Fase 4 de Troubleshooting de Trayectoria de Datos de Firepower: Política de control de acceso

Contenido

Introducción

Este artículo forma parte de una serie de artículos que explican cómo resolver sistemáticamente los problemas de la ruta de datos en sistemas Firepower para determinar si los componentes de Firepower pueden estar afectando al tráfico. Consulte el artículo Descripción general para obtener información sobre la arquitectura de las plataformas Firepower y los enlaces a otros artículos de Troubleshooting de Trayectoria de Datos.

Este artículo trata la cuarta etapa de la solución de problemas de la ruta de datos de Firepower, la política de control de acceso (ACP). Esta información es aplicable a todas las plataformas y versiones de Firepower soportadas actualmente.

Resolución de problemas de la fase de la política de control de acceso (ACP)

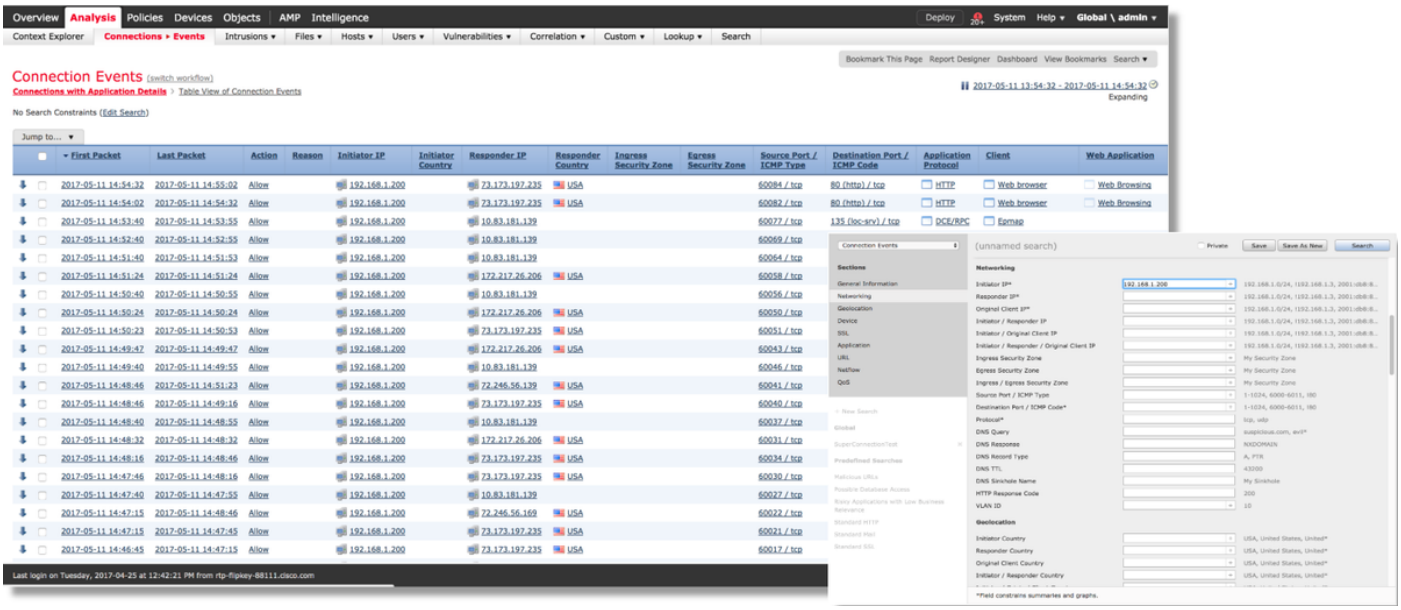
En términos generales, determinar qué regla ACP coincide con un flujo debe ser bastante directo. Los eventos de conexión se pueden revisar para ver qué regla/acción se está aplicando. Si eso no muestra claramente lo que el ACP está haciendo con el tráfico, la depuración se puede realizar en la interfaz de línea de comandos (CLI) de Firepower.

Comprobar eventos de conexión

Después de hacerse una idea de la interfaz de ingreso y egreso, el tráfico debe coincidir, así

como la información de flujo, el primer paso para identificar si Firepower está bloqueando el flujo sería verificar los Eventos de conexión para el tráfico en cuestión. Estos se pueden ver en Firepower Management Center en **Analysis > Connections > Events.**

> **Nota:** Antes de comprobar los eventos de conexión, asegúrese de que el registro esté habilitado en las reglas ACP. El registro se configura en la ficha "Registro" de cada regla de directiva de control de acceso, así como en la ficha Inteligencia de seguridad. Asegúrese de que las reglas sospechosas estén configuradas para enviar los registros al "Visor de eventos". Esto también se aplica a la acción predeterminada.



Al hacer clic en "Editar búsqueda" y filtrarse por una IP de origen (iniciador) única, puede ver los flujos que Firepower estaba detectando. La columna Acción muestra "Permitir" para el tráfico de este host.

Si Firepower bloquea el tráfico intencionalmente, la acción contendría la palabra "Block" (Bloquear). Al hacer clic en "Vista de tabla de eventos de conexión" se proporcionan más datos. Los campos siguientes de los eventos de conexión se pueden revisar si la acción es "Bloquear":

-Motivo

- Regla de control de acceso

Pasos de mitigación rápida

Con el fin de mitigar rápidamente un problema que se cree es causado por las normas ACP, se puede realizar lo siguiente:

- Cree una regla con la acción de "Confiar" o "Permitir" para el tráfico en cuestión y colóquela en la parte superior de la ACP, o sobre todas las reglas de bloqueo.
- Desactive temporalmente cualquier regla con una acción que contenga la palabra "Bloquear"
- Si la acción predeterminada está establecida en "Bloquear todo el tráfico", cambie temporalmente a "Detección de red solamente"

> **Nota:** Estas mitigaciones rápidas requieren cambios de políticas que pueden no ser posibles

en todos los entornos. Se recomienda intentar utilizar primero el seguimiento de soporte del sistema para determinar qué regla coincide el tráfico antes de realizar cambios de política.

Depuración del ACP

Se puede realizar una resolución de problemas adicional con las operaciones ACP a través de la CLI **> system support firewall-engine-debug**.

> **Nota:** En las plataformas Firepower 9300 y 4100, se puede acceder al shell en cuestión a través de los siguientes comandos:
>
> **# connect module 1 console**
> Firepower-module1**> connect ftd**
> **>**
>
> Para múltiples instancias, se puede acceder a la CLI del dispositivo lógico con los siguientes comandos.
> **# connect module 1 telnet**
> Firepower-module1**> connect ftd1**
> Conectando con la consola ftd(ftd1) del contenedor... introduzca "exit" para volver a Boot CLI
> **>**

La utilidad **system support firewall-engine-debug** tiene una entrada para cada paquete que evalúa el ACP. Muestra el proceso de evaluación de reglas que se está llevando a cabo, junto con el motivo por el que una regla coincide o no coincide.

> **Nota:** En la versión 6.2 y posteriores, se puede ejecutar la herramienta **de seguimiento de soporte del sistema**. Utiliza los mismos parámetros pero incluye más detalles. Asegúrese de ingresar 'y' cuando se le pida "**Habilitar firewall-motor-debug también?"**.

Ejemplo 1: El tráfico coincide con una regla de confianza

En el siguiente ejemplo, se evalúa el establecimiento de una sesión SSH usando **system support firewall-engine-debug**.

Este es el ACP que se está ejecutando en el dispositivo Firepower.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

La ACP tiene tres reglas.

1. La primera regla es confiar en cualquier tráfico de 192.168.0.7 con los puertos de destino utilizados por SSH.

2. La segunda regla inspecciona todo el tráfico originado en 10.0.0.0/8 en el que los criterios de red coinciden según los datos del encabezado XFF (como indica el icono junto al objeto de red)
3. La tercera regla confía en todo el tráfico desde 192.168.62.3 a 10.123.175.22

En el escenario de troubleshooting, se está analizando una conexión SSH de 192.168.62.3 a 10.123.175.22.

Se espera que la sesión coincida con la regla 3 de AC "trust server backup". La pregunta es: cuántos paquetes se necesitan para que esta sesión coincida con esta regla. ¿Se necesita toda la información necesaria en el primer paquete para determinar la regla de CA o varios paquetes y, si es así, cuántos?

En Firepower CLI, se introduce lo siguiente para ver el proceso de evaluación de reglas ACP.

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **Consejo:** Es mejor completar tantos parámetros como sea posible al ejecutar **firewall-engine-debug**, de modo que sólo se impriman en pantalla los mensajes de depuración interesantes.

En la salida de depuración que aparece a continuación, verá los primeros cuatro paquetes de la sesión que se está evaluando.

SYN

SYN,ACK

ACK

Primer paquete SSH (cliente a servidor)

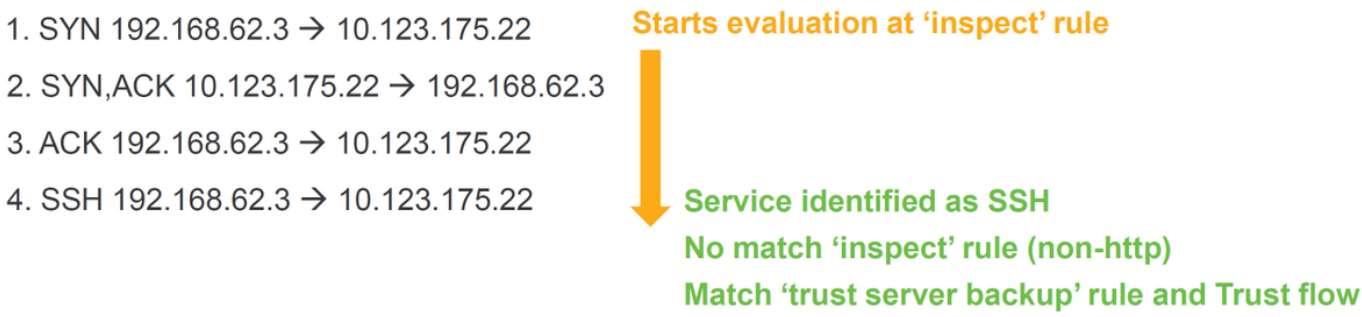
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Este es un gráfico que ilustra la lógica de depuración.



Para este flujo, se necesitan 4 paquetes para que el dispositivo coincida con la regla.

Esta es una explicación detallada del resultado de la depuración.

- El proceso de evaluación ACP comienza con la regla de "inspección" porque la regla de "confianza ssh para el host" no coincidía, ya que la dirección IP no coincidía con el requisito. Esta es una coincidencia rápida debido a toda la información necesaria para determinar si esta regla debe coincidir está presente en el primer paquete (IP y puertos)
- No se puede determinar si el tráfico coincide con la regla de "inspección" hasta que se identifique la aplicación, ya que la información de X-Forwarded-For (XFF) se encuentra en el tráfico de aplicaciones HTTP, la aplicación todavía no se conoce, por lo que la sesión pasa a un estado pendiente para la regla 2, a la espera de los datos de la aplicación.
- Una vez que la aplicación se identifica en el cuarto paquete, la regla de "inspección" produce una no coincidencia, ya que la aplicación es SSH, en lugar de HTTP
- A continuación, se compara la regla de "copia de seguridad del servidor de confianza", en función de las direcciones IP.

En resumen, la conexión toma 4 paquetes para coincidir con la sesión porque debe esperar a que el firewall identifique la aplicación, ya que la regla 2 tiene una restricción de aplicación.

Si la regla 2 sólo tenía redes de origen y no era XFF, entonces habría tomado 1 paquete para coincidir con la sesión.

Siempre que sea posible, debe colocar las reglas 1-4 por encima de todas las demás reglas de la política, ya que estas reglas normalmente requieren 1 paquete para tomar una decisión. Sin embargo, también puede notar que incluso con sólo las reglas de capas 1-4 puede que más de un paquete coincida con una regla de CA, y la razón de esto es la inteligencia de seguridad de URL/DNS. Si tiene alguno de estos dos activos habilitados, el firewall debe determinar la aplicación para todas las sesiones evaluadas por la política de CA porque debe determinar si son HTTP o DNS. A continuación, debe determinar si debe permitir la sesión basándose en las listas negras.

A continuación se muestra un resultado truncado del comando **firewall-engine-debug**, que tiene los campos relevantes resaltados en rojo. Observe el comando utilizado para obtener el nombre de la aplicación que se identifica.

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

Ejemplo 2: El tráfico que coincide con una regla de confianza está bloqueado

En algunos escenarios, el tráfico se puede bloquear a pesar de que coincida con una regla de confianza en el ACP. El siguiente ejemplo evalúa el tráfico con la misma política de control de acceso y hosts.

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

Como se ha visto anteriormente, la salida **firewall-engine-debug** muestra que el tráfico coincide con una "confianza", mientras que los eventos de conexión muestran la acción de **bloqueo** debido a una regla de política de intrusiones (determinada porque la columna Motivo muestra **Bloque de intrusiones**).

La razón por la que esto puede ocurrir se debe a la **Política de intrusiones utilizada antes de que se determine la regla de control de acceso** Configuración en la pestaña **Avanzadas** en la ACP. Antes de que el tráfico pueda ser de confianza por la acción de regla, la política de intrusión en cuestión identifica una coincidencia de patrón y descarta el tráfico. Sin embargo, la evaluación de reglas ACP da como resultado una coincidencia de la regla de confianza, ya que las direcciones IP coincidían con los criterios de la regla de "copia de seguridad del servidor de confianza".

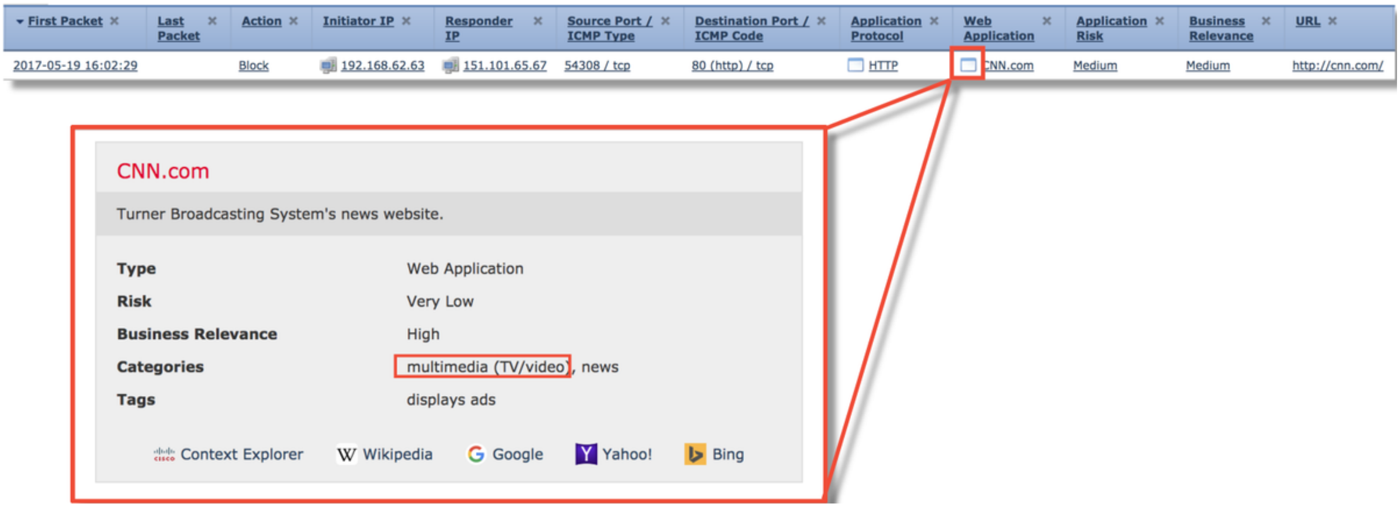
Para que el tráfico no se someta a la inspección de la política de intrusiones, la regla de confianza se puede colocar por encima de la regla de "inspección", que sería una práctica recomendada en cualquier caso. Dado que la identificación de la aplicación es necesaria para una coincidencia y no coincidencia de la regla de "inspección", la **política de intrusión utilizada antes de determinar la regla de control de acceso** se utiliza para el tráfico que se evalúa de la misma manera. Si se coloca la regla de "copia de seguridad del servidor de confianza" sobre la regla de "inspección", el tráfico coincidirá con la regla cuando se vea el primer paquete, ya que la regla se basa en la

dirección IP, que se puede determinar en el primer paquete. Por lo tanto, la **política de intrusiones utilizada antes de determinar la regla de control de acceso** no necesita ser utilizada.

Escenario 3: Tráfico bloqueado por la etiqueta de la aplicación

En este escenario, los usuarios informan que cnn.com está siendo bloqueado. Sin embargo, no hay una regla específica que bloquee CNN. Los eventos de conexión, junto con el resultado **firewall-engine-debug**, muestran la razón del bloqueo.

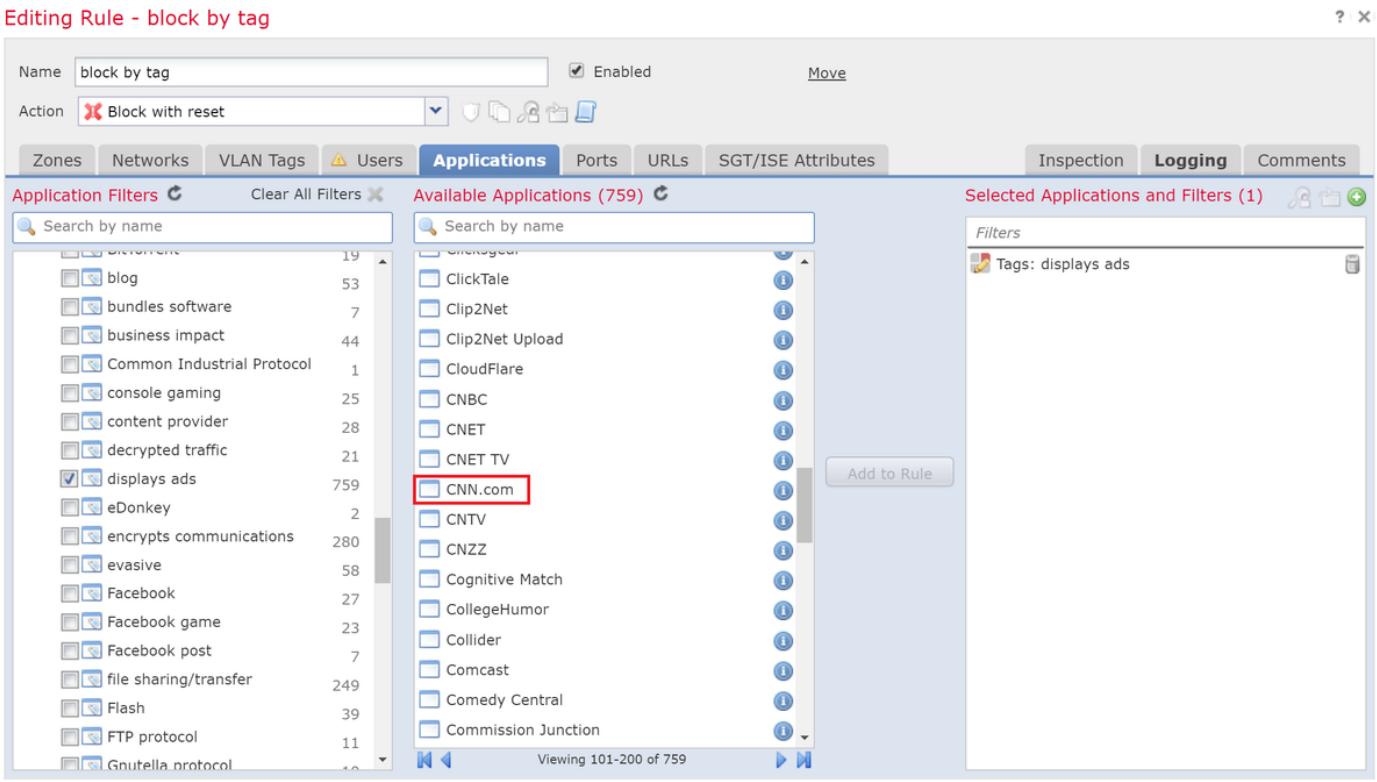
En primer lugar, los eventos de conexión tienen un cuadro de información junto a los campos de la aplicación que muestra información sobre la aplicación, así como la forma en que Firepower clasifica dicha aplicación.



Con esta información en mente, se ejecuta **firewall-engine-debug**. En el resultado de la depuración, el tráfico se bloquea en función de la etiqueta de la aplicación.

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

Aunque no hay una regla que bloquee explícitamente http://cnn.com, la **visualización de anuncios** etiquetados se bloquea dentro de la pestaña **Aplicaciones** de una regla ACP.



Datos que se deben proporcionar al TAC

Datos	Instrucciones
Solución de problemas de archivo del dispositivo Firepower que inspecciona el tráfico	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1176
system support firewall-engine-debug and **system-support-trace** output	Consulte este artículo para obtener instrucciones
Exportación de la política de control de acceso	Vaya a **System > Tools > Import / Export**, seleccione la política de control de acces

> **Precaución:** Si el ACP contiene una política SSL, elimine la política SSL del ACP antes de exportar para evitar la divulgación de información PKI sensible

Siguiente paso: Solución de problemas de la capa de política SSL

Si una política SSL está en uso y la resolución de problemas de la política de control de acceso no reveló el problema, el siguiente paso sería resolver el problema de la política SSL.