VPC 防火墙规则

Virtual Private Cloud (VPC) 防火墙规则应用于给定的项目和网络。如果要将防火墙规则应用于组织中的多个 VPC 网络，请参阅防火墙政策 (https://cloud.google.com/firewall/docs/firewall-policies-overview?hl=zh-cn)。本页面的其余部分仅介绍 VPC 防火墙规则。

通过 VPC 防火墙规则，您可以允许或拒绝传入或传出 VPC 网络中的虚拟机 (VM) 实例 (https://cloud.google.com/vpc/docs/vpc?hl=zh-cn#vm-instances)的连接。无论实例的配置和操作系统如何，无论它们是否启动，系统都始终会实施 VPC 防火墙规则来保护您的实例。

每个 VPC 网络均发挥分布式防火墙的作用。虽然防火墙规则是在网络级层上定义的，但允许或拒绝连接是按具体实例执行。您可以认为，VPC 防火墙规则不仅存在于您的实例与其他网络之间，也存在于同一网络内的各个实例之间。

注意：本页面概述了防火墙规则。如需了解如何创建和使用防火墙规则，请参阅使用 VPC 防火墙规则 (https://cloud.google.com/firewall/docs/using-firewalls?hl=zh-cn)。

如需详细了解防火墙，请参阅防火墙（计算） (https://wikipedia.org/wiki/Firewall_(computing))。

防火墙规则的最佳实践

在设计和评估防火墙规则时，请谨记以下最佳实践：

- 实现最小权限 (https://en.wikipedia.org/wiki/Principle_of_least_privilege)原则。默认阻止所有流量，并且仅允许您需要的特定流量。这包括将规则限制为仅使用所需的协议和端口。
- 使用分层防火墙政策规则 (https://cloud.google.com/firewall/docs/firewall-policies?hl=zh-cn)阻止在组织或文件夹级层不允许的流量。
- 对于“允许”规则，请通过指定虚拟机的服务账号 (https://cloud.google.com/firewall/docs/firewalls?hl=zh-cn#serviceaccounts)将它们限制为仅允许特定的虚拟机。
- 如果您需要根据 IP 地址创建规则，请尝试最大限度地减少规则的数量。与分别跟踪 16 条独立规则相比，跟踪一条允许流量流向 16 个虚拟机的规则要容易得多。
- 启用防火墙规则日志记录 (https://cloud.google.com/firewall/docs/firewall-rules-logging?hl=zh-cn)，并使用防火墙数据分析

(https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/overview?hl=zh-cn)
来验证防火墙规则是否按预期方式使用。防火墙规则日志记录可能会产生费用 (https://cloud.google.com/vpc/pricing?hl=zh-cn#network-telemetry)，因此您可能需要考虑选择性地使用它。

Google Cloud 中的防火墙规则

创建 VPC 防火墙规则时，您需要指定 VPC 网络和一些组成部分，用于定义规则的作用。利用这些组成部分，您能够根据流量的协议、目的地端口、来源和目的地来定位某些类型的流量。如需了解详情，请参阅防火墙规则组成部分 (#firewall_rule_components)。

如需创建或修改 VPC 防火墙规则，您可以使用 Google Cloud 控制台 (https://console.cloud.google.com/?hl=zh-cn)、Google Cloud CLI (https://cloud.google.com/sdk/gcloud/reference/compute/firewall-rules?hl=zh-cn) 和 REST API (https://cloud.google.com/compute/docs/reference/v1/firewalls?hl=zh-cn)。创建或修改防火墙规则时，您可以使用规则的目标参数 (#rule_assignment)来指定要应用此规则的实例。如需查看防火墙规则示例，请参阅其他配置示例 (https://cloud.google.com/firewall/docs/using-firewalls?hl=zh-cn#other-config-examples)。

除了您创建的防火墙规则外，Google Cloud 还有其他规则可以影响传入（入站）或传出（出站）的连接：

- Google Cloud 会屏蔽或限制某些流量。如需了解详情，请参阅屏蔽和受限的流量 (#blockedtraffic)。
- Google Cloud 始终允许虚拟机实例与其对应的元数据服务器（位于 `169.254.169.254`）之间的通信。如需了解详情，请参阅始终允许的流量 (#alwaysallowed)。
- 每个网络都有两条隐式防火墙规则 (#default_firewall_rules)，分别允许传出连接和禁止传入连接。您创建的防火墙规则可以覆盖这些隐式规则。
- 默认网络预先填充了一些防火墙规则 (#more_rules_default_vpc)，您可以删除或修改这些规则。

规范

VPC 防火墙规则具有以下特征：

- 每条防火墙规则均应用于传入（入站流量）或传出（出站流量）连接，但不能同时应用于两者。如需了解详情，请参阅连接方向 (#direction_of_the_rule)。

- 防火墙规则支持 IPv4 连接。已启用 IPv6 (https://cloud.google.com/vpc/docs/subnets?hl=zh-cn#ipv6-ranges) 的 VPC 网络也支持 IPv6 连接。按地址指定入站流量或出站流量规则的来源或目的地时，可以采用 CIDR 表示法指定 IPv4 或 IPv6 地址或地址块。
- 每条防火墙规则可以包含 IPv4 或 IPv6 范围，但不能同时包含两者。
- 每条防火墙规则执行的操作均为 `allow` 或 `deny` (#action_of_the_rule) 之一。只要实施 (#enforcement)了防火墙规则，该规则就会应用于连接。例如，您可以停用某一条规则，以进行问题排查。
- 创建防火墙规则时，必须选择 VPC 网络。虽然规则是在实例级层实施，但其配置与 VPC 网络相关联。这意味着您无法在 VPC 网络之间共享防火墙规则，包括通过 VPC 网络对等互连 (https://cloud.google.com/vpc/docs/vpc-peering?hl=zh-cn)或使用 Cloud VPN 隧道 (https://cloud.google.com/network-connectivity/docs/vpn/concepts/choosing-networks-routing?hl=zh-cn#dynamic-routing) 连接的网络。
- VPC 防火墙规则是有状态 (https://wikipedia.org/wiki/Stateful_firewall)的：
    - 如果允许通过任一方向的防火墙进行连接，则也允许与此连接匹配的返回流量。您不能将防火墙规则配置为拒绝关联的响应流量。
    - 返回流量必须与已接受的请求流量的 5 元组（来源 IP、目标 IP、源端口、目标端口、协议）匹配，但来源地址和目标地址以及来源端口和目标端口会被对调。
    - Google Cloud 会使用连接跟踪表，将传入数据包与相应的出站数据包相关联。IPv4 连接支持 TCP、UDP、SCTP 和 ICMP 协议。IPv6 连接支持 TCP、UDP、SCTP 和 ICMPv6 协议。
    - 无论所用协议是否支持连接，Google Cloud 都会实施连接跟踪。如果来源与目标之间（针对入站规则）或目标与目的地之间（针对出站规则）允许建立连接，只要防火墙的连接跟踪状态为活跃状态，则所有响应流量都允许通过。如果每 10 分钟至少发送一个数据包，则视为防火墙规则的跟踪状态为活跃状态。
    - 如果防火墙允许分段连接，则 Google Cloud 会使用连接跟踪，以仅允许返回流量的第一个片段。如需允许后续的返回片段，您必须添加防火墙规则。
    - 通过防火墙允许生成 ICMP 响应流量，例如，生成允许的“ICMP TYPE 3, DESTINATION UNREACHABLE”以响应允许的 TCP/UDP 连接。此行为与 RFC 792 (https://tools.ietf.org/html/rfc792) 一致。
- VPC 防火墙规则不会重组分段的 TCP 数据包。因此，适用于 TCP 协议的防火墙规则只能应用于第一个分段，因为其中包含 TCP 标头。适用于 TCP 协议的防火墙规则不适用于后续的 TCP 分段。

- 防火墙规则表中跟踪的最大连接数取决于实例的机器类型支持的有状态连接数。 如果超出跟踪连接数上限，则系统将停止跟踪具有最长空闲间隔的连接，以便跟踪新连接。

实例机器类型	有状态连接的最大数量
共享核心机器类型 (https://cloud.google.com/compute/docs/machine-types?hl=zh-cn#sharedcore)	130000 个
具有 1-8 个 vCPU 的实例	每个 vCPU 130000 个连接
具有 8 个以上 vCPU 的实例	总共 1040000 (130000×8) 个连接

隐式规则

每个 VPC 网络都有两条隐式 IPv4 防火墙规则。如果在 VPC 网络中启用了 IPv6，则该网络还具有两条隐式 IPv6 防火墙规则。这些规则不会显示在 Google Cloud 控制台中。

隐式 IPv4 防火墙规则存在于所有 VPC 网络中，无论 VPC 网络是如何创建的，也无论 VPC 网络是自动模式还是自定义模式 (https://cloud.google.com/firewall/docs/vpc?hl=zh-cn#subnet-ranges)。默认网络具有相同的隐式规则。

- 隐式 **IPv4** 允许出站流量规则。这条出站规则的操作为 `allow`、目的地为 `0.0.0.0/0`，且优先级为可能的最低优先级 (`65535`)。它允许任何实例向任何目的地发送流量，但不包括 Google Cloud 禁止 (#blockedtraffic)的流量。出站访问可能受更高优先级的防火墙规则限制。如果没有其他防火墙规则拒绝出站流量，并且实例具有外部 IP 地址或使用 Cloud NAT 实例，则允许访问互联网。如需了解详情，请参阅互联网访问要求 (https://cloud.google.com/vpc/docs/vpc?hl=zh-cn#internet_access_reqs)。
- 隐式 **IPv4** 拒绝入站流量规则。这条入站规则的操作为 `deny`、来源为 `0.0.0.0/0`，且优先级为可能的最低优先级 (`65535`)，它通过禁止发往所有实例的连接来保护所有实例。入站访问可能会被更高优先级的规则所允许。默认网络包含的一些额外规则 (#more_rules_default_vpc)会替换此规则，从而允许某些类型的传入连接。

如果启用了 IPv6，则 VPC 网络还具有以下两条隐式规则：

- 隐式 **IPv6** 允许出站流量规则。这条出站规则的操作为 `allow`、目的地为 `::/0`，且优先级为可能的最低优先级 (`65535`)。它允许任何实例向任何目的地发送流量，但不包括 Google Cloud 禁止 (#blockedtraffic)的流量。出站访问可能受更高优先级的防火墙规则限制。如果没有其他防火墙规则拒绝出站流量，并且实例具有外部 IP 地址，则允许访问

互联网。

- 隐式 **IPv6** 拒绝入站流量规则。这条入站规则的操作为 deny、来源为 `::/0`，且优先级为可能的最低优先级 (65535)，它通过禁止发往所有实例的连接来保护所有实例。入站访问可能会被更高优先级的规则所允许。

隐式规则不能移除，但它们有着可能限度内的最低优先级。只要您的规则具有更高的优先级（优先级数字小于 65535），您创建的规则就可以覆盖这些规则。由于 deny 规则的优先级高于同优先级的 allow 规则，因此优先级为 65535 的入站 allow 规则永远不会生效。

默认网络中预先填充的规则

默认网络预先填充了一些允许连接传入实例的防火墙规则。这些规则可以根据需要删除或修改：

规则名称	方向	优先级	来源范围	操作	协议和端口	说明
default-allow-internal	ingress	65534	10.128.0.0/9	allow	tcp:0-65535 udp:0-65535 icmp	允许从同一 VPC 网络内的其他实例到虚拟机实例的传入连接。
default-allow-ssh	ingress	65534	0.0.0.0/0	allow	tcp:22	允许您使用 ssh、scp 或 sftp 等工具连接到实例。
default-allow-rdp	ingress	65534	0.0.0.0/0	allow	tcp:3389	允许您使用 Microsoft 远程桌面协议 (RDP) 连接到实例。
default-allow-icmp	ingress	65534	0.0.0.0/0	allow	icmp	允许您使用 ping 等工具。

您可以为默认网络以外的网络创建类似的防火墙规则。如需了解详情，请参阅为常见使用场景配置防火墙规则
(https://cloud.google.com/firewall/docs/using-firewalls?hl=zh-cn#rules-for-common-use-cases)。

屏蔽和受限的流量

Google Cloud 与 VPC 防火墙规则和分层防火墙政策分开，会屏蔽或限制下表中所述的特定流量。

流量类型	详情

数据包速率和带宽 适用对象： • 所有出站数据包 • 所有入站数据包	针对每个网络接口 (NIC) 或 IP 地址，Google Cloud 按每个虚拟机实例考虑带宽。虚拟机的机器类型 (https://cloud.google.com/compute/docs/machine-types?hl=zh-cn) 定义了其可能的最大出站流量速率。但是，您只能在特定情况下达到此最大出站流量速率。 如需了解详情，请参阅 Compute Engine 文档中的网络带宽 (https://cloud.google.com/compute/docs/network-bandwidth?hl=zh-cn) 。
DHCP 提供和确认 适用对象： • 发送到 UDP 端口 68 (DHCPv4) 的入站数据包 • 发送到 UDP 端口 546 (DHCPv6) 的入站数据包	Google Cloud 会屏蔽来自所有来源的传入 DHCP 提供和确认，但来自元数据服务器 (#gcp-metadata-server)的 DHCP 数据包除外。
Google Cloud 外部 **IP** 地址支持的协议 适用对象： • 发送到外部 IP 地址的入站数据包	外部 IPv4 和 IPv6 地址仅接受 TCP、UDP、ICMP、IPIP、AH、ESP、SCTP 和 GRE 数据包。使用外部 IP 地址的资源会施加额外的协议限制： • 用于协议转发、外部应用负载均衡器 (https://cloud.google.com/load-balancing/docs/https?hl=zh-cn)、外部代理网络负载均衡器 (https://cloud.google.com/load-balancing/docs/tcp?hl=zh-cn)和外部直通式网络负载均衡器 (https://cloud.google.com/load-balancing/docs/network?hl=zh-cn) 的转发规则仅处理转发规则中配置的协议 (https://cloud.google.com/load-balancing/docs/forwarding-rule-concepts?hl=zh-cn#protocol-specifications) 和端口 (https://cloud.google.com/load-balancing/docs/forwarding-rule-concepts?hl=zh-cn#port_specifications) 。 • Cloud VPN (https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview?hl=zh-cn) 网关仅接受 VPN 协议 (https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview?hl=zh-cn#specifications) 。

SMTP（端口 25）流量 适用对象： • 发送到 TCP 端口 25 上的外部 IP 地址的出站数据包	默认情况下，Google Cloud 会阻止发送到外部 IP 地址（包括其他 Google Cloud 资源的外部 IP 地址）的 TCP 目的地端口 25 的出站数据包。但在部分 Google Cloud 客户拥有的项目中，此流量不会被阻止。在 Google Cloud 控制台中，VPC 网络页面 (https://console.cloud.google.com/networking/networks/list?hl=zh-cn) 和防火墙政策页面 (https://console.cloud.google.com/net-security/firewall-manager/firewall-policies/list?hl=zh-cn) 均会显示一条消息，指示您的项目是允许还是禁止 SMTP 端口 25。 此地址块不适用于发送到内部 IP 地址（包括 VPC 网络或本地网络中以非公开方式使用的公共 IP 地址）的 TCP 目的地端口 25 的出站数据包。 如果项目中允许端口 25 上的外部 SMTP 出站流量，并且您想要发送此类流量，则必须满足以下其他条件： • VPC 网络中的出站防火墙规则和适用于 VPC 网络的分层防火墙政策必须允许流向 TCP 端口 25 上的外部 IP 地址的出站流量。隐式允许出站规则 (#default_firewall_rules)符合此要求，因为它们允许流向任何 IP 地址的出站流量（以及来自任何 IP 地址的已建立的入站响应）。 • 目的地适用的路由必须使用默认互联网网关的下一个跃点。系统生成的默认路由 (https://cloud.google.com/vpc/docs/routes?hl=zh-cn#routingpacketsinternet) 符合此要求。 • 将数据包发送到外部 IP 地址的实例必须符合互联网访问要求 (https://cloud.google.com/vpc/docs/vpc?hl=zh-cn#internet_access_reqs) 。 您可以通过创建出站拒绝 VPC 防火墙规则或分层防火墙政策来阻止外部 SMTP 出站流量。

始终允许的流量

对于虚拟机实例，VPC 防火墙规则和分层防火墙政策 (https://cloud.google.com/firewall/docs/firewall-policies?hl=zh-cn)不适用于以下情况：

- 向 Google Cloud 元数据服务器发送和从其中接收的数据包 (#gcp-metadata-server)
- 数据包已发送到实例本身的网络接口 (NIC) 之一的 IP 地址，其中数据包保留在虚拟机本身中。分配给实例的 NIC 的 IP 地址包括：

- NIC 的主要内部 IPv4 地址
- NIC 的别名 IP 范围 (https://cloud.google.com/vpc/docs/alias-ip?hl=zh-cn)中的任何内部 IPv4 地址
- 如果在子网上配置 IPv6，则为分配给 NIC 的任何 IPv6 地址
- 用于负载均衡或协议转发的与转发规则相关联的内部或外部 IPv4 地址（如果实例是负载均衡器的后端或协议转发的目标实例）
- 环回地址
- 配置为在实例本身中运行的网络叠加软件的一部分的地址

Google Cloud 元数据服务器

Google Cloud 会在 `169.254.169.254` 与每个实例一起运行一个本地元数据服务器。此服务器对于实例的操作至关重要，无论您配置何种防火墙规则，实例都可以访问此服务器。元数据服务器为实例提供以下基本服务：

- DHCP (https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)
- DNS 解析：按照 VPC 网络的 DNS 名称解析顺序 (https://cloud.google.com/dns/docs/vpc-name-res-order?hl=zh-cn)进行解析。
- 实例元数据 (https://cloud.google.com/compute/docs/storing-retrieving-metadata?hl=zh-cn)
- 网络时间协议 (NTP) (https://en.wikipedia.org/wiki/Network_Time_Protocol)

产品交互

以下部分介绍了防火墙规则和分层防火墙政策如何与其他 Google Cloud 产品交互。

防火墙规则和直通式负载均衡器

VPC 防火墙规则和分层防火墙政策可以控制允许将转发规则支持的哪些协议和端口用于访问直通式负载均衡器的后端。有关详情，请参阅：

- 外部直通式网络负载均衡器文档中的防火墙规则 (https://cloud.google.com/load-balancing/docs/network/networklb-backend-service?hl=zh-cn#firewall_rules)
- 内部直通式网络负载均衡器文档中的防火墙规则 (https://cloud.google.com/load-balancing/docs/internal?hl=zh-cn#firewall_rules)

防火墙规则和代理负载均衡器

对于外部应用负载均衡器、内部应用负载均衡器、内部代理网络负载均衡器和外部代理网络负载均衡器，VPC 防火墙规则和分层防火墙政策不会控制代理负载均衡器的转发规则 IP 地址接受哪些协议和端口。转发规则单独可确定代理负载均衡器接受哪些协议和端口。

VPC 防火墙规则和分层防火墙政策可以控制这些代理负载均衡器如何与其后端通信。如需了解详情，请参阅：

- 外部应用负载均衡器文档中的防火墙规则 (https://cloud.google.com/load-balancing/docs/https?hl=zh-cn#firewall-rules)
- 内部应用负载均衡器文档中的防火墙规则 (https://cloud.google.com/load-balancing/docs/l7-internal?hl=zh-cn#firewall_rules)
- 内部代理网络负载均衡器文档中的防火墙规则 (https://cloud.google.com/load-balancing/docs/tcp/internal-proxy?hl=zh-cn#firewall_rules)
- 外部代理网络负载均衡器文档中的防火墙规则 (https://cloud.google.com/load-balancing/docs/tcp?hl=zh-cn#firewall-rules)

防火墙规则和 Cloud VPN

防火墙规则和分层防火墙政策不会控制 Cloud VPN 网关接受哪些协议和端口。

Cloud VPN 网关仅接受 Cloud VPN 规范 (https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview?hl=zh-cn#specifications) 中所述的协议和端口的数据包。

防火墙规则和 GKE

当您在集群中创建集群或资源（包括 Service 和 Ingress）时，Google Kubernetes Engine 会自动创建和管理防火墙规则。如需了解详情，请参阅 Google Kubernetes Engine 文档中的自动创建的防火墙规则 (https://cloud.google.com/kubernetes-engine/docs/concepts/firewall-rules?hl=zh-cn)。

防火墙规则组件

每条防火墙规则均由以下配置组件组成：

- 从目标的角度来看的方向 (#direction_of_the_rule)。方向可以是入站或出站。

- 数字形式的优先级 (#priority_order_for_firewall_rules)，用于确定是否应用规则。仅应用其他组件与流量匹配的最高优先级（优先级编号最小）规则；优先级较低并且与此规则存在冲突的规则会被忽略。
- 对匹配项执行的操作 (#action_of_the_rule)，要么是 `allow`，要么是 `deny`，用于确定规则是允许还是禁止连接。
- 防火墙规则的实施状态 (#enforcement)：您可以启用和停用防火墙规则，而无需删除这些规则。
- 一个目标 (#rule_assignment)，定义了哪些实例（包括 GKE 集群和 App Engine 柔性环境实例）将应用该规则。
- 数据包特征的来源或目的地 (#sources_or_destinations_for_the_rule)过滤条件。
- 协议 (#protocols_and_ports)（例如 TCP、UDP 或 ICMP）和目的地端口。
- 布尔值日志 (https://cloud.google.com/firewall/docs/firewall-rules-logging?hl=zh-cn)选项，用于将与规则匹配的连接记录到 Cloud Logging 中。

组件汇总

入站规则

优先级	操作	政策执行	目标参数	来源和目标过滤条件	协议和端口
从 `0` 到 `65535` 的整数（含边界值）；默认为 `1000`	`allow` 或 `deny`	`enabled`（默认）或 `disabled`	指定接收数据包的实例。	入站流量规则的来源 (#source_parameter_ingress_rule) 入站流量规则的目的地 (#destination_parameter_ingress_rule)	指定协议，或者同时指定协议和目标端口。 如果未设置，则该规则适用于所有协议和目标端口。 如需了解详情，请参阅协议和端口 (#protocols_and_ports)。

出站规则

优先级	操作	政策执行	目标参数	来源和目标过滤条件	协议和端口
从 `0` 到 `65535` 的整数（含边界值）；默认为	`allow` 或 `deny`	`enabled`（默认）或 `disabled`	指定发送数据包的实例。	出站流量规则的来源 (#source_parameter_egress_rule) 出站流量规则的目的地 (#destination_parameter_egress_rule)	指定协议，或者同时指定协议和目标端口。 如果未设置，则该规则适用于所有协议和目标端口。 如需了解详情，

`1000`	请参阅协议和端口 (#protocols_and_ports)。

流量方向

您可以创建应用于入站流量或出站流量的防火墙规则；但是单个规则不能同时应用于入站流量和出站流量。不过，您可以创建多条规则来定义允许或拒绝通过防火墙的入站流量和出站流量。

- 入站流量（传入）描述进入目标 (#rule_assignment)的网络接口的数据包。
- 出站流量（传出）描述离开目标 (#rule_assignment)的网络接口的数据包。
- 如果您未指定方向，Google Cloud 将使用入站方向。

优先级

防火墙规则优先级是一个从 `0` 到 `65535` 的整数（含边界值）。数字越小，优先级越高。如果您在创建规则时未指定优先级，系统会为其分配优先级 `1000`。

在评估不同的防火墙规则时，防火墙规则的相对优先级决定其应用与否。评估逻辑的工作原理如下：

- 针对给定类型的流量，在适用于目标的规则中，将应用优先级最高的规则。目标特异性并不重要。例如，如果一条针对所有目标且适用于特定目的地端口和协议的入站规则优先级较高，则它会覆盖具有类似定义且适用于相同目的地端口和协议但针对特定目标的较低优先级规则。
- 针对给定协议和目的地端口定义，将应用优先级最高的规则，即便协议和目的地端口定义更宽泛。例如，如果一条入站规则允许发往给定目标的所有协议和目的地端口的流量，而其优先级较高，则会覆盖针对同一目标但拒绝 TCP 22 端口的优先级较低的入站规则。
- 只有在两条规则的优先级相同时，操作为 `deny` 的规则才会覆盖另一条操作为 `allow` 的规则。使用相对优先级，可以构建覆盖 `deny` 规则的 `allow` 规则，也可以构建覆盖 `allow` 规则的 `deny` 规则。
- 具有相同优先级和相同操作的规则具有相同的结果。但是，评估期间使用的规则是不确定的。通常，除非您启用防火墙规则日志记录 (https://cloud.google.com/firewall/docs/firewall-rules-logging?hl=zh-cn)，否则使用哪个规则无关紧要。如果您希望日志按照一致且明确定义的顺序显示评估的防火墙规则，请为它们分配唯一的优先级。

考虑下面的例子，其中存在两条防火墙规则：

- 来自来源 `0.0.0.0/0`（任何 IPv4 地址）的入站流量规则适用于所有目标、所有协议和所有目的地端口，其操作为 `deny`，优先级为 `1000`。
- 来自来源 `0.0.0.0/0`（任何 IPv4 地址）的入站流量规则适用于具有网络标记 `webserver` 的特定目标，针对 TCP 80 端口上的流量，操作为 `allow`。

第二条规则的优先级决定了针对 `webserver` 目标，是否允许流向端口 80 的 TCP 流量：

- 如果第二条规则的优先级设置为大于 `1000` 的数字，则该规则的优先级较低，因此系统将应用拒绝所有流量的第一条规则。
- 如果第二条规则的优先级设置为 `1000`，则两条规则的优先级相同，因此系统将应用拒绝所有流量的第一条规则。
- 如果第二条规则的优先级设置为小于 `1000` 的数字，则该规则的优先级较高，因此允许 TCP 80 端口上发送到 `webserver` 目标的流量。如果没有其他规则，第一条规则仍会拒绝发送到 `webserver` 目标的其他类型的流量，以及发送到不带 `webserver` 网络标记的实例的所有流量（包括 TCP 80 端口上的流量）。

前面的示例演示了如何使用优先级来创建选择性的 `allow` 规则和全局 `deny` 规则，以实现最小权限最佳安全做法。

注意：每个网络都有两条不可移除、低优先级、隐式防火墙规则，而默认网络还具有额外的可移除防火墙规则。如需了解详情，请参阅默认规则和隐式规则 (#default_firewall_rules)。

对匹配项执行的操作

防火墙规则的操作组件会根据该规则的其他组件来确定是允许还是禁止流量：

- `allow` 操作允许与其他指定组件匹配的连接。
- `deny` 操作禁止与其他指定组件匹配的连接。

注意：一条防火墙规则只能有一个操作组件。不能在同一条规则中同时指定 **`allow`** 和 **`deny`**。您可以分别创建多条具有不同优先级的防火墙规则，以定义这些规则的应用顺序。

强制执行

您可以通过将一条防火墙规则的状态设置为 `enabled` 或 `disabled`，选择是否实施该防火墙规则。您可以在创建规则

(https://cloud.google.com/firewall/docs/using-firewalls?hl=zh-cn#creating_firewall_rules)或更新规则(https://cloud.google.com/firewall/docs/using-firewalls?hl=zh-cn#updating_firewall_rules)时设置实施状态。

如果您在创建新的防火墙规则时未设置实施状态，则防火墙规则会自动为 `enabled`。

使用场景

启用和停用规则对问题排查和执行维护非常有用。在以下情况下，请考虑更改防火墙规则的实施：

- 问题排查：结合使用防火墙规则日志记录(https://cloud.google.com/firewall/docs/firewall-rules-logging?hl=zh-cn)，您可以暂时停用防火墙规则，以确定相应规则是负责阻止流量还是允许流量。这对于为同一流量应用多个防火墙规则的情况非常有用。停用和启用规则比删除并重新创建规则更有用，因为规则的其他组成部分不会丢失。
- 维护：停用防火墙规则可以简化定期维护。例如，您可以选择启用入站防火墙规则，仅允许在您需要使用 SSH 执行维护时访问。在不执行维护时，您可以停用规则。

对现有流量的影响

如果更改防火墙规则的实施状态，或者创建已`enforced`的新规则，则更改仅适用于新连接。现有连接不受此更改的影响。

协议和端口

您可以通过指定协议或者同时指定协议和目的地端口来缩小防火墙规则的范围。您可以指定一个协议，也可以指定协议及其目的地端口的组合。如果同时省略协议和端口，防火墙规则将适用于任何协议和任何目的地端口上的所有流量。系统不支持基于来源端口的规则。

并非所有协议都支持端口。例如，存在 TCP 和 UDP 端口，但不存在 ICMP 端口。ICMP 确实具有不同的 ICMP 类型，但它们不是端口，不能在防火墙规则中指定。

您可以在防火墙规则中使用以下协议名称：`tcp`、`udp`、`icmp`（适用于 IPv4 ICMP）、`esp`、`ah`、`sctp`、`ipip`。对于所有其他协议，您必须使用 IANA 协议编号(http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml)。

许多协议在 IPv4 和 IPv6 中使用相同的名称和编号，但某些协议（如 ICMP）并非如此。

防火墙规则不支持 IPv6 逐跳协议。

下表汇总了 Google Cloud 防火墙规则的有效协议和目的地端口指定组合。

指定	示例	说明
无协议和端口	-	如果未指定协议，防火墙规则适用于所有协议及其适用目的地端口。
协议	`tcp`	如果指定的协议不包含任何端口信息，防火墙规则适用于该协议及其所有适用端口。
协议和一个端口	`tcp:80`	如果指定了一个协议和一个目的地端口，防火墙规则适用于该协议的该目的地端口。
协议和端口范围	`tcp:20-22`	如果指定了协议和端口范围，防火墙规则适用于该协议的目的地端口范围。

组合	`icmp,tcp:80`
	`tcp:443`
	`udp:67-69`
		您可以指定防火墙规则适用的多种协议和目的地端口的组合。如需了解详情，请参阅创建防火墙规则 (https://cloud.google.com/firewall/docs/using-firewalls?hl=zh-cn#creating_firewall_rules)。

重要提示：端口不能单独指定。如果仅指定一个数字，Google Cloud 会将其解读为十进制 IP 协议。例如，如果您仅指定了 **`80`**，Google Cloud 会将其解读为 IP 协议 **`80`** (ISO-IP)，这与 TCP 端口 80 (**`tcp:80`**) 并不相同。

目标、来源、目的地

目标标识防火墙规则适用的实例的网络接口。

您可以为入站流量和出站流量防火墙规则同时指定适用于数据包来源或目的地的来源和目的地参数。防火墙规则的方向决定了来源和目的地参数的可能值。

目标参数

目标参数用于标识 Compute Engine 实例（包括 GKE 节点和 App Engine 柔性环境实例）的网络接口。

您可以为入站流量或出站流量规则定义以下目标。目标、来源和目的地参数按照来源、目的地的、目标 (#sources_or_destinations_for_the_rule)中的说明协同工作。

- 默认目标 **- VPC** 网络中的所有实例。如果省略目标规范，防火墙规则将应用于 VPC 网

络中的所有实例。

- 目标网络标记指代的实例。防火墙规则仅适用于 VPC 网络中具有匹配网络标记 (https://cloud.google.com/vpc/docs/add-remove-network-tags?hl=zh-cn)的实例。如需了解您可以对每项防火墙规则应用的目标网络标记数量的上限，请参阅 VPC 资源配额 (https://cloud.google.com/vpc/docs/quota?hl=zh-cn#per_network)。
- 目标服务账号指代的实例。防火墙规则仅适用于 VPC 网络中使用特定服务账号 (#serviceaccounts)的实例。如需了解您可以对每项防火墙规则应用的目标服务账号数量的上限，请参阅 VPC 配额 (https://cloud.google.com/vpc/docs/quota?hl=zh-cn#per_network)。

如需了解目标网络标记和目标服务账号的优势和限制，请参阅按服务账号过滤与按网络标记过滤 (#service-accounts-vs-tags)。

入站规则的目标和 IP 地址

路由到目标虚拟机的网络接口的数据包将根据以下条件进行处理：

- 如果入站流量防火墙规则包含目的地 IP 地址范围，则数据包的目的地必须在其中一个明确定义的目的地 IP 地址范围内。
- 如果入站流量防火墙规则不包含目的地 IP 地址范围，则数据包的目的地必须与以下 IP 地址之一匹配：
    - 分配给实例的 NIC 的主要内部 IPv4 地址。
    - 实例的 NIC 上任何已配置的别名 IP 地址范围 (https://cloud.google.com/vpc/docs/alias-ip?hl=zh-cn)。
    - 与实例的 NIC 关联的外部 IPv4 地址。
    - 如果在子网上配置 IPv6，则为分配给 NIC 的任何 IPv6 地址。
    - 与用于直通式负载均衡的转发规则关联的内部或外部 IP 地址，其中实例是内部直通式网络负载均衡器或外部直通式网络负载均衡器的后端。
    - 与用于协议转发的转发规则关联的内部或外部 IP 地址，其中该实例由目标实例引用。
    - 将实例用作下一个跃点虚拟机（`next-hop-instance` 或 `next-hop-address`）的自定义静态路由的目标范围内的 IP 地址。
    - 使用内部直通式网络负载均衡器 (`next-hop-ilb`) 的下一个跃点的自定义静态路由目标范围内的 IP 地址（如果虚拟机是该负载均衡器的后端）。

出站规则的目标和 IP 地址

从目标的网络接口发出的数据包的处理取决于目标虚拟机上的 IP 转发 (https://cloud.google.com/vpc/docs/using-routes?hl=zh-cn#canipforward)配置。IP 转发默认处于停用状态。

- 当目标虚拟机停用 IP 转发时，该虚拟机可以发送具有以下来源的数据包：
  - 实例的 NIC 的主要内部 IPv4 地址。
  - 实例的 NIC 上任何已配置的别名 IP 地址范围。
  - 如果在子网上配置 IPv6，则为分配给 NIC 的任何 IPv6 地址。
  - 与用于直通式负载均衡或协议转发的转发规则相关联的内部或外部 IP 地址（如果实例是内部直通式网络负载均衡器、外部直通式网络负载均衡器的后端或由目标实例引用）。

  如果出站流量防火墙规则包含来源 IP 地址范围，则目标虚拟机仍然仅限于之前提到的来源 IP 地址，但来源参数可用于优化该集合（预览版功能 (https://cloud.google.com/products?hl=zh-cn#product-launch-stages)）。如果在未启用 IP 转发的情况下使用来源参数，则系统不会扩展可能的数据包来源地址集。

  如果出站流量防火墙规则不包含来源 IP 地址范围，则允许之前提到的所有来源 IP 地址。
- 当目标虚拟机启用 IP 转发时，该虚拟机可以发送具有任意来源地址的数据包。您可以使用来源参数更精确地定义允许的数据包来源集。

来源参数

来源参数值取决于防火墙规则的方向。

入站流量规则的来源

您可以将以下来源用于入站流量防火墙规则：

- 默认来源范围：如果您在入站流量规则中省略来源规范，则 Google Cloud 会使用默认来源 IPv4 地址范围 `0.0.0.0/0`（任何 IPv4 地址）。默认值不包含 IPv6 来源。
- 来源 **IPv4** 范围：采用 CIDR 格式的 IPv4 地址列表。
- 来源 **IPv6** 范围：采用 CIDR 格式的 IPv6 地址列表。
- 来源网络标记：一个或多个网络标记 (https://cloud.google.com/vpc/docs/add-remove-network-tags?hl=zh-cn)，用于标识与防火墙

规则位于同一 VPC 网络中的虚拟机实例的网络接口。如需了解每条防火墙规则的来源网络标记数上限，请参阅 VPC 资源配额 (https://cloud.google.com/vpc/docs/quota?hl=zh-cn#per_network)。如需详细了解使用此隐式来源规范时的数据包来源地址，请参阅来源网络标记和来源服务账号如何表示数据包来源 (#sources-and-ips)。

- 来源服务账号：一个或多个服务账号 (#serviceaccounts)，用于标识与防火墙规则位于同一 VPC 网络中的虚拟机实例的网络接口。如需了解每条防火墙规则的来源服务账号数量上限，请参阅 VPC 资源配额 (https://cloud.google.com/vpc/docs/quota?hl=zh-cn#per_network)。如需详细了解使用此隐式来源规范时的数据包来源地址，请参阅来源网络标记和来源服务账号如何表示数据包来源 (#sources-and-ips)。
- 有效的来源组合：对于以下所有组合，有效来源集是明确指定的 IPv4 或 IPv6 地址与来源网络标记或来源服务账号隐含的 IP 地址范围的并集：
    - 来源 IPv4 范围和来源网络标记的组合。
    - 来源 IPv6 范围和来源网络标记的组合。
    - 来源 IPv4 范围和来源服务账号的组合。
    - 来源 IPv6 范围和来源服务账号的组合。

重要提示：不能在同一条防火墙规则中同时使用网络标记和服务账号。如需了解详情，请参阅按服务账号过滤与按网络标记过滤 (#service-accounts-vs-tags)。

来源网络标记和来源服务账号如何表示数据包来源

如果入站流量防火墙规则使用来源网络标记，则数据包必须从满足以下条件的网络接口发出：

- 网络接口使用与防火墙规则相同的 VPC 网络。
- 网络接口与某个虚拟机相关联，该虚拟机具有与防火墙规则的来源网络标记匹配的网络标记。

如果入站流量防火墙规则使用来源服务账号，则数据包必须从满足以下条件的网络接口发出：

- 网络接口使用与防火墙规则相同的 VPC 网络。
- 网络接口与某个虚拟机相关联，该虚拟机具有与防火墙规则的来源服务账号匹配的服务账号。

除了指定网络接口之外，当入站流量防火墙规则使用来源网络标记或来源服务账号时，从虚拟机的网络接口发出的数据包必须使用以下有效来源 IP 地址之一：

- 该网络接口的主要内部 IPv4 地址。
- 分配给该网络接口的任何 IPv6 地址。

如果入站流量防火墙规则还包含目标 IP 地址范围 (#destination_parameter_ingress_rule)，则绑定到网络标记的网络接口将解析为与目标 IP 地址范围相同的 IP 版本。

使用来源网络标记或来源服务账号时，不隐含其他数据包来源 IP 地址。例如，与网络接口关联的别名 IP 地址范围和外部 IPv4 地址会被排除。如果您需要创建来源包含别名 IP 地址范围或外部 IPv4 地址的入站流量防火墙规则，请使用来源 IPv4 范围。

出站流量规则的来源

您可以针对出站流量防火墙规则使用以下来源：

- 默认 - 由目标决定。如果在出站流量规则中省略来源参数，则数据包来源会隐式定义，如出站流量规则的目标和 IP 地址 (#targets_and_ips_egress)中所述。
- 来源 **IPv4** 范围。CIDR 格式的 IPv4 地址列表。
- 来源 **IPv6** 范围。CIDR 格式的 IPv6 地址列表。

请遵循以下准则来为出站流量规则添加来源 IP 地址范围：

- 如果虚拟机接口同时分配了内部和外部 IPv4 地址，则规则评估期间仅使用内部 IPv4 地址。
- 如果您在出站流量规则中同时指定来源参数和目标参数，请对这两个参数使用相同的 IP 版本。您可以使用 IPv4 地址范围或 IPv6 地址范围，但不能同时使用两者。如需了解详情，请参阅出站流量规则的目的地 (#destination_parameter_egress_rule)。

目的地参数

您可以使用入站流量规则和出站流量规则均支持的 IP 地址范围来指定目的地。默认目的地行为取决于规则的方向。

入站流量规则的目的地

您可以将以下目的地用于入站流量防火墙规则：

- 默认 - 由目标决定。如果在入站流量规则中省略目的地参数，则数据包目的地将隐式定

义，如入站流量规则的目标和 IP 地址 (#targets_and_ips_ingress)中所述。

- 目的地 **IPv6** 范围。CIDR 格式的 IPv4 地址列表。
- 目的地 **IPv6** 范围。CIDR 格式的 IPv6 地址列表。

请遵循以下准则为入站流量规则添加目标 IP 地址范围：

- 如果虚拟机接口同时分配了内部和外部 IPv4 地址，则规则评估期间仅使用内部 IPv4 地址。
- 如果您在入站流量规则中同时指定来源参数和目标参数，则来源参数将解析为目标 IP 地址范围所在的 IP 版本。如需详细了解如何为入站流量规则定义来源，请参阅入站规则的来源 (#source_parameter_ingress_rule)。

出站流量规则的目的地

您可以将以下目的地用于出站流量防火墙规则：

- 默认目的地范围。如果在出站流量规则中省略目的地规范，则 Google Cloud 会使用默认目的地 IPv4 地址范围 `0.0.0.0/0`（任何 IPv4 地址）。默认值不包含 IPv6 目的地。
- 目的地 **IPv6** 范围。CIDR 格式的 IPv4 地址列表。
- 目的地 **IPv6** 范围。CIDR 格式的 IPv6 地址列表。

按服务账号过滤来源和目标

您可以使用服务账号 (https://cloud.google.com/iam/docs/service-accounts?hl=zh-cn)创建更具体的防火墙规则：

- 对于入站和出站规则，您可以使用服务账号指定目标。
- 对于入站规则，您可以将传入数据包的来源指定为网络（其中的虚拟机使用特定服务账号）中任何虚拟机的主要内部 IP 地址。

您必须先在防火墙规则所在的项目中创建 (https://cloud.google.com/iam/docs/creating-managing-service-accounts?hl=zh-cn)服务账号，然后再创建依赖该服务账号的防火墙规则。尽管系统不会阻止您创建使用来自其他项目的服务账号的规则，但是如果防火墙规则项目中不存在该服务账号，则不会强制执行该规则。

注意：您不能在 VPC 防火墙规则中使用 Workload Identity (https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity?hl=zh-cn) 服务账号进行

来源和目标过滤。

使用服务账号识别实例的防火墙规则会应用于使用服务账号新建且与服务账号关联的实例 (https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances?hl=zh-cn#createanewserviceaccount) 以及更改了服务账号 (https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances?hl=zh-cn#changeserviceaccountandscopes) 的现有实例。更改与实例关联的服务账号时，您需要停止并重启实例。您可以将服务账号与单个实例关联，也可以与代管式实例组 (https://cloud.google.com/compute/docs/instance-groups?hl=zh-cn)使用的实例模板关联。

注意：在具有独立 VPC（不参与共享 VPC 的 VPC）的项目中，您只能使用该项目中的服务账号作为防火墙规则条件。在使用共享 VPC (https://cloud.google.com/firewall/docs/shared-vpc?hl=zh-cn) 的项目中，您可以使用宿主项目或任何服务项目中的服务账号作为防火墙规则条件。如果您创建的防火墙规则使用的服务账号与这两种场景都不相符，则将不强制执行该防火墙规则。

按服务账号过滤与按网络标记过滤

本部分着重强调了在决定要使用服务账号还是网络标记来定义目标和来源（适用于入站规则）时，需要考虑的要点。

如果您需要严格控制防火墙规则应用于虚拟机的方式，请使用目标服务账号和来源服务账号（而不是目标网络标记和来源网络标记）：

- 网络标记是一种任意特性。有权修改实例的任何 Identity and Access Management (IAM) 主账号都可以将一个或多个网络标记与该实例关联 (https://cloud.google.com/vpc/docs/add-remove-network-tags?hl=zh-cn)。对项目具有 Compute Engine Instance Admin (https://cloud.google.com/iam/docs/understanding-roles?hl=zh-cn#compute-engine-roles) 角色的 IAM 主账号具有此权限。可以修改实例的 IAM 主账号可以更改其网络标记，这可能会更改该实例的适用防火墙规则集。
- 服务账号表示与实例关联的身份。一个服务账号只能与一个实例关联。通过控制为其他 IAM 主账号授予服务账号用户 (https://cloud.google.com/iam/docs/understanding-roles?hl=zh-cn#service-accounts-roles)角色这一操作，您可以控制对服务账号的访问权限。为了让 IAM 主账号使用服务账号来启动实例，该主账号必须至少使用此服务账号的 Service Account User 角色以及创建实例的适当权限（例如，具有项目的 Compute Engine Instance Admin 角色）。

在任何防火墙规则中，都不能将服务账号和网络标记混合搭配使用：

- 在任何防火墙规则（入站或出站）中，都不能将目标服务账号和目标网络标记一起使用。
- 以下是您按目标网络标记或目标服务账号指定目标时，对于入站防火墙规则无效的来源：

目标	无效来源
目标网络标记	来源服务账号 来源 IP 地址范围和来源服务账号的组合
目标服务账号	来源网络标记 来源 IP 地址范围和来源网络标记的组合

服务账号和网络标记的操作注意事项包括：

- 更改实例的服务账号时，需要停止并重启实例。可以在实例运行时添加或移除网络标记。
- 您可以对防火墙规则指定目标服务账号、来源服务账号、目标网络标记和来源网络标记数量的上限。如需了解详情，请参阅 VPC 资源配额 (https://cloud.google.com/vpc/docs/quota?hl=zh-cn#per_network)。
- 如果通过网络标记标识实例，防火墙规则适用于实例的主要内部 IP 地址。
- 服务账号防火墙规则适用于 GKE 节点，而不适用于 GKE Pod。

角色与权限

下表介绍了使用 VPC 防火墙规则所需的 Identity and Access Management (IAM) 权限。

任务	所需权限	示例角色
创建防火墙规则	`compute.firewalls.create`	Compute Security Admin (https://cloud.google.com/compute/docs/access/iam?hl=zh-cn#compute.securityAdmin) (`roles/compute.securityAdmin`)
删除防火墙规则	`compute.firewalls.delete`	Compute Security Admin

任务	所需权限	示例角色
		(https://cloud.google.com/compute/docs/access/iam?hl=zh-cn#compute.securityAdmin) (`roles/compute.securityAdmin`)
更改防火墙规则	`compute.firewalls.update`	Compute Security Admin (https://cloud.google.com/compute/docs/access/iam?hl=zh-cn#compute.securityAdmin) (`roles/compute.securityAdmin`)
查看防火墙规则的详细信息	`compute.firewalls.get`	Compute Network Viewer (https://cloud.google.com/compute/docs/access/iam?hl=zh-cn#compute.networkViewer) (`roles/compute.networkViewer`)
查看防火墙规则列表	`compute.firewalls.list`	Compute Network Viewer (https://cloud.google.com/compute/docs/access/iam?hl=zh-cn#compute.networkViewer) (`roles/compute.networkViewer`)

使用场景

以下用例演示了防火墙规则的工作原理。这些示例中均启用了所有防火墙规则。

入站场景

入站防火墙规则控制从来源发送到 VPC 网络内目标实例的传入连接。入站规则的来源可以定义为以下各项之一：

- IPv4 或 IPv6 地址范围；默认为任何 IPv4 地址 (`0.0.0.0/0`)
- 您的 VPC 网络中由网络标记标识的其他实例
- 您的 VPC 网络中由服务账号标识的其他实例
- 您的 VPC 网络中由 IPv4 或 IPv6 地址范围和网络标记标识的其他实例

- 您的 VPC 网络中由 IPv4 或 IPv6 地址范围和服务账号标识的其他实例

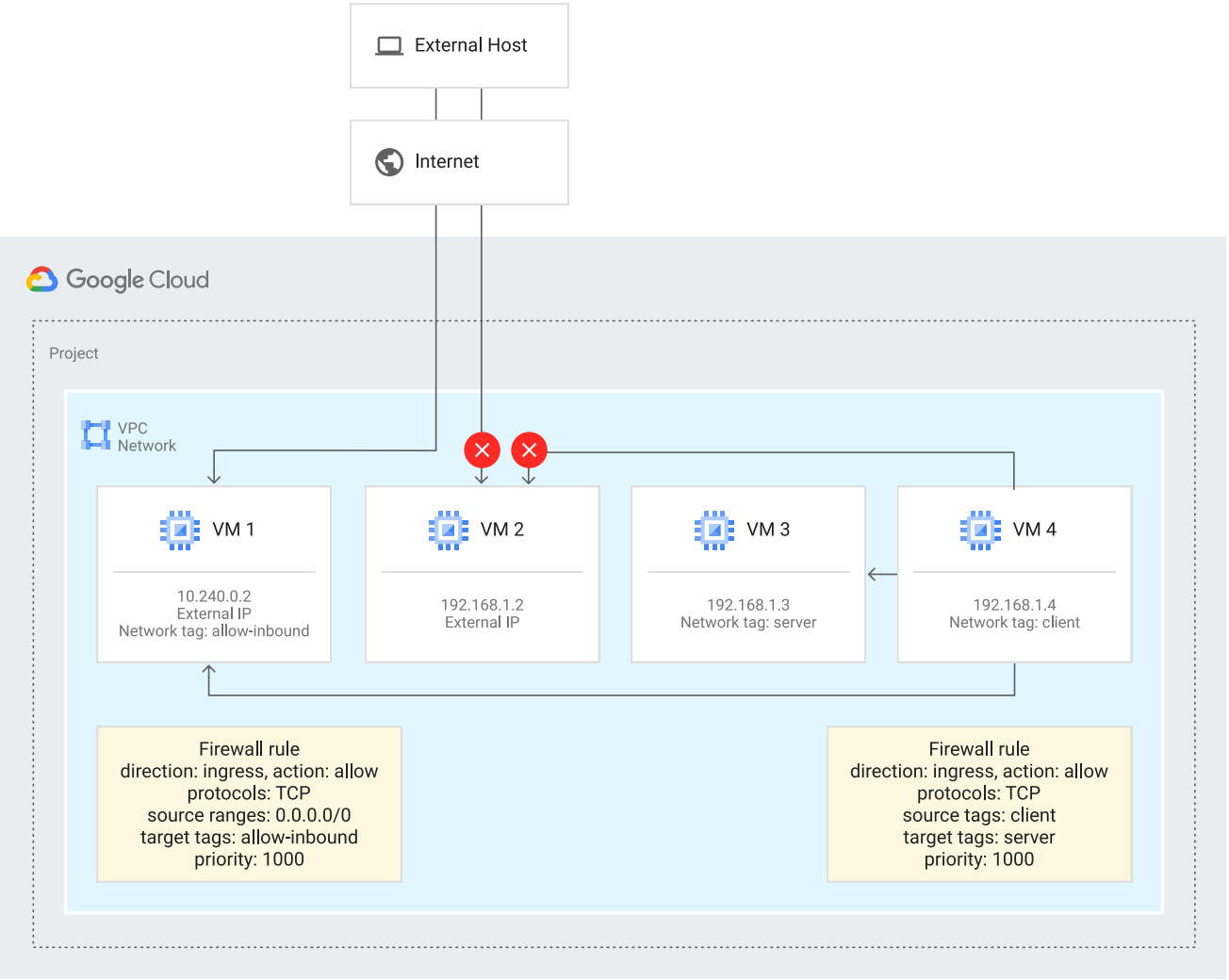
默认来源是任意 IPv4 地址 (`0.0.0.0/0`)。如果您要控制 VPC 网络之外的来源（包括互联网上的其他来源）的传入连接，请使用某个 CIDR 格式的 IP 地址范围。

操作为 `allow` 的入站规则会根据其他规则组件 (#firewall_rule_components)允许传入流量。除了指定规则的来源和目标之外，还可以将规则限制为仅应用于特定协议和目的地端口。同样，具有 `deny` 操作的入站规则可根据防火墙规则组成部分禁止传入流量，从而用于保护实例。

注意：您还可以使用目标服务账号或目标网络标记来指定入站目的地。如果您这样做，则会限制针对规则指定来源的方式。如需了解详情，请参阅按服务账号过滤与按网络标记过滤 (#service-accounts-vs-tags)。

入站示例

图 1 说明了防火墙规则可以控制入站流量连接的一些示例。这些示例在规则分配中使用目标参数将这些规则应用于特定实例。



(https://cloud.google.com/static/firewall/images/firewalls/firewall_overview_ingress_examples.svg?hl=zh-cn)

*图 **1.** 在此示例 VPC 网络中，允许入站流量防火墙规则覆盖某些虚拟机的隐式拒绝入站流量规则（点击可放大）。*

- 优先级为 `1000` 的入站规则适用于虚拟机 **1**。这条规则允许来自任意 IPv4 来源 (`0.0.0.0/0`) 的传入 TCP 流量。它允许来自 VPC 网络中其他实例的 TCP 流量，但要求其遵守适用于这些实例的相应出站流量规则。虚拟机 **4** 能够通过 TCP 与虚拟机 **1** 进行通信，因为虚拟机 **4** 不具有禁止此类通信的出站规则（仅隐式允许出站规则适用）。由于虚拟机 **1** 具有外部 IP 地址，因此这条规则还通过外部 IP 地址允许来自互联网上外部主机以及来自虚拟机 **2** 的传入 TCP 流量。
- 虚拟机 **2** 没有指定入站防火墙规则，因此隐式拒绝入站规则会禁止所有传入流量。系统会禁止来自网络中其他实例的连接，无论其他实例的出站规则如何。由于虚拟机 **2** 具有外部 IP 地址，因此存在从互联网上的外部主机到该虚拟机的一条路径，但隐式拒绝规则也会拒绝外部传入流量。
- 优先级为 `1000` 的入站规则适用于虚拟机 **3**。此规则允许来自网络中带有网络标记 `client` 的实例（如虚拟机 **4**）的 TCP 流量。系统允许虚拟机 **4** 到虚拟机 **3** 的 TCP 流量，因为虚拟机 **4** 不具有禁止此类通信的出站规则（仅隐式允许出站规则适用）。由于虚拟机 **3** 没有外部 IP 地址，因此没有从互联网上外部主机到此虚拟机的路径。

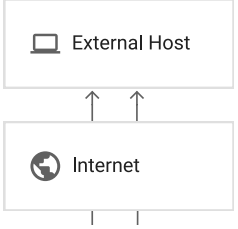
出站情景

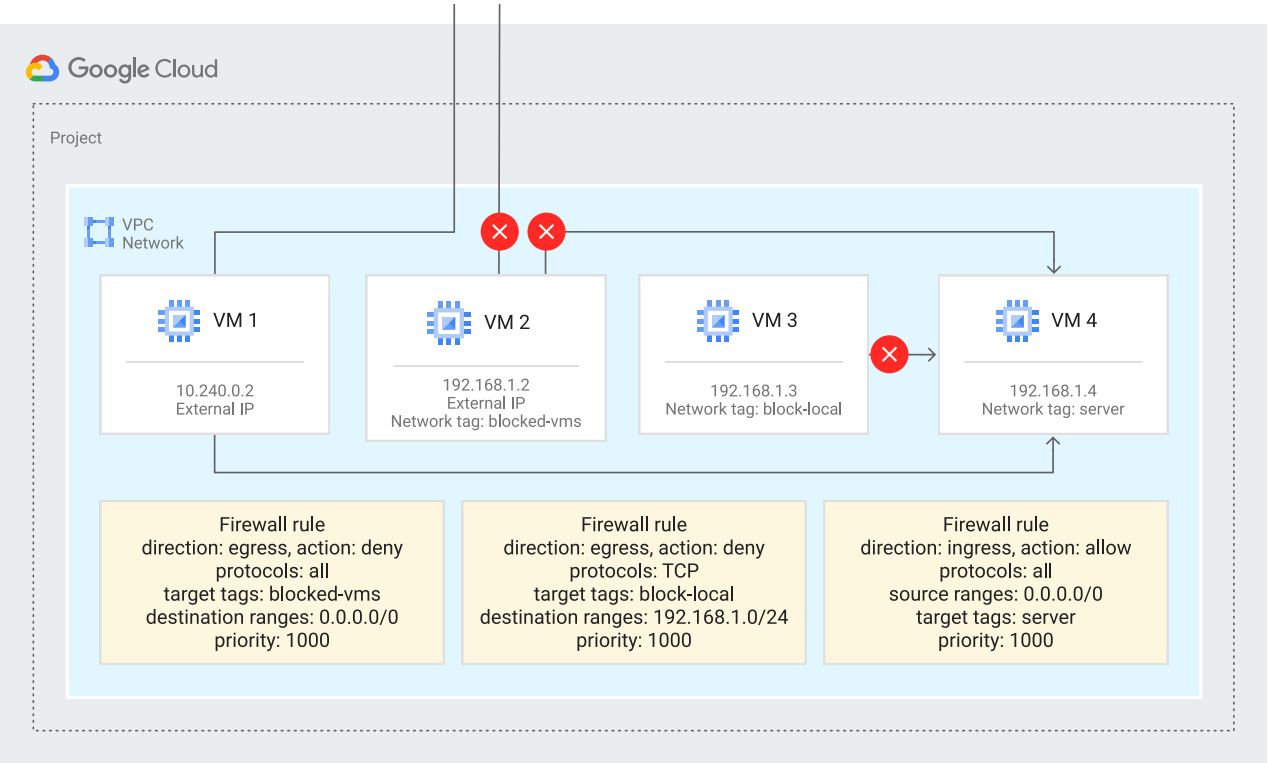
出站防火墙规则控制您的 VPC 网络中目标实例的传出连接。具有 `allow` 操作的出站规则会根据规则的其他组成部分 (#firewall_rule_components)允许来自实例的流量。例如，您可以在指定的协议和目的地端口上，允许发送到特定目的地（例如某个 IPv4 地址范围）的出站流量。类似地，具有 `deny` 操作的出站规则会以规则的其他组成部分为依据禁止流量。

每条出站规则都需要一个目的地。默认目的地是任意 IPv4 地址 (`0.0.0.0/0`)，但您可以使用 CIDR 格式的 IPv4 或 IPv6 地址范围，创建更具体的目的地。在指定 IP 地址范围时，您可以控制发送到网络中的实例以及网络外目的地（包括互联网上的目的地）的流量。

出站示例

图 2 说明了防火墙规则可以控制出站流量连接的一些示例。这些示例在规则分配中使用目标参数将这些规则应用于特定实例。





(https://cloud.google.com/static/firewall/images/firewalls/firewall_overview_egress_examples.svg?hl=zh-cn)

图 2. 在此示例 VPC 网络中，拒绝出站流量防火墙规则会覆盖某些虚拟机的隐式允许出站流量规则（点击可放大）。

- 虚拟机 **1** 没有指定出站防火墙规则，因此隐式允许出站规则允许该虚拟机将流量发送到任何目的地。该规则允许与 VPC 网络中其他实例之间的连接，但要求其遵守适用于这些实例的相应入站规则。虚拟机 **1** 可以将流量发送到虚拟机 **4**，因为虚拟机 **4** 具有允许来自任何 IP 地址范围的传入流量的入站规则。由于虚拟机 **1** 具有外部 IP 地址，因此可以将流量发送到互联网上的外部主机。由于防火墙规则是有状态的，所以允许虚拟机 **1** 所发送流量的传入响应。

- 优先级为 `1000` 的出站规则适用于虚拟机 **2**。此规则拒绝发往所有 IPv4 目的地 (`0.0.0.0/0`) 的全部传出流量。系统会禁止发送到 VPC 中其他实例的传出流量，无论适用于其他实例的入站流量规则如何。尽管虚拟机 **2** 具有外部 IP 地址，但此防火墙规则会禁止其发送到互联网上外部主机的传出流量。

- 优先级为 `1000` 的出站规则适用于虚拟机 **3**。此规则禁止其出站 TCP 流量发送到 `192.168.1.0/24` IP 地址范围内的任何目的地。虽然虚拟机 **4** 的入站规则允许所有传入流量，但虚拟机 **3** 仍不能向虚拟机 **4** 发送 TCP 流量。不过，由于出站规则仅适用于 TCP 协议，因此虚拟机 **3** 可不受限制地将 UDP 流量发送到虚拟机 **4**。

  此外，虚拟机 **3** 可以将任意流量发送到 VPC 网络中 `192.168.1.0/24` IP 地址范围以外的其他实例，前提是这些实例具有允许此类流量的入站规则。由于它没有外部 IP 地址，因此也就没有将流量发送到 VPC 网络以外的路径。