Descripción de DNS Guard en Secure Firewall 7.7.0

Contenido

Introducción

Este documento describe la función DNS Guard en Secure Firewall 7.7.0, centrándose en su funcionalidad y en la resolución de problemas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Información sobre el protocolo DNS y las sesiones UDP
- Familiaridad con Snort 3 y su gestión de sesiones

Componentes Utilizados

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

- Secure Firewall Threat Defence (FTD) versión 7.7.0
- Firepower Management Center (FMC) versión 7.7.0

- Snort versión 3

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.

Antecedentes

DNS es un protocolo UDP basado en solicitud y respuesta con sesiones de corta duración. A diferencia de Lina, las sesiones DNS de Snort 3 no se borran inmediatamente después de la respuesta DNS. En su lugar, las sesiones DNS se recortan en función de un tiempo de espera de flujo de 120 segundos o más. Esto lleva a una acumulación de sesiones innecesaria, que de otro modo se podría utilizar para otras conexiones TCP o UDP.

Comparación con la versión anterior

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• The DNS session remains as a stale Snort 3 flow until it is pruned by the UDP timeout.		• DNS sessions in Snort 3 are released immediately after the DNS Response is inspected and handled.

Nueva función en 7.7

Características nuevas

- Esta función "DNS Guard" borra el flujo UDP inmediatamente después de recibir e inspeccionar el paquete de respuesta DNS.
- Se trata de una mejora específica del protocolo con respecto al diseño y la arquitectura actuales de Snort 3.

Conceptos básicos: Plataformas admitidas, licencias

Directores y plataformas de FTD

FTD Platforms	All
FMC on 7.7.0 FMC Rest API	Yes No
FTD Supported Versions *(lowest version FMC on 7.7.0 can manage is 7.2)*	7.7.0 only
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3

Plataformas Soportadas

Otros aspectos de soporte

FTD	
Licenses Required	Essentials, URL, Threat, Malware
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes

Licencias y compatibilidad

Problema

En las versiones anteriores, en concreto Secure Firewall 7.6 y versiones posteriores, la sesión DNS permanece como un flujo Snort 3 obsoleto hasta que se elimina por el tiempo de espera UDP. Esto causa problemas con la administración de sesiones y podría dar lugar a un uso ineficiente de los recursos, ya que las sesiones DNS se acumulan innecesariamente.

Pasos para recrear el problema

Para observar el problema, ejecute el comando Line para verificar las conexiones DNS activas desde el lado Line:

```
show conn detail
```

En Secure Firewall 7.6 y versiones posteriores, las sesiones DNS permanecen activas hasta que se agota el tiempo de espera de UDP, lo que provoca la ineficacia de los recursos.

Solución

La función DNS Guard de Secure Firewall 7.7.0 soluciona este problema borrando inmediatamente el flujo UDP después de recibir e inspeccionar el paquete de respuesta DNS. Esta mejora específica del protocolo garantiza que las sesiones DNS de Snort 3 se liberan inmediatamente, lo que evita la acumulación innecesaria de sesiones y mejora la eficacia de los recursos.

Descripción general de características

La función DNS Guard borra el flujo UDP inmediatamente después de recibir e inspeccionar el paquete de respuesta DNS. El flujo de Snort no necesita esperar hasta que se produzca el tiempo de espera UDP.

- Cuando hay suficiente tráfico DNS en la caja, esta función conduce a menos flujos activos debido a la limpieza oportuna de los flujos Snort correspondientes.
- El cuadro puede administrar más conexiones TCP/UDP sin recortar las conexiones activas, lo que mejora la eficacia general del cuadro.

Resolución de problemas

Para verificar la funcionalidad de la función DNS Guard, utilice el comando Line para asegurarse de que las sesiones UDP se liberan al recibir una respuesta DNS:

<#root>

>

show snort counters | begin stream_udp

Ejemplo de salida sin función de protección DNS:

```
stream_udp sessions: 755
 max: 12
created: 755
released: 0
total_bytes: 124821
```

<#root>

>

```
show snort counters | begin stream_udp
```

Ejemplo de salida con función de protección DNS:

```
stream_udp sessions: 899
max: 14
created: 899
released: 899
total_bytes: 135671
```

Los resultados indican que todas las sesiones creadas se liberan a tiempo, lo que confirma el funcionamiento correcto de la función DNS Guard.

Información Relacionada

- Soporte técnico y descargas de Cisco

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).