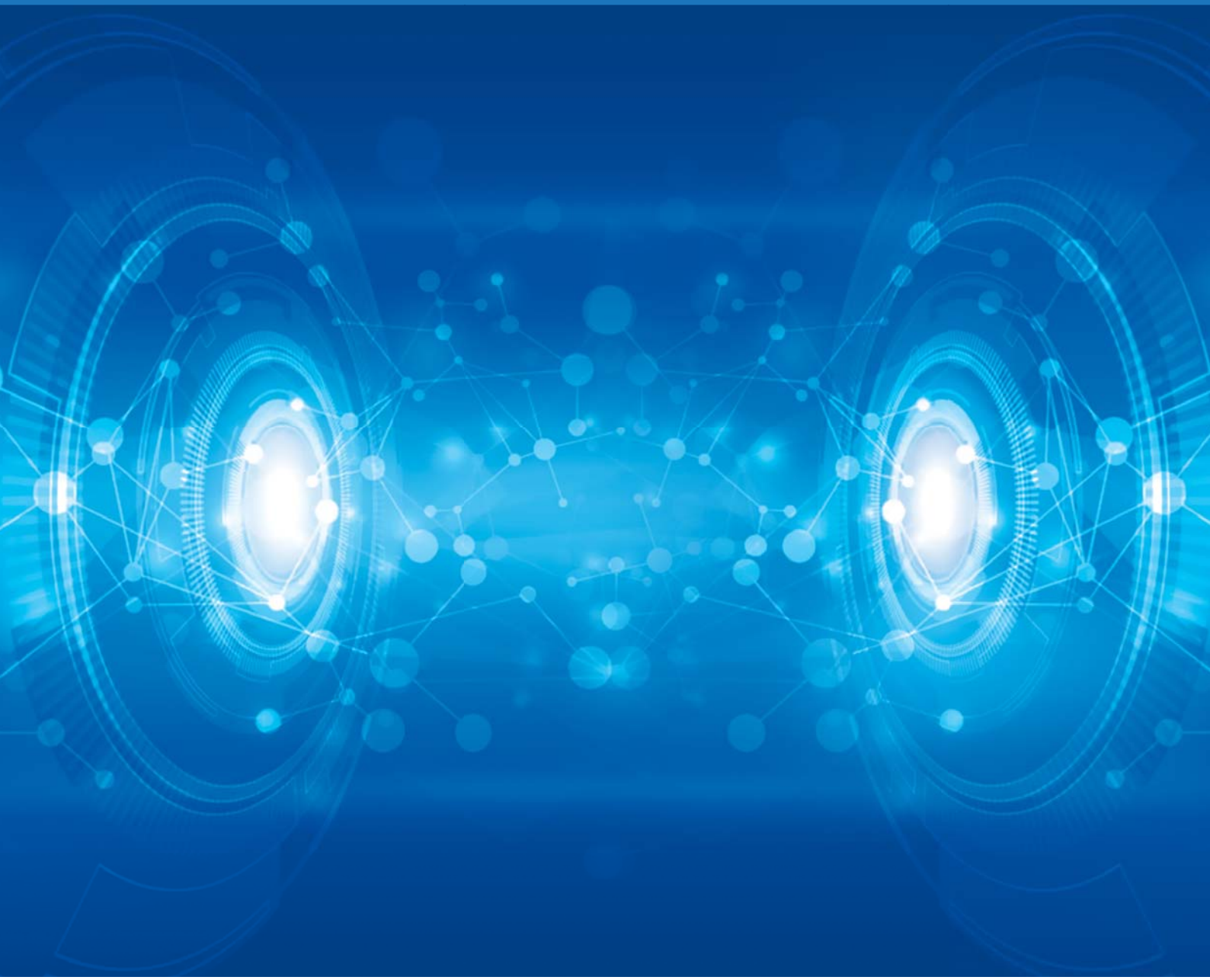
Hillstone™
NETWORKS

Hillstone Twin-Mode Solución de Firewall para Centros de Datos Redundantes



Introducción

A medida que más empresas confían en disponibilidad 24/7/365 para sus aplicaciones, el diseño de los centros de datos redundantes con conmutación por error se han vuelto cada vez más populares. Hasta hace poco, muchos de los firewall más sofisticados eran incapaces de garantizar la seguridad completa en un entorno de centro de datos redundantes. Los Firewall de Próxima Generación de Hillstone ahora abordan esta cuestión directamente con su característica de Firewall Twin-Mode, que une pares de firewall redundantes en los centros de datos para mantener completa seguridad a todos los flujos de tráfico del centro de datos redundante. Gracias a Hillstone Firewall Twin-Mode, las empresas pueden lograr la continuidad de su negocio y recuperación de desastres 24/7/365 sin brechas en la seguridad del centro de datos.

Centros de Datos Redundantes

Diseño de Centros de Datos redundantes se ha convertido en una misión cada vez más crítica ya que las empresas dependen de sus aplicaciones y de la red para cumplir con las funciones principales del negocio. Sectores de la industria, tales como los servicios financieros, la salud y los proveedores de servicios necesitan que sus aplicaciones esten activas 24/7/365, con el rendimiento y la seguridad funcional, ya que cualquier pérdida de acceso a las aplicaciones o sus datos podría ser muy grave para los ingresos y para la reputación. En el caso de la salud, el tiempo de inactividad puede costar vidas humanas.

El diseño del centro de datos redundante mitiga el impacto de los fallos de hardware, software y de centros de datos para que los sistemas y los negocios puedan seguir operando y generando ingresos 24/7/365. Esto incorpora una serie de tecnologías, incluyendo la virtualización de servidores y el balanceo de la carga de la aplicación. Muchas soluciones de firewall incorporan funciones de clúster que le fallan a los servicios de seguridad pasando a un segundo firewall si el primero no funciona por alguna razón.

Sin embargo, los desastres naturales, los ataques terroristas o los errores humanos pueden derribar las aplicaciones o el centro de datos completo, lo que requiere que las aplicaciones hagan conmutación a un segundo centro de datos geográficamente disperso para poder seguir funcionando.

Con una arquitectura de centros de datos redundantes, el mismo sistema empresarial crítico corre en al menos dos sitios y dos centros de datos al mismo tiempo, con los dos centros de datos en simultánea y funcionando como copias de seguridad uno para el otro. Cuando una aplicación en un centro de datos falla, el segundo o tercer centro de datos se hace cargo de la prestación de servicios a todos los usuarios empresariales sin interrupción. La conmutación de aplicación es instantánea y completamente invisible para el usuario, que simplemente sigue trabajando como de costumbre.

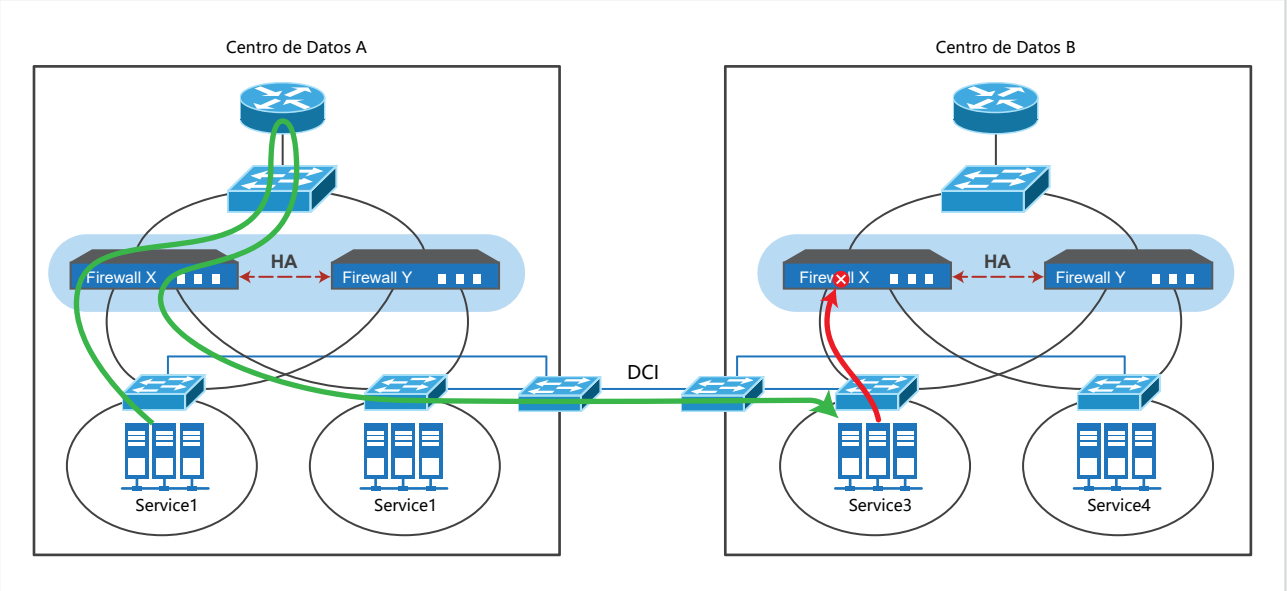
Una configuración de centro de datos redundante es intrínsecamente más eficiente que la operación legado en modo activo/pasivo, en el que los sistemas en un centro de datos esperan sin uso hasta que haya una necesidad de conmutación por error del sistema. La redundancia duplica la capacidad de un solo centro de datos a través de la integración de recursos.

Problemas de Failover del Firewall Stateful

Una arquitectura de centro de datos redundante normalmente aprovecha dispositivos especiales como un Centro de Datos de Interconexión (DCI) para extender la LAN interna a través de sitios de centros de datos para que los servidores virtuales puedan migrar a través de ellos sin esfuerzo para la recuperación de desastres, la continuidad del negocio y la asignación de recursos. La mayoría de los dispositivos de hardware del centro de datos, tales como los routers y los equilibradores de carga soportan la redundancia en conmutación por error del centro de datos con una excepción importante: los firewall de estado. ¿La razón? Los Firewall de estado necesitan analizar el estado de toda la información de la sesión para aplicar la política de seguridad efectivamente. Si una parte de una sesión de firewall de estado intenta cruzar un firewall diferente de otro, el segundo, sin darse cuenta de la sesión establecida en el primero, más probablemente dejaría caer el flujo de datos, matando a la transacción. Esta situación se conoce como flujo de tráfico asimétrico, y puede ocurrir en los siguientes escenarios:

- En una implementación de servicios distribuidos en la que unas pocas aplicaciones o los servicios se ejecutan en sólo uno de los dos centros de datos redundantes, en lugar de en ambos al mismo tiempo.
- Un escenario de copia de seguridad en el que un segundo centro de datos se ha hecho cargo de una aplicación de negocio que fracasó en el primer centro de datos.
- Una migración de máquinas virtuales a través de la LAN que se extienden desde un centro de datos a otro.

La figura a continuación ilustra cómo se puede producir este problema en un escenario de centro de datos redundante.



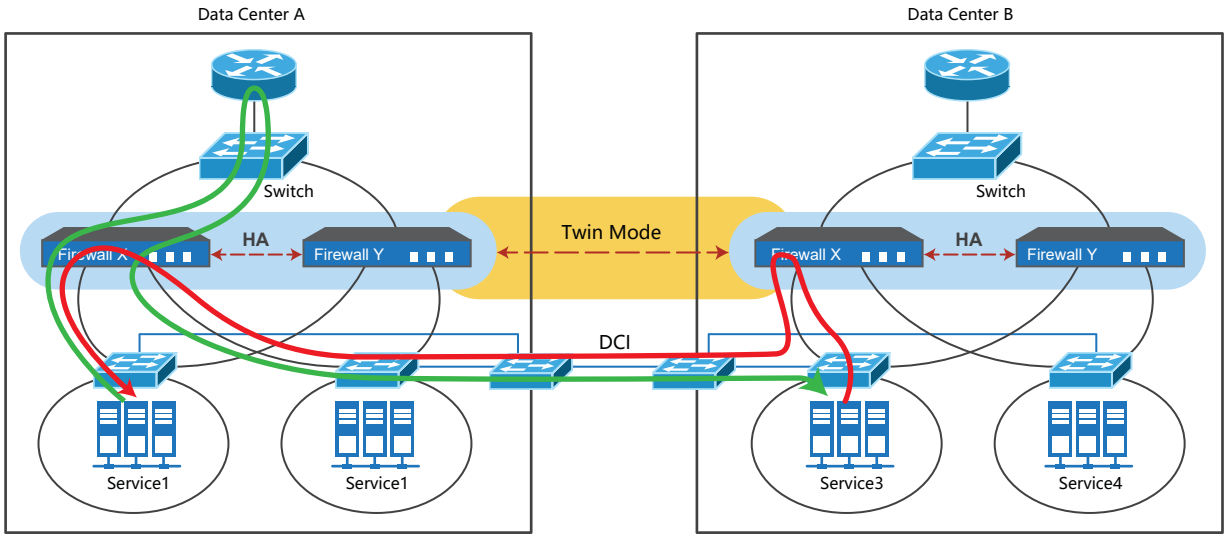
Cada centro de datos ejecuta un par de firewall activos para manejar la seguridad de los datos y servir como una reserva en standby el uno para el otro, en caso de que uno fallara.

- Una transacción envía el tráfico desde los servidores en el Service 1 de los centros de datos A (a la izquierda) al Service 3 de los servidores del centro de datos B (derecha).
- La política de Informática requiere que todo el tráfico del Centro de Datos A atraviese los firewall del Centro de Datos A (véase la línea verde). Los firewall del Centro de Datos A establecen una sesión de inspección del estado.
- El tráfico viaja a través de dispositivos de extensión DCI LAN al Centro de Datos B.
- Cuando los datos solicitados son devueltos por los servidores del Centro de Datos B, la política de Informática exige que atraviese el firewall del Centro de Datos B.
- Desafortunadamente los firewall del Centro de Datos B no son conscientes de la sesión establecida en los firewall del Centro de Datos A. Por defecto omiten los datos de retorno, matando la transacción (véase la línea roja). La información solicitada nunca retorna al usuario.

Hillstone Firewall de Doble Modo y de Alta Disponibilidad

El Firewall de Seguridad Twin-Mode de Hillstone resuelve el problema del flujo asimétrico mediante la sincronización de ambos firewall en los centros de datos redundantes a través de enlaces de control de datos dedicados, esencialmente creando un único firewall lógico.

La figura a continuación ilustra cómo el Firewall Twin-Mode funcionaría en el mismo escenario redundante centro de datos descritos anteriormente:



- Una transacción envía el tráfico desde los servidores en los centros de datos A (a la izquierda) a los servidores en un centro de datos B (derecha).
- La política de Informática requiere que todo el tráfico del Centro de Datos A atraviese los firewall del Centro de Datos A (véase la línea verde).
- Al instante, el Twin-Mode Link sincroniza la información de configuración de la sesión del firewall del Centro de Datos A con la información del estado del firewall del Centro de Datos B (línea roja punteada denominada Twin-Mode).
- El flujo de retorno golpea contra los firewall del Centro de Datos B, el cual, gracias a Twin-Mode, son conscientes de la sesión establecida en los firewall del Centro de Datos A. Devuelven el flujo de retorno a los firewall del Centro de Datos A.
- El flujo de retorno pasa a través del firewall del Centro de Datos A con éxito y completa la transacción (línea roja), que proporciona acceso a la información solicitada.

La Continuidad Empresarial Alcanzada con Seguridad

El Firewall Twin-Mode de Hillstone ofrece varios importantes beneficios empresariales. Gracias a Twin-Mode, las empresas pueden:

- Sincronizar automáticamente la configuración del firewall y la información de la sesión entre los dos firewall en los centros de datos redundantes. La conmutación por error de estado en el firewall puede ocurrir en un segundo centro de datos para asegurar la continuidad del negocio en las condiciones más difíciles.
- Proporcionar seguridad al flujo asimétrico en centros de datos.
- Lograr no sólo la seguridad, sino visibilidad total de todo el tráfico en los centros datos a través de los enlaces de DCI, gracias a la interfaz de la plataforma de gestión de seguridad de Hilllstone. Anteriormente, el tráfico DCI era a menudo invisible para los administradores de los centros de datos.
- Lograr tanto plena seguridad como la continuidad del negocio 24/7/365 a través de una gran variedad de arquitecturas de centros de datos de alta disponibilidad.

Los Firewall de Próxima Generación de Hillstone ofrecen Twin-Mode para permitir el diseño de centros de datos redundantes que puedan lograr la disponibilidad 24/7/365 sin comprometer la seguridad.

Hillstone NETWORKS

Cómo contactar a Hillstone Networks

America: +1-408-508-6750 | SEA: +65-6678-7660

Europa: +420-721-125-070 | MEA: +971-4557-1493

Email: inquiry@Hillstonenet.com