IPS汇总配置示例

目录

简介

本文为汇总的配置提供说明、优点和示例在思科入侵防御系统(IPS)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科可适应安全工具(ASA) 5500或5500x思科入侵防御系统(IPS)模块
- IPS 4200， 4300或者4500系列IPS设备
- NME-IPS模块
- IPS签名警报

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA 5500或5500x IPS模块
- IPS 4200， 4300或4500系列IPS设备
- NME-IPS模块

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。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

背景信息

IPS汇总提供模式聚集事件到单个警报，因此传感器发送的音量警报可以减小。每个签名创建以反射首选的默认，正常行为。然而，每个签名有影响的特殊参数警报如何被处理，因此签名默认行为可以在每种引擎类型的限制条件内被调整。

在阶引擎处理组分事件后，汇总和事件操作处理。这让传感器注意在一系列的事件的可疑活动。

基本聚合提供两个模式：

- **简单模式**-配置命中数阈值数字必须满足的签名的，在警报被发送前。
- **Advanced模式**-配置命中数阈值数字每秒(计时的间隔计数)必须满足的签名的，在警报被发送前。

汇总选项

- **火所有**-，每次签名被触发，射击警报。如果阈值为汇总设置，警报为每执行被射击，直到汇总发生。在汇总开始后，只有每个摘要间隔火的一警报每地址集的。其他地址集的警报所有被看到或分开汇总。签名恢复对火**所有**模式在一个期限之后没有警报该签名的。
- **摘要**-，第一次签名被触发，射击警报。该签名的另外的警报汇总在持续时间概略的间隔。仅每个概略的间隔应该为每地址集射击的一警报。如果全局概略的阈值达到，签名进入全局**汇总**模式。
- **全局汇总**-射击每个概略的间隔的一警报。签名可以为全局**汇总**预先配置。
- **火一且**-射击每地址集的一警报。此模式可以升级到全局**汇总**模式。

事件汇总

常见情况是经过调整的期限基准为了识别亢奋警告的签名。经常有需要根据流量混合的汇总的一定数量的低级和与信息有关的级别签名。查看这些签名为了确定适当的阈值。

> **Note**:小心，每当您减少相当数量警报，从高严重程度签名的特别是警报。保证安全没有被危及，并且适当的操作为汇总的所有签名是到位。

配置

Note:使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

SSH暴力攻击-签名3653

迅速安全壳SSH会话，当积极地警告，能迅速填装事件存储。目前， SSH暴力尝试拒绝。

如果只需要警报每五分钟，请使用**概略的**选项警报频率与摘要间隔300秒：

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 3653 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode summarize
sensor(config-sig-sig-ale-sum)# summary-interval 300
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-sum)# show settings
alert-frequency
-----------------------------------------------
summary-mode
-----------------------------------------------
summarize
-----------------------------------------------
summary-interval: 300 default: 15
summary-key: Axxx <defaulted>
specify-global-summary-threshold
-----------------------------------------------
yes
-----------------------------------------------
global-summary-threshold: 240 <defaulted>
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

在HTTP请求的额外的SQL查询-签名5474

精选从在HTTP请求嵌入的SQL查询是其中一个在边缘部署的最普通的亢奋警告的签名。

为了查看签名5474每小时为一个攻击者/受害者对，使用，火**一旦**警报频率的选项与摘要间隔3600秒：

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 5474 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 3600
sensor(config-sig-sig-ale-fir-yes)# summary-interval 3600
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir)# show settings
```

```
fire-once
-----------------------------------------------
summary-key: Axxx default: Axxx
specify-global-summary-threshold
-----------------------------------------------
yes
-----------------------------------------------
global-summary-threshold: 3600 default: 240
summary-interval: 3600 default: 15
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

AD内部或外部TCP/UDP扫描仪-签名13000到13008

在本例中，签名火，当检测a扫描套作为区域配置的目的地IP地址内部或外部的传输控制协议/用户数据报协议(UDP)扫描仪。如果IPS管理器Express (IME)发送默认，高严重程度事件作为电子邮件通知，那里也许在千位电子邮件。

> **Note**:确保火不是错误肯定攻击。更改异常情况检测的设置对“Learn模式” 48个小时，然后移动它回到“检测模式”为了解决问题。

为了减少电子邮件数量，请使用，火**一旦**选项警报频率，与摘要间隔720秒或一次每12分钟。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 13000 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 720
sensor(config-sig-sig-ale-fir-yes)# summary-interval 720
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir-yes)# show settings
  fire-once
  -----------------------------------------------
     summary-key: Axxx <defaulted>
     specify-global-summary-threshold
     -----------------------------------------------
        yes
        -----------------------------------------------
           global-summary-threshold: 720 default: 240
           summary-interval: 720 default: 15
        -----------------------------------------------
     -----------------------------------------------
  -----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 配置提醒的频率
- IPS配置指南
- 技术支持和文档 - Cisco Systems