地址对象

地址对象

地址对象 表示一组一个或多个 IP、CIDR 或 FQDN，用于在 **安全策略规则集规则** 中用作 **源** 或 **目标**，或者用作 **反向代理服务对象** 中的 **目标后端地址**，具体取决于其定义方式。地址对象可以使用传统结构进行静态配置，也可以使用云结构进行动态配置。

地址对象表示安全策略规则或规则集中 **源**、 **目标**或 **反向代理目标** 字段中的一组一个或多个 IP、CIDR 或 FQDN。也可以将其定义为反向代理服务对象中的目标后端地址。本节重点介绍源对象和目标对象。

源/目标

这些对象用于定义明确映射到 IP 地址或 CIDR 的匹配条件。这些对象在策略规则内被引用，并在处理策略规则时根据进入网关实例的流量进行评估。

当明确需要 IP 地址和 CIDR 来匹配进入网关实例的应用流量时，源和目标地址对象非常有用。这些对象在策略规则定义的源和目标字段中引用。用于填充每个字段的地址对象类型取决于流量、应用类型和使用案例。

源或目的地址对象

源或目标地址对象为安全策略规则集中的规则指定源或目标。规则使用它来根据流量的源或目标 IP 地址匹配流量。不同类型的地址对象定义如下：

IP/CIDR/FQDN（静态）地址对象

IP/CIDR/FQDN 地址对象配置为一组 IP 地址、CIDR 块或 FQDN。IP/CIDR 地址对象的示例包括：

- DNS 服务器的目标 IP。
- SMTP 中继服务器的目标 IP。
- NTP 服务器的目标 IP。
- 应用工作负载的源 IP 或子网。

FQDN 地址对象定义一组明确的 FQDN，用于根据 DNS 解析允许或阻止 IP。在 FQDN 地址对象内定义 FQDN 并在策略规则内进行引用时，网关实例会执行 DNS 解析来检索相应的 IP 地址，以根据其匹配传入流量。默认情况下，不会启用缓存。在这种情况下，DNS 解析每 60 秒完成一次，网关实例使用检索到的解析 60 秒。如果 FQDN 地址对象内指定的 FQDN 解析为大量 IP 地址（即每个地址超过 400 个），则可以启用缓存。在这种情况下，可以指定 DNS 解析间隔以及缓存大小和缓存 TTL。

FQDN 地址对象可用于匹配基于 UDP 的应用流量（例如NTP）或请求数据包中不存在主机信息的 TCP 流量（例如SMTP）等指定端口阵列上连接设备。在任一情况下，建议使用 FQDN 地址对象来匹配此类应用流量，而不是手动定义所有适当的NTP服务器或SMTP服务器的IP地址列表，例如，您的内部工作负载需要连接到。

动态云结构

云原生地址对象是 多云防御控制器 通过定期资产收集（基于 API）或实时事件跟踪（GCP Pub/Sub 集成）发现的动态云资源。这些资源可以是单个资源，例如 VPC/VNET、实例 ID、安全组、子网 ID，也可以是通过用户定义的标签引用的一组资源。多云防御控制器结合使用实时事件跟踪和有针对性的 API 调用来动态填充与云资源关联的 IP 地址。因此，对云原生资源所做的任何后续更改都会自动反映在引用此资源的地址对象中。

Note 通过使用云原生结构来定义源或目标地址对象，您可以跨单云和多云环境创建真正动态的云策略。在云环境中添加、删除或更改云资源时，地址对象会动态更新以反映这些更改，从而确保在您的环境中的所有应用和功能中自动更新您的安全状态。

VNet 和 VPC 环境中的用户定义标签

标签将使用一组标签定义的云资源的 IP 地址或 CIDR 映射到地址对象。在 GCP 中，标签是通常用于对专用于不同环境（即开发、暂存、生产等）的资源进行分类的键值对。在源或目标地址对象中，用户定义的标签可用于引用资源，包括实例、VPC/VNET、子网和安全组。最常见的是，组织使用标签对实例进行分类。

基于标记的策略规则是动态云策略的一个非常强大的组件。可以为具有特定标签的实例组定义精细的策略规则。部署这些策略规则后，只要部署具有适当标签的新实例，它就会自动继承为其所属的实例类别定义的所需安全策略。这是因为多云防御控制器不仅会发现已部署的新实例，还会发现已分配给该实例的标签。然后，它将使用新实例的IP地址动态更新引用此基于实例的标记的源或目标

地址对象。如果使用不正确的标签或未部署标签的实例，则不允许与任何其他资源通信，因为没有匹配相应的策略规则。

在 VNet 和 VPC 中，标签将与 VPC 关联的 CIDR 映射到地址对象 CIDR。提供创建与 VPC 或 VNET 中部署的任何实例匹配的规则的情景方式。可以使用已发现的 VPC 或 VNET 的名称来定义匹配条件，而不必手动确定与特定 VPC 或 VNET 关联的 CIDR。对 VPC 或 VNET 的任何更改都将在策略规则中动态更新，无需干预。如果删除 VPC 或 VNET 并在其位置创建新的 VPC/VNET，则即使重新使用 CIDR，该规则也将不再适用。

实例 ID

实例 ID 将与实例关联的 IP 地址映射到地址对象内的 IP 地址列表。这提供了一种为特定实例创建策略规则的上下文方法，而无需手动确定实例的配置方式。策略规则反映对实例的任何更改或其删除。请注意，策略规则不能应用于任何其他实例，即使该实例被删除并替换为具有相同配置的新实例。

安全组 (Security Group)

安全组将与安全组关联的网络接口的 IP 地址映射到地址对象内的 IP 地址列表。任何与接口相关的更改（例如向安全组添加或删除的字段）都会动态反映在地址对象内的 IP 地址列表中。这使组织能够将现有安全组与网关数据路径管道的高级安全功能保持一致。

子网 ID

子网 ID 将与子网关联的 CIDR 映射到地址对象 CIDR。这提供了一种为与特定子网 ID 关联的所有资源创建策略规则的上下文方法，而无需手动确定子网的配置方式。VPC 或 VNET 通常划分为多个子网，这些子网中部署的资源可用于不同的目的。例如，一个子网中的实例可能需要一组特定的高级安全配置文件，或者可能具有不同的流量要求。为了简化为每个子网创建不同安全规则的过程， 多云防御 允许您使用子网的名称作为匹配条件来定义策略规则。因此，每个子网都可以有唯一的策略规则和唯一的安全配置文件。对子网和子网中部署的任何实例所做的任何更改都会动态反映在策略规则中。

地理 IP

地理 IP 地址对象配置为一组地理 IP 国家/地区名称。这些对象用于根据地理位置（国家/地区）允许或阻止来自或发往 IP 地址的流量。 多云防御 与 MaxMind GeoIP2 数据库集成，用于维护更新的 GeoIP 列表。

要查看国家/地区名称和代码或 IP 地址到 GeoIP 国家/地区代码的完整列表，请访问 GeoNames 网站。

组

组地址对象配置为一组源地址或目标地址对象。组通过定义单个地址对象，然后将它们组合在一起，简化了根据组成员匹配流量所需的规则数量，从而提供了灵活性。组从组成员继承 IP、CIDR 或 FQDN 集，无论成员是静态成员、动态成员还是两者的组合。

源或目的地址对象参数

类型	模式：动态或静态	参数	必需或可选	备注
IP/CIDR/FQDN	静态	值	必需	每个地址对象的 FQDN 总数限制为 200，其中每个 FQDN 最多可解析为 400 个 IP。无论 DNS 记录的 TTL 如何，多云防御网关 都将每 60 秒执行一次 DNS 解析。
VPC/VNet ID	动态	CSP 账户	必需	
		地区	必需	
		资源组	可选	仅 Azure
		VPC/VNet ID	必需	
安全组 (Security Group)	动态	CSP 账户	必需	
		地区	必需	
		VPC/VNet ID	必需	
		资源组	可选	仅 Azure
		安全组 ID (Security Group ID)	必需	
应用安全组	动态	CSP 账户	必需	仅 Azure
		地区	必需	
		资源组	必需	
		应用安全组	必需	
实例 ID	动态	CSP 账户	必需	
		地区	必需	
		VPC/VNet ID	必需	
		资源组	可选	可选
		实例 ID	必需	

类型	模式：动态或静态	参数	必需或可选	备注
子网 ID	动态	CSP 账户	必需	
		地区	必需	
		VPC/VNet ID	必需	
		资源组	可选	仅 Azure
		子网 ID	必需	
用户定义的标签	动态	CSP 账户	可选	
		地区	可选	
		VPC/VNet ID	可选	
		资源组	可选	仅 Azure
		资源/标签/值	必需	资源和标记键值对列表。资源可以是实例、VPC/VNet、子网、负载均衡器、安全组、安全组 (Azure)。
地理 IP		值	必需	
组		Address	必填	

反向代理目标地址对象

反向代理目标地址对象被指定为反向代理服务对象中的后端目标地址。服务对象使用它来建立与应用的后端连接。应用可以是IP或FQDN形式的一个或多个应用负载均衡器或实例的地址。不同类型的反向代理目标地址对象定义如下：

静态 IP/FQDN 地址对象

IP/FQDN 地址对象配置为一组 IP 地址或 FQDN。如果配置了多个 IP 或 FQDN，则在设置后端连接时，网关会在配置的字段中处理没有优先级的地址。配置FQDN后，网关会使用DNS解析FQDN，以确定在设置后端连接时要使用的 IP 地址。

动态应用地址对象

应用地址对象配置为由其应用标记确定的单个应用负载均衡器云资源。该配置会动态填充云资源表示的一组 IP 或 FQDN，这些 IP 或 FQDN 使用 多云防御 实时资产发现功能从云账户获取。对云资源所做的任何更改都将自动反映在地址对象中。当配置产生多个IP或FQDN时，网关会在设置后端连

接时处理集合中没有优先级的字段。当配置结果为FQDN时，网关将使用DNS解析FQDN，以确定在设置后端连接时要使用的IP地址。

反向代理目标地址对象参数

类型	模式：动态或静态	参数	必需或可选	备注
IP/FQDN	静态	值	必需	
应用 (Applications)	动态	CSP 账户	必需	
		地区	必需	
		VPC/VNet ID	必需	
		资源组	可选	仅 Azure
		标签/值	必需	单标签键值对

系统对象

多云防御 提供预定义的地址对象列表，以简化策略创建。所有系统对象无法编辑或删除。如果需要修改，用户可以选择克隆系统对象。

名称	说明
Any	这表示整个 IPv4 地址空间。
any-private-rfc-1918	这表示 RFC-1918 中定义的所有 IPv4 私有地址。
互联网	这表示整个 IPv4 公共地址空间，减去私有 IPv4 地址 (RFC1918)。

创建地址对象

步骤 1 导航至 **管理** > **安全策略** > **地址**。

步骤 2 点击**创建 (Create)**。

步骤 3 选择 **源/** 目的或 **反向代理目标**。

步骤 4 输入唯一 **名称** 可标识地址对象。

步骤 5 （可选）为对象输入说明。这可以提供上下文来帮助区分对象与其他对象。

步骤 6 选择 **对象类型** 有关对象类型及其含义的信息，请参阅 地址对象, on page 1。选择以下一个类型：

- IP/CIDR/FQDN

- VPC/VNet ID
- 安全组 (Security Group)
- 应用 ID（仅限 Azure）
- 实例 ID
- 子网 ID
- 用户定义的标签
- 地理 IP
- 服务终端（云服务 IP）

步骤 7 根据您在步骤 6 中选择的类型，输入以下参数：

- **值** - 输入有效的 IP、CIDR 或 FQDN IP 地址。
- **CSP 账户** - 使用下拉菜单选择已连接到控制器的云服务提供商账户。
- **区域** - 选择您的云服务提供商所在的区域。
- **VPC** - 使用下拉菜单选择 VPC 或 VNet。请注意，可用选项可能会根据您选择的云服务提供商帐户而变化。
- **子网** - 使用下拉菜单选择适用于您的 VPC 或 VNet 的子网。
- （仅限 Azure） **资源组** - 使用下拉菜单选择与您的选择兼容的资源组。
  - **资源级别** - 使用下拉菜单选择值。
  - **资源标签** - 使用下拉菜单选择关键字作为资源标签。
  - **值** - 输入资源组的有效值。请注意，这与 IP/CIDR/FQDN 对象的 Value 条目不同。
- **地理位置 IP** - 使用下拉菜单选择与所选地理位置关联的特定 IP。
- **X-Forwarded-For Match Enabled** - 选中此框可允许网关匹配 XFF HTTP 报头字段。

步骤 8 完成后，请点击**保存**。

编辑地址对象

如果需要修改无法修改的参数，则需要 克隆地址对象 地址对象，然后根据需要更改参数。

按照以下步骤编辑地址对象。请注意，并非所有参数都可以编辑。

步骤 1 导航至 **管理** > **安全策略** > **地址**。

步骤 2 选中要 **编辑**的地址对象旁边的复选框。

步骤 3 点击**编辑**。

步骤 4 根据需要修改参数。

步骤 5 完成后，请点击**保存**。

克隆地址对象

如果希望使用副本代替原始副本，则需要将原始副本的所有关联替换为副本。关联将在一组一个或多个安全策略规则集规则或反向代理服务对象中。可以通过查看 查看详细信息来查看关联。

使用以下步骤克隆现有地址对象：

步骤 1 导航至 **管理** > **安全策略** > **地址**。

步骤 2 选中要 **克隆**的地址对象旁边的复选框。

步骤 3 点击**克隆**。

步骤 4 根据需要指定和修改参数。

步骤 5 完成后，请点击**保存**。

删除地址对象

如果在策略规则集或反向代理服务对象中主动使用某个地址对象，则该对象将再有一个关联，您将无法删除该地址对象。要删除地址对象，必须先删除所有关联，然后才能删除地址对象。可以通过查看 查看详细信息来查看关联。

步骤 1 导航至 **管理** > **安全策略** > **地址**。

步骤 2 选中要 **删除**的地址对象旁边的复选框。

步骤 3 点击**删除 (Delete)**。

步骤 4 点击 **保存** 来确认删除。

查看详细信息

您可以通过点击 **管理** > **安全** > **地址** 页面中的对象 **名称** 来查看地址对象 **详细信息** 。 **详细信息** 将显示根据其类型和配置填充的IP、CDIR和FQDN。它还将显示与策略规则集和任何对象服务的关联。

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。