Configurar o ASA para os links redundantes ou alternativos ISP

Índice

Introdução

Este documento descreve como configurar a ferramenta de segurança adaptável do 5500 Series de Cisco ASA (ASA) para o uso dos recursos de tracking da rota estática a fim permitir o dispositivo de usar conexões com o Internet redundantes ou alternativas.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- 5555-X Series de Cisco ASA que executa a versão de software 9.x ou mais tarde
- Versão ASDM Cisco 7.x ou mais tarde

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

Você pode igualmente usar esta configuração com a versão 9.1(5) do 5500 Series de Cisco ASA.

> **Note**: **O comando backup interface** é exigido a fim configurar a quarta relação no 5505 Series ASA. Refira a seção da Interface de backup da *referência de comandos do dispositivo do Cisco Security, versão 7.2* para mais informação.

Informações de Apoio

Esta seção fornecem uma vista geral dos recursos de tracking da rota estática que são descritos neste documento, assim como algumas recomendações importantes antes que você comece.

Vista geral dos recursos de tracking da rota estática

Um problema com o uso das rotas estáticas é que nenhum mecanismo inerente existe que pode determinar se a rota é para cima ou para baixo. A rota permanece na tabela de roteamento mesmo se o gateway do salto seguinte se torna não disponível. As rotas estáticas estão removidas da tabela de roteamento somente se a relação associada na ferramenta de segurança vai para baixo. A fim resolver este problema, uns recursos de tracking da rota estática são usados a fim seguir a Disponibilidade de uma rota estática. A característica remove a rota estática da tabela de roteamento e substitui-a com uma rota de backup em cima da falha.

O seguimento da rota estática permite que o ASA use uma conexão barata a um ISP secundário caso a linha alugada preliminar se tornar não disponível. A fim conseguir esta Redundância, o ASA associa uma rota estática com um alvo da monitoração que você defina. A operação do contrato de nível de serviço (SLA) monitora o alvo com requisições de eco ICMP periódicas. Se uma resposta de eco não é recebida, a seguir o objeto está considerado para baixo, e a rota associada é removida da tabela de roteamento. Uma rota de backup previamente configurada é usada no lugar da rota que é removida. Quando a rota de backup estiver no uso, a operação do monitor SLA continua suas tentativas de alcançar o alvo da monitoração. Uma vez que o alvo está disponível outra vez, a primeira rota está substituída na tabela de roteamento, e a rota de backup é removida.

No exemplo que é usado neste documento, o ASA mantém duas conexões ao Internet. A primeira

conexão é uma linha alugada de alta velocidade que seja alcançada através de um roteador fornecido pelo ISP principal. A segunda conexão é um digital subscriber line (DSL) da velocidade mais baixa que seja alcançado através de um modem DSL fornecido pelo ISP secundário.

> **Note**: A configuração que é descrita neste documento não pode ser usada para o Balanceamento de carga ou o compartilhamento de carga, porque não é apoiada no ASA. Use esta configuração para a Redundância ou os propósitos de backup somente. O tráfego de saída usa o ISP principal, e então o ISP secundário se o preliminar falha. A falha do ISP principal causa um rompimento provisório do tráfego.

A conexão DSL é quietude enquanto a linha alugada é ativa e o gateway do ISP principal é alcançável. Contudo, se a conexão ao ISP principal vai para baixo, o ASA muda o tráfego direto da tabela de roteamento à conexão DSL. O seguimento da rota estática é usado a fim conseguir esta Redundância.

O ASA é configurado com uma rota estática que dirija todo o tráfego do Internet ao ISP principal. Cada dez segundos, as verificações de processo do monitor SLA a fim confirmar que o gateway do ISP principal é alcançável. Se o processo do monitor SLA determina que o gateway do ISP principal não é alcançável, a rota estática que dirige o tráfego a essa relação é removida da tabela de roteamento. A fim substituir essa rota estática, uma rota estática alternativa que dirija o tráfego ao ISP secundário é instalada. Esta rota estática alternativa dirige o tráfego ao ISP secundário através do modem DSL até que o link ao ISP principal esteja alcançável.

Esta configuração fornece uma maneira relativamente barata de assegurar-se de que o acesso ao Internet de partida permaneça disponível aos usuários atrás do ASA. Como descrito neste documento, esta instalação não pôde ser apropriada para o acesso de entrada aos recursos atrás do ASA. As habilidades avançadas dos trabalhos em rede são exigidas a fim conseguir conexões de entrada sem emenda. Estas habilidades não são cobertas neste documento.

Recomendações importantes

Antes que você tente a configuração que está descrita neste documento, você deve escolher um alvo da monitoração que possa responder às requisições de eco do Internet Control Message Protocol (ICMP). O alvo pode ser todo o objeto de rede que você escolher, mas um alvo que seja amarrado proximamente a sua conexão do provedor de serviço do Internet (ISP) é recomendado. Estão aqui alguns alvos possíveis da monitoração:

- O endereço de gateway ISP
- Um outro endereço ISP-controlado
- Um server em uma outra rede, tal como um server do Authentication, Authorization, and Accounting (AAA) com que o ASA deve se comunicar
- Um objeto de rede persistente em uma outra rede (um desktop ou um computador notebook que você possa fechar na noite não são uma boa escolha)

Este documento supõe que o ASA é plenamente operacional e configurado a fim permitir que o Cisco Adaptive Security Device Manager (ASDM) faça alterações de configuração.

Tip: Para obter informações sobre de como permitir que o ASDM configure o dispositivo, refira o acesso configurando HTTPS para a seção ASDM do *livro 1 CLI: Guia de configuração de CLI das operações gerais da série de Cisco ASA, 9.1*.

Configurar

Use a informação que é descrita nesta seção a fim configurar o ASA para o uso dos recursos de tracking da rota estática.

Note: Use a ferramenta de consulta de comandos (clientes registrados somente) a fim obter mais informação sobre os comandos que são usados nesta seção.

Note: Os endereços IP de Um ou Mais Servidores Cisco ICM NT que são usados nesta configuração não são legalmente roteável no Internet. São os endereços do RFC 1918, que são usados em um ambiente de laboratório.

Diagrama de Rede

O exemplo que é fornecido nesta seção usa esta instalação de rede:

Configuração de CLI

Use esta informação a fim configurar o ASA através do 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 ASDM

Termine estas etapas a fim configurar o apoio redundante ou do backup ISP com o aplicativo ASDM:

1. Dentro do aplicativo ASDM, clique a **configuração**, e clique então **relações**.

2. Selecione **GigabitEthernet0/1 da** lista das relações, e clique-o então **editam**. Essa caixa de diálogo é exibida:

3. Verifique a caixa de **verificação de interface da possibilidade**, e incorpore os valores apropriados aos campos do *nome*, do *nível de segurança*, do *endereço IP de Um ou Mais Servidores Cisco ICM NT*, e da *máscara de sub-rede da relação*.

4. Clique a **APROVAÇÃO** a fim fechar a caixa de diálogo.

5. Configurar as outras relações como necessárias, e clique-as então **aplicam-se** a fim atualizar a configuração ASA:

6. Selecione o **roteamento** e clique as **rotas estáticas** situadas no lado esquerdo do aplicativo ASDM:

7. O clique **adiciona** a fim adicionar as rotas estáticas novas. Essa caixa de diálogo é exibida:

8. Da lista de drop-down do nome da relação, escolha a relação em que a rota reside, e configurar a rota padrão para alcançar o gateway. Neste exemplo, **203.0.113.2** é o gateway do ISP principal e **4.2.2.2** é o objeto a monitorar com ecos ICMP.

9. Na área das opções, clique o botão de rádio **seguido** e incorpore os valores apropriados à

trilha ID, *SLA ID*, e campos do *endereço IP de Um ou Mais Servidores Cisco ICM NT da trilha*.

10. Clique **opções da monitoração**. Essa caixa de diálogo é exibida:

11. Incorpore os valores apropriados para a frequência e outras opções da monitoração, e clique então a **APROVAÇÃO**.

12. Adicionar uma outra rota estática para o ISP secundário a fim fornecer uma rota para alcançar o Internet. A fim fazer-lhe uma rota secundária, configurar esta rota com uma métrica mais alta, tal como 254. Se a rota principal (ISP principal) falha, essa rota está removida da tabela de roteamento. Esta rota secundária (ISP secundário) é instalada na tabela de roteamento do intercâmbio de Internet privada (PIX) pelo contrário.

13. **APROVAÇÃO do** clique a fim fechar a caixa de diálogo:

    As configurações aparecem na lista de interface:

14. Selecione a configuração de roteamento, e clique-a então **aplicam-se** a fim atualizar a configuração ASA.

Verificar

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

Confirme que a configuração está completa

> **Note**: A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Use estes **comandos show** a fim verificar que sua configuração está completa:

- **mostre o monitor dos precários da executar-configuração** – A saída deste comando indica 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
```

- **mostre a configuração do monitor dos precários** – A saída deste comando indica os ajustes da configuração atual 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:
```

- **mostre o estado operacional do monitor dos precários** – A saída deste comando indica 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 falha (e o intervalo dos ecos ICMP), 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 que a rota de backup está instalada (método de CLI)

Inscreva o **comando show route** a fim confirmar que a rota de backup está instalada.

Antes que o ISP principal falhe, a tabela de roteamento parece similar 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
```

Depois que o ISP principal falha, a rota estática está removida, e a rota de backup é instalada, a tabela de roteamento parece similar 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 que a rota de backup está instalada (método ASDM)

A fim confirmar que a rota de backup está instalada através do ASDM, navegue à **monitoração > roteamento**, e escolha então **rotas da** árvore de roteamento.

Antes que o ISP principal falhe, a tabela de roteamento parece similar àquela mostrada na

imagem seguinte. Note que a **rota padrão** aponta a **203.0.113.2** através da **interface externa**:

Depois que o ISP principal falha, a rota está removida e a rota de backup é instalada. **A rota padrão** aponta agora a **198.51.100.2** através da **Interface de backup**:

Troubleshooting

Esta seção fornece alguns comandos debug úteis e descreve como pesquisar defeitos uma edição onde a rota seguida seja removida desnecessariamente.

Comandos debug

Você pode usar estes comandos debug a fim pesquisar defeitos seus problemas de configuração:

- **debugar o traço do monitor dos precários** – A saída deste comando indica o progresso da operação do eco.

  Se o objeto seguido (gateway do ISP principal) é ascendente e os ecos ICMP sucede, a saída parece similar 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
```

  Se o objeto seguido (gateway do ISP principal) está para baixo e os ecos ICMP falha, a saída parece similar 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
```

- **debugar o erro do monitor dos precários** – A saída deste comando indica todos os erros que o processo do monitor SLA encontrar.

  Se o objeto seguido (gateway do ISP principal) é ascendente e o ICMP sucede, a saída parece similar 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
```

  Se o objeto seguido (gateway do ISP principal) está para baixo e a rota seguida é removido, a saída parece similar 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 seguida é removida desnecessariamente

Se a rota seguida é removida desnecessariamente, assegure-se de que seu alvo da monitoração esteja sempre disponível para receber requisições de eco. Além, assegure-se de que o estado de seu alvo da monitoração (isto é, mesmo se o alvo é alcançável) esteja amarrado proximamente ao estado da conexão do ISP principal.

Se você escolhe um alvo da monitoração que estivesse mais distante ausente do que o gateway ISP, um outro link ao longo dessa rota pôde falhar ou um outro dispositivo pôde interferir. Esta

configuração pôde fazer com o monitor SLA conclua que a conexão ao ISP principal falhou e faça com que o ASA falhe desnecessariamente sobre ao link secundário ISP.

Por exemplo, se você escolhe um roteador do escritório filial como seu alvo da monitoração, a conexão ISP a seu escritório filial poderia falhar, assim como qualquer outro link ao longo do caminho. Uma vez que os ecos ICMP que estão enviados pela falha da operação de monitoramento, a rota seguida preliminar são removidos, mesmo que o link do ISP principal seja ainda ativo.

Neste exemplo, o gateway do ISP principal que é usado como o alvo da monitoração é controlado pelo ISP e ficado situado no outro lado do link ISP. Esta configuração assegura-se de que se os ecos ICMP que estão enviados pela falha da operação de monitoramento, o link ISP são quase certamente para baixo.

Informações Relacionadas

- Firewall da próxima geração do 5500-X Series de Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems