

Configurer le basculement ISP double pour FTD géré par FMC

Table des matières

- [Introduction](#)
- [Conditions préalables](#)
- [Exigences](#)
- [Composants utilisés](#)
- [Informations générales](#)
- [Présentation de la fonction de suivi de route statique](#)
- [Configurer](#)
- [Diagramme du réseau](#)
- [Configurations](#)
- [Vérifier](#)
- [Informations connexes](#)

Introduction

Ce document décrit comment configurer le basculement de FAI DUAL avec PBR et les SLA IP sur un FTD qui est géré par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Routage basé sur des politiques (PBR)
- Contrat de niveau de service du protocole Internet (IP SLA)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FMCv 7.3.0
- FTDv 7.3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Présentation de la fonction de suivi de route statique

La fonctionnalité de suivi de route statique permet au FTD d'utiliser une connexion à un FAI secondaire dans le cas où la ligne louée principale deviendrait indisponible. Afin d'atteindre cette redondance, le FTD associe une route statique à une cible de surveillance que vous définissez. L'opération SSLA surveille la cible avec des requêtes d'écho ICMP périodiques.

Si aucune réponse d'écho n'est reçue, l'objet est considéré comme inactif et la route associée est supprimée de la table de routage. Une route de secours précédemment configurée est utilisée au lieu de la route qui est retirée. Pendant l'utilisation de la route de secours, l'opération de surveillance SLA poursuit ses tentatives d'atteindre la cible de surveillance.

Une fois que la cible est de nouveau disponible, la première route est substituée dans la table de routage, et la route de secours est retirée.

Vous pouvez désormais configurer simultanément plusieurs sauts suivants et des actions de transfert de routage basées sur des stratégies. Lorsque le trafic correspond aux critères de la route, le système tente de transférer le trafic vers les adresses IP dans l'ordre que vous spécifiez, jusqu'à ce qu'il réussisse.

Cette fonctionnalité est disponible sur les périphériques FTD exécutant les versions 7.1 et ultérieures gérées par un FMC version 7.3 et ultérieures.

Configurer

Diagramme du réseau

Cette illustration donne un exemple de diagramme de réseau.

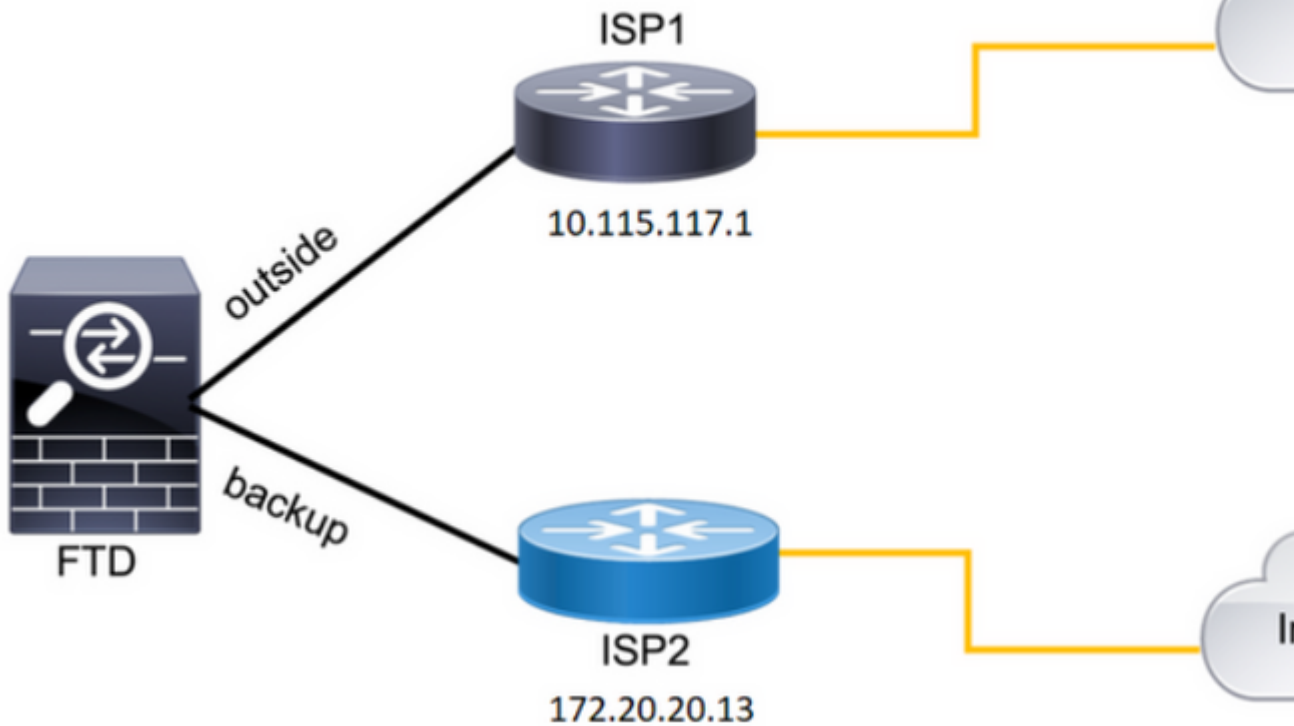


Image 1. Exemple de schéma.

FAI1 = 10.115.117.1

FAI2 = 172.20.20.13

Configurations

Étape 1. Configurez les objets SLA Monitor.

Sur le FMC, accédez à Object > Object Management > SLA Monitor > Add SLA Monitor et ajoutez un objet SLA Monitor pour les adresses IP ISP.

Moniteur SLA pour la passerelle principale par défaut (ISP1).

The screenshot shows the 'Edit SLA Monitor Object' configuration page in the FMC. The page contains the following fields and values:

Field	Value
Name:	SAL1
Description:	
Frequency (seconds):	60
SLA Monitor ID*:	1
Threshold (milliseconds):	5000
Timeout (milliseconds):	5000
Data Size (bytes):	28
ToS:	0
Number of Packets:	1
Monitor Address*:	10.115.117.1

```
route-map FMC_GENERATED_PBR_1679065711925
, permit, sequence 5
Match clauses:
ip address (access-lists): internal_networks

Set clauses:
ip next-hop verify-availability 10.115.117.1 1
track 1 [up]

ip next-hop 10.115.117.234
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr

Set clauses:
ip next-hop verify-availability 172.20.20.13 2
track 2 [up]

ip next-hop 172.20.20.77
firepower#
```

- show running-config sla monitor: cette commande affiche la configuration SLA.

```
<#root>
firepower#
show running-config sla monitor

sla monitor 1

type echo protocol ipIcmpEcho 10.115.117.1 interface outside
sla monitor schedule 1 life forever start-time now

sla monitor 2

type echo protocol ipIcmpEcho 172.20.20.13 interface backup
sla monitor schedule 2 life forever start-time now
firepower#
```

- show sla monitor configuration: cette commande affiche les valeurs de configuration SLA.

```
<#root>
firepower#
show sla monitor configuration
```

SA Agent, Infrastructure Engine-II
Entry number:

1

Owner:
Tag:
Type of operation to perform: echo
Target address: 10.115.117.1

Interface: outside
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:

Entry number:

2

Owner:
Tag:
Type of operation to perform: echo
Target address: 172.20.20.13

Interface: backup
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:

- show sla monitor operational-state: cette commande affiche l'état opérationnel de l'opération SLA.

<#root>

firepower#

```
show sla monitor operational-state
```

```
Entry number: 1
```

```
Modification time: 15:48:04.332 UTC Fri Mar 17 2023  
Number of Octets Used by this Entry: 2056  
Number of operations attempted: 74  
Number of operations skipped: 0  
Current seconds left in Life: Forever
```

```
Operational state of entry: Active
```

```
Last time this entry was reset: Never  
Connection loss occurred: FALSE  
Timeout occurred: FALSE  
Over thresholds occurred: FALSE  
Latest RTT (milliseconds): 1  
Latest operation start time: 17:01:04.334 UTC Fri Mar 17 2023  
Latest operation return code: OK  
RTT Values:  
RTTAvg: 1 RTTMin: 1 RTTMax: 1  
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

```
Entry number: 2
```

```
Modification time: 15:48:04.335 UTC Fri Mar 17 2023  
Number of Octets Used by this Entry: 2056  
Number of operations attempted: 74  
Number of operations skipped: 0  
Current seconds left in Life: Forever
```

```
Operational state of entry: Active
```

```
Last time this entry was reset: Never  
Connection loss occurred: FALSE  
Timeout occurred: FALSE  
Over thresholds occurred: FALSE  
Latest RTT (milliseconds): 1  
Latest operation start time: 17:01:04.337 UTC Fri Mar 17 2023  
Latest operation return code: OK  
RTT Values:  
RTTAvg: 1 RTTMin: 1 RTTMax: 1  
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

- show track: cette commande affiche les informations relatives aux objets suivis par le processus de suivi SLA.

```
<#root>
```

```
firepower#
```

```
show track
```

Track 1

Response Time Reporter 1 reachability

Reachability is Up

4 changes, last change 00:53:42
Latest operation return code: OK
Latest RTT (milliseconds) 1
Tracked by:
ROUTE-MAP 0
STATIC-IP-ROUTING 0

Track 2

Response Time Reporter 2 reachability

Reachability is Up

2 changes, last change 01:13:41
Latest operation return code: OK
Latest RTT (milliseconds) 1
Tracked by:
ROUTE-MAP 0
STATIC-IP-ROUTING 0

- show running-config route: cette commande affiche la configuration de route actuelle.

```
<#root>
```

```
firepower#
```

```
show running-config route
```

```
route
```

```
outside
```

```
0.0.0.0 0.0.0.0 10.115.117.1 1
```

```
track 1
```

```
route
```

```
backup
```

```
0.0.0.0 0.0.0.0 172.20.20.13 254
```

```
track 2
```

```
route vlan2816 10.42.0.37 255.255.255.255 10.43.0.1 254
```

```
firepower#
```

- show route: cette commande affiche la table de routage pour les interfaces de données.

```
<#root>
```

```
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 10.115.117.1 to network 0.0.0.0
```

```
s* 0.0.0.0 0.0.0.0 [1/0] via 10.115.117.1, outside
```

```
S 10.0.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone  
C 10.88.243.0 255.255.255.0 is directly connected, backbone  
L 10.88.243.67 255.255.255.255 is directly connected, backbone  
C 10.115.117.0 255.255.255.0 is directly connected, outside  
L 10.115.117.234 255.255.255.255 is directly connected, outside  
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816  
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816  
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816  
C 172.20.20.0 255.255.255.0 is directly connected, backup  
L 172.20.20.77 255.255.255.255 is directly connected, backup
```

En cas de défaillance de la liaison principale :

- show route-map: cette commande affiche la configuration route-map lorsqu'une liaison échoue.

```
<#root>
```

```
firepower#
```

```
show route-map FMC_GENERATED_PBR_1679065711925
```

```
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 5  
Match clauses:  
ip address (access-lists): internal_networks  
  
Set clauses:  
ip next-hop verify-availability 10.115.117.1 1  
  
track 1 [down]
```

```
ip next-hop 10.115.117.234
```



```

route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr

Set clauses:
ip next-hop verify-availability 172.20.20.13 2

track 2 [up]

ip next-hop 172.20.20.77
firepower#

```

- `show route`: cette commande affiche la nouvelle table de routage par interface.

```
<#root>
```

```
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 10.115.117.1 to network 0.0.0.0

```

```
s* 0.0.0.0 0.0.0.0 [1/0] via 172.20.20.13, backup
```

```

S 10.0.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone
C 10.88.243.0 255.255.255.0 is directly connected, backbone
L 10.88.243.67 255.255.255.255 is directly connected, backbone
C 10.115.117.0 255.255.255.0 is directly connected, outside
L 10.115.117.234 255.255.255.255 is directly connected, outside
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816
C 172.20.20.0 255.255.255.0 is directly connected, backup
L 172.20.20.77 255.255.255.255 is directly connected, backup

```

Informations connexes

- [Guide d'administration de Cisco Secure Firewall Management Center, 7.3](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.