Configurar o ASA para links ISP redundantes ou de backup

Contents

Introduction

Este documento descreve como configurar o Cisco ASA 5500 Series Adaptive Security Appliance (ASA) para o uso do recurso de rastreamento de rota estática para permitir que o dispositivo use conexões de Internet redundantes ou de backup.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco ASA 5555-X Series que executa o software versão 9.x ou posterior
- Cisco ASDM versão 7.x ou posterior

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.

Produtos Relacionados

Você também pode usar essa configuração com o Cisco ASA 5500 Series versão 9.1(5).

> **Note**: O comando **backup interface** é necessário para configurar a quarta interface no ASA 5505 Series. Consulte a seção interface de backup da *Referência de Comandos do Cisco Security Appliance Versão 7.2* para obter mais informações.

Informações de Apoio

Esta seção fornece uma visão geral do recurso de rastreamento de rota estática descrito neste documento, bem como algumas recomendações importantes antes de começar.

Visão geral do recurso de rastreamento de rota estática

Um problema com o uso de rotas estáticas é que não existe um mecanismo inerente que possa determinar se a rota está ativa ou inativa. A rota permanece na tabela de roteamento mesmo se o gateway do próximo salto ficar indisponível. As rotas estáticas serão removidas da tabela de roteamento somente se a interface associada no Security Appliance ficar inativa. Para resolver esse problema, um recurso de rastreamento de rota estática é usado para rastrear a disponibilidade de uma rota estática. O recurso remove a rota estática da tabela de roteamento e a substitui por uma rota de backup em caso de falha.

O rastreamento de rota estática permite que o ASA use uma conexão barata a um ISP secundário caso a linha alugada principal não esteja disponível. Para alcançar essa redundância, o ASA associa uma rota estática a um destino de monitoramento que você define. A operação SLA (Service Level Agreement, Contrato de Nível de Serviço) monitora o destino com solicitações de eco ICMP periódicas. Se uma resposta de eco não for recebida, o objeto será considerado inativo e a rota associada será removida da tabela de roteamento. Uma rota de backup configurada anteriormente é usada no lugar da rota removida. Enquanto a rota de backup está em uso, a operação de monitoramento SLA continua suas tentativas de alcançar o destino de monitoramento. Quando o destino estiver disponível novamente, a primeira rota será substituída na tabela de roteamento e a rota de backup será removida.

No exemplo usado neste documento, o ASA mantém duas conexões com a Internet. A primeira conexão é uma linha alugada de alta velocidade que é acessada através de um roteador

fornecido pelo ISP principal. A segunda conexão é uma linha de assinante digital (DSL) de velocidade mais baixa que é acessada por meio de um modem DSL fornecido pelo ISP secundário.

> **Note**: A configuração descrita neste documento não pode ser usada para balanceamento de carga ou compartilhamento de carga, pois não é suportada no ASA. Use essa configuração somente para fins de redundância ou backup. O tráfego de saída usa o ISP principal e, em seguida, o ISP secundário se o principal falhar. A falha do ISP principal causa uma interrupção temporária do tráfego.

A conexão DSL estará ociosa desde que a linha alugada esteja ativa e o gateway ISP principal esteja acessível. No entanto, se a conexão com o ISP principal ficar inativa, o ASA altera a tabela de roteamento para direcionar o tráfego para a conexão DSL. O rastreamento de rota estática é usado para alcançar essa redundância.

O ASA é configurado com uma rota estática que direciona todo o tráfego da Internet para o ISP principal. A cada dez segundos, o processo do monitor SLA verifica para confirmar se o gateway ISP principal está acessível. Se o processo de monitoramento de SLA determinar que o gateway ISP principal não está acessível, a rota estática que direciona o tráfego para essa interface será removida da tabela de roteamento. Para substituir essa rota estática, uma rota estática alternativa que direciona o tráfego para o ISP secundário é instalada. Essa rota estática alternativa direciona o tráfego para o ISP secundário através do modem DSL até que o link para o ISP principal esteja acessível.

Essa configuração oferece uma maneira relativamente barata de garantir que o acesso de saída à Internet permaneça disponível para os usuários por trás do ASA. Conforme descrito neste documento, essa configuração pode não ser adequada para acesso de entrada a recursos por trás do ASA. As habilidades de rede avançadas são necessárias para alcançar conexões de entrada contínuas. Essas habilidades não são abordadas neste documento.

Recomendações importantes

Antes de tentar a configuração descrita neste documento, você deve escolher um destino de monitoramento que possa responder às solicitações de eco do Internet Control Message Protocol (ICMP). O destino pode ser qualquer objeto de rede escolhido, mas é recomendável um destino intimamente ligado à sua conexão com o Provedor de Internet (ISP). Aqui estão alguns possíveis alvos de monitoramento:

- O endereço do gateway do ISP
- Outro endereço gerenciado por ISP
- Um servidor em outra rede, como um servidor de Autenticação, Autorização e Auditoria (AAA) com o qual o ASA deve se comunicar
- Um objeto de rede persistente em outra rede (um computador desktop ou notebook que pode ser desligado à noite não é uma boa opção)

Este documento pressupõe que o ASA está totalmente operacional e configurado para permitir que o Cisco Adaptive Security Device Manager (ASDM) faça alterações na configuração.

Tip: Para obter informações sobre como permitir que o ASDM configure o dispositivo, consulte a seção Configuração do Acesso HTTPS para ASDM do *CLI Book 1: Guia de configuração da CLI de operações gerais do Cisco ASA Series, 9.1*.

Configurar

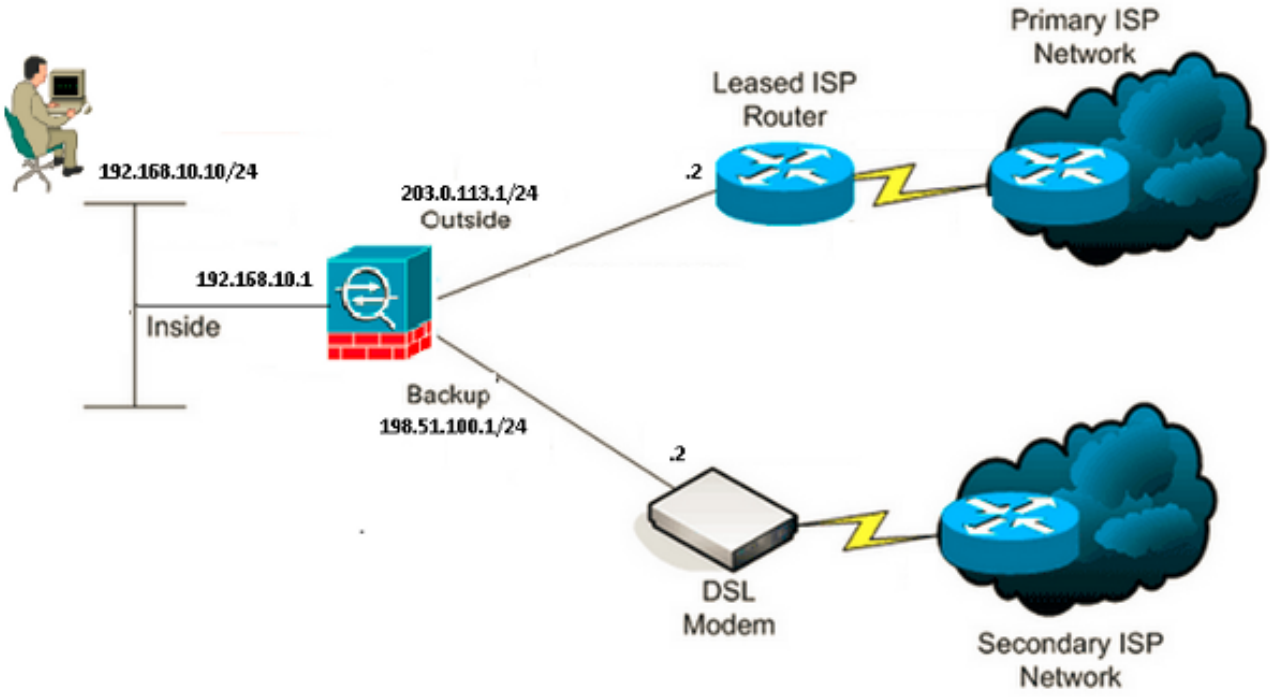
Use as informações descritas nesta seção para configurar o ASA para o uso do recurso de rastreamento de rota estática.

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

Note: Os endereços IP usados nessa configuração não são legalmente roteáveis na Internet. Eles são endereços RFC 1918, usados em um ambiente de laboratório.

Diagrama de Rede

O exemplo fornecido nesta seção usa esta configuração de rede:



Configuração de CLI

Use estas informações para configurar o ASA via CLI:

```
ASA# show running-config

ASA Version 9.1(5)
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif backup
 security-level 0
 ip address 198.51.100.1 255.255.255.0

!--- The interface attached to the Secondary ISP.
!--- "backup" was chosen here, but any name can be assigned.

!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa915-smp-k8.bin
ftp mode passive
clock timezone IND 5 30
object network Inside_Network
 subnet 192.168.10.0 255.255.255.0
object network inside_network
 subnet 192.168.10.0 255.255.255.0
pager lines 24
logging enable
mtu inside 1500
mtu outside 1500
mtu backup 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
```

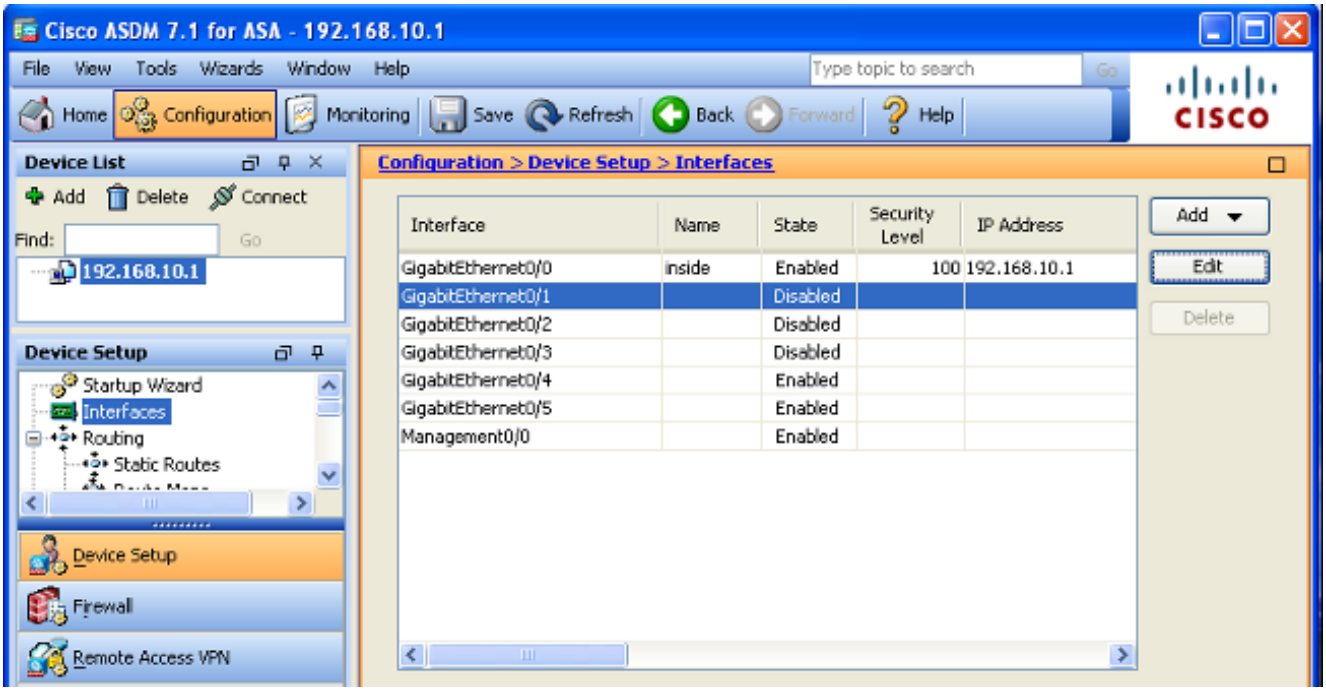
```
object network Inside_Network
 nat (inside,outside) dynamic interface
object network inside_network
 nat (inside,backup) dynamic interface

!--- NAT Configuration for Outside and Backup

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1 track 1

!--- Enter this command in order to track a static route.
!--- This is the static route to be installed in the routing
!--- table while the tracked object is reachable.  The value after
!--- the keyword "track" is a tracking ID you specify.

route backup 0.0.0.0 0.0.0.0 198.51.100.2 254

!--- Define the backup route to use when the tracked object is unavailable.
!--- The administrative distance of the backup route must be greater than
!--- the administrative distance of the tracked route.
!--- If the primary gateway is unreachable, that route is removed
!--- and the backup route is installed in the routing table
!--- instead of the tracked route.

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00

sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10

!--- Configure a new monitoring process with the ID 123.  Specify the
!--- monitoring protocol and the target network object whose availability the tracking
!--- process monitors.  Specify the number of packets to be sent with each poll.
!--- Specify the rate at which the monitor process repeats (in seconds).

sla monitor schedule 123 life forever start-time now

!--- Schedule the monitoring process.  In this case the lifetime
!--- of the process is specified to be forever.  The process is scheduled to begin
!--- at the time this command is entered.  As configured, this command allows the
!--- monitoring configuration specified above to determine how often the testing
!--- occurs.  However, you can schedule this monitoring process to begin in the
!--- future and to only occur at specified times.

crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
!
track 1 rtr 123 reachability

!--- Associate a tracked static route with the SLA monitoring process.
!--- The track ID corresponds to the track ID given to the static route to monitor:
!--- route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1
!--- "rtr" = Response Time Reporter entry.  123 is the ID of the SLA process
!--- defined above.

telnet timeout 5
ssh stricthostkeycheck
```

```
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
!
service-policy global_policy global
```

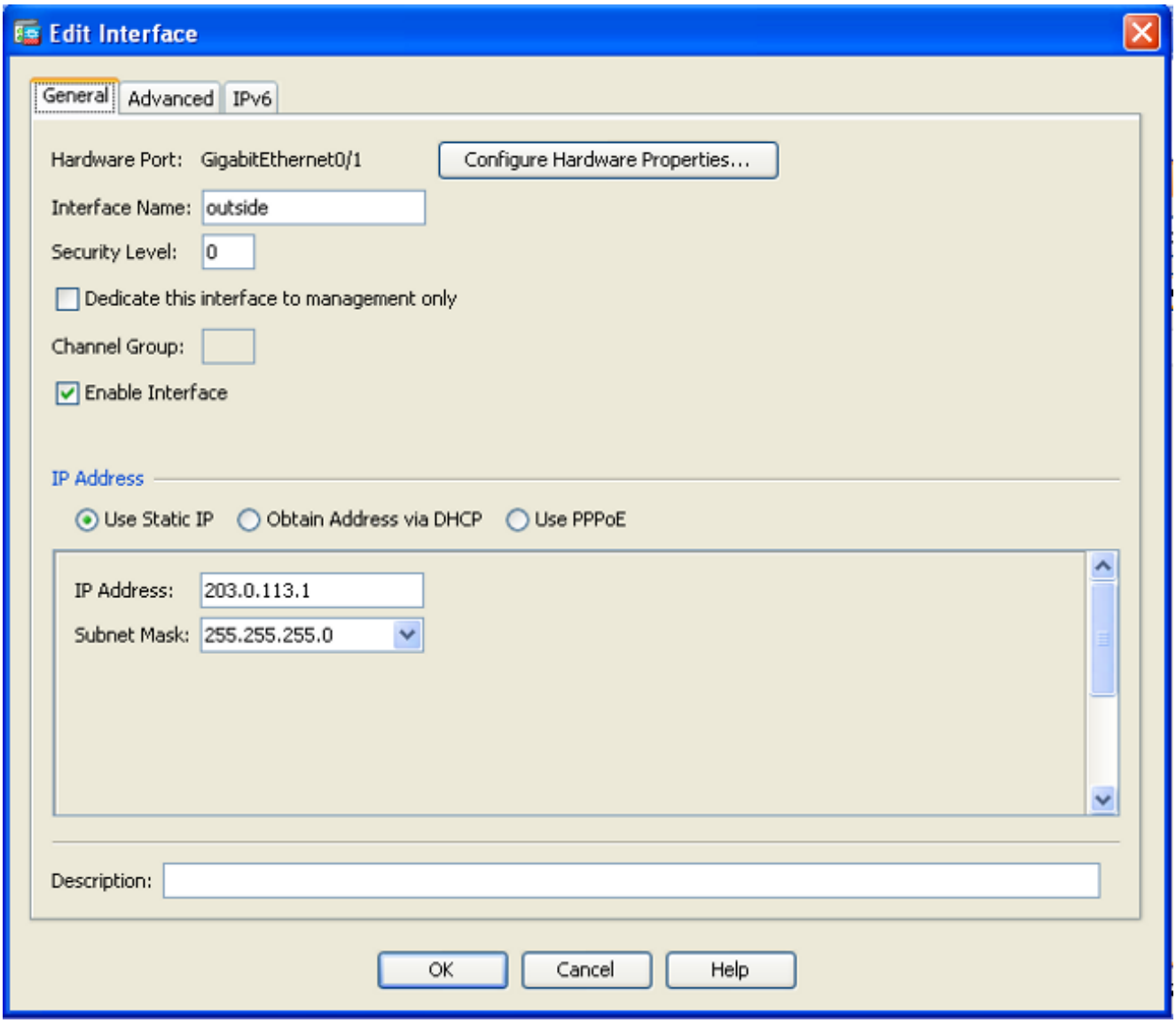
Configuração do ASDM

Conclua estes passos para configurar o suporte ISP redundante ou de backup com o aplicativo ASDM:

1. No aplicativo ASDM, clique em **Configuration** e em **Interfaces**.



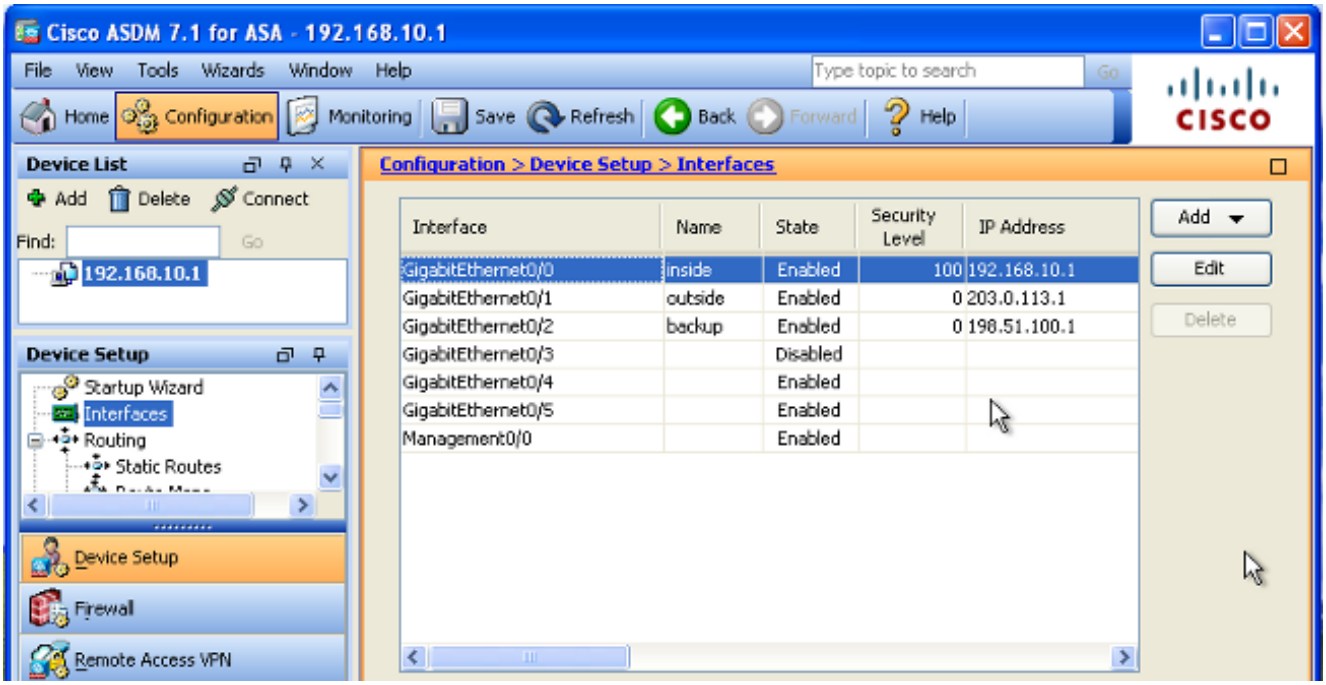
2. Selecione **GigabitEthernet0/1** na lista Interfaces e clique em **Editar**. Essa caixa de diálogo é exibida:



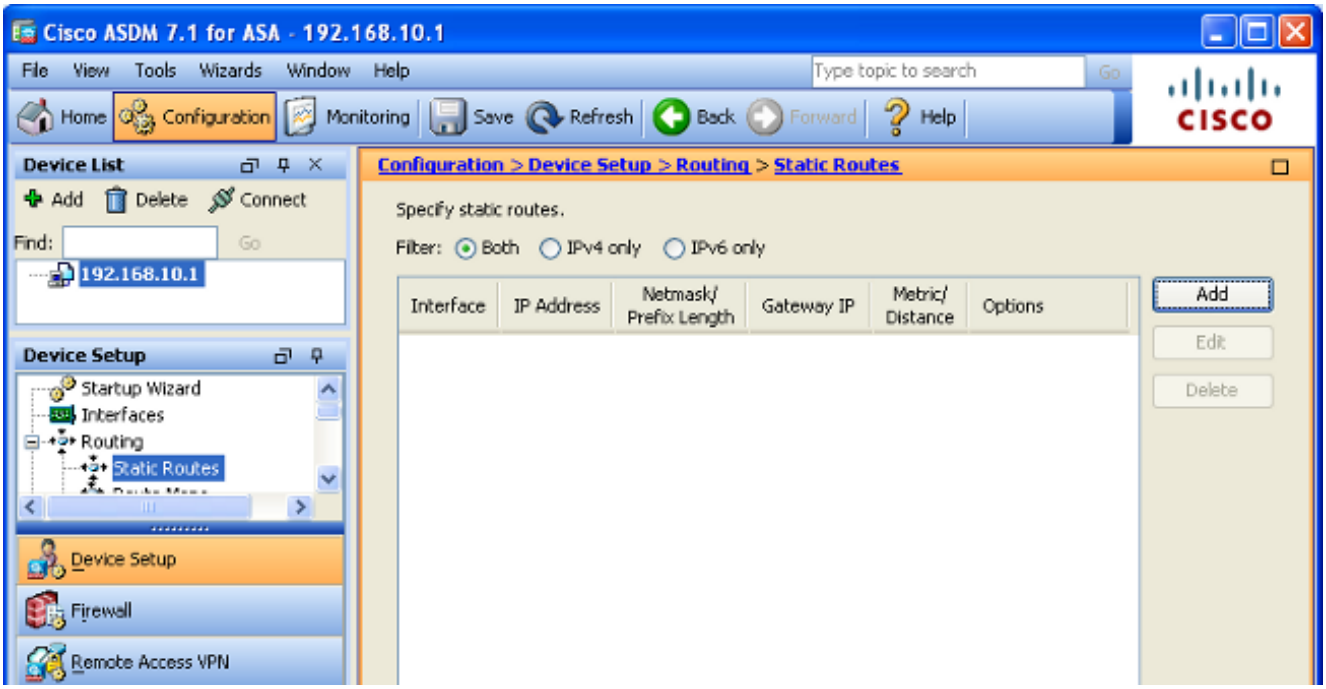
3. Marque a caixa de seleção Habilitar interface e insira os valores apropriados nos campos *Nome da interface*, *Nível de segurança*, *Endereço IP* e *Máscara de sub-rede*.

4. Clique em **OK** para fechar a caixa de diálogo.

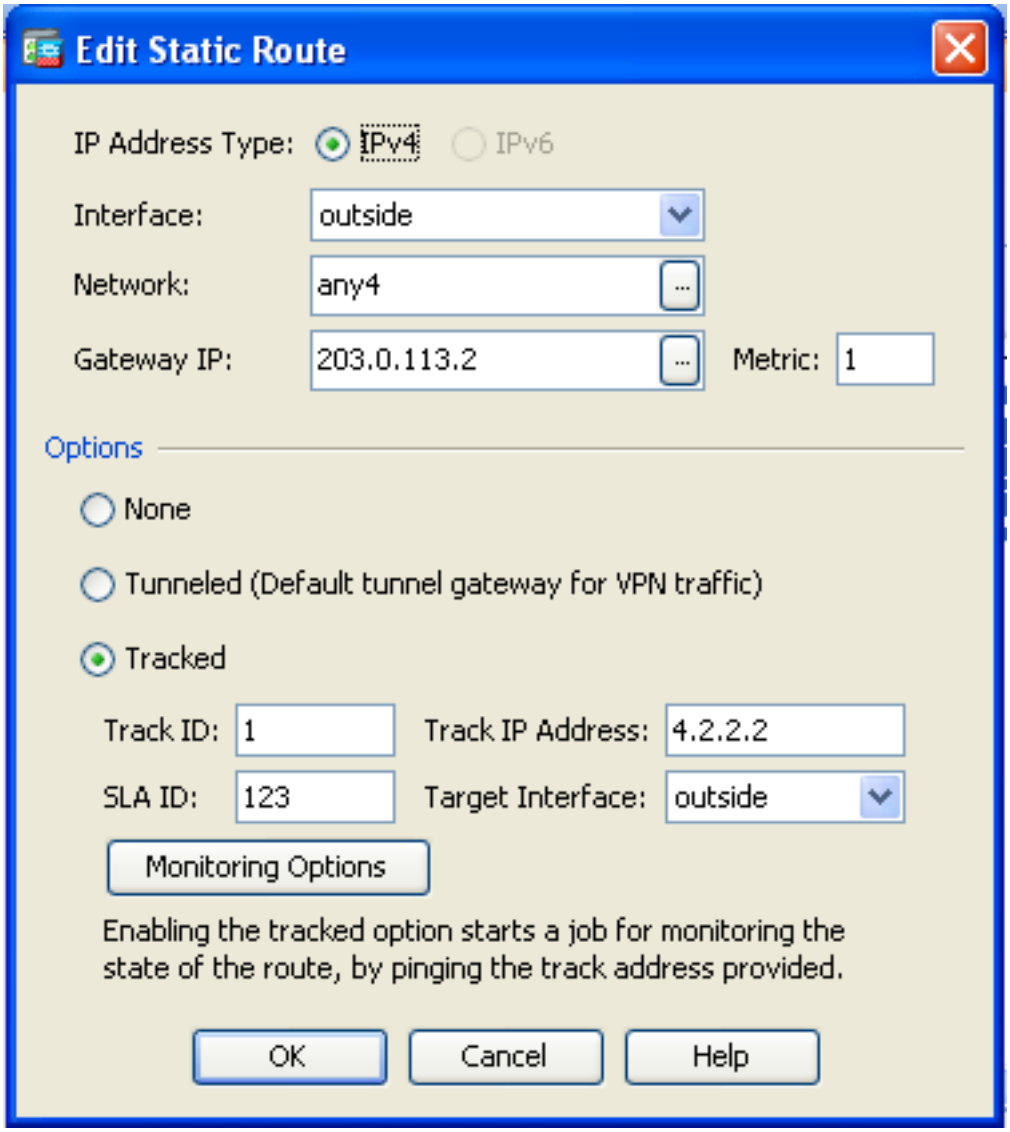
5. Configure as outras interfaces conforme necessário e clique em **Apply** para atualizar a configuração do ASA:



6. Selecione **Roteamento** e clique em **Rotas estáticas** localizadas no lado esquerdo do aplicativo ASDM:



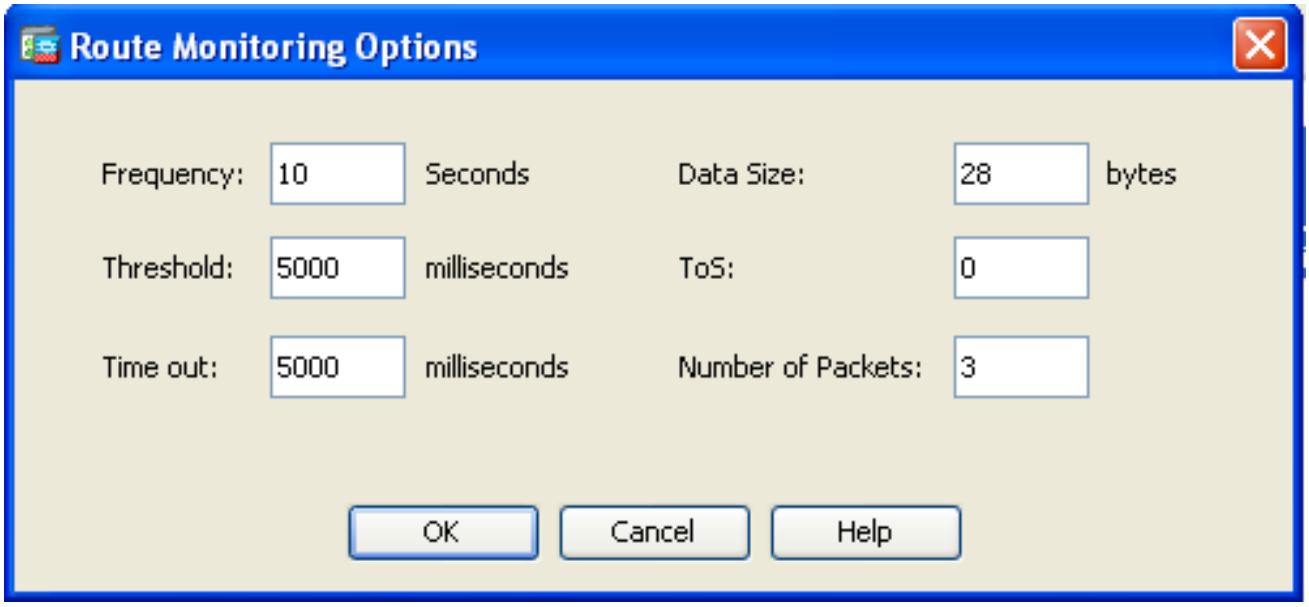
7. Clique em **Adicionar** para adicionar as novas rotas estáticas. Essa caixa de diálogo é exibida:



8. Na lista suspensa Nome da interface, escolha a interface na qual a rota reside e configure a rota padrão para acessar o gateway. Neste exemplo, **203.0.113.2** é o gateway ISP principal e **4.2.2.2** é o objeto a ser monitorado com ecos ICMP.

9. Na área Opções, clique no botão de opção **Rastreado** e insira os valores apropriados nos campos *ID do controle*, *ID do SLA* e *Rastrear endereço IP*.

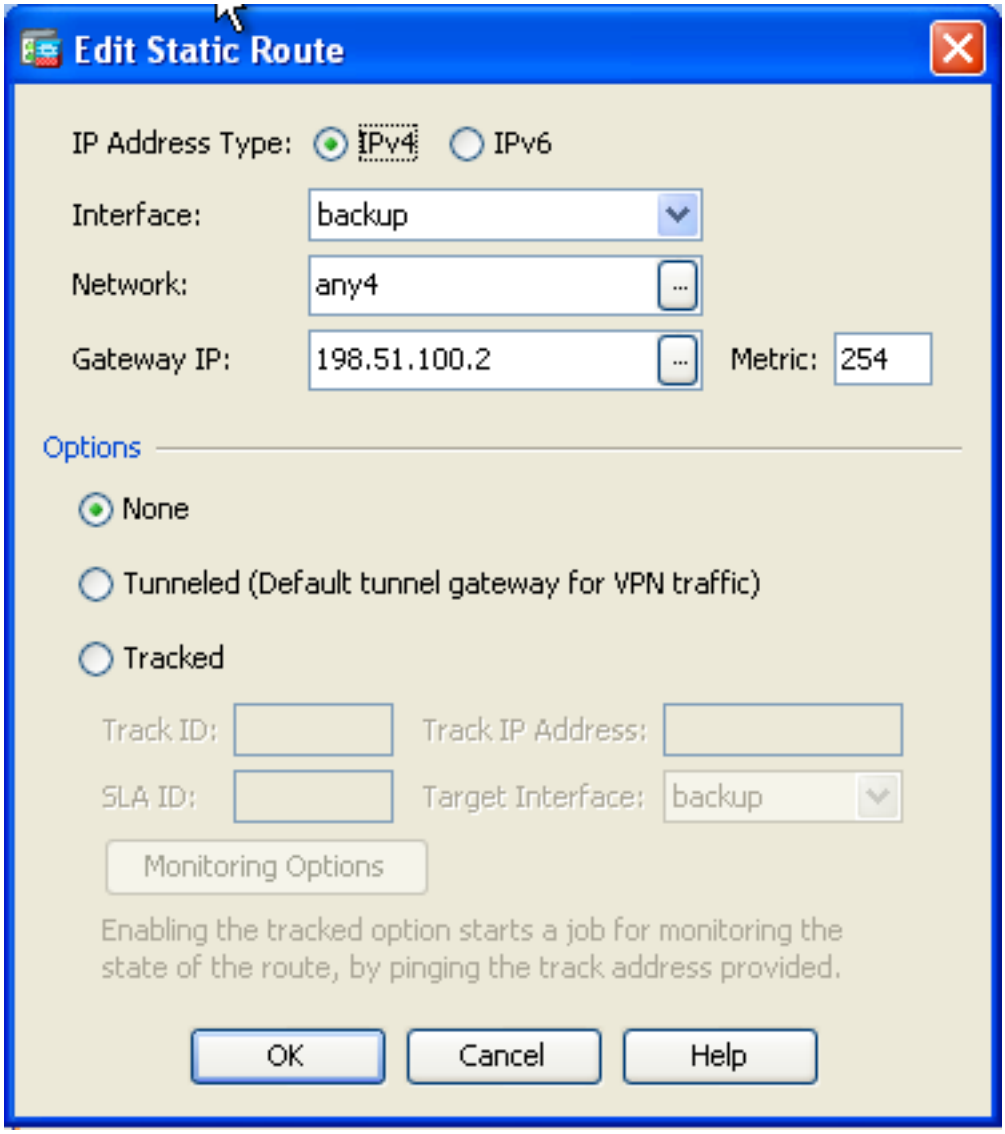
10. Clique em **Opções de monitoramento**. Essa caixa de diálogo é exibida:



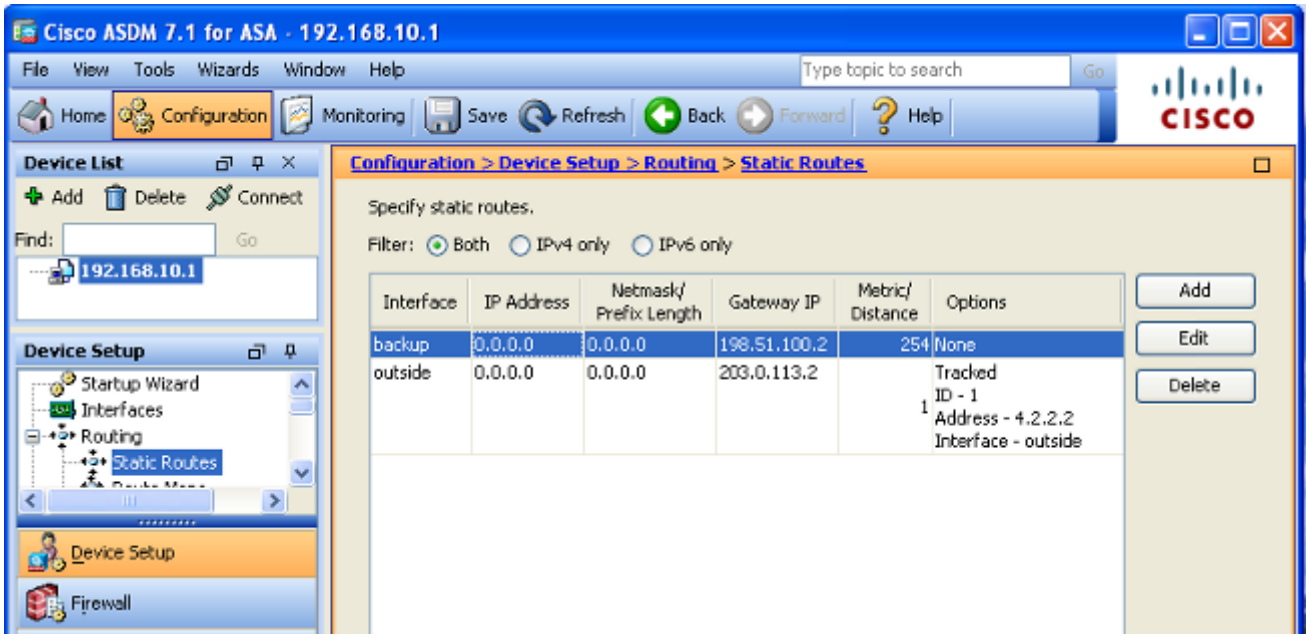
11. Insira os valores apropriados para a frequência e outras opções de monitoramento e clique em **OK**.

12. Adicione outra rota estática para o ISP secundário para fornecer uma rota para acessar a Internet. Para torná-la uma rota secundária, configure essa rota com uma métrica mais alta, como 254. Se a rota primária (ISP principal) falhar, essa rota será removida da tabela de roteamento. Essa rota secundária (ISP secundário) é instalada na tabela de roteamento do Private Internet Exchange (PIX).

13. Clique em **OK** para fechar a caixa de diálogo:



As configurações aparecem na lista Interface:



14. Selecione a configuração de roteamento e clique em **Apply** para atualizar a configuração do ASA.

Verificar

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

Confirme se a configuração foi concluída

> **Note**: A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Use estes comandos **show** para verificar se sua configuração está completa:

- **show running-config sla monitor** - A saída deste comando exibe os comandos SLA na configuração.

```
ASA# show running-config sla monitor
sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10
sla monitor schedule 123 life forever start-time now
```

- **show sla monitor configuration** - A saída desse comando exibe as configurações atuais da operação.

```
ASA# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 4.2.2.2
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data&colon; No
Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

- **show sla monitor operational-state** - A saída deste comando exibe as estatísticas operacionais da operação SLA.

  Antes que o ISP principal falhe, este é o estado operacional:

```
ASA# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:30:40.672 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
```

```
Number of operations attempted: 46
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 13:38:10.672 IND Sun Jan 4 2015
Latest operation return code: OK
RTT Values:
RTTAvg: 1       RTTMin: 1       RTTMax: 1
NumOfRTT: 3     RTTSum: 3       RTTSum2: 3
```

Depois que o ISP principal falhar (e o ICMP ecoa o tempo limite), este é o estado operacional:

```
ASA# show sla monitor operational-state
Entry number: 123
Modification time: 13:30:40.671 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
Number of operations attempted: 57
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 13:40:00.672 IND Sun Jan 4 2015
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Confirme se a rota de backup está instalada (método CLI)

Insira o comando **show route** para confirmar se a rota de backup está instalada.

Antes que o ISP principal falhe, a tabela de roteamento aparece semelhante a esta:

```
ASA# 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 203.0.113.2 to network 0.0.0.0

C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*   0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

Após a falha do ISP principal, a rota estática é removida e a rota de backup é instalada, a tabela

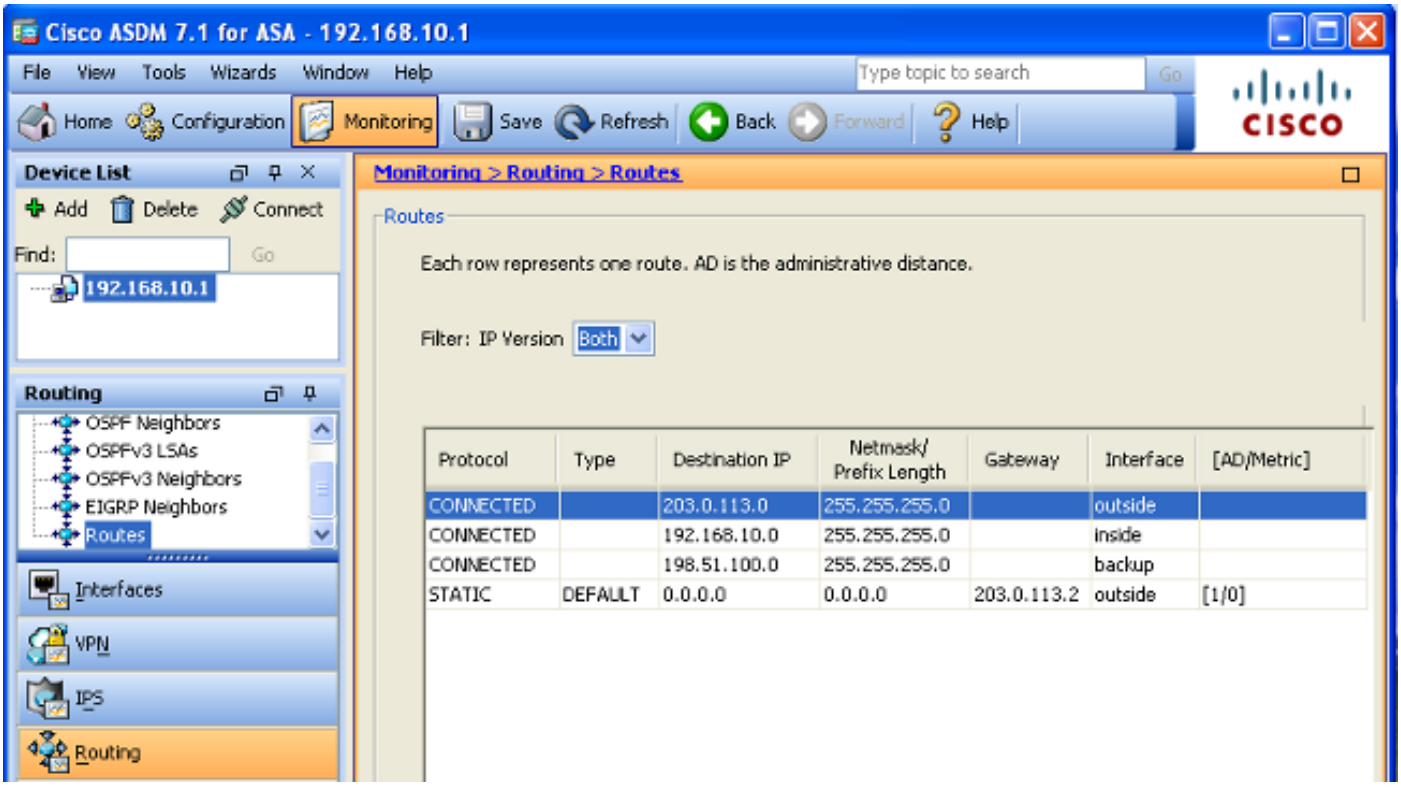
de roteamento é semelhante a esta:

```
ASA# 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 198.51.100.2 to network 0.0.0.0

C     203.0.113.0 255.255.255.0 is directly connected, outside
C     192.168.10.0 255.255.255.0 is directly connected, inside
C     198.51.100.0 255.255.255.0 is directly connected, backup
S*    0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

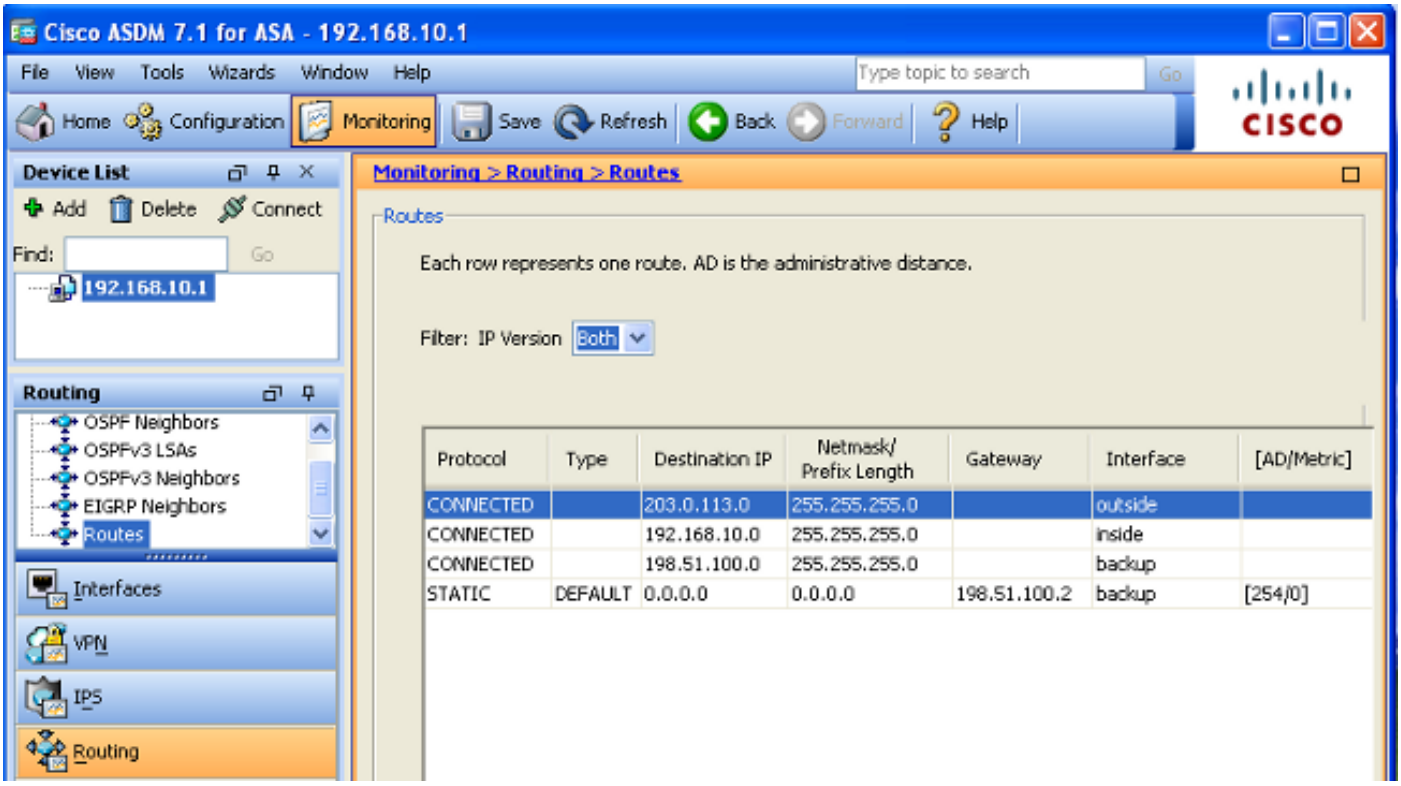
Confirme se a rota de backup está instalada (método ASDM)

Para confirmar se a rota de backup está instalada via ASDM, navegue para **Monitoring > Routing** e escolha **Routes** na árvore de roteamento.

Antes que o ISP principal falhe, a tabela de roteamento aparece semelhante à mostrada na próxima imagem. Observe que a rota **PADRÃO** aponta para **203.0.113.2** através da interface **externa**:



Após a falha do ISP principal, a rota é removida e a rota de backup é instalada. A rota **PADRÃO** agora aponta para **198.51.100.2** através da interface **de backup**:



Troubleshoot

Esta seção fornece alguns comandos debug úteis e descreve como solucionar um problema em que a rota rastreada é removida desnecessariamente.

Comandos debug

Você pode usar estes comandos debug para solucionar seus problemas de configuração:

- **debug sla monitor trace** - A saída deste comando exibe o progresso da operação de eco.

  Se o objeto rastreado (gateway ISP primário) estiver ativo e o eco ICMP for bem-sucedido, a saída será semelhante a esta:

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=1 OK
IP SLA Monitor(123) Scheduler: Updating result
```

  Se o objeto rastreado (gateway ISP primário) estiver inativo e o eco ICMP falhar, a saída será semelhante a esta:

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) Scheduler: Updating result
```

- **debug sla monitor error** - A saída deste comando exibe todos os erros que o processo do

monitor SLA encontra.

Se o objeto rastreado (gateway ISP primário) estiver ativo e o ICMP for bem-sucedido, a saída será semelhante a esta:

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
```

Se o objeto rastreado (gateway ISP primário) estiver inativo e a rota rastreada for removida, a saída será semelhante a esta:

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:02
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:02
%ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 203.0.113.2,
distance 1, table Default-IP-Routing-Table, on interface outside

!--- 4.2.2.2 is unreachable, so the route to the Primary ISP is removed.
```

A rota rastreada é removida desnecessariamente

Se a rota rastreada for removida desnecessariamente, certifique-se de que seu destino de monitoramento esteja sempre disponível para receber solicitações de eco. Além disso, certifique-se de que o estado do seu destino de monitoramento (ou seja, se o destino está acessível ou não) esteja intimamente ligado ao estado da conexão principal do ISP.

Se você escolher um destino de monitoramento mais distante do gateway do ISP, outro link nessa rota poderá falhar ou outro dispositivo poderá interferir. Essa configuração pode fazer com que o monitor SLA conclua que a conexão com o ISP principal falhou e faça com que o ASA faça failover desnecessariamente para o link ISP secundário.

Por exemplo, se você escolher um roteador de filial como destino de monitoramento, a conexão

do ISP com a filial poderá falhar, assim como qualquer outro link no caminho. Depois que os ecos ICMP enviados pela operação de monitoramento falharem, a rota rastreada primária será removida, mesmo que o link ISP principal ainda esteja ativo.

Neste exemplo, o gateway principal do ISP usado como destino de monitoramento é gerenciado pelo ISP e está localizado no outro lado do link do ISP. Essa configuração garante que, se os ecos ICMP enviados pela operação de monitoramento falharem, o link do ISP está quase certamente inoperante.

Informações Relacionadas

- Firewalls de próxima geração Cisco ASA 5500-X Series
- Suporte Técnico e Documentação - Cisco Systems