

FMCによって管理されるFTDのバックアップ ISPリンクを使用したIPSecサイトツーサイトト ンネルのフェールオーバーの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[FTDの設定](#)

[ステップ 1: プライマリおよびセカンダリISPインターフェイスの定義](#)

[ステップ 2: プライマリISPインターフェイスのVPNトポロジの定義](#)

[ステップ 3: セカンダリISPインターフェイスのVPNトポロジの定義](#)

[ステップ 4: SLAモニタの設定](#)

[ステップ 5: SLAモニタを使用したスタティックルートの設定](#)

[手順 6: NAT免除の設定](#)

[手順 7: 対象トラフィックのアクセスコントロールポリシーの設定](#)

[ASAの設定](#)

[確認](#)

[FTD](#)

[ルート](#)

[トラック](#)

[NAT](#)

[フェールオーバーの実行](#)

[ルート](#)

[トラック](#)

[NAT](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、FMCによって管理されるFTDのIP SLAトラック機能を使用して、ISPリンクのクリプトマップベースのフェールオーバーを設定する方法について説明します。

著者：Cisco TACエンジニア、Amanda Nava

前提条件

要件

次の項目に関する知識があることが推奨されます。

- バーチャルプライベートネットワーク(VPN)に関する基本的な知識
- FTDの使用経験
- FMCの使用経験
- 適応型セキュリティアプライアンス(ASA)コマンドラインの経験

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FMCバージョン6.6.0
- FTDバージョン6.6.0
- ASAバージョン9.14.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

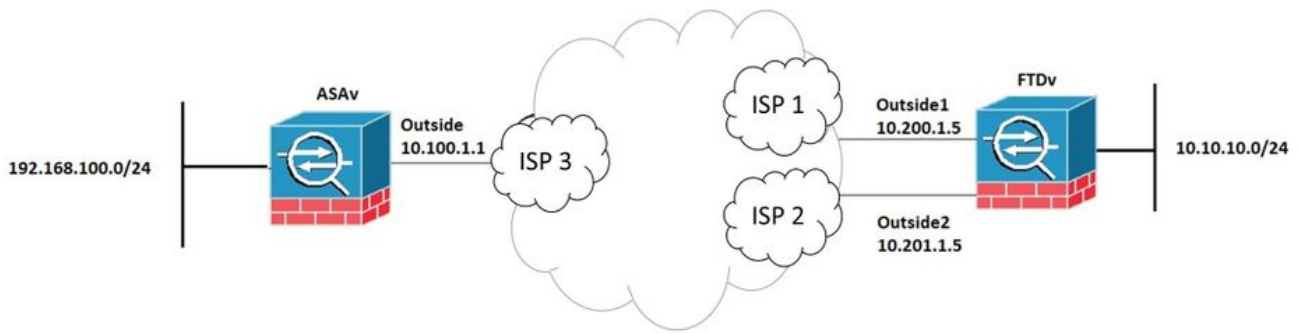
このドキュメントでは、Firepower Management Center(FMC)によって管理されるFirepower Threat Defense(FTD)のInternet Protocol Service Level Agreement(IP SLA)トラック機能を使用して、バックアップのInternet Service Provider (ISP ; インターネットサービスプロバイダー) リンクのクリプトマップベースのフェールオーバーを設定する方法について説明します。また、ISPが2つあり、シームレスなフェールオーバーが必要な場合の、VPNトラフィックのネットワークアドレス変換(NAT)除外の設定方法についても説明します。

このシナリオでは、ISPインターフェイスが1つだけのVPNピアとして、FTDからASAに向けてVPNが確立されます。FTDは、その時点で1つのISPリンクを使用してVPNを確立します。プライマリISPリンクがダウンすると、FTDがSLAモニタを介してセカンダリISPリンクを引き継ぎ、VPNが確立されます。

設定

ネットワーク図

このドキュメントの例で使用されているトポロジを次に示します。



FTDの設定

ステップ 1：プライマリおよびセカンダリISPインターフェイスの定義

1. 図に示すように、Devices > Device Management > Interfacesの順に移動します。

Firepower Management Center
Devices / NGFW Interfaces

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

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			

ステップ 2：プライマリISPインターフェイスのVPNトポロジの定義

1. Devices > VPN > Site To Siteの順に移動します。 firepower Add VPNの下でThreat Defense Deviceをクリックし、VPNを作成してOutsideインターフェイスを選択します。

注：このドキュメントでは、S2S VPNを最初から設定する方法については説明しません。FTDでのS2S VPN設定の詳細については、<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>を参照してください。

Edit VPN Topology



Topology Name:*
VPN_Outside1

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.

ステップ 3 : セカンダリISPインターフェイスのVPNトポロジの定義

1. Devices > VPN > Site To Siteの順に移動します。 Add VPNの下で、Threat Defense DeviceのFirepowerをクリックし、VPNを作成してOutside2インターフェイスを選択します。

 注 : Outside2インターフェイスを使用するVPN設定は、VPNインターフェイスを除き、Outside VPNトポロジとまったく同じである必要があります。

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.

VPNトポロジは、図に示すように設定する必要があります。

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	 

ステップ 4 : SLAモニタの設定

1. 「オブジェクト」 > 「SLAモニター」 > 「SLAモニターの追加」に移動します。 Add VPNで、 Threat Defense Deviceをクリックし、図に示すようにSLAモニタをFirepowerします。

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. SLA Monitor ID*フィールドには、外部ネクストホップIPアドレスを使用します。

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

ステップ 5 : SLAモニタを使用したスタティックルートの設定

1. Devices > Routing > Static Routeの順に移動します。Add Routeを選択し、Outside (プライマリ) インターフェイスのデフォルトルートを、Route trackingフィールドのSLA Monitor情報 (ステップ4で作成) で設定します。

Edit Static Route Configuration

Type: IPv4 IPv6

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

Available Network +

Search

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

2. Outside2 (セカンダリ) インターフェイスのデフォルトルートを設定します。メトリック値は

、プライマリデフォルトルートよりも大きい値である必要があります。このセクションでは、ルートトラッキングフィールドは不要です。

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*
Outside2
(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

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*
10.201.1.1 +

Metric:
2
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

ルートは、図に示すように設定する必要があります。

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						

手順 6 : NAT免除の設定

1. Devices > NAT > NAT Policyの順に移動し、FTDデバイスを対象とするポリシーを選択します。Add Ruleを選択し、ISPインターフェイス (OutsideおよびOutside2) ごとにNAT免除を設定します。NATルールは、宛先インターフェイスを除いて同じである必要があります。

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											

 注：このシナリオでは、両方のNATルールでRoute-lookupを有効にする必要があります。そうしないと、トラフィックは最初のルールに到達し、フェールオーバールートを維持しません。ルートルックアップがイネーブルになっていない場合、トラフィックは常に (最初の NATルール) 外部インターフェイスを使用して送信されます。ルートルックアップが有効な場合、トラフィックは常にSLAモニタを通じて制御されるルーティングテーブルに保持されます。

手順 7 : 対象トラフィックのアクセスコントロールポリシーの設定


1. Policies > Access Control > Select the Access Control Policyの順に移動します。ルールを追加するには、次の図に示すように、Add Ruleをクリックします。

InsideゾーンからOutsideゾーン (Outside1およびOutside2) に対して1つのルールを設定し、10.10.10.0/24から192.168.100/24への対象トラフィックを許可します。

Outsideゾーン (Outside1およびOutside 2) からInsideに別のルールを設定し、192.168.100/24から10.10.10.0/24への対象トラフィックを許可します。

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

ASA の設定

 注：この特定のシナリオでは、バックアップピアがIKEv2暗号マップに設定されています。この機能を使用するには、ASAが9.14.1以降のバージョンである必要があります。ASAが古いバージョンを実行している場合は、回避策としてIKEv1を使用します。詳細については、Cisco Bug ID [CSCud22276](#)を参照してください。

1. ASAの外部インターフェイスでIKEv2を有効にします。

```
Crypto ikev2 enable Outside
```

2. FTDで設定されているのと同じパラメータを定義するIKEv2ポリシーを作成します。

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

3. ikev2プロトコルを許可するグループポリシーを作成します。

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

4.各Outside FTD IPアドレス (Outside1およびOutside2) のトンネルグループを作成します。グループポリシーを参照し、事前共有キーを指定します。

```
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.暗号化するトラフィックを定義するアクセスリストを作成します(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で指定されたアルゴリズムを参照するikev2 ipsec-proposalを作成します。

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

7.設定を結び付けるクリプトマップエントリを作成し、Outside1およびOutside2のFTD IPアドレスを追加します。

```
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. VPNトラフィックがファイアウォールによってNAT処理されないようにするNAT免除ステートメントを作成します。


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

確認

このセクションでは、設定が正常に動作していることを確認します。

FTD

コマンドラインでshow crypto ikev2 saコマンドを使用して、VPNのステータスを確認します。

 注：VPNは、Outside1のIPアドレス(10.200.1.5)をローカルとして確立されます。

```
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
```

ルート

デフォルトルートは、Outside1のネクストホップIPアドレスを示しています。

```
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 10.200.1.1 to network 0.0.0.0
```

```
S*      0.0.0.0 0.0.0.0 [1/0] via 10.200.1.1, Outside1
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
```

トラック

show track 1の出力に見られるように、「Reachability is Up」。

```
firepower# sh track 1
Track 1
  Response Time Reporter 10 reachability
  Reachability is Up          <-----
  36 changes, last change 00:00:04
  Latest operation return code: OK
  Latest RTT (milliseconds) 1
  Tracked by:
    STATIC-IP-ROUTING 0
```

NAT

対象トラフィックがOutside1インターフェイスのNAT免除ルールに一致していることを確認する必要があります。

「packet-tracer input Inside icmp 10.10.10.1 8 0 192.168.100.10 detail」コマンドを使用して、対象トラフィックに適用されているNATルールを確認します。

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

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

```
Phase: 4
Type: UN-NAT
Subtype: static
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:

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

フェールオーバーの実行

この例では、フェールオーバーは、IP SLAモニタ設定で使用されるOutside1のネクストホップのシャットダウンによって実行されます。

```
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:
```

ルート

これで、デフォルトルートはOutside2のネクストホップIPアドレスを使用し、到達可能性はDownになります。

```
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
```

トラック

show track 1の出力からわかるように、この時点では「Reachability is Down」になっています。

```
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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。