服务质量

以下主题介绍如何将服务质量 (QoS) 功能用于采用 威胁防御设备的策略网络流量：

QoS 简介

访问控制允许或信任的服务质量（也称 QoS）、速率限制（策略）网络通信。系统不对快速路径的流量进行速率限制。

虽然 QoS 仅在 威胁防御 设备的路由接口上支持，但在站点间 VPN 和 VTI 接口上并不支持。

日志记录速率限制连接

没有用于 QoS 的日志记录配置。可以在不记录的情况下对连接限制速率，但不能仅因为连接被限制速率而不记录连接。要查看连接事件中的 QoS 信息，必须单独将相应连接的两端记录到 管理中心数据库。有关详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的您可以登录的其他连接。

速率限制连接的连接事件包含流量被丢弃的数量信息，以及有关限制流量的 QoS 配置的信息。您可以在事件视图（工作流）、仪表板和报表中查看此信息。

关于 QoS 策略

部署到受管设备上的 QoS 策略用于监管速率闲置。每项 QoS 策略可以多台设备为目标；每天设备每次只能部署一项 QoS 策略。

系统按照您指定的顺序将流量与 QoS 规则相匹配。系统根据第一条规则（其中所有规则的条件都与流量匹配）对流量进行速率限制。与任何规则都不匹配的流量不受速率限制。

注释 设备上的规则总数（包括 QoS 规则）不能超过 255。达到此阈值时，系统将显示部署警告消息。您需要减少成功部署的规则数量。

必须按源接口或目标（路由）接口来限制 QoS 规则。系统将对其中每个接口单独强制实施速率限制；不能为一组接口指定一个汇聚速率限制。

QoS规则还可以按其他网络特性以及情景信息（如应用、URL、用户身份和自定义安全组标记(SGT)）对流量实施速率限制。

您可以单独对下载流量和上传流量进行速率限制。系统根据连接发起方确定下载和上传方向。

注释 QoS 不从属于主访问控制配置；您将单独配置 QoS。不过，部署到同一设备上的访问控制和 QoS 策略将共享身份配置；请参阅将其他策略与访问控制相关联。

QoS 策略和多租户

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。

位于祖先域中的管理员可向位于不同后代域中的设备部署同一 QoS 策略。位于这些后代域中的管理员，既可使用这一祖先部署的 QoS 只读策略，也可使用本地策略替换此策略。

QoS 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

使用 QoS 策略的速率限制

要执行基于策略的速率限制，请配置 QoS 策略并将它们部署到受管设备。每项 QoS 策略可以多台设备为目标；每天设备每次只能部署一项 QoS 策略。

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**设备** > **QoS**。

步骤 2 点击**新建策略**创建新的 QoS 策略，并且可以选择分配目标设备；请参阅创建 QoS 策略，第 3 页。

还可以 **复制**（  ） 或 **编辑**（  ） 现有策略。

步骤 3 配置 QoS 规则；请参阅配置 QoS 规则，第 5 页和QoS 规则条件，第 6 页。

QoS 策略编辑器中的规则将按评估顺序列出每条规则，并显示规则条件和速率限制配置的摘要。右键点击菜单提供规则管理选项，包括移动、启用和禁用。

为有助于较大规模的部署，可以**按设备过滤**，以仅显示影响特定设备或设备组的规则。可以搜索规则，也可以在规则内部进行搜索；系统会将您在**搜索规则**字段中输入的文本匹配与规则名称和条件值相匹配，包括对象和对象组。

注释 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。如果不认真规划，这些规则会抢占其他规则、需要额外的许可证或包含无效配置。图标代表注释、警告和错误。如果存在问题，请点击**显示警告**显示列表。有关详细信息，请参阅访问控制规则的最佳实践。

步骤 4 点击**策略分配**识别策略针对的受管设备；请参阅为 QoS 策略设置目标设备，第 4 页。

如果在创建策略过程中识别出了目标设备，请验证您的选择。

步骤 5 保存 QoS 策略。

步骤 6 由于此功能必须允许某些数据包通过，因此必须将系统配置为检查这些数据包。请参阅处理在流量识别之前通过的数据包的最佳实践和指定策略以处理在流量识别之前通过的数据包。

步骤 7 部署配置更改；请参阅部署配置更改。

创建 QoS 策略

没有规则的新 QoS 策略不会执行速率限制。

过程

步骤 1 选择**设备** > **QoS**。

步骤 2 点击**新建策略**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 4 （可选）选择要部署策略的**可用设备**，然后点击**添加到策略**或拖放**所选设备**。要减少显示的设备，请在 **Search** 字段中键入搜索字符串。

在部署策略之前必须分配设备。

步骤 5 单击**保存**。

下一步做什么

- 配置和部署 QoS 策略；请参阅使用 QoS 策略的速率限制，第 3 页。

为 QoS 策略设置目标设备

每个 QoS 策略都可以将多个设备作为目标；每个设备一次可以有一个已部署的 QoS 策略。

过程

步骤 1 在 QoS 策略编辑器中，点击**策略分配**。

步骤 2 制定目标联系人列表：

- 添加 - 选择一个或多个**可用设备**，然后点击**添加到策略**或拖放到**所选设备**列表。
- 删除 - 点击单个设备旁边 **删除**（ ），或选择多个设备，点击鼠标右键，然后选择 **删除所选项**。
- 搜索 - 在搜索字段中输入搜索字符串。点击 **清除**（ ） 以清除搜索。

步骤 3 点击**确定**以保存策略分配。

步骤 4 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改；请参阅部署配置更改。

配置 QoS 规则

创建或编辑规则时，请使用规则编辑器的上半部分配置常规规则属性。使用规则编辑器的下半部分来配置规则条件和注释。

过程

步骤 1 在 QoS 策略编辑器的“规则”上：

- 添加规则 - 点击**添加规则 (Add Rule)**。
- 编辑规则-点击 **编辑**（）。

步骤 2 输入 **Name**。

步骤 3 配置规则组成部分。

- **已启用** -指定规则是否为已启用。
- QoS 应用位置 - 选择要进行速率限制的接口：**目标接口对象中的接口 (Interfaces in Destination Interface Objects)** 或**源接口对象中的接口 (Interfaces in Source Interface Objects)**。您的选择必须与填入的接口限制相对应（不为**任意 [any]**）。
- 每个接口的流量限制 - 以兆位/秒为单位输入**下载限制**和**上传限制**。默认值**无限制**可防止在该方向上对匹配流量进行速率限制。
- 条件 - 点击要添加的相应的条件。必须配置源或目标接口条件，与您选择的 **QoS 应用位置**相对应。
- 注释-点击 **注释**。要添加注释，请点击**新建注释 (New Comment)**，输入注释，然后点击**确定 (OK)**。您可以在保存规则之前编辑或删除此注释。

如需有关规则组成部分的详细信息，请参阅QoS 规则组成部分 ， 第 6 页。

步骤 4 保存规则。

步骤 5 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。

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。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

步骤 6 点击**保存 (Save)** 保存策略。

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

访问控制规则的最佳实践

QoS 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。

接口（QoS 应用位置）

您不能保存对所有流量都进行速率限制的 QoS 规则。对于每个 QoS 规则，必须将 QoS 应用于以下两个选项之一：

- 源接口对象中的接口 - 对通过规则源接口的流量进行速率限制。如果选择此选项，必须至少添加一个源接口限制（不能为**任何 [any]**）。
- 目标接口对象中的接口 - 对通过规则目标接口的流量进行速率限制。如果选择此选项，必须至少添加一个目标接口限制（不能为**任何 [any]**）。

每个接口的流量限制

QoS 规则对您使用“QoS 应用位置”(Apply QoS On) 选项指定的每个接口单独实施速率限制。不能为一组接口指定汇聚速率限制。

您可以按兆位/秒对流量进行速率限制。默认值**无限制 (Unlimited)** 可防止对匹配流量进行速率限制。

您可以单独对下载流量和上传流量进行速率限制。系统根据连接发起方确定下载和上传方向。

如果指定限制大于接口的最大吞吐量高，系统不会对匹配的流量进行速率限制。最大吞吐量可能受接口的硬件配置影响，可在每台设备的属性中指定硬件配置（**设备** > **设备管理**）。

条件

条件指定规则处理的特定流量。您可以为每个规则配置多个条件。流量必须匹配所有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。有关详细信息，请参阅QoS 规则条件，第 6 页。

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。

在策略编辑器中，系统会显示规则具有的注释数量。在规则编辑器中，请使用“注释”(Comments) 选项卡查看现有注释和新注释。

QoS 规则条件

条件指定规则处理的特定流量。您可以为每个规则配置多个条件。流量必须匹配所有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。您可以使用以下方式对流量进行速率限制：

有关详细信息，请参阅以下各节之一：

相关主题

接口规则条件，第 7 页
网络规则条件，第 7 页
用户规则条件，第 8 页
应用规则条件，第 8 页
端口规则条件，第 9 页
URL 规则条件，第 10 页
自定义 SGT 规则条件，第 11 页

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。

用户规则条件

用户规则条件会根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联中所述。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

应用规则条件

系统分析 IP 流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用程序规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅 应用检测器基础知识。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *1:* 应用特征

特征	说明	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

相关主题

配置应用控制的最佳实践

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

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。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

应用过滤也建议用于动态打开单独通道的应用（如 FTD），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

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 二者添加为源端口条件。

端口、协议和 ICMP 代码规则条件

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。

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。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

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。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标签。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制的规则相匹配。对于 威胁防御设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。
- SSL 规则 - SSL 规则仅支持 TCP 端口条件。
- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

URL 规则条件

使用 URL 条件控制网络上的用户可以访问的网站。

有关完整信息，请参阅URL 过滤。

自定义 SGT 规则条件

如果未将 ISE/ISE-PIC 配置为身份源，可以使用非 ISE 分配的安全组标记 (SGT) 来控制流量。SGT 会指定可信网络内的流量源的权限。

自定义 SGT 规则条件使用手动创建的 SGT 对象来过滤流量，而不是使用从系统与 ISE 服务器的连接中获取的 ISE SGT 进行过滤。这些手动创建的 SGT 对象与要控制的流量的 SGT 属性相对应。使用自定义 SGT 控制流量不属于用户控制。

ISE SGT 与自定义 SGT 规则条件

某些规则允许您根据分配的 SGT 来控制流量。根据规则类型和您的身份源配置，您可以使用 ISE 分配的 SGT 或自定义 SGT 将流量与分配的 SGT 属性进行匹配。

注释 如果您使用 ISE SGT 匹配流量，即使一个数据包没有分配的 SGT 属性，当与该数据包的源 IP 地址关联的 SGT 在 ISE 中已知时，该数据包仍会匹配 ISE SGT 规则。

条件类型	要求在目录	规则编辑器中列出的 SGT
ISE SGT	ISE 身份源	通过查询 ISE 服务器获得的 SGT，包含自动更新的元数据
自定义 SGT	无 ISE/ISE-PIC 身份源	您创建的静态 SGT 对象

从自定义 SGT 自动过渡到 ISE SGT

如果您创建与自定义 SGT 匹配的规则，然后将 ISE/ISE-PIC 配置为身份源，则系统：

- 禁用对象管理器中的**安全组标记**选项。尽管系统会保留现有 SGT 对象，但您不能修改它们或添加新的 SGT 对象。
- 保留使用自定义 SGT 条件的现有规则。但是，这些规则与流量不匹配。您也不能为现有规则添加其他自定义 SGT 条件，或创建具有自定义 SGT 条件的新规则。

如果您配置了 ISE，则思科建议您删除或禁用具有自定义 SGT 条件的现有规则。相反，使用 ISE 属性条件将流量与 SGT 属性相匹配。

QOS 历史记录

特性	Version	详细信息
能够指定具有未知信誉的 URL 的处理方式	6.7	有关详细信息，请参阅URL 过滤历史记录。

特性	Version	详细信息
增加了速率限制	6.2.1	将最大速率限制从 1000 Mbps 增加到 100,000 Mbps。 修改了屏幕：QoS 规则编辑器 支持的平台：Firepower 威胁防御
自定义 SGT 和原始客户端网络过滤	6.2.1	QoS 现在可以使用自定义安全组标记 (SGT) 和原始客户端网络信息（XFF、真实客户端 IP 或自定义的 HTTP 报头）来限制流量的速率。 修改了屏幕：QoS 规则编辑器 支持的平台：Firepower 威胁防御
QoS（速率限制）	6.1	引入的功能。 QoS 会对访问控制允许或信任的网络流量进行速率限制（策略）。 新屏幕：**设备** > **QoS** 支持的平台：Firepower 威胁防御

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。