

Configurar BGP sobre VPN baseada em rota no FTD Gerenciado pelo FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações em VPN](#)

[Configurações no BGP](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve a configuração de BGP sobre VPN site a site baseado em rota em FTDv gerenciado pelo FirePower Device Manager (FDM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendimento básico de VPN
- Configurações de BGP em FTDv
- Experiência com o FDM

Componentes Utilizados

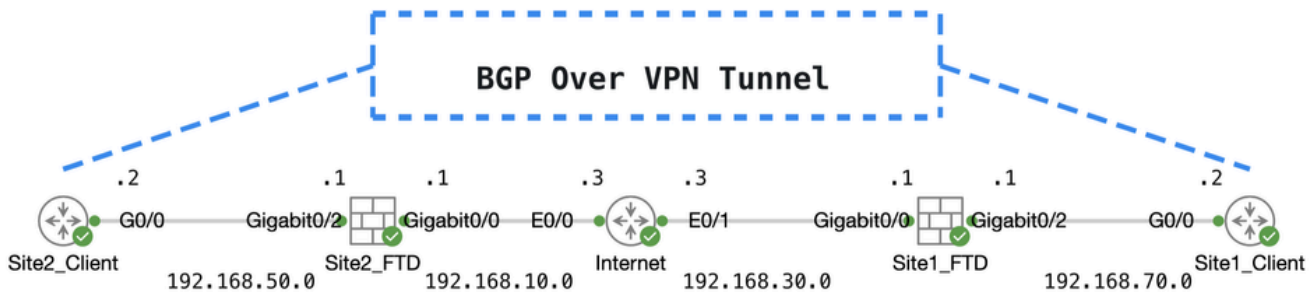
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco FTDv versão 7.4.2
- Cisco FDM versão 7.4.2

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.

Configurar

Diagrama de Rede



Topo

Configurações em VPN

Etapa 1. Verifique se a interconectividade IP entre os nós está pronta e estável. A Smart License no FDM foi registrada com êxito na Smart Account.

Etapa 2. O gateway do Site1 Client é configurado com o endereço IP interno do Site1 FTD (192.168.70.1). O gateway do cliente Site2 é configurado com o endereço IP interno do FTD Site2 (192.168.50.1). Além disso, verifique se a rota padrão em ambos os FTDs está configurada corretamente após a inicialização do FDM.

Faça login na GUI de cada FDM. Navegue até `Device > Routing`. Clique em `.View Configuration` Clique na `Static Routing` guia para verificar a rota estática padrão.

The screenshot shows the Firewall Device Manager GUI for device ftdv742. The 'Routing' section is active, and the 'Static Routing' tab is selected. A table displays the static routing configuration:

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.30.3		1	

Site1_FTD_Gateway

Device Summary
Routing

Add Multiple Virtual Routers

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

1 route

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.10.3		1	

Site2_FTD_Gateway

Etapa 3. Configure a VPN site a site baseada em rota. Neste exemplo, primeiro configure o FTD Site1.

Etapa 3.1. Faça login na GUI do FDM do FTD Site1. Crie um novo objeto de rede para a rede interna do Site1 FTD. Navegue até **Objects > Networks** e clique no botão +.

Object Types

Networks

Ports

Network Objects and Groups

9 objects

Filter

Preset filters: System defined, User defined

Criar_Objeto_De_Rede

Etapa 3.2. Forneça as informações necessárias. Clique no OK botão.

- Nome: inside_192.168.70.0
- Tipo: Rede
- Rede: 192.168.70.0/24

Add Network Object



Name

inside_192.168.70.0

Description

Type



Network



Host



FQDN



Range

Network

192.168.70.0/24

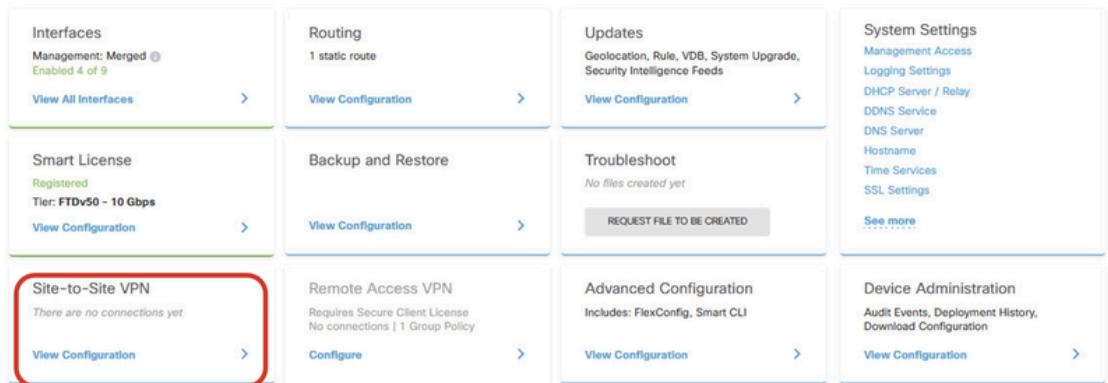
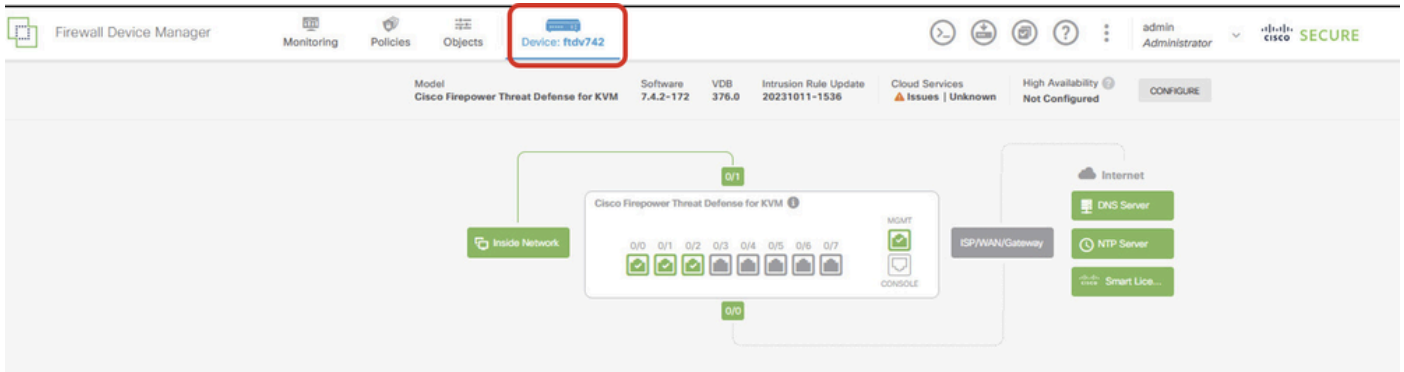
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

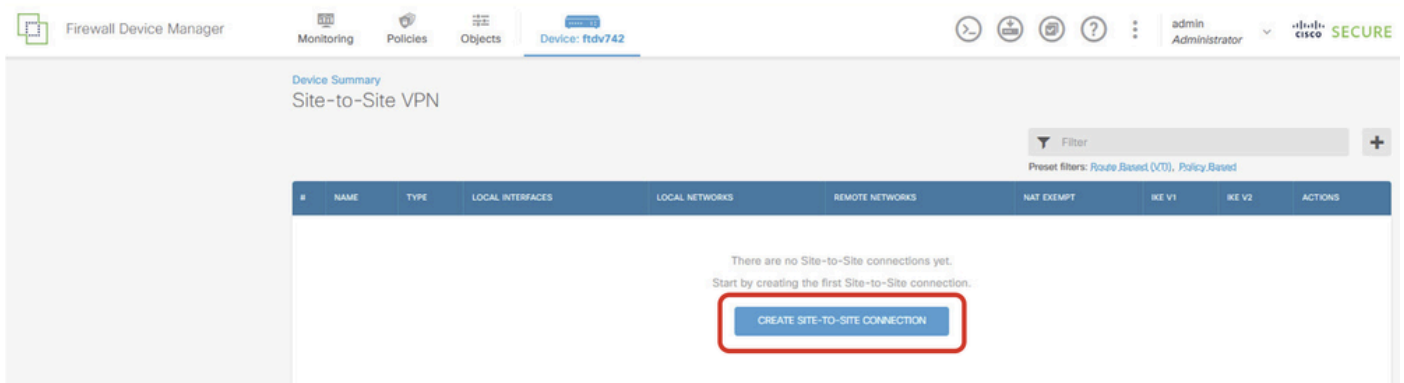
Site1_Inside_Network

Etapa 3.3. Navegue até **Device > Site-to-Site VPN** . Clique em **.View Configuration**



Exibir VPN site a site

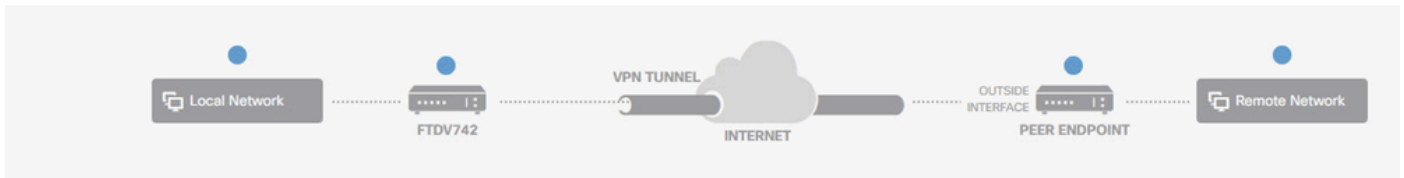
Etapa 3.4. Comece a criar uma nova VPN site a site. Clique em **.CREATE SITE-TO-SITE CONNECTION**



Create_Site-to-Site_Connection

Etapa 3.5. Forneça as informações necessárias.

- Nome do perfil de conexão: Demo_S2S
- Tipo: baseado em rota (VTI)
- Local VPN Access Interface: clique na lista suspensa e, em seguida, clique em **Create new Virtual Tunnel Interface** .



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: Demo_S2S

Type: Route Based (VTI) | Policy Based

Sites Configuration

LOCAL SITE	REMOTE SITE
Local VPN Access Interface Please select Filter Nothing found Create new Virtual Tunnel Interface	Remote IP Address

NEXT

Create_VTI_in_VPN_Wizard

Etapa 3.6. Forneça as informações necessárias para criar um novo VTI. Clique na tecla OK.

- Nome: demovti
- ID do túnel: 1
- Origem do Túnel: externo (GigabitEthernet0/0)
- Endereço IP e máscara de sub-rede: 169.254.10.1/24
- Status: clique no controle deslizante para a posição Habilitado

Name Status

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

Description

Tunnel ID 0 - 10413

Tunnel Source

IP Address and Subnet Mask /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

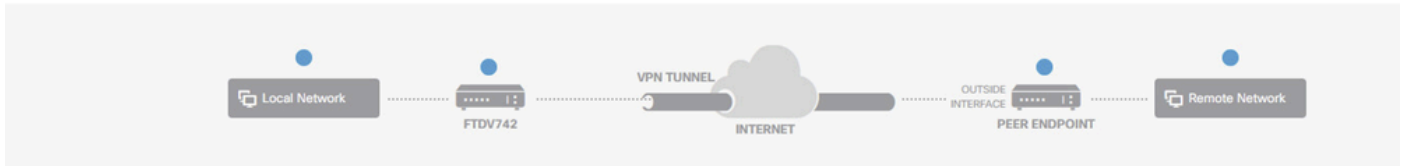
Create_VTI_Details

Etapa 3.7. Continue a fornecer as informações necessárias. Clique no botão NEXT .

- Local VPN Access Interface: demovti (criada na Etapa 3.6.)
- Endereço IP remoto: 192.168.10.1

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: Demo_S2S

Type: Route Based (VTI) Policy Based

Sites Configuration

LOCAL SITE	REMOTE SITE
Local VPN Access Interface demovti (Tunnel1)	Remote IP Address 192.168.10.1

CANCEL NEXT

VPN_Wizard_Endpoints_Step1

Etapa 3.8. Navegue até Política IKE. Clique no botão EDIT.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742

New Site-to-site VPN 1 Endpoints 2 Configuration 3 Summary

The diagram is identical to the one in Step 1, showing the VPN configuration between the local and remote networks.

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

None selected !

Edit_IKE_Policy

Etapa 3.9. Para a política IKE, você pode usar uma política predefinida ou criar uma nova clicando em Criar nova política IKE.

Neste exemplo, alterne uma política IKE existente AES-SHA-SHA e crie uma nova para fins de

demonstração. Clique no botão OK para salvar.

- Nome: AES256_DH14_SHA256_SHA256
- Criptografia: AES, AES256
- Grupo DH: 14
- Hash de integridade: SHA, SHA256
- Hash PRF: SHA, SHA256
- Vida útil: 86400 (padrão)

The image shows two screenshots of a network configuration interface. The left screenshot displays a list of IKE policies with a filter bar. The 'AES-SHA-SHA' policy is selected and highlighted with a red box. Below the list is a 'Create New IKE Policy' button and an 'OK' button. A red arrow points from the 'Create New IKE Policy' button to the right screenshot. The right screenshot shows the 'Add IKE v2 Policy' configuration dialog. The 'Priority' is set to 1, and the 'Name' is 'AES256_DH14_SHA256_SHA256'. The 'State' is turned on. The 'Encryption' section is set to 'AES' and 'AES256'. The 'Diffie-Hellman Group' is set to '14'. The 'Integrity Hash' is set to 'SHA' and 'SHA256'. The 'Pseudo Random Function (PRF) Hash' is set to 'SHA' and 'SHA256'. The 'Lifetime (seconds)' is set to '86400'. At the bottom, there are 'CANCEL' and 'OK' buttons.

Add_New_IKE_Policy

Filter

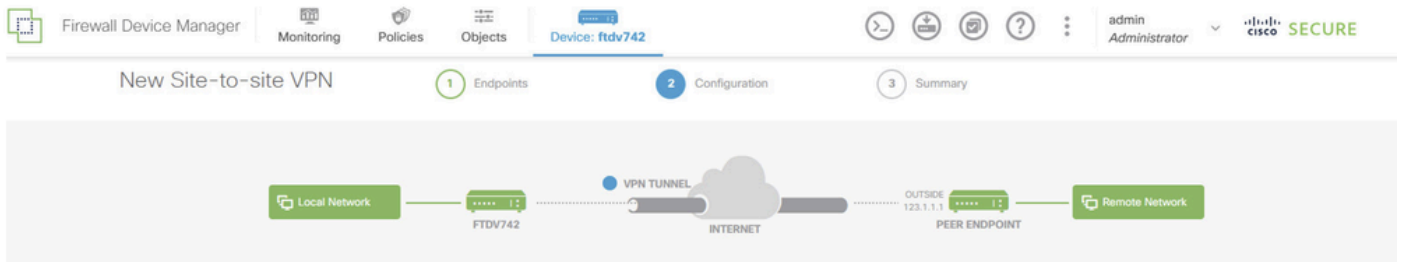
<input type="checkbox"/>	AES-GCM-NULL-SHA	i
<input checked="" type="checkbox"/>	AES-SHA-SHA	i
<input type="checkbox"/>	DES-SHA-SHA	i
<input checked="" type="checkbox"/>	AES256_DH14_SHA256_SHA256	i

Create New IKE Policy

OK

Enable_New_IKE_Policy

Etapa 3.10. Navegue até a Proposta IPsec. Clique no botão EDIT.



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

1 IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 IKE VERSION 1

IKE Policy

Globally applied

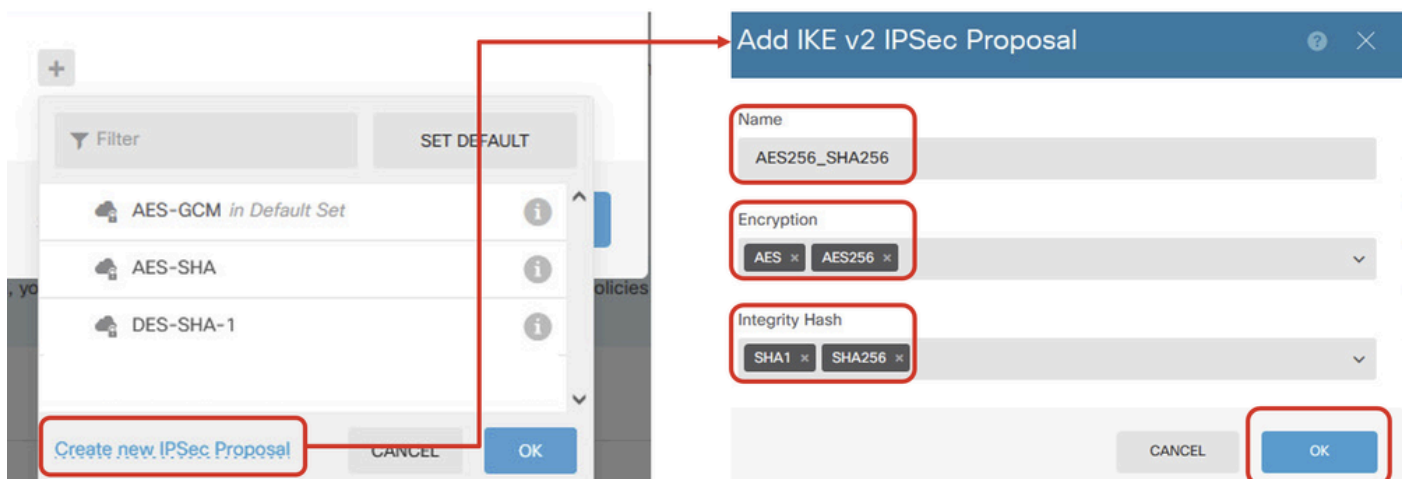
IPSec Proposal

None selected !

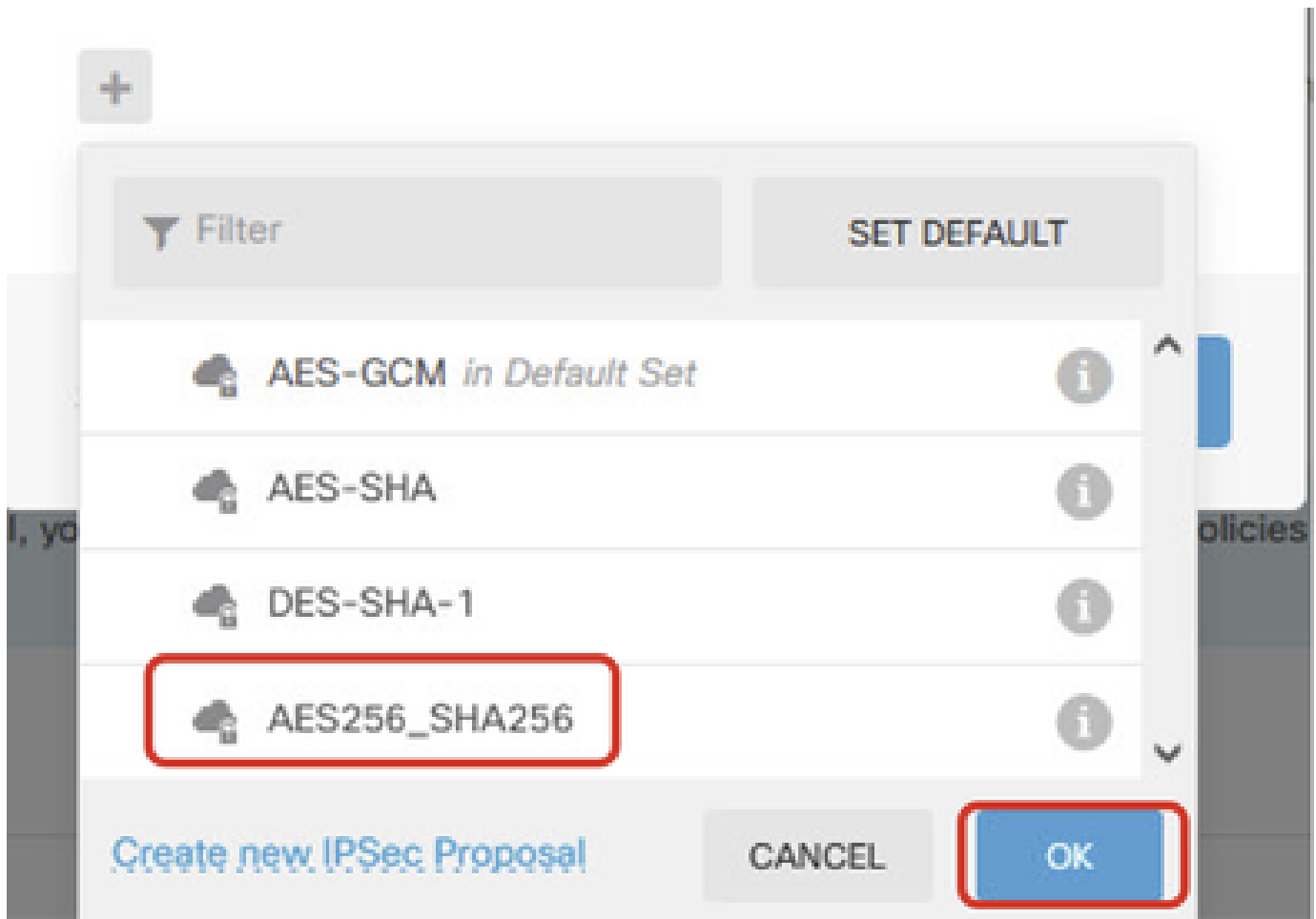
Edit_IKE_Proposal

Etapa 3.11. Para a proposta IPsec, você pode usar uma predefinida ou pode criar uma nova clicando em Criar nova proposta IPsec. Neste exemplo, crie um novo para fins de demonstração. Forneça as informações necessárias. Clique no botão OK para salvar.

- Nome: AES256_SHA256
- Criptografia: AES, AES256
- Hash de integridade: SHA1, SHA256



Add_New_IPSec_Proposal



Enable_New_IPSec_Proposal

Etapa 3.12. Configure a chave pré-compartilhada. Clique no botão NEXT.

Anote essa chave pré-compartilhada e configure-a no Site2 FTD mais tarde.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURI

FTDV742 | INTERNET | PEER ENDPOINT

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 | IKE VERSION 1

IKE Policy
Globally applied

IPSec Proposal
Custom set selected

Authentication Type
 Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

Configure_Pre_Shared_Key

Etapa 3.13. Reveja a configuração da VPN. Se algo precisar ser modificado, clique no botão BACK. Se tudo estiver bem, clique no botão FINISH.

Demo_S2S Connection Profile

i Peer endpoint needs to be configured according to specified below configuration.

VPN Access Interface

demovti (169.254.10.1)



Peer IP Address

192.168.10.1

IKE V2

IKE Policy

aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-sha,sha256-sha,sha256-14

IPSec Proposal

aes,aes-256-sha-1,sha-256

Authentication Type

Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration

28800 seconds

Lifetime Size

4608000 kilobytes

ADDITIONAL OPTIONS

Diffie-Hellman

Null (not selected)

i Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

VPN_Wizard_Complete

Etapa 3.14. Crie uma regra de Controle de Acesso para permitir que o tráfego passe pelo FTD. Neste exemplo, permita todos para fins de demonstração. Modifique sua política com base em suas necessidades reais.

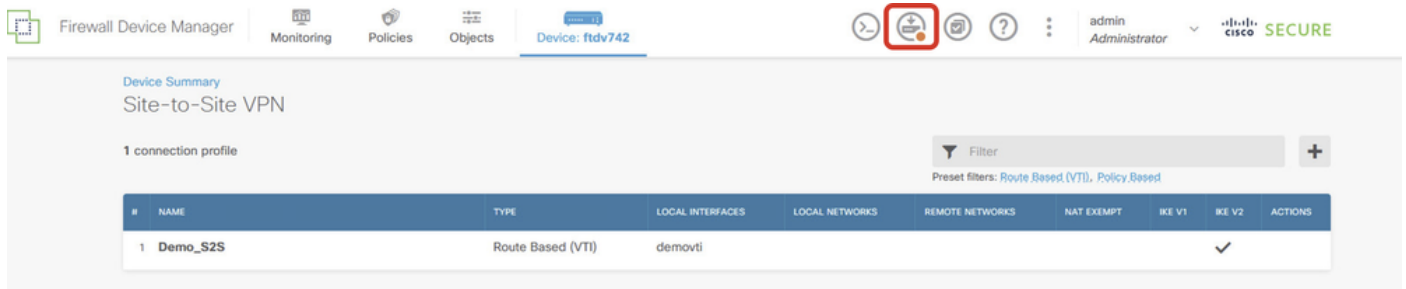
The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes "Firewall Device Manager", "Monitoring", "Policies", "Objects", and "Device: ftdv742". The breadcrumb trail is: "Security Policies" > "Access Control". A single rule is listed:

#	NAME	ACTION	SOURCE ZONES	SOURCE NETWORKS	SOURCE PORTS	DESTINATION ZONES	DESTINATION NETWORKS	DESTINATION PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	

At the bottom, the "Default Action" is set to "Access Control" with a "Block" button.

Etapa 3.15. (Opcional) Configure a regra de isenção de NAT para o tráfego do cliente no FTD se o NAT dinâmico estiver configurado para o cliente para acessar a Internet. Neste exemplo, não há necessidade de configurar uma regra isenta de NAT porque nenhum NAT dinâmico é configurado em cada FTD.

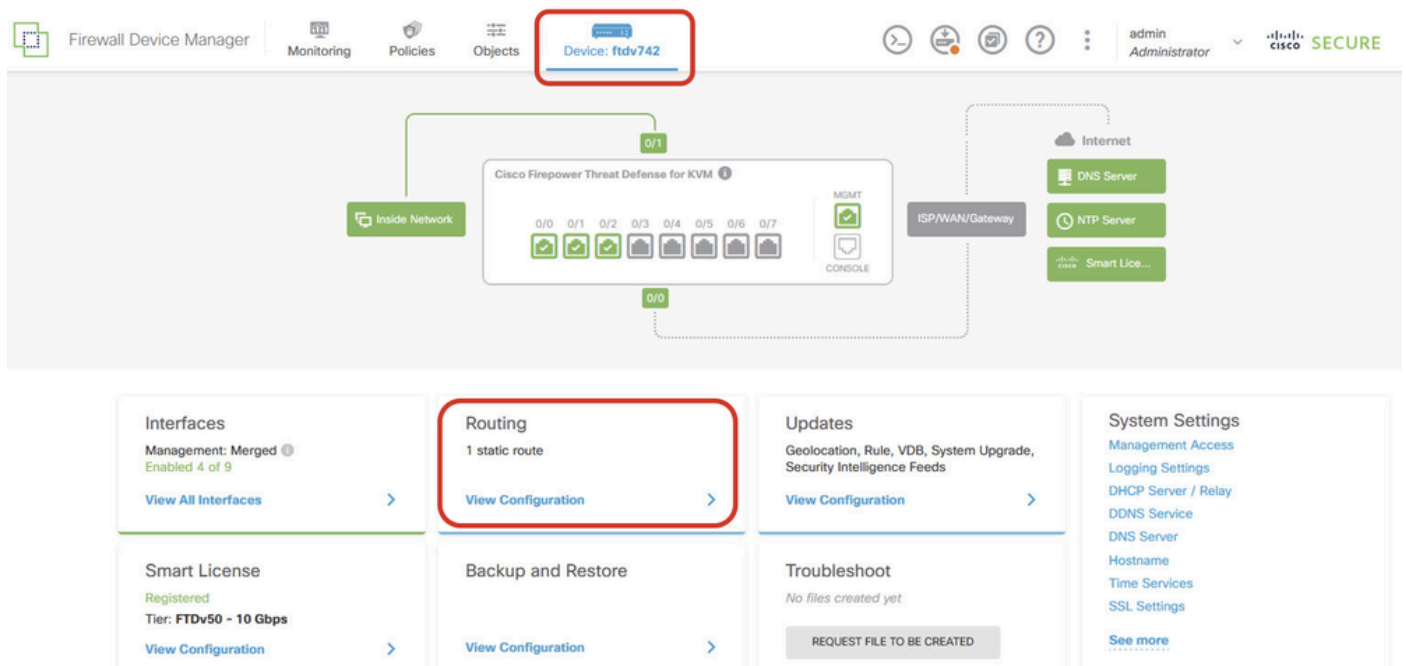
Etapa 3.16. Implante as alterações de configuração.



Deploy_VPN_Configuration

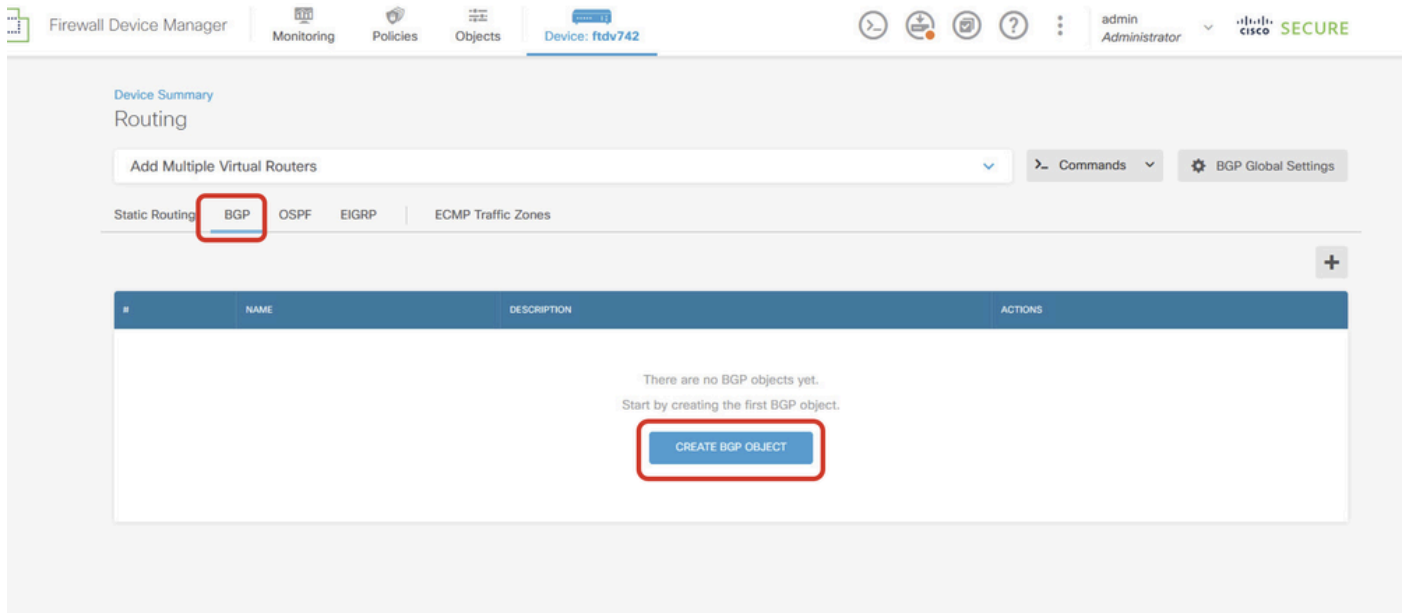
Configurações no BGP

Etapa 4. Navegue até Device > Routing. Clique em View Configuration.



View_Routing_Configuration

Etapa 5. Clique na guia BGP e clique em CREATE BGP OBJECT.



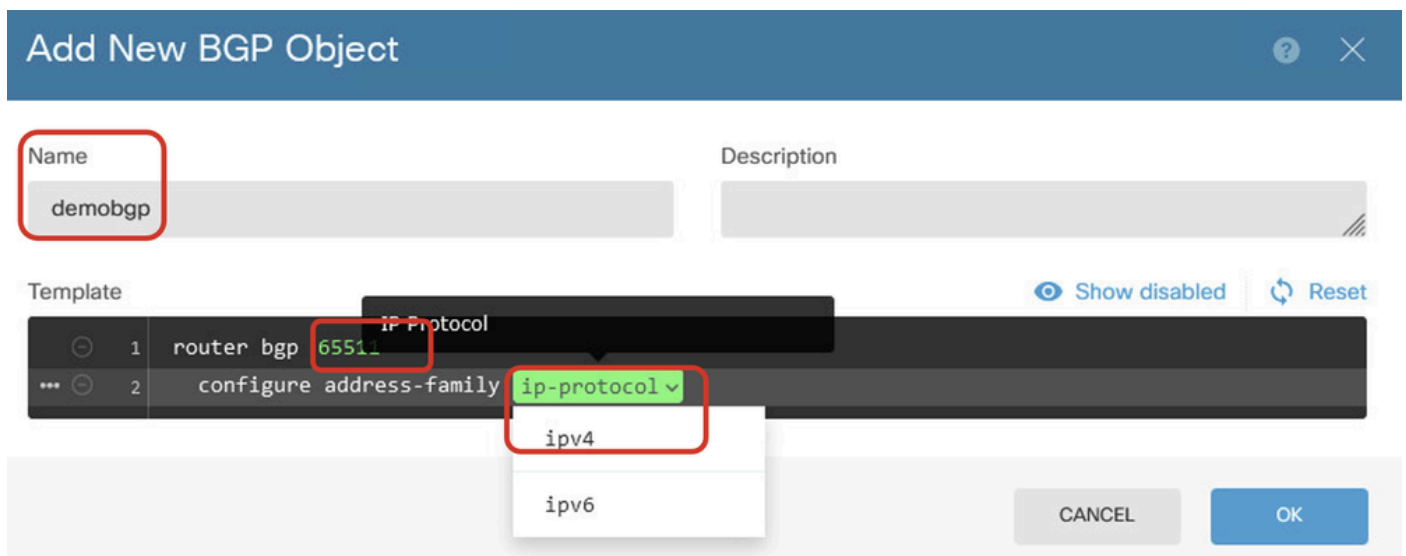
Create_BGP_Object

Etapa 6. Forneça o nome do objeto. Navegue até Template e configure. Clique no botão OK para salvar.

Nome: demobgp

Linha 1: Configurar o número AS. Clique em as-number. Número AS local de entrada manual. Neste exemplo, o número AS 65511 para Site1 FTD.

Linha 2: Configurar o protocolo IP. Clique em ip-protocol. Selecione ipv4.



Create_BGP_Object_ASNumber_Protocol

Linha 4: Defina mais configurações. Clique em configurações, escolha geral e clique em Mostrar desabilitados.

Add New BGP Object

Name: demobgp

Description:

Template: Show disabled Reset

```
1 router bgp 65511
2 configure address-family ipv4
3 address-family ipv4 unicast
4 configure address-family ipv4 settings
```

Address Family IPv4 Settings

- general
- advanced

CANCEL OK

Create_BGP_Object_AddressSetting

Linha 6: clique no ícone + para habilitar a linha para configurar a rede BGP. Clique em network-object. Você pode ver os objetos disponíveis existentes e escolher um. Neste exemplo, escolha o nome do objeto inside_192.168.70.0 (criado na Etapa 3.2.).

Add New BGP Object

Name: demobgp

Description:

Template: Hide disabled Reset

```
1 router bgp 65511
2 configure address-family ipv4
3 address-family ipv4 unicast
4 configure address-family ipv4 general
5 distance bgp 20 200 200
6 network network-object
7 network network-object route-map map-tag
8 bgp inject-map inject-map exist-map exist-map options
9 configure aggregate-address map-type
10 configure filter-rules direction
11 configure neighbor neighbor-address remote-as as-number config-options
12 configure ipv4 redistribution protocol identifier none
13 bgp router-id router-id
```

Create_BGP_Object_Add_Network

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4     configure address-family ipv4 general
5     distance bgp 20 200 200
6   network
7   network
8   bgp inje
9   configur
10  configur
11  configur
12  configur
13  bgp router-i
```

IPV4 Network address

- OutsidelPv4DefaultRoute Network
- OutsidelPv4Gateway Host
- any-ipv4 Network
- any-ipv6 Network
- inside_192.168.70.0 Network

inside_192.168.70.0

Create_BGP_Object_Add_Network2

Linha 11: clique no ícone + para permitir que a linha configure as informações relacionadas ao vizinho BGP. Clique em neighbor-address e insira manualmente o endereço do vizinho BGP do peer. Neste exemplo, é 169.254.10.2 (endereço IP VTI do FTD do Site2). Clique em as-number e insira manualmente o número AS do peer. Neste exemplo, 65510 é para FTD Site2. Clique em config-options e escolha properties.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 config-options
12        configure ipv4 redistribution protocol identifier
13        bgp router-id router-id
```

Select Configuration Option

properties

Create_BGP_Object_NeighborSetting

Linha 14: clique no ícone + para permitir que a linha configure algumas propriedades do vizinho. Clique em ativate-options e escolha properties.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 properties
12          neighbor 169.254.10.2 remote-as 65510
13          configure neighbor 169.254.10.2 activate activate-options
14            activate-options
15            properties
16        bgp router-id router-id
```

Create_BGP_Object_NeighborSetting_Properties

Linha 13: clique no ícone + para permitir que a linha mostre opções avançadas. Clique em configurações e escolha avançado.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65511 properties
12        neighbor 169.254.10.2 remote-as 65511
13        configure neighbor 169.254.10.2 remote-as 65511 settings
14        configure neighbor 169.254.10.2 activate
15        neighbor 169.254.10.2 activate
16        configure neighbor 169.254.10.2 activate
17        configure ipv4 redistribution protocol identifier
18        bgp router-id router-id
```

Select Neighbor Settings

settings

general

advanced

migration

ha-mode

CANCEL

OK

Create_BGP_Object_NeighborSetting_Properties_Advanced

Linha 18: clique em options e escolha disable para desabilitar a descoberta de MTU de caminho.

Add New BGP Object



Name

Description

demobgp

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 properties
12        neighbor 169.254.10.2 remote-as 65510
13        configure neighbor 169.254.10.2 remote-as advanced
14        neighbor 169.254.10.2 password secret
15        configure neighbor 169.254.10.2 hops options
16        neighbor 169.254.10.2 version version-number
17        neighbor 169.254.10.2 transport connection-mode options
18        neighbor 169.254.10.2 transport path-mtu-discovery options
19        configure neighbor 169.254.10.2 activate properties
20        neighbor 169.254.10.2 activate
21        configure neighbor 169.254.10.2 activate settings
22        configure ipv4 redistribution protocol identifier none
23        bgp router-id router-id
```

Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

Linha 14, 15, 16, 17: clique no botão - para desabilitar as linhas. Em seguida, clique no botão OK para salvar o objeto BGP.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6       network inside_192.168.70.0
7       network network-object route-map map-tag
8     bgp inject-map inject-map exist-map exist-map options
9     configure aggregate-address map-type
10    configure filter-rules direction
11    configure neighbor 169.254.10.2 remote-as 65510 properties
12    neighbor 169.254.10.2 remote-as 65510
13    configure neighbor 169.254.10.2 remote-as advanced
14    neighbor 169.254.10.2 password secret
15    configure neighbor 169.254.10.2 hops options
16    neighbor 169.254.10.2 version version-number
17    neighbor 169.254.10.2 transport connection-mode options
18    neighbor 169.254.10.2 transport path-mtu-discovery disable
19    configure neighbor 169.254.10.2 activate properties
20    neighbor 169.254.10.2 activate
21    configure neighbor 169.254.10.2 activate settings
22    configure ipv4 redistribution protocol identifier none
23  bgp router-id router-id
```

CANCEL

OK

Create_BGP_Object_DisableLines

Esta é uma visão geral da configuração de BGP neste exemplo. Você pode definir as outras configurações de BGP com base nas suas necessidades reais.

Name	Description
demobgp	

Template

Hide disabled

Reset

```

1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 properties
12        neighbor 169.254.10.2 remote-as 65510
13        configure neighbor 169.254.10.2 remote-as advanced
14        neighbor 169.254.10.2 password secret
15        configure neighbor 169.254.10.2 hops options
16        neighbor 169.254.10.2 version version-number
17        neighbor 169.254.10.2 transport connection-mode options
18        neighbor 169.254.10.2 transport path-mtu-discovery disable
19        configure neighbor 169.254.10.2 activate properties
20        neighbor 169.254.10.2 activate
21        configure neighbor 169.254.10.2 activate settings
22        configure ipv4 redistribution protocol identifier none
23        bgp router-id router-id

```

CANCEL

OK

Create_BGP_Object_Final_Overview

Passo 7. Implante as alterações de configuração do BGP.

The screenshot shows the Cisco Firewall Device Manager interface. The top navigation bar includes 'Firewall Device Manager', 'Monitoring', 'Policies', 'Objects', and 'Device: ftdv742'. The main content area is titled 'Device Summary' and 'Routing'. There is a search bar for 'Add Multiple Virtual Routers' and a 'Commands' dropdown. Below this, there are tabs for 'Static Routing', 'BGP', 'OSPF', 'EIGRP', and 'ECMP Traffic Zones'. The 'BGP' tab is active, showing '1 object'. A table with columns '#', 'NAME', 'DESCRIPTION', and 'ACTIONS' contains one entry: '1 demobgp'.

Deploy_BGP_Configuration

Etapa 8. Agora, a configuração do FTD do Site1 foi concluída.

Para configurar a VPN FTD e o BGP do Site2, repita a Etapa 3 a Etapa 7 com os parâmetros correspondentes do FTD do Site2.

Visão geral da configuração do FTD do Site1 e do FTD do Site2 na CLI.

FTD do Site1	FTD do Site2
<pre> NGFW versão 7.4.2 interface GigabitEthernet0/0 nameif externo manual cts propagate sgt preserve-untag policy static sgt disabled trusted nível de segurança 0 endereço ip 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside nível de segurança 0 endereço ip 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti endereço ip 169.254.10.1 255.255.255.0 tunnel source interface outside tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile e4084d322d rede de objetos ForalPv4Gateway host 192.168.30.3 rede de objeto dentro_192.168.70.0 sub-rede 192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: </pre>	<pre> NGFW versão 7.4.2 interface GigabitEthernet0/0 nameif externo manual cts propagate sgt preserve-untag policy static sgt disabled trusted nível de segurança 0 endereço ip 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside nível de segurança 0 endereço ip 192.168.50.1 255.255.255.0 interface Tunnel1 nameif demovti25 endereço ip 169.254.10.2 255.255.255.0 tunnel source interface outside tunnel destination 192.168.30.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile e4084d322d rede de objetos ForalPv4Gateway host 192.168.10.3 rede de objeto dentro_192.168.50.0 sub-rede 192.168.50.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow </pre>

<p>L5 RULE: Demo_allow</p> <p>access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458</p> <p>event-log</p> <p>access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy</p> <p>access-list NGFW_ONBOX_ACL remark rule-id 1: L5</p> <p>RULE: DefaultActionRule</p> <p>access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1</p> <p>router bgp 65511</p> <p>bgp log-neighbor-changes</p> <p>bgp router-id vrf autoassign</p> <p>address-family ipv4 unicast</p> <p>neighbor 169.254.10.2 remote-as 65510</p> <p>neighbor 169.254.10.2 transport path-mtu-discovery disable</p> <p>neighbor 169.254.10.2 ativate</p> <p>rede 192.168.70.0</p> <p>no autosummary</p> <p>sem sincronização</p> <p>exit-address-family</p> <p>rota externa 0.0.0.0 0.0.0.0 192.168.30.3 1</p> <p>crypto ipsec ikev2 ipsec-proposal AES256_SHA256</p> <p>protocol esp encryption aes-256 aes</p> <p>protocol esp integrity sha-256 sha-1</p> <p>crypto ipsec profile ipsec_profile e4084d322d</p> <p>set ikev2 ipsec-proposal AES256_SHA256</p> <p>set security-association lifetime kilobytes 4608000</p> <p>set security-association lifetime seconds 28800</p> <p>crypto ipsec security-association pmtu-aging infinito</p> <p>crypto ikev2 policy 1</p> <p>encryption aes-256 aes</p> <p>integridade sha256 sha</p> <p>grupo 14</p> <p>prf sha256 sha</p> <p>segundos de vida útil 86400</p> <p>crypto ikev2 policy 20</p> <p>encryption aes-256 aes-192 aes</p> <p>integridade sha512 sha384 sha256 sha</p> <p>grupo 21 20 16 15 14</p>	<p>access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458</p> <p>event-log</p> <p>access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy</p> <p>access-list NGFW_ONBOX_ACL remark rule-id 1: L5</p> <p>RULE: DefaultActionRule</p> <p>access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1</p> <p>router bgp 65510</p> <p>bgp log-neighbor-changes</p> <p>bgp router-id vrf autoassign</p> <p>address-family ipv4 unicast</p> <p>neighbor 169.254.10.1 remote-as 65511</p> <p>neighbor 169.254.10.1 transport path-mtu-discovery disable</p> <p>neighbor 169.254.10.1 ativate</p> <p>rede 192.168.50.0</p> <p>no autosummary</p> <p>sem sincronização</p> <p>exit-address-family</p> <p>rota externa 0.0.0.0 0.0.0.0 192.168.10.3 1</p> <p>crypto ipsec ikev2 ipsec-proposal AES256_SHA256</p> <p>protocol esp encryption aes-256 aes</p> <p>protocol esp integrity sha-256 sha-1</p> <p>crypto ipsec profile ipsec_profile e4084d322d</p> <p>set ikev2 ipsec-proposal AES256_SHA256</p> <p>set security-association lifetime kilobytes 4608000</p> <p>set security-association lifetime seconds 28800</p> <p>crypto ipsec security-association pmtu-aging infinito</p> <p>crypto ikev2 policy 1</p> <p>encryption aes-256 aes</p> <p>integridade sha256 sha</p> <p>grupo 14</p> <p>prf sha256 sha</p> <p>segundos de vida útil 86400</p> <p>crypto ikev2 policy 20</p> <p>encryption aes-256 aes-192 aes</p> <p>integridade sha512 sha384 sha256 sha</p> <p>grupo 21 20 16 15 14</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<pre>prf sha512 sha384 sha256 sha segundos de vida útil 86400 crypto ikev2 enable outside política de grupo s2sGP 192.168.10.1 internal política de grupo s2sGP atributos de 192.168.10.1 vpn-tunnel-protocol ikev2 tunnel-group 192.168.10.1 type ipsec-l2l tunnel-group 192.168.10.1 general-attributes default-group-policy s2sGP 192.168.10.1 tunnel-group 192.168.10.1 ipsec-attributes ***** de chave pré-compartilhada de autenticação remota ikev2 ikev2 local-authentication pre-shared-key *****</pre>	<pre>prf sha512 sha384 sha256 sha segundos de vida útil 86400 crypto ikev2 enable outside política de grupo s2sGP 192.168.30.1 internal política de grupo s2sGP atributos de 192.168.30.1 vpn-tunnel-protocol ikev2 tunnel-group 192.168.30.1 type ipsec-l2l tunnel-group 192.168.30.1 general-attributes default-group-policy s2sGP 192.168.30.1 tunnel-group 192.168.30.1 ipsec-attributes ***** de chave pré-compartilhada de autenticação remota ikev2 ikev2 local-authentication pre-shared-key *****</pre>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Navegue para o CLI de cada FTD através do console ou do SSH para verificar o status da VPN da fase 1 e da fase 2 através dos comandos `show crypto ikev2 sa` e `show crypto ipsec sa`.

FTD do Site1	FTD do Site2
<pre>ftdv742# show crypto ikev2 sa SAs IKEv2: Session-id:134, Status:UP-ATIVE, contagem IKE:1, contagem FILHO:1 Função de Status FVRF/IVRF Remoto Local de Tunnel-id 563984431 192.168.30.1/500 192.168.10.1/500 RESPONDENTE PRONTO Global/Global Codificação: AES-CBC, tamanho da chave: 256, Hash: SHA256, DH Grp: 14, Sinal de autenticação: PSK, Verificação de autenticação: PSK Vida/Tempo Ativo: 86400/5.145 s</pre>	<pre>ftdv742# show crypto ikev2 sa SAs IKEv2: Session-id:13, Status:UP-ATIVE, contagem de IKE:1, contagem de FILHO:1 Função de Status FVRF/IVRF Remoto Local de Tunnel-id 339797985 192.168.10.1/500 192.168.30.1/500 INICIADOR PRONTO global/global Codificação: AES-CBC, tamanho da chave: 256, Hash: SHA256, DH Grp: 14, Sinal de autenticação: PSK, Verificação de autenticação: PSK Vida Útil/Tempo Ativo: 86400/74099 s SA filho: seletor local 0.0.0.0/0 - 255.255.255.255/65535 seletor remoto 0.0.0.0/0 - 255.255.255.255/65535</pre>

<p>SA filho: seletor local 0.0.0.0/0 - 255.255.255.255/65535</p> <p>seletor remoto 0.0.0.0/0 - 255.255.255.255/65535</p> <p>ESP spi in/out: 0xf0c4239d/0xb7b5b38b</p>	<p>Entrada/saída ESP spi: 0xb7b5b38b/0xf0c4239d</p>
<p>ftdv742# show crypto ipsec sa</p> <p>interface: demovti Tag de mapa de criptografia: __vti-crypto- map-Tunnel1-0-1, seq num: 65280, endereço local: 192.168.30.1</p> <p>VRF protegido (IVRF): global identificação local (endereço/máscara/porta/porta): (0.0.0.0/0.0.0.0/0/0) identificação remota (endereço/máscara/porta/porta): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.10.1</p> <p>#pkts encaps: 5720, #pkts criptografar: 5720, resumo #pkts: 5720 #pkts decaps: 5717, #pkts decrypt: 5717, #pkts verificar: 5717 #pkts compactado: 0, #pkts descompactado: 0 #pkts não compactado: 5720, falha #pkts compactação: 0, falha #pkts descompactação: 0 #pre-frag êxitos: 0, #pre-frag falhas: 0, #fragments criado: 0 #PMTUs enviados: 0, #PMTUs rcvd: 0, frgs #decapsulated que precisam de remontagem: 0 #TFC rcvd: 0, #TFC enviado: 0 #Valid Erros ICMP rcvd: 0, #Invalid Erros ICMP rcvd: 0 #send erros: 0, erros de #recv: 0</p> <p>ponto final de criptografia local: 192.168.30.1/500, ponto final de criptografia remoto: 192.168.10.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 Tempo restante de PMTU (s): 0, política DF: copy-df</p>	<p>ftdv742# show crypto ipsec sa</p> <p>interface: demovti25 Tag de mapa de criptografia: __vti-crypto- map-Tunnel1-0-1, número seq: 65280, endereço local: 192.168.10.1</p> <p>VRF protegido (IVRF): global identificação local (endereço/máscara/porta/porta): (0.0.0.0/0.0.0.0/0/0) identificação remota (endereço/máscara/porta/porta): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1</p> <p>#pkts encaps: 5721, #pkts criptografar: 5721, resumo #pkts: 5721 #pkts decaps: 5721, #pkts decryptografar: 5721, #pkts verificar: 5721 #pkts compactado: 0, #pkts descompactado: 0 #pkts não compactado: 5721, falha #pkts compactação: 0, falha #pkts descompactação: 0 #pre-frag êxitos: 0, #pre-frag falhas: 0, #fragments criado: 0 #PMTUs enviados: 0, #PMTUs rcvd: 0, frgs #decapsulated que precisam de remontagem: 0 #TFC rcvd: 0, #TFC enviado: 0 #Valid Erros ICMP rcvd: 0, #Invalid Erros ICMP rcvd: 0 #send erros: 0, erros de #recv: 0</p> <p>ponto final de criptografia local: 192.168.10.1/500, ponto final de criptografia remoto: 192.168.30.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 Tempo restante de PMTU (s): 0, política DF: copy-df</p>

<p>Validação de erro ICMP: desabilitada, pacotes TFC: desabilitada spi de saída atual: B7B5B38B spi de entrada atual : F0C4239D</p> <p>sas esp de entrada: spi: 0xF0C4239D (4039386013) Estado do SA: ativo transform: esp-aes-256 esp-sha-256-hmac sem compactação configurações em uso ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 SA timing: tempo de vida restante da chave (kB/s): (4285389/3722) Tamanho IV: 16 bytes suporte à detecção de repetição: Y Bitmap de antireprodução: 0xFFFFFFFF 0xFFFFFFFF sas esp de saída: spi: 0xB7B5B38B (3082138507) Estado do SA: ativo transform: esp-aes-256 esp-sha-256-hmac sem compactação configurações em uso ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 SA timing: tempo de vida restante da chave (kB/s): (4147149/3722) Tamanho IV: 16 bytes suporte à detecção de repetição: Y Bitmap de antireprodução: 0 x 00000000 0 x 00000001</p>	<p>Validação de erro ICMP: desabilitada, pacotes TFC: desabilitada spi de saída atual: F0C4239D spi de entrada atual : B7B5B38B</p> <p>sas esp de entrada: spi: 0xB7B5B38B (3082138507) Estado do SA: ativo transform: esp-aes-256 esp-sha-256-hmac sem compactação configurações em uso ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 SA timing: tempo de vida restante da chave (kB/s): (3962829/3626) Tamanho IV: 16 bytes suporte à detecção de repetição: Y Bitmap de antireprodução: 0xFFFFFFFF 0xFFFFFFFF sas esp de saída: spi: 0xF0C4239D (4039386013) Estado do SA: ativo transform: esp-aes-256 esp-sha-256-hmac sem compactação configurações em uso ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 SA timing: tempo de vida restante da chave (kB/s): (4101069/3626) Tamanho IV: 16 bytes suporte à detecção de repetição: Y Bitmap de antireprodução: 0 x 00000000 0 x 00000001</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Etapa 2. Navegue para o CLI de cada FTD através do console ou SSH para verificar o status do BGP usando os comandos show bgp neighbors e show route bgp.

FTD do Site1	FTD do Site2
<pre>ftdv742# show bgp neighbors</pre> <p>O vizinho BGP é 169.254.10.2, vrf single_vf, AS 65510 remoto, link externo BGP versão 4, ID do roteador remoto</p>	<pre>ftdv742# show bgp neighbors</pre> <p>O vizinho BGP é 169.254.10.1, vrf single_vf, AS 65511 remoto, link externo BGP versão 4, ID do roteador remoto</p>

192.168.50.1
Estado do BGP = Estabelecido, até 1d20h
Última leitura 00:00:25, última gravação
00:00:45, tempo de espera é 180, intervalo de
keepalive é de 60 segundos
Sessões de vizinhos:
1 ativo, não é compatível com várias sessões
(desabilitado)
Capacidades de vizinhos:
Atualização de rota: anunciada e recebida(nova)
Recurso ASN de quatro octetos: anunciado e
recebido
Unicast IPv4 da família de endereços:
anunciado e recebido
Capacidade de multissessão:
Estatísticas da mensagem:
InQ depth é 0
OutQ profundidade é 0

Enviado recebido
Aberturas: 1 1
Notificações: 0 0
Atualizações: 2 2
Keepalives: 2423 2427
Atualização de rota: 0 0
Total: 2426 2430
O tempo mínimo padrão entre execuções de
anúncio é de 30 segundos

Para a família de endereços: unicast IPv4
Sessão: 169.254.10.2
Tabela BGP versão 3, versão vizinha 3/0
Tamanho da fila de saída: 0
Índice 1
1 membro update-group
Enviado recebido
Atividade de prefixo: ---- ----
Prefixos Atuais: 1 1 (Consome 80 bytes)
Total de prefixos: 1 1
Retirada Implícita: 0 0
Retirada Explícita: 0 0
Usado como melhor caminho: n/d 1
Usado como multipath: n/d 0

Entrada de saída
Prefixos Negados da Diretiva Local: -----

192.168.70.1
Estado do BGP = Estabelecido, até 1d20h
Última leitura 00:00:11, última gravação
00:00:52, tempo de espera é 180, intervalo de
keepalive é 60 segundos
Sessões de vizinhos:
1 ativo, não é compatível com várias sessões
(desabilitado)
Capacidades de vizinhos:
Atualização de rota: anunciada e recebida(nova)
Recurso ASN de quatro octetos: anunciado e
recebido
Unicast IPv4 da família de endereços:
anunciado e recebido
Capacidade de multissessão:
Estatísticas da mensagem:
InQ depth é 0
OutQ profundidade é 0

Enviado recebido
Aberturas: 1 1
Notificações: 0 0
Atualizações: 2 2
Keepalives: 2424 2421
Atualização de rota: 0 0
Total: 2427 2424
O tempo mínimo padrão entre execuções de
anúncio é de 30 segundos

Para a família de endereços: unicast IPv4
Sessão: 169.254.10.1
Tabela BGP versão 9, versão vizinha 9/0
Tamanho da fila de saída: 0
Índice 4
4 update-group member
Enviado recebido
Atividade de prefixo: ---- ----
Prefixos Atuais: 1 1 (Consome 80 bytes)
Total de prefixos: 1 1
Retirada Implícita: 0 0
Retirada Explícita: 0 0
Usado como melhor caminho: n/d 1
Usado como multipath: n/d 0

Entrada de saída
Prefixos Negados da Diretiva Local: -----

<p>Melhor caminho deste par: 1 n/d Total: 10 Número de NLRIs na atualização enviada: máx. 1, mín. 0</p> <p>O rastreamento de endereço está ativado, o RIB tem uma rota para 169.254.10.2 Conexões estabelecidas 1; ignoradas 0 Última reinicialização nunca Transport(tcp) path-mtu-discovery is disabled Graceful-Restart está desabilitado</p>	<p>Melhor caminho deste par: 1 n/d Total: 10 Número de NLRIs na atualização enviada: máx. 1, mín. 0</p> <p>O rastreamento de endereço está ativado, o RIB tem uma rota para 169.254.10.1 Conexões estabelecidas 4; ignoradas 3 Última reinicialização em 1d21h, devido à oscilação da interface da sessão 1 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart está desabilitado</p>
<p>ftdv742# show route bgp</p> <p>Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, B - BGP D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2 E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, V - VPN i - IS-IS, su - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2 ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário o - ODR, P - rota estática baixada periodicamente, + - rota replicada SI - InterVRF estático, BI - BGP InterVRF O gateway de último recurso é 192.168.30.3 para a rede 0.0.0.0</p> <p>B 192.168.50.0 255.255.255.0 [20/0] via 169.254.10.2, 1d20h</p>	<p>ftdv742# show route bgp</p> <p>Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, B - BGP D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2 E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, V - VPN i - IS-IS, su - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2 ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário o - ODR, P - rota estática baixada periodicamente, + - rota replicada SI - InterVRF estático, BI - BGP InterVRF O gateway de último recurso é 192.168.10.3 para a rede 0.0.0.0</p> <p>B 192.168.70.0 255.255.255.0 [20/0] via 169.254.10.1, 1d20h</p>

Etapa 3. Cliente Site1 e Cliente Site2 efetuam ping entre si com êxito.

Cliente Site1:

```
Site1_Client#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/56/90 ms
```

Cliente Site2:

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Você pode usar esses comandos de depuração para solucionar problemas da seção VPN.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

Você pode usar esses comandos de depuração para solucionar problemas da seção BGP.

```
ftdv742# debug ip bgp ?
```

```
A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range     BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpn4       Address family
vpn6       Address family
vrf        VRF scope
<cr>
```


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.