传输层和网络层预处理器

以下主题介绍传输层和网络层预处理器及其配置方式：

传输层和网络层预处理器简介

网络层和传输层预处理器检测对 IP 分片、校验和验证及 TCP 和 UDP 会话预处理加以利用的攻击。在将数据包发送到预处理器之前，数据包解码器将数据包报头和负载转换为便于预处理器和入侵规则引擎使用的格式，并检测数据包报头的各种异常行为。在数据包解码后到将数据包发送到其他预处理器之前这段期间，内联规范化预处理器会对流量进行规范化以便进行内联部署。

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。

传输层和网络层预处理器的许可证要求

威胁防御 许可证

IPS

传输层和网络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

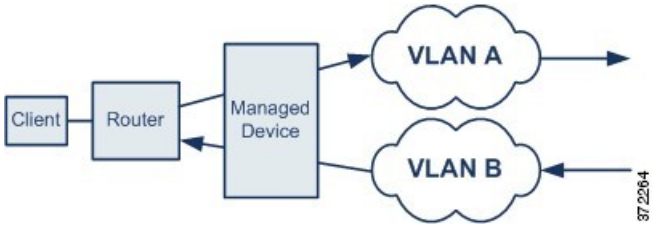
- 管理员
- 入侵管理员

高级传输/网络预处理器设置

高级传输和网络预处理器设置全局应用于会部署访问控制策略的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。

忽略的 VLAN 报头

同一连接中行进方向不同的流量中的 VLAN 标记不同，可能影响流量重组和规则处理。例如，在下图中，同一连接的流量可以通过 VLAN A 进行传输，并通过 VLAN B 进行接收。



您可以将系统配置为忽略 VLAN 报头，从而可以针对您的部署正确处理数据包。

入侵丢弃规则中的活动响应

丢弃规则是指规则状态设置为“丢弃并生成事件”(Drop and Generate Events) 的入侵规则或预处理器。在内联部署中，系统通过丢弃触发数据包并阻止数据包起始的会话来对 TCP 或 UDP 丢弃规则作出响应。

提示 由于在会话方面通常未考虑 UDP 数据流，因此数据流预处理器使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别 UDP 会话。

您可以配置系统来启动一个或多个活动响应，从而在有问题的数据包触发 TCP 或 UDP 丢弃规则时，更精确具体地关闭 TCP 连接或 UDP 会话。您可以在内联部署中使用活动响应，包括路由部署和透明部署。主动响应不适合或不支持被动部署。

要配置活动响应，请执行以下操作：

- 创建或修改 TCP 或 UDP（仅限 **resp** 关键字）入侵规则。请参阅入侵规则报头协议。
- 为入侵规则添加 **react** 或 **resp** 关键字；请参阅 x活动响应关键字。
- 或者对于 TCP 连接，可以指定要发送的其他活动响应的最大数量以及活动响应之间等待的秒数；请参阅 高级传输/网络预处理器选项，第 3 页中的 **最大活动响应数** 和 **最小响应秒数** 。

当匹配流量触发丢弃规则时，活动响应会关闭会话，如下所示：

- **TCP** - 丢弃触发数据包，并在客户端和服务器流量中插入 TCP 重置 (RST) 数据包。
- **UDP** - 向会话的两端发送 ICMP 不可达数据包。

高级传输/网络预处理器选项

在跟踪连接时忽略 VLAN 报头

指定在识别流量时是忽略还是包含 VLAN 报头，如下所示：

- 选择此选项时，系统会忽略 VLAN 报头。此设置用于在按不同方向传播的流量中可能检测到同一连接的不同 VLAN 标签的已部署设备
- 当禁用此选项时，系统会包含 VLAN 报头。此设置用于在按不同方向传播的流量中不会检测到同一连接的不同 VLAN 标签的已部署设备。

最大活动响应数

指定每个 TCP 连接的最大活动响应数。如果已启动活动响应的连接上出现其他流量，并且在先前活动响应后流量出现超过**最小响应秒数 (Minimum Response Seconds)**，系统会发送其他活动响应，除非已达到指定的最大数量。设置为 0 会禁用 **resp** 或 **react** 规则触发的其他活动响应。请参阅入侵丢弃规则中的活动响应，第 2 页和活动响应关键字。

请注意，无论此选项如何配置，所触发的 **resp** 或 **react** 规则都会启动主动响应。

最小响应秒数

指定在系统已启动活动响应的连接上的任何其他流量都会产生后续活动响应之前等待的秒数，直至出现**最大活动响应数 (Maximum Active Responses)**。

故障排除选项：会话终止日志记录阈值 (Troubleshooting Options: Session Termination Logging Threshold)

注意 请勿修改“会话终止日志记录阈值”(Session Termination Logging Threshold)，除非支持人员指示执行此操作。

支持人员可能会在故障排除呼叫期间要求您配置系统，以在单个连接超过指定阈值时记录消息。更改此选项的设置会影响性能，应仅在支持人员的指导下进行操作。

此选项指定一个字节数，当会话终止并超过该指定数字时，将会记录消息。

注释 1GB 的上限还受数据流处理分配的托管设备上的内存容量限制。

相关主题

活动响应关键字

配置高级传输/网络预处理器设置

您必须是 管理员、访问管理员 或 网络管理员 才能执行此任务。

过程

步骤 1 在访问控制策略编辑器中，点击要修改的策略上的 **编辑** (✎) 。

步骤 2 点击 **更多** > **高级设置**，然后点击 **传输/网络预处理程序设置** 部分旁边的 **编辑** (✎) 。

步骤 3 修改高级传输/网络预处理器选项，第 3 页中描述的选项，故障排除选项**会话终止日志记录阈值 (Session Termination Logging Threshold)** 除外。

注意
请勿修改**会话终止日志记录阈值 (Session Termination Logging Threshold)**，除非支持人员指示执行此操作。

步骤 4 点击**确定 (OK)**。

下一步做什么

- 或者，进一步配置策略，如编辑访问控制策略中所述。
- 部署配置更改；请参阅 部署配置更改。

校验和验证

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。

系统可验证所有协议级校验和，以确保接收完整的 IP、TCP、UDP 和 ICMP 传输，且基本级别的数据包在传输过程中未被篡改或意外修改。校验和使用算法来验证数据包中的协议是否完整。如果系统计算的值与终端主机在数据包中写入的值一致，则认为该数据包未被更改。

禁用校验和验证可能导致您的网络易受插入攻击。请注意，系统不会生成校验和验证事件。在内联部署中，可以将系统配置为丢弃校验和无效的数据包。

校验和验证选项

在被动或内联部署中，可以将以下任何选项设置为**已启用 (Enabled)** 或**已禁用 (Disabled)**；或在内联部署中设置为**丢弃 (Drop)**：

- **ICMP 校验和 (ICMP Checksums)**
- **IP 校验和 (IP Checksums)**
- **TCP 校验和 (TCP Checksums)**
- **UDP 校验和 (UDP Checksums)**

要丢弃恶意数据包，除将选项设置为**丢弃 (Drop)** 以外，还必须在关联网络分析策略中启用**内联模式 (Inline Mode)** 并确保设备为内联部署。

在被动部署中或在分流模式下的内联部署中，将这些选项设置为**丢弃 (Drop)** 与将其设置为**已启用 (Enabled)** 的作用相同。

注意 在 **TCP 校验和**下， **忽略** 选项（默认）会绕过或忽略任何已配置的 Snort 规则。

所有校验和验证选项默认为**已启用 (Enabled)**。但是，威胁防御 路由接口和透明接口始终会丢弃 IP 校验和验证失败的数据包。请注意，在将数据包传递到 Snort 进程之前，威胁防御 路由和透明接口会修复带有错误校验和的 UDP 数据包。

相关主题

内联部署中预处理器流量的修改

验证校验和

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**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**校验和验证 (Checksum Verification)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**校验和验证 (Checksum Verification)** 旁边的 **编辑** ()。

步骤 7 修改校验和验证，第 5 页中所述的选项。

注释
在 **TCP 校验和**下， **忽略** 选项（默认）会绕过或忽略任何已配置的 Snort 规则。

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

- 部署配置更改；请参阅 部署配置更改。

相关主题

层管理
冲突和更改：网络分析和入侵策略

内联规范化预处理器

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。

内联规范化预处理器会将流量规范化，从而尽可能降低攻击者在内联部署中得以避开检测的可能性。

注释 为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向托管设备部署相关配置。

您可以指定 IPv4、IPv6、ICMPv4、ICMPv6 和 TCP 流量的任意组合的规范化。大多数规范化由内联规范化预处理器逐个数据包执行。但是，TCP 数据流预处理器处理大多数状态相关的数据包和数据流规范化，包括 TCP 负载规范化。

在数据包解码器进行解码后会立即执行内联规范化，直至其他预处理器进行处理。规范化从内数据包层继续执行到外数据包层。

内联规范化预处理器不会生成事件；它准备数据包以供内联部署中的其他预处理器和规则引擎使用。预处理器还有助于确保系统处理的数据包与网络中主机接收的数据包相同。

注释 在内联部署中，我们建议您启用内联模式并配置已启用 **Normalize TCP Payload** 选项的内联规范化预处理器。在被动部署中，我们建议您使用 自适应配置文件。

相关主题

内联部署中预处理器流量的修改

关于自适应配置文件

内联规范化选项

Minimum TTL

当**重置 TTL (Reset TTL)** 大于或等于为此选项设置的值时，请指定以下设置：

- 启用**规范化 IPv4 (Normalize IPv4)** 后系统允许“IPv4 生存时间 (TTL)”(IPv4 Time to Live [TTL]) 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对**重置 TTL (Reset TTL)** 设置的值
- 启用**规范化 IPv6 (Normalize IPv6)** 后系统允许“IPv6 跳数限制”(IPv6 Hop Limit) 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对**重置 TTL (Reset TTL)** 设置的值

此字段为空时，系统假设值为 1。

注释 对于 威胁防御 路由和透明接口，**最小 TTL** 和**重置 TTL** 选项会被忽略。连接的最大 TTL 由初始数据包中的 TTL 来确定。后续数据包的 TTL 可以减少，但不能增加。系统会将 TTL 重置为该连接之前看到过的最低 TTL。这可以防止 TTL 回避攻击。

当数据包解码**检测协议报头异常**选项已启用时，可以启用解码器规则类别中的以下规则来为此选项生成事件并在内联部署中丢弃攻击性数据包：

- 当系统检测到 TTL 小于指定最小值的 IPv4 数据包时，您可以启用规则 116：428 来触发。
- 当系统检测到跳数限制小于指定最小值的 IPv6 数据包时，您可以启用规则 116：270 来触发。

Reset TTL

如果设置为大于或等于**最小 TTL (Minimum TTL)** 的值，请规范化以下字段：

- IPv4 TTL 字段（如果启用了**规范化 IPv4 [Normalize IPv4]**）
- “IPv6 跳数限制”(IPv6 Hop Limit) 字段（如果启用了**规范化 IPv6 [Normalize IPv6]**）

当数据包值小于**最小 TTL (Minimum TTL)** 时，系统会通过将其 TTL 或“跳数限制”(Hop Limit) 值更改为针对此选项设置的值来规范化数据包。将此字段留空或设置为 0，或设置为小于**最小 TTL (Minimum TTL)** 的任意值会禁用该选项。

规范化 IPv4 (Normalize IPv4)

启用 IPv4 流量规范化。在以下时候，系统还会根据需要规范化 TTL 字段：

- 此选项启用，且
- 为**重置 TTL (Reset TTL)** 设置的值启用 TTL 规范化。

此选项启用时，还可以启用额外的 IPv4 选项。

启用此选项时，系统执行以下基本 IPv4 规范化：

- 将具有多余负载的数据包截断至 IP 报头中指定的数据报长度
- 清除“差分服务 (DS)”(Differentiated Services [DS]) 字段（以前称为“服务类型 (TOS)”(Type of Service [TOS]) 字段）
- 将所有选项八位元设置为 1（“无操作”[No Operation]）

对于 威胁防御 路由和透明接口，此选项会被忽略。威胁防御 设备将丢弃任何包含除任何路由或透明接口上的路由器警报、选项列表结束 (EOOL) 以及无操作 (NOP) 选项之外的 IP 选项的 RSVP 数据包。

规范化不分片位 (Normalize Don't Fragment Bit)

清除“IPv4 标志”(IPv4 Flags) 报头字段的一位“不分片”(Don’t Fragment) 子字段。通过启用此选项，下游路由器可在必要时对数据包进行分片而不是将其丢弃；启用此选项还可以根据要丢弃的构造数据包来防止躲避检测。必须启用**规范化 IPv4 (Normalize IPv4)** 后才可以选择此选项。

规范化保留位 (Normalize Reserved Bit)

清除“IPv4 标志”(IPv4 Flags) 报头字段的一位“保留”(Reserved) 子字段。通常会启用此选项。必须启用**规范化 IPv4 (Normalize IPv4)** 后才可以选择此选项。

规范化 TOS 位 (Normalize TOS Bit)

清除一个字节的“差分服务”(Differentiated Services) 字段（以前称为“服务类型”[Type of Service]）。必须启用**规范化 IPv4 (Normalize IPv4)** 后才可以选择此选项。

规范化多余负载 (Normalize Excess Payload)

将具有多余负载的数据包截断至 IP 报头中指定的数据报长度加上第 2 层（例如以太网）报头，但是不截断为小于最小帧长度。必须启用**规范化 IPv4 (Normalize IPv4)** 后才可以选择此选项。

对于威胁防御路由和透明接口，此选项会被忽略。在这些接口上始终丢弃具有多余负载的数据包。

规范化 IPv6 (Normalize IPv6)

将“逐跳选项”(Hop-by-Hop Options)和“目标选项”(Destination Options) 扩展报头中的所有“选项类型”(Option Type) 字段设置为 00（跳过并继续处理）。此选项处于启用状态并且为**重置 TTL (Reset TTL)** 设置的值会启用跳数限制规范化时，系统还会根据需要规范化 Hop Limit 字段。

规范化 ICMPv4 (Normalize ICMPv4)

清除 ICMPv4 流量中“回应（请求）”(Echo [Request]) 和“回应答复”(Echo Reply) 消息内的 8 位“代码”(Code) 字段。

规范化 ICMPv6 (Normalize ICMPv6)

清除 ICMPv6 流量中“回应（请求）”(Echo [Request]) 和“回应答复”(Echo Reply) 消息内的 8 位“代码”(Code) 字段。

Normalize/Clear Reserved Bits

清除 TCP 报头中的保留位。

规范化/清除选项填充字节 (Normalize/Clear Option Padding Bytes)

清除任何 TCP 选项填充字节。

Clear Urgent Pointer if URG=0

如果未设置紧急 (URG) 控制位，则清除 16 位 TCP 报头 Urgent Pointer 字段。

Clear Urgent Pointer/URG on Empty Payload

如果没有负载，则清除 TCP 报头“紧急指针”(Urgent Pointer) 字段和 URG 控制位。

如果未设置紧急指针则清除 URG (Clear URG if Urgent Pointer is Not Set)

如果未设置紧急指针，则清除 TCP 报头 URG 控制位。

Normalize Urgent Pointer

如果指针大于负载长度，则将两字节的 TCP 报头 Urgent Pointer 字段设置为负载长度。

规范化 TCP 负载 (Normalize TCP Payload)

启用“TCP 数据”(TCP Data) 字段的规范化以确保重传数据的一致性。无法正确重组的所有数据段都会被丢弃。

Remove Data on SYN

如果 TCP 操作系统策略**不是** Mac OS，则移除同步 (SYN) 数据包中的数据。

此选项还会禁用规则 129:2，该规则原本会在 TCP 数据流预处理器**策略**选项未设置为 **Mac OS** 时触发。

Remove Data on RST

从 TCP 重置 (RST) 数据包中删除所有数据。

根据窗口修剪数据 (Trim Data to Window)

将“TCP 数据”(TCP Data) 字段修剪为在“窗口”(Window) 字段中指定的大小。

根据 MSS 修剪数据 (Trim Data to MSS)

如果负载长度大于 MSS，则将 TCP Data 字段修剪为 Maximum Segment Size (MSS)

阻止不可解析的 TCP 报头异常 (Block Unresolvable TCP Header Anomalies)

启用此选项时，系统阻止异常 TCP 数据包，这些数据包在规范化的情况下会无效，并可能受到接收主机的阻止。例如，系统阻止后续传输到已建立的会话上的任何 SYN 数据包。

无论是否启用规则，系统都会丢弃与以下任何 TCP 数据流预处理器规则匹配的任何数据包：

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11

- 129:14 至 129:19

Total Blocked Packets 性能图跟踪内联部署中阻止的数据包的数量，并且，在被动部署和轻触模式下的内联部署中，跟踪在内联部署中已阻止的数量。

显式堵塞通知

对显式堵塞通知 (ECN) 标志启用逐个数据包或逐条数据流规范化，如下所示：

- 选择 **Packet** 以逐个数据包清除 ECN 标志（无论协商与否）
- 选择 **Stream** 以逐条数据流清除 ECN 标志（如果未协商 ECN 的使用）

如果选择**数据流 (Stream)**，您还必须确保启用 TCP 数据流预处理器的**需要 TCP 三次握手 (Require TCP 3-Way Handshake)** 选项以进行此规范化。

清除现有 TCP 选项 (Clear Existing TCP Options)

启用**允许这些 TCP 选项 (Allow These TCP Options)**。

允许这些 TCP 选项 (Allow These TCP Options)

禁用您在流量中允许的特定 TCP 选项的规范化。

系统不对您明确允许的选项进行规范化。系统会通过将您未明确允许的选项设置为“无操作”(No Operation)（TCP 选项 1）来规范化这些选项。

由于这些选项常用于实现最佳 TCP 性能，因此无论**允许这些 TCP 选项**的配置如何，系统始终会允许以下选项：

- 最大分片大小 (MSS)
- 窗口比例
- 时间戳 TCP

系统不会自动允许其他不太常用的选项。

您可以通过配置选项关键字和/或选项编号的逗号分隔列表来允许特定选项，如下例所示：

```
sack, echo, 19
```

指定选项关键字等同于指定与该关键字相关的一个或多个 TCP 选项的编号。例如，指定 `sack` 等同于指定 TCP 选项 4（“允许选择性确认 [Selective Acknowledgment Permitted]”）和选项 5（“选择性确认”[Selective Acknowledgment]）。选项关键字不区分大小写。

您还可以指定 `any`，这样将会允许所有 TCP 选项并有效地禁用所有 TCP 选项的规范化。

下表总结了如何指定要允许的 TCP 选项。如果将字段留空，则系统仅允许 MSS、Window Scale 和 Time Stamp 选项。

可指定的内容	以允许.....
sack	TCP 选项 4（“允许选择性确认 [Selective Acknowledgment Permitted]”）和选项 5（“选择性确认”[Selective Acknowledgment]）
echo	TCP 选项 6（“回应请求”[Echo Request]）和选项 7（“回应答复”[Echo Reply]）
partial_order	TCP 选项 9（“允许的偏序连接”[Partial Order Connection Permitted]）和选项 10（“偏序服务配置文件”[Partial Order Service Profile]）
conn_count	TCP 连接计数选项 11 (CC)、选项 12 (CC.New) 和选项 13 (CC.Echo)
alt_checksum	TCP 选项 14（“替代校验和请求”[Alternate Checksum Request]）和选项 15（“替代校验和”[Alternate Checksum]）
md5	TCP 选项 19（“MD5 签名”[MD5 Signature]）
选项编号（2 至 255）	特定选项，包括没有关键字的选项
any	所有 TCP 选项；此设置会有效地禁用 TCP 选项规范化

如果没有为此选项指定 `any`，则规范化会包含以下内容：

- 除 MSS、“窗口比例”(Window Scale)、“时间戳”(Time Stamp) 及任何明确允许的选项以外，所有选项字节都设置为“无操作”(No Operation)（TCP 选项 1）
- 如果时间戳存在但无效，或者有效但未协商，则将时间戳八位元设置为“无操作”(No Operation)
- 如果“时间戳”(Time Stamp) 已协商但不存在，则阻止数据包
- 如果未设置 Acknowledgment (ACK) 控制位，则清除“时间戳回应答复 (TSecr)”(Time Stamp Echo Reply [TSecr]) 选项字段
- 如果未设置 SYN 控制位，则将 MSS 和 Window Scale 选项设置为 No Operation (TCP Option 1)

相关主题

内联部署中预处理器流量的修改
关于自适应配置文件

配置内联规范化

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

- 如果要规范化或丢弃恶意数据包，请启用**内联模式 (Inline Mode)**，如内联部署中预处理器流量的修改中所述。托管设备也必须内联部署。

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)**（不是插入符号；点击单词）。

步骤 5 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**内联规范化 (Inline Normalization)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**内联规范化 (Inline Normalization)** 旁边的 **编辑** (✎)。

步骤 7 设置选项，如内联规范化预处理器，第 7 页中所述。

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

- 如果要让内联规范化的“最小 TTL”(Minimum TTL) 选项生成入侵事件，请启用任一或两个数据包解码器规则：116:429 (IPv4) 和 116:270 (IPv6)。有关详细信息，请参阅设置入侵规则状态和内联规范化选项，第 7 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

层管理
冲突和更改：网络分析和入侵策略
内联部署中预处理器流量的修改
关于自适应配置文件

IP 分片重组预处理器

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。

由于 IP 数据报大于最大传输单位 (MTU) 而将其分为两个或多个更小的 IP 数据报，这个过程即为数据报分片。单个 IP 数据报片段可能未包含足够的信息来识别隐藏攻击。攻击者可能尝试通过将攻击数据传输到分片数据包中来躲避检测。在规则引擎对分片的 IP 数据报执行规则之前，IP 分片重组预处理器会重组这些数据报，以便规则可以更适当地识别这些数据包中的攻击。如果分片的数据报无法重组，则不对其执行规则。

IP 分片重组漏洞

启用 IP 分片重组可以帮助您检测针对网络上主机的攻击（例如泪滴 [teardrop] 攻击）和针对系统本身的资源消耗攻击（例如 Jolt2 攻击）。

泪滴攻击利用某些操作系统中在尝试重组重叠 IP 片段时会导致这些操作系统崩溃的漏洞。IP 分片重组预处理器在被启用并配置为识别重叠片段之后，会执行此操作。IP 分片重组预处理器会检测重叠片段攻击（例如泪滴攻击）中的第一批数据包，但对于同一攻击不会检测后续数据包。

Jolt2 攻击会发送同一分片的 IP 数据包的大量副本，以尝试过度使用 IP 分片重组器并导致拒绝服务攻击。内存使用上限会中断此攻击以及 IP 分片重组预处理器中的类似攻击，并在全面检查基础上注重系统自我保护。这样，系统不会因攻击而崩溃，可保持运行，并继续检查网络流量。

不同的操作系统以不同方式重组分片数据包。可以确定主机运行的操作系统的攻击者还可以对恶意数据包进行分片，以便目标主机以特定方式对这些数据包进行重组。由于系统不知道受监控网络上的主机运行的操作系统，因此预处理器可能会不正确地重组和检查数据包，致使漏洞成功躲过检测。要缓解这种攻击，您可以配置分片重组预处理器，使其会针对网络中的每个主机使用适当方法对数据包进行分片重组。

请注意，您也可以在被动部署中使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 IP 分片重组预处理器动态选择基于目标的策略。

基于目标的分片重组策略

主机的操作系统使用三个条件来确定当重组数据包时支持的数据包分片。

- 操作系统收到分片的顺序
- 其偏移量（分片与数据包开始位置之间的距离，按字节计算）
- 它与重叠分片相比的开始和结束位置。

虽然每个操作系统都使用这些条件，但是不同的操作系统在重组分片数据包时支持不同的分片。因此，网络中具有不同操作系统的两个主机可能会以完全不同的方式重组同一组重叠分片。

攻击者如果了解其中一个主机的操作系统，可能会尝试通过发送隐藏在重叠数据包片段中的恶意内容来逃避检测并攻击该主机。该数据包经过重组和检查后看似无害，但是由目标主机进行重组后则会包含恶意的漏洞。但是，如果将 IP 分片重组预处理器配置为可感知受监控网段上运行的操作系统，则它会以与目标主机相同的方式重组分片，从而识别攻击。

IP 分片重组选项

您可以选择只是启用或禁用 IP 分片重组；但是，思科建议以更精细的级别指定已启用的 IP 分片重组预处理器的行为。

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。

可以配置以下全局选项：

预分配分片 (Preallocated Fragments)

预处理器一次可以处理的最大单个分片数量。指定要预分配的片段节点的数量会启用静态内存分配。

⚠

注意 处理单个分片会使用大约1550字节的内存。如果预处理器处理单个片段所需的内存超过托管设备的预定允许的内存限制，则设备的内存限制优先。

您可以为每个 IP 分片重组策略配置以下选项：

网络 (Networks)

要对其应用分片重组策略的一个或多个主机的 IP 地址。

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。您可以指定总共最多 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 (Policy)

要为受监控网段上的主机组使用的分片重组策略。

根据目标主机的操作系统，可以选择七个分片重组策略之一。下表列出了这七个策略以及使用每个策略的操作系统。第一个和最后一个这两个策略名称反映这些策略是否支持原始或后续重叠数据包。

对于 威胁防御 路由和透明接口，此选项会被忽略。

表 *1:* 基于目标的分片重组策略

策略	操作系统
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect
首先	Mac OS HP-UX
Linux	Linux OpenBSD
最后	思科 IOS
Solaris	SunOS
Windows	Windows

超时

指定预处理器引擎在重组分片数据包时可用的最长时间（以秒为单位）。如果在指定的时间段内无法重组数据包，则预处理器引擎会停止尝试重组数据包并丢弃接收到的片段。

最小 TTL

指定数据包可具有的可接受最小 TTL 值。此选项检测基于 TTL 的插入攻击。

您可以启用规则 123:11 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测异常

确定分片问题，例如重叠分片。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以通过启用以下规则来为此选项生成事件并在内联部署中丢弃攻击性数据包：

- 123:1 至 123:4
- 123:5（BSD 策略）
- 123:6 至 123:8

重叠限制 (Overlap Limit)

指定在检测到会话中存在所配置数量的重叠片段时，将会停止该会话的分片重组。

必须启用**检测异常 (Detect Anomalies)** 后才可以配置此选项。不指定值将会禁用此选项。值为 0 指定重叠片段的数量不受限制。

对于 威胁防御 路由和透明接口，此选项会被忽略。在这些接口上始终丢弃重叠分片。

您可以启用规则 123:12 为此选项生成事件并在内联部署中丢弃攻击性数据包。

最小分片大小 (Minimum Fragment Size)

指定在检测到小于所配置数量的非最后一个分片时，数据包将被视为恶意。

必须启用**检测异常 (Detect Anomalies)** 后才可以配置此选项。不指定值将会禁用此选项。值 0 表示无限字节数。

您可以启用规则 123:13 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 IP 分片重组

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**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的 **IP 分片重组 (IP Defragmentation)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **IP 分片重组 (IP Defragmentation)** 旁边的 **编辑** ()。

步骤 7 或者，在**预分配片段 (Preallocated Fragments)** 字段中输入值。

步骤 8 有以下选项可供选择：

- 添加服务器配置文件 - 点击页面左侧**服务器 (Servers)** 旁边的 **添加** ()，然后在**主机地址 (Host Address)** 字段中输入值，并点击**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。可以创建总共 255 个基于目标的策略（包括默认策略）。
- 编辑服务器配置文件 - 点击页面左侧**服务器 (Servers)** 下的已配置地址，或点击**默认 (default)**。
- 删除配置文件 - 点击策略旁边的 **删除** ()。

步骤 9 修改IP 分片重组选项，第 15 页中所述的选项。

步骤 10 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 IP 解除分段规则 (GID 123)。有关详细信息，请参阅设置入侵规则状态和IP 分片重组选项，第 15 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

层基础知识
冲突和更改：网络分析和入侵策略

数据包解码器

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。

在将捕获的数据包发送到预处理器之前，系统首先会将数据包发送到数据包解码器。数据包解码器将数据包报头和负载转换为便于预处理器和规则引擎使用的格式。每个堆栈层依次进行解码，从数据链路层开始并继续直至网络层和传输层。

数据包解码器选项

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。

解码 GTP 数据通道 (Decode GTP Data Channel)

解码封装的GTP（通用分组无线服务[GPRS]隧道协议）数据通道。默认情况下，解码器在端口3386上解码版本0数据，在端口2152上解码版本1数据。您可以使用默认变量 `GTP_PORTS` 来修改用于识别封装 GTP 流量的端口。

您可以启用规则 116:297 和 116:298 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测非标准端口上的 Teredo (Detect Teredo on Non-Standard Ports)

检测 UDP 端口（而非端口 3544）上识别的 IPv6 流量的 Teredo 隧道。

只要 IPv6 流量存在，系统总会检测到 IPv6 流量。默认情况下，IPv6 检测包括 4in6、6in4、6to4 和 6in6 隧道方案；当 UDP 报头指定端口 3544 时，还包括 Teredo 隧道。

在 IPv4 网络中，IPv4 主机可使用 Teredo 协议通过 IPv4 网络地址转换 (NAT) 设备隧道传输 IPv6 流量。Teredo将在IPv4 UDP数据报内封装IPv6数据包，以允许在IPv4 NAT设备后面执行IPv6连接。正常情况下，系统使用 UDP 端口 3544 来识别 Teredo 流量。但是，攻击者可能会使用非标准端口来尝试避开检测。您可以启用**检测非标准端口上的 Terado (Detect Teredo on Non-Standard Ports)**，使系统检查 Teredo 隧道的所有 UDP 负载。

系统仅在外网层使用 IPv4 时才会执行 Teredo 解码，并且仅对第一个 UDP 报头执行 Teredo 解码。如果由于UDP数据封装在IPv6数据中，导致Teredo IPv6层之后还有一层UDP，规则引擎将使用UDP入侵规则来分析内外 UDP 层。

请注意，**策略-其他 (policy-other)** 规则类别中的入侵规则 12065、12066、12067 和 12068 会检测 Teredo 流量，但不对这些流量进行解码。您可以根据需要在内联部署中使用这些规则丢弃 Teredo 流量；但是，启用**检测非标准端口上的 Terado (Detect Teredo on Non-Standard Ports)** 时，应确保这些规则处于禁用状态或者设置为生成事件而不丢弃流量。

检测多余长度值 (Detect Excessive Length Value)

在数据包报头指定的数据包长度大于实际数据包长度时进行检测。

对于威胁防御路由、透明和内联接口，此选项会被忽略。始终丢弃报头长度过长的数据包。但此选项适用于 威胁防御 内联分流和被动接口。

您可以启用规则 116:6、116:47、116:97 和 116:275 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测无效 IP 选项 (Detect Invalid IP Options)

检测无效的 IP 报头选项，以识别使用无效 IP 选项的攻击。例如，有一项针对防火墙的拒绝服务攻击，导致系统冻结。防火墙尝试解析无效的“时间戳”(Timestamp) 和“安全 IP”(Security IP) 选项且未能检查到零长度，导致无法恢复的无限循环。规则引擎将识别零长度选项，并提供相关信息供您通过防火墙缓解攻击。

威胁防御 设备将丢弃任何包含除任何路由或透明接口上的路由器警报、选项列表结束 (EOOL) 以及无操作 (NOP) 选项之外的 IP 选项的 RSVP 数据包。对于内联、内联分流或被动接口，对 IP 选项的处理如上所述。

您可以启用规则 116:4 和 116:5 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测试验性 TCP 选项 (Detect Experimental TCP Options)

检测使用试验性 TCP 选项的 TCP 报头。下表介绍了这些选项。

TCP 选项	说明
9	允许的偏序连接
10	偏序服务配置文件
14	替代校验和请求
15	替代校验和数据
18	尾部校验和
20	空间通信协议标准
21	选择性否定确认
22	记录边界 (SCPS)
23	损坏 (SPCS)
24	SNAP
26	TCP 压缩过滤器

由于这些是试验性选项，所以有些系统未使用它们，从而可能遭受攻击。

注释 除上表中列出的试验性选项之外，系统还会考虑选项编号大于 26 的任何试验性 TCP 选项。

您可以启用规则 116:58 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测过时 TCP 选项 (Detect Obsolete TCP Options)

检测使用过时 TCP 选项的 TCP 报头。由于这些是过时选项，所以有些系统未使用它们，从而可能遭受攻击。下表介绍了这些选项。

TCP 选项	说明
6	回应
7	回应应答
16	Skeeter
17	Bubba
19	MD5 签名

TCP 选项	说明
25	未分配

您可以启用规则 116:57 以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 T/TCP (Detect T/TCP)

检测使用 CC.ECHO 选项的 TCP 报头。CC.ECHO 选项可确认是否正在使用 TCP 事务协议 (T/TCP)。由于 T/TCP 报头选项未被广泛应用，所以有些系统未使用它们，从而可能遭受攻击。

您可以启用规则 116:56 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测其他 TCP 选项 (Detect Other TCP Options)

检测其中的无效 TCP 选项未被其他 TCP 解码事件选项检测到的 TCP 报头。例如，此选项会检测长度不正确或长度致使选项数据超出 TCP 报头的 TCP 选项。

对于 威胁防御 路由和透明接口，此选项会被忽略。始终丢弃具有无效 TCP 选项的数据包。

您可以启用规则 116:54、116:55 和 116:59 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测协议报头异常 (Detect Protocol Header Anomalies)

检测更具体的 IP 和 TCP 解码器选项未检测到的其他解码错误。例如，解码器可能会检测到格式错误的数据链路协议报头。

对于威胁防御路由、透明和内联接口，此选项会被忽略。始终丢弃报头异常的数据包。但此选项适用于威胁防御内联分流和被动接口。

要为此选项生成事件并在内联部署中丢弃攻击性数据包，可以启用以下任一规则：

GID:SID	在以下情况下生成事件：
116:467	数据包小于用　思科 FabricPath 报头封装的数据包的最小尺寸。
116:468	报头中的思科元数据 (CMD) 字段包含长度小于有效 CMD 报头最小尺寸的报头。CMD 字段与思科 Trustsec 协议相关联。
116:469	报头中的 CMD 字段包含无效字段长度。
116:470	报头中的 CMD 字段包含无效安全组标记 (SGT) 选项类型。
116:471	报头中的 CMD 字段包含具有保留值的 SGT。

您也可以启用与其他数据包解码器选项不关联的任何数据包解码器规则。

相关主题

预定义默认变量

配置数据包解码

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 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**数据包解码 (Packet Decoding)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**数据包解码 (Packet Decoding)** 旁边的 **编辑** ()。

步骤 7 启用或禁用数据包解码器选项，第 18 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，请启用数据包解码器规则 (GID 116)。有关详细信息，请参阅设置入侵规则状态和数据包解码器选项，第 18 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

层基础知识
冲突和更改：网络分析和入侵策略

TCP 数据流预处理

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。

TCP 协议定义连接可以处于的各种状态。每个 TCP 连接通过源 IP 地址和目标 IP 地址以及源端口和目标端口进行识别。TCP 一次仅允许存在一个具有相同连接参数值的连接。

状态相关的 TCP 漏洞

如果向入侵规则添加带有 `established` 参数的 `flow` 关键字，则入侵规则引擎会在有状态模式下检查与规则和流指令匹配的数据包。状态模式仅评估通过客户端与服务器之间的合法三次握手建立的TCP会话所包含的流量。

您可以配置系统，以便预处理器对无法识别为已建立的 TCP 会话的一部分的任何 TCP 流量进行检测；但是，对于典型使用不建议此操作，因为事件会使系统迅速过载且不会提供有意义的数据。

stick 和 snot 之类的攻击针对自身使用系统的广泛规则集和数据包检测。这些工具根据基于 Snort 的入侵规则生成数据包，并通过网络发送这些数据包。如果您的规则不包括用于为状态检测配置规则的 `flow` 或 `flowbits` 关键字，则每个数据包将触发规则，进而导致系统过载。您可以通过状态检测来忽略这些数据包，因为它们不是已建立的TCP会话的一部分，而且不提供有意义的信息。执行状态检测时，规则引擎仅检测属于已建立的TCP会话的一部分的那些攻击，从而使分析人员关注这些攻击而不是由 stick 或 snot 攻击导致的事件量。

基于目标的 TCP 策略

不同操作系统以不同方法实施TCP。例如，Windows和其他一些操作系统需要TCP重置段以具有精确的 TCP 序列号来重置会话，而 Linux 和其他操作系统则允许使用一系列序列号。在本示例中，数据流预处理器必须明确了解目标主机会如何根据序列号对重置作出响应。仅当目标主机认为重置有效时，数据流预处理器才会停止跟踪会话，因此，攻击在预处理器停止检查数据流后无法通过发送数据包来躲避检测。在TCP实施中的其他变化包括操作系统是否采用TCP时间戳选项，并且在采用时如何处理时时间戳，以及操作系统接受还是忽略 SYN 数据包中的数据等等方面。

不同操作系统也以不同方式重组重叠的 TCP 数据段。重叠的 TCP 数据段可能会反映未确认的 TCP 流量的正常重传。它们也可能表示攻击者（了解其中一个主机的操作系统）尝试通过发送隐藏在重叠数据段中的恶意内容来躲避检测并利用该主机。但是，您可以将数据流预处理器配置为可感知受监控网段上运行的操作系统，使其以与目标主机相同的方式重组数据段，从而识别攻击。

您可以创建一个或多个 TCP 策略，以根据受监控网段上的不同操作系统定制 TCP 数据流检查和重组。对于每个策略，可识别 13 个操作系统策略之一。您根据需要使用尽可能多的 TCP 策略将每个 TCP 策略绑定到特定 IP 地址或地址块，以识别使用其他操作系统的任意或所有主机。默认 TCP 策略适用于在任何其他TCP策略中未识别的受监控网络上的任何主机，因此无需为默认TCP策略指定 IP 地址或地址块。

请注意，您也可以在被动部署中使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 TCP 流预处理器动态选择基于目标的策略。

TCP 数据流重组

数据流预处理器收集和重组属于TCP会话的服务器到客户端通信数据流和/或客户端到服务器通信数据流的一部分的所有数据包。这允许规则引擎将数据流作为单个已重组实体进行检查，而不是仅检查属于指定数据流的一部分的个别数据包。

数据流重组允许规则引擎识别基于数据流的攻击，在检查个别数据包时它可能无法检测此类攻击。您可以根据网络需要指定规则引擎重组哪些通信数据流。例如，在监控网络服务器上的流量时，您可能只希望检查客户端流量，因为您不太可能从自己的网络服务器接收到恶意流量。

在每个 TCP 策略中，您可以指定用于识别要重组的数据流预处理器流量的端口的逗号分隔列表。启用自适应配置文件后，您还可以列出用于识别要重组的流量的服务（以替代端口或端口组合的形式）。

您可以指定端口和/或服务。您可以为客户端端口和/或服务器端口的任意组合指定单独的端口列表。您还可以为客户端服务和/或服务器服务指定单独的服务列表。例如，假设您要重组以下内容：

- 来自客户端的 SMTP（端口 25）流量
- FTP 服务器响应（端口 21）
- 两个方向的 telnet（端口 23）流量

您可以配置以下内容：

- 对于客户端端口，指定 `23 和 25`
- 对于服务器端口，指定 `21 和 23`

或者，您可以配置以下内容：

- 对于客户端端口，指定 `25`
- 对于服务器端口，指定 `21`
- 对于客户端端口和服务器端口，指定 `23`

此外，请参考以下示例，该示例将端口和服务进行组合，并在启用自适应配置文件后有效：

- 对于客户端端口，指定 `23`
- 对于客户端服务，指定 `smtp`
- 对于服务器端口，指定 `21`
- 对于服务器服务，指定 `telnet`

取消一个端口（例如，`!80`）可通过阻止 TCP 数据流预处理器处理该端口的流量来提升性能。

虽然您也可以指定 `all` 作为参数来为所有端口提供重组，但是思科不建议将端口设置为 `all`，因为这样做可能会不必要地增加此预处理器检查的流量并降低性能。

TCP 重组自动透明地包括添加到其他预处理器的端口。但是，如果明确向已添加到其他预处理器配置的 TCP 重组列表中添加端口，则会正常处理这些附加端口。这包括下列预处理器的端口列表：

- FTP/Telnet（服务器级 FTP）
- DCE/RPC
- HTTP 检查
- SMTP
- 会话发起协议
- POP
- IMAP
- SSL

请注意，重组其他流量类型（客户端和/或服务器）会增加资源需求。

TCP 数据流预处理选项

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。

可以配置以下全局 TCP 选项：

数据包类型性能提高

支持忽略已启用规则中未指定的所有端口和应用协议的 TCP 流量，但在源端口和目标端口均设置为 `any` 的 TCP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

可为每个 TCP 策略配置以下选项：

网络

指定要对其应用 TCP 数据流重组策略的主机 IP 地址。

可以指定单个 IP 地址或地址块。总共最多可以指定 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

识别一个或多个目标主机的 TCP 策略操作系统。如果选择除 **Mac OS** 以外的其他策略，则系统会从同步 (SYN) 数据包中删除数据并禁用规则 129:2 的事件生成。请注意，启用内联规范化预处理器的 **SYN 时删除数据 (Remove Data on SYN)** 选项也会禁用规则 129:2。

下表列出了操作系统策略以及使用每个策略的主机操作系统。

表 *2: TCP* 操作系统策略

策略	操作系统
首先	未知的操作系统
最后	思科 IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 内核 Linux 2.6 内核
旧 Linux	Linux 2.2 及更低版本的内核
Windows	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 及更高版本
HPUX 10	HP-UX 10.2 及更高版本
Mac OS	Mac OS 10 (Mac OS X)

提示 当您不知道主机操作系统时，第一个操作系统策略可以提供一些保护。但是，它可能会导致未能检测出某些攻击。如果您知道操作系统，则应该编辑策略以指定正确的操作系统。

Timeout

规则引擎在状态表中保持数据流处于非活动状态的秒数（介于 1 和 86400 之间）。如果数据流在指定时间内未重组，则入侵规则引擎会将其从状态表中删除。

注释 如果托管设备部署在网络流量可能达到设备的带宽限制的网段上，则应该考虑将该值设置为较高的值（例如 600 秒），以降低处理开销。

威胁防御 设备会忽略此选项，而是使用高级访问控制**威胁防御服务策略**中的设置。有关详细信息，请参阅配置服务策略规则。

最大 TCP 窗口 (Maximum TCP Window)

指定由接收主机指定的所允许的最大 TCP 窗口大小（1 至 1073725440 字节）。值设置为 0 会禁用检查 TCP 窗口大小。

注意 上限是 RFC 允许的最大窗口大小，旨在防止攻击者躲避检测；但是，设置明显过大的最大窗口大小可能导致自愿接受的拒绝服务。

状态检查异常处于启用状态时，可以启用规则 129:6 为此选项生成事件并在内联部署中丢弃攻击性数据包。

重叠限制 (Overlap Limit)

指定在检测到某会话中存在所配置数量（介于 0 [无限制] 和 255 之间）的重叠分片时，针对该会话的分片重组将会停止，并且，如果**状态检查异常 (Stateful Inspection Anomalies)** 以及随附的预处理器规则均处于启用状态，将会生成事件。

您可以启用规则 129:7 来为此选项生成事件并在内联部署中丢弃攻击性数据包。

刷新因数 (Flush Factor)

在内联部署中，指定在经过所配置数量（介于 1 和 2048 之间）的大小未减小的分段后检测到大小减小的分段时，系统会刷新为进行检测而累积的分段数据。值设置为 0 会禁用此分段模式的检测（这可能意味着请求或响应结束）。请注意，必须启用 Inline Normalization **Normalize TCP Payload** 选项才会使此选项生效。

状态检查异常 (Stateful Inspection Anomalies)

检测 TCP 堆栈中的异常行为。启用随附的预处理器规则后，如果 TCP/IP 堆栈编写得不好，可能会生成许多事件。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以通过启用以下规则来为此选项生成事件并在内联部署中丢弃攻击性数据包：

- 129:1 至 129:5
- 129:6（仅适用于 Mac OS）
- 129:8 至 129:11

- 129:13 至 129:19

请注意以下提示：

- 为了触发规则 129:6，还必须为**最大 TCP 窗口**配置一个大于 0 的值。
- 为了触发规则 129:9 和 129:10，还必须启用 **TCP 会话劫持**。

TCP 会话劫持 (TCP Session Hijacking)

通过针对会话上接收到的后续数据包验证三次握手期间从 TCP 连接两端检测到的硬件 (MAC) 地址来检测 TCP 会话劫持。当一端或另一端的 MAC 地址不匹配时，如果启用了**状态检查异常 (Stateful Inspection Anomalies)** 以及两个对应的预处理器规则之一，系统会生成事件。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以启用规则 129:9 和 129:10 来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，为了让这些规则中任一个生成事件，还必须启用**状态检查异常 (Stateful Inspection Anomalies)**。

连续小分片 (Consecutive Small Segments)

状态检查异常 (Stateful Inspection Anomalies) 处于启用状态时，可指定允许的连续 TCP 小分片的最大数量（1 至 2048）。值设置为 0 会禁止连续小分片。

此选项必须与**小分片大小 (Small Segment Size)** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，在无干预确认的情况下接收多达2000个连续分段，即使每个分段长度为 1 字节，分段数量也会远远超出您通常的预期。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以启用规则 129:12 来为此选项生成事件并在内联部署中丢弃攻击性数据包。

小分片大小 (Small Segment Size)

状态检查异常 (Stateful Inspection Anomalies) 处于启用状态时，可指定被视为小分片的 TCP 分片大小（1 至 2048 字节）。值设置为 0 会禁止指定小分片的大小。

对于 威胁防御 路由和透明接口，此选项会被忽略。

此选项必须与**连续小分片 (Consecutive Small Segments)** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，一个 2048 字节的 TCP 分段大于普通的 1500 字节的以太网帧。

忽略小分片的端口 (Ports Ignoring Small Segments)

状态检查异常 (Stateful Inspection Anomalies)、**连续小分片 (Consecutive Small Segments)** 和**小分片大小 (Small Segment Size)** 处于启用状态时，可指定一个或多个会忽略小 TCP 分片检测的端口的逗号分隔列表。将此选项留空表示未忽略任何端口。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以向列表中添加任何端口，但是列表仅影响 TCP 策略中的某个**对端口执行数据流重组 (Perform Stream Reassembly on port)** 列表中指定的端口。

需要 TCP 三次握手 (Require TCP 3-Way Handshake)

指定仅在 TCP 三次握手完成时，会话才被视为已建立的会话。禁用此选项可提高性能，防御 SYN 泛洪攻击，并允许在部分异步环境中操作。启用此选项可避免尝试通过发送不属于已建立的 TCP 会话的信息来生成误报的攻击。

您可以启用规则 129:20 来为此选项生成事件并在内联部署中丢弃攻击性数据包。

三次握手超时 (3-Way Handshake Timeout)

指定启用**需要 TCP 三次握手 (Require TCP 3-Way Handshake)** 后必须允许用于完成握手的时间（0 [无限制] 至 86400 秒 [24 小时]）。必须启用**需要 TCP 三次握手 (Require TCP 3-Way Handshake)** 后才能修改此选项的值。

对于 Firepower 软件设备和 威胁防御 内联、内联分流和被动接口，默认值为 0。对于 威胁防御 路由和透明接口，超时始终为 30 秒；此处配置的值会被忽略。

数据包大小性能提升 (Packet Size Performance Boost)

将预处理器设置为在重组缓冲区中不对大数据包进行排队。这种性能改进可能会导致未能检测出某些攻击。禁用此选项可防止使用 1 到 20 字节的小数据包尝试躲避检测。当您肯定所有流量都由超大数据包组成并因此无此类攻击时，可启用此选项。

旧版重组 (Legacy Reassembly)

重组数据包时，将数据流预处理器设置为模拟废弃的数据流 4 预处理器，借此可以将该数据流预处理器重组的事件与基于数据流 4 预处理器重组的相同数据流的事件相比较。

异步网络 (Asynchronous Network)

指定受监控网络是否为异步网络，即，系统只能看到一半流量的网络。启用此选项后，系统不重组 TCP 数据流来提高性能。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对客户端端口执行数据流重组 (Perform Stream Reassembly on Client Ports)

根据连接的客户端的端口启用数据流重组。换句话说，它对目标为网络服务器、邮件服务器或通常由 $HOME_NET 中指定的 IP 地址定义的其他 IP 地址的数据流进行重组。如果您预计客户端会发出恶意流量，请使用此选项。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对客户端服务执行数据流重组 (Perform Stream Reassembly on Client Services)

根据连接的客户端的服务启用数据流重组。如果您预计客户端会发出恶意流量，请使用此选项。

必须为选择的每个客户端服务至少启用一个客户端检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为相关客户端应用启用检测器，则系统会自动为应用启用思科提供的所有检测器；如果不存在任何检测器，则系统会为应用启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对服务器端口执行数据流重组 (Perform Stream Reassembly on Server Ports)

根据连接的服务器端的端口启用数据流重组。换句话说，它对从网络服务器、邮件服务器或通常由 $EXTERNAL_NET 中指定的 IP 地址定义的其他 IP 地址发出的数据流进行重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定端口来禁用此选项。

对于 威胁防御 路由和透明接口，此选项会被忽略。

注释 对于服务的全面检查，除了在对服务器端口执行数据流重组字段中添加端口号以外，还要在对服务器服务执行数据流重组字段中添加服务名称。例如，除了在对服务器端口执行数据流重组字段中添加端口号 80 以外，还要在对服务器服务执行数据流重组字段中添加“**HTTP**”服务，以检查 HTTP 服务。

对服务器服务执行数据流重组 (Perform Stream Reassembly on Server Services)

根据连接的服务器端的服务启用数据流重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定服务来禁用此选项。

必须至少启用一个检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为服务启用检测器，则系统会自动为相关应用协议启用思科提供的所有检测器；如果不存在任何检测器，则系统会为该应用协议启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对客户端端口和服务器端口执行数据流重组 (Perform Stream Reassembly on Both Ports)

根据连接的客户端和服务器端的端口启用数据流重组。如果您预计相同端口的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。您可以通过不指定端口来禁用此选项。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对客户端服务和服务器服务执行数据流重组 (Perform Stream Reassembly on Both Services)

根据连接的客户端和服务器端的服务启用数据流重组。如果您预计相同服务的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。您可以通过不指定服务来禁用此选项。

必须至少启用一个检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为相关客户端应用或应用协议启用检测器，则系统会自动为应用或应用协议启用思科提供的所有检测器；如果不存在任何检测器，则系统会为应用或应用协议启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

对于 威胁防御 路由和透明接口，此选项会被忽略。

故障排除选项：最大排队字节数 (Troubleshooting Options: Maximum Queued Bytes)

支持人员可能会在故障排除呼叫期间要求您指定可以在 TCP 连接的一端排队的数据量。值 0 表示无限字节数。

注意 更改此故障排除选项的设置会影响性能，应仅在支持人员的指导下进行操作。

故障排除选项：最大排队分片数 (Troubleshooting Options: Maximum Queued Segments)

支持人员可能会在故障排除呼叫期间要求您指定可以在 TCP 连接的一端排队的数据段的最大字节数。值 0 表示无限的数据段字节数。

注意 更改此故障排除选项的设置会影响性能，应仅在支持人员的指导下进行操作。

相关主题

激活和停用检测器
层管理
冲突和更改：网络分析和入侵策略

配置 TCP 数据流预处理

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 点击要修改的策略旁边的 **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 **传输/网络层预处理器**下的 **TCP 数据流配置** 设置已禁用，请通过点击 **已启用**进行启用。

步骤 6 点击 **TCP 数据流配置 (TCP Stream Configuration)** 旁边的 **编辑** ( )。

步骤 7 选中或清除**全局设置 (Global Settings)** 部分中的**数据包类型性能提升 (Packet Type Performance Boost)** 复选框。

步骤 8 您可以执行以下操作：

- 添加基于目标的策略 - 点击“目标”(Targets) 部分中的**主机 (Hosts)** 旁边的 **添加** ( )。在**主机地址 (Host Address)** 字段中指定一个或多个 IP 地址。可以指定单个 IP 地址或地址块。可以创建总共 255 个基于目标的策略（包括默认策略）。完成后，点击**确定 (OK)**。
- 编辑基于目标的现有策略 - 在**主机 (Hosts)** 下，点击要编辑的策略的地址，或点击默认值以在**默认值 (default)** 中编辑默认配置值。
- 修改 TCP 数据流预处理选项 - 请参阅 TCP 数据流预处理选项，第 25 页。

  注意
  请勿修改**最大排队字节数 (Maximum Queued Bytes)** 或**最大排队分片数 (Maximum Queued Segments)**，除非支持人员指示执行此操作。

  提示
  要根据客户端服务和/或服务器服务修改数据流重组设置，请在要修改的字段内点击，或者点击要修改的字段旁边的**编辑 (Edit)**。使用箭头在弹出窗口中的**可用 (Available)** 和**已启用 (Enabled)** 列表之间移动服务，然后点击**确定 (OK)**。

- 删除基于目标的现有策略 - 点击要删除的策略旁边的 **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

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 TCP 流预处理器规则 (GID 129)。有关详细信息，请参阅设置入侵规则状态和TCP 数据流预处理选项，第 25 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

层管理
冲突和更改：网络分析和入侵策略

UDP 数据流预处理

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。

当规则引擎使用以下任何参数根据包含 `flow` 关键字的 UDP 规则处理数据包时，会发生 UDP 数据流预处理：

- 已建立
- 至客户端
- 自客户端
- 至服务器
- 自服务器

在会话方面通常未考虑 UDP 数据流。UDP 是一个无连接协议，并不提供在两个终端之间建立通信信道、交换数据和关闭该信道的方法。但是，数据流预处理器使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别会话。当超过可配置的计时器时，或者当任一终端收到表明另一个终端不可达或所请求的服务不可用的 ICMP 消息时，会话将会结束。

请注意，系统不生成与 UDP 数据流预处理相关的事件；但是，您可以启用相关数据包解码器规则来检测 UDP 协议报头异常。

相关主题

TCP 报头值和数据流大小

UDP 数据流预处理选项

超时

指定预处理器在状态表中保持非活动数据流的秒数。如果在指定时间内看不到其他数据报，预处理器会从状态表中删除数据流。

威胁防御 设备会忽略此选项，而是使用高级访问控制**威胁防御服务策略**中的设置。有关详细信息，请参阅配置服务策略规则。

数据包类型性能提高

将预处理器设为忽略已启用规则中未指定的所有端口和应用协议的 UDP 流量，但在源端口和目标端口均设置为 `any` 的 UDP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

相关主题

TCP 报头值和数据流大小

配置 UDP 数据流预处理

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**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的 **UDP 数据流配置 (UDP Stream Configuration)** 已禁用，请点击**启用 (Enabled)**。

步骤 6 点击 **UDP 数据流配置 (UDP Stream Configuration)** 旁边的 **编辑** (✎)。

步骤 7 设置选项，如UDP 数据流预处理选项，第 33 页中所述。

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，请启用相关数据包解码器规则 (GID 116)。有关详细信息，请参阅设置入侵规则状态和数据包解码器，第 18 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

层管理

冲突和更改：网络分析和入侵策略

TCP 报头值和数据流大小

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。