Comprender los pasos y el impacto del procedimiento de actualización de alta disponibilidad de FTD

Contenido

Problema

Un administrador de firewall debe comprender el procedimiento de actualización recomendado para los dispositivos Firewall Threat Defence (FTD) configurados en un par de alta disponibilidad (HA) y gestionados por Cisco Firewall Management Center (FMC). Las preguntas específicas incluyen cuál es el proceso recomendado para las actualizaciones de software en estas unidades, si las actualizaciones se pueden realizar "sobre la marcha" sin tiempo de inactividad y qué impacto se puede esperar durante el proceso de actualización.

Entorno

- FTD que ejecuta la versión 7.4. Otras versiones de software también pueden verse afectadas.
- FTD configurado en modo de par de alta disponibilidad (HA).
- FMC 7.4 gestión del FTD HA. Otras versiones de software también pueden verse afectadas.

Resolución

El procedimiento de actualización del FTD en la configuración de HA utiliza una secuencia específica para minimizar el tiempo de inactividad y mantener la integridad del sistema.

Pedido de actualización recomendado

Paso 1. Actualice primero el CSP

La guía de Cisco requiere que el FMC ejecute la misma versión o una versión más reciente que los dispositivos que gestiona. No se puede actualizar un dispositivo FTD pasado el FMC a una versión de mantenimiento o principal más reciente.

Paso 2. Actualización del par FTD HA desde FMC

Al actualizar un par FTD HA gestionado por FMC, FMC actualiza un par a la vez (en espera primero y después activo) y se produce una recuperación tras fallo como parte del proceso.

Expectativas de impacto del tráfico y tiempo de inactividad

- Debe planificar una ventana de mantenimiento. Las actualizaciones de las notas de Cisco pueden incluir interrupciones en el flujo y la inspección del tráfico, y los dispositivos pueden dejar de pasar tráfico durante la actualización o si ésta falla.
- Con un par HA, el objetivo es minimizar el impacto, pero debe esperar al menos un evento de failover y una posible interrupción breve (por ejemplo, adyacencia de routing o renegociación de VPN en función de su entorno).
- Evite los cambios de configuración y políticas durante la actualización (no habrá implementaciones ni cambios hasta que ambos miembros de HA se actualicen por completo y sean estables).

Comprobaciones de estado previas a la actualización para FTD HA

Antes de iniciar la actualización, confirme que FTD HA es estable y que ambas unidades coinciden en los estados Activo y Preparado en espera:

<#root>

```
device#
```

```
show failover state


               State          Last Failure Reason      Date/Time
This host  -   Primary


Active


None
Other host -   Secondary


Standby Ready


  Comm Failure             16:10:34 UTC Apr 13 2026

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

Causa

Se trata de una investigación de procedimiento sobre las mejores prácticas para actualizar los sistemas FMC y FTD en la configuración de HA. La pregunta se refiere a la necesidad de comprender la secuencia de actualización adecuada, las expectativas de tiempo de inactividad y las estrategias de mitigación de impacto para las infraestructuras de firewall críticas.

Contenido relacionado

- Planificación de actualizaciones de Secure Firewall Management Center
- Actualización de FTD HA gestionado por FMC
- Guía de compatibilidad de Management Center
- Guía de compatibilidad de Threat Defence
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).