

Konfigurieren des Failovers für IPSec-Site-to-Site-Tunnel mit Backup-ISP-Links auf FTD, die von FMC verwaltet werden

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[FTD konfigurieren](#)

[Schritt 1: Definieren der primären und sekundären ISP-Schnittstellen](#)

[Schritt 2: Definieren der VPN-Topologie für die primäre ISP-Schnittstelle](#)

[Schritt 3: Definieren der VPN-Topologie für die sekundäre ISP-Schnittstelle](#)

[Schritt 4: Konfigurieren des SLA-Monitors](#)

[Schritt 5: Konfigurieren der statischen Routen mithilfe des SLA-Monitors](#)

[Schritt 6: Konfigurieren der NAT-Ausnahme](#)

[Schritt 7: Konfigurieren der Zugriffskontrollrichtlinie für interessanten Datenverkehr](#)

[Konfigurieren der ASA](#)

[Überprüfung](#)

[FTD](#)

[Routing](#)

[Spur](#)

[NAT](#)

[Failover durchführen](#)

[Routing](#)

[Spur](#)

[NAT](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie für die ISP-Verbindung mithilfe der IP SLA-Trackfunktion auf dem von FMC verwalteten FTD ein auf der Crypto Map basierendes Failover konfigurieren.

Unterstützt von Amanda Nava, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis eines Virtual Private Network (VPN)

- Erfahrungen mit FTD
- Erfahrungen mit FMC
- Erfahrung mit der Adaptive Security Appliance (ASA) Befehlszeile

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- FMC Version 6.6.0
- FTD Version 6.6.0
- ASA Version 9.14.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

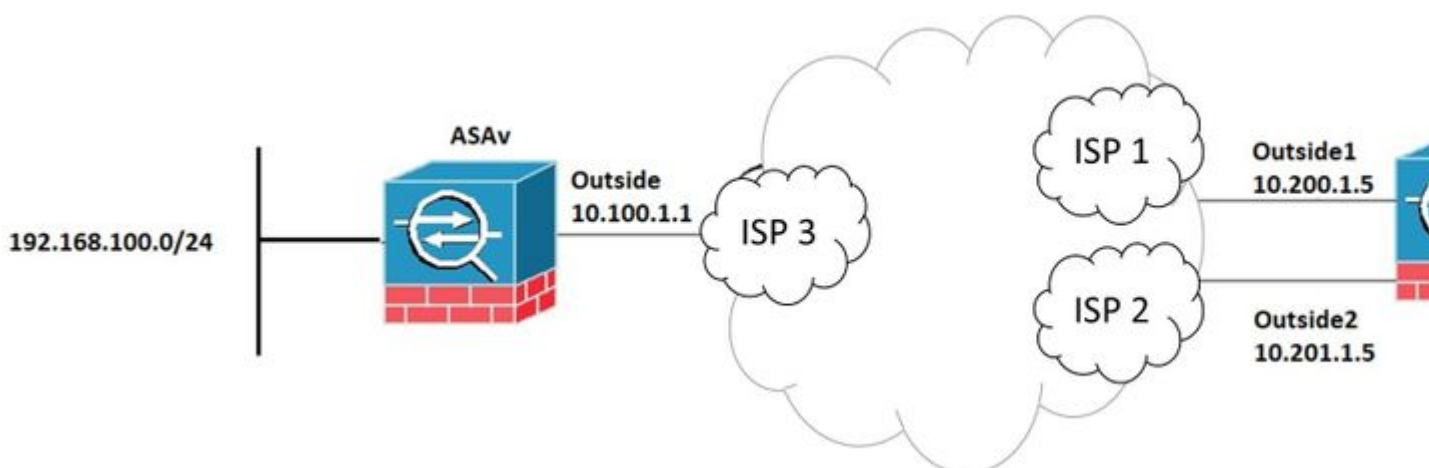
In diesem Dokument wird beschrieben, wie Sie ein krypto-map-basiertes Failover für eine Backup-Verbindung des Internet Service Providers (ISP) mit der IP SLA-Trackfunktion (Internet Protocol Service Level Agreement) auf dem vom Firepower Management Center (FMC) verwalteten Firepower Threat Defense (FTD) konfigurieren. Außerdem wird erläutert, wie die Network Address Translation (NAT)-Ausnahme für den VPN-Datenverkehr konfiguriert wird, wenn zwei ISPs vorhanden sind und ein nahtloses Failover erforderlich ist.

In diesem Szenario wird das VPN vom FTD aus in Richtung ASA als VPN-Peer mit nur einer ISP-Schnittstelle eingerichtet. Die FTD nutzt jeweils eine ISP-Verbindung, um das VPN einzurichten. Wenn die primäre ISP-Verbindung ausfällt, übernimmt die FTD die Rolle der sekundären ISP-Verbindung über den SLA Monitor und das VPN wird eingerichtet.

Konfigurieren

Netzwerkdiagramm

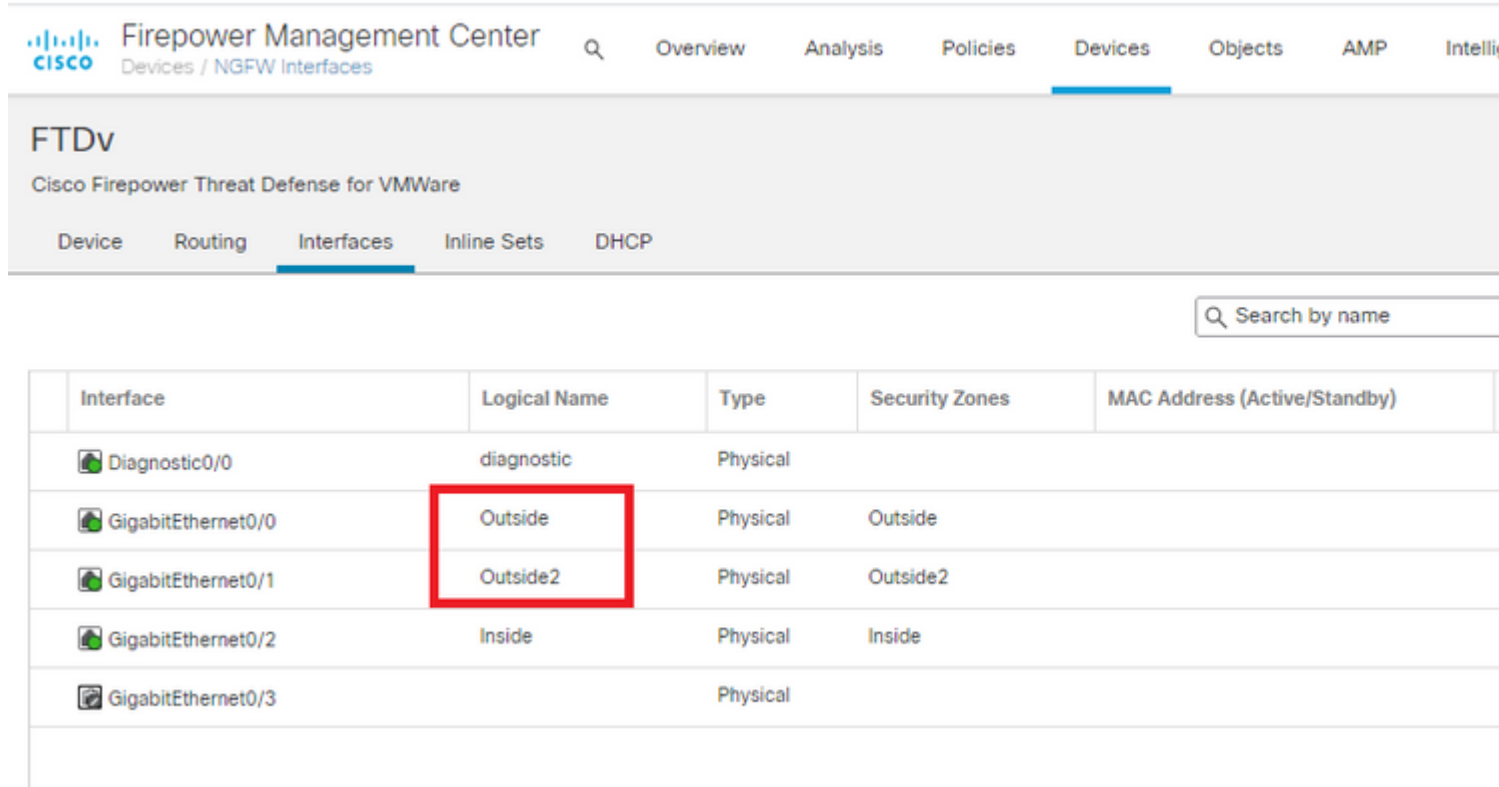
Dies ist die Topologie, die im gesamten Dokument für dieses Beispiel verwendet wird:



FTD konfigurieren

Schritt 1: Definieren der primären und sekundären ISP-Schnittstellen

1. Navigieren Sie zu **Devices (Geräte) > Device Management (Geräteverwaltung) > Interfaces (Schnittstellen)**, wie im Bild dargestellt.



Schritt 2: Definieren der VPN-Topologie für die primäre ISP-Schnittstelle

1. Navigieren Sie zu **Geräte > VPN > Site-to-Site**. Klicken Sie unter **VPN hinzufügen** auf **Firepower Threat Defense Device**, erstellen Sie das VPN, und wählen Sie die externe Schnittstelle aus.

Hinweis: In diesem Dokument wird nicht beschrieben, wie Sie ein S2S-VPN von Grund auf konfigurieren. Weitere Informationen zur S2S-VPN-Konfiguration auf FTD finden Sie unter <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:

IKE Version:* IKEv1 IKEv2

Endpoints

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.

Schritt 3: Definieren der VPN-Topologie für die sekundäre ISP-Schnittstelle

1. Navigieren Sie zu **Geräte > VPN > Site-to-Site**. Klicken Sie unter **VPN hinzufügen** auf **FirePOWER Threat Defense Device**, erstellen Sie das VPN, und wählen Sie die Outside2-Schnittstelle aus.

Hinweis: Die VPN-Konfiguration, die die Outside2-Schnittstelle verwendet, muss mit Ausnahme der VPN-Schnittstelle exakt mit der Outside VPN-Topologie übereinstimmen.

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-Topologien müssen wie im Bild dargestellt konfiguriert werden.

Firepower Management Center Overview Analysis Policies **Devices** Objects AMP Intelli

Devices / VPN / Site To Site

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

Schritt 4: Konfigurieren des SLA-Monitors

1. Navigieren Sie zu **Objekte > SLA-Monitor > SLA-Monitor hinzufügen**. Klicken Sie unter **VPN hinzufügen** auf **FirePOWER Threat Defense Device**, und konfigurieren Sie den SLA-Monitor wie im Bild dargestellt.

Firepower Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** AMP Intell

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

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. 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: 10.20

Add SLA Monitor

2. Verwenden Sie für das Feld "SLA Monitor ID*" die Next-Hop-IP-Adresse für den externen Server.

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


Selected Zones/Interfaces


Schritt 5: Konfigurieren der statischen Routen mithilfe des SLA-Monitors

1. Navigieren Sie zu **Geräte > Routing > Statische Route**. Wählen Sie **Add Route (Route hinzufügen)** aus, und konfigurieren Sie die Standardroute für die externe (primäre) Schnittstelle mit den Informationen zum SLA-Monitor (erstellt in Schritt 4) im Feld **Route Tracking (Routenverfolgung)**.

Edit Static Route Configuration

Type: IPv4 IPv6


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

Available Network  +

Selected Network

Q Search

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

any-ipv4 

Gateway*
10.200.1.1 +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)


Route Tracking:
ISP_Outside1 +


2. Konfigurieren Sie die Standardroute für die Outside2-Schnittstelle (sekundär). Der Metrikwert muss höher als die primäre Standardroute sein. In diesem Abschnitt ist kein Feld zur **Routenverfolgung** erforderlich.

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

Add

any-ipv4

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

Gateway*
10.201.1.1 +

Metric:
2
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

Die Routen müssen wie im Bild dargestellt konfiguriert werden.



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

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

Schritt 6: Konfigurieren der NAT-Ausnahme

1. Navigieren Sie zu **Devices > NAT > NAT Policy**, und wählen Sie die Policy aus, die auf das FTD-Gerät abzielt. Wählen Sie **Add Rule (Regel hinzufügen)** aus, und konfigurieren Sie eine NAT-Ausnahme pro ISP-Schnittstelle (Outside und Outside2). Die NAT-Regeln müssen bis auf die Zielschnittstelle identisch sein.



NAT_FTDv

Enter Description

Rules

[Filter by Device](#)

#	Direction	Type	Source Interface	Destination Interface	Original Packet			Translated		
					Original Sources	Original Destinations	Original Services	Sources	Destinations	
NAT Rules Before										
1	↔	Static	Inside	Outside	10.10.10.0	192.168.100.1		10.10.10.0	192.168.100.1	
2	↔	Static	Inside	Outside2	10.10.10.0	192.168.100.1		10.10.10.0	192.168.100.1	
Auto NAT Rules										
NAT Rules After										

Hinweis: In diesem Szenario müssen beide NAT-Regeln die **Routensuche** aktivieren. Andernfalls würde der Datenverkehr die erste Regel erfüllen und sich nicht an die Failover-Routen halten. Wenn die Routensuche nicht aktiviert ist, wird der Datenverkehr immer mithilfe der externen Schnittstelle (erste NAT-Regel) gesendet. Bei aktivierter **Routensuche** bleibt der Datenverkehr stets bei der Routing-Tabelle, die durch den SLA Monitor gesteuert wird.

Schritt 7. Konfigurieren der Zugriffskontrollrichtlinie für interessanten Datenverkehr

1. Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Wählen Sie die Zugriffskontrollrichtlinie aus**. Um eine Regel hinzuzufügen, klicken Sie auf **Regel hinzufügen**, wie in der Abbildung dargestellt.

Konfigurieren Sie eine Regel zwischen den Zonen Inside (Innen) und Outside2 (Außen1 und Outside2), die den interessierten Datenverkehr von 10.10.10.0/24 nach 192.168.100/24 zulässt.

Konfigurieren Sie eine weitere Regel von den externen Zonen (Outside1 und Outside 2) nach Inside, die den interessanten Datenverkehr von 192.168.100/24 nach 10.10.10.0/24 zulässt.



ACP-FTDv

Enter Description

Rules Security Intelligence HTTP Responses Logging Advanced

Prefilter Policy: Default Prefilter

Filter by Device

Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source SGT
Mandatory - ACP-FTDv (1-2)												
1	VPN_1_out	Inside	Outside Outside2	10.10.10.0	192.168.100.0	Any	Any	Any	Any	Any	Any	Any
2	VPN_1_in	Outside2 Outside	Inside	192.168.100.0	10.10.10.0	Any	Any	Any	Any	Any	Any	Any

Default - ACP-FTDv (-)

There are no rules in this section. [Add Rule](#) or [Add Category](#)

Default Action

Konfigurieren der ASA

Hinweis: Für dieses spezielle Szenario wird in der IKEv2-Krypto-Map ein Backup-Peer konfiguriert. Für diese Funktion muss die ASA Version 9.14.1 oder höher sein. Wenn auf Ihrer ASA eine ältere Version ausgeführt wird, verwenden Sie IKEv1 als Problemumgehung. Weitere Informationen finden Sie unter Cisco Bug-ID [CSCud22276](#).

1. Aktivieren Sie IKEv2 auf der externen Schnittstelle der ASA:

```
Crypto ikev2 enable Outside
```

2. Erstellen Sie die IKEv2-Richtlinie, die dieselben Parameter definiert, die auch für das FTD konfiguriert wurden:

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

3. Erstellen Sie eine Gruppenrichtlinie, um das Protokoll ikev2 zuzulassen:

```
group-policy IKEV2 internal
```

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

4. Erstellen Sie eine Tunnelgruppe für jede externe FTD-IP-Adresse (Outside1 und Outside2). Verweisen Sie auf die Gruppenrichtlinie, und geben Sie den Pre-Shared Key an:

```
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. Erstellen Sie eine Zugriffsliste, die den zu verschlüsselnden Datenverkehr definiert: (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. Erstellen Sie einen ikev2 ipsec-Vorschlag, um auf die Algorithmen zu verweisen, die auf der FTD spezifiziert sind:

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

7. Erstellen Sie einen Crypto Map-Eintrag, der die Konfiguration verknüpft, und fügen Sie die FTD-IP-Adressen Outside1 und Outside2 hinzu:

```
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. Erstellen Sie eine NAT-Ausnahmegenehmigung, die verhindert, dass der VPN-Datenverkehr von der Firewall mit NATTED versehen wird:

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

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

FTD

Verwenden Sie in der Befehlszeile den Befehl **show crypto ikev2 as**, um den VPN-Status zu überprüfen.

Hinweis: VPN wird mit der IP-Adresse von Outside1 (10.200.1.5) als lokal eingerichtet.

```
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
```

Routing

Die Standardroute zeigt die Next-Hop-IP-Adresse von Outside1.

```
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
```

Spur

Wie in der Ausgabe von Titel 1 zu sehen, "Reachability is Up" (Erreichbarkeit aktiviert).

```
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

Sie wird benötigt, um zu bestätigen, dass der interessante Datenverkehr die NAT-Ausnahmeregelung mit der Outside1-Schnittstelle erreicht.

Verwenden Sie den Befehl "packet-tracer input Inside icmp 10.10.10.1 8 0 192.168.100.10 detail", um die für den interessantesten Datenverkehr angewendete NAT-Regel zu überprüfen.

```
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

Failover durchführen

In diesem Beispiel erfolgt das Failover durch ein Herunterfahren des Next Hop von Outside1, der in der IP SLA-Monitorkonfiguration verwendet wird.

```
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:
```

Routing

Die Standardroute verwendet nun die Next-Hop-IP-Adresse von Outside2, und die Erreichbarkeit ist nicht verfügbar.

```
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
```

Spur

Wie in der Ausgabe von **show track 1** zu sehen, ist "Reachability is Down" (Erreichbarkeit ist zu diesem Zeitpunkt nicht verfügbar).

```
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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.