入侵防御

Snort 检测引擎是 Firewall Threat Defense 中不可或缺的一部分。本章提供 Snort 3 网络分析和入侵策略概述。它可以让您深入了解系统提供的和自定义的网络分析和入侵策略。在大多数情况下，系统提供的策略就足够了。对于有特定需求的高级用户，您可以创建自定义规则。要配置自定义 Snort 3 规则，请参阅用于访问控制的 *Snort 3* 自定义入侵策略。

注释 。

要配置自定义 Snort 2 规则，请参阅用于访问控制的 *Snort 2* 自定义入侵策略。

关于入侵防御

网络分析和入侵策略作为入侵检测和防御功能的一部分，共同发挥作用。

- 术语入侵检测通常是指被动监控并分析网络流量以查找潜在入侵，并存储攻击数据以进行安全分析的过程。这有时称为“IDS”。
- 术语入侵防御包括入侵检测的概念，但是增加了在恶意流量流经网络时对其进行拦截或更改的能力。这有时称为“IPS”。

在入侵防御部署中，当系统检测数据包时：

- **网络分析策略**监管如何解码和预处理流量，以便可进一步对其进行评估，尤其适用于可能表明入侵尝试的异常流量。

- **入侵策略**使用入侵和预处理程序规则（有时统称为入侵规则）根据模式检测已解码数据包是否存在攻击。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。

网络分析和入侵策略均由父访问控制策略调用，但是在不同时间调用。在系统分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（其他预处理和入侵规则）阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

系统随附若干以类似方式命名的网络分析和入侵策略（例如，平衡安全性和连接），这些策略是相辅相成的。通过使用系统提供的策略，您可以利用思科 Talos 智能小组 (Talos) 的经验。对于这些策略， Talos 提供入侵和检查器规则状态及对检查器和其他高级设置的初始配置。

您还可以创建自定义网络分析和入侵策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高托管设备的性能以及您有效响应其生成的事件的能力。

您可在网络界面中使用相似的策略编辑器创建、编辑、保存和管理网络分析和入侵策略。在您编辑任一类型的策略时，导航面板显示在网络界面的左侧；右侧显示各种配置页面。

有关其他支持和信息，请参阅视频：

- Snort 3 简明概述
- Snort 3 扩展概述

注意 **检测模式弃用**：从管理中心 7.4.0 版本开始，对于网络分析策略 (NAP)，**检测**检查模式已弃用，并将在后续版本中移除。

检测 模式旨在用作测试模式，以便您可以启用检测并查看它们在网络中的行为，然后再将其设置为丢弃流量，即显示将被丢弃的流量。

此行为已得到改进，其中所有检查器丢弃都由规则状态控制，并且您可以设置每个丢弃以生成事件。这样做是为了在配置规则状态以丢弃流量之前对其进行测试。由于我们现在可以对 Snort 3 中的流量丢弃进行精细控制，因此 **检测** 模式只会增加产品的复杂性，不需要，因此检测模式已弃用。

如果将**检测**模式下的 NAP 更改为**预防**，则处理入侵事件流量并具有结果 “会被丢弃”的 NAP 现在将为“已丢弃”，相应的流量将丢弃来自这些事件的流量。这适用于 GID 不是 1 或 3 的规则。GID 1 和 3 是文本/编译规则（通常由 Talos 提供或从您的自定义/导入规则中提供），所有其他 GID 都是异常检测。这些是在网络中触发的比较少见的规则。更改为 **预防** 模式不太可能对流量产生任何影响。您只需禁用适用于已丢弃流量的入侵规则，并将其设置为仅生成或禁用。

我们建议您选择 **预防** 作为检测模式，但如果您选择 **预防**，则无法恢复到 **检测** 模式。

Snort 检测引擎

Snort 检测引擎是 Cisco Secure Firewall Threat Defense （前称 Firepower 威胁防御）设备不可或缺的一部分。检测引擎实时分析流量，以提供深度数据包检测。网络分析和入侵策略共同利用 Snort 检测引擎的功能来检测和防御入侵。

关于 Snort 3

Snort 3 是最新版本的 Snort 检测引擎，与早期版本的 Snort 相比有很大改进。旧版 Snort 是 Snort 2，它不再受支持。Snort 3 更高效，可提供更好的性能和可扩展性。

与 Snort 2 相比，Snort 3 在架构上进行了重新设计，以使用相同的资源检查更多流量。Snort 3 提供简化且灵活的流量解析器插入。Snort 3 还提供了新的规则语法，使规则编写更加容易，并且共享对象规则等效项可见。

Snort 3 的其他重大变化包括：

- 与使用多个 Snort 实例的 Snort 2 不同，Snort 3 将多个线程与单个 Snort 实例相关联。这会使用更少的内存，缩短 Snort 重新加载时间，并支持更多入侵规则和更大的网络映射。Snort 线程的数量因平台而异，与每个平台的 Snort 2 实例数量相同。使用几乎是透明的。在 Secure Firewall 6160 和 6170 设备上，默认情况下，Snort 3 将多个线程与两个 Snort 进程关联。有关详细信息，请参阅 Snort 3 多进程支持 。
- Snort 版本 per防火墙威胁防御 - Snort 检测引擎是 防火墙威胁防御 特定的，而不是 Cisco Secure Firewall Management Center （前称 Firepower Management Center） 特定的。防火墙管理中心 可以管理多个 防火墙威胁防御，每个都使用任一版本的 Snort（Snort 2 和 Snort 3）。虽然 防火墙管理中心的入侵策略是唯一的，但系统会应用 Snort 2 或 Snort 3 版本的入侵策略，具体取决于设备所选的检测引擎。
- 解码器规则 - 仅在默认入侵策略中触发数据包解码器规则。系统会忽略您在其他策略中启用的解码器规则。
- 共享对象规则 - Snort 3 支持部分但不是全部共享对象 (SO) 入侵规则（生成器 ID (GID) 为 3 的规则）。不支持的已启用共享对象规则不会触发。
- 安全智能的多层检测 - Snort 3 会检测最内部的 IP 地址，而不考虑层。
- 平台支持 - Snort 3 需要 Firewall Threat Defense 7.0 或更高版本。ASA FirePOWER 或 NGIPSv 设备不支持此功能。
- 受管设备 - 版本 7.0 的 防火墙管理中心 可以同时支持版本 6.4、6.5、6.6、6.7 和 7.0 Snort 2 防火墙威胁防御以及版本 7.0 Snort 3 防火墙威胁防御。
- 切换 Snort 版本时的流量中断 - 切换 Snort 版本会中断流量检查，并且在部署期间可能会丢弃一些数据包。
- 统一策略 - 无论受管 防火墙威胁防御中启用的底层 Snort 引擎版本如何， 防火墙管理中心 中配置的访问控制策略、入侵策略、网络分析策略均可在应用策略时无缝地工作。 防火墙管理中心 版本 7.0 及更高版本中的所有入侵策略都有两个可用版本：Snort 2 版本和 Snort 3 版本。虽然入侵策略有两个版本（Snort 2 版本和 Snort 3 版本），但它具有统一的名称、基本策略和检测模式。Snort 2 和 Snort 3 版本的入侵策略在规则设置方面可能不同。但是，在设备上应用入侵策略时，系统会自动识别设备上启用的 Snort 版本，并应用为该版本配置的规则设置。
- 轻量级安全软件包 (LSP) - 替换适用于 Snort 3 下一代入侵规则的 Snort 规则更新 (SRU) 和配置更新的 SRU。下载更新会同时下载 Snort 3 LSP 和 Snort 2 SRU。

LSP 更新提供新的和更新后的入侵规则和检查器规则、现有规则的修改后状态以及 防火墙管理中心 和 防火墙威胁防御 版本 7.0 或更高的修改后的默认入侵策略设置。当您将 防火墙管理中心 从 6.7 或更低版本升级到 7.0 时，它同时支持 LSP 和 SRU。LSP 更新还可能删除系统提供的规则，提供新规则类别和默认变量，并修改默认变量值。有关 LSP 更新的详细信息，请参阅最新版本的 *Firepower* 管理中心配置指南 中的 更新入侵规则 主题。

- Snort 2 和 Snort 3 规则和预设的映射 - 映射 Snort 2 和 Snort 3 规则，并且映射由系统提供。但是，它不是一对一映射。系统提供的入侵基本策略是为 Snort 2 和 Snort 3 预配置的，它们提供相同的入侵防御，但规则集不同。系统为 Snort 2 和 Snort 3 提供的基本策略针对相同的入侵防御设置相互映射。
- 同步 Snort 2 和 Snort 3 规则覆盖 - 防火墙威胁防御 升级到 7.0 后，可以将 防火墙威胁防御 的检测引擎升级到 Snort 3 版本。防火墙管理中心 使用 Talos 提供的映射将 Snort 2 版本入侵策略的现有规则中的所有覆盖映射到相应的 Snort 3 规则。但是，如果在升级后执行了其他覆盖，或者如果您安装了版本为 7.0 的新 防火墙威胁防御 ，则必须手动进行同步。
- 自定义入侵规则 - 您可以在 Snort 3 中创建自定义入侵规则。您还可以将 Snort 2 的自定义入侵规则导入到 Snort 3。
- 规则组 - 防火墙管理中心 将所有 Snort 3 规则分组到规则组中。规则组是规则的逻辑组，提供简单的管理界面，以增强规则可访问性、规则导航以及对规则组安全级别的更好控制。

  从防火墙管理中心7.3.0，支持多个级别的规则组的规则导航，这为规则提供了更大的灵活性和逻辑分组。添加了 MITRE 框架，使您能够使用 MITRE 框架浏览规则。MITRE 只是另一个类别的规则组，是 Talos 规则组的一部分。

注释 有关 MITRE 的信息，请参阅 https://attack.mitre.org 。

一条规则可以是多个规则组的一部分，例如多个 MITRE ATT&CK 规则组、规则类别规则组、多个“资产类型”规则组、恶意软件活动等。入侵策略编辑器中列出了可用的规则组，可以选择这些规则组以增强策略。

使用多级分层规则组的结构，您现在可以向下遍历到最后一个元素，即“枝叶规则组”。这些规则组包含彼此相关的规则集，例如特定类型的漏洞、类似的目标系统或类似的威胁类别。规则组有四个与其关联的安全级别。您可以更改安全级别，添加或删除规则组，并且可以更改与网络上看到的流量匹配的规则的规则操作。这样做是为了在安全性、性能和防误报之间取得令人满意的平衡。

Snort 3 多进程支持

在运行 Cisco Secure Firewall 版本 10.0 的 Cisco Secure Firewall 6160 和 6170 设备上，默认情况下，Snort 3 将多个线程与两个 Snort 实例相关联。在部署过程中，每个 Snort 3 实例会根据需要自动配置线程。单独的 Snort 3 实例可以减少每个实例的内存负载，减少锁竞争，并缩短核心生成时间。这有助于提高恢复能力、性能和可扩展性。任何 Snort 实例故障都会导致流量影响，如果需要，还可以重新启动单个 Snort 进程。

Snort 线程分布在 NUMA 节点上，其中每个节点都被视为独立处理器。这可确保维护内存边界。例如，Snort 实例 0 使用节点 0 的内存，而实例 1 使用节点 1 的内存。

诸如 **show coredump** 和 **show perfstats** 等命令的 CLI 输出已经增强，可以显示两个 Snort 实例上的信息。在管理中心上，导航至“**故障排除**”**(Troubleshooting)**”“**监控**”**(Monitor)**”“**设备**”**(Devices)** 以查看 “**概述**”**(Overview)**“**关键进程**”**(Critical Processes)** 和“ **内存**”**(Memory)** 部分，以获取有关两个 Snort 实例的信息。如果存在任何规则分析错误，Snort 实例编号会随错误一起显示。

禁用 Snort 3 多进程支持

使用 **configure snort multi-process disable** 命令禁用 Snort 3 多进程支持。您还必须重新部署配置，以确保禁用 Snort 3 多进程支持。

```
> configure snort multi-process disable
----------------------------------------------------------------------
Caution: this command is intended for debugging purposes only.
A deployment is required after enabling/disabling multi-process and will cause a Snort
restart and temporary traffic interruption.
----------------------------------------------------------------------
Do you still want to continue?
Please enter 'YES' or 'NO': YES
Please perform a manual deployment to disable multi-process.
```

注释 此命令会导致 Snort 引擎重启，并且在下一次部署期间，当 Snort 从多进程状态更改为单进程状态时，还将导致流量中断。

网络分析和入侵策略的准则和限制

- 具有小数据包的流量百分比较高会导致 Snort 性能下降。即使禁用所有预处理器，也会观察到此行为。
- 当您尝试在内存不足的威胁防御设备上部署配置更改时，也会触发 Snort 部署。这会导致大量消耗 RSS 内存。如果在设备上部署大型配置（例如包含大量 Snort IPS 规则、网络对象和访问控制列表的多个 IPS 策略），Snort 内存使用率也会受到影响。可以通过优化 配置来缓解此类内存问题。有关如何配置访问控制规则以优化配置的最佳实践，请参阅 访问控制规则的最佳实践。
- 如果增加 Threat Defense Virtual 实例的内存，必须重新部署配置，Snort 3 才能利用额外的内存。

注释 增加 Threat Defense Virtual 实例的内存时，Snort 3 的内存分配不会自动调整。必须重新部署配置，以重新生成相关配置文件（例如 `memory_allocation.lua`），这些文件会将更新后的资源限制应用于 Snort 3。

- 如果 SIP 流之后跟随来自同一连接的 RTP 流，Snort 会检测用于建立连接的初始 SIP 通信，并允许 SIP 流量。默认情况下，SIP 通信之后的 RTP 流也会被信任，并绕过已配置的规则。要防止

此类情况，信任父 SIP 连接或将父 SIP 连接添加到预过滤器规则，可确保只有 SIP 流绕过 Snort 检测，并允许后续的 RTP 流分别根据相应规则进行评估。

- 如果管理中心中有多条具有相同动作的 Snort 规则匹配一个数据包，将为每条规则记录一个事件。但是，如果匹配的规则具有不同的动作，则仅具有最高优先级动作的规则会生成事件。动作优先级从高到低为：放行、重置、阻止、丢弃、警报、记录。
- 通过系统日志或 eStreamer 完全限定事件源转发入侵数据包事件时，由于可用于系统日志生成和 eStreamer 的缓冲区大小限制，数据包数据字段可能会被截断。在这种情况下，数据包长度将不匹配实际发送的数据包数据。
- 不能同时进行策略更改、切换 Snort 版本并部署这两类更改。必须先进行所需的策略更改并部署，或先切换 Snort 版本并部署。

防火墙管理中心管理的 防火墙威胁防御 的 Snort 3 的功能限制

下表列出了 防火墙管理中心管理的 防火墙威胁防御 设备的 Snort 2 支持但 Snort 3 不支持的功能。

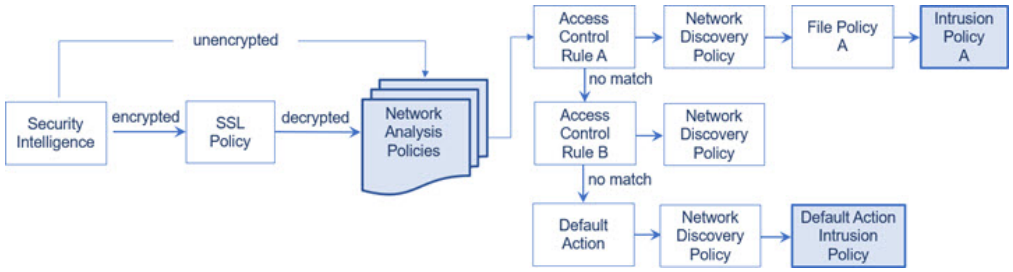
表 *1: Snort 3* 的功能限制

策略/区域	不支持的功能
访问控制策略	以下应用设置： • 安全搜索 • YouTube EDU
入侵策略	• 全局规则阈值 • 日志记录配置： • SNMP • SRU 规则更新，因为 Snort 3 仅支持 LSP 规则更新
其他功能	使用 FQDN 名称进行事件日志记录

策略如何检查流量是否存在入侵

当系统在访问控制部署过程中分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（入侵规则和高级设置）阶段之前并与其分隔开来。

下图以简化方式显示网络部署的内联、入侵防御和 AMP 中的流量分析顺序。它说明访问控制策略如何调用其他策略来检测流量，以及这些策略的调用顺序。网络分析和入侵策略选择阶段突出显示。



在内联部署中（即，使用路由接口、交换接口、透明接口或内联接口对将相关配置部署到设备），系统可以在图示过程中的几乎任何步骤阻止流量而不进行进一步检查。安全智能、SSL 策略、网络分析策略、文件策略和入侵策略均可以丢弃或修改流量。只有网络发现策略（被动检测数据包）无法影响流量的流动。

类似地，在该过程的每个步骤中，数据包都可能会导致系统生成事件。入侵和预处理程序事件（有时统称为入侵事件）指示数据包或其内容可能表示安全风险。

提示 当您的 SSL 配置允许已加密流量通过，或者您未配置 SSL 检查时，此图未反映访问控制规则处理已加密流量。默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略（如图所示），但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这**不**影响您在自定义网络分析策略中配置预处理的方式。

解码、规范化和预处理：网络分析策略

如果没有解码和预处理，则系统无法适当评估流量是否存在入侵，因为协议差异使得无法进行模式匹配。网络分析策略在以下时机监管这些流量处理任务：

- 在流量由安全智能过滤**之后**
- 在加密流量由可选 SSL 策略解密**之后**
- 在流量可由文件或入侵策略检测**之前**

网络分析策略分阶段监管数据包处理。系统首先通过前三个 TCP/IP 层解码数据包，然后继续规范化、预处理和检测协议异常：

- 数据包解码器将数据包报头和负载转换为可由检查器并在以后由入侵规则轻松使用的格式。TCP/IP 堆栈的各层从数据链路层开始并持续到网络层和传输层依次解码。数据包解码器还会检测数据包报头中的各种异常行为。
- 在内联部署中，内联规范化预处理程序重新格式化（规范化）流量，以尽量降低攻击者逃避检测的可能性。它会准备数据包以供其他检查器和入侵规则进行检测，并且帮助确保系统处理的数据包与网络上主机接收的数据包相同。

- 各种网络层和传输层检查器检测利用 IP 分段的攻击，执行校验和验证并执行 TCP 和 UDP 会话预处理。

  请注意，一些高级传输和网络检查器设置全局适用于由访问控制策略的目标设备处理的所有流量。您在访问控制策略中而不是在网络分析策略中配置这些高级设置。

- 各种应用层协议解码器将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。通过规范化应用层协议编码，系统可以将相同的内容相关的入侵规则有效地应用于以不同方式表示其数据的数据包，并且获取有意义的结果。

- Modbus、DNP3、CIP 和 s7commplus SCADA 检查器可检测流量异常并向入侵规则提供数据。监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。

- 通过若干检查器，可以检测特定威胁，如 Back Orifice、端口扫描、SYN 泛洪和其他基于速率的攻击。

  请注意，您在入侵策略中配置敏感数据检查器，该预处理器用于检测敏感数据（例如，ASCII 文本中的信用卡号和社会安全保障号）。

注释 禁用 TLS 服务器身份时，Snort 3 不会执行 SNI 不匹配检测。它仅评估客户端 Hello 数据包中的 SNI，并绕过服务器 Hello 数据包中证书的通用名称 (CN) 的验证。

在新建的访问控制策略中，一个默认网络分析策略监管对同一父访问控制策略调用的所有入侵策略的所有流量的预处理。最初，系统使用“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略作为默认值，但是，可以将其更改为另一个系统提供的网络分析策略或自定义网络分析策略。在更复杂的部署中，高级用户可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 定制流量预处理选项。

注释 对于规则操作为 **信任** 的访问控制策略和操作为 **快速路径** 的预过滤器规则并禁用日志记录选项，您将观察到仍在系统中生成流结束事件。这些事件在管理中心事件页面上不可见。

访问控制规则：入侵策略选择

在初始预处理后，访问控制规则（如果存在）会评估流量。在大多数情况下，数据包匹配的第一条访问控制规则处理该流量；您可以监控、信任、阻止或允许匹配流量。

当使用访问控制规则允许流量时，系统可能按该顺序检查流量是否存在发现数据、恶意软件、受禁文件和入侵。不与任何访问控制规则匹配的流量由访问控制策略的默认操作进行处理，该操作还检查是否存在发现数据和入侵。

注释 所有数据包（**无论**哪个网络分析策略对其进行预处理）均与配置的访问控制规则相匹配，因此可能会由上而下受到入侵策略的检测。

策略如何检查流量是否存在入侵，第 6 页 中的图显示流经内联的入侵防御和 AMP 网络部署中的设备的流量，如下所示：

- Access Control Rule A 允许匹配流量通过。然后该流量由网络发现策略检查是否存在发现数据，由文件策略 A 检查是否存在受禁文件和恶意软件，最后由入侵策略 A 检查是否存在入侵。
- 访问控制规则 B 也允许匹配流量通过。但是，在此情景中，未检查流量是否存在入侵（或文件或恶意软件），因此没有与规则关联的入侵或文件策略。请注意，默认情况下，您允许通过的流量将由网络发现策略进行检查；您不需要配置此检查。
- 在此情景中，访问控制策略的默认操作允许匹配流量。然后该流量将依次由网络发现策略和入侵策略进行检查。将入侵策略与访问控制规则或默认操作相关联时，可以（但不必）使用其他入侵策略。

图中的示例不包括任何阻止或信任规则，因为系统不检测已阻止或信任的流量。

入侵检查：入侵策略、规则和变量集

在允许流量继续到达其目标之前，可以使用入侵防御作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。入侵策略的主要功能是管理启用哪些入侵和预处理程序规则以及如何配置它们。

入侵和检查器规则

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；系统使用入侵规则来分析网络流量，以检测其是否与规则中的条件匹配。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据与规则中指定的所有条件都匹配，则触发此规则。

系统包括以下由 Cisoc Talos 智能组 (Talos) 创建的规则类型：

- 共享对象入侵规则，已编译且无法修改（规则标题信息除外，如源和目标端口及 IP 地址）
- 标准文本入侵规则，可以保存并修改为规则的新自定义实例。
- 预处理器规则，是指与网络分析策略中的检查器和数据包解码器检测选项关联的规则。不能复制或编辑检查器规则。默认情况下，大多数检查器规则均已禁用；您必须将其启用才能使用检查器生成事件，并在内联部署中丢弃有问题的数据包。

当系统根据入侵策略处理数据包时，首先，规则优化器会根据传输层、应用协议、受保护网络的方向等条件对子集中所有已激活的规则进行分类。然后，入侵规则引擎选择要应用于每个数据包的相应规则子集。最后，多规则搜索引擎执行三种不同类型的搜索以确定流量是否与规则匹配：

- 协议字段搜索在应用协议的特定字段中查找匹配项。
- 一般内容搜索在数据包负载中查找 ASCII 或二进制字节匹配项。

- 数据包异常搜索查找违反既定协议（而不是包含特定内容）的数据包报头和负载。

在自定义入侵策略中，您可以通过启用和禁用规则以及通过编写和添加自己的标准文本规则来调整检测。还可以遵从 Cisco Firepower 的建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。

注释 当没有足够的数据包根据阻止规则处理特定流量时，系统会继续根据其他规则评估剩余流量。如果任何剩余流量与设置为阻止的规则匹配，则会话将被阻止。但是，如果系统分析要传递的剩余流量，则流量状态在规则上显示为待处理，该规则因需要完整的数据包而被卡住。

变量集

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的大多数变量表示入侵规则中常用于识别源和目标 IP 地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

系统提供单个由预定义默认变量组成的默认变量集。大多数系统提供的共享对象规则和标准文本规则均使用这些预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

提示 即使您使用系统提供的入侵策略，思科也**强烈**建议修改默认变量集中的关键默认变量。当使用准确反映网络环境的变量时，处理会得以优化，并且系统可以监控相关系统是否存在可疑活动。高级用户可以创建并使用自定义变量集与一个或多个自定义入侵策略配对。

重要事项 如果要创建自定义变量集，请勿使用数字作为自定义变量集名称（例如，3Snort）中的第一个字符。当您将配置部署到 防火墙管理中心上的 Firewall Threat Defense 防火墙时，这将导致 Snort 3 验证失败。

入侵事件生成

当系统识别可能的入侵时，它会生成入侵或预处理程序事件（有时统称为入侵事件）。托管设备将其事件传输到防火墙管理中心，在其中可以查看聚合数据并更好地了解针对网络资产的攻击。在内联部署中，托管设备还可以丢弃或替换已知有害的数据包。

数据库中的每个入侵事件均包括事件报头并包含有关事件名称和分类的信息；源和目标 IP 地址；端口；生成事件的进程；事件的日期和时间，以及有关攻击源及其目标的情景信息。对于基于数据包的事件，系统还会记录一个或多个已触发事件的数据包的已解码数据包报头和负载的副本。

数据包解码器、预处理程序和入侵规则引擎均会导致系统生成事件。例如：

- 如果数据包解码器（在网络分析策略中配置）接收少于 20 字节（没有任何选项或负载的 IP 数据报的大小）的 IP 数据包，解码器将此解释为异常流量。如果之后启用了用于检测数据包的入侵策略中的配套解码器规则，则系统会生成检查器事件。
- 如果 IP 分片重组检查器遇到一系列重叠的 IP 片段，则检查器会将此解释为可能的攻击，当启用了配套预处理程序规则时，系统会生成检查器事件。
- 在入侵规则引擎内，大多数标准文本规则和共享对象规则编写为在由数据包触发时会生成入侵事件。

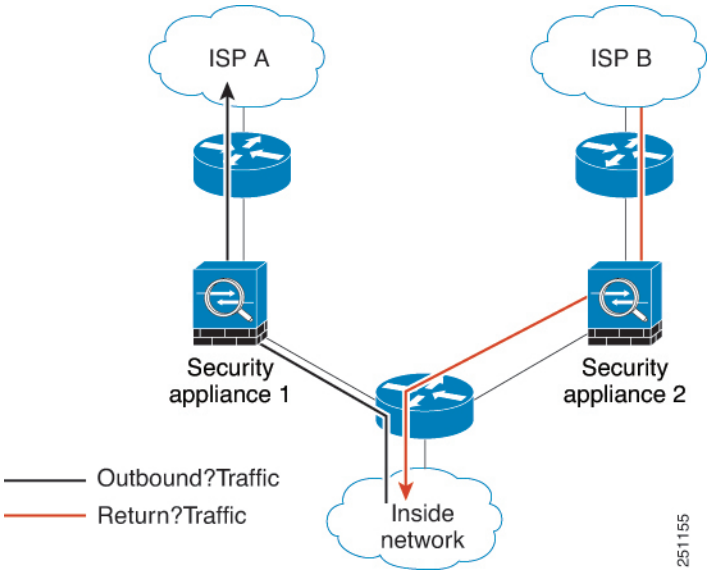
随着数据库累计入侵事件，您可以开始分析潜在攻击。系统为您提供复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

Snort 中的不对称流检查

在使用不对称路由的内联部署中，由于 Snort 的单向流量可视性有限，因此会损害数据包规范化。Snort 无法从未知流方向考虑 TCP 握手参数，例如窗口缩放或最大分段大小 (MSS)，这些参数可能导致主机接收大量数据包。

在下图中，两台设备都在运行 Snort 引擎。但是，引擎都未观察到完整的流量。未完全捕获流的 TCP 三次握手，这限制了可以应用的规范化类型。但是，在对 Snort 引擎可见的流侧会执行其他有效的规范化。

图 *1:* 非对称路由



在具有非对称路由的环境中，Snort 可以无缝适应动态变化，而无需额外配置。它会根据流模式动态调整其操作。请注意，不对称流量可能会影响防火墙的有效性，可能不是最佳选择。但是，Snort 旨在在必要时为此类部署提供支持。

系统提供的与自定义的网络分析和入侵策略

创建新的访问控制策略是使用系统管理流量过程中的头几个步骤之一。默认情况下，新创建的访问控制策略调用系统提供的网络分析和入侵策略来检测流量。

下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。

请注意以下各种操作的方式：

- 默认网络分析策略监管由访问控制策略处理的所有流量的预处理。最初，系统提供的 *Balanced Security and Connectivity* 网络分析策略是默认策略。
- 访问控制策略的默认操作允许由系统提供的 *Balanced Security and Connectivity* 入侵策略确定的所有非恶意流量。由于默认操作允许流量通过，在入侵策略能够检查并可能阻止恶意流量之前，发现功能可以检查流量中的主机、应用和用户数据。
- 策略使用默认的安全智能选项（仅全局阻止列表和非阻止列表），不使用 SSL 解密已加密的流量，并且不使用访问控制规则对网络流量执行特殊处理和检查。

可以采取用于调整入侵防御部署的一个简单步骤是使用系统提供的一组不同的网络分析和入侵策略为作为默认值。Cisco 通过系统提供若干对策略。

或者，您可以通过创建和使用自定义策略来定制入侵防御部署。您可能会发现这些策略中配置的检查器选项、入侵规则和其他高级设置无法满足网络的安全需求。通过调整网络分析和入侵策略，可以非常精细地配置系统如何处理网络流量并检测其是否存在入侵。

系统提供的网络分析和入侵策略

Cisco通过系统提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用 Cisco Talos 智能组 (Talos) 的经验。对于这些策略，Talos 提供入侵和检查器规则状态及对检查器和其他高级设置的初始配置。

没有哪一个系统提供的策略能够涵盖所有的网络配置文件、流量组合或防御安全状况。但每个此类策略都涵盖常见情况和网络设置，为提供精细调整的防御策略奠定基础。虽然您可以按原样使用系统提供的策略，但思科强烈建议您将其作为自定义策略的基础，对其进行调整以适合您的网络。

提示 即使您使用系统提供的网络分析和入侵策略，也应该配置系统的入侵变量，以准确反映网络环境。至少应修改默认变量集中的关键默认变量。

随着新的漏洞被发现，Talos 会发布入侵规则更新，又名 轻量安全安装包 (LSP)。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及检查器规则、

现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

如果规则更新影响您的部署，则网络界面将受影响的入侵和网络分析策略标记为已过期，并标记其父访问控制策略。您必须重新部署已更新的策略才能使其更改生效。

为方便起见，可以将规则更新配置为自动重新部署受影响的入侵策略（单独或与受影响的访问控制策略组合）。这使您能够轻松、自动保持部署为最新，以防范最近发现的漏洞和入侵。

为了确保获得最新的预处理设置，**必须**重新部署访问控制策略，该策略也会重新部署与当前运行的策略不同的所有关联的 SSL、网络分析和文件策略，同时还可以更新高级预处理和性能选项的默认值。

Cisco 通过系统提供以下网络分析和入侵策略：

“平衡安全和连接”网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数组织和部署类型的良好起点。系统在大多数情况下均使用“平衡安全和连接”策略和设置作为默认值。

连接优先于安全网络分析和入侵策略

这些策略专为连接性（能够获取所有资源）优先于网络基础设施安全性的组织而构建。此入侵策略启用的规则远远少于“安全优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。

“安全优先于连接”网络分析和入侵策略

这些策略专为网络基础设施安全性优先于用户便利性的组织而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。

“最大检测”网络分析和入侵策略

此类策略适用于网络基础设施安全性比在“安全性优先于连接”(Security Over Connectivity) 策略中还要重要，有可能产生更大运营影响的组织。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。

无活动规则入侵策略

在“无活动规则”入侵策略中，所有入侵规则和所有高级设置（除入侵规则阈值外）均已禁用。如果您要创建自己的入侵策略而不是将其基于系统提供的其他策略之一中的已启用规则，可以尝试使用此策略。

注释 根据所选的系统提供的基本策略，该策略的设置有所不同。要查看策略设置，请点击策略旁边的**编辑**图标，然后点击**基本策略**链接。

自定义网络分析和入侵策略的优势

您可能会发现系统提供的网络分析和入侵策略中配置的检查器选项、入侵规则和其他高级设置不完全满足贵组织的安全需要。

构建自定义策略可以提高环境中系统的性能，并且可以密切关注网络上发生的恶意流量和策略违例。通过创建和调整自定义策略，可以非常精细地配置系统如何处理和检查网络流量是否存在入侵。

所有自定义策略都具有基本策略（也称为基层），用于为策略中所有配置定义默认设置。层是可用于高效管理多个网络分析或入侵策略的构建块。

在大多数情况下，自定义策略基于系统提供的策略，但是可以使用其他自定义策略。不过，所有自定义策略在策略链中都以系统提供的策略作为最终基础。由于规则更新可能会修改系统提供的策略，因此导入规则更新可能会对您产生影响，即使使用自定义策略作为基础也如此。如果规则更新影响部署，则 Web 界面将受影响策略标记为过期。

自定义网络分析策略的优势

默认情况下，一个网络分析策略预处理访问控制策略处理的所有未加密流量。这意味着所有数据包都根据相同设置进行解码和预处理，无论后来使用哪种入侵策略（和因此使用的入侵规则集）对其进行检测。

最初，系统提供的 Balanced Security and Connectivity 网络分析策略是默认策略。调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。

可用的调整选项因检查器而异，但是可以调整检查器和解码器的一些方法包括：

- 可以禁用不适用于正在监控的流量的检查器。例如，HTTP Inspect 检查器规范化 HTTP 流量。如果确信网络中没有任何使用 Microsoft 互联网信息服务 (IIS) 的 Web 服务器，则可以禁用查找特定于 IIS 的流量的检查器选项，从而减少系统处理开销。

注释 如果禁用自定义网络分析策略中的检查器，但系统稍后需要使用该检查器利用已启用的入侵或检查器规则对数据包进行评估，系统会自动启用并使用检查器，不过它在网络分析策略 Web 界面中保持禁用。

- 指定端口（如果适用）以关注某些检查器的活动。例如，可以确定要对DNS服务器响应或加密 SSL 会话进行监控的其他端口，或者确定解码 telnet、HTTP 和 RPC 流量所在的端口

对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。（请注意，ASA FirePOWER 模块无法通过 VLAN 限制预处理。）

注释 使用自定义网络分析策略（尤其是多个网络分析策略）定制预处理是一个高级任务。由于预处理和入侵检测密切相关，因此，您**必须**注意，要确保允许检测单个数据包的网络分析和入侵策略能够互补。

自定义入侵策略的优势

在新建的初始配置为执行入侵防御的访问控制策略中，默认操作允许所有流量，但是首先会使用系统提供的 Balanced Security and Connectivity 入侵策略对流量进行检测。除非添加访问控制规则或更改默认操作，否则所有流量都由该入侵策略进行检查。

要自定义入侵防御部署，可以创建多个入侵策略，每个策略定制为以不同方式检测流量。然后，使用指定哪个策略检测哪个流量的规则来配置访问控制策略。访问控制规则可能很简单，也可能很复杂，使用多个条件来匹配和检测流量，包括安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL 或用户。

入侵策略的主要功能是管理启用哪些入侵和检查器规则及其如何配置，如下所示：

- 在每个入侵策略中，应该验证所有适用于环境的规则是否已启用，并且通过禁用不适用于环境的规则来提高性能。您可以指定哪些规则应该丢弃或修改恶意数据包。
- 如果遵从Cisco的建议，则可将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。
- 您可以修改现有规则并根据需要编写新的标准文本规则，以捕获新的漏洞或强制实施安全策略。

您可能对入侵策略进行的其他自定义包括：

- 敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他检查器。
- 全局阈值导致系统根据与入侵规则匹配的流量在指定时间段内源自或流向特定地址或地址范围的次数来生成事件。这有助于防止系统被大量事件淹没。
- 禁止入侵事件通知和设置个别规则或全体入侵策略的阈值也可以防止系统被大量事件淹没。
- 除了网络界面中的各种入侵事件视图之外，您还可以启用将日志记录到系统日志设施或者将事件数据发送到 SNMP 陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录设施的入侵事件通知，以及配置对入侵事件的外部响应。请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。

自定义策略的限制

由于预处理和入侵检测如此密切相关，因此，您**必须**小心确保自己的配置允许网络网络分析和入侵策略处理和检测单个数据包，以实现互补。

默认情况下，系统使用一个网络分析策略预处理由托管设备使用单个访问控制策略处理的所有流量。下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。

请留意默认网络分析策略如何监管访问控制策略处理的所有流量的预处理。最初，系统提供的Balanced Security and Connectivity 网络分析策略是默认策略。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。但是，如果在自定义网络分析策略中禁用检查器，但系统需要根据已启用的入侵或检查器规则评估预处理的数据包，则系统会自动启用并使用该检查器，尽管其在网络分析策略 Web 界面中保持禁用。

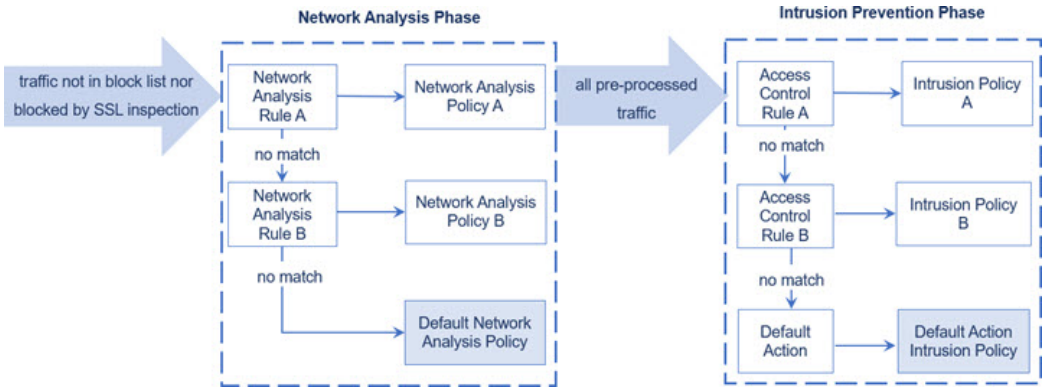
注释 要获取禁用检查器的性能优势，您 **必须** 确保自己的入侵策略均未启用需要该检查器的规则。

如果使用多个自定义网络分析策略，则会引起其他问题。对于使用复杂部署的高级用户，可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 自定义预处理。（请注意，ASA FirePOWER 模块无法通过 VLAN 限制预处理。）为此，请向访问控制策略中添加自定义网络分析规则。每条规则均具有关联的网络分析策略，用于监管与该规则匹配的流量的预处理。

提示 可以将网络分析规则配置为访问控制策略中的高级设置。与其他类型的规则不同，网络分析规则调用网络分析策略，而不是被其包含。

系统按规则号由上而下将数据包与任何已配置的网络分析规则相匹配。不与任何网络分析规则相匹配的流量由默认网络分析策略预处理。虽然这使您在预处理流量时具有极大灵活性，但请记住，所有数据包**无论**由哪个网络分析策略进行了预处理，后来都会在各自的进程中与访问控制规则匹配，从而可能会接受入侵策略的检查。换句话说，使用特定网络分析策略预处理数据包**不**保证将通过任何特殊入侵策略检测该数据包。您**必须**仔细配置访问控制策略，以使其调用正确的网络分析和入侵策略来评估特殊数据包。

下图集中细解了网络分析策略（预处理）选择阶段如何在入侵防御（规则）阶段之前发生并与其分隔开来。为简单起见，此图省去了发现和文件/恶意软件检查阶段。它还突出显示默认网络分析和默认操作入侵策略。



在此情景中，访问控制策略配置有两条网络分析规则和一个默认网络分析策略：

- 网络分析规则 A 使用网络分析策略 A 预处理匹配流量。之后，您希望此流量由入侵策略 A 进行检测。

- 网络分析规则 B 使用网络分析策略 B 预处理匹配流量。之后，您希望此流量由入侵策略 B 进行检测。
- 所有剩余流量都使用默认网络分析策略进行预处理。之后，您希望此流量由与访问控制策略的默认操作关联的入侵策略进行检测。

系统在预处理流量之后，可以检测流量是否存在入侵。该图显示具有两条访问控制规则和一个默认操作的访问控制策略：

- 访问控制规则 A 允许匹配流量。然后，流量由入侵策略 A 进行检测。
- 访问控制规则 B 允许匹配流量。然后，流量由入侵策略 B 进行检测。
- 访问控制策略的默认操作允许匹配流量。然后，流量由默认操作的入侵策略进行检测。

每个数据包的处理均由网络分析策略和入侵策略对进行监管，但系统**不**为您协调该对。请考虑以下情景：访问控制策略配置错误，以致网络分析规则 A 和访问控制规则 A 不处理相同流量。例如，您可能希望配对的策略监管特殊安全区域上流量的处理，但是在两条规则的条件中错误地使用不同的区域。这可能会导致错误地预处理流量。因此，使用网络分析规则和自定义策略定制预处理是一项**高级**任务。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略，但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这**不**影响您在自定义网络分析策略中配置预处理的方式。

网络分析和入侵策略的必备条件

要允许 Snort 检测引擎处理流量以进行入侵和恶意软件分析，必须为 防火墙威胁防御 设备启用 IPS 许可证。

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。