

VPN 连接

快速入门

产品文档



腾讯云

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

快速入门

IPSec VPN

建立 VPC 到 IDC 的连接（SPD 策略）

入门概述

步骤1：创建 VPN 网关

步骤2：创建对端网关

步骤3：创建 VPN 通道

步骤4：本地网关加载配置

步骤5：配置路由表

步骤6：激活 VPN 隧道

建立 VPC 到 IDC 的连接（目的路由）

入门概述

步骤1：创建 VPN 网关

步骤2：创建对端网关

步骤3：创建 VPN 通道

步骤4：本地网关配置

步骤5：配置路由策略

步骤6：激活 VPN 通道

SSL VPN

建立移动端与 VPC 连接

快速入门概述

步骤1：创建 SSL VPN 网关

步骤2：创建 SSL 服务端

步骤3：创建 SSL 客户端

步骤4：配置腾讯云侧路由策略

步骤5：移动端配置

步骤6：连通性验证

快速入门

IPSec VPN

建立 VPC 到 IDC 的连接（SPD 策略）

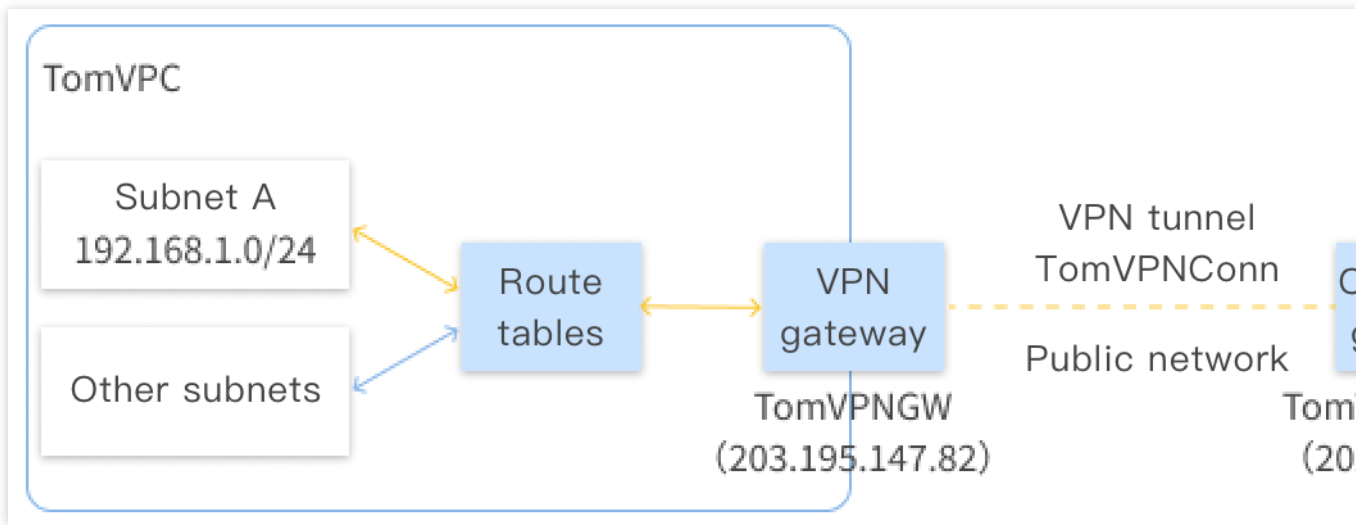
入门概述

最近更新时间：2024-01-09 14:41:10

您需要完成几个步骤使 VPN 连接生效，之后可以在控制台实现 IPsec VPN 全自助配置，下文将为您举例说明。

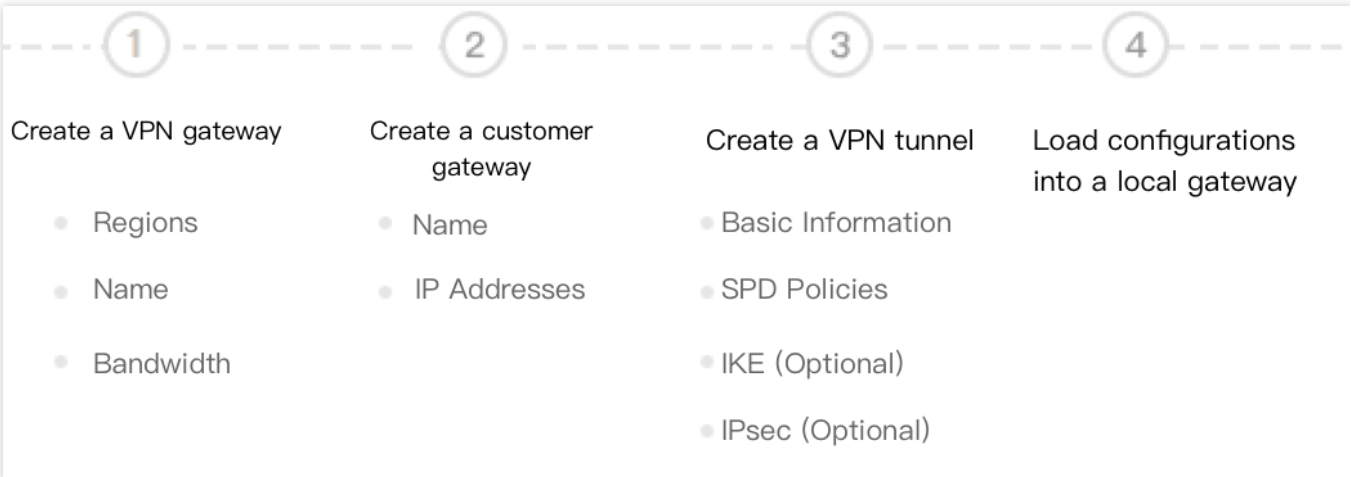
示例

通过 IPsec VPN 连接，打通您在广州的私有网络 TomVPC 中的子网 A：192.168.1.0/24 与您 IDC 中的子网：10.0.1.0/24，而您 IDC 中 VPN 网关的公网 IP 是 202.108.22.5。



步骤说明

VPN 连接激活流程图如下所示：



具体操作请参见：

- 步骤 1：创建 VPN 网关
- 步骤 2：创建对端网关
- 步骤 3：创建 VPN 通道
- 步骤 4：本地网关配置
- 步骤 5：配置路由策略
- 步骤 6：激活 VPN 隧道

步骤1：创建 VPN 网关

最近更新时间：2024-01-09 14:41:10

本文为您介绍如何创建 VPN 网关。

操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击 **VPN 连接 > VPN 网关**，进入管理页。
3. 选择地域，如示例中的**广州**，单击 **+新建**。

说明：

若 **+新建** 显示灰色，且鼠标移至上方时显示“无可私有网络”，请 [创建私有网络](#) 后再进行新建 VPN 网关。

4. 填写 VPN 网关名称（如 TomVPNGw），选择关联网络、所属网络、带宽上限、标签、计费方式，单击**创建**即可。VPN 网关创建完成后，系统随机分配公网 IP，如：`203.195.147.82`。

说明：

200Mbps、500Mbps、1000Mbps和3000Mbps带宽目前仅华北地区（北京）、华东地区（上海）、华南地区（广州）、西南地区（成都）、港澳台地区（中国香港）、华东地区（南京）等可用区开放，如需请 [提交工单](#)。

200Mbps、500Mbps、1000Mbps和3000Mbps带宽仅支持新建网关，存量网关暂不支持。

如果 VPN 网关使用200Mbps、500Mbps、1000Mbps和3000Mbps规格的带宽，VPN 通道加密协议建议使用 AES128+MD5。

Create a VPN gateway

Gateway Name

60 more chars allowed

Region

South China (Guangzhou)

Protocol type

☒ IPsec ☐ SSL

Associate Network

☐ CCN ☒ VPC

Network

Bandwidth Cap

5M

10M

20M

50M

100M

bps

Tag

Tag key	Tag value	Operation
Please select	Please select	×

Add

Billing method

Postpaid ⓘ

Total Price

Create

Cancel

说明：

标签为选配，请保持默认。

相关文档

[步骤2：创建对端网关](#)

[步骤3：创建 VPN 通道](#)

[步骤4：本地网关加载配置](#)

[步骤5：配置路由表](#)

[步骤6：激活 VPN 隧道](#)

步骤2：创建对端网关

最近更新时间：2024-01-09 14:41:10

本文为您介绍如何创建对端网关

操作步骤

在 VPN 通道创建前，需要创建对端网关：

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击 **VPN 连接** > **对端网关**，进入管理页。
3. 选择地域，如示例中的**广州**，单击**+新建**。
4. 填写对端网关名称（如：TomVPNUserGw）、标签和 IDC 的 VPN 网关的公网 IP，如：`202.108.22.5`。

说明：

标签为选配，请保持默认。

Create Customer Gateway

Name

i

60 more chars allowed

Public IP

.

.

.

i

Create

Cancel

5. 单击**创建**即可。

步骤3：创建 VPN 通道

最近更新时间：2024-01-09 14:41:10

本文为您介绍如何创建 VPN 通道。

操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击 **VPN 连接 > VPN 通道**，进入管理页。
3. 选择对应的地域和私有网络，如示例中的 **广州** 和 **TomVPC**，单击 **+新建**。
4. VPN 通道基本参数配置。

基本配置包括输入通道名称，选择网关所在地域、网络类型、VPN 网关实例、对端网关实例、预共享密钥、协商类型和通信模式，具体参数含义请参见 [创建 VPN 通道](#)。

本实例中通信模式为 **SPD 策略**，本端网段即为子网 **A** 的网段 **192.168.1.0/24**，对端网段为 **10.0.1.0/24**。

5. 高级配置。

本步骤您可以配置 **DPD**、**健康检查**、**IKE** 和 **IPSec** 等高级参数，本实例使用默认参数。

说明：

配置 **IKE** 和 **IPSec** 时请确保云侧配置和本地配置一致、相匹配，以防因两端协议配置不一致而通道不通。

6. 检查您的配置内容然后单击“创建”。创建成功后，返回 **VPN 通道** 列表页，单击 **更多**，选择下载配置文件并完成下载。

步骤4：本地网关加载配置

最近更新时间：2024-01-09 14:41:10

完成前3步后，云上 VPN 网关和 VPN 通道的配置已经完成，需要在 IDC 侧的“本地网关”上配置另一侧的 VPN 通道信息，具体请参考 [本地网关配置](#)。IDC 侧的“本地网关”即为 IDC 侧的 IPsec VPN 设备，该设备的公网 IP 记录在 [步骤2](#) 的“对端网关”中。

本地网关一般会有以下部署场景：

注意：

以下两种方式均要求您“本地网关”上的 VPN 配置，与 [步骤3](#) 中的 VPN 通道的信息一致，否则 VPN 隧道无法正常连通。

腾讯云上 VPN 通道的配置信息可以通过 [VPN 通道控制台](#) 查看，并通过[下载配置文件](#)进行下载，加载到本地数据中心的 IPsec VPN 网关中，以完成配置。

打通腾讯云和本地数据中心

本地网关是具有 VPN 功能的网络设备，一般为数据中心出口路由器或防火墙，您可在此网络设备上进行 VPN 配置，以完成“本地网关”配置。

说明：

由于网络设备生产厂商的不同（如 H3C、思科等），配置可能会有差异，请根据网络设备的实际情况进行配置。

打通腾讯云和其他公有云

本地网关是您目标公有云上的 VPN 网关，您需要在目标公有云上的 VPN 网关进行操作，以完成“本地网关”的 VPN 配置，具体配置方法请参考目标公有云的文档介绍。

步骤5：配置路由表

最近更新时间：2024-01-09 14:41:10

截止至步骤 4，我们已经将一条 VPN 通道配置成功，但仍需配置路由表，将子网 A 中的流量路由至 VPN 网关上，子网 A 中的网段才能与 IDC 中的网段通信。

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击**子网**，选择对应的地域和私有网络，如示例中的**广州**和 `TomVPC` ，单击子网 A 所关联的路由表 ID，进入详情页。
3. 单击**新增路由策略**。
4. 在弹出框中，输入目的端网段（ `10.0.1.0/24` ），下一跳类型选择**VPN 网关**，下一跳选择刚创建的 VPN 网关 `TomVPNGw` ，单击**创建**即可。

Add routing

Destination	Next hop type	Next hop
10.0.1.0/24	VPN Gateway	vpngw-0kfe9uoh (test)

+ New Line

Adding a routing entry may affect your business. Please double check before continuing.

OK

Cancel

步骤6：激活 VPN 隧道

最近更新时间：2024-01-09 14:41:10

腾讯云侧 VPN 网关、VPN 通道、对端网关和用户本地配置完成后，您可以使用 Ping 命令激活通道，即验证腾讯云侧是否和用户侧互通。

使用 VPC 内的云服务器 Ping 对端网段中的 IP。

Ping 成功，表示腾讯云侧与用户 VPN 隧道已通达。

Ping 失败，请检测客户侧本地配置。如需技术支持请 [提交工单](#)。

建立 VPC 到 IDC 的连接（目的路由）

入门概述

最近更新时间：2024-01-09 14:41:10

本章节介绍如何快速创建 VPN 连接，并使用路由功能配置路由转发策略，实现 VPC 与对端 IDC 间的安全通信。

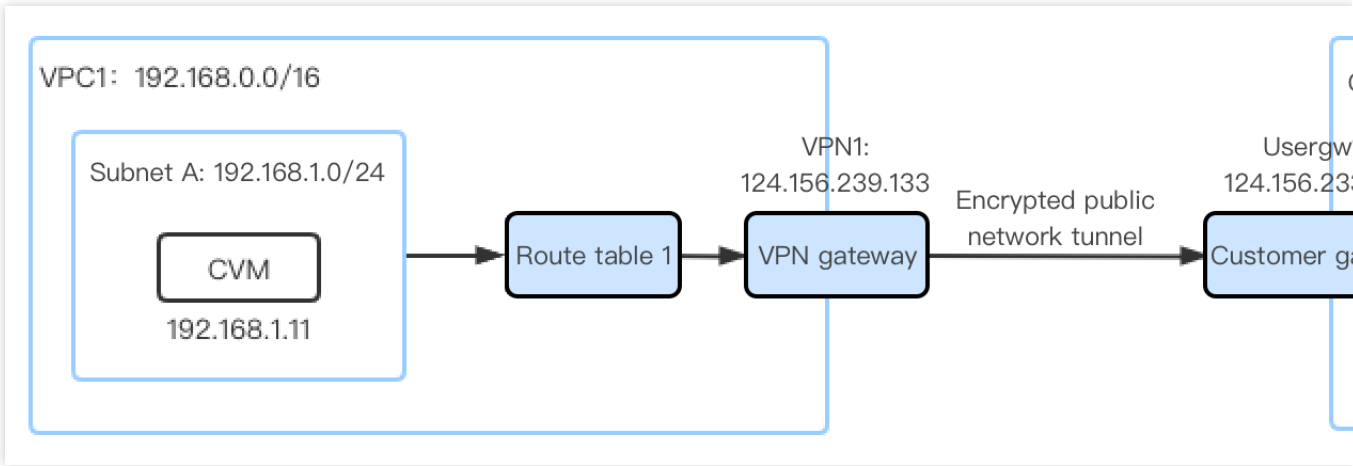
步骤说明

VPN 连接激活流程图如下所示：



示例

通过 IPsec VPN 连接，打通您在**东京**的私有网络 VPC 中的子网 1：`192.168.1.0/24` 与您本地 IDC 中的子网：`10.0.1.0/24`。



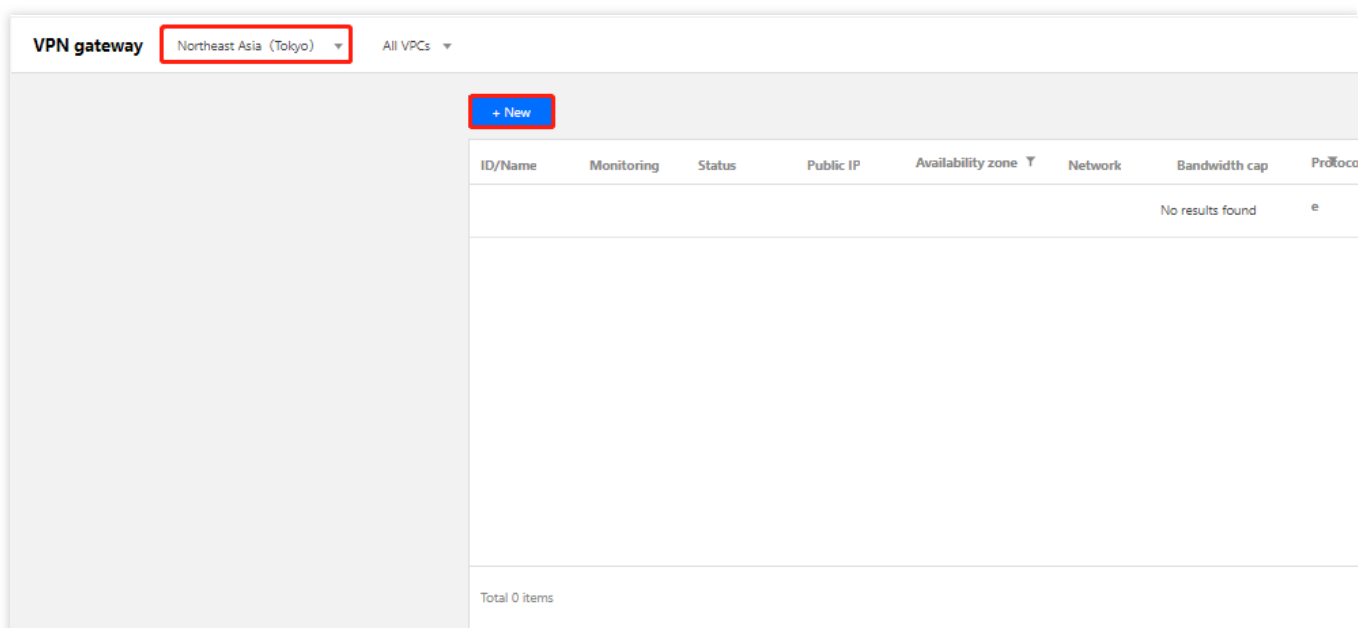
步骤1：创建 VPN 网关

最近更新時間：2024-01-09 14:41:10

1. 登錄 [私有網絡控制台](#)。
2. 在左側目錄中單擊 **VPN 連接** > **VPN 網關**，進入管理頁。
3. 選擇地域，如示例中的**東京**，單擊**新建**。

說明：

若**新建**顯示灰色，且鼠標移至上方時顯示“無可用私有網絡”，請 [創建私有網絡](#) 後再進行新建 VPN 網關。



4. 在彈出的創建對話框中填寫 VPN 網關名稱（如 VPN1），選擇關聯網絡為私有網絡、所屬網絡選擇 VPC1，設置帶寬上限及計費方式等。

說明：

如果 VPN 網關使用 200Mbps、500Mbps、1000Mbps 和 3000Mbps 規格的帶寬，VPN 通道加密協議建議使用 AES128+MD5。

Create VPN gateway

Gateway name

60 more chars allowed

Region

South China (Guangzhou)

Availability zone

Guangzhou Zone 3

Protocol type

☒ IPsec ☐ SSL

Bandwidth cap

5M

10M

20M

50M

100M

bps

Associate network

☐ CCN ☒ VPC

Network

vp

Tag

Tag key	Tag value	Operation
Please select	Please select	×

Add

Billing method

Pay-as-you-go

Total price

(Gateway fee)

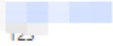
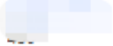
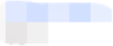
(Traffic fee)

Buy now

Cancel

5. 单击**创建**。VPN 网关创建完成后，系统随机分配公网 IP，如：`119.29.147.109`。

+ New

ID/Name	Monitoring	Status	Public IP	Availability zone ▼	Network	Bandwidth cap	Protocol typ	Network tyg
 123		Running		Guangzhou Zone 3		5Mbps 	e SSL	VPC
		Running		Guangzhou Zone 4		5Mbps 	SSL	VPC
		Running	119.29.147.109	Guangzhou Zone 3		5Mbps 	SSL	VPC
Total 3 items								

步骤2：创建对端网关

最近更新时间：2024-01-09 14:41:10

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击**VPN 连接** > **对端网关**，进入管理页。
3. 选择地域，如示例中的**东京**，单击**新建**。
4. 填写对端网关名称（如：Usergw1）和 对端 VPN 网关的公网 IP，如：`124.156.223.112`。
5. 单击**创建**，创建成功的 VPN 通道如下图所示。

步骤3：创建 VPN 通道

最近更新时间：2024-01-09 14:41:10

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击 **VPN 连接** > **VPN 通道**，进入管理页。
3. 选择对应的地域和私有网络，如示例中的**东京**和 `VPC1`，单击 **+新建**。
4. VPN 通道基本参数配置。

基本配置包括输入通道名称，选择网关所在地域、网络类型、VPN 网关实例、对端网关实例、预共享密钥、协商类型和通信模式，具体参数含义请参见 [创建 VPN 通道](#)。

本实例中通信模式为目的路由。

5. 高级配置。
本步骤您可以配置 DPD、健康检查、IKE 和 IPSec 等高级参数，本实例使用默认参数。

说明：

配置 IKE 和 IPSec 时请确保云侧配置和本地配置一致、相匹配，以防因两端协议配置不一致而通道不通。

6. 创建成功后，返回 VPN 通道列表页，单击**更多**，选择**下载配置文件**并完成下载。

步骤4：本地网关配置

最近更新时间：2024-01-09 14:41:10

完成前3步后，云上 VPN 网关和 VPN 通道的配置已经完成，需要在 IDC 侧的“本地网关”上配置另一侧的 VPN 通道信息，具体请参考 [本地网关配置](#)。IDC 侧的“本地网关”即为 IDC 侧的 IPsec VPN 设备，该设备的公网 IP 记录在 [步骤2](#) 的“对端网关”中。

本地网关一般会有以下部署场景：

注意：

以下两种方式均要求您“本地网关”上的 VPN 配置，与 [步骤3](#) 中的 VPN 通道的信息一致，否则 VPN 隧道无法正常连通。

腾讯云上 VPN 通道的配置信息可以通过 [VPN 通道控制台](#) 查看，并通过[下载配置文件](#)进行下载，加载到本地数据中心的 IPsec VPN 网关中，以完成配置。

打通腾讯云和本地数据中心

本地网关是具有 VPN 功能的网络设备，一般为数据中心出口路由器或防火墙，您可在此网络设备上进行 VPN 配置，以完成“本地网关”配置。

说明：

由于网络设备生产厂商的不同（如 H3C、思科等），配置可能会有差异，请根据网络设备的实际情况进行配置。

打通腾讯云和其他公有云

本地网关是您目标公有云上的 VPN 网关，您需要在目标公有云上的 VPN 网关进行操作，以完成“本地网关”的 VPN 配置，具体配置方法请参考目标公有云的文档介绍。

步骤5：配置路由策略

最近更新时间：2024-01-09 14:41:10

截止至步骤 4，我们已经将一条 VPN 通道配置成功，但仍需配置子网路由策略，将子网1中的流量路由至 VPN 网关上，同时配置 VPN 网关路由策略，将到达 VPN 网关上的流量导入至 VPN 通道中，这样子网1中的网段才能与 IDC 中的网段通信。

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击**子网**，选择对应的地域和私有网络，如示例中的**东京**和 `VPC1`，单击子网1所关联的路由表 ID，进入详情页。
3. 在“基本信息”页签，单击**新增路由策略**。
4. 在弹出框中，输入对端 IDC 子网网段（`10.0.1.0/24`），下一跳类型选择 **VPN 网关**，下一跳选择刚创建的 VPN 网关 `VPN1`，单击**创建**即可完成子网1路由策略的配置。
5. 在左侧目录中选择 **VPN 连接 > VPN网关**。
6. 单击 VPN 网关实例 ID 进入实例详情页。
7. 在“实例详情”页面，单击【路由表】页签，配置 VPN 网关的路由策略。
8. 单击**新增路由**，在弹出的对话框中填写如下参数：
目的端：填写对端 IDC 需要与本端 VPC 通信的内网网段，本例填写 `10.0.1.0/24`。
下一跳类型：只能是 VPN 通道，无需设置。
下一跳：选择 [步骤3](#) 中创建的 VPN 通道。
权重：当 VPC 与 IDC 之间有两条 VPN 通道时，可通过权重来设置主备链路，本例保持默认值0即可。
9. 单击**确定**，完成 VPN 网关路由策略的配置。

步骤6：激活 VPN 通道

最近更新时间：2024-01-09 14:41:10

使用 VPC 内的云服务器 ping 对端网段中的 IP，以激活 VPN 隧道，可以 ping 通表示 VPC 和 IDC 可以正常通信。
例如：VPC1 内的子网1中的云服务器 ping 对端 IDC 子网中的服务器 IP：ping 10.0.1.7。

SSL VPN

建立移动端与 VPC 连接

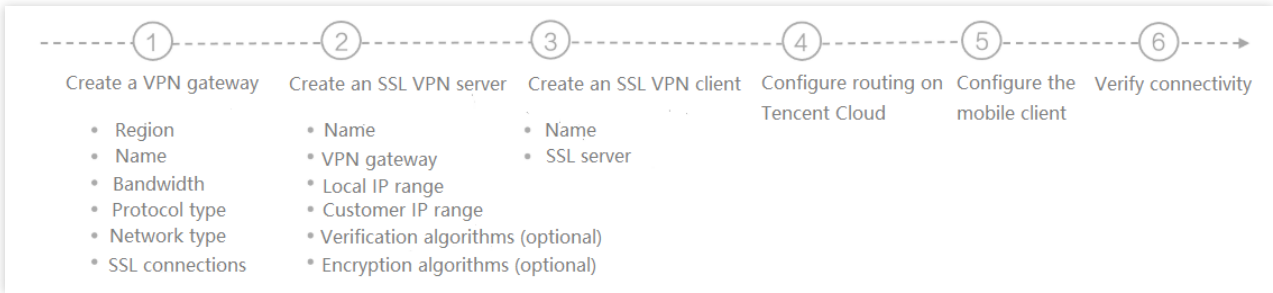
快速入门概述

最近更新时间：2024-01-09 14:41:10

本节介绍如何快速创建 SSL VPN 连接，并使用路由功能配置路由转发策略，实现 VPC 与用户侧移动端安全通信。

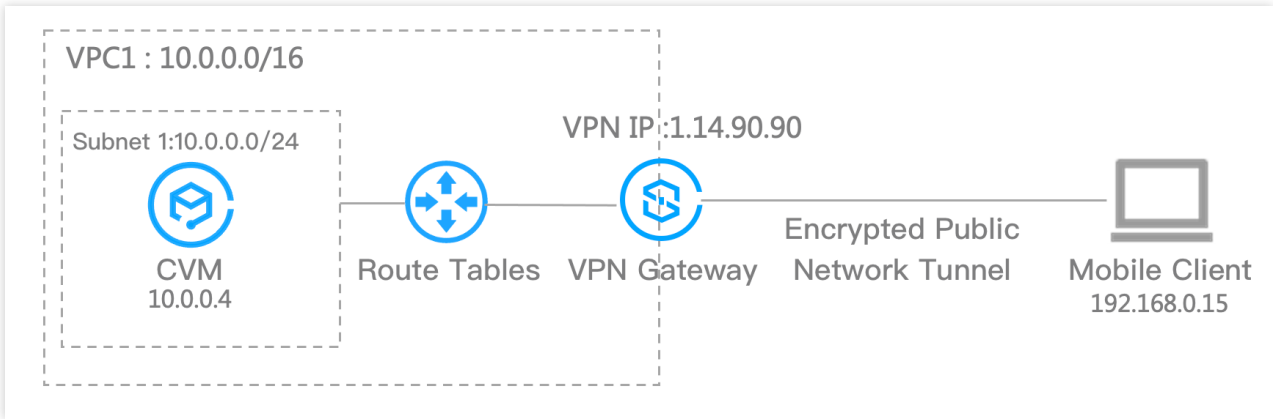
步骤说明

SSL VPN 连接激活流程图如下所示：



示例

通过 SSL VPN 连接，打通您在广东2区的私有网络 VPC 中的子网 1：10.0.0.0/16 与您移动端的子网：192.168.0.0/16。



步骤1：创建 SSL VPN 网关

最近更新时间：2024-01-09 14:41:10

SSL VPN 网关是 VPC 建立 SSL VPN 连接的出口网关，与 SSL 客户端（客户移动端）配合使用，主要用于腾讯云 VPC 和客户移动端建立安全可靠的加密网络通信。

操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在 VPN 网关管理页面，单击 **+新建**。
4. 在弹出的**新建 VPN 网关**对话框中，配置如下网关参数。

参数名称	参数说明
网关名称	填写 VPN 网关名称，不超过60个字符。
所在地域	展示 VPN 网关所在地域。
可用区	选择可用区。
协议类型	选择 SSL。
带宽上限	请根据业务实际情况，合理设置 VPN 网关带宽上限。
关联网络	表示您创建私有网络类型的 VPN，本例以 VPC 为例。
所属网络	选择 VPN 网关将要关联的具体私有网络。
SSL 连接数	连接客户移动端的数量。 说明： 该数值表示允许同时连接的最大客户端数，即所创建的网关可以关联客户端的数量。创建完成后暂不支持修改，请提前做好规划。
计费方式	默认使用按流量计费方式。

5. 完成网关参数设置后，单击**创建**。

步骤2：创建 SSL 服务端

最近更新时间：2024-01-09 14:41:10

SSL VPN 网关创建完成后，需要在腾讯云侧创建 SSL 服务端，为客户侧提供 SSL 服务。

操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击 **VPN 连接 > SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击 **+新建**。
4. 在弹出的**新建 SSL 服务端**对话框中，配置如下参数。

参数名称	参数说明
名称	填写 SSL 服务端名称，不超过60个字符。
地域	展示 SSL 服务端所在地域。
VPN 网关	选择创建好的 SSL VPN 网关。
云端网段	客户移动端访问的云上网段，即您 VPC 所在的网段。
客户端网段	分配给用户移动端进行通信的网段，该网段请勿与腾讯侧 VPC CIDR 冲突，同时也不能与您本地的网段冲突。
协议	服务端传输协议。
端口	填写 SSL 服务端用于数据转发的端口。
认证算法	目前支持 SHA1 和 MD5 两种认证算法。
加密算法	目前支持 AES-128-CBC、AES-192-CBC 和 AES-256-CBC 加密算法。
是否压缩	否。
认证方式	证书认证 和 证书认证 + 身份认证 两种方式，本示例以证书认证为例。 证书认证：该认证方式默认 SSL 服务端可被 SSL 客户端全量访问。 证书认证 + 身份认证：该认证方式仅允许在控制策略中的访问策略连接，您可选择为特定用户组或全部用户配置访问策略，勾选后需要选择对应的 EIAM 应用。

5. 完成网关参数设置后，单击**创建**。

步骤3：创建 SSL 客户端

最近更新时间：2024-01-09 14:41:10

SSL VPN 网关和 SSL 服务端创建完成后，您还需要在腾讯云侧创建 SSL 客户端。SSL 客户端记录了腾讯云分配给用户的 SSL 证书信息，即用于服务端和用户侧移动端进行双向认证的 SSL 证书。您可以下载该证书至移动端，并通过 OpenVPN 与腾讯云进行通信。

操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击 **VPN 连接** > **SSL 客户端**，进入管理页面。
3. 在 SSL 客户端管理页面，单击**新建**。
4. 在弹出的 **SSL 客户端**对话框中，配置如下参数。

参数名称	参数说明
名称	填写 SSL 客户端名称，不超过60个字符。
地域	展示 SSL 服务端所在地域。
SSL 服务端	选择创建好的 SSL 服务端。

5. 完成 SSL 客户端参数设置后，单击**确定**，当**证书状态**为**可用**表示创建完成。

步骤4：配置腾讯云侧路由策略

最近更新时间：2024-01-09 14:41:10

SSL VPN 网关、SSL 服务端、SSL 客户端配置完成，需要配置客户移动端到达腾讯云 VPC 内的路由转发策略。

操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击**路由表**，进入管理页面。
3. 在路由表管理页面，单击**新建**。
4. 在弹出的**新建路由**对话框中，配置如下参数。

参数名称	参数说明
目的端	填写用户移动端所在网段。
下一跳类型	选择 VPN 网关。
下一跳	下一跳选择创建好的具体 VPN 网关实例。

5. 完成参数设置后，单击**创建**。

步骤5：移动端配置

最近更新时间：2024-01-09 14:41:10

完成前面步骤后，云上 SSL VPN 配置已经完成，需要继续在客户侧的移动端配置 SSL 客户端文件。

操作步骤

1. 在

腾讯云侧下

载分配给客户用于与腾讯云连接的 SSL 客户端认证文件，详情请参见 [下载 SSL 客户端配置](#)。

说明：

下载的 SSL 客户端证书仅支持一个本地客户端使用，不支持多个客户端同时使用。

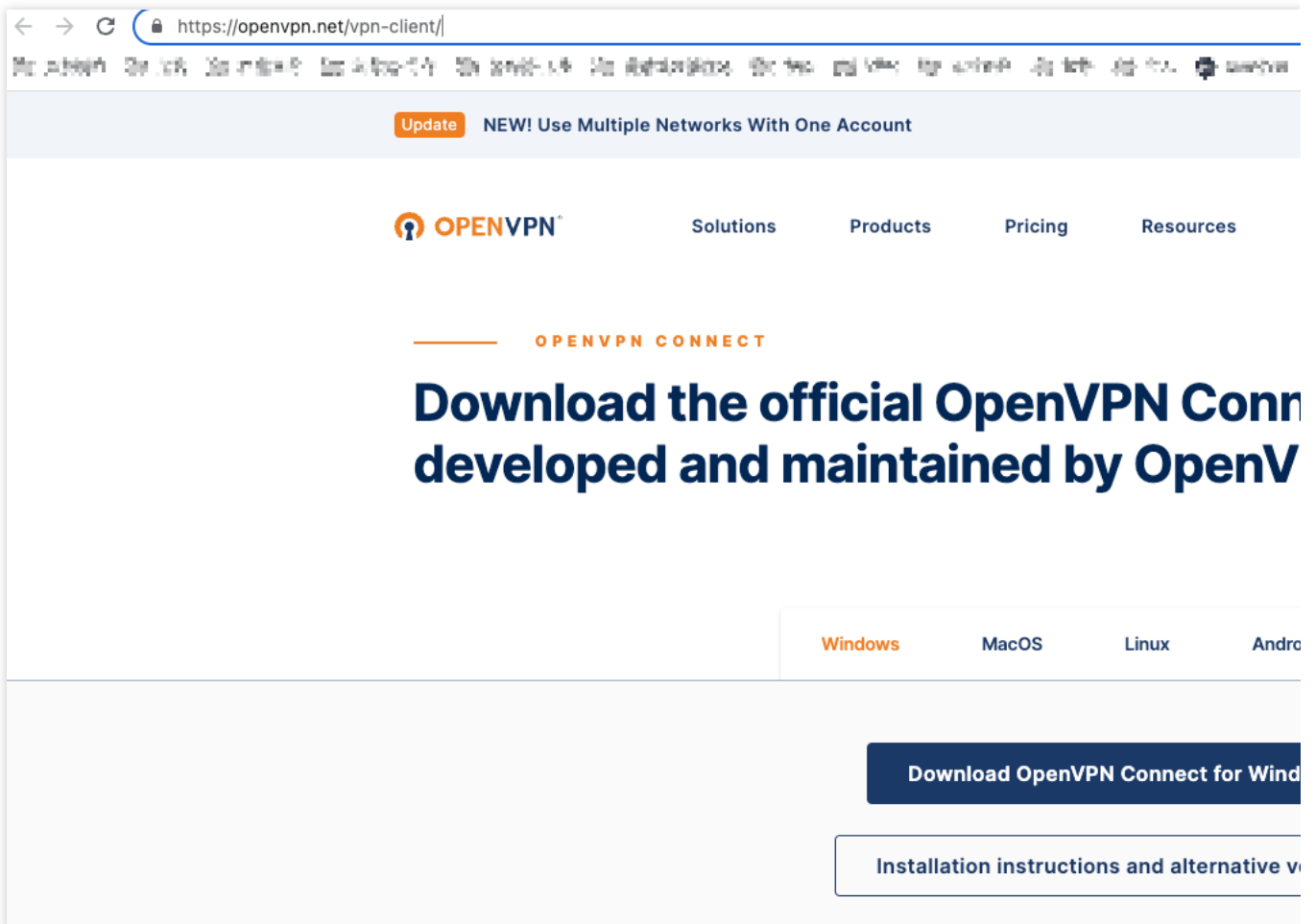
2. 下载 OpenVPN 并本地移动端的 OpenVPN。

Windows 客户端

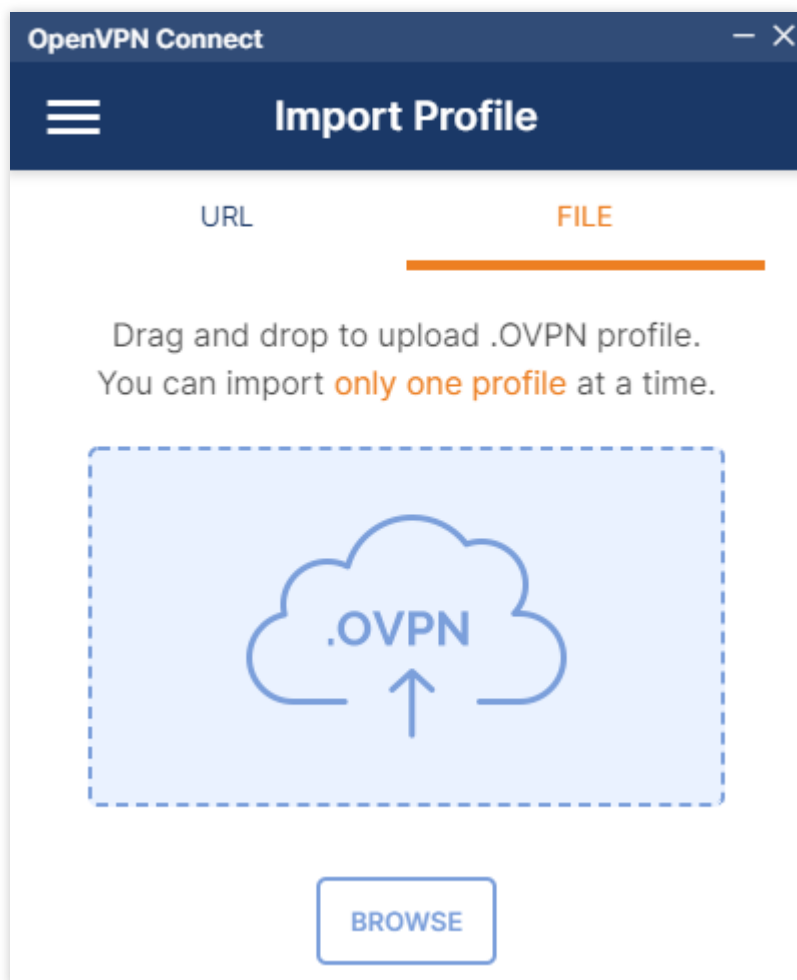
MAC 客户端

Linux 客户端

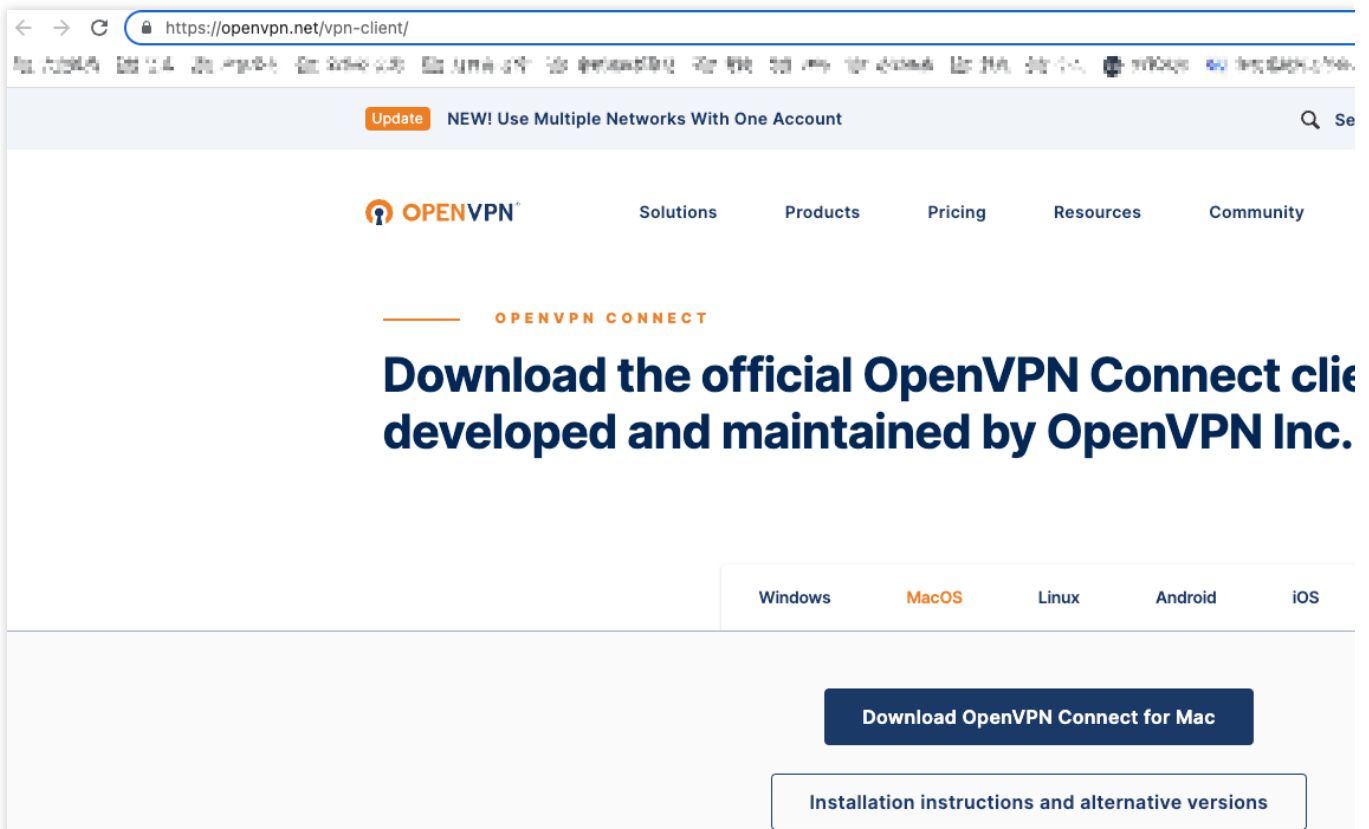
1. 首先在 OpenVPN 官方页面下载并安装 OpenVPN Connect。



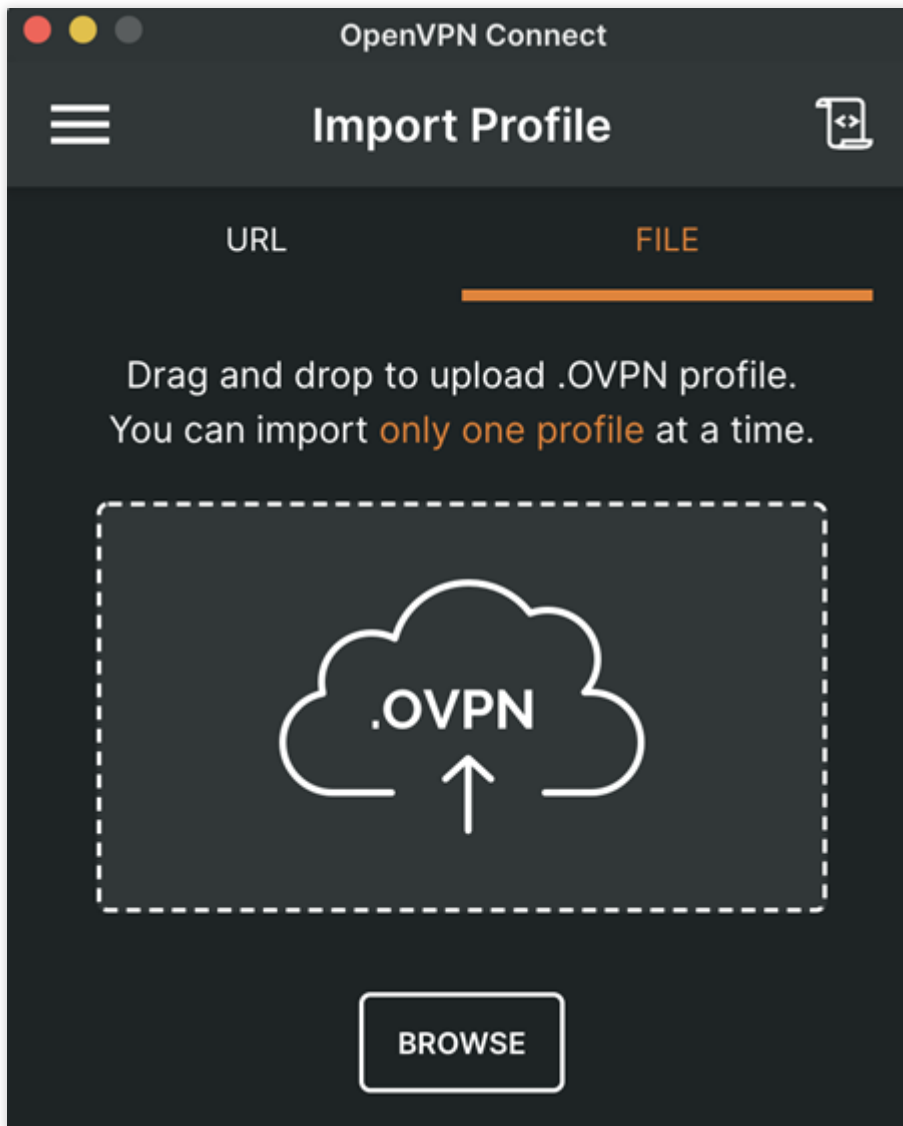
2. SSL 客户端安装完成后，选择“Import Profile”菜单中的“FILE”页面，上传 [步骤1](#) 中已下载的 SSL 客户端配置文件（.ovpn 格式）。



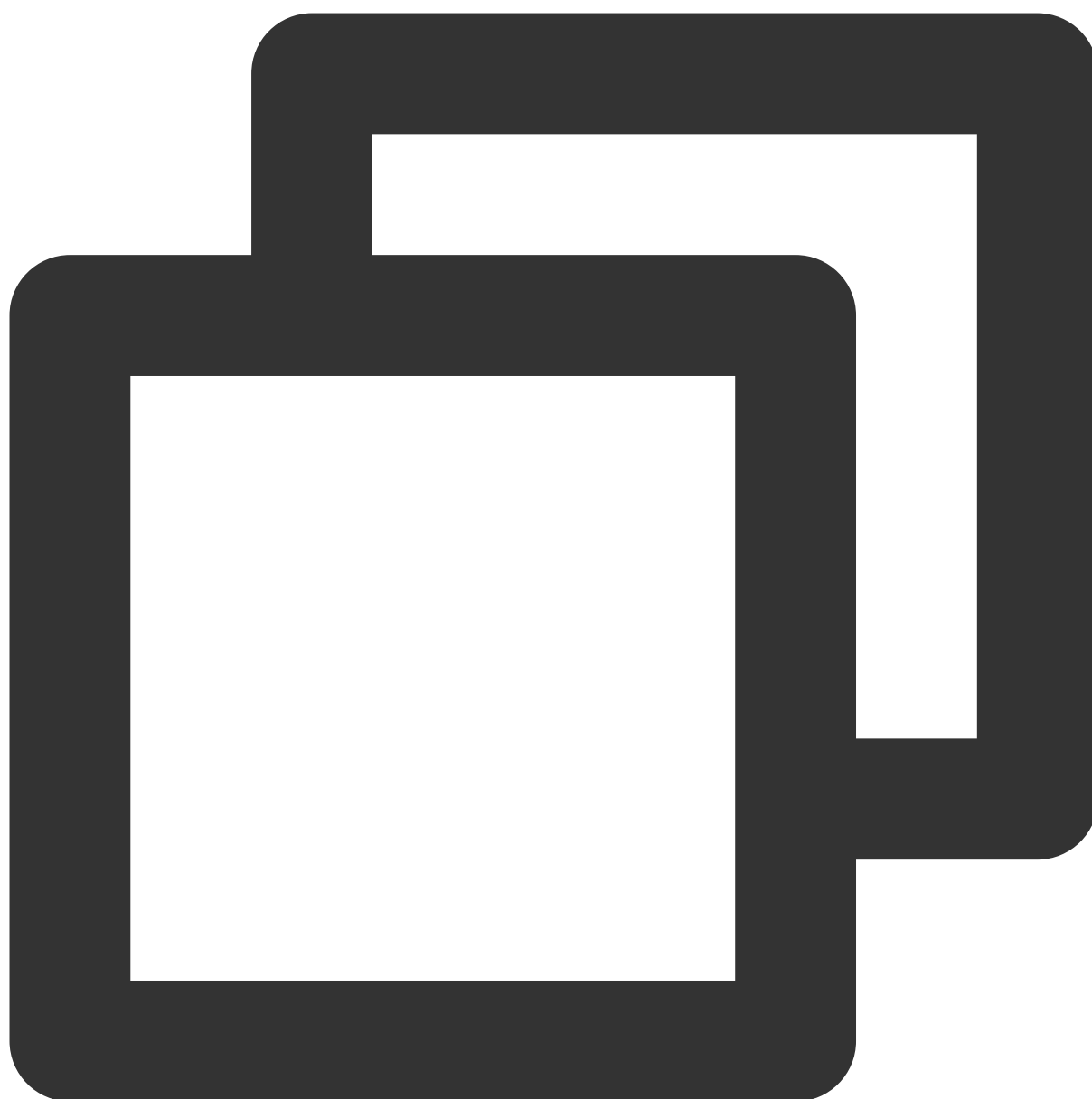
1. 首先在 OpenVPN 官方页面下载并安装 OpenVPN Connect。



2. SSL 客户端安装完成后，选择“Import Profile”菜单中的“FILE”页面，上传 [步骤1](#) 中已下载的 SSL 客户端配置文件（.ovpn 格式）。

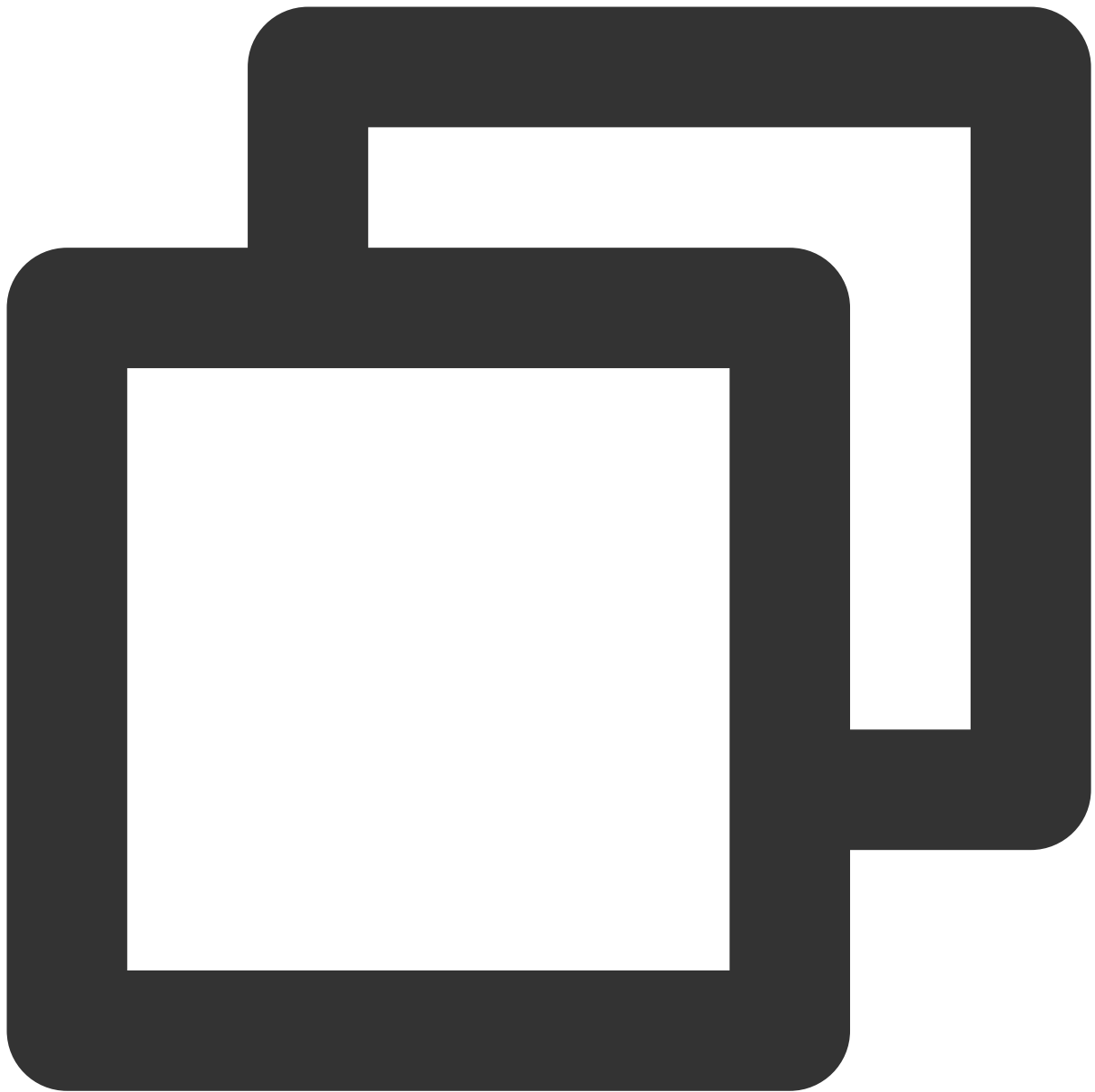


1. 打开命令行窗口。
2. 执行以下命令安装 OpenVPN 客户端。
centos 发行版



```
yum install -y openvpn
```

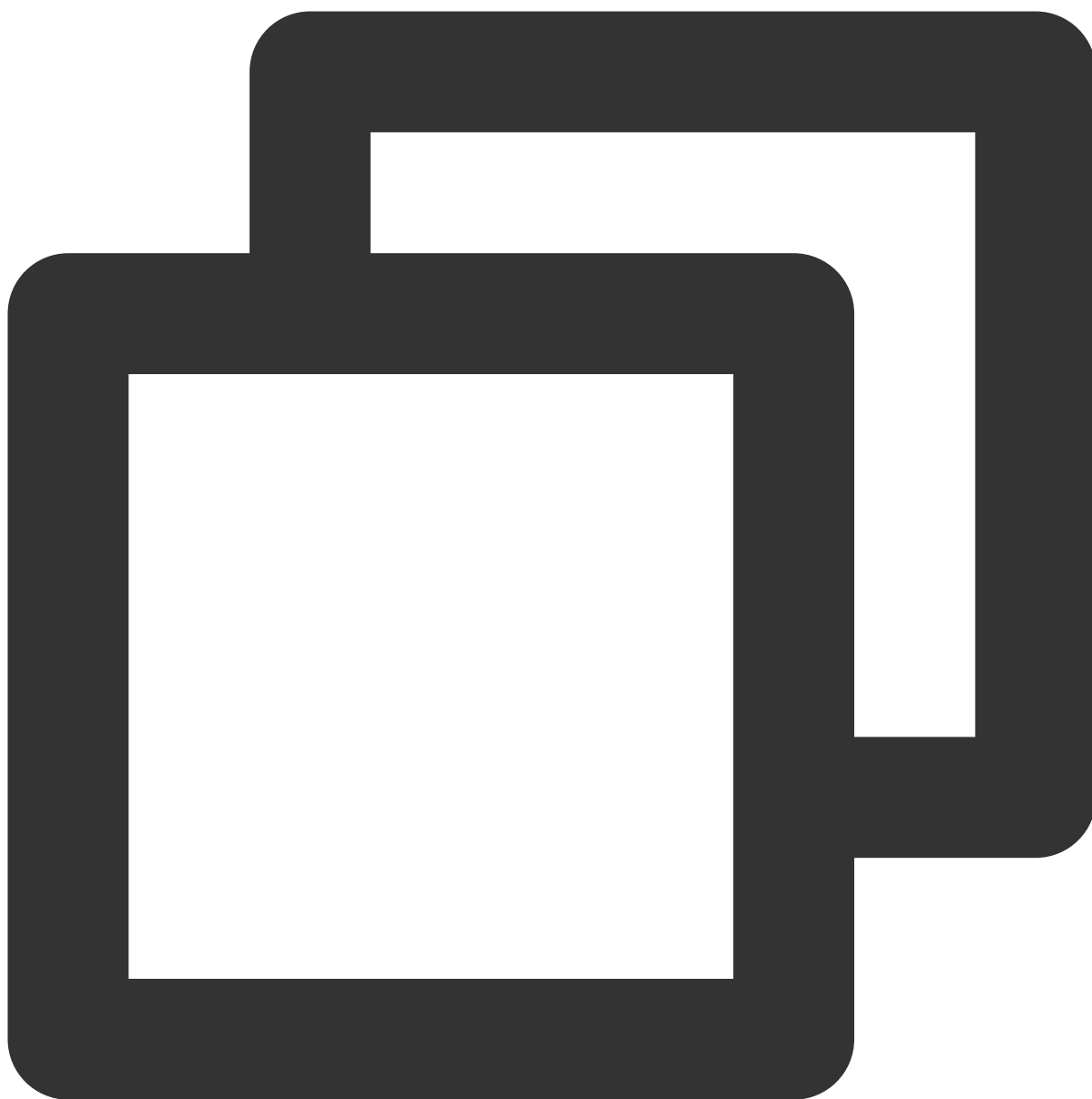
ubuntu 发行版



```
sudo apt-get install openvpn
```

3. 将 [步骤1](#) 中已下载的 SSL 客户端证书解压拷贝至 `/etc/openvpn/conf/` 目录。

进入 `/etc/openvpn/conf/` 目录，执行以下命令建立 VPN 连接。



```
openvpn --config /etc/openvpn/conf/SSLVpnClientConfiguration.ovpn --daemon
```

步骤6：连通性验证

最近更新时间：2024-01-09 14:41:10

腾讯云侧与用户移动端建立 SSL VPN 连接后，使用 Ping 命令检测连通性。

例如：使用 VPC 内的云服务器 ping 移动端网段中的 IP，可以 ping 通表示 VPC 和 移动端可以正常通信。