Exemplo de configuração EIGRP ASA 9.x

Índice

Introdução

Este documento descreve como configurar a ferramenta de segurança adaptável de Cisco (ASA) a fim aprender rotas com o Enhanced Interior Gateway Routing Protocol (EIGRP), que é apoiada na versão de software 9.x ASA e mais tarde, e executar a autenticação.

Pré-requisitos

Requisitos

Cisco exige que você está conformes estas circunstâncias antes que você tente esta configuração:

- Cisco ASA deve executar a versão 9.x ou mais recente.
- O EIGRP deve reagir do modo do único-contexto, porque não é apoiado no modo do multi-contexto.

Componentes Utilizados

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

- Versão de software 9.2.1 de Cisco ASA
- Versão 7.2.1 do Cisco Adaptive Security Device Manager (ASDM)
- Roteador do ® do Cisco IOS que executa a versão 12.4

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Diretrizes e limitações

- Um exemplo EIGRP é apoiado no modo simples e pelo contexto em multimodo.
- Duas linhas são criadas pelo contexto pelo exemplo EIGRP em multimodo e podem ser vistas com o processo da mostra.
- O resumo automático é desabilitado à revelia.
- Um relacionamento vizinho não é estabelecido entre as unidades de conjunto no modo da interface individual.
- a Padrão-informação no [<acl>] é usada a fim filtrar o bit exterior em rotas default de candidato entrantes.
- da Padrão-informação o [<acl>] para fora é usado a fim filtrar o bit exterior em rotas default de candidato que parte.

EIGRP e Failover

Versão de código 8.4.4.1 de Cisco ASA e rotas dinâmica mais atrasadas dos sincronizars da unidade ativa à unidade em standby. Além, o supressão das rotas é sincronizado igualmente à unidade em standby. Contudo, o estado de adjacências do par não é sincronizado; somente o dispositivo ativo mantém o estado vizinho e participa ativamente no roteamento dinâmico. Refira ASA FAQ: Que acontece após o Failover se as rotas dinâmica são sincronizadas? para obter mais informações.

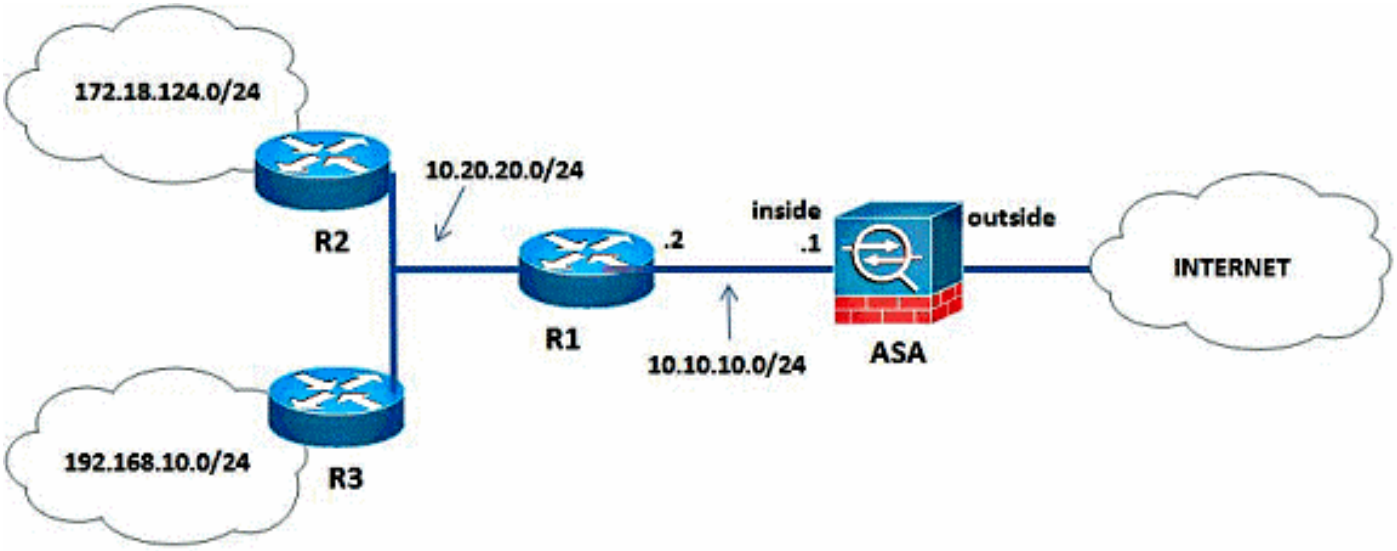
Configurar

Esta seção descreve como configurar as características cobertas 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 que é ilustrada, o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface interna de Cisco ASA é 10.10.10.1/24. O objetivo é configurar o EIGRP em Cisco ASA a fim aprender dinamicamente rotas às redes internas (10.20.20.0/24, 172.18.124.0/24, e 192.168.10.0/24) através do roteador adjacente (r1). O r1 aprende as rotas às redes internas remotas através de outro dois Roteadores (R2 e R3).

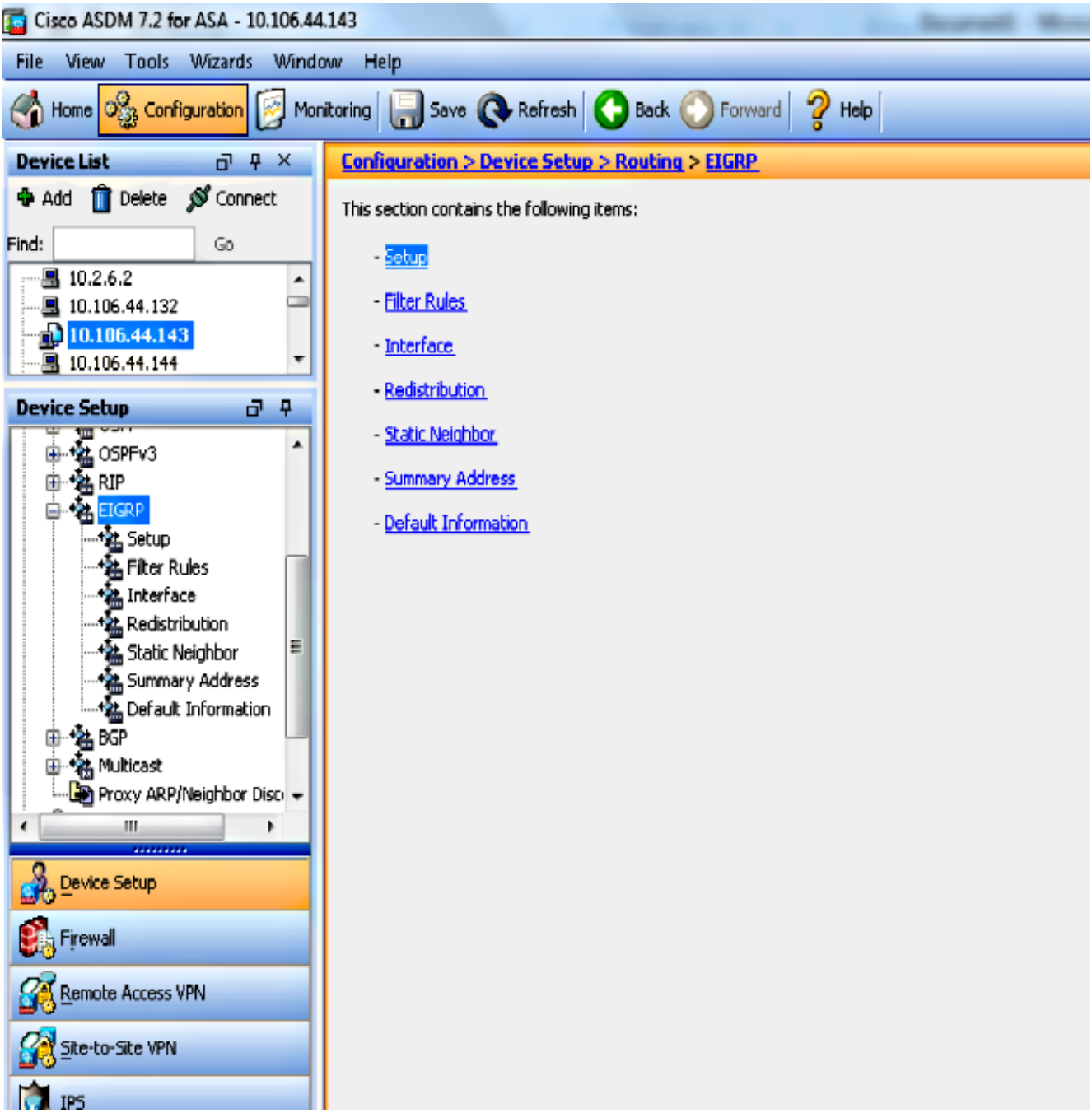
Configuração ASDM

O ASDM é um aplicativo baseado em navegador usado a fim configurar e monitorar o software em ferramentas de segurança. O ASDM é carregado da ferramenta de segurança, e usado então a fim configurar, monitorar, e controlar o dispositivo. Você pode igualmente usar a launcher ASDM a fim lançar mais rapidamente o aplicativo ASDM do que o Java applet. Esta seção descreve a informação que você precisa a fim configurar as características descritas neste documento com ASDM.

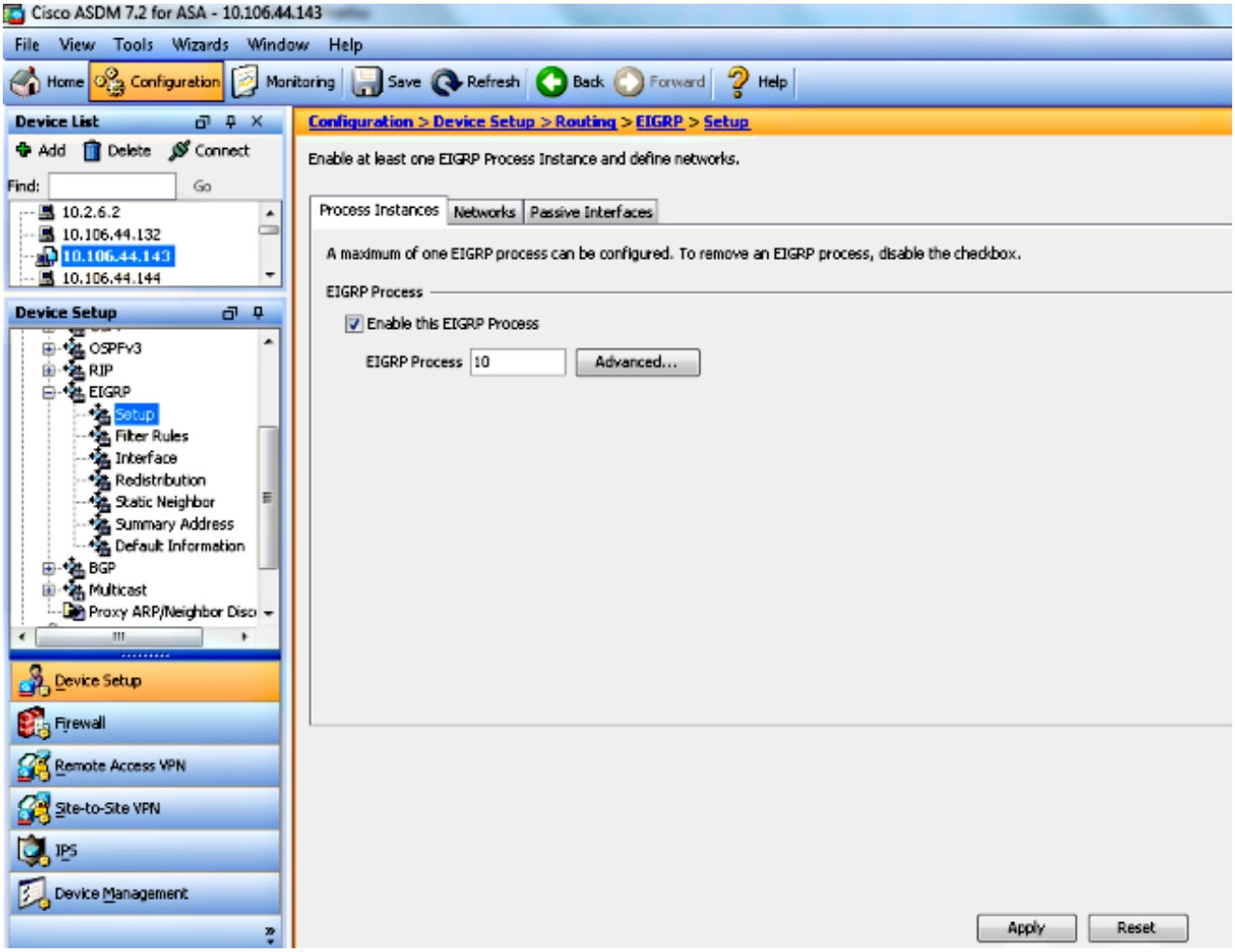
Termine estas etapas a fim configurar o EIGRP em Cisco ASA.

1. Entre a Cisco ASA com o ASDM.

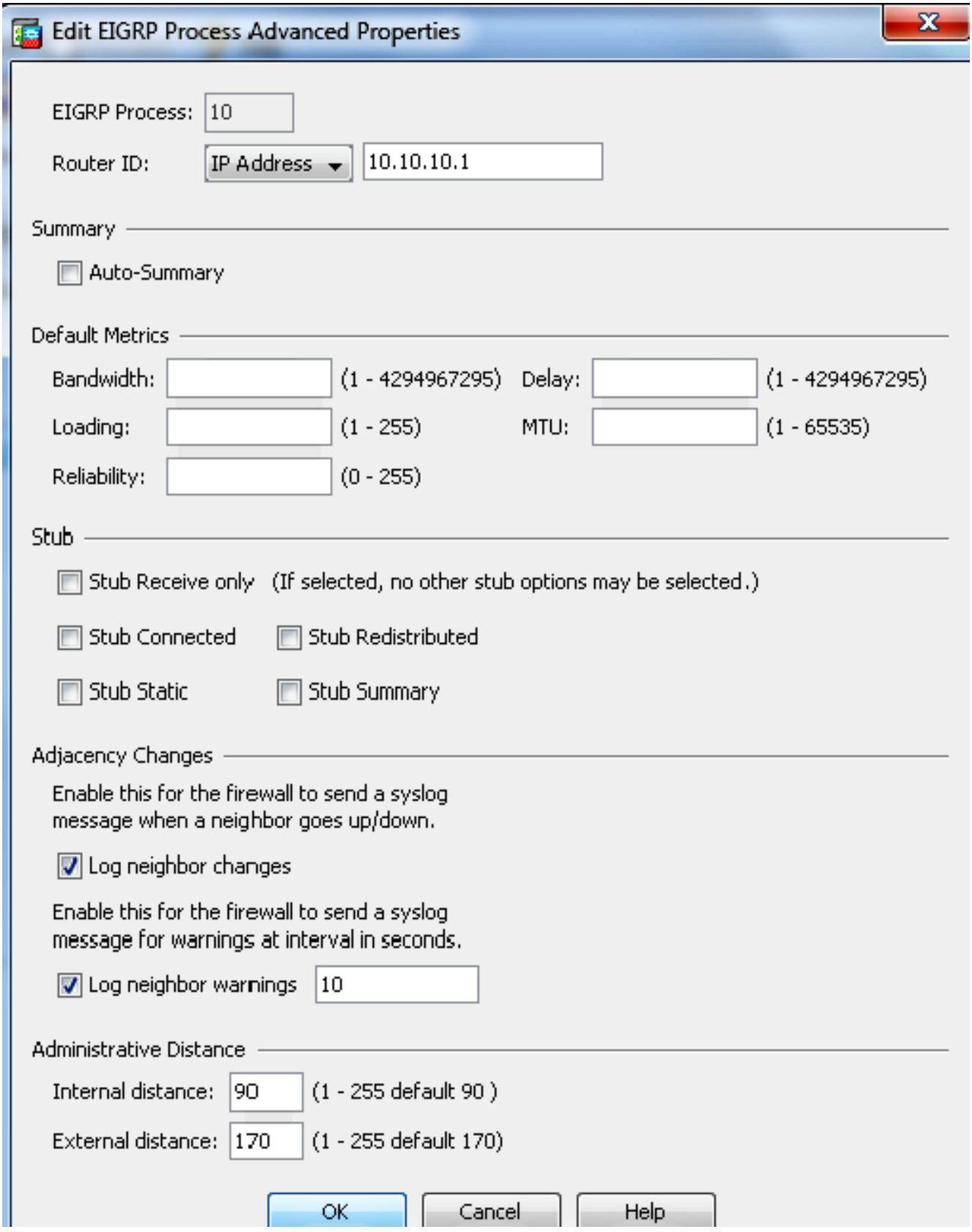
2. Navegue à **configuração > à instalação de dispositivo > ao roteamento > à** área **EIGRP da** relação ASDM, segundo as indicações deste tiro de tela.



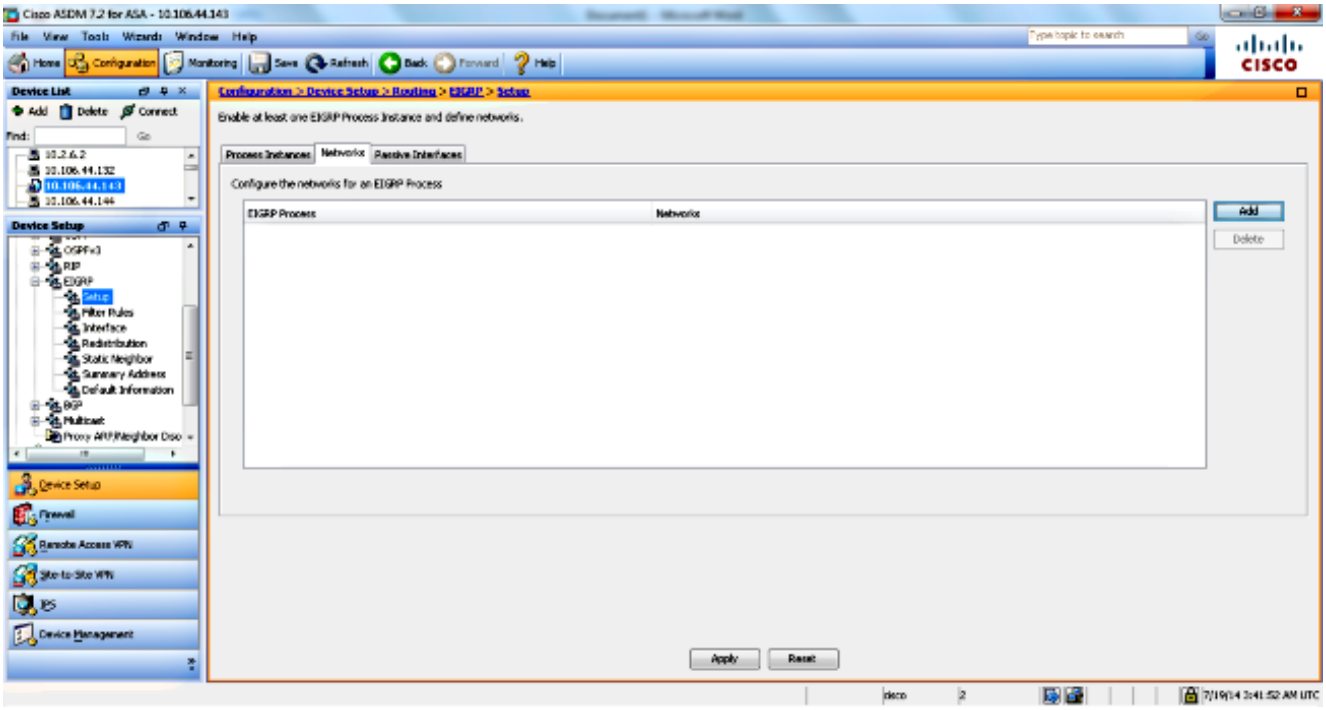
3. Permita o processo de roteamento de EIGRP na aba dos **exemplos da instalação > do processo**, segundo as indicações deste tiro de tela. Neste exemplo, o processo de EIGRP é **10.**



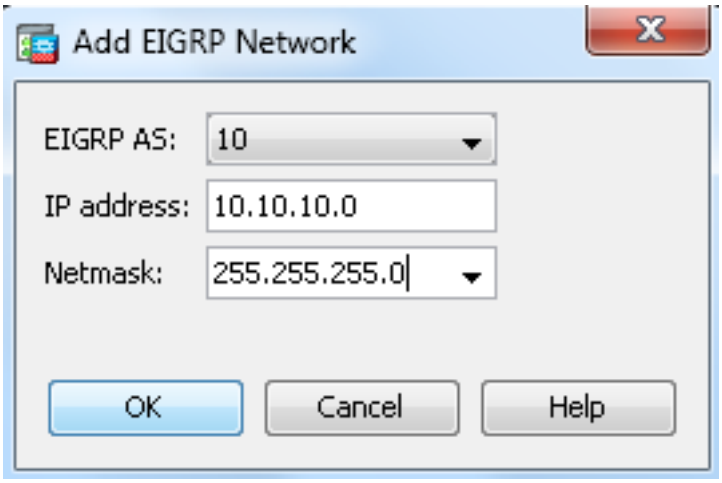
4. Você pode configurar parâmetros de processo avançados opcionais do roteamento de EIGRP. O clique **avançado na instalação > no processo cita como exemplo a** aba. Você pode configurar o processo de roteamento de EIGRP como um processo de roteamento de stub, desabilita a sumarização de rota automática, define o medidor do padrão para rotas redistribuída, muda as distâncias administrativas para interno e rotas de EIGRP externas, configura um Router ID estático, e permite ou desabilita o registro de mudanças da adjacência. Neste exemplo, o EIGRP Router ID é configurado estaticamente com o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface interna (10.10.10.1). Adicionalmente, o **resumo automático** é desabilitado igualmente. Todas as outras opções são configuradas com seus valores padrão.



5. Depois que você termina as etapas precedentes, defina as redes e as relações que participam no roteamento de EIGRP na aba da **instalação > das redes**. O clique **adiciona** segundo as indicações deste tiro de tela.



6. Esta tela aparece. Neste exemplo, a única rede que você adiciona é a rede interna (10.10.10.0/24) desde que o EIGRP é permitido somente na interface interna.



Conecta somente com um endereço IP de Um ou Mais Servidores Cisco ICM NT que as quedas dentro das redes definidas participem no processo de roteamento de EIGRP. Se você tem uma relação que você não quer participar no roteamento de EIGRP mas aquele está anexado a uma rede que você queira anunciado, configurar uma entrada de rede na aba da **instalação > das redes** que cobre a rede a que a relação é anexada, e para configurar então essa relação como uma interface passiva de modo que a relação não possa enviar ou receber atualizações EIGRP.

Note: As relações configuradas como a voz passiva não enviam nem recebem atualizações EIGRP.

7. Você pode opcionalmente definir filtros da rota na placa das regras de filtro. O filtragem de rota fornece mais controle sobre as rotas que são permitidas ser enviadas ou recebido nas atualizações EIGRP.

8. Você pode opcionalmente configurar a redistribuição de rota. Cisco ASA pode redistribuir as rotas descobertas pelo Routing Information Protocol (RIP) e pelo Open Shortest Path First (OSPF) no processo de roteamento de EIGRP. Você pode igualmente redistribuir a estática e as rotas conectadas no processo de roteamento de EIGRP. Você não precisa de redistribuir a estática ou as rotas conectadas se caem dentro da escala de uma rede configurada na aba da **instalação > das redes**. Defina a redistribuição de rota na placa da redistribução.

9. Os pacotes de hello de EIGRP são enviados como pacotes de transmissão múltipla. Se um vizinho EIGRP é ficado situado através de uma rede sem broadcast, você deve manualmente definir esse vizinho. Quando você define manualmente um vizinho EIGRP, os pacotes Hello estão enviados a esse vizinho como mensagens do unicast. A fim definir vizinhos EIGRP estáticos, vá à placa do **vizinho estático**.

10. Àrevelia, as rotas padrão são enviadas e aceitadas. A fim restringir ou desabilitar a emissão e a recepção da informação rota padrão, abra a **configuração > a instalação de dispositivo > o roteamento > o EIGRP > a** placa da **informação do padrão**. A placa da informação do padrão indica uma tabela das regras para controlar a emissão e a recepção da informação rota padrão nas atualizações EIGRP.

    Note: Você pode mandar um "*"* e um em "*para fora*" ordenar para cada processo de roteamento de EIGRP. (Somente um processo é apoiado atualmente.)

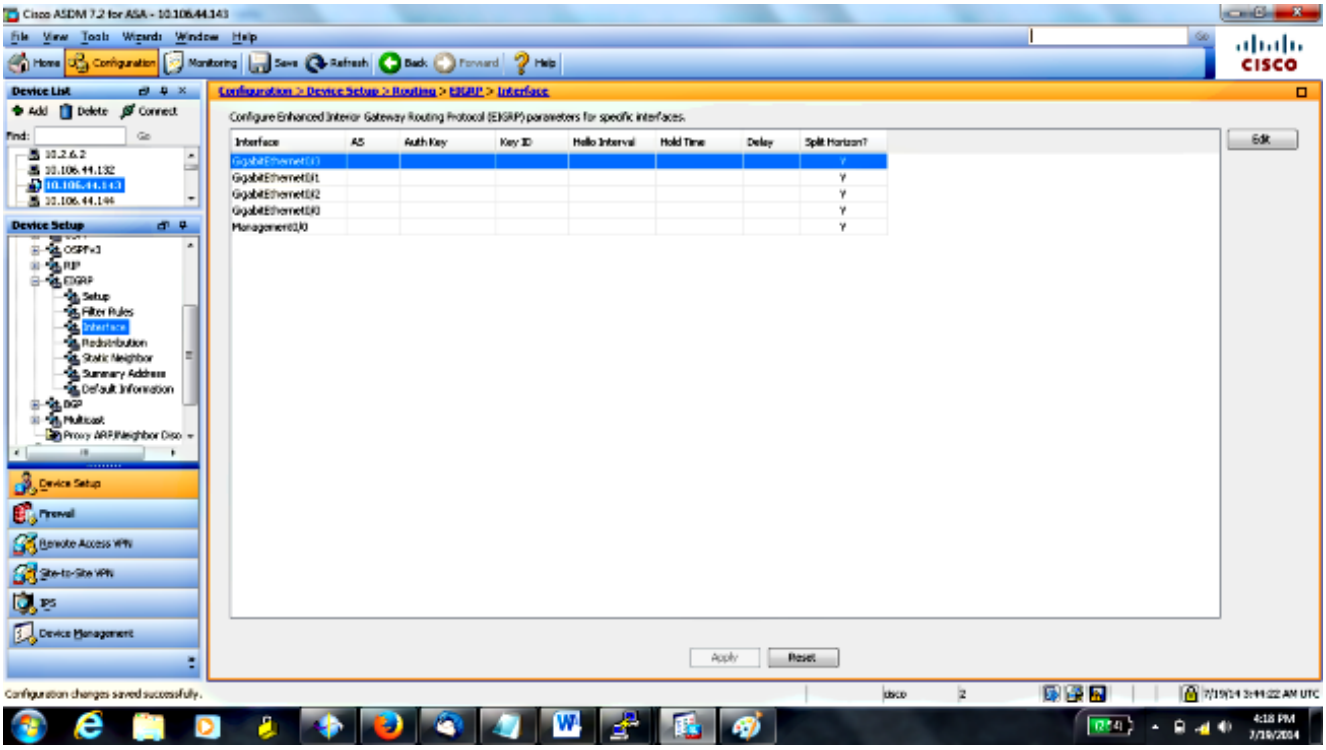
Configurar a autenticação EIGRP

Cisco ASA apoia a autenticação md5 das atualizações de roteamento do protocolo de roteamento EIGRP. O resumo MD5-keyed em cada pacote EIGRP impede a introdução de mensagens de roteamento desautorizados ou falsos das fontes unapproved. A adição de autenticação a suas mensagens EIGRP assegura-se de que seu Roteadores e Cisco ASA aceitem somente mensagens de roteamento de outros dispositivos de roteamento que são configurados com a mesma chave pré-compartilhada. Sem esta autenticação configurada, se alguém introduzem um outro dispositivo de roteamento com informação de rota diferente ou contrária sobre à rede, as tabelas de roteamento em seu Roteadores ou Cisco ASA podem tornar-se corrompidas e um ataque de recusa de serviço pode seguir. Quando você adicionar a autenticação às mensagens EIGRP enviadas entre seus dispositivos de roteamento (que inclui o ASA), impede as adições desautorizadas de EIGRP Router em sua topologia de roteamento.

A autenticação da rota de EIGRP é configurada em uma base da interface per. Todos os vizinhos EIGRP nas relações configuradas para a autenticação de mensagem EIGRP devem ser configurados com o mesmos modo de autenticação e chave para que as adjacências sejam estabelecidas.

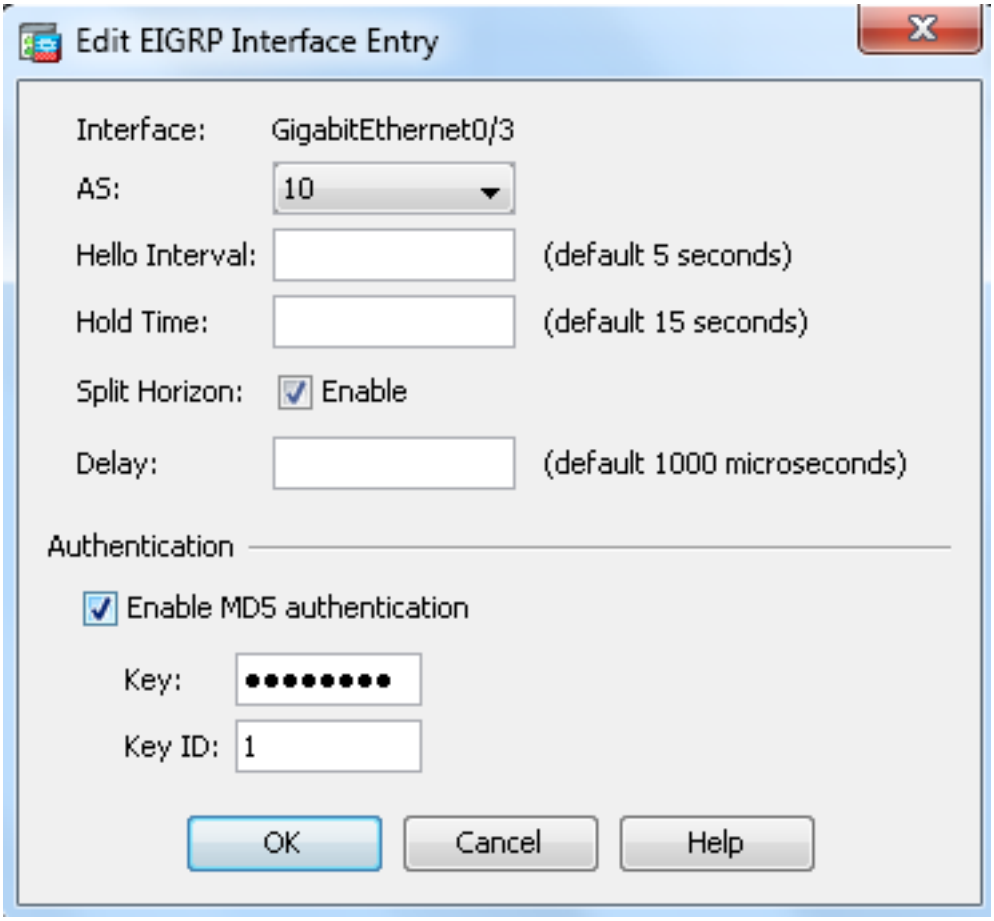
Termine estas etapas a fim permitir a autenticação md5 EIGRP em Cisco ASA.

1. No ASDM, navegue à **configuração > à instalação > ao roteamento > ao EIGRP > à relação de dispositivo** como mostrado.



2. Neste caso, o EIGRP é permitido na interface interna (gigabitethernet 0/1). Escolha o **gigabitethernet 0/1 de** relação e o clique **edita**.

3. Sob a autenticação, escolha **permitem a autenticação md5**. Adicionar mais informação sobre os parâmetros de autenticação aqui. Neste caso, a chave preshared é **cisco123**, e a chave ID é **1.**



Filtração da rota de EIGRP

Com EIGRP, você pode controlar as atualizações de roteamento que são enviadas e recebidas. Neste exemplo, você obstruirá atualizações de roteamento no ASA para o prefixo de rede 192.168.10.0/24, que é atrás do r1. Para o filtragem de rota, você pode somente usar o **PADRÃO ACL**.

```
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 de CLI de Cisco ASA

Esta é a configuração de CLI de Cisco ASA.

```
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
```

Configuração de CLI do roteador do Cisco IOS (r1)

Esta é a configuração de CLI do r1 (roteador interno).

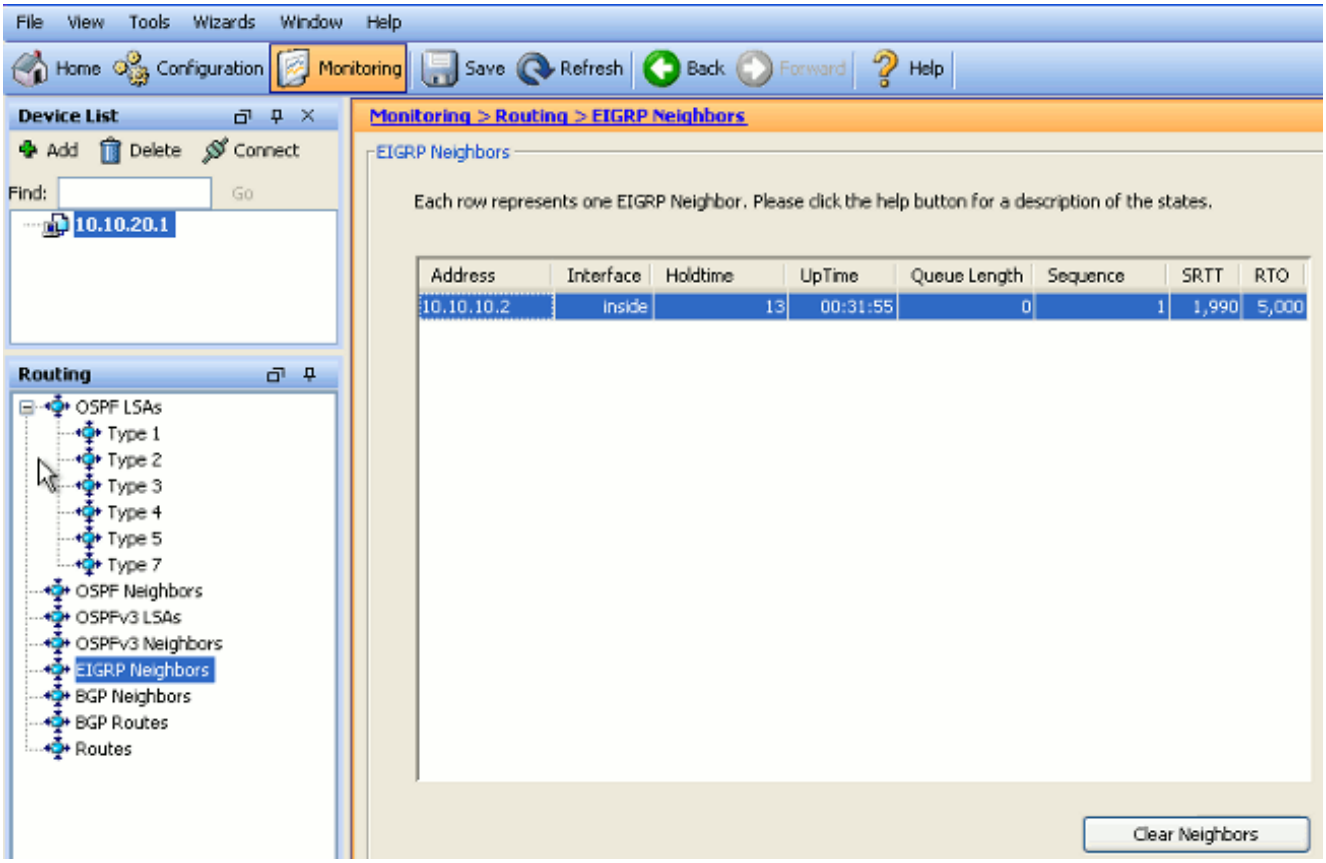
```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

Verificar

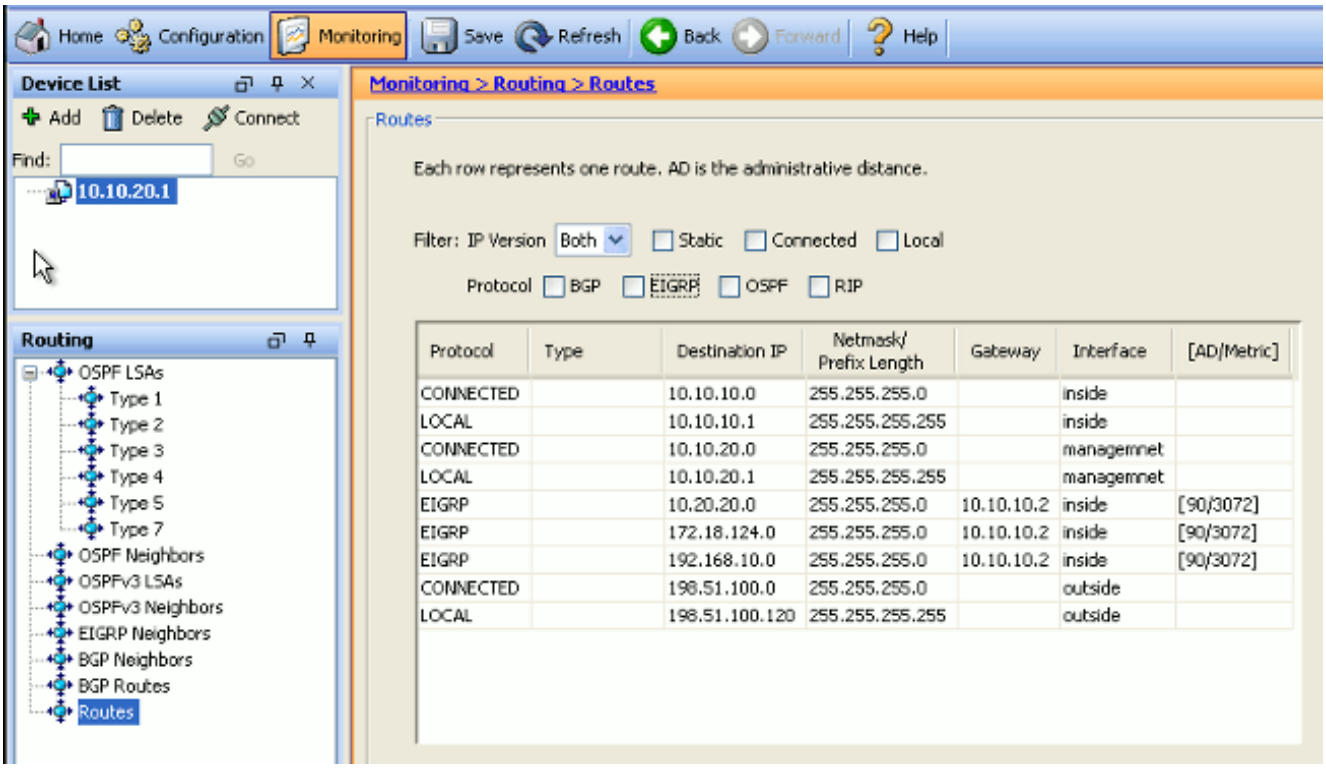
Termine estas etapas a fim verificar sua configuração.

1. No ASDM, você pode navegar à **monitoração > roteamento > vizinho EIGRP** a fim ver cada um dos vizinhos EIGRP. Este tiro de tela mostra o roteador interno (r1) como um vizinho ativo. Você pode igualmente ver a relação de onde este vizinho reside, o holdtime, e de

quanto tempo o relacionamento vizinho foi acima (UpTime).



2. Adicionalmente, você pode verificar a tabela de roteamento se você navega à **monitoração > roteamento > rotas**. Neste tiro de tela, você pode ver que as **192.168.10.0/24, 172.18.124.0/24**, e **10.20.20.0/24** redes são instruídas com o r1 (**10.10.10.2**).



Do CLI, você pode usar o **comando show route** a fim 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 versão ASA 9.2.1 e mais atrasado, você pode usar o **comando eigrp da rota da mostra** a fim indicar somente rotas de 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 pode igualmente usar o comando da **topologia do eigrp da mostra** a fim obter a informação sobre as redes instruídas 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 dos **vizinhos EIGRP da mostra** é igualmente útil a fim verificar os vizinhos ativos e a informação correspondente. Este exemplo mostra a mesma informação que você obteve do ASDM em 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

Está aqui o fluxo de pacote de informação.

1. O ASA vem acima no link e envia um pacote Hello do mcast com todas suas relações EIGRP-configuradas.

2. O r1 recebe um pacote Hello e envia um pacote Hello do 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 de atualização com um jogo do bit inicial, que indique que este é o processo de inicialização.

4. O r1 recebe um pacote de atualização e envia um pacote de atualização com um jogo do bit inicial, que indique que este é o processo de inicialização.

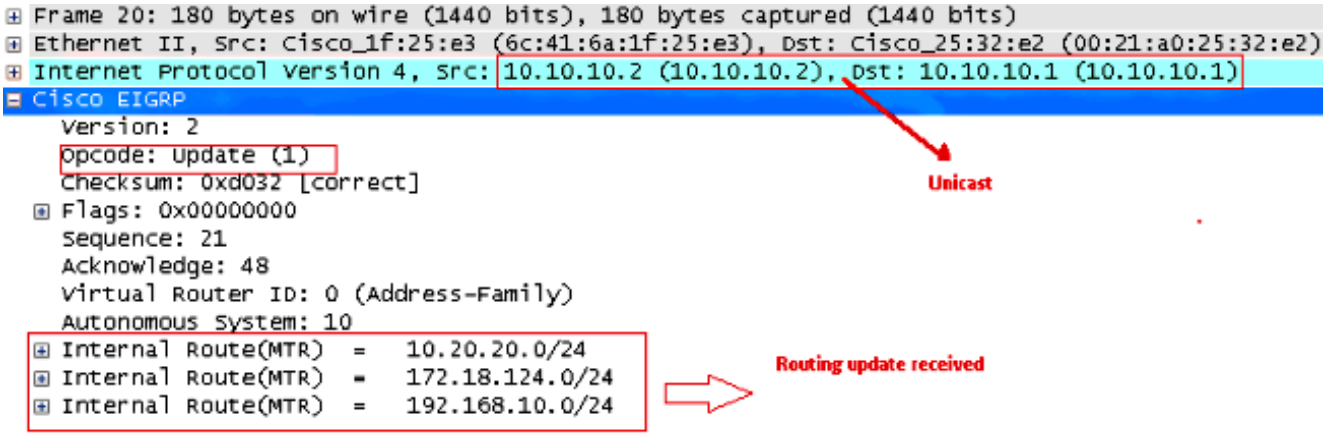
```
⊞ Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Cisco_25:32:e2 (00:21:a0:25:32:e2), Dst: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3)
⊞ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
⊟ Cisco EIGRP
    Version: 2
    Opcode: 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. Após o ASA e o r1 trocaram hellos e a adjacência vizinha é estabelecida, o ASA e resposta do r1 com um pacote de ACK, que indique que a informação de atualização esteve recebida.

6. O ASA envia sua informação de roteamento ao r1 em um pacote de atualização.

7. O r1 introduz a informação do pacote de atualização em sua tabela de topologia. A tabela de topologia inclui todos os destinos anunciados por vizinhos. É organizada de modo que cada destino esteja listado, junto com todos os vizinhos que podem viajar ao destino e a seu medidor associado.

8. O r1 envia então um pacote de atualização ao ASA.



9. Uma vez que recebe o pacote de atualização, o ASA envia um pacote de ACK ao r1. Depois que o ASA e o r1 recebem com sucesso os pacotes de atualização de se, está pronto escolheu as rotas do sucessor (melhor) e do sucessor possível (backup) na tabela de topologia, e oferece as rotas do sucessor à tabela de roteamento.

Troubleshooting

Esta seção inclui a informação sobre os **comandos debug and show** que podem ser úteis a fim pesquisar defeitos problemas EIGRP.

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**. A fim indicar debugar a informação a máquina de estado finito (DUPLA) do algoritmo de atualização em difusão, usam o **comando debug eigrp fsm no** modo de exec privilegiado. Este comando deixa-o observar a atividade do sucessor possível EIGRP e determinar se as atualizações da rota estão instaladas e suprimidas pelo processo de roteamento.

Esta é a saída do **comando debug** dentro de espreitar bem sucedido com r1. Você pode ver cada

um das rotas diferentes que é instalado com sucesso no sistema.

```
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
```

Você pode igualmente usar o comando do **vizinho EIGRP debugar**. Esta é a saída deste **comando debug** quando Cisco ASA criou com sucesso uma relação vizinha nova com o 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 pode igualmente usar os pacotes EIGRP debugar para informação detalhada da troca da mensagem EIGRP entre Cisco ASA e seus pares. Neste exemplo, a chave de autenticação foi mudada no roteador (r1), e o resultado do debug mostra-lhe que o problema é uma má combinação da 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 vai para baixo com Syslog ASA-5-336010

O ASA deixa cair a vizinhança do EIGRP quando todas as mudanças na lista de distribuição EIGRP são feitas. Este mensagem do syslog é considerado.

```
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)
```

Com esta configuração, sempre que uma **entrada acl nova é adicionada no** ACL, a vizinhança do EIGRP da EIGRP-rede-**lista** é restaurada.

```
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)
```

Você pode observar que o relacionamento vizinho está acima 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 o **padrão da EIGRP-rede-lista da lista de acesso nega 172.18.24.0 255.255.255.0**.

```
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
```

Estes logs podem ser considerados no **debug eigrp fsm**.

```
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
```

Este é comportamento esperado em todas as versões ASA novas de 8.4 e 8.6 a 9.1. O mesmo foi observado no Roteadores que executa os 12.4 a 15.1 trens do código. Contudo, este comportamento não é observado na versão ASA 8.2 e em umas versões de software mais adiantadas ASA porque as mudanças feitas a um ACL não restauram as adjacências EIGRP.

Desde que o EIGRP envia a tabela de topologia completa a um vizinho quando o vizinho vem primeiramente acima, e então ele envia somente as mudanças, configurar uma lista da distribuição com a natureza evento-conduzida do EIGRP faria difícil para que as mudanças apliquem-se sem uma restauração completa do relacionamento vizinho. O Roteadores precisaria de manter-se a par de cada rota enviada a e recebida de um vizinho a fim saber que rota mudou (isto é, ou não seria enviado/foi aceitado) a fim aplicar as mudanças como ditado pela corrente distribua a lista. É muito mais fácil rasgar simplesmente para baixo e restabelecer a adjacência entre vizinhos.

Quando uma adjacência é rasgada para baixo e restabelecida, todas as rotas aprendidas entre vizinhos específicos estão esquecidas simplesmente e a sincronização inteira entre os vizinhos é executada de novo - com o novo distribua a lista no lugar.

A maioria das técnicas EIGRP que você usa a fim pesquisar defeitos o Roteadores do Cisco IOS podem ser aplicadas em Cisco ASA. A fim pesquisar defeitos o EIGRP, use o fluxograma de

Troubleshooting principal; comece no **cano principal** marcado caixa.