PIX/ASA: Ejemplo de Configuración de Active/Active Failover

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Productos Relacionados](#)
[Convenciones](#)
[Active/Active Failover](#)
[Descripción General de Active/Active Failover](#)
[Estado Primario/Secondario y Estado Activo/Standby](#)
[Sincronización de la Configuración e Inicialización del dispositivo](#)
[Réplica de Comandos](#)
[Disparadores del Failover](#)
[Acciones de Failover](#)
[Regular y Stateful Failover](#)
[Regular Failover](#)
[Stateful Failover](#)
[Limitaciones de configuración de conmutación por fallas](#)
[Características no admitidas](#)
[Configuración de Active/Active Failover Basada en Cable](#)
[Prerequisites](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Configuración de Active/Active Failover Basada en LAN](#)
[Diagrama de la red](#)
[Configuración de la Unidad Primaria](#)
[Configuración de la Unidad Secundaria](#)
[Configuraciones](#)
[Verificación](#)
[Uso del Comando show failover](#)
[Vista de las Interfaces Monitoreadas](#)
[Visualización de los Comandos de Failover en la Configuración en Ejecución](#)
[Pruebas de Funcionalidad de Failover](#)
[Failover Forzado](#)
[Failover Inhabilitado](#)
[Restauración de una Unidad Defectuosa](#)
[Reemplazar la Unidad Defectuosa por una Nueva Unidad](#)

Troubleshoot
Mensajes del sistema de fallas
Comunicaciones de fallas perdidas primarias con el compañero en el interface_name de la interfaz
Mensajes del debug
SNMP (Protocolo de administración de red simple)
Tiempo de sondeo de fallas
ADVERTENCIA: Incidente del desciframiento del mensaje de falla.
Información Relacionada

Introducción

La configuración de failover requiere dos dispositivos de seguridad idénticos conectados el uno al otro a través de un link de failover dedicado y, opcionalmente, de un link de stateful failover. El estado de las unidades y las interfaces activas se monitorea para determinar si se cumplen las condiciones específicas de failover. Si se cumplen esas condiciones, el failover ocurre.

El dispositivo de seguridad soporta dos configuraciones de failover, **Active/Active Failover** y **Active/Standby Failover**. Cada configuración de failover tiene su propio método para determinar y para ejecutar el failover. Con Active/Active Failover, ambas unidades pueden pasar el tráfico de red. Esto le permite configurar el balanceo de carga en su red. Active/Active Failover está solamente disponible en las unidades que se ejecutan en el modo multiple context. Con Active/Standby Failover, solamente una unidad pasa el tráfico mientras que la otra unidad espera en estado standby. Active/Standby Failover está disponible en las unidades que se ejecutan en el modo single context o multiple context. Ambas configuraciones de failover soportan el stateful failover o el stateless (regular) failover.

Este documento se centra en cómo configurar un Active/Active Failover en Cisco PIX/ASA Security Appliance.

Consulte Ejemplo de Configuración de Failover Activo/En Espera de PIX/ASA 7.x para obtener más información sobre las configuraciones de Failover Activo/En Espera.

Nota: La conmutación por fallas VPN no se soporta en las unidades que se ejecutan en el modo de contexto múltiple, ya que VPN no se soporta en el contexto múltiple. Failover VPN está disponible solamente para las **configuraciones Active/Standby Failoveren las configuraciones de contexto simple.**

Esta guía de configuración proporciona una configuración de ejemplo para incluir una breve introducción a la tecnología activa/activa PIX/ASA 7.x. Refiérase a la Referencia de Comandos de Dispositivos de Seguridad de Cisco, Versión 7.2 para obtener un sentido más profundo de la teoría basada en esta tecnología.

Prerequisites

Requirements

Requisito de Hardware

Las dos unidades en una configuración de failover deben tener la misma configuración de hardware. Deben tener el mismo modelo, el mismo número y los mismos tipos de interfaces, y la misma cantidad de RAM.

Nota: Las dos unidades no necesitan tener el mismo tamaño de memoria Flash. Si usted utiliza unidades con diversos tamaños de memoria Flash en su configuración de failover, asegúrese de que la unidad con la memoria Flash más pequeña tenga bastante espacio para acomodar los archivos de imagen de software y los archivos de configuración. Si no lo hace, la sincronización de la configuración de la unidad con la memoria Flash más grande a la unidad con la memoria Flash más pequeña falla.

Requisito de Software

Las dos unidades en una configuración de failover deben estar en los modos de funcionamiento (routed o transparent, single o multiple context). Deben tener la misma versión de software principal (primer número) y de menor importancia (segundo número), pero usted puede utilizar diversas versiones del software dentro de un proceso de actualización; por ejemplo, usted puede actualizar una unidad de la Versión 7.0(1) a la Versión 7.0(2) y hacer que el failover siga siendo activo. Cisco recomienda que actualice ambas unidades a la misma versión para garantizar la compatibilidad a largo plazo.

Refiérase a Realización de Actualizaciones de Tiempo de Inactividad Cero para Pares de Failover para obtener más información sobre la actualización del software en un par de failover.

Requisitos de Licencia

En la plataforma del dispositivo de seguridad PIX/ASA, al menos una de las unidades debe tener una **licencia sin restricciones (UR)**. La otra unidad puede tener una licencia Active-Active (FO_AA) de solo conmutación por fallo u otra licencia UR. Las unidades con una licencia restringida no se pueden utilizar para la conmutación por fallas y dos unidades con licencias FO_AA no se pueden utilizar juntas como un par de conmutación por fallas.

Nota: Es posible que necesite actualizar las licencias en un par de failover para obtener funciones y beneficios adicionales. Para obtener más información sobre la actualización, consulte la Actualización de la Clave de Licencia en un Par de Failover

Nota: Las funciones con licencia, como los puntos de VPN SSL o los contextos de seguridad, en ambos dispositivos de seguridad que participan en la conmutación por fallas deben ser idénticas.

Nota: La licencia FO no admite Active/Active Failover.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PIX Security Appliance con versión 7.x y 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.

Productos Relacionados

Esta configuración también se puede utilizar con las siguientes versiones de hardware y software:

- ASA con versión 7.x y posterior

Nota: La conmutación por fallas activa/activa no está disponible en el dispositivo de seguridad adaptable ASA serie 5505.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones de los documentos.

Active/Active Failover

Esta sección describe Active/Standby Failover e incluye estos temas:

- Descripción General de Active/Active Failover
- Estado Primario/Secondario y Estado Activo/Standby
- Sincronización de la Configuración e Inicialización del dispositivo
- Réplica de Comandos
- Disparadores del Failover
- Acciones de Failover

Descripción General de Active/Active Failover

La conmutación por fallas activa/activa sólo está disponible para los dispositivos de seguridad en el modo de contexto múltiple. En una configuración de failover Activo/Activo, ambos dispositivos de seguridad pueden pasar el tráfico de red.

En Active/Active failover, usted divide los contextos de seguridad en el dispositivo de seguridad en grupos de failover. Un grupo de failover es simplemente un grupo lógico de uno o más contextos de seguridad. Puede crear un máximo de dos grupos de failover en el dispositivo de seguridad. El contexto de administración siempre es miembro del grupo de conmutación por fallas 1. Los contextos de seguridad no asignados también son miembros del grupo de conmutación por fallas 1 de forma predeterminada.

El grupo de failover forma la unidad base para failover en Active/Active failover. La supervisión de fallas de interfaz, la conmutación por fallas y el estado activo/en espera son todos atributos de un grupo de conmutación por fallas en lugar de la unidad. Cuando un grupo de failover activo falla, cambia al estado standby mientras el grupo de failover en espera se vuelve activo. Las interfaces en el grupo de failover que se activa asumen las direcciones MAC e IP de las interfaces en el grupo de failover que fallaron. Las interfaces en el grupo de conmutación por fallas que ahora está en estado de espera se hacen cargo de las direcciones IP y MAC en espera.

Nota: Un grupo de failover que falla en una unidad no significa que la unidad haya fallado. Es posible que la unidad aún tenga otro grupo de conmutación por fallas que pase tráfico sobre ella.

Estado Primario/Secondario y Estado Activo/Standby

Como en la conmutación por fallas activa/en espera, una unidad en un par de failover

activo/activo se designa como la unidad primaria y la otra unidad como la unidad secundaria. A diferencia de la conmutación por fallas activa/en espera, esta designación no indica qué unidad se activa cuando ambas unidades se inician simultáneamente. En su lugar, la designación primaria/secundaria hace dos cosas:

- Determina qué unidad proporciona la configuración en ejecución al par cuando se inician simultáneamente.
- Determina en qué unidad cada grupo de failover aparece en el estado activo cuando las unidades se inician simultáneamente. Cada grupo de failover en la configuración se configura con una preferencia de unidad primaria o secundaria. Puede configurar ambos grupos de failover en el estado activo en una sola unidad en el par, con la otra unidad que contiene los grupos de failover en el estado standby. Sin embargo, una configuración más típica es asignar a cada grupo de failover una preferencia de rol diferente para hacer cada uno activo en una unidad diferente, distribuyendo el tráfico a través de los dispositivos.**Nota:** El dispositivo de seguridad **no** proporciona servicios de equilibrio de carga. El balanceo de carga debe ser manejado por un router que pasa el tráfico al dispositivo de seguridad.

La unidad en la que se activa cada grupo de conmutación por fallas se determina como se muestra

- Cuando una unidad se inicia mientras la unidad de peer no está disponible, ambos grupos de failover se activan en la unidad.
- Cuando una unidad se inicia mientras la unidad de peer está activa (con ambos grupos de failover en el estado activo), los grupos de failover permanecen en el estado activo en la unidad activa independientemente de la preferencia primaria o secundaria del grupo de failover hasta uno de los siguientes:Se produce un failover.Usted fuerza manualmente el grupo de failover a la otra unidad con el comando **no failover active**Usted configuró el grupo de failover con el comando **preempt**, que hace que el grupo de failover se active automáticamente en la unidad preferida cuando la unidad esté disponible.
- Cuando ambas unidades se inician al mismo tiempo, cada grupo de conmutación por fallas se activa en su unidad preferida después de que las configuraciones se hayan sincronizado.

Sincronización de la Configuración e Inicialización del dispositivo

La sincronización de la configuración se produce cuando se inicia una o ambas unidades en un par de failover. Las configuraciones se sincronizan como se muestra a continuación:

- Cuando una unidad se inicia mientras la unidad de peer está activa (con ambos grupos de failover activos en ella), la unidad de arranque se pone en contacto con la unidad activa para obtener la configuración en ejecución independientemente de la designación primaria o secundaria de la unidad de arranque.
- Cuando ambas unidades se inician simultáneamente, la unidad secundaria obtiene la configuración en ejecución de la unidad primaria.

Cuando se inicia la replicación, la consola del dispositivo de seguridad en la unidad que envía la configuración muestra el mensaje **"Beginning configuration replication: Enviando a mate"** y cuando se complete, el dispositivo de seguridad muestra el mensaje **"End Configuration Replication to mate" (Finalizar replicación de configuración para aparcar).** Durante la replicación, es posible que los comandos ingresados en la unidad que envía la configuración no se replicen correctamente en la unidad de peer y que los comandos ingresados en la unidad que recibe la configuración se sobrescriban con la configuración que se recibe. Evite ingresar comandos en

cualquiera de las unidades en el par de failover durante el proceso de replicación de la configuración. Dependiendo del tamaño de la configuración, la replicación puede tardar de unos segundos a varios minutos.

En la unidad que recibe la configuración, la configuración existe solamente en la memoria en ejecución. Para guardar la configuración en la memoria Flash después de la sincronización, ingrese el comando **write memory all** en el espacio de ejecución del sistema en la unidad que tiene el grupo de conmutación por fallas 1 en el estado activo. El comando se replica en la unidad de peer, que procede a escribir su configuración en la memoria Flash. El uso de la palabra clave **all** con este comando hace que se guarden el sistema y todas las configuraciones de contexto.

Nota: Las configuraciones de inicio guardadas en servidores externos son accesibles desde cualquier unidad a través de la red y no necesitan guardarse por separado para cada unidad. Alternativamente, puede copiar los archivos de configuración de contextos del disco en la unidad primaria a un servidor externo y luego copiarlos al disco en la unidad secundaria, donde estarán disponibles cuando la unidad se recargue.

Réplica de Comandos

Después de que ambas unidades se estén ejecutando, los comandos se replican de una unidad a otra como se muestra a continuación:

- Los comandos ingresados dentro de un contexto de seguridad se replican desde la unidad en la que el contexto de seguridad aparece en el estado activo a la unidad de peer.**Nota:** el contexto se considera en el estado activo en una unidad si el grupo de failover al que pertenece está en el estado activo en esa unidad.
- Los comandos ingresados en el espacio de ejecución del sistema se replican desde la unidad en la cual el grupo de conmutación por fallas 1 está en estado activo a la unidad en la cual el grupo de conmutación por fallas 1 está en estado de espera.
- Los comandos ingresados en el contexto de administración se replican desde la unidad en la cual el grupo de conmutación por fallas 1 está en estado activo a la unidad en la cual el grupo de conmutación por fallas 1 está en estado de espera.

Todos los comandos de configuración y archivo (**copy, Rename, delete, mkdir, rmdir,** etc.) se replican, con las siguientes excepciones. Los comandos **show, debug, mode, firewall y failover lan unit** no se replican.

Si no se ingresan los comandos en la unidad adecuada para que se produzca la replicación de comandos, las configuraciones se quedarán fuera de la sincronización. Estos cambios pueden perderse la próxima vez que se produzca la sincronización de la configuración inicial.

Puede utilizar el comando **write standby** para resincronizar las configuraciones que se han quedado fuera de sincronización. Para Active/Active failover, el comando **write standby** se comporta como se muestra:

- Si ingresa el comando **write standby** en el espacio de ejecución del sistema, la configuración del sistema y las configuraciones para todos los contextos de seguridad en el dispositivo de seguridad se escriben en la unidad de peer. Esto incluye información de configuración para contextos de seguridad que se encuentran en estado de espera. Debe ingresar el comando en el espacio de ejecución del sistema en la unidad que tiene el grupo de conmutación por fallas 1 en el estado activo.**Nota:** Si hay contextos de seguridad en el estado activo en la

unidad de peer, el comando **write standby** hace que las conexiones activas a través de esos contextos terminen. Utilice el comando **failover active** en la unidad que proporciona la configuración para asegurarse de que todos los contextos estén activos en esa unidad antes de ingresar el comando **write standby**.
- Si ingresa el comando **write standby** en un contexto de seguridad, sólo la configuración para el contexto de seguridad se escribe en la unidad peer. Debe ingresar el comando en el contexto de seguridad en la unidad donde aparece el contexto de seguridad en el estado activo.

Los comandos replicados no se guardan en la memoria Flash cuando se replican en la unidad de peer. Se agregan a la configuración en ejecución. Para guardar los comandos replicados en la memoria Flash en ambas unidades, utilice el comando **write memory** o **copy running-config startup-config** en la unidad en la que realizó los cambios. El comando se replica en la unidad de peer y hace que la configuración se guarde en la memoria Flash en la unidad de peer.

Disparadores del Failover

En la conmutación por fallas activa/activa, la conmutación por fallas se puede activar en el nivel de unidad si ocurre uno de los siguientes eventos:

- La unidad tiene una falla de hardware.
- La unidad tiene una falla de alimentación.
- La unidad tiene una falla de software.
- El comando **no failover active** o el comando **failover active** se ingresa en el espacio de ejecución del sistema.

La conmutación por fallas se activa en el nivel del grupo de conmutación por fallas cuando ocurre uno de estos eventos:

- Fallo en demasiadas interfaces supervisadas en el grupo.
- Se ingresa el comando **no failover active group_id** o **failover active group_id**.

Acciones de Failover

En una configuración de failover Activo/Activo, la conmutación por fallas se produce sobre la base de un grupo de failover, no sobre la base del sistema. Por ejemplo, si se designan ambos grupos de failover como activos en la unidad primaria y falla el grupo de failover 1, entonces el grupo de failover 2 permanece activo en la unidad primaria mientras que el grupo de failover 1 se vuelve activo en la unidad secundaria.

Nota: Al configurar el failover Activo/Activo, asegúrese de que el tráfico combinado para ambas unidades esté dentro de la capacidad de cada unidad.

Esta tabla muestra la acción de failover para cada evento de failover. Para cada evento de falla, se proporcionan la política (independientemente de si se produce o no la conmutación por fallas), las acciones para el grupo de conmutación por fallas activo y las acciones para el grupo de conmutación por fallas en espera.

Evento de Falla	Política	Acción de grupo activo	Acción de grup	Notas

			o en espera	
Una unidad experimenta una falla de alimentación o software	Failover	Conviértase en una marca en espera como fallada	Pasar a standby. Marcar active como fallada	Cuando una unidad en un par de failover falla, cualquier grupo de failover activo en esa unidad se marca como fallado y se vuelve activo en la unidad peer.
Falla de interfaz en el grupo de failover activo por encima del umbral	Failover	Marcar el grupo activo como fallado	Pasar a activo	Ninguno
Falla de interfaz en el grupo de failover en espera por encima del umbral	Ningún failover	Ninguna acción	Marcar el grupo en espera como fallado	Cuando el grupo de conmutación por fallas en espera se marca como fallado, el grupo de conmutación por fallas activo no intenta conmutar, incluso si se supera el umbral de falla de la interfaz.
El grupo de conmutación por fallas antes activo se recupera	Ningún failover	Ninguna acción	Ninguna acción	A menos que se configure con el comando **preempt**, los grupos de failover permanecen activos en su unidad actual.
Link de failover fallado en el inicio	Ningún failover	Pasar a activo	Pasar a activo	Si el link de failover está inactivo al inicio, ambos grupos de failover en ambas unidades se activan.
Link de	Nin	Ningu	Ning	La información de estado

stateful failover fallado	gún failover	na acción	una acción	llega a estar desactualizada, y se terminan las sesiones si ocurre un failover.
Error en el enlace de conmutación por fallo durante la operación	Ningún failover	n/a	n/a	Cada unidad marca la interfaz de conmutación por fallas como fallada. Debe restaurar el link de failover lo antes posible porque la unidad no puede conmutar a la unidad standby mientras el link de failover está inactivo.

Regular y Stateful Failover

El dispositivo de seguridad soporta dos tipos de failover, regular y stateful. Esta sección incluye estos temas:

- Regular Failover
- Stateful Failover

Regular Failover

Cuando ocurre un failover, se interrumpen todas las conexiones activas. Los clientes necesitan restablecer las conexiones cuando la nueva unidad activa toma el control.

Stateful Failover

Cuando el stateful failover está habilitado, la unidad activa pasa continuamente la información de estado por conexión a la unidad standby. Después de que ocurre un failover, la misma información de conexión está disponible en la nueva unidad activa. Las aplicaciones del usuario final soportadas no se requieren para volver a conectarse a fin de conservar la misma sesión de comunicación.

La información de estado que se pasa a la unidad standby incluye lo siguiente:

- La tabla de traducción NAT
- Los estados de la conexión TCP
- Los estados de la conexión UDP
- La tabla ARP
- El tabla de bridge de Capa 2 (cuando se ejecuta en el modo transparent firewall)
- Los estados de la conexión HTTP (si se habilita la réplica HTTP)
- La tabla de SA ISAKMP e IPSec
- Las bases de datos de conexiones GTP PDP

La información que no se pasa a la unidad standby cuando stateful failover está habilitado incluye lo siguiente:

- La tabla de la conexión HTTP (a menos que se habilite la réplica HTTP)
- La tabla de la autenticación de usuario (uauth)
- Las tablas de ruteo
- Información del estado para los módulos del servicio de seguridad

Nota: Si la conmutación por fallas se produce dentro de una sesión activa de Cisco IP SoftPhone, la llamada permanece activa porque la información de estado de la sesión de llamada se replica en la unidad standby. Cuando se termina la llamada, el cliente del IP SoftPhone pierde la conexión con el Administrador de Llamadas. Esto ocurre porque no hay información de la sesión para el mensaje para colgar CTIQBE en la unidad standby. Cuando el cliente del IP SoftPhone no recibe una respuesta del Administrador de Llamadas dentro de cierto período, considera al Administrador de Llamadas inalcanzable y cancela su registro.

Limitaciones de configuración de conmutación por fallas

No puede configurar la conmutación por fallas con estos tipos de direcciones IP:

- Direcciones IP obtenidas a través de DHCP
- Direcciones IP obtenidas a través de PPPoE
- Direcciones IPv6

Además, estas restricciones se aplican:

- El dispositivo de seguridad adaptable ASA 5505 no admite stateful failover.
- El ASA 5505 Adaptive Security Appliance no soporta la conmutación por fallas activa/activa.
- No puede configurar la conmutación por fallas cuando Easy VPN remoto está habilitado en el dispositivo de seguridad adaptable ASA 5505.
- La conmutación por fallas de VPN no se soporta en el modo de contexto múltiple.

Características no admitidas

El modo de contexto múltiple no admite estas funciones:

- Protocolos de ruteo dinámicosLos contextos de seguridad sólo admiten rutas estáticas. No puede habilitar OSPF o RIP en el modo de contexto múltiple.
- VPN
- Multicast (multidifusión)

Configuración de Active/Active Failover Basada en Cable

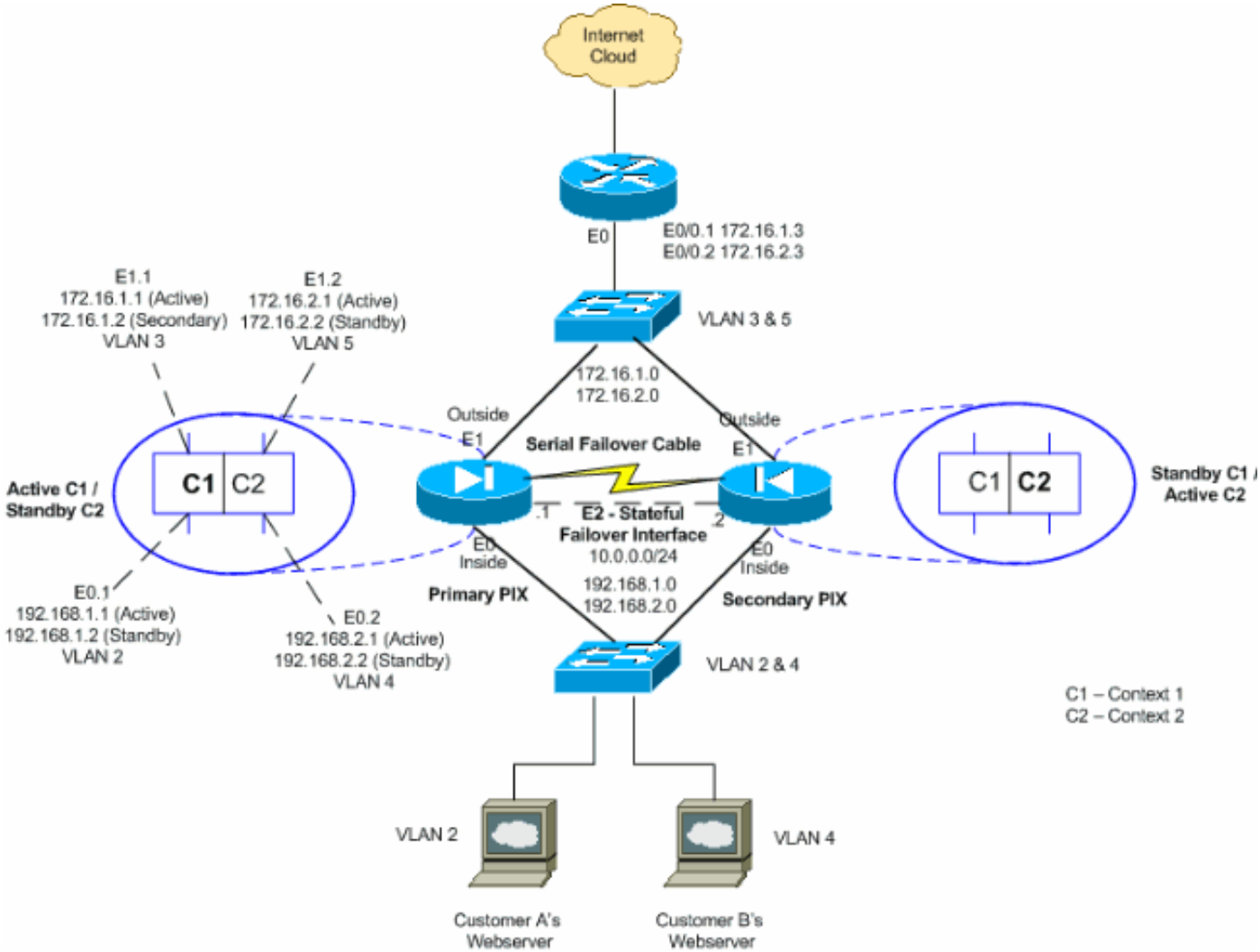
Prerequisites

Antes de comenzar, verifique lo siguiente:

- Ambas unidades tienen el mismo hardware, configuración de software y licencia adecuada.
- Ambas unidades están en el mismo modo (una o varias, transparentes o enrutadas).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Siga estos pasos para configurar el failover activo/activo usando un cable serial como el link de failover. Los comandos en esta tarea se ingresan en la unidad primaria en el par de failover. La unidad primaria es la unidad que tiene el extremo del cable etiquetado "Primary" conectado en ella. Para los dispositivos en el modo multiple context, los comandos se ingresan en el espacio de la ejecución del sistema a menos que se indique lo contrario.

Usted no necesita ejecutar el proceso de arranque de la unidad secundaria en el par de failover cuando utiliza el failover basado en cable. Deje la unidad secundaria apagada hasta que se le indique que debe encenderla.

Nota: El failover basado en cable sólo está disponible en el dispositivo de seguridad PIX de la serie 500.

Complete estos pasos para configurar el failover activo/activo basado en cable:

1. Conecte el cable de conmutación por fallas a los dispositivos de seguridad de la serie PIX 500. Asegúrese de conectar el extremo del cable marcado como "Primario" a la unidad que utiliza como unidad primaria y de conectar el extremo del cable marcado como "Secundario" a la unidad que utiliza como unidad secundaria.
2. Encienda la unidad primaria.
3. Si aún no lo ha hecho, configure las direcciones IP activas y en espera para cada interfaz de datos (modo enrutado), para la dirección IP de administración (modo transparente) o para la

interfaz de sólo administración. La dirección IP standby se utiliza en el dispositivo de seguridad que es actualmente la unidad standby. Debe estar en la misma subred que la dirección IP activa.Debe configurar las direcciones de interfaz desde dentro de cada contexto. Utilice el **comando changeto context para conmutar entre los contextos.** El comando indica cambios en hostname/context(config-if)#, donde context es el nombre del contexto actual. Debe ingresar una dirección IP de administración para cada contexto en el modo de contexto múltiple de firewall transparente.**Nota:** No configure una dirección IP para el link Stateful Failover si va a utilizar una interfaz dedicada de Stateful Failover. Usted utiliza el **comando failover interface ip para configurar una interfaz dedicada de stateful failover en un paso posterior.**

```
hostname/context(config-if)#ip address active_addr netmask standby standby_addr
```

En el ejemplo, la interfaz externa para context1 del PIX primario se configura de esta manera:

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

Para el contexto 2:

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

En el modo de firewall ruteado y para la interfaz sólo de administración, este comando se ingresa en el modo de configuración de interfaz para cada interfaz. En el modo de firewall transparente, el comando se ingresa en el modo de configuración global.

4. Para habilitar el stateful failover, configure el link de stateful failover.Especifique la interfaz que se utilizará como enlace Stateful Failover:

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

En este ejemplo, la interfaz Ethernet2 se utiliza para intercambiar la información de estado del link de stateful failover.

```
failover link stateful Ethernet2
```

El argumento if_name asigna un nombre lógico a la interfaz especificada por el argumento phy_if. El argumento phy_if puede ser el nombre del puerto físico, como Ethernet1, o una subinterfaz previamente creada, como Ethernet0/2.3. Esta interfaz no debe utilizarse para ningún otro propósito (excepto, opcionalmente, el link de failover).Asigne una dirección IP activa y standby al link de stateful failover:

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

En este ejemplo, 10.0.0.1 se utiliza como activa, y 10.0.0.2 se utiliza como dirección IP standby para el link de stateful failover.

```
PIX1(config)#failover interface ip stateful 10.0.0.1
                    255.255.255.0 standby 10.0.0.2
```

La dirección IP standby debe estar en la misma subred que la dirección IP activa. Usted no necesita identificar la máscara de subred de la dirección IP standby.La dirección IP y la dirección MAC del link de stateful failover no cambian en el failover excepto cuando Stateful Failover utiliza una interfaz de datos regular. La dirección IP activa permanece siempre con la unidad primaria, mientras que la dirección IP standby permanece con la unidad secundaria.Habilite la interfaz:

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

5. Configure los grupos de failover. Puede tener al menos dos grupos de conmutación por fallas. El comando **failover group** crea el grupo de failover especificado si no existe e ingresa al modo de configuración del grupo de failover.Para cada grupo de conmutación por fallas, debe especificar si el grupo de conmutación por fallas tiene preferencia primaria o secundaria usando el comando **primario** o **secundario**. Puede asignar la misma preferencia a ambos grupos de conmutación por fallas. Para las configuraciones de balanceo de carga, debe asignar a cada grupo de conmutación por fallas una preferencia de unidad diferente.El siguiente ejemplo asigna al grupo de conmutación por fallas 1 una preferencia primaria y al grupo de conmutación por fallas 2 una preferencia secundaria:
```
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. Asigne cada contexto de usuario a un grupo de conmutación por fallas usando el comando **Join-failover-group** en el modo de configuración de contexto.Los contextos no asignados se asignan automáticamente al grupo de conmutación por fallas 1. El contexto de administración siempre es miembro del grupo de conmutación por fallas 1.Ingrese estos comandos para asignar cada contexto a un grupo de failover:
```
hostname(config)#context context_name
hostname(config-context)#join-failover-group {1 | 2}
hostname(config-context)#exit
```

7. Habilite el failover:
```
hostname(config)#failover
```

8. Encienda la unidad secundaria y habilite el failover en la unidad si aún no está habilitado:
```
hostname(config)#failover
```

   La unidad activa envía la configuración en la memoria en ejecución a la unidad standby. A medida que la configuración se sincroniza, aparecen los mensajes "Beginning configuration replication: sending to mate" y "End Configuration Replication to mate" en la consola primaria.**Nota:** Ejecute el comando **failover** en el dispositivo primario primero y luego ejecútelo en el dispositivo secundario. Después de que usted ejecute el **comando failover en el dispositivo secundario, el dispositivo secundario toma inmediatamente la configuración del dispositivo primario y se establece como** *standby*. El ASA primario permanece activo, y pasa el tráfico normalmente y se marca como el *dispositivo activo.* A partir de ese momento, siempre que una falla ocurra en el dispositivo activo, el dispositivo standby emerge como el activo.
9. Guarde la configuración en la memoria Flash en la unidad primaria. Dado que los comandos ingresados en la unidad primaria se replican en la unidad secundaria, la unidad secundaria también guarda su configuración en la memoria Flash.
```
hostname(config)#copy running-config startup-config
```

10. Si es necesario, fuerce cualquier grupo de failover que esté activo en el estado primario al activo en el secundario. Para obligar a un grupo de conmutación por fallas a que se active en la unidad secundaria, ejecute este comando en el espacio de ejecución del sistema en la unidad primaria:

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

El argumento group_id especifica el grupo que desea activar en la unidad secundaria.

Configuraciones

En este documento, se utilizan estas configuraciones:

- PIX1 - Configuración del sistema
- Configuración de PIX1 - Contexto1
- Configuración de PIX1 - Contexto2

PIX1 - Configuración del 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
```

Configuración de PIX1 - Contexto1

```
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
```

Configuración de PIX1 - Contexto2

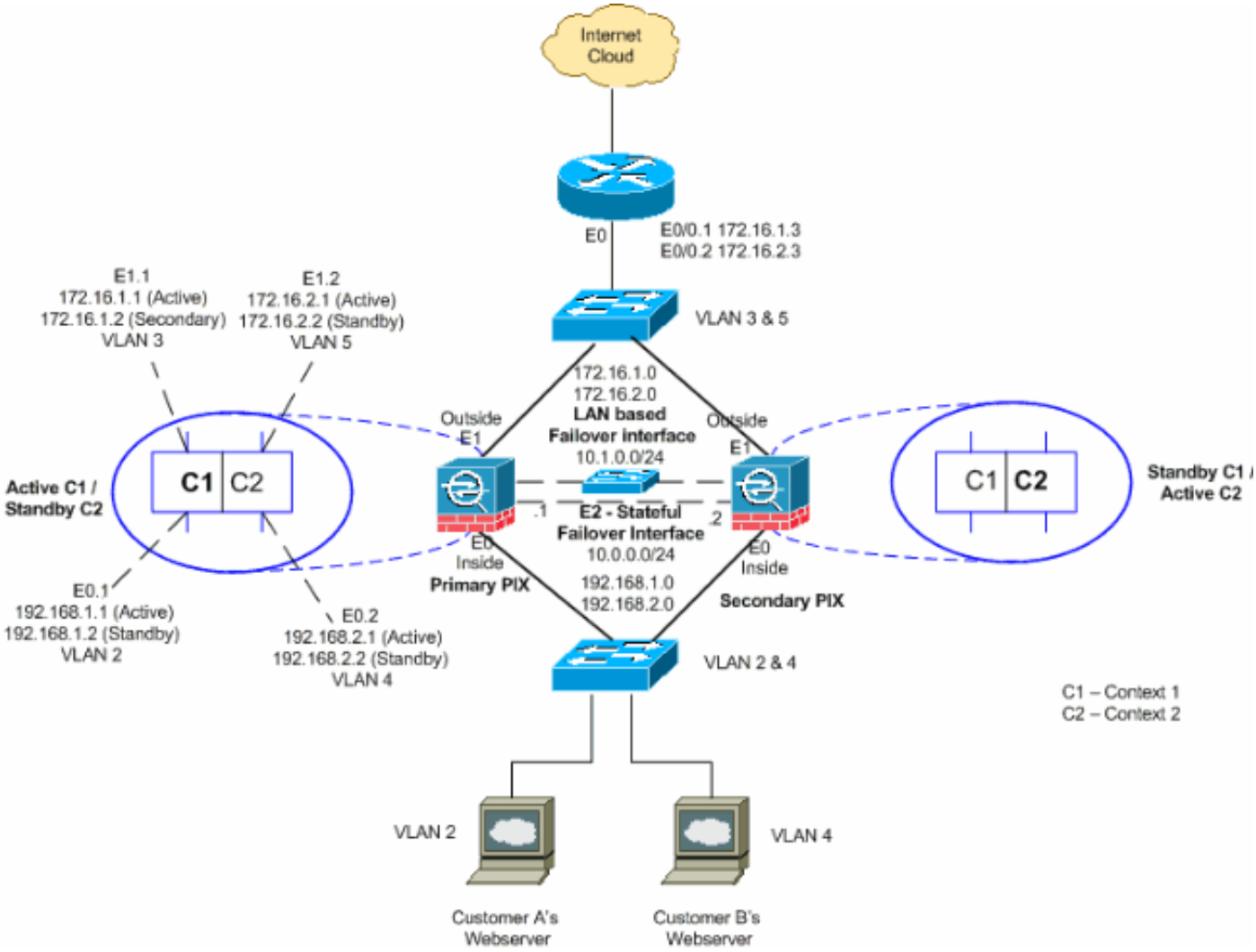
```
PIX1/context2(config)#show running-config
: Saved
:
PIX Version 7.2(2)




!
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
```

Configuración de Active/Active Failover Basada en LAN

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Esta sección describe cómo configurar el failover activo/activo usando un link de failover Ethernet. Al configurar el failover basado en LAN, debe iniciar el dispositivo secundario para reconocer el link de failover antes de que el dispositivo secundario pueda obtener la configuración en ejecución del dispositivo primario.

Nota: En lugar de utilizar un cable Ethernet de cruce para vincular directamente las unidades, Cisco recomienda utilizar un switch dedicado entre las unidades primaria y secundaria.

Esta sección incluye los temas como se muestra a continuación:

- Configuración de la Unidad Primaria
- Configuración de la Unidad Secundaria

Configuración de la Unidad Primaria

Complete estos pasos para configurar la unidad primaria en una configuración de failover Activo/Activo:

1. Si aún no lo ha hecho, configure las direcciones IP activas y en espera para cada interfaz de datos (modo enrutado), para la dirección IP de administración (modo transparente) o para la interfaz de sólo administración. La dirección IP standby se utiliza en el dispositivo de seguridad que es actualmente la unidad standby. Debe estar en la misma subred que la dirección IP activa.Debe configurar las direcciones de interfaz desde dentro de cada

contexto. Utilice el **comando changeto context para conmutar entre los contextos.** El comando indica cambios en hostname/context(config-if)#, donde context es el nombre del contexto actual. En el modo de firewall transparente, debe ingresar una dirección IP de administración para cada contexto.**Nota:** No configure una dirección IP para el link Stateful Failover si va a utilizar una interfaz dedicada de Stateful Failover. Usted utiliza el **comando failover interface ip para configurar una interfaz dedicada de stateful failover en un paso posterior.**

```
hostname/context(config-if)#ip address active_addr netmask standby standby_addr
```

En el ejemplo, la interfaz externa para context1 del PIX primario se configura de esta manera:

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

Para el contexto 2:

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

En el modo de firewall ruteado y para la interfaz sólo de administración, este comando se ingresa en el modo de configuración de interfaz para cada interfaz. En el modo de firewall transparente, el comando se ingresa en el modo de configuración global.

2. Configure los parámetros básicos de failover en el espacio de ejecución del sistema.(Solo dispositivo de seguridad PIX) Habilite la conmutación por fallas basada en LAN:

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

Designe la unidad como la unidad primaria:

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

Especifique el link de failover:

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

En este ejemplo, utilizamos la interfaz ethernet 3 como interfaz de failover basada en LAN.

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

El argumento if_name asigna un nombre lógico a la interfaz especificada por el argumento phy_if. El argumento phy_if puede ser el nombre del puerto físico, como Ethernet1, o una subinterfaz previamente creada, como Ethernet0/2.3. En el dispositivo de seguridad adaptable ASA 5505, phy_if especifica una VLAN. Esta interfaz no se debe utilizar para ningún otro propósito (excepto, opcionalmente, el link Stateful Failover).Especifique las direcciones IP activas y standby del link de failover:

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

Para este ejemplo, utilizamos 10.1.0.1 como activo y 10.1.0.2 como direcciones IP en espera para la interfaz de failover.

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

La dirección IP standby debe estar en la misma subred que la dirección IP activa. Usted no necesita identificar la máscara de subred de la dirección IP standby. La dirección IP y la dirección MAC del link de failover no cambian en el failover. La dirección IP activa permanece siempre con la unidad primaria, mientras que la dirección IP standby permanece

con la unidad secundaria.

3. Para habilitar Stateful Failover, configure el enlace Stateful Failover:Especifique la interfaz que se utilizará como enlace Stateful Failover:

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

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

El argumento if_name asigna un nombre lógico a la interfaz especificada por el argumento phy_if. El argumento phy_if puede ser el nombre del puerto físico, como Ethernet1, o una subinterfaz previamente creada, como Ethernet0/2.3. Esta interfaz no debe utilizarse para ningún otro propósito (excepto, opcionalmente, el link de failover).**Nota:** Si el link Stateful Failover utiliza el link de failover o una interfaz de datos normal, sólo necesita suministrar el argumento if_name.Asigne una dirección IP activa y standby al link de stateful failover.**Nota:** Si el link Stateful Failover utiliza el link de failover o una interfaz de datos normal, omita este paso. Usted ha definido ya las direcciones IP activas y standby para la interfaz.

```
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
```

La dirección IP standby debe estar en la misma subred que la dirección IP activa. Usted no necesita identificar la máscara de subred de la dirección standby. La dirección IP del link de estado y la dirección MAC no cambian en el failover. La dirección IP activa permanece siempre con la unidad primaria, mientras que la dirección IP standby permanece con la unidad secundaria.Habilite la interfaz.**Nota:** Si el link Stateful Failover utiliza el link de failover o la interfaz de datos regular, omita este paso. Usted ha habilitado ya la interfaz.

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

4. Configure los grupos de failover. Puede tener al menos dos grupos de conmutación por fallas. El comando **failover group** crea el grupo de failover especificado si no existe e ingresa al modo de configuración del grupo de failover.Para cada grupo de failover, especifique si el grupo de failover tiene preferencia **primaria** o **secundaria** usando el comando primario o secundario. Puede asignar la misma preferencia a ambos grupos de conmutación por fallas. Para las configuraciones de balanceo de carga, debe asignar a cada grupo de conmutación por fallas una preferencia de unidad diferente.El siguiente ejemplo asigna al grupo de conmutación por fallas 1 una preferencia primaria y al grupo de conmutación por fallas 2 una preferencia secundaria:

```
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. Asigne cada contexto de usuario a un grupo de conmutación por fallas usando el comando de **unión-conmutación por fallas-grupo** en el modo de configuración de contexto.Los contextos no asignados se asignan automáticamente al grupo de conmutación por fallas 1. El contexto de administración siempre es miembro del grupo de conmutación por fallas

1.Ingrese estos comandos para asignar cada contexto a un grupo de failover:

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

6. Habilite el failover.

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

Configuración de la Unidad Secundaria

Al configurar la conmutación por fallas activa/activa basada en LAN, debe iniciar la unidad secundaria para reconocer el link de conmutación por fallas. Esto permite que la unidad secundaria se comunique con y reciba la configuración en ejecución de la unidad primaria.

Complete estos pasos para iniciar la unidad secundaria en una configuración de failover Activo/Activo:

1. (Solo dispositivo de seguridad PIX) Habilite la conmutación por fallas basada en LAN.

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

2. Defina la interfaz de failover. Utilice la misma configuración que utilizó para la unidad primaria:Especifique la interfaz que se utilizará como la interfaz de failover.

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

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

El argumento if_name asigna un nombre lógico a la interfaz especificada por el argumento phy_if. El argumento phy_if puede ser el nombre del puerto físico, como Ethernet1, o una subinterfaz previamente creada, como Ethernet0/2.3. En el dispositivo de seguridad adaptable ASA 5505, phy_if especifica una VLAN.Asigne la dirección IP activa y standby al 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
```

Nota: Ingrese este comando exactamente como lo ingresó en la unidad primaria cuando configuró la interfaz de failover.La dirección IP standby debe estar en la misma subred que la dirección IP activa. Usted no necesita identificar la máscara de subred de la dirección standby.Habilite la interfaz.

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

3. Designe esta unidad como la unidad secundaria:

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

Nota: Este paso es opcional porque, de forma predeterminada, las unidades se designan como secundarias a menos que se haya configurado de otro modo.

4. Habilite el failover.

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

Después de que usted habilita el failover, la unidad activa envía la configuración en la memoria en ejecución a la unidad standby. A medida que la configuración se sincroniza, aparecen los mensajes **Beginning configuration replication: Sending to mate y End Configuration Replication to mate en la consola de la unidad activa.Nota:** Ejecute el comando **failover** en el dispositivo primario primero y luego ejecútelo en el dispositivo secundario. Después de que usted ejecute el **comando failover en el dispositivo secundario, el dispositivo secundario toma inmediatamente la configuración del dispositivo primario y se establece como** *standby*. El ASA primario permanece activo, y pasa el tráfico normalmente y se marca como el *dispositivo activo.* A partir de ese momento, siempre que una falla ocurra en el dispositivo activo, el dispositivo standby emerge como el activo.

5. Después de que la configuración en ejecución haya completado la replicación, ingrese este comando para guardar la configuración en la memoria Flash:
   ```
   hostname(config)#copy running-config startup-config
   ```

6. Si es necesario, fuerce cualquier grupo de failover que esté activo en el estado primario al activo en la unidad secundaria. Para obligar a un grupo de conmutación por fallas a que se active en la unidad secundaria, ingrese este comando en el espacio de ejecución del sistema en la unidad primaria:
   ```
   hostname#no failover active group group_id
   ```

   El argumento group_id especifica el grupo que desea activar en la unidad secundaria.

Configuraciones

En este documento, se utilizan estas configuraciones:

PIX Primario

```
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: Refiérase a la sección Configuración de Failover Basada en Cable, PIX1 - Configuración de Contexto1 y PIX1 - Configuración de Contexto2 para la configuración del contexto en el escenario de failover basado en LAN.

PIX Secundario

```
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
```

Verificación

Uso del Comando show failover

Esta sección describe el resultado del **comando show failover.** En cada unidad, usted puede verificar el estado de failover con el **comando show failover.**

PIX Primario

```
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 Secundario

```
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
```

Utilice el comando **show failover state para verificar el estado.**

PIX Primario

```
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
```

Unidad secundaria

```
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 las direcciones IP de la unidad de failover, utilice **show failover interfacecommand.**

Unidad primaria

```
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
```

Unidad secundaria

```
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
```

Vista de las Interfaces Monitoreadas

Para ver el estado de las interfaces monitoreadas: En el modo single context, ingrese el comando show monitor-interface en el modo global configuration. En el modo multiple context, ingrese `show monitor-interface dentro de un contexto.`

Nota: Para habilitar la supervisión de estado en una interfaz específica, utilice el comando monitor-interface en el modo de configuración global:

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

PIX Primario

```
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 Secundario

```
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
```

Nota: Si no ingresa una dirección IP de failover, el comando **show failover** muestra 0.0.0.0 para la dirección IP, y el monitoreo de las interfaces permanece en un estado de "espera". Debe establecer una dirección IP de failover para que funcione la conmutación por fallas. Para obtener más información sobre los diferentes estados para la conmutación por fallas, refiérase a show failover.

De forma predeterminada, se habilita el monitoreo de las interfaces físicas y se inhabilita el monitoreo de las subinterfaces.

Visualización de los Comandos de Failover en la Configuración en Ejecución

Para ver los comandos de failover en la configuración en ejecución, ingrese este comando:

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

Se visualizan todos los comandos de failover. En las unidades que se ejecutan en el modo multiple context, ingrese el `comando show running-config failover en el espacio de la ejecución del sistema.` Ingrese el comando **show running-config all failover** para mostrar los comandos failover en la configuración en ejecución e incluir los comandos para los cuales no ha cambiado el valor predeterminado.

Pruebas de Funcionalidad de Failover

Para probar la funcionalidad de failover, realice estos pasos:

1. Pruebe que su grupo de failover o unidad activa pase el tráfico como se espera con FTP (por ejemplo) para enviar un archivo entre hosts en diversas interfaces.
2. Fuerce un failover a la unidad standby con este comando:Para conmutación por fallas activa/activa, ingrese el siguiente comando en la unidad donde el grupo de conmutación por fallas que contiene la interfaz que conecta sus hosts está activo:
   ```
   hostname(config)#no failover active group group_id
   ```
3. Utilice FTP para enviar otro archivo entre los dos mismos hosts.
4. Si la prueba no fue satisfactoria, ingrese el **comando show failover de verificar el estado de failover.**
5. Cuando finalice, puede restaurar el grupo de failover o la unidad al estado activo con este comando:Para conmutación por fallas activa/activa, ingrese el siguiente comando en la unidad donde el grupo de conmutación por fallas que contiene la interfaz que conecta sus hosts está activo:
   ```
   hostname(config)#failover active group group_id
   ```

Failover Forzado

Para forzar la unidad standby para pasar a ser activa, ingrese uno de estos comandos:

Ingrese este comando en el espacio de ejecución del sistema de la unidad donde el grupo de failover está en estado standby:

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

O bien, ingrese este comando en el espacio de ejecución del sistema de la unidad donde el grupo de failover está en el estado activo:

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

Al ingresar este comando en el espacio de ejecución del sistema, todos los grupos de conmutación por fallas se activan:

```
hostname#failover active
```

Failover Inhabilitado

Para inhabilitar el failover, ingrese este comando:

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

Si usted inhabilita el failover en un par Active/Standby, hace que el estado activo y standby de cada unidad se mantenga hasta que usted reinicie. Por ejemplo, la unidad standby permanece en el modo standby de modo que ambas unidades no comiencen a pasar el tráfico. Para hacer que la unidad standby esté activa (incluso con failover desactivado), vea la sección Forced Failover.

Si usted inhabilita el failover en un par Activo/Activo, hace que los grupos de failover permanezcan en el estado activo en cualquier unidad en la que actualmente están activos, independientemente de la unidad de preferencia configurada. El comando **no failover puede ser ingresado en el espacio de la ejecución del sistema.**

Restauración de una Unidad Defectuosa

Para restaurar un grupo de failover activo/activo fallido a un estado sin fallas, ingrese este comando:

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

Si usted restaura una unidad defectuosa a un estado no defectuosa, no cambia automáticamente a activa; las unidades o los grupos restaurados permanecen en el estado standby hasta que pasan a activos mediante el failover (forzado o natural). Una excepción es un grupo de failover configurado con el comando preempt. Si un grupo de failover estaba previamente activo, un grupo de failover cambia a activo si lo configuran con el comando preempt y si la unidad en la que falló es su unidad preferida.

Reemplazar la Unidad Defectuosa por una Nueva Unidad

Complete estos pasos para reemplazar una unidad defectuosa por una nueva unidad:

1. Ejecute el **comando no failover en la unidad primaria.**El estado de la unidad secundaria muestra **standby unit as not detected**.
2. Desconecte la unidad primaria, y conecte la unidad primaria de reemplazo.
3. Verifique que las unidades de reemplazo funcionen con la misma versión de software y de ASDM que la unidad secundaria.
4. Ejecute estos comandos en las unidades de reemplazo:

```
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 la unidad primaria de reemplazo a la red, y ejecute este comando:
```
ASA(config)#failover
```

Troubleshoot

Cuando ocurre un failover, ambos dispositivos de seguridad envían mensajes del sistema. Esta sección incluye estos temas:

1. Mensajes del sistema de fallas
2. Mensajes del debug
3. SNMP (Protocolo de administración de red simple)

Mensajes del sistema de fallas

El dispositivo de seguridad ejecuta varios mensajes del sistema relacionados con el failover en el nivel de prioridad 2, que indica una Condición crítica. Para ver estos mensajes, consulte la configuración de registro y a los mensajes del registro del sistema de Dispositivos de Seguridad de Cisco para habilitar el registro y para ver las descripciones de los mensajes del sistema.

Nota: Dentro del switchover, la conmutación por fallas se apaga lógicamente y luego activa las interfaces, lo que genera mensajes syslog **411001** y **411002**. Esta es actividad normal.

Comunicaciones de fallas perdidas primarias con el compañero en el interface_name de la interfaz

Este mensaje de failover se muestra si una unidad del par failover ya no puede comunicarse con la otra unidad del par. Primario puede también ser enumerado como secundario para la unidad secundaria.

(Primario) perdió las comunicaciones de failover con el compañero en la interfaz interface_name

Verificar que esté funcionando la red que está conectada con la interfaz especificada correctamente.

Mensajes del debug

Para ver los mensajes del debug, ingrese el comando del **fover del debug.** Consulte Referencia de Comandos de Dispositivos de Seguridad de Cisco, versión 7.2 para obtener más información.

Nota: Debido a que se asigna alta prioridad a la salida de depuración en el proceso de CPU, puede afectar drásticamente al rendimiento del sistema. Por esta razón, utilice los comandos del **fover del debug de resolver problemas solamente los problemas específicos o dentro de las sesiones de Troubleshooting con el equipo de Soporte Técnico de Cisco.**

SNMP (Protocolo de administración de red simple)

Para recibir las trampas de Syslog SNMP para el failover, configurar al agente SNMP para enviar el SNMP traps a las estaciones de la administración de SNMP, definir un syslog host, y compilar Cisco syslog MIB en su estación de la administración de SNMP. Consulte los comandos **snmp-server** y **logging** en la Referencia de Comandos de Dispositivos de Seguridad de Cisco, Versión 7.2 para obtener más información.

Tiempo de sondeo de fallas

Para especificar el sondeo de la unidad de failover y los tiempos de espera, ejecute el comando **failover polltime** en el modo de configuración global.

El `tiempo de sondeo de fallas msec [time]` representa el intervalo de tiempo para verificar la existencia de la unidad standby sondeando los mensajes hello.

De manera similar, `failover holdtime unit msec [time]` representa el período de tiempo durante el cual una unidad debe recibir un mensaje hello en el link de failover, después del cual se declara que la unidad peer ha fallado.

Consulte tiempo de sondeo de fallas para obtener más información.

ADVERTENCIA: Incidente del desciframiento del mensaje de falla.

Mensaje de error:

```
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
```

Este problema ocurre debido a la configuración de la clave de failover. Para resolver este problema, quitar el clave de failover, y configurar la nueva clave compartida.

Información Relacionada

- Página de soporte de PIX de la serie 500 de Cisco
- Configuración de falla del módulo de servicios del firewall (FWSM)
- Troubleshooting del Failover FWSM
- Cómo el Failover trabaja en el Cisco Secure PIX Firewall
- Página de Soporte de Cisco 5500 Series Adaptive Security Appliance
- Soporte Técnico y Documentación - Cisco Systems