Solucionar problemas de caídas de paquetes FTD (tcp-not-syn) cuando "se ha mejorado la detección de aplicaciones y URL" Está habilitado en interfaces en línea con flujo de tráfico asimétrico

Contenido

Problema

Los appliances de defensa frente a amenazas de firewall (FTD) configurados con conjuntos de interfaces en línea descartan el tráfico de retorno de TCP con el motivo de descarte de ruta de seguridad acelerada (ASP) tcp-not-syn. Esto ocurre inmediatamente después de que la función de detección de identidad del servidor TLS (TSID), específicamente la opción "Aplicación mejorada y detección de URL" esté habilitada. En las versiones anteriores de Firewall Management Center (FMC), la opción se denomina "Detección temprana de aplicaciones y categorización de URL". El mismo dispositivo FTD que reenvió el SYN original descarta los paquetes SYN-ACK TCP en el trayecto de retorno, lo que impide que se establezcan sesiones TCP.

El problema se manifiesta como fallas de conectividad TCP generalizadas y no se limita al tráfico TLS. Estos síntomas se observan cuando la función está habilitada:

- Los paquetes TCP SYN-ACK en la trayectoria de retorno se descartan con la razón de descarte ASP tcp-not-syn.
- Las nuevas sesiones TCP no aparecen en la tabla de conexiones FTD.
- Los contadores de caídas de ASP altas se acumulan rápidamente, como lo ilustra este resultado capturado aproximadamente 10 minutos después de que se habilitó la función:

<#root>

```
device#
```

show asp drop

```
Frame drop:
 Flow is denied by configured rule (acl-drop)                                1

 First TCP packet not SYN (tcp-not-syn)                                  34802

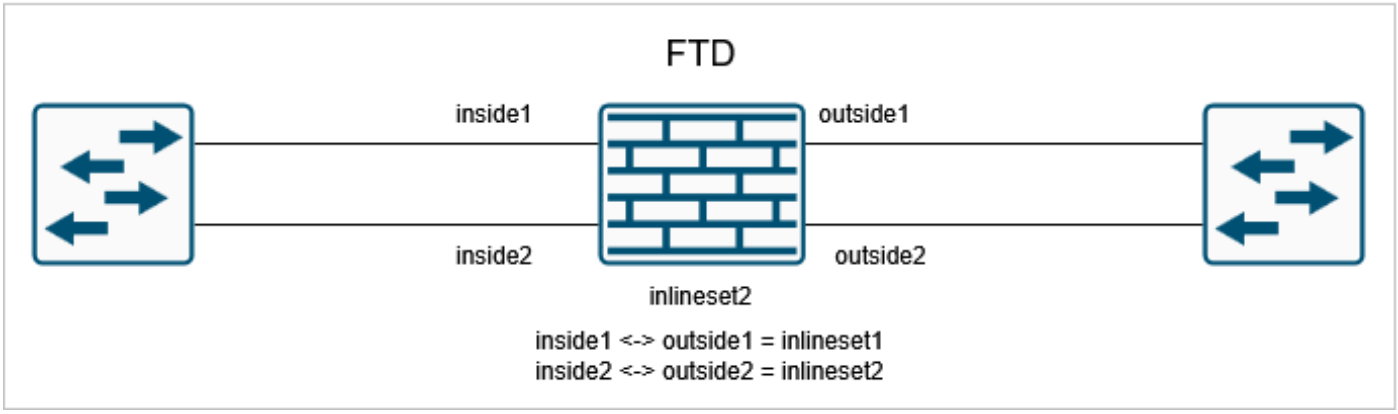

 TCP RST/FIN out of order (tcp-rstfin-ooo)                                   4
 Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                             995
 Dropped pending packets in a closed socket (np-socket-closed)               3
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)               1
 TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)               1
 Blocked or blacklisted by the reputation preprocessor (reputation)          1

Last clearing: 16:50:21 CEST Oct 24 2026 by enable_1
```

Entorno

- Plataforma: Cisco Firepower 4115. Otras plataformas también pueden verse afectadas.
- Versión del software FTD: 7.6.4. Otras versiones de software también pueden verse afectadas.
- Versión del software FMC: 10.1.0. Otras versiones de software también pueden verse afectadas.
- FTD con conjuntos de interfaces en línea.
- FTD tiene al menos dos pares de interfaz en línea: inlineset1 y inlineset2 (o hay dos FTD diferentes con un conjunto en línea cada uno).
- Flujo de tráfico asimétrico presente en el entorno: TCP SYN egresa a través de la interfaz outside1 mientras que el TCP SYN-ACK correspondiente regresa a través de la interfaz outside2 en el mismo dispositivo FTD.
- La función TSID está activada en FTD.

Topología



Resolución

La resolución recomendada para detener las caídas tcp-not-syn y restaurar la conectividad TCP a través de las interfaces FTD en línea es inhabilitar la opción "Aplicación mejorada y detección de URL" dentro del TSID. Esto permite que el desvío de estado TCP permanezca activo en los conjuntos de interfaz en línea, lo cual es necesario para acomodar los flujos de tráfico asimétrico en el entorno.

Desactivar "Detección mejorada de aplicaciones y URL" en FMC

Navegue hasta: Políticas > Control de acceso > [Su política de control de acceso] > Avanzado > Detección de identidad de servidor TLS. Desmarque o desactive la casilla de verificación "Aplicación mejorada y detección de URL" y, a continuación, implemente la política en los dispositivos FTD afectados.

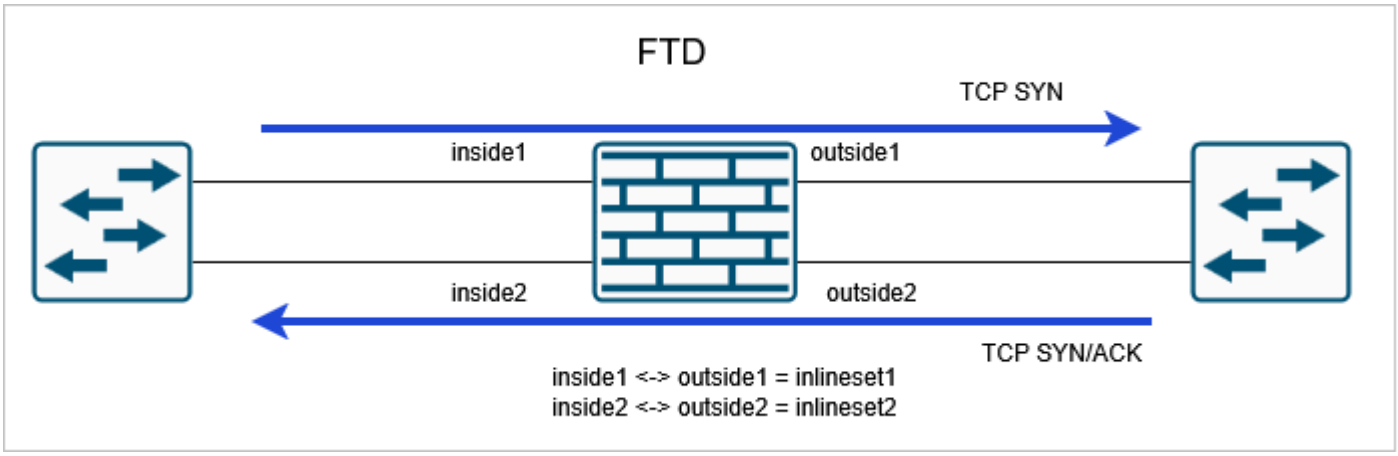
Después de desactivar la función, aparecen nuevas sesiones en la tabla de conexiones, lo que confirma que las conexiones TCP están completando correctamente el protocolo de enlace de tres vías.

Nota: Con TSID inhabilitado, el FTD ya no puede ver el certificado del servidor en las sesiones de TLS 1.3. Las reglas de aplicaciones y URL hacen coincidir el tráfico de forma menos precisa en el tráfico cifrado.

Causa

La causa raíz de las caídas tcp-not-syn es una incompatibilidad entre la función TLS Server Identity Discovery y los conjuntos de interfaz en línea de TCP State Bypass en FTD.

De forma predeterminada, para el tráfico que pasa a través de interfaces en línea en FTD, se habilita el desvío de estado TCP. El desvío de estado TCP está diseñado para permitir que el tráfico asimétrico, donde las trayectorias de reenvío y retorno de una conexión TCP pueden atravesar diferentes interfaces o incluso diferentes dispositivos, pase sin que el FTD exija un seguimiento estricto del estado TCP. Este es un comportamiento necesario en entornos donde la asimetría de ruteo está presente:

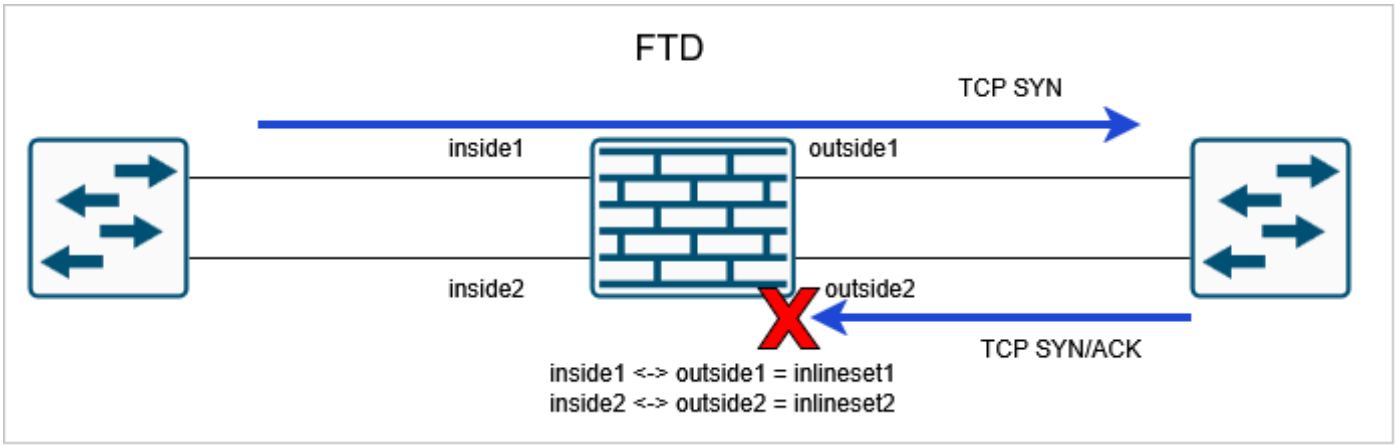


El TCP asimétrico fluye a través de conjuntos de líneas FTD cuando TSID está inhabilitado.

Sin embargo, cuando cualquiera de estas funciones está habilitada, el sistema FTD invalida el desvío de estado TCP y comienza a realizar comprobaciones de estado TCP completas en el tráfico de interfaz en línea:

- La opción "Aplicación mejorada y detección de URL" en Detección de identidad de servidor TLS.
- Cualquier política de descifrado TLS/SSL activa.

Una vez aplicadas las comprobaciones de estado de TCP, el FTD realiza un seguimiento de la secuencia de entrada en contacto de TCP completa. En entornos con ruteo asimétrico —donde, por ejemplo, el paquete SYN TCP sale a través de la interfaz outside1 pero el TCP SYN-ACK correspondiente regresa a través de la interfaz outside en el mismo dispositivo— el FTD no reconoce el SYN-ACK como perteneciente a una sesión TCP conocida y rastreada. Debido a que el SYN-ACK llega a una interfaz diferente de la esperada y no se vio ningún SYN correspondiente en esa interfaz, el FTD lo clasifica como un paquete no SYN para una conexión desconocida y lo descarta con la razón de descarte ASP tcp-not-syn.



Flujo TCP asimétrico a través de conjuntos en línea FTD cuando TSID está habilitado.

Contenido relacionado

- ID de bug de Cisco CSCwp84746 — Documentación: Incompatibilidad de la detección de identidad del servidor TLS con el desvío de estado TCP en interfaces de conjunto en línea
- ID de bug de Cisco CSCwx42897 — DOC: La detección de identidad del servidor TLS invalida el desvío de estado TCP en las interfaces de conjunto en línea, lo que hace que se descarte el tráfico TCP (tcp-not-syn)
- Cisco Bug ID CSCwx42901 — Añada una advertencia al habilitar "Early application detection and URL categorization" (TSID) que indica que inhabilita el desvío de estado TCP en las interfaces en línea
- Documentación de Cisco: directrices para la omisión del estado TCP (incluye la restricción de detección de identidad del servidor TLS)
- Caso práctico: tráfico asimétrico a través de conjuntos en línea
- Nota técnica de Cisco: Cómo generar paquetes de resolución de problemas de FTD y FMC
- 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).