目录

简介

本文描述如何启用轴向标准化预处理程序并且帮助您了解轴向标准化的两高级选项差异和影响。

先决条件

要求

思科建议您有思科火力系统的知识并且打鼾。

使用的组件

本文档中的信息根据思科FireSIGHT管理中心和火力设备。

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

一个轴向标准化预处理程序规范化流量为了最小化机会使用轴向部署，攻击者能逃避检测。标准化发生在解码的数据包之后和在所有其他预处理程序前，并且从数据包的内在层继续向外。轴向标准化不生成事件，但是准备数据包供其他预处理程序使用。

当您运用一项入侵策略用启用时的轴向标准化预处理程序，火力设备测试这两个情况为了保证您使用一轴向部署：

- 对于版本5.4和以上，*轴向模式*启用在网络分析策略(NAP)和*丢弃，当线型*在入侵策略时也配置，如果入侵策略设置降低流量。版本5.3和以下，*丢弃，当轴向*选项在入侵策略启用。

- 策略应用对轴向(或线型与failopen)接口集。

所以，除轴向标准化预处理程序的启动和配置之外，您必须也保证这些需求符合，否则预处理程序不会规范化流量：

- 必须设置您的策略降低在轴向部署的流量。
- 您必须运用您的策略到轴向集。

Enable (event)轴向标准化

此部分描述如何启用轴向标准化版本5.4和以上的，并且版本5.3和以下的。

在版本5.4和以上的Enable (event)轴向标准化

大多预处理程序设置在版本5.4和以上的NAP配置。完成这些步骤为了启用在NAP的轴向标准化：

1. 登陆对您的FireSIGHT管理中心Web UI。
2. 导航到**策略>访问控制**。
3. 在页的右上方区域附近单击**网络分析策略**。
4. 选择您要适用于您的受管理设备的*网络分析策略*。
5. 点击*铅笔*图标为了开始编辑，并且*编辑策略*页出版。
6. 在屏幕的左边单击**设置**，并且*Settings页*出版。
7. 在*传输/network层预处理程序*地区找出**轴向标准化**选项。
8. 选择**Enabled单选按钮**为了启用此功能：

必须添加与轴向标准化的NAP到您的访问控制策略为了轴向标准化能发生。NAP可以通过访问控制策略*高级选项卡*。被添加：

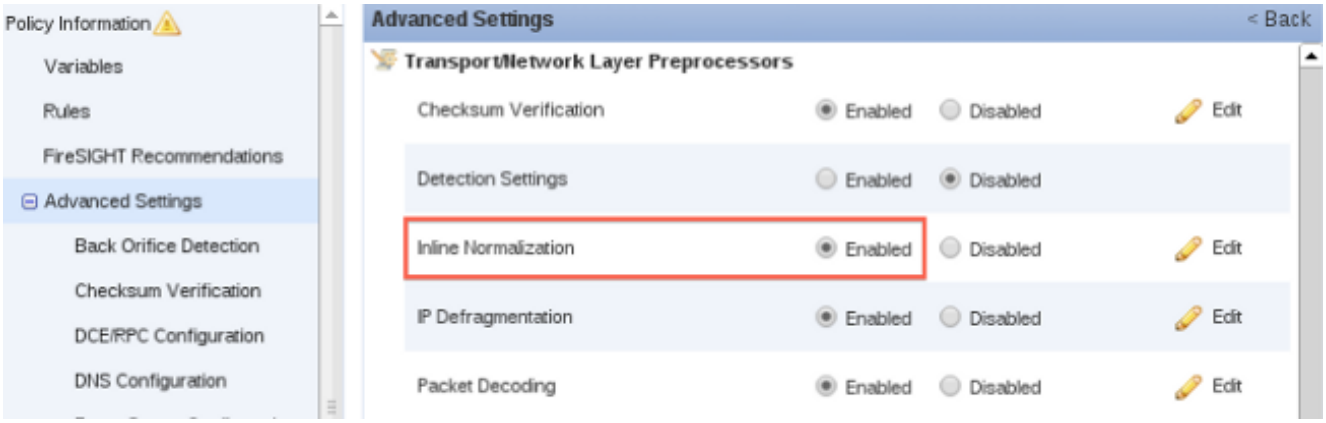
必须然后应用访问控制策略到检查的设备。

> **注意**：对于版本5.4或以上，您能启用某一流量的轴向标准化和为其他流量禁用它。如果要为特定的流量启用它，请增加一个*网络分析规则*并且设置流量标准和策略到有启用的轴向标准化的那个。如果要启用它全局，则设置*默认网络分析策略*到有启用的轴向标准化的那个。

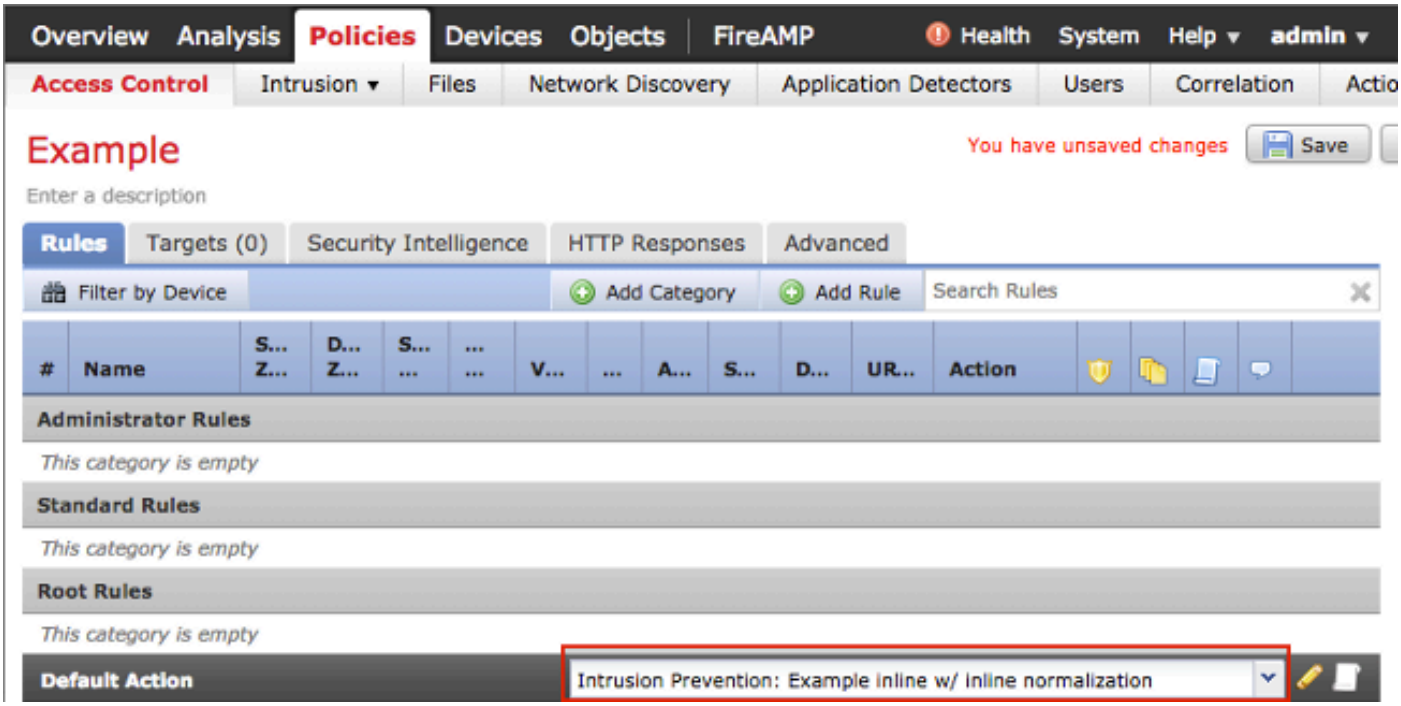
启用在版本5.3和以下的轴向标准化

完成这些步骤为了启用在入侵策略的轴向标准化：

1. 登陆对您的FireSIGHT管理中心Web UI。
2. 导航对**策略>入侵>入侵策略**。
3. 选择您要适用于您的受管理设备的*入侵策略*。
4. 点击*铅笔*图标为了开始编辑，并且*编辑策略*页出版。
5. 点击**先进的设置**，并且***先进Settings页***出版。
6. 在*传输/network层预处理程序*地区找出**轴向标准化**选项。
7. 选择**Enabled单选按钮**为了启用此功能：



一旦入侵策略为轴向标准化配置，必须添加作为在访问控制策略的默认操作：



必须然后应用访问控制策略到检查的设备。

您能配置轴向标准化预处理程序为了规范化IPv4,IPv6，互联网控制消息协议任意组合版本4 (ICMPv4)， ICMPv6和TCP数据流。当该协议标准化启用时，每份协议的标准化自动地发生。

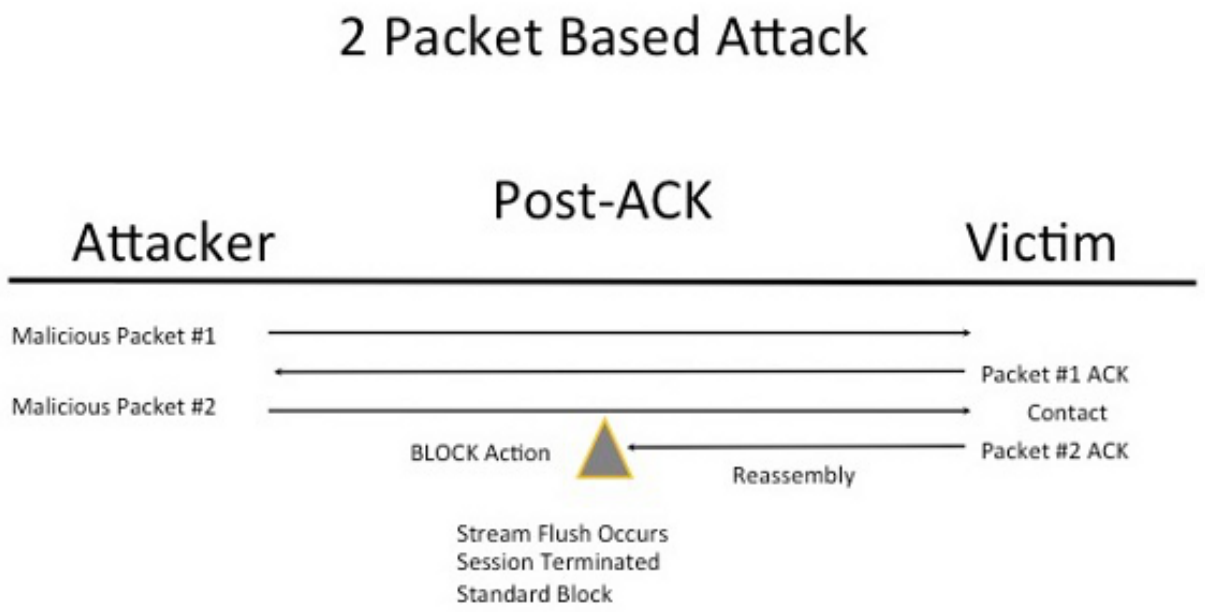
Enable (event) POST ACK检查和PRE ACK检查

在您启用轴向标准化预处理程序后，您能编辑设置为了启用*规范化TCP有效载荷*选项。在轴向标准化预处理程序交换机的此选项检查之间两个区别模式：

- 波斯特确认(POST ACK)
- 前确认(PRE ACK)

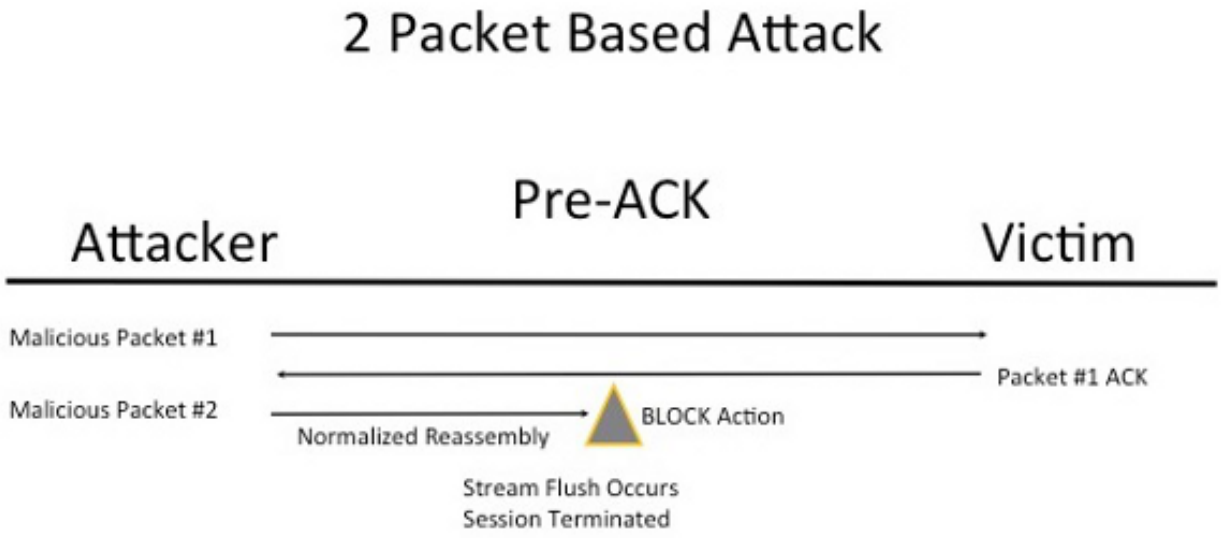
了解POST ACK检查(请规范化禁用的TCP/Normalize TCP有效载荷)

在POST ACK检查，在喷鼻息的信息包流重组、冲洗(手对检查进程的其余)和检测发生，在确认(ACK)后从完成的数据包的受害者攻击由入侵防御系统(IPS)接收。在数据流冲洗发生前，已损坏的数据包已经到达了受害者。所以，在已损坏的数据包到达了受害者后，警报/丢弃发生。当从受害者的ACK已损坏的数据包的到达IPS，此操作发生。



了解PRE ACK检查(请规范化启用的TCP/Normalize TCP有效载荷)

此功能规范化流量，在解码的数据包，并且之后，在其他喷鼻息功能处理为了最小化TCP躲避努力前。这保证到达IPS的数据包是作为那些通过对受害者的相同的。喷鼻息降低在完成攻击的数据包的流量，在攻击到达其受害者前。



当您启用时请*规范化TCP*，匹配这些情况也丢弃的流量：

- 以前丢弃的数据包的被重新传输的复制
- 尝试继续一以前已丢失会话的流量

- 匹配中的任一这些TCP数据流预处理程序的流量规定：

  129:1129:3129:4129:6129:8129:11129:14至129:19

  注意：为了启用由标准化预处理程序丢弃的TCP数据流规则的警报，您在TCP数据流配置里必须启用*状态检测反常现象*功能。