

Configuration d'ECMP avec IP SLA sur FTD géré par FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Étape 0. Préconfigurer les interfaces/objets réseau](#)

[Étape 1. Configuration de la zone ECMP](#)

[Étape 2. Configurer des objets IP SLA](#)

[Étape 3. Configuration de routes statiques avec route track](#)

[Vérifier](#)

[Équilibrage de charge](#)

[Route perdue](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer ECMP avec IP SLA sur un FTD qui est géré par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration ECMP sur Cisco Secure Firewall Threat Defense (FTD)
- Configuration IP SLA sur Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)

Composants utilisés

Les informations contenues dans ce document sont basées sur la version logicielle et matérielle suivante :

- Cisco FTD version 7.4.1

- Cisco FMC version 7.4.1

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

Ce document décrit comment configurer Equal-Cost Multi-Path (ECMP) avec le contrat de niveau de service de protocole Internet (IP SLA) sur un FTD Cisco géré par Cisco FMC. ECMP vous permet de regrouper des interfaces sur FTD et d'équilibrer la charge du trafic sur plusieurs interfaces. IP SLA est un mécanisme qui surveille la connectivité de bout en bout par l'échange de paquets réguliers. Parallèlement à ECMP, IP SLA peut être mis en oeuvre afin de garantir la disponibilité du tronçon suivant. Dans cet exemple, le protocole ECMP est utilisé pour distribuer les paquets de manière égale sur deux circuits de fournisseur d'accès Internet (FAI).

Parallèlement, un IP SLA assure le suivi de la connectivité, assurant une transition transparente vers tous les circuits disponibles en cas de panne.

Les exigences spécifiques de ce document sont les suivantes :

- Accès aux périphériques avec un compte utilisateur avec des privilèges d'administrateur
- Cisco Secure Firewall Threat Defense version 7.1 ou ultérieure
- Cisco Secure Firewall Management Center version 7.1 ou ultérieure

Configurer

Diagramme du réseau

Dans cet exemple, Cisco FTD a deux interfaces externes : outside1 et outside2. Chacun se connecte à une passerelle ISP, outside1 et outside2 appartiennent à la même zone ECMP nommée outside.

Le trafic provenant du réseau interne est acheminé via FTD et la charge est équilibrée sur Internet via les deux FAI.

Dans le même temps, FTD utilise des SLA IP afin de surveiller la connectivité à chaque passerelle ISP. En cas de défaillance sur l'un des circuits du FAI, le FTD bascule vers l'autre passerelle du FAI pour assurer la continuité des activités.

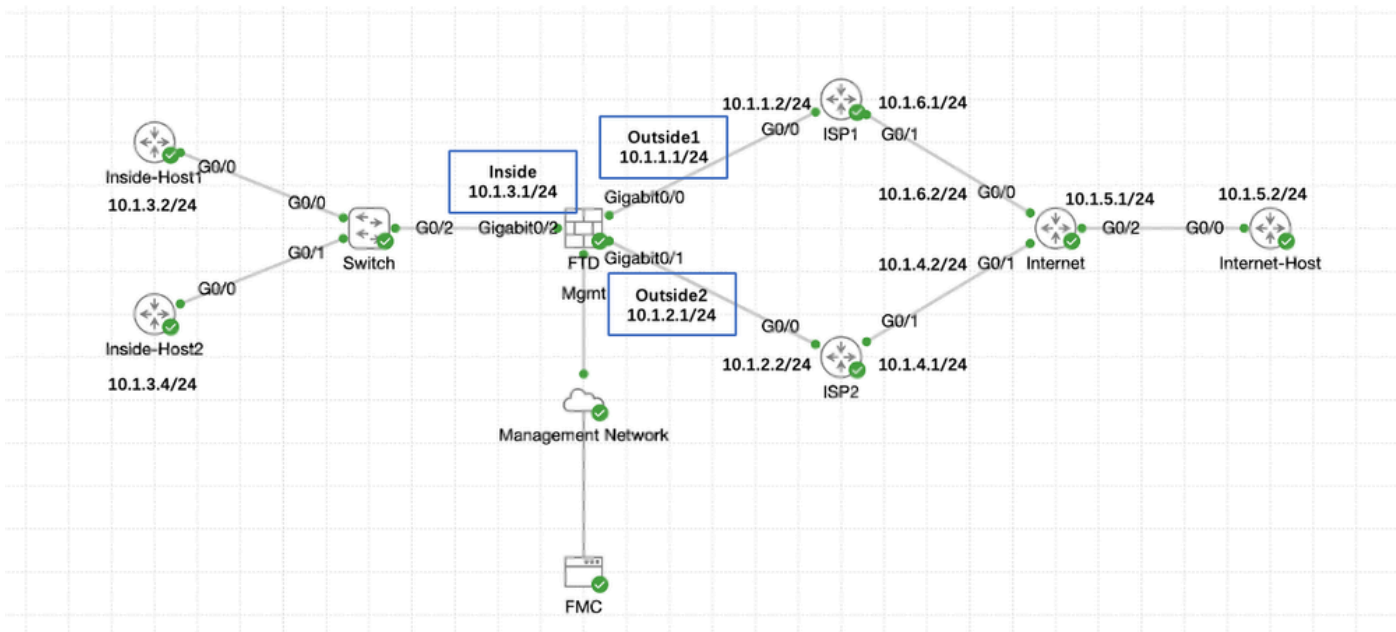


Diagramme du réseau

Configurations

Étape 0. Préconfigurer les interfaces/objets réseau

Connectez-vous à l'interface utilisateur graphique Web de FMC, sélectionnez **Devices>Device Management** et cliquez sur le bouton **Edit** pour votre périphérique de défense contre les menaces. La page **Interfaces** est sélectionnée par défaut. Cliquez sur le bouton **Edit** pour l'interface que vous souhaitez modifier, dans cet exemple **GigabitEthernet0/0**.

The screenshot shows the FMC web interface for configuring the GigabitEthernet0/0 interface. The breadcrumb navigation is **Devices > Secure Firewall Interfaces > Overview > Analysis > Policies > Devices > Objects > Integration**. The current page is **Interfaces** for the device **10.106.32.250**. The interface list table is as follows:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↶
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎
GigabitEthernet0/3		Physical				Disabled		✎
GigabitEthernet0/4		Physical				Disabled		✎
GigabitEthernet0/5		Physical				Disabled		✎
GigabitEthernet0/6		Physical				Disabled		✎
GigabitEthernet0/7		Physical				Disabled		✎

At the bottom of the page, it says "Displaying 1-9 of 9 interfaces" and "Page 1 of 1".

Modifier l'interface Gi0/0

Dans la fenêtre Edit Physical Interface, sous l'onglet General :

1. Définissez le Name, dans ce cas Outside1.
2. Activez l'interface en cochant la case Enabled.
3. Dans la liste déroulante Security Zone, sélectionnez une zone de sécurité existante ou créez-en une nouvelle, dans cet exemple Outside1_Zone.

Edit Physical Interface ?

General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Outside1

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Outside1_Zone

Interface ID:
GigabitEthernet0/0

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Interface Gi0/0 Générale

Sous l'onglet IPv4 :

1. Choisissez l'une des options de la liste déroulante IP Type, dans cet exemple Use Static IP.
2. Définissez l'adresse IP, dans cet exemple 10.1.1.1/24.
3. Click OK.

Edit Physical Interface



General **IPv4** IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use Static IP

IP Address:
10.1.1.1/24
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Cancel OK

Interface Gi0/0 IPv4

Répétez l'étape similaire pour configurer l'interface GigabitEthernet0/1, Dans la fenêtre Edit Physical Interface, sous l'onglet General :

1. Définissez le Nom, dans ce cas Outside2.
2. Activez l'interface en cochant la case Enabled.
3. Dans la liste déroulante Security Zone, sélectionnez une zone de sécurité existante ou créez-en une nouvelle, dans cet exemple Outside2_Zone.

Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Outside2

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Outside2_Zone

Interface ID:
GigabitEthernet0/1

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Cancel OK

Interface Gi0/1 Générale

Sous l'onglet IPv4 :

1. Choisissez l'une des options de la liste déroulante IP Type, dans cet exemple Use Static IP.
2. Définissez l'adresse IP, dans cet exemple 10.1.2.1/24.
3. Click OK.

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use Static IP

IP Address:
10.1.2.1/24

eg. 192.0.2.1/24, 2001:db8:2001:1::1/64, 192.0.2.1/24

Cancel OK

Interface Gi0/1 IPv4

Répétez l'étape similaire pour configurer l'interface GigabitEthernet0/2, Dans la fenêtre Edit Physical Interface, sous l'onglet General :

1. Définissez le Nom, dans ce cas Inside.
2. Activez l'interface en cochant la case Enabled.
3. Dans la liste déroulante Security Zone, sélectionnez une zone de sécurité existante ou créez-en une nouvelle, dans cet exemple Inside_Zone.

Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Inside

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Inside_Zone

Interface ID:
GigabitEthernet0/2

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Cancel OK

Interface Gi0/2 Générale

Sous l'onglet IPv4 :

1. Choisissez l'une des options de la liste déroulante IP Type, dans cet exemple Use Static IP.
2. Définissez l'adresse IP, dans cet exemple 10.1.3.1/24.
3. Click OK.

Edit Physical Interface

General **IPv4** IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use Static IP

IP Address:
10.1.3.1/24

Cancel OK

Interface Gi0/2 IPv4

Cliquez sur Save and Deploy the configuration.

Accédez à Objets > Gestion des objets, choisissez Réseau dans la liste des types d'objet, choisissez Ajouter un objet dans le menu déroulant Ajouter un réseau pour créer un objet pour la première passerelle ISP.

Firewall Management Center

Overview Analysis Policies Devices **Objects** Integration

Deploy Filter admin **SECURE**

Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network event searches, reports, and so on.

Add Network
Add Object
Import Object
Add Group

Name	Value	Type	Override
any	0.0.0.0/0 :::0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	:::0	Host	
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	:::ffff:0.0.0.0/96	Network	
IPv6-Link-Local	fe80::/10	Network	
IPv6-Private-Unique-Local-Addresses	fc00::/7	Network	
IPv6-to-IPv4-Relay-Anycast	192.68.99.0/24	Network	

Displaying 1 - 14 of 14 rows Page 1 of 1

objet réseau

Dans la fenêtre Nouvel objet réseau :

1. Définissez le Name, dans cet exemple gw-outside1.
2. Dans le champ Network, sélectionnez l'option requise et entrez une valeur appropriée, dans cet exemple Host et 10.1.1.2.

3. Cliquez sur Save.

New Network Object

Name

gw-outside1

Description

Network

Host Range Network FQDN

10.1.1.2

Allow Overrides

Cancel Save

Objet Gw-outside1

Répétez les étapes similaires pour créer un autre objet pour la deuxième passerelle ISP. Dans la fenêtre Nouvel objet réseau :

1. Définissez le Nom, dans cet exemple gw-outside2.
2. Dans le champ Network, sélectionnez l'option requise et entrez une valeur appropriée, dans cet exemple Host et 10.1.2.2.
3. Cliquez sur Save.

New Network Object



Name

gw-outside2

Description

Network



Host



Range



Network



FQDN

10.1.2.2



Allow Overrides

Cancel

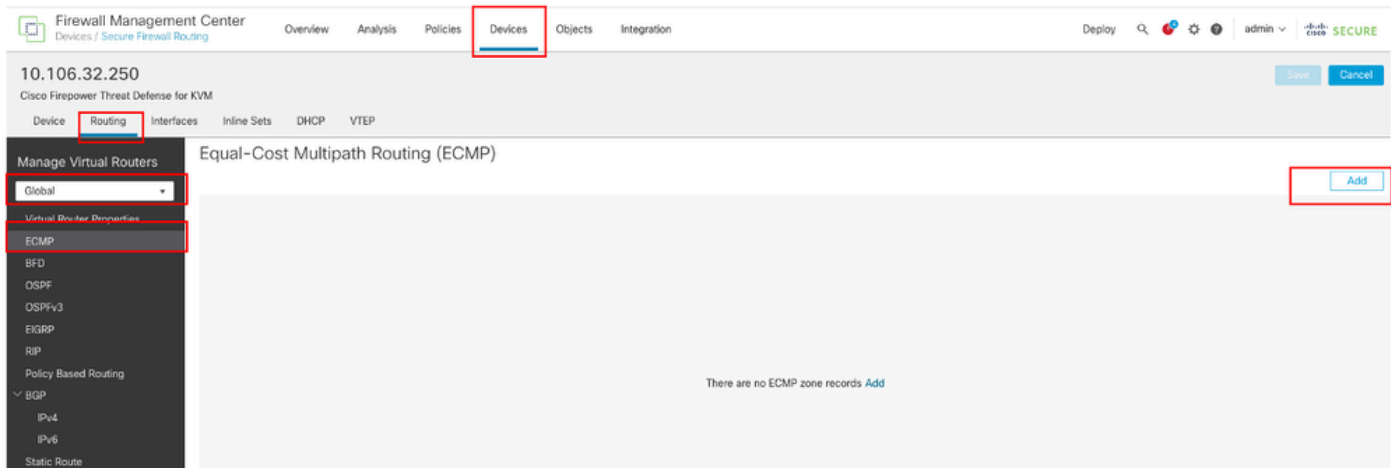
Save

Objet Gw-outside2

Étape 1. Configuration de la zone ECMP

Accédez à **Devices > Device Management** et modifiez le périphérique de défense contre les menaces, cliquez sur **Routing**. Dans la liste déroulante **virtual router**, sélectionnez le routeur virtuel dans lequel vous souhaitez créer la zone ECMP. Vous pouvez créer des zones ECMP dans les routeurs virtuels globaux et les routeurs virtuels définis par l'utilisateur. Dans cet exemple, choisissez **Global**.

Cliquez sur **ECMP**, puis sur **Add**.



Configuration de la zone ECMP

Dans la fenêtre Add ECMP :

1. Définissez Name pour la zone ECMP, dans cet exemple Outside.
2. Pour associer des interfaces, sélectionnez l'interface dans la zone Available Interfaces, puis cliquez sur Add. Dans cet exemple, Outside1 et Outside2.
3. Click OK.

Add ECMP



Name
Outside

Available Interfaces
Inside

Selected Interfaces
Outside1
Outside2

Add

Cancel OK

Configuration de la zone ECMP externe

Cliquez sur Save and Deploy the configuration.

Étape 2. Configurer des objets IP SLA

Accédez à Objects > Object Management, choisissez SLA Monitor dans la liste des types d'objet, cliquez sur Add SLA Monitor pour ajouter un nouveau SLA Monitor pour la première passerelle ISP.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 SECURE

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
No records to display	

AAA Server
Access List
Address Pools
Application Filters
AS Path
BFD Template
Cipher Suite List
Community List
DHCP IPv6 Pool
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
Route Map
Security Intelligence
SLA Monitor
Time Range

Créer un moniteur SLA

Dans la fenêtre Nouvel objet SLA Monitor :

1. Définissez le Name pour l'objet de surveillance SLA, dans ce cas sla-outside1.
2. Saisissez le numéro d'ID de l'opération SLA dans le champ SLA Monitor ID. Les valeurs sont comprises entre 1 et 2147483647. Vous pouvez créer un maximum de 2 000 opérations SLA sur un périphérique. Chaque numéro d'ID doit être unique pour la stratégie et la configuration du périphérique. Dans cet exemple, 1.
3. Dans le champ Adresse surveillée, saisissez l'adresse IP surveillée pour la disponibilité par l'opération SLA. Dans cet exemple, 10.1.1.2.
4. La liste Available Zones/Interfaces affiche à la fois les zones et les groupes d'interfaces. Dans la liste Zones/Interfaces, ajoutez les zones ou les groupes d'interfaces qui contiennent les interfaces par lesquelles le périphérique communique avec la station de gestion. Pour spécifier une interface unique, vous devez créer une zone ou les groupes d'interfaces pour l'interface. Dans cet exemple, Outside1_Zone.
5. Cliquez sur Save.

New 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/interfaces



Inside_Zone

Outside1_Zone

Outside2_Zone

Add

Selected Zones/interfaces

Outside1_Zone



Cancel

Save

SLA, objet SLA-outside1

Répétez les étapes similaires pour créer un autre moniteur SLA pour la deuxième passerelle ISP.

Dans la fenêtre Nouvel objet SLA Monitor :

1. Définissez le Nom pour l'objet de surveillance SLA, dans ce cas sla-outside2.
2. Saisissez le numéro d'ID de l'opération SLA dans le champ SLA Monitor ID. Les valeurs sont comprises entre 1 et 2147483647. Vous pouvez créer un maximum de 2 000 opérations SLA sur un périphérique. Chaque numéro d'ID doit être unique pour la stratégie et la configuration du périphérique. Dans cet exemple, 2.
3. Dans le champ Adresse surveillée, saisissez l'adresse IP surveillée pour la disponibilité par l'opération SLA. Dans cet exemple, 10.1.2.2.
4. La liste Available Zones/Interfaces affiche à la fois les zones et les groupes d'interfaces. Dans la liste Zones/Interfaces, ajoutez les zones ou les groupes d'interfaces qui contiennent les interfaces par lesquelles le périphérique communique avec la station de gestion. Pour spécifier une interface unique, vous devez créer une zone ou les groupes d'interfaces pour l'interface. Dans cet exemple, Outside2_Zone.
5. Cliquez sur Save.

New SLA Monitor Object



Name:

sla-outside2

Description:

Frequency (seconds):

60

{1-604800}

SLA Monitor ID*:

2

Threshold (milliseconds):

{0-60000}

Timeout (milliseconds):

5000

{0-604800000}

Data Size (bytes):

20

{0-16384}

ToS:

Number of Packets:

1

Monitor Address*:

10.1.2.2

Available Zones/Interfaces

Q Search

Inside_Zone

Outside1_Zone

Outside2_Zone

Add

Selected Zones/Interfaces

Outside1_Zone

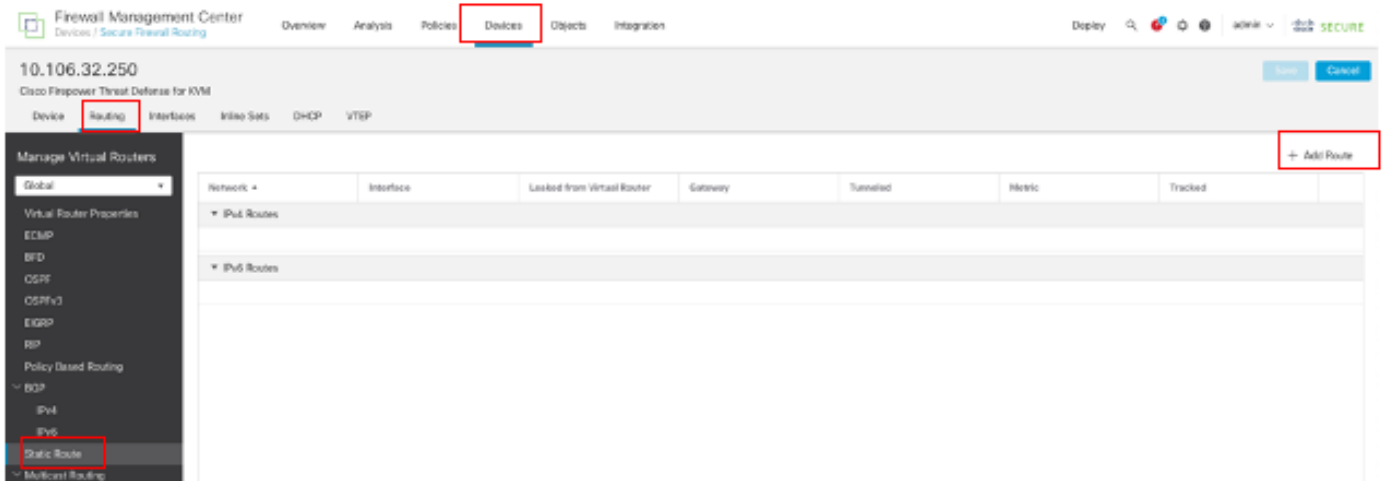
Cancel

Save

Étape 3. Configuration de routes statiques avec route track

Accédez à Devices > Device Management, et modifiez le périphérique de défense contre les menaces, cliquez sur Routing, Dans la liste déroulante virtual routers, sélectionnez le routeur virtuel pour lequel vous configurez une route statique. Dans cet exemple, Global.

Sélectionnez Static Route, cliquez sur Add Route pour ajouter la route par défaut à la première passerelle ISP.



Configurer la route statique


Dans la fenêtre Ajouter une configuration de route statique :


1. Cliquez sur IPv4 ou IPv6 selon le type de route statique que vous ajoutez. Dans cet exemple, IPv4.
2. Choisissez l'interface à laquelle cette route statique s'applique. Dans cet exemple, Outside1.
3. Dans la liste Available Network, sélectionnez le réseau de destination. Dans cet exemple, any-ipv4.
4. Dans le champ Gateway ou IPv6 Gateway, entrez ou sélectionnez le routeur de passerelle qui est le tronçon suivant pour cette route. Vous pouvez fournir une adresse IP ou un objet Réseaux/Hôtes. Dans cet exemple, gw-outside1.
5. Dans le champ Metric, saisissez le nombre de sauts vers le réseau de destination. Les valeurs valides sont comprises entre 1 et 255 ; la valeur par défaut est 1. Dans cet exemple, 1.
6. Pour surveiller la disponibilité de la route, saisissez ou sélectionnez le nom d'un objet SLA Monitor qui définit la politique de surveillance, dans le champ Suivi de route. Dans cet exemple, sla-outside1.
7. Click OK.

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
Outside1

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

Available Network  + Selected Network

Search

any-ipv4
gw-outside1
gw-outside2
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast

Add

any-ipv4

Gateway*
gw-outside1 +

Metric:
1

(1 = 254)

Tunneled: (Used only for default Routes)

Route Tracking:
sla-outside1 +

Cancel OK

Ajouter le premier FAI de route statique

Répétez les étapes similaires pour ajouter la route par défaut à la deuxième passerelle ISP. Dans la fenêtre Ajouter une configuration de route statique :

1. Cliquez sur IPv4 ou IPv6 selon le type de route statique que vous ajoutez. Dans cet exemple, IPv4.
2. Choisissez l'interface à laquelle cette route statique s'applique. Dans cet exemple, Outside2.

3. Dans la liste Available Network, sélectionnez le réseau de destination. Dans cet exemple, any-ipv4.
4. Dans le champ Gateway ou IPv6 Gateway, entrez ou sélectionnez le routeur de passerelle qui est le tronçon suivant pour cette route. Vous pouvez fournir une adresse IP ou un objet Réseaux/Hôtes. Dans cet exemple, gw-outside2.
5. Dans le champ Metric, saisissez le nombre de sauts vers le réseau de destination. Les valeurs valides sont comprises entre 1 et 255 ; la valeur par défaut est 1. Assurez-vous de spécifier la même métrique que la première route, dans cet exemple 1.
6. Pour surveiller la disponibilité de la route, saisissez ou sélectionnez le nom d'un objet SLA Monitor qui définit la politique de surveillance, dans le champ Suivi de route. Dans cet exemple, sla-outside2.
7. Click OK.

Add Static Route Configuration



Type: IPv4 IPv6

Interface*

Outside2

[Interface starting with this icon  signifies it is available for route leak]

Available Network 



Selected Network

Q Search

Add

any-ipv4

any-ipv4

gw-outside1

gw-outside2

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

Gateway*

gw-outside2



Metric:

1

[1 - 254]

Tunneled: (Used only for default Route)

Route Tracking:

sla-outside2



Cancel

OK

Ajouter un deuxième FAI de routage statique

Cliquez sur Save and Deploy the configuration.

Vérifier

Connectez-vous à l'interface de ligne de commande du FTD, exécutez la commande `show zone` pour vérifier les informations sur les zones de trafic ECMP, y compris les interfaces qui font partie de chaque zone.

```
<#root>
```

```
> show zone  
Zone: Outside ecmp  
Security-level: 0
```

```
Zone member(s): 2
```

```
Outside2 GigabitEthernet0/1
```

```
Outside1 GigabitEthernet0/0
```

Exécutez la commande `show running-config route` pour vérifier la configuration en cours de la configuration de routage. Dans ce cas, il existe deux routes statiques avec des routes.

```
<#root>
```

```
> show running-config route
```

```
route Outside1 0.0.0.0 0.0.0.0 10.1.1.2 1 track 1
```

```
route Outside2 0.0.0.0 0.0.0.0 10.1.2.2 1 track 2
```

Exécutez la commande show route pour vérifier la table de routage, dans ce cas, il y a deux routes par défaut sont via l'interface outside1 et outside2 à coût égal, le trafic peut être distribué entre deux circuits ISP.

```
<#root>
```

```
> 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 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2
```

```
[1/0] via 10.1.1.2, Outside1
```

```
C 10.1.1.0 255.255.255.0 is directly connected, Outside1  
L 10.1.1.1 255.255.255.255 is directly connected, Outside1  
C 10.1.2.0 255.255.255.0 is directly connected, Outside2  
L 10.1.2.1 255.255.255.255 is directly connected, Outside2  
C 10.1.3.0 255.255.255.0 is directly connected, Inside  
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

Exécutez la commande **show sla monitor configuration** pour vérifier la configuration du moniteur SLA.

<#root>

```
> show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 1
Owner:
Tag:
```

Type of operation to perform: echo

Target address: 10.1.1.2

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:
```

Entry number: 2

Owner:
Tag:

Type of operation to perform: echo

Target address: 10.1.2.2

Interface: Outside2

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:

Exécutez la commande `show sla monitor operational-state` pour confirmer l'état du SLA Monitor. Dans ce cas, vous pouvez trouver «**Timeout
were: FALSE**» dans le résultat de la commande, il indique que l'écho ICMP à la passerelle répond, de sorte que la route par défaut via l'interface cible est active et installée dans la table de routage.

<#root>

> show sla monitor operational-state

Entry number: 1
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 2
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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

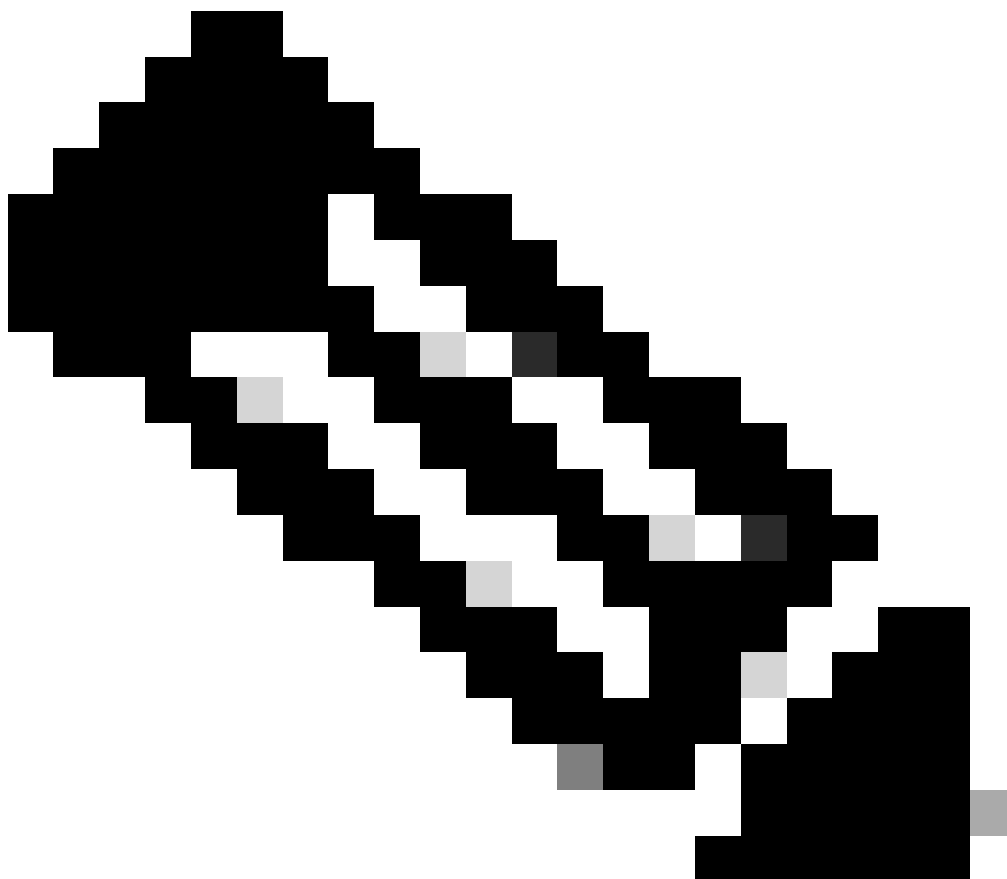
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Équilibrage de charge

Trafic initial via FTD pour vérifier si la charge ECMP équilibre le trafic entre les passerelles de la zone ECMP. Dans ce cas, lancez la connexion telnet depuis Inside-Host1 (10.1.3.2) et Inside-Host2 (10.1.3.4) vers Internet-Host (10.1.5.2), exécutez la commande **show conn** pour confirmer que la charge du trafic est équilibrée entre deux liaisons ISP, Inside-Host1 (10.1.3.2) passe par l'interface outside1, Inside-Host2 (10.1.3.4) passe par l'interface outside2.

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:24, bytes 1329, flags UIO N1
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:04, bytes 1329, flags UIO N1
```



Remarque : la charge du trafic est répartie entre les passerelles spécifiées en fonction d'un algorithme qui hache les adresses IP

source et de destination, l'interface entrante, le protocole, la source et les ports de destination. Lorsque vous exécutez le test, le trafic que vous simulez peut être routé vers la même passerelle en raison de l'algorithme de hachage, ce qui est attendu, changez n'importe quelle valeur parmi les 6 tuples (IP source, IP de destination, interface entrante, protocole, port source, port de destination) pour apporter des modifications au résultat du hachage.

Route perdue

Si la liaison vers la première passerelle ISP est désactivée, dans ce cas, arrêtez le premier routeur de passerelle pour simuler. Si le FTD ne reçoit pas de réponse d'écho de la première passerelle du FAI dans le délai spécifié dans l'objet SLA Monitor, l'hôte est considéré comme inaccessible et marqué comme inactif. La route suivie vers la première passerelle est également supprimée de la table de routage.

Exécutez la commande `show sla monitor operational-state` pour confirmer l'état actuel du SLA Monitor. Dans ce cas, vous pouvez trouver « Timeout were: True » dans le résultat de la commande, il indique que l'écho ICMP à la première passerelle ISP ne répond pas.

<#root>

```
> show sla monitor operational-state
Entry number: 1
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
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: TRUE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0
```

```
Entry number: 2
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
```

Number of operations attempted: 104
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: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Exécutez la commande **show route** pour vérifier la table de routage actuelle, la route vers la première passerelle ISP via l'interface outside1 est supprimée, il n'y a qu'une seule route active par défaut vers la deuxième passerelle ISP via l'interface outside2.

<#root>

> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2

C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1

```
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

Exécutez la commande `show conn`, vous pouvez constater que les deux connexions sont toujours actives. Les sessions telnet sont également actives sur Inside-Host1 (10.1.3.2) et Inside-Host2 (10.1.3.4) sans interruption.

```
<#root>
```

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect
```

```
TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:22, bytes 1329, flags UIO N1
```

```
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:02, bytes 1329, flags UIO N1
```



Remarque : vous pouvez remarquer dans le résultat de `show conn` , que la session telnet de l'hôte interne 1 (10.1.3.2) passe toujours par l'interface `outside1`, bien que la route par défaut via l'interface `outside1` ait été supprimée de la table de routage. ceci est normal et, par conception, le trafic réel passe par l'interface `outside2`. Si vous initiez une nouvelle connexion de l'hôte interne 1 (10.1.3.2) à l'hôte Internet (10.1.5.2), vous pouvez constater que tout le trafic passe par l'interface `outside2`.

Dépannage

Afin de valider la modification de la table de routage, exécutez la commande `debug ip routing`.

Dans cet exemple, lorsque la liaison vers la première passerelle ISP est désactivée, la route passant par l'interface outside1 est supprimée de la table de routage.

```
<#root>
```

```
> debug ip routing  
IP routing debugging is on
```

```
RT: ip_route_delete 0.0.0.0 0.0.0.0 via 10.1.1.2, Outside1
```

```
ha_cluster_synced 0 routetype 0
```

```
RT: del 0.0.0.0 via 10.1.1.2, static metric [1/0]NP-route: Delete-Output 0.0.0.0/0 hop_count:1 , via 0.0.0.0
```

```
RT(mgmt-only): NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, Outside2
```

```
NP-route: Update-Input 0.0.0.0/0 hop_count:1 Distance:1 Flags:0X0 , via 10.1.2.2, Outside2
```

Exécutez la commande show route pour confirmer la table de routage actuelle.

```
<#root>
```



```
> 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 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2
```

```
C 10.1.1.0 255.255.255.0 is directly connected, Outside1  
L 10.1.1.1 255.255.255.255 is directly connected, Outside1  
C 10.1.2.0 255.255.255.0 is directly connected, Outside2  
L 10.1.2.1 255.255.255.255 is directly connected, Outside2  
C 10.1.3.0 255.255.255.0 is directly connected, Inside  
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

Lorsque la liaison vers la première passerelle ISP est à nouveau active, la route passant par l'interface outside1 est ajoutée à la table de routage.

```
<#root>
```

```
> debug ip routing  
IP routing debugging is on
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, Outside2
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.1.2, Outside2
```

```
NP-route: Update-Input 0.0.0.0/0 hop_count:2 Distance:1 Flags:0X0 , via 10.1.2.2, Outside2
```

```
via 10.1.1.2, Outside1
```

Exécutez la commande show route pour confirmer la table de routage actuelle.

```
<#root>
```

```
> 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 10.1.2.2 to network 0.0.0.0
```

```
s* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2
```

```
[1/0] via 10.1.1.2, Outside1
```

C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside

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.