# ASA/PIX 7.x: Exemplo de Configuração de Links de ISP Redundantes ou de Backup

## Índice



## Introdução

Um problema com as rotas estáticas é que não existe um mecanismo inerente para determinar se a rota está ativa ou inativa. A rota permanecerá na tabela de roteamento mesmo que o gateway do próximo salto se torne indisponível. As rotas estáticas são removidas da tabela de roteamento somente se a interface associada do Security Appliance se tornar inativa. Para resolver esse problema, um recurso de rastreamento de rota estática é utilizado para rastrear a disponibilidade de uma rota estática e, caso a rota falhe, removê-la da tabela de roteamento e substituí-la por uma rota de backup.

Este documento fornece um exemplo de como utilizar o recurso de rastreamento de rota estática no PIX 500 Series Security Appliance ou no ASA 5500 Series Adaptive Security Appliance para permitir que o dispositivo use conexões de Internet redundantes ou de backup. Neste exemplo, o rastreamento de rota estática permite que o Security Appliance utilize uma conexão de baixo custo para um provedor de serviços de Internet (ISP) secundário para o caso da linha alugada principal tornar-se indisponível.

Para obter essa redundância, o Security Appliance associa uma rota estática a um destino de monitoração definido por você. A operação de contrato de nível de serviço (SLA) monitora o destino com solicitações periódicas de eco de Internet Control Message Protocol (ICMP). 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 previamente configurada é utilizada no lugar da rota removida. Enquanto a rota de backup estiver em uso, a operação de monitoramento do SLA continuará a tentar alcançar o destino de monitoramento. Uma vez que o destino esteja disponível novamente, a primeira rota será substituída na tabela de roteamento e a rota de backup será removida.

**Nota:** A configuração descrita neste documento não pode ser utilizada para o balanceamento ou compartilhamento de carga. Use essa configuração apenas para fins de redundância ou backup. O tráfego de saída usa o ISP principal e então o ISP secundário no caso de falha do principal. A falha do ISP principal causa uma interrupção temporária do tráfego.

## Pré-requisitos

### Requisitos

Selecione um destino de monitoração que possa responder a solicitações de eco de ICMP. O destino pode ser qualquer objeto de rede que você escolha, mas é recomendável um destino próximo à conexão do seu ISP. Alguns destinos de monitoração possíveis incluem:

- O endereço do gateway do ISP
- Outro endereço gerenciado pelo ISP

- Um servidor em outra rede, tal como um servidor AAA com o qual o Security Appliance precisa se comunicar
- Um objeto de rede persistente em outra rede (um desktop ou notebook que você pode desligar à noite não é uma boa escolha)

Este documento pressupõe que o Security Appliance esteja completamente operacional e configurado de forma a permitir que o Cisco ASDM efetue alterações de configuração.

**Nota:** Para obter informações sobre como permitir que o ASDM configure o dispositivo, consulte Permitindo o Acesso HTTPS ao ASDM.

### Componentes Utilizados

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

- Cisco PIX Security Appliance 515E com software versão 7.2(1) ou posterior
- Cisco Adaptive Security Device Manager 5.2(1) ou posterior

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. Se a sua rede estiver em um ambiente de produção, esteja ciente do impacto potencial de qualquer comando.

### Produtos Relacionados

Você também pode utilizar essa configuração com o Cisco ASA 5500 Series Security Appliance versão 7.2(1).

**Nota:** O comando **backup interface** é necessário para configurar a quarta interface no ASA 5505. Para obter mais informações, consulte Interface de Backup.

### Convenções

Para obter mais informações sobre convenções de documentos, consulte as Convenções de Dicas Técnicas da Cisco.

## Informações de Apoio

Neste exemplo, o Security Appliance mantém duas conexões com a Internet. A primeira conexão é uma linha alugada de alta velocidade acessada por meio de um roteador fornecido pelo ISP principal. A segunda conexão é uma linha de assinante digital (DSL) de menor velocidade acessada por meio de um modem DSL fornecido pelo ISP secundário.

**Nota:** Não há balanceamento de carga neste exemplo.

A conexão DSL permanecerá ociosa pelo tempo em que a linha alugada estiver ativa e o gateway do ISP principal puder ser acessado. Entretanto, se a conexão com o ISP principal cair, o Security Appliance modificará a tabela de roteamento para direcionar o tráfego pela conexão DSL. O rastreamento de rotas estáticas é utilizado para obter essa redundância.

O Security Appliance é configurado com uma rota estática que direciona todo o tráfego da Internet para o ISP principal. A cada 10 segundos, o processo monitor de SLA efetua verificações para confirmar que o gateway do ISP principal pode ser acessado. Se o processo monitor de SLA determinar que o gateway do ISP principal não pode ser acessado, a rota estática que direciona o tráfego para essa interface é removida da tabela de roteamento. Para substituir a rota estática, uma rota estática alternativa que direciona o tráfego para o ISP secundário é instalada. A rota estática alternativa direciona o tráfego para o ISP secundário por meio do modem DSL até que o link do ISP principal possa ser acessado novamente.

Essa configuração fornece uma maneira relativamente barata de garantir que o acesso de saída à Internet permaneça disponível aos usuário por trás do Security Appliance. Como descrito neste documento, essa configuração pode não ser adequada para o acesso de entrada a recursos por trás do Security Appliance. São necessárias habilidades avançadas de redes para que a continuidade das conexões de entrada não seja afetada. Essas habilidades não são cobertas neste documento.

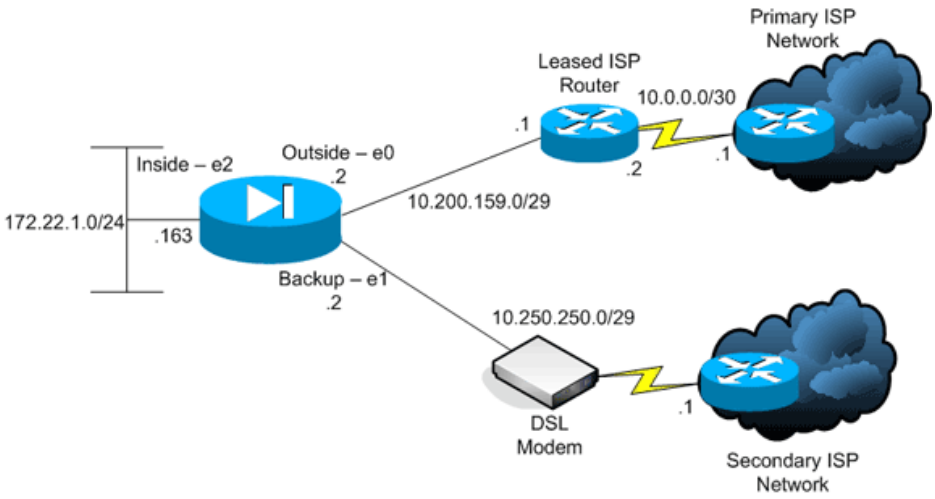
## Configuração

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

**Nota:** Os endereços IP utilizados nesta configuração não são legalmente roteáveis na Internet. Eles são endereços da RFC 1918 utilizados em um ambiente de laboratório.

### Diagrama de Rede

Este documento usa esta configuração de rede:




## Configurações

Este documento utiliza estas configurações:

- Interface de Linha de Comando (CLI)
- Adaptive Security Device Manager (ASDM)

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

## Configuração via CLI

**PIX**

```
pix# show running-config
: Saved
:
PIX Version 7.2(1)
!
hostname pix
domain-name default.domain.invalid
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 10.200.159.2 255.255.255.248
!
interface Ethernet1
nameif backup

!--- A interface conectada ao ISP secundário.
!--- "backup" foi escolhido aqui, mas qualquer nome pode ser atribuído.

security-level 0
ip address 10.250.250.2 255.255.255.248
!
interface Ethernet2
nameif inside
security-level 100
ip address 172.22.1.163 255.255.255.0
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
```

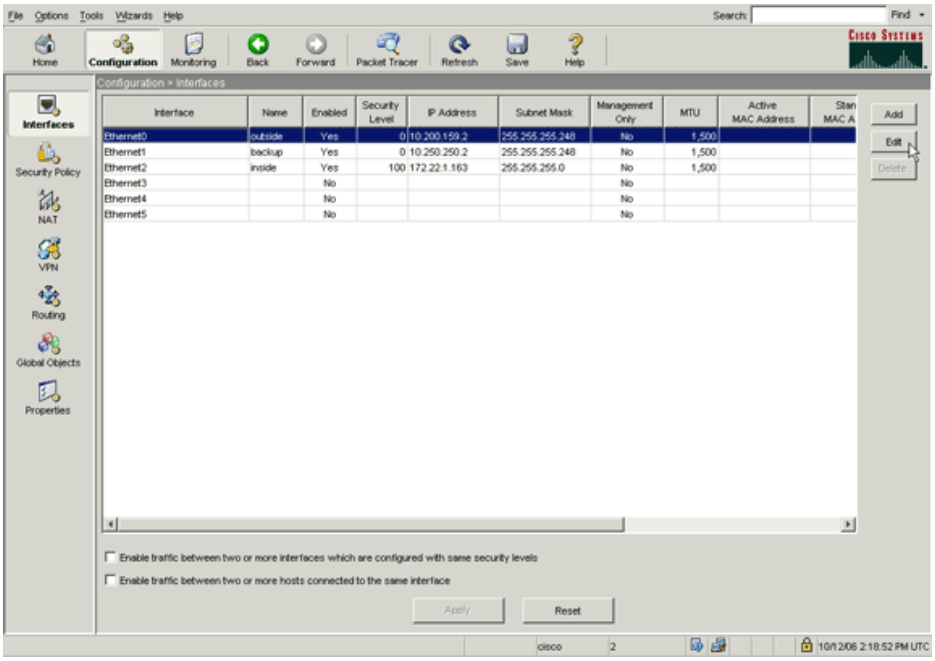
```
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name default.domain.invalid
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu backup 1500
mtu inside 1500
no failover
asdm image flash:/asdm521.bin
no asdm history enable
arp timeout 14400

global (outside) 1 interface
global (backup) 1 interface
nat (inside) 1 172.16.1.0 255.255.255.0

!--- Configuração de NAT para Outside e Backup

route outside 0.0.0.0 0.0.0.0 10.200.159.1 1 track 1

!--- Insira este comando para controlar uma rota estática.
!--- Esta é a rota estática que será instalada na tabela
!--- de roteamento enquanto o objeto rastreado pode ser alcançado.  O valor após a
!--- palavra-chave "track" é um ID de rastreamento especificado.

route backup 0.0.0.0 0.0.0.0 10.250.250.1 254

!--- Define a rota de backup que será usada quando o objeto controlado não estiver disponível.
!--- A distância administrativa da rota de backup deve ser superior à
!--- distância administrativa da rota controlada.
!--- Se o gateway primário não puder ser contatado, a rota será removida
!--- e a rota de backup será instalada na tabela de roteamento
!--- em vez de na rota controlada.

timeout xlate 3:00:00
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 uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted
http server enable
http 172.22.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

sla monitor 123
type echo protocol ipIcmpEcho 10.0.0.1 interface outside
num-packets 3
frequency 10

!--- Configure um novo processo de monitoração com ID 123. Especifique o
!--- protocolo de monitoração e o objeto de rede de destino cuja disponibilidade o processo
!--- de rastreamento monitora.  Especifique o número de pacotes que serão enviados com cada poll.
!--- Especifique a taxa na qual o processo de monitoração é repetido (em segundo).

sla monitor schedule 123 life forever start-time now

!--- Agende o processo de monitoração.  Neste caso, a duração
!--- do processo é especificada como para sempre.  O processo está agendado para começar
!--- assim que este comando for executado.  Da forma como está configurado, este comando permite que
!--- a configuração de monitoração especificada acima determine a frequência na qual o teste
!--- ocorre.  No entanto, você pode agendar este processo de monitoramento para começar no
!--- futuro e ocorrer somente nos horários especificados.

!
track 1 rtr 123 reachability

!--- Associe uma rota estática rastreada com o processo de monitoração do SLA.
!--- O ID de rastreamento corresponde ao ID de rastreamento fornecido para a rota estática a ser monitorada:
!--- route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1
!--- "rtr" = Entrada do Response Time Reporter.  123 é o ID do processo do SLA
!--- definido acima.

telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
```

```
!
policy-map type inspect dns preset_dns_map
parameters
 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 netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:a4a0e9be4593ad43bc17a1cc25e32dc2
: end
```

## Configuração via ASDM

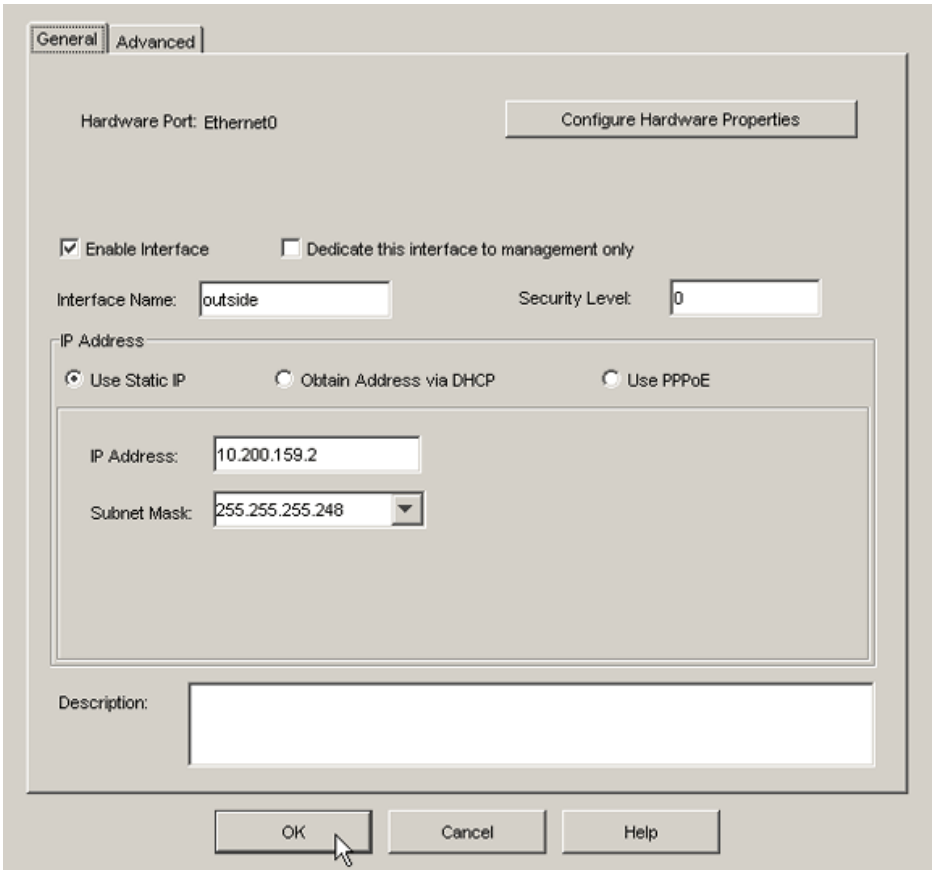
Para configurar o suporte de ISP redundante ou de backup com o aplicativo ASDM, execute estes passos:

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




2. Na lista Interfaces, selecione **Ethernet0** e, em seguida, clique em **Edit**.

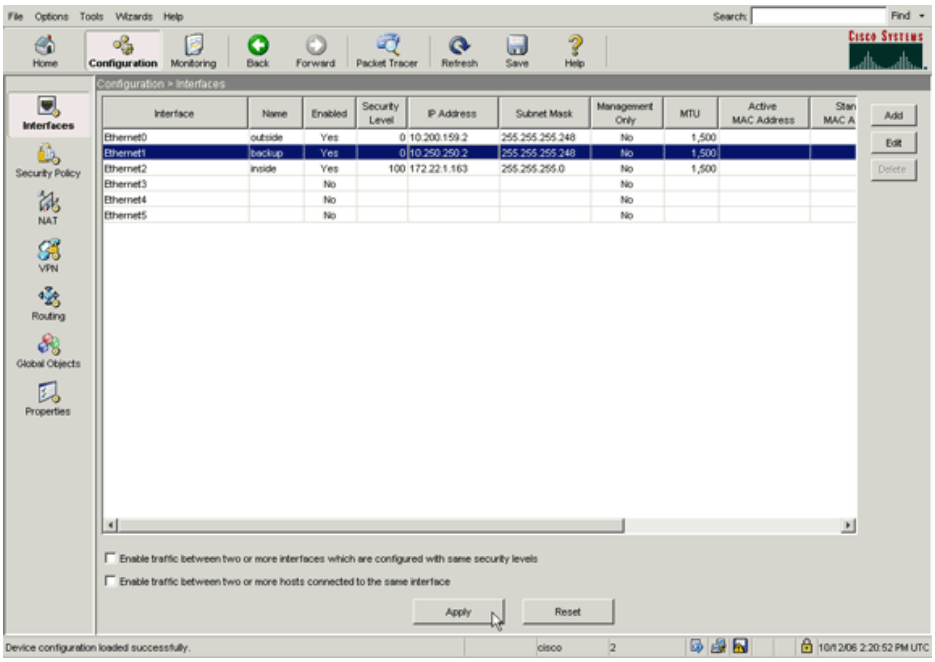
   Esta caixa de diálogo é exibida.



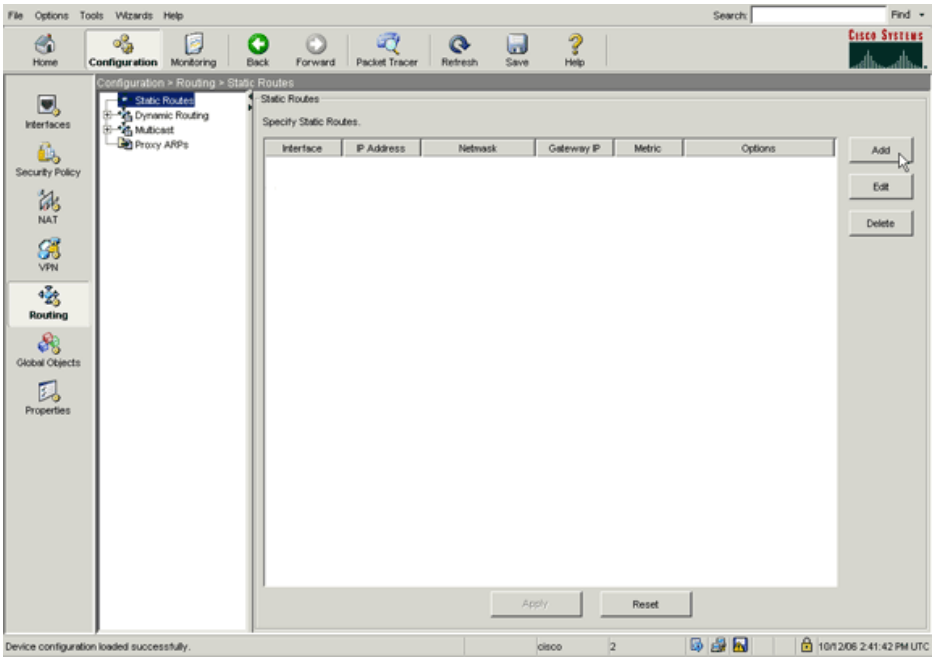

3. Marque a caixa de seleção **Enable Interface** e insira os valores para os campos Interface Name, Security Level, IP Address e Subnet Mask.

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

5. Configure as outras interfaces conforme o necessário e clique em **Apply** para atualizar a configuração do Security Appliance.

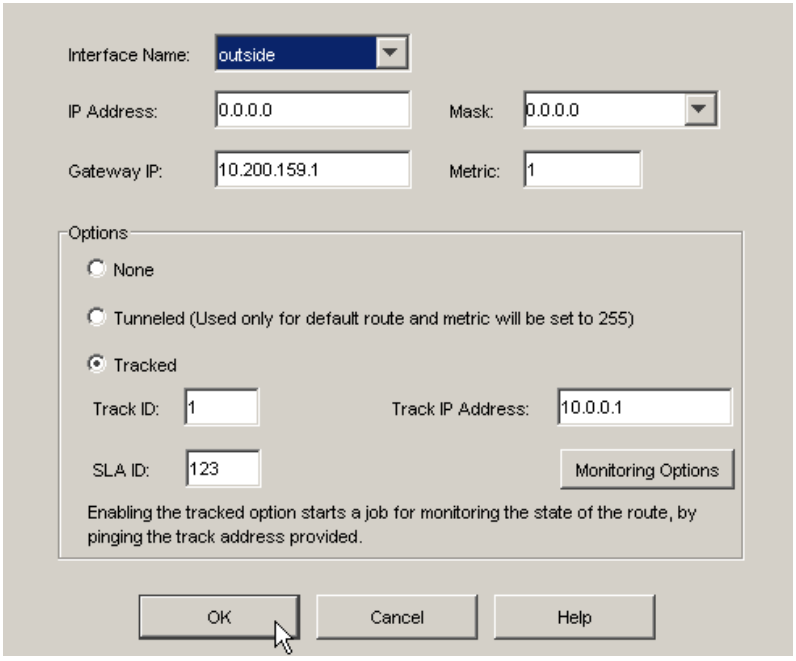



6. Clique na opção **Routing** localizada no lado esquerdo do aplicativo ASDM.




7. Clique em **Add** para adicionar as novas rotas estáticas.

   Esta caixa de diálogo é exibida.

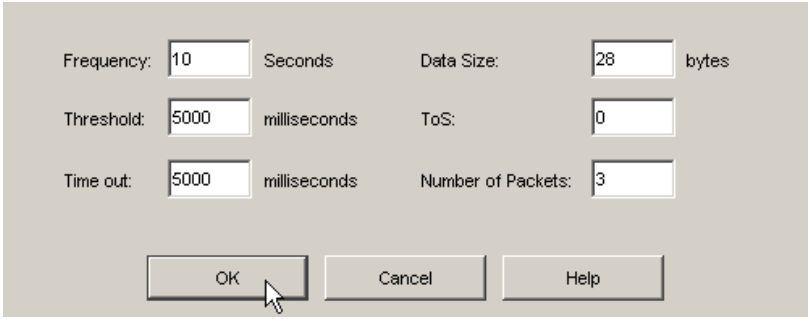



8. Na lista suspensa Interface Name, selecione a interface onde a rota reside e configure a rota padrão para atingir o gateway. Neste exemplo, o gateway do ISP principal é 10.0.0.1, bem como o objeto a ser monitorado pelos ecos de ICMP.

9. Na área Options, clique no botão de opção **Tracked** e insira valores para os campos Track ID, SLA ID e Track IP Address.

10. Clique em **Monitoring Options**.

    Esta caixa de diálogo é exibida.

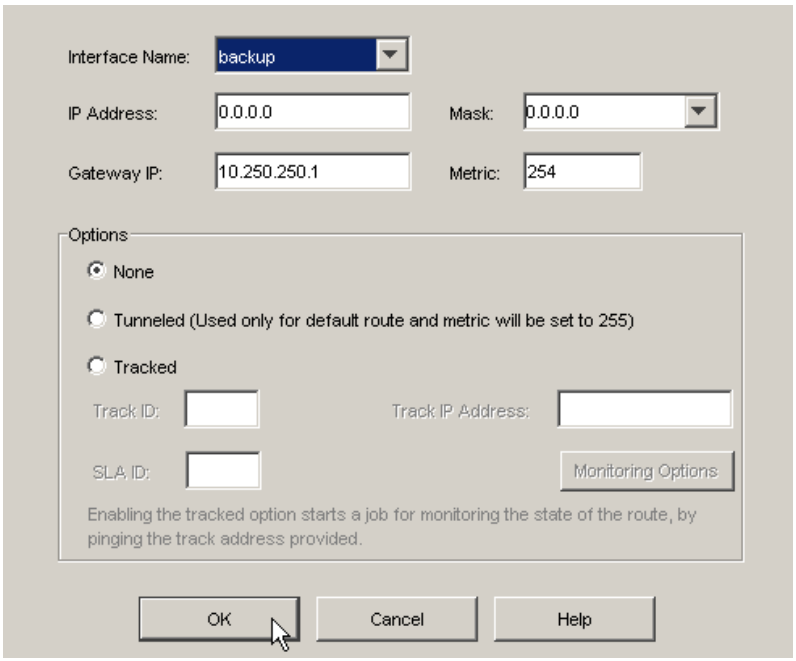



11. Insira os valores de frequência e as outras opções de monitoração e clique em **OK**.

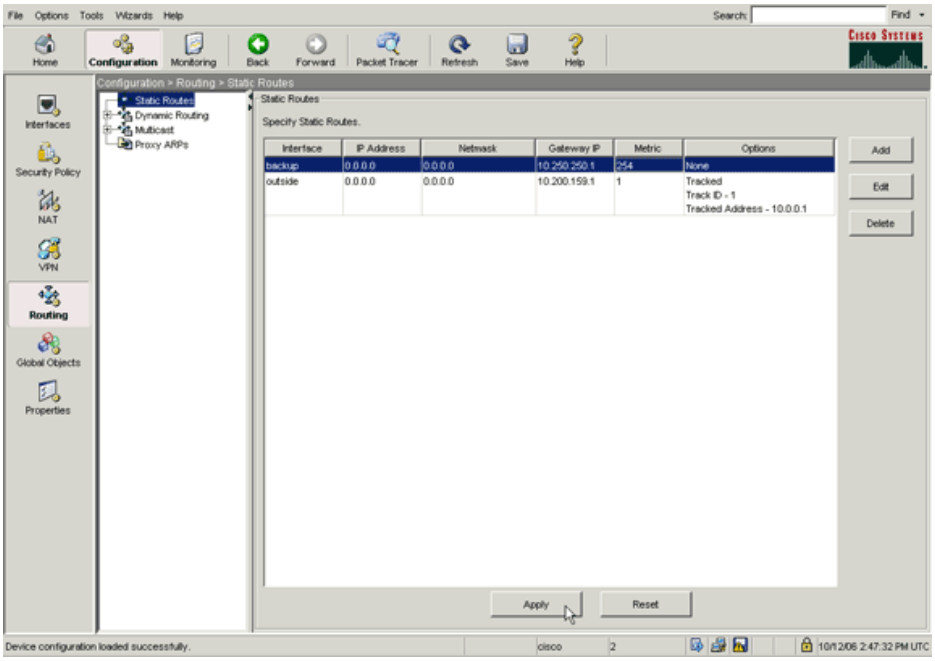
12. Adicione outra rota estática para o ISP secundário para fornecer uma rota para a Internet.

    Para torná-la uma rota secundária, configure-a com uma métrica maior, tal como 254. Caso a rota primária (ISP principal) falhe, ela será removida da tabela de roteamento. Essa rota secundária (ISP secundário) será instalada na tabela de roteamento do PIX.

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




    As configurações serão exibidas na lista Interface.




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

# Verificação

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

## Confirmação de que a Configuração Foi Concluída

Use estes comandos **show** para verificar se sua configuração foi concluída.

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

- **show running-config sla monitor** — Exibe os comandos de SLA na configuração.

```
pix# show running-config sla monitor
sla monitor 123
type echo protocol ipIcmpEcho 10.0.0.1 interface outside
num-packets 3
frequency 10
sla monitor schedule 123 life forever start-time now
```

- **show sla monitor configuration** — Exibe as configurações atuais da operação.

```
pix# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.0.0.1
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: 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** — Exibe as estatísticas operacionais da operação do SLA.
  - Antes do ISP principal falhar, este é o estado operacional:

```
pix# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:59:37.824 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 367
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: 15:00:37.825 UTC Thu Oct 12 2006
Latest operation return code: OK
RTT Values:
RTTAvg: 1       RTTMin: 1       RTTMax: 1
NumOfRTT: 3     RTTSum: 3       RTTSum2: 3
```

  - Após o ISP principal falhar (e o timeout dos ecos de ICMP ser excedido), este será o estado operacional:

```
pix# show sla monitor operational-state
Entry number: 123
Modification time: 13:59:37.825 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 385
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: 15:03:27.825 UTC Thu Oct 12 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

## Confirmação de que a Rota de Backup Está Instalada (Método via CLI)

Use o comando **show route** para determinar quando a rota de backup foi instalada.

- Antes do ISP principal falhar, esta é a tabela de roteamento:

```
pix# 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 10.200.159.1 to network 0.0.0.0

S     64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C     172.22.1.0 255.255.255.0 is directly connected, inside
C     10.250.250.0 255.255.255.248 is directly connected, backup
C     10.200.159.0 255.255.255.248 is directly connected, outside
S*    0.0.0.0 0.0.0.0 [1/0] via 10.200.159.1, outside
```

- Após o ISP principal falhar, a rota estática será removida e, se a rota de backup for instalada, esta será a tabela de roteamento:

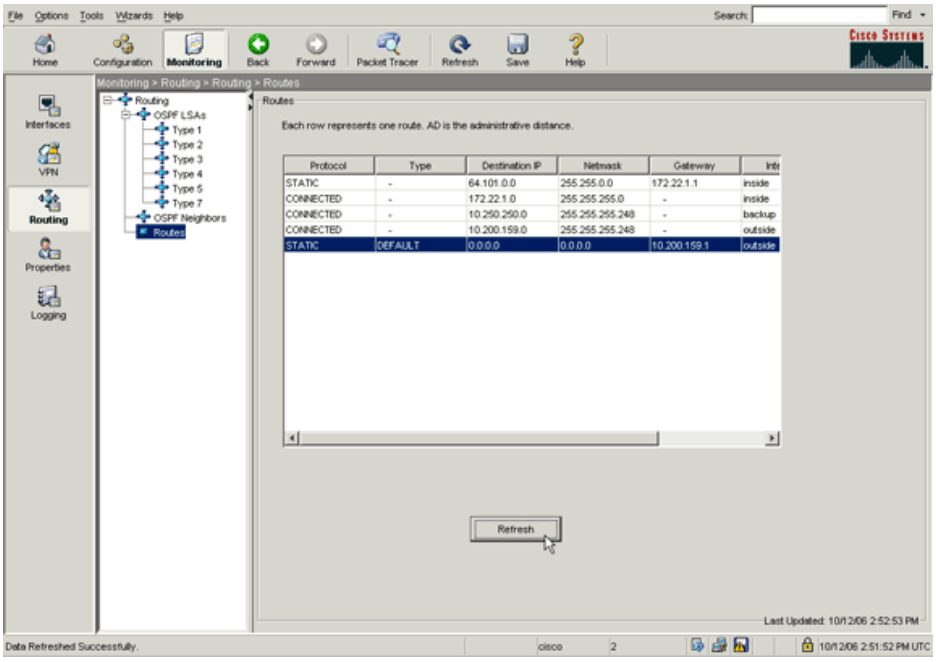
```
pix(config)# show route

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 10.250.250.1 to network 0.0.0.0

S     64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C     172.22.1.0 255.255.255.0 is directly connected, inside
C     10.250.250.0 255.255.255.248 is directly connected, backup
C     10.200.159.0 255.255.255.248 is directly connected, outside
S*    0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

## Confirmação de que a Rota de Backup Está Instalada (Método via ASDM)

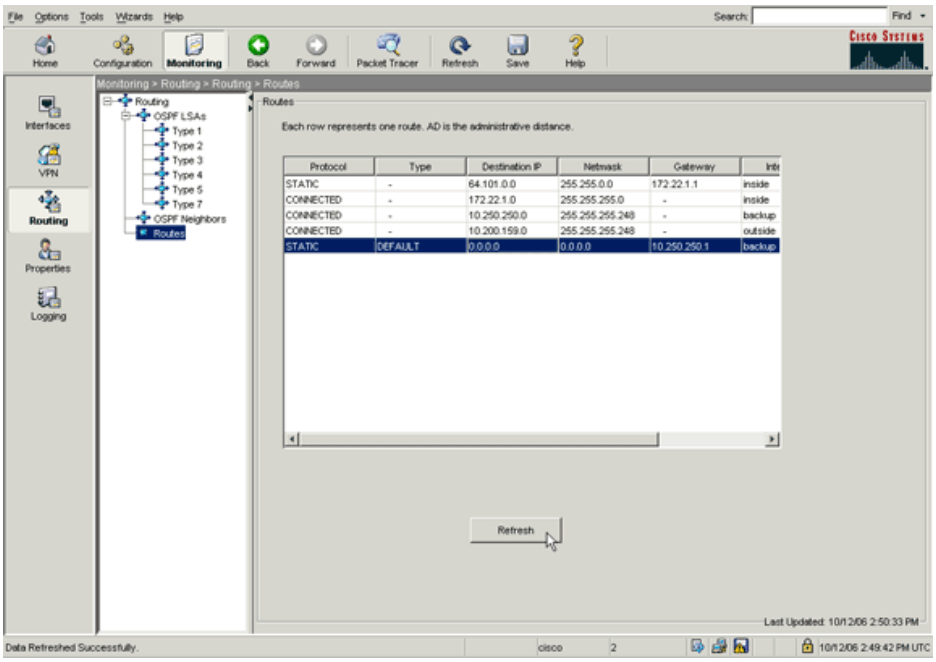
Para confirmar junto ao ASDM que a rota de backup está instalada, execute estes passos:

1. Clique em **Monitoring** e, em seguida, clique em **Routing**.
2. Na árvore Routing, selecione **Routes**.

   - Antes do ISP principal falhar, esta é a tabela de roteamento:




   A rota DEFAULT aponta para 10.0.0.2 pela interface externa.
   - Após o ISP principal falhar, a rota será removida e a rota de backup será instalada. A rota DEFAULT agora apontará para 10.250.250.1 pela interface de backup.




# Troubleshooting

## Comandos de Depuração

- **debug sla monitor trace** — Exibe o progresso da operação de eco.
  - O objeto rastreado (gateway do ISP principal) está ativo e os ecos de ICMP retornam com êxito.

```
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=3 OK
IP SLA Monitor(123) echo operation: RTT=3 OK
IP SLA Monitor(123) echo operation: RTT=4 OK
IP SLA Monitor(123) Scheduler: Updating result
```

  - O objeto rastreado (gateway do ISP principal) está inativo e os ecos de ICMP falham.

```
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** — Exibe os erros encontrados pelo processo monitor de SLA.
  - O objeto rastreado (gateway do ISP principal) está ativo e os ecos de ICMP retornam com êxito.

```
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52696 laddr 10.200.159.2/52696
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52696 laddr 10.200.159.2/52696
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2 duration
               0:00:00
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:00
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               0.200.159.2/52697 laddr 10.200.159.2/52697
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52697 laddr 10.200.159.2/52697
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2
               duration 0:00:00
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:00
```

  - O objeto rastreado (gateway do ISP principal) está inativo e a rota rastreada é removida.

```
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
```

```
              10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
              10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
              10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
              10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
              10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
              10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2
              duration 0:00:02
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:02
%PIX-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.200.159.1,
              distance 1, table Default-IP-Routing-Table, on interface
              outside

!--- 10.0.0.1 está inatingível, assim a rota para o ISP principal é removida.
```

## A Rota Rastreada É Removida Desnecessariamente

Caso a rota rastreada seja 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 pode ou não ser alcançado) está suficientemente próximo do estado da conexão do ISP principal.

Se você selecionar um destino de monitoramento muito distante do gateway do ISP, um outro link contido na rota pode falhar, ou outro dispositivo pode interferir. Essa configuração pode fazer com que o monitor de SLA conclua que a conexão ao ISP principal falhou e forçar o Security Appliance a fazer um failover desnecessário para o link do ISP secundário.

Por exemplo, se você escolher um roteador de uma filial como seu destino de monitoração, a conexão do ISP até a sua filial poderá falhar, bem como quaisquer outros links pelo caminho. Uma vez que os ecos de ICMP enviados pela operação de monitoração falhem, a rota principal rastreada será removida, mesmo que o link do ISP principal ainda esteja ativo.

Neste exemplo, o gateway do ISP principal utilizado como destino de monitoração é gerenciado pelo ISP e se localiza no outro lado do link do ISP. Essa configuração garante que, se os ecos de ICMP que são enviados pela operação de monitoramento falharem, o link do ISP estará quase com certeza inativo.

---



Data da Geração do PDF: 1 Julho 2009

http://www.cisco.com/cisco/web/support/BR/106/1067/1067724_pix-dual-isp.html