ASA/PIX: Configurar failover ativo/standby no modo transparente

Contents

Introduction

A configuração de failover exige dois mecanismos de segurança conectados entre si através de um link de failover dedicado e, opcionalmente, de um link de failover stateful. A integridade das interfaces ativas e das unidades é monitorada para determinar se as condições específicas do failover são atendidas. Se essas condições são atendidas, o failover ocorre.

O Security Appliance oferece suporte a duas configurações de failover:

- Failover Ativo/Ativo
- Failover Ativo/Standby

Cada configuração de failover tem seu próprio método para determinar e executar failover. Com Failover Ativo/Ativo, ambas as unidades podem passar o tráfego de rede. Isso permite configurar o balanceamento de carga na rede. O Failover Ativo/Ativo está disponível somente em unidades executadas em modo de contexto múltiplo. Com o Failover Ativo/Standby, apenas uma unidade passa o tráfego enquanto a outra unidade espera em um estado de espera. O Failover Ativo/Standby está disponível em unidades executadas em modo de contexto único ou múltiplo. Ambas as configurações de failover suportam failover stateful ou stateless (regular).

Um firewall transparente é um firewall de Camada 2 que atua como um *bump no fio*, ou um *firewall furtivo*, e não é visto como um salto de roteador para dispositivos conectados. O Security Appliance conecta a mesma rede em suas portas interna e externa. Como o firewall não é um salto na rota, você pode facilmente introduzir um firewall transparente em uma rede existente; não é necessário endereçar o IP novamente. Você pode configurar o aplicativo de segurança adaptável para ser executado no modo de firewall roteado padrão ou no modo de firewall transparente. Quando você altera os modos, o aplicativo de segurança adaptável limpa a configuração porque muitos comandos não são suportados em ambos os modos. Se você já tiver uma configuração preenchida, faça o backup dessa configuração antes de alterar o modo; você pode usar essa configuração de backup para referência ao criar uma nova configuração. Consulte Exemplo de Configuração de Firewall Transparente para obter mais informações sobre a configuração do dispositivo de firewall no modo Transparente.

Este documento concentra-se em como configurar um Failover Ativo/Standby no Modo Transparente no ASA Security Appliance.

Nota:Não há suporte ao failover de VPN em unidades no modo de contexto múltiplo. O failover de VPN está disponível somente nas configurações de **Failover Ativo/Standby**.

A Cisco recomenda que você não use a interface de gerenciamento para o failover,

especialmente o failover stateful no qual o Security Appliance envia constantemente informações de conexão de um Security Appliance para o outro. A interface do failover deverá ser pelo menos da mesma capacidade que as interfaces que transmitem tráfego normal e, enquanto as interfaces no ASA 5540 são gigabit, a interface de gerenciamento é somente FastEthernet. A interface de gerenciamento foi projetada somente para o tráfego de gerenciamento e é especificada como management0/0. Mas você pode usar o comando **management-only** para configurar qualquer interface como uma interface somente de gerenciamento. Além disso, para Management 0/0, é possível desabilitar o modo somente de gerenciamento para que a interface possa transmitir tráfego da mesma forma que qualquer outra. Consulte Cisco Security Appliance Command Reference, Versão 8.0 para obter mais informações sobre o comando **management-only**.

Este guia de configuração fornece um exemplo de configuração para incluir uma breve introdução à tecnologia PIX/ASA 7.x Ativo/Standby. Consulte a Referência de Comandos do ASA/PIX para obter mais detalhes sobre a teoria por trás desta tecnologia.

Prerequisites

Requirements

Requisito de hardware

As duas unidades em uma configuração de failover devem ter a mesma configuração de hardware. Eles devem ser do mesmo modelo, ter o mesmo número e tipos de interfaces e a mesma quantidade de RAM.

Nota:O tamanho da memória Flash das duas unidades não precisa ser o mesmo. Se você usar unidades com tamanhos de memória Flash diferentes em sua configuração de failover, verifique se a unidade com memória Flash menor tem espaço suficiente para acomodar os arquivos de imagem de software e os arquivos de configuração. Caso contrário, a sincronização da configuração da unidade com a memória Flash maior para a unidade com a memória Flash menor falhará.

Requisito de software

As duas unidades em uma configuração de failover devem estar nos modos operacionais (roteados ou transparentes, único ou contexto múltiplo). Eles devem ter a mesma versão de software principal (primeiro número) e secundária (segundo número), mas você pode usar versões diferentes do software em um processo de atualização; por exemplo, você pode atualizar uma unidade da versão 7.0(1) para a versão 7.0(2) e manter o failover ativo. A Cisco recomenda que você atualize ambas as unidades para a mesma versão para garantir compatibilidade a longo prazo.

Consulte a seção Performing Zero Downtime Upgrades for Failover Pairs do *Cisco Security Appliance Command Line Configuration Guide, Versão 8.0* para obter mais informações sobre como atualizar o software em um par de failover.

Requisitos de licença

Na plataforma do dispositivo de segurança ASA, pelo menos uma das unidades deve ter uma **licença irrestrita (UR)**.

Observação: talvez seja necessário atualizar as licenças em um par de failover para obter

recursos e benefícios adicionais. Consulte Atualização da Chave de Licença em um Par de Failover para obter mais informações.

Observação: os recursos licenciados (como peers de VPN SSL ou contextos de segurança) em ambos os dispositivos de segurança que participam do failover devem ser idênticos.

Componentes Utilizados

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

- ASA Security Appliance com versão 7.x e 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

Esta configuração também pode ser utilizada com estas versões de hardware e software:

- PIX Security Appliance com versão 7.x e posterior

Conventions

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

Failover Ativo/Standby

Esta seção descreve o Failover Ativo/Standby e inclui estes tópicos:

Visão geral de failover ativo/standby

O Failover Ativo/Standby permite que você use um dispositivo de segurança em standby para assumir a funcionalidade de uma unidade com falha. Quando a unidade ativa falha, ela muda para o estado de espera enquanto a unidade de standby muda para o estado ativo. A unidade que fica ativa assume os endereços IP ou, para um firewall transparente, o endereço IP de gerenciamento e os endereços MAC da unidade com falha e começa a passar o tráfego. A unidade que está agora no estado de standby assume os endereços IP e os endereços MAC em standby. Como os dispositivos de rede não veem nenhuma alteração no emparelhamento de endereços MAC para IP, nenhuma entrada ARP é alterada ou o tempo limite é excedido em qualquer lugar da rede.

Observação: para o modo de contexto múltiplo, o Security Appliance pode fazer o failover de toda a unidade, o que inclui todos os contextos, mas não pode fazer o failover de contextos individuais separadamente.

Status primário/secundário e status ativo/em espera

As principais diferenças entre as duas unidades em um par de failover estão relacionadas a qual unidade está ativa e qual unidade está em standby, a saber, quais endereços IP usar e qual unidade é primária e passa tráfego ativamente.

Existem algumas diferenças entre as unidades com base em qual unidade é primária, conforme especificado na configuração, e qual unidade é secundária:

- A unidade primária torna-se sempre a unidade ativa se ambas as unidades forem ativadas ao mesmo tempo (e tiverem saúde operacional igual).
- O endereço MAC da unidade primária está sempre associado aos endereços IP ativos. A exceção a essa regra ocorre quando a unidade secundária está ativa e não pode obter o endereço MAC primário no link de failover. Nesse caso, o endereço MAC secundário é usado.

Inicialização de dispositivo e sincronização de configuração

A sincronização da configuração ocorre quando um ou ambos os dispositivos no par de failover inicializam. As configurações são sempre sincronizadas da unidade ativa com a unidade em standby. Quando a unidade de standby conclui sua inicialização inicial, ela limpa sua configuração em execução, exceto os comandos de failover necessários para se comunicar com a unidade ativa, e a unidade ativa envia toda sua configuração para a unidade de standby.

A unidade ativa é determinada por:

- Se uma unidade inicializa e detecta um peer já operante como ativo, ela se torna a unidade de standby.
- Se uma unidade inicializa e não detecta um peer, ela se torna a unidade ativa.
- Se ambas as unidades inicializarem simultaneamente, a unidade primária torna-se a unidade ativa e a unidade secundária torna-se a unidade de espera.

Nota:Se a unidade secundária inicializar e não detectar a primária, ela se tornará a unidade ativa. Ele usa seus próprios endereços MAC para os endereços IP ativos. Quando a unidade primária se torna disponível, a unidade secundária altera os endereços MAC para os da unidade primária, o que pode causar uma interrupção no tráfego da rede. Para evitar isso, configure o par de failover com endereços MAC virtuais. Consulte a seção Configuração do Failover Ativo/Standby deste documento para obter mais informações.

Quando a replicação é iniciada, o console do Security Appliance na unidade ativa exibe a mensagem `Beginning configuration replication: Enviando para mate` e, quando estiver concluído, o Security Appliance exibirá a mensagem `End Configuration Replication to mate.` Na replicação, os comandos inseridos na unidade ativa não podem ser replicados corretamente para a unidade de standby, e os comandos inseridos na unidade de standby podem ser sobrescritos pela configuração que é replicada da unidade ativa. Não insira comandos em nenhuma das unidades no par de failover no processo de replicação de configuração. Dependendo do tamanho da configuração, a replicação pode levar de alguns segundos a vários minutos.

Na unidade secundária, você pode observar a mensagem de replicação à medida que ela é sincronizada da unidade primária:

```
ASA> .

        Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.

ASA>
```

Na unidade de espera, a configuração existe apenas na memória de execução. Para salvar a configuração na memória Flash após a sincronização, digite estes comandos:

- Para o modo de contexto único, insira o comando **copy running-config startup-config** na unidade ativa. O comando é replicado para a unidade de standby, que continua a gravar sua configuração na memória Flash.
- Para o modo de contexto múltiplo, insira o comando **copy running-config startup-config** na unidade ativa do espaço de execução do sistema e de dentro de cada contexto no disco. O comando é replicado para a unidade de standby, que continua a gravar sua configuração na memória Flash. Os contextos com configurações de inicialização em servidores externos podem ser acessados de qualquer unidade na rede e não precisam ser salvos separadamente para cada unidade. Como alternativa, você pode copiar os contextos no disco da unidade ativa para um servidor externo e, em seguida, copiá-los para o disco na unidade de standby, onde ficam disponíveis quando a unidade é recarregada.

Replicação de comandos

A replicação de comandos flui sempre da unidade ativa para a unidade de standby. À medida que os comandos são inseridos na unidade ativa, eles são enviados através do link de failover para a unidade de standby. Você não precisa salvar a configuração ativa na memória Flash para replicar os comandos.

Nota:As alterações feitas na unidade de standby não são replicadas para a unidade ativa. Se você executar um comando na unidade de standby, o Security Appliance exibirá a mensagem **** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit. As configurações não estão mais sincronizadas. Essa mensagem é exibida mesmo se você digitar comandos que não afetam a configuração.

Se você inserir o comando **write standby** na unidade ativa, a unidade de standby limpará sua configuração em execução, exceto os comandos failover usados para se comunicar com a unidade ativa, e a unidade ativa enviará toda sua configuração para a unidade de standby.

Para o modo de contexto múltiplo, quando você insere o comando **write standby** no espaço de execução do sistema, todos os contextos são replicados. Se você inserir o comando write standby em um contexto, o comando replicará somente a configuração de contexto.

Os comandos replicados são armazenados na configuração atual. Para salvar os comandos replicados na memória Flash na unidade de standby, insira estes comandos:

- Para o modo de contexto único, insira o comando **copy running-config startup-config** na unidade ativa. O comando é replicado para a unidade de standby, que continua a gravar sua

configuração na memória Flash.
- Para o modo de contexto múltiplo, introduza o comando **copy running-config startup-config** na unidade ativa a partir do espaço de execução do sistema e dentro de cada contexto no disco. O comando é replicado para a unidade de standby, que continua a gravar sua configuração na memória Flash. Os contextos com configurações de inicialização em servidores externos podem ser acessados de qualquer unidade na rede e não precisam ser salvos separadamente para cada unidade. Como alternativa, você pode copiar os contextos no disco da unidade ativa para um servidor externo e, em seguida, copiá-los para o disco na unidade de standby.

Acionadores de failover

A unidade pode falhar se um destes eventos ocorrer:

- A unidade apresenta uma falha de hardware ou de energia.
- A unidade apresenta uma falha de software.
- Muitas interfaces monitoradas falham.
- O comando **no failover ative** é inserido na unidade ativa ou o comando **failover ative** é inserido na unidade de standby.

Ações de failover

No Failover Ativo/Standby, o failover ocorre em uma base de unidade. Mesmo em sistemas executados em modo de contexto múltiplo, você não pode fazer failover de contextos individuais ou de grupos.

Esta tabela mostra a ação de failover para cada evento de falha. Para cada evento de falha, a tabela mostra a política de failover (failover ou sem failover), a ação tomada pela unidade ativa, a ação tomada pela unidade de standby e quaisquer observações especiais sobre a condição de failover e as ações. A tabela mostra o comportamento de failover.

Evento de falha	Política	Ação ativa	Ação em espera	Notas
Falha na unidade ativa (alimentação ou hardware)	Failover	n/a	Tornar-se ativo; marcar como ativo como falha	Nenhuma mensagem de saudação é recebida em nenhuma interface monitorada ou no link de failover.
A unidade anteriormente ativa recupera	Sem failover	Tornar standby	Nenhuma ação	Nenhum
Falha na	Se	Marca	n/a	Quando a unidade de

unidade de espera (alimentação ou hardware)	m failover	r standby como falha		standby é marcada como com falha, a unidade ativa não tenta fazer failover, mesmo que o limite de falha da interface seja ultrapassado.
Falha no link de failover na operação	Sem failover	Marcar a interface de failover como falha	Marcar a interface de failover como falha	Você deve restaurar o link de failover o mais rápido possível porque a unidade não pode fazer failover para a unidade de standby enquanto o link de failover está inativo.
Falha no link de failover na inicialização	Sem failover	Marcar a interface de failover como falha	Torne-se ativo	Se o link de failover estiver inativo na inicialização, ambas as unidades se tornarão ativas.
Falha no link de failover stateful	Sem failover	Nenhuma ação	Nenhuma ação	As informações de estado ficam desatualizadas e as sessões são encerradas se ocorrer um failover.
Falha de interface na unidade ativa acima do limite	Failover	Marcar ativo como falha	Torne-se ativo	Nenhum
Falha de interface na unidade de standby acima do limite	Sem failover	Nenhuma ação	Marcar standby como falha	Quando a unidade de standby é marcada como com falha, a unidade ativa não tenta fazer failover, mesmo que o limite de falha da interface seja ultrapassado.

Failover regular e stateful

O Security Appliance oferece suporte a dois tipos de failover, regular e stateful. Esta seção inclui estes tópicos:

- Failover regular

- Failover stateful

Failover regular

Quando ocorre um failover, todas as conexões ativas são descartadas. Os clientes precisam restabelecer conexões quando a nova unidade ativa assumir o controle.

Failover stateful

Quando o failover stateful está ativado, a unidade ativa transmite continuamente as informações de estado por conexão para a unidade em standby. Após um failover, as mesmas informações de conexão estão disponíveis na nova unidade ativa. Os aplicativos de usuário final suportados não são necessários para se reconectar para manter a mesma sessão de comunicação.

As informações de estado passadas para a unidade de standby incluem:

- A tabela de tradução NAT
- Os estados da conexão TCP
- Os estados da conexão UDP
- A tabela ARP
- A tabela de bridge de Camada 2 (somente quando o Firewall é executado no modo de **firewall transparente**)
- Os estados da conexão HTTP (se a replicação HTTP estiver habilitada)
- A tabela SA ISAKMP e IPSec
- O banco de dados de conexão GTP PDP

As informações que não são passadas para a unidade de standby quando o failover stateful está ativado incluem:

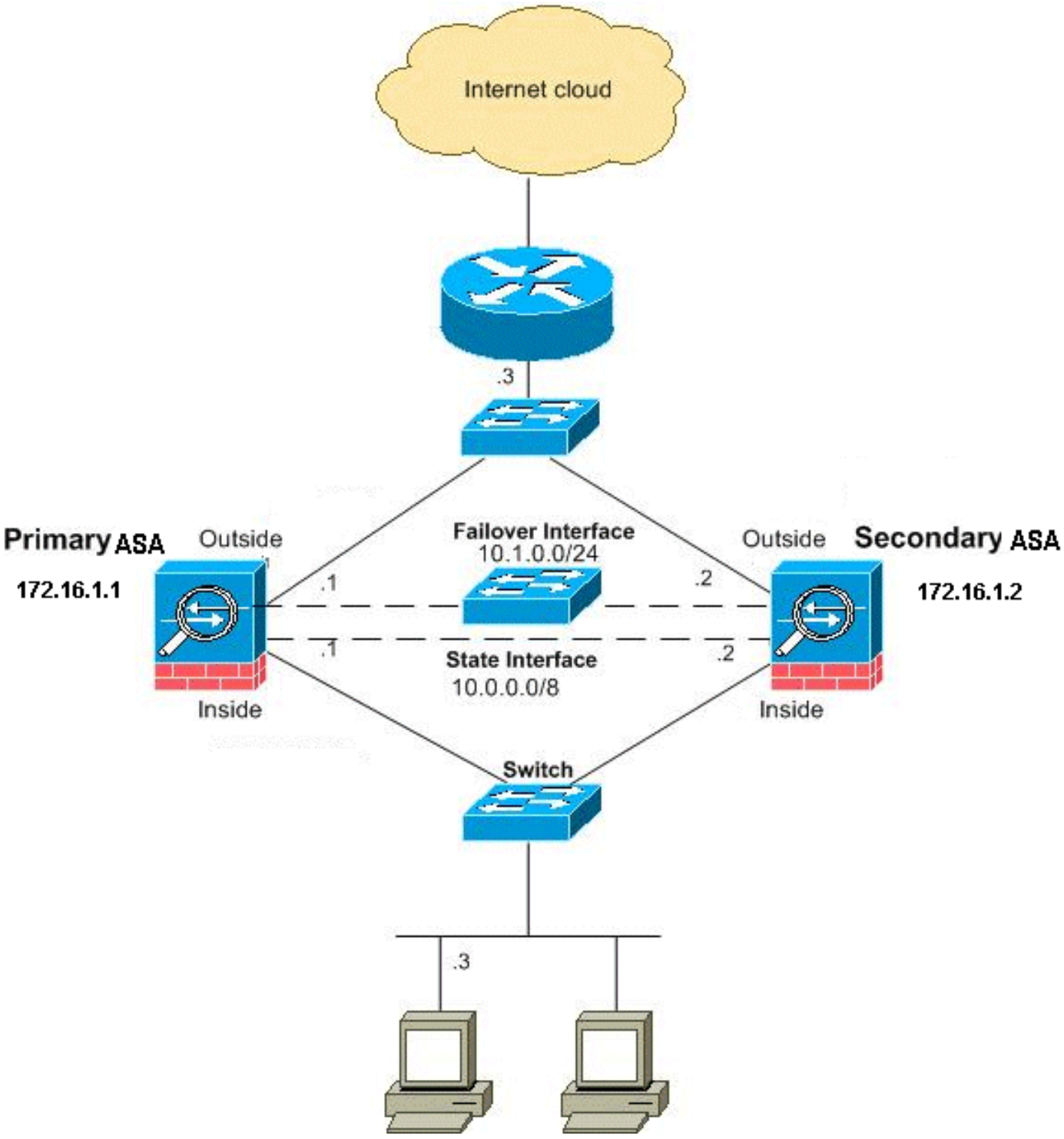
- A tabela de conexão HTTP (a menos que a replicação HTTP esteja habilitada)
- A tabela de autenticação de usuário (uauth)
- As tabelas de roteamento
- Informações de estado para módulos de serviço de segurança

Observação: se ocorrer failover em uma sessão ativa do Cisco IP SoftPhone, a chamada permanecerá ativa porque as informações de estado da sessão de chamada serão replicadas para a unidade em espera. Quando a chamada é encerrada, o cliente IP SoftPhone perde a conexão com o Cisco CallManager . Isso ocorre porque não há informações de sessão para a mensagem de desligamento CTIQBE na unidade de standby. Quando o cliente IP SoftPhone não recebe uma resposta do Cisco CallManager em um determinado período, ele considera o Cisco CallManager inalcançável e se cancela o registro.

Configuração de failover ativo/standby baseado em LAN

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Esta seção descreve como configurar o Failover Ativo/Standby no modo Transparente com um link de failover Ethernet. Quando você configura o failover baseado em LAN, você deve inicializar o dispositivo secundário para reconhecer o link de failover antes que o dispositivo secundário possa obter a configuração atual do dispositivo primário.

Nota:Se você migrar de um failover baseado em cabo para um failover baseado em LAN, será possível pular vários passos, como a atribuição dos endereços IP ativos e de standby para cada interface, que foram concluídos na configuração do failover baseado em cabo.

Configuração da unidade principal

Conclua estes passos para configurar a unidade primária em uma configuração de failover ativo/standby baseada em LAN. Estas etapas fornecem a configuração mínima necessária para

ativar o failover na unidade primária. Para o modo de contexto múltiplo, todas as etapas são executadas no espaço de execução do sistema, a menos que indicado de outra forma.

Para configurar a unidade primária em um par de Failover Ativo/Standby, faça o seguinte:

1. Se ainda não o fez, configure os endereços IP ativo e em standby para a interface de gerenciamento (modo transparente). O endereço IP em standby é usado no Security Appliance que atualmente é a unidade em standby. Ele deve estar na mesma sub-rede do endereço IP ativo.**Nota:Não configure um endereço IP para o link de failover stateful se usar uma interface de failover stateful dedicada.** Use o comando **failover interface ip** para configurar uma interface de failover stateful dedicada em um passo posterior.
   ```
   hostname(config-if)#ip address active_addr netmask
                           standby standby_addr
   ```

   Ao contrário do modo roteado, que exige um endereço IP para cada interface, um firewall transparente tem um endereço IP atribuído a todo o dispositivo. O Security Appliance usa esse endereço IP como o endereço de origem para pacotes que se originam no Security Appliance, como mensagens do sistema ou comunicações AAA. No exemplo, o endereço IP do ASA principal é configurado conforme mostrado abaixo:
   ```
   hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
   ```

   Aqui, 172.16.1.1 é usado para a unidade primária e 172.16.1.2 é atribuído à unidade secundária (standby).**Nota:No modo de contexto múltiplo, você deve configurar o endereço da interface dentro de cada contexto.** Use o comando **change to context** para alternar entre contextos. O prompt de comando muda para `hostname/context(config-if)#`, onde context é o nome do contexto atual.
2. (Somente plataforma PIX Security Appliance) Habilite o failover baseado em LAN.
   ```
   hostname(config)#failover lan enable
   ```

3. Defina a unidade como a unidade primária.
   ```
   hostname(config)#failover lan unit primary
   ```

4. Defina a interface de failover.Especifique a interface a ser usada como a interface de failover.
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   Nesta documentação, o "failover" (nome da interface para Ethernet0) é usado para uma interface de failover.
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   O argumento *if_name* atribui um nome à interface especificada pelo argumento *phy_if* . O argumento *phy_if* pode ser o nome da porta física, como Ethernet1, ou uma subinterface criada anteriormente, como Ethernet0/2.3.Atribua o endereço IP ativo e de standby ao link de failover
   ```
   hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
   ```

   Nesta documentação, para configurar o link de failover, 10.1.0.1 é usado para ativo, 10.1.0.2 para a unidade de standby e "failover" é um nome de interface de Ethernet0.
   ```
   hostname(config)#failover interface ip failover 10.1.0.1
                           255.255.255.0 standby 10.1.0.2
   ```

O endereço IP em standby deve estar na mesma sub-rede do endereço IP ativo. Você não precisa identificar a máscara de sub-rede do endereço de standby.O endereço IP e o endereço MAC do link de failover não são alterados no failover. O endereço IP ativo do link de failover sempre permanece com a unidade primária, enquanto o endereço IP em standby permanece com a unidade secundária.Ative a interface

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

No exemplo, Ethernet3 é usado para failover:

```
hostname(config)#interface ethernet3

hostname(config-if)#no shutdown
```

5. (Opcional) Para ativar o failover stateful, configure o link de failover stateful.Especifique a interface a ser usada como o link de failover stateful.

```
hostname(config)#failover link if_name phy_if
```

Este exemplo usou "state" como um nome de interface para Ethernet2 para trocar informações de estado do link de failover:

```
hostname(config)#failover link state Ethernet2
```

Nota:Se o link de failover stateful usar o link de failover ou uma interface de dados, você só precisará fornecer o argumento if_name.O argumento *if_name* atribui um nome lógico à interface especificada pelo argumento *phy_if.* O argumento *phy_if* pode ser o nome da porta física, como Ethernet1, ou uma subinterface criada anteriormente, como Ethernet0/2.3. Essa interface não deve ser usada para nenhuma outra finalidade, exceto, opcionalmente, como o link de failover.Atribua um endereço IP ativo e em standby ao link de failover stateful.**Nota:Se o link de failover stateful usar o link de failover ou uma interface de dados, pule este passo.** Você já definiu os endereços IP ativos e em standby para a interface.

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

O 10.0.0.1 é usado como um ativo e o 10.0.0.2 como um endereço IP em standby para o link de failover stateful neste exemplo.

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                      standby 10.0.0.2
```

O endereço IP em standby deve estar na mesma sub-rede do endereço IP ativo. Você não precisa identificar a máscara de sub-rede do endereço de standby.O endereço IP e o endereço MAC do link de failover stateful não são alterados no failover, a menos que usem uma interface de dados. O endereço IP ativo permanece sempre com a unidade primária, enquanto o endereço IP em standby permanece com a unidade secundária.Ative a interface.**Nota:Se o link de failover stateful usar o link de failover ou uma interface de dados, pule este passo.** Você já ativou a interface.

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

Nota:Por exemplo, neste cenário, Ethernet2 é usada para o link de failover stateful:

```
hostname(config)#interface ethernet2

hostname(config-if)#no shutdown
```

6. Ative o failover.
```
hostname(config)#failover
```

   Nota:Execute o comando failover no dispositivo primário primeiro. Em seguida, execute-o no dispositivo secundário. Após você executar o comando **failover** no dispositivo secundário, ele começará imediatamente a obter a configuração do dispositivo primário e definirá a si mesmo como *standby*. O ASA primário permanece em operação, transmite tráfego normalmente e marca a si mesmo como o dispositivo *ativo*. Desse ponto em diante, sempre que houver uma falha no dispositivo ativo, o dispositivo de standby se tornará o ativo.
7. Salve a configuração do sistema na memória Flash.
```
hostname(config)#copy running-config startup-config
```

Configuração da unidade secundária

A única configuração necessária na unidade secundária é para a interface de failover. A unidade secundária exige que esses comandos se comuniquem inicialmente com a unidade primária. Depois que a unidade primária envia sua configuração para a unidade secundária, a única diferença permanente entre as duas configurações é o comando **failover lan unit**, que identifica cada unidade como primária ou secundária.

Para o modo de contexto múltiplo, todas as etapas são executadas no espaço de execução do sistema, a menos que observado de outra forma.

Para configurar a unidade secundária, faça o seguinte:

1. (Somente plataforma PIX Security Appliance) Habilite failover baseado em LAN.
```
hostname(config)#failover lan enable
```

2. Defina a interface de failover. Use as mesmas configurações que você usou para a unidade primária.Especifique a interface a ser usada como a interface de failover.
```
hostname(config)#failover lan interface if_name phy_if
```

   Nesta documentação, a Ethernet0 é usada para uma interface de failover de LAN.
```
hostname(config)#failover lan interface failover Ethernet3
```

   O argumento *if_name* atribui um nome à interface especificada pelo argumento *phy_if* .Atribua o endereço IP ativo e de standby ao link de failover.
```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

   Nesta documentação, para configurar o link de failover, 10.1.0.1 é usado para ativo, 10.1.0.2 para a unidade de standby e "failover" é um nome de interface de Ethernet0.
```
hostname(config)#failover interface ip failover 10.1.0.1
                        255.255.255.0 standby 10.1.0.2
```

   Nota:Insira este comando exatamente da mesma forma que ele foi executado na unidade primária quando a interface de failover foi configurada naquela unidade. Ative a interface.
```
hostname(config)#interface phy_if
```

```
hostname(config-if)#no shutdown
```

Por exemplo, neste cenário, Ethernet0 é usada para failover.

```
hostname(config)#interface ethernet3

hostname(config-if)#no shutdown
```

3. (Opcional) Designe esta unidade como a unidade secundária.

```
hostname(config)#failover lan unit secondary
```

Nota:Este passo é opcional porque, por padrão, as unidades são designadas como secundárias, a menos que tenham sido configuradas previamente de outra forma.

4. Ative o failover.

```
hostname(config)#failover
```

Nota:Após o failover ser habilitado, a unidade ativa envia a configuração na memória de execução para a unidade de standby. À medida que a configuração é sincronizada, as mensagens *Beginning configuration replication: O envio para o mate* e *a replicação de configuração final para mate* aparecem no console da unidade ativa.

5. Após a conclusão da replicação da configuração em execução, salve a configuração na memória Flash.

```
hostname(config)#copy running-config startup-config
```

Configurações

Este documento utiliza as seguintes configurações:

ASA principal

```
ASA#show running-config
 ASA Version 7.2(3)
!
!--- To set the firewall mode to transparent mode, !---
use the firewall transparent command !--- in global
configuration mode.

firewall transparent
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif failover

  description LAN Failover Interface
!
interface Ethernet1
 nameif inside
 security-level 100
!
interface Ethernet2
 nameif outside
 security-level 0

!--- Configure no shutdown in the stateful failover
```

```
interface !--- of both Primary and secondary ASA.

interface Ethernet3
 nameif state
 description STATE Failover Interface
!
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
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Assign the IP address to the Primary and !---
Seconday ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2

failover
failover lan unit primary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover link state Ethernet3
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
failover interface ip state 10.0.0.1 255.0.0.0 standby
10.0.0.2

asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
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
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
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:d41d8cd98f00b204e9800998ecf8427e
: end
```

ASA secundário

```
ASA#show running-config
ASA Version 7.2(3)
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
failover
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

Verificar

Uso do comando show failover

Esta seção descreve a saída do comando **show failover**. Em cada unidade, você pode verificar o status do failover com o comando **show failover**.

ASA principal

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
```

```
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 00:08:03 UTC Jan 1 1993
        This host: Primary - Active
                Active time: 1820 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         185        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7012
        Xmit Q:         0       1       185
```

ASA secundário

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 16:39:12 UTC Aug 9 2009
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Active time: 1871 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         183        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
```

```
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7043
        Xmit Q:         0       1       183
```

Use o comando **show failover state** para verificar o estado.

ASA principal

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             00:02:36 UTC Jan 1 1993

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

Unidade secundária

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set
```

Para verificar os endereços IP da unidade de failover, use o comando **show failover interface**.

Unidade primária

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.1
                Other IP Address : 10.1.0.2
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.1
                Other IP Address : 10.0.0.2
```

Unidade secundária

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
```

```
                My IP Address    : 10.1.0.2
                Other IP Address : 10.1.0.1
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.2
                Other IP Address : 10.0.0.1
```

Exibição de interfaces monitoradas

Para visualizar o status das interfaces monitoradas: No modo de contexto único, insira o comando show monitor-interface no modo de configuração global. No modo de contexto múltiplo, insira o comando **show monitor-interface** em um contexto.

ASA principal

```
ASA(config)#show monitor-interface
        This host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

ASA secundário

```
ASA(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
```

Observação: se você não inserir um endereço IP de failover, o comando **show failover** exibirá 0.0.0.0 para o endereço IP e o monitoramento da interface permanecerá em um estado *de espera*. Consulte a seção show failover da *Referência de Comandos do Cisco Security Appliance Versão 7.2* para obter mais informações sobre os diferentes estados de failover.

Exibição dos comandos de failover na configuração atual

Para exibir os comandos failover na configuração atual, insira este comando:

```
hostname(config)#show running-config failover
```

Todos os comandos failover são exibidos. Nas unidades em execução no modo de contexto múltiplo, execute o comando **show running-config failover** no espaço de execução do sistema. Insira o comando **show running-config all failover** para exibir os comandos failover na configuração em execução e incluir comandos para os quais você não alterou o valor padrão.

Testes de funcionalidade de failover

Conclua estes passos para testar a funcionalidade de failover:

1. Teste se sua unidade ativa ou grupo de failover passa o tráfego conforme esperado com o

FTP (por exemplo) para enviar um arquivo entre hosts em diferentes interfaces.
2. Force um failover para a unidade de standby com este comando:Para Failover Ativo/Standby, insira este comando na unidade ativa:
```
hostname(config)#no failover active
```

3. Use o FTP para enviar outro arquivo entre os mesmos dois hosts.
4. Se o teste não tiver sido bem-sucedido, insira o **comando show failover** para verificar o status do failover.
5. Quando terminar, você poderá restaurar a unidade ou o grupo de failover para o status ativo com este comando:Para Failover Ativo/Standby, insira este comando na unidade ativa:
```
hostname(config)#failover active
```

Failover forçado

Para forçar a unidade de standby a se tornar ativa, insira um destes comandos:

Insira este comando na unidade de standby:

```
hostname#failover active
```

Digite este comando na unidade ativa:

```
hostname#no failover active
```

Failover desativado

Para desabilitar o failover, insira este comando:

```
hostname(config)#no failover
```

Se você desabilitar o failover em um par Ativo/Standby, ele fará com que o estado ativo e standby de cada unidade seja mantido até que você reinicie. Por exemplo, a unidade de standby permanece no modo de espera para que ambas as unidades não comecem a passar o tráfego. Para ativar a unidade de standby (mesmo com failover desabilitado), consulte a seção Forçando failover.

Se você desabilitar o failover em um par Ativo/Ativo, isso fará com que os grupos de failover permaneçam no estado ativo em qualquer unidade em que estejam atualmente ativos, independentemente da unidade em que estejam configurados. O comando **no failover** pode ser executado no espaço de execução do sistema.

Restauração de uma unidade com falha

Para restaurar uma unidade com falha para um estado sem falha, insira este comando:

```
hostname(config)#failover reset
```

Se você restaurar uma unidade com falha para um estado sem falha, ela não a tornará automaticamente ativa; as unidades ou grupos restaurados permanecem no estado de espera até serem ativados por failover (forçado ou natural). Uma exceção é um grupo de failover configurado com o comando preempt. Se estiver anteriormente ativo, um grupo de failover se tornará ativo se estiver configurado com o comando preempt e se a unidade na qual ele falhou for sua unidade preferencial.

Troubleshoot

Quando ocorre um failover, ambos os dispositivos de segurança enviam mensagens do sistema. Esta seção inclui estes tópicos

Monitoramento de failover

Este exemplo demonstra o que acontece quando o failover não começou a monitorar as interfaces de rede. O failover não começa a monitorar as interfaces de rede até ouvir o segundo pacote `hello` da outra unidade nessa interface. Isso leva cerca de 30 segundos. Se a unidade estiver conectada a um switch de rede que executa o Spanning Tree Protocol (STP), isso levará o dobro do tempo de `atraso de encaminhamento` configurado no switch, que normalmente é configurado como 15 segundos, mais esse atraso de 30 segundos. Isso ocorre porque na inicialização do ASA e imediatamente após um evento de failover, o switch de rede detecta um loop temporário de bridge. Após a detecção desse loop, ele pára de encaminhar pacotes nessas interfaces para o tempo de `atraso de encaminhamento`. Em seguida, ele entra no modo `de escuta` por um tempo `de atraso de encaminhamento` adicional, dentro do qual o switch escuta os loops de bridge, mas não encaminha tráfego ou encaminha pacotes `hello de failover`. Após o dobro do tempo de atraso de encaminhamento (30 segundos), o tráfego volta a fluir. Cada ASA permanece em um modo de `espera` até que ouça 30 segundos de pacotes `hello` da outra unidade. Dentro do tempo em que o ASA passa tráfego, ele não falha na outra unidade com base em não ouvir os pacotes `hello`. Todos os outros monitoramentos de failover ainda ocorrem, ou seja, Power, Interface Loss of Link e Failover Cable `hello`.

Para failover, a Cisco recomenda que os clientes ativem o portfast em todas as portas de switch que se conectam às interfaces do ASA. Além disso, o trunking e a canalização devem ser desabilitados nessas portas. Se a interface do ASA for desativada no failover, o switch não terá que esperar 30 segundos enquanto a porta passa de um estado de escuta para aprendizado e encaminhamento.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
```

```
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

Em resumo, verifique estes passos para restringir os problemas de failover:

- Verifique os cabos de rede conectados à interface no estado de espera/falha e, se possível, substitua-os.
- Se houver um switch conectado entre as duas unidades, verifique se as redes conectadas à interface no estado de espera/falha estão funcionando corretamente.
- Verifique a porta do switch conectada à interface no estado de espera/falha e, se possível, use outra porta de FE no switch.
- Verifique se você habilitou o port fast e desabilitou o trunking e a canalização nas portas do switch conectadas à interface.

Falha de unidade

Nesse exemplo, o failover detectou uma falha. Observe que a Interface 1 na unidade principal é a origem da falha. As unidades estão de volta no modo `de espera` devido à falha. A unidade com falha se removeu da rede (as interfaces estão inoperantes) e não envia mais pacotes `hello` na rede. A unidade ativa permanece em um estado de `espera` até que a unidade com falha seja substituída e as comunicações de failover sejam iniciadas novamente.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
```

Falha na conexão de alocação de LU

Um problema de memória pode existir se você receber esta mensagem de erro:

```
Falha na conexão de alocação de LU
```

Esse problema está documentado na ID de bug da Cisco CSCte80027 (somente clientes registrados) . Para resolver esse problema, atualize o firewall para uma versão de software na qual esse bug é corrigido. Algumas das versões do software ASA sob as quais esse bug foi corrigido são 8.2(4), 8.3(2) e 8.4(2).

Mensagens do sistema de failover

O Security Appliance emite várias mensagens do sistema relacionadas ao failover no nível de prioridade 2, o que indica uma condição crítica. Para exibir estas mensagens, consulte

Configuração de Log e Mensagens do Log do Sistema do Cisco Security Appliance para habilitar o log e ver descrições das mensagens de sistema.

Nota:Na troca, o failover encerra de forma lógica e ativa interfaces, o que gera as mensagens 411001 e 411002 do Syslog. Esta é uma atividade normal.

Mensagens de depuração

Para ver mensagens de depuração, insira o comando **debug fover**. Consulte a Referência de Comandos do Cisco Security Appliance para obter mais informações.

Nota:Como a saída de depuração recebe uma prioridade alta no processamento da CPU, ela pode afetar drasticamente o desempenho do sistema. Por isso, use o comando **debug fover** somente para fazer o troubleshooting de problemas específicos ou em sessões de troubleshooting acompanhadas pela equipe de suporte técnico da Cisco.

SNMP

Para receber armadilhas de syslog SNMP para failover, configure o agente SNMP para enviar interceptações SNMP para estações de gerenciamento SNMP, definir um host syslog e compilar o MIB de syslog da Cisco em sua estação de gerenciamento SNMP. Consulte os comandos **snmp-server** e **logging** na Referência de Comandos do Cisco Security Appliance para obter mais informações.

Tempo de Poll do Failover

Para especificar os tempos de poll e espera da unidade de failover, use o comando **failover polltime** no modo de configuração global.

O `failover polltime unit msec [time]` pesquisa mensagens de saudação para representar o intervalo de tempo a fim verificar a existência da unidade em standby.

De forma semelhante, failover holdtime unit msec [time] representa o período de tempo durante o qual uma unidade deve receber uma mensagem de hello no link de failover. Decorrido esse tempo, a unidade peer é declarada como tendo sofrido uma falha.

Para especificar os tempos de poll e espera da interface de dados em uma configuração de failover Ativo/Standby, use o comando **failover polltime interface** no modo de configuração global. Para restaurar os tempos de poll e espera padrão, use a forma **no** deste comando.

failover polltime interface [msec] *time* **[holdtime** *time***]**

Use o comando **failover polltime interface** para alterar a freqüência na qual cada pacote de hello é enviado pelas interfaces de dados. Esse comando está disponível somente no failover Ativo/Standby. No failover Ativo/Ativo, use o comando **polltime interface** no modo de configuração de grupo do failover em vez do comando **failover polltime interface**.

Não é possível inserir um valor de **holdtime inferior a 5 vezes o tempo de poll da interface.** Quando um tempo de poll menor é usado, o Security Appliance pode detectar uma falha e acionar o failover mais rápido. No entanto, uma detecção muito rápida pode causar trocas desnecessárias

quando a rede está congestionada temporariamente. O teste da interface começa quando um pacote de hello não é ouvido na interface por metade do tempo de espera.

Você pode incluir o comando failover polltime unit e o comando failover polltime interface na configuração.

Este exemplo define a freqüência do tempo de poll da interface como 500 milissegundos e o tempo de espera como 5 segundos:

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

Consulte a seção failover polltime da *Referência de Comandos do Cisco Security Appliance, Versão 7.2* para obter mais informações.

Configuração da Exportação do Certificado/Chave Privada no Failover

O dispositivo primário replica automaticamente o certificado/chave privada para a unidade secundária. Emita o comando **write memory** na unidade ativa para replicar a configuração, que inclui o certificado/chave privada, para a unidade em espera. Todos os certificados/chaves na unidade de standby são apagados e preenchidos novamente com a configuração da unidade ativa.

Nota:Você não deve importar manualmente certificados, chaves e pontos de confiança do dispositivo ativo para exportá-los para o dispositivo de standby.

AVISO: Falha na descriptografia da mensagem de failover.

Mensagem de Erro:

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

Esse problema ocorre devido à configuração da chave de failover. Para resolver esse problema, remova a chave de failover e configure a nova chave compartilhada.

Problema: O failover está sempre oscilando após a configuração do failover transparente de vários modos Ativo/Standby

O failover é estável quando as interfaces internas de ambos os ASAs estão diretamente conectadas e as interfaces externas de ambos os ASA estão diretamente conectadas. No entanto, o failover não é bem-sucedido quando um switch é usado no intervalo.

Solução: Desative a BPDU nas interfaces do ASA para resolver esse problema.

Failover de Módulos ASA

Se o Advanced Inspection and Prevention Security Services Module (AIP-SSM) ou o Content Security and Control Security Services Module (CSC-SSM) forem usados nas unidades ativa e de standby, eles funcionarão de forma independente do ASA em termos de failover. **Os módulos devem ser configurados manualmente em unidades ativas e em standby; o failover não replica a**

configuração do módulo.

Em termos de failover, ambas as unidades ASA que possuem os módulos AIP-SSM ou CSC-SSM devem ser do mesmo tipo de hardware. Por exemplo, se a unidade primária possuir o módulo ASA-SSM-10, a unidade secundária deverá possuir o módulo ASA-SSM-10.

Falha na alocação do bloco de mensagem de failover

Mensagem de erro `%PIX|ASA-3-105010: Falha na alocação do bloco de mensagem de failover (principal)`

Explicação: A memória de bloqueio foi esgotada. Essa é uma mensagem transitória e o Security Appliance deve se recuperar. *Primary* também pode ser listado como *Secondary* para a unidade secundária.

Ação recomendada: Use o comando **show block** para monitorar a memória de bloco atual.

Problema de failover do módulo AIP

Se houver dois ASAs em uma configuração de failover e cada um tiver um AIP-SSM, você deverá replicar manualmente a configuração dos AIP-SSMs. Somente a configuração do ASA é replicada pelo mecanismo de failover. O AIP-SSM não está incluído no failover.

Primeiro, o AIP-SSM opera independentemente do ASA em termos de failover. Para failover, tudo o que é necessário do ponto de vista do ASA é que os módulos AIP sejam do mesmo tipo de hardware. Além disso, como em qualquer outra parte do failover, a configuração do ASA entre o ativo e o standby deve estar sincronizada.

Quanto à configuração dos AIPs, eles são efetivamente sensores independentes. Não há failover entre os dois e eles não têm conhecimento um do outro. Eles podem executar versões independentes de código. Ou seja, eles não precisam ser iguais e o ASA não se importa com a versão do código no AIP em relação ao failover.

O ASDM inicia uma conexão com o AIP através do IP da interface de gerenciamento que você configurou no AIP. Em outras palavras, ele se conecta ao sensor tipicamente através do HTTPS, que depende de como você configura o sensor.

Você pode ter um failover do ASA independente dos módulos IPS (AIP). Você ainda está conectado ao mesmo IP de gerenciamento. Para se conectar ao outro AIP, você deve se reconectar ao IP de gerenciamento para configurá-lo e acessá-lo.

Consulte o ASA: Exemplo de Configuração de Envio de Tráfego de Rede do ASA para o AIP SSM para obter mais informações e exemplos de configurações sobre como enviar o tráfego de rede que passa pelo Cisco ASA 5500 Series Adaptive Security Appliance (ASA) para o Advanced Inspection and Prevention Security Services Module (AIP-SSM) (IPS)

Problemas conhecidos

Quando você tenta acessar o ASDM no ASA secundário com software versão 8.x e ASDM versão 6.x para configuração de failover, este erro é recebido:

```
Erro: O nome no certificado de segurança é inválido ou não corresponde ao nome do site
```

No certificado, o Emitente e o Nome do assunto são o endereço IP da unidade *ativa*, não o endereço IP da unidade *standby*.

No ASA versão 8.x, o certificado interno (ASDM) é replicado da unidade ativa para a unidade em standby, o que causa a mensagem de erro. Mas, se o mesmo firewall for executado no código versão 7.x com ASDM 5.x e você tentar acessar o ASDM, você receberá este aviso de segurança regular:

```
O certificado de segurança tem um nome válido que corresponde ao nome da página que está a
tentar ver
```

Quando você verifica o certificado, o emissor e o nome do assunto são o endereço IP da unidade de standby.

Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Cisco PIX Firewall Software
- Configuração de failover do módulo de serviços de firewall (FWSM)
- Solução de problemas de failover do FWSM
- Como o failover funciona no Cisco Secure PIX Firewall
- Suporte Técnico e Documentação - Cisco Systems