

# Configurar ECMP com SLA IP no FTD Gerenciado pelo FDM

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

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

[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](#)

[Informações Relacionadas](#)

---

## Introdução

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

## 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)
- Gerenciador de dispositivos do Cisco Secure Firewall (FDM)

### Componentes Utilizados

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

- Cisco FTD versão 7.4.1 (Build 172)

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 Cisco FTD que é gerenciado pelo Cisco FDM. 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

## 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.

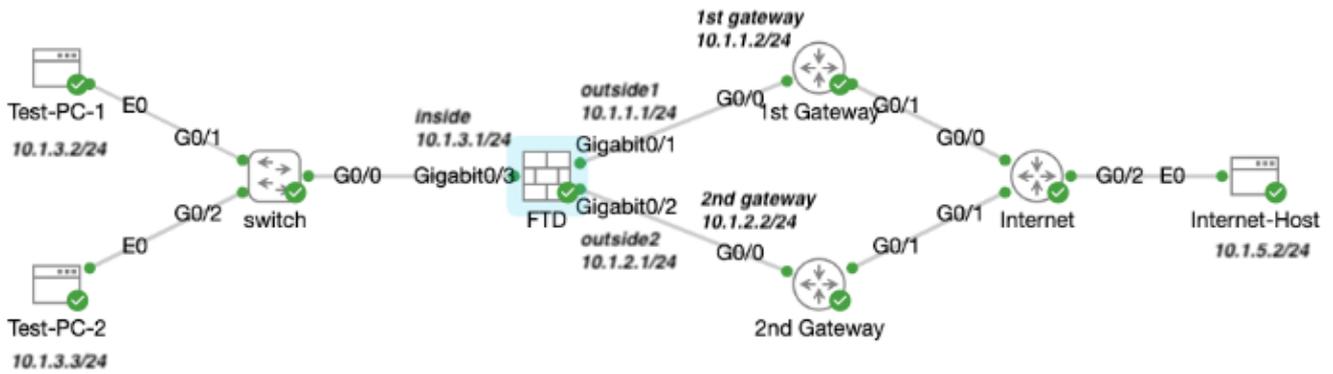
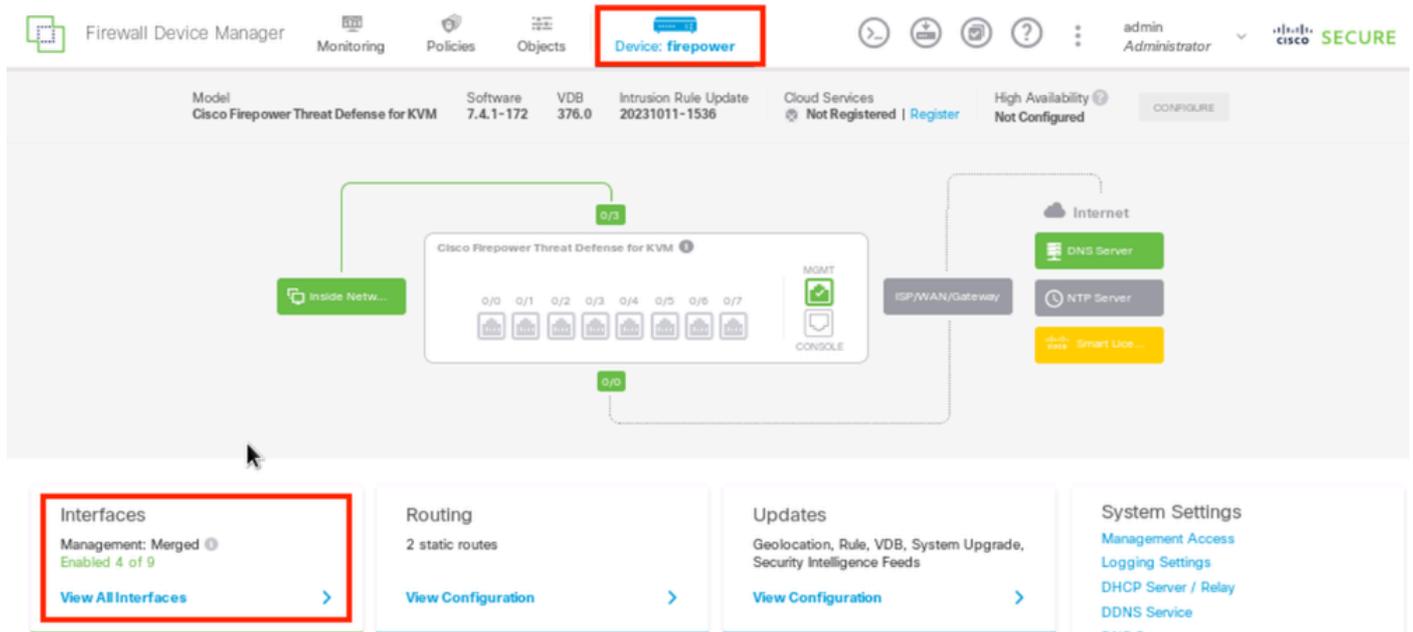


Diagrama de Rede

## Configurações

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

Efetue login na GUI da Web do FDM, clique em Dispositivo e, em seguida, clique no link no resumo de Interfaces . A lista Interfaces mostra as interfaces disponíveis, seus nomes, endereços e estados.



Interface de Dispositivo do FDM

Clique no ícone de edição (



) da interface física que deseja editar. Neste exemplo, GigabitEthernet0/1.

Device Summary  
Interfaces

Cisco Firepower Threat Defense for KVM

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7

MGMT  
CONSOLE

Interfaces Virtual Tunnel Interfaces

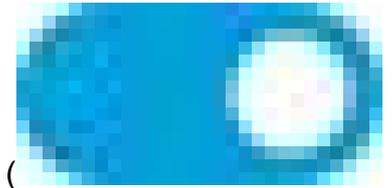
9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STAND BY ADDRESS	MONITOR FOR HA	ACTIONS
> GigabitEthernet0/0	outside	<input type="checkbox"/>	Routed			Enabled	
> GigabitEthernet0/1	outside 1	<input checked="" type="checkbox"/>	Routed	10.1.1.1		Enabled	

Etapa 0 Interface Gi0/1

Na janela Edit Physical Interface:

1. Defina o nome da interface , nesse caso, outside1 .



2. Defina o controle deslizante Status para a configuração habilitada ( ).

3. Clique na guia Endereço IPv4 e configure o endereço IPv4, nesse caso 10.1.1.1/24.

4. Click OK.

# GigabitEthernet0/1

## Edit Physical Interface



Interface Name

outside1

Mode

Routed

Status



*Most features work with named interfaces only, although some require unnamed interfaces.*

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

10.1.1.1

/

255.255.255.0

*e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0*

Standby IP Address and Subnet Mask

/

*e.g. 192.168.5.16*

CANCEL

OK



Observação: somente interfaces roteadas podem ser associadas a uma região ECMP.

---

Repita as etapas semelhantes para configurar a interface para a conexão ISP secundária, neste exemplo, a interface física é GigabitEthernet0/2 . Na janela Edit Physical Interface:

1. Defina o nome da interface , nesse caso, outside2.



2. Defina o controle deslizante Status para a configuração habilitada ( ).

3. Clique na guia IPv4 Address e configure o endereço IPv4, nesse caso 10.1.2.1/24.

4. Click OK.

## GigabitEthernet0/2 Edit Physical Interface

Interface Name  
outside2

Mode  
Routed

Status

Most features work with named interfaces only, although some require unnamed interfaces.

Description  
|

IPv4 Address   IPv6 Address   Advanced

Type  
Static

IP Address and Subnet Mask  
10.1.2.1 / 24  
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

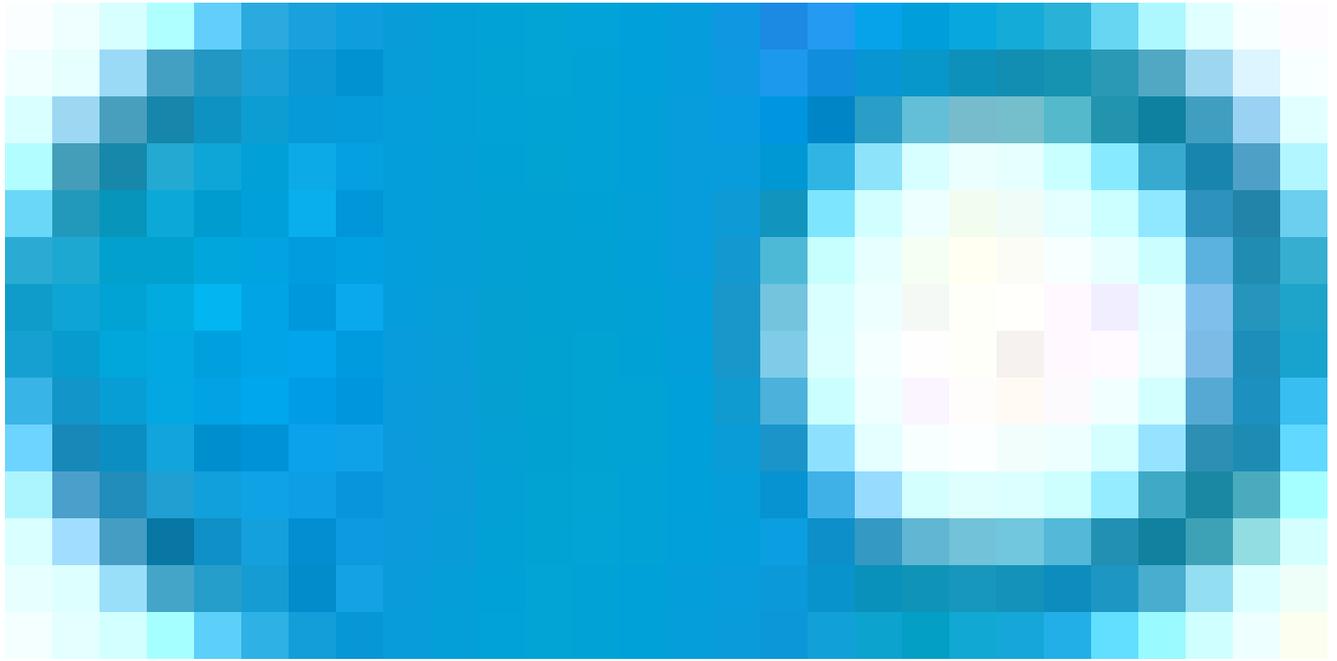
Standby IP Address and Subnet Mask  
  
e.g. 192.168.5.16

CANCEL   OK

Etapa 0 Editar A Interface Gi0/2

Repita as etapas semelhantes para configurar a interface para a conexão interna, neste exemplo, a interface física é GigabitEthernet0/3. Na janela Edit Physical Interface:

1. Defina o nome da interface , nesse caso, dentro .
2. Defina o controle deslizante Status para a configuração habilitada (



).

3. Clique na guia Endereço IPv4 e configure o endereço IPv4, nesse caso 10.1.3.1/24.
4. Click OK.

## GigabitEthernet0/3 Edit Physical Interface

Interface Name:

Mode: Routed

Status:

Description:

IPv4 Address | IPv6 Address | Advanced

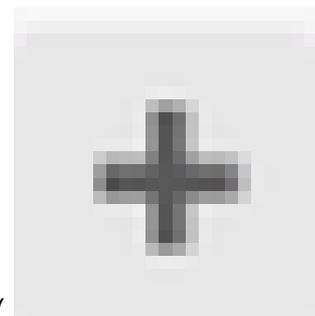
Type: Static

IP Address and Subnet Mask:  /

Standby IP Address and Subnet Mask:  /

CANCEL OK

Etapa 0 Editar A Interface Gi0/3



Navegue até Objetos > Tipos de objeto > Redes , clique no ícone adicionar ( ) para adicionar um novo objeto.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | CISCO SECURE

Object Types

- Networks**
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies

### Network Objects and Groups

8 objects

Filter +

Preset filters: *Default, Applied, User, Applied*

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16	
2	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	
3	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12	
4	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16	
5	any-ipv4	NETWORK	0.0.0.0/0	
6	any-ipv6	NETWORK	::/0	

Etapa 0 Objeto1

Na janela Add Network Object, configure o primeiro gateway do ISP:

1. Defina o Nome do objeto, neste caso gw-outside1.
2. Selecione o Tipo do objeto, neste caso Host.
3. Defina o endereço IP do Host , nesse caso 10.1.1.2.
4. Click OK.

## Add Network Object



Name

gw-outside1

Description

Type



Network



Host



FQDN



Range

Host

10.1.1.2

*e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A*

CANCEL

OK

Etapa 0 Objeto2

Repita as etapas semelhantes para configurar outro objeto de rede para o segundo gateway do ISP:

1. Defina o Nome do objeto, neste caso gw-outside2.
2. Selecione o Tipo do objeto, neste caso Host.
3. Defina o endereço IP do Host , nesse caso 10.1.2.2.
4. Click OK.

# Add Network Object



Name

gw-outside2

Description

A large, empty text area for entering a description, with a small diagonal icon in the bottom right corner.

Type



Network



Host



FQDN



Range

Host

10.1.2|2

*e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A*

CANCEL

OK

Etapa 0 Objeto3

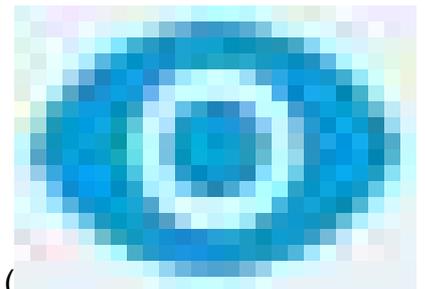


Observação: sua política de controle de acesso deve estar configurada no FTD para permitir o tráfego; essa parte não está incluída neste documento.

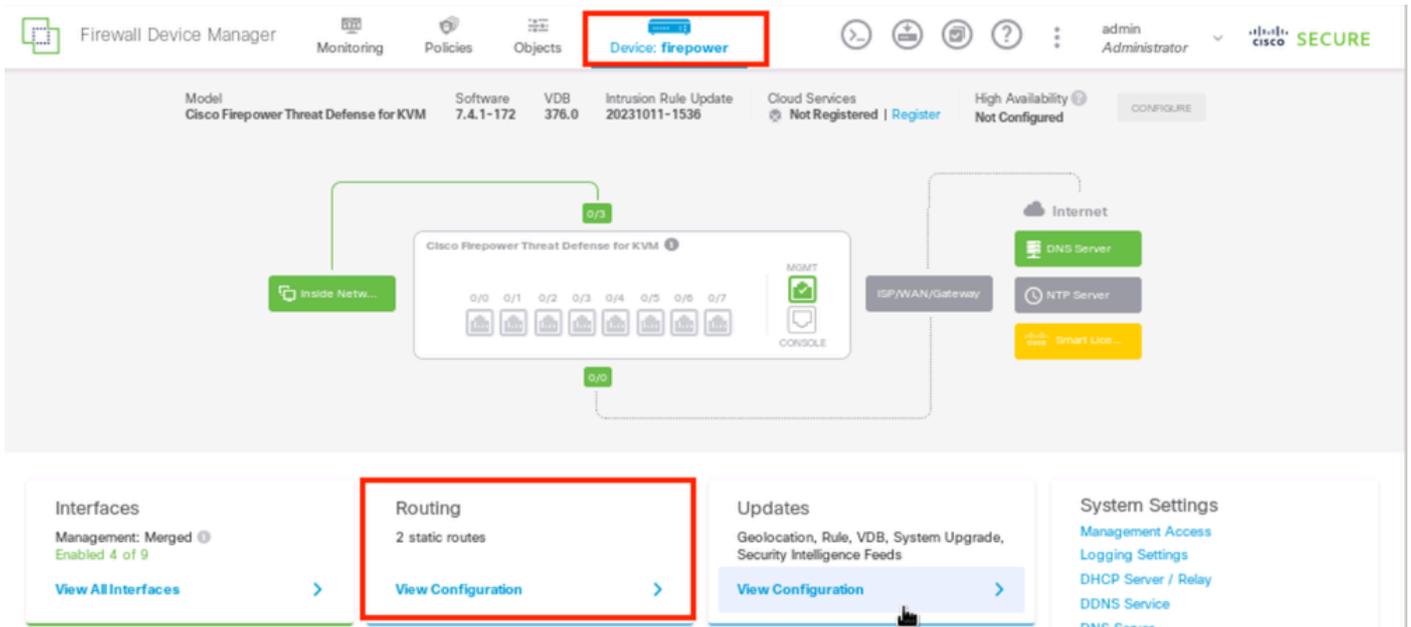
---

## Etapa 1. Configurar região ECMP

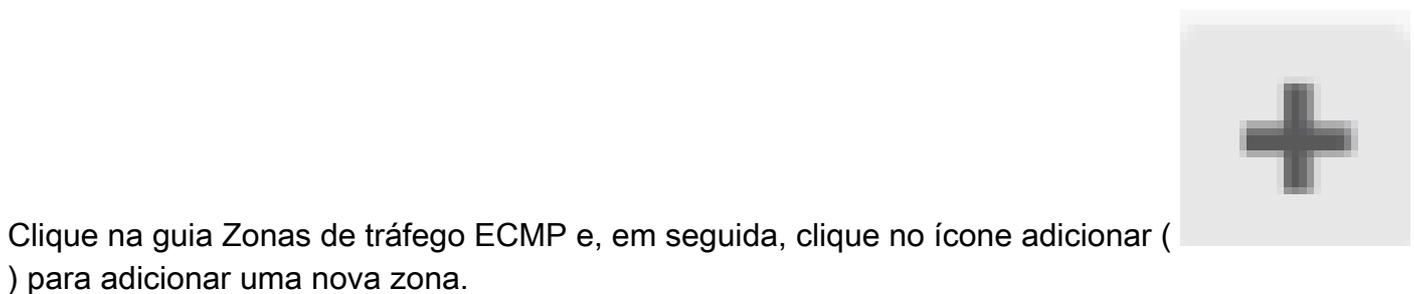
Navegue até Device e clique no link no resumo de roteamento.



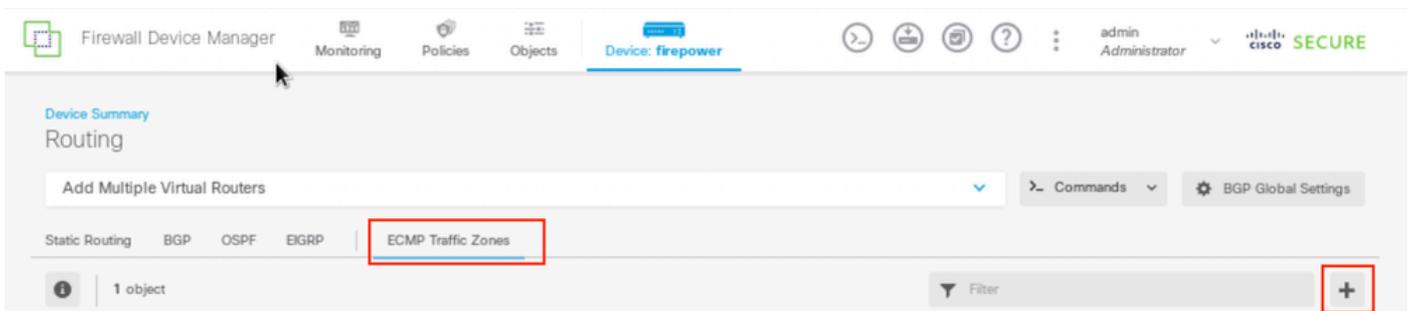
Se você habilitou roteadores virtuais, clique no ícone de visualização ( ) do roteador no qual você está configurando uma rota estática. Nesse caso, os roteadores virtuais não estão ativados.



Etapa 1 Zona ECMP1



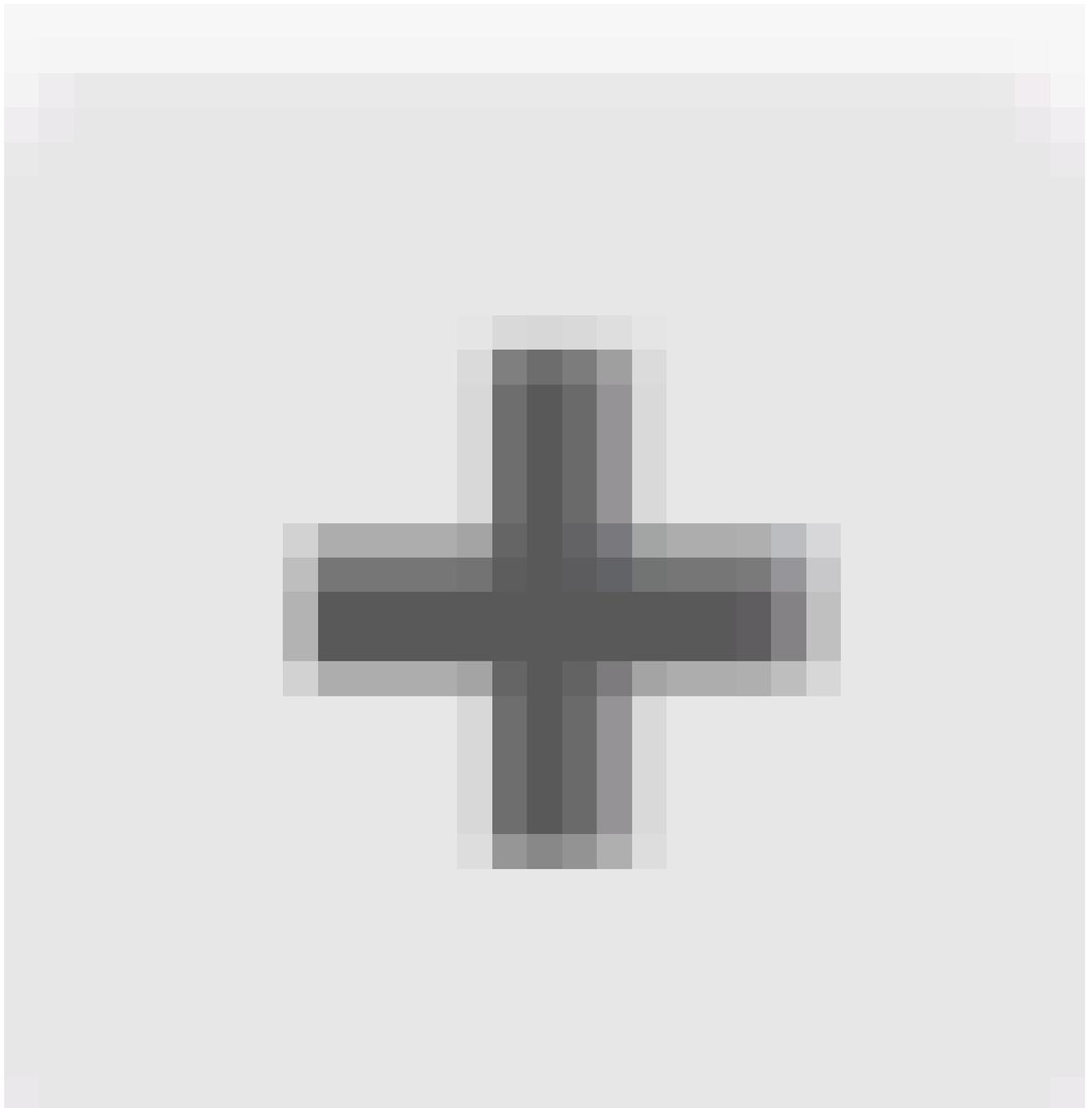
Clique na guia Zonas de tráfego ECMP e, em seguida, clique no ícone adicionar ( ) para adicionar uma nova zona.



Etapa 1 Zona ECMP2

Na janela Add ECMP Traffic Zone:

1. Defina o Nome para a região ECMP e, opcionalmente, uma descrição.
2. Clique no ícone adicionar (



) para seleccionar até 8 interfaces para incluir na zona. Neste exemplo, o nome ECMP é Outside , as interfaces outside1 e outside2 são adicionadas à região.

3. Click OK.

# Add ECMP Traffic Zone



**i** Keep the member interfaces of a ECMP traffic zone in the same security zone to prevent different access rules being applied to those interfaces.

Name

Outside

Description

Interfaces



- > inside (GigabitEthernet0/3)
- > management (Management0/0)
- > outside (GigabitEthernet0/0)
- > outside1 (GigabitEthernet0/1)
- > outside2 (GigabitEthernet0/2)

2 item(s) selected

Create new Subinterface

CANCEL

OK

CANCEL

OK

NETWORK

INSIDE HOST

ADD ECMP TRAFFIC ZONE

Etapa 1 Zona ECMP3

Ambas as interfaces outside1 e outside2 foram adicionadas à zona ECMP outside com êxito.

Device Summary  
Routing

Add Multiple Virtual Routers ▼ Commands BGP Global Settings

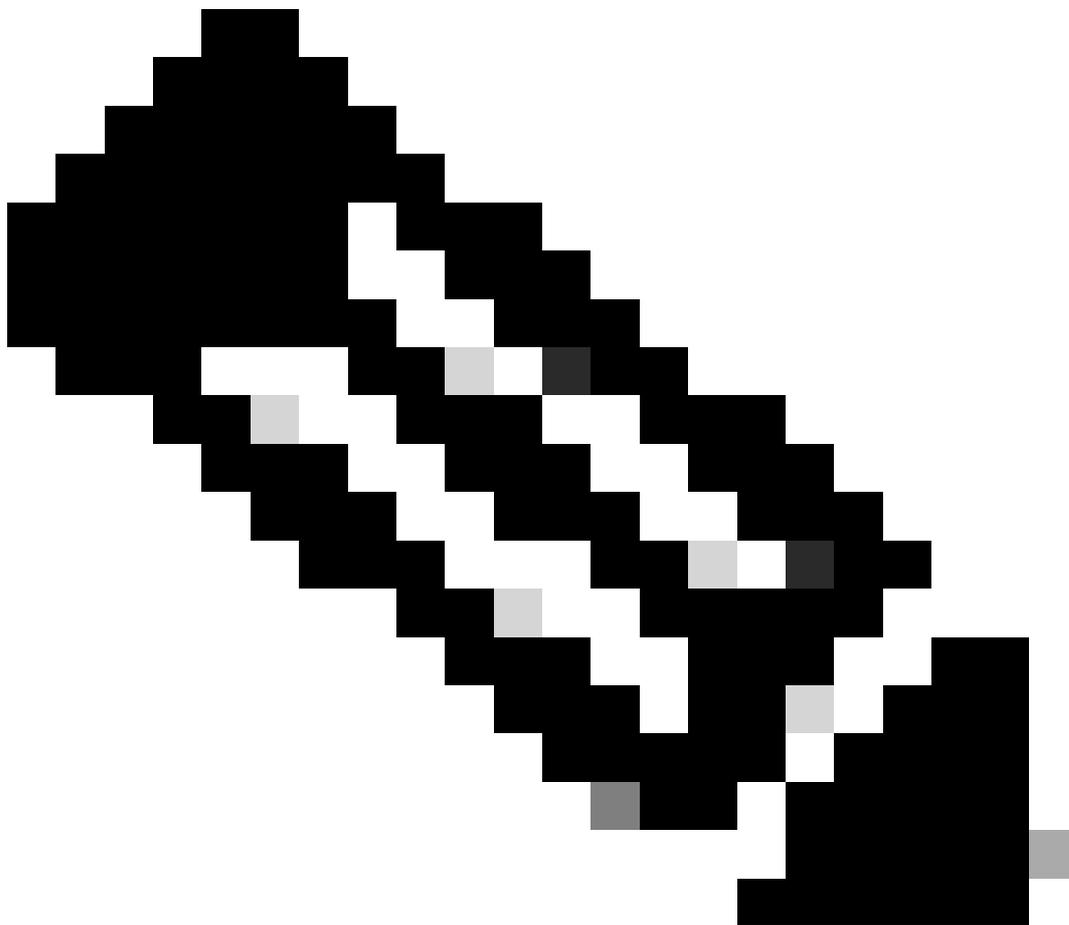
Static Routing | BGP | OSPF | EIGRP | **ECMP Traffic Zones**

1 object Filter +

#	NAME	INTERFACES	ACTIONS
1	Outside	outside1 (GigabitEthernet0/1) outside2 (GigabitEthernet0/2)	

Etapa 1 Zona ECMP4

---



Observação: uma zona de tráfego de roteamento ECMP não está relacionada a zonas de segurança. A criação de uma zona de segurança que contenha as interfaces externa1 e externa2 não implementa uma zona de tráfego para fins de roteamento ECMP.

---

Etapa 2. Configurar objetos IP SLA

Para definir os objetos de SLA usados para monitorar a conectividade com cada gateway,



navegue até Objetos > Tipos de objeto > Monitores de SLA, clique no ícone adicionar ( ) para adicionar um novo monitor de SLA para a primeira conexão do ISP.

Firewall Device Manager

Monitoring Policies **Objects** Device: firepower

admin Administrator

OBJECT TYPES

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors**

SLA Monitors

Filter +

#	NAME	MONITORED ADDRESS	TARGET INTERFACE	ACTIONS
There are no SLA Monitors yet. Start by creating the first SLA Monitor.				

CREATE SLA MONITOR

Etapa 2 IP SLA1

Na janela Adicionar objeto de monitoramento de SLA:

1. Defina o Nome para o objeto de monitor de SLA e, opcionalmente, uma descrição, nesse caso, sla-outside1.
2. Defina o endereço do monitor , nesse caso gw-outside1 (o primeiro gateway do ISP).
3. Defina a Interface de Destino através da qual o endereço do monitor é alcançável, neste caso, outside1 .
4. Além disso, também é possível ajustar o Timeout e o Threshold . Click OK.

# Add SLA Monitor Object



Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

## IP ICMP ECHO OPTIONS

**i** Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes

CANCEL

OK

Repita a etapa semelhante para configurar outro objeto de monitoramento do SLA para a segunda conexão do ISP, na janela Adicionar objeto de monitoramento do SLA:

1. Defina o Nome para o objeto de monitor de SLA e, opcionalmente, uma descrição, nesse caso, sla-outside2 .
2. Defina o endereço do monitor , nesse caso gw-outside2 (o segundo gateway do ISP).
3. Defina a Interface de Destino através da qual o endereço do monitor pode ser alcançado, nesse caso, outside2.
4. Além disso, também é possível ajustar o Timeout e o Limite. Click OK.

# Add SLA Monitor Object



Name

sla-outside2

Description

Monitor Address

gw-outside2

Target Interface

outside2 (GigabitEthernet0/2)

## IP ICMP ECHO OPTIONS



Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes

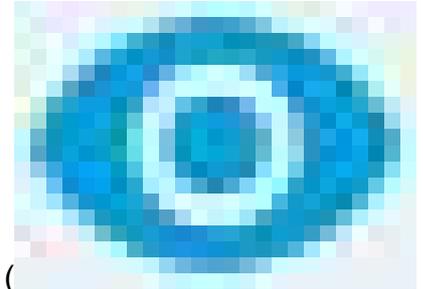
CANCEL

OK

Etapa 2 IP SLA3

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

Navegue até Device e clique no link no resumo de roteamento.



Se você habilitou roteadores virtuais, clique no ícone de visualização ( ) do roteador no qual você está configurando uma rota estática. Nesse caso, os roteadores virtuais não estão ativados.

Firewall Device Manager

Monitoring Policies Objects **Device: firepower**

Model: Cisco Firepower Threat Defense for KVM | Software: 7.4.1-172 | VDB: 376.0 | Intrusion Rule Update: 20231011-1536 | Cloud Services: Not Registered | Register | High Availability: Not Configured

Inside Netw... | Cisco Firepower Threat Defense for KVM | 0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7 | MGMT | CONSOLE | ESP/WAN/Gateway | Internet | DNS Server | NTP Server | Smart Lic...

Interfaces: Management: Merged, Enabled 4 of 9 | [View All Interfaces](#)

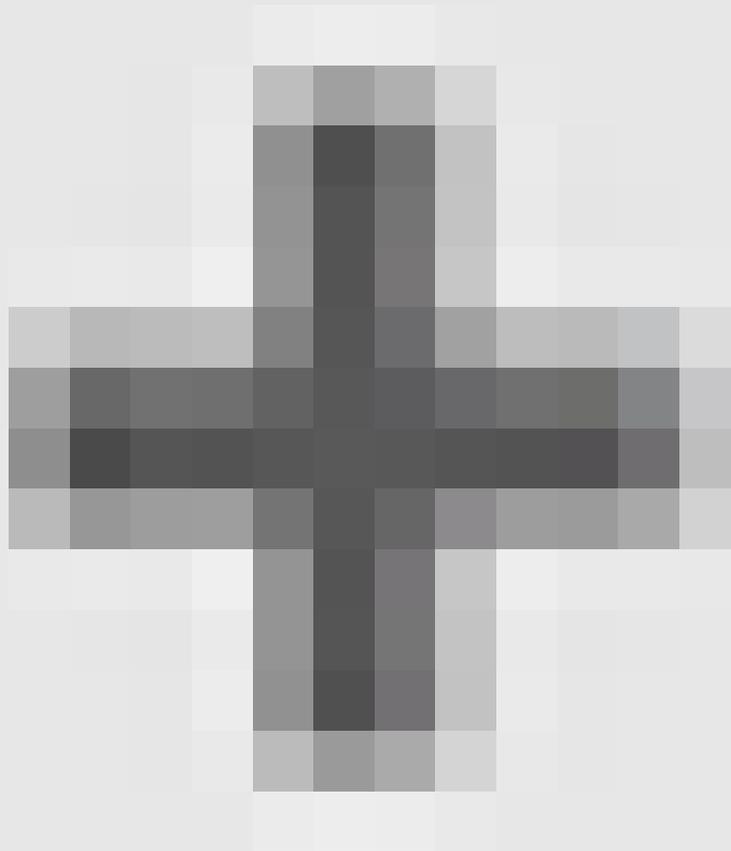
**Routing: 2 static routes** | [View Configuration](#)

Updates: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds | [View Configuration](#)

System Settings: Management Access, Logging Settings, DHCP Server / Relay, DDNS Service, DNS Server

Etapa 3 Rota1

Na página Static Routing, clique no ícone add (



) para adicionar uma nova rota estática para o primeiro link do ISP.

Na janela Add Static Route :

1. Defina o Nome da rota e, opcionalmente, a descrição. Nesse caso, `route_outside1`.
2. Na lista suspensa Interface, selecione a interface pela qual deseja enviar o tráfego, o endereço do gateway precisa estar acessível através da interface. Neste caso, `fora de 1 (GigabitEthernet0/1)`.
3. Selecione as redes que identificam as redes ou os hosts de destino que usam o gateway nesta rota. Nesse caso, o `any-ipv4` predefinido.
4. Na lista suspensa Gateway , selecione o objeto de rede que identifica o endereço IP do gateway. O tráfego é enviado para esse endereço. Nesse caso, `gw-outside1` (o primeiro

gateway do ISP).

5. Defina a métrica da rota, entre 1 e 254. Neste exemplo, 1.
6. Na lista suspensa Monitor do SLA, selecione o objeto do monitor do SLA. Neste caso, sla-outside1.
7. Click OK.

# Add Static Route



Name

route\_outside1

Description

Interface

outside1 (GigabitEthernet0/1)

Protocol

IPv4  IPv6

Networks



any-ipv4

Gateway

gw-outside1

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside1

CANCEL

OK

Repita a etapa semelhante para configurar outra rota estática para a segunda conexão do ISP, na janela Add Static Route :

1. Defina o Nome da rota e, opcionalmente, a descrição. Nesse caso, route\_outside2.
2. Na lista suspensa Interface, selecione a interface pela qual deseja enviar o tráfego, o endereço do gateway precisa estar acessível através da interface. Nesse caso, fora de 2 (GigabitEthernet0/2).
3. Selecione as redes que identificam as redes ou os hosts de destino que usam o gateway nesta rota. Nesse caso, o any-ipv4 predefinido.
4. Na lista suspensa Gateway, selecione o objeto de rede que identifica o endereço IP do gateway. O tráfego é enviado para esse endereço. Nesse caso, gw-outside2 (o segundo gateway do ISP).
5. Defina a métrica da rota, entre 1 e 254. Neste exemplo, 1.
6. Na lista suspensa Monitor do SLA, selecione o objeto do monitor do SLA. Neste cenário, sla-outside2.
7. Click OK.

# Add Static Route



Name

route\_outside2

Description

Interface

outside2 (GigabitEthernet0/2)

Protocol

IPv4

IPv6

Networks



any-ipv4

Gateway

gw-outside2

Metric

1

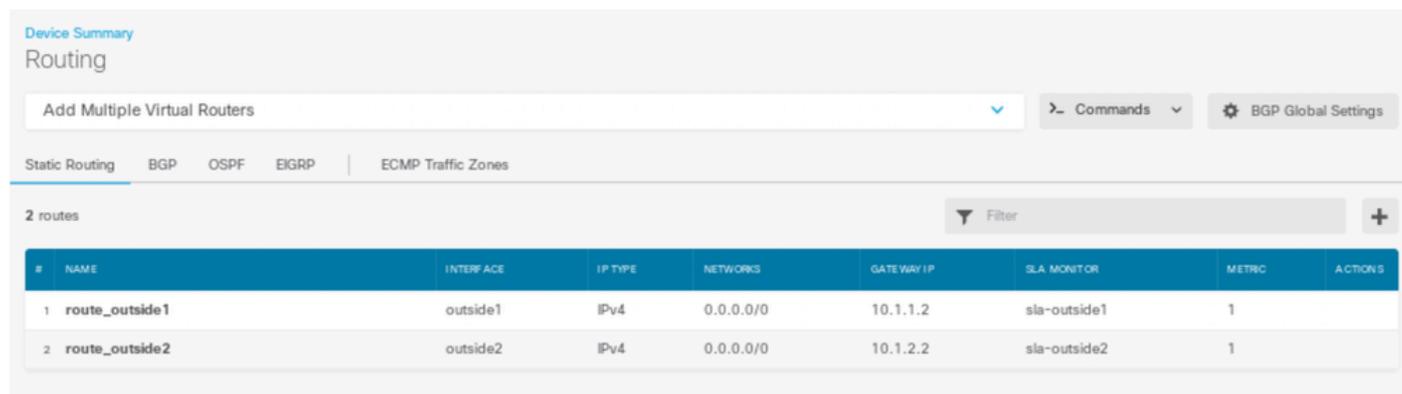
SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

Você tem 2 rotas através das interfaces outside1 e outside2 com rotas.



#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	route_outside1	outside1	IPv4	0.0.0.0/0	10.1.1.2	sla-outside1	1	
2	route_outside2	outside2	IPv4	0.0.0.0/0	10.1.2.2	sla-outside2	1	

Etapa 3 Rota4

Implante a alteração no FTD.

## Verificar

Efetue login no CLI do FTD, 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 GigabitEthernet0/2
```

```
outside1 GigabitEthernet0/1
```

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: 1037119999  
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: 1631063762  
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 comando `show 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, de modo que a rota padrão através da interface de destino está ativa e instalada na tabela de roteamento.

<#root>

```
> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
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: 05:32:32.791 UTC Tue Jan 30 2024

Latest operation return code: OK

RTT Values:

RTTAvg: 1 RTTMin: 1 RTTMax: 1

NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 1631063762

Modification time: 04:14:32.771 UTC Tue Jan 30 2024

Number of Octets Used by this Entry: 2056

Number of operations attempted: 79

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: 05:32:32.791 UTC Tue Jan 30 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 SSH a partir de Test-PC-1 (10.1.3.2) e Test-PC-2 (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 ISP, Test-PC-1 (10.1.3.2) passa pela interface `outside1`, Test-PC-2 (10.1.3.4) passa pela interface `outside2`.

<#root>

> show conn

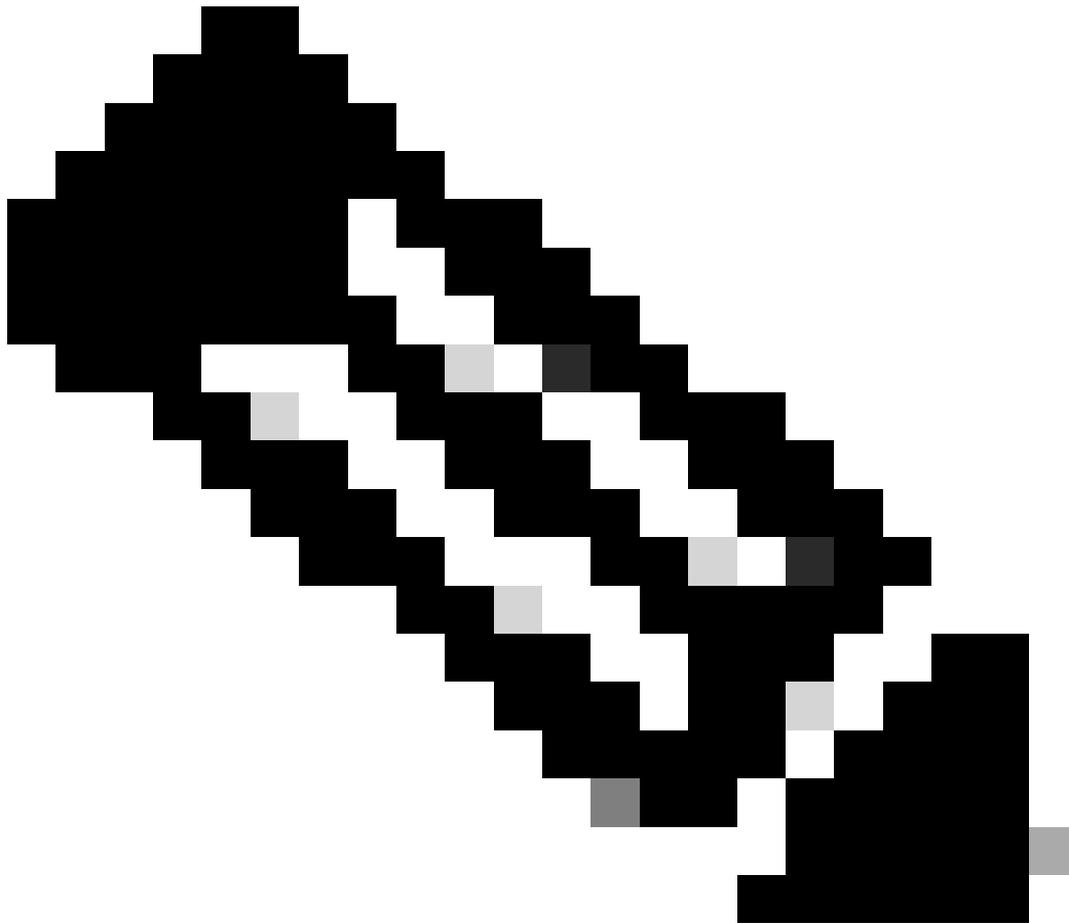
4 in use, 14 most used

Inspect Snort:

preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

**TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:02:10, bytes 5276, flags UIO N1**

**TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:00:04, bytes 5276, 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: 1037119999

Modification time: 04:14:32.771 UTC Tue Jan 30 2024

Number of Octets Used by this Entry: 2056

Number of operations attempted: 121

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: 06:14:32.801 UTC Tue Jan 30 2024

Latest operation return code: Timeout

RTT Values:

RTTAvg: 0 RTTMin: 0 RTTMax: 0

NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 1631063762

Modification time: 04:14:32.771 UTC Tue Jan 30 2024

Number of Octets Used by this Entry: 2056

Number of operations attempted: 121

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: 06:14:32.802 UTC Tue Jan 30 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
```

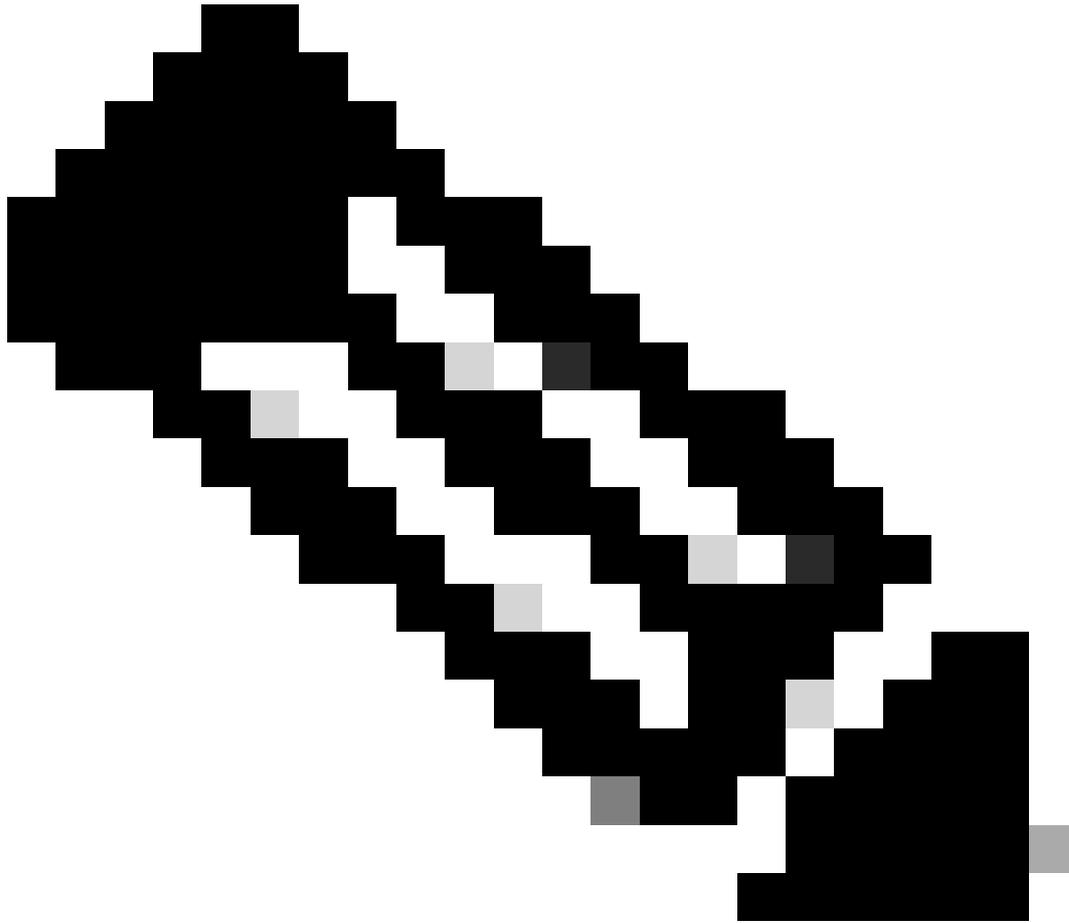
Execute o comando show conn , você pode descobrir que as duas conexões ainda estão ativas. As sessões SSH também estão ativas no Test-PC-1 (10.1.3.2) e no Test-PC-2 (10.1.3.4) sem nenhuma interrupção.

```
<#root>
```

```
> show conn  
4 in use, 14 most used  
Inspect Snort:  
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect
```

```
TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:19:29, bytes 5276, flags UIO N1
```

```
TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:17:22, bytes 5276, flags UIO N1
```



**Observação:** você pode observar na saída de `show conn` , a sessão SSH de Test-PC-1 (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 Test-PC-1 (10.1.3.2) para Internet-Host (10.1.5.2), você 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

RT(mgmt-only):

**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.

> 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

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

## 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.