

# Configurar o ECMP com SLA IP no FTD gerenciado pelo FMC

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Etapa 0. Pré-configurar interfaces/objetos de rede](#)

[Etapa 1. Configurar região ECMP](#)

[Etapa 2. Configurar objetos IP SLA](#)

[Etapa 3. Configurar rotas estáticas com o Route Track](#)

[Verificar](#)

[Balanceamento de carga](#)

[Rota Perdida](#)

[Troubleshooting](#)

---

## Introdução

Este documento descreve como configurar o ECMP junto com o IP SLA em um FTD gerenciado pelo FMC.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do ECMP no Cisco Secure Firewall Threat Defense (FTD)
- Configuração IP SLA no Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)

### Componentes Utilizados

As informações neste documento são baseadas nesta versão de software e hardware:

- Cisco FTD versão 7.4.1

- Cisco FMC versão 7.4.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Este documento descreve como configurar o Equal-Cost Multi-Path (ECMP) junto com o Internet Protocol Service Level Agreement (IP SLA) em um FTD da Cisco que é gerenciado pelo FMC da Cisco. O ECMP permite que você agrupe interfaces em FTD e faça o balanceamento de carga do tráfego em várias interfaces. O IP SLA é um mecanismo que monitora a conectividade de ponta a ponta através da troca de pacotes regulares. Junto com o ECMP, o SLA IP pode ser implementado para garantir a disponibilidade do próximo salto. Neste exemplo, o ECMP é utilizado para distribuir pacotes igualmente em dois circuitos do Provedor de serviços de Internet (ISP). Ao mesmo tempo, um SLA IP rastreia a conectividade, garantindo uma transição transparente para todos os circuitos disponíveis no caso de uma falha.

Os requisitos específicos deste documento incluem:

- Acesso aos dispositivos com uma conta de usuário com privilégios de administrador
- Cisco Secure Firewall Threat Defense versão 7.1 ou posterior
- Cisco Secure Firewall Management Center versão 7.1 ou posterior

## Configurar

### Diagrama de Rede

Neste exemplo, o Cisco FTD tem duas interfaces externas: outside1 e outside2 . Cada um se conecta a um gateway ISP, outside1 e outside2 pertencem à mesma zona ECMP denominada outside.

O tráfego da rede interna é roteado através do FTD e tem a carga balanceada para a Internet através dos dois ISP.

Ao mesmo tempo, o FTD usa SLAs IP para monitorar a conectividade com cada gateway do ISP. Em caso de falha em qualquer circuito do ISP, os failovers de FTD para o outro gateway do ISP para manter a continuidade dos negócios.

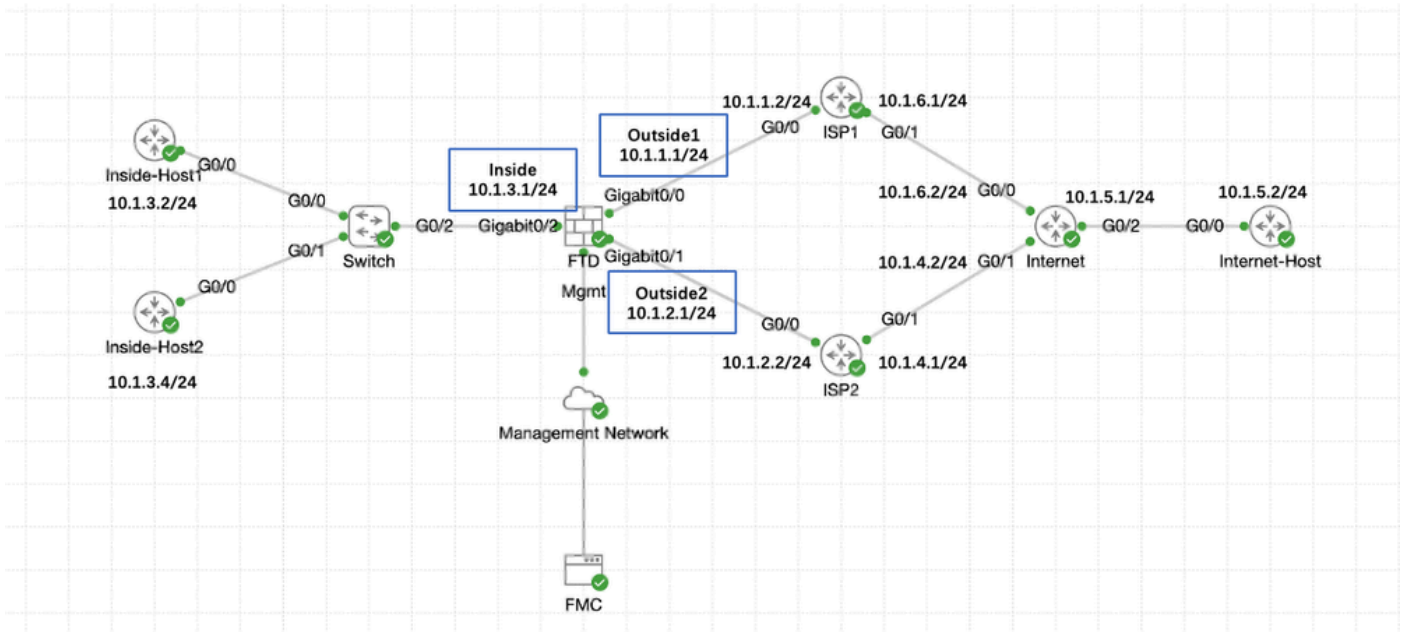


Diagrama de Rede

## Configurações

### Etapa 0. Pré-configurar interfaces/objetos de rede

Faça login na GUI da Web do FMC, selecione Devices>Device Management e clique no botão Edit para seu dispositivo de defesa contra ameaças. A página Interfaces é selecionada por padrão. Clique no botão Edit da interface que você deseja editar, neste exemplo GigabitEthernet0/0.

Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration

10.106.32.250  
Cisco Firepower Threat Defense for KVM

Device Routing Interfaces Inline Sets DHCP VTEP

All Interfaces Virtual Tunnels

Search by name Sync Device Add Interfaces

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		✎

Displaying 1-9 of 9 interfaces | Page 1 of 1

Editar Interface Gi0/0

Na janela Edit Physical Interface, na guia General:

1. Defina o Nome, nesse caso Fora1.
2. Ative a interface marcando a caixa de seleção Enabled.
3. Na lista suspensa Zona de segurança, selecione uma Zona de segurança existente ou crie uma nova, neste exemplo 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 Geral

Na guia IPv4:

1. Escolha uma das opções na lista suspensa IP Type, neste exemplo Use Static IP.
2. Defina o endereço IP, neste exemplo 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

Repita a etapa semelhante para configurar a interface GigabitEthernet0/1, Na janela Editar interface física, na guia Geral:

1. Defina o Nome, nesse caso Fora2.
2. Ative a interface marcando a caixa de seleção Enabled.
3. Na lista suspensa Zona de segurança, selecione uma Zona de segurança existente ou crie uma nova, neste exemplo 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 Geral

### Na guia IPv4:

1. Escolha uma das opções na lista suspensa IP Type, neste exemplo Use Static IP.
2. Defina o endereço IP, neste exemplo 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 or 192.0.2.1/24

Cancel OK

Interface Gi0/1 IPv4

Repita a etapa semelhante para configurar a interface GigabitEthernet0/2, Na janela Editar interface física, na guia Geral:

1. Defina Name, neste caso Inside.
2. Ative a interface marcando a caixa de seleção Enabled.
3. Na lista suspensa Zona de segurança, selecione uma Zona de segurança existente ou crie uma nova, neste exemplo 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 Geral

### Na guia IPv4:

1. Escolha uma das opções na lista suspensa IP Type, neste exemplo Use Static IP.
2. Defina o endereço IP, neste exemplo 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

Clique em Salvar e Implantar a configuração.

Navegue até Objetos > Gerenciamento de objetos, Escolha Rede na lista de tipos de objetos, Escolha Adicionar objeto no menu suspenso Adicionar rede para criar um objeto para o primeiro gateway do ISP.

Firewall Management Center  
Objects / Object Management

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:0.0.0/96	Network	
IPv6-Link-Local	fe80::/10	Network	
IPv6-Private-Unique-Local-Addresses	fc00::/7	Network	
IPv6-to-IPv4-Relay-Anycast	192.88.99.0/24	Network	

Displaying 1 - 14 of 14 rows << Page 1 of 1 >>

Objeto de rede

Na janela New Network Object:

1. Defina o Nome, neste exemplo gw-outside1.
2. No campo Network, selecione a opção necessária e insira um valor apropriado, neste exemplo Host e 10.1.1.2.

3. Click Save.

**New Network Object**

Name  
gw-outside1

Description

Network  
 Host  Range  Network  FQDN  
10.1.1.2

Allow Overrides

Cancel Save

Objeto Gw-outside1

Repita etapas semelhantes para criar outro objeto para o segundo gateway do ISP. Na janela New Network Object:

1. Defina o Nome, neste exemplo gw-outside2.
2. No campo Network, selecione a opção necessária e insira um valor apropriado, neste exemplo Host e 10.1.2.2.
3. Click Save.

## New Network Object



Name

gw-outside2

Description

Network



Host



Range



Network



FQDN

10.1.2.2



Allow Overrides

Cancel

Save

Objeto Gw-outside2

### Etapa 1. Configurar região ECMP

Navegue até Devices > Device Management e edite o dispositivo de defesa contra ameaças, clique em Routing. No menu suspenso virtual router, selecione o roteador virtual no qual deseja criar a zona ECMP. Você pode criar regiões ECMP no roteador virtual global e nos roteadores virtuais definidos pelo usuário. Neste exemplo, escolha Global.

Clique em ECMP e em Adicionar.

Firewall Management Center  
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

10.106.32.250

Cisco Firepower Threat Defense for KVM

Device **Routing** Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Equal-Cost Multipath Routing (ECMP)

There are no ECMP zone records [Add](#)

Save Cancel

Configurar região ECMP

Na janela Adicionar ECMP:

1. Defina Name para a região ECMP, neste exemplo Outside.
2. Para associar interfaces, selecione a interface na caixa Interfaces disponíveis e clique em Adicionar. Neste exemplo, Outside1 e Outside2.
3. Click OK.

## Add ECMP



Name  
Outside

Available Interfaces  
Inside

Selected Interfaces  
Outside1  
Outside2

Add

Cancel OK

Configurar região ECMP externa

Clique em Salvar e Implantar a configuração.

### Etapa 2. Configurar objetos IP SLA

Navegue até Objetos > Gerenciamento de objetos, escolha Monitor de SLA na lista de tipos de objetos, clique em Adicionar monitor de SLA para adicionar um novo monitor de SLA para o primeiro gateway do 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

Criar monitor de SLA

Na janela Novo objeto de monitoramento de SLA:

1. Defina o Nome do objeto de monitor de SLA, nesse caso sla-outside1.
2. Insira o número de ID da operação do SLA no campo ID do monitor do SLA. Os valores variam de 1 a 2147483647. Você pode criar no máximo 2000 operações SLA em um dispositivo. Cada número de ID deve ser exclusivo à política e à configuração do dispositivo. Neste exemplo, 1.
3. Insira o endereço IP que está sendo monitorado quanto à disponibilidade pela operação do SLA, no campo Endereço monitorado. Neste exemplo, 10.1.1.2.
4. A lista Zonas/interfaces disponíveis exibe as zonas e os grupos de interface. Na lista Zonas/Interfaces, adicione as zonas ou grupos de interface que contêm as interfaces através das quais o dispositivo se comunica com a estação de gerenciamento. Para especificar uma única interface, você precisa criar uma região ou os grupos de interface para a interface. Neste exemplo, Outside1\_Zone.
5. Click Save.

## New SLA Monitor Object



Name:

sla-outside1

Description:

Frequency (seconds):

60

{1-604800}

SLA Monitor ID\*:

1

Threshold (milliseconds):

{0-60000}

Timeout (milliseconds):

5000

{0-604800000}

Data Size (bytes):

28

{0-16384}

ToS:

Number of Packets:

1

Monitor Address\*:

10.1.1.2

Available Zones/interfaces



Q Search

Inside\_Zone

Outside1\_Zone

Outside2\_Zone

Add

Selected Zones/interfaces

Outside1\_Zone



Cancel

Save

Sla-outside1 do objeto de SLA

Repita etapas semelhantes para criar outro monitor de SLA para o segundo gateway do ISP.

Na janela Novo objeto de monitoramento de SLA:

1. Defina o Nome do objeto de monitor de SLA, nesse caso sla-outside2.
2. Insira o número de ID da operação do SLA no campo ID do monitor do SLA. Os valores variam de 1 a 2147483647. Você pode criar no máximo 2000 operações SLA em um dispositivo. Cada número de ID deve ser exclusivo à política e à configuração do dispositivo. Neste exemplo, 2.
3. Insira o endereço IP que está sendo monitorado quanto à disponibilidade pela operação do SLA, no campo Endereço monitorado. Neste exemplo, 10.1.2.2.
4. A lista Zonas/Interfaces disponíveis exibe as zonas e os grupos de interface. Na lista Zonas/Interfaces, adicione as zonas ou grupos de interface que contêm as interfaces através das quais o dispositivo se comunica com a estação de gerenciamento. Para especificar uma única interface, você precisa criar uma região ou os grupos de interface para a interface. Neste exemplo, Outside2\_Zone.
5. Click 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

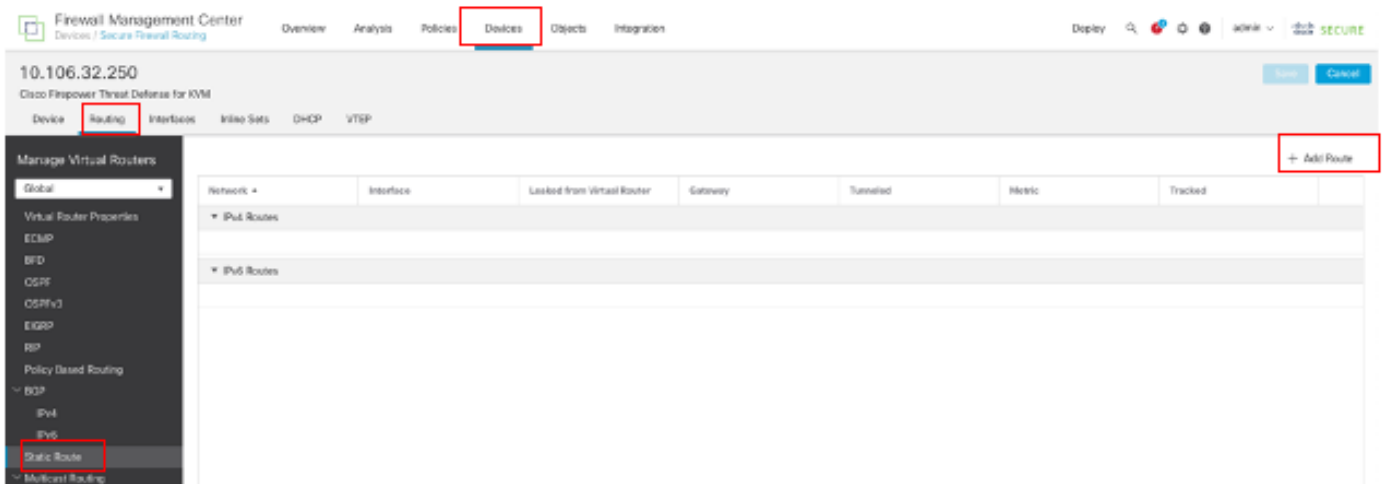
Cancel

Save

### Etapa 3. Configurar rotas estáticas com o Route Track

Navegue até Devices > Device Management e edite o dispositivo de defesa contra ameaças, clique em Routing, Na lista suspensa virtual routers, selecione o roteador virtual para o qual você está configurando uma rota estática. Neste exemplo, Global.

Selecione Static Route, clique em Add Route para adicionar a rota padrão ao primeiro gateway do ISP.



Configurar a rota estática


Na janela Add Static Route Configuration:


1. Clique em IPv4 ou IPv6 dependendo do tipo de rota estática que você está adicionando. Neste exemplo, IPv4.
2. Escolha a Interface à qual esta rota estática se aplica. Neste exemplo, Outside1.
3. Na lista Available Network, escolha a rede de destino. Neste exemplo any-ipv4.
4. No campo Gateway ou IPv6 Gateway, insira ou escolha o roteador do gateway que é o próximo salto para essa rota. Você pode fornecer um endereço IP ou um objeto Redes/Hosts. Neste exemplo, gw-outside1.
5. No campo Metric, insira o número de saltos para a rede destino. Os valores válidos variam de 1 a 255; o valor padrão é 1. Neste exemplo, 1.
6. Para monitorar a disponibilidade da rota, insira ou escolha o nome de um objeto Monitor de SLA que define a política de monitoramento, no campo Rastreamento de rota. Neste exemplo, 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

Adicionar rota estática primeiro ISP

Repita etapas semelhantes para adicionar a rota padrão ao segundo gateway do ISP. Na janela Add Static Route Configuration:

1. Clique em IPv4 ou IPv6 dependendo do tipo de rota estática que você está adicionando. Neste exemplo, IPv4.
2. Escolha a Interface à qual esta rota estática se aplica. Neste exemplo, Outside2.

3. Na lista Available Network, escolha a rede de destino. Neste exemplo any-ipv4.
4. No campo Gateway ou IPv6 Gateway, insira ou escolha o roteador do gateway que é o próximo salto para essa rota. Você pode fornecer um endereço IP ou um objeto Redes/Hosts. Neste exemplo gw-outside2.
5. No campo Metric, insira o número de saltos para a rede destino. Os valores válidos variam de 1 a 255; o valor padrão é 1. Certifique-se de especificar a mesma métrica da primeira rota, neste exemplo 1.
6. Para monitorar a disponibilidade da rota, insira ou escolha o nome de um objeto Monitor de SLA que define a política de monitoramento, no campo Rastreamento de rota. Neste exemplo, 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

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

Adicionar rota estática segundo ISP

Clique em Salvar e Implantar a configuração.

## Verificar

Efetue login no CLI do FTD e execute o comando `show zone` para verificar informações sobre zonas de tráfego ECMP, incluindo as interfaces que fazem parte de cada zona.

```
<#root>
```

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

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

```
Outside2 GigabitEthernet0/1
```

```
Outside1 GigabitEthernet0/0
```

Execute o comando `show running-config route` para verificar a configuração atual da configuração de roteamento; nesse caso, há duas rotas estáticas com rotas.

```
<#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
```

Execute o comando `show route` para verificar a tabela de roteamento; nesse caso, há duas rotas padrão através da interface `outside1` e `outside2` com custo igual; o tráfego pode ser distribuído entre dois circuitos 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
```

Execute o comando **show sla monitor configuration** para verificar a configuração do monitor de 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:

Execute o comandoshow sla monitor operational-state para confirmar o estado do Monitor do SLA. Nesse caso, você pode encontrar "**Timeout occurred: FALSE**" na saída do comando, ele indica que o eco ICMP para o gateway está respondendo, portanto, a rota padrão através da interface de destino está ativa e instalada na tabela de roteamento.

<#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**

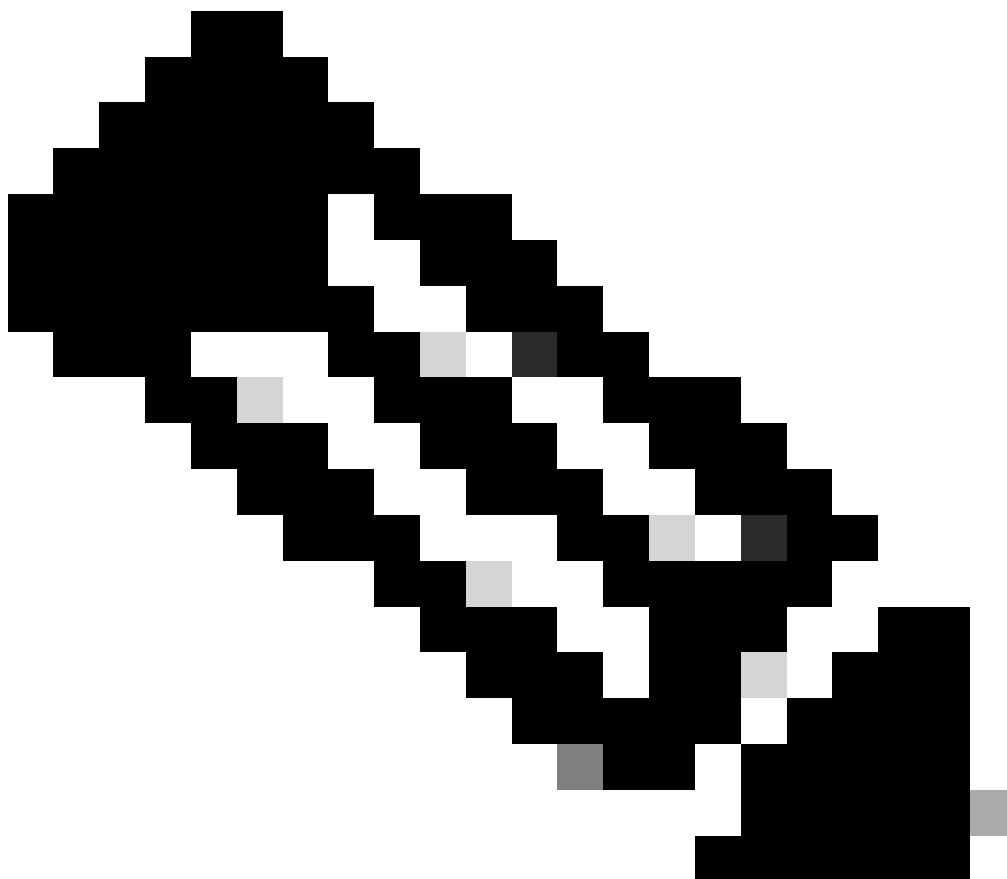
Over thresholds occurred: FALSE  
Latest RTT (milliseconds): 1  
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024  
Latest operation return code: OK  
RTT Values:  
RTTAvg: 1 RTTMin: 1 RTTMax: 1  
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

**Balanceamento de carga**

Tráfego inicial através do FTD para verificar se a carga do ECMP equilibra o tráfego entre os gateways na zona do ECMP. Nesse caso, inicie a conexão telnet de Inside-Host1 (10.1.3.2) e Inside-Host2 (10.1.3.4) em direção a Internet-Host (10.1.5.2), execute o comando **show conn** para confirmar se o tráfego tem a carga balanceada entre dois links de ISP, Inside-Host1 (10.1.3.2) passa pela interface outside1, Inside-Host2 (10.1.3.4) passa pela 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
```



**Observação:** o tráfego tem balanceamento de carga entre os gateways especificados com base em um algoritmo que mistura os

---

---

endereços IP origem e destino, a interface de entrada, o protocolo, as portas origem e destino. quando você executa o teste, o tráfego simulado pode ser roteado para o mesmo gateway devido ao algoritmo de hash, isso é esperado, altere qualquer valor entre as 6 tuplas (IP origem, IP destino, interface de entrada, protocolo, porta origem, porta destino) para fazer alterações no resultado de hash.

---

## Rota Perdida

Se o link para o primeiro Gateway do ISP estiver inoperante, nesse caso, desligue o primeiro roteador de gateway para simular. Se o FTD não receber uma resposta de eco do primeiro gateway do ISP dentro do temporizador de limite especificado no objeto Monitor do SLA, o host será considerado inalcançável e marcado como inativo. A rota rastreada para o primeiro gateway também é removida da tabela de roteamento.

Execute o comando `show sla monitor operational-state` para confirmar o estado atual do Monitor do SLA. Nesse caso, você pode encontrar "Timeout occurred: True" na saída do comando, que indica que o eco ICMP para o primeiro gateway do ISP não está respondendo.

<#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

Execute o comando **show route** para verificar a tabela de roteamento atual, a rota para o primeiro gateway do ISP através da interface outside1 é removida e há apenas uma rota padrão ativa para o segundo gateway do ISP através da 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
```

Execute o comando `show conn`, você poderá descobrir que as duas conexões ainda estão ativas. As sessões telnet também estão ativas no Host Interno 1 (10.1.3.2) e no Host Interno 2 (10.1.3.4) sem nenhuma interrupção.

<#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
```

---

---



**Observação:** você pode observar na saída de `show conn`, a sessão telnet de Inside-Host1 (10.1.3.2) ainda está através da interface `outside1`, embora a rota padrão através da interface `outside1` tenha sido removida da tabela de roteamento. isso é esperado e, por design, o tráfego real flui através da interface `outside2`. Se você iniciar uma nova conexão de Inside-Host1 (10.1.3.2) para Internet-Host (10.1.5.2), poderá descobrir que todo o tráfego passa pela interface `outside2`.

---

## Troubleshooting

Para validar a alteração na tabela de roteamento, execute o comando `debug ip routing`.

Neste exemplo, quando o link para o primeiro gateway do ISP está inoperante, a rota através da interface outside1 é removida da tabela de roteamento.

```
<#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
```

Execute o comando `show route` para confirmar a tabela de roteamento atual.

```
<#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
```

Quando o link para o primeiro gateway do ISP estiver ativo novamente, a rota através da interface outside1 será adicionada de volta à tabela de roteamento.

```
<#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
```

Execute o comando `show route` para confirmar a tabela de roteamento atual.

```
<#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

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.