Resolución de problemas de tráfico en CSF CLI

Contenido

Introducción

Este documento describe cómo utilizar Cisco Secure Firewall CLI para resolver problemas de tráfico validando el ruteo, el flujo de paquetes y el comportamiento de Snort.

Prerequisites

No hay requisitos específicos para este documento.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de objetos y políticas de Firepower Management Center (FMC)
- Routing de Cisco Secure Firewall (CSF) y lógica de interfaz
- Conceptos de solución de problemas de firewall e inspección de paquetes

Componentes Utilizados

Este documento no se limita a versiones específicas de software y hardware para CSF. El dispositivo utilizado en el documento ejecuta el código 7.6.5.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- Centro de gestión de firewall seguro (FMC)
- Firewall seguro de Cisco (CSF)
- Herramientas CLI de Firepower Threat Defence

Información importante

Cuando un dispositivo experimenta un uso elevado de la CPU, la memoria o la E/S, la ejecución de comandos de solución de problemas puede exacerbar la degradación del rendimiento. Se recomienda investigar y resolver primero la condición de agotamiento de recursos y luego proceder con el diagnóstico de problemas de tráfico. Los comandos de diagnóstico consumen recursos adicionales del sistema, lo que puede degradar aún más la disponibilidad y prolongar el tiempo de recuperación.

Antecedentes

La resolución de problemas del tráfico en CSF a menudo comienza por confirmar la trayectoria lógica que un paquete debe tomar a través del firewall. Una vez que se entienden la ruta y la asignación de interfaz, el siguiente paso es comparar la trayectoria esperada con el flujo de paquetes real. Esto se puede realizar mediante búsquedas de rutas, simulación de trazador de paquetes, capturas de paquetes y seguimiento del motor Snort.

Cada herramienta proporciona una capa de visibilidad diferente:

- show route confirma el trayecto de ruteo del paquete y la identidad de la interfaz.

- packet-tracer simula el flujo de tráfico e identifica las decisiones de ACL, NAT e interfaz.
- las capturas de paquetes examinan el tráfico activo que atraviesa el firewall.
- system support trace expone la toma de decisiones de Snort para los eventos de inspección o bloques relacionados con políticas.

Consejo: Comience con el ruteo y la validación del rastreador de paquetes antes de capturar el tráfico, de modo que pueda confirmar si las decisiones esperadas sobre el trayecto y el control de acceso son correctas antes de analizar el tráfico en vivo.

Problema

Un flujo de tráfico no funciona como se esperaba y el administrador debe determinar si el paquete está tomando la ruta correcta, si el firewall está permitiendo o denegando la conexión y si la inspección de políticas o Snort está bloqueando el tráfico.

Paso 1: Encuentre la ruta

Identifique la trayectoria de ruteo y determine los nombres de interfaz lógica asociados con las direcciones IP de origen y destino. La mayoría de los comandos de solución de problemas requieren los nombres de interfaz lógica, por lo que este debe ser el primer paso del flujo de trabajo de solución de problemas.

Ejecute el comando para la dirección IP de origen y de destino:

```
show route <IP>
```

El tráfico con destino a Internet que depende de la ruta predeterminada requiere la identificación de la interfaz de salida lógica. El nombre de la interfaz lógica se puede determinar ejecutando este paso:

```
show route 0.0.0.0
```

Ejemplo de salida:

```
FTD1# show route 192.168.0.11


Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

En este ejemplo, la interfaz de ingreso lógico es Inside y la interfaz de egreso es Outside.

Precaución: La traducción de direcciones de red (NAT) puede redirigir el tráfico a través de interfaces diferentes de las que indica la tabla de routing cuando las políticas de NAT coinciden con el flujo de tráfico. Al resolver problemas de conectividad, verifique que su configuración de NAT esté alineada con la trayectoria de tráfico esperada.

Consejo: Los nombres de interfaz lógica se utilizan en los comandos de solución de problemas de CLI. Tome nota del nombre lógico para futuras referencias.

Paso 2: Ejecutar Packet-Tracer

Utilice packet-tracer para simular cómo el firewall evalúa un flujo de tráfico específico. Esta herramienta ayuda a confirmar qué interfaces se utilizan, si se aplica una política NAT y si una ACL permite o deniega el tráfico.

Utilice esta sintaxis de comando:

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

Ejemplo de comando:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

Revise la salida para confirmar que el paquete sigue la trayectoria esperada y que se permite durante la simulación. Esto es útil cuando necesita determinar si el problema está relacionado con el ruteo, NAT o coincidencia de políticas antes de participar en el análisis de paquetes en vivo.

La palabra clave transmit en packet-tracer hace que el paquete simulado se inyecte en la interfaz de ingreso, lo que le permite atravesar todas las fases de procesamiento del firewall en lugar de permanecer como una simulación.

Ejemplo de comando:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

Paso 3: Ejecutar capturas

Utilice capturas de paquetes para inspeccionar el tráfico activo a medida que pasa a través del firewall. Las capturas de paquetes son diferentes de packet-tracer porque capturan el tráfico real y, por lo tanto, deben coincidir con el flujo real que atraviesa el firewall en el momento en que la captura está activa. Las capturas de paquetes son bidireccionales y documentan ambos lados de la conexión.

Para la mayoría de los escenarios de resolución de problemas de tráfico, configure estas capturas:

- Captura de entrada: captura el tráfico que llega a la interfaz de origen
- Captura de salida: captura el tráfico que sale de la interfaz de destino
- Captura de descarte de ASP: captura los paquetes descartados por el firewall y que coinciden con los criterios configurados.

Sintaxis general de la captura:

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

Ejemplo de captura de ingreso:

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

Ejemplo de captura de salida:

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

Ejemplo de captura de borrado ASP:

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

Las capturas de paquetes son bidireccionales, lo que significa que tanto el tráfico de reenvío como el de retorno se pueden capturar en función de los criterios de coincidencia definidos. La función de seguimiento permite visualizar las decisiones que toma el firewall sobre el tráfico real.

⚠ Precaución: Si se está realizando NAT, la captura de salida debe utilizar la IP de origen traducida, no la IP de origen original, para capturar el tráfico posterior a NAT correctamente.

Paso 4: Ejecutar seguimiento de compatibilidad del sistema

Utilice el seguimiento de asistencia del sistema para ver el proceso de inspección de Snort en tiempo real para un flujo de tráfico específico. Esto es especialmente útil cuando el tráfico coincide con una regla de permiso ACL pero sigue bloqueado por la inspección de políticas. Las capturas de paquetes estándar muestran que se bloqueó un paquete, pero el seguimiento de compatibilidad del sistema proporciona visibilidad de por qué se gestionó el paquete de esa manera. El seguimiento de compatibilidad del sistema es bidireccional, lo que significa que recibe tráfico de ambos lados. Esto significa que no importa el orden en que se agregan las direcciones IP a la herramienta.

Ejecute este comando y responda a las indicaciones:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

Esta herramienta resulta especialmente útil cuando el entorno utiliza reglas de aplicaciones o URL, reglas basadas en identidad, políticas de archivos o políticas de intrusiones. Estas funciones se evalúan después de la coincidencia de ACL, por lo que la política de control de acceso puede permitir un paquete pero la inspección de Snort puede bloquearlo.

Nota: El puerto del cliente puede dejarse en blanco si se desconoce el puerto de origen exacto.

Verificación

Utilice el resultado de la búsqueda de rutas, la simulación del trazador de paquetes, las capturas de paquetes y el seguimiento de la compatibilidad del sistema para confirmar el comportamiento del flujo de tráfico. El objetivo es determinar si el paquete está tomando la ruta correcta, si el firewall lo permite o lo niega y si Snort lo está bloqueando en función de una inspección más profunda.

Un flujo de resolución de problemas completo normalmente confirma:

- La búsqueda de rutas muestra las interfaces lógicas de ingreso y egreso.
- Packet-tracer confirma la ruta de reenvío prevista y la evaluación de la política.
- Las capturas de paquetes confirman si el tráfico llega y sale como se esperaba.
- El seguimiento de soporte del sistema confirma si la inspección de políticas o Snort está causando el bloqueo.

Troubleshoot

Cuando un problema de tráfico persiste, revise las siguientes áreas:

- Verifique si la búsqueda de rutas coincide con las interfaces de origen y destino esperadas.
- Verifique si el resultado del rastreador de paquetes muestra el tráfico que se está denegando en la etapa de ACL o NAT.
- Revise las capturas de paquetes de entrada y salida para confirmar que el tráfico está

llegando al firewall y saliendo de la interfaz correcta.
- Utilice capturas de caídas de ASP para confirmar si el firewall está descartando el tráfico internamente.
- Utilice el seguimiento de soporte del sistema para determinar si Snort está bloqueando el tráfico después de la decisión de permiso de ACL.

Información Relacionada

- Analizar capturas de firewalls de Firepower para solucionar problemas de red
- Utilice capturas de Firepower Threat Defence y Packet Tracer

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).