应用层预处理器

以下主题介绍应用层预处理器及其配置方法：

应用层预处理器简介

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

应用层协议可以通过多种方式表示相同的数据。Firepower 系统提供应用层协议解码器，这些解码器可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。规范化应用层协议编码使得规则引擎可以有效地将相同的内容相关规则应用于其数据以不同方式呈现的数据包，并获得有意义的结果。

当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

请注意，大多数情况下，除非在入侵策略中启用随附预处理器规则，否则预处理器不会生成事件。

应用层预处理器的许可证要求

威胁防御 许可证

IPS

应用层预处理器的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员

DCE/RPC 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

DCE/RPC 协议使不同网络主机上的进程可以像在同一主机上一样进行通信。这些进程间通信一般通过 TCP 和 UDP 在主机之间传输。在 TCP 传输中，DCE/RPC 也可以进一步封装在 Windows 服务器消息块 (SMB) 协议或 Samba 中；Samba 是一种在由 Windows 和类似 UNIX 或类似 Linux 操作系统组成的混合环境中用于进程间通信的开源 SMB 实现。此外，网络上的 Windows IIS Web 服务器可能使用 IIS RPC over HTTP，后者通过防火墙向代理 TCP 传输 DCE/RPC 流量提供分布式通信。

请注意，对 DCE/RPC 预处理器选项和功能的说明包括 DCE/RPC 的 Microsoft 实现（又称为 MSRPC）；对 SMB 选项和功能的说明涉及 SMB 和 Samba。

虽然大多数 DCE/RPC 漏洞出现在针对 DCE/RPC 服务器（实际上可能是网络上运行 Windows 或 Samba 的任何主机）的 DCE/RPC 客户端请求中，但在服务器响应中也可能出现漏洞。DCE/RPC 预处理器检测封装在 TCP、UDP 和 SMB 传输（包括使用版本 1 RPC over HTTP 的 TCP 传输 DCE/RPC）中的 DCE/RPC 请求和响应。此预处理器分析 DCE/RPC 数据流并检测 DCE/RPC 流量中的异常行为和逃避技术。它还分析 SMB 数据流并检测异常 SMB 行为和逃避技术。

除 IP 分片重组预处理器提供的 IP 分片重组和 TCP 数据流预处理器无缝提供的 TCP 数据流以外，DCE/RPC 预处理器还会将 SMB 分段重组并将 DCE/RPC 分片重组。

最后，DCE/RPC 预处理器会规范化 DCE/RPC 流量，以便规则引擎进行处理。

无连接和面向连接的 DCE/RPC 流量

DCE/RPC 消息符合两种不同的 DCE/RPC 协议数据单元（PDU）之一：

面向连接的 DCE/RPC PDU 协议

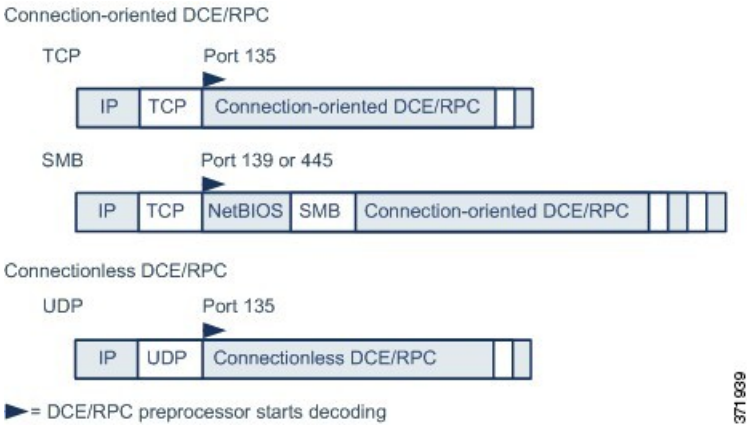
DCE/RPC 预处理器在 TCP、SMB 和 RPC over HTTP 传输中检测面向连接 DCE/RPC。

无连接 DCE/RPC PDU 协议

DCE/RPC 预处理器在 UDP 传输中检测无连接 DCE/RPC。

这两种 DCE/RPC PDU 协议都有独特的报头和数据特性。例如，面向连接的 DCE/RPC 的报头长度通常为 24 字节，而无连接 DCE/RPC 的报头长度固定为 80 字节。此外，分片无连接 DCE/RPC 的正确分片顺序不能通过无连接传输处理，而必须通过无连接 DCE/RPC 报头值提供保证；相比之下，传输协议可确保面向连接 DCE/RPC 的分片顺序正确。DCE/RPC 预处理器使用这些特性及其他特定协议特性监控这两种协议是否存在异常和其他躲避技术，对流量进行解码和分片重组，然后再将流量传送到规则引擎。

下图说明了 DCE/RPC 预处理器开始为不同传输处理 DCE/RPC 流量的点。



对于上图，请注意以下几点：

- 已知 TCP 或 UDP 端口 135 识别 TCP 和 UDP 传输中的 DCE/RPC 流量。
- 图中未包含 RPC over HTTP。

对于 RPC over HTTP，面向连接 DCE/RPC 在完成 HTTP 初始设置序列后直接通过 TCP 传输（如图所示）。

- DCE/RPC 预处理器通常接收适用于 NetBIOS 会话服务的已知 TCP 端口 139 或以类似方式实现的已知 Windows 端口 445 上的 SMB 流量。

  由于 SMB 具有除传输 DCE/RPC 以外的许多功能，因此，预处理器会首先测试 SMB 流量是否携带 DCE/RPC 流量，如果不是则停止处理，如果是则继续处理。

- IP 封装所有 DCE/RPC 传输。
- TCP 传输所有面向连接 DCE/RPC。
- UDP 传输无连接 DCE/RPC。

DCE/RPC 基于目标的策略

Windows 和 Samba DCE/RPC 的实现有很大不同。例如，在对 DCE/RPC 流量进行分片重组时，所有 Windows 版本都在第一个分片中使用 DCE/RPC 上下文 ID，而所有 Samba 版本都在最后一个分片中使用上下文 ID。再如，Windows Vista 在第一个分片中使用操作编号报头字段来识别特定函数调用，而 Samba 及其他所有 Windows 版本都在最后一个分片中使用操作编号字段。

Windows 和 Samba SMB 的实现也有很大不同。例如，Windows 在与命名管道配合使用时可识别 SMB OPEN 和 READ 命令，而 Samba 不能识别这些命令。

启用 DCE/RPC 预处理器会自动启用默认基于目标的策略。或者，您可以添加将运行不同 Windows 或 Samba 版本的其他主机设为目标的基于目标的策略。默认基于目标的策略适用于未包含在其他基于目标的策略的任何主机。

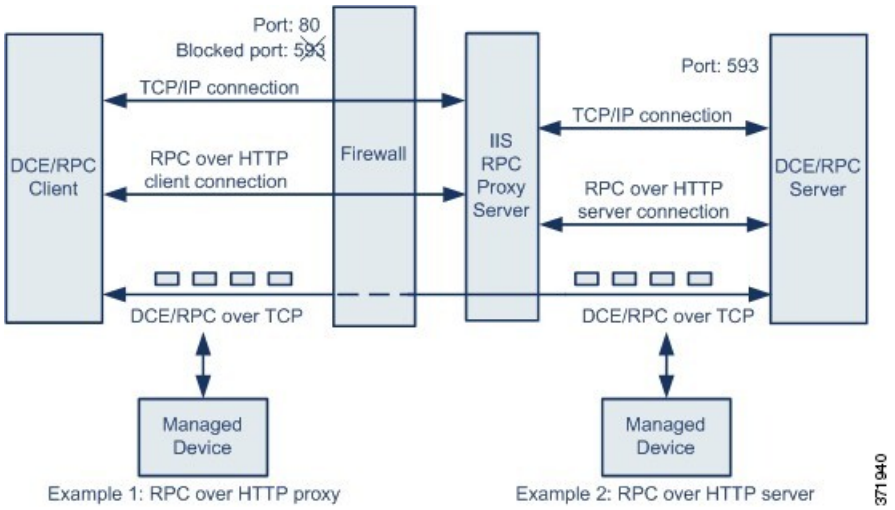
在每个基于目标的策略中，可以：

- 启用一个或多个传输并为每个传输指定检测端口
- 启用并指定自动检测端口
- 设置预处理器，以检测尝试连接到一个或多个所识别的共享 SMB 资源的情况
- 将预处理器配置为检测 SMB 流量中的文件，以及检查检测到的文件中的指定字节数
- 修改应仅由具备 SMB 协议专业知识的用户修改的高级选项；通过该选项，可以将预处理器设置为检测链式 SMB AndX 命令数量超过指定最小数量的情况

除在 DCE/RPC 预处理器中启用 SMB 流量文件检测以外，还可以配置文件策略以选择性地捕获和阻止这些文件，或者将这些文件提交到思科 AMP 云以进行动态分析。在策略中，必须创建具有**操作**为 **Detect Files** 或 **Block Files** 且选定**应用协议**为 **Any** 或 **NetBIOS-ssn (SMB)** 的文件规则。

RPC over HTTP 传输

借助 Microsoft RPC over HTTP，可以引导 DCE/RPC 流量穿过防火墙，如下图所示。DCE/RPC 预处理器检测版本 1 Microsoft RPC over HTTP。



Microsoft IIS 代理服务器和 DCE/RPC 服务器可以位于同一主机上，也可以位于不同的主机上。对于这两种情况，我们提供独立的代理和服务器选项。对于上图，请注意以下几点：

- DCE/RPC 服务器监控端口 593 的 DCE/RPC 客户端流量，但防火墙阻止该端口。

  默认情况下，防火墙通常会阻止端口 593。

- RPC over HTTP 使用已知 HTTP 端口 80（防火墙很可能允许此端口）通过 HTTP 传输 DCE/RPC。
- 在示例 1 中，将会选择 **RPC over HTTP 代理 (RPC over HTTP proxy)** 选项来监控 DCE/RPC 客户端和 Microsoft IIS RPC 代理服务器之间流量。
- 在示例 2 中，如果 Microsoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机，且设备监控这两个服务器之间的流量，将会选择 **RPC OVER HTTP 服务器 (RPC OVER HTTP SERVER)** 选项。
- RPC over HTTP 完成 DCE/RPC 客户端和服务器代理设置后，流量仅包含通过 TCP 传输的面向连接 DCE/RPC。

DCE/RPC 全局选项

DCE/RPC 预处理器全局选项控制预处理器的工作方式。请注意，除**已达到内存限制 (Memory Cap Reached)** 和 **SMB 会话上自动检测策略 (Auto-Detect Policy on SMB Session)** 这两个选项外，修改这些选项可能会对性能或检测能力造成负面影响。除非您已充分理解此预处理器及其与已启用的 DCE/RPC 规则之间的交互，否则请勿修改这些选项。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

最大分片大小 (Maximum Fragment Size)

当选择**启用分片重组 (Enable Defragmentation)** 时，可指定允许的最大 DCE/RPC 分片长度。预处理器会在分片重组前将较大分片截断成为指定的尺寸以便进行处理，但不会改变实际数据包。空白字段将禁用此选项。

确保**最大分片大小 (Maximum Fragment Size)** 选项大于或等于规则需要检测到的深度。

重组阈值 (Reassembly Threshold)

当选择**启用分片重组 (Enable Defragmentation)** 时，0 表示禁用此选项，或者指定分片 DCE/RPC 最小字节数，并且如果适用，则指定在向规则引擎发送已重组的数据包之前要加入队列的分段 SMB 字节数。值越小，实现早期检测的可能性越高，但可能会对性能造成负面影响。如果启用此选项，应当测试性能所受的影响。

确保**重组阈值 (Reassembly Threshold)** 选项大于或等于规则需要检测到的深度。

启用分片重组 (Enable Defragmentation)

指定是否对 DCE/RPC 流量进行分片重组。当此选项处于禁用状态时，预处理器仍会检测异常并向规则引擎发送 DCE/RPC 数据，但可能会检测不出分片 DCE/RPC 数据中的漏洞。

尽管通过此选项可灵活选择是否对 DCE/RPC 流量进行分片重组，但大多数 DCE/RPC 漏洞都会尝试利用分片隐藏自己。禁用此选项将会忽略大多数已知漏洞，从而造成大量误报。

已达到内存限制 (Memory Cap Reached)

检测达到或超过分配给预处理器的最大内存限制的时间。当达到或超过最大内存上限时，预处理器会释放与造成内存上限事件的会话相关的所有待处理数据并忽略该会话的剩余部分。

您可以启用规则 133:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

SMB 会话上自动检测策略 (Auto-Detect Policy on SMB Session)

检测在 SMB `Session Setup AndX` 请求和响应中识别出的 Windows 或 Samba 版本。如果检测到的版本不同于为**策略 (Policy)** 配置选项配置的 Windows 或 Samba 版本，检测到的版本将会仅覆盖为该会话配置的版本。

例如，如果将**策略 (Policy)** 设置为 Windows XP，而预处理器检测到 Windows Vista，则预处理器将对该会话使用 Windows Vista 策略。其他设置仍然有效。

如果 DCE/RPC 传输不是 SMB（即传输协议为 TCP 或 UDP 时），则无法检测到版本，并且策略不能实现自动配置。

要启用此选项，请从下拉列表中选择以下其中一项：

- 选择**客户端 (Client)**，检查该策略类型的服务器到客户端流量。
- 选择**服务器 (Server)**，检查该策略类型的客户端到服务器流量。
- 选择**两者 (Both)**，检查该策略类型的服务器到客户端流量和客户端到服务器流量。

传统 SMB 检测模式 (Legacy SMB Inspection Mode)

如果启用了**传统 SMB 检测模式 (Legacy SMB Inspection Mode)**，则系统只会将 SMB 入侵规则应用于 SMB 版本 1 流量，并将 DCE/RPC 入侵规则应用于使用 SMB 版本 1 作为传输的 DCE/RPC 流量。

如果禁用此选项，系统会将SMB入侵规则应用于使用SMB版本1、2和3的流量，但会将DCE/RPC入侵规则应用于使用 SMB 作为 SMB 版本 1 传输的 DCE/RPC 流量。

相关主题

基本 content 和 protected_content 关键字参数
概述：byte_jump 和 byte_test 关键字

DCE/RPC 基于目标的策略选项

在每个基于目标的策略中，都可以启用一个或多个TCP、UDP、SMB和RPC over HTTP传输。启用传输时，还必须指定一个或多个检测端口（即，已知用于传输 DCE/RPC 流量的端口）。

思科建议使用默认检测端口，这些端口可以是已知端口，也可以是各协议的常用端口。在非默认端口检测到 DCE/RPC 流量的情况下才可以添加端口。

可以在Windows基于目标的策略中为一个或多个传输指定任意组合的端口，以便与网络流量匹配，但是，在Samba基于目标的策略中只能为SMB传输指定端口。

注释 在基于目标的默认策略中必须至少启用一个 DCE/RPC 传输，除非已添加至少启用了一个传输的 DCE/RPC 基于目标的策略。例如，可能要为所有 DCE/RPC 实施指定主机且不将基于目标的默认策略部署到未指定的主机，在此情况下，不会为基于目标的默认策略启用传输。

或者，也可以启用和指定自动检测端口；预处理器会首先对这些端口进行测试，以确定它们是否传输 DCE/RPC 流量，仅在检测到 DCE/RPC 流量的情况下，预处理器才会继续进行处理。

启用自动检测端口时，请确保将端口范围设置为 1024 到 65535，以便覆盖整个临时端口范围。

请注意，仅对于传输检测端口尚未识别的端口才会出现自动检测。

对于“RPC over HTTP 代理自动检测端口”(RPC over HTTP Proxy Auto-Detect Ports) 选项或“SMB自动检测端口”(SMB Auto-Detect Ports) 选项，不太可能会启用或指定自动检测端口，因为除非是在指定的默认检测端口上，否则任一端口出现流量的可能性极低甚至不可能出现。

每个基于目标的策略都允许指定以下各个选项。如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络 (Networks)

要部署DCE/RPC基于目标的服务器策略的主机IP地址。此外，当添加基于目标的策略时，命名“添加目标”(Add Target) 弹出窗口中的**服务器地址 (Server Address)** 字段。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可以配置总共255 个配置文件，包括默认策略。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定IP地址或CIDR块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

策略

目标主机或受监控网段上主机使用的 Windows 或 Samba DCE/RPC 实现。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖每个会话的此选项的设置。

SMB Invalid Shares

用于在尝试连接到指定的共享资源时，识别预处理器将检测的一个或多个SMB共享资源。您可以在逗号分隔列表中指定多个共享，或者可以将共享用引号引起来（旧版软件要求这样做，但现在不再有此要求），例如：

```
"C$", D$, "admin", private
```

启用 **SMB 端口 (SMB Ports)** 后，预处理器会检测 SMB 流量中的无效共享。

请注意，大多数情况下，对于被识别为无效共享的 Windows 命名的驱动器，应该在其后面附上一个美元符号。例如，将驱动器 C 标识为 C$ 或 "C$"。

另请注意，要检测 SMB 无效共享，还必须启用 **SMB 端口 (SMB Ports)** 或 **SMB 自动检测端口 (SMB Auto-Detect Ports)**。

可以启用规则 133:26 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

SMB Maximum AndX Chain

允许的链式 SMB AndX 命令的最大数量。通常，超过若干链式 AndX 命令即表示存在异常行为，可能代表有躲避行为。指定 1 表示不允许链式命令，指定 0 将会禁止检测链式命令数量。

请注意，预处理器会首先计算链式命令数量，如果随附的SMB预处理器规则已启用，并且链式命令数量等于或超过配置的值，预处理器将会生成事件。然后会继续进行处理。

注意　只有 SMB 协议专业人员可以修改 **SMB Maximum AndX Chains** 选项的设置。

可以启用规则 133:20 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

RPC proxy traffic only

启用 **RPC over HTTP 代理端口 (RPC over HTTP Proxy Ports)** 指示检测到的客户端 RPC over HTTP 流量只是代理流量还是可能包含其他 Web 服务器流量。例如，端口 80 可能传输代理流量和其他网络服务器流量。

此选项处于禁用状态时，将会同时传输代理流量和其他网络服务器流量。例如，如果服务器是专用代理服务器，请启用此选项。启用此选项后，预处理器会测试流量以确定其是否传输DCE/RPC，如果不是，预处理器将会忽略该流量，如果是，则继续进行处理。请注意，仅在已选择**RPC over HTTP 代理端口 (RPC over HTTP Proxy Ports)** 复选框的情况下，此选项才有用。

RPC over HTTP 代理端口 (RPC over HTTP Proxy Ports)

如果托管设备位于 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间，可以使用此选项对 RPC over HTTP 通过每个指定端口传输的 DCE/RPC 流量启用检测。

启用此选项后，可以添加任意发现DCE/RPC流量的端口，但是这项操作一般并不必要，因为网络服务器通常使用默认端口传输 DCE/RPC 和其他流量。启用此选项后，不可以启用 **RPC over HTTP 代理自动检测端口 (RPC over HTTP Proxy Auto-Detect Ports)**，但如果检测到的客户端 RPC over HTTP 流量仅包含代理流量而不包含其他网络服务器流量，则可以启用**仅 PRC 代理流量 (RPC Proxy Traffic Only)**。

注释 如有可能，很少会选择此选项。

RPC over HTTP Server Ports

当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间流量时，对每个指定端口上通过 RPC over HTTP 传输的 DCE/RPC 流量启用检测。

启用此选项后，通常还应启用 **RPC over HTTP 服务器自动检测端口 (RPC over HTTP Server Auto-Detect Ports)**（端口范围介于 1025 到 65535 之间），即使不知道网络上是否存在任何代理网络服务器。请注意，RPC over HTTP 服务器端口有时会重新配置，在这种情况下，应该为此选项将重新配置的服务器端口添加到端口列表。

TCP 端口

对每个指定端口上 TCP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **TCP 自动检测端口 (TCP Auto-Detect Ports)**（端口范围介于 1025 到 65535 之间），即使不知道网络上是否存在任何代理网络服务器。

UDP 端口

对每个指定端口上 UDP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **UDP 自动检测端口 (UDP Auto-Detect Ports)**（端口范围介于 1025 到 65535 之间）。

SMB 端口 (SMB Ports)

对每个指定端口上 SMB 中的 DCE/RPC 流量启用检测。

可能会出现使用默认检测端口的 SMB 流量。其他端口很少见。通常使用默认设置。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖为每个会话的目标策略配置的策略类型。

RPC over HTTP Proxy Auto-Detect Ports

如果托管设备位于 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间，可以使用此选项对 RPC over HTTP 通过指定端口传输的 DCE/RPC 流量启用自动检测。

启用此选项后，通常需要指定介于 1025 到 65535 之间的端口范围，以覆盖整个临时端口范围。

RPC over HTTP 服务器自动检测端口 (RPC over HTTP Server Auto-Detect Ports)

当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间流量时，对指定端口上通过 RPC over HTTP 传输的 DCE/RPC 启用自动检测。

TCP 自动检测端口 (TCP Auto-Detect Ports)

对指定端口上 TCP 中的 DCE/RPC 流量启用自动检测。

UDP 自动检测端口 (UDP Auto-Detect Ports)

对每个指定端口上 UDP 中的 DCE/RPC 流量启用自动检测。

SMB 自动检测端口 (SMB Auto-Detect Ports)

对 SMB 中的 DCE/RPC 流量启用自动检测。

注释 如有可能，很少会选择此选项。

SMB 文件检查 (SMB File Inspection)

启用 SMB 流量检查以检测文件。您有以下选择：

- 选择**关闭 (Off)** 禁用文件检查。
- 选择**仅限 (Only)**，检查文件数据但不检查 SMB 中的 DCE/RPC 流量。选择此选项可以提高文件和 DCE/RPC 流量检查性能。
- 选择**打开 (On)**，检查 SMB 中的文件和 DCE/RPC 流量。选择此选项可能会影响性能。

以下各项不支持 SMB 流量检查：

- 单一 TCP 或 SMB 会话同时传输的文件
- 在多个 TCP 或 SMB 会话之间传输的文件
- 与非连续数据一起传输的文件（例如，协商了消息签名时）
- 与具有相同偏移量的不同数据一起传输的文件（与数据重叠）
- 在远程客户端打开用于编辑并由客户端保存到文件服务器的文件

SMB 文件检查深度 (SMB File Inspection Depth)

如果 **SMB 文件检查 (SMB File Inspection)** 设置为**仅限 (Only)** 或**打开 (On)**，此选项表示在 SMB 流量中检测到文件时检查的字节数。指定以下各项之一：

- 正值
- `0` 以检查整个文件
- `-1` 以禁用文件检查

在此字段中输入小于或等于访问控制策略中“高级”(Advanced)选项卡的“文件和恶意软件设置”(File and Malware Settings) 部分中定义的值。如果为此选项设置的值大于为**限制执行文件类型检测时检查到的字节数 (Limit the number of bytes inspected when doing file type detection)** 定义的值，则系统使用访问控制策略设置作为有效的最大值。

如果 **SMB File Inspection** 设置为 **Off**，此字段将被禁用。

与流量关联的 DCE/RPC 规则

大多数 DCE/RPC 预处理器规则都会针对 SMB、面向连接的 DCE/RPC 或无连接 DCE/RPC 流量中检测到的异常和规避技术触发。下表列出了可为各类流量启用的规则。

表 *1:* 与流量关联的 *DCE/RPC* 规则

交通	预处理器规则 GID:SID
中小企业	133:2 到 133:26，以及 133:48 到 133:59
面向连接的 DCE/RPC	133:27 到 133:39
检测无连接 DCE/RPC	133:40 至 133:43

配置 DCE/RPC 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

要配置DCE/RPC预处理器，可以修改控制预处理器工作方式的全局选项，并指定一个或多个基于目标的服务器策略，从而通过 IP 地址和运行的 Windows 或 Samba 版本识别网络上的 DCE/RPC 服务器。基于目标的策略配置还包括启用传输协议、指定将DCE/RPC流量传输到这些主机的端口以及设置其他服务器特定选项。

开始之前

- 确认您要在基于目标的自定义策略中识别的网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击左侧导航面板中的 **Settings**。

步骤 5 如果**应用层预处理器(Application Layer Preprocessors)** 下的 **DCE/RPC 配置 (DCE/RPC Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **DCE/RPC 配置 (DCE/RPC Configuration)** 旁边的 **编辑** ()。

步骤 7 修改**全局设置 (Global Settings)** 部分中的选项；请参阅DCE/RPC 全局选项，第 5 页。

步骤 8 有以下选项可供选择：

- 添加服务器配置文件 - 点击**服务器 (Server)** 旁边的 **添加** ()。在**服务器地址 (Server Address)** 字段中指定一个或多个 IP 地址，然后点击**确定 (OK)**。
- 删除服务器配置文件 - 点击策略旁边的 **删除** ()。
- 编辑服务器配置文件 - 在**服务器 (Servers)** 下点击配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的任何设置；请参阅DCE/RPC 基于目标的策略选项，第 7 页。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成入侵事件，请启用 DCE/RPC 预处理器规则（GID 132 或 133）。有关详细信息，请参阅设置入侵规则状态、DCE/RPC 全局选项，第 5 页、DCE/RPC 基于目标的策略选项，第 7 页和与流量关联的 DCE/RPC 规则，第 11 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

文件和恶意软件检测性能和存储选项
DCE/RPC 关键字
管理层
冲突和更改：网络分析和入侵策略

DNS 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

DNS 预处理器会检查 DNS 域名服务器响应中是否存在以下具体漏洞：

- RData 文本字段中的溢出尝试
- 过时的 DNS 资源记录类型
- 试验性 DNS 资源记录类型

最常见的 DNS 域称服务器响应类型提供与促成响应的查询中域名对应的一个或多个 IP 地址。其他服务器响应类型提供邮件消息目的地或者可提供从最初查询的服务器无法获得的信息的域名服务器位置等等。

DNS 响应包括：

- 消息报头
- 包含一个或多个请求的问题部分
- 与问题部分中的请求对应的三个部分
  - 回答
  - 权限
  - 其他信息 (Additional Information)。

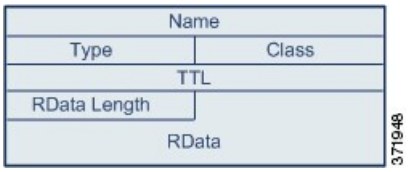
这三个部分中的响应反映域名服务器内保留的资源记录 (RR)。下表将介绍这三个部分。

表 *2: DNS* 域名服务器 *RR* 响应

部分	包含的内容	示例
回答	（可选）为查询提供明确答复的一个或多个资源记录	对应于域名的 IP 地址

部分	包含的内容	示例
权限 (Authority)	（可选）指向授权域名服务器的一个或多个资源记录	用于响应的授权域名服务器的名称
更多信息	（可选）提供与“答案”(Answer) 部分相关的其他信息的一个或多个资源记录	要查询的另一个服务器的 IP 地址

有许多类型的资源记录，全部遵循以下结构：



理论上，任何类型的资源记录均可用于域名服务器响应消息的回答、授权或附加信息部分。DNS 预处理器会检查这三个响应部分中的资源记录是否存在其会检测的漏洞。

“类型”(Type) 和 RData 资源记录字段对于 DNS 预处理器特别重要。“类型”(Type) 字段识别资源记录类型。RData（资源数据）字段提供响应内容。RData 字段的大小和内容因资源记录类型而异。

DNS 消息通常使用 UDP 传输协议，但如果消息类型需要可靠传输或者消息大小超过 UDP 能力，DNS 消息也会使用 TCP。DNS 预处理器会检查 UDP 和 TCP 流量中的 DNS 服务器响应。

DNS 预处理器不会检查在中途恢复的 TCP 会话，如果会话因丢包而丧失状态，DNS 预处理器将会停止检查。

DNS 预处理器选项

端口

此字段指定 DNS 预处理器应为 DNS 服务器响应监控的源端口。使用逗号分隔多个端口。

为 DNS 预处理器配置的典型端口为已知端口 53，DNS 域名服务器对在 UDP 和 TCP 中传输的 DNS 消息使用该端口。

检测 RData 文本字段中的溢出尝试 (Detect Overflow attempts on RData Text fields)

当资源记录类型为 TXT（文本）时，RData 字段为长度可变的 ASCII 文本字段。

如果选择此选项，系统将会检测条目 CVE-2006-3441 在 MITRE 的当前漏洞和风险数据库中识别出的特定漏洞。这是 Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1、Windows XP Service Pack 2 和 Windows Server 2003 Service Pack 1 中的已知漏洞。攻击者可以利用该漏洞发送或者导致主机接收恶意域名服务器响应，导致 RData 文本字段长度计算错误，造成缓冲区溢出，最终全面控制主机。

如果网络上可能有主机运行尚未升级纠正该漏洞的操作系统，应该启用此选项。

您可以启用规则131:3生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

检测过时的 DNS RR 类型 (Detect Obsolete DNS RR Types)

RFC 1035 将多种资源记录类型识别为过时类型。由于这些是过时记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测过时的资源记录类型。下表列出并说明这些记录类型。

表 *3:* 过时的 *DNS* 资源记录类型

RR 类型	代码	说明
3	MD	邮件目的地
4	MF	邮件转发器

您可以启用规则131:1生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

检测试验性 DNS RR 类型 (Detecting Experimental DNS RR Types)

RFC 1035 将多种资源记录类型识别为试验性类型。由于这些是试验性记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测试验性资源记录类型。下表列出并说明这些记录类型。

表 *4:* 试验性 *DNS* 资源记录类型

RR 类型	代码	说明
7	MB	邮箱域名
8	MG	邮件组成员
9	MR	邮件重命名域名
10	NUL	空资源记录

您可以启用规则131:2生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

配置 DNS 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **DNS 配置 (DNS Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **DNS 配置 (DNS Configuration)** 旁边的 **编辑** ()。

步骤 7 修改DNS 预处理器选项，第 14 页中所述的设置。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成入侵事件，请启用 DNS 预处理器规则 (GID 131)。有关详细信息，请参阅设置入侵规则状态和DNS 预处理器选项，第 14 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

入侵和网络分析策略中的层
冲突和更改：网络分析和入侵策略

FTP/Telnet 解码器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

FTP/Telnet 解码器会分析 FTP 和 Telnet 数据流，对 FTP 和 Telnet 命令进行规范化，再由规则引擎处理这些命令。

全局 FTP 和 Telnet 选项

可以设置全局选项以确定 FTP/Telnet 解码器是否对数据包执行状态检查或无状态检查，是否检测加密 FTP 或 Telnet 会话，以及是否在遇到加密数据后继续检查数据流。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

状态性检查

如果选择此选项，FTP/Telnet 解码器将会保存状态，提供各个数据包的会话情景，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

要检查 FTP 数据传输，必须选择此选项。

检测加密流量 (Detect Encrypted Traffic)

检测加密 Telnet 和 FTP 会话。

您可以启用规则 125:7 和 126:2 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

继续检查加密数据 (Continue to Inspect Encrypted Data)

指示预处理器在数据流加密后持续检查数据流，以寻找可处理的最终解密数据。

Telnet 选项

可以通过 FTP/Telnet 解码器启用或禁用 Telnet 命令规范化，启用或禁用特定异常情况，以及设置允许的 Are You There (AYT) 攻击阈值。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指明要实现 Telnet 流量规范化的端口。Telnet 通常连接到 TCP 端口 23。可在此界面列出多个端口，端口之间用逗号分隔。

注意 由于加密流量 (SSL) 无法解码，因此，添加端口 22 (SSH) 可能会产生意外结果。

规范化 (Normalize)

对流向指定端口的 Telnet 流量进行规范化。

检测异常

允许检测没有对应 SE（下级协商终点）的 Telnet SB（下级协商起点）。

Telnet 支持以 SB（下级协商起点）开始并且必须以 SE（下级协商终点）结束的下级协商。但是，Telnet 服务器的某些实现将忽略无对应 SE 的 SB。这是异常行为，可能意味着存在躲避行为。由于 FTP 在控制接口使用 Telnet 协议，因此也容易受此行为影响。

如果在 Telnet 流量中检测到这种异常，可以启用规则 126:3 生成事件，并在内联部署中丢弃恶意数据包；如果在 FTP 命令通道中检测到这种异常，可以启用规则 125:9 生成事件。请参阅设置入侵规则状态。

Are You There 攻击阈值数 (Are You There Attack Threshold Number)

检测超过指定阈值的连续 AYT 命令数量。思科建议将 AYT 阈值设置为不超过默认值的数值。

可以启用规则 126:1生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

服务器级别 FTP 选项

可以在多个 FTP 服务器上设置解码选项。创建的每个服务器配置文件都包含服务器 IP 地址以及应监控其流量的服务器端口。可以为特定服务器指定需要验证的 FTP 命令和可忽略的 FTP 命令，并可设置最大命令参数长度。还可以设置解码器应针对特定命令验证的具体命令语法，并可设置替代最大命令参数长度。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络 (Networks)

使用此选项可指定 FTP 服务器的一个或多个 IP 地址。

可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可配置 1024 个字符，最多可指定 255 个配置文件（包括默认配置文件）。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

端口

使用此选项可指定托管设备应监控其流量的 FTP 服务器上的端口。可在此界面列出多个端口，端口之间用逗号分隔。端口 21 是已知的 FTP 流量端口。

文件获取命令 (File Get Commands)

使用此选项可定义用于从服务器向客户端传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员指示执行此操作。

⚠

注意 请勿修改**文件获取命令 (File Get Commands)** 字段，除非支持人员指示执行此操作。

文件放置命令 (File Put Commands)

使用此选项可定义用于从客户端向服务器传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员指示执行此操作。

⚠

注意 请勿修改**文件放置命令 (File Put Commands)** 字段，除非支持人员指示执行此操作。

附加 FTP 命令 (Additional FTP Commands)

使用此行可指定解码器应检测的其他命令。使用空格隔开其他命令。

可能需要添加的其他命令包括 `XPWD`、`XCWD`、`XCUP`、`XMKD` 和 `XRMD`。有关这些命令的详细信息，请参阅网络工作组发布的 RFC775《面向目录的 FTP 命令规范》。

默认最大参数长度 (Default Max Parameter Length)

在未设置替代最大参数长度的情况下，使用此选项可检测命令的最大参数长度。可以根据需要添加尽可能多的替代最大参数长度。

可以启用规则 125:3 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

替代最大参数长度 (Alternate Max Parameter Length)

使用此选项可指定要为其检测其他最大参数长度的命令，并指定这些命令的最大参数长度。点击**添加 (Add)** 可添加行，在添加的行中可指定其他最大参数长度，以便检测特定命令。

检查字符串格式攻击命令 (Check Commands for String Format Attacks)

使用此选项可检查指定命令的字符串格式攻击。

可以启用规则 125:5 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

命令有效性 (Command Validity)

使用此选项可为特定命令输入有效格式。点击 **Add** 可添加命令验证行。

可以启用规则 125:2 和 125:4 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

忽略 FTP 传输 (Ignore FTP Transfers)

使用此选项可禁用除数据传输通道状态检查之外的所有检查，从而提高 FTP 数据传输的性能。

注释 要检查数据传输，必须选择 FTP/Telnet **Stateful Inspection** 全局选项。

检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

忽略规范化过程中的擦除命令 (Ignore Erase Commands during Normalization)

如果选择了**检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 服务器处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 服务器通常会忽略 Telnet 擦除命令，而旧服务器通常会进行处理。

故障排除选项：记录 FTP 命令验证配置 (Troubleshooting Option: Log FTP Command Validation Configuration)

支持人员可能要求您在故障排除呼叫期间配置系统，以打印为服务器列出的每个 FTP 命令的配置信息。

注意 请勿启用**记录 FTP 命令验证配置 (Log FTP Command Validation Configuration)**，除非支持人员指示执行此操作。

FTP 命令验证语句

为 FTP 命令创建验证语句时，可以通过使用空格隔开参数来指定一组替代参数。还可以在两个参数之间建立二进制 OR 关系，方法是使用竖线 (|) 隔开这两个参数。用方括号 ([]) 引起来的参数是可选参数。用花括号 ({}) 引起来的参数是必要参数。

可以创建 FTP 命令参数验证语句，以验证作为 FTP 通信一部分接收的参数的语法。

下表中列出的任何参数均可用于 FTP 命令参数验证语句中。

表 5: FTP 命令参数

使用的参数	出现的验证
int	所代表的参数必须是整数。
number	所代表的参数必须是 1 到 255 之间的整数。
char _chars	所代表的参数必须是单个字符，并且是 _chars 参数中指定的字符成员。 例如，使用验证语句 char SBC 验证定义 MODE 的命令有效性会检查 MODE 命令的参数是否包含字符 S（表示流模式）、字符 B（表示阻止模式）或字符 C（表示压缩模式）。
date _datefmt	如果 _datefmt 包含 #，所代表的参数必须是数字。 如果 _datefmt 包含 C，所代表的参数必须是字符。 如果 _datefmt 包含文字字符串，所代表的参数必须与文字字符串相匹配。
string	所代表的参数必须是字符串。
host_port	所代表的参数必须是有效的主机端口说明符（如网络工作组发布的 RFC959《文件传输协议规范》中所规定）。

可以根据需要结合使用上表中的语法来创建参数验证语句，以便在需要验证流量时能够正确验证每个 FTP 命令。

注释 如果要在 TYPE 命令中包含复杂的表达式，应将表达式放在空格之间。此外，应将每个操作数放在空格之间。例如，键入 char A | B，而非 char A|B。

相关主题

服务器级别 FTP 选项，第 18 页
FTP 命令验证语句，第 20 页

客户端级别 FTP 选项

使用这些选项可以配置自定义 FTP 客户端配置文件。如果某选项说明不包括预处理器规则，则该选项不与预处理器规则关联。

网络

使用此选项可指定 FTP 客户端的一个或多个 IP 地址。

可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可指定 1024 个字符，最多可指定 255 个配置文件（包括默认配置文件）。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

最大响应长度 (Max Response Length)

使用此选项可以指定客户端接受的 FTP 命令的最大允许响应长度。这可以检测到基本的缓冲区溢出。

您可以启用规则 125:6 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

检测 FTP 退回尝试 (Detect FTP Bounce Attempts)

使用此选项可检测 FTP 退回攻击。

您可以启用规则 125:8 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

允许 FTP 退回至 (Allow FTP Bounce to)

使用此选项可配置包含附加主机以及这些主机上端口的列表，在这些主机上，FTP PORT 命令不应被视为 FTP 退回攻击。

检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

忽略规范化过程中的擦除命令 (Ignore Erase Commands During Normalization)

如果选择了**检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 客户端处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 客户端通常会忽略 Telnet 擦除命令，而旧客户端通常会进行处理。

配置 FTP/Telnet 解码器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

可以为 FTP 客户端配置客户端配置文件，以监控来自客户端的 FTP 流量。

开始之前

- 确认您要在基于目标的自定义策略中识别的任何网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **FTP 和 Telnet 配置 (FTP and Telnet Configuration)** 已禁用，请点击**已启用 (Enabled)**.。

步骤 6 点击 **FTP 和 Telnet 配置 (FTP and Telnet Configuration)** 旁边的 **编辑** ()。

步骤 7 设置**全局设置 (Global Settings)** 部分中的选项，如全局 FTP 和 Telnet 选项，第 17 页中所述。

步骤 8 设置 **Telnet 设置 (Telnet Settings)** 部分中的选项，如Telnet 选项，第 17 页中所述。

步骤 9 管理 FTP 服务器配置文件：

- 添加服务器配置文件 - 点击 **FTP 服务器 (FTP Server)** 旁边的 **添加** ()。在**服务器地址 (Server Address)** 字段中为客户端指定一个或多个 IP 地址，然后点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。
- 编辑服务器配置文件 - 在 **FTP 服务器 (FTP Servers)** 下点击自定义配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的设置；请参阅服务器级别 FTP 选项，第 18 页。
- 删除服务器配置文件 - 点击配置文件旁边的 **删除** ()。

步骤 10 管理 FTP 客户端配置文件：

- 添加客户端配置文件 - 点击 **FTP 客户端 (FTP Client)** 旁边的 **添加** ()。在**客户端地址 (Client Address)** 字段中为客户端指定一个或多个 IP 地址，然后点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。
- 编辑客户端配置文件 - 在 **FTP 客户端 (FTP Client)** 下点击已添加配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改“配置”(Configuration) 页面区域中的设置；请参阅客户端级别 FTP 选项，第 21 页。

- 删除客户端配置文件 - 点击自定义配置文件旁边的 **删除** ( )。

步骤 11 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成入侵事件，请启用 FTP 和 Telnet 预处理器规则（GID 125 和 126）。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层
冲突和更改：网络分析和入侵策略

HTTP 检查预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

HTTP 检查预处理器负责以下工作：

- 解码和规范化发送到网络上 Web 服务器的 HTTP 请求以及来自该服务器的 HTTP 响应
- 将发送到 Web 服务器的消息分成 URI、非 cookie 报头、cookie 报头、方法和消息正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 将从 Web 服务器接收到的消息分成状态代码、状态消息、非 set-cookie 报头、cookie 报头和响应正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 检测可能的 URI 编码攻击
- 使规范化数据可用于附加规则处理
- 通过 JavaScript 等恶意脚本检测和预防攻击。

HTTP 流量可以各种格式进行编码，因此规则很难适当地进行检查。HTTP 检查可解码 14 种编码，从而确保 HTTP 流量获得可能的最佳检查。

可以在一个服务器上或者对服务器列表全局配置 HTTP 检查选项。

请注意，预处理器引擎无状态地执行 HTTP 规范化。也就是说，它会逐个数据包进行 HTTP 字符串规范化，并且只能处理已由 TCP 数据流预处理器重组的 HTTP 字符串。

fast_blocking

在 HTTP 检查预处理器的全局配置选项中，从 Snort 版本 2.9.16.0 开始引入了 fast_blocking 选项。此选项允许在清除数据之前检查 HTTP 数据。这将启用 IPS 规则评估，以便应用阻止规则并最早阻止连接，而不是在清除数据后阻止它。仅当启用内联规范化时，此配置才有效。

要启用 fast_blocking 选项，必须使用以最大检测为基础的网络分析策略。

全局 HTTP 规范化选项

为 HTTP 检查预处理器的全局 HTTP 选项用于控制预处理器的工作方式。如果由未指定为网络服务器的端口接收 HTTP 流量，可使用这些选项启用或禁用 HTTP 规范化。

请注意以下提示：

- 如果启用**无限压缩 (Unlimited Decompression)**，提交修改时，**最大压缩数据深度 (Maximum Compressed Data Depth)** 和**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 选项将会自动设置为 65535。
- 当**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 的值在以下位置不同时，将会使用最高值：
  - 默认网络分析策略
  - 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

检测异常 HTTP 服务器 (Detect Anomalous HTTP Servers)

检测发送到未指定为网络服务器的端口或由其接收的 HTTP 流量。

注释 如果启用此选项，请确保在“HTTP 配置”(HTTP Configuration) 页面上的服务器配置文件中列出会接收 HTTP 流量的所有端口。如果不这样做，并且启用此选项以及随附的预处理器规则，则与该服务器之间的正常流量会生成事件。默认的服务器配置文件包含所有通常用于 HTTP 流量的端口，但如果修改了该配置文件，可能需要将这些端口添加到另一个配置文件中，以防止生成事件。

可以启用规则 120:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

检测 HTTP 代理服务器 (Detect HTTP Proxy Servers)

检测使用未由**允许 HTTP 代理使用 (Allow HTTP Proxy Use)** 选项定义的代理服务器的 HTTP 流量。

可以启用规则 119:17 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

最大压缩数据深度 (Maximum Compressed Data Depth)

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，设置要解压缩的压缩数据的最大大小。

最大解压缩数据深度 (Maximum Decompressed Data Depth)

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，设置规范化解压缩数据的最大大小。

服务器级别 HTTP 规范化选项

可以为监控的每个服务器、全局地为所有服务器或者为服务器列表设置服务器级别选项。此外，可以使用预定义的服务器配置文件来设置这些选项，也可以单独设置它们来满足环境需求。可以使用这些选项或设置这些选项的其中一个默认配置文件来指定要规范化其流量的 HTTP 服务器端口、要规范化的服务器响应负载数量以及要规范化的编码的类型。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络 (Networks)

使用此选项可指定一个或多个服务器的 IP 地址。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

除总共最多 255 个配置文件（包括默认配置文件）的限制以外，还可以在 HTTP 服务器列表中包含最多 496 个字符（或大约 26 个条目），并为所有服务器配置文件指定总共最多 256 个地址条目。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

端口

预处理器引擎会对其 HTTP 流量进行规范化的端口。使用逗号分隔多个端口号。

过大的目录长度 (Oversize Dir Length)

检测长度超过指定值的 URL 目录。

当预处理器检测到长于指定长度的 URL 请求时，您可以启用规则 119:15 来生成事件并在内联部署中丢弃攻击性数据包。

客户端流量深度 (Client Flow Depth)

为要在**端口 (Ports)** 中定义的客户端 HTTP 流量中的原始 HTTP 数据包（包括报头和负载数据）中检查的规则指定字节数。如果规则中的 HTTP 内容规则选项检查请求消息的特定部分，客户端流量深度不适用。

可指定以下任意值：

- 正值，检查第一个数据包中的指定字节数。如果第一个数据包包含的字节数小于指定值，则检查整个数据包。请注意，指定值适用于分段和重组的数据包。

  另请注意，值 300 通常表示许多客户端请求报头末尾出现的大尺寸 HTTP Cookie 无需检查。

- 0 将会检查所有客户端流量，包括会话中的多个数据包，在必要时可超出字节上限。请注意，此值可能会影响性能。

- -1 将会忽略所有客户端流量。

服务器流量深度 (Server Flow Depth)

为要在**端口 (Ports)** 中指定的服务器端 HTTP 流量中的原始 HTTP 数据包中检查的规则指定字节数。**Inspect HTTP Responses** 处于禁用状态时，会检查原始报头和负载；**Inspect HTTP Response** 处于启用状态时，仅检查原始响应正文。

服务器流量深度为要在**端口 (Ports)** 中定义的服务器端 HTTP 流量中检查的规则指定会话中原始服务器响应数据的字节数。可以使用此选项来平衡 HTTP 服务器响应数据的性能和检查级别。如果规则中的 HTTP 内容规则选项检查响应消息的特定部分，服务器流量深度不适用。

不同于客户端流量深度，服务器流量深度为要检查的规则指定每个 HTTP 响应而非每个 HTTP 请求数据包的字节数。

可以指定以下任何内容：

- 正值：

  当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查非原始 HTTP 报头；当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，还会同时检查解压缩数据。

  当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于**禁用**状态时，会检查原始数据包报头和负载。

  如果会话包含的响应字节数小于指定值，规则将会根据需要在多个数据包中彻底检查给定会话中的所有响应数据包。如果会话包含的响应字节数大于指定值，规则将会根据需要在多个数据包中仅检查该会话中的指定字节数。

  请注意，流量深度值小可能会导致针对**端口 (Ports)** 中定义的服务器端流量的规则出现漏报。大多数这些规则针对的是，可能处于非报头数据的大约前 100 字节中的 HTTP 报头或内容。报头长度通常少于 300 字节，但报头大小可以不同。

  另请注意，指定值适用于分段和重组的数据包。

- 0 将会为**端口 (Ports)** 中定义的所有 HTTP 服务器端流量检查整个数据包（包括超过 65535 字节的会话中的响应数据）。

  请注意，此值可能会影响性能。

- -1：

  当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查原始 HTTP 响应正文。

当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于**禁用**状态时，会忽略在**端口 (Ports)** 中定义的所有服务器端流量。

最大报头长度 (Maximum Header Length)

检测 HTTP 请求中长度超过指定最大字节数的报头字段；如果启用了**检查 HTTP 响应 (Inspect HTTP Responses)**，还会对 HTTP 响应执行此项检查。值为 0 将会禁用此选项。指定正值可启用此选项。

您可以启用规则 119:19 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。。

最大报头数 (Maximum Number of Headers)

检测 HTTP 请求中的报头数量超过此设置的情况。值为 0 将会禁用此选项。指定正值可启用此选项。

您可以启用规则 119:20 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。。

最大空格数 (Maximum Number of Spaces)

检测 HTTP 请求的折线中的空格数量等于或超过此设置的情况。值为 0 将会禁用此选项。指定正值可启用此选项。

您可以启用规则 119:26 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。。

HTTP 客户端正文提取深度 (HTTP Client Body Extraction Depth)

指定从 HTTP 客户端请求的消息正文提取的字节数。通过选择 `content` 或 `protected_content` 关键字 **HTTP Client Body** 选项，可以使用入侵规则检查提取的数据。

指定 -1 将会忽略客户端正文。指定 0 将会提取整个客户端正文。请注意，确定要提取的特定字节数可提高系统性能。另请注意，要使 **HTTP 客户端正文 (HTTP Client Body)** 选项在入侵规则中起作用，必须为此选项指定一个大于或等于 0 的值。

小数据块大小 (Small Chunk Size)

指定被认为是小数据块的数据块可包含的最大字节数。指定一个正值。值 0 将会禁用对异常连续小分片的检测。有关详细信息，请参阅**连续小数据块 (Consecutive Small Chunks)** 选项。

连续小数据块 (Consecutive Small Chunks)

指定在使用分块传输编码的客户端流量或服务器流量中，代表异常大数量的连续小数据块的数量。**小数据块大小 (Small Chunk Size)** 选项指定小数据块的最大大小。

例如，将**小数据块大小 (Small Chunk Size)** 设置为 10 并将**连续小数据块 (Consecutive Small Chunks)** 设置为 5，可检测包含 10 个或更少字节的 5 个连续数据块。

对于客户端流量和服务器流量，可分别启用预处理器规则 119:27 和 120:7 针对过多小数据块进行生成事件并在内联部署中丢弃攻击性数据包。如果 **Small Chunk Size** 已启用且此选项设置为 0 或 1，启用这些规则将会对每个指定大小或更小的数据块触发事件。

HTTP 方法 (HTTP Methods)

指定除预期系统会在流量中遇到的 GET 和 POST 以外的 HTTP 请求方法。使用逗号隔开多个值。

入侵规则将 `content` 或 `protected_content` 关键字与 **HTTP Method** 参数配合使用来搜索 HTTP 方法中的内容。如果在流量中遇到 GET、POST 或为此选项配置的方法以外的方法，您可以启用规则 119:31 来生成事件并在内联部署中丢弃攻击性数据包。请参阅设置入侵规则状态。

无警报 (No Alerts)

当随附的预处理器规则处于启用状态时禁用入侵事件。

注释 此选项**不会**禁用 HTTP 标准文本规则和共享对象规则。

规范化 HTTP 报头 (Normalize HTTP Headers)

当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，启用请求和响应报头中非 cookie 数据的规范化。如果**未**启用**检查 HTTP 响应 (Inspect HTTP Responses)**，则启用请求和响应报头中整个 HTTP 报头（包括 cookie）的规范化。

检查 HTTP Cookie (Inspect HTTP Cookies)

允许从 HTTP 请求报头中提取 cookie。当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，还允许从响应报头提取 set-cookie 数据。当不需要提取 cookie 时，禁用此选项可提高性能。

请注意，`Cookie:` 和 `Set-Cookie:` 报头名称、报头行中的前导空格以及终止报头行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP 报头中的规范化 Cookie (Normalize Cookies in HTTP headers)

启用 HTTP 请求报头中 cookie 的规范化。当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，还会启用响应报头中 set-cookie 数据的规范化。必须选择**检查 HTTP Cookie (Inspect HTTP Cookies)** 之后才能选择此选项。

允许 HTTP 代理使用 (Allow HTTP Proxy Use)

允许将受监控的 Web 服务器用作 HTTP 代理。此选项仅用于检查 HTTP 请求。

仅检查 URI (Inspect URI Only)

仅检查规范化 HTTP 请求数据包的 URI 部分。

检查 HTTP 响应 (Inspect HTTP Responses)

启用对 HTTP 响应的延展检查，从而使预处理器不仅会对 HTTP 请求消息进行解码和规范化，还会提取响应字段以供规则引擎进行检查。启用此选项后，系统会提取响应报头、正文、状态代码等；如果还启用了**检查 HTTP Cookie (Inspect HTTP Cookies)**，系统还会提取 set-cookie 数据。

您可以启用规则 120:2 和 120:3 来生成事件并在内联部署中丢弃攻击性数据包，如下所述：

表 *6:* 检查 *HTTP* 响应规则

规则	遇到以下情况时触发...
120:2	出现无效的 HTTP 响应状态代码。
120:3	HTTP 响应不包括内容长度或传输编码。

将 UTF 编码规范化为 UTF-8 (Normalize UTF Encodings to UTF-8)

如果启用了**检查 HTTP 响应 (Inspect HTTP Responses)**，此选项检测 HTTP 响应中的 UTF-16LE、UTF-16BE、UTF-32LE 和 UTF32-BE 编码，并将其规范化为 UTF-8。

当 UTF 规范化失败时，您可以启用规则 120:4 来生成事件并在内联部署中丢弃攻击性数据包。

检查压缩数据 (Inspect Compressed Data)

当**检查 HTTP 响应 (Inspect HTTP Responses)** 已启用时，此选项启用 HTTP 响应正文中的 gzip 和兼容 deflate 的压缩数据的解压，以及对规范化解压缩数据的检查。系统将检查分块和非分块 HTTP 响应数据。系统会根据需要逐一检查多个数据包中的解压缩数据；也就是说，系统不会将来自不同数据包的解压缩数据合并来进行检查。当达到**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到**服务器流量深度 (Server Flow Depth)** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了**无限制解压缩 (Unlimited Decompression)**。您可以使用 `file_data` 规则关键字来检查解压缩数据。

您可以启用规则 120:6 和 120:24 来生成事件并在内联部署中丢弃攻击性数据包，如下所述：

表 *7:* 检查压缩 *HTTP* 响应规则

规则	遇到以下情况时触发...
120:6	压缩 HTTP 响应的解压缩失败。
120:24	压缩 HTTP 响应的部分解压缩失败。

无限解压

当启用**检查压缩数据 (Inspect Compressed Data)**（或者 **解压缩 SWF 文件 (LZMA) [Decompress SWF File (LZMA)]**、**解压缩 SWF 文件 (Deflate) [Decompress SWF File (Deflate)]** 或**解压缩 PDF 文件 (Deflate) [Decompress PDF File (Deflate)]**）时，会跨多个数据包覆盖**最大压缩数据深度 (Maximum Compressed Data Depth)**；也就是说，此选项支持跨多个数据包无限制解压缩。请注意，启用此选项不会影响单个数据包中的**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)**。另请注意，如果启用此选项，确认修改时**最大压缩数据深度 (Maximum Compressed Data Depth)** 和**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 将会设置为 65535。

规范化 Javascript (Normalize Javascript)

当**检查 HTTP 响应 (Inspect HTTP Responses)** 已启用时，此选项启用对 HTTP 响应正文中 Javascript 的检测和规范化。预处理器会对模糊 JavaScript 数据（例如，unescape 函数、decodeURI 函数和 String.fromCharCode 方法）进行规范化。预处理器会对 unescape、decodeURI 和 decodeURIComponent 函数中的以下编码进行规范化：

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

预处理器检测连续空格，并将其规范化为一个空格。此选项处于启用状态时，配置字段允许您指定模糊 Javascript 数据中允许的最大连续空格数量。可输入 1 到 65535 之间的值。值 0 将会禁止生成事件，不管与该字段相关的预处理器规则 (120:10) 是否启用。

预处理器还会对 Javascript 加号 (+) 运算符进行规范化，并使用该运算符连接字符串。

您可以使用 `file_data` 入侵规则关键字使入侵规则指向规范化的 Javascript 数据。

您可以启用规则 120:9、120:10 和 120:11 以生成事件并在内联部署中丢弃攻击性数据包，如下所示：

表 *8:* 规范化 *Javascript* 选项规则

规则	遇到以下情况时触发...
120:9	预处理器内的模糊级别大于或等于 2。
120:10	Javascript 模糊数据中的连续空格数量大于或等于为允许的最大连续空格数量配置的值。
120:11	经转义或编码的数据包含多种类型的编码。

“解压缩 SWF 文件 (LZMA)” (Decompress SWF File [LZMA]) 和“解压缩 SWF 文件 (Deflate)” (Decompress SWF File [Deflate])

启用 **HTTP Inspect Responses** 后，这些选项解压缩位于 HTTP 请求的 HTTP 响应主体中文件的压缩部分。.

注释 您只能解压缩在 HTTP GET 响应中找到的文件的压缩部分。

- **Decompress SWF File (LZMA)** 解压缩 Adobe ShockWave Flash (`.swf`) 文件的 LZMA 兼容压缩部分。

- **Decompress SWF File (Deflate)** 解压缩 Adobe ShockWave Flash (`.swf`) 文件的 deflate 兼容压缩部分。

当达到**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到**服务器流量深度 (Server Flow Depth)** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了**无限制解压缩 (Unlimited Decompression)**。您可以使用 `file_data` 入侵规则关键字来检查解压缩数据。

您可以启用规则 120:12 和 120:13 以生成事件并在内联部署中丢弃攻击性数据包，如下所示：

表 *9:* 解压缩 ***SWF*** 文件选项规则

规则	遇到以下情况时触发...
120:12	deflate 文件解压缩失败。
120:13	LZMA 文件解压缩失败。

Decompress PDF File (Deflate)

检查 HTTP 响应 (Inspect HTTP Responses) 处于启用状态时，**解压缩 SWF 文件 (Deflate) (Decompress PDF File [Deflate])** 会解压缩位于 HTTP 请求的 HTTP 响应主体中可移植文档格式 (`.pdf`) 文件的 deflate 兼容压缩部分。系统只能使用 `/FlateDecode` 数据流过滤器解压缩 PDF 文件。不支持其他数据流过滤器（包括 `/FlateDecode /FlateDecode`）。

注释 您只能解压缩在 HTTP GET 响应中找到的文件的压缩部分。

当达到**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到**服务器流量深度 (Server Flow Depth)** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了**无限制解压缩 (Unlimited Decompression)**。您可以使用 `file_data` 入侵规则关键字来检查解压缩数据。

您可以启用规则 120:14、120:15、120:16 和 120:17 以生成事件并在内联部署中丢弃攻击性数据包，如下所示：

表 *10:* 解压缩 ***PDF*** 文件 ***(Deflate)*** 选项规则

规则	遇到以下情况时触发...
120:14	文件解压缩失败。
120:15	由于压缩类型不受支持，文件解压缩失败。
120:16	由于 PDF 数据流过滤器不受支持，文件解压缩失败。
120:17	文件解析失败。

提取原始客户端 IP 地址 (Extract Original Client IP Address)

在入侵检查过程中启用原始客户端 IP 地址的检查。系统从您在 **XFF 报头优先级 (XFF Header Priority)** 选项中定义的 X-Forwarded-For (XFF)、True-Client-IP 或自定义 HTTP 报头提取原始客户端 IP 地址。您可以在入侵事件表中查看提取的原始客户端 IP 地址。

您可以启用规则 119:23、119:29 和 119:30 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。。

XFF 报头优先级 (XFF Header Priority)

指定当 HTTP 请求中存在多个报头时，系统处理原始客户端 IP 报头的顺序。默认情况下，系统会检查 X-Forwarded-For (XFF) 报头，然后检查 True-Client-IP 报头。使用每种报头类型旁边的向上和向下箭头图标调整其优先级。

此选项还允许您指定除 XFF 或 True-Client-IP 以外的原始客户端 IP 报头来进行提取和评估。点击**添加 (Add)** 以将自定义报头名称添加到优先级列表中。系统仅支持与 XFF 或 True-Client-IP 报头使用相同语法的自定义报头。

配置此选项时请记住以下几点：

- 在评估原始客户端 IP 地址报头时，系统同时对访问控制和入侵检查使用此优先顺序。
- 如果存在多个原始客户端 IP 报头，则系统仅处理优先级最高的报头。
- XFF 报头包含 IP 地址列表，表示请求所通过的代理服务器。为防止欺骗，系统使用列表中的最后一个 IP 地址（即受信任代理附加的地址）作为原始客户端 IP 地址。

日志 URI (Log URI)

允许从 HTTP 请求数据包提取原始 URI（如果有），并将该 URI 与为会话生成的所有入侵事件相关联。

启用此选项后，可以在入侵事件表视图的“HTTP URI”列中显示提取的 URI 的前 50 个字符。可以在数据包视图中显示完整的 URI（最多 2048 字节）。

日志主机名 (Log Hostname)

允许从 HTTP 请求主机报头中提取主机名（如果有），并将该主机名与为会话生成的所有入侵事件相关联。如果存在多个主机报头，系统将会从第一个报头中提取主机名。

启用此选项后，可以在入侵事件表视图的“HTTP 主机名”(HTTP Hostname) 列中显示提取的主机名的前 50 个字符。可以在数据包视图中显示完整的主机名（最多 256 字节）。

您可以启用规则 119:25 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

请注意，如果启用了规则 119:24，它将在于 HTTP 请求中检测到多个主机报头时触发，而不管该选项的设置为何。

配置文件

指定为 HTTP 流量规范化的编码的类型。系统提供了一个适用于大多数服务器的默认配置文件、适用于 Apache 服务器和 IIS 服务器的若干默认配置文件以及自定义默认设置，您可以对这些设置进行自定义，以满足受监控流量的需求：

- 选择 **All** 将会使用适用于所有服务器的标准默认配置文件。
- 选择 **IIS** 将会使用系统提供的 IIS 配置文件。
- 选择 **Apache** 将会使用系统提供的 Apache 配置文件。
- 选择**自定义 (Custom)** 将会创建您自己的服务器配置文件。

服务器级别 HTTP 规范化编码选项

将 HTTP 服务器级别**配置文件 (Profile)** 选项设置为 `Custom` 时，可以指定为 HTTP 流量规范化的编码类型，并启用 HTTP 预处理器规则以根据包含不同编码类型的流量生成事件。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

ASCII 编码 (ASCII Encoding)

对编码的 ASCII 字符进行解码，并指定规则引擎是否生成关于 ASCII 编码 URI 的事件。

可以启用规则 119:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

UTF-8 编码 (UTF-8 Encoding)

对 URI 中的标准 UTF-8 Unicode 序列进行解码。

可以启用规则 119:6 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

Microsoft %U Encoding

对 IIS %u 编码方案进行解码，该编码方案使用 %u，后跟四个字符；其中这四个字符是与 IIS Unicode 代码点相关的十六进制编码值。

提示 合法的客户端很少使用 %u 编码，因此思科建议对使用 %u 编码的 HTTP 流量进行解码。

可以启用规则 119:3 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

裸字节 UTF-8 编码 (Bare Byte UTF-8 Encoding)

对裸字节编码进行解码（这种解码方法使用非 ASCII 字符作为解码 UTF-8 值时的有效值）。

提示 裸字节编码允许用户模拟 IIS 服务器和正确解释非标准编码。思科建议启用此选项，因为合法的客户端不以这种方式编码 UTF-8。

可以启用规则 119:4 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

Microsoft IIS 编码 (Microsoft IIS Encoding)

使用 Unicode 代码点映射进行解码。

提示 思科建议启用此选项，因为它主要出现在攻击和躲避尝试中。

可以启用规则 119:7 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

双重编码 (Double Encoding)

通过在每个进行解码的请求 URI 中形成两条通道，解码 IIS 双编码流量。思科建议启用此选项，因为它通常只存在于攻击情况中。

可以启用规则 119:2 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

多斜杠混淆 (Multi-Slash Obfuscation)

将连续的多个斜杠规范化为一个斜杠。

可以启用规则 119:8 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

IIS 反斜杠混淆 (IIS Backslash Obfuscation)

将反斜线规范化为前斜线。

可以启用规则 119:9 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

目录遍历

对目录遍历和自引用目录进行规范化。如果启用随附的预处理器规则来生成关于此类型流量的事件，可能会产生误报，因为有些网站使用目录遍历来引用文件。

可以启用规则 119:10 和 119:11 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

制表符混淆 (Tab Obfuscation)

规范化有关对空格分隔符使用制表符的非 RFC 标准。Apache 及其他非 IIS Web 服务器在 URL 中使用制表符 (0x09) 作为分隔符。

注释 无论此选项的配置如何，如果制表符前有空格字符 (0x20)，HTTP 检查预处理器都将制表符看作空格。

可以启用规则 119:12 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

RFC 分隔符无效 (Invalid RFC Delimiter)

规范化 URI 数据中的换行符 (\n)。

可以启用规则 119:13 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

Webroot 目录遍历 (Webroot Directory Traversal)

检测穿过 URL 中初始目录的目录遍历。

可以启用规则 119:18 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

制表符 URI 分隔符 (Tab URI Delimiter)

允许使用制表符 (0x09) 作为 URI 的分隔符。Apache、IIS 较新版本以及某些其他 Web 服务器在 URL 中使用制表符作为分隔符。

注释 无论此选项的配置如何，如果制表符前有空格字符 (0x20)，HTTP 检查预处理器都将制表符看作空格。

非 RFC 字符 (Non-RFC characters)

检测在相应字段中添加的并出现在传入或传出 URI 数据中的非 RFC 字符列表。当修改此字段时，请使用代表该字节字符的十六进制格式。如果要配置此选项，在配置此选项时，请小心设置此值。使用很常见的字符可能会使您面临大量事件。

可以启用规则 119:14 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

最大块编码大小 (Max Chunk Encoding Size)

检测 URI 数据中异常大的数据块的大小。

可以启用规则 119:16 和 119:22 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

禁用管道解码 (Disable Pipeline Decoding)

对于管道请求禁用 HTTP 解码。当此选项被禁用时，性能会提升，因为系统不会解码或分析管道中等待的 HTTP 请求，只是使用通用模式匹配对它们进行检测。

非严格 URI 解析 (Non-Strict URI Parsing)

允许非严格的 URI 解析。应仅在接受“GET /index.html abc xo qr \n”格式的非标准 URI 的服务器上使用此选项。使用此选项时，解码器会假定 URI 位于第一个空格与第二个空格之间，即使第二个空格之后没有有效的 HTTP 标识符。

扩展的 ASCII 编码 (Extended ASCII Encoding)

允许解析 HTTP 请求 URI 中的扩展 ASCII 字符。请注意，此选项仅可用于自定义服务器配置文件，在为 Apache、IIS 或所有服务器提供的默认配置文件中不可用。

相关主题

概述：HTTP content 和 protected_content 关键字参数

配置 HTTP 检查预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

开始之前

- 确认您要在基于目标的自定义策略中识别的任何网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **HTTP 配置 (HTTP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **HTTP 配置 (HTTP Configuration)** 旁边的 **编辑** ()。

步骤 7 修改“全局设置”(Global Settings) 页面区域中的选项；请参阅全局 HTTP 规范化选项，第 25 页。

步骤 8 此时，您有三种选择：

- 添加服务器配置文件 - 点击**服务器 (Servers)** 部分中的 **添加** ()。在**服务器地址 (Server Address)** 字段中为客户端指定一个或多个 IP 地址，然后点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可在列表中包含 496 个字符，为所有服务器配置文件总共最多可指定 256 个地址条目，总共最多可创建 255 个配置文件（包括默认配置文件）。
- 编辑服务器配置文件 - 在**服务器 (Servers)** 下点击已添加配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的任何设置；请参阅服务器级别 HTTP 规范化选项，第 26 页。如果为**配置文件 (Profile)** 值选择**自定义 (Custom)**，还可以修改服务器级别 HTTP 规范化编码选项，第 34 页中所述的编码选项。
- 删除服务器配置文件 - 点击自定义配置文件旁边的 **删除** ()。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果需要生成事件并在内联部署中丢弃攻击性数据包，请启用 HTTP 预处理器规则 (GID 119)。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层
冲突和更改：网络分析和入侵策略

其他 HTTP 检查预处理器规则

可以启用下表的 **Preprocessor Rule GID:SID** 列中的规则，为与特定配置选项无关的 HTTP 检查预处理器规则生成事件。

表 *11:* 其他 *HTTP* 检查预处理器规则

预处理器规则 GID:SID	触发场景..
119:21	HTTP 请求报头包含多于一个 `content-length` 字段时。
119:24	HTTP 请求包含多于一个主机报头时。
119:28	HTTP POST 方法既没有 `content-length` 报头，也没有数据块 `transfer-encoding`。
119:32	在流量中遇到 HTTP 0.9 时。请注意，还必须启用“TCP 流配置”(TCP Stream Configuration)。
119:33	HTTP URI 包含非转义空格时。
119:34	TCP 连接包含 24 个或更多管道化 HTTP 请求时。
120:5	HTTP 响应流量中遇到 UTF-7 编码时；UTF-7 应仅在需要 7 位奇偶校验的情况下出现，例如，SMTP 流量。
120:8	`content-length` 或数据库大小无效。
120:18	在客户端请求之前发生 HTTP 服务器响应时。
120:19	HTTP 响应包括多个内容长度时。
120:20	HTTP 响应包括多个内容编码时。
120:25	HTTP 响应包括无效报头折叠时。
120:26	在 HTTP 响应报头之前出现乱码行时。
120:27	HTTP 响应不包括报头尾部时。
120:28	数据块大小无效时，或者数据块大小后跟乱码字符时。

Sun RPC 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

远程过程调用 (RPC) 规范化采用分片 RPC 记录，并将这些记录规范化为单个记录，以便规则引擎可以检查完整的记录。例如，攻击者可能会试图发现运行 RPC `admind` 的端口。某些 UNIX 主机使用 RPC `admind` 执行远程分布式系统任务。如果主机执行的身份验证强度较弱，恶意用户可能会控制远

程管理。Snort ID (SID) 为 575 的标准文本规则 (GID: 1) 会搜索特定位置中的内容，并识别不适当的 `portmap GETPORT` 请求，以此来检测这种攻击。

Sun RPC 预处理器选项

端口

指定要规范化其流量的端口。可在此界面列出多个端口，端口之间用逗号分隔。典型的 RPC 端口为 111 和 32771。如果网络将 RPC 流量发送到其他端口，可考虑添加这些端口。

检测分片 RPC 记录 (Detect fragmented RPC records)

检测 RPC 分片记录。

您可以启用规则 106:1 和 106:5 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

检测一个数据包中的多个记录 (Detect multiple records in one packet)

在每个数据包（或重组数据包）中检测多于一个 RPC 请求。

可以启用规则 106:2生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

检测超出一个分片的片段的记录和

检测超过当前数据包长度的重组分片记录长度。

可以启用规则 106:3生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

检测超过一个数据包长度的单个分片记录

检测部分记录

可以启用规则 106:4生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

配置 Sun RPC 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择策略 > 访问控制标题 > 访问控制，然后点击网络分析策略 或策略 > 访问控制标题 > 入侵，然后点击网络分析策略。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的编辑 (✎)。

如果显示视图 (👁)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的设置 **(Settings)**。

步骤 5 如果应用层预处理器 **(Application Layer Preprocessors)** 下的 **Sun RPC 配置 (Sun RPC Configuration)** 被禁用，请点击已启用 **(Enabled)**。

步骤 6 点击 **Sun RPC 配置 (Sun RPC Configuration)** 旁边的 编辑 (✎)。

步骤 7 修改Sun RPC 预处理器选项，第 40 页中所述的设置。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击策略信息 **(Policy Information)**，然后点击确认更改 **(Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果希望生成事件并在内联部署中丢弃攻击性数据包，则请启用 Sun RPC 预处理器规则 (GID 106)。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层
冲突和更改：网络分析和入侵策略

SIP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

会话初始协议 (SIP) 为客户端应用（例如网络电话、多媒体会议、即时消息、网络游戏和文件传输）的一个或多个用户提供一个或多个会话的呼叫建立、修改和取消。每个SIP请求中的“方法”(*method*) 字段识别请求的目的，请求 URI 则指定发送请求的目的地。每个 SIP 响应中的状态代码指明请求操作的结果。

使用 SIP 建立呼叫后，实时传输协议 (RTP) 负责随后的音频和视频通信；会话的此部分有时又称为呼叫通道、数据通道或音频/视频数据通道。对于数据通道参数协商、会话公告和会话邀请，RTP 在 SIP 消息正文中使用会话描述协议 (SDP)。

SIP 预处理器负责：

- 解码和分析 SIP 2.0 流量
- 提取包括 SDP 数据（如果有）在内的 SIP 报头和消息正文，并将提取的数据传递给规则引擎，以进行进一步检查
- 在检测到以下条件并且相应的预处理器规则已启用的情况下，将会生成事件：
  - SIP 数据包中存在异常和已知漏洞
  - 调用序列乱序和无效
- 或者，忽略呼叫通道

预处理器会根据在 SDP 消息中识别出的端口来识别 RTP 通道（该消息嵌入在 SIP 消息正文中），但预处理器不提供 RTP 协议检查。

使用 SIP 预处理器时，请注意以下几点：

- UDP 通常传输 SIP 支持的媒体会话。UDP 数据流预处理为 SIP 预处理器提供 SIP 会话跟踪。
- SIP 规则关键字允许您指向 SIP 数据包报头或消息正文，并限制为对特定 SIP 方法或状态代码进行数据包检测。

SIP 预处理器选项

对于以下选项，您可以指定从 1 到 65535 字节的正值或 0，以禁用选项的事件生成（无论是否启用关联规则）。

- **Maximum Request URI Length**
- **Maximum Call ID Length**
- **Maximum Request Name Length**
- **Maximum From Length**
- **Maximum To Length**
- **Maximum Via Length**
- **Maximum Contact Length**

- **Maximum Content Length**

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 SIP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

检查方法 (Methods to Check)

指定 SIP 检测方法。可以指定以下当前定义的任何 SIP 方法：

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

方法不区分大小写。方法名称可以包含字母字符、数字和下划线字符。不允许任何其他特殊字符。使用逗号隔开多种方法。

由于将来可能会定义新的 SIP 方法，因此，配置可以包含当前未定义的字母字符串。系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。

请注意，除为此选项指定的任何方法外，总共 32 种方法包括入侵规则中使用 `sip_method` 关键字指定的方法。

会话中的最大对话数 (Maximum Dialogs within a Session)

指定数据流会话中允许的最大对话数量。如果创建的对话框数量超过该数量，则最早的对话框会被丢弃，直至对话框数量不超过指定的最大数量。可指定 1 到 4194303 之间的整数。

您可以启用规则 140:27 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态。

最大请求 URL 长度 (Maximum Request URI Length)

指定 Request-URI 报头字段中允许的最大字节数。如果启用了规则 140:3，则更长的“URI”生成事件并在内联部署中丢弃攻击性数据包。请求 URI 字段指明请求的目标路径或目标页面。

最大调用 ID 长度 (Maximum Call ID Length)

指定请求或响应 Call-ID 报头字段中允许的最大字节数。如果启用了规则 140:5，则更长的“调用 ID”生成事件并在内联部署中丢弃攻击性数据包。“调用 ID”字段唯一地识别请求和响应中的 SIP 会话。

最大请求名称长度 (Maximum Request Name Length)

指定请求名称中允许的最大字节数（该名称是CSeq事务标识符中指定的方法的名称）。如果启用了规则 140:7，则更长的“请求名称”生成事件并在内联部署中丢弃攻击性数据包。

最大发件人长度 (Maximum From Length)

指定请求或响应“发件人”(From)报头字段中允许的最大字节数。如果启用了规则140:9，则更长的“发件人”生成事件并在内联部署中丢弃攻击性数据包。“发件人”(From) 字段识别消息发起方。

最大收件人长度 (Maximum To Length)

指定请求或响应“收件人”(To) 报头字段中允许的最大字节数。如果启用了规则 140:11，则更长的“收件人”生成事件并在内联部署中丢弃攻击性数据包。“收件人”(To) 字段识别消息收件人。

最大路径长度 (Maximum Via Length)

指定请求或响应“路径”(Via) 报头字段中允许的最大字节数。如果启用了规则 140:13，则更长的“通过”生成事件并在内联部署中丢弃攻击性数据包。“路径”(Via)字段提供请求的路径，并在响应中提供回执信息。

最大联系人长度 (Maximum Contact Length)

指定请求或响应“联系人”(Contact) 报头字段中允许的最大字节数。如果启用了规则 140:15，则更长的“联系人”生成事件并在内联部署中丢弃攻击性数据包。“联系人”(Contact) 字段提供用以指定与后续消息进行联系的位置的 URI。

最大内容长度 (Maximum Content Length)

指定在请求或响应消息正文的内容中允许的最大字节数。如果启用了规则 140:16，则更长的内容生成事件并在内联部署中丢弃攻击性数据包。

忽略音频/视频数据通道 (Ignore Audio/Video Data Channel)

启用和禁用数据通道流量检查。请注意，如果启用了此选项，预处理器会继续检查其他非数据通道 SIP 流量。

相关主题

SIP 关键字

配置 SIP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** (✎)。

如果显示**视图** (👁)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SIP 配置 (SIP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **SIP 配置 (SIP Configuration)** 旁边的 **编辑** (✎)。

步骤 7 修改SIP 预处理器选项，第 42 页中所述的选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 SIP 预处理器规则 (GID 140)。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层
冲突和更改：网络分析和入侵策略

其他 SIP 预处理器规则

下表中的 SIP 预处理器规则与特定配置选项无关。与其他 SIP 预处理器规则一样，如果要使这些规则生成事件并在内联部署中丢弃攻击性数据包，必须启用这些规则。

表 *12:* 其他 *SIP* 预处理器规则

预处理器规则 GID:SID	触发场景..
140:1	预处理器监控系统允许的最大 SIP 会话数量。
140:2	必填的 Request_URI 字段在 SIP 请求中为空。
140:4	Call-ID 报头字段在 SIP 请求或响应中为空。
140:6	SIP 请求或响应 CSeq 字段中的序列号值不是小于 231 的 32 位无符号整数。

预处理器规则 GID:SID	触发场景..
140:8	From 报头字段在 SIP 请求或响应中为空。
140:10	To 报头字段在 SIP 请求或响应中为空。
140:12	Via 报头字段在 SIP 请求或响应中为空。
140:14	必填的 Contact 报头字段在 SIP 请求或响应中为空。
140:17	UDP 流量中的单个 SIP 请求或响应数据包包含多条消息。请注意，旧版本 SIP 支持多条消息，但 SIP 2.0 仅在每个数据包中支持一条消息。
140:18	UDP 流量中的 SIP 请求或响应中消息正文的实际长度与 SIP 请求或响应中的 Content-Length 报头字段中指定的值不匹配。
140:19	预处理器无法识别 SIP 响应的 CSeq 字段中的方法名称。
140:20	SIP 服务器不质询经过身份验证的邀请消息。请注意，当有 InviteReplay 计费攻击时，会出现这种情况。
140:21	在设置调用之前，会话信息发生更改。请注意，当有 FakeBusy 计费攻击时，会出现这种情况。
140:22	响应状态代码不是三位数字。
140:23	Content-Type 报头字段未指定内容类型且消息正文包含数据。
140:24	SIP 版本不是1、1.1 或2.0。
140:25	CSeq 报头字段中指定的方法与 SIP 请求中的“方法”字段不匹配。
140:26	预处理器无法识别在 SIP 请求“方法”字段中命名的方法。

GTP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

通用分组无线业务 (GPRS) 隧道协议 (GTP) 实现通过 GTP 核心网络进行通信。GTP 预处理器检测 GTP 流量中的异常，并将命令通道信令消息转发到规则引擎以进行检查。可以使用 `gtp_version`、`gtp_type` 和 `gtp_info` 规则关键字检查 GTP 命令通道流量中是否存在漏洞。

单一配置选项允许为预处理器进行 GTP 命令通道消息检查的端口修改默认设置。

GTP 预处理器规则

如果要下表中所列的 GTP 预处理器规则生成事件并在内联部署中丢弃攻击性数据包，必须启用它们。

表 *13: GTP* 预处理器规则

预处理器规则 GID:SID	说明
143:1	如果预处理器检测到无效的消息长度，将会生成事件。
143:2	如果预处理器检测到无效的信息元素长度，将会生成事件。
143:3	如果预处理器检测到无序的信息元素，将会生成事件。

配置 GTP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

可以使用以下程序修改 GTP 预处理器监控以获取 GTP 命令消息的端口。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击左侧导航面板中的 **Settings**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **GTP 命令通道配置 (GTP Command Channel Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **GTP 命令通道配置 (GTP Command Channel Configuration)** 旁边的 **编辑** ()。

步骤 7 输入**端口 (Ports)** 值。

使用逗号分隔多个端口。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 GTP 预处理器规则 (GID 143)。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

IMAP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

互联网邮件应用协议 (IMAP) 用于从远程 IMAP 服务器检索邮件。IMAP 预处理器检查服务器到客户端的IMAP4流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器IMAP4流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。

提取和解码涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

IMAP 预处理器选项

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 IMAP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 解码深度 (Base64 Decoding Depth)

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

当启用此选项时，您可以启用规则 141:4 以在解码失败时生成事件并在内联部署中丢弃攻击性数据包；解码可能会由于不正确的编码或损坏的数据等原因而失败。

7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

当启用此选项时，您可以启用规则 141:6 以在提取失败时生成事件并在内联部署中丢弃攻击性数据包；提取可能会由于损坏的数据等原因而失败。

Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

当启用此选项时，您可以启用规则 141:5 以在解码失败时生成事件并在内联部署中丢弃攻击性数据包；解码可能会由于不正确的编码或损坏的数据等原因而失败。

Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)

指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

当启用此选项时，您可以启用规则 141:7 以在解码失败时生成事件并在内联部署中丢弃攻击性数据包；解码可能会由于不正确的编码或损坏的数据等原因而失败。

相关主题

file_data 关键字

配置 IMAP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **IMAP 配置 (IMAP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **IMAP 配置 (IMAP Configuration)** 旁边的 **编辑** ()。

步骤 7 修改IMAP 预处理器选项，第 48 页中所述的设置。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 IMAP 预处理器规则 (GID 141)；请参阅设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

入侵和网络分析策略中的层
冲突和更改：网络分析和入侵策略

其他 IMAP 预处理器规则

下表中的 IMAP 预处理器规则与特定配置选项无关。与其他 IMAP 预处理器规则一样，如果要使这些规则能够生成事件并在内联部署中丢弃攻击性数据包，则必须启用它们。

表 *14:* 其他 *IMAP* 预处理器规则

预处理器规则 **GID:SID**	说明
141:1	如果预处理器检测到未在 RFC 3501 中定义的客户端命令，将会生成事件。

预处理器规则 GID:SID	说明
141:2	如果预处理器检测到未在 RFC 3501 中定义的服务器响应，将会生成事件。
141:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

POP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

邮局协议 (POP) 用于从远程 POP 邮件服务器检索邮件。POP 预处理器检查服务器到客户端的 POP3 流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器 POP3 流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。

提取和解码涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

POP 预处理器选项

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 POP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 解码深度 (Base64 Decoding Depth)

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

启用此选项时，您可以在解码失败时启用规则 142:4 至生成事件并在内联部署中丢弃攻击性数据包，例如，由于解码不正确或数据损坏，解码可能会失败。

7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

启用此选项时，您可以在提取失败时启用规则 142:6 至生成事件并在内联部署中丢弃攻击性数据包；例如，由于数据损坏，提取可能会失败。

Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

启用此选项时，您可以在解码失败时启用规则 142:5 至生成事件并在内联部署中丢弃攻击性数据包；例如，由于解码不正确或数据损坏，解码可能会失败。

Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)

指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

启用此选项时，您可以在解码失败时启用规则 142:7 到生成事件并在内联部署中丢弃攻击性数据包；例如，由于解码不正确或数据损坏，解码可能会失败。

相关主题

管理层
冲突和更改：网络分析和入侵策略
file_data 关键字

配置 POP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释

如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** (✎)。

如果显示**视图** (👁)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **POP 配置 (POP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **POP 配置 (POP Configuration)** 旁边的 **编辑** (✎)。

步骤 7 修改POP 预处理器选项，第 51 页中所述的设置。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 POP 预处理器规则 (GID 142)。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层

冲突和更改：网络分析和入侵策略

其他 POP 预处理器规则

下表中的 POP 预处理器规则与特定配置选项无关。与其他 POP 预处理器规则一样，如果您需要它们来生成事件并在内联部署中丢弃攻击性数据包，则必须启用这些规则。

表 *15:* 其他 *POP* 预处理器规则

预处理器规则 GID:SID	说明
142:1	如果预处理器检测到未在 RFC 1939 中定义的客户端命令，将会生成事件。
142:2	如果预处理器检测到未在 RFC 1939 中定义的服务器响应，将会生成事件。
142:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

SMTP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

SMTP 预处理器指示规则引擎对 SMTP 命令进行规范化。预处理器还可以提取和解码客户端到服务器流量中的邮件附件，并根据不同的软件版本，提取邮件的文件名、地址和报头数据，以在显示 SMTP 流量触发的入侵事件时提供上下文。

SMTP 预处理器选项

可以启用或禁用规范化，还可以对选项进行配置以控制 SMTP 解码器检测的异常流量类型。

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定要规范化其 SMTP 流量的端口。可以指定大于或等于 0 的值。使用逗号分隔多个端口。

状态检查 (Stateful Inspection)

如果选择此选项，SMTP 解码器将会保存状态，提供各个数据包的会话上下文，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

规范化 (Normalize)

如果设置为 `All`，将会规范化所有命令。会检查命令后是否有多个空格字符。

如果设置为 `None`，则不会对命令进行规范化。

如果设置为 `Cmds`，将会规范化**自定义命令 (Custom Commands)** 中列出的命令。

自定义命令

如果**规范化 (Normalize)** 设置为 `Cmds`，则会规范化列出的命令。

可在文本框中指定应进行规范化的命令。会检查命令后是否有多个空格字符。

空格 (ASCII 0x20) 和制表符 (ASCII 0x09) 字符被视为是用于规范化目的的空格字符。

忽略数据 (Ignore Data)

不处理邮件数据；仅处理 MIME 邮件报头数据。

忽略 TLS 数据 (Ignore TLS Data)

不处理根据传输层安全协议加密的数据。

无警报 (No Alerts)

当随附的预处理器规则处于启用状态时禁用入侵事件。

检测未知命令 (Detect Unknown Commands)

检测 SMTP 流量中的未知命令。

可以启用规则 124:5，为此选项生成事件并在内联部署中丢弃攻击性数据包。

最大命令行长度 (Max Command Line Len)

检测 SMTP 命令行的长度何时大于此值。指定 0 将不会检测命令行长度。

RFC2821（网络工作组制定的关于简单邮件传输协议的规范）建议将最大命令行长度设置为 512。

可以启用规则 124:1，为此选项生成事件并在内联部署中丢弃攻击性数据包。

最大报头行长度 (Max Header Line Len)

检测 SMTP 数据报头行的长度何时大于此值。指定 0 将不会检测数据报头行长度。

可以启用规则 124:2 和 124:7，为此选项生成事件并在内联部署中丢弃攻击性数据包。

最大响应行长度 (Max Response Line Len)

检测 SMTP 响应行的长度何时大于此值。指定 0 将不会检测响应行长度。

RFC 2821 建议将最大响应行长度设置为 512。

可以启用规则 124:3，为此选项以及**替代最大命令行长度**（如已启用）生成事件并在内联部署中丢弃攻击性数据包。

替代最大命令行长度 (Alt Max Command Line Len)

检测任何指定命令的 SMTP 命令行的长度何时大于此值。指定 0 将不会检测指定命令的命令行长度。为众多命令设置了不同的默认行长度。

此设置将覆盖指定命令的“最大命令行长度”(Max Command Line Len) 设置。

可以启用规则 124:3，为此选项以及**最大响应行长度**（如已启用）生成事件并在内联部署中丢弃攻击性数据包。

无效命令 (Invalid Commands)

检测命令是否是从客户端发出的。

可以启用规则 124:6，为此选项以及**无效命令**生成事件并在内联部署中丢弃攻击性数据包。

有效命令 (Valid Commands)

允许此列表中的命令。

即使此列表为空，预处理器仍允许下列有效命令：ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

注释 RCPT TO 和 MAIL FROM 是 SMTP 命令。对这两个命令，预处理器配置分别使用命令名 RCPT 和 MAIL。在代码中，预处理器会将 RCPT 和 MAIL 映射到正确的命令名。

可以启用规则 124:4，为此选项以及**无效命令**（如已配置）生成事件并在内联部署中丢弃攻击性数据包。

数据命令 (Data Commands)

列出以与 SMTP DATA 命令按照 RFC5321 的要求发送数据相同的方法发起数据发送的命令。使用空格分隔多个命令。

二进制数据命令 (Binary Data Commands)

列出以与 BDAT 命令按照 RFC 3030 的要求发送数据类似的方法发起数据发送的命令。使用空格分隔多个命令。

身份验证命令 (Authentication Commands)

列出发起客户端和服务器之间的身份验证交换的命令。使用空格分隔多个命令。

检测 xlink2state (Detect xlink2state)

检测作为 X-Link2State Microsoft Exchange 缓冲区数据溢出攻击的一部分的数据包。在内联部署中，系统还可以丢弃这些数据包。

可以启用规则 124:8，为此选项生成事件并在内联部署中丢弃攻击性数据包。

Base64 解码深度 (Base64 Decoding Depth)

在**忽略数据 (Ignore Data)** 已禁用的情况下，指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。如果选择了**忽略数据 (Ignore Data)**，预处理器将不会对数据进行解码。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

当启用此选项时，可以启用规则124:10，在解码失败时生成事件并在内联部署中丢弃攻击性数据包；举例来说，解码可能会由于不正确的编码或损坏的数据而失败。

请注意，此选项取代已被弃用的**启用 MIME 解码 (Enable MIME Decoding)** 和**最大 MIME 解码深度 (Maximum MIME Decoding Depth)** 选项，后两个选项由于具有向后兼容性，因此在现有入侵策略中仍受到支持。

7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)

在**忽略数据 (Ignore Data)** 已禁用的情况下，指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括7位、8位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。如果选择了**忽略数据 (Ignore Data)**，预处理器将不会提取数据。

Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)

在**忽略数据 (Ignore Data)** 已禁用的情况下，指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。

可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。如果选择了**忽略数据 (Ignore Data)**，预处理器将不会对数据进行解码。

当启用此选项时，可以启用规则124:11，在解码失败时生成事件并在内联部署中丢弃攻击性数据包；举例来说，解码可能会由于不正确的编码或损坏的数据而失败。

Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)

在**忽略数据 (Ignore Data)** 已禁用的情况下，指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。如果选择了**忽略数据 (Ignore Data)**，预处理器将不会对数据进行解码。

当启用此选项时，可以启用规则124:13，在解码失败时生成事件并在内联部署中丢弃攻击性数据包；举例来说，解码可能会由于不正确的编码或损坏的数据而失败。

记录 MIME 附件名称 (Log MIME Attachment Names)

允许从 MIME Content-Disposition 报头提取 MIME 附件文件名，并将提取的文件名与为会话生成的所有入侵事件相关联。支持多个文件名。

启用此选项后，可以在入侵事件表视图的“邮件附件”(Email Attachment) 列中查看与事件相关的文件名。

记录收件人地址 (Log To Addresses)

允许从 SMTP RCPT TO 命令提取收件人邮件地址，并将提取的收件人地址与为会话生成的所有入侵事件相关联。支持多个收件人。

启用此选项后，可以在入侵事件表视图的“邮件收件人”(Email Recipient) 列中查看与事件相关的收件人。

记录发件人地址 (Log From Addresses)

允许从 SMTP MAIL FROM 命令提取发件人邮件地址，并将提取的发件人地址与为会话生成的所有入侵事件相关联。支持多个发件人地址。

启用此选项后，可以在入侵事件表视图的“邮件发件人”(Email Sender) 列中查看与事件相关的收件人。

记录报头 (Log Headers)

允许提取邮件报头。要提取的字节数取决于为**报头日志深度 (Header Log Depth)** 指定的值。

可以使用 `content` 或 `protected_content` 关键字来编写将邮件报头数据用作模式的入侵规则。还可以在入侵事件数据包视图中查看提取的邮件报头。

报头日志深度 (Header Log Depth)

指定在**记录报头 (Log Headers)** 已启用的情况下要提取的邮件报头的字节数。可指定 0 到 20480 字节。值 0 将会禁用**记录报头 (Log Headers)**。

相关主题

基本 content 和 protected_content 关键字参数

配置 SMTP 解码

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** (✎)。

如果显示**视图** (👁)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航窗格中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SMTP 配置 (SMTP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **SMTP 配置 (SMTP Configuration)** 旁边的 **编辑** (✎)。

步骤 7 修改SMTP 预处理器选项，第 54 页中所述的选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 SMTP 预处理器规则 (GID 124)。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层
冲突和更改：网络分析和入侵策略

SSH 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

SSH 预处理器检测：

- 质询-响应缓冲区溢出攻击
- CRC-32 攻击
- SecureCRT SSH 客户端缓冲区溢出攻击
- 协议不匹配
- SSH 消息方向不正确
- 任何版本字符串（版本 1 和 2 除外）

密钥交换后，会发生质询-响应缓冲区溢出攻击和 CRC-32 攻击，并会因此进行加密。这两种攻击在身份验证质询之后立即向服务器发送超过 20 KB 的反常态大量负载。CRC-32 攻击仅适用于 SSH 版本 1；质询-响应缓冲区溢出攻击仅适用于 SSH 版本 2。版本字符串在会话开端读取。除版本字符串的差异之外，这两种攻击的处理方式相同。

密钥交换前，如果试图保护连接，会发生 SecureCRT SSH 攻击和协议不匹配攻击。SecureCRT 攻击会向客户端发送过长的协议标识符字符串，从而导致缓冲区溢出。如果非 SSH 客户端应用试图连接到安全 SSH 服务器或者服务器和客户端的版本号不匹配，会出现协议不匹配攻击。

可以将SSH预处理器配置为检查指定端口或端口列表的流量，或者自动检测SSH流量。预处理器将会继续检查SSH流量，直至传递了未超过指定字节数的指定数量的加密数据包，或者直至超过指定数量的数据包中指定的最大字节数。如果超过最大字节数，系统将会假设出现了CRC-32（SSH版本1）攻击或质询-响应缓冲区溢出（SSH版本2）攻击。请注意，预处理器检测时无需配置任何版本字符串值（版本 1 和 2 除外）。

另请注意，SSH 预处理器不处理蛮力攻击。

SSH 预处理器选项

如果发生以下任何一种情况，预处理器将停止检查会话流量：

- 对于某个数量的加密数据包，服务器与客户端之间发生有效交换；连接继续保持。
- 在达到在**服务器无响应时可发送的字节数 (Number of Bytes Sent Without Server Response)** 中设置的值之前，达到要检查的加密数据包数量；假设发生了攻击。

在**待检查的加密数据包数量 (Number of Encrypted Packets to Inspect)** 中设置的数量内的每个有效服务器响应会重置**服务器无响应时可发送的字节数 (Number of Bytes Sent Without Server Response)**，且数据包计数继续进行。

可考虑以下 SSH 预处理器配置示例：

- **服务器端口 (Server Ports)**：22
- **自动检测端口 (Autodetect Ports)**：off
- **协议版本字符串最大长度 (Maximum Length of Protocol Version String)**：80
- **要检查的加密数据包数量 (Number of Encrypted Packets to Inspect)**：25
- **Number of Bytes Sent Without Server Response**：19600
- 所有检测选项均启用。

在本示例中，预处理器仅检查端口 22 的流量。也就是说，自动检测被禁用，因此只检查指定的端口。

此外，如果发生以下任何一种情况，本示例中的预处理器会停止检查流量：

- 客户端发送 25 个加密数据包，这些数据包总共不超过 19600 字节。假设没有发生攻击。
- 客户端发送25个加密数据包，这些数据包总共不超过19600字节。在这种情况下，预处理器可将发生的攻击视为质询-响应缓冲区溢出攻击，因为本示例中的会话为 SSH 版本 2 会话。

本示例中的预处理器还将检测处理流量过程中发生的以下任何情况：

- 服务器溢出，由大于 80 字节的版本字符串触发，表明为 SecureCRT 攻击
- 协议不匹配
- 数据包的传输方向错误

最后，预处理器将自动检测任何版本字符串（版本 1 和 2 除外）。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

服务器端口 (Server Ports)

指定 SSH 预处理器应检查其流量的端口。

可以配置单个端口或端口的逗号分隔列表。

自动检测端口 (Autodetect Ports)

将预处理器设置为会自动检测 SSH 流量。

如果选择此选项，预处理器会检查某个 SSH 版本号的所有流量。如果客户端和服务器数据包均没有包含版本号，预处理器将会停止处理。禁用此选项时，预处理器只会检查在**服务器端口 (Server Ports)**选项中确定的流量。

要检查的加密数据包数量 (Number of Encrypted Packets to Inspect)

指定每个会话待检查的数据流重组加密数据包的数量。

将此选项设置为 0 将允许所有流量通过。

减少待检查的加密数据包的数量可能会导致一些攻击避开检测。增加待检查的加密数据包的数量可能会对性能造成负面影响。

服务器无响应时可发送的字节数 (Number of Bytes Sent Without Server Response)

指定在假设存在质询-响应缓冲区溢出或 CRC-32 攻击之前，SSH 客户端在未获得响应的情况下可以向服务器发送的最大字节数。

如果预处理器对于质询-响应缓冲区溢出或 CRC-32 攻击生成误报，请增加此选项的值。

协议版本字符串的最大长度 (Maximum Length of Protocol Version String)

指定在假设存在 SecureCRT 攻击之前，服务器版本字符串中允许的最大字节数。

检测质询-响应缓冲区溢出攻击 (Detect Challenge-Response Buffer Overflow Attack)

启用或禁用质询-响应缓冲区溢出攻击检测。

您可以启用规则 128:1 为此选项生成事件并在内联部署中丢弃攻击性数据包。请注意，SFTP 会话可偶尔触发规则 128:1。

检测 SSH1 CRC-32 攻击 (Detect SSH1 CRC-32 Attack)

启用或禁用 CRC−-32 攻击检测。

您可以启用规则 128:2 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测服务器溢出 (Detect Server Overflow)

启用或禁用 SecureCRT SSH 客户端缓冲区溢出攻击检测。

您可以启用规则 128:3 为此选项 生成事件并在内联部署中丢弃攻击性数据包。

检测协议不匹配 (Detect Protocol Mismatch)

启用或禁用协议不匹配检测。

您可以启用规则 128:4 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测错误消息方向 (Detect Bad Message Direction)

允许或禁止检测流量传输方向错误这种情况（即，如果假定的服务器生成客户端流量，或者客户端生成服务器流量）。

您可以启用规则 128:5 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测给定负载的负载大小不正确 (Detect Payload Size Incorrect for the Given Payload)

允许或禁止检测负载大小不正确的数据包，例如，SSH 数据包中指定的长度与 IP 报头中指定的总长度不一致，或者消息被截断（即，无足够的数据用于整个 SSH 报头）。

您可以启用规则 128:6 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测错误版本字符串 (Detect Bad Version String)

请注意，启用预处理器后，它在检测时无需配置任何版本字符串（版本 1 和 2 除外）。

您可以启用规则 128:7 为此选项生成事件并在内联部署中丢弃攻击性数据包。

配置 SSH 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SSH 配置 (SSH Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **SSH 配置 (SSH Configuration)** 旁边的 **编辑** ()。

步骤 7 修改SSH 预处理器选项，第 60 页中所述的选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 SSH 预处理器规则 (GID 128)。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层

冲突和更改：网络分析和入侵策略

SSL 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

SSL 预处理器可供您配置 SSL 检查，从而可以阻止、解密或使用访问控制检查已加密的流量。无论是否配置 SSL 检查，SSL 预处理器也会分析在流量中检测到的 SSL 握手消息，并确定会话何时被加密。系统通过识别已加密流量可以停止对已加密负载执行入侵和文件检查，这有助于减少误报并提高性能。

SSL 预处理器还可以检查已加密流量以检测 Heartbleed 漏洞攻击尝试，并在检测到此类漏洞攻击时生成事件。

会话加密之后，可以暂停检查流量是否存在入侵和恶意软件。如果配置 SSL 检查，则 SSL 预处理器还将确定您可以阻止、解密或使用访问控制进行检查的已加密流量。

使用 SSL 预处理器解密已加密流量无需许可证。所有其他 SSL 预处理器功能（包括暂停检查已加密负载是否存在恶意软件和入侵，并检测 Heartbleed 漏洞攻击）均需要保护许可证。

SSL 预处理的工作原理

如果配置了 SSL 检查，则 SSL 预处理器停止对已加密数据进行入侵和文件检查，然后使用 SSL 策略对已加密流量进行检查。这有助于清除误报。SSL 预处理器在检查 SSL 握手时会维护状态信息，跟踪该会话的状态和 SSL 版本。如果预处理器检测到会话状态已被加密，系统会将该会话的流量标记为“加密”。可将系统配置为在确定会话已加密时停止处理已加密会话中的所有数据包，并在检测到 Heartbleed 漏洞攻击尝试时生成事件。

对于每个数据包，SSL 预处理器都会验证流量是否包含 IP 报头、TCP 报头和 TCP 负载，以及流量发生在指定适用于 SSL 预处理的端口上。对于符合条件的流量，可根据以下情况确定流量是否已加密：

- 系统观察会话中的所有数据包，未启用**服务器端数据受信任 (Server side data is trusted)**，并且会话包含来自服务器和客户端的“已完成”消息以及至少一个来自各端的数据包（包含应用记录但不包含警报记录）。
- 系统遗漏某些流量，未启用**服务器端数据受信任 (Server side data is trusted)**，并且会话至少包含一个来自服务器端和客户端的数据包（包含未使用警报记录应答的应用记录）。
- 系统观察会话中的所有数据包，已启用**服务器端数据受信任 (Server side data is trusted)**，并且会话包含来自客户端的“已完成”消息和至少一个来自客户端的数据包（包含应用记录但不包含警报记录）。
- 系统遗漏某些流量，已启用**服务器端数据受信任 (Server side data is trusted)**，并且会话至少包含一个来自客户端的数据包（包含未使用警报记录应答的应用记录）。

如果选择停止处理加密流量，系统会在将该会话标记为“加密”后忽略其中的后续数据包。

此外，在 SSL 握手期间，预处理器监控检测信号请求和响应。检测到以下对象时，预处理器生成事件。

- 包含大于负载本身的负载长度值的检测信号请求
- 大于“最大检测信号长度”(Max Heartbeat Length) 字段中存储的值的检测信号响应

注释 可向某规则添加 `ssl_state` 和 `ssl_version` 关键字，以便在该规则中使用 SSL 状态或版本信息。

相关主题

SSL 关键字

SSL 预处理器选项

注释 默认情况下，系统提供的网络分析策略启用 SSL 预处理器。如果预期有已加密流量通过您的网络，思科建议不要在自定义部署中禁用 SSL 预处理器。

如果未配置 SSL 检查，则系统尝试检查已加密流量是否存在恶意软件和入侵，而不对其进行解密。如果启用了 SSL 预处理器，它会检测会话加密的时间。启用 SSL 预处理器后，规则引擎可以调用预处理器来获得 SSL 状态和版本信息。如果在某个入侵策略中启用使用 `ssl_state` 和 `ssl_version` 关键字的规则，则还应在该策略中启用 SSL 预处理器。

端口

指定 SSL 预处理器应监控加密会话流量的端口（用逗号隔开）。只会检查此字段中指定端口的加密流量。

注释 如果 SSL 预处理器检测到指定用于 SSL 监控的端口上有非 SSL 流量，它会尝试将该流量作为 SSL 流量进行解码，然后将其标记为“损坏”。

停止检查加密流量 (Stop inspecting encrypted traffic)

启用或禁止在会话被标记为“加密”后检查会话中的流量。

启用此选项以禁止检查和重组加密的会话。SSL 预处理器会维护会话状态，因此，它可以禁止对会话中所有流量的检查。启用此选项时，系统会验证会话的几个数据包来确保流被加密，然后绕过深度检查。每个绕过的会话会增加 **show snort statistics** 命令的响应中显示的快速转发流计数。此外，由于绕过深度检查，连接事件中的发起方和响应方字节数将会不准确。发起方和响应方字节数小于实际会话的值，因为它只包括 Snort 检查的数据包，而不包括绕过深度检查后的任何数据包。这种行为适用于连接摘要事件和各构件中显示的所有流量值。

如果满足以下两个条件，则系统只会停止检查加密会话中的流量：

- 已启用 SSL 预处理
- 已选择此选项

如果清除此选项，则无法修改**服务器端数据受信任 (Server side data is trusted)** 选项。

服务器端数据受信任 (Server side data is trusted)

当“停止检查加密流量”(Stop inspecting encrypted traffic) 启用时，将支持仅根据客户端流量识别加密流量。

最大检测信号长度 (Max Heartbeat Length)

通过指定数个字节，支持检查 SSL 握手内的检测信号请求和响应以了解是否存在 Heartbleed 漏洞攻击尝试。您可以指定介于 `1` 和 65535 之间的整数，或指定 `0` 禁用该选项。

如果预处理器检测的检测信号请求的负载长度大于实际负载长度且规则 137:3 已启用，或者检测信号响应的大小大于当规则 137:4 已启用时为此选项配置的值，则预处理器生成事件并在内联部署中丢弃攻击性数据包。

配置 SSL 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略** 或**策略** > **访问控制标题** > **入侵**，然后点击**网络分析策略**。

注释
如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SSL 配置 (SSL Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **SSL 配置 (SSL Configuration)** 旁边的 **编辑** ()。

步骤 7 修改SSL 预处理器选项，第 64 页中所述的任意设置。

- 在**端口 (Ports)** 字段中输入值。多个值之间用逗号隔开。
- 选中或清除**停止检查加密流量 (Stop inspecting encrypted traffic)** 复选框。
- 如果选中**停止检查加密流量 (Stop inspecting encrypted traffic)**，请选中或清除**服务器端数据受信任 (Server side data is trusted)**。
- 在**最大检测信号长度 (Max Heartbeat Length)** 字段中输入值。

  提示
  值为 0 将会禁用此选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 SSL 预处理器规则 (GID 137)。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层
冲突和更改：网络分析和入侵策略

SSL 预处理器规则

如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 SSL 预处理器规则 (GID 137)。

下表说明了可启用的 SSL 预处理器规则。

表 *16: SSL* 预处理器规则

预处理器规则 GID:SID	说明
137:1	在 ServerHello 消息之后检测 ClientHello 消息，此操作无效并被视为异常行为。
137:2	在禁用 SSL 预处理器选项**服务器端数据受信任 (Server side data is trusted)** 时检测没有 ClientHello 消息的 ServerHello 消息，此操作无效并被视为异常行为。
137:3	在 SSL 预处理器选项**最大检测信号长度 (Max Heartbeat Length)** 包含非零值时检测负载长度大于负载本身的检测信号请求，此操作指示尝试利用 Heartbleed 漏洞。
137:4	检测大于 SSL 预处理器选项**最大检测信号长度 (Max Heartbeat Length)** 中指定的非零值的检测信号响应，此操作指示尝试利用 Heartbleed 漏洞。

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。