

دي دهت دض ٽي امحلـا هـي جـوت ءـاطـخـا فـاشـكـتـسـأـ FirePOWER اـحـالـصـإـوـ

تـايـوـتـحـمـلـا

[قـمـدـقـمـلـا](#)

[قـيـسـاسـأـلـا تـابـلـطـتـمـلـا](#)

[تـابـلـطـتـمـلـا](#)

[قـمـدـخـتـسـمـلـا تـابـنـوـكـمـلـا](#)

[قـيـسـاسـأـتـامـوـلـعـمـ](#)

[هـنـجـهـيـجـوتـذـاعـاـتـايـلـا FTD](#)

[قـيـسـيـئـرـقـطـقـنـ](#)

[قـيـسـيـئـرـلـاـيـوـتـسـمـهـيـجـوتـكـولـسـ \(LINA\)](#)

[قـيـسـيـئـرـلـاـطـاقـنـلـا](#)

[قـيـسـيـئـرـلـاـمـعـبـيـثـرـتـ FTD](#)

[نـيـوـكـتـلـا](#)

[لـاصـتـالـانـعـثـحـبـلـاـيـلـاـاـدـانـتـسـهـيـجـوتـلـاـذـاعـاـ1ـقـلـاحـلـا](#)

[مـيـوـعـتـلـاـقـلـمـ](#)

[قـلـمـ Conn-holddown](#)

[لـحـبـلـاـيـلـاـاـدـانـتـسـهـيـجـوتـلـاـذـاعـاـ2ـقـلـاحـلـا NAT](#)

[لـحـبـلـاـيـلـاـيـلـعـمـيـاـقـلـاـهـيـجـوتـلـاـيـلـاـاـدـانـتـسـهـيـجـوتـلـاـذـاعـاـ3ـقـلـاحـلـا \(PBR\)](#)

[تـابـلـطـتـمـلـا](#)

[لـحـلـا](#)

[قـيـقـيـقـحـرـوـمـقـرـحـعـمـرـابـتـخـا](#)

[قـيـقـيـقـحـرـوـمـقـرـحـعـمـرـابـتـخـا PBR](#)

[قـيـقـيـقـحـرـوـمـقـرـحـعـمـرـابـتـخـا PBR](#)

[مـاءـعـلـاـهـيـجـوتـلـاـنـعـثـحـبـلـاـيـلـاـاـدـانـتـسـهـيـجـوتـلـاـذـاعـاـ4ـقـلـاحـلـا](#)

[قـهـجـاوـNull0](#)

[تـابـلـطـتـمـلـا](#)

[لـحـلـا](#)

[قـفـلـكـتـلـاـقـيـوـاسـتـمـقـدـدـعـتـمـتـارـاسـمـ \(ECMP\)](#)

[قـرـادـاـيـوـتـسـمـ FTD](#)

[قـيـسـيـئـرـلـاـقـطـقـنـلـا](#)

[قـيـصـيـخـشـتـلـاـقـهـجـاوـهـيـجـوتـ LINA FTD](#)

قـمـدـقـمـلـا

هـيـجـوتـذـاعـاـبـ"FTD"ـقـيـرـانـلـاـقـقـاطـلـاـدـيـدـهـتـدـضـعـافـدـلـاـ"ـمـاـيـقـقـيـفـيـكـدـنـتـسـمـلـاـاـذـهـفـصـيـ.ـفـلـتـخـمـهـيـجـوتـمـيـهـافـمـذـيـفـنـتـوـمـزـحـلـاـ.

قـيـسـاسـأـلـا تـابـلـطـتـمـلـا

تابل طتملا

- ئياس سالا ھيچو تلا ئفرعم

ۋەم دختسىمىلا تانوكىملا

ئيلاتلا ئيداملا تانوكىملا و جماربلا تارادصىلى دنتسىمىلا اذه يف ئەرداوەلا تامولۇملا دنتسىت:

- رادصىلا Cisco Firepower 41xx، 7.1.x دىدەتلا دض عافدىلا
- رادصىلا Firepower (FMC)، 7.1.x ۋەردى زىرىم

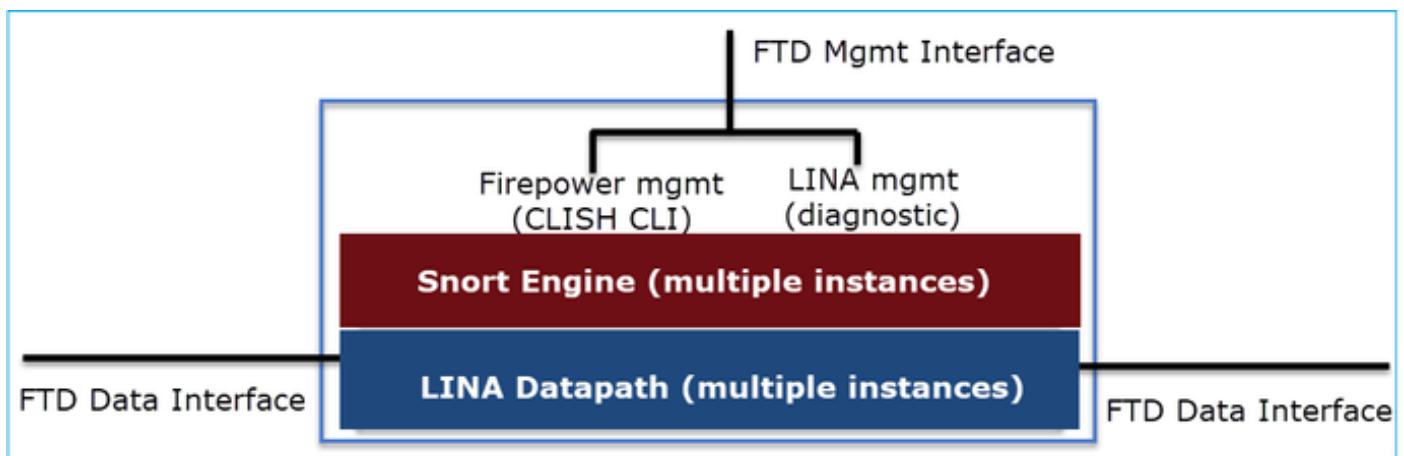
ئىچىم ئەلەم ئەيىپ يىف ئەردوچوملا ئەزەجألا نم دنتسىمىلا اذه يف ئەرداوەلا تامولۇملا ئاشنەمەت تنانك اذا. (يىچارتىف) حوسىم نىوكتىپ دنتسىمىلا اذه يف ئەم دختسىمىلا ئەزەجألا ئېمەج تأدب رەمأ يىل مەتەحمللا رېيىتەتلل كەمەف نم دكأتىف، لېغشتىلا دىق كەتكېبىش.

ئياس سالا تامولۇم

مۇز ھيچو تەداعى تايىلما

نېيىسىئر نېيەر ئەر دەحوم جمانرب ئەروص نع ئەرابع FTD:

- تانايىب كەرەم (LINA)
- كەرەم Snort



تانايىب ئوتسمىل نايىسىئرلا ناعزىللا امە FTD. و Snort Engine

ئيلاتلا ئەروصلارا صخلەت. ئەجداوەلا عضۇلىع FTD ل تانايىبلا ئوتسمىل ھيچو تەداعى ئەيل آدمەتىع ئەرسىلارا قىاف لاسىلا جمانرب" رىشنى عاضوا عم ئەفلىتەحمللا ئەجداوەلا عاضوا:

FTD Deployment and Interface Modes

Deployment Modes:

- Routed
- Transparent

from classic ASA

Interface Modes:

- Routed
- Switched (BVI)
- Passive
- Passive (ERSPAN)
- Inline Pair
- Inline Pair with tap

} from classic ASA

} from classic Firepower IPS

عوضى ادانتسا تانايبلالا يوتسم يف مزحلا هيجوت ةداعاب FTD موقعي فيك لودجلالا صخللي
هيلصفالا بسح هيجوتلا ةداعا تايلا آدرس. هجأولـا:

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

*: تالاحللا ضعب يف راسملالا نع ثحبلاـ فافـشـلا عـضـولـا يـفـ FTDـ مـوقـيـ

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.

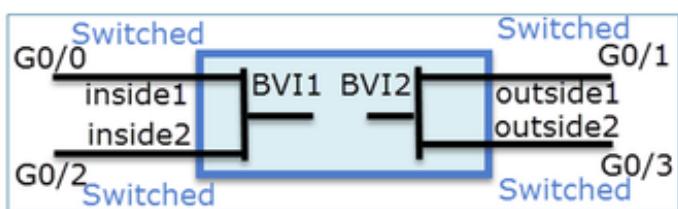
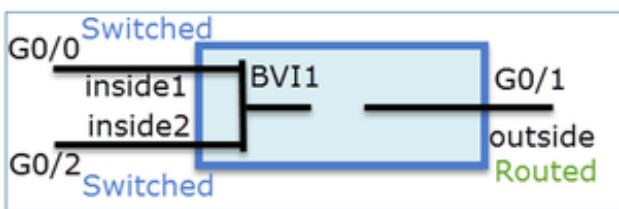


لیصافتلا نم دیزم ىلع لوصحلل [FMC](#) لیلد عجار.

لماكتمل هیجوتلا (FTD) ۋە رسلا قىاف لاسرا لا جمانرب معدي، 6.2.x رادىصا عم لاحلا وە امكى طېرلەو:

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



نم ققحتلا رماوا BVI:

Verification commands

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

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
```

ةيسيئر ةطقن

رملأا اذه ىلإ ٥مزحلا هيجوت ٤داع٤ دنتس٤ ، ٥هجومل٤ تاهجاولل ٤بسنلاب:

- لاصتا نع ثحبلا
- ب اضيأ فرع٤ ، ٤ياغ٤ (UN-NAT)
- (PBR) ٤سايسل٤ ٤لعم٤ هيجوتلا
- يمومعل٤ هيجوتلا ٤لودج٤ ثحب٤

ردصم نع اذام NAT؟

ماعلا هيجوتلا ثحب دعب ردصملا NAT نم ققحتلا متي.

٤هجومل٤ تاهجاولل ٤اضوىل٤ دنتس٤ اذه ٤يقب زكرت.

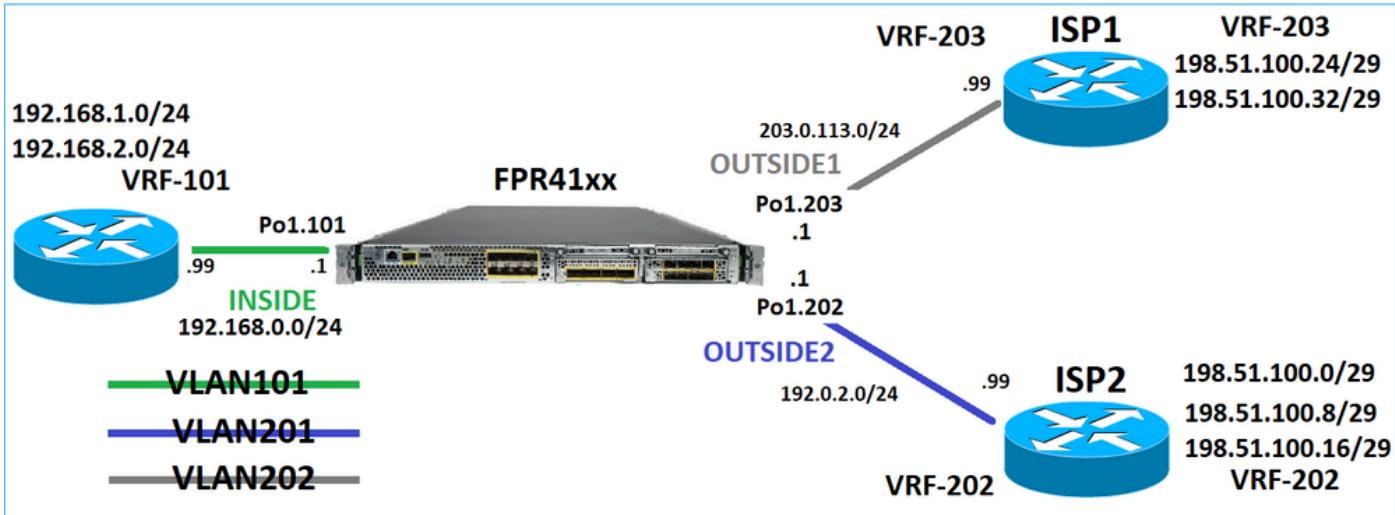
(LINA) تانايبل٤ ٤وتسم٤ هيجوت كولس

نيلحرم يف مزحلا هيجوت ٤داع٤ FTD LINA موقعي ٤هجومل٤ تاهجاولل ٤اضوىف:

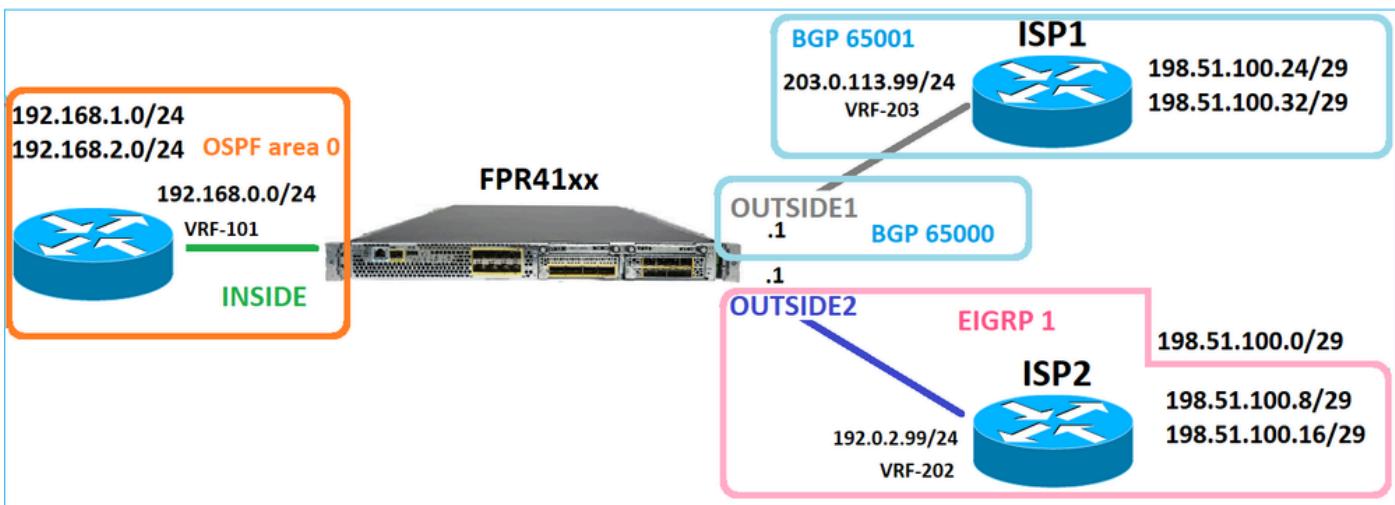
جورخل٤ تاهجاو ديدحت - 1 ٤لحرمل٤

٤يلاتل٤ ٤وطخل٤ ديدحت - 2 ٤لحرمل٤

لکيهل٤ اذه رابتعالا نيعب ذخ:



اذه هيجوت لا ميامصت و:



هيجوت نيوكت FTD:

```

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

```

مکاحتلا یوتس م - FTD (RIB) - هیجوت تامولع م ڈعاق:

```

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

```

تانا یبل یوتس م - قفاوت مل ا FTD (ASP) ل عیرس لان ام ال راس م ھیجوت لودج:

```

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 fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff01:3 fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff00:1 fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fe80::200:ff:fe01:3 fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fd00:0:0:1::1 fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity

```

```

in fd00:0:0:1:: fffff: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 fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff nlp_int_tap
out fd00:0:0:1:: fffff: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

```

ةيسيئرلا طاقنلا

(جورخلا) جورخلا ةهجاو ASA - فيكتلل لباقلا نامألا زاهجل ةهباسم ةقيرطب) FTD ددحي لواجي ،ددحملا نراقلل مث ASP. هيجوت لودجل 'in' تالاخدا لىا رظنني هناف ،كلذل) ڦمزحلل ىلع هيجوت لودجل 'out' تالاخدا لىا رظنني هناف ،كلذل) ةيلاتلا ڦوطخلاءا ىلع روشعلا لاثملما ليبس:

```

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 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

```

تقمـلـا ARP نـيـزـخـتـ ةـرـكـادـنـم LINA قـقـحـتـيـ، اـهـلـحـ مـتـ يـتـلـاـ ةـيـلـاتـلـاـ ةـوـطـخـلـلـ ةـبـسـنـلـابـ، اـرـيـخـأـوـ حـلـاصـ رـواـجـتـلـ

ةـيـلـمـعـلـاـ هـذـهـ مـزـحـلـاـ عـبـتـتـلـ FTD ةـادـأـ دـكـوـتـ:

```
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

```

مکحتلایوتس میف رهظی امک لوج FTD ARP:

```

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

```

رارق ضرفل ARP:

```

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

```

تانا يابلا ىوتسم يف رهظي امك لوج FTD ARP:

```

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

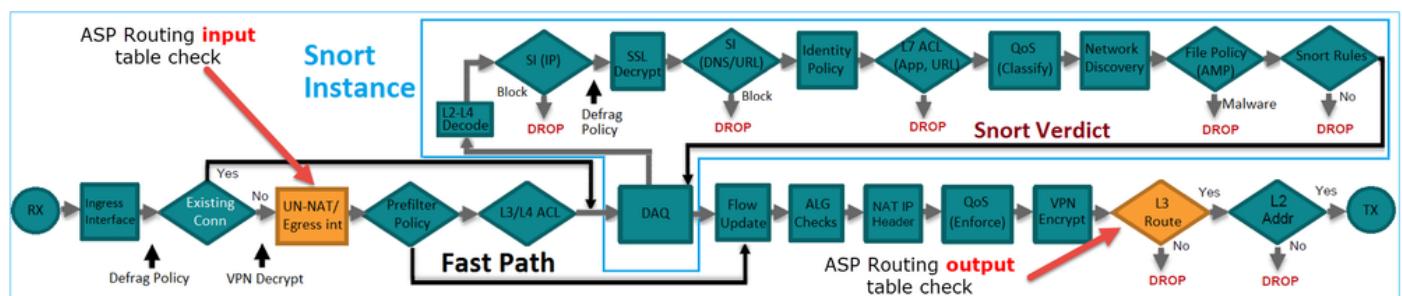
Context: single_vf, Interface: identity
:: Active 0000.0000.0000 hits 0 reference 0
0.0.0.0 Active 0000.0000.0000 hits 848 reference 0

Last clearing of hits counters: Never

```

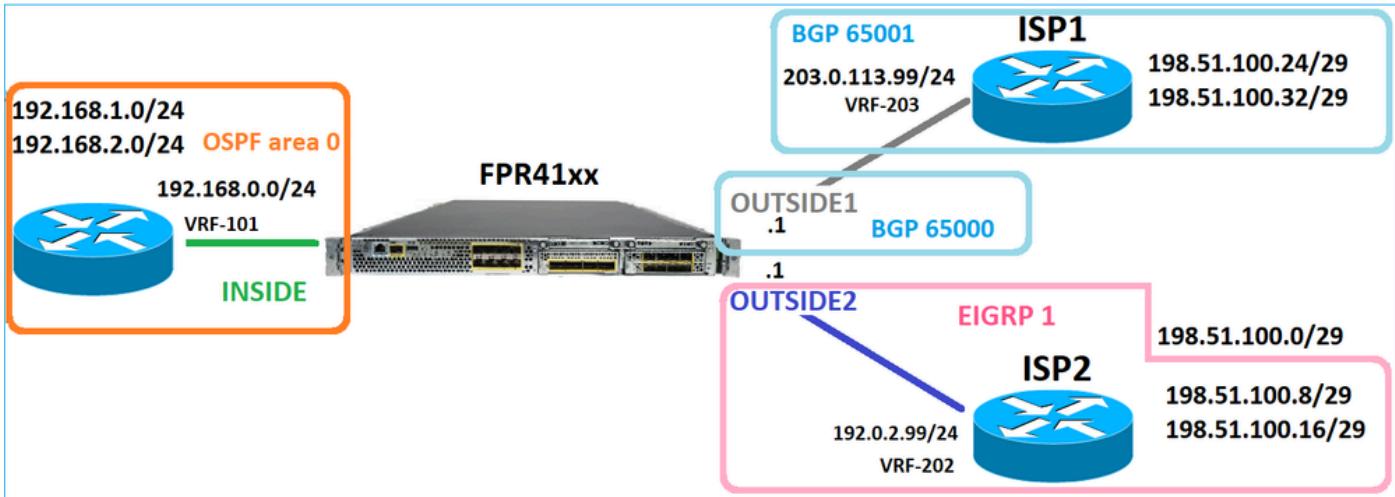
تايلمع بيترت FTD

جاخال او لاخدلل ASP هي جوت تاصوفف عاجن اكم و تاي لمعلاب يترت ةروصل اضرعات:



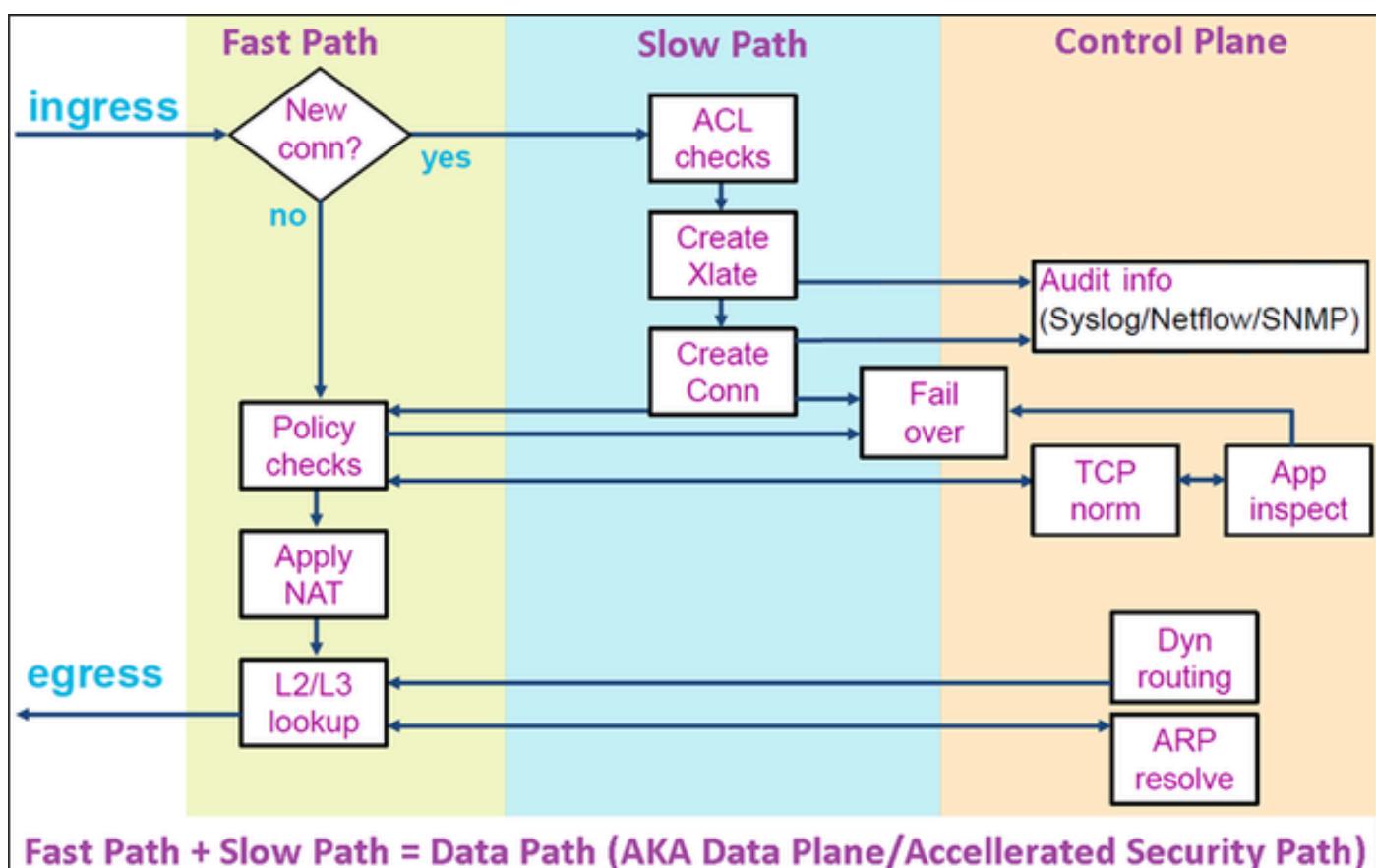
نيوك تلا

لاصتالا نع ثحبلا ىلإ ادانتسا هي جوتلا ١ - ةلاحلا



وہ یہ ملے کر جمل یسیئرلا نوکملا ناف، اقبسم ڈراش الا تمت امک و فورع مل (DataPath) نوکتی، کل ذیل عوامل (زاہجلا یون ددع یل ادانتسا ڈدعتم تالیثم) اپنی راسم نم (ASP) - عیرسلا نامآل راسم مساب اضی:

1. عیرسلا راسملا علمب موقی) دی دج لاصتا عاشن نع لوؤسم = عیطب راسم.
2. اأشنملا تالاصتا یل ایمتننت یتللا مزحل جلاعی = عیرسلا راسملا.



- مکھتلہ یوتسم تایوتھم show route و show arp لثم رم اوأ ضرعت.
- تایوتھم ASP (Datapath) لعلم رم اوأ ضرعت، یرخا ڈیحان نم لعفلاب هقیبھٹ متي ام وھو.

وہ جاویل عبۃتلا مادختساب طاقتل الا نیکم ت FTD Inside:

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

لآلخ نم لمع ةسلج حتف Telnet:

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

(ا) اجلت إلـا ةيـثالـث TCP ةـحـفـاصـم طـاقـتـلـا مـتـيـ) لـاصـتـالـا ةـيـادـبـ نـم مـزـحـلـا رـوـصـ رـهـظـاتـ:

```
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) w  
2: 10:50:38.408929 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: S 1412677784:1412677784(0) a  
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) a  
9: 10:50:38.413140 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: P 1306692157:1306692166(9) a  
10: 10:50:38.414071 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: . 1412677797:1412678322(525)  
...
```

لـماـشـ صـحـفـوـ، رـمـمـ عـيـطـبـ لـاـلـخـ نـمـ طـبـرـ اـذـهـ رـمـيـ) TCP SYNـ) لـىـلـوـلـاـ ةـمـزـحـلـاـ عـبـتـتـ
ـةـلـاحـلـاـ هـذـهـ يـفـ مـتـيـ دـشـحـتـ:

```
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, 13_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#

```

طشن لاصتا قباطت يتلا ةمزحلا . قفتلسا فن نم يرخأ لخدم ةمزح عبtt:

```
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, 13_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#
```

میوعلما ۋەلەم

ۋەلەكشەملا

ةصاخ) لجألا ۋەلەيوط UDP تالاصلتىغا ئاشنالى تىقۇملا راسملاراقتسا مدعى دۇي ناكىمى بولطملا نم رىشكى ئەفلىخ ئەلخ نم FTD تاھجاو ئەلخ نم (ۋەلەيەپلاب.

لەحلە

ةمېقلانىع ئەفلىخ ئەمېق ئىلەلەملىلىن مىزلا لىصاپلا نىيىعتبىمۇ، كىلذ حالسىل ئەلطۇملا ئىضارت فالا:



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

UCAPI/CC Compliance

Console Timeout*	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}

رم أوألا عجم نم:

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.

قس لج نم ليمح تل ا ةداعا دعب UDP تالاصت ا لشف في : ئلاحلا ئسارد عجار ، ليصافت لا نم ديزمل CiscoLive BRKSEC-3020:

Floating Connection Timeout

- The “bad” connection never times out since the UDP traffic is constantly flowing
 - TCP is stateful, so the connection would terminate and re-establish on its own
 - ASA needs to tear the original connection down when the corresponding route changes
 - ASA 8.4(2)+ introduces **timeout floating-conn** to accomplish this goal

```
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-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 9:00:00 absolute uauth 0:01:00 inactivity
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 conn entry for termination in **1 minute** if a matching packet yields a different egress interface on route lookup

ةلهم Conn-holddown

ةلكلش ملأ

تباث لاصتا قباطت رورملأا ةكرح نكلو، (هتلإا مرت) راسملأا طبهـي.

لحـلا

لـكـشـبـ ظـيـمـلـاـ نـيـكـمـتـ مـتـيـ ASA 9.6.2ـ ئـلـعـ conn-holddownـ مـنـ مـنـيـ فـاضـاـ تـمـتـ FMCـ وـأـ مـدـخـتـسـمـ ةـهـجـ اوـ ةـطـسـ اوـبـ مـوعـ دـمـ رـيـغـ (7.1.xـ)ـ اـيـلـاحـ نـكـلـوـ،ـ يـضـارـتـ فـاـ ENHـ يـفـ نـيـوـكـتـلـلـ فـقـوـتـلـاـ ةـلـهـمـ رـفـوتـ مـدـعـ:ـ FMCـ

لمـلـيـلـدـ نـمـ ASA CLIـ:

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 igrp stale-route 0:01:10
```

نات جوتو لایا ادانتسا هیجوتلا ةداعی - 2 ئەلەحەل

تابلەتەملا

نات ئەلەخاندرا ئەدعاق:

- نات باش: عونلار
- لەخاد: رەدىصەملار ئەجەواو
- جىراخ: ئەجەولار ئەجەواولار
- يىلىصلار ئەجەولار: 192.168.1.1
- يىلىصلار ئەجەولار: 198.51.100.1
- مەجرىتمەلار رەدىصەملار: 192.168.1.1
- مەجرىتمەلار ئەجەولار: 198.51.100.1

لەحل

NAT_FTD4100-1											Show Warnings	Save	Cancel
Enter Description											Policy Assignments (1)		
Rules													
Filter by Device											X	Add Rule	
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options		
1	IN TO OUT	Static	INSIDE_FTD4100-1	OUTSIDE1_FTD4100	host_192.168.1.1	host_198.51.100.1		host_192.168.1.1	host_198.51.100.1		Dns false		

نات ئەلەخاندرا ئەدعاق FTD (CLI) رەماؤلار ئەجەوايلۇر ئەروش نەملا:

```
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
```

نەيەك ئەنۋەتىلۇرى:

```
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
```

جمانرب ىلع لمع ۋەسلىج أدبا Telnet نم 192.168.1.1 ىلإ 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
```

نراق 2 جراخ و 1 جراخ كرتى عىش ال نكلو، FTD ىلإ مزحلا لىصت:

```
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
```

ۆمزلالىوچ (صاخ لکشپ NAT (UN-NAT نأ) ۆلەرەملا حضوت TCP ماظن ۆمزلەنەتت ۆييلاتلا ۆوطخلانۇغىچىسى Outside1 ىلإ:

```
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) w
2: 11:23:01.179632 802.1Q vlan#101 P0 192.168.1.1.38790 > 198.51.100.1.23: S 1174675193:1174675193(0) w
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 412
...
```

```
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 ...
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

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

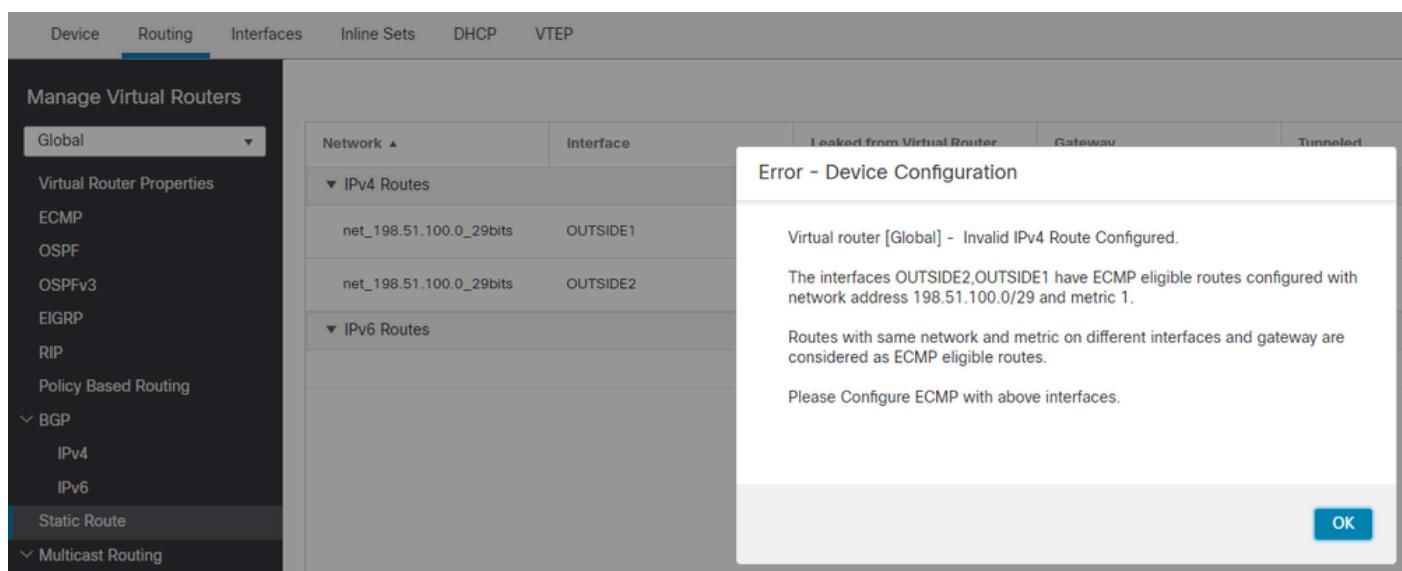
ةيـلـمـع ةـطـسـاـوب اـهـدـيـدـحـت مـت يـتـلـا جـوـرـخـلـا ةـهـجـاـوـنـأـلـمـأـلـا نـوـدـثـحـبـلـا يـنـعـي ،ةـلـاحـلـا هـذـهـ يـفـ لـاخـدا لـوـدـجـ يـفـ ةـدـدـحـمـلـا جـوـرـخـلـا ةـهـجـاـوـنـعـ فـلـتـخـتـ (1ـجـراـخـ) ASP:

```
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
```

ةـيـجـرـاخـلـا ةـهـجـاـوـلـا ىـلـعـ مـئـاعـ يـكـيـتـاتـسـا نـكـاسـ رـاـسـمـ ةـفـاضـاـ وـهـ لـمـتـحـمـلـا لـيـدـبـلـا لـحـلـا:

```
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
```

أـطـخـلـا اـذـهـ رـهـظـيـ ،لـعـفـلـاب دـوـجـوـمـلـا سـاـيـقـمـلـا سـفـنـبـ تـبـاـثـ رـاـسـمـ ةـفـاضـاـ تـلـواـحـ اـذـاـ: ظـاحـالـمـ



ةـيـجـوـتـلـا لـوـدـجـ يـفـ 255 ةـفـاسـمـلـا سـاـيـقـمـلـا مـئـاعـلـا رـاـسـمـلـا تـيـبـثـتـ مـتـيـ مـلـ: ظـاحـالـمـ

لـا لـالـخـ نـمـ تـلـسـرـأـ طـبـرـكـانـهـ نـأـ تـلـواـحـ: FTD:

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

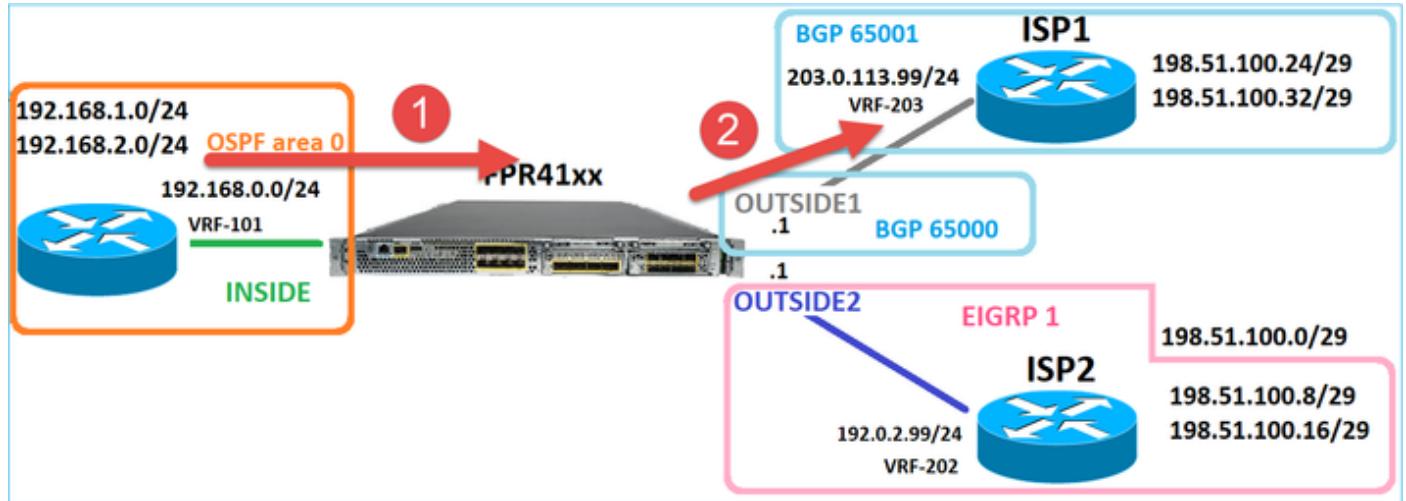
```
firepower# show capture
capture CAPI type raw-data trace detail interface INSIDE [Capturing - 156 bytes]
```

```

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

```

ببسـبـ ISP2 نـم الـدـبـ (1ـجـرـاـخـ) اـهـيـجـوـتـ دـاعـ مـتـ مـزـحـلـاـ نـأـقـمـزـ حـضـوـيـ عـبـتـ حـضـوـيـ نـعـ ثـحـبـلـاـ NAT:



```
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) w
...
```

```
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#
```

جورخ لـا تـاهـجـاـوـاـلـكـوـلـخـادـلـاـىـلـعـقـصـومـمـزـحـكـيـوـ،ـمـامـتـهـاـلـلـرـيـثـمـلـاـنـمـوـ:

```
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) w  
2: 09:03:05.176565 802.1Q vlan#101 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3031010184:3031010184(0) w
```

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) w  
2: 09:03:02.774557 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) w  
3: 09:03:05.176702 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) w  
4: 09:03:05.176870 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) w
```

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  
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  
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  
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) a
```

تـاهـجـاـوـاـلـكـوـلـخـادـلـاـىـلـعـقـصـومـمـزـحـكـيـوـ،ـمـامـتـهـاـلـلـرـيـثـمـلـاـنـمـوـ OUTSIDE1
وـOUTSIDE2ـمـزـحـلـاـرـاسـمـ:

```
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
```

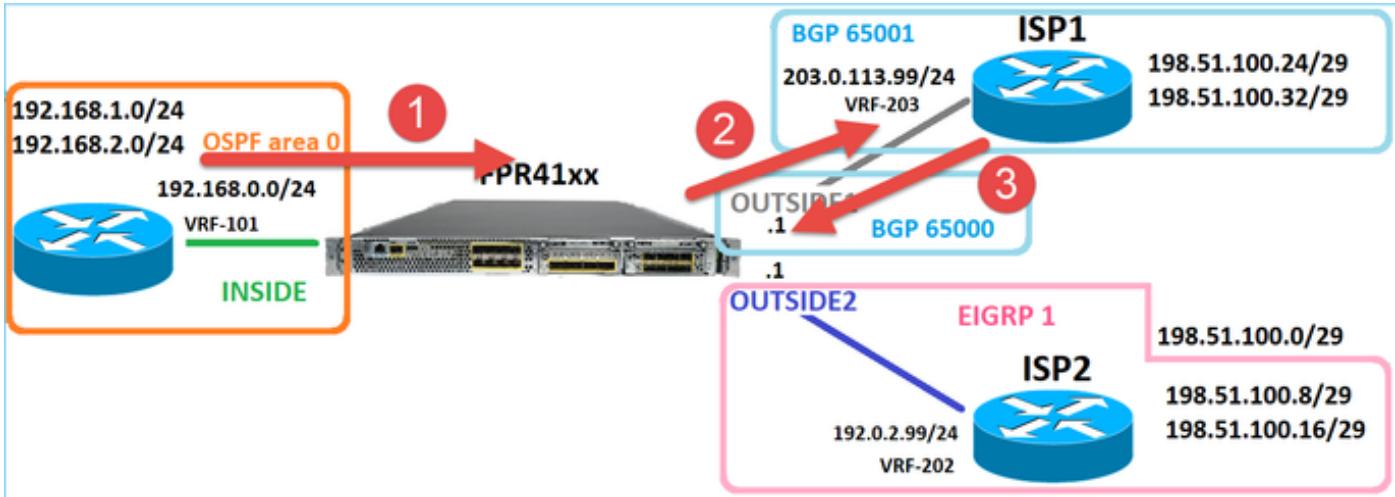
```
3: 09:03:05.176702 00be.75f6.1dae 4c4e.35fc.fcd8 0x8100 Length: 62
```

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

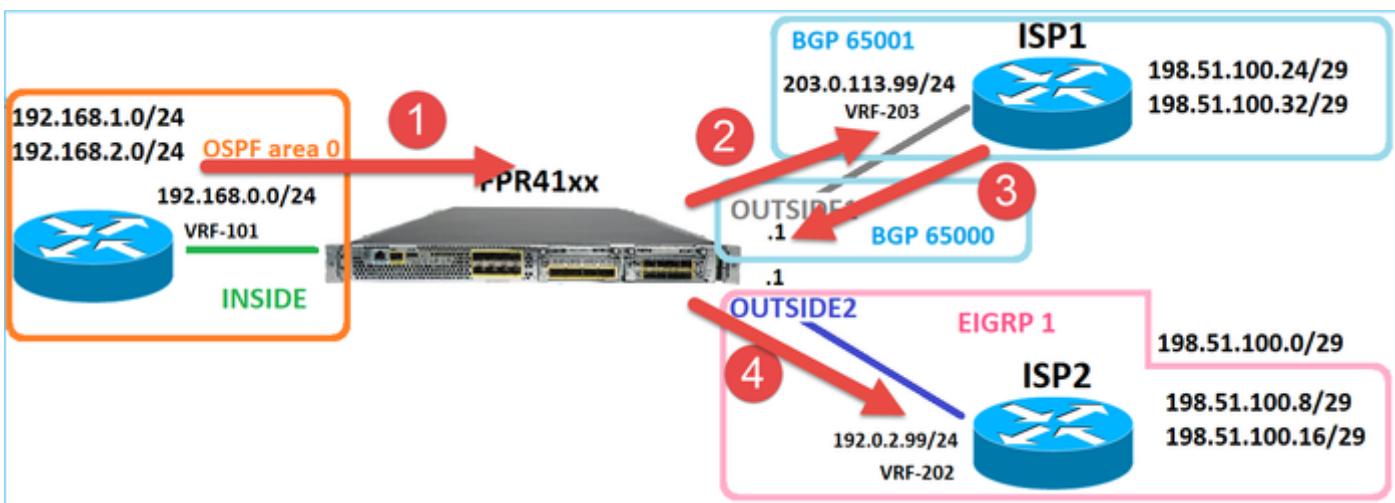
```
4: 09:03:05.176870 4c4e.35fc.fcd8 00be.75f6.1dae 0x8100 Length: 62
```

```
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



لودج نع ثحبلاب ببسن OUTSIDE2 ڦڌڳا هي جو تلا ڦڌڳا هي جو تلا عبٽت رهڙي: ماعلا هي جو تلا:



```
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) w
```

```
...
```

```
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)
```

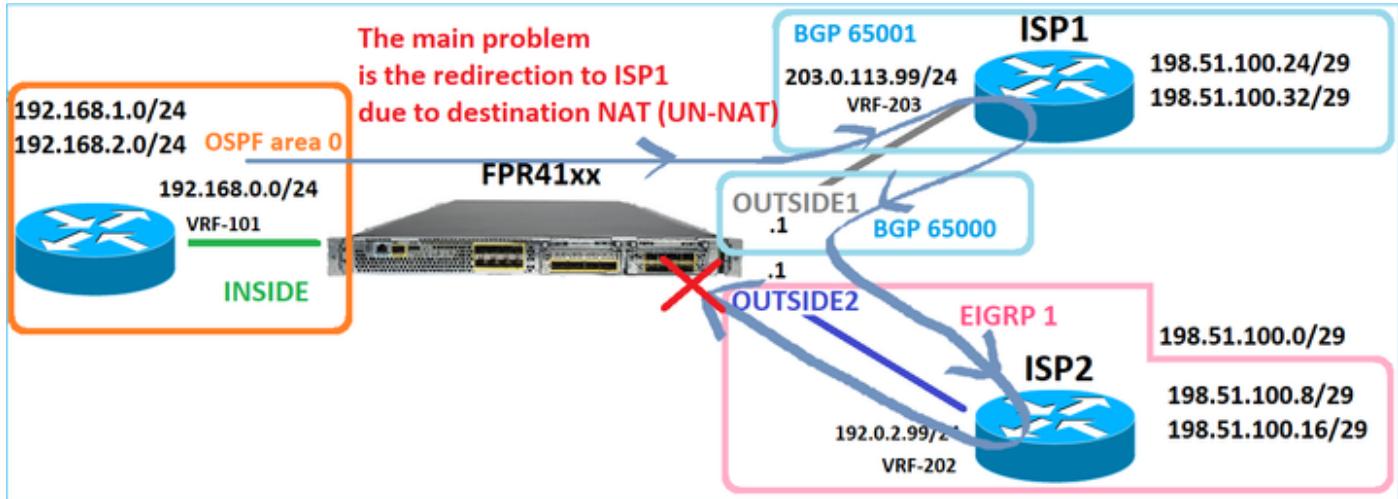
```
Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1338 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 0 reference 1
```

...

```
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#
```

قباط اهنأ ISP1 لى ISP2 هذه هي جوت ةداعاً متت نكلو، (SYN/ACK) درلا طاس او ب ةمزلجا طاقسا متي. أشنملالا لاصتا لـ ASP: جورخ لودج يف يناثل



```
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
```

3 - ۋەلەخىلا (PBR) ئىلۇم ئاپلىقلا ھېجوتلا ئىلإ ادانتسا ھېجوتلا ۋەدائعى

نأ نكىمى يىذلا يىلاتلا رصىنعلا وھ PBR نوکىي، ۋەھجولى NAT ۋەھجۇرلا قىفتالا قىفدىت ۋەھجۇر دىعېب قس اىسلىا ئىلإ دەنتىسمىللا ھېجوتلا يىف PBR قىيىت مەتى جەخەملە ۋەھج او دىدەت ئىلۇر رەتھۇيى.

ھېجوتلا اذەب ۋەيارد ئىلۇن نوکت نأ مەھمەلە نم، ئىلۇن ئەپسەنلاب كنكمى لازىي ال 7.1. لېق FTD تارادىصىل FMC يىف PBR نوکتلىك FlexConfig مادختىسى مەت ئەل، لۇخدىلا ۋەھج اول ئەپسەنلاب، كەلذۇمۇ تارادىصىل ئەھەمچى يىف PBR نوکتلىك FlexConfig مادختىسى ئەل، ۋەھج ئىلإ دەنتىسمىللا ھېجوتلا ۋەھجۇرلا ئەھەمچى يىف PBR نوکتلىك FlexConfig و FMC ئەل، ۋەھج ئىلإ دەنتىسمىللا ھېجوتلا ۋەھجۇرلا ئەھەمچى يىف PBR نوکتلىك FlexConfig.

ئىلإ رېشىي 198.51.100.0/24 وھن قىيرط ھىدل FTD نەف، ھەزەر ئەپسارد يىف ISP2:

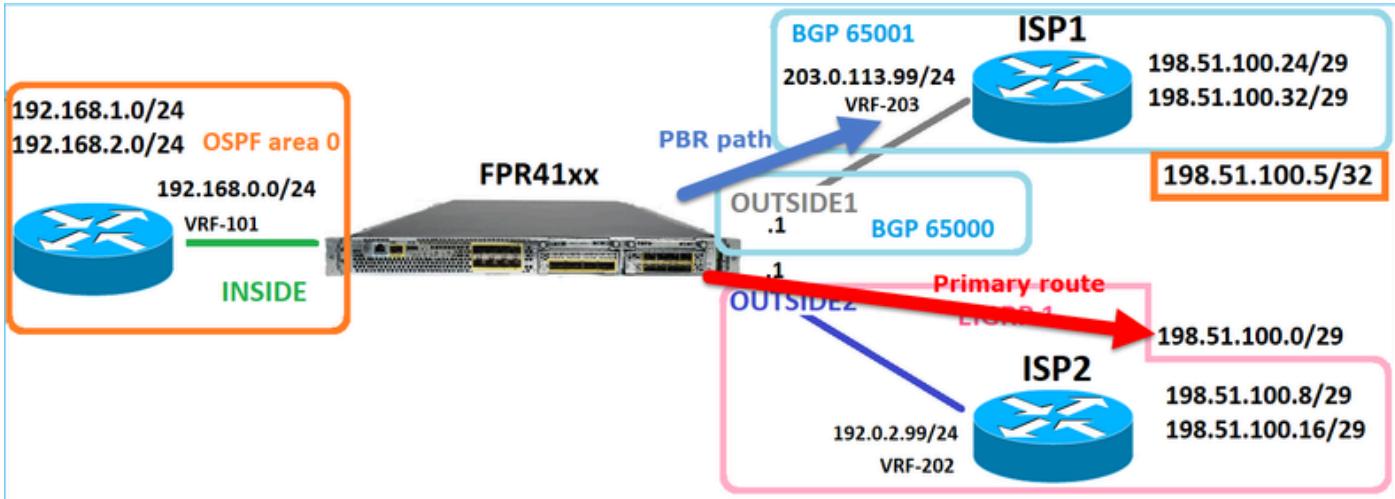
```
firepower# show route | begin Gate
Gateway of last resort is not set

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
0 192.168.1.1 255.255.255.255 [110/11] via 192.168.0.99, 5d01h, INSIDE
0 192.168.2.1 255.255.255.255 [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
```

تەبلىغىملىك

صىئاصخلە ھەزەر ئەپسارد PBR ئەپسارد نوکت:

- ISP1 ئىلإ 198.51.100.5 ئىلإ ۋەھجۇرمىللا IP 192.168.2.0/24 نم رورمەلە ۋەھج لاسرا بىچىي ۋەھج او خالا رداشمەلە مەدختىست نأ بىچىي امنىيپ (203.0.113.99) Outside2.



لحل

نويوكتل 7.1، لبقو ام تارادصا يف

ىلع) ۋەرەپەرەلە رورملا ۋەكەن قېباتەت ئەسەرمەن (ACL) لوصۇلما يف مەكتەپ ئەشىناب مەق. 1. لاثمەلە لېپس PBR_ACL).

يىف اهۋاشنامەت يىتلە (ACL) لوصۇلما يف مەكتەپ قېباتەت راسىم ئەطىرخ ئاشىناب مەق. 2. ۋەبولطمەلە ئىلاتلە ۋەوطخىلە نىيۇتۇ، 1. ۋەوطخىلە راسىملا ئەطىرخ مادختساب لۇخدىلە ۋەجاوىلىع PBR نىكمىي يىذلە FlexConfig نىئاك ئاشىناب مەق.

3. ۋەوطخىلە يىف اهۋاشنامەت يىتلە 2.

كىنکەمىي وأ 7.1، لبقو ام ئەقىرەت مادختساب PBR نىويوكت كىنکەمىي ، 7.1 دىب ام تارادصا يف

ھىجوتلە مىسىق > زاھىجىلە نەمىزدىي دىدەجىلە ئەسايىسلە ىلىع مەئاقلە ھىجوتلە رايىخ مادختسا:

ىلع) ۋەرەپەرەلە رورملا ۋەكەن قېباتەت ئەسەرمەن (ACL) لوصۇلما يف مەكتەپ ئەشىناب مەق. 1. لاثمەلە لېپس PBR_ACL).

2. دەحۋو PBR ئەسايىس فەضىأ.

3. ۋەقباطىمەلە رورملا ۋەكەن

لۇخدىلە ۋەجاوىب

ئىلاتلە ۋەوطخىلە - ج

(ۋەدبىج ئەقىرەت) PBR نىويوكت

ۋەقباطىمەلە رورملا ۋەكەن لوصۇلە ئەشىناب دىدەجىت - 1 ۋەوطخىلە.

The screenshot shows the Firewall Management Center interface under Object Management. The 'Objects' tab is selected. In the left sidebar, 'Access List' is expanded, and 'Extended' is selected, indicated by a red box labeled '2'. In the main pane, an 'Edit Extended Access List Object' window is open. It shows a table with one entry. The table columns are Sequence, Action, Source, Source Port, Destination, Destination Port, and Application. The entry is: Sequence 1, Action Allow, Source 192.168.2.0/24, Destination 198.51.100.5, and Application Any. A red box labeled '3' highlights the 'Source' column.

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

ةس اي س ةفاضا - 2 ةوطخل

ةس اي س لى دنتس م هيجوت > هيجوت رتخأ FTD. زاهج ررح و ةزهج ألا ةرادا > ةزهج ألا لى لقتنا. ةفاضا ددح، ةس اي س لى دنتس م لى دنتس ملا هيجوت لى دل ع.

The screenshot shows the 'Manage Virtual Routers' interface with the 'Policy Based Routing' tab selected (marked with a red box and number 1). The main area displays 'Policy Based Routing' settings with a table for defining ingress interfaces, match criteria, and forward actions. A blue 'Configure Interface Priority' button and a red 'Add' button are visible. The 'Add' button is highlighted with a red box and number 2.

نراق لخدملا تنيع:

The screenshot shows the 'Add Policy Based Route' dialog box. It includes fields for 'Ingress Interface*' (set to 'INSIDE' and highlighted with a red box and number 1) and 'Match Criteria and Egress Interface'. A red 'Add' button is highlighted with a red box and number 2. The dialog also contains a note about defining forward actions and standard save/cancel buttons at the bottom.

هيجوت لى داعا] ةداعا] ديدحت:

Add Forwarding Actions

Match ACL:*	<input type="text" value="ACL_PBR"/> 1	+
Send To:*	<input type="text" value="IP Address"/> 2	
IPv4 Addresses	<input type="text" value="203.0.113.99"/> 3	
IPv6 Addresses	Eg: 2001:db8::, 2001:db8::1234:5678	

رشن و ظفح.

لسرى' لقحلا يف تبثى نأ رطضى تنانأ نرافق جرخم ددعتى لكشى نأ تنانأ ديري نا: ظحالم نم ققحت، ليصافتلا نم دي زمل (7.0+). ئغىص نم نأ امب رفوتى) رايىخ 'نرافق جرخم' لا 'لىا قس ايسلالا دنتسملانىوكتلل لاثم

ةمي دقلا ئقيرطلار (PBR) نىوكت

ةقباطملار رورملار كرجل لوصو ئمئاق ديدحت - 1 ۋوطخلا.

The screenshot shows the Firewall Management Center interface. The 'Objects' tab is selected (1). In the left sidebar, 'Access List' is expanded, and 'Extended' is selected (2). The main panel displays the configuration for an 'Extended' access list named 'ACL_PBR'. It shows one entry (3) with the following details:

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

ۋوطخلا نىييعت (ACL) لوصولار يف مكحتلا ئمئاق قباطم راسم ئطييرخ ديدحت - 2 ۋوطخلا.

ةقباطملار ئرابع فيرعتب مق، الوا:

Firewall Management Center

Objects / Object Management

Overview Analysis Policies Devices Objects Integration

1

AS Path
Cipher Suite List
> Community List
> Distinguished Name
DNS Server Group
> External Attributes
File List
> FlexConfig
Geolocation
Interface
Key Chain
Network
> PKI
Policy List
Port
> Prefix List
2 Route Map
> Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone

Route Map

Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a redistributed into the target routing process.

Name: New Route Map Object

Name: PBR_RMAP

3

Entries (0)

Add

Sequence No ▲	Redistribution
No records to display	

Allow Overrides

Cancel Save

Route Map

Route maps are used when redistributing routes into the target routing process.

Name: New Route Map Object

Name: PBR_RMAP

Entries (0)

No records

Allow Overrides

1

Sequence No:

2

Redistribution: Allow

3

Match Clauses Set Clauses

Security Zones

IPv4 **4**

IPv6

BGP

Others

Address (2) Next Hop (0) Route Source (0)

Select addresses to match as access list or prefix list addresses of route.

Access List
 Prefix List

Available Access Lists :

Extended **5**

Available Extended Access List C

Search **6**

ACL_PBR

Add

Selected Extended Access List

ACL_PBR

مهمة رابع فيرعت:

Edit Route Map Entry

Sequence No: 1

Redistribution: Allow

Match Clauses 1

Metric Values 2

BGP Clauses 2

Set Clauses 1

AS Path

Community List

Others 3

Local Preference : Range: 1-4294967295

Set Weight : Range: 0-65535

Origin:

- Local IGP
- Incomplete

IPv4 settings:

Next Hop: 4

Specific IP

Specific IP : 203.0.113.99

Use comma to separate multiple values

Prefix List:

IPv6 settings:

ظفح و ةفاضا.

FlexConfig نئاك نيوكتب مق. 3. ۋوطخل FlexConfig PBR.

دوچوملا PBR نئاك (ةفعاضم) خسن ، الوا

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration Deploy Q mzafeiro \ mzafeiro SECURE

AS Path

Cipher Suite List

> Community List

> Distinguished Name

DNS Server Group

> External Attributes

File List

< FlexConfig 1

FlexConfig Object

Add FlexConfig Object Policy 2

FlexConfig Object

FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig policies.

Name	Domain	Description
Policy_Based_Routing	Global	The template is an ex...
Policy_Based_Routing_Clear	Global	Clear configuration of ...

3

اقبسم ددملا راسمل ا ططخم نئاك ۋەزاب مقو نئاكلما مسا ددح:

Add FlexConfig Object

Name: **FTD4100_PBR** **1 Specify a new name**

Description:
The template is an example of PBR policy configuration. It

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

Insert Deployment: Once Type: Append

interface Port-channel1.101
policy-route route-map \$r-map-object **2 Specify the correct ingress interface** **3 Remove this route-map**

دەرىجىلار ئەطىرخ دىدەت:

Add FlexConfig Object

Name: FTD4100_PBR

Description:
The template is an example of PBR policy configuration. It

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

Insert Deployment: Once Type: Append **1**

Insert Policy Object **2** Route Map

- Text Object
- Network
- Security Zones
- Standard ACL Object
- Extended ACL Object

Insert Route Map Variable

Variable Name: **PBR_RMAP** 1

Description:

Available Objects C

Selected Object PBR_RMAP

Q Search 2

PBR_RMAP 3

Add

هذا هو ترتيب الخطوات:

Add FlexConfig Object

Name: **FTD4100_PBR**

Description:

The template is an example of PBR policy configuration. It

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

Insert | Deployment: Once | Type: Append

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

خطوة 4: إدخال PBR في FlexConfig على FTD.

Firewall Management Center
Devices / Flexconfig Policy Editor

Overview Analysis Policies Devices Objects Integration Deploy ? mzafeiro \ mzafeiro Cisco SECURE

FTD4100_FlexConfig

Enter Description

Policy Assignments (1)

Available FlexConfig C FlexConfig Object

User Defined 1
FTD4100_PBR 2

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 policy configuration. It can not be used...

دیجت و ظنی اعمالا نیوکت طفح:

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-confia Appended CLI ####
interface Port-channel1.101
    policy-route route-map PBR_RMAP
```

جنهنلا رشنب مق ،اريخأ

مدختسنم ةهجاو FlexConfig و FMC سفنل او سفنب اسلاس بـ PBR نـيـوكـتـ نـكمـيـ الـ ظـاحـالـمـ لـ وـخـدـلـاـ

[IP SLAs J ISP مادختس اب](#) [PBR نیوکت](#): دنتسمل اذه نم ققحت، PBR SLA، ظطس اوپ هترادا متت یذلا [FTD جودزملا FMC](#)

نم ققحتا PBR

لوجدل اههجاو نم ققحتا:

```
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
```

راسمل اه طيـرـخ نـم قـقـحـتـلـا:

```
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)
```

راسـمـلـا رـاسـمـلـا نـم قـقـحـتـلـا:

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

ريـيـغـتـلـا دـعـبـوـلـبـقـ رـيـيـغـتـلـا:

نودب PBR

```
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:
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
```

پغ PBR

```
firepower# packet-tracer input INSIDE tcp 192.168.2.100 1111 198.51.100.5 23
...
Phase: 3
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Elapsed time: 39694 ns
Config:
Additional Information:
Input route lookup returned
Phase: 4
Type: ECMP load balancing
Subtype:
Result: ALLOW
Elapsed time: 2230 ns
Config:
Additional Information:
ECMP load balancing
Found next-hop 203.0.113.99

Phase: 5
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 446 ns
Config:
route-map FMC_GENERATED_PBR
match ip address ACL_PBR
set adaptive-interface cost
Additional Information:
Matched route-map FMC_GENERATED_PBR
Found next-hop 203.0.113.99

...
Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 5352 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: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 825100 ns
```

ةيقيقح رورم ةكح عم رابتخا

عابتت مادختساب ۆمزحلا طاقتلانیوکت:

```
firepower# capture CAPI trace interface INSIDE match ip host 192.168.2.1 host 198.51.100.5
firepower# capture CAPO1 trace interface OUTSIDE1 match ip host 192.168.2.1 host 198.51.100.5
firepower# capture CAPO2 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
```

طاقتلالا رهظي:

```
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 CAPO1 type raw-data trace interface OUTSIDE1 [Capturing - 4389 bytes]
match ip host 192.168.2.1 host 198.51.100.5
capture CAPO2 type raw-data trace interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.2.1 host 198.51.100.5
```

ماظن ۆمزح عابتت TCP:

```
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

```

ةسأيـسـلـا تـابـرـضـ مـاقـرأـ ASP PBR لـوـجـ ضـرـعـيـ

```
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

 برضأ دادعل ااضيأ packet-tracer لـ ديزي: ظحالم.

اطخأ حيحصت PBR

 لـ اسـرـلـا نـم رـيـثـكـلـا ظـحـالـا اـطـخـأـا حـيـحـصـتـ جـتـنـيـ نـأـ نـكـمـيـ،ـجـاتـنـإـلـاـ ةـئـيـبـ يـفـ:ـرـيـذـحـتـ.

اده ظـحـالـا حـيـحـصـتـ نـيـكـمـتـ:

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

يـقـيقـحـ رـوـرـمـ ةـكـرـحـ لـاسـرـاـ:

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

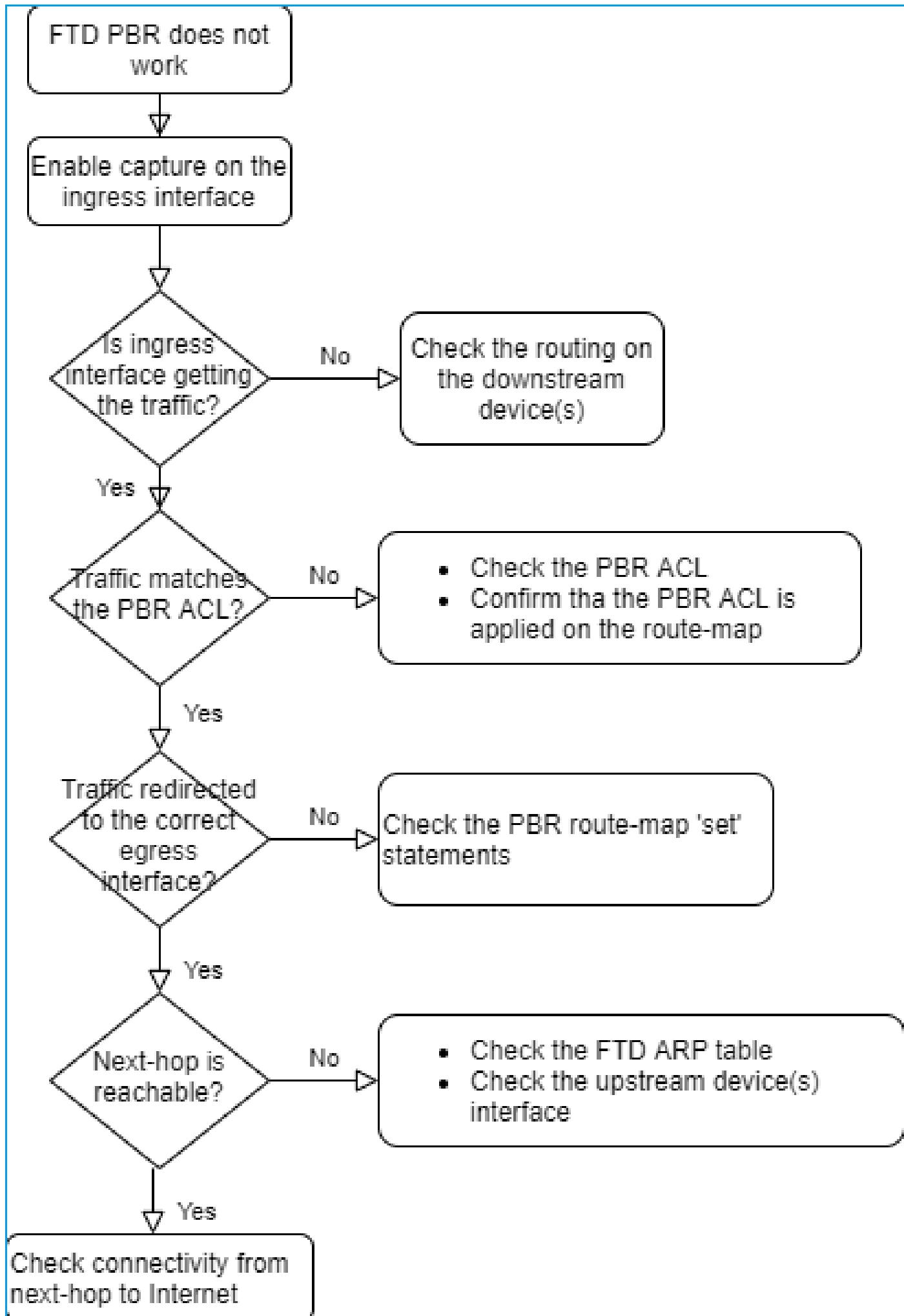
اطخأ حـيـحـصـتـ رـهـظـيـ:

```
firepower#
```

```
pbr: policy based route lookup called for 192.168.2.1/37256 to 198.51.100.5/23 proto 6 sub_proto 0 rece  
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
```

 ظـحـالـا حـيـحـصـتـ جـارـخـاـ ظـحـالـاـ مـوقـيـ اـمـكـ:ـظـحـالـمـ.

اـحـالـصـ اوـ ظـحـالـمـ اـطـخـأـ فـاشـكـتـسـ الـ يـبـاـيـسـنـ الـ طـطـخـمـلـ اـدـهـ مـادـخـتـسـ نـكـمـيـ:



show arp drop

ماعلـا هـيـجـوـتـلـا نـعـثـحـبـلـا إـلـا اـدـانـتـسـا هـيـجـوـتـلـا ةـدـاعـا - 4 ةـلـاحـلـا

جـرـخـمـلـا ةـهـجـاـوـ دـيـدـحـتـلـ هـصـفـ مـتـيـ رـصـنـعـ رـخـآـ نـوـكـيـ، PBRـ وـ، NATـ ثـحـبـ ، لـاـصـتـالـا نـعـثـحـبـلـا دـعـبـ جـمـعـلـا مـاعـلـا هـيـجـوـتـلـا لـوـدـجـ وـ.

هـيـجـوـتـلـا لـوـدـجـ نـمـ قـقـحـتـلـا

هـيـجـوـتـلـا لـوـدـجـ جـارـخـا صـحـفـنـ اـنـعـدـ FTD:

```
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

Dest. Mask          Metric
Dest. Network       Next Hop
Administrative Distance
o 192.0.0.2 255.255.255.0 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, 01:36:53, INSIDE
o 192.168.2.1 255.255.255.255
  [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
  [90/128512] via 192.0.2.99, 15:13:23, OUTSIDE2
D 198.51.100.16 255.255.255.248
  [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
```

اذـهـبـ رـاسـمـلـا دـيـدـحـتـ . ةـيـلـاـتـلـا ةـوـطـخـلـا إـلـعـ رـوـثـعـلـا وـهـيـجـوـتـلـا ةـيـلـمـعـلـ يـسـيـئـرـلـا فـدـهـلـا بـيـتـرـتـلـا:

1. زـوـفـتـ ةـأـرـابـمـ لـوـطـأـ.
- (ةـفـلـتـخـمـلـا هـيـجـوـتـلـا لـوـكـوـتـوـرـبـ رـدـاصـمـ نـيـبـ) ئـنـدـأـلـا AD
- (هـيـجـوـتـلـا لـوـكـوـتـوـرـبـ - هـسـفـنـ رـدـصـمـلـا نـمـ مـلـعـتـلـا ةـلـاحـيـفـ) ئـنـدـأـلـا سـايـقـمـلـا

هـيـجـوـتـلـا لـوـدـجـ عـلـمـ ةـيـفـيـكـ:

- IGP (R (L1, L2, E1, E2, N1, N2), O (IA, SU))

- BGP (B)

- BGP InterVRF (BI)

- ئـكـيـتـاـتـسـاـ نـكـاسـ

- تـبـاـثـلـاـ لـوـكـوـتـوـرـبـ (SI)

- لـصـتـمـ (C)

- ئيچملـا IP نـيـوانـع

- ئـيرـهـاظـلـا ئـصـاخـلـا ئـكـبـشـلـا

- عـيـزـوـتـلـا ئـدـاعـا

- يـضـارـتـفـالـا

:رمـأـلـا اـذـهـ مـادـخـتـسـأـ،ـيـجـوـتـلـا لـوـدـجـ صـخـلـمـ ضـرـعـلـ

```
<#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

:رمـأـلـا اـذـهـ مـادـخـتـسـابـ هـيـجـوـتـلـا لـوـدـجـ تـاـثـيـدـحـتـ بـقـعـتـ كـنـكـمـيـ

```
<#root>
```

```
firepower#
```

```
debug ip routing
```

```
IP routing debugging is on
```

نـمـ 192.168.1.0/24 رـاسـمـ ئـلـاـزاـ دـنـعـ ئـاطـخـأـلـاـ حـيـحـصـتـ هـرـهـظـيـ اـمـ اـذـهـ،ـلـاـثـمـلـاـ لـيـبـسـ ئـلـعـ
مـاعـلـاـ هـيـجـوـتـلـاـ لـوـدـجـ:

```
<#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

```

ىرخأ ةرم هتفضل ام دنع:

<#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
```

طاقيس إلأ اذهل نوكى .اهي ف بوعرمل ريملا ةكرح طاقس إلأ null0 ةهجاولى مادختسا نكمى يف مكحتلا ةسايىس ڈدعاق مادختساب رورمل ريملا ةكرح يف طاقس إلأ نم لقأ عادلأا ىلع ريثأت لوصولى (ACL).

تابلطتملا

فيفضمل Null0 راسم نيوكت 198.51.100.4/32.

لحل

FTD4100-1
Cisco Firepower 4140 Threat Defense

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

- Global
- Virtual Router Properties
- ECMP
- OSPF
- OSPFv3
- EIGRP
- RIP
- Policy Based Routing
- BGP
 - IPv4
 - IPv6
- Static Route **1**
- Multicast Routing

Add Static Route Configuration

Type: IPv4 IPv6

Interface* **2**: Null0

(Interface starting with this icon signifies it is available for route leak)

Available Network **3**: host_198.51.100.4

Selected Network **4**: host_198.51.100.4

Gateway*

Metric:

رشن و ظفح.

ققحتا:

```
<#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
```

ديعبلا فيضملا ىلا لوصول ا لواح:

```
<#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)
```

تالجس رهظت FTD:

```
<#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
```

طاقس! تايـلـمـع ضـرـع

```
<#root>
```

```
firepower#
```

```
show asp drop
```

Frame drop:

No route to host (no-route)	1920
-----------------------------	------

ةـفـلـكـتـلـا ةـيـوـاسـتـم ةـدـدـعـتـم تـارـاسـم

رورـمـلـا قـطـانـم

- مساب اهيل راشي) اعم تاهج اولا عيمجتب مدخلـسـمـلـل ECMP رورـمـلـا ةـكـرـحـ لـمـحـ ةـنـزاـومـ كـلـذـكـو ECMP.
- ةـدـدـعـتـمـلـا تـاهـجـ اـولـا رـبـعـ رـوـرـمـلـا ةـكـرـحـ لـمـحـ ةـنـزاـومـ هـيـجـوـتـبـ حـمـسـيـ اـذـهـوـ.
- ةـتـبـاـثـ تـارـاسـمـ عـاـشـنـا مـدـخـتـسـمـلـلـ نـكـمـيـ، رـوـرـمـلـا ةـكـرـحـ ةـقـطـنـمـبـ تـاهـجـ اـولـا نـاـرـتـقـاـ دـنـعـ.
- تـارـاسـمـ يـهـ ةـفـلـكـتـلـا ةـيـوـاسـتـمـ ةـتـبـاـثـلـا تـارـاسـمـلـاـ. تـاهـجـ اـولـا رـبـعـ ةـفـلـكـتـلـا ةـيـوـاسـتـمـ ةـيـرـتـمـلـا ةـمـيـقـلـا سـفـنـ اـهـلـ اـهـسـفـنـ ةـهـجـوـلـا ةـكـبـشـ يـلـاـ.

تـاسـاـيـسـ لـالـخـ نـمـ FirePOWER هيـجـوـتـ دـيـدـهـتـ نـعـ عـافـدـلـاـ مـعـ دـيـ، 7.1ـ رـادـصـاـلـاـ لـبـقـ
هيـجـوـتـ نـيـوـكـتـوـ رـوـرـمـلـا ةـكـرـحـ قـطـانـمـ يـفـ تـاهـجـ اـولـا عـيمـجـتـ كـنـكـمـيـ، 7.1ـ رـادـصـاـنـمـ اـعـدـبـ.
ECMP يـفـ زـكـرـمـ Firepower.

يـفـ ةـيـثـوـتـ مـتـيـ EMCP

عـاجـرـاـلـا رـوـرـمـ ةـكـرـحـ طـاقـسـاـ مـتـوـ، لـثـامـتـمـ رـيـغـ هيـجـوـتـ كـانـهـ، لـاثـمـلـاـ اـذـهـ يـفـ:

```
<#root>
```

```
firepower#
```

```
show log
```

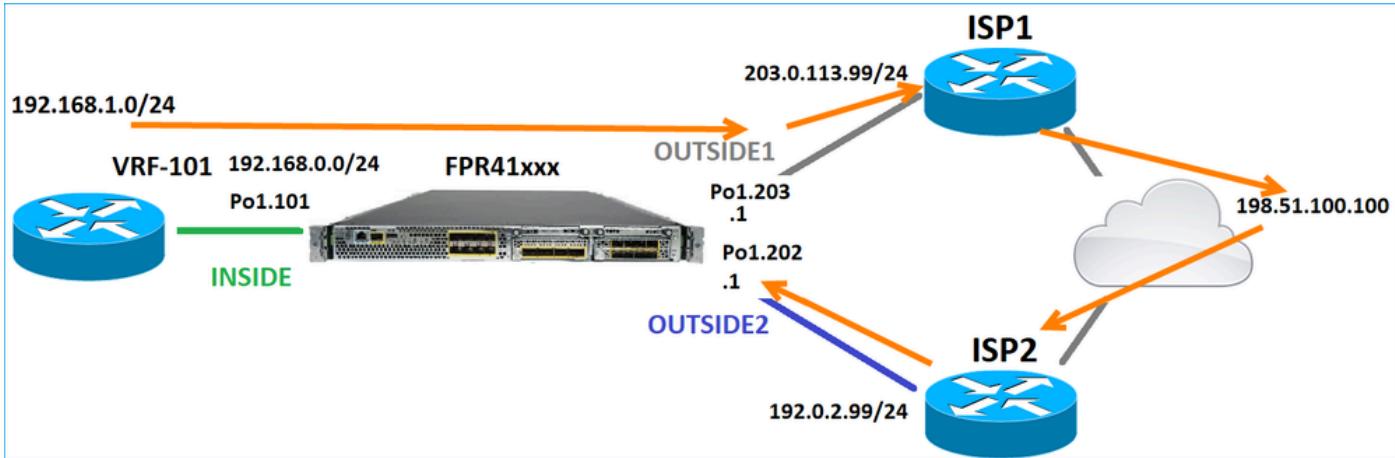
```
Apr 13 2022 07:20:48: %FTD-6-302013:
```

```
B
```

```
uilt inbound TCP connection 4046 for INSIDE:192.168.1.1/23943 (192.168.1.1/23943) to OUTSIDE1:198.51.100.100/23
```

```
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 OUTSIDE1
```



مدى تسلسلي او نم نويوكت FMC:

The screenshot shows the Juniper Network Management interface under the 'Routing' tab. The left sidebar lists various routing protocols: Global, Virtual Router Properties, ECMP (highlighted), OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP (expanded), and IPv4. The main pane displays 'Equal-Cost Multipath Routing (ECMP)' with a message stating 'There are no ECMP zone records' and an 'Add' button highlighted with a red box.

فاصلاً اولاً تاهاج ومجم يف 2 ئوغى عۆمۈچ:

Add ECMP

Name: **ECMP_OUTSIDE**

Available Interfaces	Selected Interfaces
INSIDE	OUTSIDE1 OUTSIDE2

Add

Cancel OK

ةجیتنل:

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

OSPF

Equal-Cost Multipath Routing (ECMP)

Name	Interfaces
ECMP_OUTSIDE	OUTSIDE2, OUTSIDE1

رشن و ظفح.

ةقطنم نم ققحتل: ECMP:

```
<#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
```

حالات قوقعتل اولانم:

```
<#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
```

لاصتا لیغشت متي و، دئاعلا رورملا ةكرحب حامسلا نآل ا متى:

```
<#root>

Router1#
telnet 198.51.100.100 /vrf VRF-101 /source-interface lo1

Trying 198.51.100.100 ... Open
```

رورم ةكرح جرخملان راق ISP1 ايلع ضبق ىلع يدبى:

```
<#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
```

عاجرا لا رورم ةكرح جاوىل ع طاقت لا رهظى:

```
<#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
```

ةرادإ يوتسم FTD

ةرادإ لل نويوتسم ىلع FTD:

- يعرفلا ماظنلا ىلإ لوصولا رفوت - Management0 ةهجاولـا
- يعرفلا ماظنلا ىلإ لوصولا ريفوت - ةيسيختلا LINA ةهجاولـا FTD LINA

ةكبشلا راهظإ و ةكبشلا نيكوت رماوأ مدخلـسـا، اهنـمـ قـقـحتـلـاـوـ Management0 ةهجـاـوـ نـيـكـوـتـلـ

تـالـاخـدـاـ رـابـتـعـاـ نـكـمـيـ اـهـسـفـنـ LINA تـاهـجـاـوـرـفـوـتـ،ـىـرـخـأـ ةـيـحـانـ نـمـوـ

(RIB) هـيـجـوـتـلـاـ تـامـوـلـعـمـ لـوـكـوـتـوـرـبـ "ـيـفـ"ـ (FTD)ـ عـرـسـلـاـ قـئـافـ لـاسـرـالـاـ جـمـانـرـبـ "ـةـهـجـاـوـ"

ةـيـلـحـمـ تـارـاسـمـكـ"ـ (FTD)ـ هـيـجـوـتـلـاـ تـامـوـلـعـمـ لـوـكـوـتـوـرـبـ):

```
<#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
```

هـيـجـوـتـ لـوـدـجـ يـفـ ةـيـوـهـ تـالـاخـدـاـكـ اـهـتـيـفـرـ نـكـمـيـ ،ـلـثـمـلـابـ وـ

```
<#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
```

ةيسيئرلا ةطقنلا

نأ FTD فرعى ،ةي وهل IP نيوانع دحأ ةهجولل IP ناونع قباطي و FTD ئلإ ةمزح لصت امدنع ةمزحلا كالهتسا هيلع.

ةيسيخشتلا ةهجاوه يجوت

م ت ةهجاو يأول VRF هبشي هيجوت لودجب (9.5 دعب ام زمر لغشى يذلا ASA لثم) ظفتحي ةيسيخشتلا ةهجاوللا ةهجاوللا ةلثما نمو .طقف ةرادإك اهنويكت

نيهجوم نيوكتب (ECMP) ةي ساسألا ةرادإلا يف مكحتلا ةدحو كل حمسن ال امنيـب راسم نيوكتب كـنـكمـي ،ـسـايـقـمـلـاـ سـفـنـ مـادـخـتـسـابـ ةـفـلـتـخـمـ تـاهـجـاـوـىـلـعـ نـيـيـضـارـتـفـاـ ةـيـصـيـخـشـتـلـاـ ةـهـجـاـوـلـاـ ئـلـعـ رـخـآـ يـضـارـتـفـاـ هـجـوـمـوـ FTD تـانـاـيـبـ ةـهـجـاـوـلـاـ ئـلـعـ دـحـاوـيـضـارـتـفـاـ

Device	Routing	Interfaces	Inline Sets	DHCP	VTEP
Manage Virtual Routers					
Global					
Virtual Router Properties		Network ▲	Interface	Leaked from Virtual Router	Gateway
ECMP		▼ IPv4 Routes	diagnostic	Global	gw_10.62.148.1
OSPF		any-ipv4	OUTSIDE1	Global	203.0.113.99
OSPFv3					

مدختسـتـ اـمـنـيـبـ ،ـمـاعـلـاـ لـوـدـجـلـلـ ةـيـضـارـتـفـاـ تـانـاـيـبـلـاـ ئـوـتـسـمـ روـرـمـ ةـكـرـحـ مـدـخـتـسـتـ ةـيـصـيـخـشـتـلـاـ يـضـارـتـفـاـلـاـ ئـوـتـسـمـ روـرـمـ ةـكـرـحـ:

```
<#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
```

ماعلا هيجوتلا لودج ئبأوب:

```
<#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
```

ساسأ ىلع يقتني نراق جرخمل ،(رورم ئكرح عبرملا نم) FTD لىا نم رورم ئكرح تنا لسرىي امدنع:

1. ماعلا هيجوتلا لودج
2. طقف ئرادلاب صاخلا هيجوتلا لودج

نراق جرخمل ايودي نيعت تنا نا دي دحـت نراق جرخـمل تـلـدـبـتـسـا عـيـطـتـسـيـ تـنـاـ.

رابـتـخـا لـشـفـيـ، رـدـصـمـلـا ئـهـجـاوـ دـدـحـتـ مـلـ اـذـاـ. ئـيـصـيـخـشـتـلـا ئـهـجـاـوـلـا ئـبـأـوـلـا لـاصـتـا رـابـتـخـا لـواـجـ رـاسـمـ ىـلـعـ ئـلـاحـلـا هـذـهـ يـفـ يـوـتـحـيـ يـذـلـاوـ، مـاعـلـا هـيـجـوـتـلـا لـودـجـ الـوـأـ مـدـخـتـسـيـ FTD نـأـلـ لـاصـتـالـا لـودـجـ ىـلـعـ رـاسـمـلـا ثـحـبـبـ FTD مـوـقـيـ، مـاعـلـا لـودـجـلـا يـفـ رـاسـمـ كـانـهـ نـكـيـ مـلـ اـذـاـ. يـضـارـتـفـا طـقـفـ ئـرـادـلـابـ صـاخـلـا هـيـجـوـتـلـا:

```
<#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
```

رمألا مادختساب CLI LINA نم فلم خسنت نأ تلواح اذا هسفن قبطي copy.

هاجت إلـا يـئـانـثـ هـيـجـوـتـلـاـ ةـدـاعـ إـفـاشـتـكـاـ (BFD)

هـيـجـوـتـ: BGP لـوكـوتـورـبـلـ طـقـفـوـ 9.6 رـادـصـإـلـاـ يـديـلـقـتـلـاـ ASAـ يـلـعـ BFDـ مـعـدـ ةـفـاضـإـ تـمـتـ [هـاجـتـ إـلـاـ يـئـانـثـ هـيـجـوـتـلـاـ ةـدـاعـ إـفـاشـتـكـاـ](#)

يف FTD:

- جـمانـربـلـاـ (IPv4 و IPv6) ةـمـوـعـدـ 6. 4).
- ةـمـوـعـدـ رـيـغـ (EIGRP و OSPFv3 و OSPFv2) تـالـوـكـوتـورـبـ.
- BFD ةـمـوـعـدـ رـيـغـ ةـتـبـاـثـلـاـ تـارـاسـمـلـلـ.

(VRF) ةـيـرـهـاـظـلـاـ تـاهـجـوـمـلـاـ

نم قـقـحـتـ ،ـلـيـصـاـفـتـلـاـ نـمـ دـيـزـمـلـ 6.6 رـادـصـإـلـاـ يـفـ (VRF) يـكـلـسـاـلـلـاـ دـدـرـتـلـاـ مـعـدـ ةـفـاضـإـ تـمـتـ [ةـيـرـهـاـظـلـاـ تـاهـجـوـمـلـلـ نـيـوـكـنـلـاـ ةـلـثـمـأـ](#) :ـدـنـتـسـمـلـاـ اـذـهـ.

ةلص تاذ تامولع

- [ل ئيضا تفال او قتباثلا تا جو ملا FTD](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).