ASA/PIX com exemplo da configuração RIP

Índice

Introdução

Este documento explica como configurar Cisco ASA a fim aprender rotas com o Routing Information Protocol (RIP), executa a autenticação, e a redistribuição.

Refira PIX/ASA 8.X: Configurando o EIGRP na ferramenta de segurança adaptável de Cisco (ASA) para obter mais informações sobre da configuração de EIGRP.

Nota: Esta configuração do documento é baseada na versão RIP 2.

Nota: O roteamento assimétrico não é apoiado em ASA/PIX.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Cisco ASA/PIX deve executar a versão 7.x ou mais recente.
- O RASGO não é apoiado no modo do multi-contexto; é apoiado somente no modo simples.

Componentes Utilizados

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

- Segurança adaptável Appliance(ASA) do Cisco 5500 Series que executa a versão de software 8.0 e mais atrasado.
- Versão de software adaptável 6.0 de Manager(ASDM) do dispositivo de segurança de Cisco e mais atrasado.

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.

Produtos Relacionados

A informação neste documento é igualmente aplicável ao PIX Firewall do Cisco 500 Series que executa a versão de software 8.0 e mais atrasado.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O RASGO é um protocolo de roteamento de vetor de distância que use o contagem de saltos como a métrica para a seleção de trajeto. Quando o RASGO é permitido em uma relação, o RASGO das trocas da relação transmite com dispositivos confinante a fim aprender dinamicamente aproximadamente e anunciar rotas.

A versão RIP 1 da versão RIP 1 e da versão RIP 2. do apoio da ferramenta de segurança não envia a máscara de sub-rede com a atualização de roteamento. A versão RIP 2 envia a máscara de sub-rede com a atualização de roteamento e apoia máscaras de sub-rede de comprimento variável. Adicionalmente, a versão RIP 2 apoia a autenticação de vizinho quando as atualizações de roteamento são trocadas. Esta autenticação assegura-se de que a ferramenta de segurança receba a informação de roteamento segura de um origem confiável.

Limitações:

1. A ferramenta de segurança não pode passar atualizações do RASGO entre relações.
2. A versão RIP 1 não apoia as máscaras de sub-rede de comprimento variável (VLS).
3. O RASGO tem uma contagem do salto máximo de 15. Uma rota com um contagem de saltos maior de 15 é considerada inacessível.
4. A convergência do RASGO é relativamente lenta comparada a outros protocolos de

roteamento.

5. Você pode somente permitir um único processo do RASGO na ferramenta de segurança.

Nota: Esta informação aplica-se à versão RIP 2 somente:

1. Se você usa a autenticação de vizinho, a chave de autenticação e a chave ID devem ser a mesma em todos os dispositivos vizinho que fornecem atualizações da versão RIP 2 à relação.
2. Com versão RIP 2, a ferramenta de segurança transmite e recebe atualizações da rota padrão com o uso do endereço de multicast 224.0.0.9. No modo passivo, recebe atualizações da rota nesse endereço.
3. Quando a versão RIP 2 é configurada em uma relação, o endereço de multicast 224.0.0.9 está registrado nessa relação. Quando uma configuração da versão RIP 2 é removida de uma relação, esse endereço de multicast está removido registro.

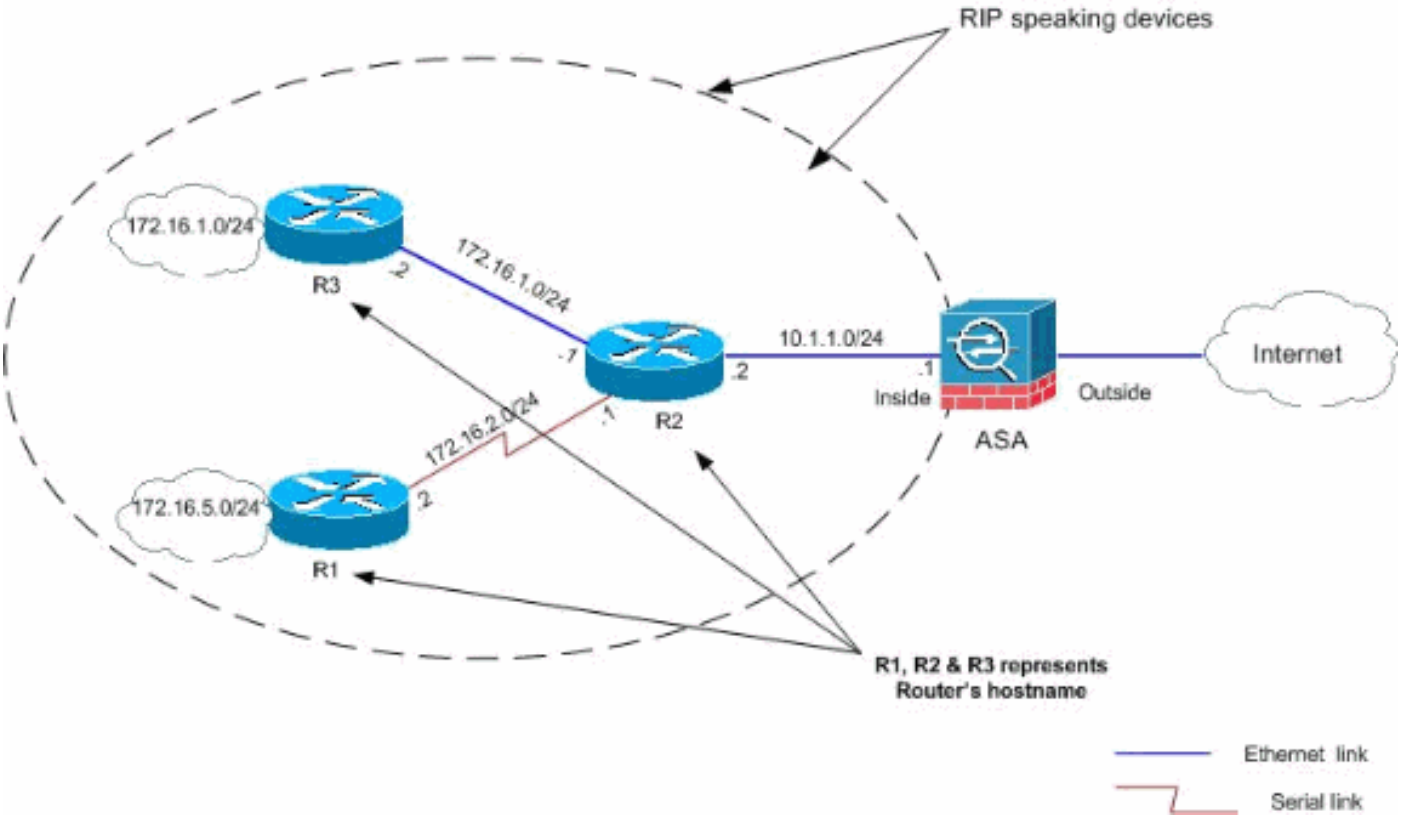
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: 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:



Configurações

Este documento utiliza as seguintes configurações:

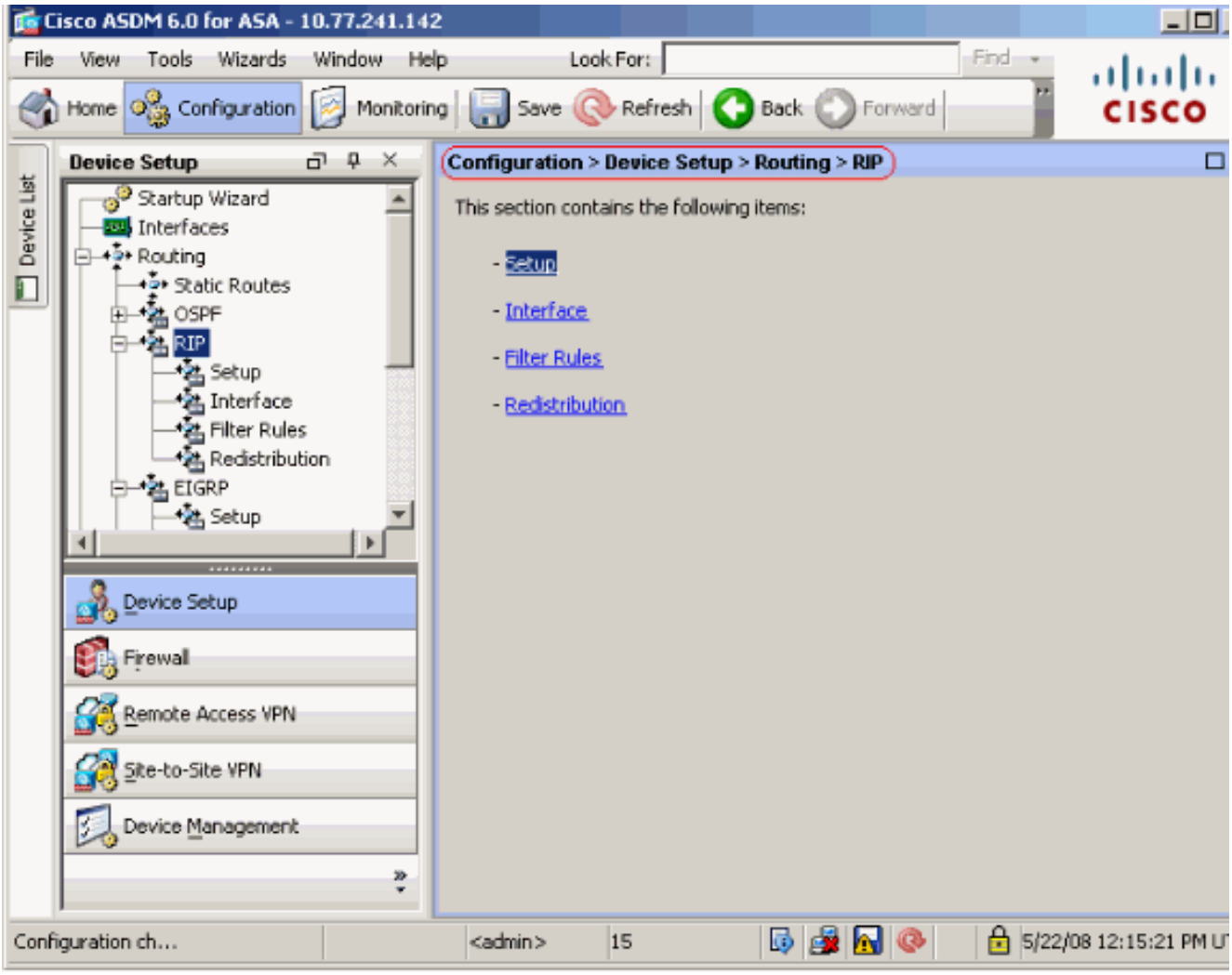
- Configuração ASDM
- Configurar a autenticação do RASGO
- Configuração de CLI de Cisco ASA
- Configuração de CLI do roteador do Cisco IOS (R2)
- Configuração de CLI do roteador do Cisco IOS (r1)
- Configuração de CLI do roteador do Cisco IOS (R3)

Configuração ASDM

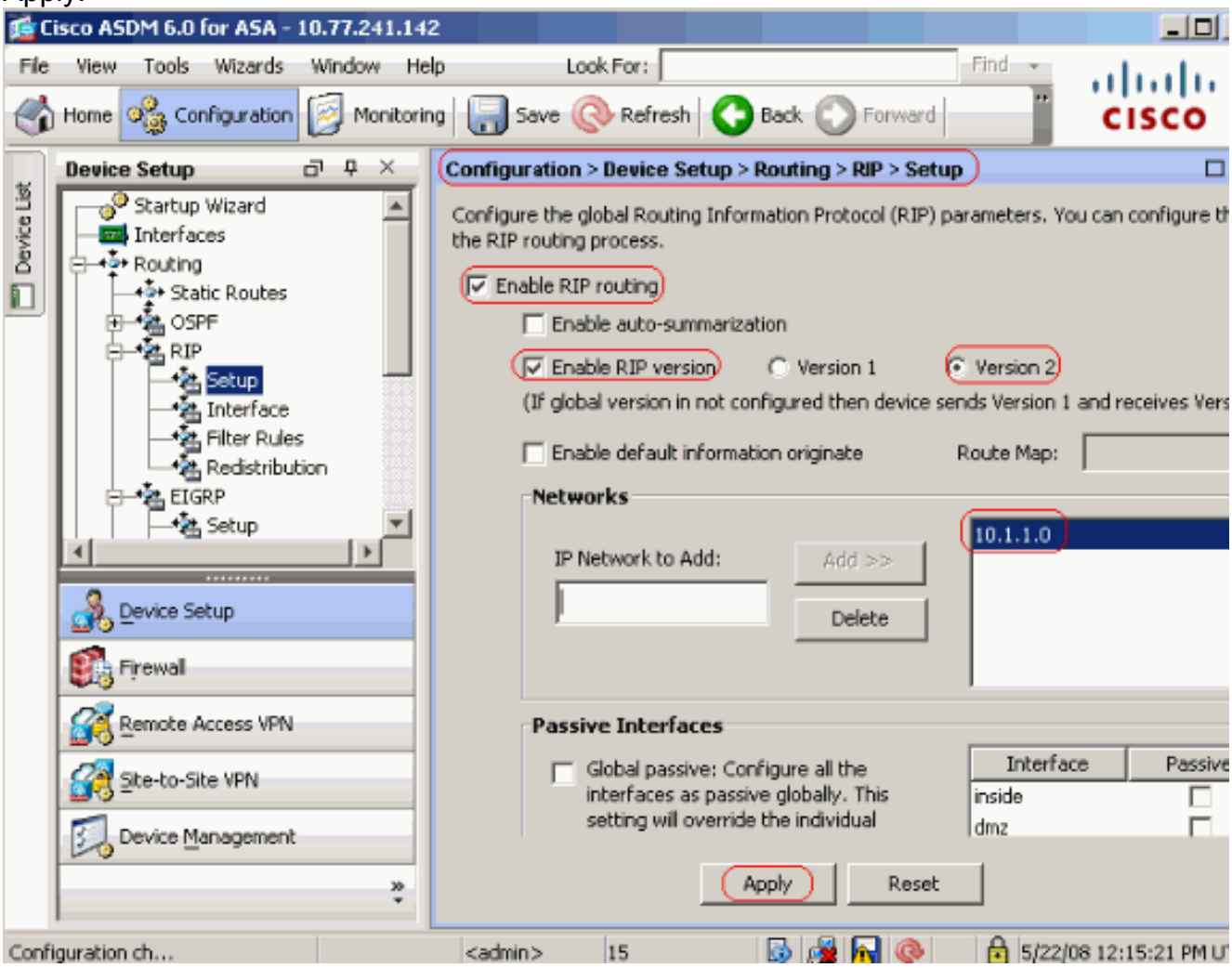
O Security Device Manager adaptável (ASDM) é um aplicativo baseado em navegador usado a fim configurar e monitorar o software em ferramentas de segurança. O ASDM é carregado da ferramenta de segurança, e usado então para configurar, monitorar, e controlar o dispositivo. Você pode igualmente usar a launcher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

Termine estas etapas a fim configurar o RASGO em Cisco ASA:

1. Entre a Cisco ASA com ASDM.
2. Escolha a **configuração > a instalação > o roteamento > o RASGO de dispositivo na** relação ASDM, segundo as indicações do tiro de tela.



3. Escolha a **configuração > a instalação > o roteamento > o RASGO de dispositivo > Setup** a fim permitir o RASGO que distribui como mostrado.Escolha a caixa de verificação **permitem o roteamento do RASGO**.Escolha a caixa de verificação **permitem a versão RIP** com **versão 2 do** botão de rádio.Sob **redes** catalogue, adicionar a rede **10.1.1.0**.Clique em Apply.



CamposPermita o roteamento do RASGO — Verifique esta ordem do inb da caixa de verificação para permitir o roteamento do RASGO na ferramenta de segurança. Quando você permite o RASGO, está permitido em todas as relações. Se você verifica esta caixa de verificação, esta igualmente permite os outros campos nesta placa. Desmarcar esta caixa de verificação a fim desabilitar o roteamento do RASGO na ferramenta de segurança.Permita o resumo automático — Cancele esta caixa de verificação a fim desabilitar a sumarização de rota automática. Verifique esta caixa de verificação a fim reenable a sumarização de rota automática. A versão RIP 1 usa sempre a sumarização automática. Você não pode desabilitar a sumarização automática para a versão RIP 1. Se você usa a versão RIP 2, você pode desligar a sumarização automática se você desmarca esta caixa de verificação. Desabilite a sumarização automática se você deve executar o roteamento entre sub-redes desligado. Quando a sumarização automática é desabilitada, as sub-redes estão anunciadas.Permita a versão RIP — Verifique esta caixa de verificação a fim especificar a versão do RASGO usada pela ferramenta de segurança. Se esta caixa de verificação é cancelada, a seguir a ferramenta de segurança envia a versão RIP 1 atualiza e aceita atualizações da versão RIP 1 e da versão 2. Este ajuste pode ser cancelado em uma base da interface per. na placa da relação.Versão 1 — Especifica que a ferramenta de segurança somente envia e recebe atualizações da versão RIP 1. Todas as atualizações da versão 2

recebidas são deixadas cair.Versão 2 — Especifica que a ferramenta de segurança somente envia e recebe a versão RIP 2 atualizações. Todas as atualizações da versão 1 recebidas são deixadas cair.Permita a informação do padrão originam — Verifique esta caixa de verificação a fim gerar uma rota padrão no processo de roteamento do RASGO. Você pode configurar um mapa de rota que deva ser satisfeito antes que a rota padrão possa ser gerada.Mapa de rotas — Dê entrada com o nome do mapa de rota a fim aplicar-se. O processo de roteamento gerencie a rota padrão se o mapa de rota é satisfeito.Rede IP a adicionar — Define uma rede para o processo de roteamento do RASGO. O network number especificado não deve conter nenhuma informação de sub-rede. Não há nenhum limite ao número de rede que você pode adicionar à configuração da ferramenta de segurança. As atualizações de roteamento do RASGO são enviadas e recebidas somente através das relações nas redes especificadas. Também, se a rede de uma relação não é especificada, a relação não é anunciada em nenhuma atualizações do RASGO.Adicionar — Clique este botão a fim adicionar a rede especificada à lista de rede.Supressão — Clique este botão a fim remover a rede selecionada da lista de redeConfigurar relações como a voz passiva globalmente — Verifique esta caixa de verificação para ajustar todas as relações na ferramenta de segurança ao modo passivo do RASGO. A ferramenta de segurança escutam transmissões do roteamento do RASGO em todas as relações e os usos que a informação para povoar as tabelas de roteamento mas não transmite atualizações de roteamento. Use a tabela das interfaces passivas a fim ajustar relações específicas ao RASGO passivo.Tabela das interfaces passivas — Alista as interfaces configuradas na ferramenta de segurança. Verifique a caixa de verificação na coluna passiva para ver se há aquelas relações que você quer se operar no modo passivo. As outras relações ainda enviam e recebem transmissões do RASGO.

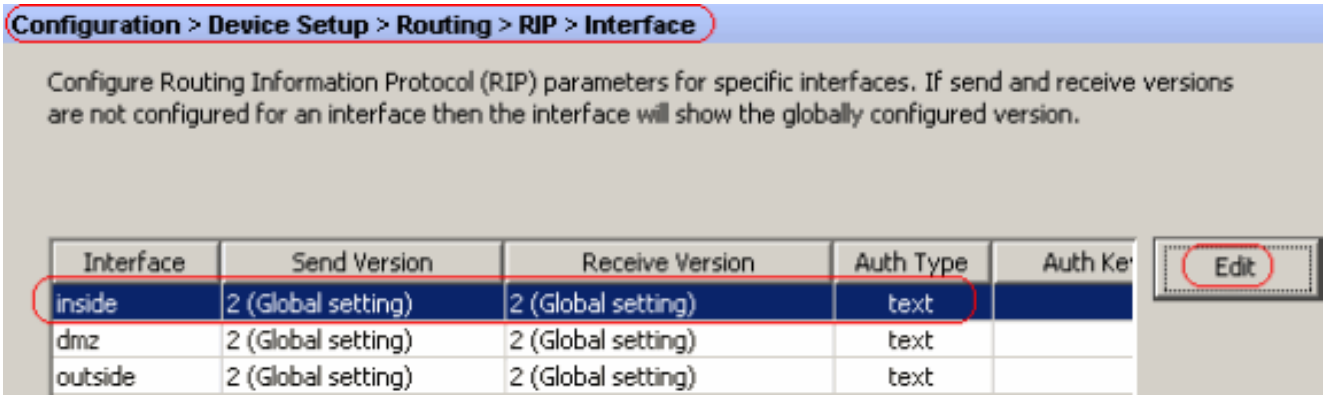
Configurar a autenticação do RASGO

Cisco ASA apoia a autenticação md5 das atualizações de roteamento do protocolo de roteamento do RIP v2. O resumo fechado MD5 em cada pacote RIP impede a introdução de mensagens de roteamento desautorizados ou falsos das fontes unapproved. A adição de autenticação a suas mensagens do RASGO 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 você 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 adiciona a autenticação às mensagens do RASGO enviadas entre seus dispositivos de roteamento, que inclui o ASA, impede a adição decidido ou acidental de um outro roteador à rede e a todo o problema.

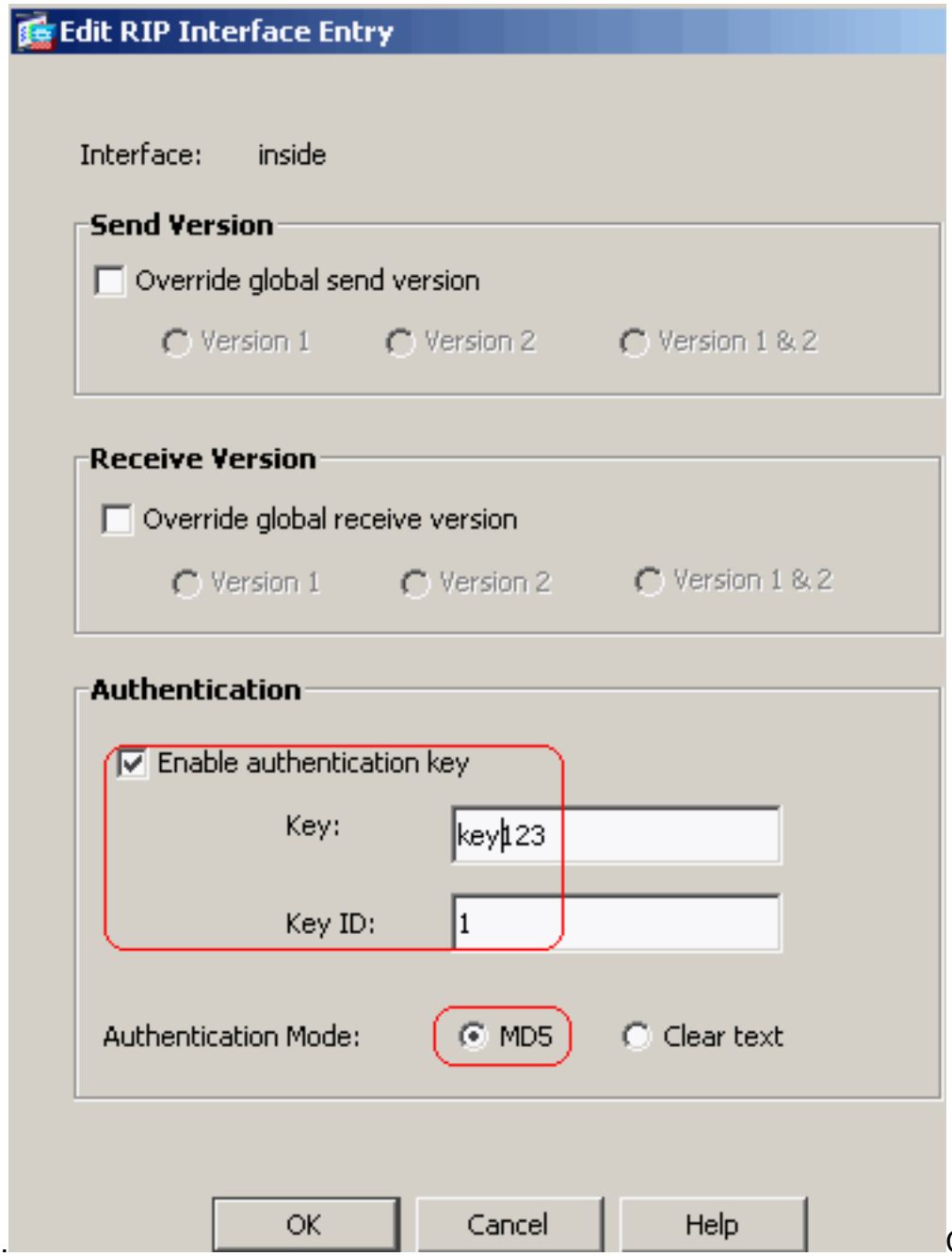
A autenticação da rota RIP é configurada em uma base da interface per. Todos RASGAM vizinhos nas relações configuradas para a autenticação de mensagem do RASGO devem ser configurados com o mesmos modo de autenticação e chave.

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

1. No ASDM, escolha a **configuração > a instalação > o roteamento > o RASGO > a relação de dispositivo** e escolha a interface interna com o rato. O clique **edita**.



2. Escolha a caixa de seleção da **chave de autenticação da possibilidade** e incorpore então o valor do **valor chave** e o **chave**



ID. Clique em **OK** e, em seguida, em **Apply**.

Configuração de CLI de Cisco ASA

Cisco ASA

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! !--- Inside interface
configuration interface Ethernet0/1 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !--
- RIP authentication is configured on the inside
interface. rip authentication mode md5 rip
authentication key <removed> key_id 1 ! !--- Output
Suppressed !--- Outside interface configuration
interface Ethernet0/2 nameif outside security-level 0 ip
address 192.168.1.2 255.255.255.0 !--- RIP Configuration
router rip network 10.0.0.0 version 2 !--- This is the
static default gateway configuration in !--- order to
reach the Internet. route outside 0.0.0.0 0.0.0.0
192.168.1.1 1
```

Configuração de CLI do roteador do Cisco IOS (R2)

Roteador do Cisco IOS (R2)

`interface Ethernet0`
` ip address 10.1.1.2 255.255.255.0`
` ip rip authentication mode md5 ip rip authentication key-chain 1 ! router rip version 2 network 10.0.0.0 network 172.16.0.0 no auto-summary`

Configuração de CLI do roteador do Cisco IOS (r1)

Roteador do Cisco IOS (r1)
`router rip version 2 network 172.16.0.0 no auto-summary`

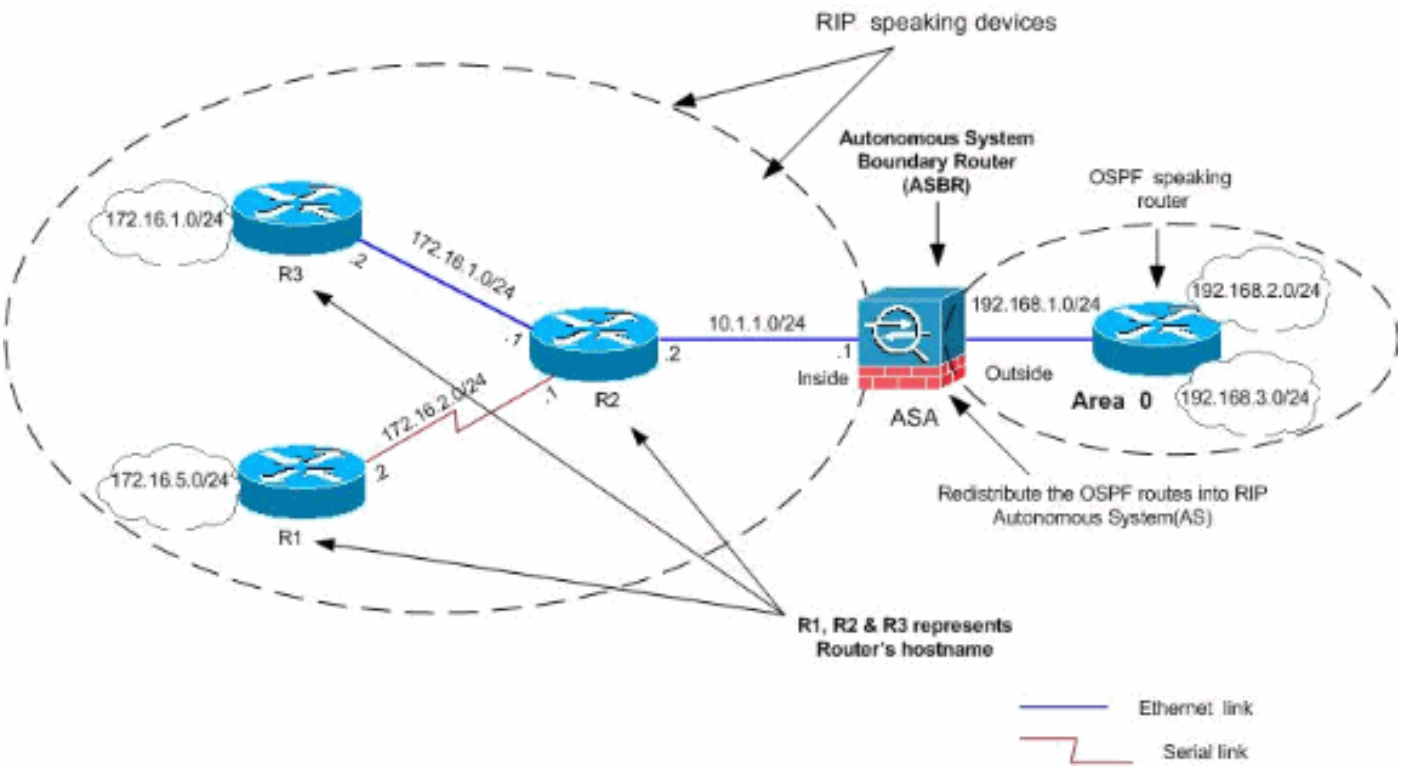
Configuração de CLI do roteador do Cisco IOS (R3)

Roteador do Cisco IOS (R3)
`router rip version 2 network 172.16.0.0 no auto-summary`

Redistribua no RASGO com ASA

Você pode redistribuir rotas do OSPF, do EIGRP, da estática, e dos processos de roteamento conectados no processo de roteamento do RASGO.

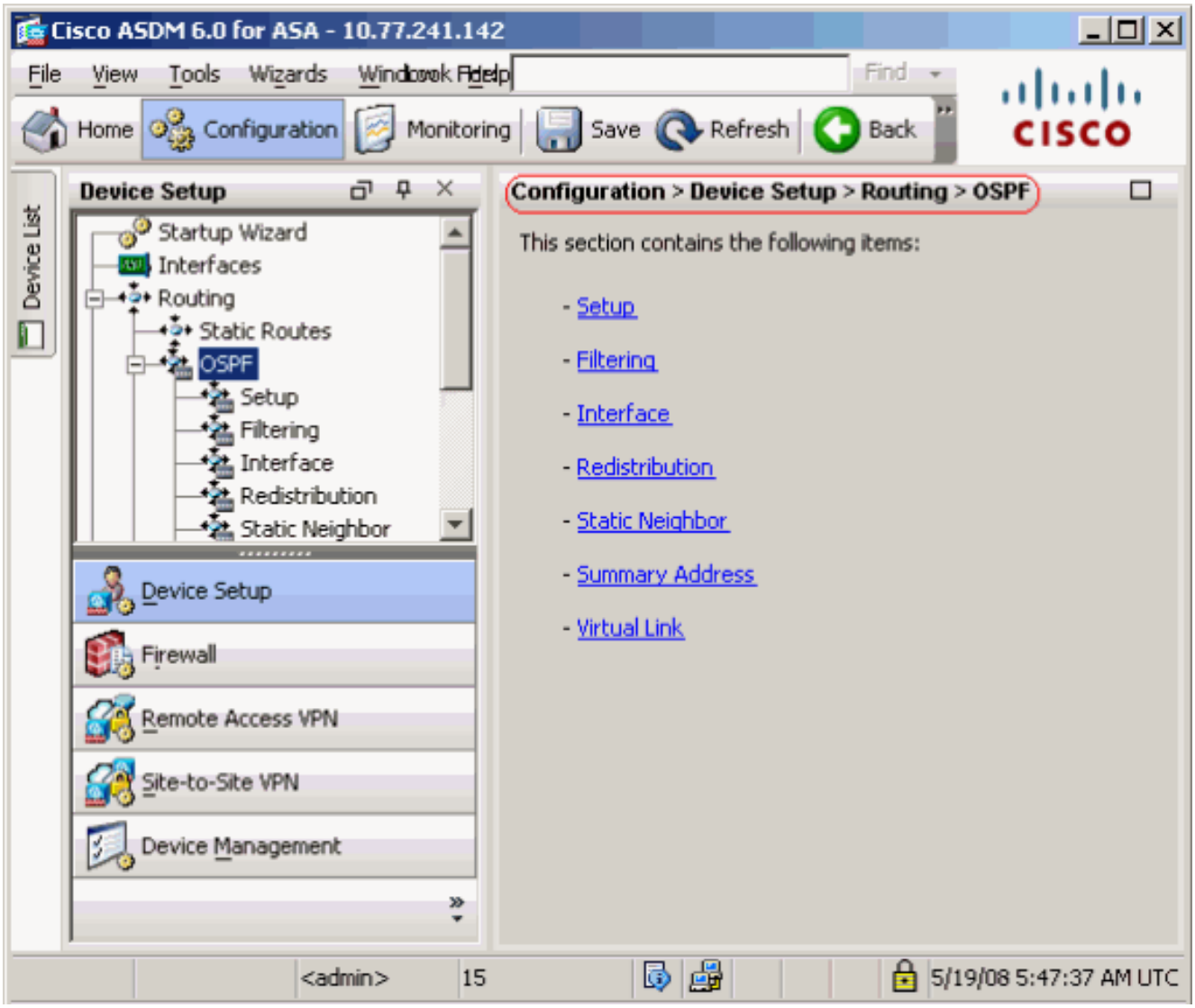
Neste exemplo, a redistribuição das rotas de OSPF no RASGO com o diagrama da rede é mostrada:



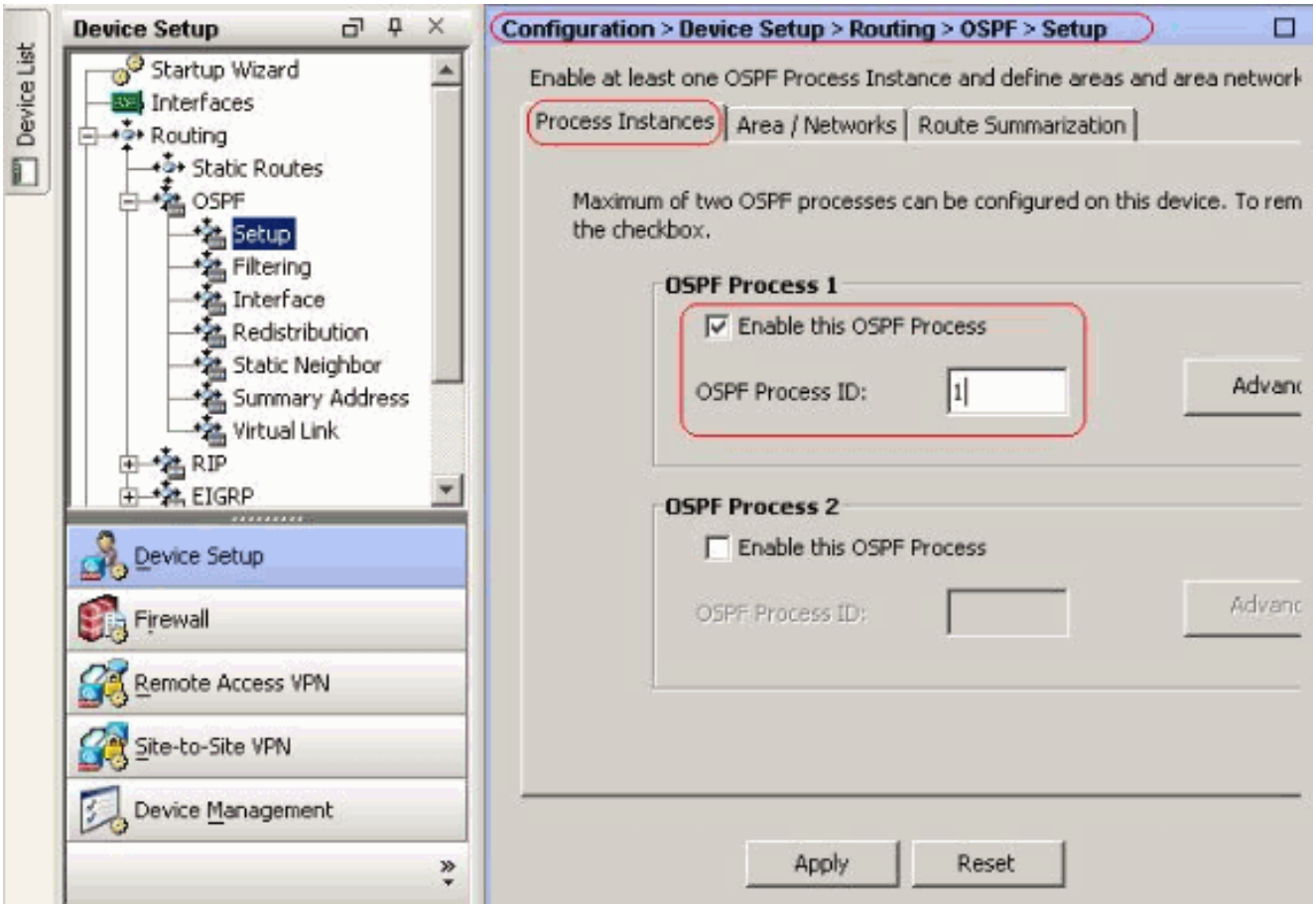
Configuração ASDM

Conclua estes passos:

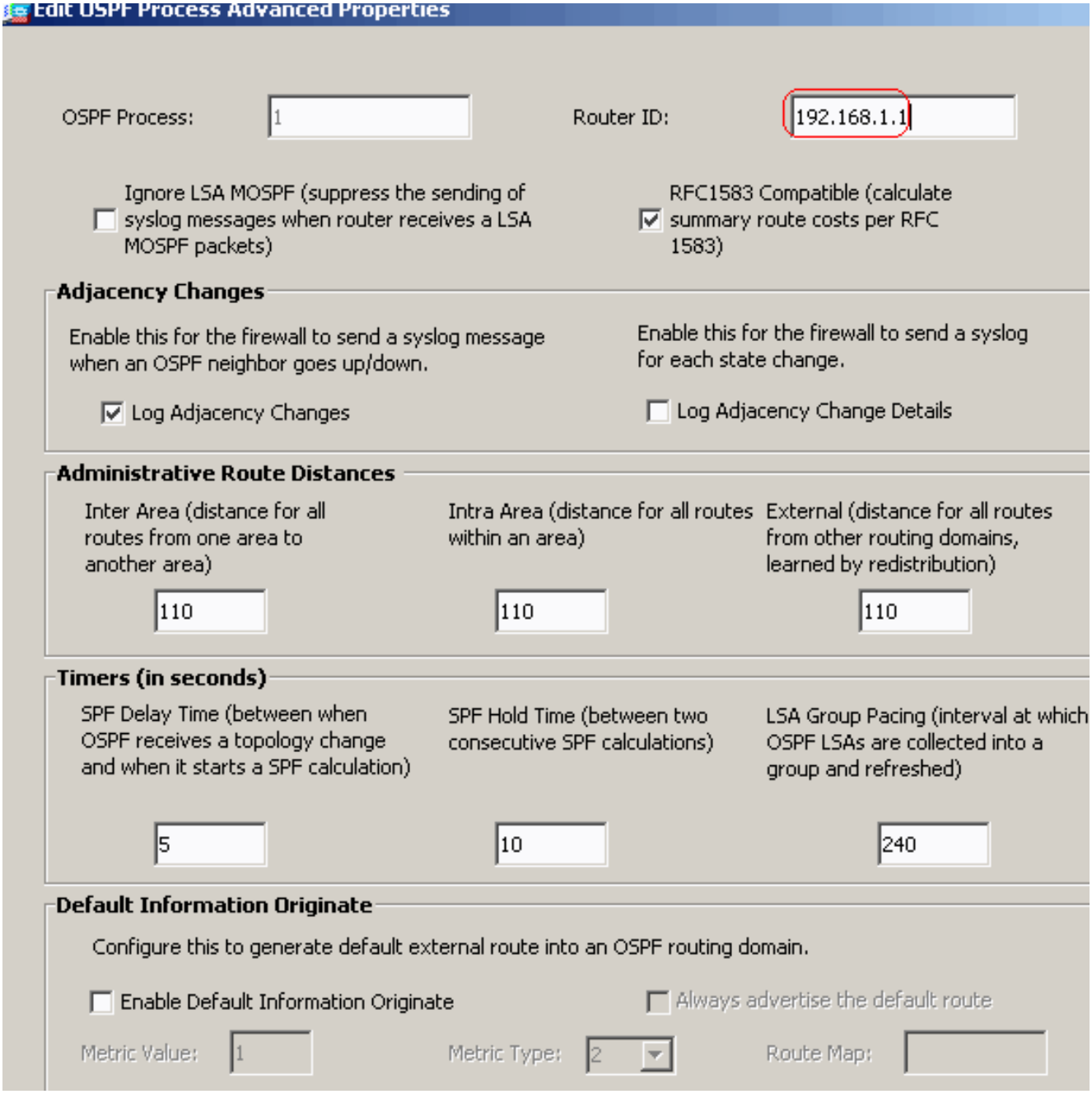
1. **Configuração de OSPF**Escolha a **configuração > a instalação > o roteamento > o OSPF de dispositivo na** relação ASDM, segundo as indicações do tiro de tela.



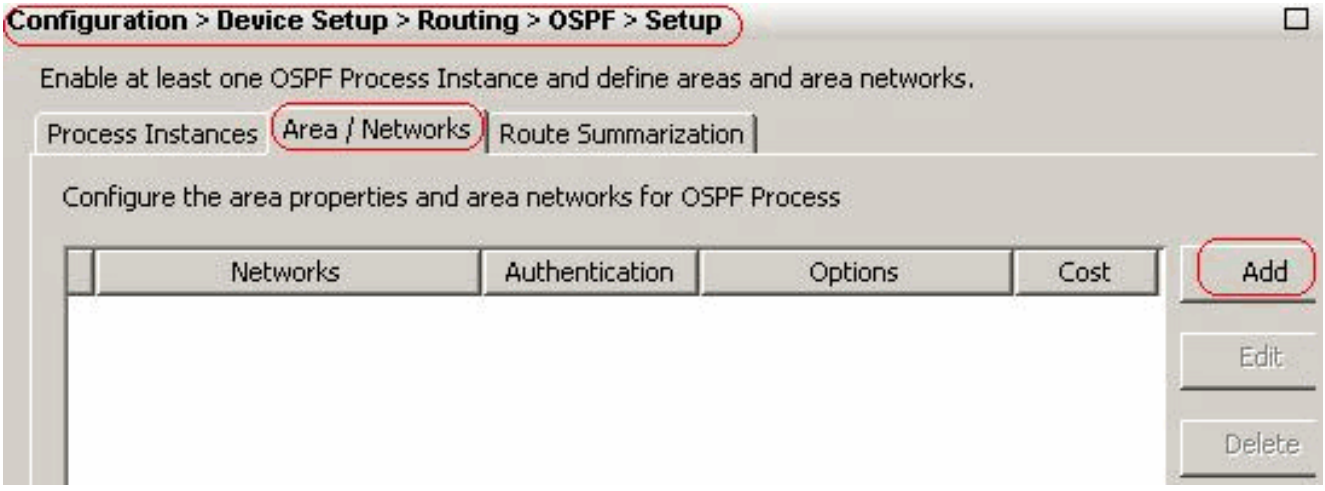
Permita o processo de roteamento OSPF na aba dos **exemplos da instalação > do processo**, segundo as indicações do tiro de tela. Neste exemplo, o processo OSPF ID é **1.**



O clique **avançado na instalação > no processo cita como exemplo a** aba a fim configurar parâmetros de processo de roteamento OSPF avançados opcionais. Você pode editar ajustes processo-específicos, tais como o Router ID, mudanças da adjacência, distâncias administrativas da rota, temporizadores, e a informação do padrão origina ajustes.

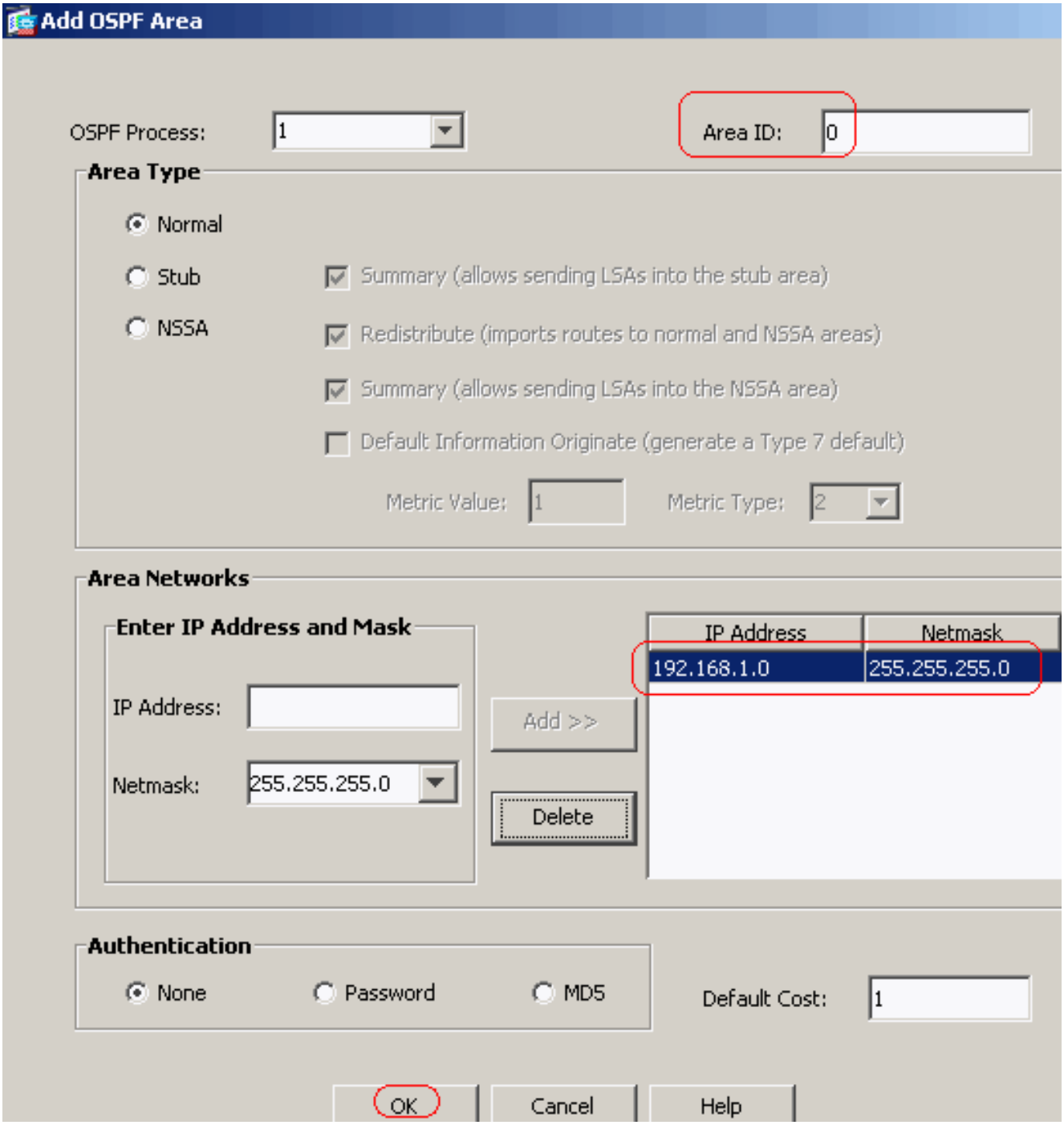


Clique em **OK**.Depois que você termina as etapas precedentes, defina as redes e as relações que participam no roteamento OSPF aba nos **/Networks da instalação > da área**. O clique **adiciona** segundo as indicações deste tiro de tela.

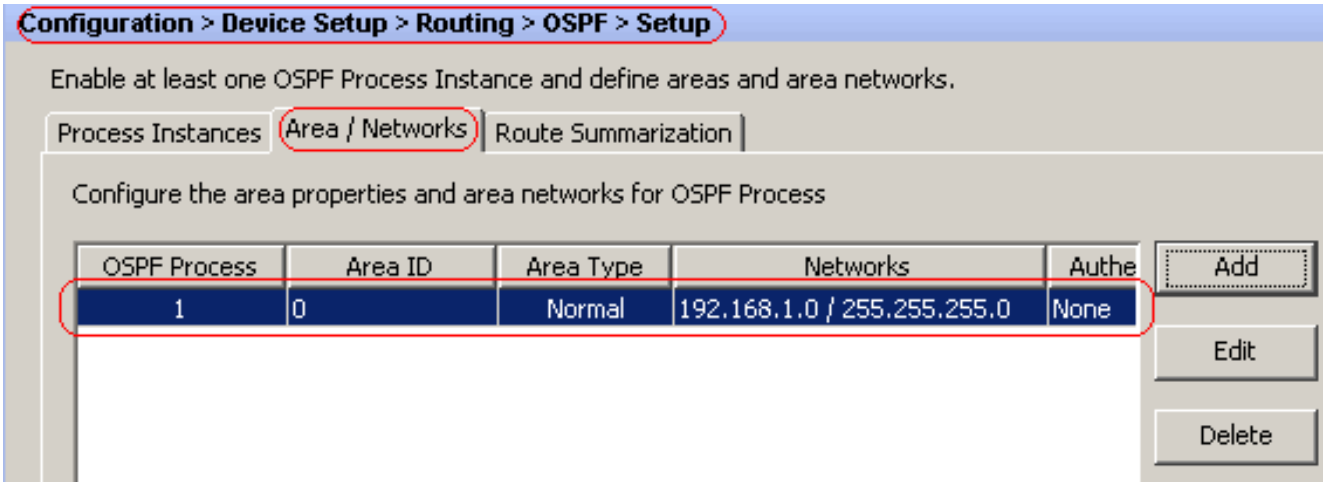


Esta tela aparece. Neste exemplo, a única rede que nós adicionamos é a rede externa

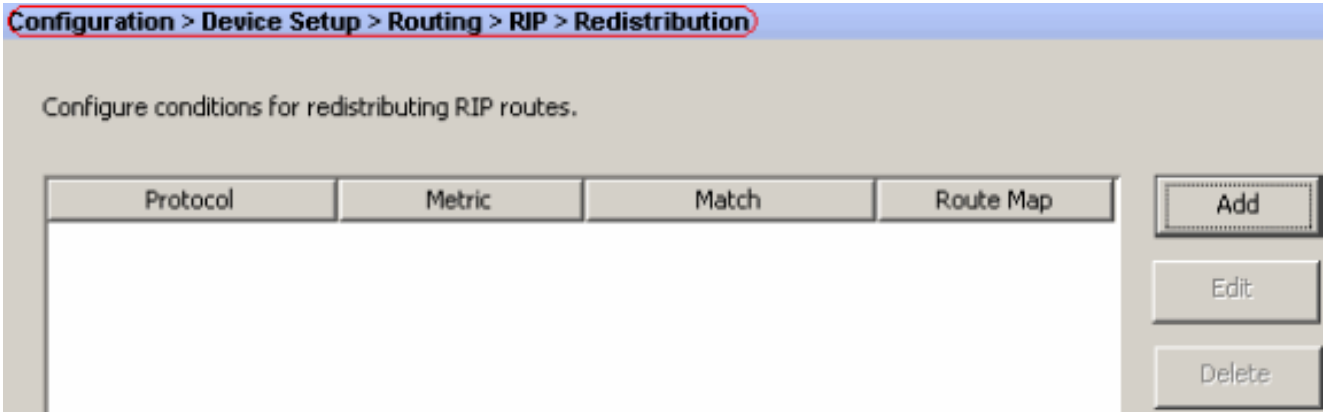
(192.168.1.0/24) desde que o OSPF é permitido somente na interface externa.**Nota:** Conecta somente com um endereço IP de Um ou Mais Servidores Cisco ICM NT que cai dentro das redes definidas participa no processo de roteamento
OSPF.



Clique em **OK**.Clique em
Apply.

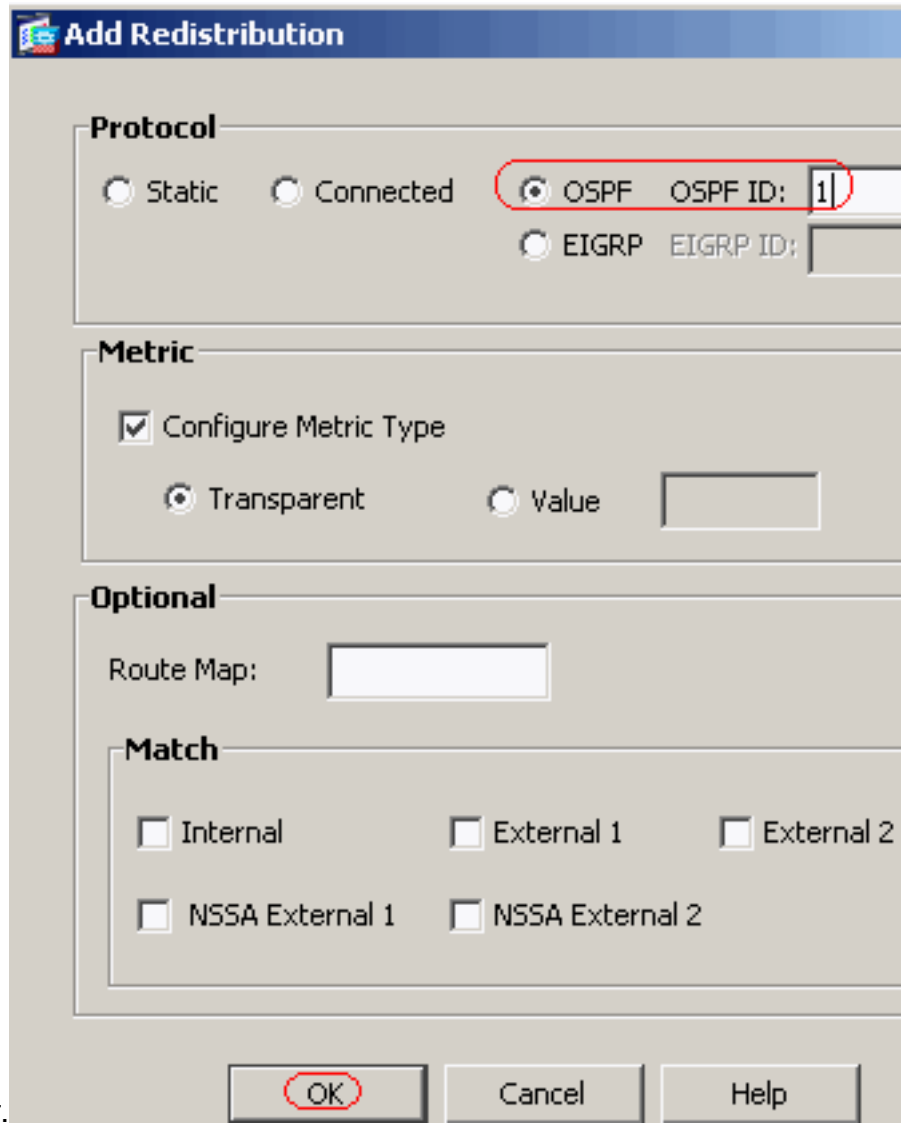


2. Escolha o **> Add da instalação da configuração > de dispositivo > do roteamento > do RASGO > da redistribuição** a fim redistribuir rotas de OSPF no RASGO.



3. Clique em **OK** e, em seguida, em

Apply.



Configuração de CLI equivalente

A configuração de CLI do ASA para redistribui o OSPF no RASGO COMO
router rip network 10.0.0.0 **redistribute ospf 1 metric transparent** version 2 ! router ospf 1 router-id 192.168.1.1 network 192.168.1.0 255.255.255.0 area 0 area 0 log-adj-changes

Você pode ver a tabela de roteamento do Cisco IOS vizinho Router(R2) após ter redistribuído rotas de OSPF no RASGO COMO.

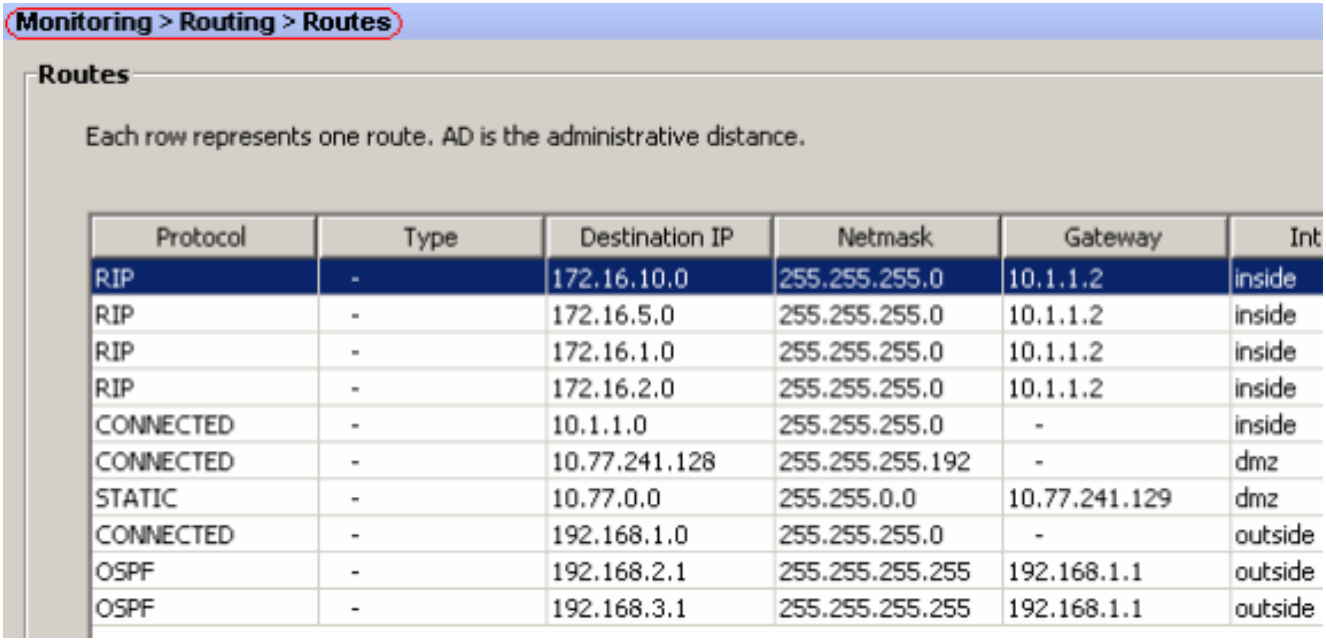
R2#**show ip route** Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, su - IS-IS 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 Gateway of last resort is not set 172.16.0.0/24 is subnetted, 4 subnets R 172.16.10.0 [120/1] via 172.16.1.2, 00:00:25, Ethernet1 R 172.16.5.0 [120/1] via 172.16.2.2, 00:00:20, Serial1 C 172.16.1.0 is directly connected, Ethernet1 C 172.16.2.0 is directly connected, Serial1 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C 10.1.1.0/24 is directly connected, Ethernet0 R 10.77.241.128/26 [120/1] via 10.1.1.1, 00:00:06, Ethernet0 **R 192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:05, Ethernet0 192.168.2.0/32 is subnetted, 1 subnets R 192.168.2.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0 192.168.3.0/32 is subnetted, 1 subnets R 192.168.3.1 [120/12]**

```
via 10.1.1.1, 00:00:05, Ethernet0 !--- Redistributed route advertised by Cisco ASA
```

Verificar

Termine estas etapas a fim verificar sua configuração:

1. Você pode verificar a tabela de roteamento se você navega à **monitoração > roteamento > rotas**. Neste tiro de tela, você pode ver que as 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 e 172.16.10.0/24 redes são instruídas com R2 (10.1.1.2) com RASGO.



Protocol	Type	Destination IP	Netmask	Gateway	Int
RIP	-	172.16.10.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.5.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.2.0	255.255.255.0	10.1.1.2	inside
CONNECTED	-	10.1.1.0	255.255.255.0	-	inside
CONNECTED	-	10.77.241.128	255.255.255.192	-	dmz
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dmz
CONNECTED	-	192.168.1.0	255.255.255.0	-	outside
OSPF	-	192.168.2.1	255.255.255.255	192.168.1.1	outside
OSPF	-	192.168.3.1	255.255.255.255	192.168.1.1	outside

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 not set R 172.16.10.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside R 172.16.5.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside R 172.16.1.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside R 172.16.2.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside C 10.1.1.0 255.255.255.0 is directly connected, inside C 10.77.241.128 255.255.255.192 is directly connected, dmz S 10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz C 192.168.1.0 255.255.255.0 is directly connected, outside O 192.168.2.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside O 192.168.3.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside ciscoasa#`

Troubleshooting

Esta seção inclui a informação sobre os comandos debug que podem ser úteis pesquisar defeitos problemas OSPF.

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **debugar eventos do rasgo** — Permite a eliminação de erros de eventos do RASGO`ciscoasa#`**`debug rip events`** `rip_route_adjust for inside coming up RIP: sending request on inside to 224.0.0.9 RIP: received v2 update from 10.1.1.2 on inside 172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops RIP: Update contains 4 routes RIP: received v2 update from 10.1.1.2 on inside 172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops RIP: Update contains 4 routes RIP: sending v2 flash update to 224.0.0.9 via dmz (10.77.241.142) RIP: build flash update entries 10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0 172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 RIP: Update contains 5 routes RIP: Update queued RIP: sending v2 flash update to 224.0.0.9 via inside (10.1.1.1) RIP: build flash update entries - suppressing null update RIP: Update sent via dmz rip-len:112 RIP: sending v2 update to 224.0.0.9 via dmz (10.77.241.142) RIP: build update entries 10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0 172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0 192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 RIP: Update contains 8 routes RIP: Update queued RIP: sending v2 update to 224.0.0.9 via inside (10.1.1.1) RIP: build update entries 10.77.241.128 255.255.255.192 via 0.0.0.0, metric 1, tag 0 192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0 192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 RIP: Update contains 4 routes RIP: Update queued RIP: Update sent via dmz rip-len:172 RIP: Update sent via inside rip-len:92 RIP: received v2 update from 10.1.1.2 on inside 172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops RIP: Update contains 4 routes`

Informações Relacionadas

- Página de Suporte do Cisco 5500 Series Adaptive Security Appliance
- Página do suporte de PIX do Cisco 500 Series
- PIX/ASA 8.X: Configurando o EIGRP na ferramenta de segurança adaptável de Cisco (ASA)
- Suporte Técnico e Documentação - Cisco Systems