服务对象

反向代理服务对象（入口）

入口服务对象用于 ngress/反向代理规则。该对象定义 多云防御 网关侦听其接收并转发到目标/后端地址的流量的侦听程序端口。可以使用配置了 TLS 证书的解密配置文件来配置侦听程序端口。当流量到达侦听程序端口时， 多云防御网关 会返回已配置的 TLS 证书。考虑以下可配置选项：

- 可以在此端口上配置 SNI。这使得单个侦听程序端口（例如 443）能够根据 SNI 代理到多个后端目标。
- 可以在服务上配置 L7 DoS（L7 拒绝服务），以设置 URI 和/或 HTTP 方法的速率限制。
- 目标定义用于转发流量的后端地址对象和端口。代理的流量可以作为 HTTP、HTTPS、TCP 或 TLS 转发。

使用以下程序创建和添加反向代理服务对象：

步骤 1 导航至 **管理** > **安全策略** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 点击 **反向代理**。

步骤 4 提供 **名称** 和 **说明**。

步骤 5 配置如下定义的代理参数：

选项	说明
解密配置文件	分配要用于代理服务的解密配置文件，其中还包括服务器证书。

选项	说明
目标端口	分配目标端口。对于大多数基于Web的服务，目的端口为 443。这是端口 多云防御网关 侦听传入流量。
Protocol	默认值是“TCP”。
SNI	输入 SNI 列表。
L7 DoS	输入要分配给此代理服务的第 7 层 DoS 配置文件。
目标后端端口	启用目标/后端应用端口号。
Protocol	选择后端协议。
Address	选择后端IP地址。在大多数情况下，IP地址是内部负载均衡器的前端 IP。

Note 如果需要在多个端口上运行代理服务，可以添加更多条目。但是，所有端口都提供相同的证书，并代理到相同的后端目标地址对象。

转发代理服务对象（出口/东西向）

转发代理服务专门用于基于HTTP的流量。该对象定义了一个侦听程序端口， 多云防御网关 用于侦听其接收的流量并转发到 TLS SNI 扩展报头或 HTTP 主机报头中可用的地址/主机。

Note 我们建议将其用于出口/东西向流量。

使用以下程序创建和添加转发代理服务。

步骤 1 导航至 **管理** > **安全策略** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 点击 **转发代理**。

步骤 4 提供名称和说明。

步骤 5 或者，选择要匹配的应用 ID。

步骤 6 配置如下定义的代理参数。

选项	description
解密配置文件	分配解密配置文件，其中还包括证书。多云防御通过使用此配置文件中提供的证书对其进行签名来模拟外部证书。假定根证书已安装在所有客户端应用实例上。
目标端口	分配目标端口。对于大多数基于Web的服务，目的端口为443。
Protocol	HTTP 或 HTTPS。

Note

- 多云防御 侦听 **目标端口** 并等待 HTTP 主机报头或 TLS SNI 报头数据包。 多云防御 收到此数据包后，它会使用该协议连接到主机。如果协议是 HTTPS，则从外部主机接收的证书数据由解密配置文件中的证书签名并发送到客户端。 **必须** 在客户端应用实例上安装根证书，以避免出现证书错误。
- 对于给定的目标端口，所有服务对象的策略规则集中只能有一个解密配置文件（根 CA 证书）关联。
- 在转发代理会话期间， 多云防御网关 在目标上执行 DNS 查找，DNS 请求超时为 30 秒，缓存老化时间为 TTL 秒。

转发服务对象（出口/东西向）

转发服务对象用于转发规则。与此类型的规则/服务匹配的流量不会被代理，而是按原样转发。这意味着对 加密 流量没有深度数据包检测和应用 ID。

Note 我们 **强烈** 建议将其用于东西向流量。

使用以下程序创建和添加转发代理服务：

步骤 1 导航至 **管理** > **安全策略** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 点击 **转发**。

步骤 4 提供名称和说明。

步骤 5 多云防御 在每个服务级别上支持源 NAT。对于需要保留源 IP 的流量（例如东西流量），请禁用 SNAT。

对于出口流量， **必须** 始终启用 SNAT。

步骤 6 配置如下定义的端口参数。

选项	**description**
目标端口	将目的端口或目的端口范围分配为 `start-end`。
Protocol	TCP、 UDP、 ICMP

Note 在转发策略中，深度数据包检测操作 **仅** 发生在非加密流量上。

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。