

ASA/PIX: Configuración de Active/Standby Failover en Modo Transparente

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Active/Standby Failover](#)

[Descripción General del Active/Standby Failover](#)

[Estado Primario/Secundario 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](#)

[Configuración de Active/Standby Failover Basado 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](#)

[Troubleshoot](#)

[Monitoreo de Failover](#)

[Falla en la Unidad](#)

[El LU afecta un aparato la conexión fallada](#)

[Mensajes del sistema de fallas](#)

[Mensajes del debug](#)

[SNMP \(Protocolo de administración de red simple\)](#)

[Tiempo de sondeo de fallas](#)

[Certificado de exportación/clave privada en configuración de falla](#)

[ADVERTENCIA: Incidente del desciframiento del mensaje de falla.](#)

[Problema: La conmutación por fallas siempre es inestable después de configurar la conmutación por fallas multimodo Activo/En espera transparente](#)

[Failover de los módulos ASA](#)

[Alloc del bloque del mensaje de falla fallado](#)

[Problema del Failover del módulo AIP](#)

[Problemas conocidos](#)

[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](#)
- [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.

Un firewall transparente, es un firewall de Capa 2 que actúa como un *parpadeo en el cable*, o un *firewall sigiloso*, y no se ve como un salto de router a los dispositivos conectados. El dispositivo de seguridad conecta la misma red en sus puertos internos y externos. Dado que el firewall no es un salto ruteado, es fácil introducir un firewall transparente en una red existente; no es necesario volver a direccionar IP. Puede configurar el dispositivo de seguridad adaptable para que se ejecute en el modo de firewall ruteado predeterminado o en el modo de firewall transparente. Cuando cambia de modo, el dispositivo de seguridad adaptable borra la configuración porque muchos comandos no se soportan en ambos modos. Si ya tiene una configuración cumplimentada, asegúrese de realizar una copia de seguridad de esta configuración antes de cambiar el modo; puede utilizar esta configuración de copia de seguridad como referencia al crear una nueva configuración. Consulte [Ejemplo de Configuración de Firewall Transparente](#) para obtener más información sobre la configuración del dispositivo de firewall en el modo Transparente.

Este documento se centra en cómo configurar un Failover Activo/En Espera en el Modo Transparente en el Dispositivo de Seguridad ASA.

Nota: La conmutación por fallas VPN no se soporta en las unidades que se ejecutan en el modo multiple context. La conmutación por fallas de VPN está disponible para configuraciones

Active/Standby Failover solamente.

Cisco le recomienda que no utilice la interfaz de administración para el failover, especialmente para el stateful failover en el que el dispositivo de seguridad envía constantemente la información de conexión de un dispositivo de seguridad a otro. La interfaz para el failover debe tener por lo menos la misma capacidad que las interfaces que pasan el tráfico normal, y mientras que las interfaces en el ASA 5540 son gigabit, la interfaz de administración es FastEthernet solamente. La interfaz de administración está diseñada para el tráfico de administración solamente y se especifica como management0/0. Sin embargo, puede utilizar el comando **management-only** para configurar cualquier interfaz para que sea una interfaz sólo de administración. Además, para la gestión 0/0, usted puede inhabilitar el modo management-only para que la interfaz pueda pasar con el tráfico como cualquier otra interfaz. Consulte [Referencia de Comandos de Dispositivos de Seguridad de Cisco, Versión 8.0](#) para obtener más información sobre el comando **management-only**.

Esta guía de configuración proporciona un ejemplo de configuración para incluir una introducción breve a tecnología PIX/ASA 7.x Active/Standby. Consulte [Guía de Referencia de Comandos de ASA/PIX para un sentido más profundizado de la teoría basada en función de 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 la sección [Ejecución de Actualizaciones de Tiempo de Inactividad Cero para Pares de Failover](#) de la *Guía de Configuración de Línea de Comandos de Dispositivos de Seguridad de Cisco, Versión 8.0* para obtener más información sobre cómo actualizar el software en un par de failover.

Requisitos de Licencia

En la plataforma de dispositivos de seguridad ASA, al menos una de las unidades debe tener una **licencia sin restricciones (UR)**.

Nota: Puede ser necesario actualizar las licencias en un par de failover para obtener características y beneficios adicionales. Refiérase a [Actualización de Clave de Licencia en un Par de Failover](#) para obtener más información.

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

Componentes Utilizados

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

- Dispositivo de seguridad ASA 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:

- PIX Security Appliance con versión 7.x y posterior

Convenciones

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

Active/Standby Failover

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

- [Descripción General del Active/Standby Failover](#)
- [Estado Primario/Secundario y Estado Activo/Standby](#)
- [Sincronización de la Configuración e Inicialización del dispositivo](#)
- [Réplica de Comandos](#)
- [Disparadores del Failover](#)
- [Acciones de Failover](#)

Descripción General del Active/Standby Failover

Active/Standby Failover le permite utilizar un dispositivo de seguridad standby para asumir el control de la funcionalidad de una unidad defectuosa. Cuando la unidad activa falla, cambia al estado standby mientras que la unidad standby cambia al estado activo. La unidad que se activa asume las direcciones IP o, para un firewall transparente, la dirección IP de administración y las direcciones MAC de la unidad fallida y comienza a pasar tráfico. La unidad que ahora está en el

estado standby asume el control sobre las direcciones IP y las direcciones MAC en standby. Dado que los dispositivos de red no ven ningún cambio en el emparejamiento de direcciones MAC a IP, ninguna entrada ARP cambia o se desconecta en ningún lugar de la red.

Nota: Para el modo de contexto múltiple, el dispositivo de seguridad puede conmutar por error toda la unidad, que incluye todos los contextos, pero no puede fallar en contextos individuales por separado.

[Estado Primario/Secundario y Estado Activo/Standby](#)

Las diferencias principales entre las dos unidades en un par de failover se relacionan con qué unidad está activa y qué unidad está standby, a saber, qué direcciones IP deben utilizarse, y qué unidad es primaria y activamente pasa el tráfico.

Existen algunas diferencias entre las unidades basadas en qué unidad es primaria, como se especifica en la configuración, y qué unidad es secundaria:

- La unidad primaria siempre se convierte en la unidad activa si ambas unidades empiezan se inician al mismo tiempo (y tienen el mismo estado de funcionamiento).
- La dirección MAC de la unidad primaria siempre se junta con las direcciones IP activas. La anomalía a esta regla ocurre cuando la unidad secundaria es activa y no puede obtener la dirección MAC primario sobre el link de failover. En este caso, se utiliza la dirección MAC secundaria.

[Sincronización de la Configuración e Inicialización del dispositivo](#)

La sincronización de la configuración ocurre cuando uno o ambos dispositivos en un par de failover se inician. Las configuraciones se sincronizan siempre de la unidad activa a la unidad standby. Cuando la unidad standby completa su inicio inicial, borra su configuración en ejecución, excepto por los comandos failover que son necesarios para comunicarse con la unidad activa, y la unidad activa envía su configuración completa a la unidad standby.

La unidad activa es determinada por lo siguiente:

- Si una unidad se inicia y detecta un peer ya operativo como activa, se convierte en la unidad standby.
- Si una unidad se inicia y no detecta un peer, se convierte en la unidad activa.
- Si ambas unidades se inician simultáneamente, la unidad primaria se convierte en la unidad activa, y la unidad secundaria se convierte en la unidad standby.

Nota: Si la unidad secundaria se inicia y no detecta la unidad primaria, se convierte en la unidad activa. Utilice sus propias direcciones MAC para las direcciones IP activas. Cuando la unidad primaria está disponible, la unidad secundaria cambia las direcciones MAC a las de la unidad primaria, que puede causar una interrupción en su tráfico de red. Para evitar esto, configurr un par de failover con las direcciones MAC virtuales. Consulte la sección [Configuración de Active/Standby Failover de este documento para obtener más información](#).

Cuando se inicia la replicación, la consola del dispositivo de seguridad en la unidad activa muestra el mensaje `Beginning configuration replication: Enviando a mate` y, cuando se completa, el dispositivo de seguridad muestra el mensaje `End Configuration Replication to mate`. Dentro de la réplica, los comandos ingresados en la unidad activa no pueden replicarse correctamente en la unidad standby, y los comandos ingresados en la unidad standby pueden ser sobrescritos por la

configuración que se replica de la unidad activa. No ingrese comandos en cualquier unidad en un par de failover dentro del proceso de la réplica de la configuración. Según el tamaño de la configuración, la réplica puede llevar desde algunos segundos hasta varios minutos.

Desde la unidad secundaria, puede observar el mensaje de replicación a medida que se sincroniza desde la unidad primaria:

```
ASA> .
```

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

```
ASA>
```

En la unidad standby, la configuración existe solamente en la memoria en ejecución. Para guardar la configuración en la memoria Flash después de la sincronización, ingrese estos comandos:

- Para el modo single context, ingrese el **comando copy running-config startup-config en la unidad activa**. El comando se replica en la unidad standby, que procede a escribir su configuración en la memoria Flash.
- Para el modo multiple context, ingrese el **comando copy running-config startup-config en la unidad activa desde el espacio de la ejecución del sistema y desde dentro de cada contexto en el disco**. El comando se replica en la unidad standby, que procede a escribir su configuración en la memoria Flash. Los contextos con las configuraciones de inicio en los servidores externos son accesibles desde cualquier unidad a través de la red y no necesitan ser guardados por separado para cada unidad. Alternativamente, usted puede copiar los contextos en el disco de la unidad activa a un servidor externo, y después los copia al disco en la unidad standby, donde están disponibles cuando la unidad se recarga.

Réplica de Comandos

La réplica de los comandos fluye siempre de la unidad activa a la unidad standby. Si bien los comandos se ingresan en la unidad activa, se envían a través del link de failover a la unidad standby. Usted no tiene que guardar la configuración activa en la memoria Flash para replicar los comandos.

Nota: Los cambios realizados en la unidad en espera no se replican en la unidad activa. Si usted ingresa un comando en la unidad standby, el dispositivo de seguridad muestra el mensaje ****** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit**. Las configuraciones ya no se sincronizan. Se visualiza este mensaje incluso si usted ingresa los comandos que no afectan la configuración.

Si ingresa el comando **write standby** en la unidad activa, la unidad standby borra su configuración en ejecución, excepto por los comandos failover usados para comunicarse con la unidad activa, y la unidad activa envía su configuración completa a la unidad standby.

Para el modo multiple context, cuando usted ingresa el **comando write standby en el espacio de la ejecución del sistema, se replican todos los contextos**. Si usted ingresa el comando write standby dentro de un contexto, el comando replica solamente la configuración del contexto.

Los comandos replicados se guardan en la configuración en ejecución. Para guardar los

comandos replicados en la memoria Flash en la unidad standby, ingrese estos comandos:

- Para el modo single context, ingrese el **comando copy running-config startup-config en la unidad activa**. El comando se replica en la unidad standby, que procede a escribir su configuración en la memoria Flash.
- Para el modo multiple context, ingrese el **comando copy running-config startup-config en la unidad activa desde el espacio de la ejecución del sistema y desde dentro de cada contexto en el disco**. El comando se replica en la unidad standby, que procede a escribir su configuración en la memoria Flash. Los contextos con las configuraciones de inicio en los servidores externos son accesibles desde cualquier unidad a través de la red y no necesitan ser guardados por separado para cada unidad. Alternativamente, usted puede copiar los contextos en el disco de la unidad activa a un servidor externo, y después los copia al disco en la unidad standby.

Disparadores del Failover

La unidad puede fallar si ocurre uno de estos eventos:

- La unidad tiene una falla de hardware o una falla de energía.
- La unidad tiene una falla de software.
- Fallan demasiadas interfaces monitoreadas.
- El **comando no failover active se ingresa en la unidad activa o el comando failover active se ingresa en la unidad standby**.

Acciones de Failover

En Active/Standby Failover, el failover ocurre por unidad. Incluso en los sistemas que se ejecutan en el modo multiple context, usted no puede conmutar por error contextos individuales o grupos de contextos.

Esta tabla muestra la acción de failover para cada evento de failover. Para cada evento de failover, la tabla muestra la política de failover (failover o ningún failover), medidas tomadas por la unidad activa, medidas tomadas por la unidad standby, y cualquier nota especial sobre la condición y las acciones de failover. La tabla muestra el comportamiento de failover.

Evento de Falla	Política	Acción de Active	Acción de Standby	Notas
Unidad activa fallada (energía o hardware)	Failover	n/a	Pasar a activa; marcar active como fallada	No se reciben mensajes hello en ninguna interfaz monitoreada o el link de failover.
La unidad	Ningún	Pasar a	Ninguna	Ninguno

activa anterior se recupera	n failover	stand by	acción	
Unidad standby fallada (energía o hardware)	Ningún failover	Marcar standby como fallado	n/a	Cuando la unidad standby es marcada como fallado, la unidad activa no intenta conmutar por error, incluso si se supera el umbral de falla de la interfaz.
Link de failover fallado dentro de la operación	Ningún failover	Marcar la interfaz de failover como fallada	Marcar la interfaz de failover como fallada	Usted debe restaurar el link de failover cuanto antes porque la unidad no puede conmutar por error la unidad standby mientras que el link de failover está inactivo.
Link de failover fallado en el inicio	Ningún failover	Marcar la interfaz de failover como fallada	Pasar a activo	Si el link de failover está inactivo en el inicio, ambas unidades pasar a estar activas.
Link de stateful failover fallado	Ningún failover	Ninguna acción	Ninguna acción	La información de estado llega a estar desactualizada, y se terminan las sesiones si ocurre un failover.
Falla de la interfaz en la unidad activa por sobre el umbral	Failover	Marcar active como fallada	Pasar a activo	Ninguno
Falla de la interfaz en la unidad standby sobre el umbral	Ningún failover	Ninguna acción	Marcar standby como fallado	Cuando la unidad standby es marcada como fallada, la unidad activa no intenta conmutar por error incluso si se supera el umbral de falla de la interfaz.

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 asume 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
- La tabla de puente de Capa 2 (sólo cuando el firewall se ejecuta en el modo **firewall transparente**)
- 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:

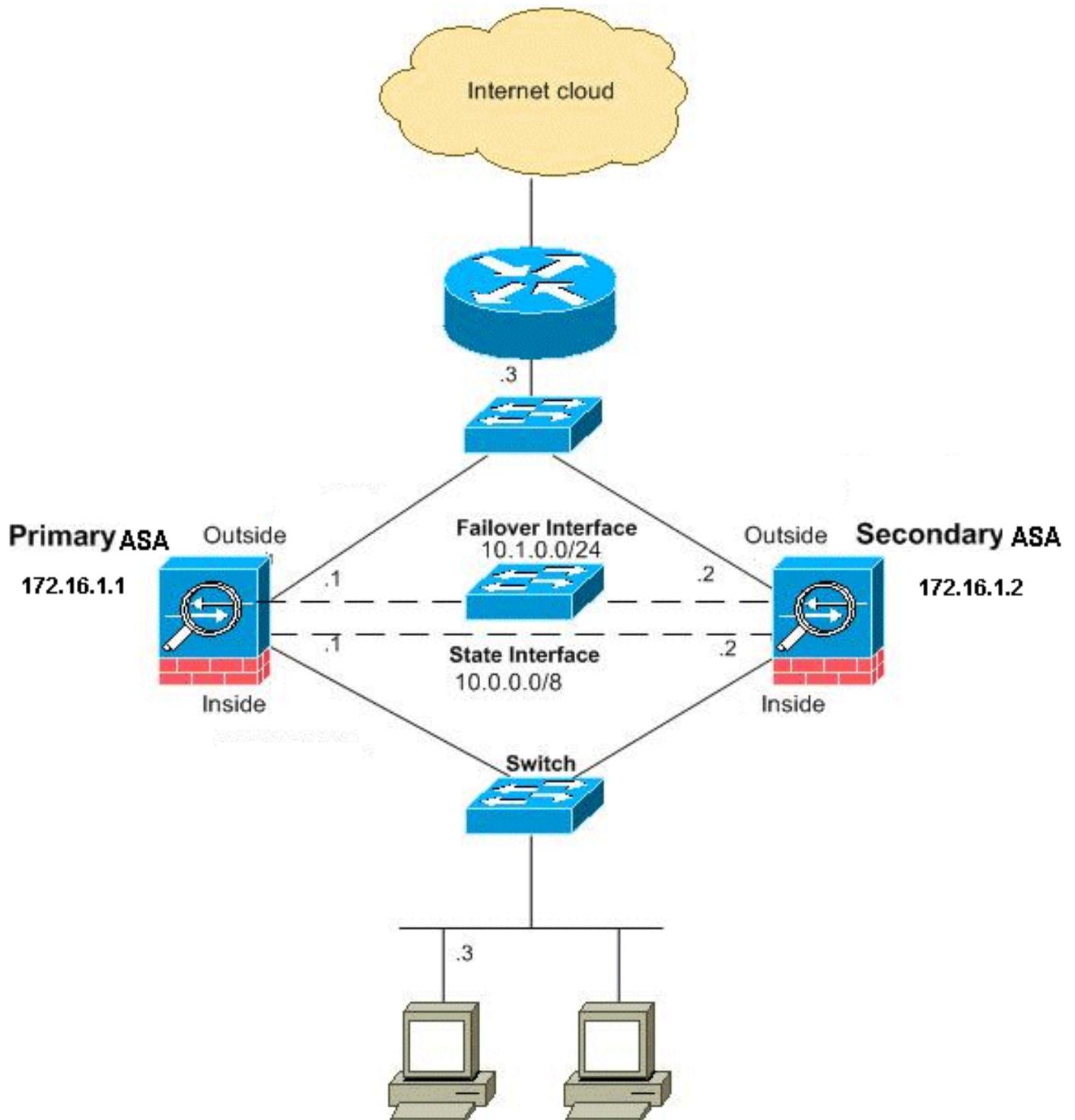
- La tabla de la conexión HTTP (a menos que se habilite la réplica HTTP)
- La tabla de la autenticación de usuario (uauth)
- Las tablas de ruteo
- Información del estado para los módulos del servicio de seguridad

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 finaliza la llamada, el cliente IP SoftPhone pierde la conexión con Cisco CallManager. Esto ocurre porque no hay información de la sesión para el mensaje para colgar CTIQBE en la unidad standby. Cuando el cliente IP SoftPhone no recibe una respuesta de Cisco CallManager dentro de un período determinado, considera que Cisco CallManager es inalcanzable y se desregistra.

Configuración de Active/Standby Failover Basado en LAN

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Esta sección describe cómo configurar Active/Standby Failover en el modo Transparente con un link de failover Ethernet. Cuando usted configura el failover basado en LAN, debe ejecutar el proceso de arranque del dispositivo secundario para reconocer el link de failover antes de que el dispositivo secundario pueda obtener la configuración en ejecución del dispositivo principal.

Nota: Si cambia de la conmutación por fallas basada en cable a la conmutación por fallas basada en LAN, puede omitir muchos pasos, como la asignación de las direcciones IP activas y en espera para cada interfaz, que completó para la configuración de conmutación por fallas basada en cable.

Configuración de la Unidad Primaria

Complete estos pasos para configurar la unidad primaria en una configuración de Active/Standby Failover basada en LAN. Estos pasos proporcionan la configuración mínima necesaria para habilitar el failover en la unidad primaria. Para el modo multiple context, todos los pasos se ejecutan en el espacio de la ejecución del sistema a menos que se indique lo contrario.

Para configurar la unidad primaria en un par Active/Standby Failover, complete estos pasos:

1. Si aún no lo ha hecho, configure las direcciones IP activas y en espera para la interfaz de administración (modo transparente). 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.**Nota:** No configure una dirección IP para el link de stateful failover si utiliza una interfaz de stateful failover dedicada. Usted utiliza el **comando failover interface ip para configurar una interfaz dedicada de stateful failover en un paso posterior.**

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

A diferencia del modo ruteado, que requiere una dirección IP para cada interfaz, un firewall transparente tiene una dirección IP asignada a todo el dispositivo. El dispositivo de seguridad utiliza esta dirección IP como dirección de origen para los paquetes que se originan en el dispositivo de seguridad, como los mensajes del sistema o las comunicaciones AAA. En el ejemplo, la dirección IP para el ASA primario se configura como se muestra a continuación:

```
hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
```

Aquí, 172.16.1.1 se utiliza para la unidad primaria y 172.16.1.2 se asigna a la unidad secundaria (en espera).**Nota:** En el modo de contexto múltiple, debe configurar las direcciones de interfaz desde dentro de cada contexto. Utilice el comando **changeto context** para cambiar entre contextos. El comando indica cambios en hostname/context(config-if)#, donde context es el nombre del contexto actual.

2. Habilite el failover basado en LAN (plataforma de dispositivos de seguridad PIX solamente).

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

3. Designe la unidad como la unidad primaria.

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

4. Defina la interfaz de failover. Especifique la interfaz que se utilizará como la interfaz de failover.

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

En esta documentación, el "failover" (nombre de la interfaz para Ethernet0) se utiliza para una interfaz de failover.

```
hostname(config)#failover lan interface failover Ethernet3
```

El argumento *if_name* asigna un nombre 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. Asigne la dirección IP activa y standby al link de failover.

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

En esta documentación, para configurar el link de failover, 10.1.0.1 se utiliza para active, 10.1.0.2 para la unidad standby, y "failover" es un nombre de interfaz de Ethernet0.

```
hostname(config)#failover interface ip failover 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 standby. La dirección IP y la dirección MAC del link de failover no cambian en el failover. La dirección IP activa para el link de failover 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
```

En el ejemplo, Ethernet3 se utiliza para el failover:

```
hostname(config)#interface ethernet3
```

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

5. Para habilitar el stateful failover, configure el link de stateful failover (opcional). Especifique la interfaz que se utilizará como el link de stateful failover.

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

Este ejemplo utilizó "state" como un nombre de interfaz para que Ethernet2 intercambie la información de estado de link de failover:

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

Nota: Si el link de stateful failover utiliza el link de failover o una interfaz de datos, sólo necesita suministrar el argumento *if_name*. 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 se debe utilizar para ningún otro propósito, excepto, opcionalmente, como el link de failover. Asigne una dirección IP activa y standby al link de stateful failover. **Nota:** Si el link de stateful failover utiliza el link de failover o la interfaz de datos, 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
```

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

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                    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 y la dirección MAC del link de stateful failover no cambian en el failover a menos que utilicen una interfaz de datos. 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 de stateful failover utiliza el link de failover o la interfaz de datos, omita este paso. Usted ha habilitado ya la interfaz.

```
hostname(config)#interface phy_if
```

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

Nota: Por ejemplo, en este escenario, Ethernet2 se utiliza para el link de stateful failover:

```
hostname(config)#interface ethernet2
```

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

6. Habilite el failover.

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

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.

7. Guarde la configuración del sistema en la memoria Flash.

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

Configuración de la Unidad Secundaria

La única configuración requerida en la unidad secundaria es para la interfaz de failover. La unidad secundaria requiere estos comandos de comunicarse inicialmente con la unidad primaria. Después de que la unidad primaria envía su configuración a la unidad secundaria, la única diferencia permanente entre las dos configuraciones es el comando **failover lan unit**, que identifica cada unidad como primaria o secundaria.

Para el modo multiple context, todos los pasos se realizan en el espacio de la ejecución del sistema a menos que se indique lo contrario.

Para configurar la unidad secundaria, complete estos pasos:

1. Habilite el failover basado en LAN (plataforma de dispositivos de seguridad PIX solamente).

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

2. Defina la interfaz de failover. Utilice las mismas configuraciones 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
```

En esta documentación, Ethernet0 se utiliza para una interfaz de conmutación por fallas LAN.

```
hostname(config)#failover lan interface failover Ethernet3
```

El argumento *if_name* asigna un nombre a la interfaz especificada por el argumento *phy_if*. Asigne la dirección IP activa y standby al link de failover.

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

En esta documentación, para configurar el link de failover, 10.1.0.1 se utiliza para active, 10.1.0.2 para la unidad standby, y "failover" es un nombre de interfaz de Ethernet0.

```
hostname(config)#failover interface ip failover 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 en la unidad primaria. Habilite la interfaz.

```
hostname(config)#interface phy_if
```

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

Por ejemplo, en este escenario, Ethernet0 se utiliza para la conmutación por fallas.

```
hostname(config)#interface ethernet3
```

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

3. Designe esta unidad como la unidad secundaria (opcional).

```
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 hayan configurado previamente.

4. Habilite el failover.

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

Nota: Después de habilitar 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.

5. Después de que la configuración en ejecución ha completado la réplica, guarde la configuración en la memoria Flash.

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

Configuraciones

En este documento, se utilizan estas configuraciones:

```
ASA principal  
ASA#show running-config  
ASA Version 7.2(3)  
!  
!--- To set the firewall mode to transparent mode, !---  
use the firewall transparent command !--- in global  
configuration mode.  
  
firewall transparent  
hostname ASA  
domain-name default.domain.invalid  
enable password 2KFQnbNIdI.2KYOU encrypted  
names  
!  
interface Ethernet0  
  nameif failover  
  
  description LAN Failover Interface
```

```
!  
interface Ethernet1  
  nameif inside  
  security-level 100  
!  
interface Ethernet2  
  nameif outside  
  security-level 0  
  
!--- Configure no shutdown in the stateful failover  
interface !--- of both Primary and secondary ASA.  
  
interface Ethernet3  
  nameif state  
  description STATE Failover Interface  
!  
interface Ethernet4  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface Ethernet5  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
passwd 2KFQnbNIdI.2KYOU encrypted  
ftp mode passive  
dns server-group DefaultDNS  
  domain-name default.domain.invalid  
access-list 100 extended permit ip any any  
pager lines 24  
mtu outside 1500  
mtu inside 1500  
  
!--- Assign the IP address to the Primary and !---  
Secondary ASA Security Appliance. ip address 172.16.1.1  
255.255.255.0 standby 172.16.1.2  
  
failover  
failover lan unit primary  
failover lan interface failover Ethernet0  
failover lan enable  
failover key *****  
failover link state Ethernet3  
failover interface ip failover 10.1.0.1 255.255.255.0  
standby 10.1.0.2  
failover interface ip state 10.0.0.1 255.0.0.0 standby  
10.0.0.2  
  
asdm image flash:/asdm-522.bin  
no asdm history enable  
arp timeout 14400  
access-group 100 in interface outside  
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1  
timeout xlate 3:00:00  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00  
icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp  
0:05:00 mgcp-pat 0:05:00  
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00  
sip-disconnect 0:02:00
```

```

timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end

```

ASA secundario

```

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

```

[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**.

ASA principal

ASA#**show failover**

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

Stateful Failover Logical Update Statistics

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

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	1	7012
Xmit Q:	0	1	185

ASA secundario

ASA(config)#**show failover**

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

Interface inside (172.16.1.1): Normal
Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics

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

Logical Update Queue Information

```
                Cur      Max      Total
Recv Q:          0       1       7043
Xmit Q:          0       1       183
```

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

ASA principal

ASA#**show failover state**

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

====Configuration State====

Sync Done

====Communication State====

Mac set

Unidad secundaria

ASA#**show failover state**

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

====Configuration State====

Sync Done - STANDBY

====Communication State====

Mac set

Para verificar las direcciones IP de la unidad de failover, utilice el comando **show failover interface**.

Unidad primaria

ASA#**show failover interface**

```
interface failover Ethernet0
  System IP Address: 10.1.0.1 255.255.255.0
  My IP Address      : 10.1.0.1
```

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

Unidad secundaria

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

[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**.

ASA principal

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

ASA secundario

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

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 la interfaz permanece en un estado de *espera*. Consulte la sección [show failover de Referencia de Comandos de Dispositivos de Seguridad de Cisco, Versión 7.2](#) para obtener más información sobre los diversos estados de failover.

[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](#)

Complete estos pasos para probar la funcionalidad de failover:

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 Active/Standby Failover, ingrese este comando en la unidad activa:
`hostname(config)#no failover active`
3. Utilice FTP para enviar otro archivo entre los dos mismos hosts.
4. Si la prueba no fue exitosa, ingrese el **comando show failover** para verificar el estado de failover.
5. Cuando finalice, puede restaurar el grupo de failover o la unidad al estado activo con este comando: Para Active/Standby Failover, ingrese este comando en la unidad activa:
`hostname(config)#failover active`

[Failover Forzado](#)

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

Ingrese este comando en la unidad standby:

```
hostname#failover active
```

Ingrese este comando en la unidad activa:

```
hostname#no 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 pase a activa (incluso con failover inhabilitado), vea la sección [Cómo Forzar un 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 una unidad defectuosa a un estado no defectuosa, ingrese este comando:

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

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.

[Troubleshoot](#)

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

- [Monitoreo de Failover](#)
- [Falla en la Unidad](#)
- [%ASA-3-210005: El LU afecta un aparato la conexión fallada](#)
- [Mensajes del sistema de fallas](#)
- [Mensajes del debug](#)
- [SNMP \(Protocolo de administración de red simple\)](#)
- [Problemas conocidos](#)

[Monitoreo de Failover](#)

Este ejemplo demuestra qué sucede cuando el failover no ha comenzado a monitorear las interfaces de red. La conmutación por fallas no comienza a monitorear las interfaces de red hasta que escucha el segundo paquete `hello` de la otra unidad en esa interfaz. Esto tarda cerca de 30 segundos. Si la unidad está conectada a un switch de red que ejecuta el protocolo de árbol de extensión (STP), esto toma el doble del tiempo de `demora de reenvío` configurado en el switch, que normalmente se configura como 15 segundos, más este retardo de 30 segundos. Esto se debe a que en el arranque de ASA e inmediatamente después de un evento de failover, el switch de red detecta un loop de puente temporal. Cuando se detecta este loop, se detiene para reenviar paquetes en estas interfaces durante el tiempo de `demora de reenvío`. Luego ingresa en el modo `escucha` para un tiempo de `demora de reenvío` adicional, dentro del cual el switch escucha los loops de puente pero no reenvía el tráfico o reenvía los paquetes de `saludo` de conmutación por fallas. Después de transcurrido dos veces el tiempo de `demora de reenvío` (30 segundos), el flujo de tráfico se reanuda. Cada ASA permanece en un modo de `espera` hasta que escucha 30 segundos de `paquetes hello` de la otra unidad. En el momento en que ASA pasa el tráfico, no falla la otra unidad basándose en no escuchar los paquetes `hello`. El resto del monitoreo de failover aún ocurre, es decir, la alimentación, la pérdida de link de la interfaz y el `saludo` del cable de failover.

Para el failover, Cisco recomienda encarecidamente que los clientes habiliten portfast en todos los puertos de switch que se conectan a las interfaces ASA. Además, la canalización y el trunking se deben inhabilitar en estos puertos. Si la interfaz del ASA se cae dentro del failover, el switch no tiene que esperar 30 segundos mientras el puerto pasa de un estado de escucha a aprendizaje a reenvío.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

En resumen, verifique estos pasos para reducir los problemas de failover:

- Verifique los cables de red conectados con la interfaz en estado de espera o fallido y, si es posible, reemplácelos.
- Si hay un switch conectado entre las dos unidades, verifique que las redes conectadas con la interfaz en estado de espera o fallido funcionen correctamente.
- Verifique el puerto del switch conectado con la interfaz en estado de espera/fallido y, si es posible, utilice el otro puerto FE en el switch.
- Verifique si tiene portfast habilitado, el trunking y la canalización inhabilitados en los puertos del switch que están conectados con la interfaz.

[Falla en la Unidad](#)

En este ejemplo, la conmutación por fallas ha detectado una falla. Observe que la Interfaz 1 en la unidad primaria es el origen de la falla. Las unidades están nuevamente en modo de espera debido a la falla. La unidad defectuosa se ha quitado de la red (las interfaces están inactivas) y ya no envía paquetes `hello` en la red. La unidad activa permanece en un estado de espera hasta que se reemplace la unidad fallida y las comunicaciones de conmutación por fallas vuelvan a iniciarse.

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

[El LU afecta un aparato la conexión fallada](#)

Un problema de memoria pudo existir si usted recibe este mensaje de error:

El LU afecta un aparato la conexión fallada

Este problema se documenta con el ID de bug de Cisco [CSCte80027](#) (sólo clientes registrados) . Para resolver este problema, actualice su firewall a una versión de software en la que se corrija este error. Algunas de las versiones de software ASA bajo las cuales se corrigió este bug son 8.2(4), 8.3(2), 8.4(2).

[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.

[Mensajes del debug](#)

Para ver los mensajes del debug, ingrese el comando del **fover del debug**. Consulte la [Referencia de Comandos de Dispositivos de Seguridad de Cisco 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 **snmp servidor y a los comandos logging en la [Referencia de Comandos de Dispositivos de Seguridad de Cisco para obtener más información.](#)**

[Tiempo de sondeo de fallas](#)

Para especificar la encuesta y el tiempo en espera de la unidad de failover, utilice el comando del **tiempo de sondeo de fallas en el modo global configuration.**

La `unidad de tiempo de sondeo de fallas msec [time]` sondea los mensajes hello para representar el intervalo de tiempo para verificar la existencia de la unidad standby.

Semejantemente, el `[time]` milisegundo de la unidad del holdtime de failover representa la configuración al período de tiempo durante el cual una unidad debe recibir un mensaje Hello Messages en el link de failover, después de lo cual la unidad del par se declara fallada.

Para especificar la encuesta y el tiempo en espera de la interfaz de datos en una configuración de failover activo/espera, utilice el **comando interface del tiempo de sondeo de fallas en el modo global configuration.** Para restablecer la encuesta y el tiempo en espera predeterminados, no utilizar la **ninguna forma de este comando.**

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

Utilice el comando **interface del tiempo de sondeo de fallas** para cambiar la frecuencia en la que los paquetes de saludo se envían en las Interfaces de datos. Este comando está disponible para el failover activo/espera solamente. Para el failover activo/activo, utilice el comando **interface del polltime** en el modo de la configuración de grupo de failover en vez del comando **interface del tiempo de sondeo de fallas**.

Usted no puede ingresar un *valor de retención de tiempo que sea menos de 5 veces el tiempo de la encuesta de la interfaz*. Con un rato más rápido de la encuesta, el dispositivo de seguridad puede detectar el failover del incidente y del disparador más rápidamente. Sin embargo, una detección más rápida puede causar los intercambios innecesarios cuando la red se congestiona temporalmente. La prueba de la interfaz comienza cuando un paquete de saludo no se oye en la interfaz para la mitad excesiva del tiempo en espera.

Usted puede incluir la unidad del tiempo de sondeo de fallas y los comandos **interface del tiempo de sondeo de fallas** en la configuración.

Este ejemplo fija la frecuencia del tiempo de la encuesta de la interfaz a 500 milisegundos y al tiempo en espera a 5 segundos:

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

Consulte la sección del [tiempo de sondeo de fallas de la Referencia de Comandos de Dispositivos de Seguridad de Cisco, versión 7.2](#) para obtener más información.

[Certificado de exportación/clave privada en configuración de falla](#)

El dispositivo primario replica automáticamente la clave privada/el certificado a la unidad secundaria. Ejecute el comando **write memory** en la unidad activa para replicar la configuración, que incluye el certificado/clave privada, a la unidad standby. Todos las claves/certificados en la unidad standby son borrados y repoblados por la configuración de la unidad activa.

Nota: No debe importar manualmente los certificados, claves y puntos de confianza del dispositivo activo y luego exportar al dispositivo en espera.

[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.

[Problema: La conmutación por fallas siempre es inestable después de configurar la conmutación por fallas multimodo Activo/En espera transparente](#)

La conmutación por fallas se mantiene cuando las interfaces internas de ambos ASA están

conectadas directamente y las interfaces externas de ambos ASA están conectadas directamente. Pero la conmutación por fallas está inestable cuando se utiliza un switch en el medio.

Solución: Inhabilite la BPDU en las interfaces ASA para resolver este problema.

Failover de los módulos ASA

Si el módulo avanzado de los servicios de seguridad del examen y de la prevención (AIP-SSM) o el módulo contenido de los servicios de seguridad de la seguridad y del control (CSC-SSM) se utilizan en las unidades activas y en espera, después actúa independientemente del ASA en términos de failover. **Los módulos se deben configurar manualmente en unidades activas y en espera, el failover no replica la configuración del módulo.**

En términos de failover, las unidades ASA que tienen módulos AIP-SSM o CSC-SSM deben estar del mismo tipo de hardware. Por ejemplo, si la unidad primaria tiene el módulo ASA-SSM-10, la unidad secundaria debe tener el módulo ASA-SSM-10.

Alloc del bloque del mensaje de falla fallado

Mensaje de error %PIX|ASA-3-105010: Alloc (primario) del bloque del mensaje de falla fallado

Explicación: La memoria del bloque fue agotada. Esto es un mensaje transitorio, y el dispositivo de seguridad debe recuperarse. *Primario puede también ser enumerado como secundario para la unidad secundaria.*

Acción Recomendada: Utilice el comando `show blocks` para monitorear la memoria del bloque actual.

Problema del Failover del módulo AIP

Si usted tiene dos ASA en una configuración de failover y cada uno tiene un AIP-SSM, usted debe replicar manualmente la configuración del AIP-SS. Solamente la configuración del ASA es replegada por el mecanismo de failover. El AIP-SSM no se incluye en el failover.

Primero, el AIP-SSM actúa independientemente del ASA en términos de failover. Para el failover, todo que es necesario de una perspectiva ASA es que los módulos AIP estén del mismo tipo de hardware. Más allá de eso, como con cualquier otra porción de failover, la configuración del ASA entre el activo y standby debe estar adentro sincroniza.

En cuanto a la configuración de los AIP, son con eficacia sensores independientes. No hay failover entre los dos, y no tienen ninguna conciencia de uno a. Pueden funcionar con las versiones del código independientes. Es decir, no tienen que corresponder con, y el ASA no cuida sobre la versión del código en el AIP en cuanto al failover.

El ASDM inicia una conexión al AIP con el IP de la interfaz de administración que usted configuró en el AIP. En otras palabras, se conecta al sensor normalmente a través de HTTPS, que depende de cómo se configura el sensor.

Usted podría tener un failover de la independiente ASA de los módulos IP (AIP). Todavía está conectado al mismo porque se conecta a su IP de administración. Para conectar con el otro AIP,

usted debe volver a conectar a su IP del manangement para configurarlo y para accederlo.

Consulte [ASA: Ejemplo de Configuración de Enviar Tráfico de Red desde el ASA al AIP SSM](#) para obtener más información y configuraciones de muestra sobre cómo enviar el tráfico de red que pasa a través del Cisco ASA 5500 Series Adaptive Security Appliance (ASA) al Advanced Inspection and Prevention Security Services Module (AIP-SSM) (IPS)

Problemas conocidos

Cuando intenta acceder al ASDM en el ASA secundario con la versión 8.x del software y la versión 6.x del ASDM para la configuración de failover, se recibe este error:

Error: El nombre en el Security Certificate es inválido o no corresponde con el nombre del sitio

En el certificado, el emisor y el nombre del sujeto es la dirección IP de la unidad *activa*, no la dirección IP de la *unidad standby*.

En la Versión de ASA 8.x, el certificado interno (del ASDM) se replica de la unidad activa a la unidad standby, que causa el mensaje de error. Pero, si el mismo firewall se ejecuta en el código de la versión 7.x con ASDM 5.x e intenta acceder a ASDM, recibe esta advertencia de seguridad regular:

El Security Certificate tiene un nombre válido el corresponder con del nombre de la paginación que usted está intentando ver

Cuando usted marca el certificado, el emisor y los asuntos es la dirección IP de la unidad standby.

Información Relacionada

- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Cisco PIX Firewall Software](#)
- [Configuración de falla del módulo de servicios del firewall \(FWSM\)](#)
- [Troubleshooting del Failover FWSM](#)
- [Cómo el Failover trabaja en el Cisco Secure PIX Firewall](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)