

FirePOWER Management Center muestra algunos eventos de conexión TCP en la dirección equivocada

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)


[Solución](#)

[Conclusión](#)

[Información Relacionada](#)

Introducción

Este documento describe los motivos y los pasos de mitigación para que FirePOWER Management Center (FMC) muestre los eventos de conexión TCP en la dirección inversa, donde IP del iniciador es la IP del servidor de la conexión TCP e IP del respondedor es la IP del cliente de la conexión TCP.

 Nota: Existen múltiples razones para que ocurran tales eventos. Este documento explica la causa más común de este síntoma.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tecnología FirePOWER
- Conocimientos básicos de Adaptive Security Appliance (ASA)
- Comprensión del mecanismo de temporización del Protocolo de control de transmisión (TCP)

Componentes Utilizados

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

- Defensa frente a amenazas ASA Firepower (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que ejecuta la versión de software 6.0.1 y posteriores
- Defensa frente a amenazas ASA Firepower (5512-X, 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, FP9300, FP4100) que ejecuta la versión de software 6.0.1 y posteriores
- ASA con módulos Firepower (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) que ejecuta las versiones de software 6.0.0 y posteriores
- Firepower Management Center (FMC) versión 6.0.0 y posteriores


La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos utilizados en este documento comenzaron con una configuración clara (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Background

En una conexión TCP, client se refiere a la IP que envía el paquete inicial. FirePOWER Management Center genera un evento de conexión cuando el dispositivo administrado (sensor o FTD) ve el paquete TCP inicial de una conexión.

Los dispositivos que realizan un seguimiento del estado de una conexión TCP tienen un tiempo de espera inactivo definido para asegurarse de que las conexiones que erróneamente no están cerradas por los terminales no consumen la memoria disponible durante largos períodos de tiempo. El tiempo de espera por inactividad predeterminado para las conexiones TCP establecidas en FirePOWER es de tres minutos. El sensor IPS FirePOWER no realiza el seguimiento de las conexiones TCP que han permanecido inactivas durante tres minutos o más.

El paquete subsiguiente después del tiempo de espera se trata como un nuevo flujo TCP y la decisión de reenvío se toma según la regla que coincida con este paquete. Cuando el paquete proviene del servidor, la IP del servidor se registra como el iniciador de este nuevo flujo. Cuando el registro está habilitado para la regla, se genera un evento de conexión en FirePOWER Management Center.

 Nota: Según las políticas configuradas, la decisión de reenvío para el paquete que viene después del tiempo de espera es diferente de la decisión para el paquete TCP inicial. Si la acción predeterminada configurada es "Bloquear", el paquete se descarta.

Un ejemplo de este síntoma es como se muestra en la siguiente captura de pantalla:

	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

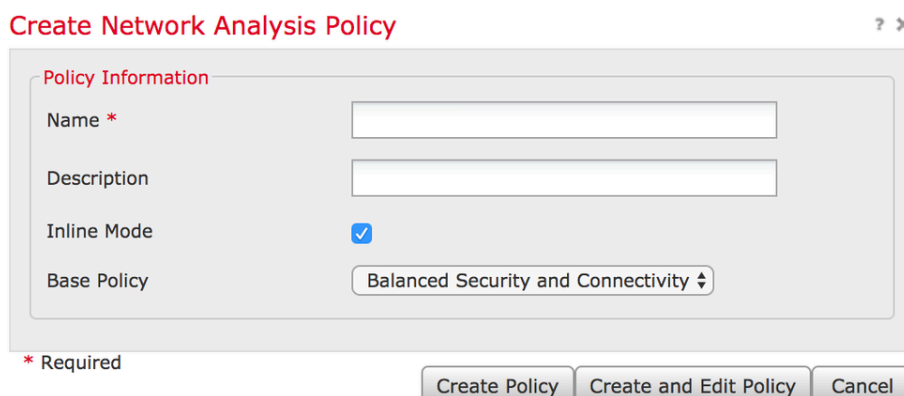
Solución

Este problema se mitiga al aumentar el tiempo de espera de las conexiones TCP. Para cambiar el tiempo de espera,

1. Vaya a Políticas > Control de acceso > Intrusión.
2. Desplácese hasta la esquina superior derecha y seleccione Network Access Policy.



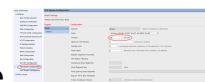
3. Seleccione Create Policy, elija un nombre y haga clic en Create and Edit Policy. No



modifique la política base.

4. Expanda la opción Settings y elija TCP Stream Configuration.

5. Vaya a la sección de configuración y cambie el valor de Timeout según desee.



6. Vaya a Políticas > Control de acceso > Control de acceso.

7. Seleccione la opción Edit para editar la política aplicada al dispositivo administrado

relevante o crear una nueva política.



8. Seleccione la pestaña Advanced en la política de acceso.

9. Localice la sección Análisis de red y Políticas de intrusión y haga clic en el icono Editar.

10. En el menú desplegable de Default Network Analysis Policy, elija la política creada en el paso 2.

11. Haga clic en Aceptar y Guardar los cambios.

12. Haga clic en la opción Deploy para implementar las políticas en los dispositivos administrados relevantes.

⚠ Precaución: se espera que el aumento del tiempo de espera provoque una mayor utilización de la memoria. FirePOWER tiene que realizar un seguimiento de los flujos que los terminales no cierran durante más tiempo. El aumento real en la utilización de la memoria es diferente para cada red única, ya que depende del tiempo que las aplicaciones de red mantienen inactivas las conexiones TCP.

Conclusión

Los parámetros de referencia de cada red para el tiempo de espera inactivo de las conexiones TCP son diferentes. Depende completamente de las aplicaciones que se estén utilizando. Se debe establecer un valor óptimo observando durante cuánto tiempo las aplicaciones de red

mantienen inactivas las conexiones TCP. En el caso de los problemas relacionados con el módulo de servicio FirePOWER en un Cisco ASA, cuando no se puede deducir un valor óptimo, el tiempo de espera se puede ajustar aumentando el tiempo de espera en pasos hasta el valor de tiempo de espera de ASA.

Información Relacionada

- [Guías de instalación y actualización](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)
- [Guía de inicio rápido de ASA Firepower](#)

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).