Solución de problemas de ruta de datos de Firepower: Overview

Contenido

Introducción

El objetivo de esta guía es ayudar a identificar rápidamente si un dispositivo Firepower Threat Defense (FTD) o un dispositivo de seguridad adaptable (ASA) con FirePOWER Services está causando un problema con el tráfico de red. Asimismo, ayuda a reducir qué componentes de Firepower se deben investigar y qué datos se deben recopilar antes de ponerse en contacto con el Cisco Technical Assistance Center (TAC).

Lista de todos los artículos de la serie de resolución de problemas de la ruta de datos de Firepower.

Fase 1 de Troubleshooting de Trayectoria de Datos de Firepower: Entrada de paquetes

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html

Fase 2 de Troubleshooting de Trayectoria de Datos de Firepower: Capa DAQ
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

Fase 3 de Troubleshooting de Trayectoria de Datos de Firepower: Inteligencia de seguridad
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Fase 4 de Troubleshooting de Trayectoria de Datos de Firepower: Política de control de acceso
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Fase 5 de Troubleshooting de Trayectoria de Datos de Firepower: Política SSL
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Fase 6 de Troubleshooting de Trayectoria de Datos de Firepower: Autenticación activa
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Fase 7 de Troubleshooting de Trayectoria de Datos de Firepower: Política de intrusiones
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Fase 8 de Troubleshooting de Trayectoria de Datos de Firepower: Política de análisis de red

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html

Prerequisites

- En este artículo se supone que se tiene un conocimiento básico de las plataformas FTD y ASA.
- Se recomienda el conocimiento del snort de código abierto, aunque no es necesario.

Para obtener una lista completa de la documentación de Firepower, incluidas las guías de instalación y configuración, visite la página hoja de ruta de la documentación.

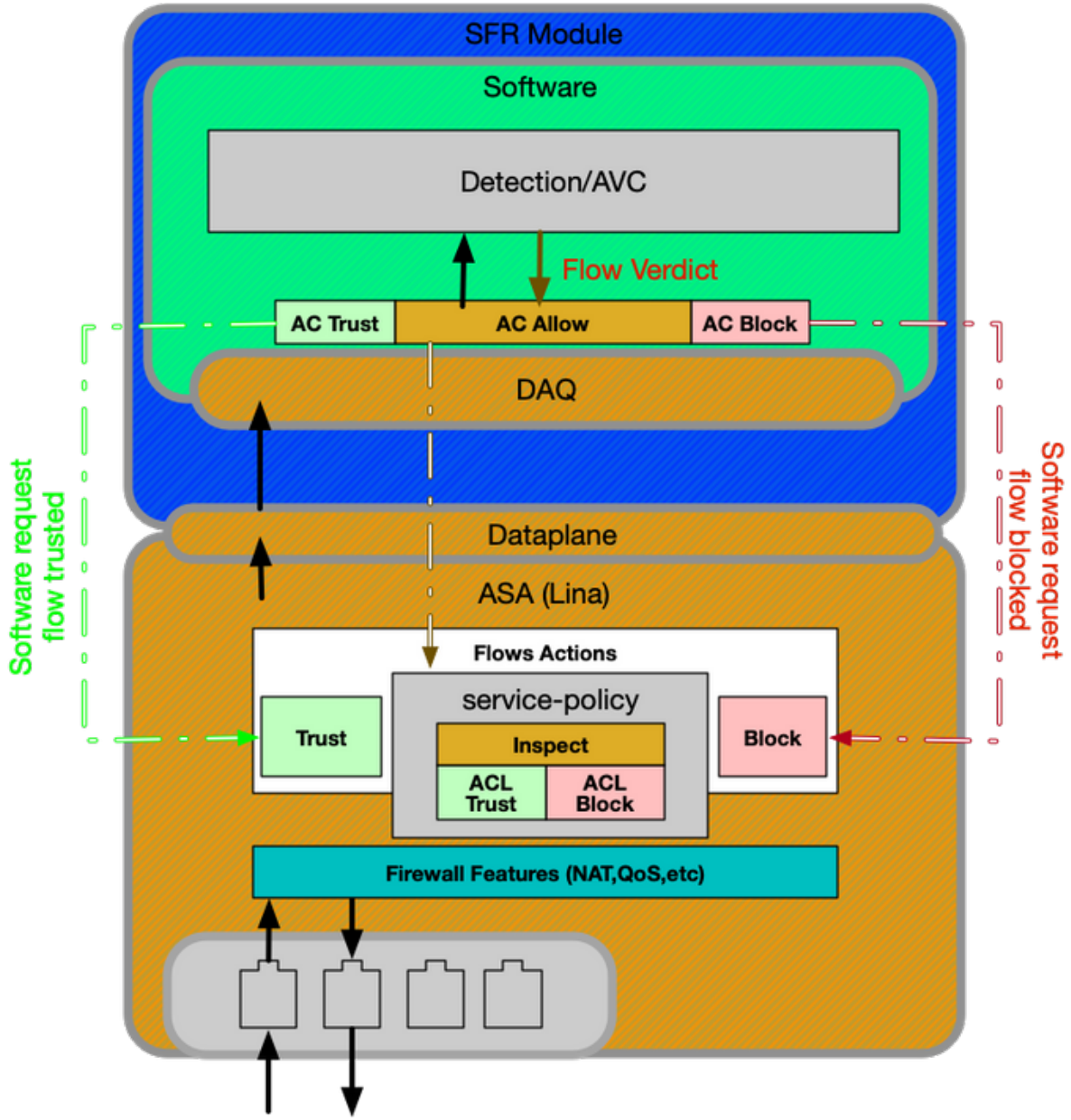
Descripción general de la arquitectura de la ruta de datos

En la siguiente sección se analiza la ruta de datos de la arquitectura para varias plataformas Firepower. Con la arquitectura en mente, seguiremos con la forma de determinar rápidamente si el dispositivo Firepower está bloqueando o no el flujo de tráfico.

> **Nota:** Este artículo no cubre los dispositivos Firepower 7000 y 8000 antiguos, ni la plataforma virtual NGIPS (sin FTD). Para obtener información sobre la resolución de problemas de esas plataformas, visite nuestra página TechNotes.

Plataforma ASA con FirePOWER Services (módulo SFR)

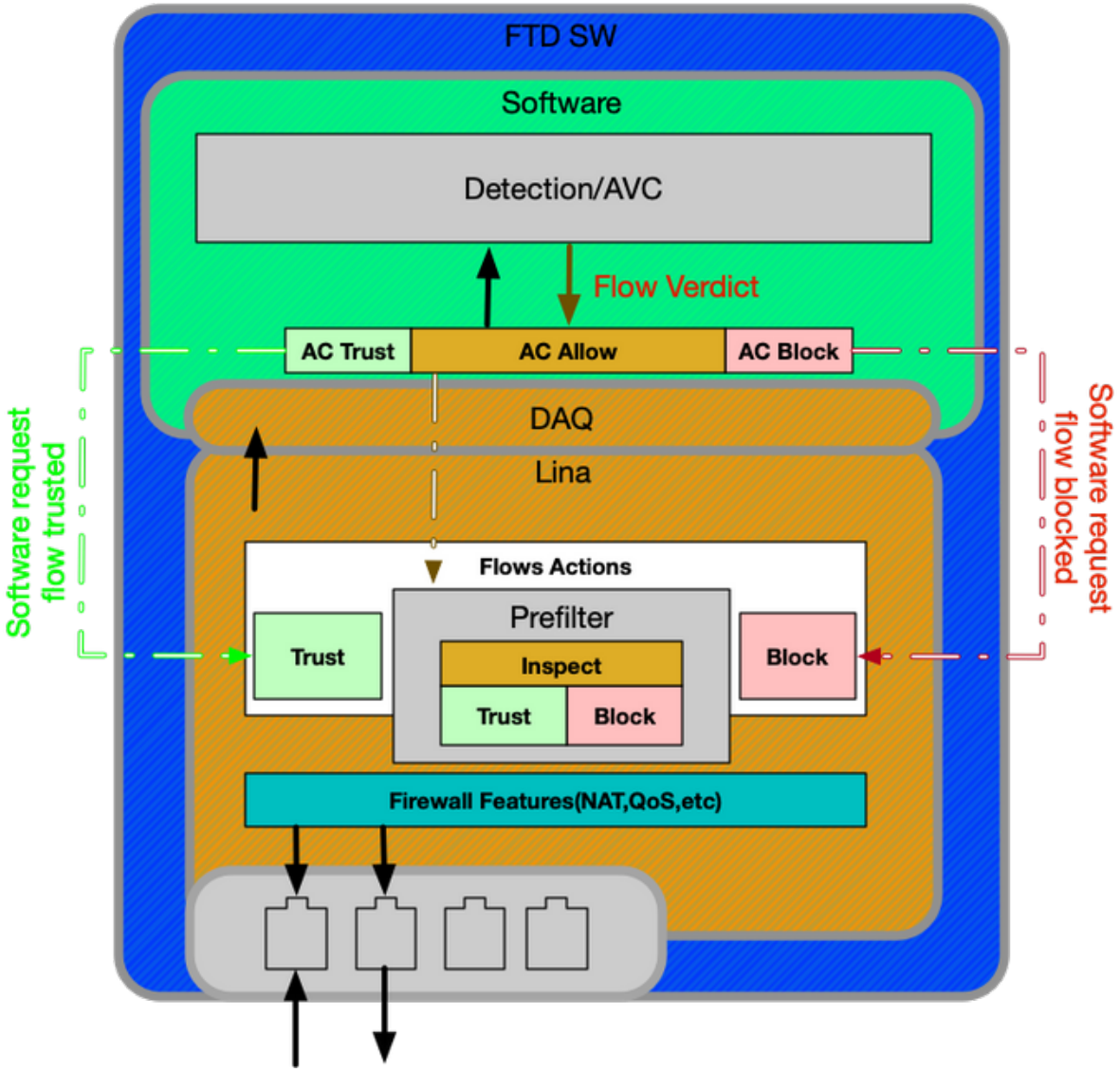
La plataforma FirePOWER Services también se denomina módulo SFR. Se trata básicamente de una máquina virtual que se ejecuta en plataformas ASA 5500-X.



La política de servicio en el ASA determina qué tráfico se envía al módulo SFR. Hay una capa de plano de datos que se utiliza para comunicarse con el motor de adquisición de datos de Firepower (DAQ), que se utiliza para traducir paquetes de una manera que el snort puede entender.

Firepower Threat Defense en ASA500-X y plataforma FTD virtual

La plataforma FTD consiste en una única imagen que contiene el código Lina (ASA) y Firepower. Una diferencia importante entre esto y ASA con la plataforma de módulo SFR es que hay comunicaciones más eficientes entre Lina y Snort.

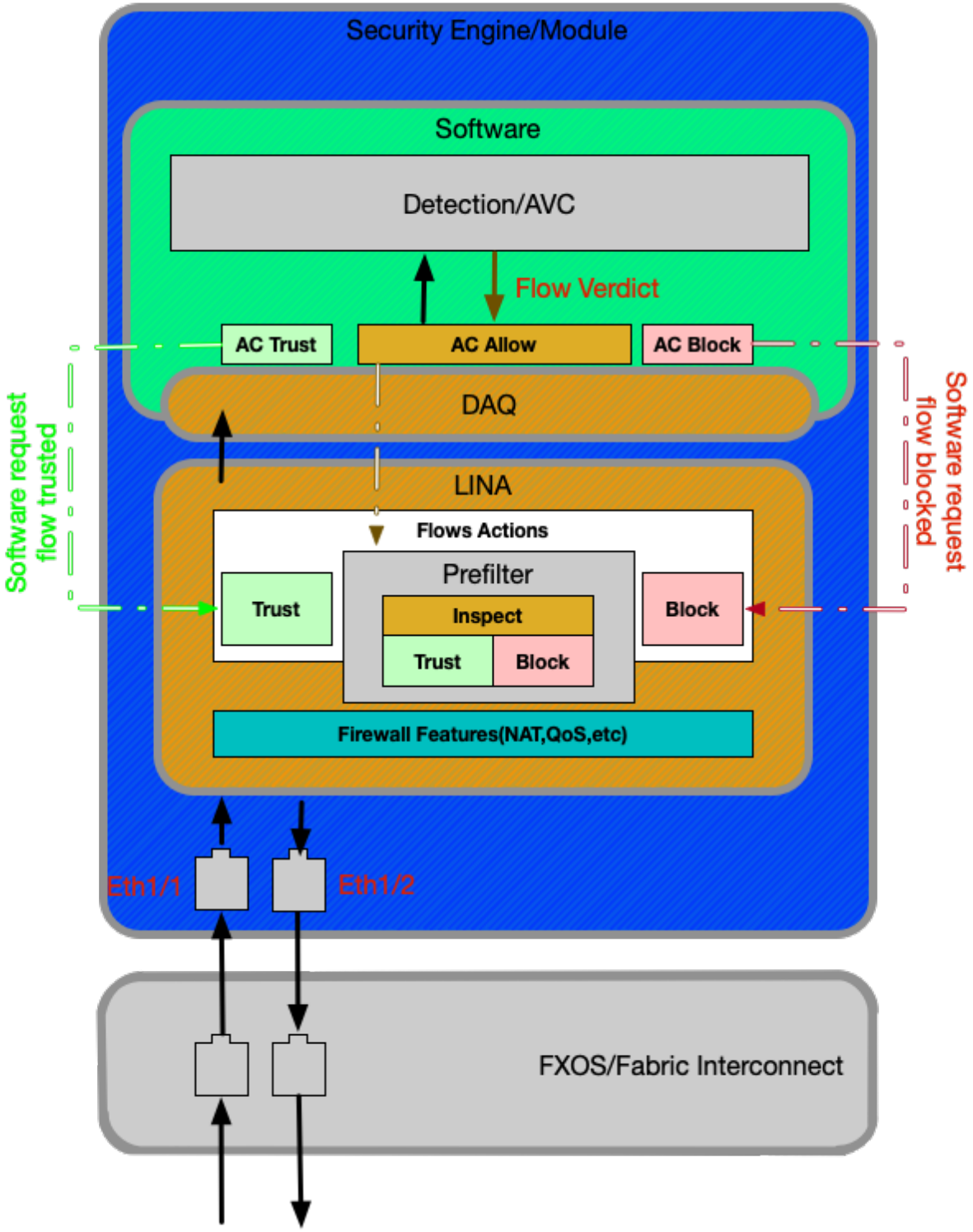


FTD en plataformas SSP

En los modelos de plataformas de servicios de seguridad (SSP), el software FTD se ejecuta sobre la plataforma Firepower eXtensible Operative System (FXOS), que es un sistema operativo subyacente que se utiliza para administrar el hardware del chasis y alojar diversas aplicaciones conocidas como dispositivos lógicos.

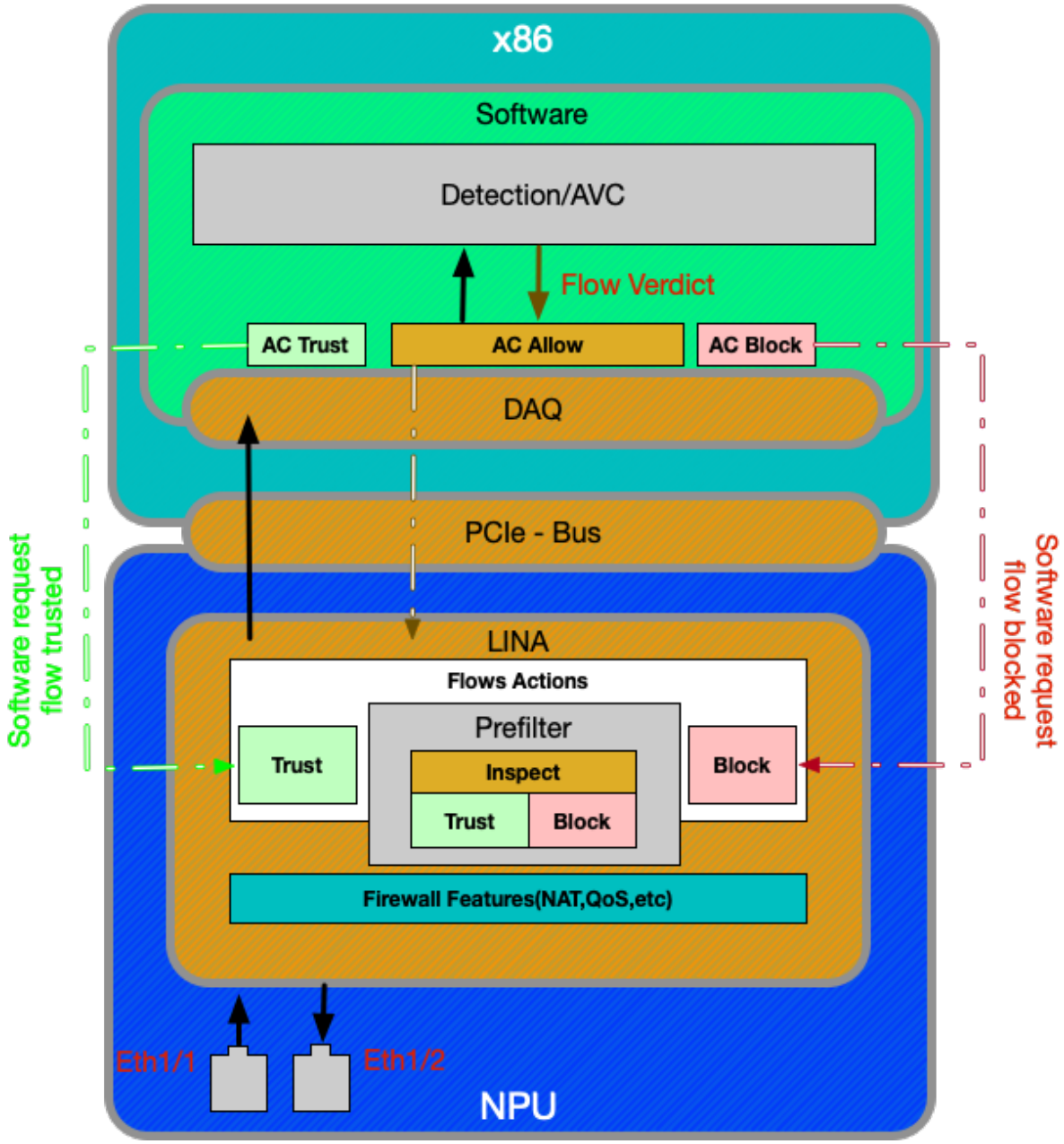
Dentro de la plataforma SSP, existen algunas diferencias entre los modelos, como se ve en los diagramas y descripciones siguientes.

Dispositivos FirePOWER 9300 y 4100



En las plataformas Firepower 9300 y 4100, los paquetes de entrada y salida son manejados por un switch con el firmware FXOS (Fabric Interconnect). Los paquetes se envían luego a las interfaces asignadas al dispositivo lógico (en este caso, FTD). Después de eso, el procesamiento de paquetes es el mismo que en las plataformas FTD no SSP.

Dispositivos Firepower 2100



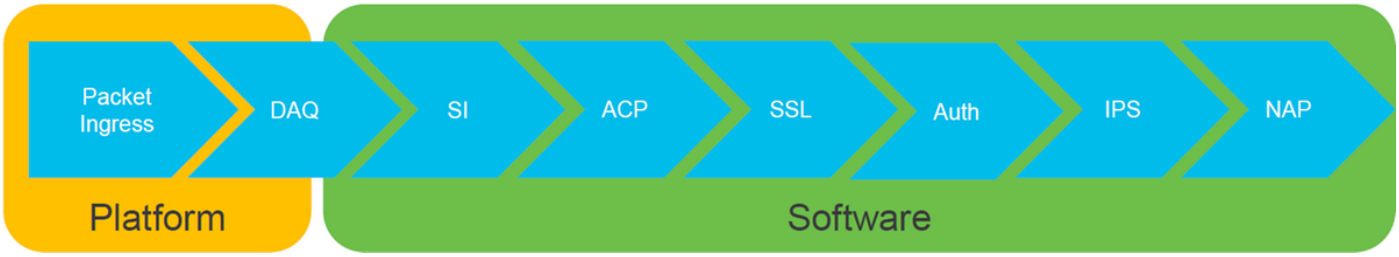
El dispositivo Firepower 2100 funciona de forma muy parecida a las plataformas FTD que no son SSP. No contiene la capa de fabric interconectada que está presente en los modelos 9300 y 4100. Sin embargo, hay una diferencia importante en los dispositivos de la serie 2100 en comparación con los otros dispositivos, y es la presencia del circuito integrado específico de la aplicación (ASIC). Todas las funciones de ASA tradicionales (Lina) se ejecutan en el ASIC y todas las funciones de firewall de última generación (NGFW) (snort, filtrado de URL, etc.) se ejecutan en la arquitectura x86 tradicional. La forma en que Lina y Snort se comunican en esta plataforma es a través de una interfaz de interconexión de componentes periféricos (PCIe) a través de una cola de paquetes, a diferencia de las otras plataformas que utilizan acceso directo a memoria (DMA) para poner en cola los paquetes a modo de suspensión.

> **Nota:** Se seguirán los mismos métodos para solucionar problemas de las plataformas FTD que no son SSP en la plataforma FPR-2100.

Proceso recomendado para Troubleshooting de Firepower Data-Path

Ahora que hemos tratado cómo identificar el tráfico único, así como la arquitectura de ruta de datos básica en las plataformas Firepower, ahora examinamos los lugares específicos en los que se pueden descartar los paquetes. Hay ocho componentes básicos que se tratan en los artículos de Ruta de datos, que pueden resolver problemas sistemáticamente para determinar posibles pérdidas de paquetes. Estos incluyen:

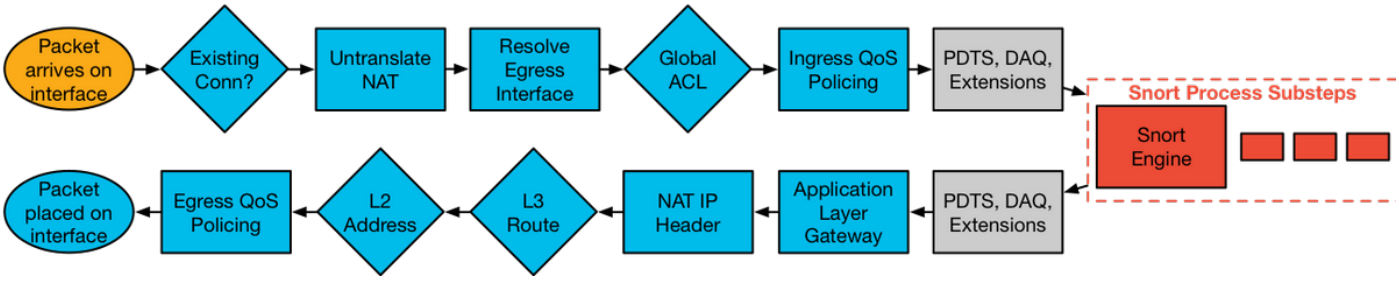
1. Entrada de paquetes
2. Capa de firewall DAQ
3. Inteligencia de seguridad
4. Política de control de acceso
5. Política SSL
6. Funciones de autenticación activa
7. Política de intrusiones (reglas IPS)
8. Política de análisis de red (configuración previa al procesador de SNU)



Nota: Estos componentes no se enumeran en el orden exacto de las operaciones en el procesamiento de Firepower, sino que se solicitan de acuerdo con nuestro flujo de trabajo de solución de problemas recomendado. Consulte la ilustración siguiente para ver la ruta real del diagrama de paquetes.

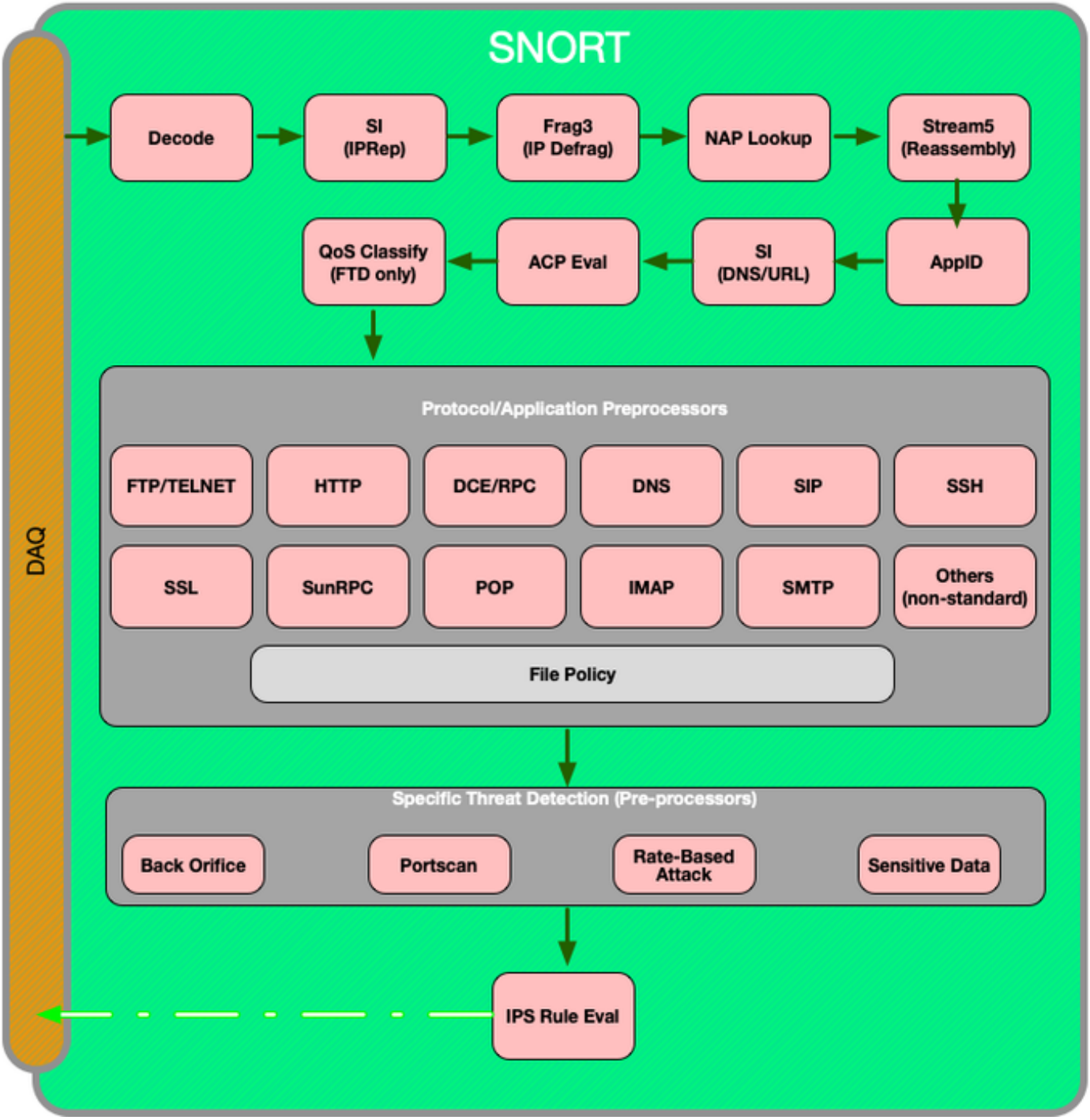
Ruta real del paquete a través de FTD

La ilustración siguiente muestra la ruta real del paquete a medida que atraviesa FTD.



Ruta del paquete Snort

La ilustración siguiente muestra la trayectoria del paquete a través del motor Snort.



Entrada y salida de paquetes

El primer paso para la solución de problemas del trayecto de datos es asegurarse de que no se produzcan pérdidas en la etapa de ingreso o egreso del procesamiento de paquetes. Si un paquete ingresa pero no se arroja, puede estar seguro de que el dispositivo está descartando el paquete en algún lugar dentro del trayecto de datos.

Este artículo explica cómo resolver problemas de ingreso y egreso de paquetes en sistemas Firepower.

Capa de firewall DAQ

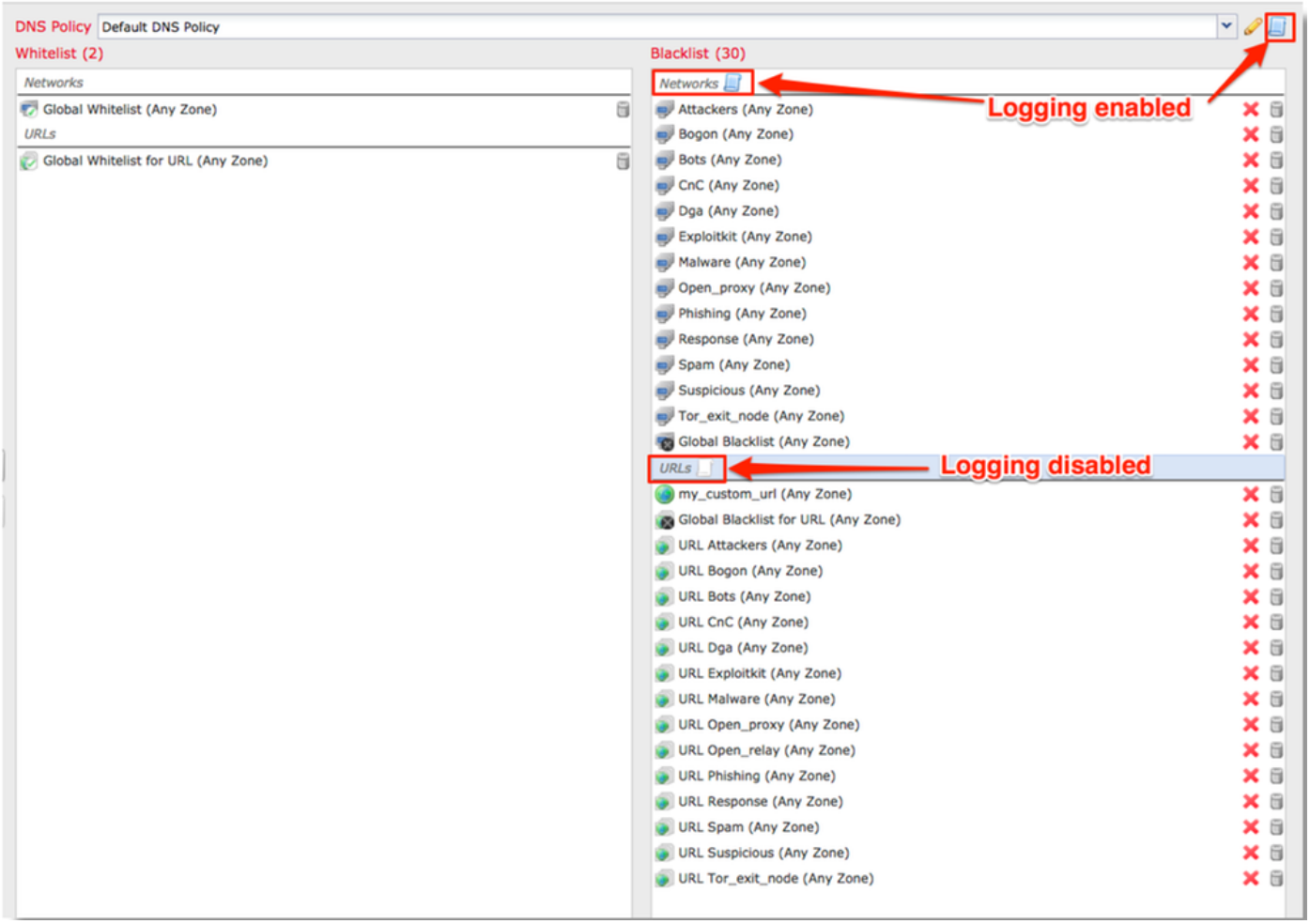
Si se ha determinado que el paquete ingresa pero no se agota, el siguiente paso en la solución de problemas de ruta de datos debe ser en la capa Firepower DAQ (Data Acquisition) para asegurarse de que el tráfico en cuestión se envíe a Firepower para su inspección y, si es así, si se lo descarta o modifica.

Este artículo analiza cómo resolver problemas de la gestión inicial del tráfico por Firepower, así como la trayectoria que está tomando a través del dispositivo.

También se explica cómo se puede omitir totalmente el dispositivo Firepower para determinar si un componente Firepower es responsable del problema del tráfico.

Inteligencia de seguridad

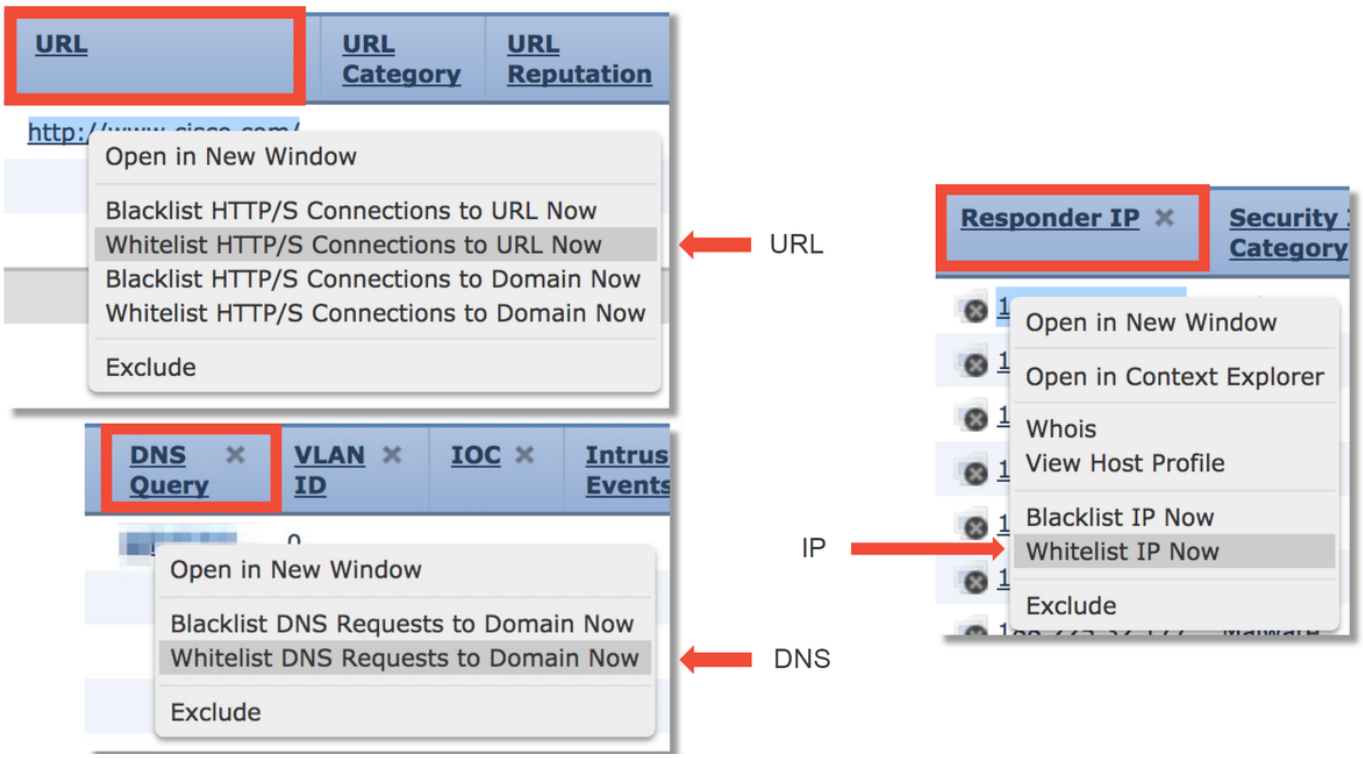
La inteligencia de seguridad es el primer componente de Firepower que inspecciona el tráfico. Los bloques de este nivel son muy fáciles de determinar siempre y cuando el registro esté habilitado. Esto se puede determinar en la GUI de FMC navegando hasta **Políticas > Control de acceso > Directiva de control de acceso**. Después de hacer clic en el icono de edición junto a la política en cuestión, navegue hasta la pestaña **Seguridad Inteligente**.



Una vez que se habilita el registro, puede ver los Eventos de Seguridad Inteligente en **Análisis > Conexiones > Eventos de Seguridad Inteligente**. Debe estar claro por qué se bloquea el tráfico.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

Como paso de mitigación rápida, puede hacer clic con el botón derecho del ratón en la IP, URL o consulta DNS bloqueada por la función Security Intelligence y elegir una opción de lista blanca.



Si sospecha que algo se ha incluido incorrectamente en la lista negra o desea solicitar un cambio de reputación, puede abrir un ticket directamente con Cisco Talos en el siguiente enlace:

https://www.talosintelligence.com/reputation_center/support

También puede proporcionar los datos al TAC para informar sobre lo que se está bloqueando y tal vez eliminar una entrada de una lista negra.

Para la resolución de problemas en profundidad del componente de Inteligencia de Seguridad, revise el artículo pertinente de Troubleshooting de Trayectoria de Datos.

Política de control de acceso

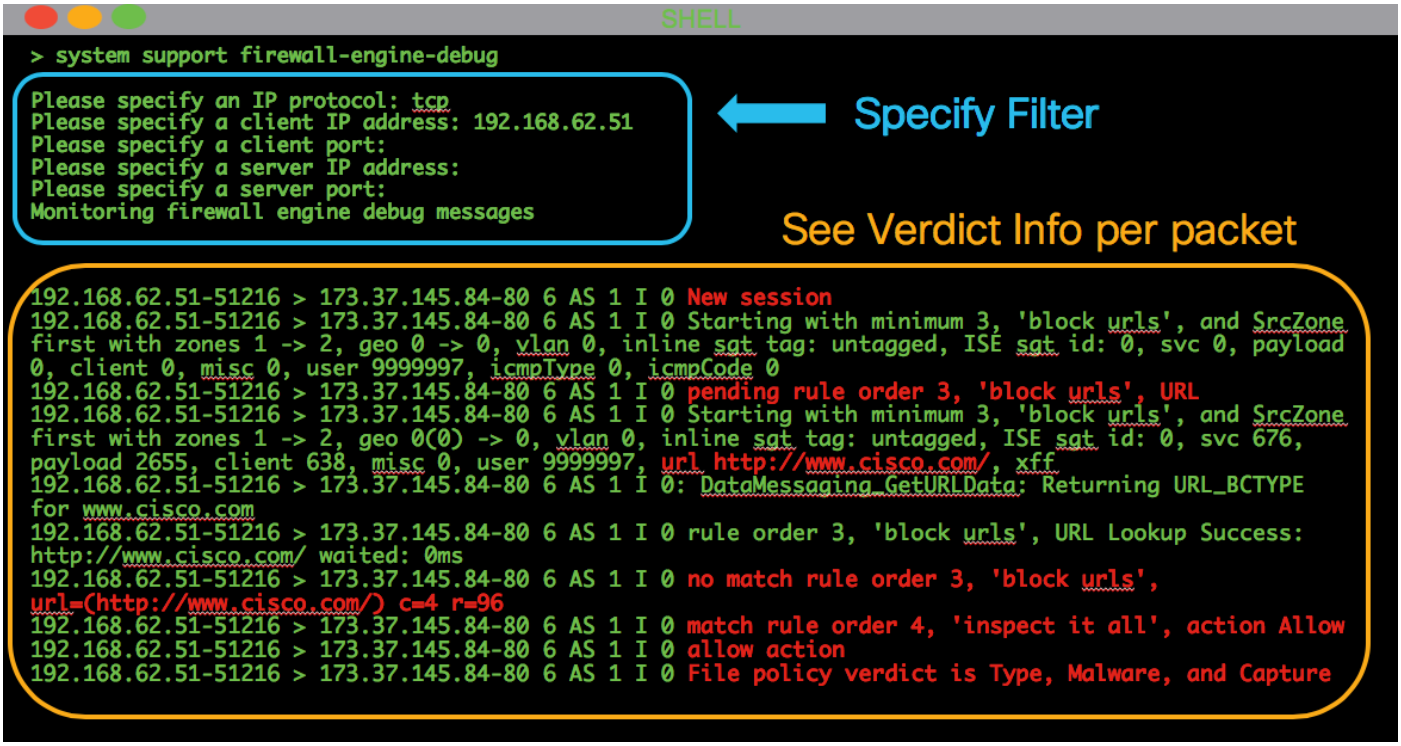
Si se ha determinado que la función de inteligencia de seguridad no está bloqueando el tráfico, el siguiente paso recomendado es resolver problemas de las reglas de la política de control de acceso para ver si una regla con una acción de bloqueo está descartando el tráfico.

Se recomienda comenzar a utilizar el comando "firewall-engine-debug" o capturar con seguimiento. Normalmente, estas herramientas pueden ofrecerle la respuesta de inmediato y

explicarle qué regla tiene el tráfico y por qué motivos.

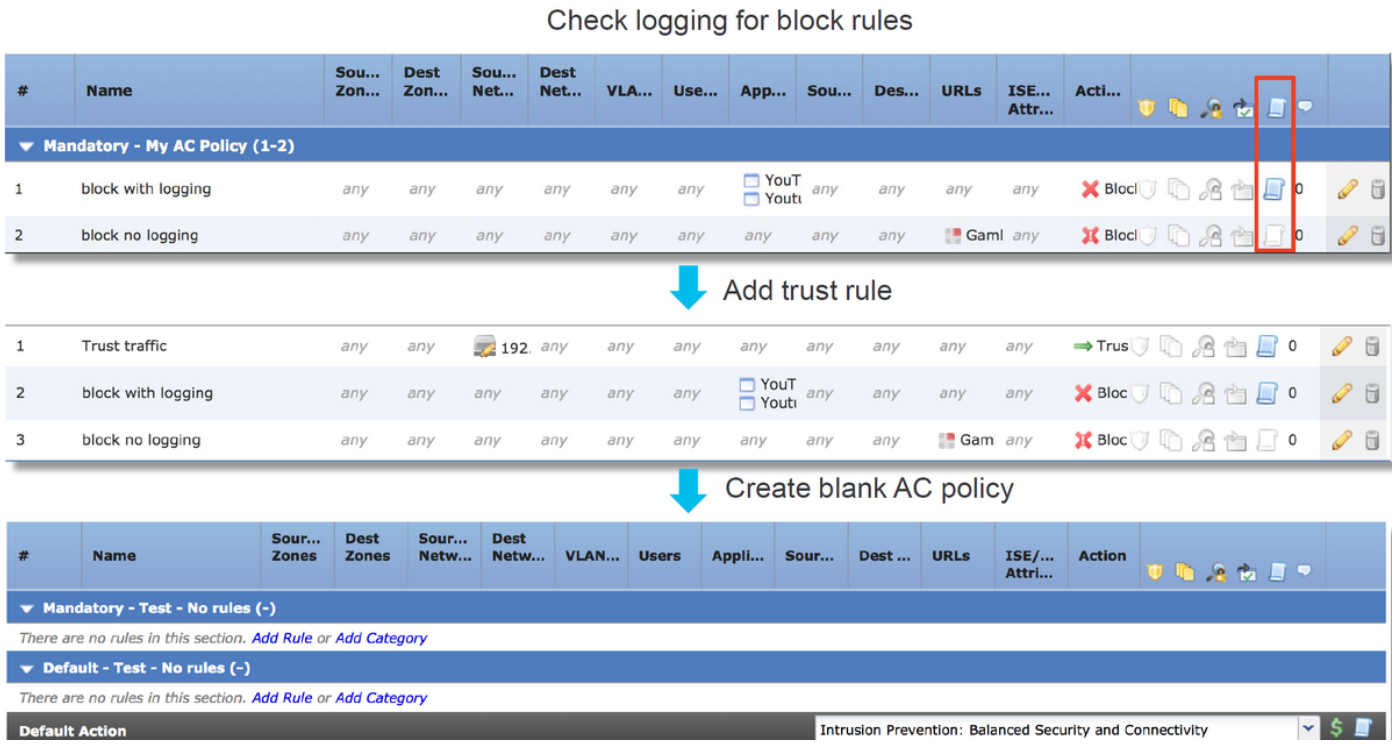
- Ejecute la depuración en Firepower CLI para ver qué regla bloquea el tráfico (asegúrese de introducir tantos parámetros como sea posible) mediante el siguiente comando: **> system support firewall-engine-debug**
- El resultado de la depuración se puede proporcionar al TAC para su análisis

A continuación se muestra un ejemplo de salida que muestra la evaluación de reglas para el tráfico que coincide con una regla de control de acceso con la acción 'Permitir':



Si no puede determinar qué regla de control de acceso (AC) coincide o no puede determinar si la política de CA es el problema mediante las herramientas anteriores, a continuación se indican algunos pasos básicos para solucionar el problema de la política de control de acceso (tenga en cuenta que estas opciones no son la primera porque requieren cambios o implementaciones de políticas):

- Habilitar el registro para cualquier regla con una acción de 'Bloquear'
- Si todavía no ve los eventos de conexión para el tráfico y se está bloqueando, a continuación cree una regla de confianza para el tráfico en cuestión como paso de mitigación
- Si la regla de confianza para el tráfico todavía no resuelve el problema pero todavía sospecha que la política de CA es defectuosa, a continuación, cree una nueva política de control de acceso en blanco si es posible, utilizando una acción predeterminada distinta de 'Bloquear todo el tráfico'

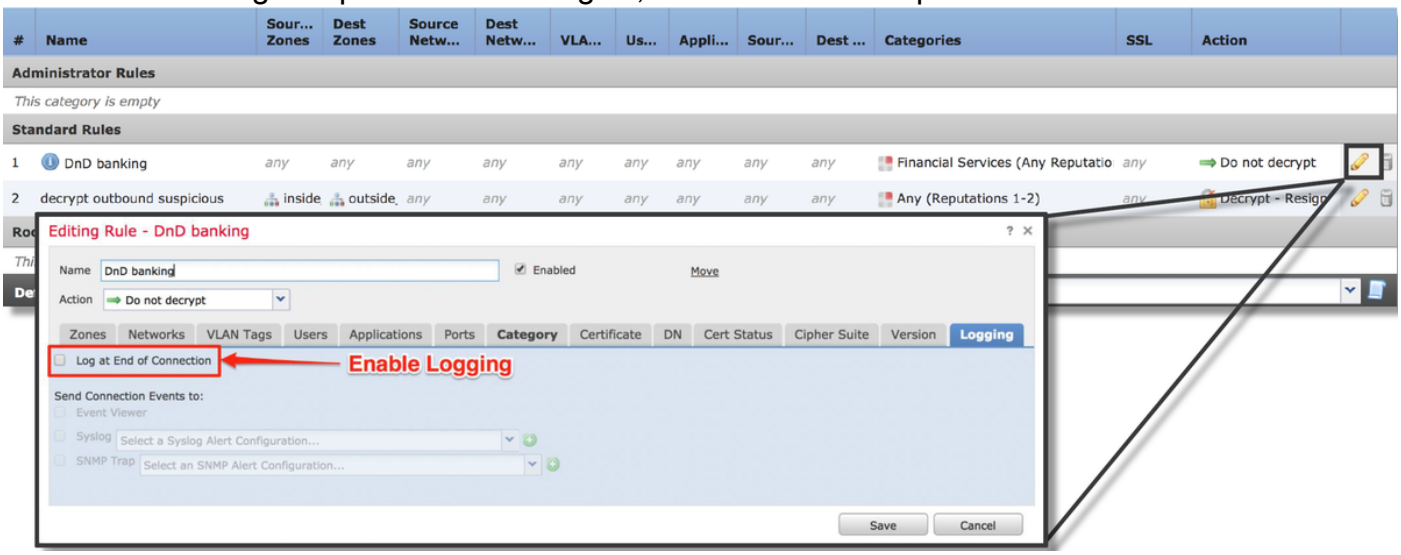


Para obtener información detallada sobre la resolución de problemas de la política de control de acceso, revise el artículo pertinente sobre la solución de problemas de ruta de datos.

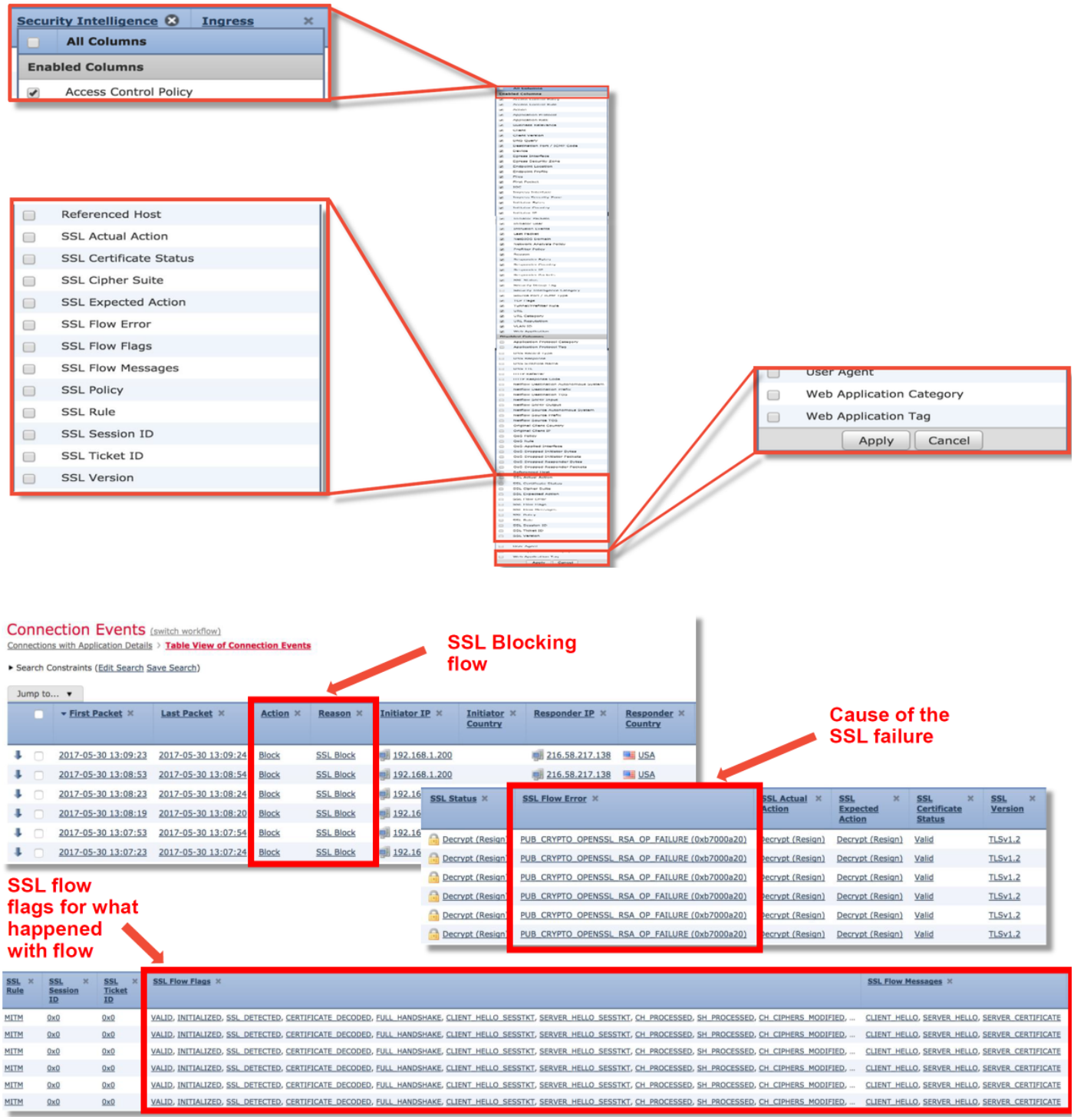
Política SSL

Si se utiliza la política SSL, es posible que esté bloqueando el tráfico. A continuación se muestran algunos pasos básicos para la resolución de problemas de la política SSL:

- Habilitar el registro para todas las reglas, incluida la 'Acción predeterminada'



- Verifique la ficha Undecryptable Actions (Acciones descifrables) para ver si se ha establecido una opción para bloquear el tráfico
- En la sección Eventos de conexión, active todos los campos con 'SSL' en el nombre
  La mayoría de ellas están desactivadas de forma predeterminada y deben habilitarse en el visor de eventos de conexión haciendo clic en la cruz situada junto a cualquier nombre de columna



- Cree una política SSL en blanco con No descifrar como acción predeterminada como paso de mitigación
- Eliminar la política SSL de la política de control de acceso como paso de mitigación
  Esto se establece en la ficha Opciones avanzadas

Se sospecha que la política SSL ha descartado tráfico, los eventos de conexión junto con la configuración de la política se pueden enviar al TAC.

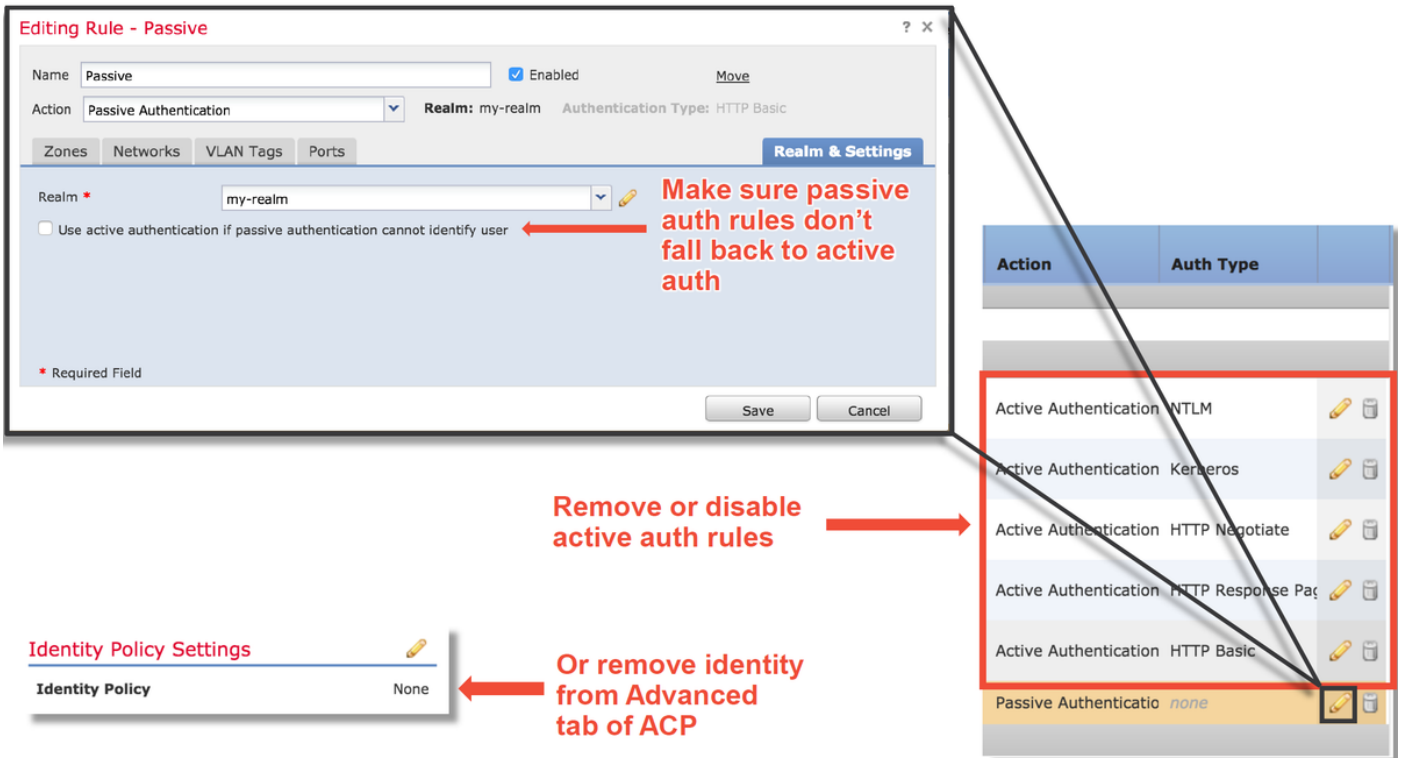
Para obtener una resolución de problemas más detallada de la política SSL, revise el artículo pertinente sobre la solución de problemas de la ruta de datos.

Autenticación activa

Cuando se utiliza en una política de identidad, la autenticación activa tiene la capacidad de descartar el tráfico que debería permitirse si algo sale mal. La propia función de autenticación activa puede afectar directamente a todo el tráfico HTTP/HTTPS porque si se determina que necesitamos autenticar a un usuario, todo esto sucede solamente sobre el protocolo HTTP. Esto significa que la autenticación activa no debe afectar a otros servicios de red (como DNS, ICMP, etc.) a menos que tenga reglas de control de acceso específicas que se bloqueen en función del usuario, y los usuarios no pueden autenticarse a través de los servicios de autenticación activos en el FTD. Sin embargo, esto no sería un problema directo de la función de autenticación activa, sino un resultado de que los usuarios no pueden autenticarse y tienen una política que bloquea a los usuarios no autenticados.

Un paso de mitigación rápido sería inhabilitar cualquier regla dentro de la política de identidad con la acción de 'Autenticación activa'.

Además, asegúrese de que las reglas con la acción 'Autenticación pasiva' no tengan marcada la opción 'Usar autenticación activa si la autenticación pasiva no puede identificar al usuario'.



Para obtener más información sobre la resolución de problemas de Active Authentication, revise el artículo pertinente sobre la resolución de problemas de ruta de datos.

Política de intrusiones

Una política de intrusiones puede estar descartando tráfico o causando latencia de red. Una política de intrusiones se puede utilizar en una de las tres ubicaciones siguientes dentro de la política de control de acceso:

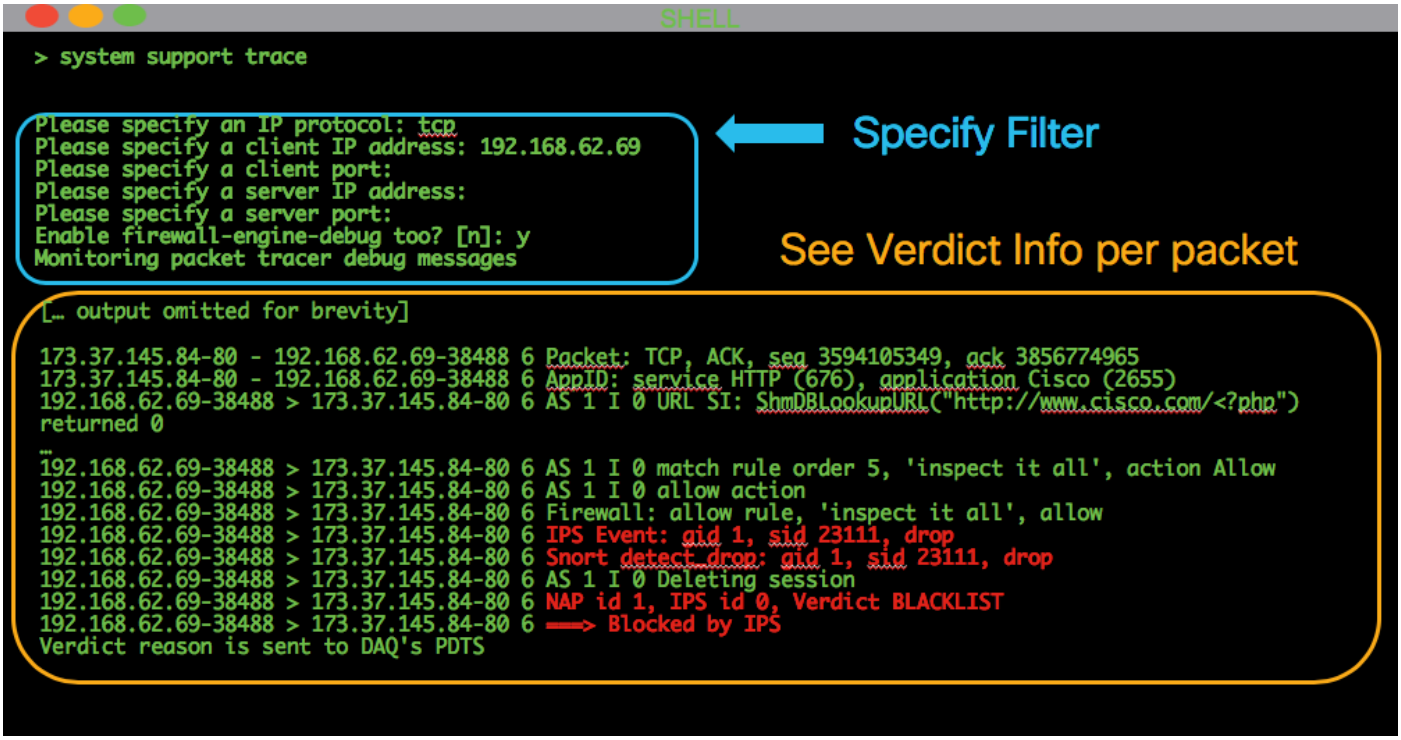
- En una regla de control de acceso, en la ficha "Inspección"
- En la acción predeterminada
- En la pestaña Advanced, en la sección **Network Analysis and Intrusion Policies > Intrusion Policy used before Access Control rule are determine**

Para ver si una regla de política de intrusiones está bloqueando el tráfico, vaya a la página

Análisis > Intrusiones > Eventos en el FMC. La vista **de tabla de eventos de intrusiones** proporciona información sobre los hosts involucrados en los eventos. Consulte el artículo de solución de problemas de ruta de datos pertinente en información relativa al análisis de eventos.

El primer paso recomendado para determinar si una firma de política de intrusión (IPS) está bloqueando el tráfico sería utilizar la función **> de seguimiento de compatibilidad del sistema** de la CLI del FTD. Este comando debug funciona de manera similar a firewall-engine-debug, y también le ofrece la opción de habilitar firewall-engine-debug junto con el seguimiento.

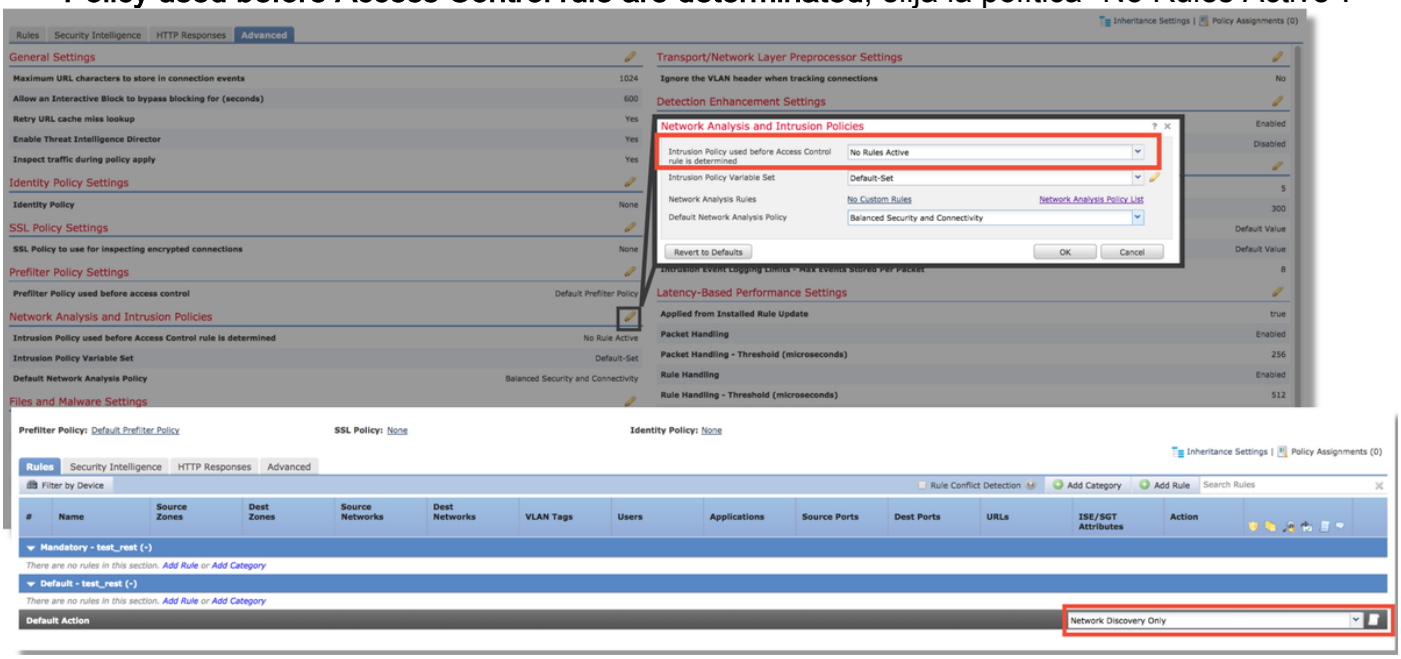
La ilustración siguiente muestra un ejemplo de uso de la herramienta de seguimiento de soporte del sistema donde el resultado mostró que un paquete fue bloqueado debido a una regla de intrusión. Esto le proporciona todos los detalles como el identificador de grupo (GID), el identificador de firma (SID), el ID de análisis de red (NAP Policy) y el ID de IPS para que pueda ver exactamente qué política/regla está bloqueando este tráfico.



Si no puede determinar que IPS está bloqueando la salida de seguimiento, pero sospecha que IPS está cayendo debido a una política de intrusiones personalizada, puede reemplazar la política de intrusiones por una política de "seguridad y conectividad equilibradas" o una política de "conectividad sobre seguridad". Estas son políticas de intrusión proporcionadas por Cisco. Si realiza ese cambio, resuelve el problema, el TAC puede solucionar los problemas de la política de intrusiones personalizada utilizada anteriormente. Si ya se utiliza una política predeterminada de Cisco, puede intentar cambiar el valor predeterminado a uno menos seguro, ya que tienen menos reglas, por lo que puede ayudar a reducir el alcance. Por ejemplo, si el tráfico se bloquea y se utiliza una política equilibrada, entonces se cambia a la conectividad a través de la política de seguridad y el problema desaparece, es probable que haya una regla en la política equilibrada que descarte el tráfico que no está configurado para disminuir la conectividad a través de la política de seguridad.

Se pueden realizar los siguientes cambios en la política de control de acceso para eliminar todas las posibilidades de bloqueo de inspección de la política de intrusiones (se recomienda realizar el menor número posible de cambios para no alterar su eficacia de seguridad, por lo que se recomienda establecer reglas de CA específicas para el tráfico en cuestión, en lugar de inhabilitar IPS en toda la política):

- En todas las reglas de control de acceso (o sólo las reglas que coinciden con el tráfico específico que se ve afectado), elimine la directiva de intrusión de la ficha Inspección
- En la pestaña Advanced, en la sección **Network Analysis and Intrusion Policies > Intrusion Policy used before Access Control rule are determinated**, elija la política "No Rules Active".



Si esto todavía no resuelve el problema, continúe con la solución de problemas de la política de análisis de red.

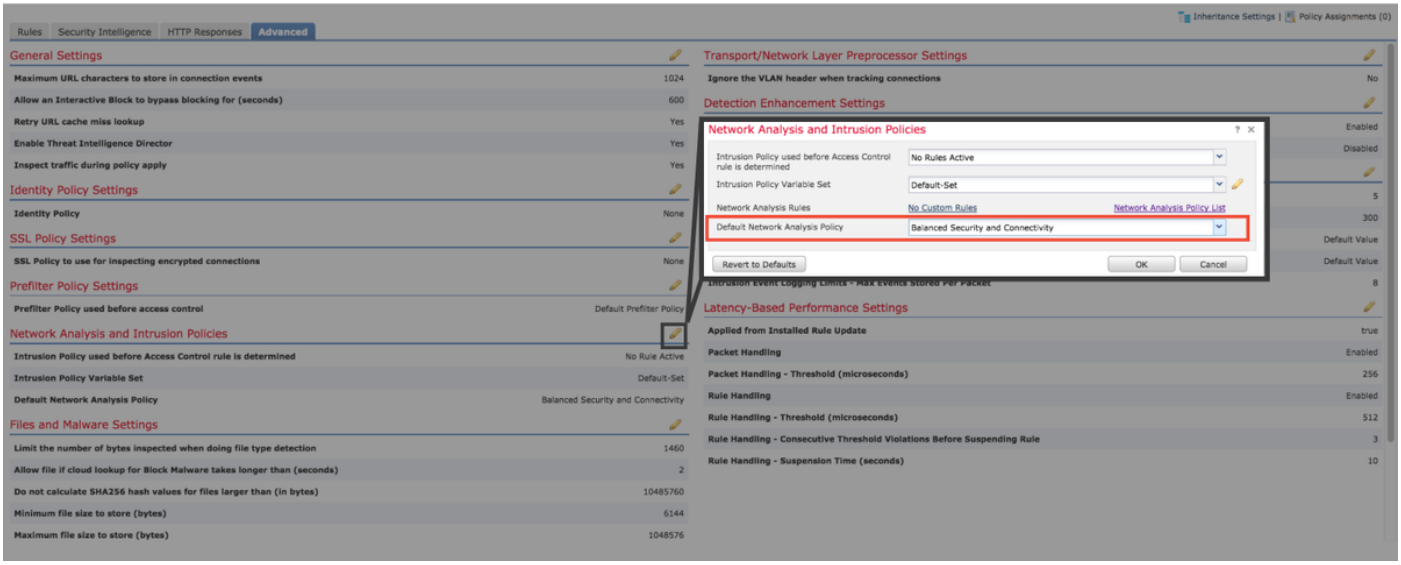
Para obtener más información acerca de la solución de problemas de la función de política de intrusiones, revise el artículo pertinente sobre la solución de problemas de la ruta de datos.

Política de análisis de red

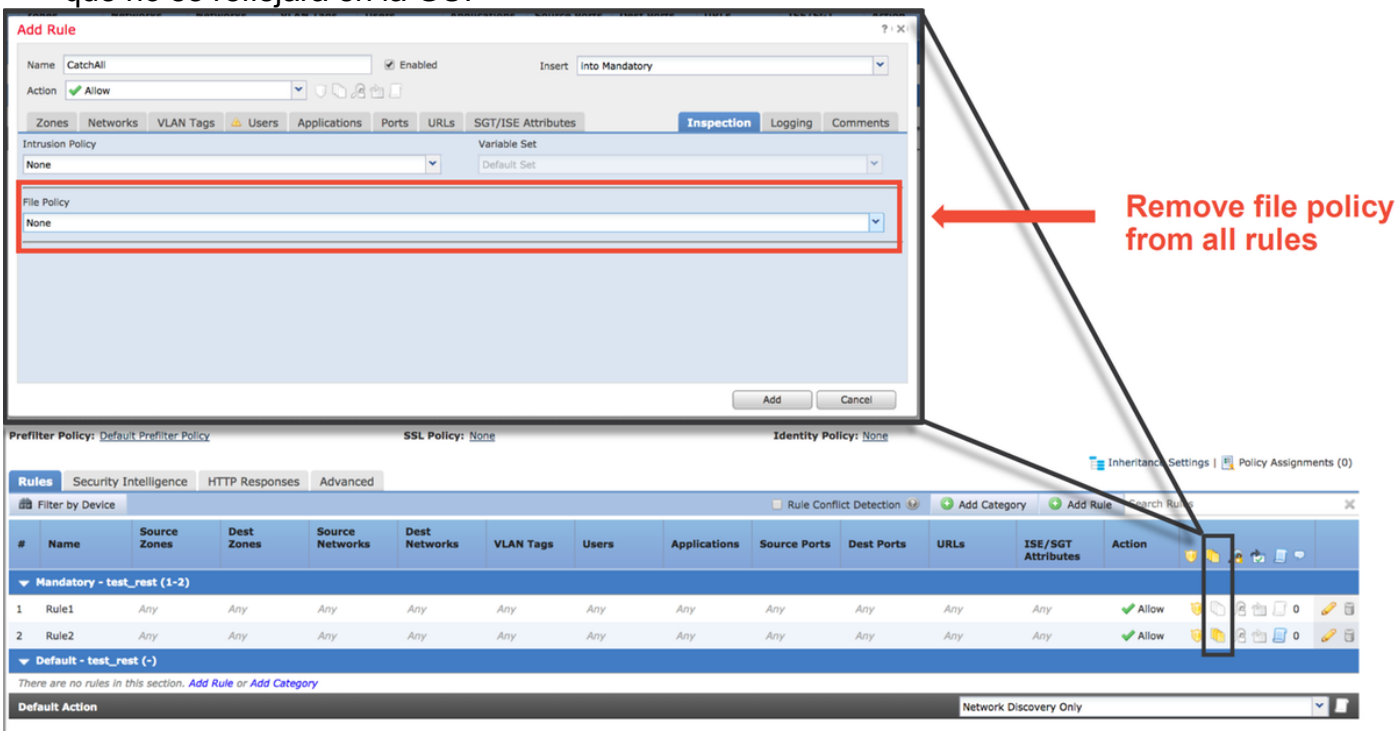
La política de análisis de red (NAP) contiene la configuración previa al procesador de Firepower, algunas de las cuales pueden descartar el tráfico. El primer paso recomendado para la resolución de problemas es el mismo que para la resolución de problemas de IPS, que es utilizar la herramienta **> system support trace** para tratar de encontrar qué en el snort está bloqueando el tráfico. Consulte la sección "Política de intrusiones" anterior para obtener más información sobre esta herramienta y ejemplos de uso.

Para mitigar rápidamente los posibles problemas con el NAP, se pueden realizar los siguientes pasos:

- Si se está utilizando un NAP personalizado, reemplácelo por una política de "Conectividad y seguridad equilibradas" o "Conectividad sobre seguridad"



- Si se está utilizando alguna "Reglas personalizadas", asegúrese de establecer el NAP en uno de los valores predeterminados mencionados anteriormente
- Si alguna regla de control de acceso utiliza una política de archivos, quítela temporalmente ya que una política de archivos puede habilitar la configuración previa al procesador en el motor que no se reflejará en la GUI



En este artículo se puede revisar la resolución de problemas más detallada de la función de política de análisis de red.

Información Relacionada

Enlaces a la documentación de Firepower

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html