El centro de administración de la potencia de fuego visualiza algunos eventos de la conexión TCP en la dirección incorrecta

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedente](#)
[Solución](#)
[Conclusión](#)
[Información Relacionada](#)

Introducción

Este documento describe las razones y los pasos de la mitigación para la Administración Center(FMC) de la potencia de fuego que visualiza los eventos de la conexión TCP en la dirección inversa donde está la conexión TCP el IP del iniciador IP del servidor y IP del respondedor es la conexión TCP IP del cliente.

> Nota: Hay razones múltiples del acontecimiento de tales eventos. Esto documenta explica la mayoría de la causa común de este síntoma.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tecnología de la potencia de fuego
- Conocimiento básico del dispositivo de seguridad adaptante (ASA)
- Comprensión del mecanismo de la sincronización de Transmission Control Protocol(TCP)

Componentes Utilizados

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

- La defensa de la amenaza de la potencia de fuego ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) esa funciona con la versión de software 6.0.1 y posterior

- La defensa de la amenaza de la potencia de fuego ASA (5512-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X,FP9300,FP4100) esa funciona con la versión de software 6.0.1 y posterior
- El ASA con los módulos de la potencia de fuego (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) esos funciona con las versiones de software 6.0.0 y posterior
- Versión 6.0.0 y posterior del centro de administración de la potencia de fuego (FMC)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos usados en este documento comenzaron con una configuración (predeterminada) clara. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedente

En una conexión TCP, el **cliente** refiere al IP que envía el paquete inicial. El centro de administración de la potencia de fuego genera un evento de conexión cuando el dispositivo administrado (sensor o FTD) considera el paquete TCP inicial de una conexión.

Los dispositivos que siguen el estado de una conexión TCP tienen un **tiempo de inactividad** definido para aseegurarse que las conexiones que no son cerradas erróneamente por los puntos finales no consumen memoria disponible por los períodos prolongados de tiempo. El tiempo de espera ocioso predeterminado para las conexiones TCP establecidas en la potencia de fuego es **tres minutos**. Una conexión TCP que ha permanecido ociosa por tres minutos o más, no es seguida por el sensor IPS de la potencia de fuego.

El paquete subsiguiente después de que el descanso se trate como un nuevo flujo TCP y la decisión de reenvío se toma según la regla que hace juego este paquete. Cuando el paquete es del servidor, el IP del servidor se registra como el iniciador de este nuevo flujo. Cuando la registración se habilita para la regla, un evento de conexión se genera en el centro de administración de la potencia de fuego.

> Nota: Según las directivas configuradas, la decisión de reenvío para el paquete que viene después de que el descanso sea diferente de la decisión para el paquete TCP inicial. Si la acción predeterminada configurada es “bloque”, se cae el paquete.

Un ejemplo de este síntoma está según el tiro de pantalla abajo:

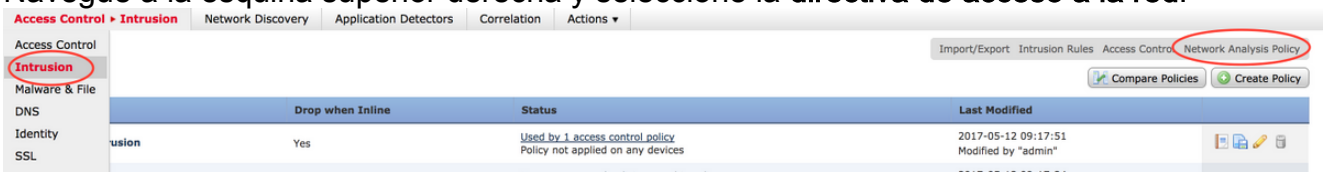
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

Solución

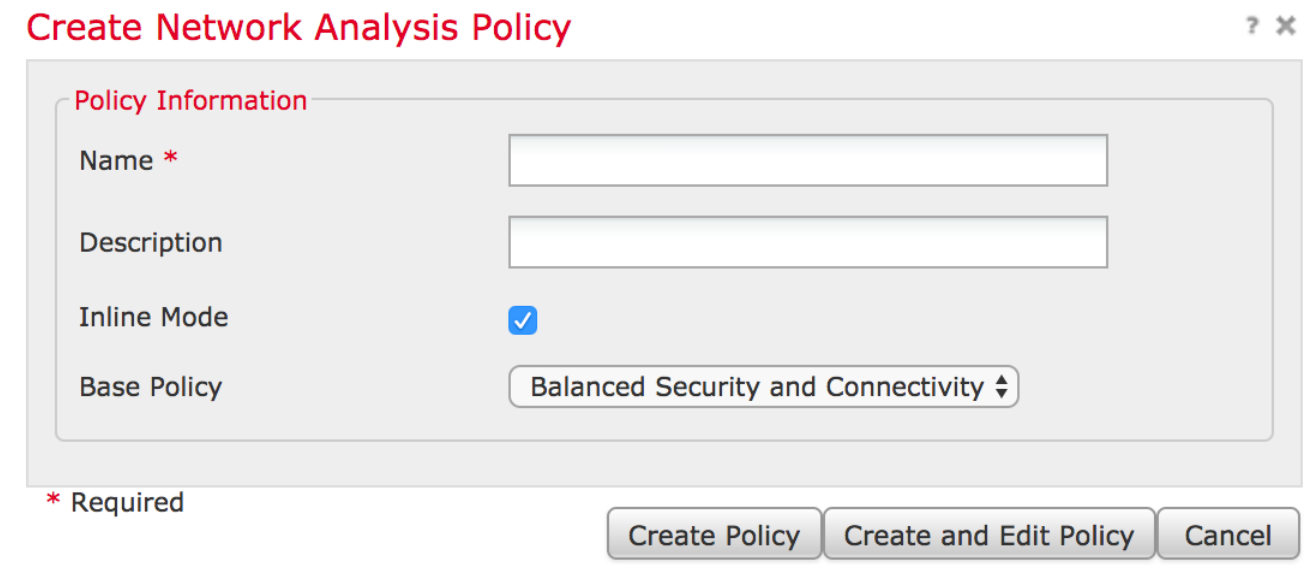
El problema antedicho es atenuado aumentando el **descanso de las** conexiones TCP. En la orden cambie el descanso,

1. Navegue a las **directivas > al control de acceso > a la intrusión**.

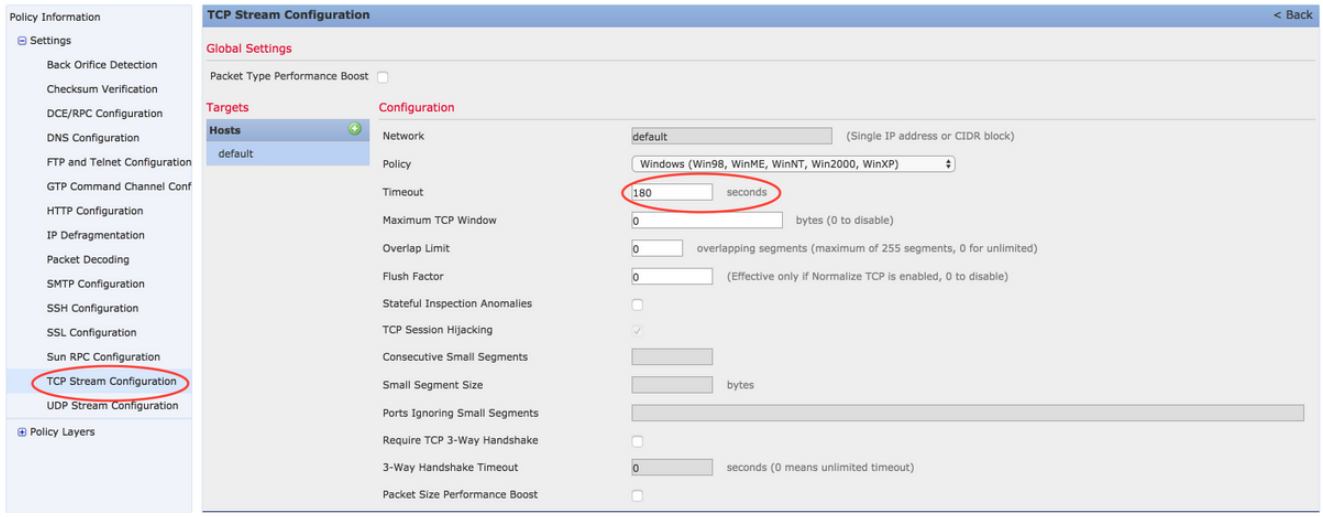
2. Navegue a la esquina superior derecha y seleccione la **directiva de acceso a la red**.



3. Selecto **cree la directiva**, elija un nombre y haga clic en **crean y editan la directiva**. No modifique la **directiva**
baja.

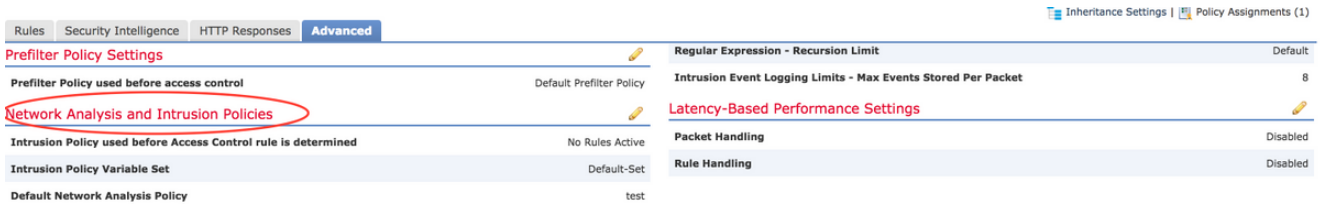


4. Amplíe la **opción Settings** y elija la **configuración de la secuencia TCP**.
5. Navegue a la sección de configuración y cambie el valor del **descanso** según lo deseado.



6. Navegue a las **directivas > al control de acceso > al control de acceso**.
7. Seleccione la opción **editan** para editar el directiva aplicada al dispositivo administrado relevante o para crear una nueva
directiva.

8. Seleccione la **ficha Avanzadas** en la política de acceso.
9. Localice la **Análisis de red y la** sección de las **directivas de la intrusión** y haga clic en **editan el**
icono.



10. Del menú desplegable de la **directiva del análisis de red predeterminada**, elija la directiva creada en el paso 2.
11. El Haga Click en OK y **salva los** cambios.
12. Haga clic en **despliegan la** opción para desplegar limpia a los dispositivos manged relevantes.

Precaución: Se espera que el descanso cada vez mayor cause una utilización de la memoria más alta, potencia de fuego tiene que seguir los flujos que no son cerrados por los puntos finales por un tiempo más largo. El aumento real en la utilización de la memoria es diferente para cada red única pues depende de cuánto tiempo las aplicaciones de red guardan la marcha lenta de las conexiones TCP.

Conclusión

La prueba patrón de cada red para el tiempo de inactividad de las conexiones TCP es diferente. Depende totalmente de las aplicaciones que son funcionando. Un valor óptimo debe ser establecido observando cuánto tiempo las aplicaciones de red guardan la marcha lenta de las conexiones TCP. Para los problemas que pertenecen al módulo de servicio de la potencia de fuego en Cisco ASA, cuando un valor óptimo no puede ser deducido, el descanso se puede ajustar aumentándolo adentro intensifica al valor de agotamiento del tiempo ASA.

Información Relacionada

- Guía de inicio rápido de la defensa de la amenaza de la potencia de fuego de Cisco para el ASA
- Soporte Técnico y Documentación - Cisco Systems
- Guía de inicio rápido de la potencia de fuego ASA