规则和规则集

规则

通常，规则指定用户、组、角色或组织访问域中指定类型和状态的对象的权限。多云防御支持各种云服务提供商，每种环境都有自己的规则要求或方法。在云账户中创建的规则的处理方式可能与在多云防御控制器中创建的规则不同。某些规则默认应用于网关和实例，因此在您继续添加和修改规则和策略以实现最佳性能和覆盖范围时，环境具有基本的保护级别。

考虑您要适应的网关环境类型时，规则**类型**非常重要。并非所有规则或规则类型都与每个网关环境完全兼容。 多云防御控制器 中支持的网关类型包括入口、出口和东西向。

有关规则和规则集的信息，或者如何创建或修改策略和组的规则和规则集，请阅读本章的其余部分。

策略管理

策略在 多云防御 控制面板中创建，或使用 多云防御 Terraform 提供程序通过协调创建。策略作为 多云防御控制器 数据库的一部分进行存储和保留。网关通过定期心跳检索策略或任何策略更改，其中网关提供控制器运行状况和遥测信息，同时请求是否需要应用任何策略更改。与控制器通信的网关是完全加密的，并通过相互 TLS 会话建立。检测信号每 5 秒发生一次，以确保网关上的策略与用户创建或修改的策略同步。

策略规则集网关和管理

策略规则管理

分配给网关的策略规则集可以动态更改为不同的策略规则集。如果需要将不同的策略规则集交换到活动网关，则可以以非影响方式启动此操作。新策略规则集的分配与网关更新/升级过程类似。新的网关实例使用新的策略规则集进行实例化。一旦新流量会话处于活动状态且运行状况正常，它们将

被重定向到新的流量会话。旧的流量会话从旧的命途实例中刷新。旧的未来实例将被删除。操作将在几分钟内完成。此更改作为网关配置设置的一部分启动。导航至 **管理** > **网关** > **网关**。可以使用 多云防御 门户或 多云防御 Terraform 提供程序启动更改。

策略规则集网关状态

策略规则与其关联的网关之间的连接状态可以是以下两个选项之一：

- **已更新** - 策略在网关上处于活动状态，并与控制器同步。
- **正在更新** - 网关正在主动处理策略更改。策略更改为网关所知，但尚未激活。网关仍在使用当前策略处理流量。

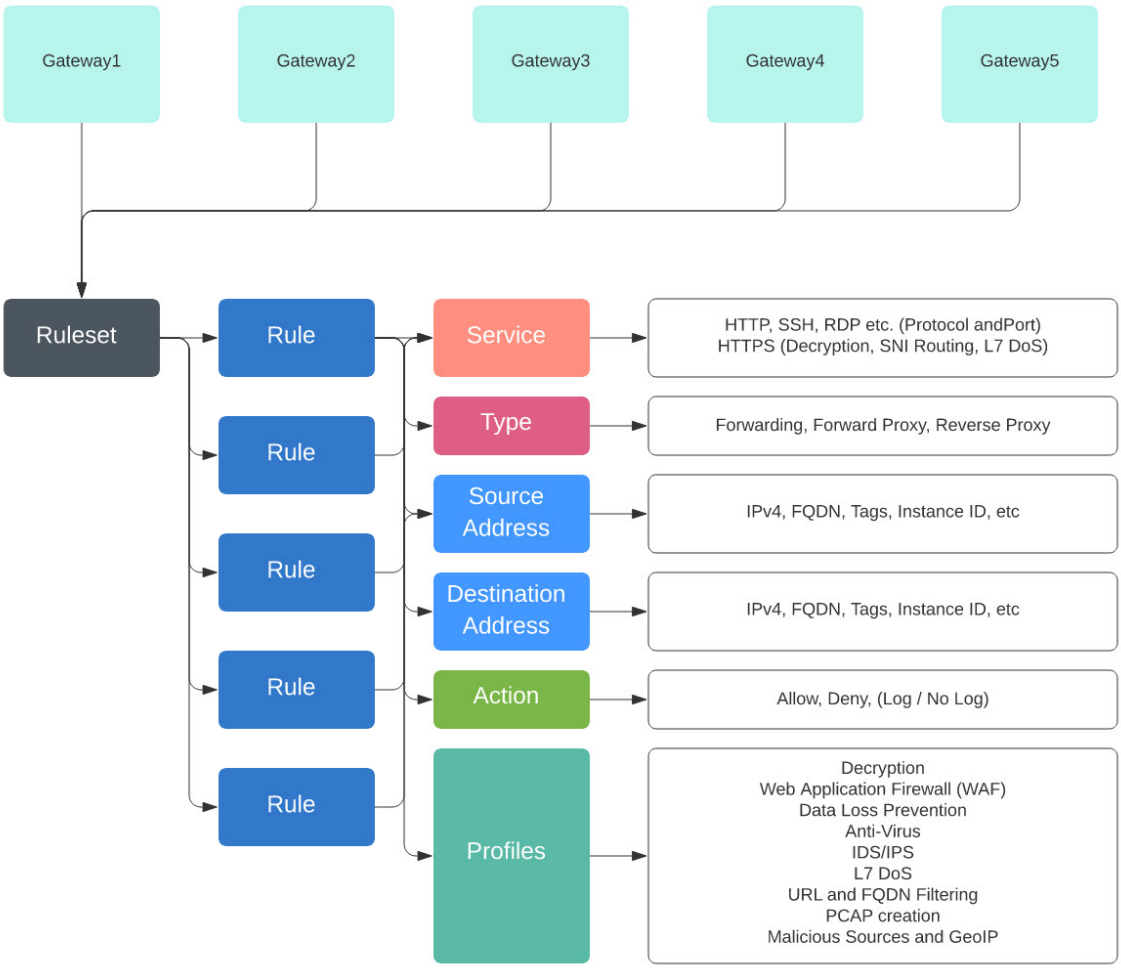
规则集和规则集组

规则集

规则集由一组规则组成，这些规则定义应用于一组一个或多个网关以适应应用和工作负载保护的分段和高级安全策略。规则以优先级列表的形式组织，其中流量由匹配的规则处理，采取常规操作来允许或拒绝，并通过高级安全性进行进一步检查。

规则集必须至少与一个 多云防御网关相关联。以下限制适用于所有规则集：

- 规则集与云无关，可应用于多个云环境中的一个或多个网关操作。
- 网关只能与一个规则集关联，但使用规则集组可以应用多个规则集。
- 规则集中的规则可以使用已发现的云资产信息来形成动态策略或实时适应变化的策略。
- 规则集可以包括仅适用于特定云账户和/或云区域的规则，但规则集适用于跨云环境的网关。以下为输出示例：
  - 应用于跨两个云的两个网关的规则集中的基于动态标记的地址对象可以解析为与一个云中的网关关联的一组 IP 地址，同时解析为一组不同的 IP与另一个云中的网关关联的地址。
- 可以从 **管理** > **安全策略** > **规则集** 页面或从网关创建工作流程中创建规则集。下图显示了应用于多个网关的单个规则集：



另一个受支持的使用案例是与多个网关关联的多个规则集。

策略规则集组

策略规则集组是独立规则集的集合。用户可以将多个独立规则集组合到一个策略规则集组中，并将该组与一个或多个 多云防御网关关联。策略规则集组允许组织以有组织的方式分离策略，并将其组合为总体策略。

Note

- 策略规则集组只能包含规则集成员。
- 确保与策略规则集组关联的所有规则集没有冲突规则。
- 一个策略规则集组最多可以有 100 个规则集成员。

创建策略规则集

要创建策略规则集，请执行以下操作：

步骤 1 导航至 **管理** > **安全策略** > **规则集**。
步骤 2 点击**创建 (Create)**。
步骤 3 添加策略规则集的名称和说明。
步骤 4 点击 **Save**。

What to do next

创建策略规则集后， 在规则集中添加或编辑转发代理规则 到规则集中。

在规则集中创建规则

-

在规则集中添加或编辑转发规则

使用以下程序将现有规则添加到策略规则集中或编辑策略规则集中已包含的规则：

开始之前

您可以在 多云防御网关中创建新规则。在向规则集中添加或编辑规则之前，请注意以下限制：

- 单个策略规则集最多可以有 2047 条规则。
- 一个策略规则集组最多可以包含 2047 条规则。

步骤 1 导航至 **管理** > **安全策略** > **规则集**。
步骤 2 点击策略规则集名称以查看策略规则集。
步骤 3 点击 **添加规则** 以创建新规则或添加现有规则。这会生成一个提示符。
步骤 4 输入以下属性：

- **名称** - 用于引用规则的唯一名称。
- （可选） **说明** - 规则的简要说明。
- **类型** - 选择 **转发**。

步骤 5 输入以下对象信息：

- **服务** - 用于确定规则将应用的协议和端口的服务对象。
- **源** - 用于确定将应用规则的资源的地址对象。

- **目标** - 用于确定将应用规则的目标资源的地址对象。对于 **ReverseProxy** 规则类型，目标始终是 多云防御网关。对于 **ForwardProxy** 规则类型，目标始终为任意。
- **FQDN** - 使用下拉菜单选择一组用于 SNI 匹配的 FQDN。请注意，这仅适用于 **转发** 规则类型。

步骤 6 输入详细信息：

- **操作** - 操作定义应允许还是拒绝流量，以及是否应在事件中记录流量。无论操作设置为 **记录** 还是 **无记录**，流量始终记录在流量摘要中。对于规则允许的流量，系统将评估高级安全配置文件。请注意，每个高级安全配置文件都有自己的操作，这些操作将使用或覆盖此操作。
- **拒绝时重置** - 如果启用， 多云防御网关 将为匹配此策略的会话发送 TCP 重置数据包，并被网关丢弃。请注意，这仅适用于 **转发** 规则类型。

步骤 7 输入以下配置文件信息：

- （可选） **网络入侵** - 用于实现高级安全的网络入侵 (IPS) 配置文件。
- （可选） **防恶意软件** - 用于实现高级安全的防恶意软件配置文件。如果尚未创建防恶意软件配置文件，请点击此处的 **+ 创建防恶意软件** 。
- （可选） **防数据丢失** - 用于实现高级安全的防数据丢失 (DLP) 配置文件。请注意，这仅适用于 **ForwardProxy** 规则类型。
- （可选） **FQDN 过滤** - 要用于高级安全的 FQDN 过滤 (FQDN) 配置文件。
- （可选） **恶意 IP** - 要用于高级安全的恶意 IP (MIP) 配置文件。
- （可选） **PCAP** - 选中此框可启用。为规则启用还是禁用数据包捕获。只要流量与启用了 PCAP 的规则匹配，就会发生会话流量的数据包捕获，并且 PCAP 将存储在 PCAP 配置文件指定的位置。在 多云防御网关上配置了 PCAP 配置文件。

步骤 8 指定规则的配置后，点击 **保存**。

步骤 9 继续添加更多规则。添加所有所需规则后，点击 **保存更改**。您将看到对规则集所做的所有更改的前后视图。完成所需更改后，点击 **保存**。如果需要进行进一步更改，请点击 **取消** 以返回编辑规则集。

在规则集中添加或编辑反向代理规则

使用以下程序将现有规则添加到策略规则集中或编辑策略规则集中已包含的规则：

开始之前

您可以在 多云防御网关中创建新规则。在向规则集中添加或编辑规则之前，请注意以下限制：

- 单个策略规则集最多可以有 2047 条规则。
- 一个策略规则集组最多可以包含 2047 条规则。

步骤 1 导航至 **管理** > **安全策略** > **规则集**。

步骤 2 点击策略规则集名称以查看策略规则集。

步骤 3 点击 **添加规则** 以创建新规则或添加现有规则。这会生成一个提示符。

步骤 4 输入以下属性：

- **名称** - 用于引用规则的唯一名称。
- （可选） **说明** - 规则的简要说明。
- **类型** - 选择 **ReverseProxy**。

步骤 5 输入以下对象信息：

- **服务** - 用于确定规则将应用的协议和端口的服务对象。
- **源** - 用于确定将应用规则的资源的地址对象。
- **目标** - 用于确定将应用规则的目标资源的地址对象。对于 **ReverseProxy** 规则类型，目标始终是 多云防御网关。
- **目标** - 用于指定 多云防御网关 将建立到服务器连接的网关的地址对象。

步骤 6 选择首选规则 **操作**。这定义了应允许还是拒绝流量，以及是否应在事件中记录流量。无论操作设置为 **记录** 还是 **无记录**，流量始终记录在流量摘要中。对于规则允许的流量，系统将评估高级安全配置文件。请注意，每个高级安全配置文件都有自己的操作，这些操作将使用或覆盖此操作。

步骤 7 输入以下配置文件信息：

- （可选） **网络入侵** - 用于实现高级安全的网络入侵 (IPS) 配置文件。
- （可选） **防恶意软件** - 用于实现高级安全的防恶意软件配置文件。如果尚未创建防恶意软件配置文件，请点击此处的 **+ 创建防恶意软件** 。
- （可选） **Web 保护** - 用于实现高级安全的 Web 保护 (WAF) 配置文件。请注意，这仅适用于 **ReverseProxy** 规则类型。
- （可选） **URL 过滤** - 要用于高级安全的 URL 过滤 (URL) 配置文件。请注意，这仅适用于 **ForwardProxy** 和 **ReverseProxy** 规则类型。
- （可选） **恶意 IP** - 要用于高级安全的恶意 IP (MIP) 配置文件。
- （可选） **PCAP** - 选中此框可启用。为规则启用还是禁用数据包捕获。只要流量与启用了 PCAP 的规则匹配，就会发生会话流量的数据包捕获，并且 PCAP 将存储在 PCAP 配置文件指定的位置。在 多云防御网关上配置了 PCAP 配置文件。

步骤 8 指定规则的配置后，点击 **保存**。

步骤 9 继续添加更多规则。添加所有所需规则后，点击 **保存更改**。您将看到对规则集所做的所有更改的前后视图。完成所需更改后，点击 **保存**。如果需要进行进一步更改，请点击 **取消** 以返回编辑规则集。

在规则集中添加或编辑转发代理规则

使用以下程序将现有规则添加到策略规则集中或编辑策略规则集中已包含的规则：

Before you begin

您可以在 多云防御网关中创建新规则。在向规则集中添加或编辑规则之前，请注意以下限制：

- 单个策略规则集最多可以有 2047 条规则。
- 一个策略规则集组最多可以包含 2047 条规则。

步骤 1 导航至 **管理** > **安全策略** > **规则集**。

步骤 2 点击策略规则集名称以查看策略规则集。

步骤 3 点击 **添加规则** 以创建新规则或添加现有规则。这会生成一个提示符。

步骤 4 输入以下属性：

- **名称** - 用于引用规则的唯一名称。
- （可选） **说明** - 规则的简要说明。
- **类型** - 选择 **ForwardProxy**。

步骤 5 输入以下对象信息：

- **服务** - 用于确定规则将应用的协议和端口的服务对象。
- **源** - 用于确定将应用规则的资源的地址对象。
- **目标** - 用于确定将应用规则的目标资源的地址对象。对于 **ForwardProxy** 规则类型，目标始终为任意。
- **FQDN** - 使用下拉菜单选择一组用于 SNI 匹配的 FQDN。请注意，这仅适用于 **转发** 规则类型。

步骤 6 输入首选规则 **操作**。这定义了应允许还是拒绝流量，以及是否应在事件中记录流量。无论操作设置为 **记录** 还是 **无记录**，流量始终记录在流量摘要中。对于规则允许的流量，系统将评估高级安全配置文件。请注意，每个高级安全配置文件都有自己的操作，这些操作将使用或覆盖此操作：

步骤 7 输入以下配置文件信息：

- （可选） **网络入侵** - 用于实现高级安全的网络入侵 (IPS) 配置文件。
- （可选） **防恶意软件** - 用于实现高级安全的防恶意软件配置文件。如果尚未创建防恶意软件配置文件，请点击此处的 **+ 创建防恶意软件** 。
- （可选） **防数据丢失** - 用于实现高级安全的防数据丢失 (DLP) 配置文件。请注意，这仅适用于 **ForwardProxy** 规则类型。
- （可选） **URL 过滤** - 要用于高级安全的 URL 过滤 (URL) 配置文件。请注意，这仅适用于 **ForwardProxy** 和 **ReverseProxy** 规则类型。
- （可选） **FQDN 过滤** - 要用于高级安全的 FQDN 过滤 (FQDN) 配置文件。

- （可选） **恶意 IP** - 要用于高级安全的恶意 IP (MIP) 配置文件。
- （可选） **PCAP** - 选中此框可启用。为规则启用还是禁用数据包捕获。只要流量与启用了 PCAP 的规则匹配，就会发生会话流量的数据包捕获，并且 PCAP 将存储在 PCAP 配置文件指定的位置。在 多云防御网关上配置了 PCAP 配置文件。

步骤 8 指定规则的配置后，点击 **保存**。

步骤 9 继续添加更多规则。添加所有所需规则后，点击 **保存更改**。您将看到对规则集所做的所有更改的前后视图。完成所需更改后，点击 **保存**。如果需要进行进一步更改，请点击 **取消** 以返回编辑规则集。

禁用、编辑、克隆或删除规则集中的规则

使用以下程序可编辑或克隆为规则集配置的现有规则。如果当前策略或规则集不需要某个规则处于活动状态，也可以禁用该规则。如果现在或将来的部署不需要规则，可以将其删除。

请注意，一次只能编辑或克隆一个规则。您可以同时禁用或删除多个规则。

步骤 1 导航至 **管理** > **安全策略** > **规则集**。

步骤 2 找到包含要禁用、编辑、克隆或删除的规则的规则集，然后点击规则集名称。

步骤 3 选中独立规则的复选框。

步骤 4 展开 **操作** 按钮。

步骤 5 选择您的可操作项目：

- **禁用** - 此选项将规则保留在规则集中，但会禁用规则和配置的规则操作，以免影响流量。
- **编辑** - 此选项将启动“属性”窗口，并允许您编辑规则的配置。点击 **保存** 以保留所做的更改。
- **克隆** - 此选项将创建规则的副本，并打开“属性”窗口，以便为克隆的规则命名，或对规则的配置进行任何其他更改。点击 **保存** 以确认配置。保存克隆的规则会自动将其添加到您正在查看的规则集中。
- **删除** - 此选项从规则集中永久删除规则。请注意，这也会从网关中删除该规则。

步骤 6 点击 **保存更改** 以确认对规则所做的更改，并间接执行规则集。如果您不想保存更改，可以点击 **取消**。确认丢失对网关所做的任何更改。

创建策略规则集组

要创建策略规则集组，请执行以下操作：

步骤 1 导航至 **管理** > **安全策略** > **规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 添加策略组的名称和说明。

步骤 4 选择 **类型** 作为组。

步骤 5 展开下拉菜单，在 **规则集列表** 部分添加规则集。如果要添加更多规则集，请点击 **添加规则集** 以添加另一行。

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。