目录

简介

本文解释什么入侵防御系统(IPS)事件汇总是，并且什么原因是为出现作为0.0.0.0:0在IPS签名事件的IP地址。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科IPS签名警告配置
- IPS事件汇总配置

注意：参见IPS汇总配置示例关于事件汇总配置示例。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 可适应安全工具(ASA) 5500或5500x IPS模块
- IPS 4200， 4300或者4500系列IPS设备
- 改进的网络模块(NME) - IPS模块
- IPS 7.x软件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

IPS事件汇总是使用的方法聚集多个事件到单个警报。这导致音量的减少传感器处理和发送的警报。

问题

在IPS生成的事件显示攻击者/受害者的IP地址作为0.0.0.0:0。

解决方案

当IPS生成签名警报时，提供信息例如签名ID，时间戳，攻击者/受害者的IP地址，等等。在一定条件下，生成的事件显示作为0.0.0.0:0/受害者的显示的IP地址攻击者。在作为0.0.0.0:0显示的IP地址后的原因是汇总。为了配置汇总，添加一个新的自定义签名或编辑一个当前签名和选择**提醒的频率>概略的模式**。

可用的汇总选项是：

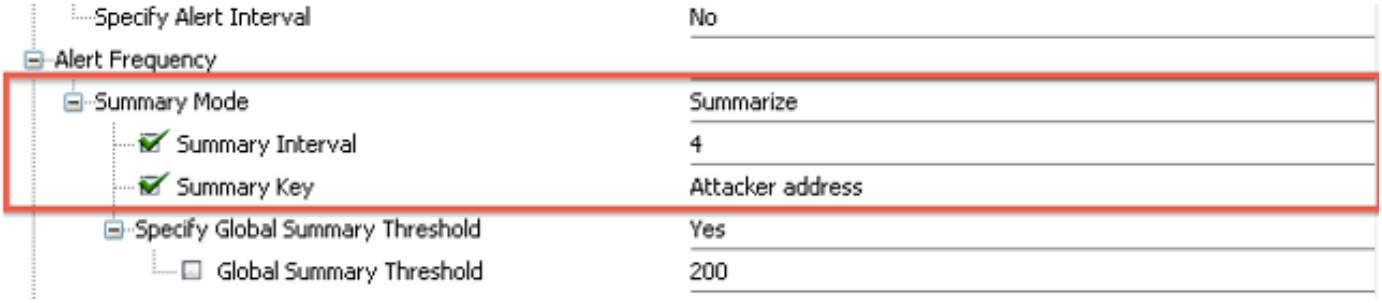
- 在签名被触发时候，火所有-射击警报。
- 火一旦-射击地址集的一警报。
- 汇总-射击警报，第一次签名被触发。该签名的另外的警报汇总在持续时间概略的间隔。
- 全局汇总-射击每个概略的间隔的一警报。

摘要关键和全局概略的阈值有何区别？

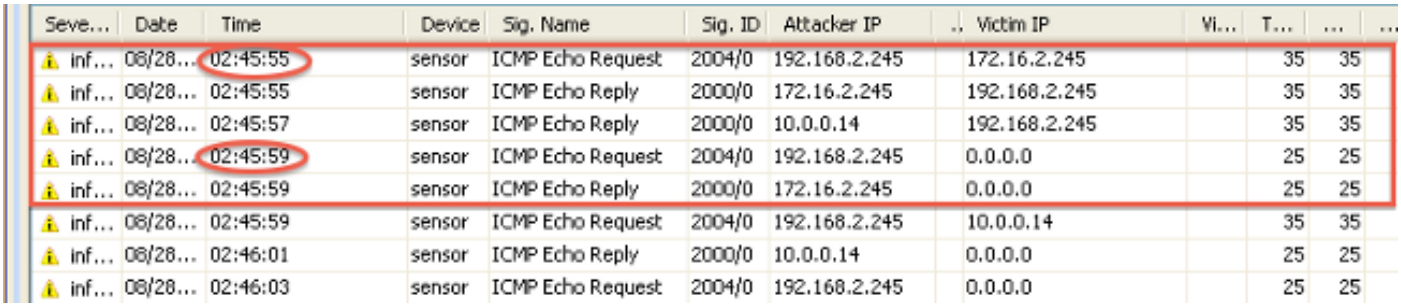
摘要密钥是IPS用于的密钥为了推断如何创建一个概略的事件。默认情况下，这是含义那的攻击者地址，如果有触发所有签名的一名攻击者，一个正则事件，并且一摘要生成。如果有两名攻击者，两个正常和两个概略的事件为已配置的概略的间隔生成。如果设置概略的密钥为受害者地址，并且有瞄准一个受害者的两名攻击者，则两名攻击者只将记录一个正常和一个概略的事件。

概略的模式有两个选项;概略的间隔和摘要密钥。概略的间隔以秒钟代表，并且为每个概略的间隔射击。摘要密钥是IPS决定如何创建概略的事件的标准。默认情况下，这是攻击者地址。可用的摘要密钥选项包括：

- 攻击者地址(默认)
- 攻击者地址和受害者端口
- 攻击者和受害者地址
- 攻击者和受害者地址和端口
- 受害者地址



前一个示例显示签名汇总与一个概略的间隔4和摘要密钥作为攻击者地址。在此方案中，签名第一次射击一个正常事件，在后指向签名为间隔4秒汇总。



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	

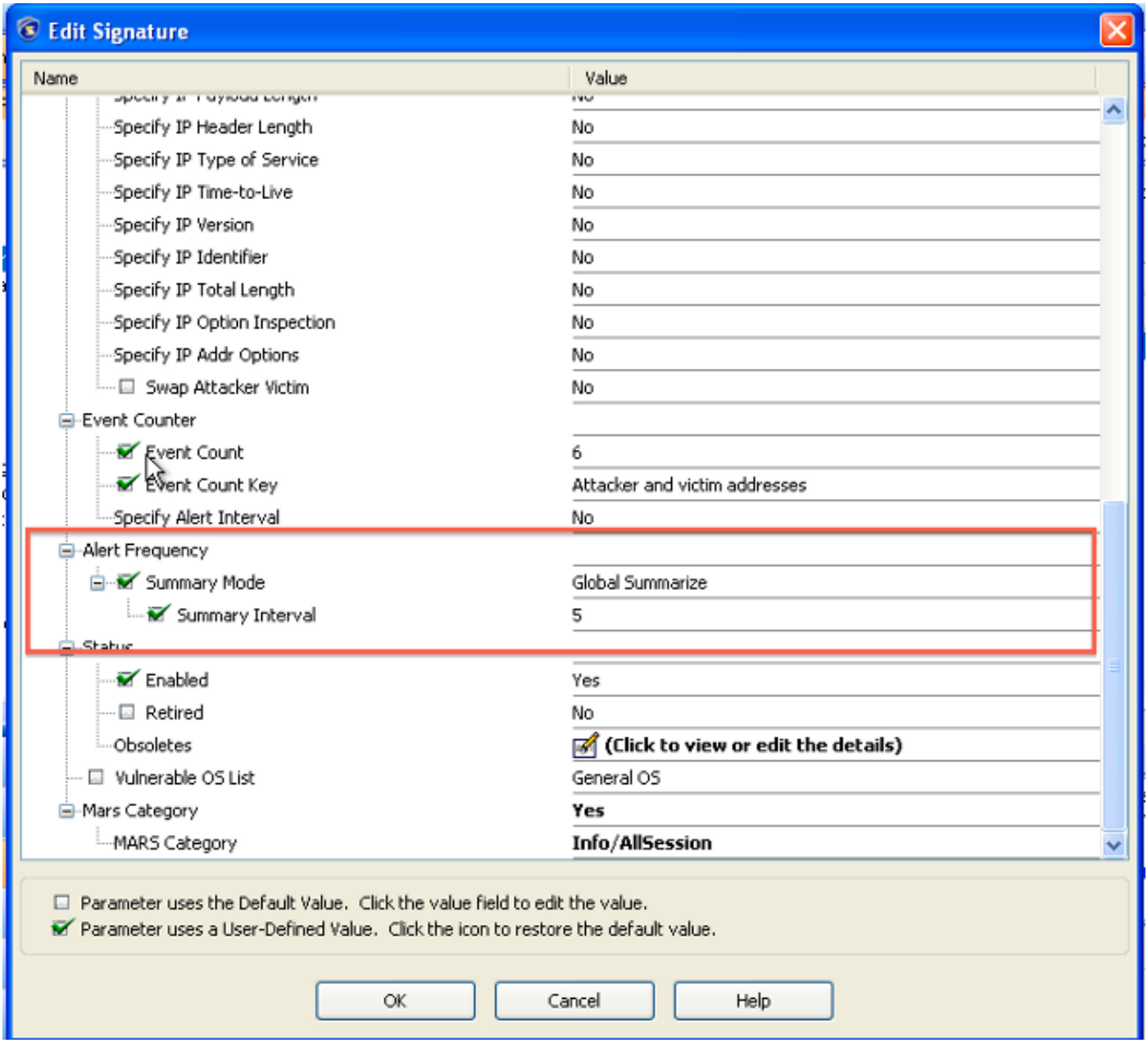
全局概略的阈值-，如果全局摘要没有指定，并且，如果有被看到的两个攻击者IP地址， IPS记录两个正常事件。在期限概略的间隔之后，两个另外的汇总的事件生成，一个每个攻击者IP地址的。总共，您会安排4个事件被记录在指定的时间间隔内。

当全局汇总启用与一全局概略的阈值请说，两，并且，如果重复前一个示例， IPS然后记录三个事件：两每个攻击者地址的最初的命中数的和一个人汇总所有攻击者的(两事件在这种情况下)在指定的时间间隔内。现在，如果按比例提高攻击者和命中数数量，您看到一全局汇总保存很多事件/日志和因而处理器循环。

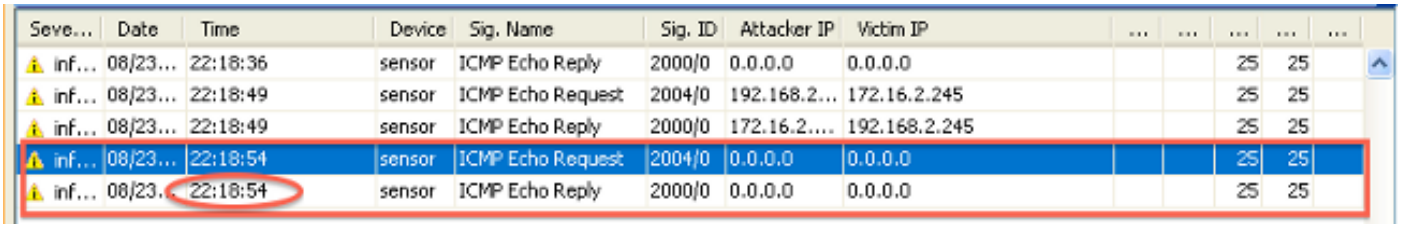
全局汇总只有是“概略的间隔”以秒钟配置的一子选项。当签名设置对全局summarizarion时，为每个概略的间隔射击。即，如果概略的间隔设置为'5'，它射击警报，第一次签名被触发，并且为每个概略的间隔5秒尔后射击。

为了编辑签名，请选择**Configuration>策略>活动签名**然后搜索相关签名。

例如， ‘ICMP请求的’签名ID是2004年。用鼠标右键单击签名并且选择**编辑**为了达到显示的对话框此处：



在先前配置片断，概略的模式设置对‘全局汇总’与一个概略的间隔5秒。



警报示例显示签名的ICMP echo请求’和‘ICMP echo应答’，汇总并且显示攻击者/受害者IP地址作为'0.0.0.0'。

请勿与全局汇总事件混淆‘签名1102.0事件(不可能的IP数据包)’。黑客也许设法逃避与使用的IPS可能触发此签名，也许看起来象一个汇总的事件的来源/目的地IP地址和端口的所有零。

相关信息

- [思科入侵防御系统签名常见问题]

- 思科入侵防御系统传感器IPS的7.1 CLI配置指南
- IPS汇总配置示例
- 技术支持和文档 - Cisco Systems