Modo de seguimiento de la sesión TCP en línea en el IPS

Contenido

Introducción

Este documento describe la característica de seguimiento en línea de la sesión TCP del dispositivo del Sistema de prevención de intrusiones (IPS).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivos de las 4200 Series IPS configurados con las interfaces en línea.
- Conocimiento del protocolo TCP y de los flujos de tráfico.

Componentes Utilizados

La información en este documento se basa encendido:

- IPS 4270 con el Software Release 7.1(7)

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Antecedentes

En ciertos escenarios de instrumentación en línea IPS, los paquetes de una secuencia TCP se pueden ver dos veces por el motor del normalizador, que da lugar a los descensos debido al seguimiento incorrecto de la secuencia. Esta situación se considera típicamente cuando el tráfico se rutea con las redes de área local virtuales múltiples (VLA N) o los pares de la interfaz que son monitoreados por un solo sensor virtual. Este problema es complicado más a fondo por la necesidad para permitir que el tráfico asimétrico se combine para la secuencia apropiada que sigue cuando el tráfico para cualquier dirección se recibe de los diversos VLA N o interfaces.

Diagrama de la red

Problema

En esta topología de red, un cliente en la red interna inicia una conexión HTTP al servidor en la red externa. Ambos segmentos de red son separados por un Firewall adaptante del dispositivo de seguridad (ASA). En este diseño, un solo dispositivo IPS se configura para golpear ligeramente en ambos los VLA N interiores y exteriores con dos conjuntos de los pares en línea de la interfaz. Cuando el cliente inicia la sesión al servidor, el paquete TCP SYN (sincronice) toma esta trayectoria (secuencia saliente) con el IPS y el ASA:

Cliente > IPS G3/0 > *vs0* > IPS G3/1 > ASA G0/0 > ASA G0/1 > IPS G3/2 > *vs0* > IPS G3/3 > servidor

Después de la secuencia saliente, el TCP SYN enviado por el cliente es visto por el sensor virtual **vs0** mientras que el paquete atraviesa los pares de la interfaz interior hacia la interfaz interior ASA y otra vez cuando el paquete atraviesa los pares de la interfaz exterior hacia el servidor Web. En un escenario simétrico, la misma situación ocurre en el trayecto de retorno con el SYN ACK (un reconocimiento positivo) y paquetes subsiguientes del servidor Web. Cuando el IPS intenta combinar las secuencias en una sola conexión TCP, los duplicados de cada paquete en la conexión se observan, que da lugar a un normalizador confuso y a los paquetes perdidos. Para confirmar si un IPS encuentra esta situación, la salida del comando del **virt stat de la demostración** muestra un gran número de 1330 firmas del normalizador TCP que fuego, así como un gran número de paquetes y de conexiones modificados y negados.

Solución

La opción de modo de seguimiento de la sesión TCP en línea se puede utilizar para superar las situaciones tales como esto. Hay tres modos posibles que pueden ser configurados:

1. **Sensor virtual (configuración predeterminada)** - Monitorea en una situación asimétrica del despliegue donde los paquetes del cliente se ven en un par en línea, mientras que los paquetes del servidor se ven en un segundo par de la interfaz. Los dos pares de la interfaz se deben monitorear juntos para considerar los ambos lados de la conexión.
2. **Interfaz y VLA N** - Esto es una solución alternativa al ejemplo de topología mostrado en este documento, en el cual pares dos o más en línea de la interfaz se asignan al mismo sensor virtual. Con esta opción habilitada, una conexión TCP puede atravesar más de un par, que permite que el normalizador siga a las sesiones TCP independientemente para cada par en línea.
3. **VLA N solamente** - Ésta es una combinación muy rara de las primeras dos opciones y se utiliza le monitor las redes asimétricas a la suma de múltiples. **El VLAN1** en los pares izquierdos de la interfaz tiene paquetes del cliente y se debe combinar con el **VLAN1** en el par correcto de la interfaz, que tiene los paquetes del servidor. En este caso, el tráfico se agrega a través de todos los pares de la interfaz, pero es segregado por el VLA N. Por ejemplo, los paquetes del VLAN1 a través de todas las interfaces se colocan juntos; Los paquetes VLAN2 de todas las interfaces se colocan juntos, pero el VLAN1 y los paquetes VLAN2 nunca se colocan juntos para el seguimiento de la sesión TCP.

Para el ejemplo de topología antedicho, hay dos maneras que el problema puede ser resuelto:

Solución 1

Trasládese cada par en línea de la interfaz a su propio sensor virtual. Por ejemplo, un par en **vs0** y un par en **vs1**. Este método se recomienda generalmente cuando hay menos de cuatro pares en línea (debido al límite de la plataforma de cuatro sensores virtuales). El normalizador trata las secuencias duplicados como dos otras conexiones.

Solución 2

Configure el modo de seguimiento de la sesión TCP en línea **para interconectar y el VLA N**. Se recomienda este método cuando hay más de cuatro pares en línea, en este caso, le fuerzan a poner los pares en línea múltiples en un solo sensor virtual. El normalizador trata los paquetes en diversos pares en línea como conexiones totalmente diversas dentro del mismo sensor virtual.

Configurar

Aquí está la configuración para separar el sensor virtual por los pares en línea de la interfaz:

```
IPS4510-01# conf t

IPS4510-01(config)# service analysis-engine
```

```
IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Inside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# virtual-sensor vs1

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Outside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

IPS4510-01(config)# exit
```

Aquí está la configuración para la interfaz y el VLA N:

```
IPS4510-01# config t

IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# inline-tcp-session interface-and-vlan

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

Apply Changes?[yes]: yes

Warning: Change of TCP session tracking mode will not take effect until restart.

IPS4510-01(config)# exit

IPS4510-01# reset
```

Verificación

- Utilice el **virt stat de la demostración | comando statistics** y estudio de la **etapa del normalizador b TCP** para **caído**, el **duplicado**, **negado**, o los **paquetes de SendAck envió las** estadísticas no-cero en el normalizador TCP.
- Utilice el **virt stat de la demostración | comando count** y estudio de **SigEvent de la Por-firma b** para 1330 firmas que han encendido conjuntamente con las estadísticas TCP Normalier del comando anterior.

Información Relacionada

- Guía de configuración CLI del sensor de Cisco Intrusion Prevention System para IPS 7.0 - modo de seguimiento de la sesión TCP en línea
- Guía de configuración expresa del administrador del Cisco Intrusion Prevention System para IPS 7.1 - modo de seguimiento de la sesión TCP en línea
- Soporte Técnico y Documentación - Cisco Systems