入侵防御系统设备管理器5.1 -调整签名

目录

简介

入侵防御系统(IPS) 5.1包含1000个内置的默认签名。您不能重命名或删除从内置的签名列表的签名，但是您能退休签名从感觉的引擎删除他们。您能以后激活收回签名。然而，此进程要求感觉的引擎重建他们的配置，花费时间，并且可能延迟处理流量。当您调整几个签名参数时，您能调整内置的签名。修改了的内置的签名呼叫*被调整的签名*。

使用IPS设备管理器(IDM)，本文说明步骤使用为了调整签名。IDM基于Web的，使您配置与管理您的传感器的Java应用程序。IDM的Web服务器在传感器驻留。您能通过Internet Explorer、Netscape或者Mozilla Web浏览器访问它。

注意： 您能创建签名，呼叫*自定义签名*。自定义签名ID开始在60000。您能为几件事配置他们，例如匹配在UDP连接的字符串，跟踪网络充斥和扫瞄。每个签名创建使用为是受监视的流量类型特别地设计的签名引擎。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据思科入侵防御系统设备管理器5.x。

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

为了配置传感器到一个特定的签名的监控网络流量，您必须启用签名。默认情况下，当您安装签名更新时，最关键的签名启用。当匹配已启用签名的攻击检测时，传感器生成警报，在传感器的事件存储存储。警报，以及其他事件，可以从事件存储获取由基于Web的客户端。默认情况下，传感器记录所有信息性警报或高。

一些签名有子签名。即签名分开成子范畴。当您配置子签名时，做的变动对一子签名参数仅适用于该子签名。例如，如果编辑签名3050子签名1并且更改严重性，严重性更改仅适用对子签名1和不于3050 2， 3050 3和3050 4。

调整签名

A +图标表明更多选项为此参数是可用的。点击+扩展部分和查看剩余的参数的图标。

绿色图标表明参数当前使用默认值。点击绿色图标更改它到红色，激活参数字段，因此您能编辑值。

逐步程序

完成这些步骤为了调整签名：

1. 使用一个帐户有管理员或操作员权限，登陆对IDM。
2. 选择**Configuration>签名定义>签名配置**。签名配置窗格出现。
3. 为了找出签名，请从**精选**选择一个排序的选项**由**列表。例如，如果搜索UDP充斥签名，请选择**L2/L3/L4协议**然后**UDP充斥**。签名配置窗格刷新并且显示匹配您排序的标准仅的那些签名。
4. 为了调整一个现有签名，请选择签名并且完成这些步骤：单击**编辑**打开编辑签名对话框。查看参数值并且更改您要调整的值所有参数。**注意：** 为了选择超过一事件操作，请持续**Ctrl**密钥。在状态下，请选择**是**启用签名。**注意：** 必须启用签名为了传感器能由签名积极地检测指定的攻击。在状态下，如果此签名退休，请指定。单击**不**激活签名。这在引擎里安置签名。**注意：** 必须激活签名为了传感器能由签名积极地检测指定的攻击。**注意：** 点击**取消**为了取消您的更改和关闭编辑签名对话框。单击 **Ok**。编辑的签名在与类型集的列表当前出现对调整。**注意：** 如果要取消您的更改，请点击**“Reset”**。
5. 单击**应用**应用您的更改和保存已修订配置。

相关信息

- Cisco Intrusion Prevention System
- 技术支持和文档 - Cisco Systems