

ASA/PIX com exemplo da configuração de OSPF

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração ASDM](#)

[Configurar a autenticação OSPF](#)

[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 \(R3\)](#)

[Redistribua no OSPF com ASA](#)

[Verificar](#)

[Troubleshooting](#)

[Configuração do vizinho estático para a rede Point-to-Point](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como configurar o Cisco ASA para aprender rotas pelo Open Shortest Path First (OSPF), executar 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 a configuração de EIGRP.

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 OSPF 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:

- A ferramenta de segurança adaptável do Cisco 5500 Series (ASA) essa executa a versão de software 8.0 e mais atrasado
- Versão de software 6.0 do Cisco Adaptive Security Device Manager (ASDM) 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

OSPF usa um algoritmo de estado do enlace para criar e calcular o caminho mais curto para todos os destinos conhecidos. Cada roteador em uma área do OSPF contém uma base de dados de link-state idêntica, que seja uma lista de cada um das relações e dos vizinhos de alcançável úteis do roteador.

As vantagens do OSPF sobre o RASGO incluem:

- As atualizações do base de dados de estado de link OSPF são enviadas a menos frequentemente do que RASGAM as atualizações, e a base de dados de link-state está atualizada imediatamente um pouco do que gradualmente enquanto a informação antiga é cronometrada para fora.
- As decisões de roteamento são baseadas no custo, que é uma indicação das despesas gerais exigidas para enviar pacotes através de uma determinada interface. A ferramenta de segurança calcula o custo de uma relação baseada na largura de banda de enlace um pouco do que o número de saltos ao destino. O custo pode ser configurado para especificar caminhos preferidos.

A desvantagem de primeiros algoritmos do caminho mais curto é que exigem muitos ciclos de CPU e memória.

A ferramenta de segurança pode executar dois processos de protocolo de OSPF

simultaneamente, em grupos diferentes de relações. Você pôde querer executar dois processos se você tem as relações que usam os mesmos endereços IP de Um ou Mais Servidores Cisco ICM NT (o NAT permite que estas relações coexistam, mas o OSPF não permite endereços de sobreposição). Ou você pôde querer executar um processo no interior, e outro na parte externa, e redistribui um subconjunto das rotas entre os dois processos. Similarmente, você pôde precisar de segregar endereços privados dos endereços públicos.

Você pode redistribuir rotas em um processo de roteamento OSPF de um outro processo de roteamento OSPF, um processo de roteamento do RASGO, ou da estática e das rotas conectadas configuradas em relações OSPF-permitidas.

A ferramenta de segurança apoia estas características OSPF:

- Apoio do intra-área, da inter-área, e (tipo I e tipo II) de rotas externas.
- Apoio de um enlace virtual.
- Inundação OSPF LSA.
- Autenticação aos pacotes de OSPF (senha e autenticação md5).
- Apoio para configurar a ferramenta de segurança como um roteador designado ou um roteador de backup designado. A ferramenta de segurança igualmente pode ser estabelecida um ABR. Contudo, a capacidade para configurar a ferramenta de segurança como um ASBR é limitada para optar pela informação somente (por exemplo, injetando uma rota padrão).
- Apoio para áreas de stub e Not-So-Stubby Areas.
- Filtração do roteador type-3 LSA do limite de área.

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:

Nesta topologia de rede, o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface interna de Cisco ASA é 10.1.1.1/24. O objetivo é configurar o OSPF em Cisco ASA a fim aprender dinamicamente rotas às redes internas (172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 e 172.16.10.0/24) através do roteador adjacente (R2). O R2 aprende as rotas às redes internas remotas através de outro dois Roteadores (r1 e R3).

Configurações

Este documento utiliza as seguintes configurações:

- [Configuração ASDM](#)
- [Configurar a autenticação OSPF](#)
- [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 \(R3\)](#)
- [Redistribua no OSPF com ASA](#)

Configuração ASDM

O Security Device Manager adaptável (ASDM) é um aplicativo baseado em navegador usado para 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 OSPF em Cisco ASA:

1. Entre a Cisco ASA com ASDM.
2. Navegue à **configuração > à instalação > ao roteamento > à área do OSPF de dispositivo da relação ASDM**, segundo as indicações desta imagem.
3. Permita o processo de roteamento OSPF na aba dos **exemplos da instalação > do processo**, segundo as indicações desta imagem. Neste exemplo, o processo OSPF ID é 1.
4. Você pode clicar **avançado na** aba dos **exemplos da instalação > do processo** 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 original ajustes. Esta lista descreve cada campo:
 - Processo de OSPF — Indica o processo de OSPF que você está configurando. Você não pode mudar este valor.
 - Router ID — A fim usar um Router ID fixo, incorpore um Router ID ao formato de endereço IP no campo de ID de roteador. Se você deixa esta placa do valor, o endereço IP de Um ou Mais Servidores Cisco ICM NT o mais de nível elevado na ferramenta de segurança está usado como o Router ID. Neste exemplo, o Router ID é configurado estaticamente com o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface interna (10.1.1.1).
 - Ignore LSA MOSPF — Verifique esta caixa de verificação a fim suprimir a emissão dos mensagens de Log de sistema quando a ferramenta de segurança recebe o tipo pacotes LSA 6 (MOSPF). Este ajuste é desmarcado à revelia.
 - RFC 1583 compatível — Verifique esta caixa de verificação a fim calcular custos da rota sumária pelo RFC 1583. Desmarcar esta caixa de verificação a fim calcular custos da rota sumária pelo RFC 2328. A fim minimizar a possibilidade dos loop de roteamento, todos os dispositivos OSPF em um domínio de roteamento OSPF devem ter a compatibilidade RFC ajustada identicamente. Este ajuste é selecionado à revelia.
 - Mudanças da adjacência — Contém os ajustes que definem as mudanças da adjacência que fazem com que os mensagens de Log de sistema sejam enviados.
 - Mudanças da adjacência do log — Verifique esta caixa de verificação a fim fazer com que a ferramenta de segurança envie um mensagem de Log de sistema sempre que um vizinho de OSPF vai para cima ou para baixo. Este ajuste é selecionado à revelia.
 - A adjacência do log muda o detalhe — Verifique esta caixa de verificação a fim fazer com que a ferramenta de segurança envie um mensagem de Log de sistema sempre que toda a mudança de estado ocorre, não no exato momento em que um vizinho vai para cima ou para baixo. Este ajuste é desmarcado à revelia.
 - Distâncias administrativas da rota — Contém os ajustes para as

distâncias administrativas de rotas baseadas no tipo da rota. Área inter — Ajusta a distância administrativa para todas as rotas de uma área a outra. Os valores válidos variam de 1 a 255. O valor padrão é 100. Área intra — Ajusta a distância administrativa para todas as rotas dentro de uma área. Os valores válidos variam de 1 a 255. O valor padrão é 100. Externo — Ajusta a distância administrativa para todas as rotas de outros domínios de roteamento que são instruídos com a redistribuição. Os valores válidos variam de 1 a 255. O valor padrão é 100. Temporizadores — Contém os ajustes usados para configurar temporizadores do passeio LSA e do cálculo SPF. Tempo de retardo SPF — Especifica o tempo entre quando o OSPF recebe uma alteração de topologia e quando o cálculo SPF começa. Os valores válidos variam de 0 a 65535. O valor padrão é 5. Tempo de contenção SPF — Especifica o tempo de contenção entre cálculos consecutivos SPF. Os valores válidos variam de 1 a 65534. O valor padrão é 10. Passeio do grupo LSA — Especifica o intervalo em que os LSA são recolhidos em um grupo e refrescados, checksummed, ou envelhecidos. Os valores válidos variam do 10 a 1800. O valor padrão é 240. A informação do padrão origina — Contém os ajustes usados por um ASBR para gerar uma rota externa do padrão em um domínio de roteamento OSPF. Permita a informação do padrão originam — Verifique esta caixa de verificação a fim permitir a geração da rota padrão no domínio de roteamento OSPF. Anuncie sempre a rota padrão — Verifique esta caixa de verificação a fim anunciar sempre a rota padrão. Esta opção é desmarcada à revelia. Valor de métrica — Especifica a métrica do OSPF padrão. Os valores válidos variam de 0 a 16777214. O valor padrão é 1. Tipo de métrica — Especifica o tipo de link externo associado com a rota padrão anunciada no domínio de roteamento OSPF. Os valores válidos são 1 ou 2, indicando um tipo-1 ou uma rota externa do Tipo 2. O valor padrão é 2. Mapa de rota — (*opcional*) o nome do mapa de rota a aplicar-se. O processo de roteamento gerencie a rota padrão se o mapa de rota é satisfeito.

5. 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**, e clique-os então **adicionam** segundo as indicações desta imagem: A caixa de diálogo da área do OSPF adicionar aparece. Neste exemplo, a única rede que é adicionada é a rede interna (10.1.1.0/24) desde que o OSPF é permitido somente na interface interna. **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.
6. Clique em **OK**. Esta lista descreve cada um coloca: Processo de OSPF — Quando você adiciona uma área nova, escolha o ID para o processo de OSPF. Se há somente um processo de OSPF permitido na ferramenta de segurança, a seguir esse processo está selecionado à revelia. Quando você edita uma área existente, você não pode mudar o processo de OSPF ID. ID da área — Quando você adiciona uma área nova, entre no ID da área. Você pode especificar o ID da área como um número decimal ou um endereço IP de Um ou Mais Servidores Cisco ICM NT. Os valores decimais válidos variam de 0 a 4294967295. Você não pode mudar o ID da área quando você edita uma área existente. Neste exemplo, o ID da área é 0. Tipo de área — Contém os ajustes para o tipo de área que está sendo configurado. Normal — Escolha esta opção a fim fazer à área um a área do OSPF padrão. Esta opção está selecionada à revelia quando você cria primeiramente uma área. Stub — Escolha esta opção a fim fazer à área um a área de stub. As áreas de stub não têm nenhuma Roteadores ou áreas além dela. As áreas de stub impedem COMO o LSAs externo (tipo 5 LSA) da inundação na área de stub. Quando você cria uma área de stub, você pode desmarcar a caixa de verificação sumária para impedir que os LSA sumário (tipo 3 e 4) estejam inundados na área. Sumário — Quando a área que está sendo definida é

uma área de stub, desmarcar esta caixa de verificação a fim impedir que os LSA estejam enviados na área de stub. Esta caixa de verificação é selecionada à revelia para áreas de stub. **NSSA** — Escolha esta opção a fim fazer à área um Not-So-Stubby Area. Os NSSA aceitam o tipo 7 LSA. Quando você cria um NSSA, você pode desmarcar a caixa de verificação sumária a fim impedir que os LSA sumário estejam inundados na área. Além, você pode desmarcar a caixa de verificação da redistribuição e para permitir a informação de Defaultl origine a fim desabilitar a redistribuição de rota. **Redistribua** — Desmarcar esta caixa de verificação a fim impedir que as rotas estejam importadas no NSSA. Esta caixa de verificação é selecionada à revelia. **Sumário** — Quando a área que está sendo definida é um NSSA, desmarcar esta caixa de verificação a fim impedir que os LSA estejam enviados na área de stub. Esta caixa de verificação é selecionada à revelia para NSSA. **A informação do padrão origina** — Verifique esta caixa de verificação a fim gerar um tipo padrão 7 no NSSA. Esta caixa de verificação é desmarcada à revelia. **Valor de métrica** — Incorpore um valor a fim especificar o valor de métrica OSPF para a rota padrão. Os valores válidos variam de 0 a 16777214. O valor padrão é 1. **Tipo de métrica** — Escolha um valor a fim especificar o tipo de métrica OSPF para a rota padrão. As escolhas são 1 (tipo-1) ou 2 (tipo-2). O valor padrão é 2. **Redes de área** — Contém os ajustes que definem uma área do OSPF. **Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT e a máscara** — Contém os ajustes usados para definir as redes na área. **Endereço IP de Um ou Mais Servidores Cisco ICM NT** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT da rede ou hospede-o para ser adicionado à área. Use 0.0.0.0 com um netmask de 0.0.0.0 para criar a área do padrão. Você pode usar 0.0.0.0 em somente uma área. **Máscara de rede** — Escolha a máscara de rede para o endereço IP de Um ou Mais Servidores Cisco ICM NT ou hospede-a para ser adicionada à área. Se você adiciona um host, escolha a máscara de 255.255.255.255. Neste exemplo, **10.1.1.0/24** são a rede a ser configurada. **Adicionar** — Adiciona a rede definida na área do endereço IP de Um ou Mais Servidores Cisco ICM NT e da máscara da entrada à área. A rede adicionada aparece na tabela de redes de área. **Supressão** — Suprime da rede selecionada da tabela de redes de área. **Redes de área** — Indica as redes definidas para a área. **Endereço IP de Um ou Mais Servidores Cisco ICM NT** — Indica o endereço IP de Um ou Mais Servidores Cisco ICM NT da rede. **Máscara de rede** — Indica a máscara de rede para a rede. **Autenticação** — Contém os ajustes para a autenticação da área do OSPF. **Nenhum** — Escolha esta opção a fim desabilitar a autenticação da área do OSPF. Esta é a configuração padrão. **Senha** — Escolha esta opção a fim usar uma senha de texto sem formatação para a autenticação de área. Esta opção não é recomendada onde a Segurança é um interesse. **MD5** — Escolha esta opção a fim usar a autenticação md5. **Custos padrão** — Especifique uns custos padrão para a área. Os valores válidos variam de 0 a 65535. O valor padrão é 1.

7. Clique em Apply.

8. Opcionalmente, você pode 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 em atualizações OSPF.
9. Você pode opcionalmente configurar a redistribuição de rota. Cisco ASA pode redistribuir as rotas descobertas pelo RASGO e pelo EIGRP no processo de roteamento OSPF. Você pode igualmente redistribuir a estática e as rotas conectadas no processo de roteamento OSPF. Defina a redistribuição de rota na placa da redistribuição.
10. Os pacotes de hello de OSPF são enviados como pacotes de transmissão múltipla. Se um vizinho de OSPF é ficado situado através de uma rede do nonbroadcast, você deve manualmente definir esse vizinho. Quando você define manualmente um vizinho de OSPF,

os pacotes Hello estão enviados a esse vizinho como mensagens do unicast. A fim definir vizinhos de OSPF estáticos, vá à placa do vizinho estático.

11. As rotas aprendidas de outros protocolos de roteamento podem ser resumidas. A métrica usada para anunciar o sumário é a métrica a menor de umas rotas mais específicas. As rotas sumárias ajudam a reduzir o tamanho da tabela de roteamento. Usar rotas sumárias para o OSPF faz com que um OSPF ASBR anuncie uma rota externa como um agregado para todas as rotas redistribuída que são cobertas pelo endereço. Somente as rotas de outros protocolos de roteamento que estão sendo redistribuídos no OSPF podem ser resumidas.
12. Na placa do enlace virtual, você pode adicionar uma área a uma rede de OSPF, e não é possível conectar a área diretamente à área Backbone; você deve criar um enlace virtual. Um enlace virtual conecta dois dispositivos OSPF que têm uma área comum, chamados a área de trânsito. Um dos dispositivos OSPF deve ser conectado à área Backbone.

Configurar a autenticação OSPF

Cisco ASA apoia a autenticação md5 das atualizações de roteamento do protocolo de roteamento OSPF. O resumo fechado MD5 em cada pacote de OSPF impede a introdução de mensagens de roteamento desautorizados ou falsos das fontes unapproved. A adição de autenticação a suas mensagens OSPF 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 na 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 a adição decidido ou acidental de um outro roteador à rede e a todo o problema.

A autenticação da rota de OSPF é configurada em uma base da interface per. Todos os vizinhos de OSPF nas relações configuradas para a autenticação de mensagem OSPF 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 OSPF em Cisco ASA:

1. No ASDM, navegue à **configuração > à instalação > ao roteamento > ao OSPF > à relação de dispositivo**, e clique então a aba da **autenticação** segundo as indicações desta imagem. Neste caso, o OSPF é permitido na interface interna.
2. Escolha a **interface interna**, e o clique **edita**.
3. Sob a autenticação, escolha a **autenticação md5**, e adicionar mais informação sobre parâmetros de autenticação aqui. Neste caso, a chave preshared é **cisco123**, e a chave ID é **1**.
4. A **APROVAÇÃO** do clique, e clica então **aplica-se**.

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
ospf cost 10 !--- OSPF authentication is configured on
the inside interface ospf message-digest-key 1 md5
<removed> ospf authentication message-digest ! !---
Outside interface configuration interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.2
255.255.255.0 ospf cost 10 ! !--- Output Suppressed icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-602.bin no asdm history enable arp timeout
14400 ! !--- OSPF Configuration router ospf 1 network
10.1.1.0 255.255.255.0 area 0 log-adj-changes ! !---
This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#
```

Configuração de CLI do roteador do Cisco IOS (R2)

Roteador do Cisco IOS (R2)

```
!--- Interface that connects to the Cisco ASA. !---
Notice the OSPF authentication parameters interface
Ethernet0 ip address 10.1.1.2 255.255.255.0 ip ospf
authentication message-digest ip ospf message-digest-key
1 md5 cisco123 !--- Output Suppressed !--- OSPF
Configuration router ospf 1 log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0 network 172.16.1.0
0.0.0.255 area 0 network 172.16.2.0 0.0.0.255 area 0
```

Configuração de CLI do roteador do Cisco IOS (r1)

Roteador do Cisco IOS (r1)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1 log-adjacency-changes network 172.16.5.0
0.0.0.255 area 0 network 172.16.2.0 0.0.0.255 area 0
```

Configuração de CLI do roteador do Cisco IOS (R3)

Roteador do Cisco IOS (R3)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1 log-adjacency-changes network 172.16.1.0
0.0.0.255 area 0 network 172.16.10.0 0.0.0.255 area 0
```

Redistribua no OSPF com ASA

Como mencionado mais cedo, você pode redistribuir rotas em um processo de roteamento OSPF de um outro processo de roteamento OSPF, um processo de roteamento do RASGO, ou da estática e das rotas conectadas configuradas em relações OSPF-permitidas.

Neste exemplo, redistribuindo as rotas RIP no OSPF com o diagrama da rede como mostrado:

Configuração ASDM

1. Escolha a **configuração > a instalação > o roteamento > o RASGO de dispositivo > Setup** a fim permitir o RASGO, e adicionar a rede 192.168.1.0 segundo as indicações desta imagem.
2. Clique em Apply.
3. Escolha a **configuração > a instalação de dispositivo > o roteamento > o > Add OSPF > de redistribuição** a fim redistribuir rotas RIP no OSPF.
4. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.

Configuração de CLI equivalente

A configuração de CLI do ASA para redistribui o RASGO no OSPF COMO

```
router ospf 1
network 10.1.1.0 255.255.255.0 area 0
log-adj-changes
redistribute rip subnets router rip network 192.168.1.0
```

Você pode ver a tabela de roteamento do vizinho IO Router(R2) após ter redistribuído rotas RIP no OSPF 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 172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks O
172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1 O 172.16.5.1/32 [110/65] via
172.16.2.2, 01:17:29, Serial1 C 172.16.1.0/24 is directly connected, Ethernet1 C 172.16.2.0/24
is directly connected, Serial1 10.0.0.0/24 is subnetted, 1 subnets C 10.1.1.0 is directly
connected, Ethernet0 O E2 192.168.1.0/24 [110/20] via 10.1.1.1, 01:17:29, Ethernet0 !---
```

Redistributed route adversted by Cisco ASA

Verificar

Termine estas etapas para verificar sua configuração:

1. No ASDM, você pode navegar à **monitoração > roteamento > vizinhos de OSPF** para ver cada um dos vizinhos de OSPF. Esta imagem mostra o roteador interno (R2) como um vizinho ativo. Você pode igualmente ver a relação onde este vizinho reside, o ID de roteador vizinho, o estado, e o período inoperante.
2. Adicionalmente, você pode verificar a tabela de roteamento se você navega à **monitoração > roteamento > rotas**. Nesta imagem, 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).
3. 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 192.168.1.1 to network 0.0.0.0 O 172.16.10.1 255.255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside O 172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside O 172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, 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 S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside
4. Você pode igualmente usar o **comando de base de dados ASPF da mostra** a fim obter a

informação sobre as redes instruídas e a topologia OSPF.

```
ciscoasa#show ospf database OSPF
Router with ID (192.168.1.2) (Process ID 1) Router Link States (Area 0) Link ID ADV Router
Age Seq# Checksum Link count 172.16.1.2 172.16.1.2 123 0x80000039 0xfd1d 2 172.16.2.1
172.16.2.1 775 0x8000003c 0x9b42 4 172.16.5.1 172.16.5.1 308 0x80000038 0xb91b 3
192.168.1.2 192.168.1.2 1038 0x80000037 0x29d7 1 Net Link States (Area 0) Link ID ADV
Router Age Seq# Checksum 10.1.1.1 192.168.1.2 1038 0x80000034 0x72ee 172.16.1.1 172.16.2.1
282 0x80000036 0x9e68
```

5. O comando `show ospf neighbors` 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 ospf neighbor Neighbor ID Pri State Dead Time Address
Interface 172.16.2.1 1 FULL/BDR 0:00:36 10.1.1.2 inside
```

Troubleshooting

Esta seção fornece a informação que pôde facilitar pesquisar defeitos edições OSPF.

Configuração do vizinho estático para a rede Point-to-Point

Se você configurou *sem transmissão ponto a ponto da rede de OSPF no ASA*, você deve definir vizinhos de OSPF estáticos para anunciar rotas de OSPF sobre um ponto a ponto, rede sem broadcast. Refira a [definição de vizinhos de OSPF estáticos](#) para mais informação.

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.

- **debug eventos de OSPF** — Permite a eliminação de erros dos eventos de

```
OSPF.ciscoasa(config)#debug ospf events OSPF events debugging is on ciscoasa(config)# int
e0/1 ciscoasa(config-if)# no shu ciscoasa(config-if)# OSPF: Interface inside going Up OSPF:
Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: 2
Way Communication to 172.16.2.1 on inside, state 2WAY OSPF: Backup seen Event before WAIT
timer on inside OSPF: DR/BDR election on inside OSPF: Elect BDR 172.16.2.1 OSPF: Elect DR
172.16.2.1 DR: 172.16.2.1 (Id) BDR: 172.16.2.1 (Id) OSPF: Send DBD to 172.16.2.1 on inside
seq 0xlabd opt 0x2 flag 0x7 len 32 OSPF: Send with youngest Key 1 OSPF: End of hello
processing OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello
processing OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32 mtu
1500 state EXSTART OSPF: First DBD and we are not SLAVE OSPF: Rcv DBD from 172.16.2.1 on
inside seq 0xlabd opt 0x42 flag 0x2 len 152 mt u 1500 state EXSTART OSPF: NBR Negotiation
Done. We are the MASTER OSPF: Send DBD to 172.16.2.1 on inside seq 0xlabe opt 0x2 flag 0x3
len 132 OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Database request
to 172.16.2.1 OSPF: sent LS REQ packet to 10.1.1.2, length 12 OSPF: Rcv DBD from 172.16.2.1
on inside seq 0xlabe opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE OSPF: Send DBD to
172.16.2.1 on inside seq 0xlabf opt 0x2 flag 0x1 len 32 OSPF: Send with youngest Key 1 OSPF:
Send with youngest Key 1 OSPF: Rcv DBD from 172.16.2.1 on inside seq 0xlabf opt 0x42 flag
0x0 len 32 mtu 1500 state EXCHANGE OSPF: Exchange Done with 172.16.2.1 on inside OSPF:
Synchronized with 172.16.2.1 on inside, state FULL OSPF: Send with youngest Key 1 OSPF: Send
with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF:
Neighbor change Event on interface inside OSPF: DR/BDR election on inside OSPF: Elect BDR
192.168.1.2 OSPF: Elect DR 172.16.2.1 OSPF: Elect BDR 192.168.1.2 OSPF: Elect DR 172.16.2.1
DR: 172.16.2.1 (Id) BDR: 192.168.1.2 (Id) OSPF: End of hello processing OSPF: Send with
youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Send with
youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of
```

hello processing OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing

Nota: Refira a seção [OSPF debugar da](#) referência de comandos do dispositivo do Cisco Security, versão 8.0 para obter mais informações sobre dos vários comandos que são úteis para pesquisar defeitos o problema.

[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](#)