PIX/ASA: Exemplo de Configuração de Failover Ativo/Ativo

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** e **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).

Este documento descreve como configurar o Failover Ativo/Ativo no Cisco PIX/ASA Security Appliance.

Consulte PIX/ASA 7.x: Exemplo de Configuração de Failover Ativo/Standby para obter mais informações sobre as configurações de Failover Ativo/Standby.

Observação: o failover de VPN não é suportado em unidades que são executadas em modo de contexto múltiplo, pois a VPN não é suportada em contexto múltiplo. O failover de VPN está disponível somente para configurações **de failover ativo/standby** em configurações de contexto único.

Este guia de configuração apresenta um exemplo de configuração que inclui uma rápida introdução à tecnologia Ativo/Ativo do PIX/ASA 7.x. Consulte a Referência de Comandos do Cisco Security Appliance Versão 7.2 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 Performing Zero Downtime Upgrades for Failover Pairs para obter mais informações sobre como atualizar o software em um par de failover.

Requisitos de licença

Na plataforma PIX/ASA Security Appliance, ao menos uma das unidades deve possuir uma **licença irrestrita (UR)**. A outra unidade pode ter uma licença Somente Failover Ativo-Ativo (FO_AA) ou outra licença UR. Unidades com licenças restritas não podem ser usadas para o failover, e duas unidades com licenças FO_AA não podem ser usadas em conjunto como um par de failover.

Observação: talvez seja necessário atualizar as licenças em um par de failover para obter recursos e benefícios adicionais. Para obter mais informações sobre atualização, consulte Atualização da chave de licença em um par de failover

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.

Observação: a licença de FO não oferece suporte a Failover Ativo/Ativo.

Componentes Utilizados

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

- PIX 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:

- ASA com versão 7.x e posterior

Nota:O Failover Ativo/Ativo não está disponível no ASA 5505 Series Adaptive Security Appliance.

Conventions

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

Failover Ativo/Ativo

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

Visão Geral do Failover Ativo/Ativo

O Failover Ativo/Ativo está disponível somente em Security Appliances em execução no modo de contexto múltiplo. Em uma configuração de Failover Ativo/Ativo, ambos os Security Appliances podem transmitir tráfego de rede.

No Failover Ativo/Ativo, os contextos de segurança no Security Appliance são divididos em grupos de failover. Um grupo de failover nada mais é do que um grupo lógico de um ou mais contextos de segurança. É possível criar no máximo dois grupos de failover no Security Appliance. O contexto admin é sempre um membro do grupo de failover 1. Os contextos de segurança não atribuídos também são membros do grupo de failover 1 por padrão.

Os grupos de failover formam a unidade base do Failover Ativo/Ativo. Monitoração de falhas de interface, failover e os status ativo/standby são todos atributos de um grupo de failover, e não da unidade. Quando um grupo de failover ativo falha, ele entra no estado de standby. Ao mesmo tempo, o grupo de failover de standby se torna ativo. As interfaces no grupo de failover que se torna ativo assumem os endereços MAC e IP das interfaces do grupo de failover que falhou. As interfaces no grupo de failover que agora está no estado de standby assumem os endereços MAC e IP de standby.

Nota:A falha de um grupo de failover em uma unidade não significa que a unidade falhou. A unidade ainda pode ter outro grupo de failover transmitindo tráfego.

Status primário/secundário e status ativo/em espera

Assim como no Failover Ativo/Standby, uma unidade em um par de Failover Ativo/Ativo é designada como a unidade primária e a outra como unidade secundária. Ao contrário do Failover Ativo/Standby, essa designação não indica que unidade se torna ativa quando ambas as unidades são iniciadas simultaneamente. Em vez disso, a designação primária/secundária faz duas coisas:

- Determina qual unidade fornece a configuração em execução para o par quando eles tentam inicializar simultaneamente.
- Determina em qual unidade cada grupo de failover entra no estado ativo quando as unidades inicializam ao mesmo tempo. Cada grupo de failover na configuração é configurado com uma preferência de unidade primária ou secundária. Você pode configurar ambos os grupos de failover no estado ativo em uma única unidade do par, enquanto que as outras unidades contêm os grupos de failover no estado de standby. No entanto, uma configuração mais típica é atribuir cada grupo de failover a uma preferência de função diferente para tornar cada um ativo em uma unidade diferente, distribuindo o tráfego entre os dispositivos.**Nota:O Security Appliance não fornece serviços de balanceamento de carga.** O balanceamento de carga deve ser gerenciado por um roteador que envia tráfego para o Security Appliance.

A unidade em que cada grupo de failover se torna ativo é determinada conforme mostrado.

- Quando uma unidade inicializa sem que a unidade peer esteja disponível, ambos os grupos de failover se tornam ativos na unidade.
- Quando uma unidade inicializa enquanto a unidade peer está ativa (com ambos os grupos de failover no estado ativo), os grupos de failover permanecerão no estado ativo na unidade ativa independentemente da preferência de primário ou secundário do grupo de failover até que:Um failover ocorra.Você force manualmente o grupo de failover para a outra unidade com o comando **no failover active**.Você configure o grupo de failover com o comando **preempt**, o que fará com que o grupo de failover se torne ativo automaticamente na unidade preferida quando a unidade se tornar disponível.
- Quando ambas as unidades inicializarem ao mesmo tempo, cada grupo de failover se tornará ativo em sua unidade preferencial após as configurações terem sido sincronizadas.

Inicialização de dispositivo e sincronização de configuração

A sincronização da configuração ocorre quando uma ou ambas as unidades em um par de failover inicializam. As configurações são sincronizadas da seguinte forma:

- Quando uma unidade inicializa quando a unidade peer está ativa (com ambos os grupos de failover ativos), a unidade que está inicializando se comunica com a unidade ativa para obter a configuração em execução, independentemente da designação de primária ou secundária da primeira unidade.
- Quando ambas as unidades inicializam ao mesmo tempo, a unidade secundária obtém a configuração em execução da unidade primária.

Quando a replicação é iniciada, o console do Security Appliance na unidade que está enviando a configuração exibe a mensagem **"Começando a replicação da configuração: Enviando para mate,"** e quando estiver concluído, o Security Appliance exibirá a mensagem **"End Configuration Replication to mate".** Durante a replicação, os comandos inseridos na unidade que envia a configuração podem não ser replicados adequadamente na unidade peer, e os comandos inseridos na unidade que recebe a configuração podem ser sobrescritos pela configuração que está sendo recebida. Evite executar comandos em qualquer uma das unidades do par de failover durante o processo de replicação de configuração. Dependendo do tamanho da configuração, a replicação pode levar de alguns segundos a vários minutos.

Na unidade que recebe a configuração, a configuração existe somente na memória de execução. Para salvar a configuração na memória Flash após a sincronização, insira o comando **write memory all** no espaço de execução do sistema na unidade que possui o grupo de failover 1 no

estado ativo. O comando é replicado para a unidade peer, a qual escreve sua configuração na memória Flash. O uso da palavra-chave **all** com esse comando faz com que o sistema e todas as suas configurações de contexto sejam salvas.

Nota:As configurações de inicialização salvas em servidores externos são acessíveis de cada unidade da rede e não precisam ser salvas separadamente para cada unidade. Você também pode copiar os contextos dos arquivos de configuração do disco na unidade primária para um servidor externo, e então copiá-los para o disco da unidade secundária, onde eles se tornarão disponíveis quando a unidade recarregar.

Replicação de comandos

Após ambas as unidades começarem a executar, os comandos serão replicados de uma unidade para a outra:

- Os comandos inseridos com um contexto de segurança são replicados da unidade na qual o contexto de segurança está no estado ativo para a unidade peer.**Observação:** o contexto é considerado no estado ativo em uma unidade se o grupo de failover ao qual ele pertence estiver no estado ativo nessa unidade.
- Os comandos inseridos no espaço de execução do sistema são replicados da unidade na qual o grupo de failover 1 está no estado ativo para a unidade na qual o grupo de failover 1 está no estado de standby.
- Os comandos inseridos no contexto de administrador são replicados da unidade na qual o grupo de failover 1 está no estado ativo para a unidade na qual o grupo de failover 1 está no estado de standby.

Todos os comandos de configuração e arquivo (**copy, rename, delete, mkdir, rmdir** e assim por diante) são replicados, com as seguintes exceções: os comandos **show, debug, mode, firewall, failover lan unit** não são replicados.

Falhar ao executar os comandos na unidade apropriada para que a replicação de comandos ocorra fará com que as configurações fiquem fora de sincronia. Essas alterações poderão ser perdidas na próxima vez que a sincronização de configuração inicial ocorrer.

Você pode usar o comando **write standby** para ressincronizar as configurações dessincronizadas. No Failover Ativo/Ativo, o comando **write standby** se comporta da seguinte forma:

- Se você executar o comando **write standby** no espaço de execução do sistema, a configuração do sistema e as configurações para todos os outros contextos de segurança no Security Appliance serão escritas na unidade peer. Isso inclui informações de configuração para contextos de segurança no estado de standby. Você deve executar o comando no espaço de execução do sistema na unidade que possui o grupo de failover 1 no estado ativo.**Nota:Se houver contextos de segurança no estado ativo na unidade peer, o comando write standby causará o encerramento das conexões ativas por meio desses contextos.** Use o comando **failover active** na unidade que fornece a configuração para ter certeza de que todos os contextos estejam ativos nessa unidade antes de executar o comando **write standby**.
- Se você inserir o comando **write standby** em um contexto de segurança, somente a configuração do contexto de segurança será escrita na unidade peer. Você deve inserir o comando no contexto de segurança da unidade em que o contexto está no estado ativo.

Os comandos replicados não são salvos na memória Flash ao serem replicados para a unidade peer. Eles são adicionados à configuração em execução. Para salvar os comandos replicados na

memória Flash de ambas as unidades, execute o comando **write memory** ou **copy running-config startup-config** na unidade na qual você fez as alterações. O comando é replicado para a unidade peer e faz com que a configuração seja salva na memória Flash da unidade peer.

Acionadores de failover

No Failover Ativo/Ativo, o failover pode ser acionado no nivel da unidade quando um dos seguintes eventos ocorre:

- A unidade sofre uma falha de hardware.
- A unidade sofre uma falha de alimentação de energia.
- A unidade apresenta uma falha de software.
- O comando **no failover active ou failover active** é inserido no espaço de execução do sistema.

O failover é acionado no nível do grupo de failover quando um destes eventos ocorre:

- Um número excessivo de interfaces monitoradas no grupo falha.
- O comando **no failover active group group_id** ou **failover active group group_id é inserido.**

Ações de failover

Na configuração de Failover Ativo/Ativo, o failover ocorre com base em grupos de failover, e não em sistema. Por exemplo, se você designar ambos os grupos de failover como ativos na unidade primária e o grupo 1 falhar, o grupo 2 permanecerá ativo na unidade primária e o grupo 1 se tornará ativo na unidade secundária.

Nota:Ao configurar o Failover Ativo/Ativo, certifique-se de que o tráfego combinado para ambas as unidades esteja dentro da capacidade de cada unidade.

Esta tabela mostra a ação de failover para cada evento de falha. Para cada evento de falha, a política (se o failover ocorre ou não), as ações para o grupo de failover ativo e as ações para o grupo de failover de standby são fornecidas.

Evento de falha	Política	Ação do grupo ativo	Ação do grupo de standby	Notas
A unidade sofre uma falha de alimentação de energia ou software	Failover	Tornar standby. Marcar como falha.	Tornar standby. Marcar ativo como falha	Quando uma unidade em um par de failover falha, todos os grupos de failover ativos nessa unidade são marcados como com falha e se tornam ativos na unidade peer.
Falha de interface	Failove	Marcar	Torne-se	Nenhum

no grupo de failover ativo acima do limite	r	grupo ativo com o falha.	ativo	
Falha de interface no grupo de failover standby acima do limite	Sem failover	Nenhuma ação	Marcar grupo de standby como falha.	Quando o grupo de failover de standby é marcado como falha, o grupo de failover ativo não tenta executar o failover, mesmo quando o limite de falha da interface é ultrapassado.
O grupo de failover ativo anterior se recupera	Sem failover	Nenhuma ação	Nenhuma ação	A menos que configurado com o comando **preempt, o grupo de failover permanece ativo em sua unidade atual.**
Falha no link de failover na inicialização	Sem failover	Torne-se ativo	Torne-se ativo	Se o link de failover estiver inativo na inicialização, ambos os grupos de failover em ambas as unidades se tornarão ativos.
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 do link de failover durante a operação	Sem failover	n/a	n/a	Cada unidade marca a interface do failover como falha. Você deve restaurar o link de failover o mais rápido possível porque a unidade não pode executar o failover para a unidade de standby quando o link está inoperante.

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 as conexões quando a nova unidade ativa assume.

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 da camada 2 (quando ela é executada 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 Call Manager. 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 Call Manager em um determinado período, ele considera o Call Manager inalcançável e se cancela o registro.

Limitações da Configuração do Failover

Não é possível configurar o failover com estes tipos de endereços IP:

- Endereços IP obtidos por DHCP
- Endereços IP obtidos por PPPoE
- Endereços IPv6

Além disso, essas restrições se aplicam:

- Não há suporte ao failover stateful no ASA 5505 Adaptive Security Appliance.
- Não há suporte ao Failover Ativo/Ativo no ASA 5505 Adaptive Security Appliance.
- Não é possível configurar o failover quando o Easy VPN Remote está habilitado no ASA 5505

Adaptive Security Appliance.
- Não há suporte ao failover de VPN no modo de contexto múltiplo.

Recursos não suportados

O modo de contexto múltiplo não suporta estes recursos:

- Protocolos de roteamento dinâmicoOs contextos de segurança aceitam somente rotas estáticas. Não é possível ativar o OSPF ou o RIP em modo de contexto múltiplo.
- VPN
- Multicast

Configuração de Failover Ativo/Ativo Baseado em Cabo

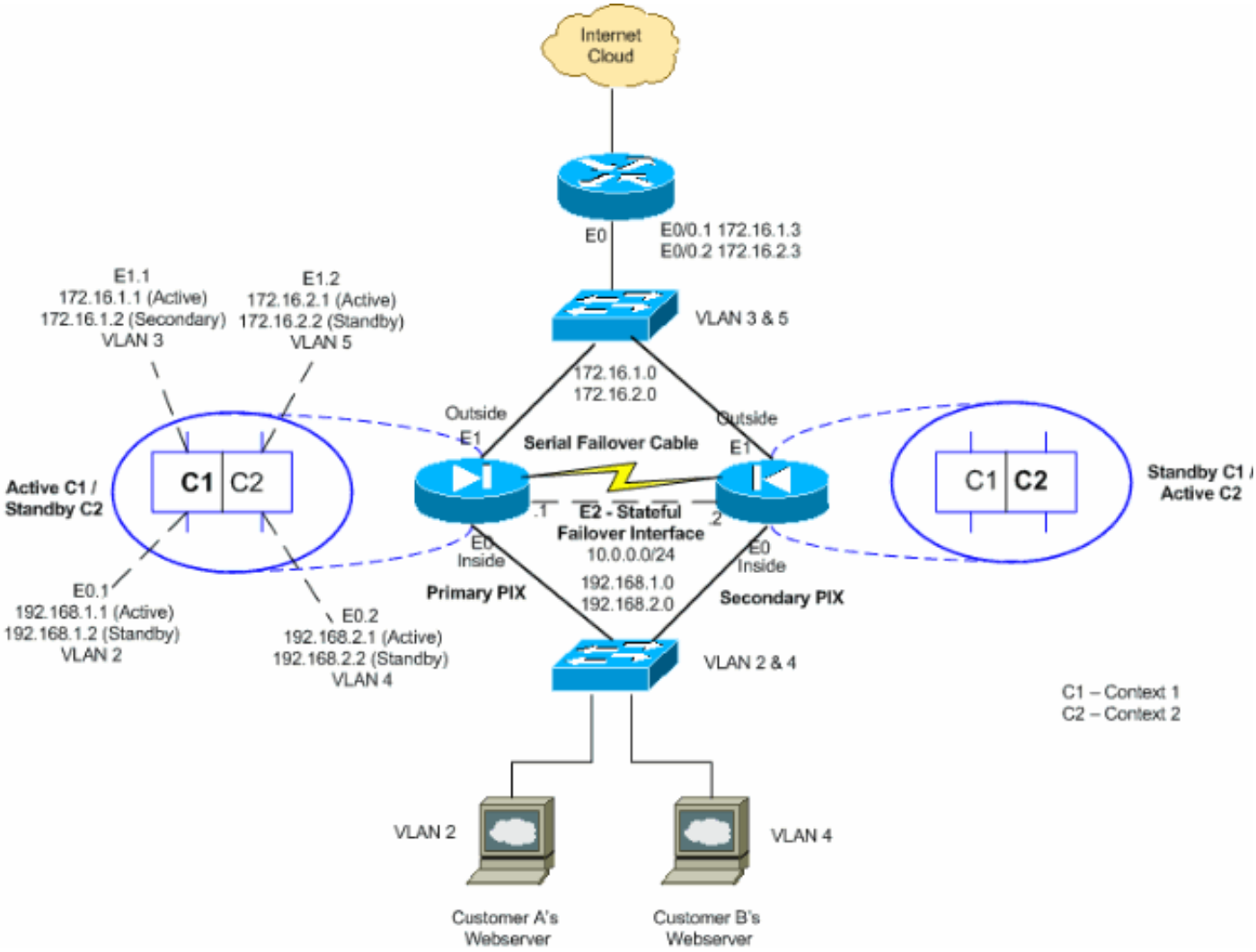
Prerequisites

Antes de começar, verifique o seguinte:

- Se ambas as unidades possuem o mesmo hardware, a mesma configuração de software e a licença apropriada.
- Se ambas as unidades estão no mesmo modo (simples ou múltiplo, transparente ou roteado).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Siga estas etapas para configurar o Failover Ativo/Ativo usando um cabo serial como o link de failover. Os comandos nesta tarefa são inseridos na unidade primária no par de failover. A unidade primária é a unidade que tem a extremidade do cabo "Primário" conectada a ela. Para dispositivos no modo de contexto múltiplo, os comandos são inseridos no espaço de execução do sistema, a menos que observado de outra forma.

Não é necessário inicializar a unidade secundária no par de failover quando você usa o failover baseado em cabo. Deixe a unidade secundária desligada até ser instruída a ligá-la.

Nota:O failover baseado em cabo está disponível somente no PIX 500 Series Security Appliance.

Conclua estes passos para configurar o failover ativo/ativo baseado em cabo:

1. Conecte o cabo de failover aos PIX 500 Series Security Appliances. Certifique-se de conectar a extremidade do cabo marcada como "Primary" à unidade usada como primária e a outra extremidade marcada como "Secondary" à unidade usada como secundária.
2. Ligue a unidade primária.
3. Caso ainda não tenha feito, configure os endereços IP ativo e de standby para cada interface de dados (modo roteado), para o endereço IP de gerenciamento (modo transparente) ou para a interface somente de gerenciamento. 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.Você deve configurar os endereços da interface em cada contexto de segurança. 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. É necessário inserir um endereço IP de gerenciamento para cada contexto no modo de contexto múltiplo do firewall transparente.**Nota:Não configure um endereço IP para o link de failover stateful se pretender 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/context(config-if)#ip address active_addr netmask standby standby_addr
```

No exemplo, a interface externa de context1 do PIX primário é configurada desta forma:

```
PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0
                                    standby 172.16.1.2
```

Para Context2:

```
PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0
                                      standby 192.168.2.2
```

No modo de firewall roteado e para a interface somente de gerenciamento, este comando é inserido no modo de configuração de cada interface. No modo de firewall transparente, o comando é inserido no modo de configuração global.

4. Para habilitar o failover stateful, configure o link failover stateful.Especifique a interface que será usada como link de failover stateful:

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

Neste exemplo, a interface Ethernet2 é usada para trocar as informações de estado do link de failover stateful.

```
failover link stateful Ethernet2
```

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 nenhum outro fim (exceto, opcionalmente, para o link de failover).Atribua um endereço IP ativo e em standby ao link de failover stateful:

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

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

```
PIX1(config)#failover interface ip stateful 10.0.0.1
                    255.255.255.0 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 IP de standby.Os endereços IP e MAC do link de failover stateful não são alterados no failover, exceto quando o failover stateful usa uma interface de dados regular. O endereço IP ativo permanece sempre 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
```

5. Configure os grupos de failover. É possível haver no máximo dois grupos de failover. O comando **failover group cria o grupo de failover especificado se ele ainda não existe e entra no modo de configuração do grupo de failover.**Para cada grupo de failover, é necessário especificar se o grupo possui preferência primária ou secundária por meio do comando primary ou secondary. Você pode atribuir a mesma preferência a ambos os grupos de

failover. Para configurações de balanceamento de carga, você deve atribuir a cada grupo de failover uma preferência de unidade diferente.O exemplo a seguir atribui ao grupo de failover 1 uma preferência primária e ao grupo de failover 2 uma preferência secundária:

```
hostname(config)#failover group 1
hostname(config-fover-group)#primary
hostname(config-fover-group)#exit
hostname(config)#failover group 2
hostname(config-fover-group)#secondary
hostname(config-fover-group)#exit
```

6. Atribua o contexto de cada usuário a um grupo de failover usando o comando **join-failover-group** no modo de configuração de contexto.Todos os contextos não atribuídos são automaticamente atribuídos ao grupo de failover 1. O contexto admin é sempre um membro do grupo de failover 1.Insira estes comandos para atribuir cada contexto a um grupo de failover:

```
hostname(config)#context context_name
hostname(config-context)#join-failover-group {1 | 2}
hostname(config-context)#exit
```

7. Ativar failover:

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

8. Ligue a unidade secundária e ative a ativação pós-falha na unidade se ainda não estiver ativada:

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

   A unidade ativa envia a configuração na memória de execução para a unidade de espera. À medida que a configuração é sincronizada, as mensagens "Iniciando replicação da configuração: O envio para o mate" e "End Configuration Replication to mate" aparecem no console principal.**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.
9. Salve a configuração na memória Flash na unidade primária. Como os comandos inseridos na unidade primária são replicados para a unidade secundária, a unidade secundária também salva sua configuração na memória Flash.

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

10. Se necessário, force qualquer grupo de failover ativo na unidade primária a entrar no estado ativo na secundária. Para forçar um grupo de failover a se tornar ativo na unidade secundária, emita este comando no espaço de execução do sistema na unidade primária:

```
hostname#no failover active group group_id
```

    O argumento group_id especifica o grupo que você deseja que se torne ativo na unidade secundária.

Configurações

Este documento utiliza as seguintes configurações:

- PIX1 - Configuração do Sistema
- PIX1 - Configuração de Context1
- PIX1 - Configuração de Context2

PIX1 - Configuração do Sistema

```
PIX1#show running-config
: Saved
PIX Version 7.2(2)




!
hostname PIX1
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto

!--- Enable the physical and logical interfaces in the
system execution !--- space by giving "no shutdown"
before configuring the same in the contexts ! interface
Ethernet0 ! interface Ethernet0.1
 vlan 2
!
interface Ethernet0.2
 vlan 4
!
interface Ethernet1
!
interface Ethernet1.1
 vlan 3
!
interface Ethernet1.2
 vlan 5
!
!--- Configure "no shutdown" in the stateful failover
interface !--- of both Primary and secondary PIX.
interface Ethernet2
 description STATE Failover Interface
!
interface Ethernet3
 shutdown
!
interface Ethernet4
 shutdown
!
interface Ethernet5
 shutdown
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

ftp mode passive
pager lines 24
```

```
!--- Command to enable the failover feature failover
!--- Command to assign the interface for stateful
failover failover link stateful Ethernet2
!--- Command to configure the active and standby IP's
for the !--- stateful failover failover interface ip
stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2
!--- Configure the group 1 as primary failover group 1
!--- Configure the group 1 as secondary failover group 2
  secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  config-url flash:/admin.cfg
!
!--- Command to create a context called "context1"
context context1
!--- Command to allocate the logical interfaces to the
contexts allocate-interface Ethernet0.1 inside_context1
  allocate-interface Ethernet1.1 outside_context1
  config-url flash:/context1.cfg
!--- Assign this context to the failover group 1 join-
failover-group 1
!

context context2
  allocate-interface Ethernet0.2 inside_context2
  allocate-interface Ethernet1.2 outside_context2
  config-url flash:/context2.cfg
  join-failover-group 2
!

prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX1 - Configuração de Context1

```
PIX1/context1(config)#show running-config
: Saved
:
PIX Version 7.2(2)




!
hostname context1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context1
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context1. ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
interface outside_context1
 nameif outside
```

```
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.1.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.1.1 192.168.1.5 netmask
255.255.255.255
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
telnet timeout 5
ssh timeout 5
!
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
Cryptochecksum:00000000000000000000000000000000
: end
```

PIX1 - Configuração de Context2

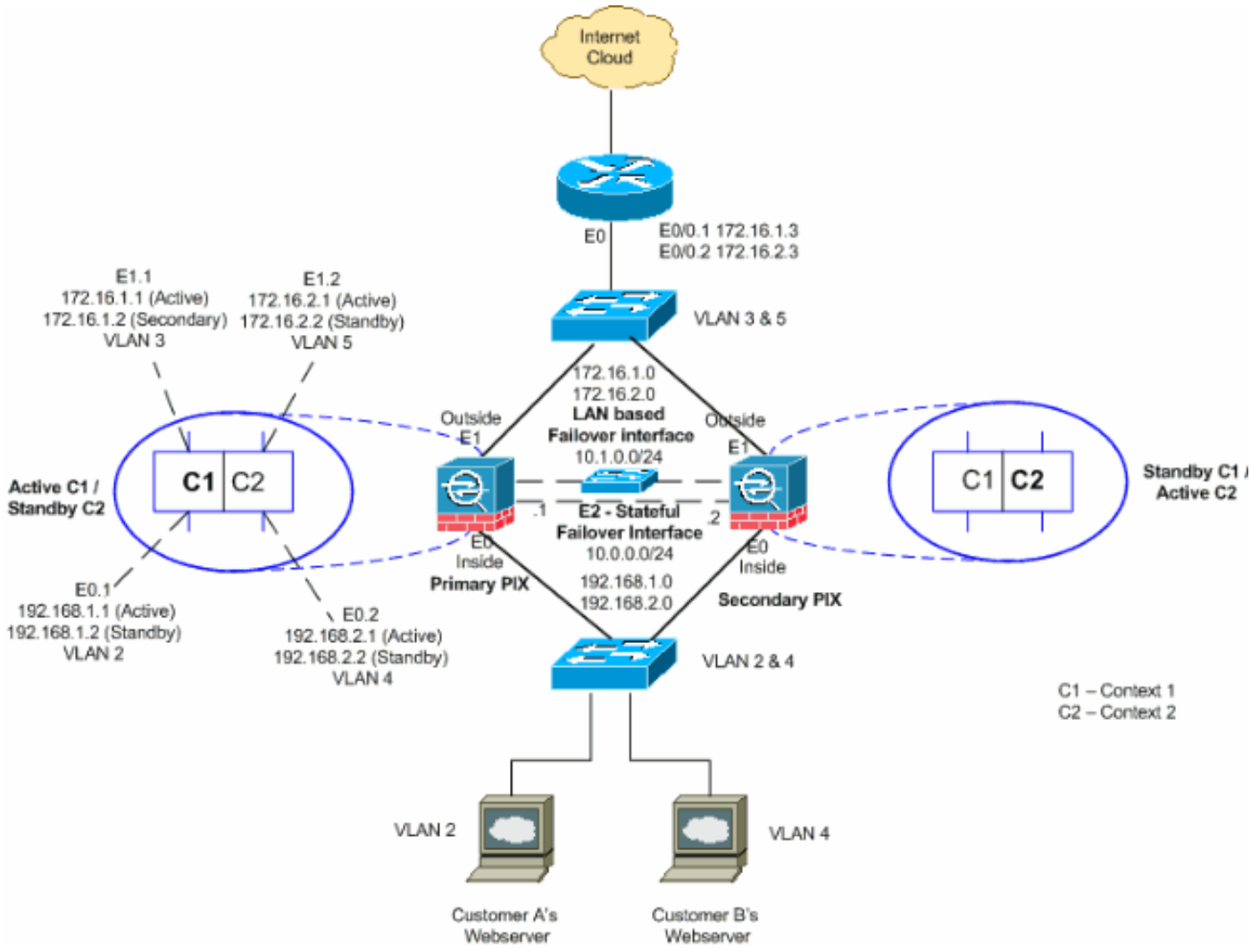
```
PIX1/context2(config)#show running-config
: Saved
:
PIX Version 7.2(2)




!
hostname context2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context2
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context2. ip
address 192.168.2.1 255.255.255.0 standby 192.168.2.2
!
interface outside_context2
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context2. ip
address 172.16.2.1 255.255.255.0 standby 172.16.2.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.2.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.2.1 192.168.2.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.2.3 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
telnet timeout 5
ssh timeout 5
!
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
Cryptochecksum:00000000000000000000000000000000
: end
```

Configuração de Failover Ativo/Ativo Baseado em LAN

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Esta seção descreve como configurar o Failover Ativo/Ativo usando um link de failover Ethernet. Ao configurar o failover baseado em LAN, você deve fazer o bootstrap do dispositivo secundário para reconhecer o link de failover para que o dispositivo secundário possa obter a configuração em execução do dispositivo primário.

Observação: em vez de usar um cabo Ethernet cruzado para ligar diretamente as unidades, a Cisco recomenda que você use um switch dedicado entre as unidades primária e secundária.

Esta seção inclui estes tópicos:

Configuração da unidade principal

Conclua estes passos para configurar a unidade primária em uma configuração de failover Ativo/Ativo:

1. Caso ainda não tenha feito, configure os endereços IP ativo e de standby para cada interface de dados (modo roteado), para o endereço IP de gerenciamento (modo transparente) ou para a interface somente de gerenciamento. 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.Você deve configurar os endereços da interface em cada contexto de segurança. 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. No modo de firewall transparente, você deve inserir um endereço IP de gerenciamento para cada contexto.**Nota:Não configure um endereço IP para o link de failover stateful se pretender 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/context(config-if)#ip address active_addr netmask standby standby_addr
   ```

   No exemplo, a interface externa de context1 do PIX primário é configurada desta forma:
   ```
   PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0
                                    standby 172.16.1.2
   ```

   Para Context2:
   ```
   PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0
                                    standby 192.168.2.2
   ```

   No modo de firewall roteado e para a interface somente de gerenciamento, este comando é inserido no modo de configuração de cada interface. No modo de firewall transparente, o comando é inserido no modo de configuração global.
2. Configure os parâmetros básicos de failover no espaço de execução do sistema.(Somente PIX Security Appliance) Habilite o failover baseado em LAN:
   ```
   hostname(config)#failover lan enable
   ```

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

Especifique o link de failover:

```
hostname(config)#failover lan interface if_name phy_if
```

Neste exemplo, usamos a interface ethernet3 como a interface de failover baseado em LAN.

```
PIX1(config)#failover lan interface LANFailover ethernet3
```

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. No ASA 5505 Adaptive Security Appliance, phy_if especifica uma VLAN. Essa interface não deve ser usada para nenhum outro fim (exceto, opcionalmente, para o link de failover stateful).Especifique os endereços IP ativo e de standby do link de failover:

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

Neste exemplo, usamos 10.1.0.1 e 10.1.0.2 como endereços IP ativo e de standby para a interface de failover.

```
PIX1(config)#failover interface ip LANFailover
      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 IP de standby. O endereço IP e o endereço MAC do link de failover não são alterados no failover. O endereço IP ativo permanece sempre com a unidade primária, enquanto o endereço IP em standby permanece com a unidade secundária.

3. Para habilitar o failover stateful, configure o link de failover stateful:Especifique a interface que será usada como link de failover stateful:

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

```
PIX1(config)#failover link stateful ethernet2
```

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 nenhum outro fim (exceto, opcionalmente, para o link de failover).**Nota:Se o link de failover stateful usar o link de failover ou uma interface de dados convencional, você só precisará fornecer o argumento if_name.**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 regular, 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
```

```
PIX1(config)#failover interface ip stateful 10.0.0.1
                  255.255.255.0 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 não são alterados no failover. 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 regular, pule este passo.** Você já ativou a interface.

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

4. Configure os grupos de failover. É possível haver no máximo dois grupos de failover. O comando **failover group cria o grupo de failover especificado se ele ainda não existe e entra no modo de configuração do grupo de failover.**Para cada grupo de failover, especifique se o grupo possui preferência **primária** ou **secundária por meio do comando primary ou secondary.** Você pode atribuir a mesma preferência a ambos os grupos de failover. Para configurações de balanceamento de carga, você deve atribuir a cada grupo de failover uma preferência de unidade diferente.O exemplo a seguir atribui ao grupo de failover 1 uma preferência primária e ao grupo de failover 2 uma preferência secundária:

```
hostname(config)#failover group 1
hostname(config-fover-group)#primary
hostname(config-fover-group)#exit
hostname(config)#failover group 2
hostname(config-fover-group)#secondary
hostname(config-fover-group)#exit
```

5. Atribua o contexto de cada usuário a um grupo de failover usando o comando join-failover-group no modo de configuração de contexto.Todos os contextos não atribuídos são automaticamente atribuídos ao grupo de failover 1. O contexto admin é sempre um membro do grupo de failover 1.Insira estes comandos para atribuir cada contexto a um grupo de failover:

```
hostname(config)#context context_name
hostname(config-context)#join-failover-group {1 | 2}
hostname(config-context)#exit
```

6. Ative o failover.

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

Configuração da unidade secundária

Ao configurar o Failover Ativo/Ativo baseado em LAN, você deve fazer o bootstrap da unidade secundária para reconhecer o link de failover. Isso permite que a unidade secundária se comunique com e receba a configuração em execução da unidade primária.

Conclua estes passos para fazer o bootstrap da unidade secundária em uma configuração de failover Ativo/Ativo:

1. (Somente PIX Security Appliance) Habilite o failover baseado em LAN.

```
hostname(config)#failover lan enable
```

2. Defina a interface de failover. Use as mesmas configurações aplicadas à unidade primária:Especifique a interface a ser usada como a interface de failover.

```
hostname(config)#failover lan interface if_name phy_if
```

```
PIX1(config)#failover lan interface LANFailover ethernet3
```

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. No ASA 5505 Adaptive Security Appliance, phy_if especifica uma VLAN.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
```

```
PIX1(config)#failover interface ip LANFailover 10.1.0.1
                      255.255.255.0 standby 10.1.0.2
```

Observação: insira este comando exatamente como você o inseriu na unidade primária quando configurou a interface de failover.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.Ative a interface.
```
hostname(config)#interfacephy_if
hostname(config-if)#no shutdown
```

3. Defina 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
```

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 da configuração final para o mate** aparecem no console da unidade ativa.**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.
5. Após a conclusão da replicação da configuração em execução, digite este comando para salvar a configuração na memória Flash:
```
hostname(config)#copy running-config startup-config
```

6. Se necessário, force qualquer grupo de failover ativo na unidade primária a entrar no estado ativo na unidade secundária. Para forçar um grupo de failover a se tornar ativo na unidade secundária, insira este comando no espaço de execução do sistema na unidade primária:
```
hostname#no failover active group group_id
```

O argumento group_id especifica o grupo que você deseja que se torne ativo na unidade secundária.

Configurações

Este documento utiliza as seguintes configurações:

PIX principal

```
PIX1(config)#show running-config
: Saved
:
PIX Version 7.2(2) <system>
!
hostname PIX1
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto
!
interface Ethernet0
!
interface Ethernet0.1
 vlan 2
!
interface Ethernet0.2
 vlan 4
!
interface Ethernet1
!
interface Ethernet1.1
 vlan 3
!
interface Ethernet1.2
 vlan 5
!
 !--- Configure "no shutdown" in the stateful failover
interface as well as !--- LAN Failover interface of both
Primary and secondary PIX/ASA. interface Ethernet2
description STATE Failover Interface
!
interface Ethernet3
 description LAN Failover Interface
!
interface Ethernet4
 shutdown
!
interface Ethernet5
 shutdown
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

ftp mode passive
pager lines 24
failover
failover lan unit primary
!--- Command to assign the interface for LAN based
failover failover lan interface LANFailover Ethernet3
!--- Command to enable the LAN based failover failover
lan enable
!--- Configure the Authentication/Encryption key
failover key *****
failover link stateful Ethernet2
!--- Configure the active and standby IP's for the LAN
based failover failover interface ip LANFailover
10.1.0.1 255.255.255.0 standby 10.1.0.2
failover interface ip stateful 10.0.0.1 255.255.255.0
```

```
standby 10.0.0.2
failover group 1
failover group 2
  secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  config-url flash:/admin.cfg
!

context context1
  allocate-interface Ethernet0.1 inside_context1
  allocate-interface Ethernet1.1 outside_context1
  config-url flash:/context1.cfg
  join-failover-group 1
!

context context2
  allocate-interface Ethernet0.2 inside_context2
  allocate-interface Ethernet1.2 outside_context2
  config-url flash:/context2.cfg
  join-failover-group 2
!

prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Nota:Consulte a seção Configuração do Failover Ativo/Ativo Baseado em Cabo, PIX1 - Configuração de Context1 e PIX1 - Configuração de Context2 para obter informações de contexto em um cenário de failover baseado em LAN.

PIX secundário

```
PIX2#show running-config

failover
failover lan unit secondary
failover lan interface LANFailover Ethernet3
failover lan enable
failover key *****
failover interface ip LANFailover 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**.

PIX principal

```
PIX1(config-subif)#show failover
```

```
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(2), Mate 7.2(2)
Group 1 last failover at: 06:12:45 UTC Apr 16 2007
Group 2 last failover at: 06:12:43 UTC Apr 16 2007

  This host:    Primary
  Group 1       State:          Active
                Active time:    359610 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
                  context2 Interface inside (192.168.2.2): Normal
                  context2 Interface outside (172.16.2.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3900 (sec)

                  context1 Interface inside (192.168.1.2): Normal
                  context1 Interface outside (172.16.1.2): Normal
                  context2 Interface inside (192.168.2.1): Normal
                  context2 Interface outside (172.16.2.1): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         48044      0          48040      1
        sys cmd         48042      0          48040      1
        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         2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       72081
        Xmit Q:         0       1       48044
```

PIX secundário

```
PIX1(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(2), Mate 7.2(2)
```

```
Group 1 last failover at: 06:12:46 UTC Apr 16 2007
Group 2 last failover at: 06:12:41 UTC Apr 16 2007

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3975 (sec)

                  context1 Interface inside (192.168.1.2): Normal
                  context1 Interface outside (172.16.1.2): Normal
                  context2 Interface inside (192.168.2.1): Normal
                  context2 Interface outside (172.16.2.1): Normal

  Other host:   Primary
  Group 1       State:          Active
                Active time:    359685 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
                  context2 Interface inside (192.168.2.2): Normal
                  context2 Interface outside (172.16.2.2): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         940        0          942        2
        sys cmd         940        0          940        2
        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          2          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1419
        Xmit Q:         0       1       940
```

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

PIX principal

```
PIX1(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  None
Other host -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None

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

Unidade secundária

```
PIX1(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None
Other host -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  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

```
PIX1(config)#show failover interface
        interface stateful Ethernet2
                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
        interface LANFailover Ethernet3
                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
```

Unidade secundária

```
PIX1(config)#show failover interface
        interface LANFailover Ethernet3
                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 stateful Ethernet2
                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.

Observação: para habilitar o monitoramento de integridade em uma interface específica, use o comando monitor-interface no modo de configuração global:

```
monitor-interface <if_name>
```

PIX principal

```
PIX1/context1(config)#show monitor-interface
```

```
        This host: Secondary - Active
                Interface inside (192.168.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

PIX secundário

```
PIX1/context1(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Secondary - Active
                Interface inside (192.168.1.1): 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 das interfaces permanecerá em um estado de "espera". Você deve definir um endereço IP de failover para que o failover funcione. Para obter mais informações sobre diferentes estados para failover, consulte show failover.

Por padrão, o monitoramento de interfaces físicas é ativado e o monitoramento de subinterfaces é desativado.

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 atual e incluir comandos para os quais você não alterou o valor padrão.

Testes de funcionalidade de failover

Para testar a funcionalidade de failover, execute estas etapas:

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 o Failover Ativo/Ativo, insira o seguinte comando na unidade em que o grupo de failover que contém a interface conectada aos seus hosts está ativo:
   ```
   hostname(config)#no failover active group group_id
   ```
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 o Failover Ativo/Ativo, insira o seguinte comando na unidade em que o grupo de failover que contém a interface conectada aos seus hosts está ativo:

```
hostname(config)#failover active group group_id
```

Failover forçado

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

Insira este comando no espaço de execução do sistema da unidade onde o grupo de failover está no estado de espera:

```
hostname#failover active group group_id
```

Ou insira este comando no espaço de execução do sistema da unidade onde o grupo de failover está no estado ativo:

```
hostname#no failover active group group_id
```

Inserir este comando no espaço de execução do sistema faz com que todos os grupos de failover se tornem ativos:

```
hostname#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 Failover Forçado.

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 um grupo de failover Ativo/Ativo com falha para um estado sem falha, insira este comando:

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

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.

Substitua a unidade com falha por uma nova unidade

Conclua estes passos para substituir uma unidade com falha por uma nova unidade:

1. Execute o comando **no failover** na unidade primária.O status da unidade secundária mostra a **unidade em standby como não detectada**.
2. Desligue a unidade primária e ligue a unidade primária de substituição.
3. Verifique se a unidade de substituição executa o mesmo software e a mesma versão ASDM da unidade secundária.
4. Execute estes comandos na unidade de substituição:

```
ASA(config)#failover lan unit primary
ASA(config)#failover lan interface failover Ethernet3
ASA(config)#failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2
ASA(config)#interface Ethernet3
ASA(config-if)#no shut
ASA(config-if)#exit
```

5. Conecte a unidade primária de substituição à rede e execute este comando:
```
ASA(config)#failover
```

Troubleshoot

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

1. Mensagens do sistema de failover
2. Mensagens de depuração
3. SNMP

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.

Comunicação de failover principal perdida com o mate na interface interface_name

Essa mensagem de failover será exibida se uma unidade do par de failover não puder mais se comunicar com a outra unidade do par. O Primário também pode ser listado como Secundário para a unidade secundária.

(Primário) Perda de comunicações de failover com o mate no interface interface_name

Verifique se a rede conectada à interface especificada está funcionando corretamente.

Mensagens de depuração

Para ver mensagens de depuração, insira o comando **debug fover**. Consulte a Referência de Comandos do Cisco Security Appliance Versão 7.2 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 Versão 7.2 para obter mais informações.

Tempo de Poll do Failover

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

O comando failover polltime unit msec [time] representa o intervalo de tempo da verificação da existência da unidade de standby com o uso de mensagens de hello de polling.

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.

Consulte failover polltime para obter mais informações.

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.

Informações Relacionadas

- Página de suporte do Cisco 500 Series PIX
- 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
- Página de Suporte do Cisco 5500 Series Adaptive Security Appliance
- Suporte Técnico e Documentação - Cisco Systems