Contenido

Introducción

Este documento explica cuáles es el resumen del evento del Sistema de prevención de intrusiones (IPS) y cuáles son las razones para los IP Addresses que aparecen como 0.0.0.0:0 en los eventos de la firma IPS.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- La firma del IPS de Cisco alerta la configuración
- Configuración de resumen del evento IPS

> Nota: Vea los ejemplos de la configuración de resumen IPS para los ejemplos de la configuración de resumen del evento.

Componentes Utilizados

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

- Dispositivo de seguridad adaptante (ASA) 5500 o módulos 5500x IPS
- IPS 4200, 4300, o dispositivos IPS de las 4500 Series
- Módulo de red aumentado (NME) - Módulo ips
- IPS de software 7.x

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.

Antecedentes

El resumen del evento IPS es un método usado para agregar los eventos múltiples en una sola alerta. Esto da lugar a una reducción del volumen de alertas procesado y enviado por el sensor.

Problema

Los eventos generados en el IPS muestran la dirección IP del atacante/de la víctima como 0.0.0.0:0.

Solución

Cuando el IPS genera las alertas de la firma, proporciona la información tal como ID de la firma, grupo fecha/hora, dirección IP del atacante/de la víctima, y así sucesivamente. Bajo ciertas condiciones, los eventos generados muestran la dirección IP del atacante/de la víctima visualizados como 0.0.0.0:0. La razón detrás de los IP Addresses visualizados como 0.0.0.0:0 es resumen. Para configurar el resumen, para agregar una nueva firma de encargo o para editar una firma actual y para seleccionar la **frecuencia alerta > modo sumario**.

Las opciones disponibles del resumen son:

- Fuego-todo - enciende una alerta cada vez que se acciona una firma.
- Fuego-una vez que - enciende una alerta para un conjunto del direccionamiento.
- Resuma - enciende una alerta la primera vez que se acciona una firma. Las alertas adicionales para esa firma se resumen para la duración del intervalo sumario.
- Global-resumen - enciende una alerta para cada intervalo sumario.

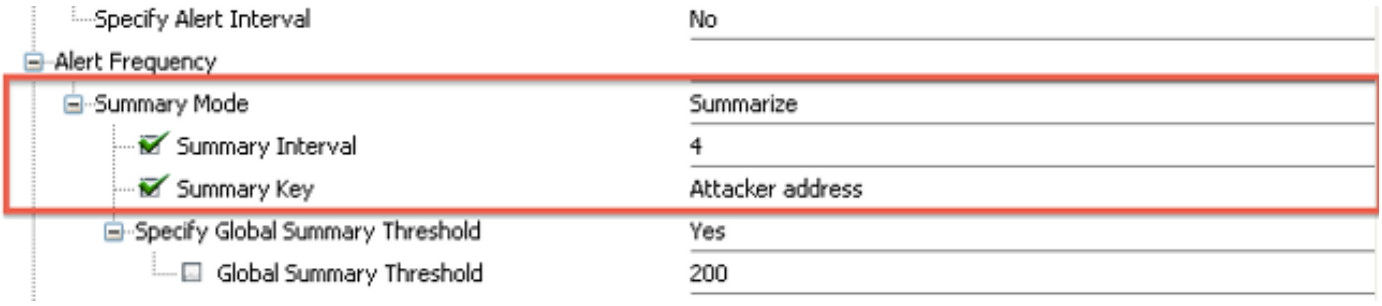
¿Cuál es la diferencia entre la clave sumaria y el umbral sumario global?

La clave sumaria es una clave usada por el IPS para concluir cómo crear un evento sumario. Por abandono, éste es un direccionamiento del atacante que significa eso si usted tiene un atacante que accione cualquier firma, un evento regular y se genera un resumen. Si usted tiene dos atacantes, dos eventos regulares y dos sumarios se generan para el intervalo sumario configurado. Si usted fija la clave sumaria al direccionamiento de la víctima y usted tiene dos atacantes que apunten a una víctima, después dos atacantes registrarán solamente un evento regular y un sumario.

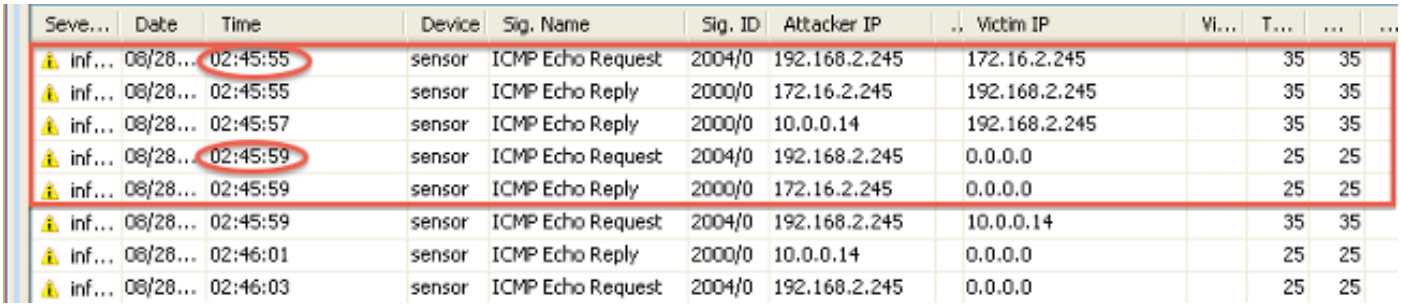
El modo sumario tiene dos opciones; Clave sumaria del intervalo y del resumen. El intervalo sumario se representa en los segundos y enciende para cada intervalo sumario. La clave sumaria es un criterio por el cual el IPS decide sobre cómo crear el evento sumario. Por abandono, éste es el direccionamiento del atacante. Las opciones dominantes sumarias disponibles incluyen:

- Direccionamiento del atacante (valor por defecto)
- Direccionamiento del atacante y puerto de la víctima

- Direccionamientos del atacante y de la víctima
- Atacante y direccionamientos y puertos de la víctima
- Direccionamiento de la víctima



El ejemplo anterior muestra una firma resumido con un intervalo sumario de 4 y la clave sumaria como direccionamiento del atacante. En este escenario, la firma enciende un evento normal la primera vez después de lo cual señala la firma se resume para un intervalo de 4 segundos.



Seve...	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Vi...	T...	...	...
inf...	08/28...	02:45:55	sensor	ICMP Echo Request	2004/0	192.168.2.245	172.16.2.245		35	35	
inf...	08/28...	02:45:55	sensor	ICMP Echo Reply	2000/0	172.16.2.245	192.168.2.245		35	35	
inf...	08/28...	02:45:57	sensor	ICMP Echo Reply	2000/0	10.0.0.14	192.168.2.245		35	35	
inf...	08/28...	02:45:59	sensor	ICMP Echo Request	2004/0	192.168.2.245	0.0.0.0		25	25	
inf...	08/28...	02:45:59	sensor	ICMP Echo Reply	2000/0	172.16.2.245	0.0.0.0		25	25	
inf...	08/28...	02:45:59	sensor	ICMP Echo Request	2004/0	192.168.2.245	10.0.0.14		35	35	
inf...	08/28...	02:46:01	sensor	ICMP Echo Reply	2000/0	10.0.0.14	0.0.0.0		25	25	
inf...	08/28...	02:46:03	sensor	ICMP Echo Request	2004/0	192.168.2.245	0.0.0.0		25	25	

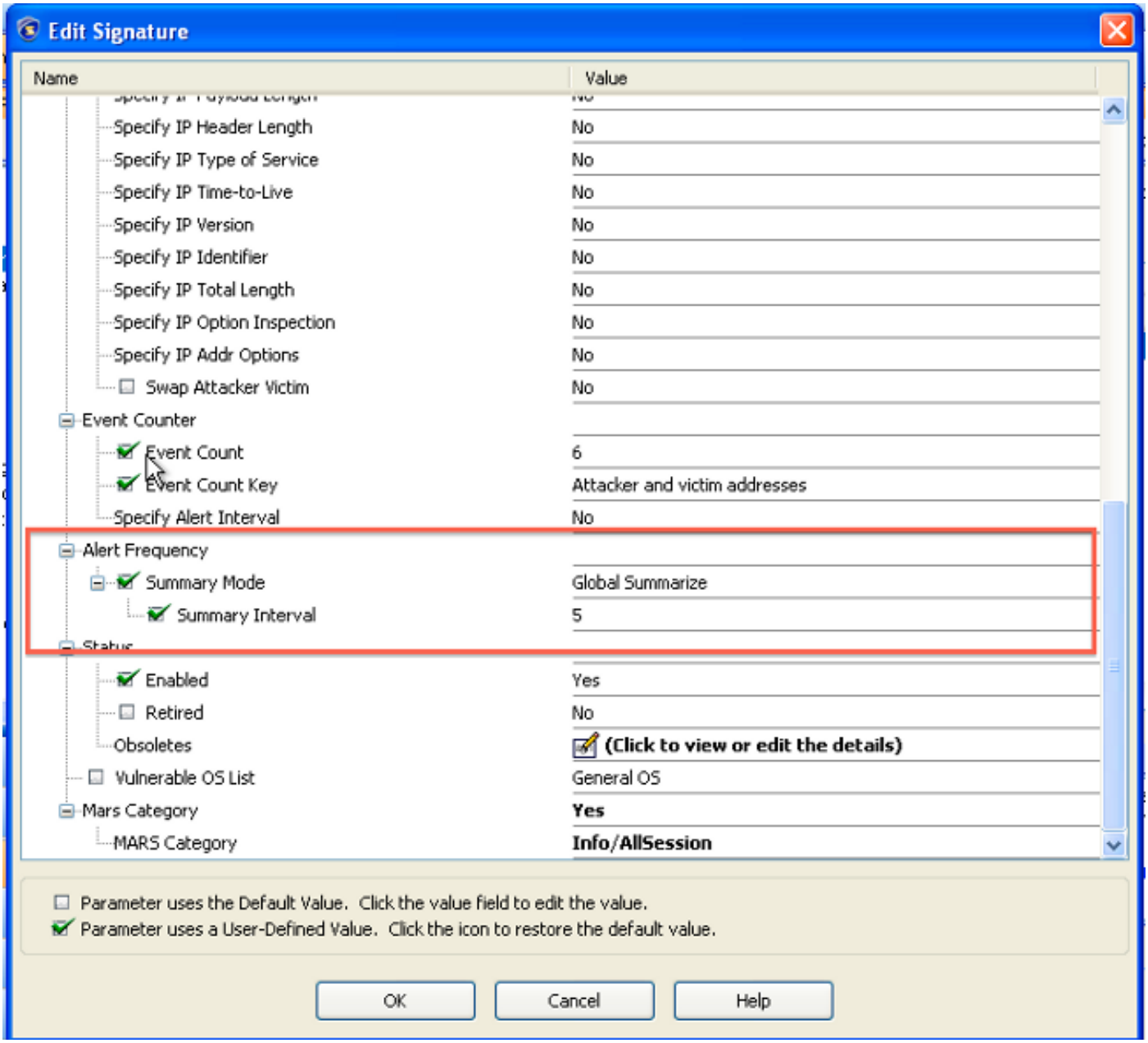
Umbral sumario global - si el resumen global no se especifica y si hay dos IP Addresses del atacante vistos, el IPS registra dos eventos normales. Después de un período de intervalo sumario, se generan dos eventos resumidos adicionales, uno para cada dirección IP del atacante. En el total, usted hizo 4 eventos registrar dentro del intervalo especificado.

Con el resumen global habilitado con un umbral sumario global de diga, dos, y si usted relanza el ejemplo anterior, después el IPS registra TRES eventos: dos para los golpes iniciales para cada direccionamiento del atacante y uno resumieron el evento para todos los atacantes (dos en este caso) dentro del intervalo especificado. Ahora si usted escalara encima del número de atacantes y de golpes, usted vería que un resumen global guarda para arriba muchos eventos/registros y así los ciclos de procesador.

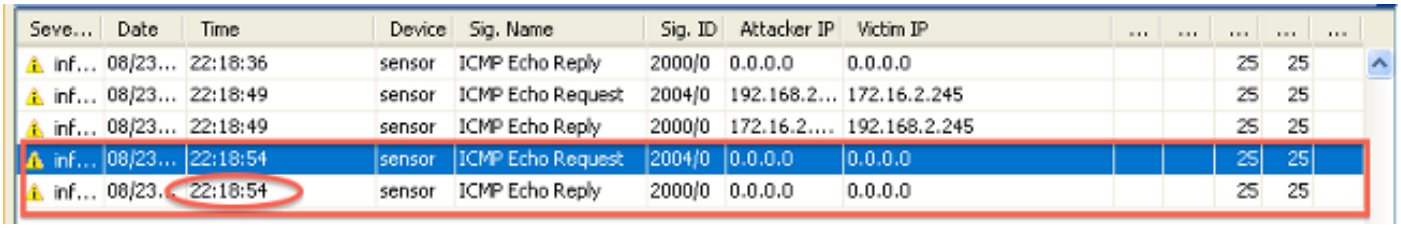
El resumen global tiene solamente un submarino option que sea el “intervalo sumario” que se configura en los segundos. Cuando la firma se fija a global-summarizarion, enciende para cada intervalo sumario. Es decir, si el intervalo sumario se fija al '5', enciende una alerta la primera vez que se acciona la firma y enciende después de eso para cada intervalo sumario de 5 segundos.

Para editar una firma, una **configuración** selecta **> las directivas > firma activa** y después buscar para la firma relevante.

Por ejemplo, el SIG ID para la “petición ICMP” es 2004. Haga clic con el botón derecho del ratón la firma y selecto **edite** para conseguir al cuadro de diálogo mostrado aquí:



En el snippet de la configuración previa, el modo sumario se ha fijado a “global resume” con un intervalo sumario de 5 segundos.



Seve...	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	...	...	...	...	...
inf...	08/23...	22:18:36	sensor	ICMP Echo Reply	2000/0	0.0.0.0	0.0.0.0			25	25	
inf...	08/23...	22:18:49	sensor	ICMP Echo Request	2004/0	192.168.2...	172.16.2.245			25	25	
inf...	08/23...	22:18:49	sensor	ICMP Echo Reply	2000/0	172.16.2....	192.168.2.245			25	25	
inf...	08/23...	22:18:54	sensor	ICMP Echo Request	2004/0	0.0.0.0	0.0.0.0			25	25	
inf...	08/23...	22:18:54	sensor	ICMP Echo Reply	2000/0	0.0.0.0	0.0.0.0			25	25	

La muestra de alertas muestra las firmas “pedido de eco ICMP” y la “respuesta de eco ICMP”, que se han resumido y por lo tanto visualizan los IP Addresses del atacante/de la víctima como '0.0.0.0'.

No confunda los eventos globales del resumen con los “eventos de la firma 1102.0 (paquete del IP imposible)”. Los hackers pudieron intentar evadir un IPS con el uso de todos los ceros para los IP Address de origen/destino y virar hacia el lado de babor que podrían accionar esta firma, que pudo parecer un evento resumido.

Información Relacionada

- Preguntas frecuentes de las firmas del Cisco Intrusion Prevention System
- Guía de configuración CLI del sensor de Cisco Intrusion Prevention System para IPS 7.1
- Ejemplos de la configuración de resumen IPS
- Soporte Técnico y Documentación - Cisco Systems