

عقوم نم IPSec قافنال لاطعالا زواجت نيوكت ةيطايتحالال ISP تااطابترا مادختساب عقوم ىلا FMC ةطساوب ةرادملا FTD ىلع

تايتوتملا

[ةمدقملا](#)

[ةيساسال تابلطتملا](#)

[تابلطتملا](#)

[قمذختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتل](#)

[ةكبشليليطيظختملا مسرلا](#)

[FTD نيوكت](#)

[ةيونائل او ةيساسال ISP تامولعم ديذحت 1. ةوطخل](#)

[ةيساسال ISP ةمول VPN ةكبش ططخم ديذحت 2. ةوطخل](#)

[ةيونائل ISP ةمول VPN ةكبش ططخم ديذحت 3. ةوطخل](#)

[SLA ةبقارم نيوكت 4. ةوطخل](#)

[SLA ةشاش مادختساب ةتائل تاراسملا نيوكت 5. ةوطخل](#)

[NAT ءارنثتسلا نيوكت 6. ةوطخل](#)

[ةديفملا روملا ءكرجل لوصولا يف مكحتل ةسايس نيوكت 7. ةوطخل](#)

[ASA نيوكت](#)

[ةحصلا نم ققحتلا](#)

[Firepower Threat Defense \(FTD\) ماطن](#)

[قيرط](#)

[رثا](#)

[nat](#)

[لشفلا زواجت ذيذحت](#)

[قيرط](#)

[رثا](#)

[nat](#)

[ءخالص او ءاطخال افاشكتسا](#)

ةمدقملا

طابترال ريفشتلا ةطيرخ ىلا دنتملا لشفلا زواجت نيوكت ةيفيك دنتملا اذه حضوي
FMC ةطساوب اهترادامتتلا FTD ىلع IP SLA بقعت ةزيم مادختساب ISP.

Cisco نم TAC سدنهم ،افان ادنام لبق نم ةمهاسملا تمت

ةيساسال تابلطتملا

تاب لطلت مل

ةة لالتل عيضاوم لابل ةفرعم كيدل نوكت نأب Cisco ي صوت

- (VPN) ةيرهاظ ةصاخ ةكبشل يساسأل مهفل
- FTD جم انرب مادختسا ةبرجت
- FMC عم ةبرجت
- (ASA) ةلدعمل نامأل ةزهجأ رماوأ رطس عم ةبرجت

ةمدختس مل تانوك مل

ةة لالتل جم اربال تارادصل لىل دننتس مل اذه يف ةدراول تامولعمل دننتست

- FMC، رادصلال 6.6.0
- FTD، رادصلال 6.6.0
- (ASA) يف فيكتل نامأل ةزهجأ نم 9.14.1 رادصلال

ةصاخ ةيلمعم ةئيبي يف ةدوجومل ةزهجأل نم دننتس مل اذه يف ةدراول تامولعمل عاشنل مت تناك اذل. (يضا رتفا) حوسمم نيوكتب دننتس مل اذه يف ةمدختس مل ةزهجأل عيجم تادب رما يأل لم تحمل ريثأتلل كمهف نم دكأتف، ليغشتل ديقتك كبش

ةيساسأ تامولعم

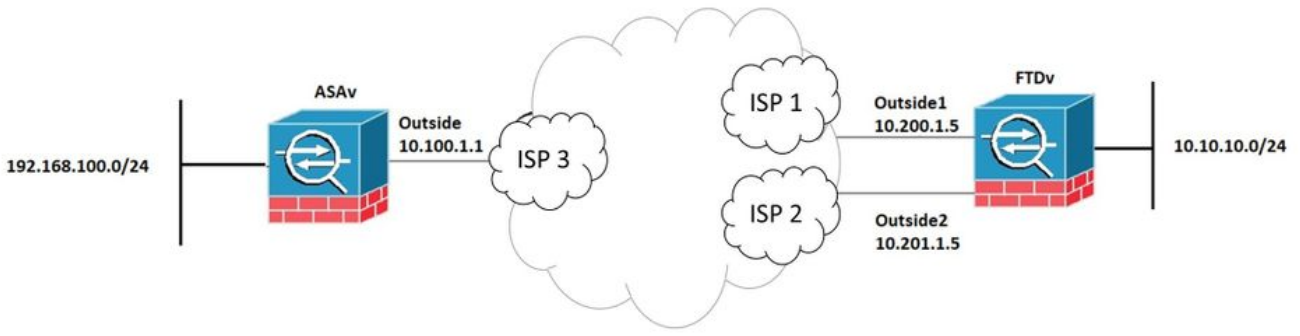
خسنلل ريفشتل ةطيرخ لىل دننتس مل لشفل زواجت نيوكت ةيفي دننتس مل اذه حضوي ةمدخ يوتسم ةيقافتا" بقت ةزيم مادختساب (ISP) تنرتنل ةمدخ دوزم طابترال يطايتحال اهريدي يتل " (FTD) ةيرانل ةقائل ديدهت نع عافدل" لىل " (IP SLA) تنرتنل لوكوتورب ةكبشل ناو نع ةمجت عافعل نيوكت ةيفي اضيأ حرشي وهو. (FMC) FirePOWER ةراد زكرم تنرتنل تامدخال الصوم كانه نوكي ام دنع (VPN) ةيرهاظل ةصاخل ةكبشل رورم ةكرحل (NAT) ةسالسب لشفل زواجت بلطتيو (ISP).

ريظنك ASA هاجت FTD نم (VPN) ةيرهاظل ةصاخل ةكبشل عاشنل متي، ويرانيسل اذه يف ISP طابترال FTD مدختسي. طقف ةدحاو ISP ةهجاو مادختساب (VPN) ةيرهاظل ةصاخل ةكبشل ةمدخ دوزم طابترال ل طعت دنع. (VPN) ةيرهاظل ةصاخل ةكبشل عاشنل تقولا كلذ يف دحاو لال نم رمال " (FTD) ةعرسل قئافل لاسرال جم انرب" لىلوتي، يساسأل (ISP) تنرتنل ةعباتل ةبقارملا ةادأ لال نم (ISP) تنرتنل ةمدخ دوزم لىل مئاقلا يوناتل طابترال (VPN) ةيرهاظل ةصاخل ةكبشل عاشنل متي و (SLA) ةمدخال يوتسم ةيقافتال

نيوكتل

ةكبشل لىل يطيختل مسرل

دننتس مل اذه يف لال ملل مدختس مل طاطخمل وه اذه



FTD نيوكت

ةيوناثللاو ةيساسأل ISP تاهجاو دي دحت 1. ةوطخلا

ةروصللا ي حضورم وه امك تاهجاو > ةزهجال ةرادا > ةزهجال لىل لقتنا 1.

Firepower Management Center
Devices / NGFW Interfaces

Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin

FTDv
Cisco Firepower Threat Defense for VMWare

Device Routing Interfaces Inline Sets DHCP

Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	Outside	Physical	Outside		10.200.1.5/24(Static)
GigabitEthernet0/1	Outside2	Physical	Outside2		10.201.1.5/24(Static)
GigabitEthernet0/2	Inside	Physical	Inside		10.10.10.5/24(Static)
GigabitEthernet0/3		Physical			

ةيساسأل ISP ةهجاو VPN ةكبش ططخم دي دحت 2. ةوطخلا

زاهج قوف رقنا، VPN ةكبش ةفاضل تحت. عقوم لىل عقوم > VPN > ةزهجال لىل لقتنا 1. ةجراخلا ةهجاو ددحو VPN ةكبش ءاشناب مقو، FirePOWER دي دعت دض عافدلا

نم دي زمل. ةيادبل نم VPN S2S ةكبش نيوكت ةي فيك دنتسملا اذه فص ي ال: ةظالم لىل لقتنا، FTD لىل VPN S2S نيوكتل عجرملا

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html>

Edit VPN Topology



Topology Name:*

Network Topology:
 Point to Point Hub and Spoke Full Mesh



IKE Version:* IKEv1 IKEv2


Endpoints IKE IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks	
ASAv	10.100.1.1	10.10.20.0_24	 


Node B: +

Device Name	VPN Interface	Protected Networks	
FTDv	Outside/10.200.1.5	10.10.10.0_24	 

 Ensure the protected networks are allowed by access control policy of each device.

ةيوناتال ISP ةهجال VPN ةكبش ططخم ديدحت 3. ةوطخال

زاهج قوف رقونا، VPN ةكبش ةفاضل تحت. عقوم يلى عقوم > VPN > ةزهجال يلى لقتنا 1. Outside2 ةهجال ددحو VPN ةكبش عاشناب مقو، FirePOWER ديدت دض عافدل

 ةهجاوم دختسي يذلا (VPN) ةيرهالال ةصخالال ةكبشال نيوكت نوكي نأ بجي: ةطخالام ءانثساب ةجخالال (VPN) ةيرهالال ةصخالال ةكبشال ططخمك امامت هسفن وه Outside2 (VPN) ةيرهالال ةصخالال ةكبشال ةهجاو

Edit VPN Topology

Topology Name:*

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks	
ASAv	10.100.1.1	10.10.20.0_24	

Node B: +

Device Name	VPN Interface	Protected Networks	
FTDv	Outside2/10.201.1.5	10.10.10.0_24	

Ensure the protected networks are allowed by access control policy of each device.

ةروصل ايف حضورم وه امك VPN ايجولوبط نيوكت بجي.

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin

Devices / VPN / Site To Site

Add VPN

Node A	Node B	
-- VPN_Outside1		
extranet : ASAv / 10.100.1.1	FTDv / Outside / 10.200.1.5	
-- VPN_Outside2		
extranet : ASAv / 10.100.1.1	FTDv / Outside2 / 10.201.1.5	

ةبقارم نيوكت 4. ةوطخلال SLA

رقونا VPN، ةكبش ةفاضل تحت SLA ةشاش ةفاضل > SLA ةشاش > تانئاللا لىل لقتنا 1. ةروصل ايف حضورم وه امك SLA ةشاش نيوكتب مقو، FirePOWER ديدت دض عافدلا زاخ قوف.

Firepower Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy admin

Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
RADIUS Server Group
Route Map
Security Group Tag
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set
VLAN Tag
VPN

SLA Monitor

Add SLA Monitor Filter

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Name	Value
ISP_Outside1	Security Zone: Outside Monitor ID: 10 Monitor Address: 10.200.1.1

2. ةللاتلا ةوطخلل لجراخل ال IP ناونع لقلحلا مدختسأ ، SLA* ةبقارم فرعمل ةبسنلاب .

Edit SLA Monitor Object



Name:

Description:

Frequency (seconds):

(1-604800)

SLA Monitor ID*:

Threshold

(milliseconds):

(0-60000)

Timeout

(milliseconds):

(0-604800000)

Data Size (bytes):

(0-16384)

ToS:

Number of Packets:

Monitor Address*:

Available Zones

Inside

Outside

Outside2

Selected Zones/Interfaces

Add

Outside

Cancel

Save

SLA ةشاش مادختساب ةتباثال تاراسملا نيوكت 5. ةوطخلال

راسملا نيوكتب مقو، راسم ةفاضل دح. تباثال راسملا > هجوتال > ةزهألإ ل لقتنا 1. اهؤاشنإ مت يتال) SLA ةبقارم تامولعم مادختساب (ةيساسأل) ةيجراخلال ةهجالولل يضارتفالال راسملا بقت ل قح يف (4 ةوطخلال يف

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*
Outside1
(Interface starting with this icon signifies it is available for route leak)

Available Network +
10.10.10.0
192.168.100.1
192.168.200.0
any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local

Add

Selected Network
any-ipv4

Gateway*
10.200.1.1 +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
ISP_Outside1 +

Cancel OK


ةيرتملا ةميقلال نوكت نأ بحج. (ةيونالال) 2 ةيجراخلال ةهجالولل يضارتفالال راسملا نيوكت 2.


ممسقلا اذه يف راسملا بقعت ل قح ىلإ ةجاح دجوت ال .يساسألا يضارت فال راسملا نم ىلعأ

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*
Outside2

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


Available Network  +

Selected Network

Search

10.10.10.0
192.168.100.1
192.168.200.0
any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local

Add

any-ipv4 

Gateway*
10.201.1.1 +

Metric:
2
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

ةروصللا يف حضورم وه امك تاراسملا نيوكت بچي

Firepower Management Center
Devices / NGFW Routing

Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin

FTDv
Cisco Firepower Threat Defense for VMWare

Device Routing Interfaces Inline Sets DHCP

OSPF
OSPFv3
RIP
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM
Multicast Routes
Multicast Boundary Filter

+ Add Route

Network	Interface	Gateway	Tunneled	Metric	Tracked	
IPv4 Routes						
any-ipv4	Outside2	10.201.1.1	false	2		
any-ipv4	Outside	10.200.1.1	false	1	ISP_Outside1	
IPv6 Routes						

NAT انثتسإ نيوكت 6 ةوطخلا

دح FTD زاهج فدهتست يتلا ةسايسلا دحو NAT ةسايس > NAT > ةزهجألا ىلإ لقتنا 1. به NAT دعاوق نوكت نأ بجي. (2جراخ و جراخ) ISP ةهجاو لك NAT انثتسإ تلکش و ةدعاق ةفاضا ةهجولا ةهجاو انثتساب اهسفن.

Firepower Management Center
Devices / NGFW NAT Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin

NAT_FTDv
Enter Description

Rules Policy Assignments (1)

Filter by Device + Add Rule

#	Direction	Type	Source Interface	Destination Interface	Original Packet			Translated Packet			Options	
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
NAT Rules Before												
1		Static	Inside	Outside	10.10.10.0	192.168.100.1		10.10.10.0	192.168.100.1		route-lookup no-proxy-arp	
2		Static	Inside	Outside2	10.10.10.0	192.168.100.1		10.10.10.0	192.168.100.1		route-lookup no-proxy-arp	
Auto NAT Rules												
NAT Rules After												

نع شحبلا نيكمت NAT دعاوق نم لك بلطتت، ويرانييسلا اذهل ةبسنبلااب: ةظالم كولس يف رمتست نلو ىلوالا ةدعاقلا برضت فوس رورملا ةكرح نإف الو. راسملا رورملا ةكرح لاسرا مئيسف، راسملا شحب نيكمت مئيل اذإ. لشفلا زواجت تاراسم ىقبت، راسملا نع شحبلا نيكمت عم. (ىلوالا nat ةدعاق) ةيجراخلا ةهجاو مادختساب امئاد ةبقارم لالخنم هي فمكحتلا مئيل يذلا هي جوتلا لودج يف امئاد تانايبلا رورم ةكرح SLA.

ةديفملا رورملا ةكرحلا لوصولا يف مكحتلا ةسايس نيوكت 7 ةوطخلا

يف م كحتل ةسايس ديحت > لوصولي ف م كحتل > تاسايسلا لى لقتنا 1. انه ةروصولا يف حضوم وه امك ، ةدعاق ةفاضل قوف رقنا ، ةدعاق ةفاضل .لوصولا

ةكرحل حيتت يتلاو (2 جراخو 1 جراخ) ةيجراخلا قطانملا لى لخالل نم ةدحاو ةدعاق نيوكتب مق 192.168.100/24 لى 10.10.10.0/24 نم ةمتهملا رورملا

ةكرحب حمسي امم لخالل لى (2 جراخو 1 جراخ) ةيجراخلا قطانملا نم ىرخا ةدعاق نيوكتب مق 192.168.100/24 لى 10.10.10.0/24 نم مامتهال ةريثملا رورملا

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action	Icons
1	VPN_1_out	Inside	Outside Outside2	10.10.10.0	192.168.100.0	Any	Any	Any	Any	Any	Any	Any	Any	Allow	Icons
2	VPN_1_in	Outside2 Outside	Inside	192.168.100.0	10.10.10.0	Any	Any	Any	Any	Any	Any	Any	Any	Allow	Icons

ASA نيوكت

ةطيرخ لى ع يطايتح | خسن ريظن نيوكت متي ، ددحملا ويراني سلا اذهل : ةظحالم اذا . ثدحالا تارادصلا و 9.14.1 لى ع ASA نوكي نأ ةزيملا هذه بلطتتو ، IKEv2 ريفشتلا ريثك ل تلحأ . ليدب لحك IKEv1 مدختساف ، اميدق ارادصلا لغشي كب صاخلا ASA ناك [CSCud2276](#) id قب cisco لى ع جرم

1. لى ع ASA نم يجراخ نراقلا لى ع IKEv2 تنك:

```
Crypto ikev2 enable Outside
```

2. لى ع اهنيوكت مت يتلا تامل عمل س فن ددحي يذلا IKEv2 جهن ءاشناب مق:

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

3. iKEV2 لوكوتوربب حامس لل ةومجم ةسايس عاشنإب مق:

```
group-policy IKEV2 internal
group-policy IKEV2 attributes
vpn-tunnel-protocol ikev2
```

4. ةومجم لاهن عجار. (2جراخ و 1جراخ) FTD يف يجراخ IP ناوع لكل قافناً ةومجم عاشنإب مق:
اقبس م كرتشمل اجاتفم لادحو:

```
tunnel-group 10.200.1.5 type ipsec-l2l
tunnel-group 10.200.1.5 general-attributes
default-group-policy IKEV2
tunnel-group 10.200.1.5 ipsec-attributes
ikev2 remote-authentication pre-shared-key Cisco123
ikev2 local-authentication pre-shared-key Cisco123
```

```
tunnel-group 10.201.1.5 type ipsec-l2l
tunnel-group 10.201.1.5 general-attributes
default-group-policy IKEV2
tunnel-group 10.201.1.5 ipsec-attributes
ikev2 remote-authentication pre-shared-key Cisco123
ikev2 local-authentication pre-shared-key Cisco123
```

5. اهرفش متيس يتل رورم لة كرح دحت لوصو ةمئاق عاشنإب مق. (FTD-Subnet 10.10.10.0/24) (ASA-Subnet 192.168.100.0/24):

```
Object network FTD-Subnet
Subnet 10.10.10.0 255.255.255.0
Object network ASA-Subnet
Subnet 192.168.100.0 255.255.255.0
access-list VPN_1 extended permit ip 192.168.100.0 255.255.255.0 10.10.10.0 255.255.255.0
```

6. FTD يف ةدحمل ائمزراوخل اىل اءراش لال ikev2 ipSec حرتقم عاشنإب مق:

```
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
protocol esp encryption aes-256
protocol esp integrity sha-256
```

لوكوتورب ل IP ناونع فيضي و اع م نيوكتلا طبري ريفشت ةطي رخ لاخدا عاشن اب مق 7.
2: جرخالا او 1 جرخالا (FTD) تنرتنالا

```
crypto map CSM_Outside_map 1 match address VPN_1
crypto map CSM_Outside_map 1 set peer 10.200.1.5 10.201.1.5
crypto map CSM_Outside_map 1 set ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_map 1 set reverse-route
crypto map CSM_Outside_map interface Outside
```

8: ةياملال رادج ةطساوب ثدحت نا م VPN رورم ةكرح عنمي NAT ءانثتسا نايب عاشن اب مق 8.


```
Nat (inside,Outside) 1 source static ASA-Subnet ASA-Subnet destination static FTD-Subnet FTD-Subnet
```

ةحصلال نم ققحتلا

جحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

ماظن Firepower Threat Defense (FTD)

VPN ةكبش ةلاح نم ققحتلال show crypto ikev2 sa رمالا مدختسا، رمالا رطس ي

 ب صاخلا IP ناونع مادختساب (VPN) ةيره اظلال ةصاخلا ةكبشلا عاشن اب متي: ةظحالم
Outside1 (10.200.1.5) يلحم ناونعك

```
firepower# sh crypto ikev2 sa
```

IKEv2 SAs:

Session-id:24, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
373101057 10.200.1.5/500 10.100.1.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/37 sec
Child sa: local selector 10.10.10.0/0 - 10.10.10.255/65535
          remote selector 192.168.100.0/0 - 192.168.100.255/65535
          ESP spi in/out: 0x829ed58d/0x2051ccc9
```

قيرط

External1 ل ةيلالاتلا ةوطخلل IP ناونع يضا رتفالا راسملا ضرعي

Config:

```
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
```

Additional Information:

NAT divert to egress interface Outside1(vrfid:0)

Untranslate 192.168.100.1/0 to 192.168.100.1/0

-----OMITTED OUTPUT -----

Phase: 7

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
```

Additional Information:

Static translate 10.10.10.1/0 to 10.10.10.1/0

Forward Flow based lookup yields rule:

in id=0x2b3e09576290, priority=6, domain=nat, deny=false

hits=19, user_data=0x2b3e0c341370, cs_id=0x0, flags=0x0, protocol=0

src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0

input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)

Phase: 8

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true

hits=3596, user_data=0x0, cs_id=0x0, reverse, 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

input_ifc=any, output_ifc=any

-----OMITTED OUTPUT -----

Phase: 12

Type: VPN

Subtype: encrypt

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

out id=0x2b3e0c8d0250, priority=70, domain=encrypt, deny=false

hits=5, user_data=0x16794, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0

src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0

input_ifc=any(vrfid:65535), output_ifc=Outside1

Phase: 13

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
```

Additional Information:

Forward Flow based lookup yields rule:

out id=0x2b3e095d49a0, priority=6, domain=nat-reverse, deny=false

hits=1, user_data=0x2b3e0c3544f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0

src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0

```
input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)
```

Phase: 14

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

```
in id=0x2b3e0c8ad890, priority=70, domain=ipsec-tunnel-flow, deny=false
  hits=5, user_data=0x192ec, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
  src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=Outside1(vrfid:0), output_ifc=any
```

Phase: 15

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

```
in id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
  hits=3598, user_data=0x0, cs_id=0x0, reverse, 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
  input_ifc=any, output_ifc=any
```

-----OMITTED OUTPUT -----

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

لش فال زواجت ذي فنت

ةوطخال لى لع لي غشت فاق ية طساوب لش فال زواجت ذي فنت متي ، لاثم ل لى بس لى لع
ة شاش نيوكت لى لع ةم دخت س م ل Outside1 ل ة ل ل ل

```
firepower# sh sla monitor configuration 10
```

```
IP SLA Monitor, Infrastructure Engine-II.
```

```
Entry number: 10
```

```
Owner:
```

```
Tag:
```

```
Type of operation to perform: echo
```

```
Target address: 10.200.1.1
```

```
Interface: Outside1
```

```
Number of packets: 1
```

```
Request size (ARR data portion): 28
```

```
Operation timeout (milliseconds): 5000
```

```
Type Of Service parameters: 0x0
```


Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

قيرط

نأ امك External2 ب صاخلا ةيلالاتلا ةوطخلل IP ناو نع نآلا يضا رتفال راسملا مدختسي ةفقوتم لوصولا ةيناكمإ.

```
firepower# sh 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

Gateway of last resort is 10.201.1.1 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [2/0] via 10.201.1.1, Outside2
C       10.10.10.0 255.255.255.0 is directly connected, Inside
L       10.10.10.5 255.255.255.255 is directly connected, Inside
C       10.200.1.0 255.255.255.0 is directly connected, Outside1
L       10.200.1.5 255.255.255.255 is directly connected, Outside1
C       10.201.1.0 255.255.255.0 is directly connected, Outside2
L       10.201.1.5 255.255.255.255 is directly connected, Outside2
```

رثأ

ةطقنلا هذه دنع "ةفقوتم لوصولا ةيناكمإ"، 1 show track جارخإ يف رهظي امك.

```
firepower# sh track 1
Track 1
Response Time Reporter 10 reachability
Reachability is Down <----
37 changes, last change 00:17:02
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0
```

nat

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det
```

```
-----OMITTED OUTPUT -----
```

Phase: 4

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
```

Additional Information:

Static translate 10.10.10.1/0 to 10.10.10.1/0

Forward Flow based lookup yields rule:

in id=0x2b3e0c67d470, priority=6, domain=nat, deny=false

hits=44, user_data=0x2b3e0c3170e0, cs_id=0x0, flags=0x0, protocol=0

src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0

input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)

```
-----OMITTED OUTPUT -----
```

Phase: 9

Type: VPN

Subtype: encrypt

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

out id=0x2b3e0c67bdb0, priority=70, domain=encrypt, deny=false

hits=1, user_data=0x1d4cfb24, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0

src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0

input_ifc=any(vrfid:65535), output_ifc=Outside2

Phase: 10

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
```

Additional Information:

Forward Flow based lookup yields rule:

out id=0x2b3e0c6d5bb0, priority=6, domain=nat-reverse, deny=false

hits=1, user_data=0x2b3e0b81bc00, cs_id=0x0, use_real_addr, flags=0x0, protocol=0

src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0

input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)

Phase: 11

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

in id=0x2b3e0c8a14f0, priority=70, domain=ipsec-tunnel-flow, deny=false

hits=1, user_data=0x1d4d073c, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0

src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0

input_ifc=Outside2(vrfid:0), output_ifc=any

Phase: 12

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

in id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true

hits=3669, user_data=0x0, cs_id=0x0, reverse, 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

input_ifc=any, output_ifc=any

-----OMITTED OUTPUT -----

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

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا