启用内联规范化预处理器并了解Pre-ACK和Post-ACK检测

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

启用内联规范化

- 在版本5.4及更高版本中启用内联规范化
- 在版本5.3及更低版本中启用内联规范化

启用确认后检查和确认前检查

- 了解ACK后检测（禁用Normalize TCP/Normalize TCP Payload）
- 了解Pre-ACK检测（已启用规范化TCP/规范化TCP负载）

简介

本文档介绍如何启用内联规范化预处理器，并帮助您了解内联规范化的两个高级选项的区别和影响。

先决条件

要求

Cisco建议您了解Cisco Firepower系统和Snort。

使用的组件

本文档中的信息基于Cisco FireSIGHT管理中心和Firepower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

内联规范化预处理器对流量进行规范化，以便最大限度地减少攻击者使用内联部署逃避检测的可能性。规范化在数据包解码后立即执行，并在任何其他预处理器之前执行，并从数据包的内部层向外执行。内联规范化不会生成事件，但它会准备数据包以供其他预处理器使用。

当您应用启用了内联规范化预处理器的入侵策略时，Firepower设备会测试以下两个条件以确保使用

内联部署：

- 对于版本5.4及更高版本，在网络分析策略(NAP)中启用内联模式，如果入侵策略设置为丢弃流量，则入侵策略中还会配置Drop when Inline。对于版本5.3及更低版本，在入侵策略中启用Drop when Inline选项。
- 策略应用于内联（或与失效开放内联）接口集。

因此，除了启用和配置内联规范化预处理器外，还必须确保满足这些要求，否则预处理器不会规范化流量：

- 策略必须设置为在内联部署中丢弃流量。
- 必须将策略应用于内联集。

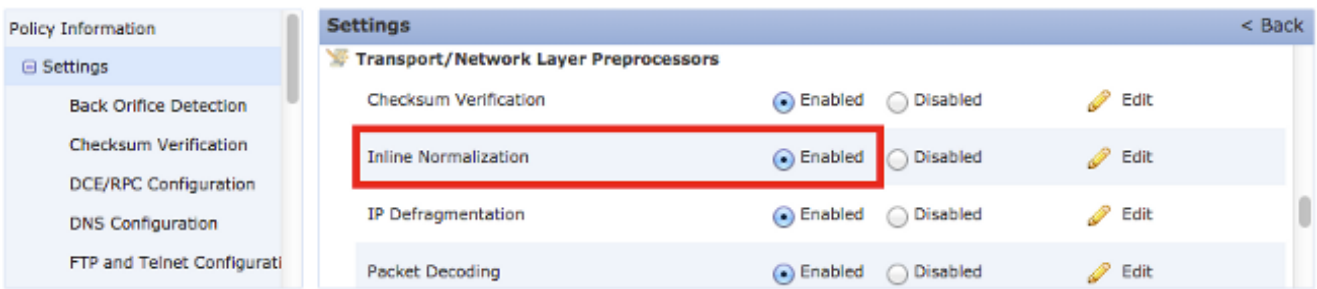
启用内联规范化

本节介绍如何为版本5.4及更高版本以及版本5.3及更低版本启用内联规范化。

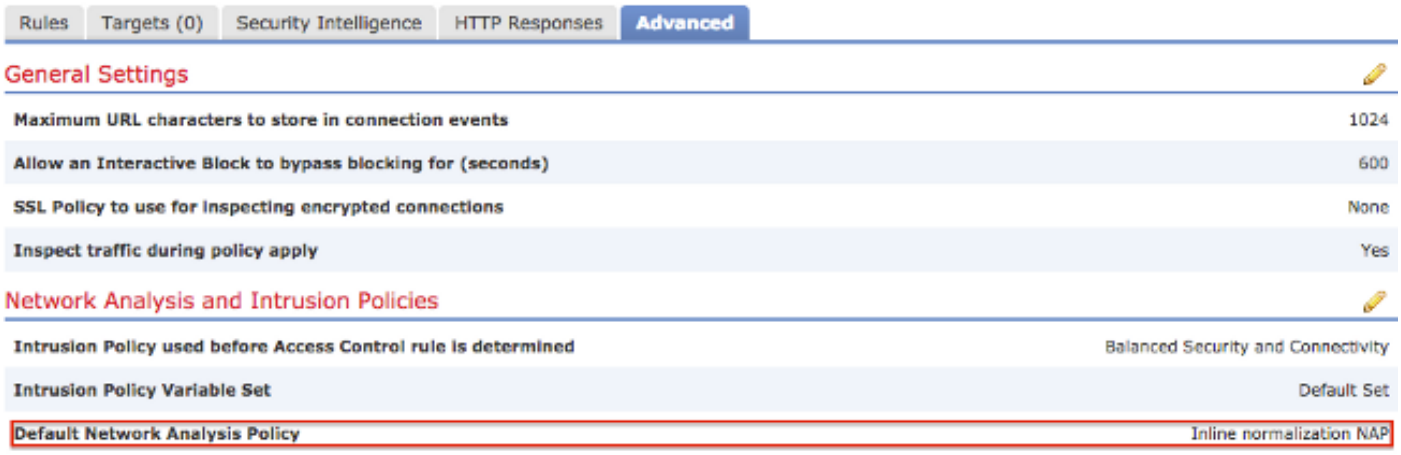
在版本5.4及更高版本中启用内联规范化

大多数预处理器设置在5.4版及更高版本的NAP中配置。要在NAP中启用内联规范化，请完成以下步骤：

1. 登录到FireSIGHT管理中心的Web用户界面。
2. 导航到策略 > 访问控制。
3. 点击页面右上方区域附近的网络分析策略。
4. 选择要应用于受管设备的网络分析策略。
5. 单击铅笔图标开始编辑，然后显示Edit Policy页面。
6. 单击屏幕左侧的Settings，将显示Settings页面。
7. 在Transport/Network Layer Preprocessor区域中找到Inline Normalization选项。
8. 选择Enabled单选按钮以启用此功能：



必须将具有内联规范化的NAP添加到访问控制策略，以便进行内联规范化。可以通过访问控制策略Advanced选项卡添加NAP:



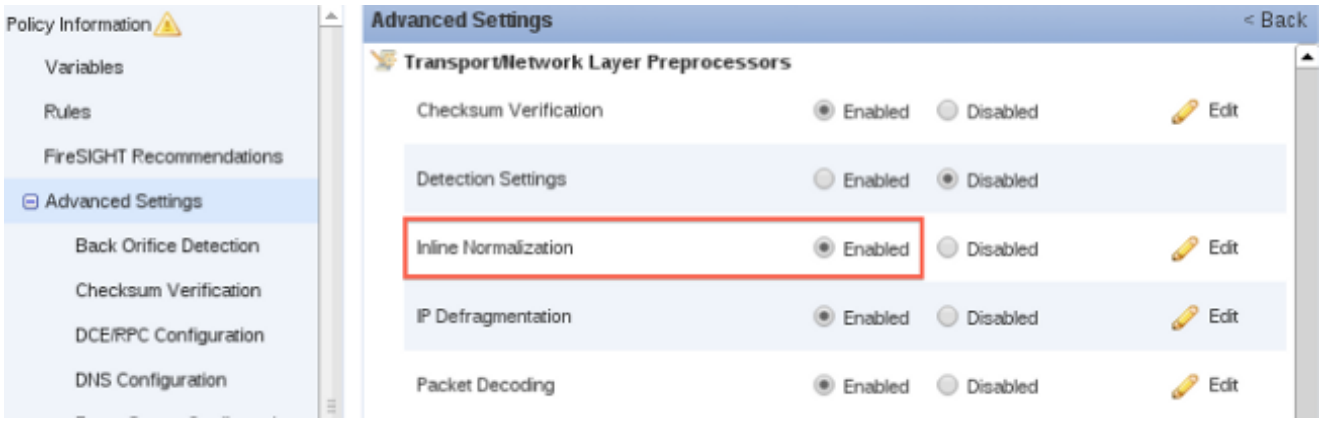
然后，必须将访问控制策略应用到检查设备。

注意：对于版本5.4或更高版本，您可以为特定流量启用内联规范化，并为其他流量禁用内联规范化。如果要为特定流量启用它，请添加网络分析规则，并将流量标准和策略设置为已启用内联规范化的规则。如果要全局启用它，请将默认网络分析策略设置为已启用内联规范化的策略。

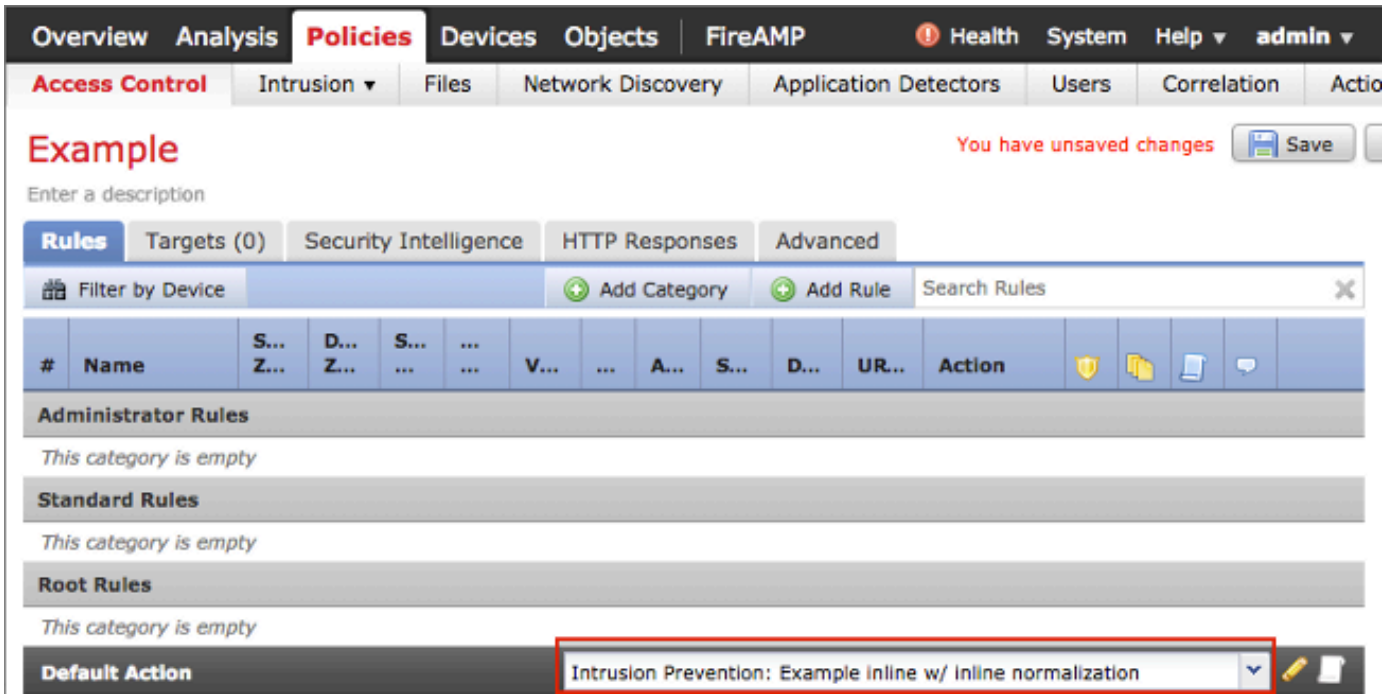
在版本5.3及更低版本中启用内联规范化

要在入侵策略中启用内联规范化，请完成以下步骤：

1. 登录到FireSIGHT管理中心的Web用户界面。
2. 导航到Policies > Intrusion > Intrusion Policies。
3. 选择要应用到受管设备的入侵策略。
4. 单击铅笔图标开始编辑，然后显示Edit Policy页面。
5. 单击Advanced Settings，然后显示Advanced Settings页面。
6. 在Transport/Network Layer Preprocessor区域中找到Inline Normalization选项。
7. 选择Enabled单选按钮以启用此功能：



为内联规范化配置入侵策略后，必须将其添加为访问控制策略中的默认操作：



然后，必须将访问控制策略应用到检查设备。

您可以配置内联规范化预处理器，以规范化IPv4、IPv6、互联网控制消息协议版本4(ICMPv4)、ICMPv6和TCP流量的任意组合。当协议规范化被启用时，每个协议的规范化自动发生。

启用确认后检查和确认前检查

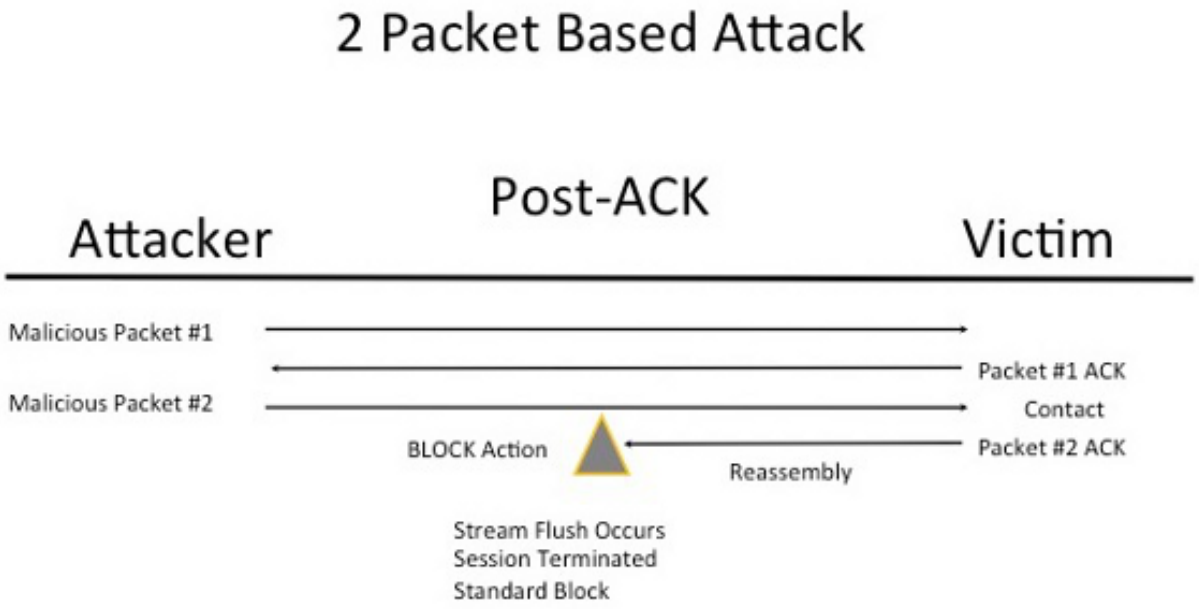
启用内联规范化预处理器后，可以编辑设置以启用Normalize TCP Payload选项。内联规范化预处理器中的此选项可在两种不同的检测模式之间切换：

- 确认后（ACK后）
- 预确认(Pre-ACK)

了解ACK后检测（禁用Normalize TCP/Normalize TCP Payload）

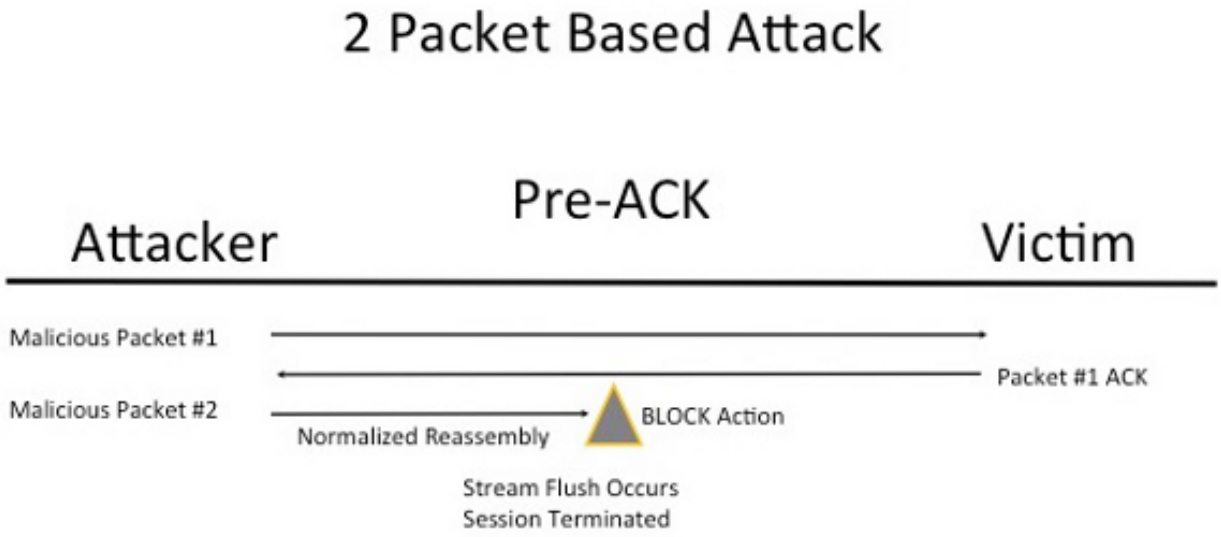
在ACK后检查中，数据包流重组、刷新（切换到检查过程的其余部分）和Snort中的检测在入侵防御

系统(IPS)收到完成攻击的数据包的受害者的确认(ACK)后发生。 在数据流刷新发生之前，有问题的数据包已经到达受害者。因此，当有问题的数据包到达受害者时，就会发生警报/丢弃。当来自违规数据包的受害者的ACK到达IPS时，会发生此操作。



了解Pre-ACK检测（已启用规范化TCP/规范化TCP负载）

此功能会在数据包解码后以及处理任何其他Snort功能之前立即规范化流量，以最大程度减少TCP逃避工作。这可确保到达IPS的数据包与传递到受害者的数据包相同。Snort会丢弃数据包上的流量，在攻击到达其受害者之前完成攻击。



当您启用Normalize TCP时，匹配以下条件的流量也会被丢弃：

- 重新传输之前丢弃的数据包副本
- 尝试继续之前丢弃的会话的流量
- 匹配以下TCP数据流预处理器规则的流量：
    - 129:1
    - 129:3
    - 129:4
    - 129:6
    - 129:8
    - 129:11
    - 129:14 到 129:19

注意：要启用规范化预处理器丢弃的TCP流规则的警报，必须在TCP流配置中启用状态检测异常功能。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。