网络分析和入侵策略概述

以下主题概述 Snort 检测引擎以及网络分析和入侵策略：

网络分析和入侵策略基础知识

网络分析和入侵策略作为系统的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”。

注释 如果您使用的是 Snort 3 和 SSL 解密或 TLS 服务器身份，则您必须在**预防**模式下配置网络分析策略 (NAP)。当 Snort 3 NAP 处于检测模式时，SSL 功能将不会起作用。

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Talos 情报小组 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，以及提供预处理器和其他高级设置的初始配置。

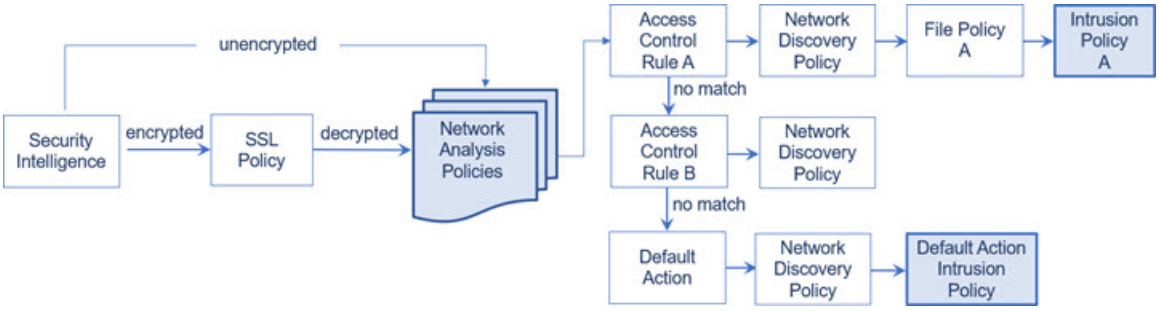
您还可以创建自定义网络分析和入侵策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

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。

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内联、入侵防御和恶意软件防护 部署中的流量分析顺序。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预处理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预处理程序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。

注释 在被动部署中，思科建议您在访问控制策略级别启用自适应配置文件更新，而非在网络分析级别配置内联规范化。

- 各种网络层和传输层预处理器检测利用 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预处理程序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 预处理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。
- 通过若干预处理器，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预处理器，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）。

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。

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 2 页中的图显示流经内联部署、入侵防御部署和恶意软件防护 部署中设备的流量，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 预处理程序 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。

系统包含Talos 情报小组 创建的以下类型的规则：

- 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。
- 预处理程序 规则，是指与网络分析策略中的 预处理程序 和数据包解码器检测选项关联的规则。不能复制或编辑 预处理程序 规则。默认情况下，大多数 预处理器 规则是被禁用的；您必须启用它们才可以 对 生成事件并在内联部署中丢弃攻击性数据包使用 预处理器 。

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。还可以遵从思科 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。

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。

相关主题

预定义默认变量

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）。受管设备将其事件传输到管理中心，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，受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，则系统会生成预处理程序事件。
- 如果 IP 分片重组预处理程序遇到一系列重叠的 IP 片段，则预处理程序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，系统会生成预处理程序事件。
- 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。

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。

图 *1:* 新的访问控制策略：入侵防御

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情报选项（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预处理程序选项、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Talos 情报小组 的经验。对于这些策略，Talos 会提供入侵和预处理器规则状态，以及预处理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 （也称为 *Snort* 规则更新）。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预处理程序规则、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**管理基本策略**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预处理程序选项、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由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。

可用的调整选项因预处理程序而异，但是可以调整预处理程序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预处理程序。例如，HTTP Inspect 预处理程序规范化 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 的流量的预处理程序选项，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预处理器，但系统稍后需要使用该预处理器利用已启用的入侵或预处理器规则对数据包进行评估，系统会自动启用并使用预处理器，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）以关注某些预处理程序的活动。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。

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预处理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。在内联部署中，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）的其他预处理程序。
- 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工具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工具的入侵事件通知，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受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。

图 *2:* 新的访问控制策略：入侵防御

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预处理器，但系统需要根据已启用的入侵或预处理器规则评估预处理的数据包，则系统会自动启用并使用该预处理器，尽管其在网络分析策略 Web 界面中保持禁用。

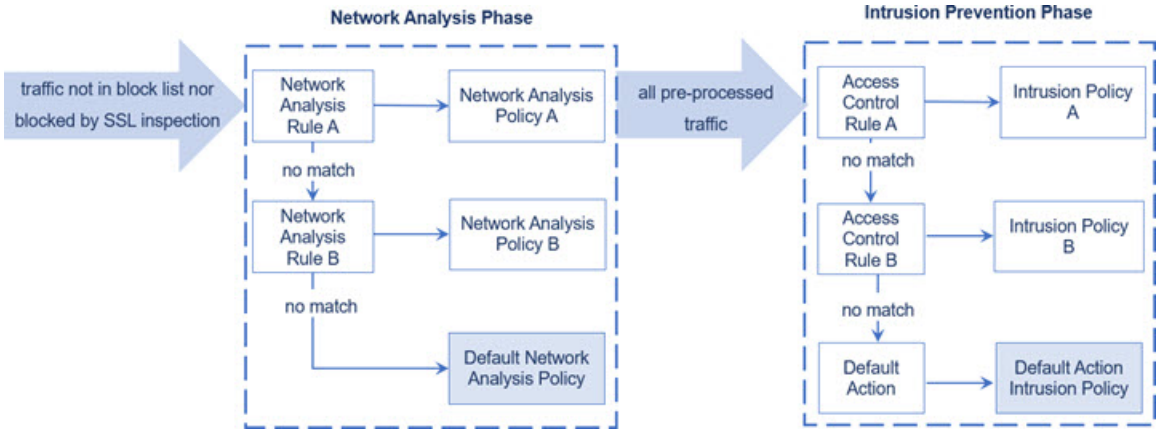
注释 要获取禁用预处理程序的性能优势，您**必须**确保自己的入侵策略均未启用需要该预处理程序的规则。

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。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。与系统中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许可证要求

威胁防御 许可证

IPS

经典许可证

保护

网络分析和入侵策略的要求和必备条件

型号支持

任意。

支持的域

任意

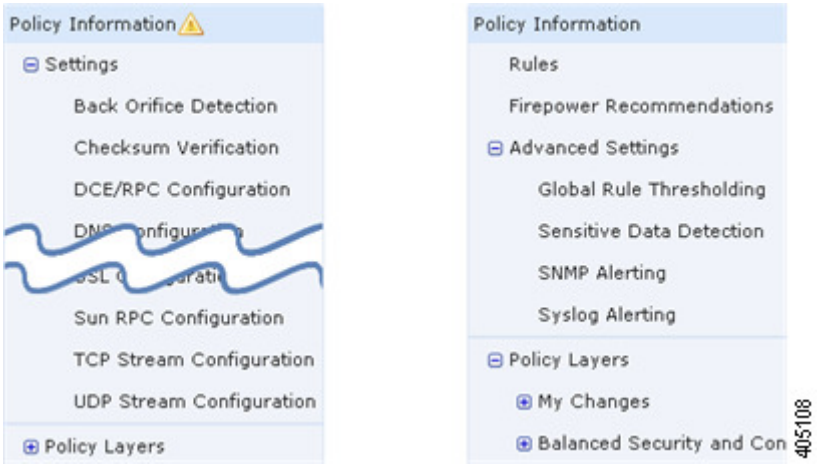
用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

导航面板：网络分析和入侵策略

网络分析和入侵策略使用类似的 Web 界面编辑和保存对其配置进行的更改。

编辑任一类型的策略时，导航面板会出现在网络界面左侧。下图显示网络分析策略（左）和入侵策略（右）的导航面板。



分隔线将导航面板分隔成指向策略设置的链接，可以通过（下方）或不通过（上方）与策略层的直接交互来配置这些设置。要导航到任何设置页面，请在导航面板中点击其名称。某项在导航面板中的浓阴影突出显示当前设置页面。例如，在上方的插图中，“策略信息”页面会显示到导航面板的右侧。

策略信息

“策略信息”页面提供常用设置的配置选项。如以上网络分析策略面板的插图所示，当策略包含未保存的更改时，在导航面板中的**策略信息 (Policy Information)** 旁边会显示**策略更改图标**。保存更改后，该图标消失。

规则（仅入侵策略）

通过入侵策略中的“规则”(Rules) 页面，您可以为共享对象规则、标准文本规则和预处理器规则配置规则状态和其他设置。

思科 建议（仅入侵策略）

通过入侵策略中的“思科 建议”页面，您可以将在网络上检测到的操作系统、服务器和客户端应用协议与专门编写用于保护这些资产的入侵规则相关联。这样，您就可根据自己的受监控网络的特定需求定制您的入侵策略。

设置（网络分析策略）和高级设置（入侵策略）

网络分析策略中的“设置”(Settings) 页面可供您启用或禁用预处理程序以及访问预处理程序配置页面。展开 **Settings** 链接会显示指向策略中所有已启用预处理程序的个别配置页面的子链接。

入侵策略中的Advanced Settings页面可供您启用或禁用高级设置以及访问这些高级设置的配置页面。展开 **Advanced Settings** 链接会显示指向策略中所有已启用高级设置的个别配置页面的子链接。

策略层

“策略层”(Policy Layers) 页面显示构成网络分析或入侵策略的各层的摘要。展开“策略层”(Policy Layers) 链接会显示指向策略中的各层的摘要页面的子链接。展开各层子链接会显示指向层中已启用的所有规则、预处理程序或高级设置的配置页面的进一步子链接。

冲突和更改：网络分析和入侵策略

在编辑网络分析或入侵策略时， **策略更改图标** 显示在导航面板中**策略信息 (Policy Information)** 的旁边以指示策略包含未保存的更改。必须首先保存（或提交）更改，然后系统才会认可这些更改。

注释 保存后，必须部署网络分析或入侵策略，更改才会生效。如果部署策略而不保存，则系统会使用最新保存的配置。

解决编辑冲突

“网络分析策略”页面（**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**）和“入侵策略”页面（**策略** > **访问控制** > **入侵**）显示每个策略是否有未保存的更改，以及有关当前正在编辑策略的用户的信息。思科建议每次仅由一位人员编辑一个策略。如果执行同时编辑，则将产生以下后果：

- 如果在您编辑某条网络分析或入侵策略的同时另一用户也在编辑该策略，并且该用户保存对此策略的更改，则当您提交策略时系统将警告您会覆盖另一用户的更改。
- 如果以同一用户身份通过多个网络界面实例编辑同一网络分析或入侵策略，而且，您保存对一个实例的更改，则无法保存对其他实例的更改。

解析配置依赖关系

为了执行特殊分析，许多预处理程序和入侵规则均要求流量首先以某种方式得以解码或预处理，或者具有其他依存关系。保存网络分析或入侵策略时，系统会自动启用必需的设置，或者警告您已禁用的设置不会影响流量，如下所示：

- 如果已添加 SNMP 规则警报，但未配置 SNMP 告警，则无法保存入侵策略。必须配置 SNMP 告警或禁用规则警报，然后再次保存。
- 如果入侵策略包含已启用的敏感数据规则，但是您尚未启用敏感数据预处理程序，则无法保存该入侵策略。必须允许系统启用预处理程序并保存策略，或者禁用规则并再次保存。
- 如果在网络分析策略中禁用必需的预处理程序，则仍然可以保存该策略。但是，系统会通过已禁用预处理程序的当前设置使用该预处理程序，即使该预处理程序在网络界面中保持禁用亦如此。
- 如果在网络分析策略中禁用内联模式，但是启用内联规范化预处理程序，则仍然可以保存该策略。不过，系统会警告您将忽略规范化设置。禁用内联模式还会导致系统忽略允许预处理程序修改或阻止流量的其他设置，包括校验和验证和基于速率的攻击防御。

提交、丢弃和缓存策略更改

在编辑网络分析或入侵策略时，如果退出策略编辑器而不保存更改，则系统会缓存这些更改。即使注销系统或系统崩溃，仍然会缓存更改。系统缓存可以按照每个用户一个网络分析和一个入侵策略来存储未保存的更改；编辑同一类型的另一个策略之前，必须提交或放弃更改。编辑另一个策略而不保存对第一个策略的更改时，或者导入入侵规则更新时，系统会丢弃缓存的更改。

您可以在网络分析或入侵策略编辑器的“策略信息”(Policy Information) 页面上提交或丢弃策略更改。

在 Cisco Secure Firewall Management Center配置中，您可以控制：

- 是否提示（或要求）您在提交网络分析或入侵策略更改时对其添加注释
- 是否将更改和注释记录到审核日志中

退出网络分析或入侵策略

过程

如果要退出网络分析或入侵策略高级编辑器，您有以下选择：

- 缓存 - 要退出策略和缓存更改，请选择任何菜单或指向另一个页面的其他路径。请在系统提示时点击**离开页面 (Leave page)** 退出，或者点击**停留在页面上 (Stay on page)** 停留在高级编辑器中。
- 放弃 - 要放弃未保存的更改，请点击“策略信息”(Policy Information) 页面上的**放弃更改 (Discard Changes)**，然后点击**确定 (OK)**。
- 保存 - 要保存对策略的更改，请点击“策略信息”(Policy Information) 页面上的**确认更改 (Commit Changes)**。如果出现提示，请输入注释，然后点击**确认 (OK)**。

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。