预过滤和预过滤策略

- 关于预过滤， 第 1 页
- 快速路径预过滤的最佳实践， 第 5 页
- 封装流量处理的最佳实践 ， 第 6 页
- 预过滤器策略的要求和必备条件， 第 7 页
- 配置预过滤， 第 7 页
- 隧道区域与预过滤， 第 13 页
- 将预过滤器规则移至访问控制策略， 第 16 页
- 预过滤器策略命中计数， 第 18 页
- 大型流量分流， 第 18 页

关于预过滤

在系统执行更多资源密集型评估之前，预过滤是访问控制的第一阶段。预过滤非常简单、快速并且可以及早执行。预过滤使用有限的外部报头条件来快速处理流量。将此过滤操作与后续评估进行比较，后续评估使用内部报头并具有更强大的检测功能。

配置预过滤：

- 提高性能 - 越早排除不需要检查的流量，越好。您可以基于隧道的外部封装报头传递隧道为某些类型的明文设置快速路径或加以阻止，而不检查其封装的连接。您还可以为从及早处理中受益的其他任何连接设置快速路径或加以阻止。
- 为封装流量定制深度检查 - 您可以对某些类型的隧道重新分区，以便以后可以使用相同的检查标准处理其封装的连接。重新分区是必要的，因为在预过滤后，访问控制使用内部报头。

关于预过滤策略

预过滤是一种基于策略的功能。要将它分配给设备，请将其分配给分配给该设备的访问控制策略。

策略要素：规则和默认操作

在预过滤策略中，隧道规则、预过滤规则和默认操作处理网络流量：

- 隧道和预过滤规则 - 首先，预过滤策略中的规则按您指定的顺序处理流量。隧道规则只与特定隧道匹配，并支持重新分区。预过滤规则的约束范围更广，不支持重新分区。有关详细信息，请参阅隧道与预过滤器规则，第 2 页。
- 默认操作（仅限隧道）- 如果隧道不与任何规则匹配，则对隧道应用默认操作。默认操作可以阻止这些隧道，或继续对其单独封装的连接进行访问控制。不能使用默认操作对隧道重新分区。

  没有用于未封装流量的默认操作。如果未封装的连接与任何预过滤规则都不匹配，系统将继续进行访问控制。

连接日志记录

您可以记录被预过滤策略使用快速路径或阻止的连接。

连接事件包含有关记录的连接（包括整个隧道）是否被预过滤以及如何预过滤的信息。您可以在事件视图（工作流）、仪表板和报表中查看此信息，并将其用作关联标准。注意，由于被快速路径和阻止的连接不进行深度检查，因此关联的连接事件包含的信息有限。

默认预过滤策略

每个访问控制策略都有一个关联的预过滤策略。

如果不配置自定义预过滤，系统将使用默认策略。最初，此系统提供的策略将所有流量传递到访问控制的下一阶段。您可以更改策略的默认操作并配置其日志记录选项，但不能向其添加规则或将其删除。

预过滤策略继承和多租户

访问控制使用基于分层的实施，完善了多租户策略。除了其他高级设置之外，您还可以锁定预过滤策略关联，在所有子代访问控制策略中实施该关联。有关详细信息，请参阅访问控制策略继承。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。默认的预过滤策略属于全局域。

隧道与预过滤器规则

配置隧道规则还是预过滤器规则取决于要匹配的特定流量类型和要执行的操作或进一步分析。

特征	隧道规则	预过滤器规则
主要功能	对明文传递隧道快速使用快速路径、加以阻止或重新分区。	对从早期处理中受益的其他任何连接快速使用快速路径或加以阻止。
封装和端口/协议标准	封装条件只与所选协议上的明文隧道匹配，请参阅封装规则条件，第 13 页。	与隧道规则相比，端口规则可以使用范围更广泛的端口和协议限制；请参阅端口、协议和 ICMP 代码规则条件。
网络标准	隧道终端条件限制要处理的隧道的终端；请参阅网络规则条件。	网络条件限制每个连接中的源主机和目标主机；请参阅网络规则条件。

特征	隧道规则	预过滤器规则
方向	双向或单向（可配置）。 默认情况下，隧道规则是双向的，这样便于它们处理隧道终端之间的所有流量。	仅单向（不可配置）。 预处理器规则只与源到目标流量匹配。
对会话进行重新分区以便进一步分析	支持，使用隧道区域；请参阅隧道区域与预过滤，第 13 页。	不支持。

预过滤与访问控制

预过滤和访问控制策略都允许您阻止和信任流量，但预过滤“信任”功能被称为“快速路径”，因为它会跳过更多检查。下表说明了这一点以及预过滤与访问控制之间的其他差异，以帮助您决定是否配置自定义预过滤。

如果不配置自定义预过滤，则只能在访问控制策略中使用早期放置的“阻止”和“信任”规则来接近而非复制预过滤功能。

特征	预过滤	访问控制	有关详细信息，请参阅.....
主要功能	对特定类型的明文、直通隧道快速使用快速路径或加以阻止（请参阅封装规则条件，第 13 页），或针对其封装的流量定制后续检查。 对从早期处理中受益的其他任何连接使用快速路径或加以阻止。	使用简单或复杂的条件检查和控制所有网络流量，包括情景信息和深度检查结果。	关于预过滤，第 1 页
实施	预过滤策略。 预过滤策略由访问控制策略调用。	访问控制策略。 访问控制策略是主配置。除了调用子策略，访问控制策略还具有自己的规则。	关于预过滤策略，第 1 页 将其他策略与访问控制相关联
访问控制中的序列	首先。 在所有其他访问控制配置之前，系统会将流量与预过滤条件匹配。	-	-
规则操作	更少。 您可以停止进一步检查（快速路径和阻止），或对其余访问控制允许进一步分析（分析）。	更多。 访问控制规则有更广泛的操作，包括监控、深度检查、阻止并重置和交互式阻止。	隧道和预过滤器规则组成部分，第 8 页 访问控制规则操作

特征	预过滤	访问控制	有关详细信息，请参阅.....
绕过功能	快速路径规则操作。 在预过滤阶段为流量使用快速路径可绕过所有进一步检查和处理，包括： • 安全情报 • 身份策略强加的身份验证要求 • SSL 解密 • 访问控制规则 • 对数据包负载的深度检验 • 能源成本 • 速率限制	信任规则操作。 访问控制规则信任的流量仅免于深度检查和发现。	访问控制规则简介
规则条件	限制版。 预过滤策略中的规则使用简单网络条件：IP 地址、VLAN 标记、端口和协议。 对于隧道，隧道终端条件会指定隧道任一端上网络设备的路由接口的 IP 地址。	强健。 访问控制规则使用网络条件，但同时也采用用户、应用、请求的 URL 和数据包负载中可用的其他情景信息。 网络条件指定源和目标主机的 IP 地址。	隧道与预过滤器规则，第 2 页 预过滤器规则条件，第 10 页 隧道规则条件，第 12 页
使用的 IP 报头（隧道处理）	最外层。 使用外部报头使您可以处理整个明文、直通隧道。 对于未封闭的流量，预过滤仍使用“外部”标头 - 在这种情况下，它们是唯一报头。	尽可能在内部。 对于未加密隧道，访问控制作用于其各个封装的连接，而不是作用于整个隧道。	传递隧道和访问控制，第 5 页
对封装的连接重新分区以进行进一步分析	重新分区隧道传输的流量。 隧道区域允许您对预过滤的封装流量定制后续检查。	使用隧道区域。 访问控制使用在预过滤期间分配的隧道区域。	隧道区域与预过滤，第 13 页
连接日志记录	仅使用快速路径和阻止的流量。允许的连接仍然可由其他配置进行记录。	任何连接。	
支持的设备	仅限 Cisco Secure Firewall Threat Defense。	All.	—

传递隧道和访问控制

明文（非加密）隧道可以封装多个连接，通常在非连续网络之间流动。这些隧道对通过 IP 网络的路由自定义协议、通过 Ipv4 网络的 IPv6 流量等尤其有用。

外部封装报头指定隧道终端（隧道任一端的网络设备的路由接口）的源 IP 地址和目标 IP 地址。内部负载报头指定封装连接的实际终端的源 IP 地址和目标 IP 地址。

通常，网络安全设备将明文隧道处理为传递流量。也就是说，设备不是隧道终端之一。该设备部署在隧道终端之间，用于监控终端之间流动的流量。

某些网络安全设备（例如运行思科 ASA 软件[而不是 Cisco Secure Firewall Threat Defense]的思科 ASA 防火墙）可使用外部 IP 报头实施安全策略。即使对于明文隧道，这些设备也不能控制或洞察各个封装连接及其负载。

相比之下，Firepower 系统可利用访问控制进行以下操作：

- 外部报头评估 - 首先，预过滤使用外部报头处理流量。可以对此阶段的整个明文、传递隧道进行阻止或使用快速路径。
- 内部报头评估 - 然后，其余访问控制（和 QoS 等其他功能）使用报头最深处可检测的级别确保实现最精细的检测和处理。

  如果传递隧道未加密，则系统会在此阶段对它的各个封装连接执行操作。您必须对隧道进行重新分区（请参阅隧道区域与预过滤，第 13 页）以对其所有封装连接执行操作。

访问控制无法洞察已加密的传递隧道。例如，访问控制规则会将一个传递 VPN 隧道看做一个连接。系统仅使用其外部封装报头中的信息处理整个隧道。

快速路径预过滤的最佳实践

在预过滤器规则中使用快速路径操作时，匹配的流量会绕过检查并直接通过设备进行传输。请对您可以信任但不会受益于任何可用安全功能的流量使用此操作。

以下类型的流量是快速路径的理想选择。例如，您可以将规则配置为对来自或到达终端或服务器的 IP 地址的任何流量进行快速路径处理。您可以根据使用的端口来进一步限制规则。

- 通过设备的站点间 VPN 流量。也就是说，该设备不是 VPN 拓扑中的终端。
- 扫描程序流量。扫描程序探测可以从入侵策略中创建大量误报响应。
- 语音/视频。
- 备份。
- 流经 威胁防御 设备的管理流量。对管理流量执行深度检查（使用访问控制策略）可能会导致问题。

封装流量处理的最佳实践

本主题讨论以下类型的封装流量的准则：

- 通用路由封装 (GRE)
- 点对点协议 (PPTP)
- IPinIP
- IPv6inIP
- Teredo

了解托管设备的 Snort 版本支持

托管设备使用的检测引擎被称为 Snort。Snort 3 支持的功能比 Snort 2 多。要了解这些因素如何影响网络上的托管设备，您必须了解：

- 您的设备支持哪些版本的 Snort。

  Snort 版本支持可以在《思科 *Firepower*兼容性指南》中关于捆绑组件的部分找到。

- 管理中心 和 威胁防御 软件如何支持 Snort 2 和 Snort 3

  有关 Snort 2 和 Snort 3 的限制，请参阅《Cisco Secure Firewall Management Center Snort 3 配置指南》中的适用于 管理中心 管理的 威胁防御 的 *Snort 3* 的功能限制主题。

GRE v1 和 PPTP 会绕过外部流处理

GRE v1（有时称为状态性 *GRE*）和 PPTP 流量会绕过外部流处理。

IPv6inIP 和 Teredo 支持客流处理，但存在以下限制：

- 会话位于未进行负载均衡的单个隧道上
- 没有 HA 或集群复制
- 不维护主要和辅助流关系
- 不支持预过滤策略白名单和黑名单

GRE v0 序列号字段必须为可选

在网络上发送流量的所有终端都必须发送带有可选序列号字段的GREv0流量；否则，序列号字段会被删除。RFC 1701 和 RFC 2784 都将序列字段指定为可选。

隧道如何与接口配合使用

预过滤器和访问控制策略规则适用于路由、透明、内联集、内联分流和被动接口上的所有隧道类型。

参考资料

有关 GRE 和 PPTP 协议的详细信息，请参阅以下内容：

- RFC 1701、RFC 2784 和 RFC 2890（GRE 协议 v0）
- RFC 2637（PPTP 和 GRE 协议 v1）

预过滤器策略的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置预过滤

要执行自定义预过滤，请配置预过滤策略并将策略分配给访问控制策略。预过滤器策略是通过访问控制策略分配给受管设备的。

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

过程

步骤 1 选择**策略** > **访问控制** > **预过滤器**。

步骤 2 点击**新建策略 (New Policy)** 以创建自定义预过滤器策略。

新的预过滤器策略不包含规则及“分析所有隧道流量”(Analyze all tunnel traffic) 这一默认操作。它不执行日志记录或隧道重新分区。您也可以 **复制**（ ） 或 **编辑**（ ） 现有策略。

步骤 3 配置预过滤器策略的默认操作及其日志记录选项。

- 默认操作 - 为受支持的明文、传递隧道选择默认操作：**分析所有隧道流量 (Analyze all tunnel traffic)**（具有访问控制）或**阻止所有隧道流量 (Block all tunnel traffic)**。
- 默认操作日志记录 - 点击默认操作旁边的 **日志记录**（ ）。您只能为被阻止的隧道配置默认操作日志记录。

步骤 4 配置隧道规则和预过滤器规则。

在自定义预过滤器策略中，可以按任意顺序使用这两种规则。根据要匹配的具体流量类型和要执行的操作或进一步分析创建规则；请参阅隧道与预过滤器规则，第 2 页。

注意　使用隧道规则分配隧道区域时应格外小心。在之后进行评估时，重新分区后的隧道中的连接可能与安全区域限制不匹配。有关详细信息，请参阅隧道区域与预过滤，第 13 页。

有关配置规则组成部分的详细信息，请参阅 隧道和预过滤器规则组成部分，第 8 页。

步骤 5 评估规则顺序。要移动规则，请点击并拖动，或使用右键点击菜单进行剪切并粘贴。

正确创建规则并将其排序是一项复杂的任务，但却是构建有效部署的一项重要任务。如果您未缜密地计划，有些规则可能会抢占其他规则，或者包含无效的配置。有关详细信息，请参阅访问控制规则的最佳实践。

步骤 6 保存预过滤器策略。

步骤 7 对于支持隧道区域限制的配置，请适当处理重新分区后的隧道。

通过将隧道区域用作源区域限制来匹配重新分区后的隧道中的连接。

步骤 8 关联预过滤器策略与部署到受管设备的访问控制策略。

请参阅将其他策略与访问控制相关联。

步骤 9 部署配置更改。

注释　部署预过滤器策略时，其规则不会应用于现有隧道会话。因此，现有连接上的流量不受部署的新策略的限制。此外，仅对匹配策略的连接的第一个数据包增加策略命中计数。因此，从命中计数中忽略了可能与策略匹配的现有连接上的流量。要有效应用策略规则，请清除现有隧道会话，然后部署策略。

下一步做什么

如果要部署基于时间的规则，请指定策略分配到的设备的时区。请参阅为策略应用配置设备时区。

隧道和预过滤器规则组成部分

状态（启用/禁用）

默认情况下，规则处于启用状态。如果禁用某规则，系统将不使用该规则并停止为该规则生成警告和错误。

位

规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则，无论规则是何类型（隧道与预过滤器）。

操作

规则操作确定系统如何处理和记录匹配的流量。

- 快速路径 - 让匹配流量免于进行所有进一步检查和控制，包括访问控制、身份要求和速率限制。对隧道执行快速路径操作可为所有封装连接提供快速路径。
- 阻止 - 阻止匹配流量，不进行任何类型的进一步检查。阻止隧道将阻止所有封装连接。
- 分析 - 允许其余访问控制继续使用内部报头分析流量。即使流量被访问控制和所有相关深度检查放行，也可能会受到速率限制。对于隧道规则，使用“分配隧道区域”(Assign Tunnel Zone) 选项启用重新分区。

方向（仅限隧道规则）

隧道规则的方向用于确定系统源和目标条件：

- 仅从源匹配隧道（单向）- 仅匹配源到目标的流量。匹配流量必须源自其中一个指定的源接口或隧道终端，并通过其中一个目标接口或隧道终端流出。
- 从源和目标匹配隧道（双向）- 同时匹配源到目标的流量和目标到源的流量。其效果与编写两个互为镜像的单向规则相同。

预过滤器规则始终是单向的。

分配隧道区域（仅限隧道规则）

在隧道规则中，分配隧道区域（无论是现有的还是即时创建的）会对匹配隧道进行重新分区。重新分区需要“分析”(Analyze) 操作。

对隧道进行重新分区允许其他配置（例如访问控制策略）识别隧道中所有互相归属的封装连接。通过将隧道的已分配隧道区域用作接口限制，可以针对其封装连接定制检查。有关详细信息，请参阅隧道区域与预过滤，第 13 页。

注意 分配隧道区域时应格外小心。在之后进行评估时，重新分区后的隧道中的连接可能与安全区域限制不匹配。请参阅使用隧道区域，第 14 页，查看隧道区域实施的简要步骤，以及对在不明确处理重新分区流量的情况下进行重新分区的影响的说明。

条件

条件指定规则处理的特定流量。流量必须匹配所有规则条件才能与规则匹配。每种条件类型在规则编辑器中都有自己的选项卡。

您可以使用以下 外部报头 限制预过滤流量。您必须按照封装协议限制隧道规则。

- 接口 -接口规则条件
- 网络（预过滤器规则）/隧道终端（隧道规则）-网络规则条件
- VLAN -VLAN 标记规则条件
- 端口（预过滤器规则）/封装和端口（隧道规则）-预过滤器规则的端口规则条件，第 12 页 或 封装规则条件，第 13 页
- 时间范围-时间和日期规则条件

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。

在隧道和预过滤器规则中，您可以记录快速路径流量和受阻流量（“快速路径”[Fastpath] 和“阻止”[Block] 操作）。对于需要接受进一步分析（“分析”[Analyze] 操作）的流量，预过滤器策略中的日志记录功能被禁用，但匹配连接可能仍然被其他配置记录下来。日志记录在内部流上执行，而不是在封装流上执行。

备注

每次保存对规则所做的更改时，都可以添加备注。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。

保存规则后，您无法编辑或删除相关备注。

相关主题

访问控制规则的最佳实践

预过滤器规则条件

通过规则条件，您可以微调预过滤器策略，以您要控制的网络为目标。有关详细信息，请参阅以下各节之一：

接口规则条件

接口规则条件按流量的源接口和目标接口控制流量。

根据规则类型和部署中的设备，您可以使用名为 安全区域 或 接口组 的预定义 接口对象 构建接口条件。接口对象对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量；请参阅接口。

提示 按接口限制规则是提高系统性能的一种最佳方式。如果规则排除了某个设备的所有接口，则该规则不影响该设备的性能。

正如接口对象中的所有接口都必须为同一类型（均为内联、被动、交换、路由或ASA FirePOWER），接口条件中使用的所有接口对象也必须为同一类型。由于被动部署的设备不会传输流量，因此无法在被动部署中按目标接口限制规则。

网络规则条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

预过滤器规则的端口规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以配置端口条件以匹配预过滤器规则中的其他协议，但在匹配 GRE、IP in IP、IPv6 in IP 和 Toredo 端口 3544 时，应改为使用隧道规则。

时间和日期规则条件

您可以指定连续时间范围或周期性时间段。

例如，规则只能在工作日工作时间或每个周末或节假关闭期间应用。

基于时间的规则基于处理流量的设备的本地时间应用。

基于时间的规则仅在 FTD 设备上受支持。如果将具有基于时间的规则的策略分配给不同类型的设备，则在该设备上会忽略与该规则关联的时间限制。在这种情况下，您将看到警告。

隧道规则条件

通过规则条件，您可以微调隧道策略，以您要控制的网络为目标。对于隧道规则，您可以使用以下条件：

- **接口对象 (Interface Objects)** - 定义连接所通过的设备接口的安全区域或接口组。请参阅接口规则条件。

- **隧道终端 (Tunnel Endpoints)** - 定义隧道的源和目标 IP 地址的网络对象。
- **VLAN 标记 (VLAN Tags)** - 隧道中最外层的 VLAN 标记。请参阅VLAN 标记规则条件。
- **封装和端口 (Encapsulation and Ports)** - 隧道的封装协议。请参阅封装规则条件，第 13 页。
- **时间范围 (Time Range)** - 规则处于活动状态的日期和时间。如果不指定时间范围，规则将始终处于活动状态。请参阅时间和日期规则条件。

封装规则条件

封装条件特定于隧道规则。

这些条件通过其封装协议控制某些类型的明文、传递隧道。必须先至少选择一个协议进行匹配，然后才能保存规则。您可以选择：

- GRE (47)
- IP-in-IP (4)
- IPv6-in-IP (41)
- Teredo (UDP (17)/3455)

隧道区域与预过滤

隧道区域允许您使用预过滤针对封装连接定制后续流量处理。

由于通常情况下，系统使用报头最深处可检测的级别处理流量，因此这需要用到特殊机制。这可确保尽可能进行最精细的检查。但同时这也意味着，如果传递隧道未加密，系统会对其各个封装连接执行操作；请参阅传递隧道和访问控制，第 5 页。

隧道区域可解决此问题。在访问控制的第一阶段（预过滤），您可以使用外部报头识别特定类型的明文传递隧道。然后，可通过分配自定义隧道区域对这些隧道进行重新分区。

对隧道进行重新分区允许其他配置（例如访问控制策略）识别隧道中所有互相归属的封装连接。通过将隧道的已分配隧道区域用作接口限制，可以针对其封装连接定制检查。

尽管名称相似，但隧道区域不是安全区域。隧道区域不代表一组接口。将隧道区域理解为在某些情况下替换与封装连接关联的安全区域的标记更为准确。

⚠

注意 对于支持隧道区域限制的配置，重新分区后的隧道中的连接与安全区域限制**不**匹配。例如，在对某个隧道进行重新分区后，访问控制规则可将其封装连接与这些连接新分配的隧道区域相匹配，而不与任何原始安全区域相匹配。

请参阅使用隧道区域，第 14 页，查看隧道区域实施的简要步骤，以及对在不明确处理重新分区流量的情况下进行重新分区的影响的说明。

支持隧道区域限制的配置

只有访问控制规则支持隧道区域限制。

其他配置均不支持隧道区域限制。例如，您不能使用 QoS 对整个明文隧道进行速率限制，而只能对其单独的封装会话进行速率限制。

使用隧道区域

此操作步骤示例总结了如何对GRE隧道进行重新分区，以便使用隧道区域执行进一步分析。您可以将此示例中描述的概念加以调整并应用到需要根据明文、传递隧道中封装的连接定制流量检查的其他情景中。

设想一种情形，在该情形中，您组织的内部流量流过受信任的安全区域。受信任的安全区域表示部署在不同地方的多个受管设备上的一组接口。您组织的安全策略要求您在对漏洞和恶意软件进行深度检查后允许内部流量。

内部流量有时包含特定终端之间的明文、传递及 GRE 隧道。由于此封装流量的流量配置文件与您“正常”的局间活动（可能为已知且为良性）不同，因此您可以在遵守安全策略的前提下限制对某些封装连接的检查。

在本示例中，部署配置更改后：

- 在受信任区域中检测到的明文、传递和GRE封装隧道各自的封装连接由一组入侵和文件策略评估。
- 受信任区域中的所有其他流量则由另外一组不同的入侵和文件策略评估。

您可以通过对 GRE 隧道进行重新分区来完成这项任务。重新分区可以确保访问控制将 GRE 封装连接与自定义隧道区域（而非其原始的受信任安全区域）关联。鉴于访问控制对封装流量的处理方式，需要进行重新分区；请参阅 传递隧道和访问控制，第 5 页 和 隧道区域与预过滤，第 13 页。

过程

步骤 1 配置根据封装流量定制深度检查的自定义入侵和文件策略，以及专为非封装流量定制的另外一组入侵和文件策略。

步骤 2 配置自定义预过滤，以便对流过受信任安全区域的 GRE 隧道进行重新分区。

创建自定义预过滤器策略并将其与访问控制关联。在此自定义预过滤器策略中，创建隧道规则（在此示例中，隧道规则为 **GRE_tunnel_rezone**）和对应的隧道区域 (**GRE_tunnel**)。有关详细信息，请参阅配置预过滤，第 7 页。

表 *1: GRE_tunnel_rezone* 隧道规则

规则组件	说明
接口对象条件	通过将受信任的安全区域同时用作源接口对象和目标接口对象限制来匹配仅内部隧道。

规则组件	说明
隧道终端条件	为组织中使用的 GRE 隧道指定源终端和目标终端。 默认情况下，隧道规则是双向的。如果不更改**从...匹配隧道 (Match tunnels from...)** 选项，则您将哪些终端指定为源、哪些终端指定为目标都可以。
封装条件	匹配 GRE 流量。
分配隧道区域	创建 **GRE_tunnel** 隧道区域，并将其分配到与规则匹配的隧道。
操作	分析（借助其他访问控制）。

步骤 3 配置访问控制以处理重新分区后的隧道中的连接。

在部署到受管设备的访问控制策略中，配置用于处理重新分区后的流量的规则（在此示例中，规则为 **GRE_inspection**）。有关详细信息，请参阅创建和编辑访问控制规则。

表 *2: GRE_inspection* 访问控制规则

规则组件	说明
安全区域条件	通过将 GRE_tunnel 安全区域用作源区域限制来匹配重新分区后的隧道。
操作	允许（已启用深度检查） 选择专门用于检查封装内部流量的文件和入侵策略。

注意 如果您跳过此步骤，重新分区后的连接可能会与不受安全区域限制的**任何**访问控制规则匹配。如果重新分区后的连接与任何访问控制规则都不匹配，则由访问控制策略默认操作处理。请确定您想这么做。

步骤 4 配置访问控制以处理流过受信任安全区域的非封装连接。

在同一访问控制策略中，配置用于处理受信任安全区域中未重新分区的流量的规则（在此示例中，规则为 **internal_default_inspection**）。

表 *3: internal_default_inspection* 访问控制规则

规则组件	说明
安全区域条件	通过将受信任的安全区域同时用作源区域和目标区域限制来匹配未重新分区的仅内部流量。
操作	允许（已启用深度检查） 选择专门用于检查非封装内部流量的文件和入侵策略。

步骤 5 评估新访问控制规则相对于预先存在的规则的位置。如有必要，请更改规则顺序。

如果将两个新的访问控制规则放在一起，则哪一个规则放在前面都可以。由于您对GRE隧道进行了重新分区，因此，这两个规则无法相互抢占。

步骤 6 保存所有更改的配置。

下一步做什么

- 部署配置更改。

创建隧道区域

以下步骤介绍如何在对象管理器中创建隧道区域。您还可以在编辑隧道规则时创建区域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中，选择**隧道区域**。

步骤 3 点击**添加隧道区域**。

步骤 4 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 5 点击**保存 (Save)**。

下一步做什么

- 在自定义预过滤的过程中，将隧道区域指定为明文直通隧道；请参阅配置预过滤 ， 第 7 页。

将预过滤器规则移至访问控制策略

您可以将预过滤器规则从预过滤器策略移至关联的访问控制策略。

开始之前

请在继续之前注意以下条件：

- 只能将预过滤器规则移至访问控制策略。无法移动隧道规则。
- 只能将预过滤器规则移至关联的访问控制策略。
- 无法移动已配置接口组的预过滤器规则。
- 移动时，预过滤器规则中的**操作 (Action)** 参数将更改为访问控制规则中的适当操作。要了解预过滤器规则中的每项操作，请参阅下表：

预过滤器规则中的操作	访问控制规则中的操作
分析	允许
阻止	阻止
快速路径	信任

- 同样，根据预过滤器规则中配置的操作，在移动规则后，日志记录配置会被设置为适当的设置，如下表中所述。

预过滤器规则中的操作	访问控制规则中已启用的日志记录配置
分析	未启用任何日志设置。
阻止	• 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱
快速路径	• 在连接开始时记录 • 在连接结束时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱

- 移动规则后，预过滤器规则配置中的注释会丢失。但是，新注释会被添加到提及源预过滤器策略的移动规则中。
- 从源策略移动规则时，如果其他用户修改了这些规则，则FMC会显示一条消息。您可以在刷新页面后继续该过程。

过程

步骤 1 在预过滤器策略编辑器中，通过点击鼠标左键来选择要移动的规则。

提示 要选择多个规则，请使用键盘上的 Ctrl (Control) 键。

步骤 2 右键点击所选规则，然后选择**移至另一个策略 (Move to another policy)**。

步骤 3 从**访问策略 (Access Policy)** 下拉列表中选择目标访问控制策略。

步骤 4 从**放置规则 (Place Rules)** 下拉列表中，选择要放置移动规则的位置：

- 要将其定位为默认 **(Default)** 部分中的最后一组规则，请选择底部（在“默认”部分中） **(At the bottom [within the Default section])**。
- 要将其定位为必填 **(Mandatory)** 部分中的第一组规则，请选择顶部（在“必填”部分中）**(At the top [within the Mandatory section])**。

步骤 5 点击 **移动**。

下一步做什么

- 部署配置更改。

预过滤器策略命中计数

命中计数表示为匹配连接触发策略规则的次数。

有关查看预过滤器策略命中计数的完整信息，请参阅查看策略命中计数。

大型流量分流

在运行 FXOS 的设备上（例如 Firepower 4100/9300 机箱），您配置为通过预过滤器策略进行快速路径的某些流量由硬件（具体而言，在 NIC 中）处理，而不是由您的 威胁防御 软件来处理。分流这些连接流会导致更高的吞吐量和更低的延迟，特别是对于大型文件传输等数据密集型应用。此功能对于数据中心尤为有用。这称为静态数据流分流。

此外，默认情况下，威胁防御 设备会根据其他条件（包括信任）来分流数据流。这称为动态数据流分流。

已分流数据流会继续接收受限的状态检测，例如基础 TCP 标志和选项检查。如有必要，系统可以有选择地将数据包上报至防火墙系统以进行进一步处理。

可以从分流大流量中受益的应用示例如下：

- 高性能计算 (HPC) 研究站点，其中 威胁防御设备部署在存储和高计算站点之间。当一个研究站点使用 NFS 上的 FTP 文件传输或文件同步进行备份时，大量数据流量会影响所有连接。对 NFS 上的 FTP 文件传输或文件同步分流可降低对其他流量的影响。
- 高频交易 (HFT)，其中 威胁防御部署在工作站与交易所之间，主要是出于合规目的。通常无需担心安全问题，但延迟是一个重大问题。

可以分流以下数据流：

- （仅限静态数据流分流。）按预过滤器策略使用快速路径的连接。
- 仅有标准或 802.1Q 标记的以太网帧。
- （仅限动态数据流分流）：

- 检测引擎认定无需再检测的已检测数据流。这些数据流包括：
  - 由应用“信任”操作且仅基于安全区域、源和目标网络以及端口匹配的访问控制规则处理的流。
  - 未选择使用 an SSL 策略 进行解密的 TLS/SSL 流。
  - 明确受智能应用绕行 (IAB) 策略信任或由于超出数据流绕行阈值而受其信任的数据流。
  - 与文件或入侵策略相匹配而受其信任的数据流。
  - 不再需要检查的任何允许的流。
- 以下 IPS 预处理器检测的数据流：
  - SSH 和 SMTP。
  - FTP 预处理器辅助连接。
  - 会话初始协议 (SIP) 预处理器辅助连接。
- 使用关键字的入侵规则（也称为选项）

重要事项 有关上述内容的详细信息、例外情况和限制，请参阅数据流分流限制，第 20 页。

使用静态数据流分流

要将符合条件的流量卸载到硬件上，请创建应用**快速路径 (Fastpath)** 操作的预过滤器策略规则。为 TCP/UDP 使用预过滤器规则，并为 GRE 使用隧道规则。

(Not recommended.) 要禁用静态数据流分流并将动态数据流分流作为副产品，请使用 FlexConfig 来运行 **no flow-offload enable** 命令。有关此命令的信息，请参阅 https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html 上的思科 *ASA* 系列命令参考。

使用动态数据流分流

默认情况下启用动态数据流分流，。

要禁用动态分流，请执行以下操作：

```
> configure flow-offload dynamic whitelist disable
```

要重新启用动态分流，请执行以下操作：

```
> configure flow-offload dynamic whitelist enable
```

请注意，无论是否配置了预过滤，只有启用静态数据流分流时才会发生动态分流。

数据流分流限制

并非所有数据流都可分流。即使在分流后，在某些情况下可取消对数据流的分流。以下是一些限制条件：

无法分流的数据流

以下数据流类型无法分流。

- 任何不使用 IPv4 寻址的流，例如 IPv6 寻址。
- 除 TCP、UDP 和 GRE 之外的任意协议的数据流。

注释 无法分流 PPTP GRE 连接。

- 被动、内联或内联分流模式下配置的接口上的数据流。仅支持已路由和已交换的接口类型。
- 需要由Snort或其他检查引擎检查的数据流。在某些情况下（例如FTP），虽然无法分流控制通道，但可以分流次要数据通道。
- 在设备上终止的 IPsec 和 TLS/DTLS VPN 连接。
- 需要加密或解密的数据流。例如，由于 an SSL 策略 而解密的连接。
- 路由模式下的组播数据流。如果桥接组中只有两个成员接口，则它们在透明模式下受支持。
- TCP 拦截数据流。
- TCP 状态绕过流。不能在同一流量上配置数据流分流和 TCP 状态绕行。
- 使用安全组标记的数据流。
- 从不同集群节点转发来的逆向数据流（在集群中数据流不对称的情况下）。
- 集群中的集中数据流（如果数据流的所有者不是控制设备）。
- 无法动态分流包含 IP 选项的数据流。

其他限制

- 流分流与死连接检测 (DCD) 不兼容。不要在可分流的连接上配置 DCD。
- 如果多个与数据流分流条件匹配的数据流排队等待同时分流到硬件上的同一位置，则只会分流第一个数据流。其他数据流则会照常处理。这称为冲突。在CLI中使用**show flow-offload flow** 命令显示此情况的统计信息。
- 动态数据流分流会禁用所有 TCP 规范器检查。
- 虽然分流的数据流通过FXOS接口，但这些数据流的统计信息不会显示在逻辑设备接口上。因此，逻辑设备接口计数器和数据包速率不会反映分流流量。

逆向分流的条件

对数据流分流后，如果数据流中的数据包符合以下条件，则将被返回到威胁防御接受进一步处理：

- 数据包包含时间戳以外的 TCP 选项。
- 数据包经过分段。
- 它们会进行等价多路径 (ECMP) 路由，并且入口数据包会从一个接口移至另一个接口。

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。