Exemplo de Configuração do ASA 9.x EIGRP

Contents

Introduction

Este documento descreve como configurar o Cisco Adaptive Security Appliance (ASA) para aprender rotas através do Enhanced Interior Gateway Routing Protocol (EIGRP), que é suportado no software ASA versão 9.x e posterior, e executar a autenticação.

Prerequisites

Requirements

A Cisco exige que você atenda a estas condições antes de tentar esta configuração:

- O Cisco ASA deve executar a versão 9.x ou posterior.

- O EIGRP deve estar no modo de contexto único, porque não é suportado no modo multicontexto.

Componentes Utilizados

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

- Software Cisco ASA versão 9.2.1
- Cisco Adaptive Security Device Manager (ASDM) versão 7.2.1
- Cisco IOS® Router com versão 12.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Diretrizes e limitações

- Uma instância do EIGRP é suportada em modo único e por contexto em multimodo.
- Dois segmentos são criados por contexto por instância do EIGRP em multimodo e podem ser vistos com o processo show.
- O resumo automático está desativado por padrão.
- Uma relação de vizinhos não é estabelecida entre as unidades de cluster no modo de interface individual.
- As informações padrão em [<acl>] são usadas para filtrar o bit Exterior em rotas padrão de candidato de entrada.
- O padrão-information out [<acl>] é usado para filtrar o bit Exterior em rotas padrão de candidatos de saída.

EIGRP e failover

O código Cisco ASA versão 8.4.4.1 e posterior sincroniza rotas dinâmicas da unidade ATIVE para a unidade STANDBY. Além disso, a exclusão de rotas também é sincronizada com a unidade STANDBY. No entanto, o estado das adjacências de peer não está sincronizado; somente o dispositivo ATIVE mantém o estado vizinho e participa ativamente do roteamento dinâmico. Consulte as Perguntas frequentes do ASA: O que acontece após o failover se as rotas dinâmicas forem sincronizadas? para obter mais informações.

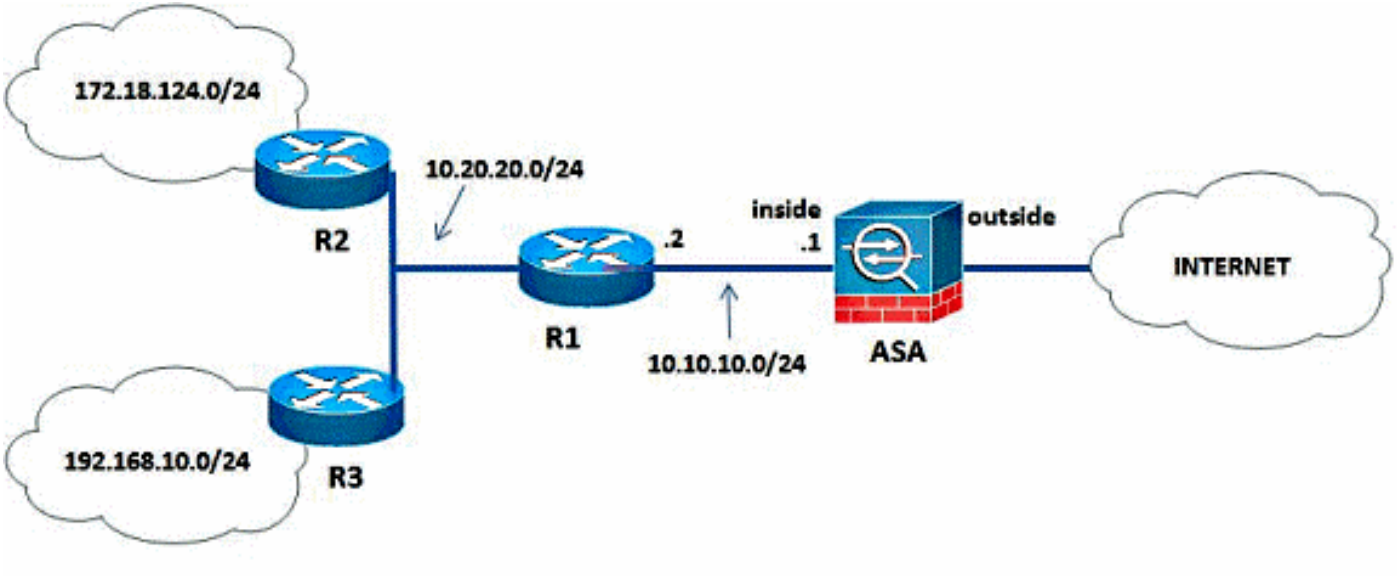
Configurar

Esta seção descreve como configurar os recursos abordados neste documento.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Na topologia de rede ilustrada, o endereço IP da interface interna do Cisco ASA é 10.10.10.1/24. O objetivo é configurar o EIGRP no Cisco ASA para aprender rotas para as redes internas (10.20.20.0/24, 172.18.124.0/24 e 192.168.10.0/24) dinamicamente através do roteador adjacente (R1). O R1 aprende as rotas para redes internas remotas através dos outros dois roteadores (R2 e R3).

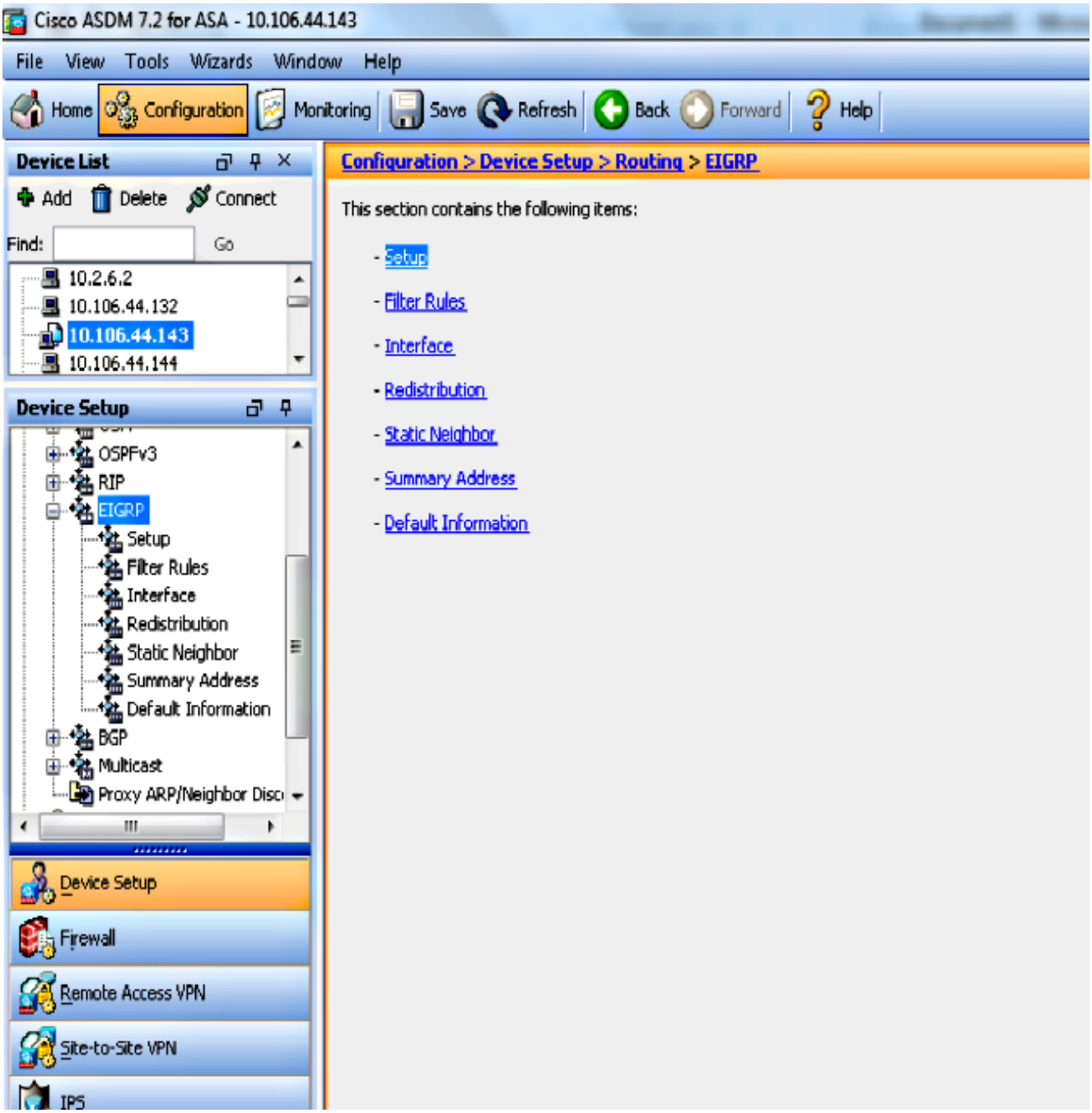
Configuração do ASDM

O ASDM é um aplicativo baseado em navegador usado para configurar e monitorar o software em dispositivos de segurança. O ASDM é carregado do Security Appliance e usado para configurar, monitorar e gerenciar o dispositivo. Você também pode usar o ASDM Launcher para iniciar o aplicativo ASDM mais rápido do que o miniaplicativo Java. Esta seção descreve as informações necessárias para configurar os recursos descritos neste documento com o ASDM.

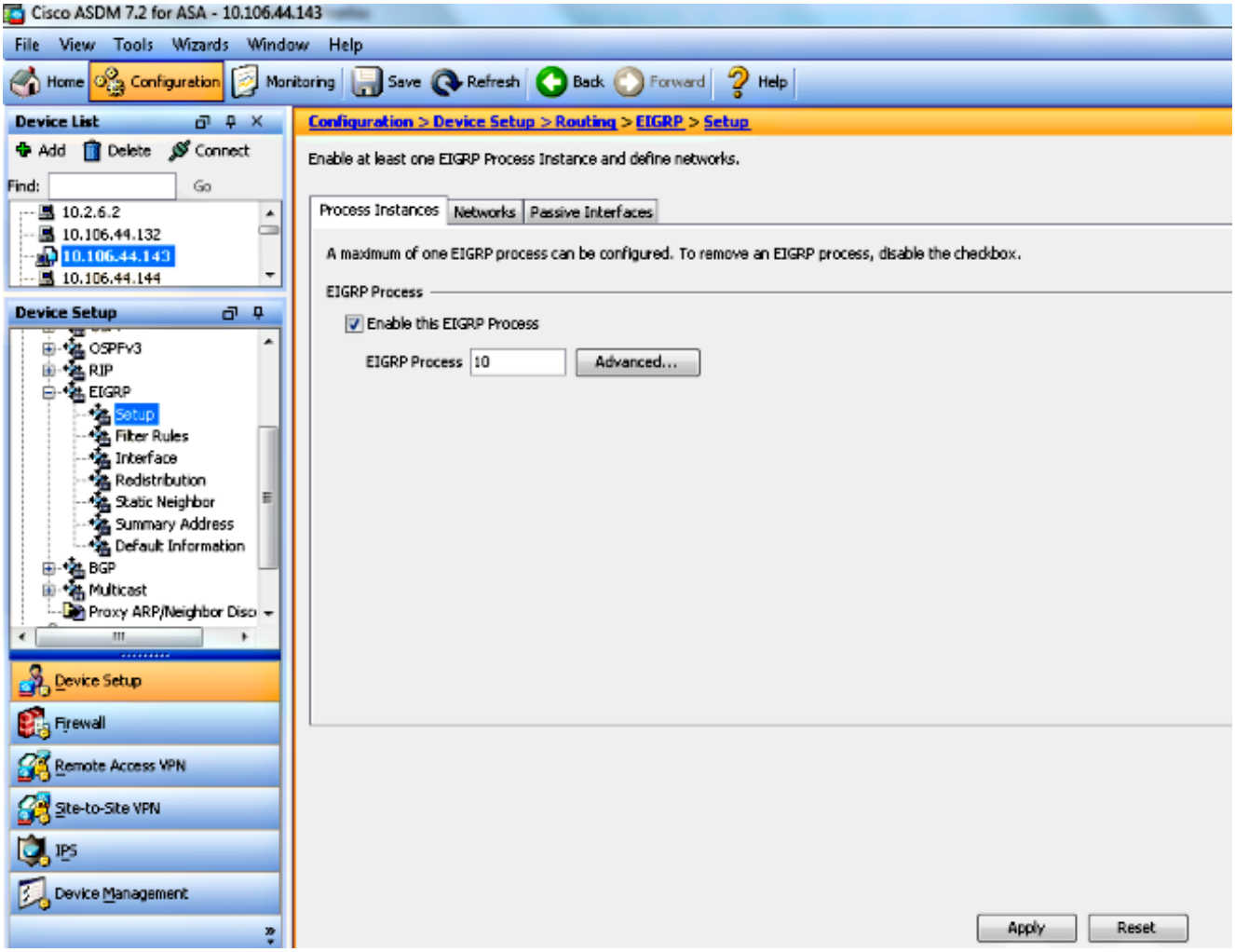
Conclua estes passos para configurar o EIGRP no Cisco ASA.

1. Faça login no Cisco ASA com o ASDM.

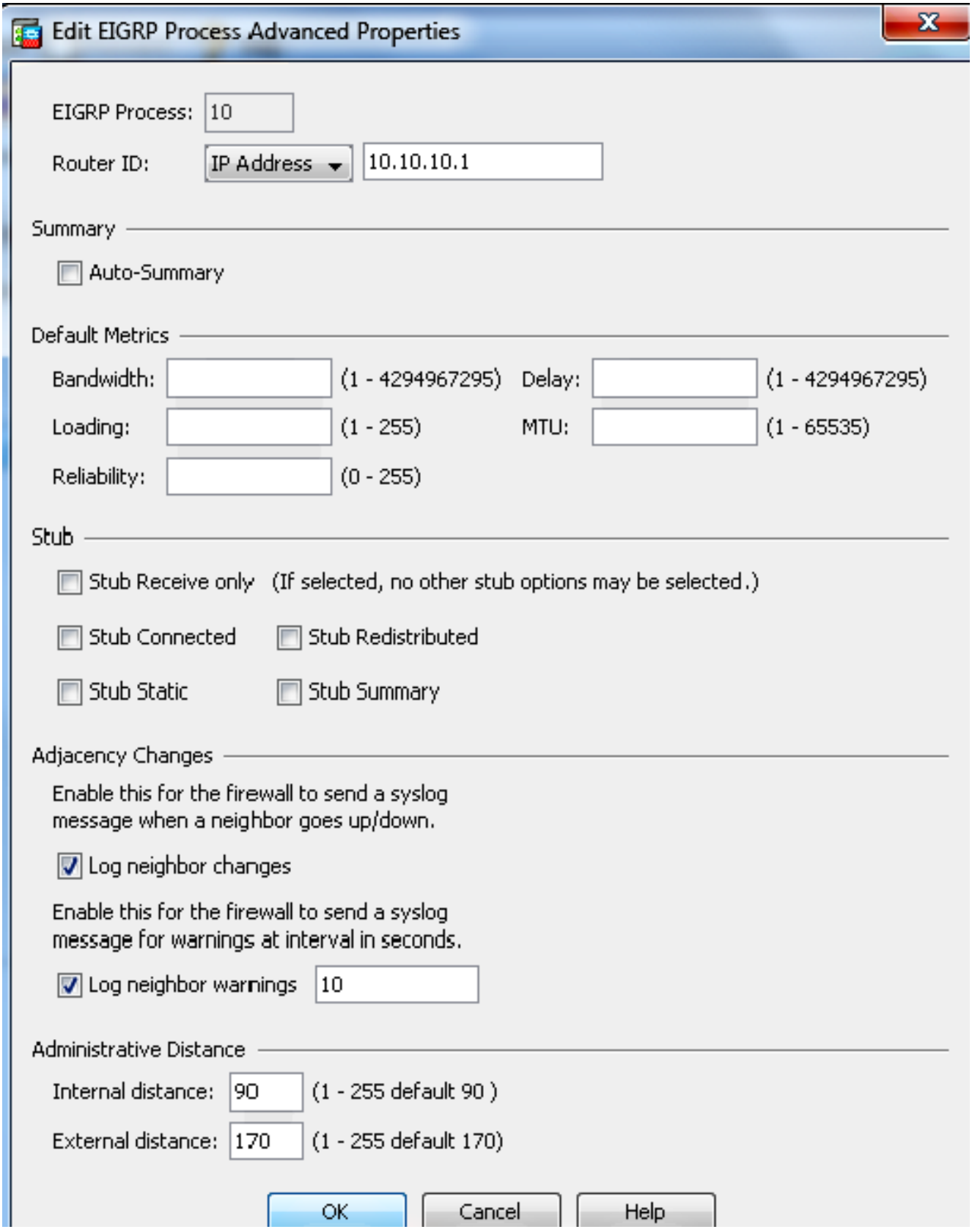
2. Navegue até a área **Configuration > Device Setup > Routing > EIGRP** da interface do ASDM, como mostrado nesta captura de tela.



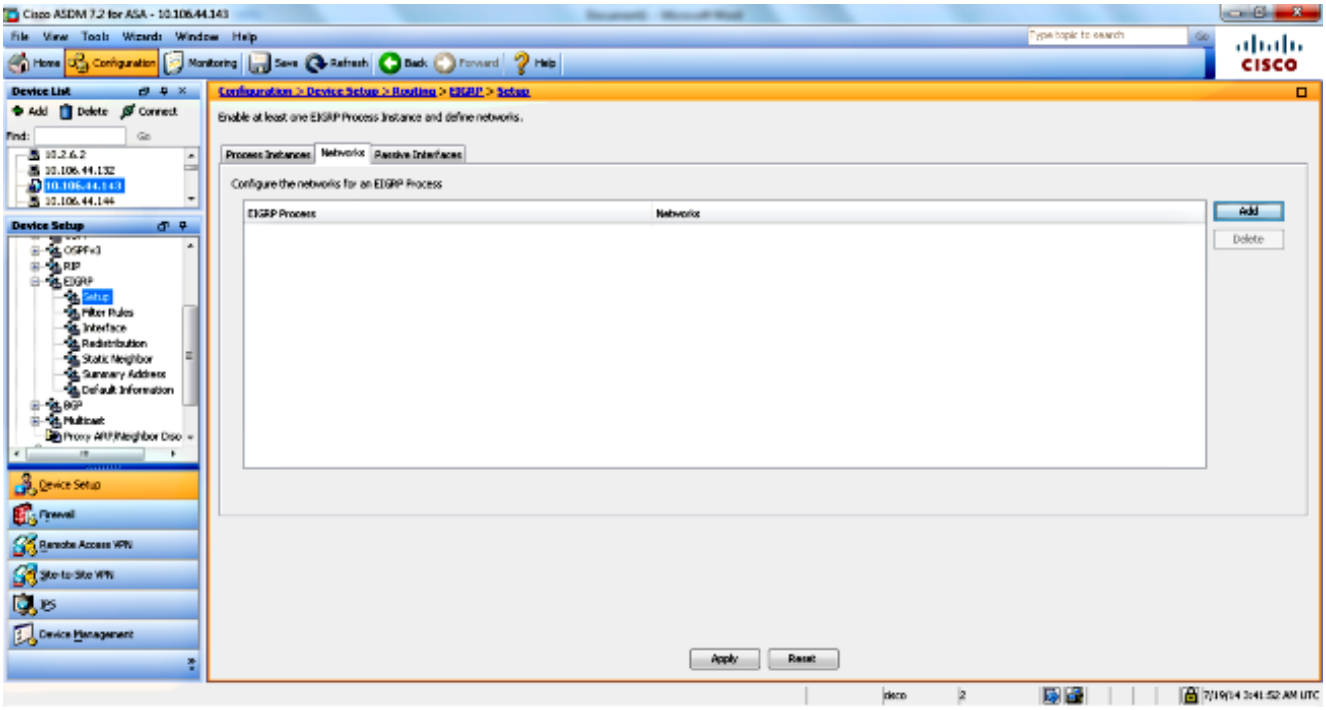
3. Ative o processo de roteamento EIGRP na guia **Setup > Process Instances**, como mostrado nesta captura de tela. Neste exemplo, o processo EIGRP é **10**.



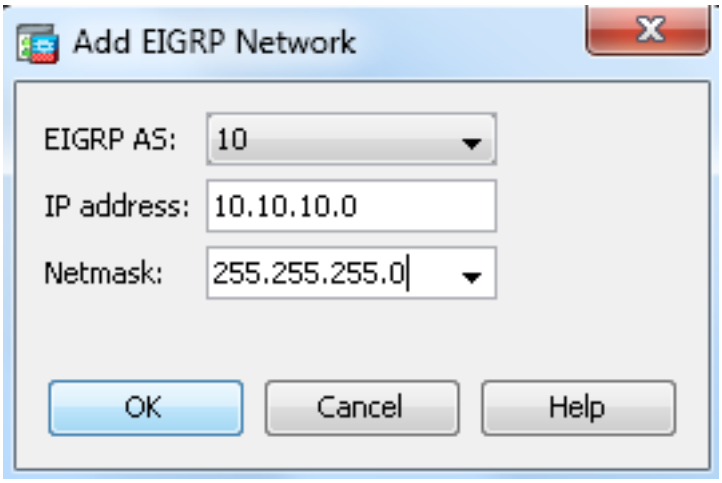
4. Você pode configurar parâmetros do processo de roteamento EIGRP avançados opcionais. Clique em **Advanced** na guia **Setup > Process Instances**. Você pode configurar o processo de roteamento EIGRP como um processo de roteamento stub, desativar a sumarização automática de rotas, definir as métricas padrão para rotas redistribuídas, alterar as distâncias administrativas para rotas EIGRP internas e externas, configurar um ID de roteador estático e ativar ou desativar o registro de alterações de adjacência. Neste exemplo, o ID do Roteador EIGRP é configurado estaticamente com o endereço IP da interface interna (10.10.10.1). Além disso, a **Sumarização Automática** também está desativada. Todas as outras opções são configuradas com seus valores padrão.



5. Depois de concluir as etapas anteriores, defina as redes e as interfaces que participam do roteamento EIGRP na guia **Setup > Networks**. Clique em **Adicionar** conforme mostrado nesta imagem.



6. Esta tela é exibida. Neste exemplo, a única rede que você adiciona é a rede interna (10.10.10.0/24), já que o EIGRP está habilitado somente na interface interna.



Somente as interfaces com um endereço IP que se enquadra nas redes definidas participam do processo de roteamento EIGRP. Se você tiver uma interface que não deseja participar do roteamento EIGRP, mas que esteja conectada a uma rede que deseja anunciar, configure uma entrada de rede na guia **Setup > Networks** que cobre a rede à qual a interface está conectada e configure essa interface como uma interface passiva para que a interface não possa enviar ou receber atualizações do EIGRP.

Note: As interfaces configuradas como passivas não enviam nem recebem atualizações do EIGRP.

7. Opcionalmente, você pode definir filtros de rota no painel Regras de filtro. A filtragem de rotas fornece mais controle sobre as rotas que podem ser enviadas ou recebidas em atualizações do EIGRP.

8. Você também pode configurar a redistribuição de rotas. O Cisco ASA pode redistribuir rotas

descobertas pelo Routing Information Protocol (RIP) e pelo Open Shortest Path First (OSPF) no processo de roteamento EIGRP. Você também pode redistribuir rotas estáticas e conectadas no processo de roteamento EIGRP. Você não precisa redistribuir rotas estáticas ou conectadas se elas estiverem dentro do intervalo de uma rede configurada na guia **Setup > Networks**. Defina a redistribuição da rota no painel Redistribuição.

9. Os pacotes Hello do EIGRP são enviados como pacotes multicast. Se um vizinho EIGRP estiver localizado em uma rede não broadcast, você deve definir manualmente esse vizinho. Quando você define manualmente um vizinho EIGRP, os pacotes Hello são enviados a esse vizinho como mensagens unicast. Para definir vizinhos EIGRP estáticos, vá para o painel **Vizinho Estático**.

10. Por padrão, as rotas padrão são enviadas e aceitas. Para restringir ou desabilitar o envio e o recebimento de informações de rota padrão, abra o painel **Configuração > Configuração do dispositivo > Roteamento > EIGRP > Informações padrão**. O painel Informações Padrão exibe uma tabela de regras para controlar o envio e o recebimento de informações de rota padrão nas atualizações do EIGRP.

    Note: Você pode ter uma regra "*in"* e uma "*out*" para cada processo de roteamento EIGRP. (Apenas um processo é suportado atualmente.)

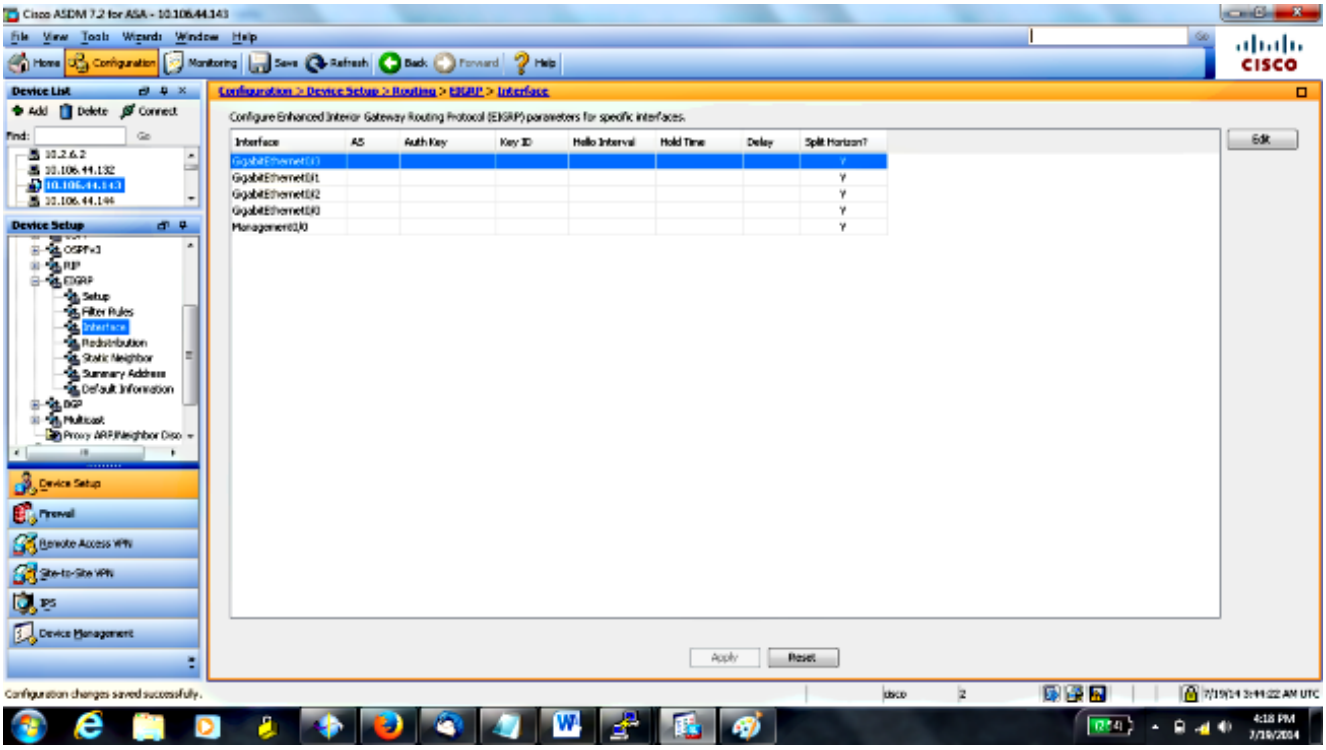
Configurar a Autenticação do EIGRP

O Cisco ASA suporta a autenticação MD5 de atualizações de roteamento do protocolo de roteamento EIGRP. O resumo de MD5 em cada pacote EIGRP impede a introdução de mensagens de roteamento não autorizadas ou falsas de fontes não aprovadas. A adição de autenticação às mensagens do EIGRP garante que seus roteadores e o Cisco ASA aceitem apenas mensagens de roteamento de outros dispositivos de roteamento configurados com a mesma chave pré-compartilhada. Sem essa autenticação configurada, se alguém introduzir outro dispositivo de roteamento com informações de rota diferentes ou contrárias na rede, as tabelas de roteamento em seus roteadores ou no Cisco ASA podem se tornar corrompidas e um ataque de negação de serviço pode ocorrer. Quando você adiciona autenticação às mensagens do EIGRP enviadas entre seus dispositivos de roteamento (que inclui o ASA), ele impede as adições não autorizadas dos roteadores do EIGRP na topologia de roteamento.

A autenticação de rota EIGRP é configurada por interface. Todos os vizinhos EIGRP em interfaces configuradas para autenticação de mensagem EIGRP devem ser configurados com o mesmo modo de autenticação e chave para que as adjacências sejam estabelecidas.

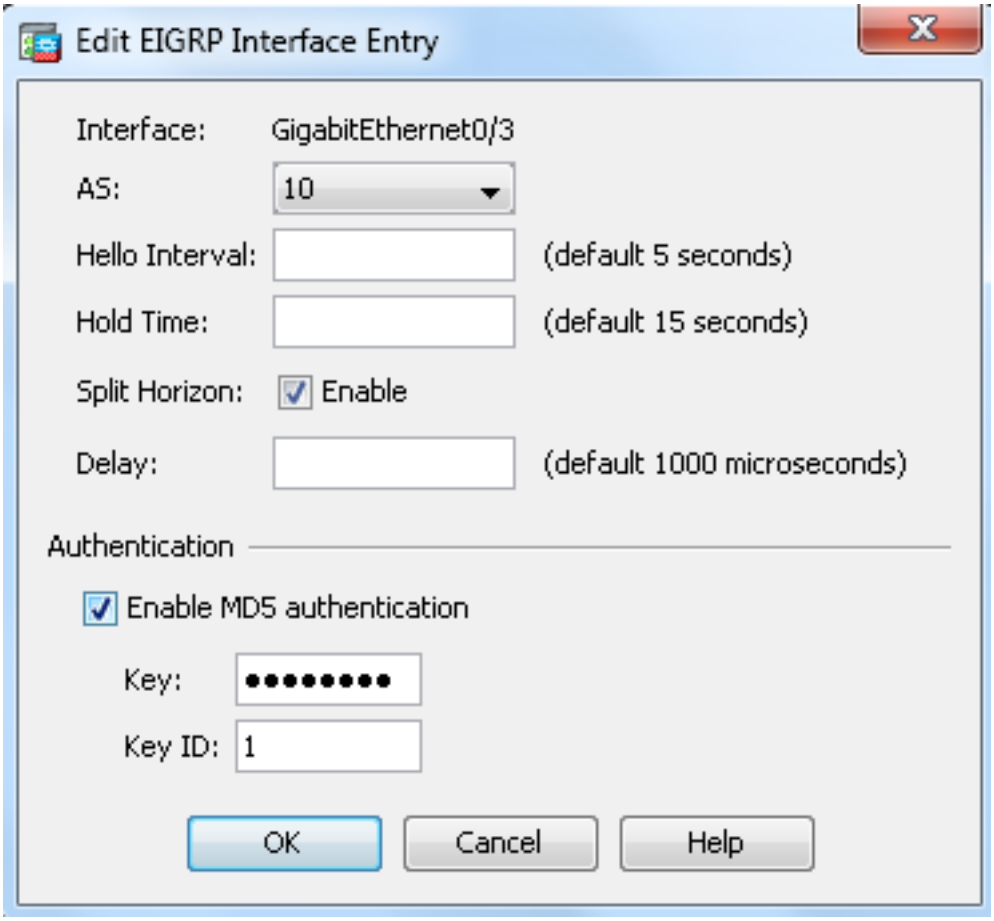
Conclua estes passos para habilitar a autenticação MD5 do EIGRP no Cisco ASA.

1. No ASDM, navegue para **Configuration > Device Setup > Routing > EIGRP > Interface** conforme mostrado.



2. Nesse caso, o EIGRP é ativado na interface interna (GigabitEthernet 0/1). Escolha a interface **GigabitEthernet 0/1** e clique em **Editar**.

3. Em Authentication, escolha **Enable MD5 authentication**. Adicione mais informações sobre os parâmetros de autenticação aqui. Nesse caso, a chave pré-compartilhada é **cisco123**, e a ID da chave é **1**.



Filtragem de Rota do EIGRP

Com o EIGRP, você pode controlar as atualizações de roteamento que são enviadas e recebidas. Neste exemplo, você bloqueará as atualizações de roteamento no ASA para o prefixo de rede 192.168.10.0/24, que está atrás de R1. Para filtragem de rota, você só pode usar a **ACL PADRÃO**.

```
access-list eigrp standard deny 192.168.10.0 255.255.255.0
access-list eigrp standard permit any

router eigrp 10
distribute-list eigrp in
```

Verificar

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

Configurações

Configuração do Cisco ASA CLI

Esta é a configuração do Cisco ASA CLI.

```
!outside interface configuration

interface GigabitEthernet0/0
description outside interface connected to the Internet
nameif outside
security-level 0
ip address 198.51.100.120 255.255.255.0
!

!inside interface configuration

interface GigabitEthernet0/1
description interface connected to the internal network
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!

!EIGRP authentication is configured on the inside interface

authentication key eigrp 10 cisco123 key-id 1
authentication mode eigrp 10 md5
!

!management interface configuration

interface Management0/0
```

```
nameif management
security-level 99
ip address 10.10.20.1 255.255.255.0 management-only
!
!

!EIGRP Configuration - the CLI configuration is very similar to the
!Cisco IOS router EIGRP configuration.

router eigrp 10
no auto-summary
eigrp router-id 10.10.10.1
network 10.10.10.0 255.255.255.0
!

!This is the static default gateway configuration

route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Configuração do Cisco IOS Router (R1) CLI

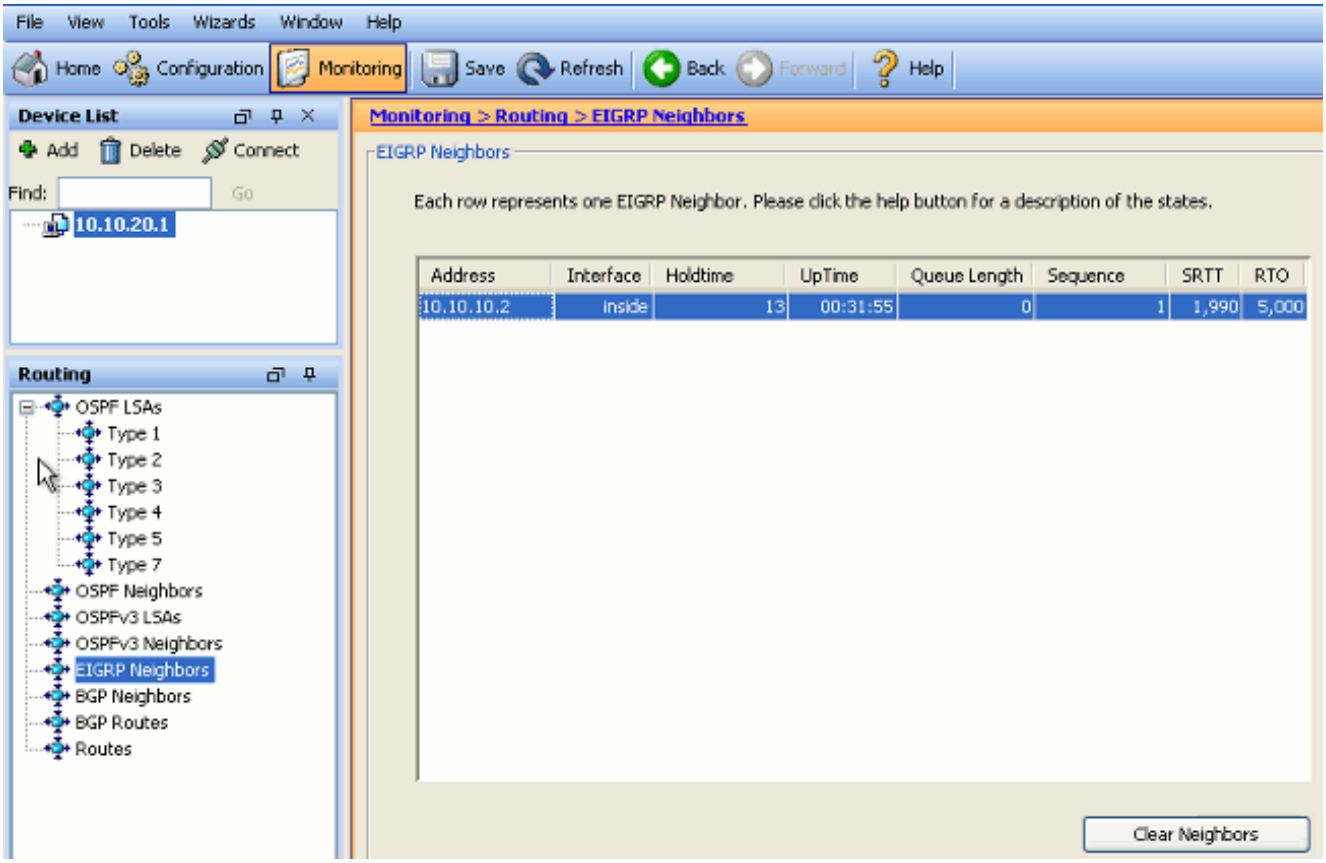
Esta é a configuração CLI de R1 (roteador interno).

```
!!Interface that connects to the Cisco ASA. Notice the EIGRP authentication
paramenters.


interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip authentication mode eigrp 10 md5
ip authentication key-chain eigrp 10 MYCHAIN
!
!

! EIGRP Configuration

router eigrp 10
network 10.10.10.0 0.0.0.255
network 10.20.20.0 0.0.0.255
network 172.18.124.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

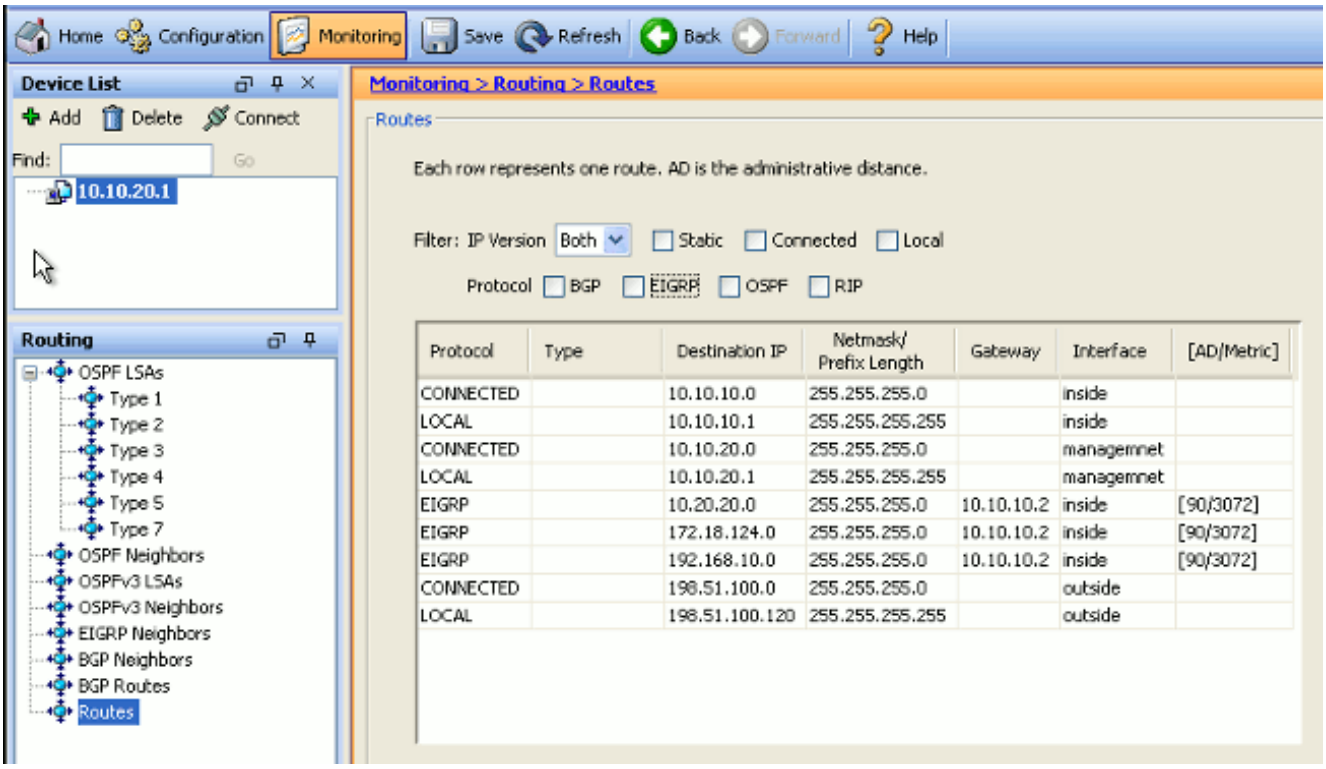
Verificar

Conclua estes passos para verificar sua configuração.

1. No ASDM, você pode navegar para **Monitoring > Routing > EIGRP Neighbor** para ver cada um dos vizinhos EIGRP. Essa captura de tela mostra o roteador interno (R1) como um vizinho ativo. Você também pode ver a interface onde esse vizinho reside, o tempo de espera e por quanto tempo o relacionamento de vizinhança está ativo (UpTime).



2. Além disso, você pode verificar a tabela de roteamento se navegar para **Monitoring > Routing > Routes**. Nesta captura de tela, você pode ver que as redes **192.168.10.0/24, 172.18.124.0/24** e **10.20.20.0/24** são aprendidas através de R1 (**10.10.10.2**).



Na CLI, você pode usar o comando **show route** para obter a mesma saída.

```
ciscoasa# show route
```

```
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, 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
Gateway of last resort is 100.10.10.2 to network 0.0.0.0
C 198.51.100.0 255.255.255.0 is directly connected, outside
D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
C 127.0.0.0 255.255.0.0 is directly connected, cplane
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
C 10.10.10.0 255.255.255.0 is directly connected, inside
C 10.10.20.0 255.255.255.0 is directly connected, management
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Com o ASA versão 9.2.1 e posterior, você pode usar o comando **show route eigrp** para exibir apenas rotas EIGRP.

```
ciscoasa(config)# show route eigrp

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
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

Gateway of last resort is not set

D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
```

3. Você também pode usar o comando **show eigrp topology** para obter informações sobre as redes aprendidas e a topologia EIGRP.

```
    ciscoasa# show eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(10.10.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.20.20.0 255.255.255.0, 1 successors, FD is 28672
via 10.10.10.2 (28672/28416), GigabitEthernet0/1
P 10.10.10.0 255.255.255.0, 1 successors, FD is 2816
via Connected, GigabitEthernet0/1
P 192.168.10.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
P 172.18.124.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
```

4. O comando **show eigrp neighbors** também é útil para verificar os vizinhos ativos e as informações correspondentes. Este exemplo mostra as mesmas informações obtidas do ASDM na Etapa 1.

```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

Fluxo de pacote

Aqui está o fluxo do pacote.

1. O ASA é ativado no link e envia um pacote mCast Hello por meio de todas as interfaces configuradas com EIGRP.

2. R1 recebe um pacote Hello e envia um pacote de Hello mCast.

13 5.572557	10.10.10.1	224.0.0.10	EIGRP	86 0x3b1a (15130)	Hello
14 5.573335	10.10.10.2	224.0.0.10	EIGRP	86 0x2321 (8993)	Hello
15 5.575212	10.10.10.1	10.10.10.2	EIGRP	54 0x0589 (1417)	Update
16 5.581712	10.10.10.2	10.10.10.1	EIGRP	54 0x19d9 (6617)	Update
17 5.585145	10.10.10.1	10.10.10.2	EIGRP	54 0x755e (30046)	Hello (Ack)
18 5.585373	10.10.10.1	10.10.10.2	EIGRP	96 0x1c93 (7315)	Update
19 5.591919	10.10.10.2	10.10.10.1	EIGRP	54 0x6695 (26261)	Hello (Ack)
20 5.591950	10.10.10.2	10.10.10.1	EIGRP	180 0x7925 (31013)	Update
21 5.595200	10.10.10.1	10.10.10.2	EIGRP	96 0x62e8 (25320)	Update
22 5.601913	10.10.10.2	10.10.10.1	EIGRP	54 0x08a7 (2215)	Hello (Ack)
23 5.601944	10.10.10.2	10.10.10.1	EIGRP	96 0x31c5 (12741)	Update

3. O ASA recebe o pacote Hello e envia um pacote Update com um bit inicial definido, o que indica que esse é o processo de inicialização.

4. R1 recebe um pacote Update e envia um pacote Update com um bit inicial definido, o que indica que esse é o processo de inicialização.

```
⊞ Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Cisco_25:32:e2 (00:21:a0:25:32:e2), Dst: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3)
⊞ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
⊟ Cisco EIGRP
    Version: 2
    Opcode: Update (1)
    Checksum: 0xfdc4 [correct]
  ⊟ Flags: 0x00000001, Init
      .... .... .... .... .... .... .... ...1 = Init: Set
      .... .... .... .... .... .... .... ..0. = Conditional Receive: Not set
      .... .... .... .... .... .... .... .0.. = Restart: Not set
      .... .... .... .... .... .... .... 0... = End Of Table: Not set
    Sequence: 47
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 10
```

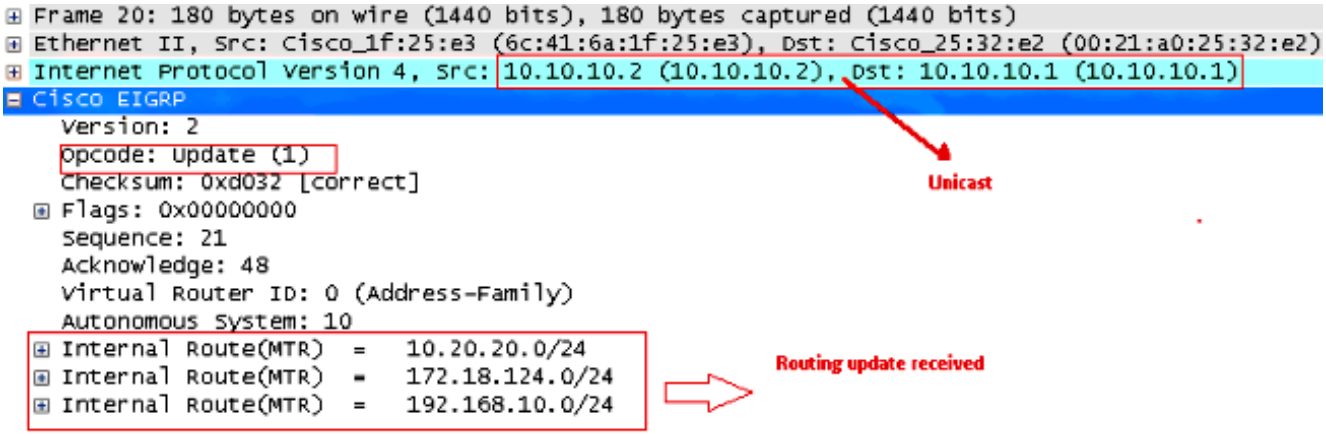
5. Depois que o ASA e o R1 trocaram pacotes de hello e a adjacência de vizinhos é estabelecida, tanto o ASA quanto o R1 respondem com um pacote ACK, o que indica que as

informações de atualização foram recebidas.

6. O ASA envia suas informações de roteamento para R1 em um pacote Update.

7. O R1 insere as informações do pacote Update em sua tabela de topologia. A tabela de topologia inclui todos os destinos anunciados por vizinhos. Ele é organizado para que cada destino seja listado, junto com todos os vizinhos que podem viajar até o destino e suas métricas associadas.

8. Em seguida, R1 envia um pacote Update ao ASA.



9. Depois de receber o pacote Update, o ASA envia um pacote ACK para R1. Depois que o ASA e o R1 receberem com êxito os pacotes Update um do outro, eles estarão prontos para escolher as rotas sucessora (melhor) e sucessora viável (backup) na tabela de topologia e oferecer as rotas sucessoras à tabela de roteamento.

Troubleshoot

Esta seção inclui informações sobre os comandos **debug** e **show** que podem ser úteis para solucionar problemas do EIGRP.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para visualizar uma análise da saída do comando **show**.

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.** Para exibir informações de depuração na máquina de estado finito DUAL (Diffusing Update Algorithm), use o comando **debug eigrp fsm** no modo EXEC privilegiado. Esse comando permite observar a atividade de sucessor viável do EIGRP e determinar se as atualizações de rota são instaladas e excluídas pelo processo de roteamento.

Esta é a saída do comando **debug** no peering bem-sucedido com R1. Você pode ver cada uma das diferentes rotas instaladas com êxito no sistema.

```
EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust GigabitEthernet0/1
DUAL: dest(10.10.10.0 255.255.255.0) not active
DUAL: rcvupdate: 10.10.10.0 255.255.255.0 via Connected metric 2816/0 on topoid 0
DUAL: Find FS for dest 10.10.10.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
DUAL: RT installed 10.10.10.0 255.255.255.0 via 0.0.0.0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(10.20.20.0 255.255.255.0) not active
DUAL: rcvupdate: 10.20.20.0 255.255.255.0 via 10.10.10.2 metric 28672/28416 on t
opoid 0
DUAL: Find FS for dest 10.20.20.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
DUAL: RT installed 10.20.20.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(172.18.124.0 255.255.255.0) not active
DUAL: rcvupdate: 172.18.124.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 172.18.124.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
DUAL: RT installed 172.18.124.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(192.168.10.0 255.255.255.0) not active
DUAL: rcvupdate: 192.168.10.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 192.168.10.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
DUAL: RT installed 192.168.10.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: new if on topoid 0
```

Você também pode usar o comando **debug eigrp neighbor**. Esta é a saída desse comando **debug** quando o Cisco ASA criou com êxito uma nova relação de vizinhança com R1.

```
ciscoasa# EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust Gigabi
tEthernet0/1
EIGRP: New peer 10.10.10.2
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
```

Você também pode usar a depuração de pacotes EIGRP para informações detalhadas de troca de mensagens do EIGRP entre o Cisco ASA e seus pares. Neste exemplo, a chave de autenticação foi alterada no roteador (R1) e a saída de depuração mostra que o problema é uma incompatibilidade de autenticação.

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

A vizinhança do EIGRP cai com o Syslogs ASA-5-336010

O ASA descarta a vizinhança do EIGRP quando qualquer alteração na lista de distribuição do EIGRP é feita. Esta mensagem de Syslog é exibida.

```
EIGRP Nieghborship Resets with syslogs ASA-5-336010: EIGRP-IPv4: PDM(314 10:
Neighbor 10.15.0.30 (GigabitEthernet0/0) is down: route configuration changed
```

Com essa configuração, sempre que uma **nova entrada de acl é adicionada** na ACL, a vizinhança **Eigrp-network-list** EIGRP é redefinida.

```
router eigrp 10
distribute-list Eigrp-network-list in
network 10.10.10.0 255.0.0.0
passive-interface default
no passive-interface inside
redistribute static

access-list Eigrp-network-list standard permit any
```

Você pode observar que a relação de vizinhança está ativa com o dispositivo adjacente.

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

Agora você pode adicionar **lista de acesso Eigrp-network-list standard deny 172.18.24.0 255.255.255.0**.

```
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'debug
eigrp fsm'
%ASA-7-111009: User 'enable_15' executed cmd: show access-list
%ASA-5-111008: User 'enable_15' executed the 'access-list Eigrp-network-list line
1 permit 172.18.24.0 255.255.255.0' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'access-list
Eigrp-network-list line 1 permit 172.18.24.0 255.255.255.0'
%ASA-7-111009: User 'enable_15' executed cmd: show eigrp neighbors
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
down: route configuration changed
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
up: new adjacency
```

Esses registros podem ser vistos em **debug eigrp fsm**.

```
IGRP2: linkdown: start - 10.10.10.2 via GigabitEthernet0/3
DUAL: Destination 10.10.10.0 255.255.255.0 for topoid 0
DUAL: linkdown: finish
```

Esse comportamento é esperado em todas as novas versões do ASA de 8.4 e 8.6 para 9.1. O mesmo foi observado em roteadores que executam as trilhas de código 12.4 a 15.1. No entanto,

esse comportamento não é observado no ASA versão 8.2 e nas versões anteriores do software ASA porque as alterações feitas em uma ACL não redefinem as adjacências do EIGRP.

Como o EIGRP envia a tabela de topologia completa para um vizinho quando o vizinho é ativado pela primeira vez, e depois envia apenas as alterações, configurar uma lista de distribuição com a natureza orientada a eventos do EIGRP dificultaria a aplicação das alterações sem uma redefinição completa do relacionamento vizinho. Os roteadores precisariam manter o controle de cada rota enviada e recebida de um vizinho para saber qual rota mudou (ou seja, seria ou não enviada/aceita) para aplicar as alterações conforme ditado pela lista de distribuição atual. É muito mais fácil simplesmente rasgar e restabelecer a adjacência entre vizinhos.

Quando uma adjacência é dividida e restabelecida, todas as rotas aprendidas entre vizinhos específicos são simplesmente esquecidas e toda a sincronização entre vizinhos é executada novamente - com a nova lista de distribuição em vigor.

A maioria das técnicas do EIGRP que você usa para solucionar problemas dos roteadores Cisco IOS pode ser aplicada no Cisco ASA. Para solucionar problemas do EIGRP, use o Fluxograma Principal de Troubleshooting; inicie na caixa marcada como **Main**.