Impacto de la inspección de la capa 7 en el tráfico de varias capas: Revisión de la implementación de Snort3

Contenido

Problema

Después de habilitar las reglas DNS Sinkhole en una política de control de acceso (ACP), el tráfico VXLAN encapsulado comenzó a descartarse de forma inesperada en los dispositivos Firepower Threat Defence (FTD) que ejecutan versiones de motor Snort 3.

· El tráfico encapsulado VXLAN descarta después de habilitar la política DNS Sinkhole.

· Eventos de conexión que muestran direcciones IP internas (por ejemplo, 100.70.x.x) en lugar de encabezados VXLAN externos.

· Se ha detectado un comportamiento inesperado con la implementación de Snort 3 durante las pruebas de laboratorio.

Entorno

•Plataforma: Par de alta disponibilidad (HA) de FTD

· Versión afectada: 7.6.2.1 (Snort 3)

· Versión fija: 7.6.4+ (Snort 3)

Resolución

Solución en 7.6.2.1:

###############

Paso 1:

Política de filtrado previo (recomendado)

Cree una regla de filtro previo para omitir la inspección de Snort para el tráfico VXLAN:

· Política de filtrado previo

•Acción: Fastpath (regla de túnel)

•Fuente: <Outer_VXLAN_Source_IPs>

•Destino: <Outer_VXLAN_Destination_IPs>

•Protocolo: UDP

•Puerto: 4789

Paso 2:

Borrar conexiones existentes

· clear conn address <outer_ip_1> address <outer_ip_2>

Ajustar el orden de las reglas si no se utiliza la directiva de filtros previos

Coloque las reglas L7 (DNS Sinkhole, App-ID) por delante de las reglas de permisos de IP internas en el ACP.

Solución a largo plazo:

###############

1. Actualización a FTD 7.6.4 o posterior

· Resuelve CSCwo54753 (DEFECTO PSIRT)

· Proporciona un comportamiento uniforme de inspección multicapa.

2. Configure las reglas internas y externas para DNS Sinkhole:

· Cuando utilice DNS Sinkhole u otras funciones de inteligencia de seguridad con tráfico encapsulado.

3. Para funciones que no sean de SI de capa 7 (filtrado de URL, control de aplicaciones):

· Solo se requieren reglas de encabezado interno en ACP.

· Las reglas de cabecera externa no son necesarias.

Más detalles sobre la función de inspección de VXLAN multicapa

##

FTD incluye una capacidad de inspección multicapa para las funciones de inteligencia de seguridad (SI) y capa 7. Esta función determina si Snort inspecciona los encabezados de encapsulación externa o los encabezados de carga útil internos en función de las políticas de capa 7 configuradas.

Las Funciones De Capa 7 Incluyen:

· Sumidero DNS

· Control de aplicaciones (App-ID)

•Filtrado de URL

· Geolocalización

· Prevención de intrusiones

Comportamiento clave:

##########

Cuando se habilita cualquier función de Capa 7 en el ACP, Snort pasa a inspeccionar los encabezados más internos de los paquetes encapsulados (por ejemplo, VXLAN, GRE, IP en IP).

Análisis técnico:
###############
Snort 3 (7.6.2.1): comportamiento defectuoso

Sin reglas de capa 7:

· Snort se basa en los metadatos de conexión de Lina (motor de ruta de datos ASA).

· El tráfico está permitido/denegado según las reglas del encabezado externo solamente.

· La inspección interna del encabezado no se realiza.

Con reglas de capa 7:

· Snort realiza controles ACP y aplica la inspección multicapa.

· Cuestiones de orden normativo (defecto en Snort 3).

· Si la regla de IP interna aparece antes que la regla L7 → caída de tráfico Vxlan —>
Comportamiento defectuoso

Salida de LAB:
LAB FTD — 7.6.2.1 — snort3 — Regla de ACP de IP interna seguida de la regla L7 — Abandono

Detalles de Lab Packet Tracer:

17:46:48.773778 10.142.133.15:36066 > 10.126.133.15:4789 udp 80

Interior (vrfid:0)

BÚSQUEDA_DE_GRUPO_DE_OBJETOS

MODO NGIPS

| ngips-mode

ACCESS-LIST

NGIPS-EGRESS-INTERFACE-LOOKUP

| Resolver interfaz de salida

CREACIÓN DE FLUJO

EXTERNAL-INSPECT

SNORT

Tipo:

SNORT

Resultado:

DEJAR CAER

Config:

Tiempo transcurrido:

814472 ns

Additional Information

Resultado: dejar caer

Interfaz de Entrada:

Interior (vrfid:0)

Estado de entrada:

en funcionamiento

Estado de línea de entrada:

en funcionamiento

Interfaz de salida:

Exterior (vrfid:0)

Estado de salida:

en funcionamiento

Estado de línea de salida:

en funcionamiento

Acción:

dejar caer

Tiempo empleado:

928908 ns

Motivo del descarte:

(firewall) Bloqueado por el preprocesador del firewall <— MOTIVO DEL RECHAZO

Abandonar detalle:

Ubicación de destino: frame inspect_dp_snort_snp_drop_frame_wcaller:58 flow (NA)/NA

Exterior (vrfid:0)

· Si la regla L7 aparece antes que la regla IP interna → Se permite el tráfico Vxlan

Comportamiento específico de DNS Snort 3:

· DNS Sinkhole activa la inspección multicapa incluso cuando la ordenación de reglas permitiría el tráfico.

Snort 3 (7.6.4+): comportamiento fijo

Post-corrección (CSCwo54753):

· La inspección multicapa se habilita de forma consistente cuando hay funciones L7 presentes.

· El orden de las reglas no afecta el comportamiento.

· La inspección del tráfico se basa en los encabezados más internos, independientemente de la posición de la regla.

· Se deben permitir los encabezados internos y externos en el ACP para los escenarios de DNS Sinkhole.

Matriz de comparación de casos de prueba

Escenario de prueba	FTD 7.6.2.1 (Snort 3)	FTD 7.6.4+ (Snort 3)	Comportamiento esperado
Regla L7 seguida de Regla IP interna	PERMITIDO	PERMITIDO	Tráfico permitido
Regla de IP interna seguida de regla L7	Descartado (Defecto)	PERMITIDO	Tráfico permitido
Sólo regla de IP interna (no L7)	Bloqueado	Bloqueado	Bloqueado (sin permiso interno)
Sólo regla de IP externa (no L7)	PERMITIDO	Bloqueado	Snort 3 inspecciona el encabezado más interno

Sólo IP externa + DNS sinkhole	Bloqueado	Bloqueado	Regla L7 que aplica la inspección interna
Sólo IP interna + DNS sinkhole	Bloqueado	Bloqueado	Regla L7 que aplica la inspección interna

Causa

Este comportamiento se debe a la capacidad de inspección multicapa de Snort 3 para las funciones de inteligencia de seguridad. Cuando DNS Sinkhole (parte de la inteligencia de seguridad) está habilitado, Snort 3 realiza una inspección profunda de paquetes que detecta y evalúa las direcciones IP más internas dentro de los paquetes encapsulados, independientemente de la capa de transporte.

El problema se documenta en el Id. de bug Cisco CSCwt12564, que establece: "Si utiliza una condición L7 (filtrado de url, id de aplicación, geolocalización, etc.) en la regla o una función de inteligencia de seguridad en el ACP, necesita una regla ACP con encabezado interno para que las reglas coincidan. Con el sinkhole de DNS, que forma parte de la política de DNS en SI, se requieren tanto el encabezado interno como el externo en un ACP para que las reglas coincidan".

Este comportamiento difiere del funcionamiento normal, en el que sólo se evalúan los encabezados exteriores para el tráfico VXLAN de tránsito cuando no se configuran funciones de inteligencia de seguridad o capa 7.

Contenido relacionado

- Guía de configuración de Snort 3
- Soporte técnico y descargas de Cisco
- ID de bug de Cisco CSCwt12564
- ID de bug de Cisco CSCwt07320
- ID de bug de Cisco CSCwu75396
- ID de bug de Cisco CSCwt58320

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).