193:0:0)
Half-Closed	Default	0:10:00	(0:0:0 or 0:0:30 - 1193:0:0)
UDP	Default	0:02:00	(0:0:0 or 0:1:0 - 1193:0:0)
ICMP	Default	0:00:02	(0:0:2 or 0:0:2 - 1193:0:0)
RPC/Sun RPC	Default	0:10:00	(0:0:0 or 0:1:0 - 1193:0:0)
H.225	Default	1:00:00	(0:0:0 or 0:0:0 - 1193:0:0)
H.323	Default	0:05:00	(0:0:0 or 0:0:0 - 1193:0:0)
SIP	Default	0:30:00	(0:0:0 or 0:5:0 - 1193:0:0)
SIP Media	Default	0:02:00	(0:0:0 or 0:1:0 - 1193:0:0)
SIP Disconnect:	Default	0:02:00	(0:02:0 or 0:0:1 - 0:10:0)
SIP Invite	Default	0:03:00	(0:1:0 or 0:1:0 - 0:30:0)
SIP Provisional Media	Default	0:02:00	(0:2:0 or 0:1:0 - 0:30:0)
Floating Connection	Default	0:00:00	(0:0:0 or 0:0:30 - 1193:0:0)
Xlate-PAT	Default	0:00:30	(0:0:30 or 0:0:30 - 0:5:0)

Vanaf de opdrachtreferentie:

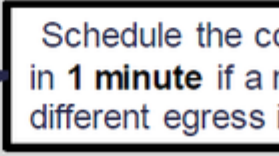
floating-conn When multiple routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To make it possible to use better routes, set the timeout to a value between 0:0:30 and 1193:0:0.

Zie voor meer informatie Case Study: UDP-verbindingen mislukken na opnieuw laden van de Cisco Live BRKSEC-3020-sessie:

Floating Connection Timeout

- The “bad” connection never times out since the UDP traffic is stateless
 - TCP is stateful, so the connection would terminate and re-establish
 - ASA needs to tear the original connection down when the connection is replaced
 - ASA 8.4(2)+ introduces **timeout floating-conn** to accomplish this

```
asa# show run timeout
timeout xlate 9:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-discover
timeout sip-provisional-media 0:02:00 uauth 9:00:00 absolute uauth
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
asa#
asa# configure terminal
asa(config)# timeout floating-conn 0:01:00
```



Schedule the connection to be torn down in 1 minute if a new connection is established on a different egress interface.

Time-out voor conn-holddown

Het probleem

Een route daalt (wordt verwijderd), maar het verkeer past een gevestigde verbinding aan.

De oplossing

Timeout conn-holddown functie is toegevoegd op ASA 9.6.2. Deze functie is standaard ingeschakeld, maar wordt momenteel (7.1.x) niet ondersteund door FMC UI of FlexConfig. Verwante verbetering: [ENH: timeout conn-holddown niet beschikbaar voor configuratie in FMC](#)

Vanuit de ASA CLI-handleiding:

conn-holddown	How long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. The purpose of the connection holddown timer is to reduce the effect of route flapping, where routes might come up and go down quickly. You can reduce the holddown timer to make route convergence happen more quickly. The default is 15 seconds, the range is 00:00:00 to 00:00:15.
----------------------	--

```
firepower# show run all timeout
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
```

```
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
```

Case 2 - Forwarding gebaseerd op NAT Lookup

Vereiste

Configureer deze NAT-regel:

- Type: Statisch
- Broninterface: BINNENKANT
- Bestemmingsinterface: BUITEN1
- Oorspronkelijke bron: 192.168.1.1
- Oorspronkelijke bestemming: 198.51.100.1
- Vertaalde bron: 192.168.1.1
- Vertaalde bestemming: 198.51.100.1

Oplossing

						Original Packet				
<input type="checkbox"/>	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations
NAT Rules Before										
<input type="checkbox"/>	1	#	Static	INSIDE_FTD4100-1	OUTSIDE_FTD4100	host_192.168.1.1	host_198.51.100.1		host_192.168.1.1	host_198.51.100.1
Auto NAT Rules										

De geïmplementeerde NAT-regel op de FTD CLI:

```
firepower# show run nat
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.100.1
firepower# show nat
Manual NAT Policies (Section 1)
1 (INSIDE) to (OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.100.1
translate_hits = 0, untranslate_hits = 0
```

Configureren 3 opnamen:

```
firepower# capture CAPI trace detail interface INSIDE match ip host 192.168.1.1 host 198.51.100.1
firepower# capture CAP01 interface OUTSIDE1 match ip host 192.168.1.1 any
firepower# capture CAP02 interface OUTSIDE2 match ip host 192.168.1.1 any
firepower# show capture
capture CAPI type raw-data trace detail interface INSIDE [Capturing - 0 bytes]
match ip host 192.168.1.1 host 198.51.100.1
capture CAP01 type raw-data interface OUTSIDE1 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
capture CAP02 type raw-data interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
```

Start een telnet sessie van 192.168.1.1 t/m 198.51.100.1:

```
Router1# telnet 198.51.100.1 /vrf VRF-101 /source-interface lo1
Trying 198.51.100.1 ...
% Connection timed out; remote host not responding
```

Pakketten komen aan op FTD, maar er gaat niets over buitenkant1 of buitenkant2 interfaces:

```
firepower# show capture
capture CAPI type raw-data trace detail interface INSIDE [Capturing - 156 bytes]
match ip host 192.168.1.1 host 198.51.100.1
capture CAP01 type raw-data interface OUTSIDE1 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
capture CAP02 type raw-data interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
```

Traceer het TCP/SYN-pakket. Fase 3 (UN-NAT) toont aan dat NAT (UN-NAT specifiek) het pakket naar de REMOTE1-interface heeft omgeleid voor raadpleging van de volgende hop:

```
firepower# show capture CAPI
2 packets captured
1: 11:22:59.179678 802.1Q vlan#101 P0 192.168.1.1.38790 > 198.51.100.1.23: S 1174675193:1174675193(0) wi
2: 11:23:01.179632 802.1Q vlan#101 P0 192.168.1.1.38790 > 198.51.100.1.23: S 1174675193:1174675193(0) wi
2 packets shown
firepower#
```

```
firepower# show capture CAPI packet-number 1 trace detail
```

```
2 packets captured
1: 11:22:59.179678 4c4e.35fc.fcd8 00be.75f6.1dae 0x8100 Length: 62
802.1Q vlan#101 P0 192.168.1.1.38790 > 198.51.100.1.23: S [tcp sum ok] 1174675193:1174675193(0) win 4128
...
```


Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 6244 ns
Config:
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.100.1
Additional Information:
NAT divert to egress interface OUTSIDE1(vrfid:0)
Untranslate 198.51.100.1/23 to 198.51.100.1/23

...
Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 25422 ns
Config:
Additional Information:
New flow created with id 2614, packet dispatched to next module
Module information for forward flow ...
snf_fp_inspect_ip_options
snf_fp_tcp_normalizer
snf_fp_tcp_proxy
snf_fp_snort
snf_fp_tcp_proxy
snf_fp_translate
snf_fp_tcp_normalizer
snf_fp_adjacency
snf_fp_fragment
snf_ifc_stat

Phase: 15
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 8028 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 16
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Elapsed time: 446 ns
Config:
Additional Information:
Input route lookup returned ifc OUTSIDE2 is not same as existing ifc OUTSIDE1

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 777375 ns
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame 0x00005577204a7287 flow (NA)/NA

1 packet shown

In dit geval betekent de SUBOPTIMAL-LOOKUP dat de uitgangsinterface die door het NAT-proces wordt bepaald (BUITEN1), anders is dan de uitgangsinterface die in de ASP-inputtabel is gespecificeerd:

```
firepower# show asp table routing | include 198.51.100.0
in 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
```

Een mogelijke tijdelijke oplossing is om een zwevende statische route op de REMOTE1 interface toe te voegen:

```
firepower# show run route
route OUTSIDE2 198.51.100.0 255.255.255.248 192.0.2.99 1
route OUTSIDE1 198.51.100.0 255.255.255.248 203.0.113.99 200
```

Opmerking: als u probeert een statische route toe te voegen met dezelfde metriek als de route die al bestaat, wordt deze fout weergegeven:

The screenshot shows the 'Routing' tab in the Palo Alto Networks GUI. The left sidebar is open to 'Manage Virtual Routers' > 'Global' > 'Static Route'. The main area displays a routing table with the following entries:

Network	Interface	Leaked from Virtual Router
IPv4 Routes		
net_198.51.100.0_29bits	OUTSIDE1	
net_198.51.100.0_29bits	OUTSIDE2	
IPv6 Routes		

An error message is displayed on the right side of the screen:

```
Error - Device Configuration
Virtual router [Global] - Invalid IPv4
The interfaces OUTSIDE2, OUTSIDE1
network address 198.51.100.0/29 are
considered as ECMP eligible routes.
Please Configure ECMP with above i
```

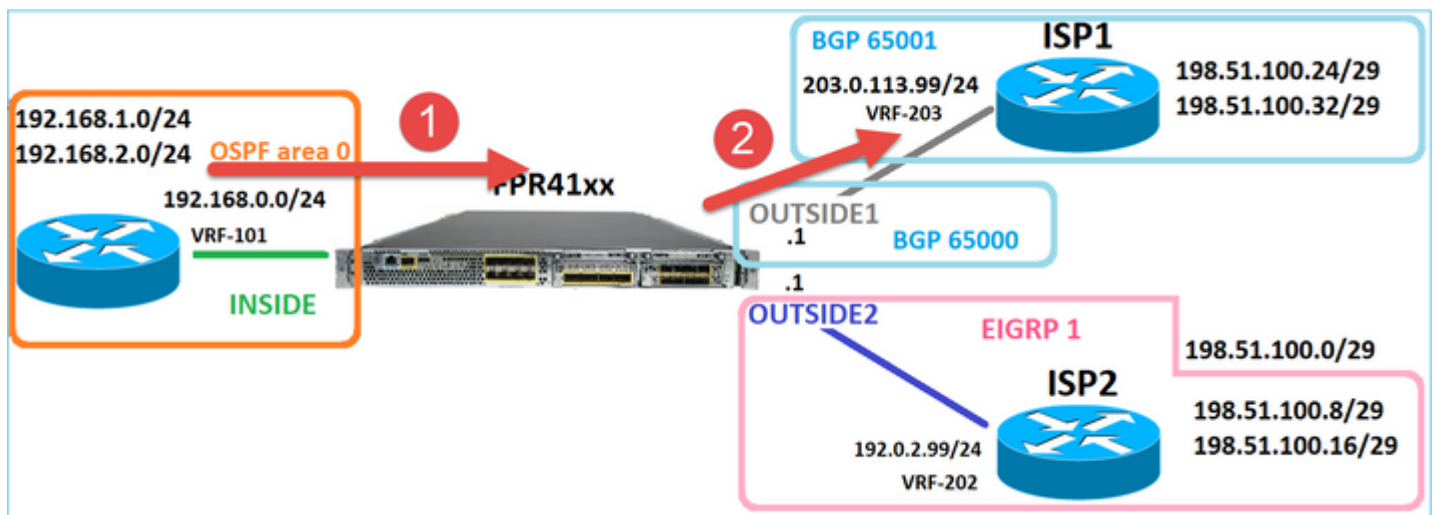
Opmerking: Zwevende route met een afstand metriek van 255 is niet geïnstalleerd in de routingstabel.

Probeer aan Telnet dat er pakketten zijn die door FTD worden verzonden:

```
Router1# telnet 198.51.100.1 /vrf VRF-101 /source-interface lo1
Trying 198.51.100.1 ...
% Connection timed out; remote host not responding
```

```
firepower# show capture
capture CAPI type raw-data trace detail interface INSIDE [Capturing - 156 bytes]
match ip host 192.168.1.1 host 198.51.100.1
capture CAP01 type raw-data interface OUTSIDE1 [Capturing - 312 bytes]
match ip host 192.168.1.1 any
capture CAP02 type raw-data interface OUTSIDE2 [Capturing - 386 bytes]
match ip host 192.168.1.1 any
```

Het pakketspoor toont aan dat de pakketten aan ISP1 (BUITEN1) interface in plaats van ISP2 wegens NAT Raadpleging door:sturen:



```
firepower# show capture CAPI packet-number 1 trace
```

```
2 packets captured
```

```
1: 09:03:02.773962 802.1Q vlan#101 P0 192.168.1.1.16774 > 198.51.100.1.23: S 2910053251:2910053251(0) wi
...
```

```
Phase: 3
```

```
Type: UN-NAT
```

```
Subtype: static
```

```
Result: ALLOW
```

```
Elapsed time: 4460 ns
```

```
Config:
```

```
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.100.1
```

```
Additional Information:
```

```
NAT divert to egress interface OUTSIDE1(vrfid:0)
```

```
Untranslate 198.51.100.1/23 to 198.51.100.1/23
```

...

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 29436 ns
Config:
Additional Information:
New flow created with id 2658, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_snort
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 15
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 5798 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 16
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Elapsed time: 446 ns
Config:
Additional Information:
Input route lookup returned ifc OUTSIDE2 is not same as existing ifc OUTSIDE1

Phase: 17
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Elapsed time: 1784 ns
Config:
Additional Information:
Found next-hop 203.0.113.99 using egress ifc OUTSIDE1(vrfid:0)

Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1338 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 203.0.113.99 on interface OUTSIDE1
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 106 reference 2

...

Result:
input-interface: INSIDE(vrfid:0)
input-status: up

```
input-line-status: up
output-interface: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 723409 ns
```

```
1 packet shown
firepower#
```

Interessant, in dit geval, zijn er pakketten die op BINNENKANT en beide uitgangsinterfaces worden getoond:

```
firepower# show capture CAPI
```

```
2 packets captured
```

```
1: 09:03:02.773962 802.1Q vlan#101 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3031010184:3031010184(0) win 4128
2: 09:03:05.176565 802.1Q vlan#101 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3031010184:3031010184(0) win 4128
2 packets shown
firepower# show capture CAP01
```

```
4 packets captured
```

```
1: 09:03:02.774358 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) win 4128
2: 09:03:02.774557 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) win 4128
3: 09:03:05.176702 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) win 4128
4: 09:03:05.176870 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) win 4128
4 packets shown
firepower# show capture CAP02
```

```
5 packets captured
```

```
1: 09:03:02.774679 802.1Q vlan#202 P0 192.168.1.1.32134 > 198.51.100.1.23: S 194652172:194652172(0) win 4128
2: 09:03:02.775457 802.1Q vlan#202 P0 198.51.100.1.23 > 192.168.1.1.32134: S 4075003210:4075003210(0) win 4128
3: 09:03:05.176931 802.1Q vlan#202 P0 192.168.1.1.32134 > 198.51.100.1.23: S 194652172:194652172(0) win 4128
4: 09:03:05.177282 802.1Q vlan#202 P0 198.51.100.1.23 > 192.168.1.1.32134: . ack 194652173 win 4128
5: 09:03:05.180517 802.1Q vlan#202 P0 198.51.100.1.23 > 192.168.1.1.32134: S 4075003210:4075003210(0) win 4128
```

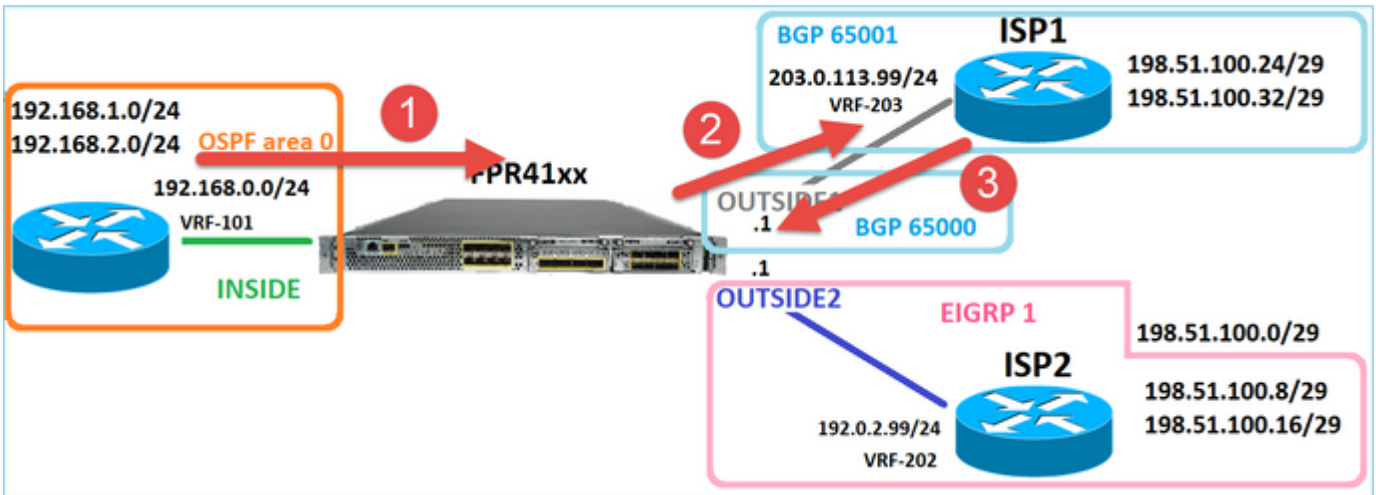
De pakketdetails omvatten de MAC-adresinfo, en een spoor van de pakketten op REMOTE1 en REMOTE2 interfaces onthult het pad van de pakketten:

```
firepower# show capture CAP01 detail
```

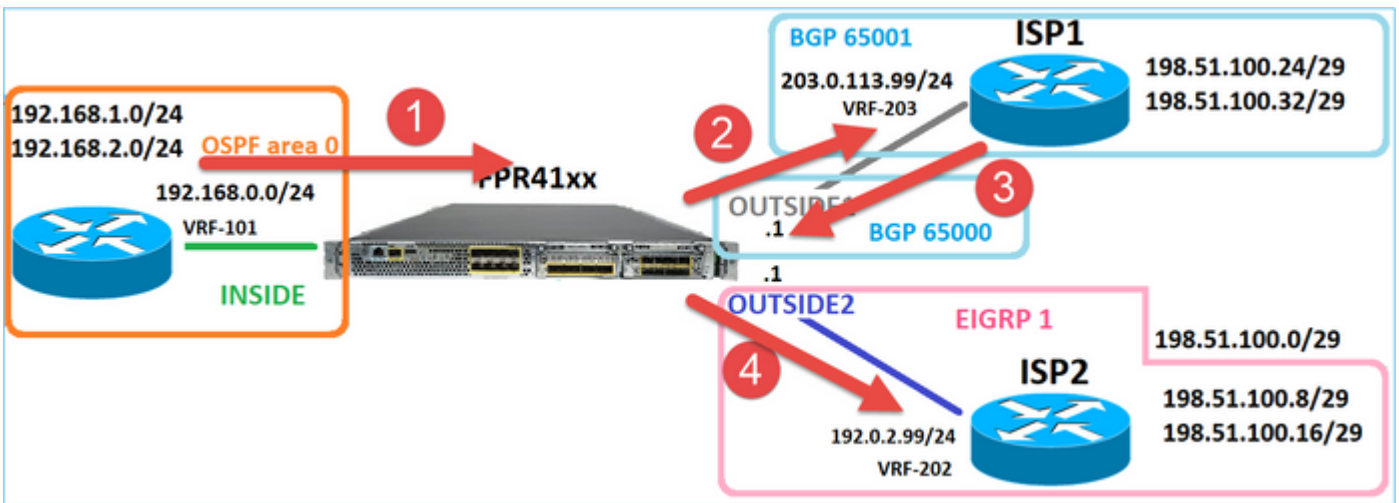
```
4 packets captured
```

```
1: 09:03:02.774358 00be.75f6.1dae 4c4e.35fc.fcd8 0x8100 Length: 62
802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S [tcp sum ok] 3249840142:3249840142(0) win 4128
2: 09:03:02.774557 4c4e.35fc.fcd8 00be.75f6.1dae 0x8100 Length: 62
802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S [tcp sum ok] 3249840142:3249840142(0) win 4128
3: 09:03:05.176702 00be.75f6.1dae 4c4e.35fc.fcd8 0x8100 Length: 62
802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S [tcp sum ok] 3249840142:3249840142(0) win 4128
4: 09:03:05.176870 4c4e.35fc.fcd8 00be.75f6.1dae 0x8100 Length: 62
```

```
802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S [tcp sum ok] 3249840142:3249840142(0) win 4128
4 packets shown
```



Het overtrekken van het pakket dat terugkeert toont omleiding aan interface EXTERN2 toe te schrijven aan Globale Routingstabel Lookup:



```
firepower# show capture CAP01 packet-number 2 trace
```

```
4 packets captured
```

```
2: 09:03:02.774557 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) wi
...
```

```
Phase: 3
```

```
Type: INPUT-ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Elapsed time: 7136 ns
```

```
Config:
```

```
Additional Information:
```

```
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)
```

```
...
```

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 12488 ns
Config:
Additional Information:
New flow created with id 13156, packet dispatched to next module

...

Phase: 13
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 3568 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

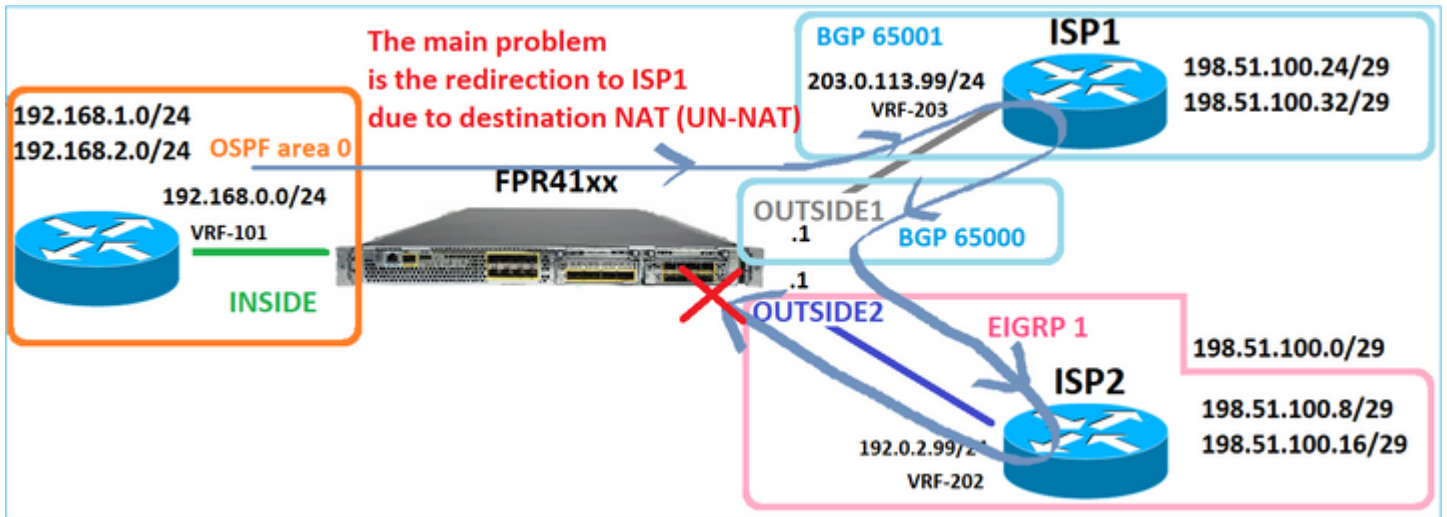
Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1338 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 0 reference 1

...

Result:
input-interface: OUTSIDE1(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 111946 ns

1 packet shown
firepower#

De ISP2 router verzendt het antwoord (SYN/ACK), maar dit pakket wordt doorgestuurd naar ISP1 omdat het overeenkomt met de ingestelde verbinding. Het pakket wordt door de FTD laten vallen vanwege geen L2-nabijheid in de ASP out-tabel:



```
firepower# show capture CAP02 packet-number 2 trace
```

```
5 packets captured
```

```
2: 09:03:02.775457 802.1Q vlan#202 P0 198.51.100.1.23 > 192.168.1.1.32134: S 4075003210:4075003210(0) a
...
```

```
Phase: 3
```

```
Type: FLOW-LOOKUP
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 2230 ns
```

```
Config:
```

```
Additional Information:
```

```
Found flow with id 13156, using existing flow
```

```
...
```

```
Phase: 7
```

```
Type: SUBOPTIMAL-LOOKUP
```

```
Subtype: suboptimal next-hop
```

```
Result: ALLOW
```

```
Elapsed time: 0 ns
```

```
Config:
```

```
Additional Information:
```

```
Input route lookup returned ifc INSIDE is not same as existing ifc OUTSIDE1
```

```
Result:
```

```
input-interface: OUTSIDE2(vrfid:0)
```

```
input-status: up
```

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

```
output-interface: INSIDE(vrfid:0)
```

```
output-status: up
```

```
output-line-status: up
```

```
Action: drop
```

```
Time Taken: 52628 ns
```

```
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame 0x00005577204a7287 flow (NA)/NA
```


Case 3 - Forwarding op basis van beleidsgebaseerde routing (PBR)

Na de raadpleging van de verbindingstroom en de NAT-raadpleging van de bestemming, is PBR het volgende item dat de bepaling van de uitgaande interface kan beïnvloeden. PBR is gedocumenteerd in: [op beleid gebaseerde routing](#)

Voor de PBR-configuratie op het VCC is het belangrijk dat u zich bewust bent van deze richtlijn: FlexConfig is gebruikt om PBR in FMC te configureren voor FTD-versies eerder dan 7.1. U kunt FlexConfig nog steeds gebruiken om PBR in alle versies te configureren. Voor een toegangsinterface kunt u PBR echter niet configureren met behulp van de op beleid gebaseerde routingpagina van zowel FlexConfig als FMC.

In deze casestudy heeft de FTD een route naar 198.51.100.0/24 die naar ISP2 wijst:

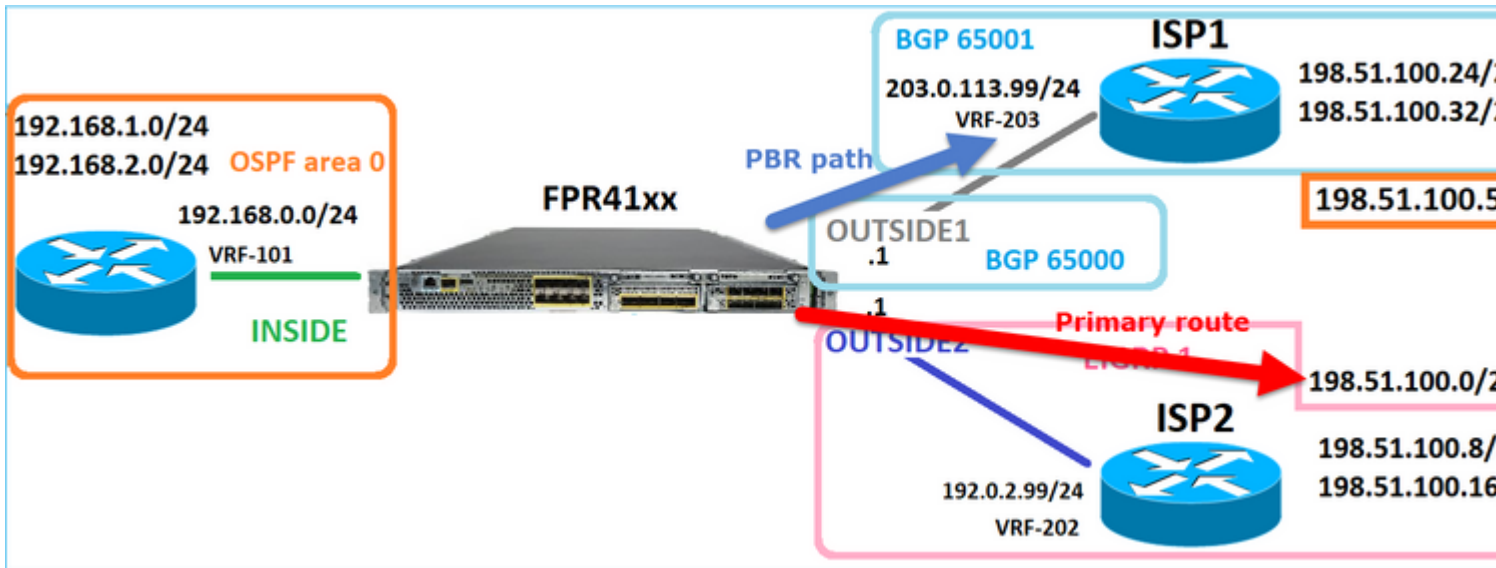
```
firepower# show route | begin Gate
Gateway of last resort is not set

C 192.0.2.0 255.255.255.0 is directly connected, OUTSIDE2
L 192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
C 192.168.0.0 255.255.255.0 is directly connected, INSIDE
L 192.168.0.1 255.255.255.255 is directly connected, INSIDE
O 192.168.1.1 255.255.255.255 [110/11] via 192.168.0.99, 5d01h, INSIDE
O 192.168.2.1 255.255.255.255 [110/11] via 192.168.0.99, 5d01h, INSIDE
S 198.51.100.0 255.255.255.248 [1/0] via 192.0.2.99, OUTSIDE2
D 198.51.100.8 255.255.255.248
[90/130816] via 192.0.2.99, 5d01h, OUTSIDE2
D 198.51.100.16 255.255.255.248
[90/130816] via 192.0.2.99, 5d01h, OUTSIDE2
B 198.51.100.24 255.255.255.248 [20/0] via 203.0.113.99, 5d00h
B 198.51.100.32 255.255.255.248 [20/0] via 203.0.113.99, 5d00h
C 203.0.113.0 255.255.255.0 is directly connected, OUTSIDE1
L 203.0.113.1 255.255.255.255 is directly connected, OUTSIDE1
```

Vereiste

Configureer een PBR-beleid met deze kenmerken:

- Verkeer van IP 192.168.2.0/24 naar 198.51.100.5 moet naar ISP1 (next-hop 203.0.113.99) worden verzonden terwijl andere bronnen de REMOTE2-interface moeten gebruiken.



Oplossing

In pre-7.1 versies, om PBR te vormen:

1. Maak een uitgebreide ACL die overeenkomt met het interessante verkeer (bijvoorbeeld PBR_ACL).
2. Maak een routekaart die overeenkomt met de ACL die in Stap 1 is gemaakt en stel de gewenste volgende hop in.
3. Maak een FlexConfig-object dat PBR op de toegangsinterface mogelijk maakt met behulp van de routekaart die in Stap 2 is gemaakt.

In post-7.1 releases kunt u PBR configureren met de pre-7.1 manier, of u kunt de nieuwe op beleid gebaseerde routing optie gebruiken onder de sectie Apparaat > Routing:

1. Maak een uitgebreide ACL die overeenkomt met het interessante verkeer (bijvoorbeeld PBR_ACL).
2. Voeg een PBR-beleid toe en specificeer:
 - a. Het overeenkomende verkeer
 - b. De toegangsinterface
 - c. De volgende hop

PBR configureren (nieuwe manier)

Stap 1 - Bepaal een toegangslijst voor het overeenkomende verkeer.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies t
Supports IPv4 a

Edit Extended Access List Object

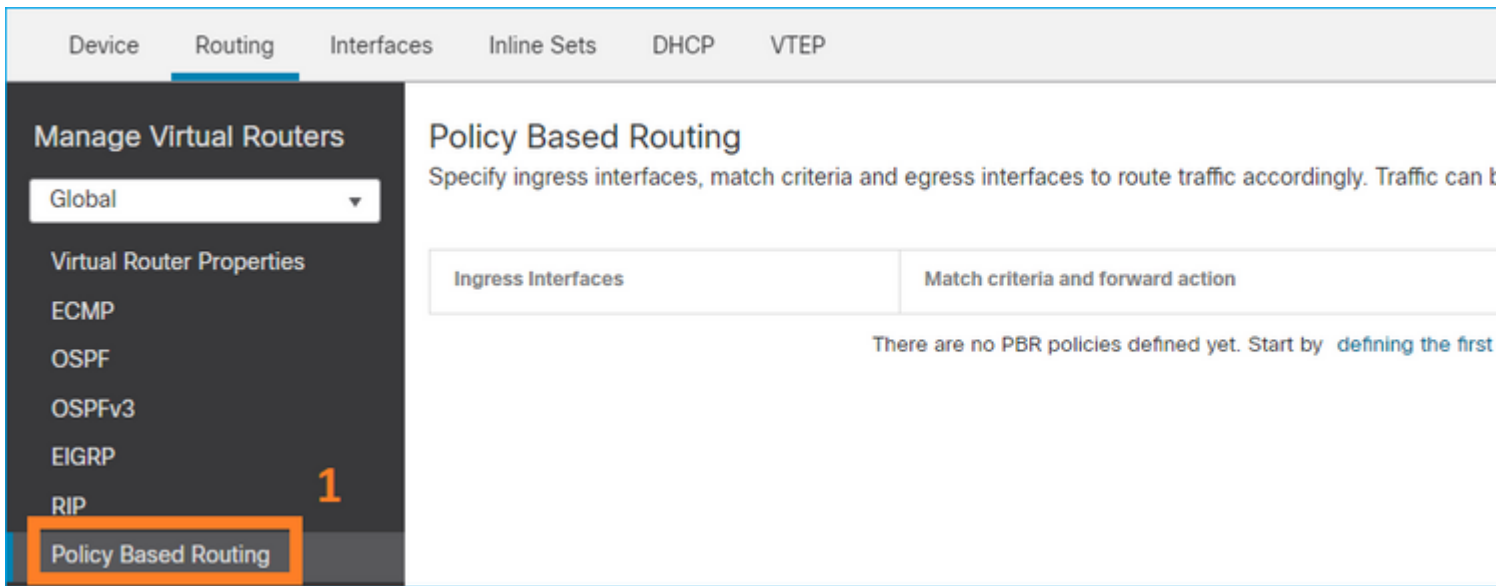
Name
ACL_PBR

Entries (1)

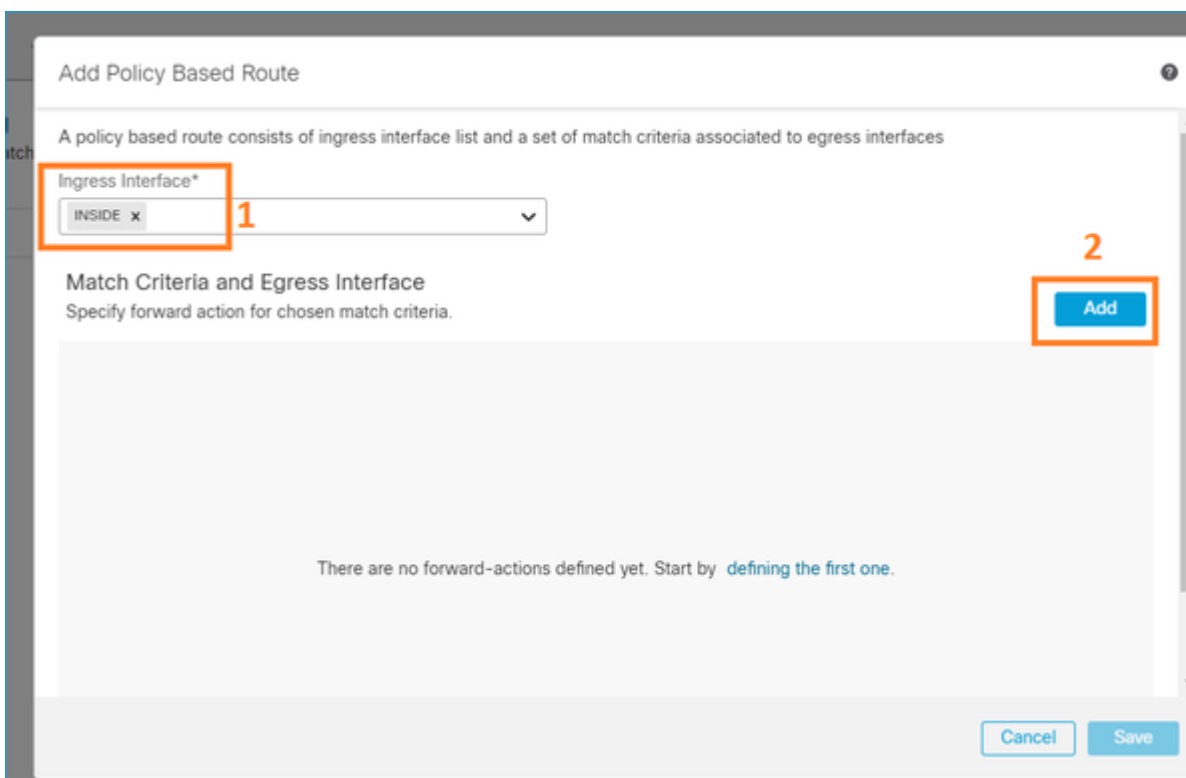
Sequence	Action	Source	Source Port	Destination	Destinat
1	Allow	192.168.2.0/24	Any	198.51.100.5	Any

Stap 2 - Een PBR-beleid toevoegen

Navigeer naar Apparaten > Apparaatbeheer en bewerk het FTD-apparaat. Kies Routing > Policy Based Routing, en selecteer op de pagina Policy Based Routing de optie Add.



Specificeer de toegangsinterface:



Specificeer de doorsturen acties:

Add Forwarding Actions

Match ACL:* 1

Send To:* 2

IPv4 Addresses 3

IPv6 Addresses

Opslaan en implementeren

Opmerking: als u meerdere uitgangsiinterfaces wilt configureren, moet u in het veld 'Verzenden naar' de optie 'Uitgangen interfaces' instellen (beschikbaar vanaf versie 7.0+). Voor meer details check: [Configuration Voorbeeld voor op beleid gebaseerde routing](#)

PBR configureren (oudere manier)

Stap 1 - Bepaal een toegangslijst voor het overeenkomende verkeer.

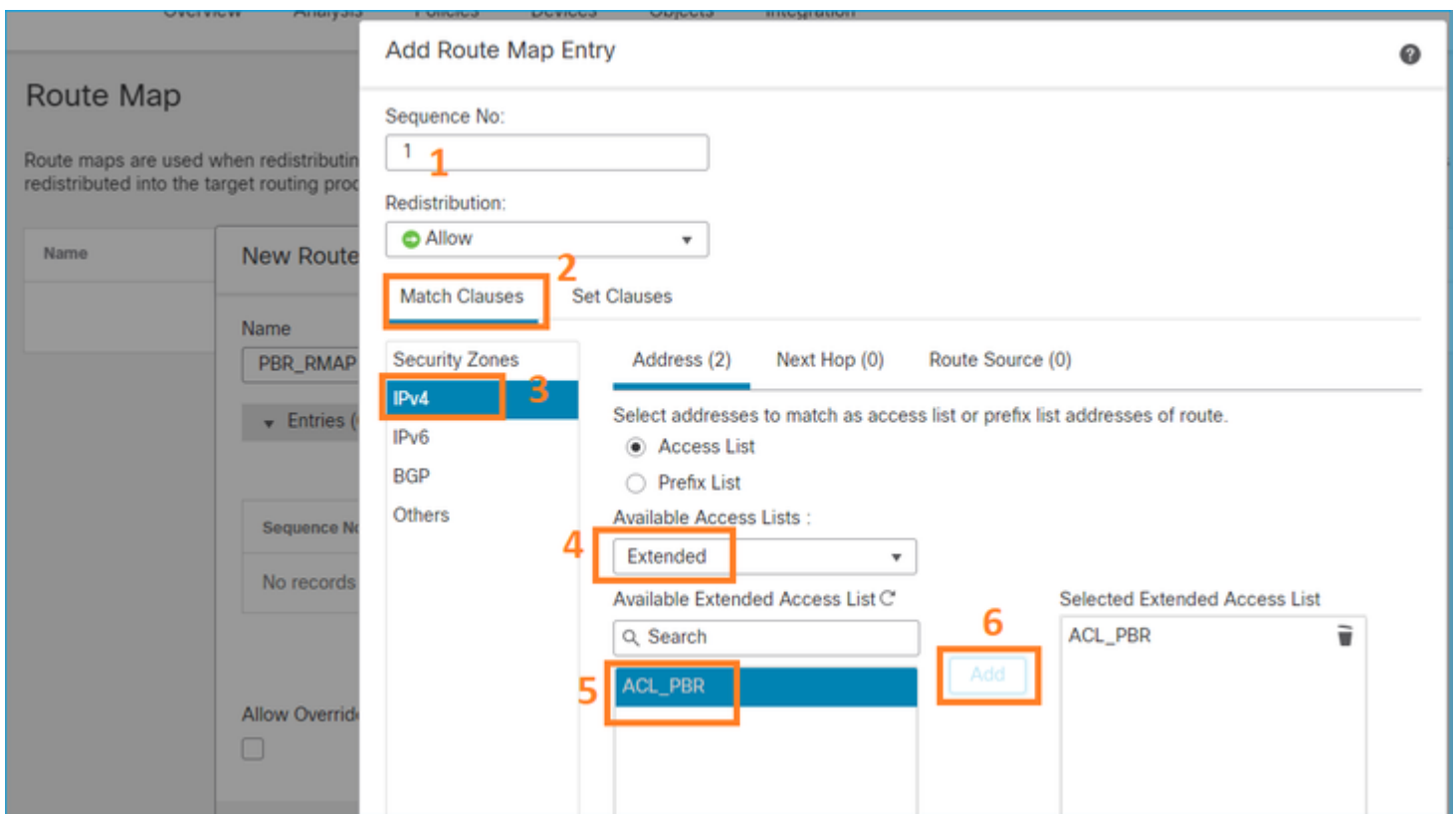
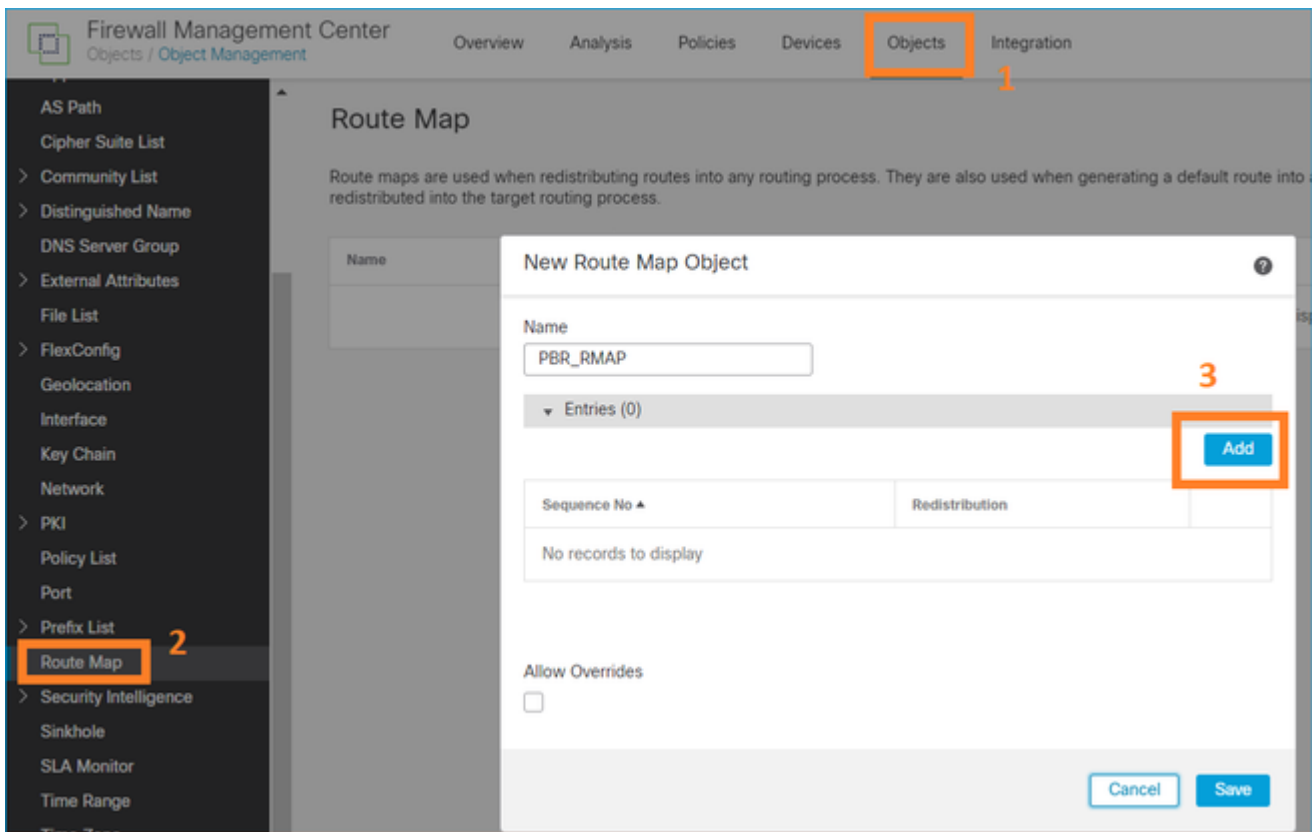
The screenshot shows the Firewall Management Center interface. The 'Objects' tab is selected and highlighted with an orange box and a '1'. In the left sidebar, the 'Access List' menu is expanded, and 'Extended' is selected with an orange box and a '2'. The main content area shows the 'Edit Extended Access List Object' dialog. The 'Name' field contains 'ACL_PBR'. Below, a table lists the entries for the ACL:

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Allow	192.168.2.0/24	Any	198.51.100.5	Any

The table row is highlighted with an orange box and a '3'.

Stap 2 - Definieer een routekaart die overeenkomt met de ACL en stelt de volgende hop in.

Bepaal eerst de overeenstemmingsclausule:



Bepaal de Setclausule:

Edit Route Map Entry

Sequence No:

Redistribution:

Match Clauses **Set Clauses** **1**

Metric Values **BGP Clauses** **2**

AS Path Community List **Others** **3**

Local Preference :
Range: 1-4294967295

Set Weight :
Range: 0-65535

Origin:

Local IGP

Incomplete

IPv4 settings:

Next Hop:

Specific IP :
Use comma to separate multiple values

Prefix List:

IPv6 settings:

4

Toevoegen en opslaan.

Stap 3 - Het FlexConfig PBR-object configureren.

Kopieer eerst (dupliceer) het bestaande PBR-object:

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration Deploy

FlexConfig Object Add FlexConfig O

FlexConfig Object include device configuration commands, variables, and scripting language instructions

Name	Domain
Policy_Based_Routing	Global
Policy_Based_Routing_Clear	Global

1

AS Path
Cipher Suite List
> Community List
> Distinguished Name
DNS Server Group
> External Attributes
File List
FlexConfig **1**
FlexConfig Object
Text Object
Geolocation

Specificeer de Objectnaam en verwijder het vooraf bepaalde route-kaart voorwerp:

Add FlexConfig Object

Name: **1 Specify a new name**

Description:

▲ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | | Type:

```
interface  2 Specify the correct ingress interface  
policy-route route-map  3 Remove this route-map
```

Specificeer de nieuwe routekaart:

Add FlexConfig Object

Name:

Description:

▲ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | | Type:

- Insert Policy Object
- Insert System Variable
- Insert Secret Key
- Route Map **2**

Insert Route Map Variable

Variable Name: **1**

Description:

Available Objects **2**

- PBR_RMAP **3**

Selected Object

- PBR_RMAP

Dit is het eindresultaat:

Add FlexConfig Object

Name:

Description:

▲ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | | Deployment: | Type:

```
interface Port-channel1.101
  policy-route route-map $PBR_RMAP
```

Stap 4 - Voeg het PBR-object toe aan het FTD FlexConfig-beleid.

Firewall Management Center
Devices / Flexconfig Policy Editor

Overview Analysis Policies Devices Objects Integration Deploy

FTD4100_FlexConfig

Enter Description

Available FlexConfig FlexConfig Object

- User Defined **1**
 - FTD4100_PBR** **2**
 - no_ICMP
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure

Selected Prepend FlexConfigs

#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
1	FTD4100_PBR	The template is an example of PBR p

Opslaan en voorbeeldconfiguratie selecteren:

Preview FlexConfig

Select Device:

mzafeiro_FTD4100-1

```
route-map PBR_RMAP permit 1
match ip address ACL_PBR
set ip next-hop 203.0.113.99
vpn-addr-assign local
```

```
!INTERFACE_START
no logging FMC MANAGER_VPN_EVENT_LIST
```

```
!INTERFACE_END
```

```
###Flex-config Appended CLI ###
```

```
interface Port-channel1.101
 policy-route route-map PBR_RMAP
```

Ten slotte, implementeren van het beleid.

Opmerking: PBR kan niet worden geconfigureerd met FlexConfig en FMC UI voor dezelfde toegangsinterface.

Controleer voor de PBR SLA-configuratie dit document: [Configureer PBR met IP SLA™s voor DUBBELE ISP op FTD beheerde door FMC](#)

PBR-verificatie

Verificatie van toegangsinterface:

```
firepower# show run interface Po1.101
!
interface Port-channel1.101
vlan 101
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.0.1 255.255.255.0
policy-route route-map FMC_GENERATED_PBR_1649228271478
ospf authentication null
```

Verificatie routekaart:

```
firepower# show run route-map
!
route-map FMC_GENERATED_PBR_1649228271478 permit 5
  match ip address ACL_PBR
  set ip next-hop 203.0.113.99
```

```
firepower# show route-map
route-map FMC_GENERATED_PBR_1649228271478, permit, sequence 5
Match clauses:
ip address (access-lists): ACL_PBR

Set clauses:
adaptive-interface cost OUTSIDE1 (0)
```

Verificatie beleidsroute:

```
firepower# show policy-route
Interface Route map
Port-channel1.101 FMC_GENERATED_PBR_1649228271478
```

Packet-Tracer voor en na de wijziging:

Zonder PBR	Met PBR
<pre>firepower# packet-tracer input INSIDE tcp 192.168.2.100 1111 198.51.100.5 23 Phase: 3 Type: INPUT-ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Elapsed time: 11596 ns Config: Additional Information: Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0) ... Phase: 13 Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP Subtype: Resolve Preferred Egress interface Result: ALLOW Elapsed time: 6244 ns Config:</pre>	<pre>firepower# packet-tracer i ... Phase: 3 Type: SUBOPTIMAL-LOOKUP Subtype: suboptimal next-h Result: ALLOW Elapsed time: 39694 ns Config: Additional Information: Input route lookup returne Phase: 4 Type: ECMP load balancing Subtype: Result: ALLOW Elapsed time: 2230 ns Config: Additional Information: ECMP load balancing Found next-hop 203.0.113.9 Phase: 5 Type: PBR-LOOKUP Subtype: policy-route Result: ALLOW Elapsed time: 446 ns</pre>

```

Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 2230 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 0 reference 1

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 272058 ns

```

```

Config:
route-map FMC_GENERATED_PB
match ip address ACL_PBR
set adaptive-interface cos
Additional Information:
Matched route-map FMC_GENE
Found next-hop 203.0.113.9
...

Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop I
Result: ALLOW
Elapsed time: 5352 ns
Config:
Additional Information:
Found adjacency entry for
Adjacency :Active
MAC address 4c4e.35fc.fcd8

Result:
input-interface: INSIDE(vr
input-status: up
input-line-status: up
output-interface: OUTSIDE1
output-status: up
output-line-status: up
Action: allow
Time Taken: 825100 ns

```

Testen met echt verkeer

Configureer pakketopname met een spoor:

```

firepower# capture CAPI trace interface INSIDE match ip host 192.168.2.1 host 198.51.100.5
firepower# capture CAP01 trace interface OUTSIDE1 match ip host 192.168.2.1 host 198.51.100.5
firepower# capture CAP02 trace interface OUTSIDE2 match ip host 192.168.2.1 host 198.51.100.5

```

```

Router1# telnet 198.51.100.5 /vrf VRF-101 /source-interface lo2
Trying 198.51.100.5 ... Open

```

De opname laat zien:

```

firepower# show capture
capture CAPI type raw-data trace interface INSIDE [Capturing - 4389 bytes]
match ip host 192.168.2.1 host 198.51.100.5
capture CAP01 type raw-data trace interface OUTSIDE1 [Capturing - 4389 bytes]
match ip host 192.168.2.1 host 198.51.100.5
capture CAP02 type raw-data trace interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.2.1 host 198.51.100.5

```

Overtrek van het TCP/SYN-pakket:

```
firepower# show capture CAPI packet-number 1 trace
```

```
44 packets captured
```

```
1: 13:26:38.485585 802.1Q vlan#101 P0 192.168.2.1.49032 > 198.51.100.5.23: S 571152066:571152066(0) win  
...
```

```
Phase: 3
```

```
Type: SUBOPTIMAL-LOOKUP
```

```
Subtype: suboptimal next-hop
```

```
Result: ALLOW
```

```
Elapsed time: 13826 ns
```

```
Config:
```

```
Additional Information:
```

```
Input route lookup returned ifc OUTSIDE2 is not same as existing ifc OUTSIDE1
```

```
Phase: 4
```

```
Type: ECMP load balancing
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 1784 ns
```

```
Config:
```

```
Additional Information:
```

```
ECMP load balancing
```

```
Found next-hop 203.0.113.99 using egress ifc OUTSIDE1(vrfid:0)
```

```
Phase: 5
```

```
Type: PBR-LOOKUP
```

```
Subtype: policy-route
```

```
Result: ALLOW
```

```
Elapsed time: 446 ns
```

```
Config:
```

```
route-map FMC_GENERATED_PBR_1649228271478 permit 5
```

```
match ip address ACL_PBR
```

```
set adaptive-interface cost OUTSIDE1
```

```
Additional Information:
```

```
Matched route-map FMC_GENERATED_PBR_1649228271478, sequence 5, permit
```

```
Found next-hop 203.0.113.99 using egress ifc OUTSIDE1
```

```
...
```

```
Phase: 15
```

```
Type: ADJACENCY-LOOKUP
```

```
Subtype: Resolve Nexthop IP address to MAC
```

```
Result: ALLOW
```

```
Elapsed time: 4906 ns
```

```
Config:
```

```
Additional Information:
```

```
Found adjacency entry for Next-hop 203.0.113.99 on interface OUTSIDE1
```

```
Adjacency :Active
```

```
MAC address 4c4e.35fc.fcd8 hits 348 reference 2
```

```
...
```

```
Result:
```

```
input-interface: INSIDE(vrfid:0)
```

```
input-status: up
```

```
input-line-status: up
output-interface: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 222106 ns
```

De ASP PBR-tabel toont de beleidshit tellingen:

```
firepower# show asp table classify domain pbr
```

Input Table

```
in id=0x1505f26d3420, priority=2147483642, domain=pbr, deny=false
hits=7, user_data=0x1505f26e7590, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.2.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=198.51.100.5, mask=255.255.255.255, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=INSIDE(vrfid:0), output_ifc=any
```

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never

Opmerking: de packet-tracer verhoogt ook de hit teller.

PBR-debug

Waarschuwing: in een productieomgeving kan de debug veel berichten genereren.

Schakel deze debug in:

```
firepower# debug policy-route
debug policy-route enabled at level 1
```

Verzend echt verkeer:

```
Router1# telnet 198.51.100.5 /vrf VRF-101 /source-interface lo2
Trying 198.51.100.5 ... Open
```

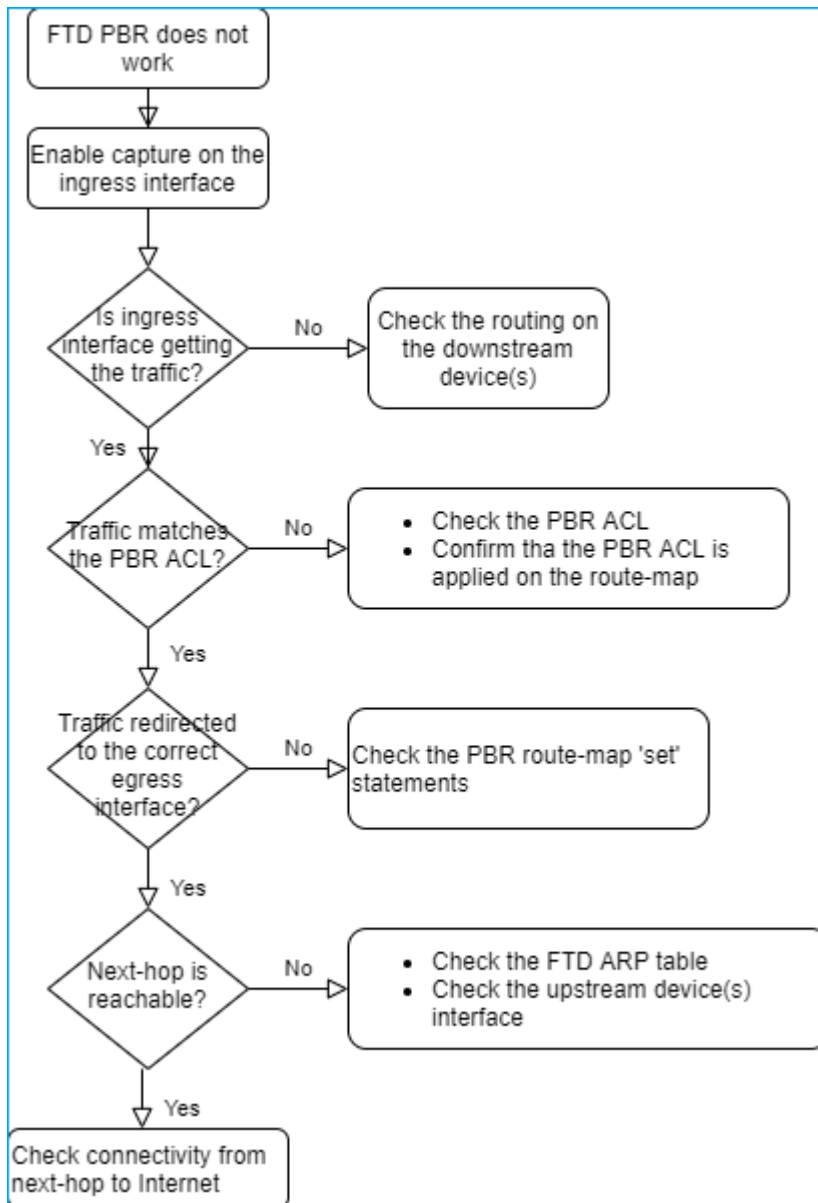
Het debug toont:

firepower#

```
pbr: policy based route lookup called for 192.168.2.1/32 to 198.51.100.5/23 proto 6 sub_proto 0 received
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1649228271478, sequence 5, permit; proceed with policy routing
pbr: policy based routing applied; egress_ifc = OUTSIDE1 : next_hop = 203.0.113.99
```

Opmerking: Packet-tracer genereert ook een debug-uitvoer.

Dit stroomschema kan worden gebruikt voor probleemoplossing bij PBR:



Samenvatting van PBR-opdrachten

Zo verifieert u de configuratie:

```
show run route-map
show run interface
```

Als SLA Monitor ook met PBR wordt gebruikt:

```
show run sla monitor
show run track
```

U verifieert de bewerking als volgt:

```
show route-map
packet-tracer
capture w/trace (for example, capture CAPI interface INSIDE trace match ip host 192.168.0.1 host 203.0.113.1)
ASP drop capture (for example, capture ASP type asp-drop all)
show asp table classify domain pbr
show log
show arp
```

Als SLA Monitor ook met PBR wordt gebruikt:

```
show sla monitor operational-state
show sla monitor configuration
show track
```

Zo debugt u PBR:

```
debug policy-route
show asp drop
```

Case 4 - Forwarding op basis van Global Routing Lookup

Na de verbinding lookup, NAT lookup, en PBR, het laatste punt dat wordt gecontroleerd om de uitgangsinterface te bepalen is de Globale Verpletterende lijst.

Routing-tabelverificatie

Laat ons een FTD routingstabel output onderzoeken:

```

firepower# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

C      192.0.2.0 255.255.255.0 is directly connected, OUTSIDE2
L      192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
C      192.168.0.0 255.255.255.0 is directly connected, INSIDE
L      192.168.0.1 255.255.255.255 is directly connected, INSIDE
O      192.168.1.1 255.255.255.255
O      192.168.2.1 255.255.255.255
O      [110/11] via 192.168.0.99, 01:36:53, INSIDE
O      192.168.2.1 255.255.255.255
O      [110/11] via 192.168.0.99, 01:36:53, INSIDE
S      198.51.100.0 255.255.255.248 [1/0] via 192.0.2.99, OUTSIDE2
D      198.51.100.8 255.255.255.248
D      [90/128512] via 192.0.2.99, 15:13:23, OUTSIDE2
D      198.51.100.16 255.255.255.248
D      [90/128512] via 192.0.2.99, 15:13:23, OUTSIDE2
B      198.51.100.24 255.255.255.248 [20/0] via 203.0.113.99, 15:13:26
B      198.51.100.32 255.255.255.248 [20/0] via 203.0.113.99, 15:13:26

```

Het belangrijkste doel van het routeringsproces is de volgende hop te vinden. De routeselectie is in deze volgorde:

1. Langste wedstrijd wint
2. Laagste AD (tussen verschillende routingprotocolbronnen)
3. Laagste metriek (voor het geval dat de routes van dezelfde bron worden geleerd - routeringsprotocol)

Hoe de routingstabel wordt bevolkt:

- IGP (R, D, EX, O, IA, N1, N2, E1, E2, i, su, L1, L2, ia, o)
- BGP (B)
- BGP InterVRF (BI)
- Statisch (S)
- Statische InterVRF (SI)
- Verbonden (C)
- lokale IP-adressen (L)
- VPN (V)
- Herdistributie
- Standaard

Om de routingstabel samenvatting te bekijken gebruik dit bevel:


```
<#root>
```

```
firepower#
```

```
show route summary
```

```
IP routing table maximum-paths is 8
```

Route Source	Networks	Subnets	Replicates	Overhead	Memory (bytes)
connected	0	8	0	704	2368
static	0	1	0	88	296
ospf 1	0	2	0	176	600
Intra-area: 2 Inter-area: 0 External-1: 0 External-2: 0					
NSSA External-1: 0 NSSA External-2: 0					
bgp 65000	0	2	0	176	592
External: 2 Internal: 0 Local: 0					
eigrp 1	0	2	0	216	592
internal	7				3112
Total	7	15	0	1360	7560

U kunt de updates van de routingstabel met dit bevel volgen:

```
<#root>
```

```
firepower#
```

```
debug ip routing
```

```
IP routing debugging is on
```

Bijvoorbeeld, is dit wat debug toont wanneer OSPF route 192.168.1.0/24 wordt verwijderd uit de globale routingstabel:

```
<#root>
```

```
firepower#
```

```
RT: ip_route_delete 192.168.1.0 255.255.255.0 via 192.0.2.99, INSIDE
```

```
ha_cluster_synced 0 routetype 0
```

```
RT: del 192.168.1.0 via 192.0.2.99, ospf metric [110/11]NP-route: Delete-Output 192.168.1.0/24 hop_count:1
```

```
RT: delete network route to 192.168.1.0 255.255.255.0NP-route: Delete-Output 192.168.1.0/24 hop_count:1
```

```
NP-route: Delete-Input 192.168.1.0/24 hop_count:1 Distance:110 Flags:0X0 , via 0.0.0.0, INSIDE
```

Als het terug wordt toegevoegd:

```
<#root>
```

```
firepower#
```

```
RT: NP-route: Add-Output 192.168.1.0/24 hop_count:1 , via 192.0.2.99, INSIDE
```

NP-route: Add-Input 192.168.1.0/24 hop_count:1 Distance:110 Flags:0X0 , via 192.0.2.99, INSIDE

Null0-interface

De interface van Null0 kan worden gebruikt om ongewenst verkeer te laten vallen. Deze daling heeft minder prestatieeffect dan de daling in het verkeer met een ACL-regel (Access Control Policy).

Vereiste

Configureer een Null0-route voor de 198.51.100.4/32-host.

Oplossing

The screenshot shows the Cisco Firepower 4140 Threat Defense configuration interface for device FTD4100-1. The 'Routing' tab is active. On the left, the 'Manage Virtual Routers' sidebar has 'Static Route' selected under the 'IPv6' section, marked with a red '1'. The main area displays a table of routes:

Network	Interface
IPv4 Routes	
net_198.51.100.0_29bits	OUTSIDE1
net_198.51.100.0_29bits	OUTSIDE2
IPv6 Routes	

On the right, the 'Add Static Route Configuration' dialog is open. The 'Type' is set to 'IPv4'. The 'Interface*' dropdown is set to 'Null0', marked with a red '2'. The 'Available Network' search box contains 'host_198.51.100.4', and the selected result 'host_198.51.100.4' is highlighted, marked with a red '3'. The 'Gateway*' field is empty.

Opslaan en implementeren.

Verificatie:

```
<#root>
```

```
firepower#
```

```
show run route
```

```
route OUTSIDE2 198.51.100.0 255.255.255.248 192.0.2.99 1
route OUTSIDE1 198.51.100.0 255.255.255.248 203.0.113.99 200
```

```
route Null0 198.51.100.4 255.255.255.255 1
```

```
<#root>
```

```
firepower#
```

```
show route | include 198.51.100.4
```

```
S 198.51.100.4 255.255.255.255 [1/0] is directly connected, Null0
```

Probeer toegang te krijgen tot de externe host:

```
<#root>
```

```
Router1#
```

```
ping vrf VRF-101 198.51.100.4
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 198.51.100.4, timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

De FTD-logboeken tonen:

```
<#root>
```

```
firepower#
```

```
show log | include 198.51.100.4
```

```
Apr 12 2022 12:35:28:
```

```
%FTD-6-110002: Failed to locate egress interface for ICMP from INSIDE:192.168.0.99/0 to 198.51.100.4/0
```

ASP druppels tonen:

```
<#root>
```

```
firepower#
```

```
show asp drop
```

Frame drop:

Equal Cost Multi-Path (ECMP)

Verkeerszones

- De ECMP Traffic Zone biedt een gebruiker de mogelijkheid om interfaces te groeperen (een ECMP Zone genoemd).
- Dit maakt ECMP-routing mogelijk en taakverdeling voor verkeer over meerdere interfaces.
- Wanneer interfaces zijn gekoppeld aan ECMP Traffic Zone, kan de gebruiker statische routers met gelijke kosten maken voor alle interfaces. Statische routes met gelijke kosten zijn routes naar hetzelfde doelnetwerk met dezelfde metrische waarde.

Vóór versie 7.1 ondersteunde Firepower Threat Defence ECMP-routing via FlexConfig-beleid. Vanaf de release 7.1 kunt u interfaces in verkeerszones groeperen en ECMP-routing configureren in Firepower Management Center.

EMCP is gedocumenteerd in: [ECMP](#)

In dit voorbeeld is er asymmetrische routing en wordt het retourverkeer gedropt:

```
<#root>
```

```
firepower#
```

```
show log
```

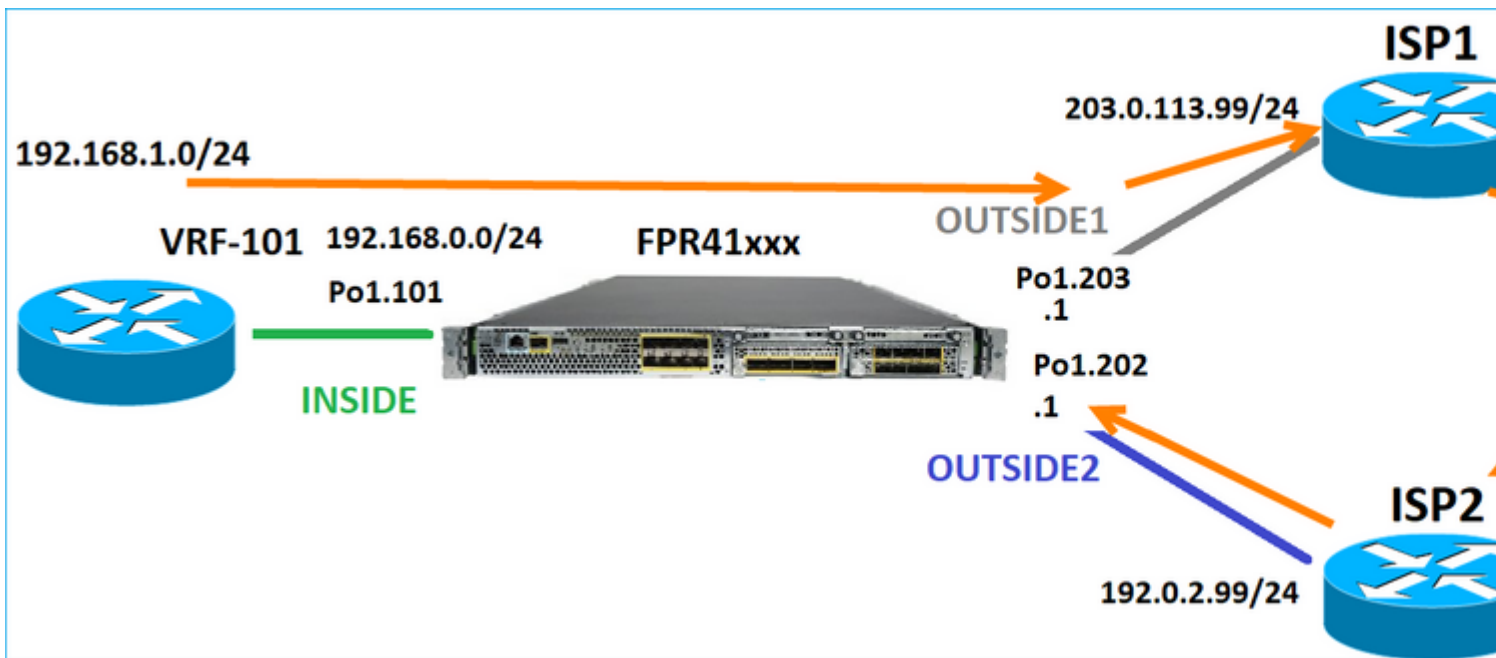
```
Apr 13 2022 07:20:48: %FTD-6-302013:
```

```
B
```

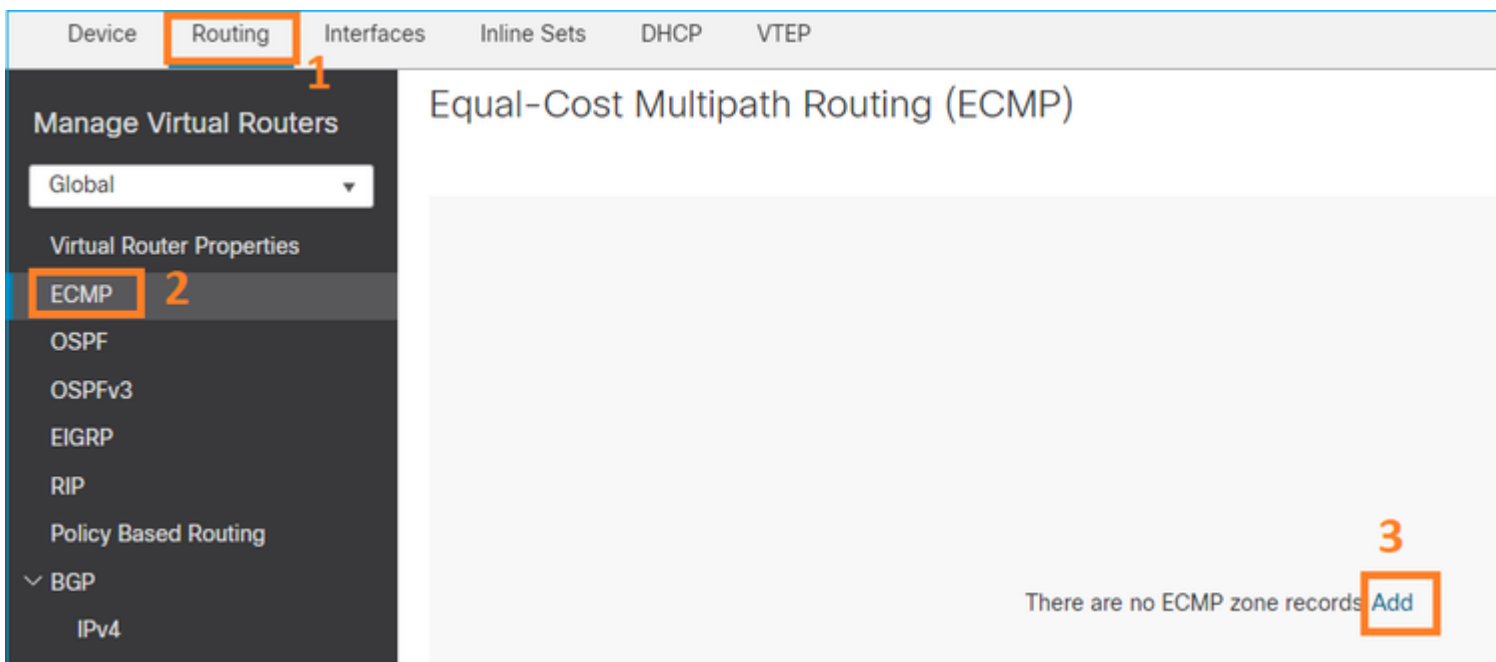
```
uilt inbound TCP connection 4046 for INSIDE:192.168.1.1/23943 (192.168.1.1/23943) to OUTSIDE:198.51.100.100/23
```

```
Apr 13 2022 07:20:48: %FTD-6-106015:
```

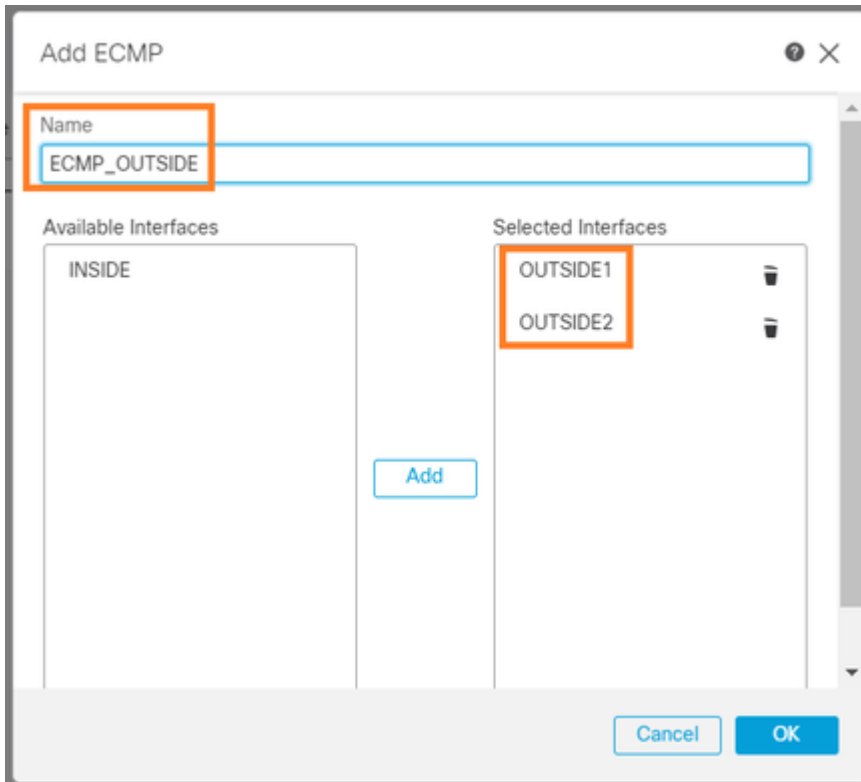
```
Deny TCP (no connection) from 198.51.100.100/23 to 192.168.1.1/23943 flags SYN ACK on interface OUTSIDE2
```



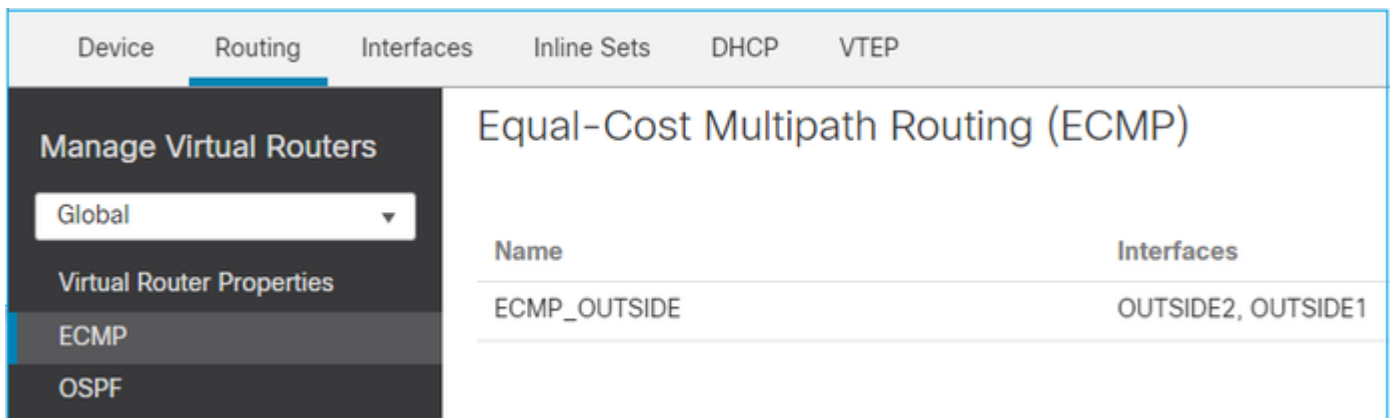
ECMP vanuit de FMC UI configureren:



Voeg de 2 interfaces in de ECMP-groep toe:



Het resultaat:



Opslaan en implementeren.

ECMP-zoneverificatie:

```
<#root>
```

```
firepower#
```

```
show run zone
```

```
zone ECMP_OUTSIDE ecmp
```

```
firepower#
```

```
show zone
```

Zone: ECMP_OUTSIDE ecmp

Security-level: 0

Zone member(s): 2

OUTSIDE1 Port-channel1.203

OUTSIDE2 Port-channel1.202

Interfaceverificatie:

<#root>

firepower#

show run int po1.202

```
!  
interface Port-channel1.202  
vlan 202  
nameif OUTSIDE2  
cts manual  
propagate sgt preserve-untag  
policy static sgt disabled trusted  
security-level 0
```

zone-member ECMP_OUTSIDE

ip address 192.0.2.1 255.255.255.0

firepower#

show run int po1.203

```
!  
interface Port-channel1.203  
vlan 203  
nameif OUTSIDE1  
cts manual  
propagate sgt preserve-untag  
policy static sgt disabled trusted  
security-level 0
```

zone-member ECMP_OUTSIDE

ip address 203.0.113.1 255.255.255.0

Nu, is het terugkeerverkeer toegestaan, en de verbinding is omhoog:

```
<#root>
```

```
Router1#
```

```
telnet 198.51.100.100 /vrf VRF-101 /source-interface lo1
```

```
Trying 198.51.100.100 ... Open
```

Capture on ISP1 interface toont het uitgaande verkeer:

```
<#root>
```

```
firepower#
```

```
show capture CAP1
```

```
5 packets captured
```

```
1: 10:03:52.620115 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: S 1782458734:1782458734(0)
2: 10:03:52.621992 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128
3: 10:03:52.622114 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128
4: 10:03:52.622465 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: P 1782458735:1782458753(18)
5: 10:03:52.622556 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128
```

Capture on ISP2 interface toont het retourverkeer:

```
<#root>
```

```
firepower#
```

```
show capture CAP2
```

```
6 packets captured
```

```
1: 10:03:52.621305 802.1Q vlan#202 P0 198.51.100.100.23 > 192.168.1.1.56199:
s
2000807245:2000807245(0)
ack
1782458735 win 64240 <mss 1460>
3: 10:03:52.623808 802.1Q vlan#202 P0 198.51.100.100.23 > 192.168.1.1.56199: . ack 1782458753 win 64222
```

FTD-beheerplan

Het FTD heeft 2 beheersplannen:

- Management0-interface - Biedt toegang tot het subsysteem Firepower
- LINA diagnostische interface - Toegang bieden tot FTD LINA subsysteem

Om de Management0 interface te configureren en te verifiëren, gebruikt u respectievelijk het configuratienetwerk en toont u netwerkopdrachten.

Aan de andere kant bieden de LINA-interfaces toegang tot de LINA zelf. De FTD-interfacegegevens in het FTD RIB kunnen worden beschouwd als lokale routes:

```
<#root>
firepower#
show route | include L

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
L 192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
L 192.168.0.1 255.255.255.255 is directly connected, INSIDE
L 203.0.113.1 255.255.255.255 is directly connected, OUTSIDE1
```

Op dezelfde manier kunnen ze worden gezien als identiteitsgegevens in de ASP-routeringstabel:

```
<#root>
firepower#
show asp table routing | include identity

in 169.254.1.1 255.255.255.255 identity
in
192.0.2.1 255.255.255.255 identity

in
203.0.113.1 255.255.255.255 identity

in
192.168.0.1 255.255.255.255 identity

in ff02::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff01:3 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff00:1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fe80::200:ff:fe01:3 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
out 0.0.0.0 0.0.0.0 via 0.0.0.0, identity
out :: :: via 0.0.0.0, identity
```

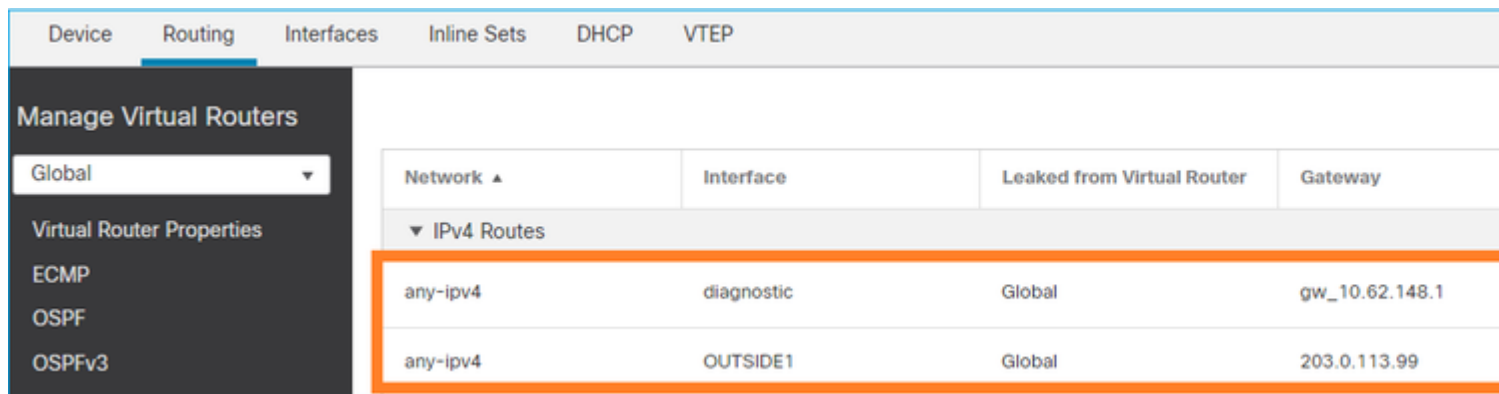
Hoofdpunt

Wanneer een pakket op FTD aankomt, en de bestemming IP één van de identiteit IPs aanpast, weet FTD dat het het pakket moet verbruiken.

FTD LINA diagnostische interfacerouting

FTD (als een ASA die post-9.5 code in werking stelt) handhaaft een VRF-achtige routingstabel voor om het even welke interface die als beheer-slechts wordt gevormd. Een voorbeeld van zo'n interface is de diagnostische interface.

Hoewel het FMC u (zonder ECMP) niet toestaat om 2 standaardroutes op 2 verschillende interfaces met dezelfde metriek te configureren, kunt u 1 standaardroute op een FTD-gegevensinterface en een andere standaardroute op de diagnostische interface configureren:



Network ▲	Interface	Leaked from Virtual Router	Gateway
▼ IPv4 Routes			
any-ipv4	diagnostic	Global	gw_10.62.148.1
any-ipv4	OUTSIDE1	Global	203.0.113.99

Het verkeer van het gegevensvliegtuig gebruikt de globale lijst standaardgateway, terwijl het verkeer van het beheervliegtuig het kenmerkende gebrek GW gebruikt:

```
<#root>
```

```
firepower#
```

```
show route management-only
```

Routing Table: mgmt-only

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

```
Gateway of last resort is 10.62.148.1 to network 0.0.0.0
```

```
s* 0.0.0.0 0.0.0.0 [1/0] via 10.62.148.1, diagnostic
```

De mondiale routingstabel voor gateway:

```
<#root>
```

```
firepower#
```

```
show route | include S\*|Gateway
```

```
Gateway of last resort is 203.0.113.99 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.99, OUTSIDE1
```

Wanneer u verkeer vanaf de FTD (van-de-box verkeer) verzendt, wordt de uitgaande interface geselecteerd op basis van:

1. Wereldwijde routingstabel
2. Alleen beheer voor routingstabel

U kunt de selectie van de uitgangsinterface overschrijven als u de uitgangsinterface handmatig specificeert.

Probeer de diagnostische interfacegateway te pingen. Als u de broninterface niet specificeert, pingelt ontbreekt omdat FTD eerst de globale routingstabel gebruikt die, in dit geval, het een standaardroute bevat. Als er geen route in de globale lijst is, doet FTD een routerraadpleging op de beheer-enige routingstabel:

```
<#root>
```

```
firepower#
```

```
ping 10.62.148.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.62.148.1, timeout is 2 seconds:
```

```
?????
```

```
Success rate is 0 percent (0/5)
```

```
firepower#
```

```
show capture CAP1 | include 10.62.148.1
```

```
1: 10:31:22.970607 802.1Q vlan#203 P0
```

```
203.0.113.1 > 10.62.148.1 icmp: echo request
```

```
2: 10:31:22.971431 802.1Q vlan#203 P0
```

```
10.1.1.2 > 203.0.113.1 icmp: host 10.62.148.1 unreachable
```

```
<#root>
```

```
firepower#
```

```
ping diagnostic 10.62.148.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.62.148.1, timeout is 2 seconds:  
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Het zelfde is van toepassing als u probeert om een dossier van LINA CLI met het exemplaarbevel te kopiëren.

Detectie van bidirectioneel doorsturen (BFD)

BFD-ondersteuning is toegevoegd op klassieke ASA versie 9.6 en alleen voor BGP-protocol: [Bidirectionele Forwarding Detection Routing](#)

FTD:

- BGP IPv4- en BGP IPv6-protocollen worden ondersteund (software 6.4).
- OSPFv2-, OSPFv3- en EIGRP-protocollen worden niet ondersteund.
- BFD voor statische routers wordt niet ondersteund.

Virtuele routers (VRF)

VRF-ondersteuning is toegevoegd in de 6.6-release. Controleer dit document voor meer informatie: [Configuratievoorbeelden voor virtuele routers](#)

Gerelateerde informatie

- [Statische FTD- en standaardrouters](#)

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.