

Configurar o PBR com o HTTP Path Monitor no FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o PBR para o monitoramento de caminho HTTP](#)

[Configurar ECMP \(Equal-cost-multi-path, vários caminhos de custo igual\)](#)

[Configurar DNS confiável para FTD seguro](#)

[Habilitar monitoramento de caminho](#)

[Adicionar painel de monitoramento](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o Roteamento Baseado em Políticas (PBR - Policy-Based Routing) com o Monitoramento de Caminho HTTP no Cisco Secure Firewall Management Center (FMC - Cisco Secure Firewall Management Center).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- conhecimento básico de PBR
- Experiência básica do Cisco Secure Management Center
- Cisco Secure Firewall Threat Defense (FTD) básica

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware executando a versão 7.4

- Dispositivo virtual Cisco Secure Firewall Threat Defense (FTDv) VMware executando a versão 7.4

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

No roteamento tradicional, os pacotes são roteados com base no endereço IP de destino; no entanto, é difícil alterar o roteamento de especificação de tráfego em um sistema de roteamento baseado em destino. O PBR oferece mais controle sobre o roteamento, estendendo e complementando os mecanismos existentes fornecidos pelos protocolos de roteamento.

O PBR permite definir a precedência do IP. Ele também permite a especificação de um caminho para determinado tráfego, como o tráfego prioritário sobre um link de alto custo. Com o PBR, o roteamento é baseado em critérios diferentes da rede de destino, como porta de origem, endereço de destino, porta de destino, aplicativos de protocolo ou uma combinação desses objetos. O PBR pode ser usado para classificar o tráfego de rede com base no aplicativo, nome de usuário, associação de grupo e associação de grupo de segurança. Esse método de roteamento é aplicável em situações em que vários dispositivos acessam aplicativos e dados em uma grande implantação de rede. Tradicionalmente, grandes implantações têm topologias que fazem o backhaul de todo o tráfego de rede para um hub como tráfego criptografado em uma VPN baseada em roteamento. Essas topologias geralmente resultam em problemas como latência de pacote, largura de banda reduzida e queda de pacote.

O PBR é suportado apenas no modo de firewall roteado e não é aplicado para conexões embrionárias. A aplicação baseada em HTTP é suportada em interfaces físicas, de canal de porta, de subinterfaces e de túnel de status. Não há suporte para ele em dispositivos de cluster.

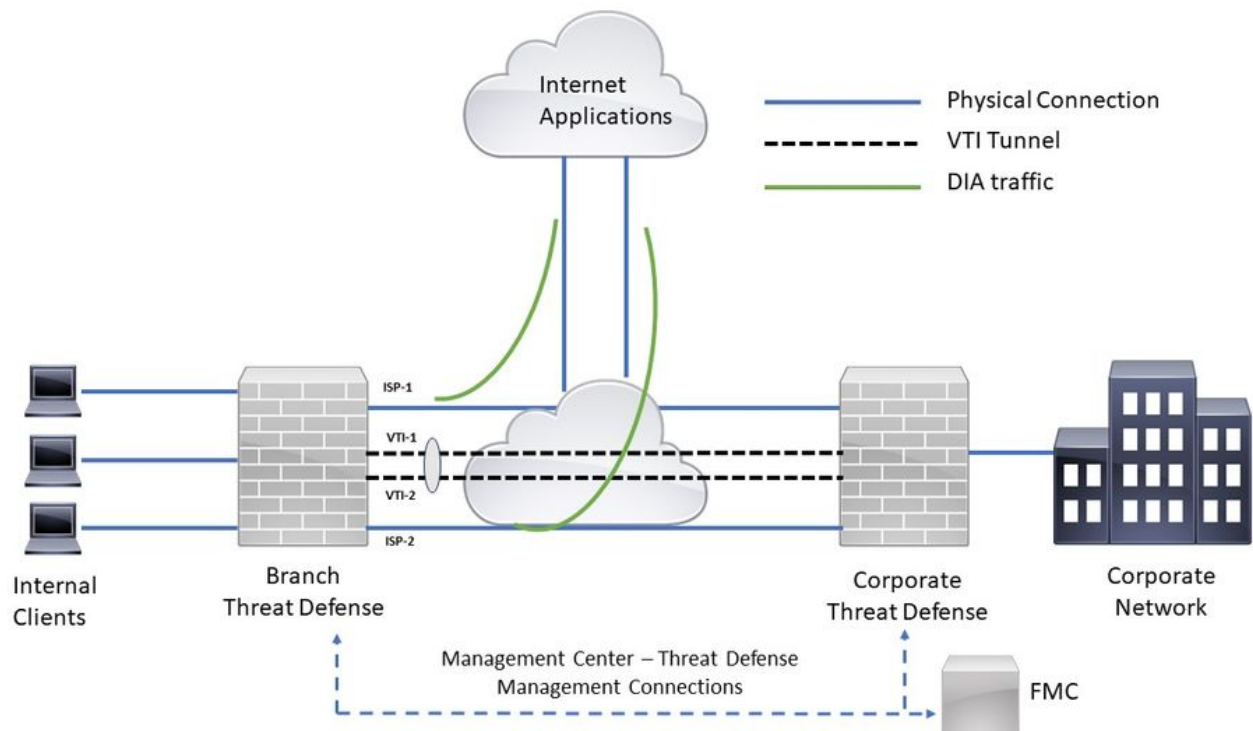
Quando as interfaces configuradas derivam métricas como tempo de ida e volta (RTT), jitter, pontuação média de opinião (MOS) e perda de pacotes por interface, elas são usadas para determinar o melhor caminho para rotear o tráfego PBR. O Path Monitoring calcula métricas flexíveis para vários pontos remotos por interface. Para monitorar e determinar o melhor caminho para vários aplicativos por meio de uma política em um firewall de filial, o HTTP tem preferência sobre o ICMP pelos seguintes motivos:

- O ping HTTP pode derivar as métricas de desempenho do caminho até a camada de aplicação do servidor, onde o aplicativo está hospedado.
- A necessidade de alterar a configuração do firewall sempre que o endereço IP do servidor de aplicativos é alterado é removida, pois o domínio do aplicativo é rastreado em vez do endereço IP.

Configurar

Diagrama de Rede

Considere um cenário típico de rede corporativa em que todo o tráfego da rede da filial é enviado através de uma VPN baseada em rota da rede corporativa e diverge para a extranet quando necessário. A próxima topologia mostra uma rede de filial conectada à rede corporativa por meio de uma VPN baseada em rota. Tradicionalmente, a defesa contra ameaças corporativa é configurada para lidar com o tráfego interno e externo da filial. Com a política de PBR, a defesa contra ameaças da filial é configurada com uma política que roteia tráfego específico para a rede WAN, em vez de túneis virtuais. O restante do tráfego flui pela VPN baseada em rota, como de costume.



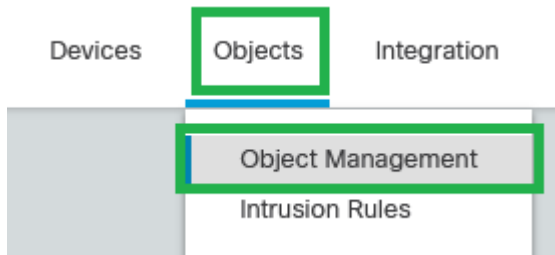
Topologia de rede

A seção de configuração assume que as interfaces do ISP e VTI já estão configuradas para a defesa contra ameaças da filial no FMC seguro.

Configurar o PBR para o monitoramento de caminho HTTP

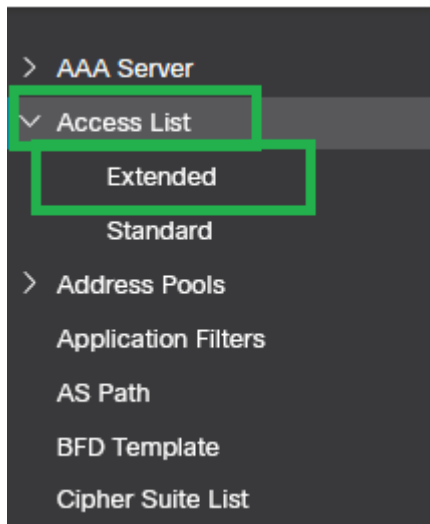
Esta seção de configuração mostra a configuração Path Monitoring nas interfaces ISP-1 e ISP-2.

Etapa 1. Criar uma lista de acesso Estendida para Aplicativos monitorados. Navegue até **Objects > Object Management**.



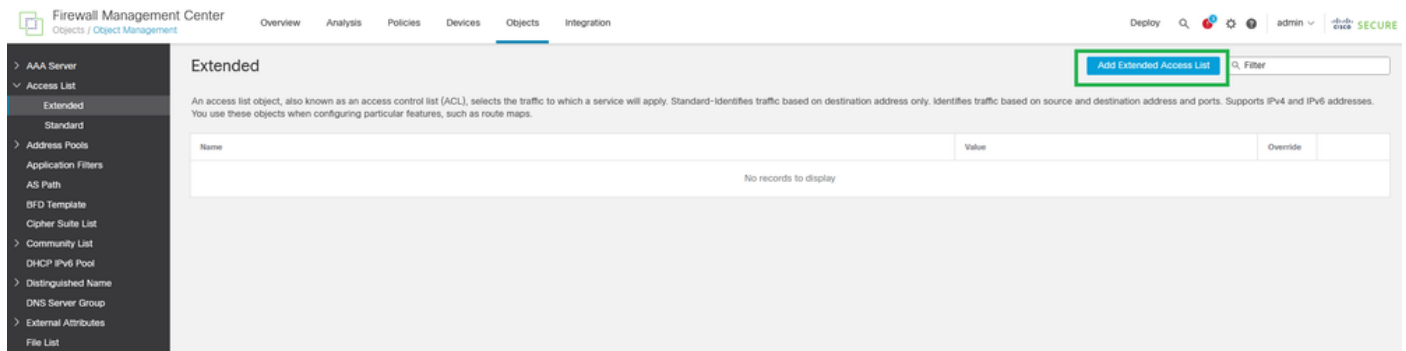
Objetos - Gerenciamento de Objetos

Etapa 2. Navegue até Access-list > Extended no menu à esquerda.



Lista de acesso - Estendida

Etapa 3. Clique em Add Extended Access List.



Adicionar Lista de Acesso Estendida

Etapa 4. Configure um nome na Lista de Acesso Estendida e clique em Add.

New Extended Access List Object

Name

Entries (0)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

☐ Allow Overrides

Cancel Save

Novo Objeto da Lista de Acesso Estendida

Etapa 5. Clique **Application** e escolha os aplicativos desejados (alguns aplicativos Cisco foram escolhidos para este exemplo). Depois, clique em **Add**.

Add Extended Access List Entry

Action:

Logging:

Log Level:

Log Interval:
 Sec.

Network Port **Application** Users Security Group Tag

Application Filters Clear All Filters

Risks (Any Selected)
☐ Very Low 730
☐ Low 622
☐ Medium 734
☐ High 1556
☐ Very High 577

Business Relevance (Any Selected)
☐ Very Low 885

Available Applications (4)

Cisco
Cisco Jabber
Cisco Secure Endpoint
Cisco Webex Assistant

Add to Rule

Selected Applications and Filters (6)

Applications
Cisco Jabber
Cisco Secure Endpoint
Cisco Webex Assistant
WebEx
WebEx Connect
Webex Teams

Cancel Add

Adicionar Entrada de Lista de Acesso Estendida



Note: A lista de acesso estendida pode ser configurada com portas e IPs de origem/destino para corresponder o tráfego específico aos aplicativos desejados. Você pode criar várias listas de controle de acesso estendidas para aplicar à configuração do PBR.

Etapa 6. Valide a configuração da Lista de acesso estendida e clique em **Save**.

New Extended Access List Object

Name
Applications

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	Any	Any	Any	Any	Cisco Jabber Cisco Secure Endpoint Cisco Webex Assistant WebEx (2 more...)	Any		 

☐ Allow Overrides

Cancel Save

Salvar Objeto da Lista de Acesso Estendida

Passo 7. Navegue até **Devices > Device Management** e edite a defesa contra ameaças.

Firewall Management Center

Overview Analysis Policies **Devices** Objects Integration

View By: Group

Device Management

Name	Model	Version	Configuration	Access Control Policy	Auto Rollback	
FTD TAC 1 172.16.1.101 - Routed	FTDv for VMware	7.4.0	N/A	Essentials, Secure Client VPN Only Cisco TAC		
FTD TAC 2 172.16.1.28 - Routed	FTDv for VMware	7.4.0	N/A	Essentials, Secure Client VPN Only Cisco TAC 2		

Dispositivo - Gerenciamento de dispositivos

Etapa 8. Navegue até **Routing > Policy-Based Routing**.

Firewall Management Center

Overview Analysis Policies **Devices** Objects Integration

FTD TAC

Cisco Firepower Threat Defense for VMware

Device **Routing** Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

IGRP

RP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

Virtual Router Properties

These are the basic details of this virtual router.

VRF Name: Global

Description: This is a Global Virtual Router

Select Interface: Q Search

Available Interfaces

management

ISP-1

ISP-2

VTI-1

VTI-2

Selected Interfaces

management

ISP-1

VTI-2

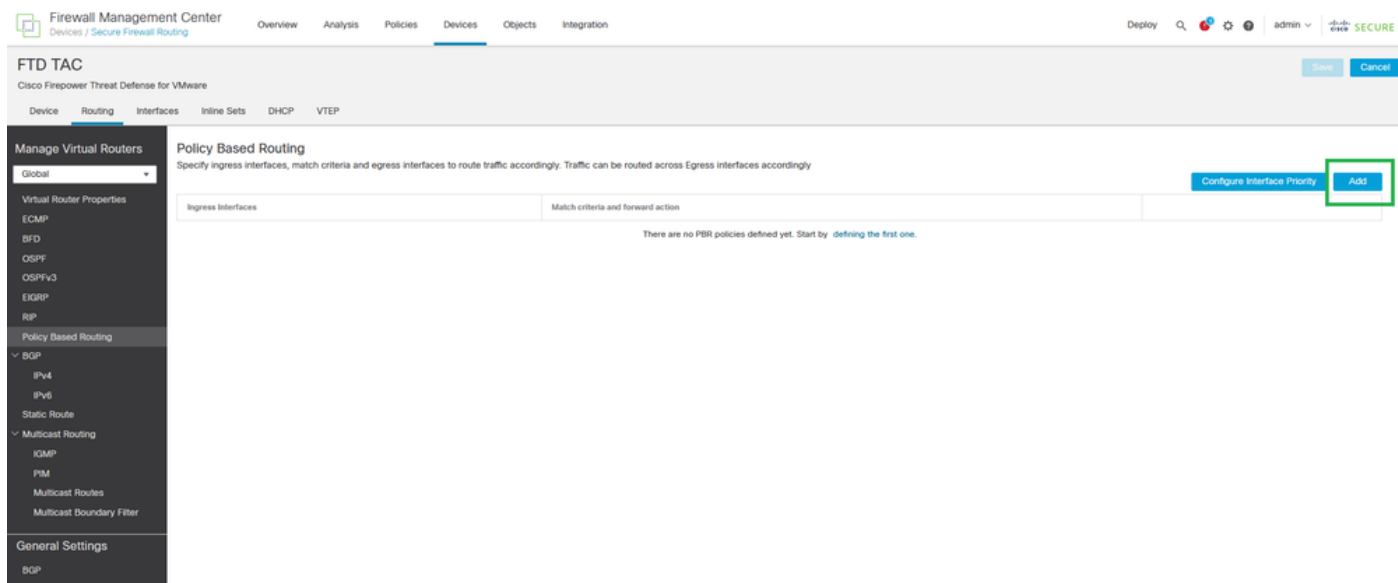
INSIDE

ISP-1

ISP-2

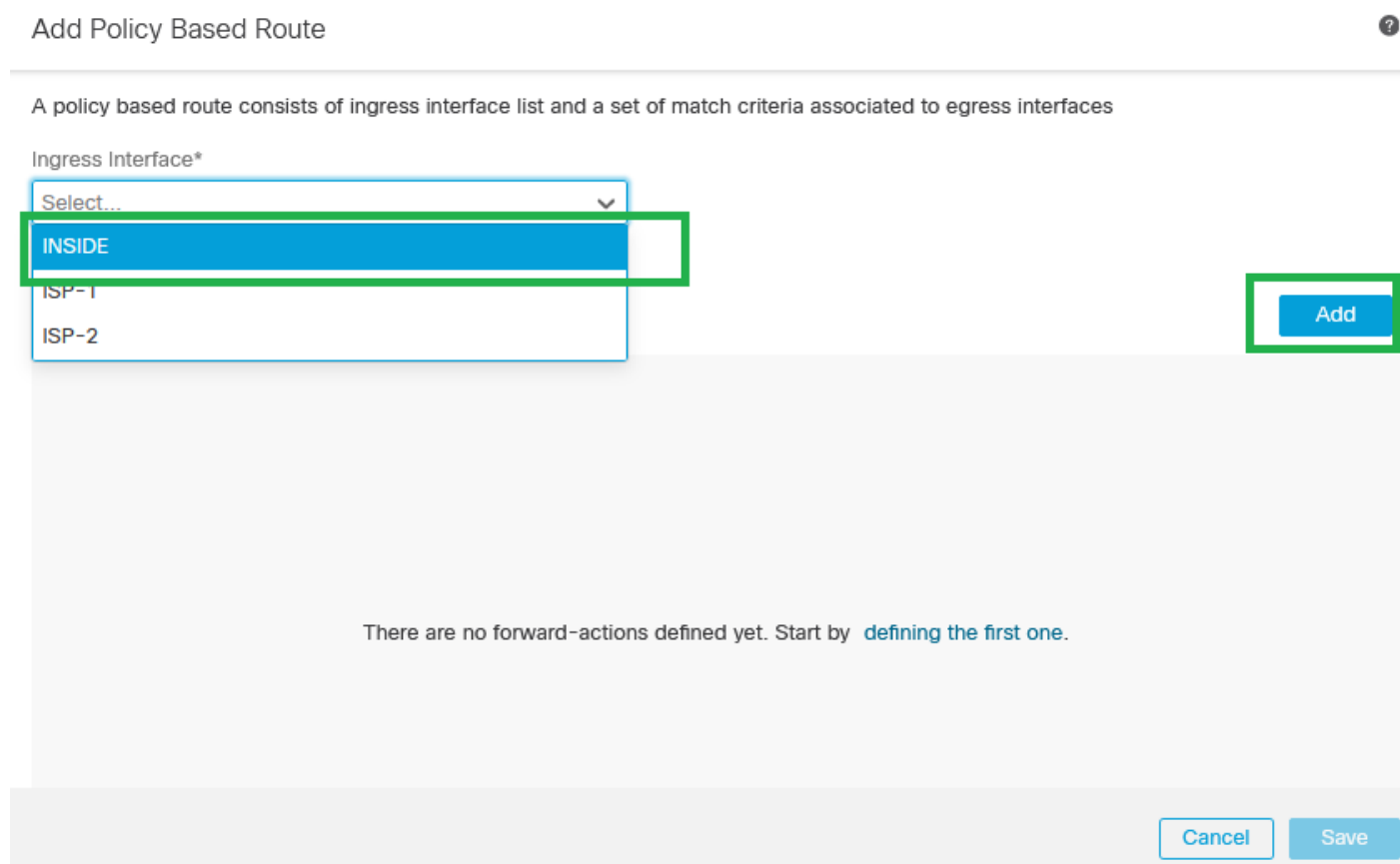
Roteamento - Roteamento baseado em políticas

Etapa 9. Clique em **Add**.



Adicionar Roteamento Baseado em Política

Etapa 10. Adicione a interface de ingresso para a configuração do PBR (INSIDE neste exemplo) e clique em Add.



Adicionar Rota Baseada em Política

Etapa 11. Defina Critérios de Correspondência (com a Lista de Acesso Estendida Criada nas etapas anteriores), Interfaces de Saída e Ordenação de Interface.

Add Forwarding Actions



Match ACL:*

Applications

+

Send To:*

Egress Interfaces

▼

Interface Ordering:*

Minimal Jitter

▼

i

Available Interfaces

Search by interface name

Q

Interface	
INSIDE	+
ISP-1	+
ISP-2	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

No interfaces selected

Cancel

Save

Adicionar ações de encaminhamento



Observação: Egress Interfaces e Minimal Jitter foram escolhidos para este guia de configuração. Consulte a [documentação oficial do PBR](#) para saber mais sobre as outras opções.

Etapa 12. Escolha as Interfaces de saída (ISP-1 e ISP-2 para este exemplo) e clique em Save.

Add Forwarding Actions



Match ACL:* Applications

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter

Available Interfaces

Search by interface name



Interface	
INSIDE	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

Interface

ISP-1



ISP-2



Cancel

Save

Interfaces de saída selecionadas

Etapa 13. Valide a configuração do PBR e clique em Save.

Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

INSIDE x



Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Match ACL

Forwarding Action

Applications

Send through minimum jitter interface



ISP-1



ISP-2



Cancel

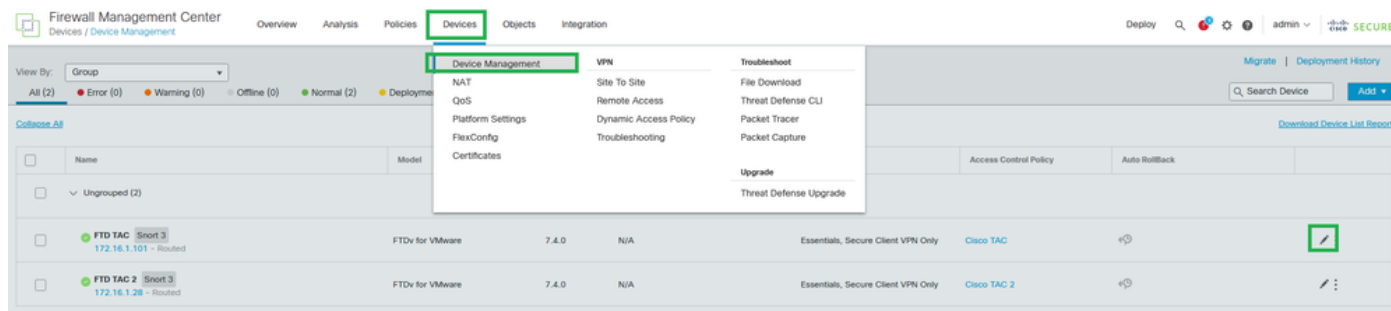
Save

Etapa 14. (Opcional) Repita as Etapas 9, 10, 11, 12 e 13 se forem criadas mais Listas de Controle de Acesso Estendidas ou se houver mais interfaces de origem onde a configuração de PBR deva ser aplicada.

Etapa 15. Salvar e implantar alterações do FMC.

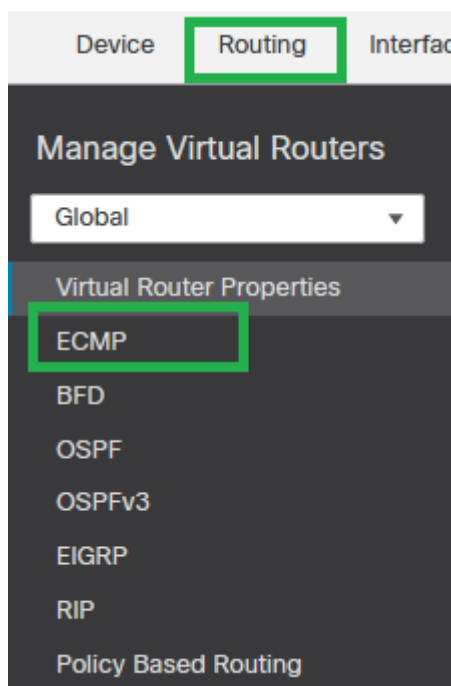
Configurar ECMP (Equal-cost-multi-path, vários caminhos de custo igual)

Etapa 1. Navegue até Devices > Device Management e edite a defesa contra ameaças.



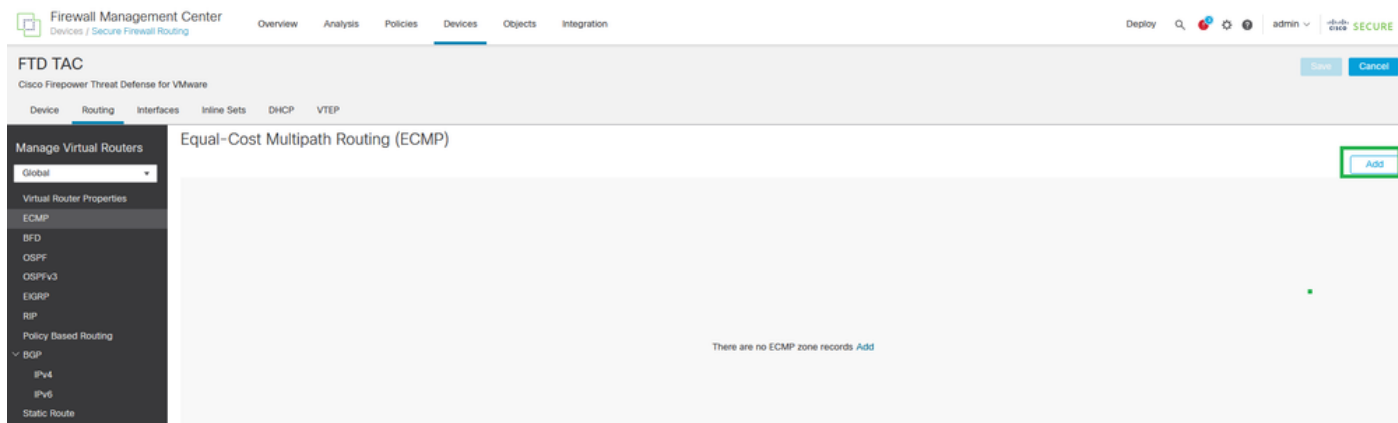
Dispositivo - Gerenciamento de dispositivos

Etapa 2. Navegue até Routing > ECMP.



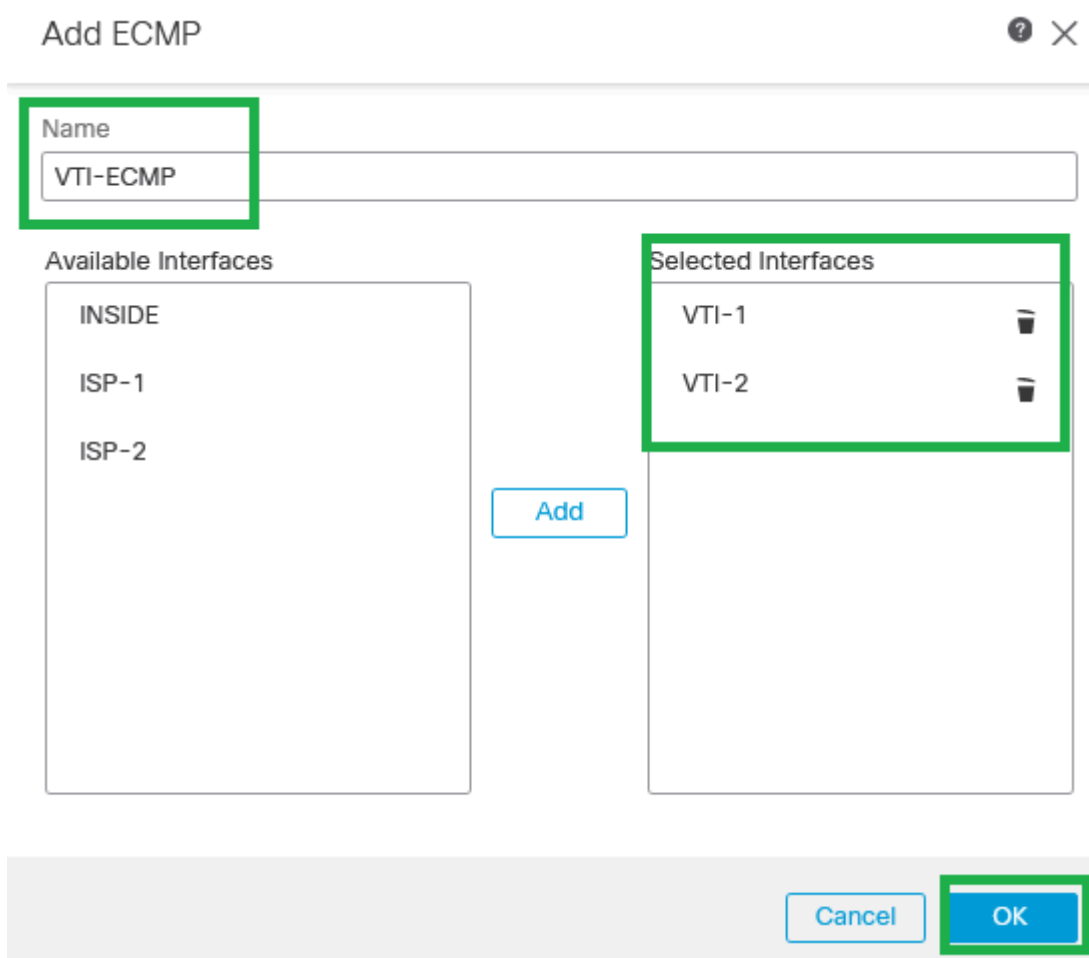
Roteamento - ECMP

Etapa 3. Clique Add para criar o ECMP entre as interfaces VTIs e WAN (ISP-1 e ISP-2 para este guia de configuração).



Roteamento de vários caminhos de custo igual (ECMP)

Etapa 4. Configure o nome ECMP, escolha todas as interfaces VTIs e clique em Add.



ECMP para VTIs

Etapa 5. Repita as Etapas 3 e 4 para criar o ECMP entre as interfaces WAN (ISP-1 e ISP-2 para este guia de configuração).

Add ECMP

?

×

Name

ISP-ECMP

Available Interfaces

INSIDE

VTI-1

VTI-2

Add

Selected Interfaces

ISP-2

🗑

ISP-1

🗑

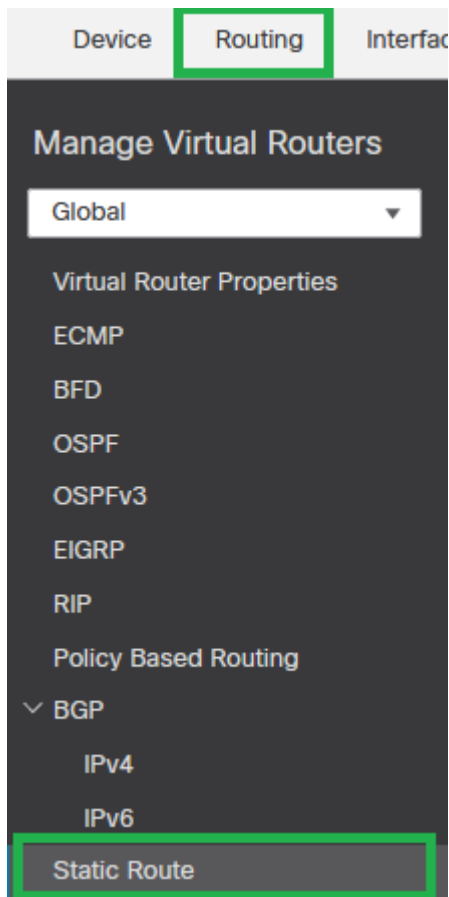
Cancel

OK

ECMP para interfaces ISP

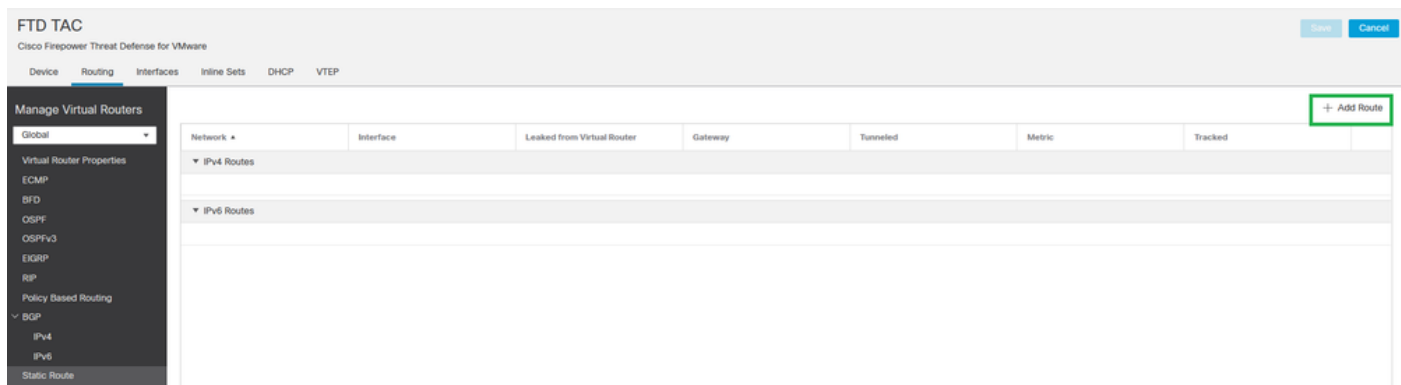
Etapa 6. Salvar a configuração do ECMP.

Etapa 7. Configure as rotas estáticas para as interfaces de região para fazer o balanceamento de carga. Navegue até [Routing > Static Route](#).



Roteamento - Rota estática

Etapa 8. Clique em + Add Route.



+ Adicionar rota

Etapa 9. Crie uma rota estática padrão para a(s) interface(s) VTI (VTI-1 para este guia de configuração) com 1 como valor da métrica e clique em OK.

Add Static Route Configuration



Type:

☒ IPv4 ☐ IPv6

Interface*

VTI-1

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

Available Network 



any



Add

any-ipv4

IPv6-to-IPv4-Relay-Anycast

Selected Network

any-ipv4



Gateway*

VTI-Tunnel1-FPR2



Metric:

1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

Rota estática padrão para VTI-1

Etapa 10. Repita a Etapa 8. se houver mais interfaces VTI configuradas.



Note: Crie uma Rota Padrão para cada interface VTI configurada.

Etapa 11. Crie uma rota estática padrão para a(s) interface(s) WAN/ISP (ISP-1 para este guia de configuração) com um valor métrico maior que o VTI e clique em OK.

Add Static Route Configuration



Type: ☒ IPv4 ☐ IPv6

Interface*

ISP-1

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

Available Network 



any-

Add

any-ipv4

Selected Network

any-ipv4



Gateway*

172.16.1.254GW-24



Metric:

10

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

Rota estática padrão para ISP-1

Etapa 12. Repita a Etapa 10 se houver mais interfaces WAN/ISP configuradas.



Note: Crie uma Rota Padrão para cada interface WAN/ISP configurada.

Etapa 13. Valide a configuração de rotas padrão e clique em OK.

FTD TAC
Cisco Firepower Threat Defense for VMware

You have unsaved changes **Save** **Cancel**

Device **Routing** Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EGRP

RIP

Policy Based Routing

✓ BGP

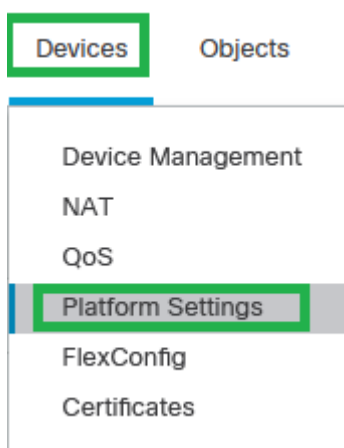
Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
▼ IPv4 Routes							
any-ipv4	ISP-2	Global	172.16.11.254-GW-24	false	10		 
any-ipv4	ISP-1	Global	172.16.1.254GW-24	false	10		 
any-ipv4	VTI-2	Global	VTI-Tunnel2-FPR2	false	1		 
any-ipv4	VTI-1	Global	VTI-Tunnel1-FPR2	false	1		 
▼ IPv6 Routes							

+ Add Route

Configuração de rota estática

Configurar DNS confiável para FTD seguro

Etapa 1. Navegue até **Devices > Platform Settings**.



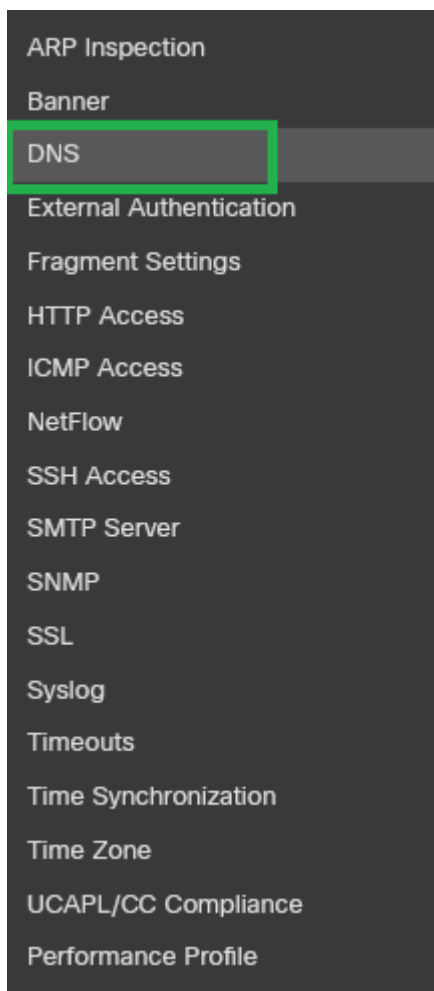
Dispositivos - Configurações da plataforma

Etapa 2. Criar ou editar uma Política de Configurações de Plataforma existente.



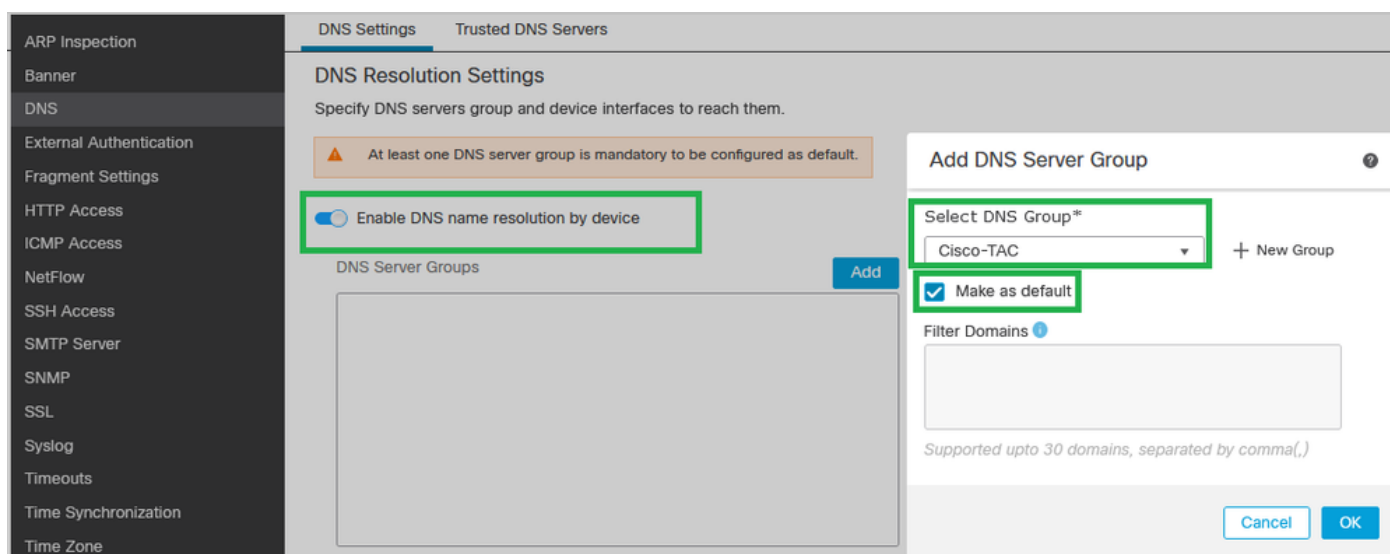
Note: Certifique-se de que a política de configurações da plataforma esteja aplicada aos dispositivos Secure Threat Defense.

Etapa 3. Clique em **DNS**.



Configurações da plataforma DNS

Etapa 4. Habilite DNS name resolution by device e clique Add ou escolha um grupo DNS existente. Escolha Make as default e clique em OK.



Adicionar grupo de servidores DNS



Note: Se você quiser saber mais sobre a configuração DNS na Política de configurações

de plataforma, consulte a documentação oficial de [Configurações de plataforma](#).

Etapa 5. Escolha as interfaces WAN/ISP na seção Interface Objects.

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Expiry Entry Timer:

1 Range: 1-65535 minutes

Poll Timer:

240 Range: 1-65535 minutes

Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects

Search

INSIDE

ISP-1

ISP-2

VTI-1

VTI-11

VTI-2

Add

Selected Interface Objects

ISP-1

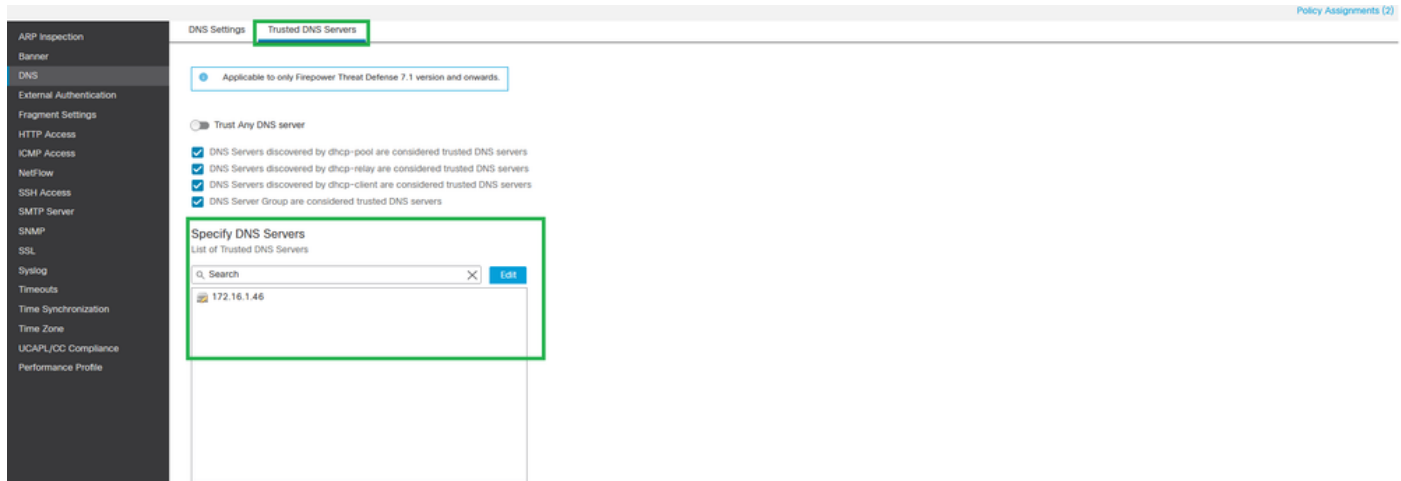
ISP-2

☐ Enable DNS Lookup via diagnostic/Management interface also.

Configuração da interface DNS

Etapa 6. Salve as alterações.

Etapa 7. Navegue até o Trusted DNS Servers e especifique os servidores DNS confiáveis.

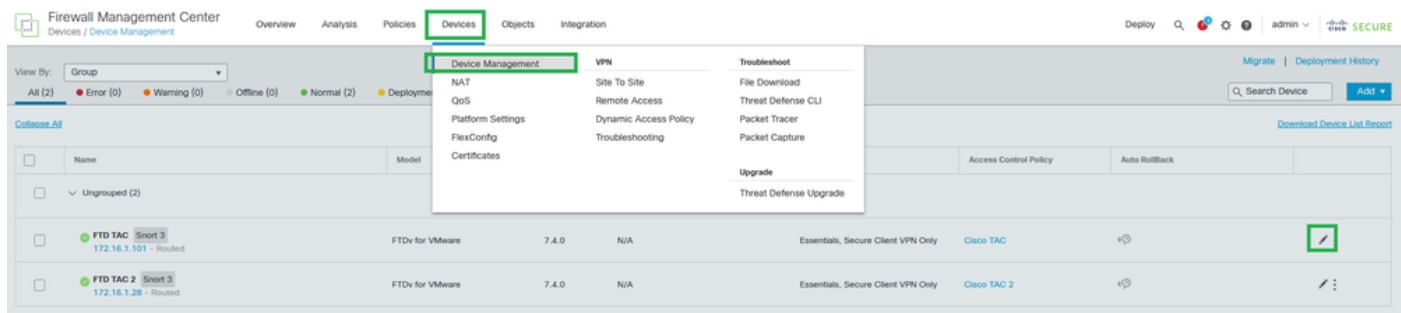


Servidores DNS confiáveis

Etapa 8. Clique **Save** e implante as alterações.

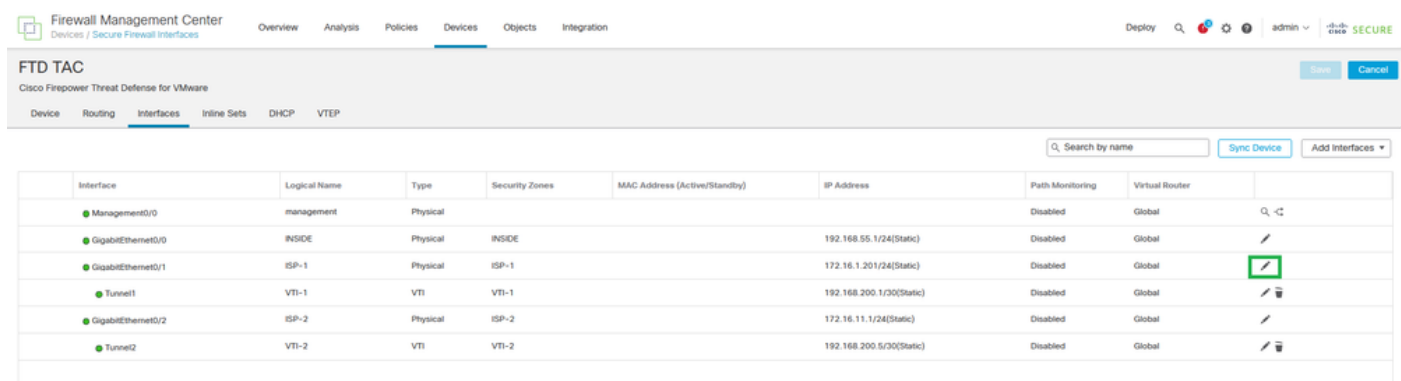
Habilitar monitoramento de caminho

Etapa 1. Navegue até **Devices > Device Management** e edite a defesa contra ameaças.



Dispositivo - Gerenciamento de dispositivos

Etapa 2. Na guia **Interfaces**, edite as interfaces WAN/ISP (ISP-1 e ISP-2 para este guia de configuração).



Configuração da interface

Etapa 3. Clique na **Path Monitoring** guia, escolha a caixa de seleção **Enable IP Monitoring** e ative **HTTP-based Application Monitoring**. Depois, clique em **Save**.

Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

☒ Enable IP based Monitoring

Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface.

Monitoring Type:

Next-hop of default route out of interface (Auto) ▼

System monitors the next hop of the interface. Tries IPv4 and then IPv6.
If the peer is unavailable, monitoring is not done.

☒ Enable HTTP based Application Monitoring

By enabling application monitoring you are allowing all the applications configured in Extended ACLs used in policy based routing with this interface as egress interface to be monitored automatically.

Applications

Cisco Jabber

Cisco Secure Endpoint

Cisco Webex Assistant

WebEx

WebEx Connect

Cancel

OK

Configuração de monitoramento de caminho de interface



Caution: Os aplicativos configurados na seção de configuração anterior devem ser listados.



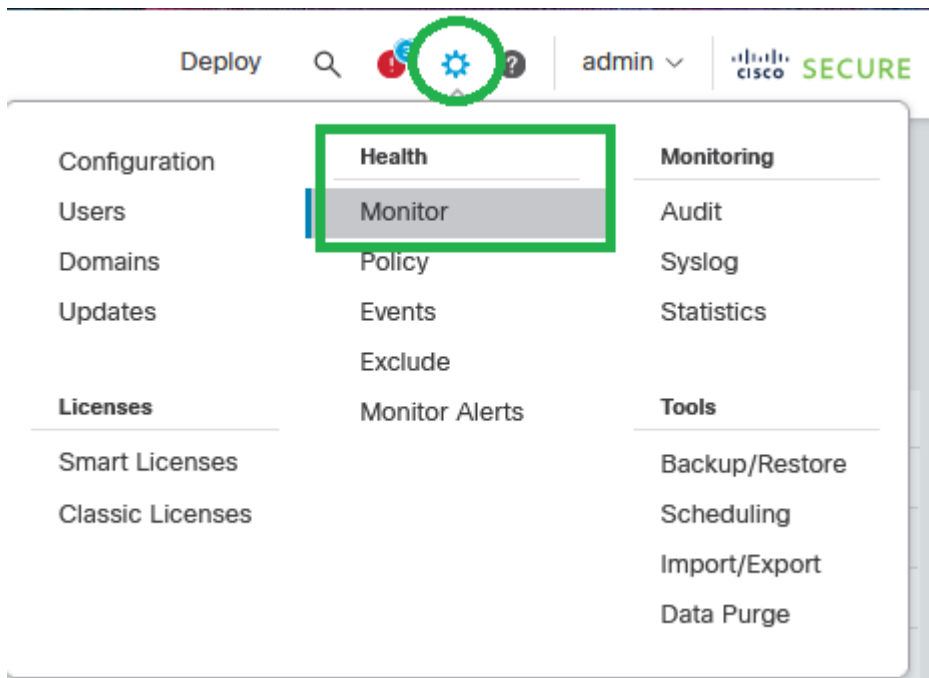
Note: 'Tipo de monitoramento' foi escolhido para este guia de configuração. Verifique as Configurações de monitoramento de caminho no [guia de configuração oficial](#) para saber mais sobre outras opções.

Etapa 4. Repita as Etapas 2 e 3 para todas as interfaces WAN/ISP configuradas.

Etapa 5. Clique **Save** e implante as alterações.

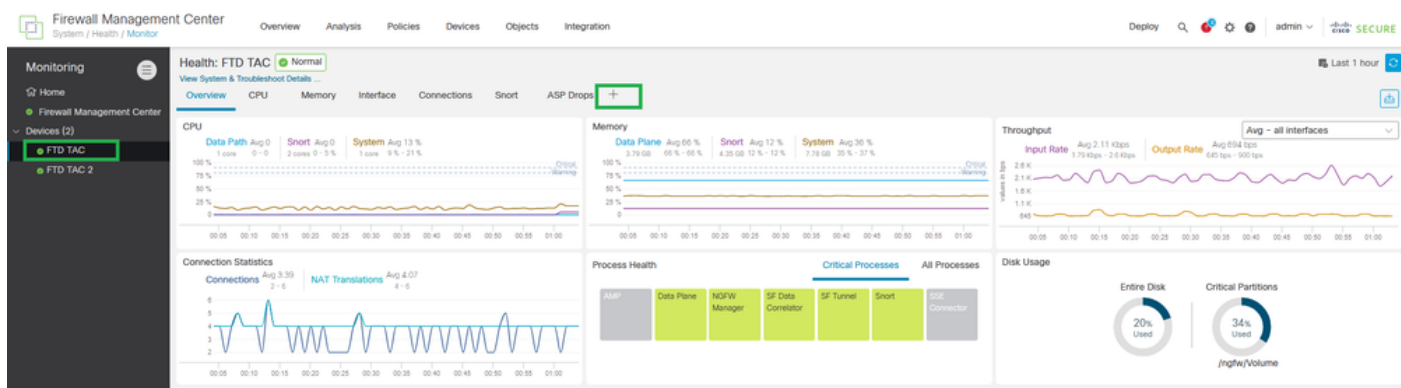
Adicionar painel de monitoramento

Etapa 1. Navegue até **System > Health > Monitor**.



Sistema - Integridade - Monitor

Etapa 2. Escolha o dispositivo FTD seguro e clique em Add New Dashboard.



Adicionar novo painel

Etapa 3. Configure o Nome do Painel e, na caixa de diálogo Correlate Metrics, na lista suspensa, escolha Interface - Path Metrics. Depois, clique em . Add Dashboard

Add New Dashboard



Name*

FTD HTTP Path Monitoring

Metrics*

Metrics can be chosen from pre-defined correlation groups or/and metrics of your choice. Related metrics are grouped together, select a group and then the metrics.

Interface

Jitter x

x

v



Interface

Mean Opinion Score (MOS) x

x

v



Interface

Round Trip Time x

x

v



Interface

Packet Loss x

x

v



Add Metrics

Add from Predefined Correlations v

Clear All

Cancel

Add Dashboard

Adicionar novo painel com métricas de caminho

Verificar

Esta seção descreve como verificar as rotas estáticas flutuantes, o ECMP, o grupo de objetos com aplicativos e as configurações de PBR.

Verifique a configuração das rotas padrão e das rotas estáticas flutuantes:

```
firepower# show run route
route VTI-1 0.0.0.0 0.0.0.0 192.168.200.1 1
route VTI-2 0.0.0.0 0.0.0.0 192.168.200.5 1
route ISP-1 0.0.0.0 0.0.0.0 172.16.1.254 10
route ISP-2 0.0.0.0 0.0.0.0 172.16.11.254 10
```

Verifique a configuração do ECMP:

```
firepower# sh run | i ecmp
zone ECMP-VTI ecmp
zone ECMP-ISP ecmp
```

Verifique se o tráfego está sendo balanceado pelo ECMP, na tabela de roteamento. A tabela de roteamento deve instalar ambas as rotas na tabela de roteamento do FTD seguro.

```
firepower# show route static
```

```
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 172.16.11.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.200.5, VTI-2
[1/0] via 192.168.200.1, VTI-1
```

Verifique a configuração do mapa de rota PBR:

```
firepower# show run route-map
!
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set adaptive-interface cost ISP-1 ISP-2
!
```

Verifique a ACL atribuída à configuração de PBR (verifique o nome da ACL na configuração do mapa de rota):

```
firepower# show run access-list | i Applications
access-list Applications extended permit ip any object-group-network-service FMC_NSG_639950173988
```

Verifique o grupo de objetos com os aplicativos atribuídos à lista de acesso (verifique o nome do grupo de objetos na configuração da ACL):

```
firepower# show run object-group
object-group network-service FMC_NSG_639950173988
network-service-member "Cisco Jabber"
network-service-member "Cisco Secure Endpoint"
network-service-member "Cisco Webex Assistant"
network-service-member "WebEx"
network-service-member "WebEx Connect"
network-service-member "Webex Teams"
```

Verifique a rota de política atribuída às interfaces de dados usadas na configuração de PBR:

```

interface GigabitEthernet0/0
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.35.1 255.255.255.0
policy-route route-map FMC_GENERATED_PBR_1694885402369
!
interface GigabitEthernet0/1
nameif ISP-1
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
zone-member ECMP-ISP
ip address 172.16.1.202 255.255.255.0
policy-route path-monitoring auto
!
interface GigabitEthernet0/2
nameif ISP-2
security-level 0
zone-member ECMP-ISP
ip address 172.16.11.2 255.255.255.0
policy-route path-monitoring auto
!

```

Verifique as estatísticas de Jitter, MOS, Round Trip Time e Packet Loss nas informações do Painel de monitoramento de caminho HTTP.



Verificar Painel de Monitoramento de Caminho HTTP

Troubleshooting

Em caso de falha no Path Monitoring, com o monitoramento baseado em IP habilitado, as interfaces WAN/ISP são configuradas para enviar pacotes de prova ICMP ao gateway configurado em rotas estáticas. Configure as capturas de ingresso/saída nas interfaces WAN/ISP

para verificar se o ICMP funciona.

Captura de ingresso e saída:

```
firepower# cap in interface ISP-1 trace match icmp any any
firepower# cap in2 interface isP-2 trace match icmp any any
```

Captura de entrada:

```
firepower# show cap in
```

12 packets captured

```
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
```

12 packets shown

```
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
```

12 packets shown

Captura de saída:

```
firepower# show cap in2
```

12 packets captured

```
1: 00:08:28.073543 172.16.11.2 > 172.16.11.254 icmp: echo request
2: 00:08:28.074764 172.16.11.254 > 172.16.11.2 icmp: echo reply
3: 00:08:29.150810 172.16.11.2 > 172.16.11.254 icmp: echo request
4: 00:08:29.151954 172.16.11.254 > 172.16.11.2 icmp: echo reply
5: 00:08:30.217640 172.16.11.2 > 172.16.11.254 icmp: echo request
```

```
6: 00:08:30.218799 172.16.11.254 > 172.16.11.2 icmp: echo reply
7: 00:08:31.247667 172.16.11.2 > 172.16.11.254 icmp: echo request
8: 00:08:31.248888 172.16.11.254 > 172.16.11.2 icmp: echo reply
9: 00:08:32.308913 172.16.11.2 > 172.16.11.254 icmp: echo request
10: 00:08:32.310012 172.16.11.254 > 172.16.11.2 icmp: echo reply
11: 00:08:33.386576 172.16.11.2 > 172.16.11.254 icmp: echo request
12: 00:08:33.387888 172.16.11.254 > 172.16.11.2 icmp: echo reply
12 packets captured
```



Caution: Certifique-se de configurar as capturas com endereços IP de origem e destino, já que as capturas podem aumentar consideravelmente o desempenho na caixa.



Tip: Se o ping não funcionar, solucione os problemas da conexão direta com o gateway padrão, verifique a tabela ARP ou entre em contato com o TAC da Cisco.

Para verificar se o PBR funciona, você pode usar a ferramenta packet tracer para garantir que o tráfego do aplicativo seja roteado com o PBR.

```
firepower# packet-tracer input inside tcp 172.16.35.2 54352 'PUBLIC-IP-ADDRESS-FOR-WEBEX' $
---
[Output omitted]
---
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set ip next-hop 172.16.1.254
Additional Information:
Matched route-map FMC_GENERATED_PBR_1694885402369, sequence 5, permit
Found next-hop 172.16.1.254 using egress ifc ISP-1
---
[Output omitted]
---
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: ISP-1
output-status: up
output-line-status: up
Action: allow
```



Note: Para aprender sobre os endereços IP do aplicativo para o serviço de rede configurado em grupos de objetos, use o comando `show object-group network-service detail`.

Informações Relacionadas

Documentos adicionais relacionados ao PBR com monitoração de caminho HTTP podem ser encontrados aqui:

- [Configuração de roteamento com base em políticas no Guia de configuração de dispositivos do Secure Firewall Management Center](#)
- [Path Monitoring on Policy-Based Routing Configuration on Secure Firewall Management Center Device Configuration Guide \(Monitoramento de caminho em configuração de roteamento baseada em política no Guia de configuração de dispositivo do Secure Firewall Management Center\)](#)
- [Configurar Política de Roteamento Baseada em Política](#)
- [Exemplo de configuração para roteamento baseado em política](#)
- [Configurar exemplo para monitoramento de caminho PBR](#)
- [Adicionar Painel de Monitoramento de Caminho](#)
- [Configuração de Configurações de Plataforma DNS no Guia de Configuração de Dispositivo do Secure Firewall Management Center](#)
- [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.