VPN 连接

实践教程

产品文档

腾讯云

文档目录

实践教程

IPsec VPN

通过专线接入和 VPN 连接实现混合云主备冗余通信（自动切换）

最近更新时间：2024-08-15 16:32:15

当用户业务分别部署于云下数据中心和云上 VPC 中时，可通过专线接入或 VPN 连接实现云上云下业务互通，为提升业务高可用性，可同时创建专线接入和 VPN 连接服务，结合 CCN 配置两条链路为主备链路，来实现冗余通信。

说明

路由优先级功能目前处于内测中，如有需要，请 在线咨询。

暂不支持控制台修改路由优先级，如需调整，请 在线咨询。

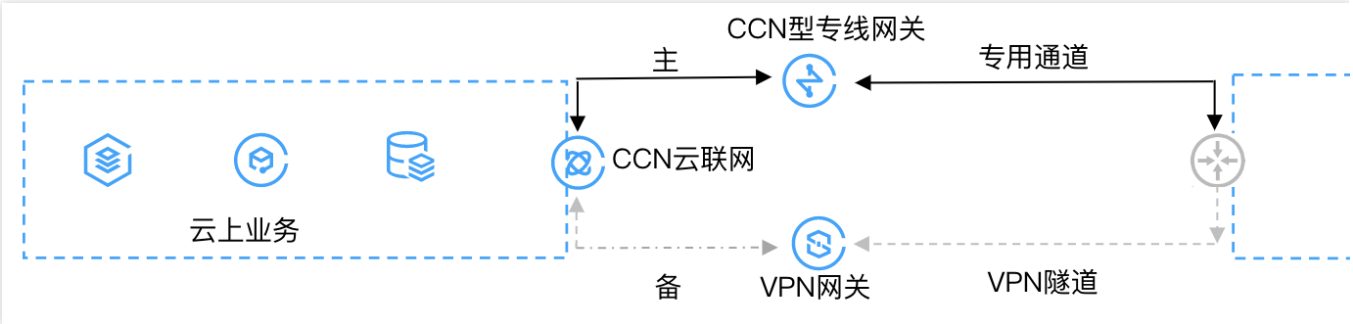
配置主备路由时，专线网段掩码长度须大于 VPN 网段掩码长度。

业务场景

如下图所示，用户在 VPC 和 IDC 中部署了业务，为了实现云上与云下业务交互，用户需要部署网络连接服务来实现业务互通，为实现高可用通信，故障时业务自动切换，部署方案如下：

专线接入（主）：本地 IDC 通过物理专线，接入CCN型的专线网关实现云下云上业务通信。在物理专线链路正常时，本地 IDC 与 VPC 之间所有的通信流量都通过物理专线进行转发。

VPN 连接（备）：本地 IDC 与云上 VPC 通过建立 CCN 型 VPN 安全隧道来实现云上云下业务通信，当专线链路出现异常时，自动将流量切换至该链路，确保业务可用性。



前提条件

用户本地 IDC 网关设备具有 IPsec VPN 功能，可同时作为用户侧 VPN 网关设备，与云侧 VPN 设备建立 IPsec 隧道通信。

用户 IDC 侧网关设备已配置静态 IP。
已创建 CCN 实例，并开启了 ECMP 和路由重叠特性，详情联系 在线支持。
专线侧已开启动态 BGP 传递特性，详情请联系 在线支持。

操作步骤

步骤一：配置 IDC 通过专线接入上云

1. 登录 专线接入控制台，单击左侧导航栏的物理专线，单击**新建**，创建物理专线，详情可参见 申请接入物理专线。
2. 单击左侧导航栏的专线网关，单击**新建**，创建 CCN 型专线网关，创建完成后在其详情发布指向 CCN 的网段，详细操作可参见 创建专线网关、发布网段至云联网。
3. 单击左侧导航栏的**专用通道** > **独享专用通道**，单击**新建**，创建独享专用通道，此处需要配置通道名称、选择专线类型、已创建的专线网关、腾讯云侧和用户侧的互联 IP、路由方式选择静态路由、填写 IDC 通信网段等，配置完成后下载配置指引并在 IDC 设备完成配置。详细操作可参见 独享专用通道。

说明
更多详细配置可参考 IDC 通过云联网上云。

步骤二：配置 IDC 通过 VPN 连接上云

1. 登录 VPN 网关控制台，单击**新建**，创建 CCN 型 VPN 网关可参见 创建 VPN 网关，创建完成后，在其详情页关联 CCN 实例，详细操作可参见 绑定云联网实例。
2. 单击左侧导航栏的对端网关，配置对端网关（即 IDC 侧 VPN 网关的逻辑对象），填写 IDC 侧 VPN 网关的公网 IP 地址，例如202.xx.xx.5。详细操作可参见 创建对端网关。
3. 单击左
侧导航栏的 VPN 通道
，单击**新建**，创建 VPN 通道，请页面引导配置 SPD 策略、IKE、IPsec 等参数。详细配置信息可参见 创建 VPN 通道。

在 IDC 本地网关设备上配置 VPN 通道信息，此处配置需要和 步骤3 中的 VPN 通道信息一致，否则 VPN 隧道无法正常连通。
在网关的路由表页签配置指向对端网关的路由。

说明
更多详细配置请参考 建立 IDC 到云联网的连接。

步骤三：配置告警

为及时发现探测链路异常，可配置告警策略。当检测到链路异常时，告警信息将通过电子邮件和短信等形式发送到您，帮助您提前预警风险。
1. 登录腾讯云可观测平台的 告警策略控制台。
2. 单击**新建**，填写策略名称、策略类型选择私有网络/网络探测，告警对象选择具体的网络探测实例，配置触发条件和告警通知等信息，并单击**完成**即可。

步骤四：切换主备路由

当收到专线网关主路径的网络探测异常告警时，自动会将您的流量切换至 VPN 网关备份路由上。
如果主路专线恢复正常后，您需要手动将流量切会至专线网关。

通过专线接入和 VPN 连接实现混合云主备冗余通信（手动切换）

最近更新时间：2024-01-09 14:41:10

当用户业务分别部署于云下数据中心和云上 VPC 中时，可通过专线接入或 VPN 连接实现云上云下业务互通，为提升业务高可用性，可同时创建专线接入和 VPN 连接服务，结合 VPC 路由优先级功能，配置两条链路为主备链路，来实现冗余通信。本文指导您如何配置专线和 VPC 主备链路来实现云上云下混合通信。

说明：

路由优先级功能目前处于内测中，如有需要，请 提交工单。

VPC 路由表中根据不同的下一跳类型定义了不同的优先级，目前默认路由优先级为：云联网 > 专线网关 > VPN 网关 > 其他。

暂不支持控制台修改路由优先级，如需调整，请 提交工单。

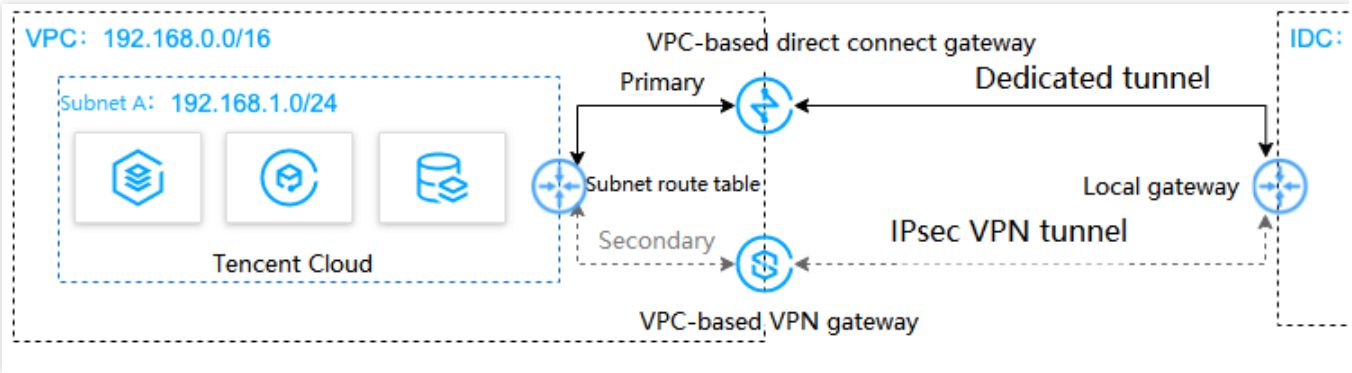
当故障发生后您需要在 VPC 手动切换路由，当前暂不支持自动切换。

业务场景

如下图所示，用户在 VPC 和 IDC 中部署了业务，为了实现云上与云下业务交互，用户需要部署网络连接服务来实现业务互通，为实现高可用通信，部署方案如下：

专线接入（主）：本地 IDC 通过物理专线，接入 VPC 的专线网关实现云下云上业务通信。在物理专线链路正常时，本地 IDC 与 VPC 之间所有的通信流量都通过物理专线进行转发。

VPN 连接（备）：本地 IDC 与云上 VPC 通过建立 VPN 安全隧道来实现云上云下业务通信，当专线链路出现异常时，可将流量切换至该链路，确保业务可用性。



前提条件

用户本地 IDC 网关设备具有 IPsec VPN 功能，可同时作为用户侧 VPN 网关设备，与 VPC 侧 VPN 设备建立 IPsec 隧道通信。

用户 IDC 侧网关设备已配置静态 IP。

数据准备如下：

配置项			示例值
网络配置	VPC 信息	子网 CIDR	192.168.1.0/24
		VPN 网关公网 IP	203.xx.xx.82
	IDC 信息	子网 CIDR	10.0.1.0/24
		网关公网 IP	202.xx.xx.5

操作步骤

步骤一： 配置 IDC 通过专线接入上云

1. 登录 专线接入控制台 ，单击左侧导航栏的**物理专线**创建物理专线。

2. 单击左侧导航栏的**专线网关**创建专线网关，本例选择接入私有网络，标准型的专线网关，如果 IDC 和 VPC 通信网段冲突也可以选择 NAT 型。

3. 单击左侧导航栏的**独享专用通道**创建专用通道，此处需要配置通道名称、选择专线类型、已创建的专线网关、腾讯云侧和用户侧的互联 IP、路由方式选择静态路由、填写 IDC 通信网段等，配置完成后下载配置指引并在 IDC 设备完成配置。

4. 在 VPC 通信子网关联的路由表中配置下一跳为专线网关、目的端为 IDC 通信网段的路由策略。

说明：

更多详细配置可参考 专线接入快速入门。

步骤二：配置 IDC 通过 VPN 连接上云

1. 登录 VPN 网关控制台 ，单击**新建**创建 VPN 网关，本例关联网络选择私有网络。

2. 单击左侧导航栏的**对端网关**，配置对端网关（即 IDC 侧 VPN 网关的逻辑对象），填写 IDC 侧 VPN 网关的公网 IP 地址，例如202.xx.xx.5。

3. 单击左侧导航栏的**VPN 通道**，请配置 SPD 策略、IKE、IPsec 等配置。

4. 在 IDC 本地网关设备上配置 VPN 通道信息，此处配置需要和步骤3中的 VPN 通道信息一致，否则 VPN 隧道无法正常连通。

5. 在 VPC 通信子网关联的路由表中配置下一跳为 VPN 网关、目的端为 IDC 通信网段的路由策略。

说明：

更多详细配置请参考 建立 VPC 到 IDC 的连接（路由表）。

步骤三：配置网络探测

说明：

如上两步配置完成后，VPC 去往 IDC 已经有两条路径，即下一跳为专线网关和 VPN 网关，根据路由默认优先级：专线网关 > VPN 网关，则专线网关为主路径，VPN 网关为备路径。
为了解主备路径的连接质量，需要分别配置两条路径的网络探测，实时监控到网络连接的时延、丢包率等关键指标，以探测主备路由的可用性。
1. 登录 网络探测控制台。
2. 单击**新建**，创建网络探测，填写网络探测名称，选择私有网络、子网、探测目的IP，并指定源端下一跳路由，如专线网关。
3. 请再次执行 步骤2，指定源端下一跳路由为 VPN 网关。配置完成后，即可查看专线接入和VPN连接主备路径的网络探测时延和丢包率。
说明：
更多详细配置请参考 网络探测。

步骤四：配置告警

为及时发现探测链路异常，可配置告警策略。当检测到链路异常时，告警信息将通过电子邮件和短信等形式发送到您，帮助您提前预警风险。
1. 登录腾讯云可观测平台下的 告警策略控制台。
2. 单击**新建**，填写策略名称、策略类型选择**私有网络/网络探测**，告警对象选择具体的网络探测实例，配置触发条件和告警通知等信息，并单击**完成**即可。

步骤五：切换主备路由

当收到专线网关主路径的网络探测异常告警时，您需要手动禁用主路由，将流量切换至 VPN 网关备份路由上。
1. 登录 路由表控制台。
2. 单击 VPC 通信子网关联路由表 ID，进入路由详情页，单击

禁用下一跳到专线网关的主路由，此时 VPC 去往 IDC 的流量将从专线网关切换至 VPN 网关。

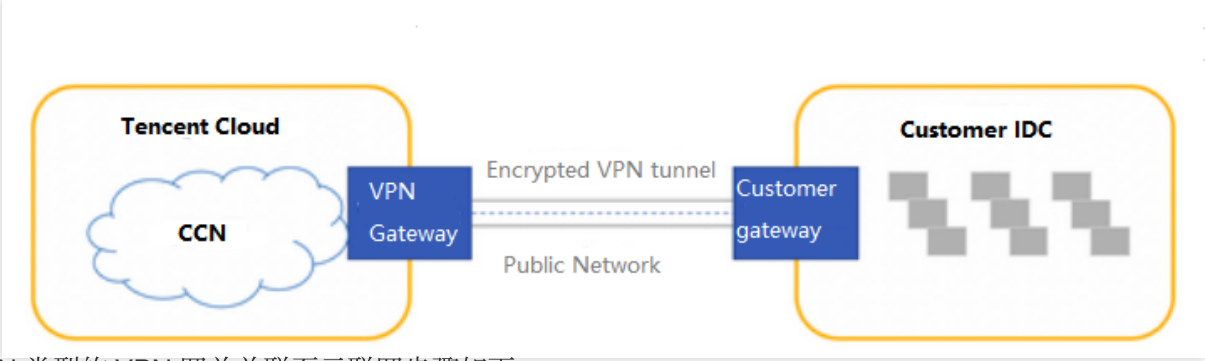
建立 IDC 到云联网的连接

最近更新时间：2024-01-09 14:41:10

CCN 型 VPN 网关可以关联至云联网，实现 IDC 与云联网间的加密通信。本文介绍如何将 CCN 型 VPN 网关关联至云联网。

背景信息

CCN 类型的 VPN 网关可以关联至云联网，每个 CCN 型 VPN 网关可以建立多个 VPN 加密通道，每个 VPN 通道可以打通一个本地 IDC。



将 CCN 类型的 VPN 网关关联至云联网步骤如下：

1. 创建 CCN 型 VPN 网关：VPN 网关是云联网建立 VPN 连接的出口网关，与对端网关配合使用。
2. 关联云联网实例：将创建的 CCN 型 VPN 网关与云联网实例关联。
3. 创建对端网关：对端网关是用来记录 IDC 端的 IPsec VPN 网关公网 IP 地址的逻辑对象（IDC 端必须有固定公网 IP），需与腾讯云 VPN 网关配合使用，一个 VPN 网关可与多个对端网关建立加密的 VPN 网络通道。
4. 创建 VPN 通道： VPN 通道支持 IPsec 加密协议，用于保护数据传输的信息安全。
5. 配置 VPN 网关路由：VPN 通道配置成功后，需要配置 VPN 网关至对端网关的路由。
6. IDC本地配置：在 IDC 侧的“本地网关”上配置另一侧（腾讯云侧）的 VPN 通道信息。
7. 启用 IDC 网段：将 SPD 策略中的对端网段加入云联网中。

操作步骤

步骤一：创建 CCN 型 VPN 网关

1. 登录 私有网络控制台。
2. 在左侧导航栏中选择 **VPN连接** > **VPN网关**。
3. 在顶部导航栏选择**地域**，并在 “VPN 网关”页面单击 **+新建** 。

4. 在弹出的“新建VPN网关”窗口中，填写 VPN 网关名称（如 TomVPNGw），选择关联网络、带宽上限、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：

如需将 CCN 型 VPN 网关新建在指定的可用区下，请提交 工单申请。

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	选择当前网关所在的可用区。
协议类型	支持 IPSec 和 SSL 两种协议类型。
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	此处选择云联网。
标签	标签是对 VPN 网关资源的标识，目的是为了方便更快速的查询和管理 VPN 网关资源，非必选配置，您可按需定义。
计费方式	支持按流量计费。按流量计费适用于带宽波动较大的场景。

步骤二：关联云联网实例

若您已创建云联网实例，请按如下操作关联云联网：

1.1 返回 “VPN 网关“页面，在 VPN 网关列表中，单击已创建的云联网型 VPN 网关 ID。

1.2 在“基本信息“页面，单击所属网络右侧的

，在下拉列表中选择目标云联网实例，并单击**保存**即可。

若您未创建云联网实例，请按如下步骤关联云联网：

1.1 在左侧导航栏单击 **云联网** 。

1.2 在“云联网”页面上方选择**地域**，单击 **+新建** 。

1.3 在弹出的“新建云联网实例”窗口中进行如下操作，完成后单击**确定**。

1.4 填写云联网实例名称、描述，选择计费模式、服务质量、限速方式。

1.5 在“关联实例”下方选择 **VPN 网关**，以及已创建的云联网型 VPN 网关的地域和 ID。

步骤三：创建对端网关

1. 登录 私有网络控制台。

2. 在左侧导航栏选择 **VPN 连接** > **对端网关**。

3. 在“对端网关”页面上方选择**地域**，并单击 **+新建** 。

4. 在弹出的“新建对端网关”窗口中，填写对端网关名称和 IDC 端 VPN 网关的公网 IP，并单击**创建**。

步骤四：创建 VPN 通道

1. 登录 私有网络控制台。
2. 在左侧导航栏选择 **VPN 连接** > **VPN 通道**。
3. 在 “VPN 通道”页面上方选择**地域**，并单击 **+新建** ，进入“新建 VPN 通道”页面。
4. 依据界面提示配置 VPN 通道基本信息。

注意：

每个规则中的多个对端网段间相互不能重叠。

同一网关下多个通道内的规则不能重叠。

SPD 策略中的对端网段可以加入云联网中。

5. DPD 检测配置和健康检查。

DPD 检测：保持默认配置，默认开启，如需修改请参见界面参数进行配置。

健康检查：保持默认配置，默认关闭。

6. （可选）配置 IKE 参数，如果不需要高级配置，可直接单击**下一步**。
7. （可选）配置 IPsec 参数，如果不需要配置，可直接单击**完成**。
8. 基本配置和高级配置完成后单击**创建**。创建成功后，返回 VPN 通道列表页，在操作栏下单击**更多** > **下载配置文件**并完成下载。

步骤五：配置 VPN 网关路由

VPN 通道配置成功后，需要配置 VPN 网关至对端网关的路由。

1. 在左侧导航栏选择 **VPN 链接** > **VPN 网关**，并在右侧 VPN 网关列表中找到创建好的 VPN 网关，并单击其名称。
2. 在 VPN 网关详情页签，单击**路由表**页签，然后单击**新增路由**。
3. 在**新建路由**页面配置 VPN 网关至对端网关的路由策略。

配置项	说明
目的端	填写待访问的对端网络的网段，即对端网关中配置的 IDC 侧提供对外访问的网段。
下一跳类型	系统自动填充 VPN 通道。
下一跳	选择创建好的 VPN 通道。
权重	0 表示优先级高，100表示优先级低。

4. 单击**确定**。

步骤六：IDC 本地配置

完成前4步后，云上 VPN 网关和 VPN 通道的配置已经完成，需要继续在 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。

步骤七：启用 IDC 网段

说明：

本步骤仅针对1.0和2.0版本的VPN网关。3.0版本的 VPN 网关，此处为**路由表**页签。

如果是3.0版本的 CCN 型 VPN 网关，且 VPN 网关已关联至云联网实例时，则下一跳到**云联网**的路由策略，系统将自动学习到并展示在路由条目中，无需手动再次配置。此外，VPN 网关中配置的路由策略也会自动同步到云联网。

针对1.0和2.0版本的 VPN，请执行如下操作启用 IDC 网段：

1. 登录 私有网络控制台。
2. 在左侧导航栏中选择 **VPN 连接** > **VPN 网关**。
3. 在 VPN 网关列表中，单击云联网型 VPN 网关 ID。
4. 在 VPN 网关详情页面，选择 **IDC 网段**页签，并启用目标网段。

结果验证

1. 登录 私有网络控制台。
2. 在左侧导航栏中选择**云联网**。
3. 在云联网列表页中，单击 CCN 型 VPN 网关关联的云联网实例 ID。
4. 在云联网详情页面，选择**路由表**页签，若启用的网段在路由表中，且“状态”为有效，“下一跳”为 CCN 型 VPN 网关，则说明关联成功。

本地网关配置
思科防火墙配置

最近更新时间：2024-01-09 14:41:10

使用 IPsec VPN 建立腾讯云 VPC 到用户 IDC 的连接时，在配置完腾讯云 VPN 网关后，您还需要在用户 IDC 本地站点的网关设备中进行 VPN 配置。本文以思科防火墙为例，介绍如何在本地站点中进行 VPN 配置。

注意：

本文为 Cisco ASA 系列防火墙通用配置，所有版本均支持。

本文所有IP、接口等参数取值均仅用于举例，请具体配置时，使用实际值进行替换。

前提条件

请确保您已经在腾讯云 VPC 内 创建 VPN，并完成 VPN 通道配置。

数据准备

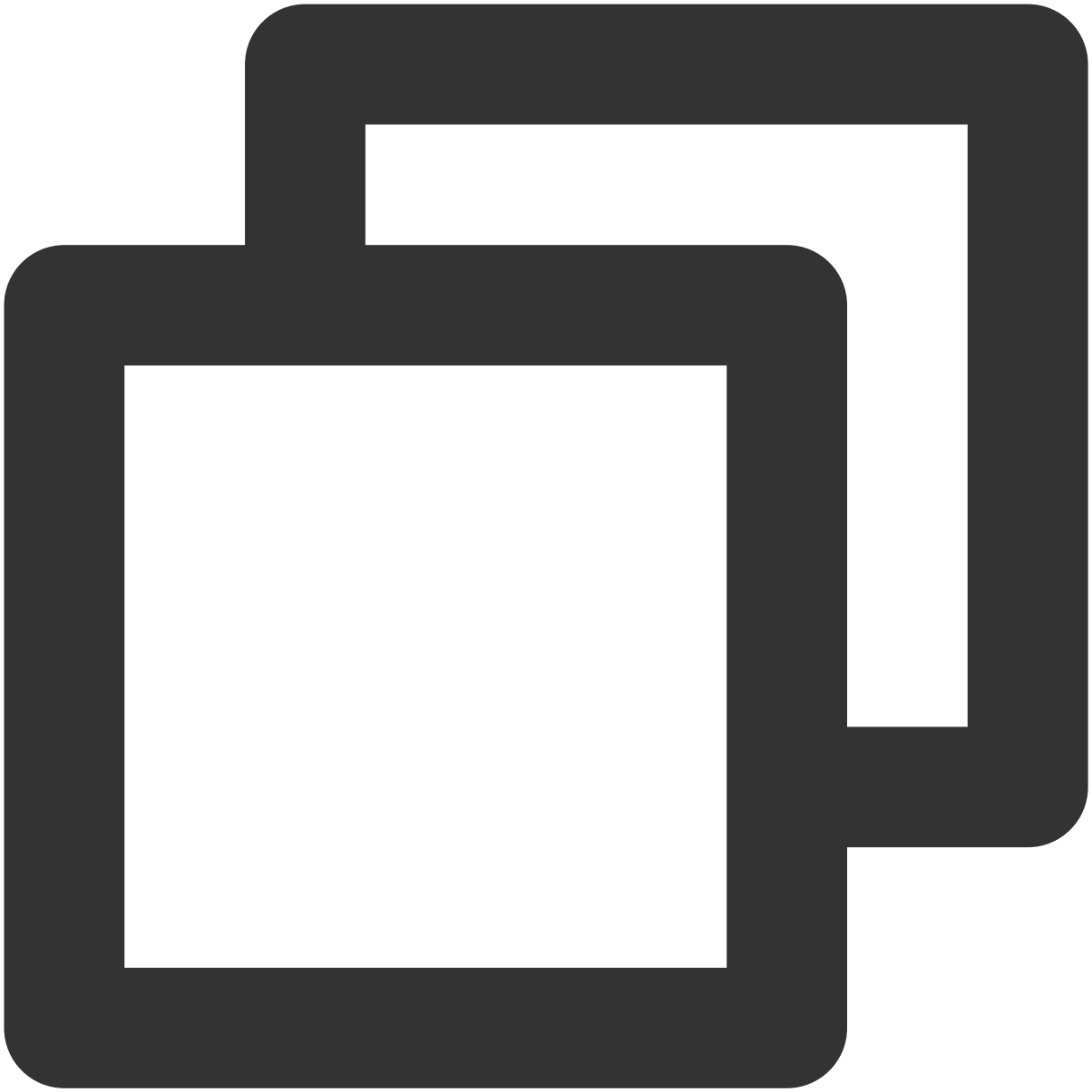
本文 IPsec VPN 配置数据举例如下：

配置项			示例值
网络配置	VPC 信息	子网 CIDR	10.1.1.0/24
		VPN 网关公网 IP	159.xx.xx.242
	IDC 信息	内网 CIDR	172.16.0.0/16
		网关公网 IP	120.xx.xx.76
IPsec 连接配置	IKE 配置	版本	IKEV1
		身份认证方法	预共享密钥
		PSK	tencent@123
		加密算法	AES-128
		认证算法	MD5
		协商模式	main
		本端标识	IP Address：120.xx.xx.76

		远端标识	IP Address：159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec 配置	加密算法	AES-128
		认证算法	MD5
		报文封装模式	Tunnel
		安全协议	ESP
		PFS	disable
		IPsec SA 生存周期（s）	3600s
		IPsec SA 生存周期（KB）	1843200KB
防火墙配置	接口信息	Nameif	outside

操作步骤

适用于基于 SPD 策略转发的 VPN（IKEv1）
适用于基于路由转发的 VPN（IKEv1）
适用于基于 SPD 策略转发的 VPN（IKEv2）
适用于基于路由转发的 VPN（IKEv2）
1. 登录防火墙设备命令配置界面。

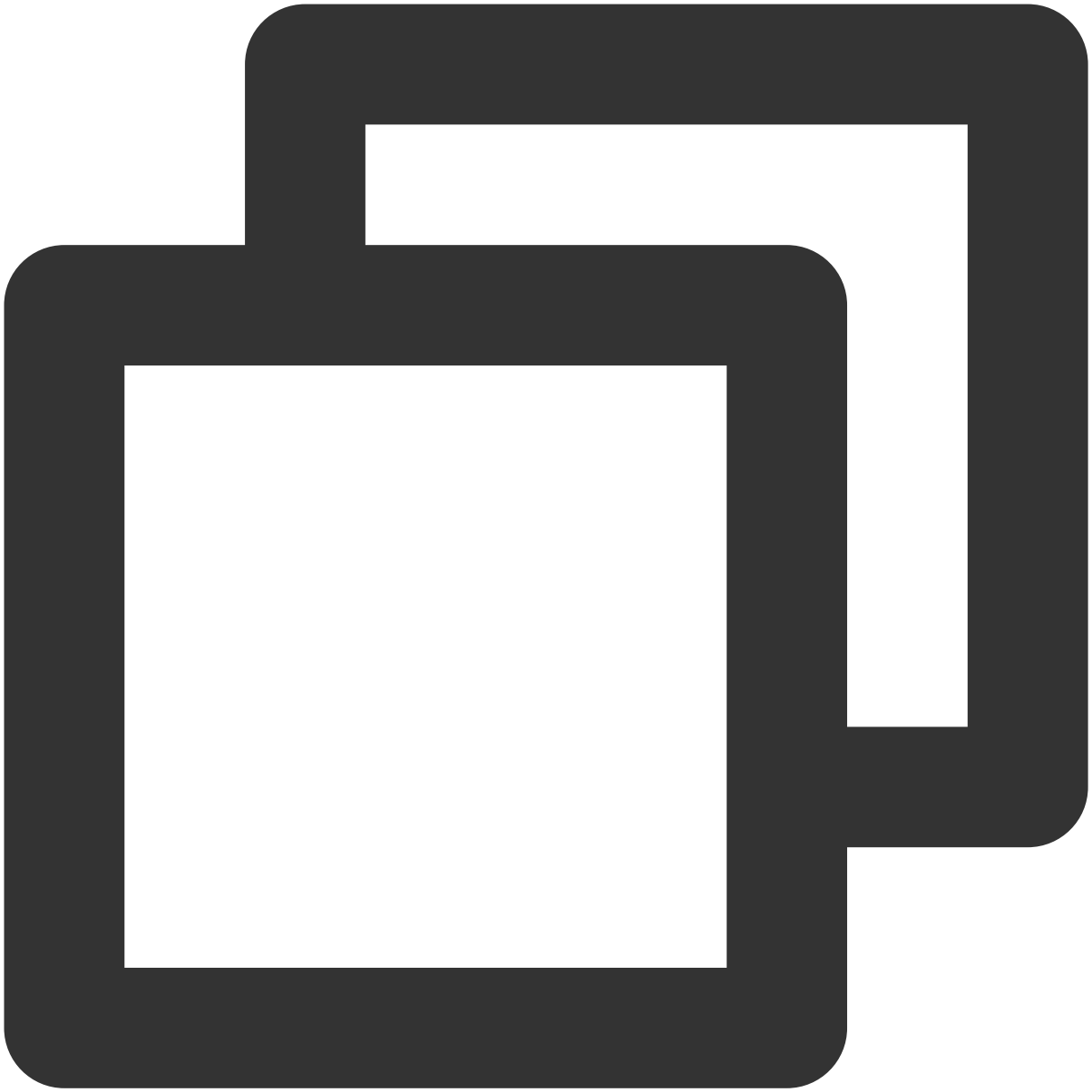


```
   ssh -p admin@10.XX.XX.56

# 通过 SSH 命令登录防火墙配置界面。

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# 输入账号密码，进入用户模式。
```

```
ASA>
ASA> en
Password:

# 输入 enable 和设置的 enable 密码进入特权模式，该模式下只支持查看。

ASA# conf t
ASA(config)#

# 键入“config ter”进入全局模式，在该模式下进行防火墙配置。
```

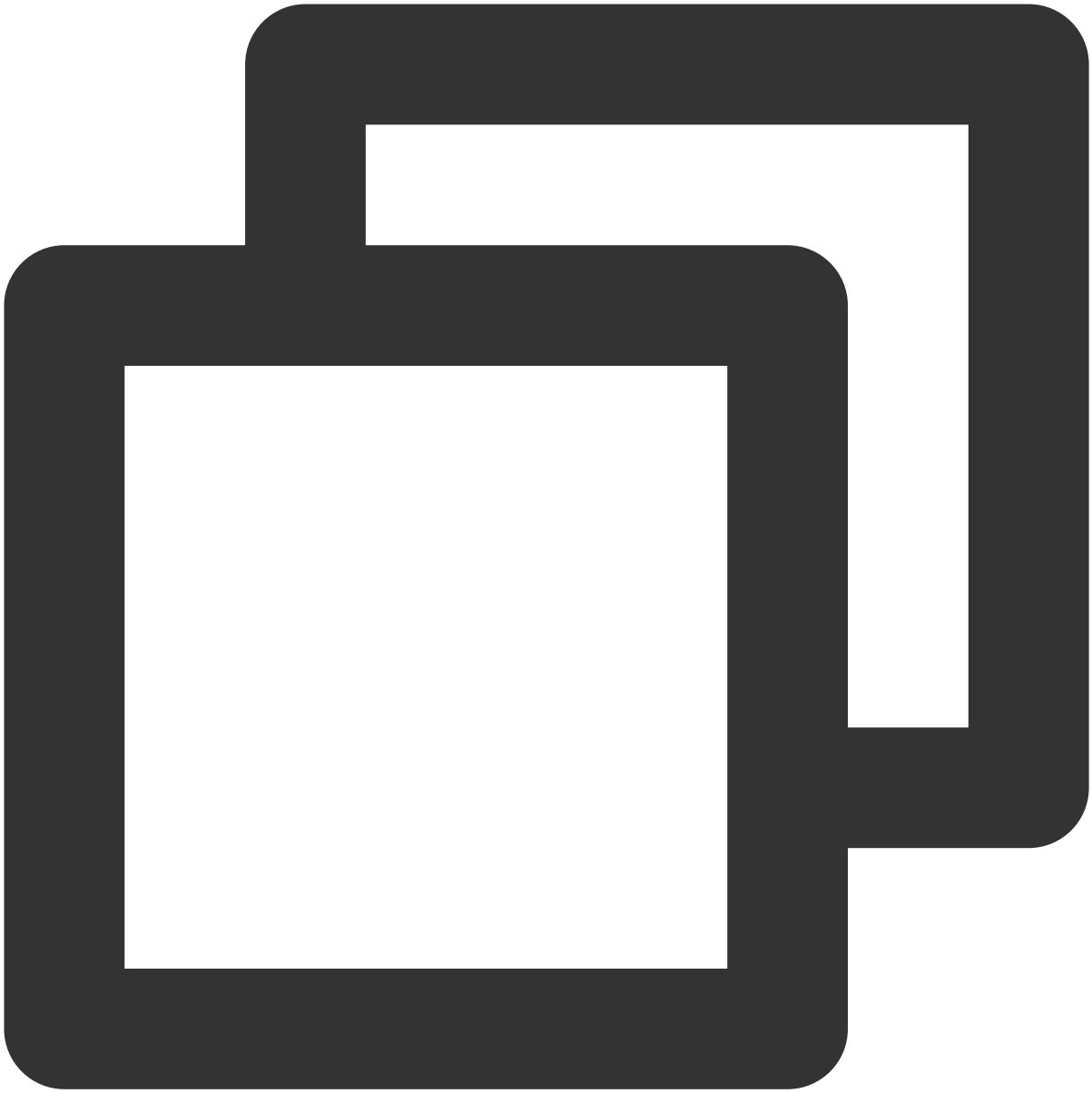
2. 配置防火墙接口。

在全局模式下配置对接腾讯云端的防火墙接口。



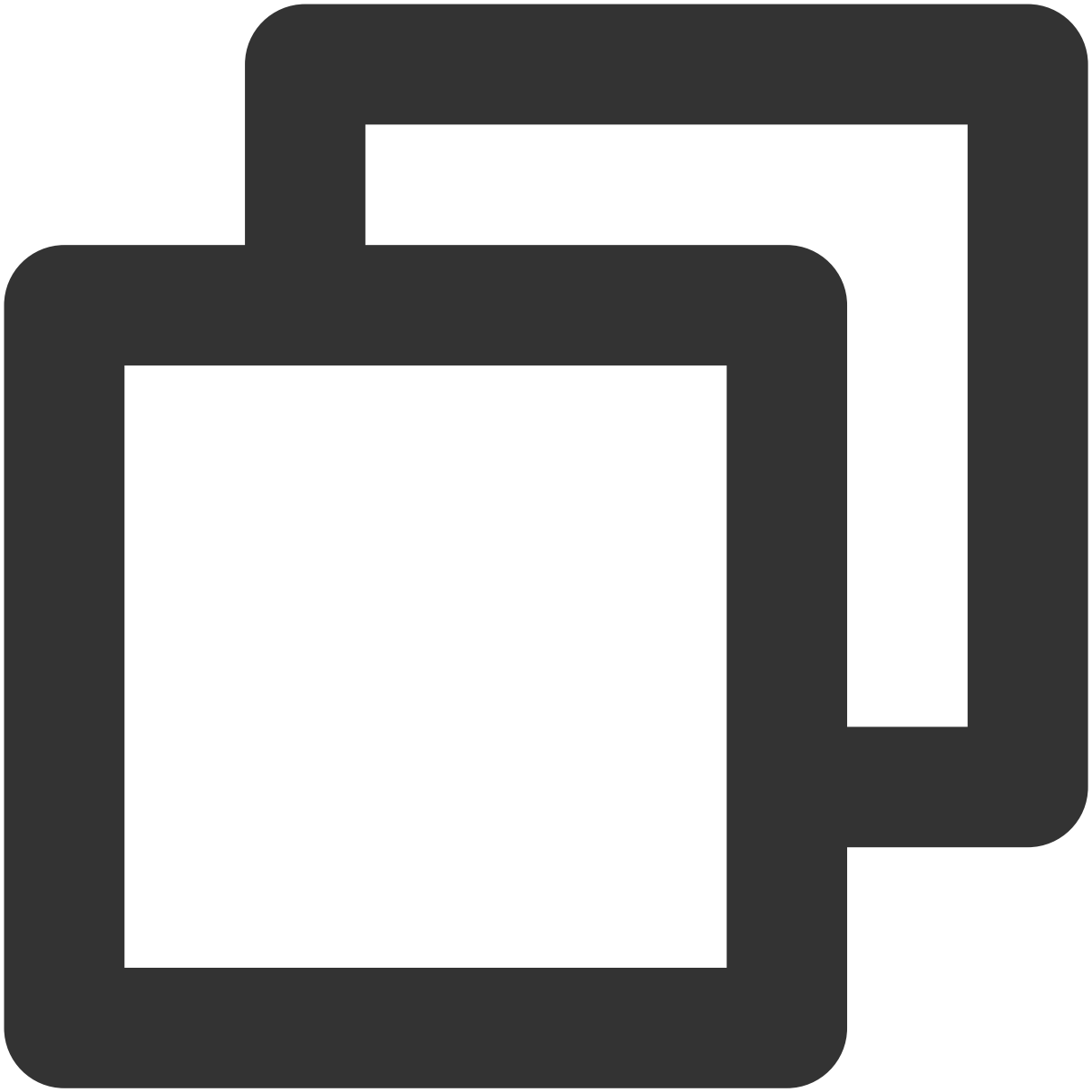
```
interface GigabitEthernet0/0
nameif outside   # 定义端口的安全域名。
security-level 0   # 定义端口的安全域等级。
ip address 120.XX.XX.76 255.255.255.252   # 配置 VPN 通道本端公网 IP 地址。
```

3. 配置 isakmp 策略。



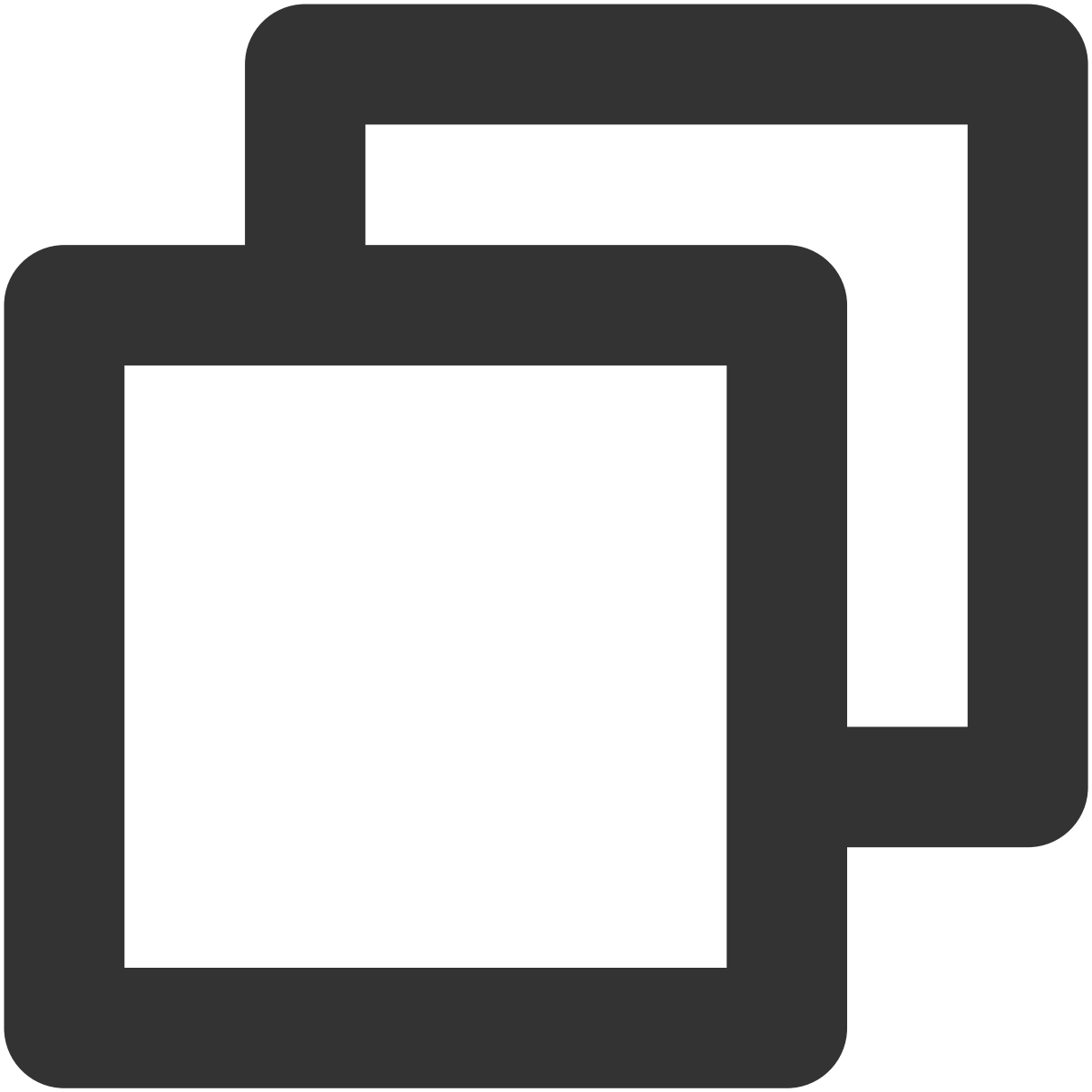
```
crypto ikev1 enable outside  # 在外部接口上启用 IKE。
crypto ikev1 policy 10  # 定义 ikev1 第一阶段协商使用参数，序号为10，序号越小越优先，范围
authentication pre-share  # 配置认证方法为预共享密钥。
encryption AES-128  #配置第一阶段协商数据包封装加密算法，默认为AES-128。
hash MD5  # 为 IKE 策略指定哈希算法为 MD5，默认为 SHA。
group 2  # 为 IKE 策略指定 Diffie-Hellman 组为组2，默认为 group 2
lifetime 86400  # 指定 SA 生命周期，默认为86400秒。
```

4. 配置预共享密码。



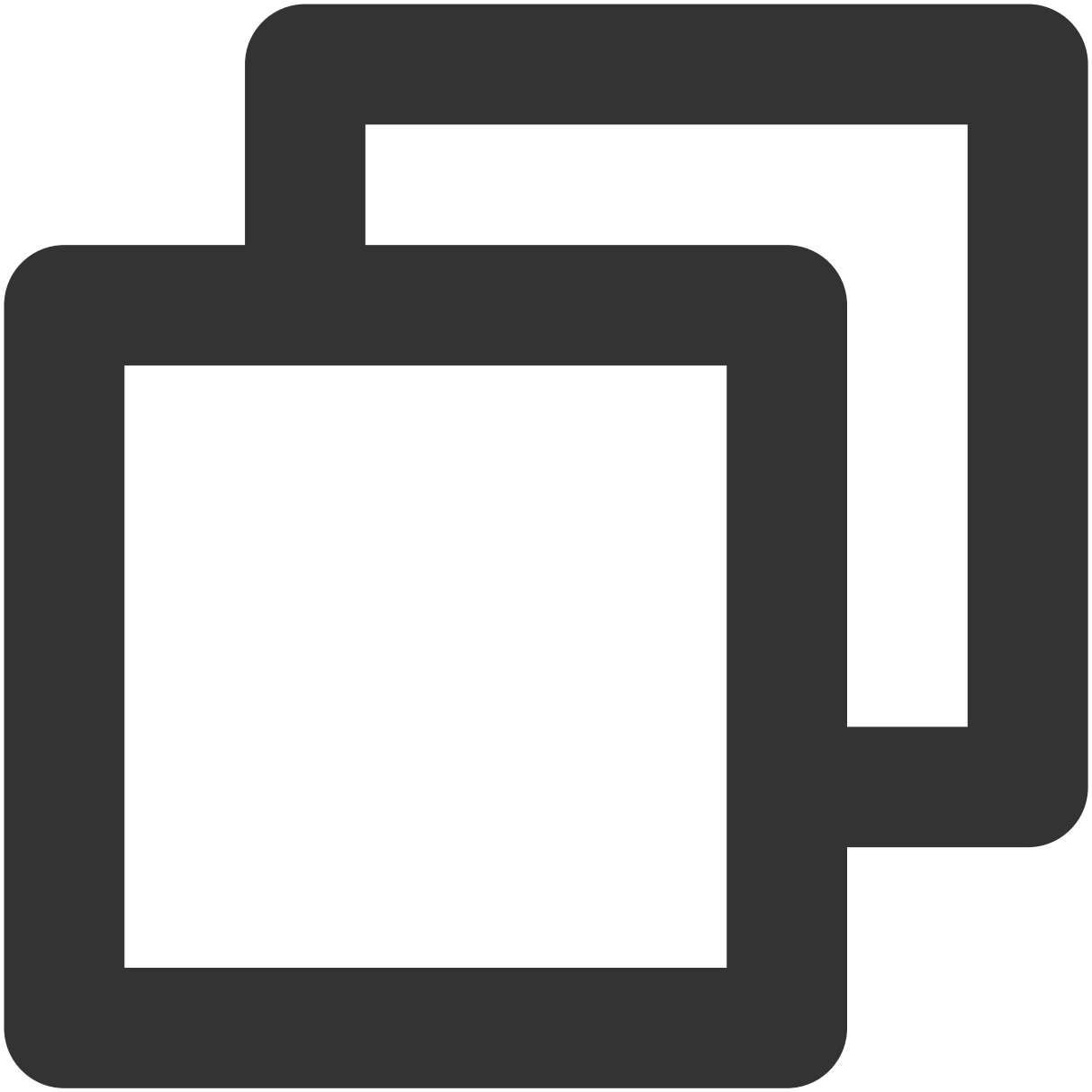
```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # 创建一个ipsec隧道组，type 为点到点。
tunnel-group 159.XX.XX.242 ipsec-attributes  # 配置隧道组属性，并指定预共享密钥。
ikev1 pre-shared-key tencent@123  # 密钥可为1～128个字符的字母、数字或者字符串。
```

5. 配置 IPsec 安全协议。



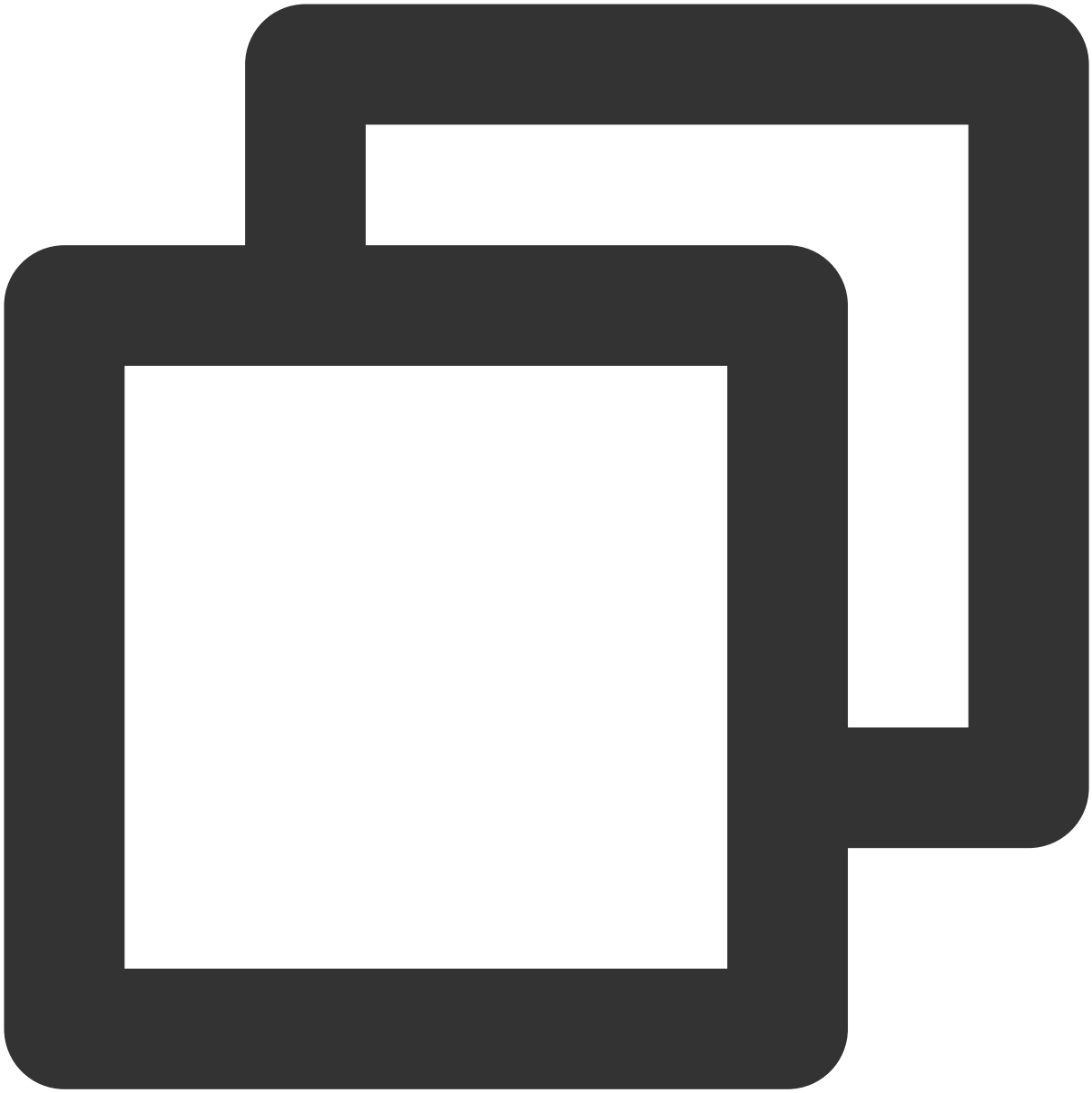
```
crypto ipsec ikev1 transform-set TS esp-aes esp-md5-hmac  # 指定 IPsec 第二阶段协商
```

6. 配置 ACL。



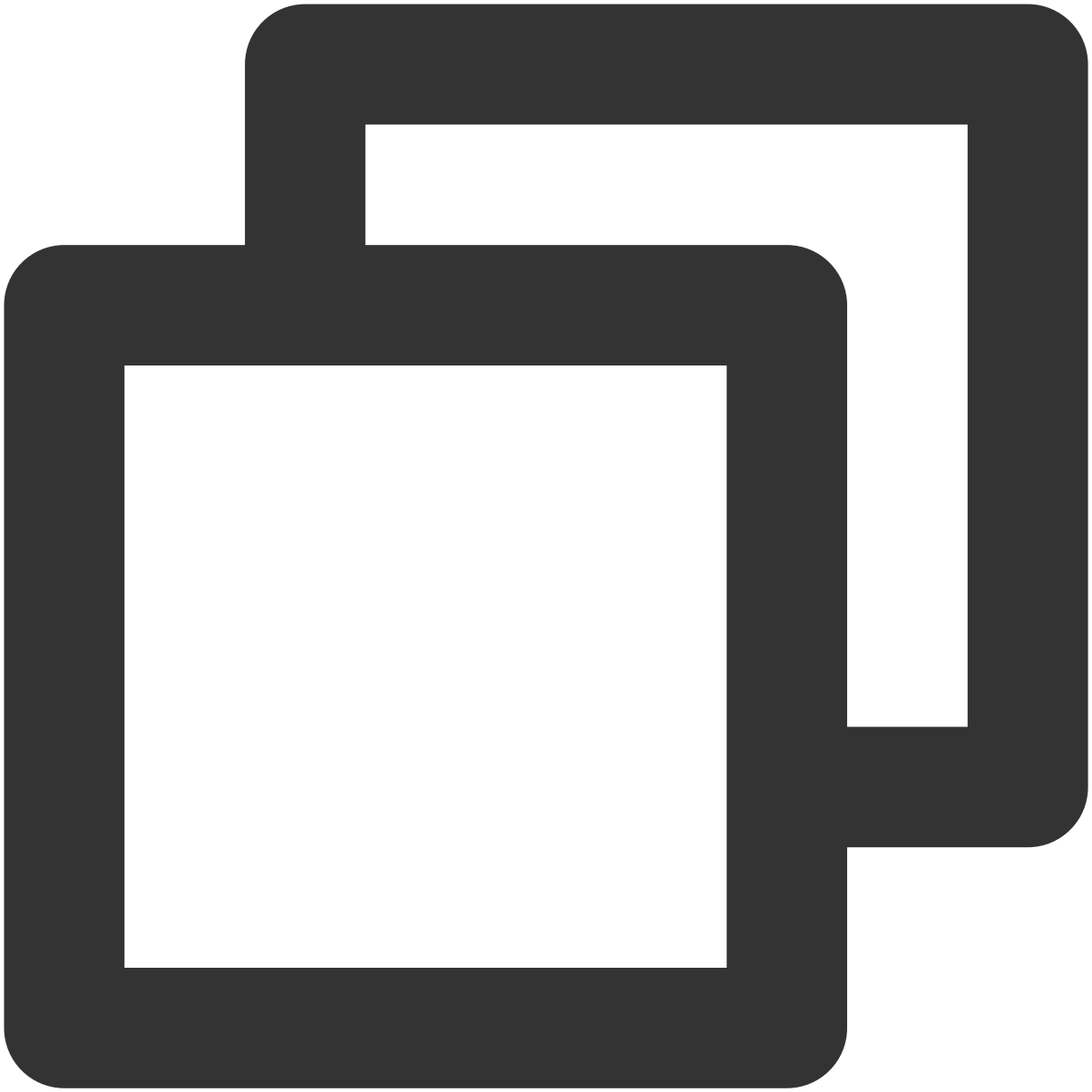
```
access-list INTERESTING extended permit ip 172.XX.XX.0 255.255.0.0 10.1.1.0 255.
```

7. 配置 IPsec 策略。



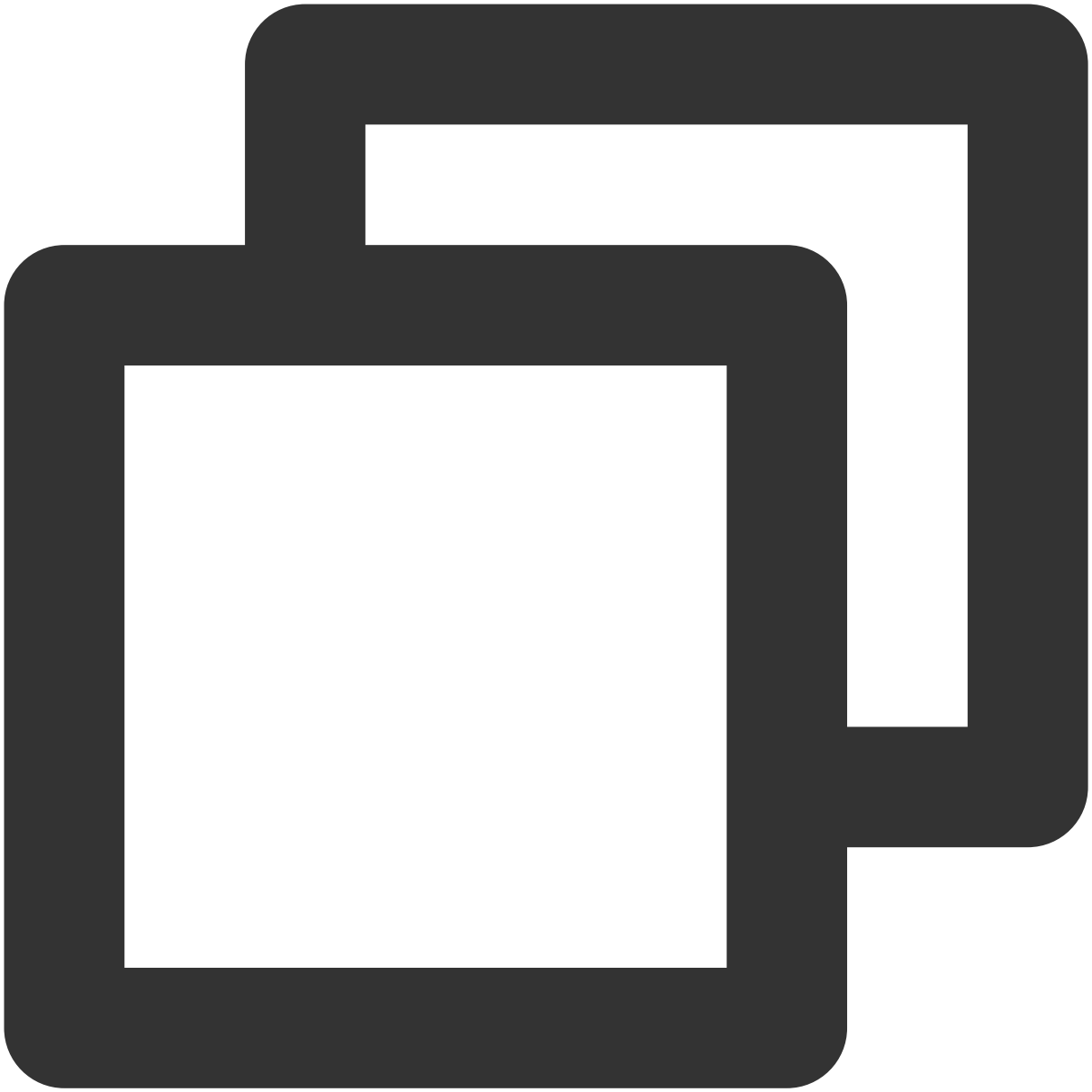
```
crypto map CMAP 1 match address INTERESTING  # 调用 ACL，使满足 ACL 的源网段或者目的网
crypto map CMAP 1 set peer 159.XX.XX.242  # 将被 IPsec 保护的流量转发到的对端 VPN 公网
crypto map CMAP 1 set ikev1 transform-set TS  # 为加密映射条目配置 IKEv1 协议。
crypto map CMAP 1 set security-association lifetime seconds 3600  # 配置加密密钥的生
```

8. 启用 IPsec 策略。



```
rypto map CMAP interface outside  # 将上一步配置的加密映射应用于外部接口。
```

9. 配置静态路由。

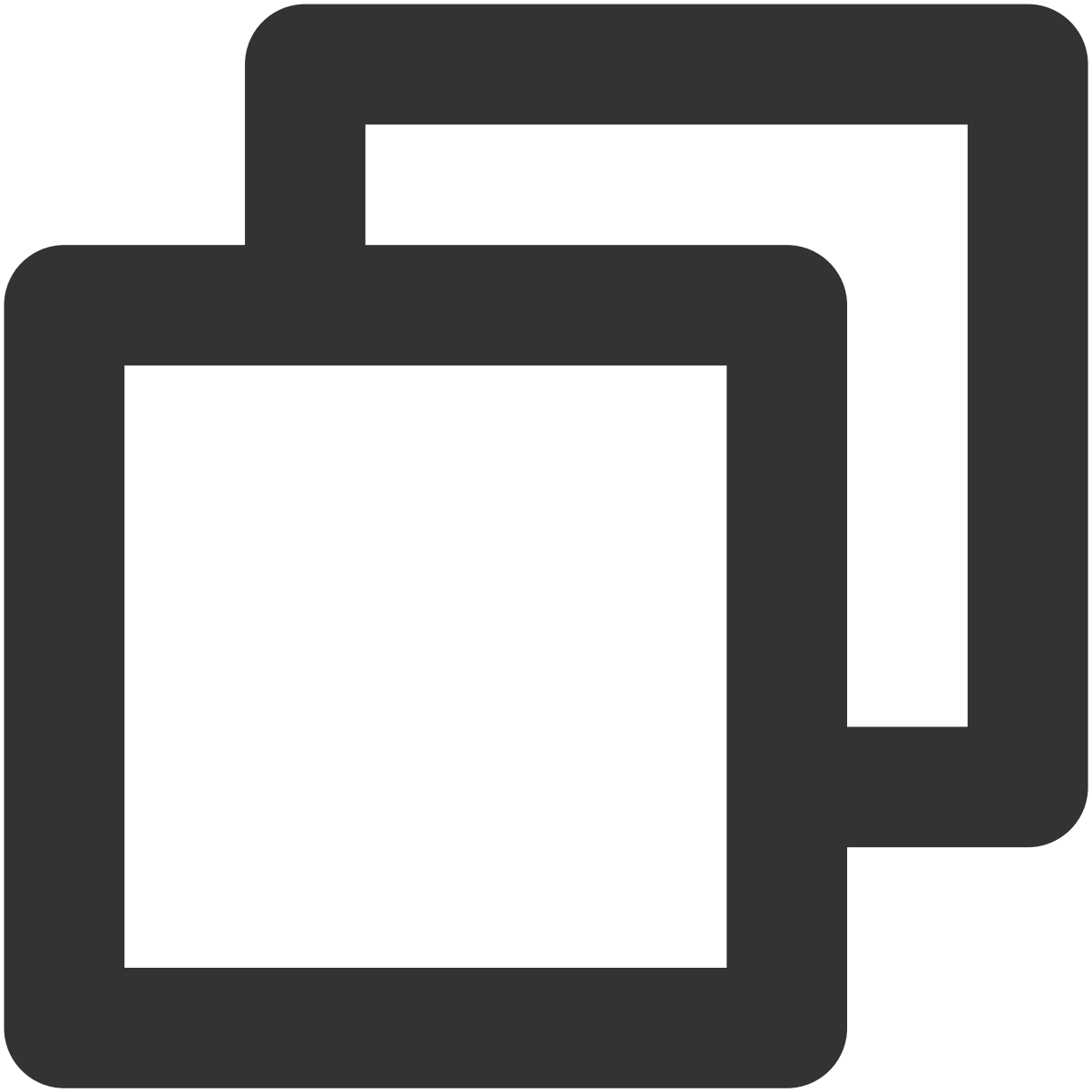


```
route outside 10.1.1.0 255.255.255.0 159.XX.XX.242 1   # 将待加密保护的数据网段引向 IP
```

10. 测试 VPN 连通性。

执行 Ping 命令测试 VPN 的连通性。

1. 登录防火墙设备命令配置界面。

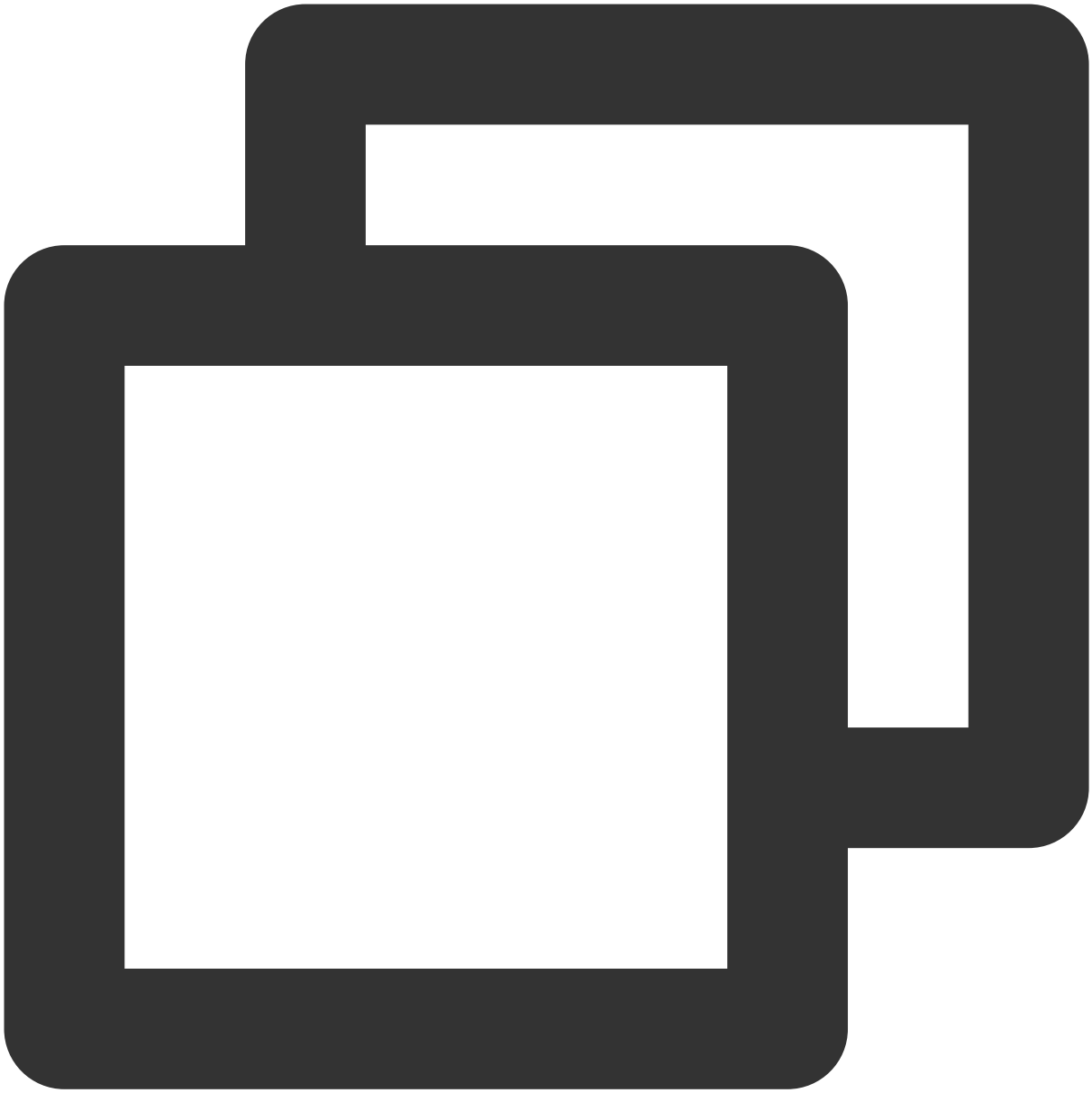


```
   ssh -p admin@10.XX.XX.56

# 通过 SSH 命令登录防火墙配置界面。

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# 输入账号密码，进入用户模式。
```

```
ASA>
ASA> en
Password:

# 输入enable和设置的enable密码进入特权模式，该模式下只支持查看。

ASA# conf t
ASA(config)#

# 键入“config ter”进入全局模式，在该模式下进行防火墙配置。
```

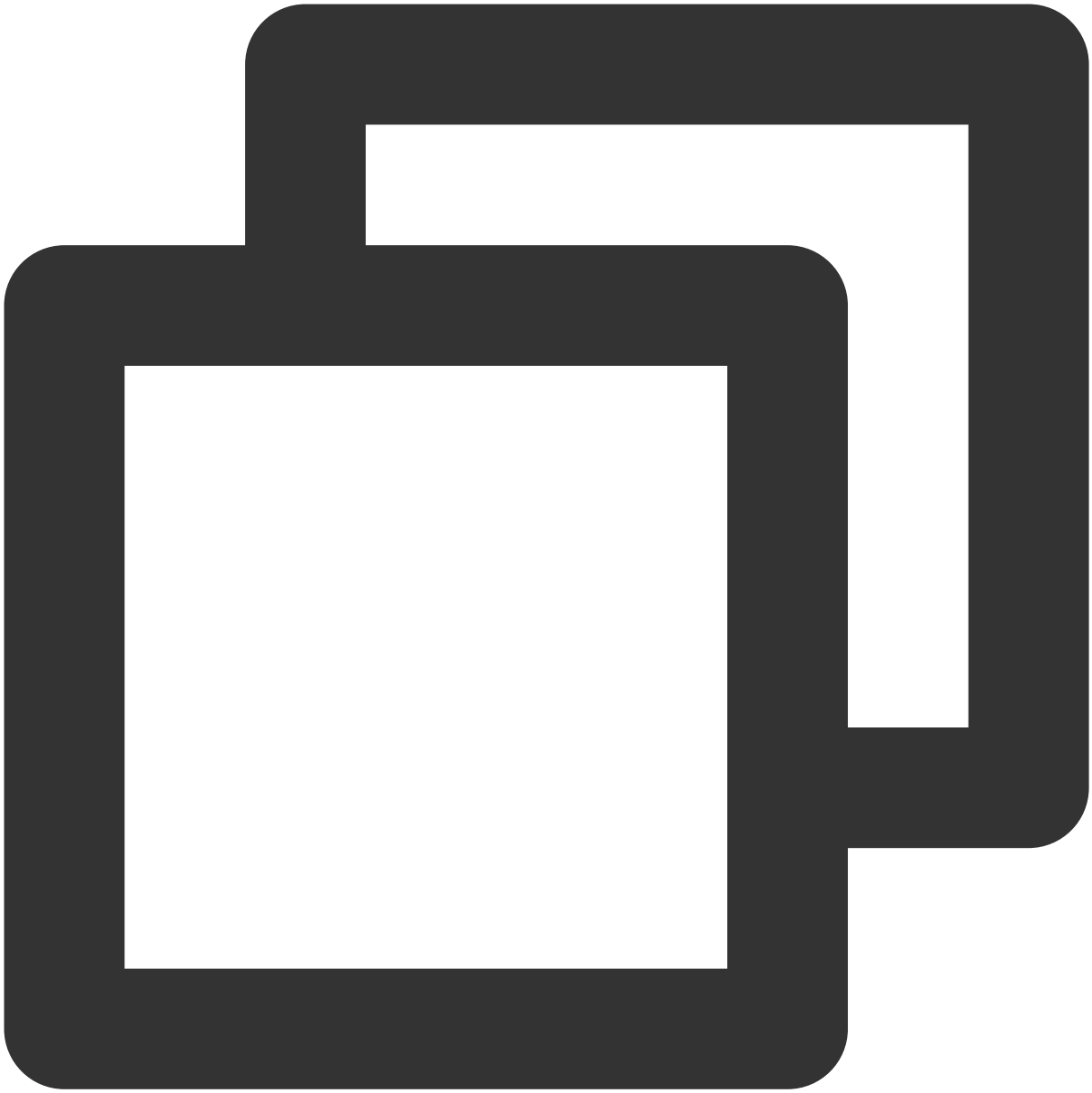
2. 配置防火墙接口。

在全局模式下配置对接腾讯云端的防火墙接口



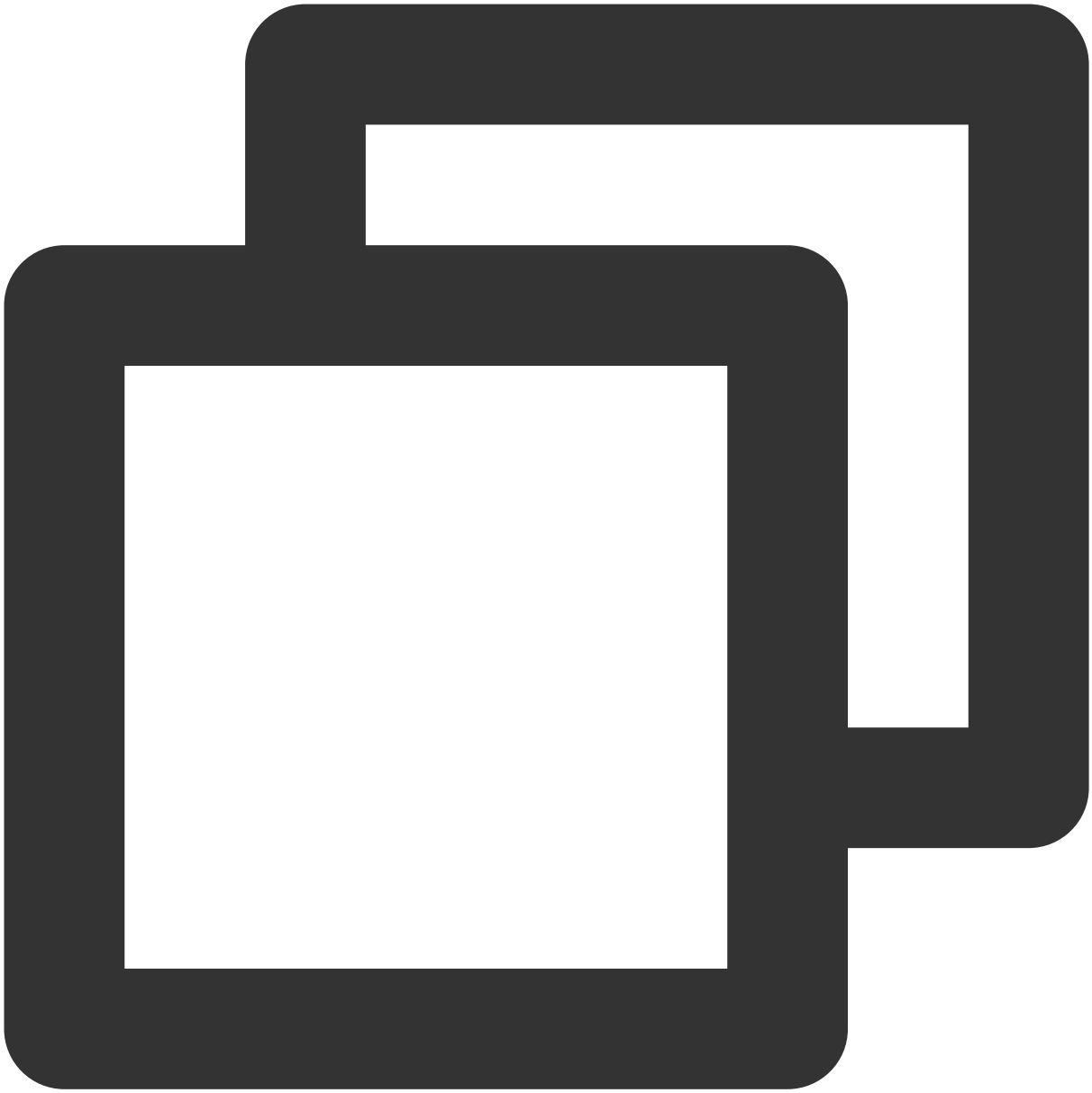
```
interface GigabitEthernet0/0
nameif outside   # 定义端口的安全域名。
security-level 0   # 定义端口的安全域等级。
ip address 120.XX.XX.76 255.255.255.252   # 配置 VPN 通道本端的公网 IP 地址。
```

3. 配置 isakmp 策略。



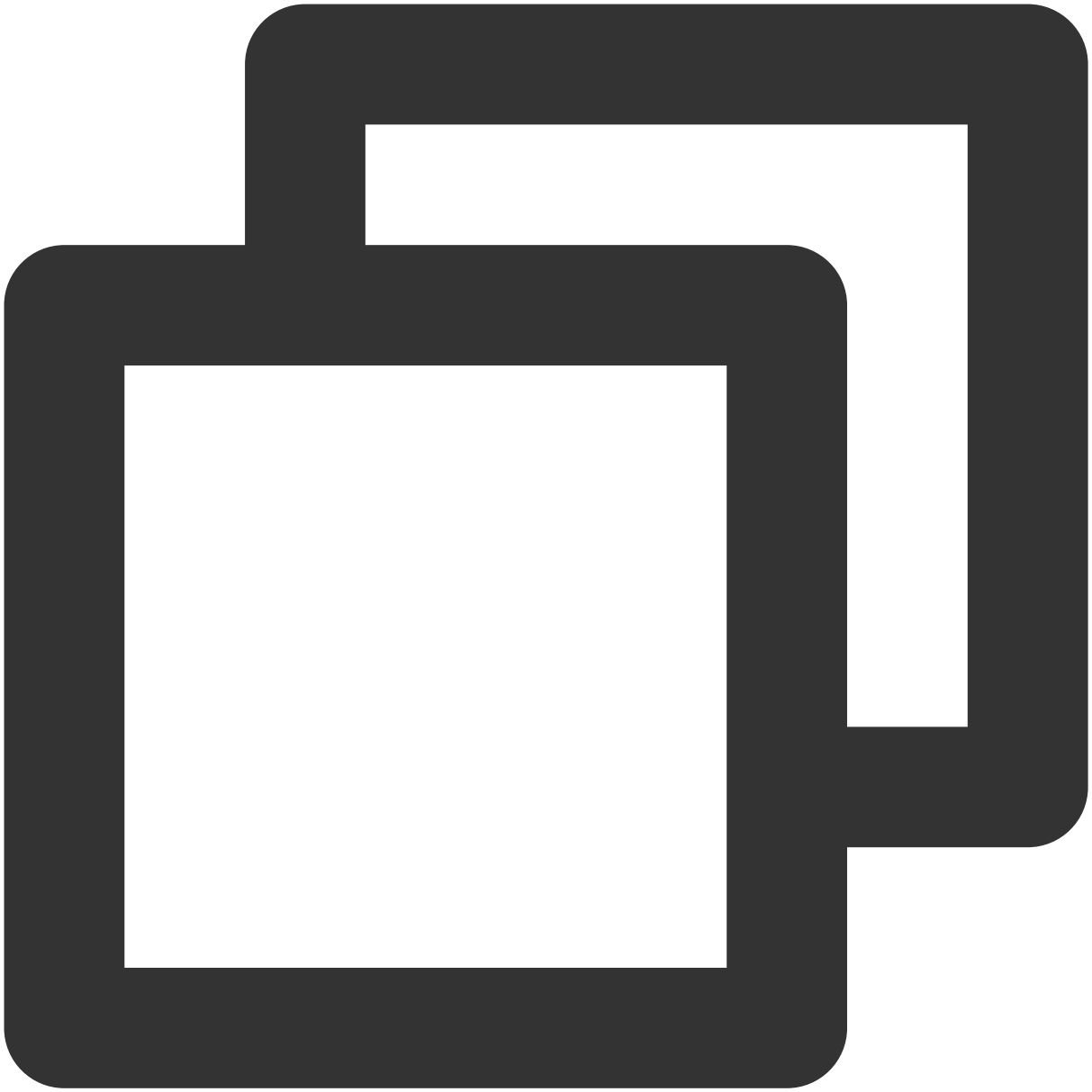
```
crypto ikev1 policy 10  # 定义 ikev1 第一阶段协商使用参数，序号为10，序号越小越优先，范围
authentication pre-share  # 配置认证方法为预共享密钥。
encryption AES-128  # 配置第一阶段协商数据包封装加密算法，默认为AES-128。
hash MD5  # 为 IKE 策略指定哈希算法为 MD5，默认为 SHA。
group 2  # 为 IKE 策略指定 Diffie-Hellman 组为组2，默认为 group 2
lifetime 86400  # 指定 SA 生命周期，默认为86400秒。
```

4. 配置预共享密码。



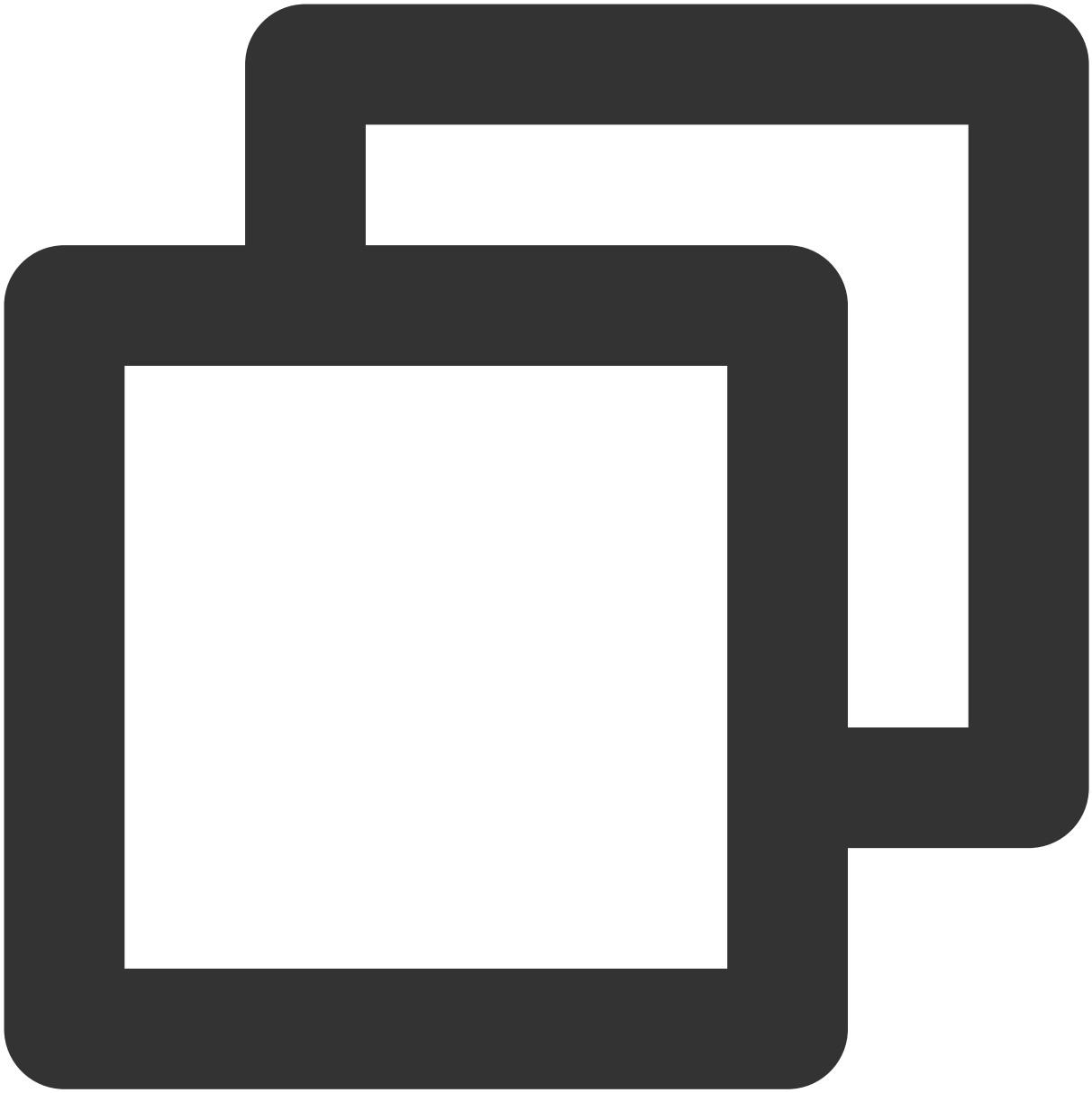
```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # 创建一个ipsec隧道组，type 为点到点。
tunnel-group 159.XX.XX.242 ipsec-attributes  # 配置隧道组属性，并指定预共享密钥。
 ikev1 pre-shared-key tencent@123  # 密钥可为1～128个字符的字母、数字或者字符串。
```

5. 配置 IPsec 安全协议。



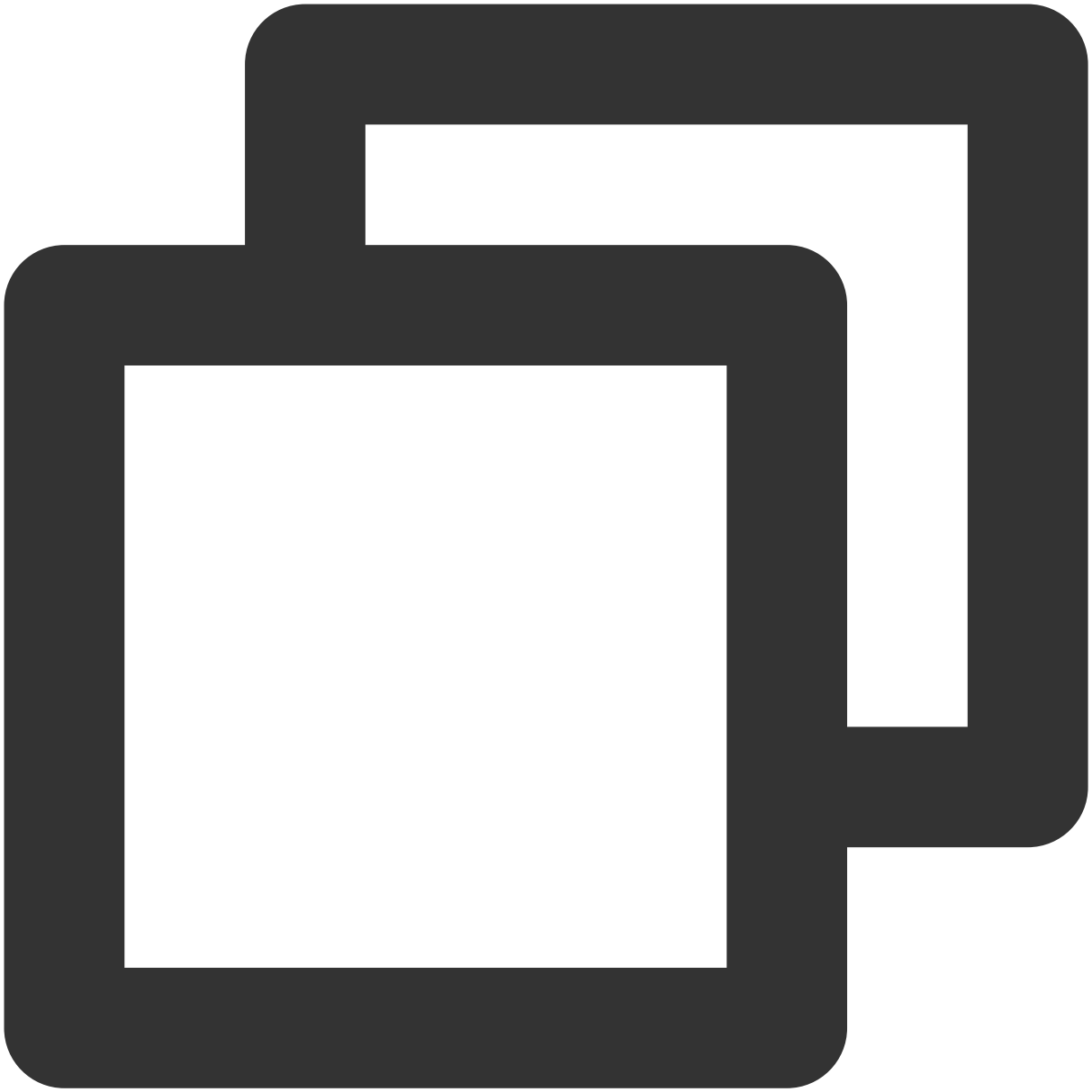
```
crypto ipsec ikev1 transform-set TS esp-aes esp-md5-hmac  # 指定 IPsec 第二阶段协商
```

6. 配置 IPsec 策略。



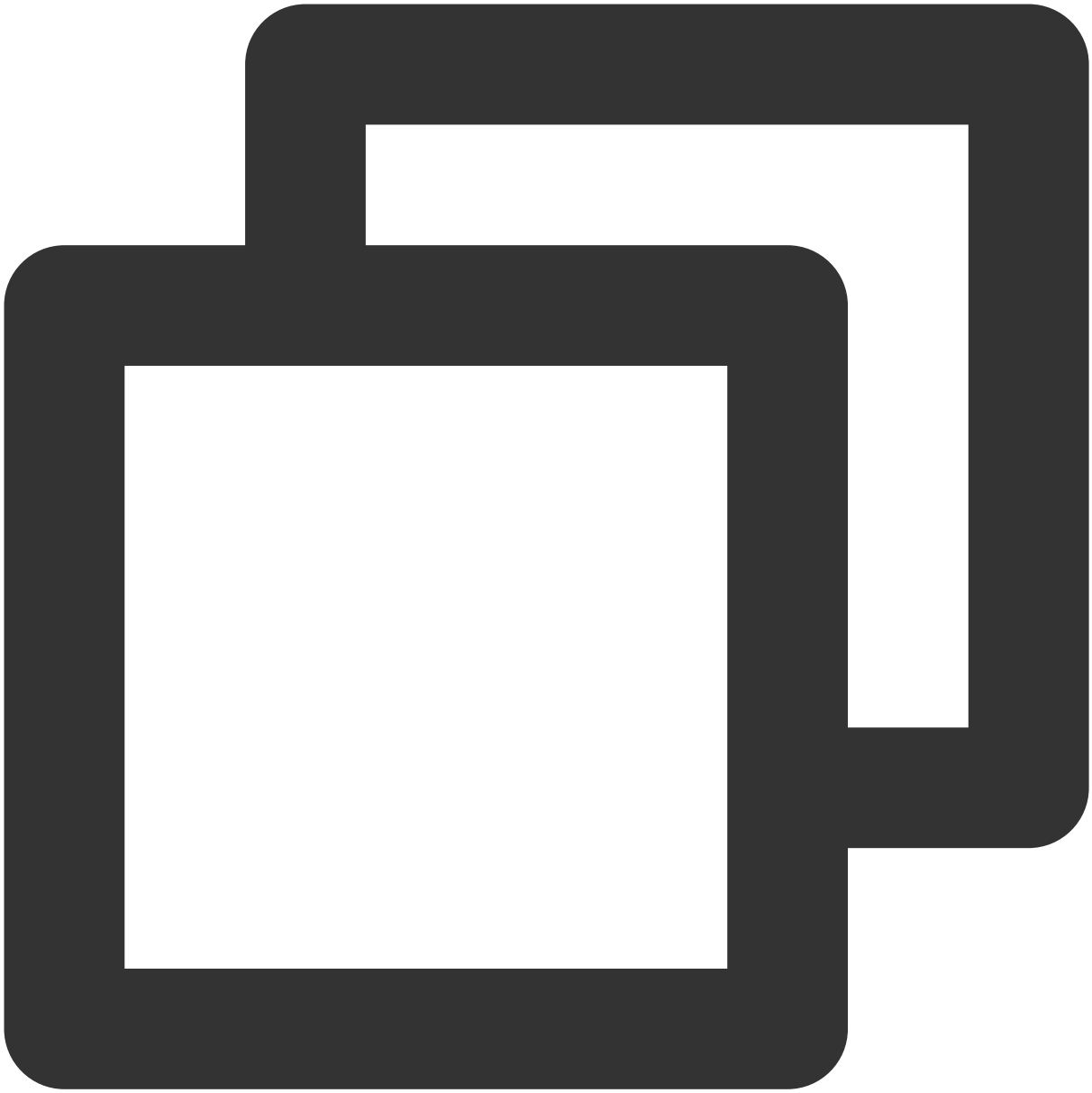
```
crypto ipsec profile PROFILE1
set ikev1 transform-set TS  # 为加密映射条目指定IKEv1 ipsec安全提议
set security-association lifetime kilobytes 1843200  # 设置 SA 生命周期内，VPN之间可
set security-association lifetime seconds 3600  # 设置加密密钥的生命周期，默认千字节数
```

7. 启用 IPsec 策略。



```
interface Tunnel100
tunnel source interface outside  # 配置 VPN 的更新源为outside口。
tunnel destination 159.XX.XX.242  # 配置对端 VPN 的公网 IP 地址，本处为腾讯云 VPN 公网
tunnel mode ipsec ipv4  # 配置 tunnel口 使用的协议。
tunnel protection ipsec profile PROFILE1  # 调用 IPsec 策略对经过 tunnel 口的数据进行
```

8. 配置静态路由。

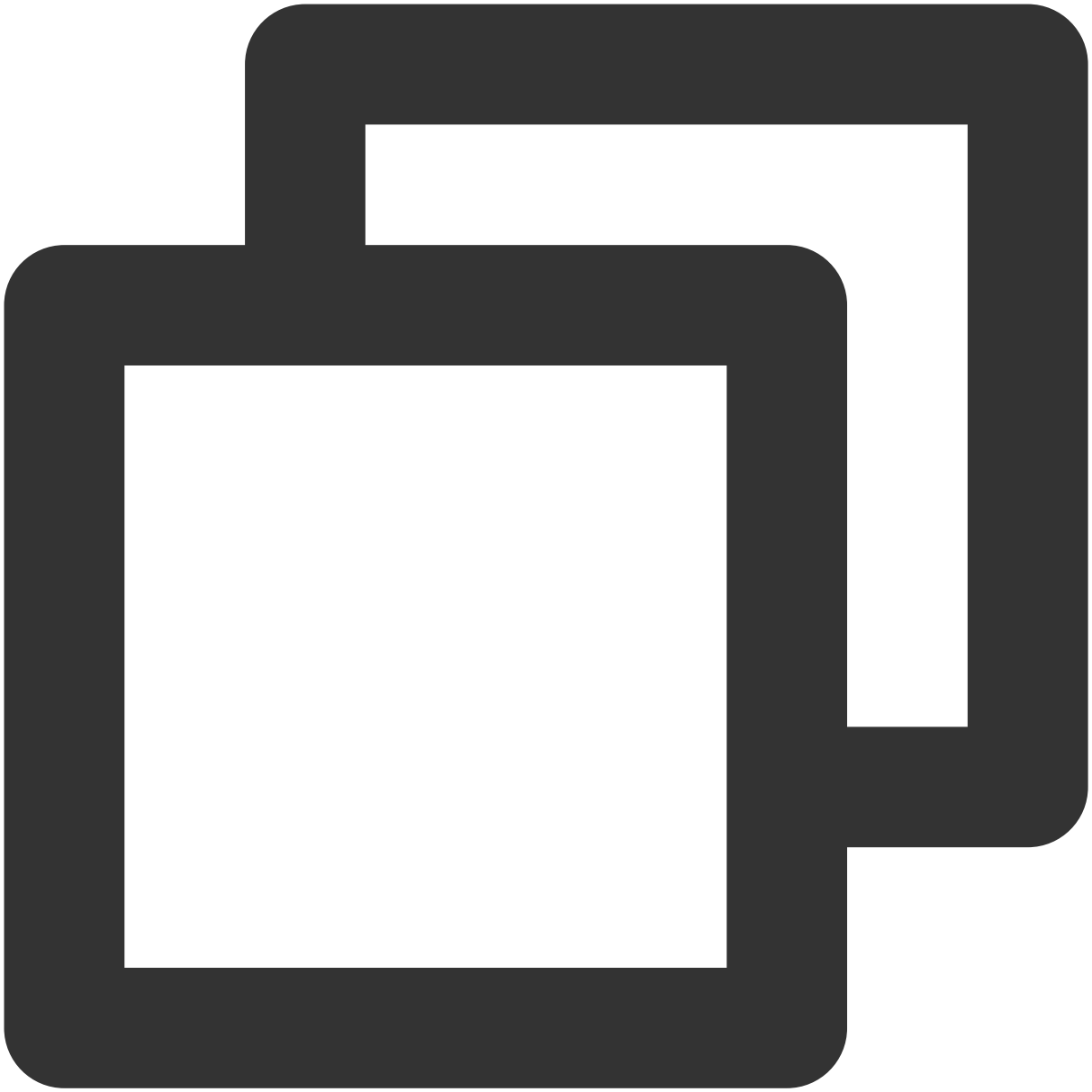


```
route vti 10.1.1.0 255.255.255.0 159.XX.XX.242    # 将待加密保护的数据包引到 tunnel 口
```

9. 测试 VPN 连通性。

执行 Ping 命令测试 VPN 的连通性。

1. 登录防火墙设备命令配置界面。

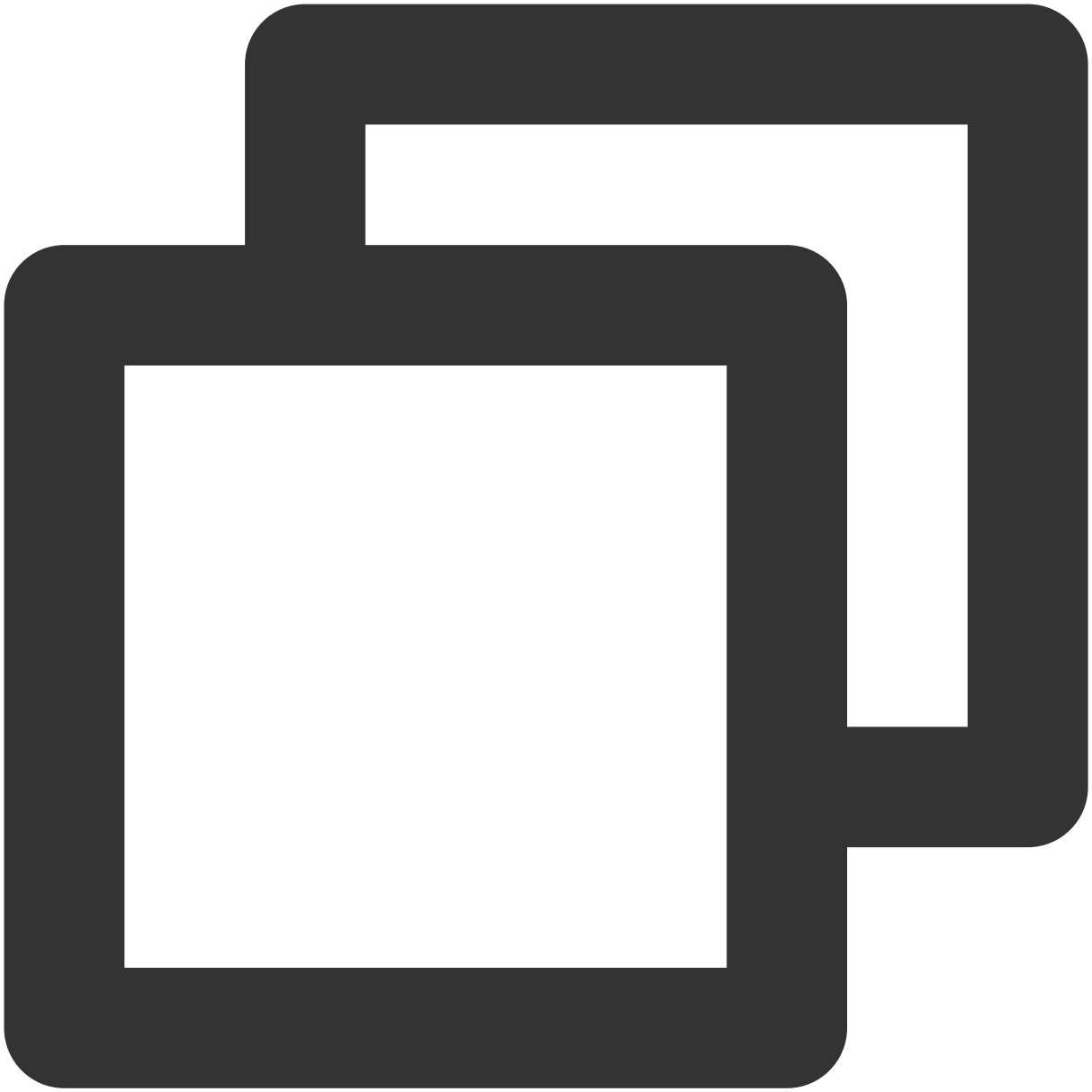


```
   ssh -p admin@10.XX.XX.56

# 通过 SSH 命令登录防火墙配置界面。

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# 输入账号密码，进入用户模式。
```

```
ASA>
ASA> en
Password:

# 输入enable和设置的enable密码进入特权模式，该模式下只支持查看。

ASA# conf t
ASA(config)#

# 键入“config ter”进入全局模式，在该模式下进行防火墙配置。
```

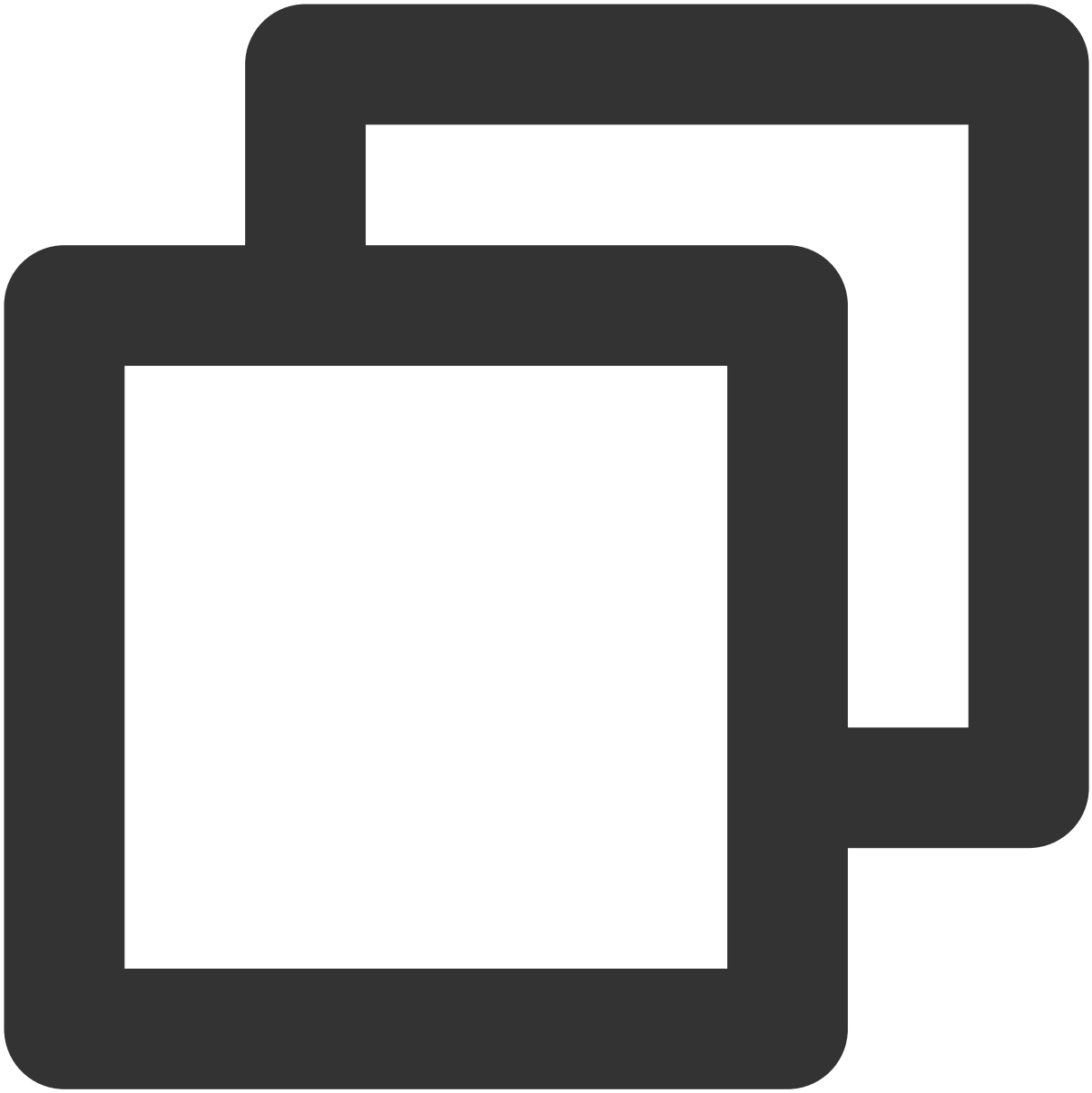
2. 配置防火墙接口。

在全局模式下配置对接腾讯云端的防火墙接口。



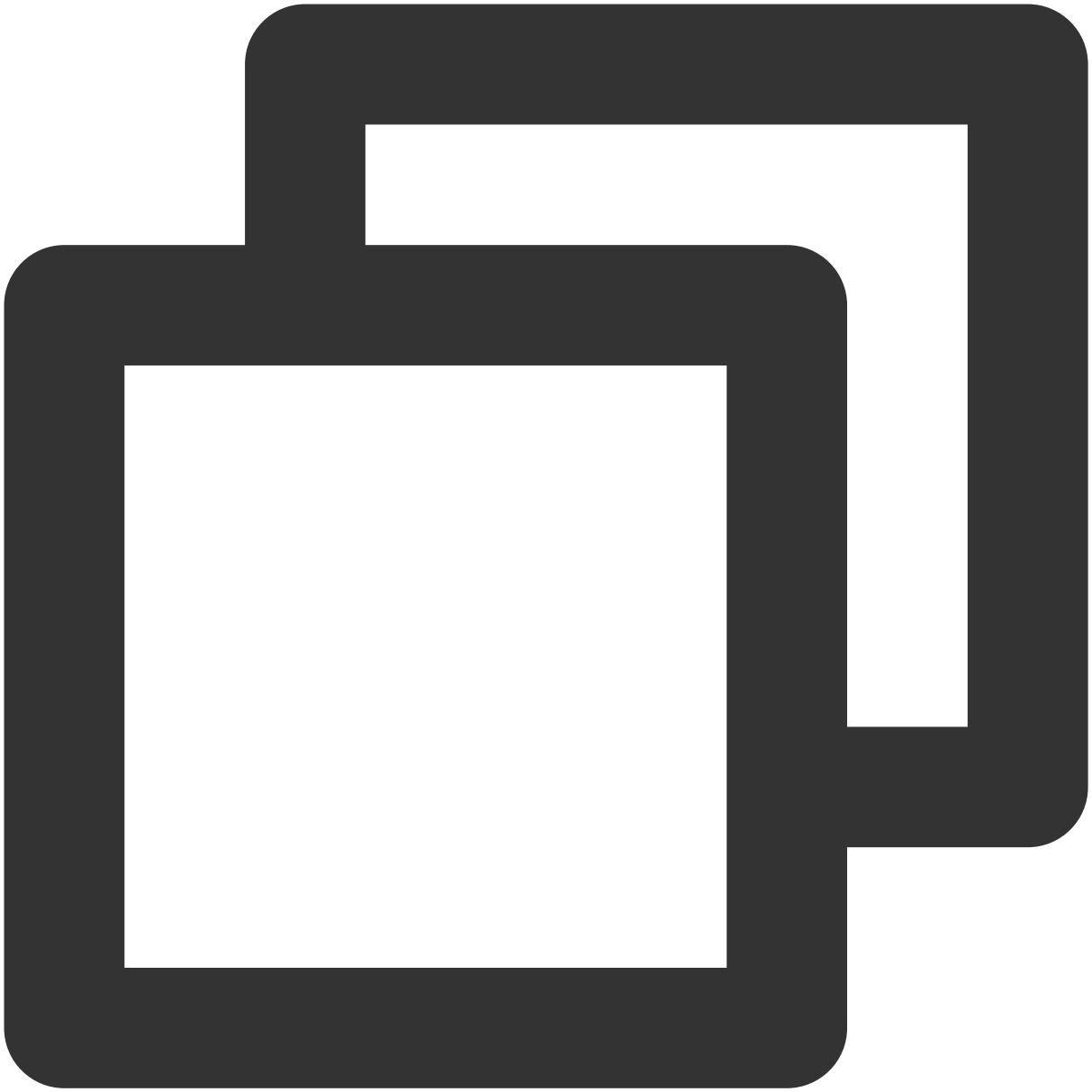
```
interface GigabitEthernet0/0
nameif outside   # 定义端口的安全域名。
security-level 0   # 定义端口的安全域等级。
ip address 120.XX.XX.76 255.255.255.252   # 配置 VPN 通道本端公网 IP 地址。
```

3. 配置 isakmp 策略。



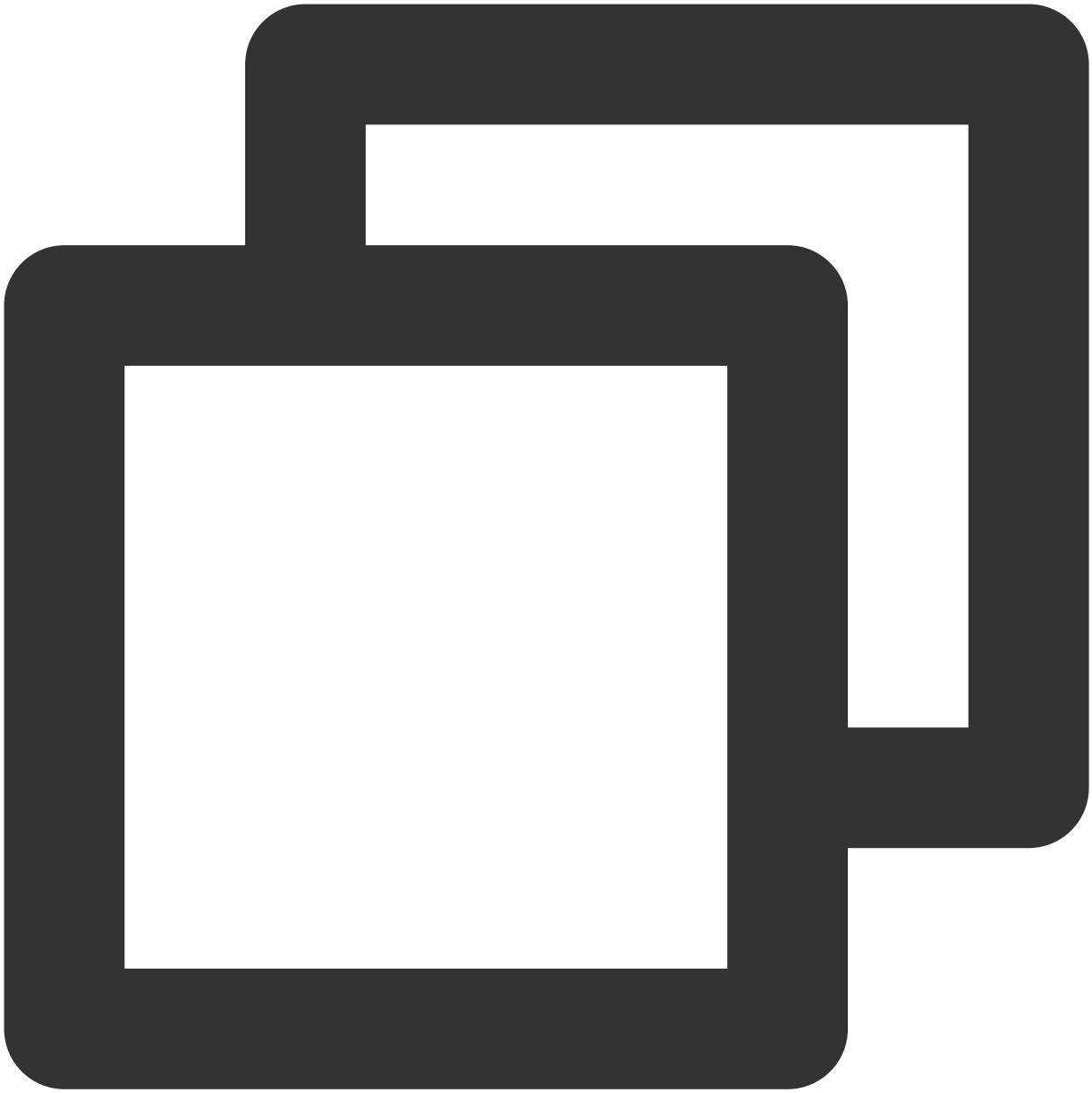
```
crypto ikev2 enable outside  # 在外部接口上启用 IKEv2。
crypto ikev2 policy 10  # 定义 ikev2 第一阶段协商使用参数，序号为10，序号越小越优先，范围
authentication pre-share  # 配置认证方法为预共享密钥。
encryption AES-128  # 配置第一阶段协商数据包封装加密算法，默认为AES-128。
integrity MD5  # 为 IKE 策略指定哈希算法为 MD5，默认为 SHA。
group 2  # 为 IKE 策略指定 Diffie-Hellman 组为组2，默认为 group 2。
prf sha # 设置加密算法。
lifetime seconds 86400  # 设置 SA 生命周期，默认为86400秒。
```

4. 配置组策略



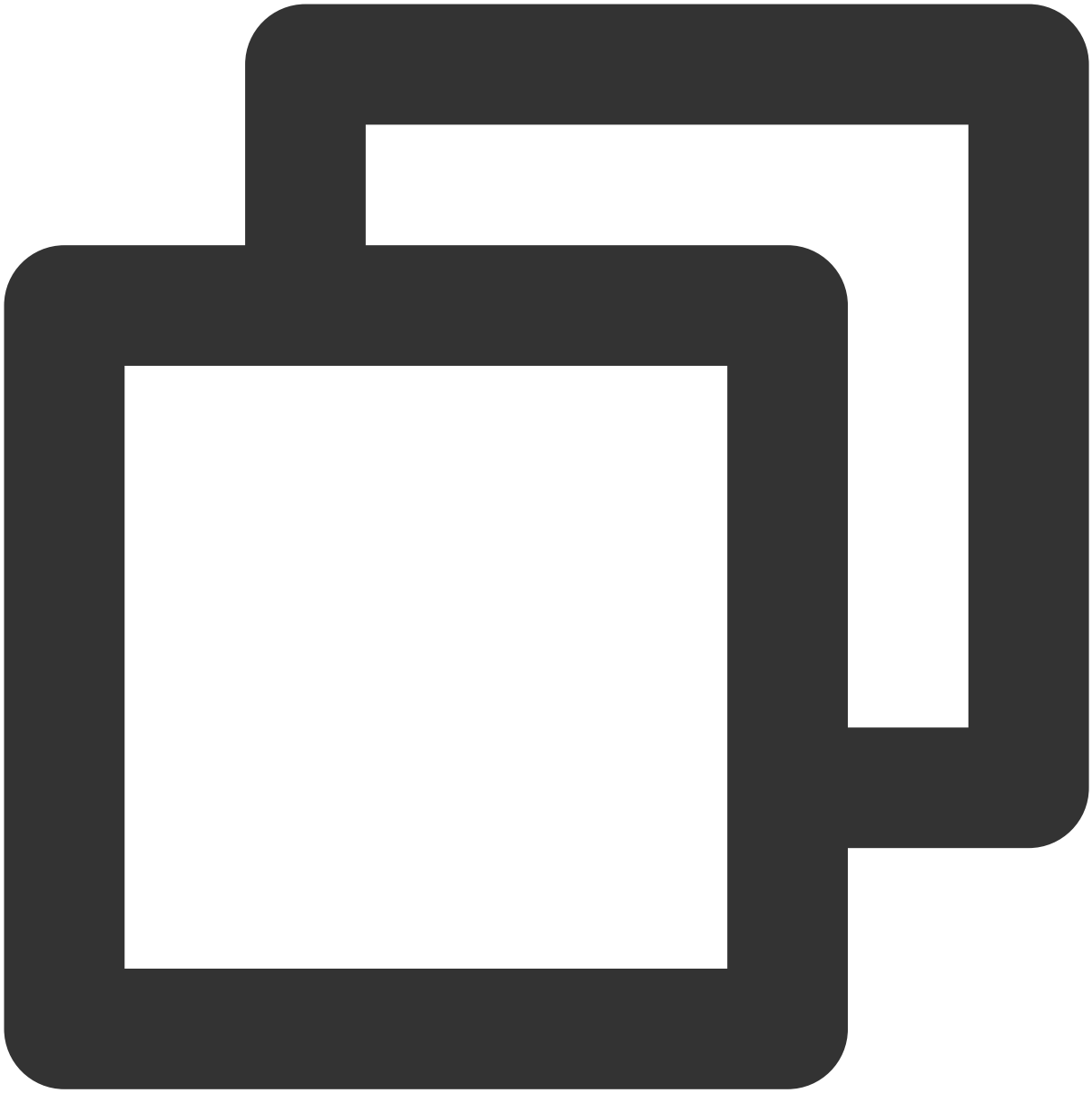
```
group-policy group_policy internal  # 为设备设置组策略。
group-policy group_policy attributes  # 设置组策略属性。
vpn-tunnel-protocol ikev2 # 配置 vpn-tunnel 使用协议为 ikev2。
```

5. 配置预共享密码。



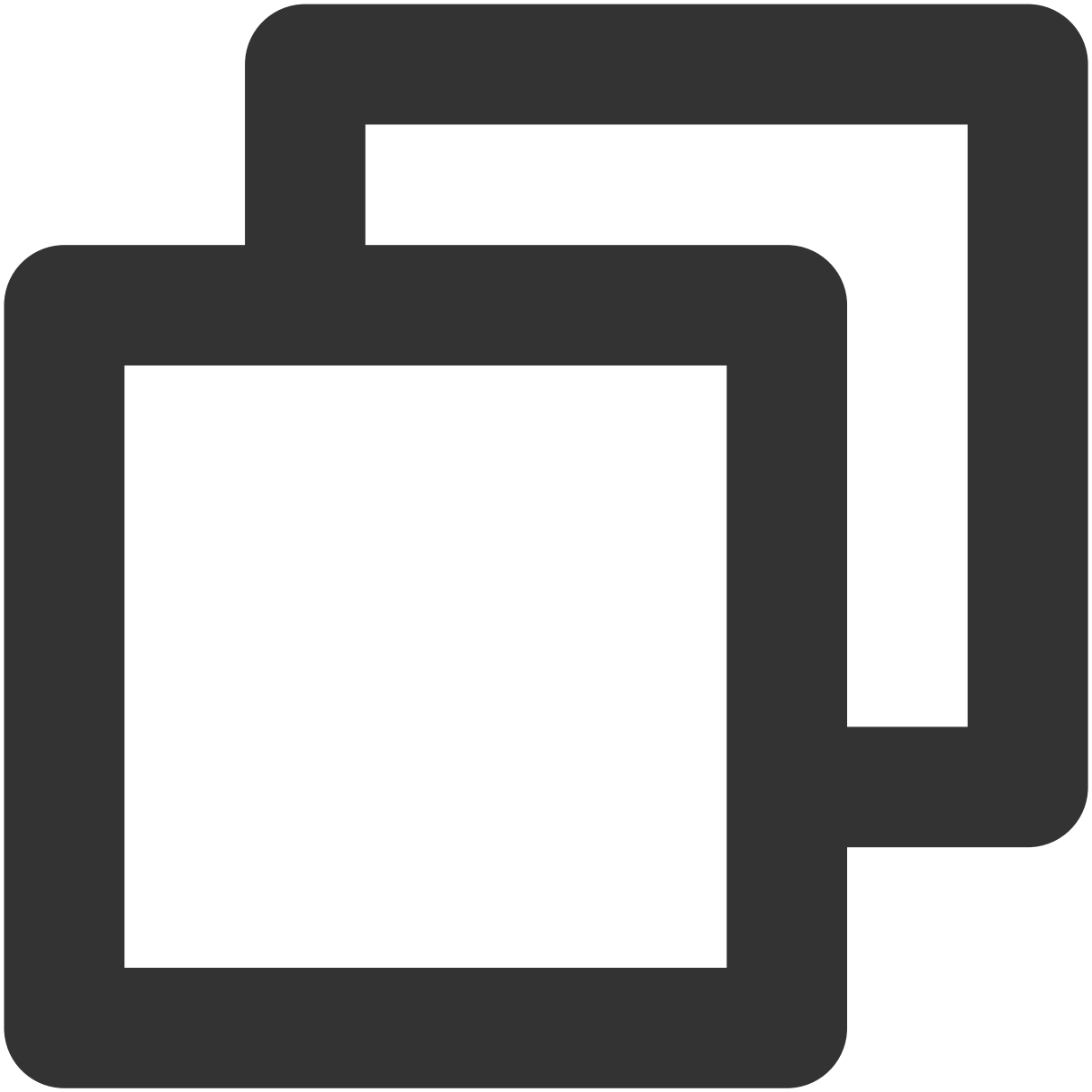
```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # 创建一个ipsec隧道组，type 为点到点。
tunnel-group 159.XX.XX.242 general-attributes default-group-policy group_policy
tunnel-group 159.XX.XX.242 ipsec-attributes  # 配置隧道组的属性，并指定预共享密钥。
ikev2 remote-authentication pre-shared-key tencent@123
ikev2 local-authentication pre-shared-key tencent@123  # 密钥可为1～128个字符的字母、
```

6. 配置 IPsec 安全协议。



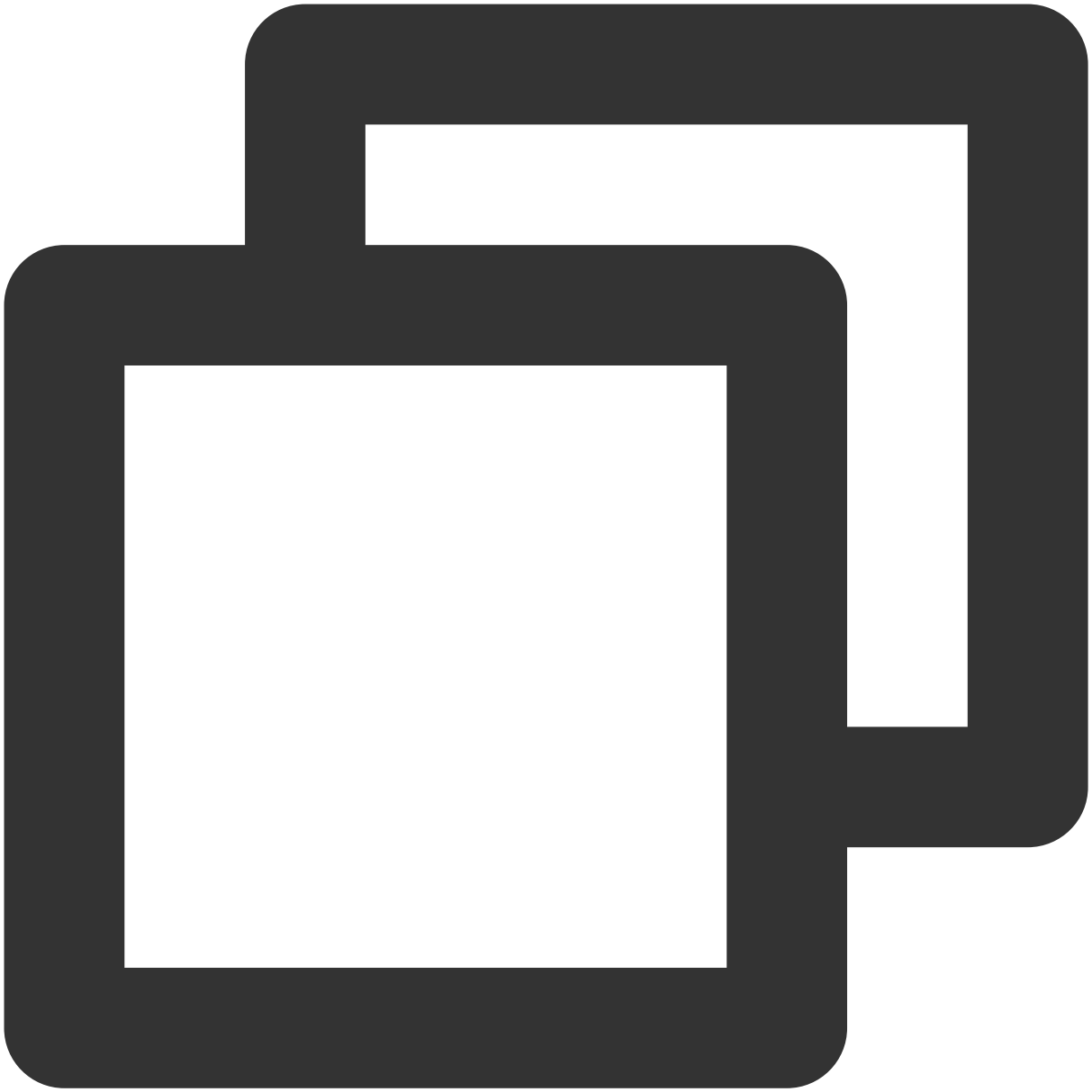
```
crypto ipsec ikev2 ipsec-proposal ikev2_proposal  # 配置 IPsec 第二阶段协商的加密算法
protocol esp encryption aes-128  # 配置加密算法。
protocol esp integrity sha-1 # 配置完整性检查算法。
```

7. 配置 ACL。



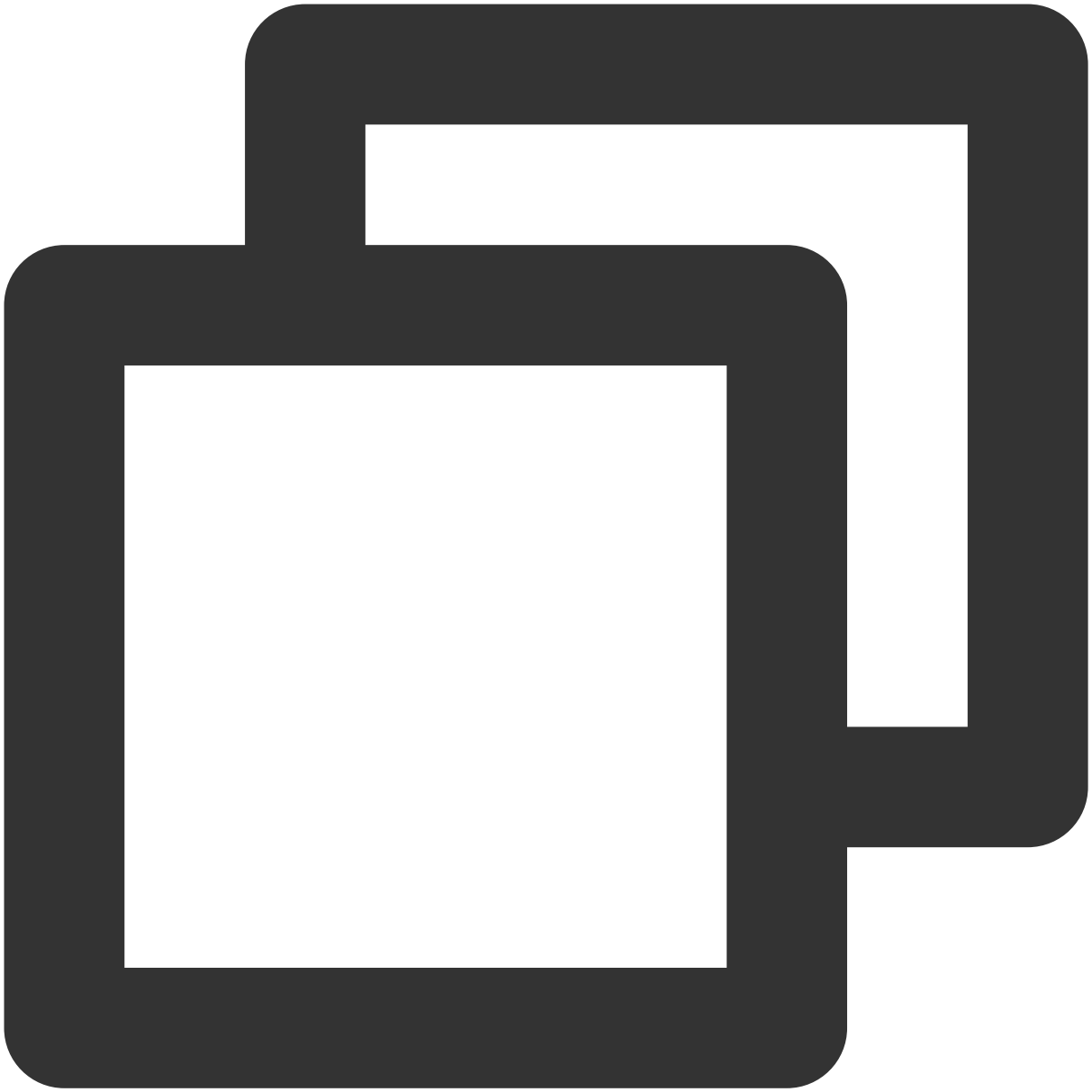
```
access-list INTERESTING extended permit ip 172.XX.XX.0 255.255.0.0 10.1.1.0 255.
```

8. 配置 IPsec 策略。



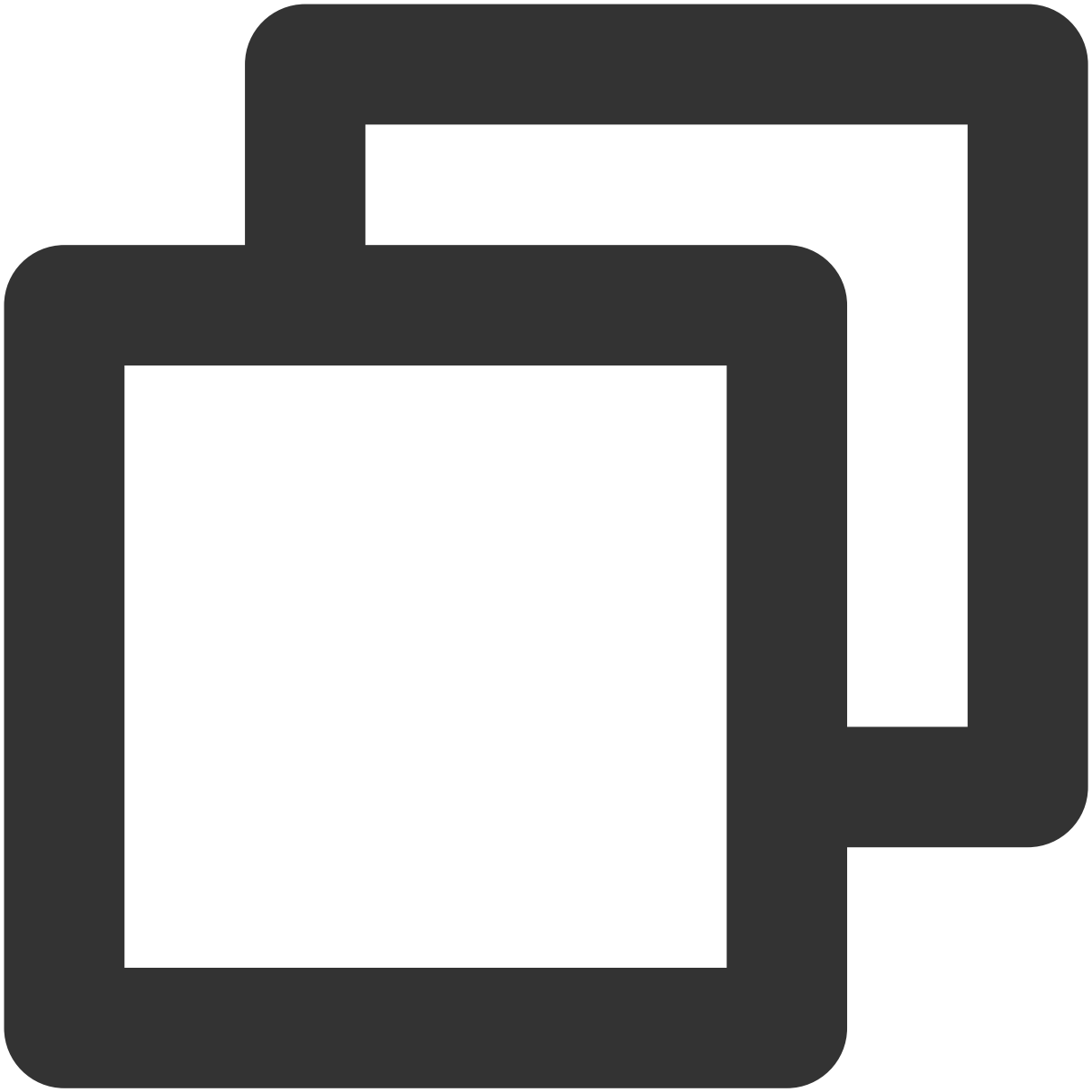
```
crypto map CMAP 1 match address INTERESTING  # 调用 ACL，使满足 ACL 的源网段或者目的网
crypto map CMAP 1 set peer 159.XX.XX.242  # 将被 IPsec 保护的流量转发到的对端 VPN 公网
crypto map CMAP 1 set ikev2 ipsec-proposal ikev2_proposal # 为加密映射条目配置 IKEv
crypto map CMAP 1 set security-association lifetime seconds 3600 # 配置加密密钥的生
crypto map CMAP 1 set security-association lifetime kilobytes 1843200  # 设置协商
```

9. 启用 IPsec 策略。



```
rypto map CMAP interface outside  # 将上一步配置的加密映射应用于外部接口。
```

10. 配置静态路由。

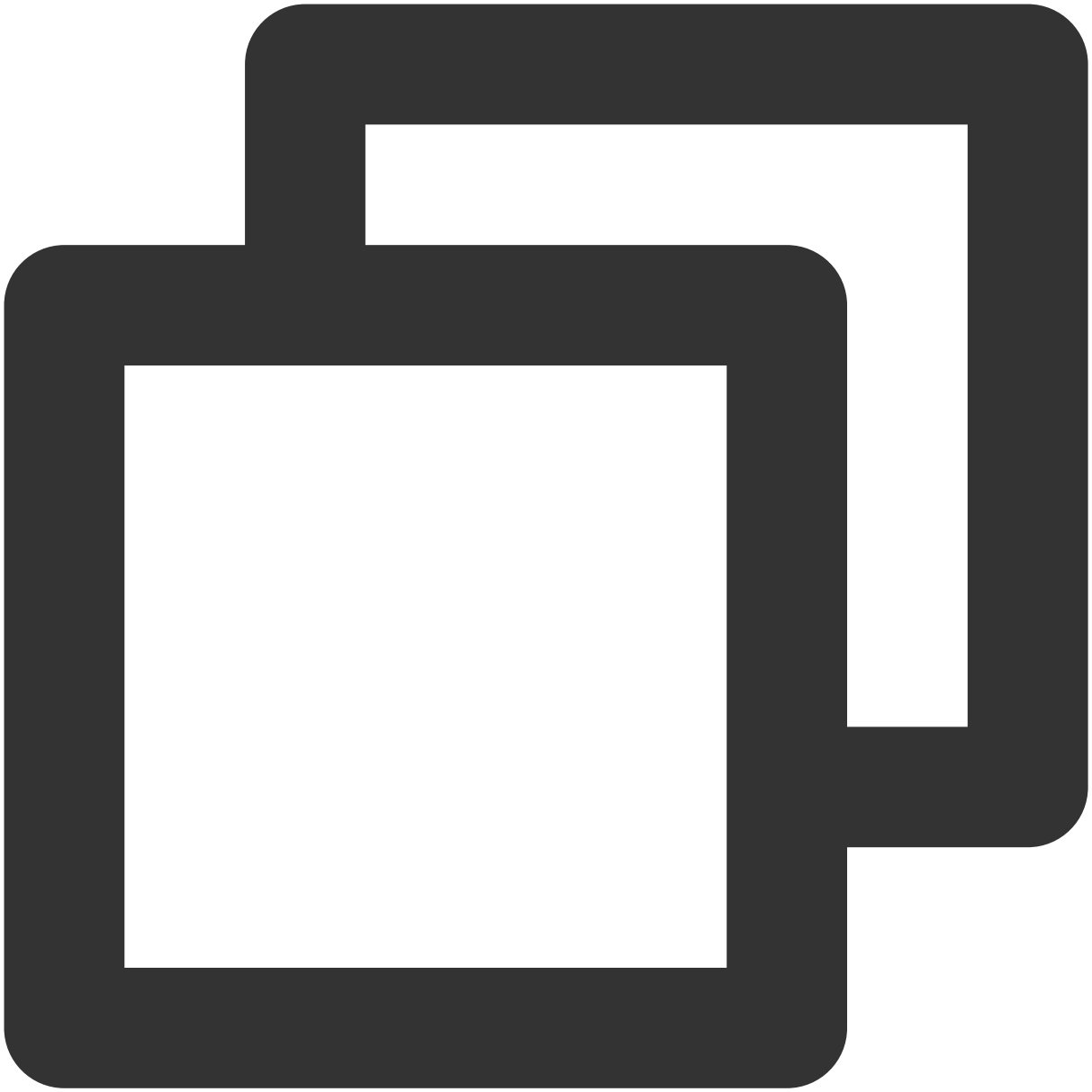


```
route outside 10.1.1.0 255.255.255.0 159.XX.XX.242 1   # 将待加密保护的数据网段引向
```

11. 测试 VPN 连通性。

执行 Ping 命令测试 VPN 的连通性。

1. 登录防火墙设备命令配置界面。

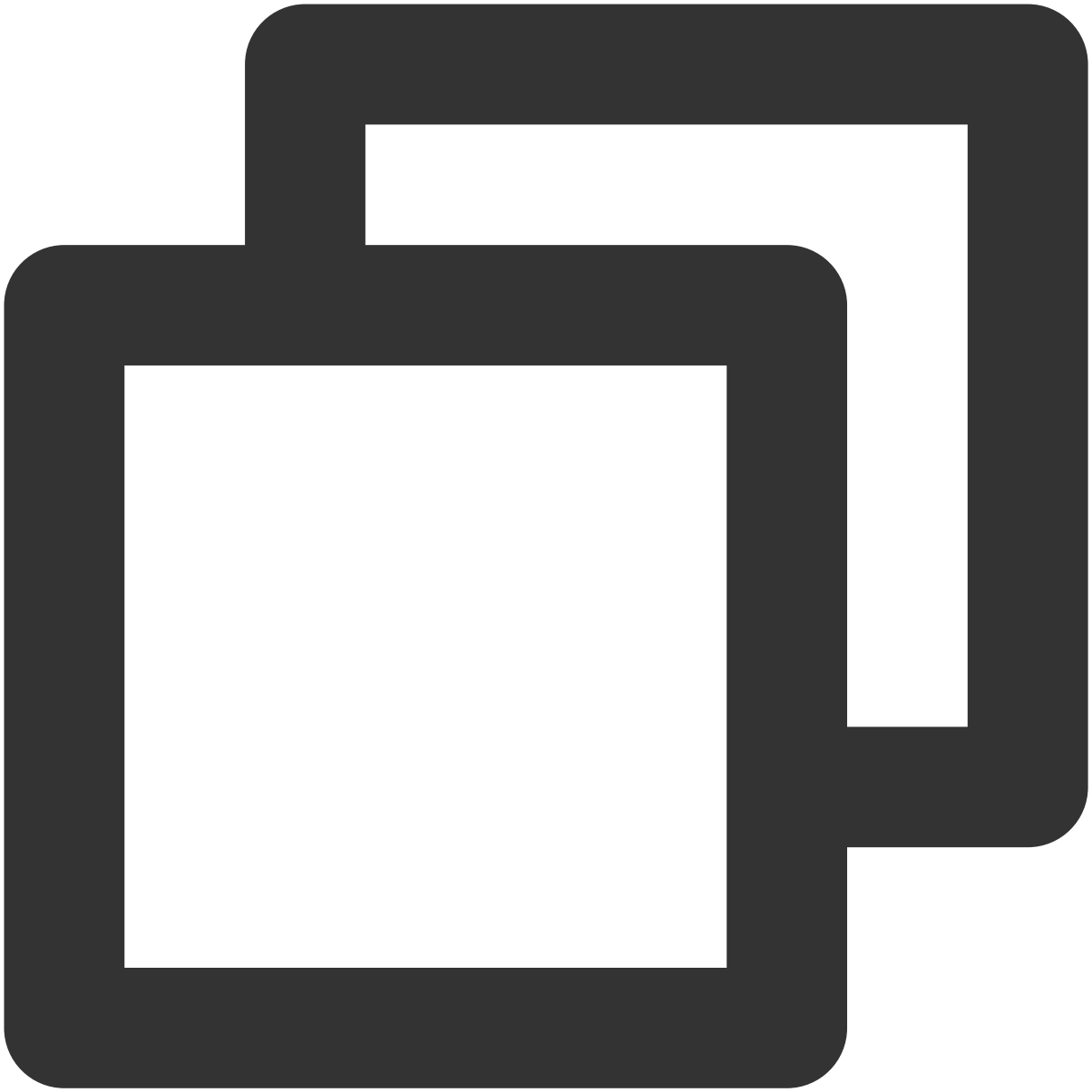


```
   ssh -p admin@10.XX.XX.56

# 通过 SSH 命令登录防火墙配置界面。

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# 输入账号密码，进入用户模式。
```

```
ASA>
ASA> en
Password:

# 输入enable和设置的enable密码进入特权模式，该模式下只支持查看。

ASA# conf t
ASA(config)#

# 键入“config ter”进入全局模式，在该模式下进行防火墙配置。
```

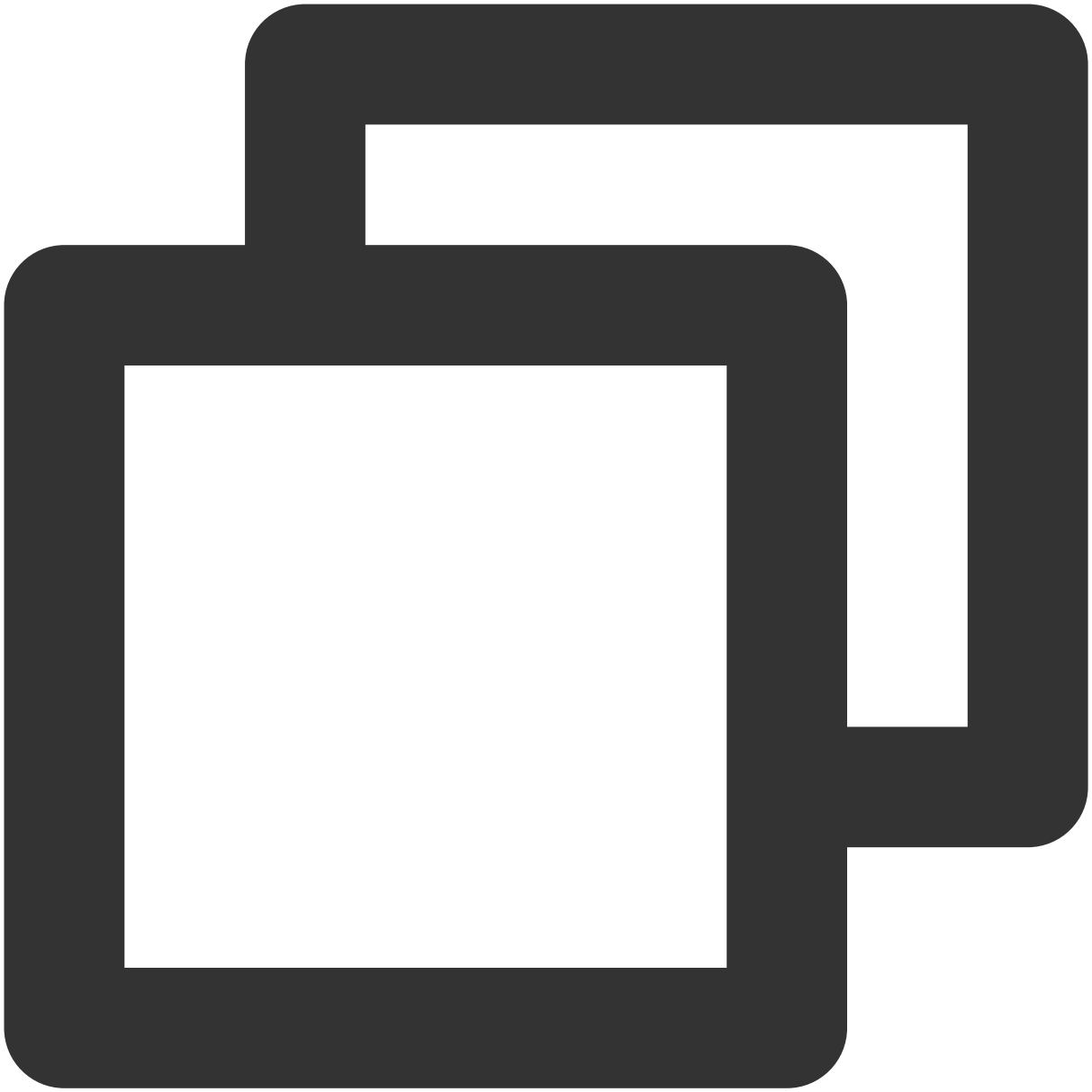
2. 配置防火墙接口。

在全局模式下配置对接腾讯云端的防火墙接口以及 Tunnel 口。



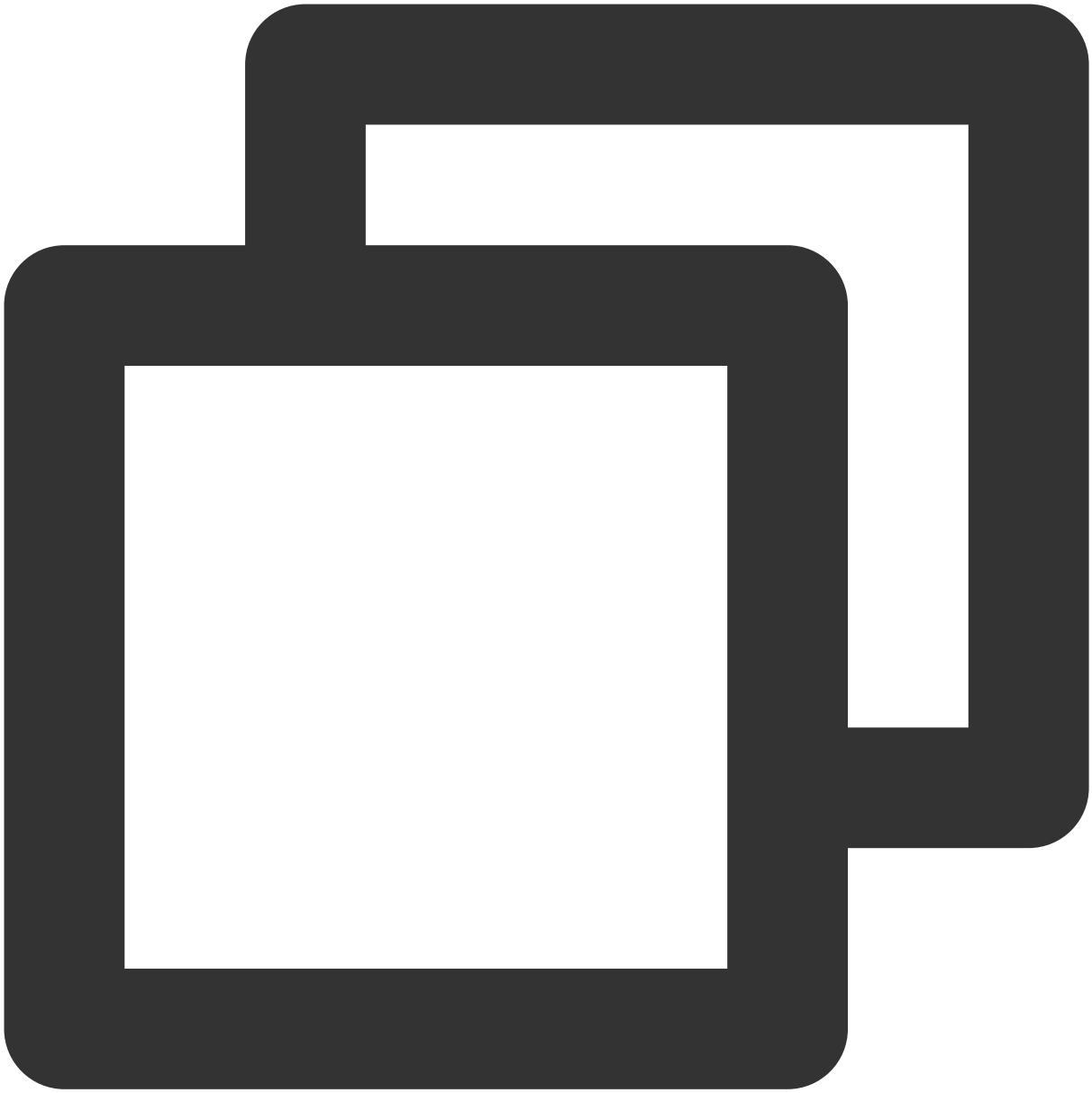
```
interface GigabitEthernet0/0
nameif outside   # 定义端口的安全域名。
security-level 0 # 定义端口的安全域等级。
ip address 120.XX.XX.76 255.255.255.252   # 配置对接腾讯云 VPN 公网 IP 地址。
interface Tunnel100
nameif vti
ip address 172.XX.XX.2 255.255.255.0 # 该 IP 地址用于激活 Tunnel 口。
```

3. 配置 isakmp 策略。



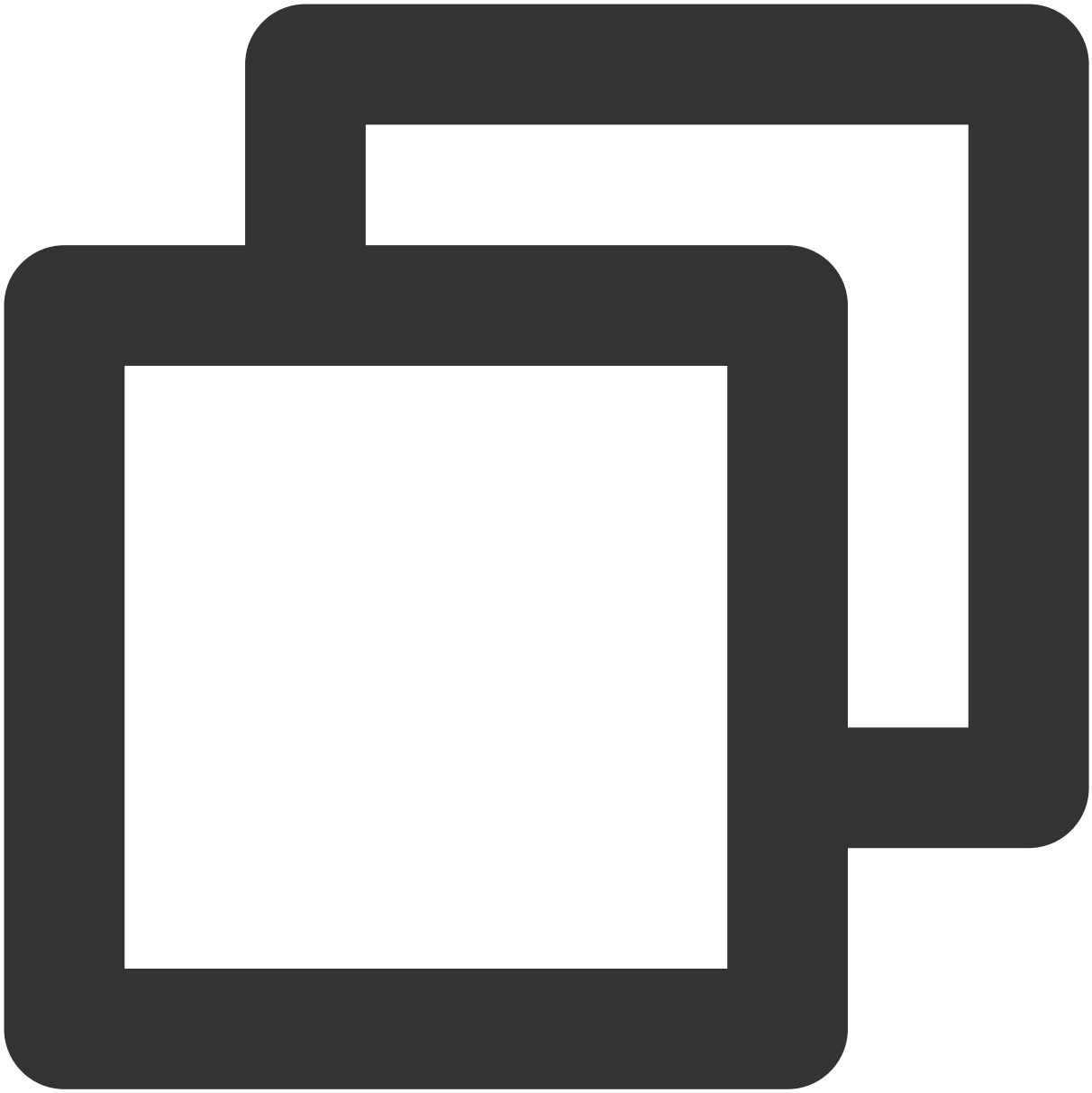
```
crypto ikev2 policy 1    # 定义 ikev2 第一阶段协商使用参数，序号为1，序号越小越优先，范围为
encryption AES-128     # 配置第一阶段协商数据包封装加密使用AES-128算法，默认为AES-128。
integrity MD5  /# 为IKE策略配置哈希算法为MD5，默认为sha。
group 2  # 为IKE策略配置 Diffie-Hellman 组为组2，默认为group 2。
prf sha # 配置加密算法。
lifetime seconds 86400  # 配置 SA 生存时间（即生命周期），默认为86400秒。
```

4. 配置组策略。



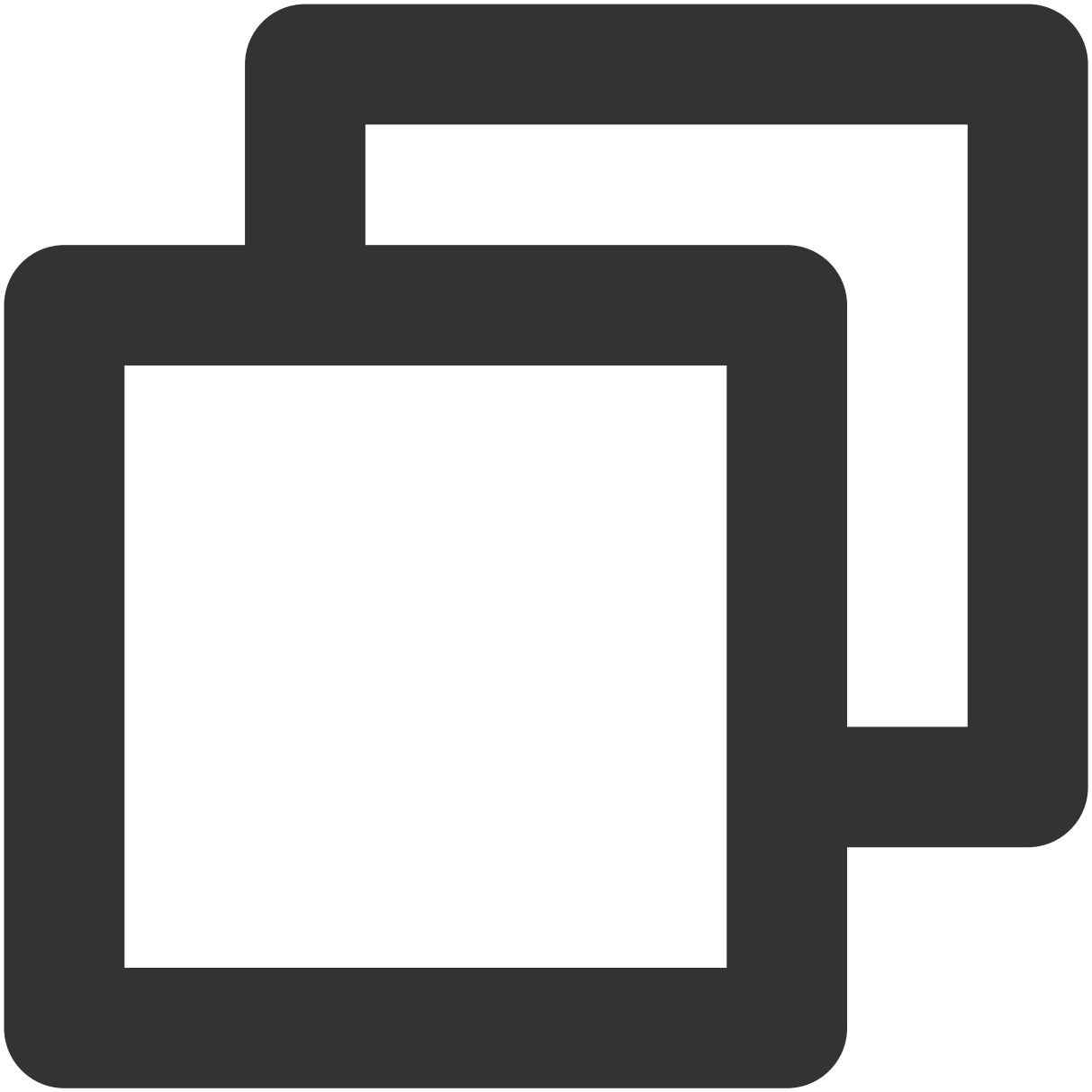
```
group-policy group_policy internal  # 为设备设置组策略。
group-policy group_policy attributes  # 设置组策略属性。
vpn-tunnel-protocol ikev2 # 配置 vpn-tunnel 使用协议为 ikev2。
```

5. 配置预共享密码。



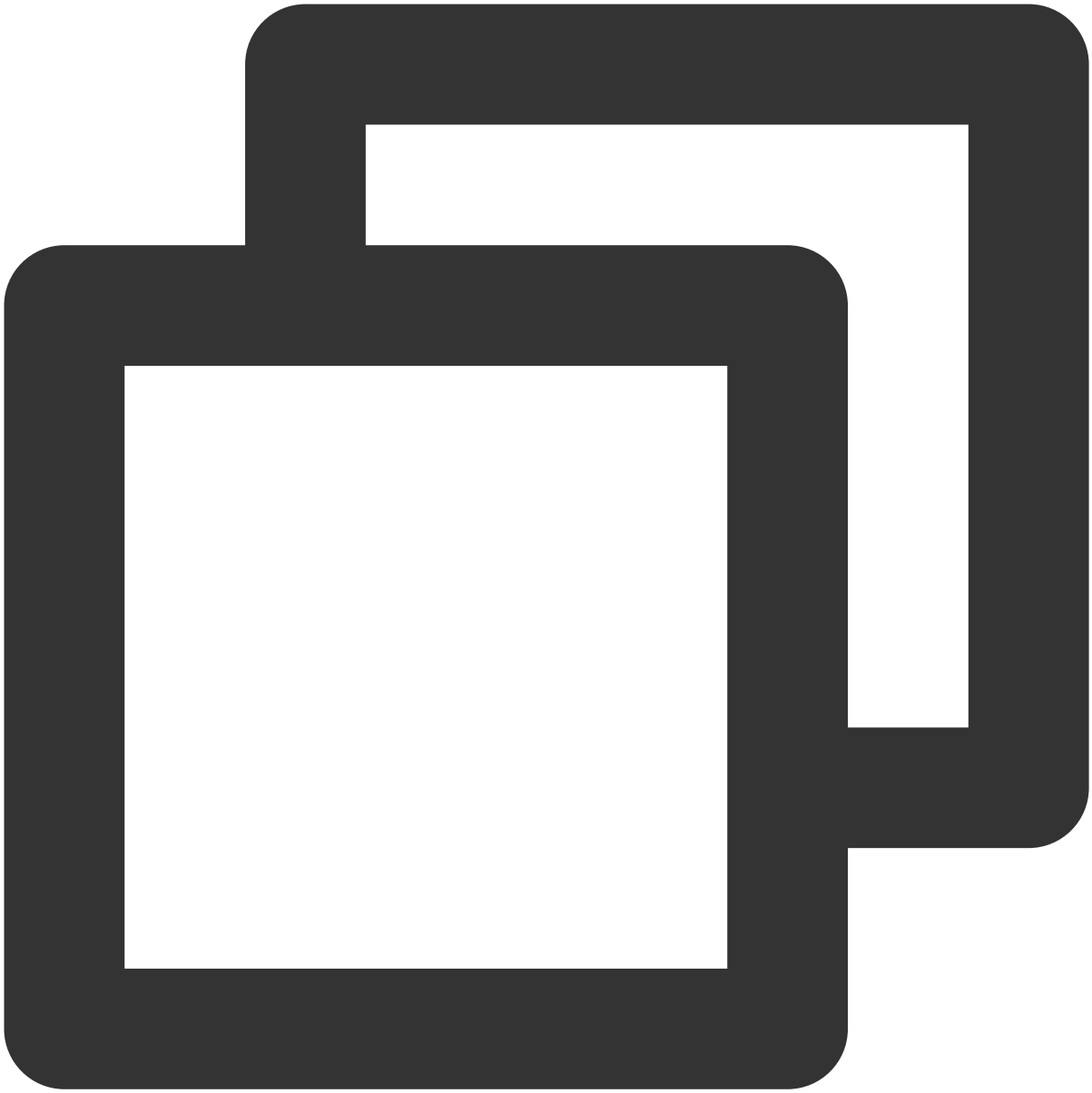
```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # 创建一个ipsec隧道组，type 为点到点。
tunnel-group 159.XX.XX.242 general-attributes default-group-policy group_policy
tunnel-group 159.XX.XX.242 ipsec-attributes  # 配置隧道组的属性，并指定预共享密钥。
ikev2 remote-authentication pre-shared-key tencent@123
ikev2 local-authentication pre-shared-key tencent@123  # 密钥可为1～128个字符的字母、
```

6. 配置 IPsec 安全协议。



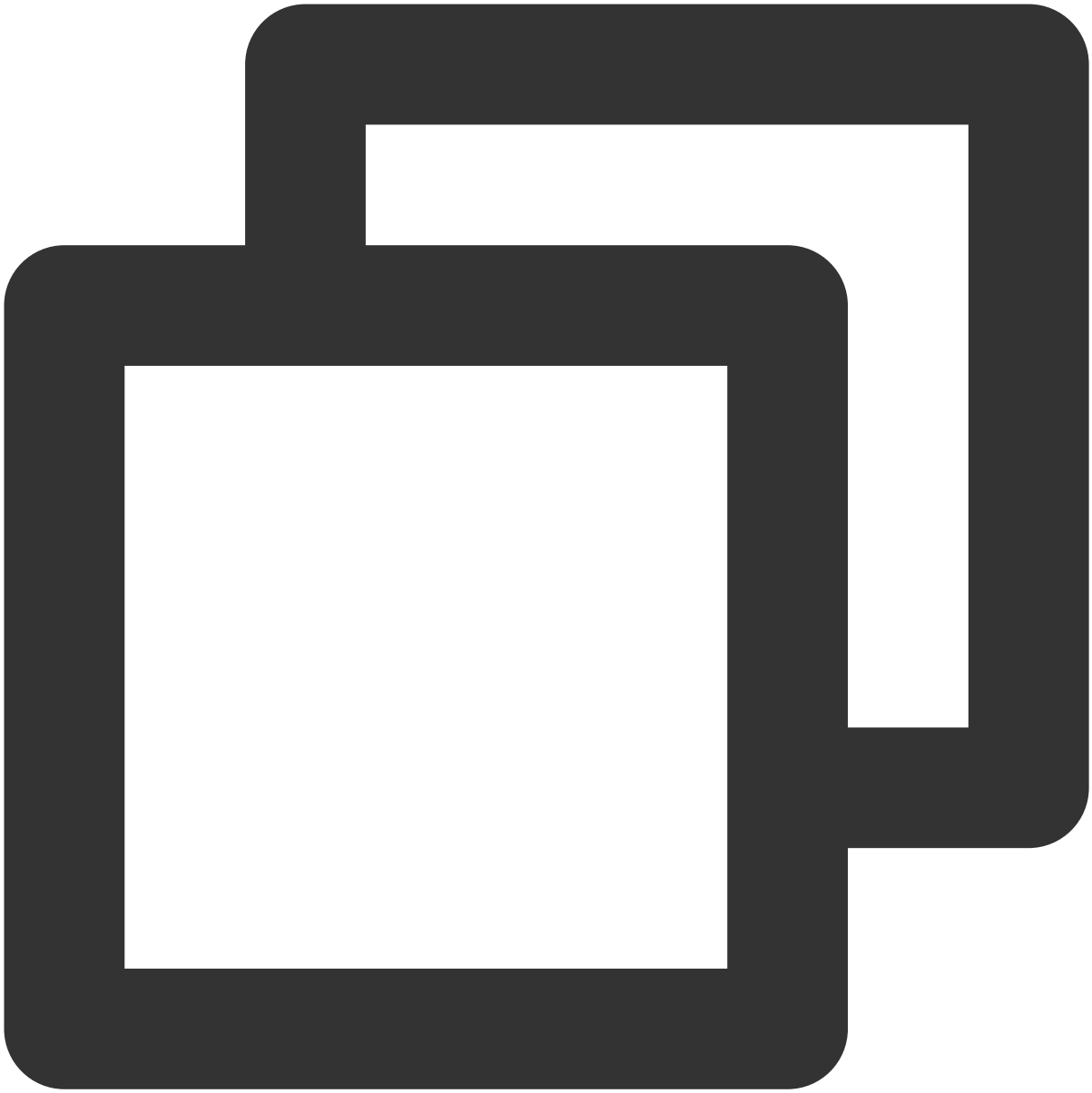
```
crypto ipsec ikev2 ipsec-proposal ikev2_proposal  # 设置 IPsec 第二阶段协商的加密算法
protocol esp encryption aes-128  # 设置加密算法。
protocol esp integrity sha-1 # 设置完整性检查算法。
```

7. 配置 IPsec 策略。



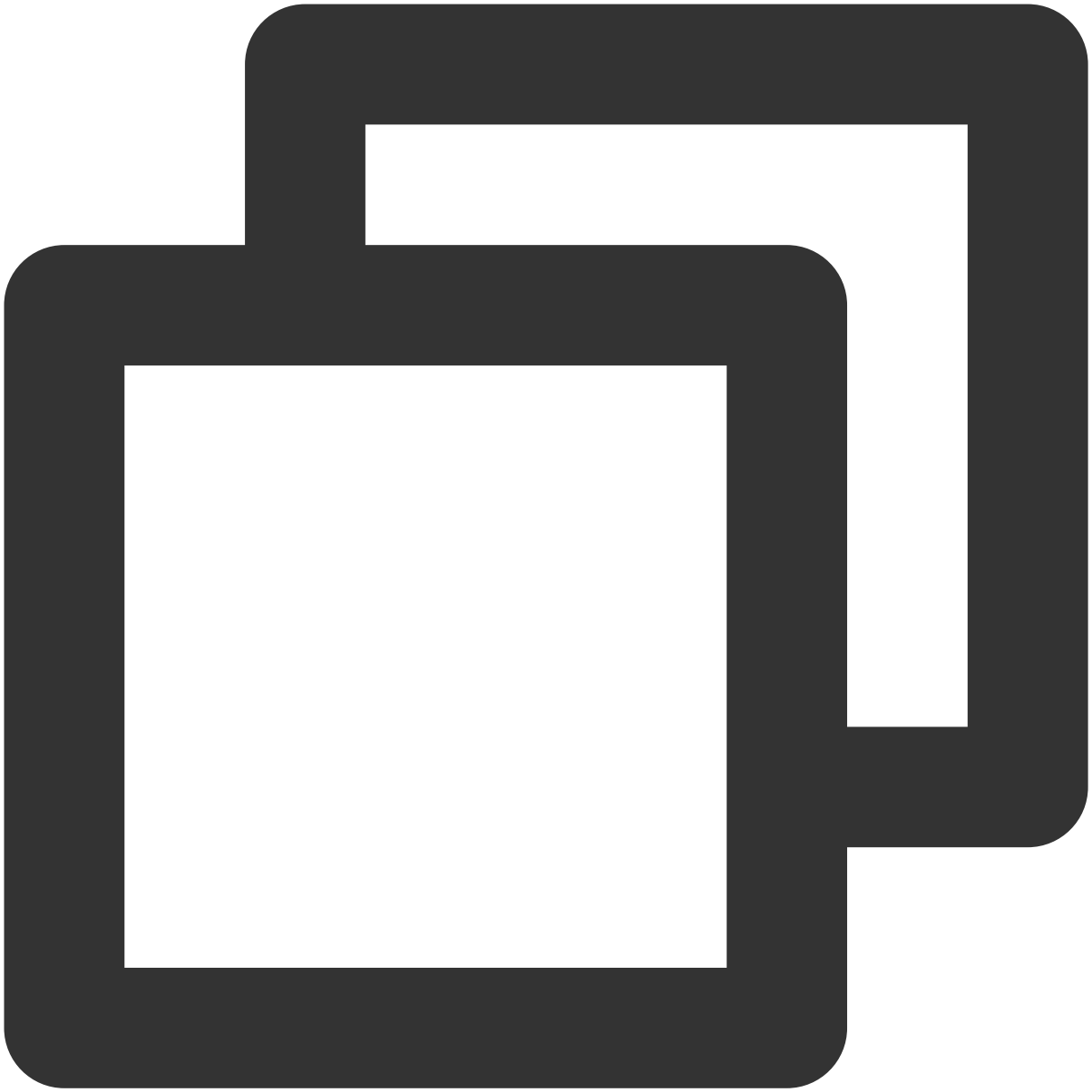
```
crypto ipsec profile PROFILE1
set ikev2 ipsec-proposal ikev2_proposal  /# 为加密映射条目设置 IKEv2 安全协议。
set security-association lifetime kilobytes 1843200  # 设置 SA 生命周期内，VPN之间可
set security-association lifetime seconds 3600   # 设置加密密钥的生命周期，默认千字节数
```

8. 启用 IPsec 策略。



```
interface Tunnel100
tunnel source interface outside  # 配置 VPN 的更新源为outside口。
tunnel destination 159.XX.XX.242  # 配置对端 VPN 的公网 IP 地址，本处为腾讯云 VPN 公网
tunnel mode ipsec ipv4  #  配置 tunnel口 使用的协议。
tunnel protection ipsec profile PROFILE1  # 调用 IPsec 策略对经过 tunnel 口的数据进行
```

9. 配置静态路由。



```
route vti 10.1.1.0 255.255.255.0 159.XX.XX.242    # 将待加密保护的数据包引到 tunnel 口
```

10. 测试 VPN 连通性。

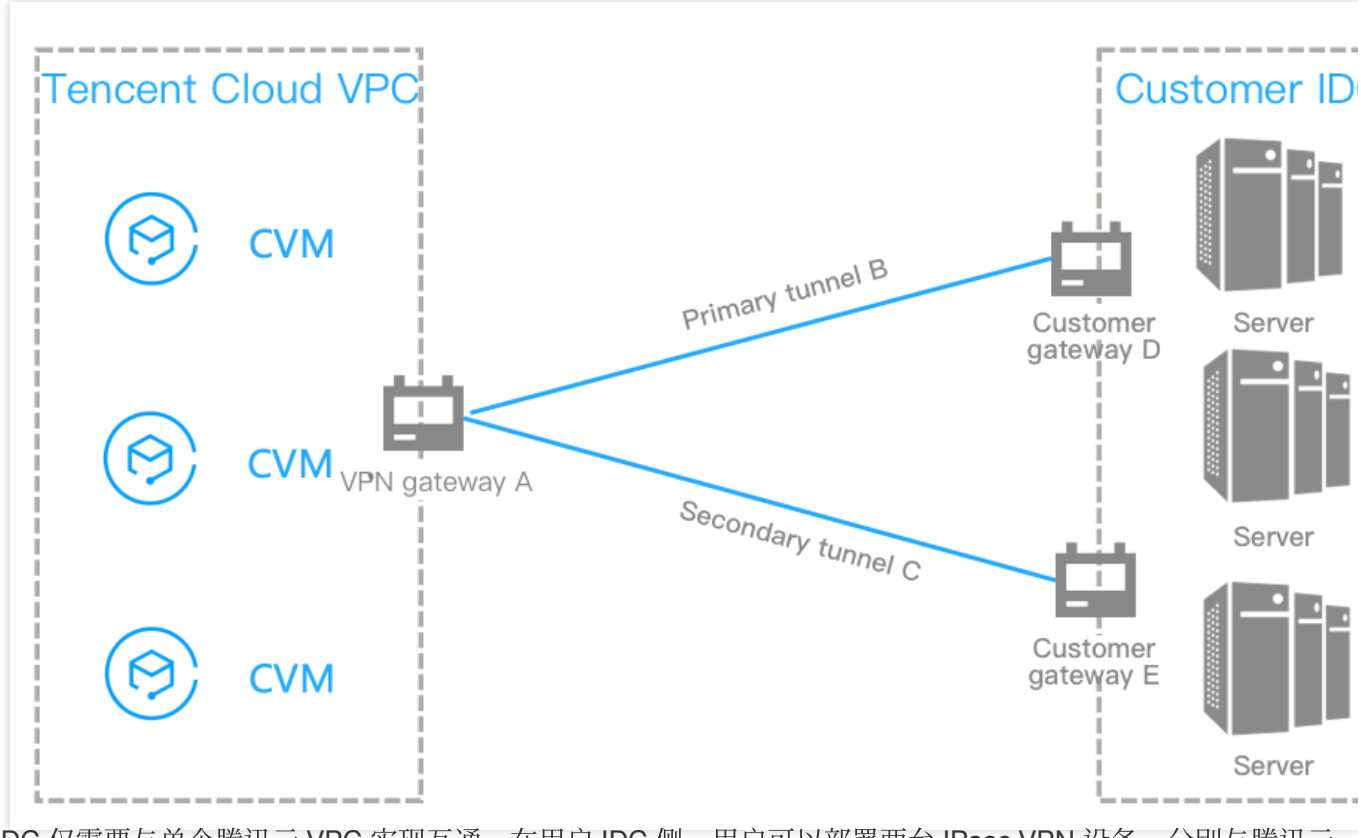
执行 Ping 命令测试 VPN 的连通性。

IDC 与单个腾讯云 VPC 实现主备容灾

最近更新时间：2024-01-09 14:41:10

腾讯云 VPN 连接具备高可用性，当用户 IDC 通过主备 VPN 通道上云，且主通道发生故障时，业务将自动切换到备用通道上，保证了业务的持续性、从而提高业务可靠性。本文以 IDC 与单个腾讯云 VPC 实现主备容灾为例。

容灾方案



用户 IDC 仅需要与单个腾讯云 VPC 实现互通，在用户 IDC 侧，用户可以部署两台 IPsec VPN 设备，分别与腾讯云私有网络型 VPN 建立 IPSec VPN 通道。VPN 网关路由表配置两条目的端一致的路由，通过优先级控制，实现主备通道效果，在发生故障时，可以实现路由自动切换。

前提条件

已在腾讯云侧 创建 VPC 网络。

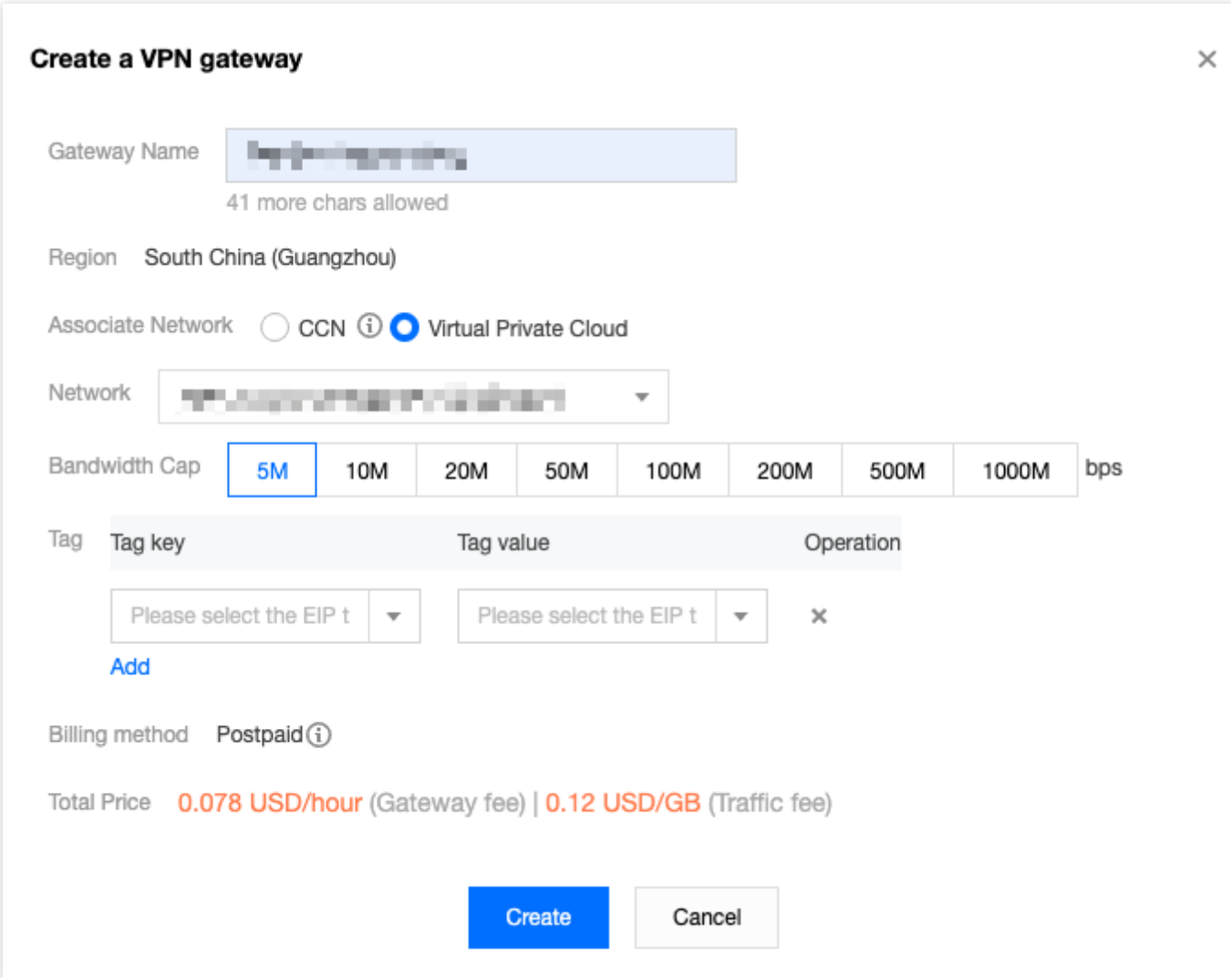
操作步骤

步骤一：创建 VPN 网关

说明：

本文以3.0版本的 VPN 网关为例。

1. 登录 私有网络控制台。
2. 在左侧目录中选择 **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。



网关名称：填写自定义网关名称。

关联网络：选择创建好的 VPC 网络。

带宽上限：依据实际需求选择带宽。

计费方式：按需选择计费方式，本示例中以按量计费为例。

其他可选不配置或者保持默认即可。

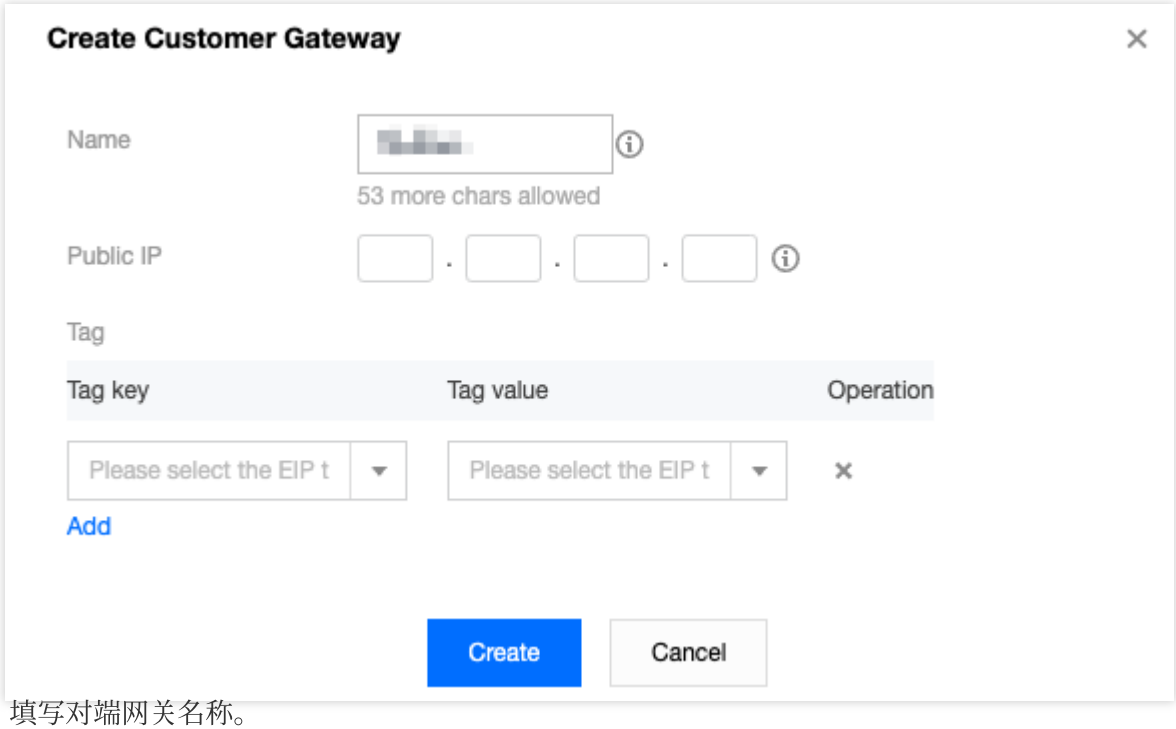
5. 完成网关参数设置后，单击**创建**启动 VPN 网关的创建。

此时**状态**为**创建中**，等待约1～2分钟，创建成功的 VPN 网关状态为**运行中**，系统为 VPN 网关分配一个公网 IP。

步骤二：创建对端网关

在腾讯云侧创建对端网关 D。

1. 在左侧导航栏选择 **VPN 连接** > **对端网关**。
2. 在“对端网关”管理页面，选择地域，单击**+新建**。
3. 填写对端网关名称，公网 IP 填写对端 IDC 侧的 VPN 网关设备的静态公网 IP ，根据需要设置标签。



名称：填写对端网关名称。
公网IP：填写 IDC 侧 VPN 网关所在的 公网 IP 地址。
4. 单击**创建**。

在腾讯云侧创建对端网关 E。

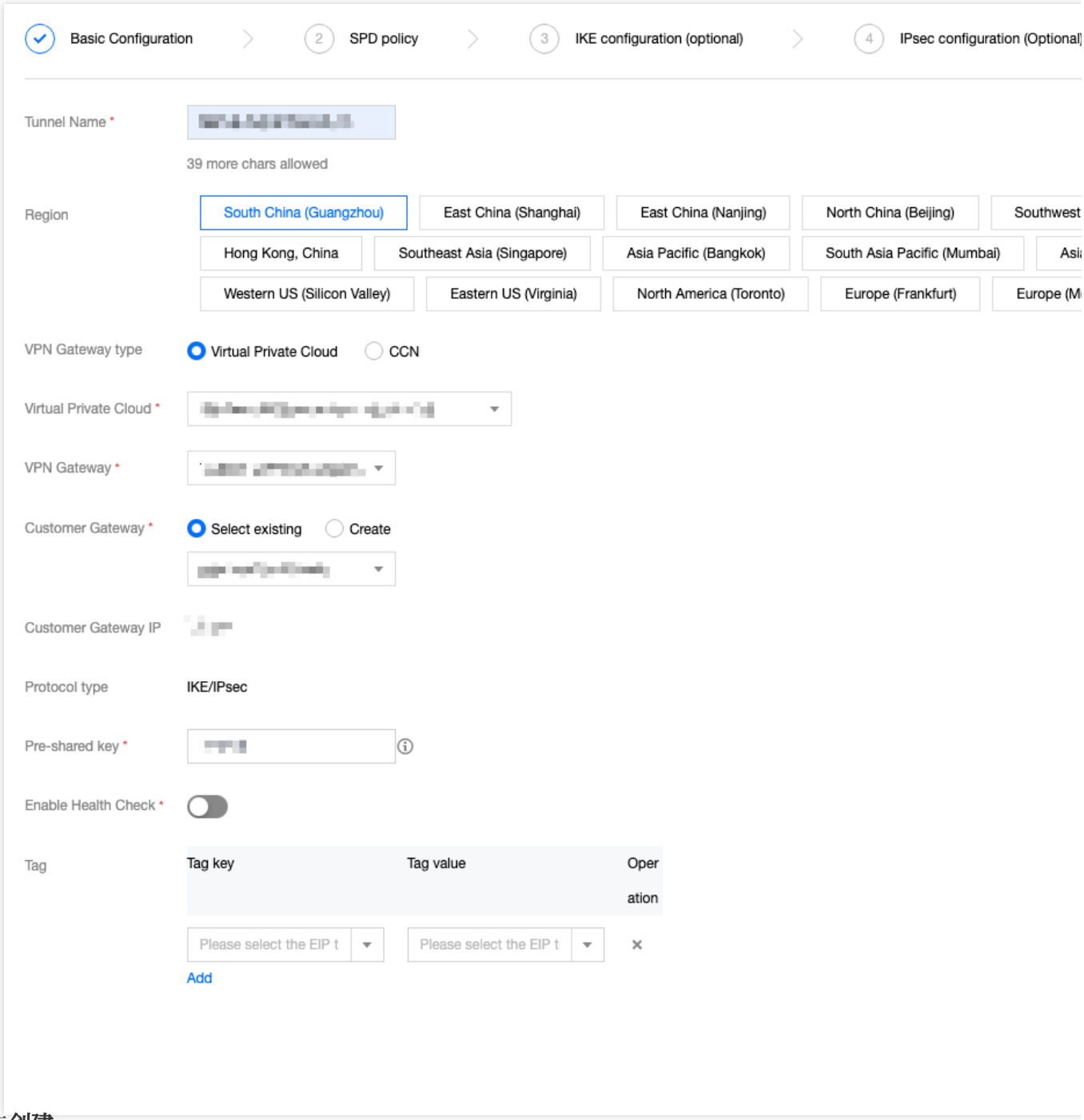
重复对端网关 D 的创建步骤1 ～ 步骤4。

步骤三：创建 VPN 通道（主备）

VPN 网关和对端网关创建完成后，需要创建两条 VPN 网关与 IDC 侧相连的 VPN 通道，一条作为主通道，一条作为备用通道。

创建主用通道 B

1. 在左侧导航栏选择 **VPN 连接** > **VPN 通道**。
2. 在“VPN 通道”管理页面，选择地域，单击**+新建**。
3. 在弹出的页面中填写 VPN 通道信息，具体参数配置请参考 新建 VPN 通道。SPD 策略配置时，“对端网段”配置为 `0.0.0.0/0` 。



4. 单击**创建**。

创建备用通道 C

重复主用通道 B 的创建步骤1 ～ 步骤4，其中 SPD 策略配置时，“对端网段”配置为 `0.0.0.0/0` 。

步骤四：IDC 侧配置

完成前3步骤后，腾讯云上 VPN 网关和 VPN 通道的配置已经完成，需要继续在 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 步骤二 的“对端网关”中。

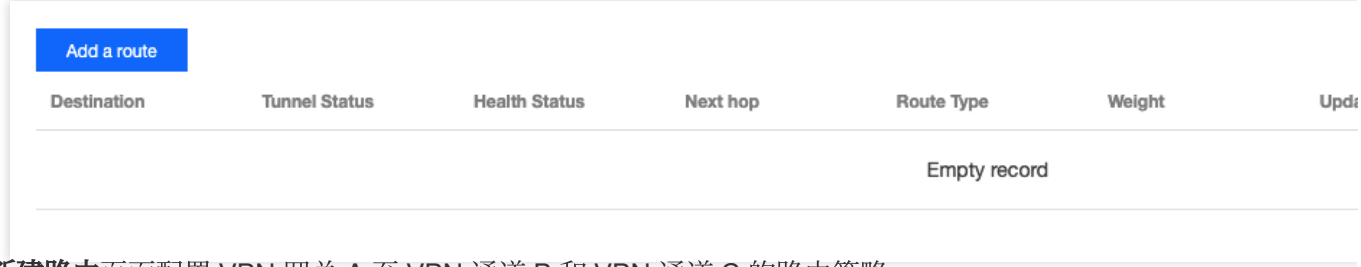
注意：

配置时，主备 VPN 通道对应的 IDC 侧 VPN 网关均需配置。

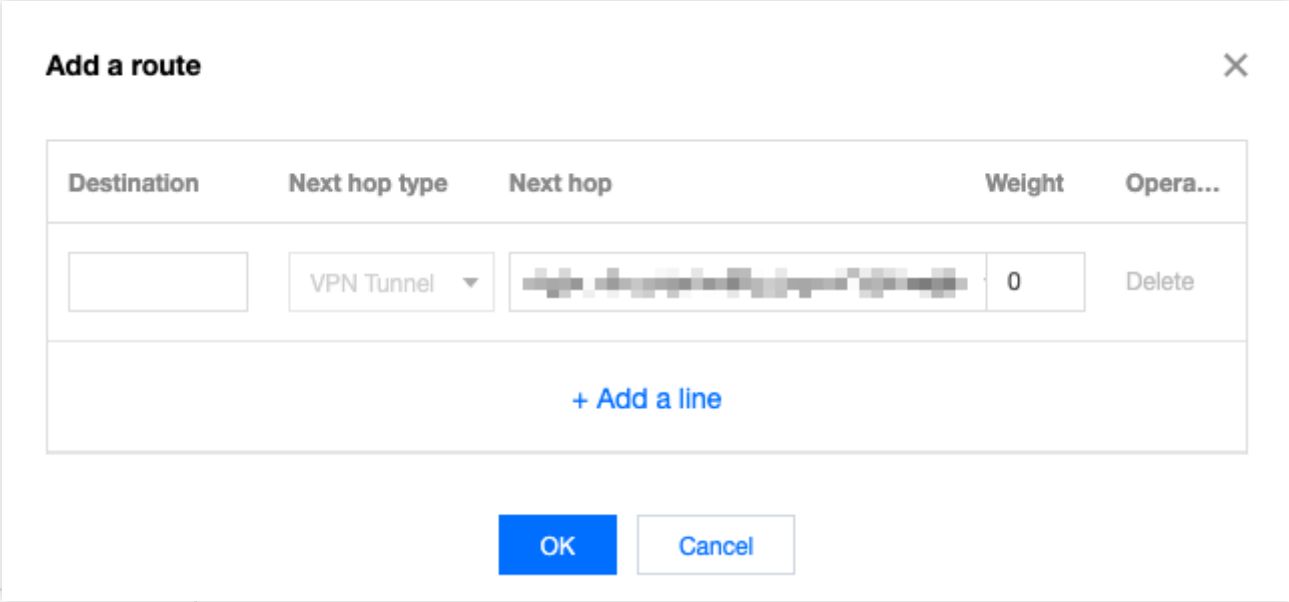
步骤五：配置 VPN 网关路由

截止至步骤四，已经将主备 VPN 通道配置成功，需要在 VPN 控制台配置 VPN 网关至 VPN 通道的路由。

1. 在左侧导航栏选择 **VPN 连接** > **VPN 网关**，并在右侧 VPN 网关列表中找到步骤一创建的 VPN 网关 A，并单击其名称。
2. 在 VPN 网关 A 详情页签，单击**路由表**页签，并单击**新增路由**。



3. 在**新建路由**页面配置 VPN 网关 A 至 VPN 通道 B 和 VPN 通道 C 的路由策略。



配置项	说明
目的端	填写待访问的对端网络的网段，即 IDC 侧提供对外访问的网段。
下一跳类型	系统自动填充**VPN 通道**。
下一跳	选择创建好的 VPN 通道。
权重	VPN 通道 B 填写 0。 VPN 通道 C 填写100。 0 表示优先级高，100表示优先级低。

4. 单击**确定**。

步骤六：配置通道健康检查

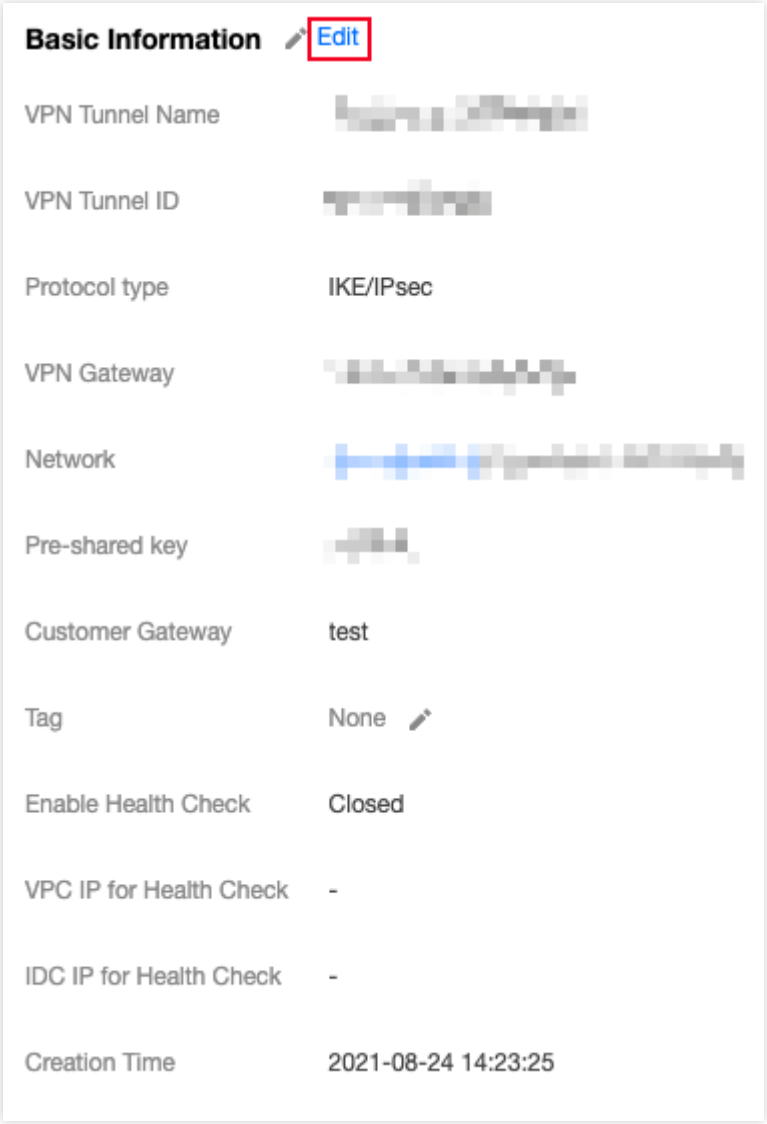
VPN 网关路由配置完成后，为 VPN 通道健康检查（主备通道均需配置）。

说明：

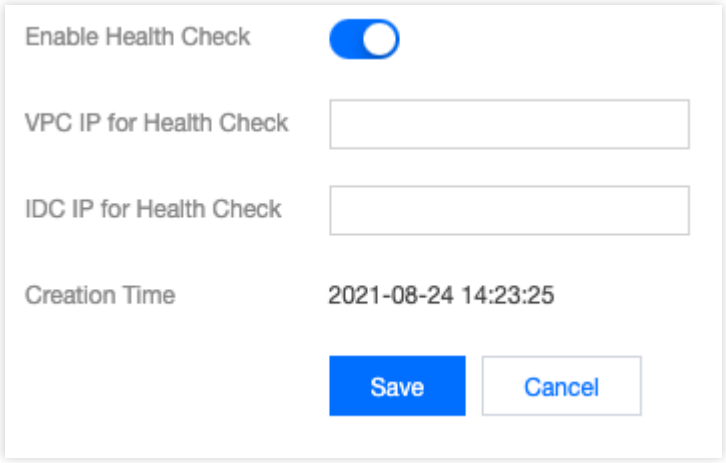
当健康检查触发主备通道切换，可能会出现短暂的业务中断，请勿担心，1～2秒后主备通道切换成功后业务恢复正常。

主用通道 B 健康检查配置

1. 在左侧导航栏选择 **VPN 连接** > **VPN 通道**，并在右侧 VPN 通道列表中找到创建好的 VPN 通道，然后单击 VPN 通道名称。
2. 在通道**基本信息**页签单击**编辑**。



3. 打开健康检查开关，输入**健康检查本端地址**和健康检查对端地址，并单击**保存**。



说明：

本端地址：填写腾讯云侧向 IDC 发起健康检查的访问请求 IP 地址。该 IP 地址不能为 VPC 内 IP 地址。

对端地址：填写 IDC 侧用于响应腾讯云健康检查请求的 IP 地址。该 IP 地址请勿与腾讯云侧地址相同，以防 IP 冲突。

当腾讯云侧发起健康检查请求，访问请求通过通道到达 IDC 后，发现有健康检查响应 IP 地址，表示通道健康正常，如果没有表示异常。

备用通道 C 健康检查配置

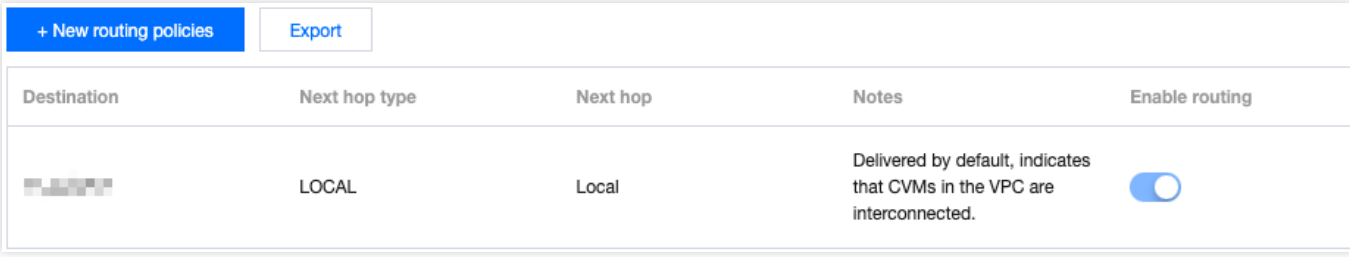
重复主用通道健康检查配置步骤1 ～ 步骤3，其中健康检查连接不能与主用通道的健康检查连接相同。

步骤七：配置 VPC 路由策略

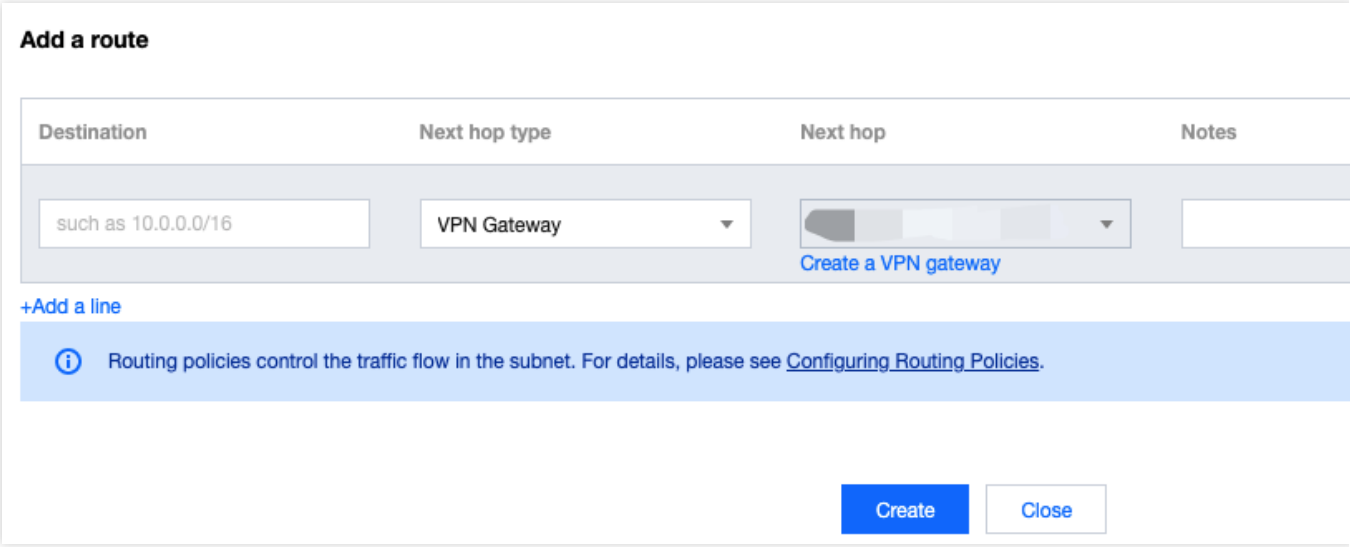
截止至步骤五，已经将主备 VPN 通道配置成功，需要配置 VPC 路由策略，将子网中的流量路由至 VPN 网关上，子网中的网段才能与 IDC 中的网段通信。

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，单击子网所关联的路由表 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，下一跳类型选择 **VPN 网关**，下一跳选择刚创建的 VPN 网关，单击**创建**即可。



步骤八：激活 VPN 通道

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。
当 VPN 路由表中探测VPN 主用通道 B 路由不可达时，系统自动将流量切换至 VPN 通道 C，确保业务的高可用性。

Dedicated Private Network Traffic Encrypted Via a Private Network VPN Gateway 方案概述

最近更新时间：2024-08-15 16:11:56

说明：

私网 VPN 网关 IP 地址归属租户 VPC。

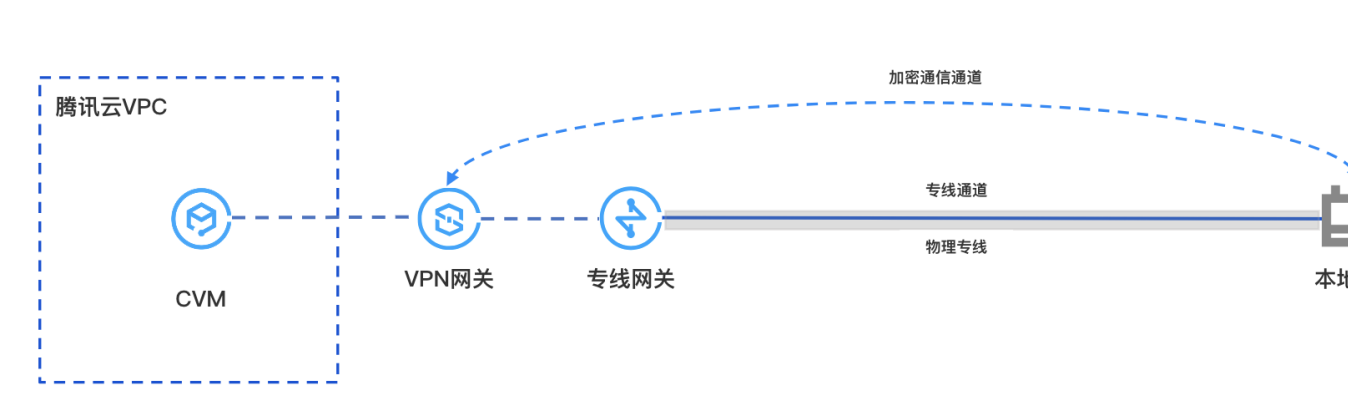
私网 VPN 目前仅支持 VPC 型VPN，CCN型 VPN 网关暂不支持。

私网 VPN 暂不支持动态 BGP。

如需使用私网类型的 VPN，请 提交工单 进行咨询。

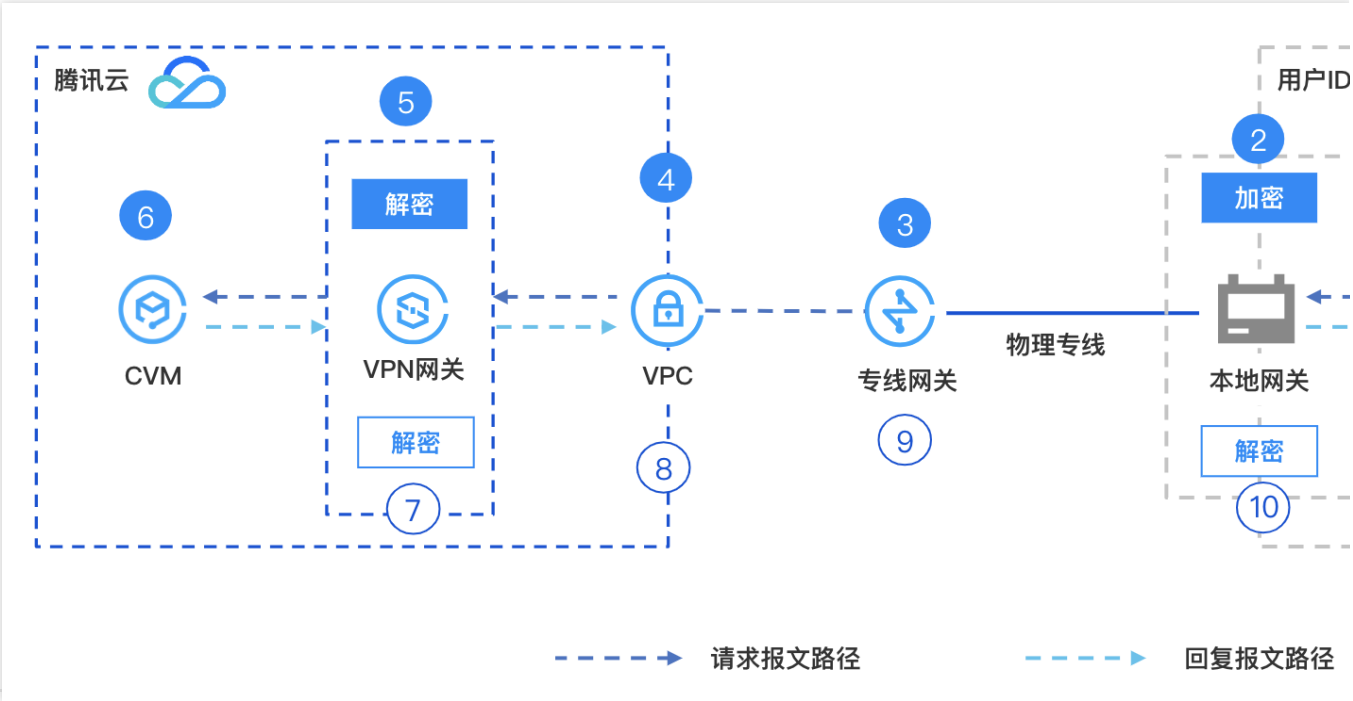
场景说明

在本地数据中心 IDC 通过物理专线和云上 VPC 实现私网通信后，私网 VPN 网关可通过已建立的私网连接与本地网关设备建立加密通信通道。您可以通过相关路由配置引导本地 IDC 和 VPC 要互通的流量进入加密通信通道，实现私网流量加密通信。



私网流量加密通信原理

为了方便您理解，以下具体实例为您介绍私网 VPN 流量加密通行过程。



序号	转发对象	说明
①	用户 IDC 服务器	客户发起访问请求，请求报文路由至 IDC 本地网关。
②	IDC 本地网关	本地网关对请求报文进行加密封装，封装后依据配置的路由将请求报文转发至云上专线网关。
③	专线网关	专线网关接收封装的请求报文后转发至私有网络 VPC。
④	私有网络 VPC	私有网络 VPC 接收封装的请求报文后，将请求报文转发至私网 VPN 网关。
⑤	VPN 网关	1. 私网 VPN 网关接收到封装的请求报文并对其进行解密。 2. 私网 VPN 网关依据解密后报文中的目的地址遍历路由表，然后将请求报文转发至云服务器 CVM。
⑥	云服务器 CVM	1. 云服务器 CVM 接收到解密后的请求报文后进行响应，向客户端发送回复报文。 2. 云服务器 CVM 依据回复报文的目的地址查询路由表，将回复报文转发至 VPN 网关。
⑦	VPN 网关	1. 私网 VPN 网关接收到回复报文后，对回复报文进行加密。 2. VPN 网关依据回复报文被加密的目的 IP 地址查询路由表，将回复报文转发至 VPC。
⑧	私有网络 VPC	私有网络 VPC 接收到加密后的回复报文后，查询路由表将加密后的回复报文转发至专线网关。
⑨	专线网关	专线网关接收到加密后的回复报文后，查询路由表将加密后的回复报文转发至

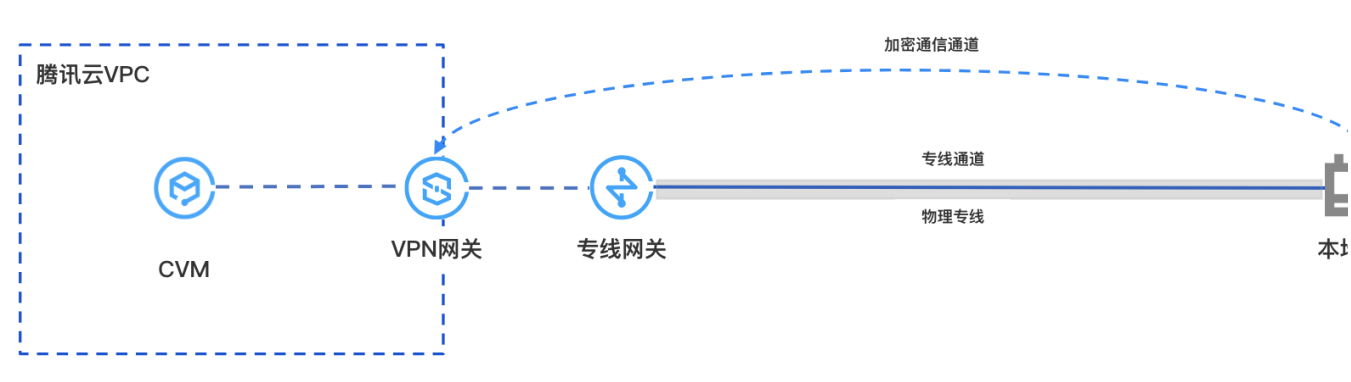
		IDC 本地网关。
⑩	IDC 本地网关	1. IDC 本地网关接收到回复报文后，对回复报文进行解密。 2. 本地网关设备依据回复报文被解密后的目的 IP 地址查询路由表，将回复报文转发至服务器。

专线私网流量通过私网 VPN 网关实现加密通信

最近更新时间：2024-08-15 16:12:06

在本地数据中心 IDC 通过物理专线和云上 VPC 实现私网通信后，私网 VPN 网关可通过已建立的私网连接与本地网关设备建立加密通信通道。您可以通过相关路由配置引导本地 IDC 和 VPC 要互通的流量进入加密通信通道，实现私网流量加密通信。

业务场景



使用限制

私网 VPN 目前仅支持 VPC 型 VPN，CCN 型 VPN 暂不支持。
私网 VPN 暂不支持动态 BGP 路由。
仅 VPN4.0版本支持。

网络规划

配置对象	网段规划	IP地址和说明
VPC	10.7.0.0/16	CVM：10.7.6.10 私网 VPN 网关IP：10.7.6.15 **说明：** 私网 VPN 网关 IP 归属租户 VPC。
专线网关	195.168.0.0/29	VLAN ID：1234 腾讯云边界 IP1：195.168.0.3/29

		腾讯云边界 IP2：195.168.0.2/29 客户边界 IP：195.168.0.1/29。
本地网关	195.168.0.0/24	与云上 VPN 连接的本地网关 IP：195.168.0.6 与云上专线网关连接的网段：195.168.0.1/29
本地 IDC 服务器	133.168.0.0/16	客户端地址：133.168.0.3/32

前提条件

已 创建 VPC 网络。

物理专线 已建设完成并连通。

已申请私网 VPN 使用权限，如需使用，请 提交工单 申请。

IDC 侧设备已准备就绪。

配置流程

步骤一：部署专线业务

步骤1. 创建 VPC 型专线网关

1. 登录 专线接入控制台，并在左侧导航栏单击**专线网关**。
2. 在**专线网关**页面上方选择地域和私有网络，然后单击**新建**。
3. 在**新建专线网关**对话框中配置网关详情，完成后单击**确定**。

字段	含义
名称	专线网关的名称。
可用区	选择地域所在可用区。
关联网络	选择私有网络。
所在网络	关联创建好的私有网络实例，vpc-xxx。

步骤2. 创建专线专用通道

1. 登录 专线接入 - 专用通道 控制台。
2. 在左侧导航栏，单击**专用通道** > **独享专用通道**，在页面上方单击**新建**，并配置名称、专线类型、接入网络、地域、关联的专线网关等基本名称配置，完成后单击**下一步**。

字段	含义
专用通道名称	专用通道名称。
专线类型	选“我的专线”
物理专线	选择已经就绪的物理专线。
接入网络	选择私有网络。
网关地域	选择目标私有网络实例所在地域，如广州。
专线网关	关联步骤1中创建的私网专线网关。

3. 在**高级配置**页面配置以下参数。

字段	含义
VLAN ID	配置规划好的 VLAN，例如1234。 一个 VLAN 对应一个通道，取值范围[0，3000)。
带宽	专用通道的最大带宽值，不可超过关联的物理专线的带宽值。月95后付费的计费模式下，“带宽”参数不代表计费带宽。
腾讯云边界 IP1	配置规划好的物理专线腾讯云侧的边界互联 IP，例如 `195.168.0.3/29` 请勿使用以下网段或网络地址： `169.254.0.0/16` 、 `127.0.0.0/8` 、 `255.255.255.255/32` 、 `224.0.0.0/8` - `239.255.255.255/32` 、 `240.0.0.0/8` - `255.255.255.254/32` 。
腾讯云边界 IP2	配置规划好的备用边界互联 IP，例如 `195.168.0.2/29` 。 在主边界 IP 发生故障不可用时，自动启用备用 IP，来确保您的业务正常运行。 若配置腾讯云边界 IP 掩码为30、31时，则不支持配置腾讯云边界备 IP。
用户边界 IP	配置 IDC 侧用于与专线互通的云上 IP，例如 `195.168.0.1/29` 。
路由方式	选择 BGP 路由。
健康检查	默认开启健康检查，详情请参见 专用通道健康检查。
检测模式	选择 BFD 模式。
健康检查	两次健康检查间隔时间。

间隔	
健康检查次数	如果连续执行设定次数的健康检查失败后，则执行路由切换。
BGP ASN	输入 CPE 侧的 BGP 邻居的 AS 号，腾讯云 ASN 为 45090。若不输入将由系统随机分配。
BGP 密钥	输入 BGP 邻居的 MD5 值。默认“tencent”，留空表示不需要 BGP 密钥。BGP 密钥不支持 ? & 空格" \\ +六种特殊字符。

4. 单击**提交**。

步骤二：部署 VPN 业务

步骤1. 创建私网 VPN 网关

1. 登录 私有网络控制台。
2. 在左侧目录中选择 **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
计费方式	选择按流量计费。私网 VPN 暂不支持包年包月。
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。
协议类型	选择 IPSEC。
网络类型	选择“私网”。
关联网络	此处选择私有网络。私网 VPN 暂不支持云联网。
云上子网	选择 VPC 侧创建的子网。 私网 VPN 网关 IP 地址归属租户 VPC，从该子网中分配。
带宽上	选择5M。

限	
所属网络	仅当关联网络为私有网络时，此处需要选择 VPN 网关将要关联的具体私有网络。
标签	标签是对 VPN 网关资源的标识，目的是为了方便更快速的查询和管理 VPN 网关资源，非必选配置，您可按需定义。

5. 完成网关参数设置后，单击**创建**启动 VPN 网关的创建。

步骤2. 创建对端网关

1. 在左侧导航栏选择 **VPN 连接** > **对端网关**。
2. 在**对端网关**管理页面，选择地域，单击**新建**。
3. 填写对端网关名称，私网 IP 填写 IDC 侧本地网关设备的私网 IP（195.168.0.6）。
4. 单击**创建**。

步骤3. 创建 VPN 通道

1. 在左侧导航栏选择 **VPN 连接** > **VPN 通道**。
2. 在 **VPN 通道**管理页面，选择地域，单击**新建**。
3. 在弹出的页面中填写 VPN 通道信息。

本处仅介绍重点参数配置，其他参数配置请参考 新建 VPN 通道。

参数名称	参数说明
通道名称	输入通道名称。
网络类型	选择私有网络。
私有网络	选择创建好的私有网络实例。
VPN 网关	选择 步骤1 中创建的私有 VPN 网关。
对端网关	选择 步骤2 中创建的对端网关。
预共享秘钥	配置为123456。
协商类型	选择“流量协商”。
通信模式	选择“目的路由”。
高级配置	选择当前默认值。

4. 单击**创建**。

步骤4. IDC 本地配置

完成前三步骤后，腾讯云上 VPN 网关和 VPN 通道的配置已经完成，需要继续在 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，该设备的私网 IP 记录在 步骤2 的“对端网关”中。

步骤三：配置云上路由

完成上述配置后，本地网关设备和 VPN 网关之间已经可以建立加密通信通道了。您还需要为云上网络实例配置路由，将云上和云下流量引导进入 VPN 加密通信通道。

步骤1. 配置云上 VPC 自定义路由

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，单击子网所关联的路由表 ID，进入详情页。
3. 单击**新增路由策略，**在弹出框中配置到VPN网关的路由。

参数名称	说明
目的端地址	填写本地 IDC 网段，例如 `133.168.0.3/32` 。
下一跳类型	选择“私网 VPN 网关”。
下一跳	选择 部署 VPN 时步骤1 创建的 VPN 网关，vpngw-xxxx。

4. 单击**+新增一行**，配置到专线网关的路由策略。

参数名称	说明
目的端地址	填写本地网关网关设备 VPN IP 地址，例如 `195.168.0.6` 。
下一跳类型	选择**专线网关**。
下一跳	选择 部署专线网关时 创建的专线网关，dcg-xxxx。

5. 单击**创建**。

步骤2. 配置 VPN 网关路由

注意：

为了引导 VPC 去往云下的流量进入 VPN 网关加密通信通道，需要在 VPN 网关中添加比本地 IDC 网段的路由。

1. 单击左导航栏中 **VPN 连接** > **VPN 网关**。
2. 在 **VPN 网关**页面，选择地域和私有网络，单击 VPN 网关实例 ID 进入详情页。
3. 在**实例详情**页面，单击**路由表**页签，然后单击**新增路由**配置路由策略。

说明：

VPN 网关路由表新增路由时，列表默认显示 VPN 网关下所有 VPN 通道（即 VPN 网关下所有 SPD 策略型和路由型 VPN 通道）。

配置项	说明
目的端	填写本地IDC网段，例如133.168.0.3/32。
下一跳类型	不可选，默认“VPN 通道”。
下一跳	选择部署 VPN 时创建的 VPN 通道。
权重	通道的权重值选择0。 0：优先级高。 100：优先级低。

4. 完成路由策略的配置后，单击**确定**。

步骤四：业务验证

完成上述配置后，本地 IDC 和 VPC 之间已经可以进行私网加密通信。测试本地 IDC 和 VPC 之间的私网连通性以及验证流量是否经过 VPN 网关加密。

1. 测试连通性

登录 CVM 实例，使用 **Ping** 命令访问本地 IDC 网段内服务器。

2. 加密验证

在 VPN 控制台，查看 VPN 通道监控流量情况，有流量表示加密成功。

在腾讯云和 AzureChina 之间建立 VPN 连接

最近更新时间：2024-01-09 14:41:10

在两个公有云之间建议使用 VPN 连接，保证了公有云之间流量使用内网传输，增强了网络安全性，减少了攻击面。

说明：

由于 VPN 连接涉及创建腾讯云产品与 AzureChina 云资源，教程中的步骤由于时效性原因可能与产品最新的操作步骤不一致。

本文第三方教程来自腾讯云产品“用户实践”征集，仅供学习和参考。

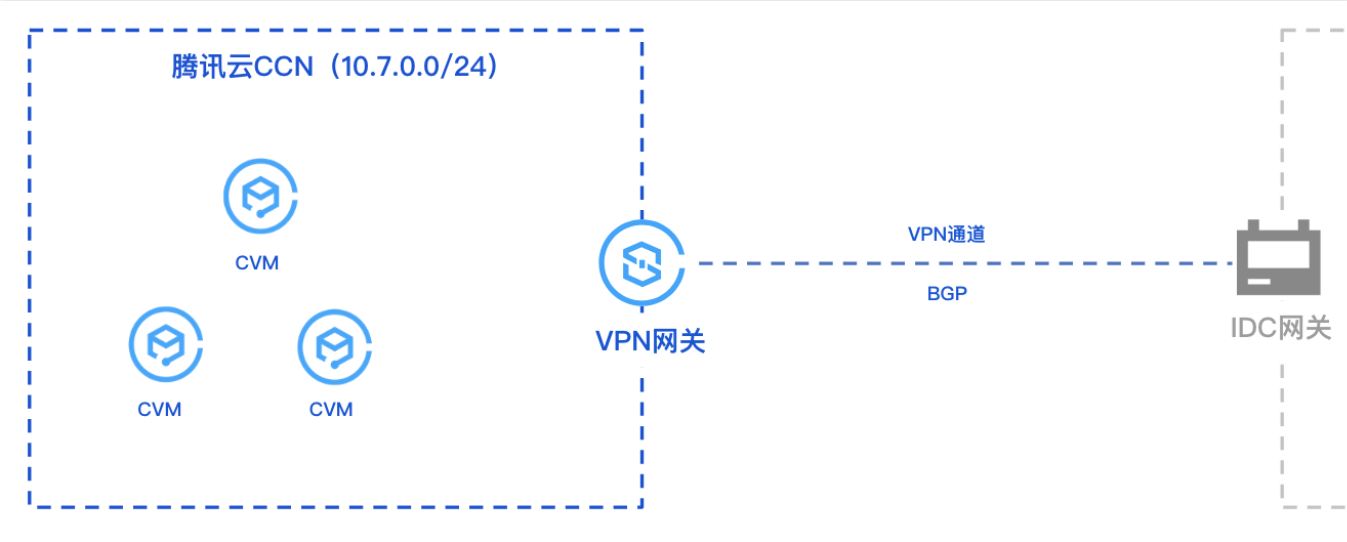
建立 IDC 与云上资源的连接（动态 BGP）

最近更新时间：2024-04-10 14:46:50

本文介绍如何通过 VPN 的动态 BGP 打通 IDC 和云上资源，实现业务通信。

业务场景

用户部分业务部署在云上，使用 VPN 连接打通了 IDC 与云上网络，并通过 BGP 进行通信。



操作流程

1. 创建云联网实例。
2. 创建 CCN 型 VPN 网关，并绑定创建好的云联网实例。
3. 创建对端网关并指定 IDC 侧 ASN。
4. 创建 VPN 通道，配置 BGP 参数。
5. IDC 侧本地配置。

操作步骤

本指引仅介绍操作过程中必要的配置步骤及其参数，其他参数详情请查看各自具体的操作文档。

步骤一：创建云联网实例

您需要在云联网控制台创建所需的云联网实例，具体操作请参见 新建云联网实例。

步骤二：创建云联网型 VPN 网关

1. 登录 VPN 网关控制台，在VPN网关页面单击**新建**。
2. 在 VPN购买页 配置 CCN 型网关参数。

地域：选择首尔。

网络类型：选择云联网。

带宽：选择200Mbps及以上规格。

BGP ASN：腾讯侧 VPN 网关 ASN 号，默认64551，取值范围为 1 - 4294967295，其中 139341、45090、58835 不可用。

3. 在 VPN 网关详情页面，绑定 步骤一 创建好的云联实例。

步骤三：创建对端网关

1. 登录 对端网关控制台，在右边对端网关页面，单击**新建**。
2. 在**新建对端网关**页面，配置 IDC 侧用于公网访问的 IP 地址和所规划的 ASN，详情可参见 创建对端网关。

步骤四：创建 BGP 路由型 VPN 通道

1. 登录 VPN 通道控制台，在右侧 VPN 通道页面，单击**新建**。
2. 在新建 VPN 通道页面，依据实际情况配置通道基本参数，配置完成继续后续配置。

参数	说明
网络类型	选择云联网。
VPN 网关	选择已配置 ASN 的云联网型 VPN 网关。
对端网关	选择配置有 ASN 对端网关。
通信模式	选择动态 BGP 路由。
BGP 邻居	用于云端和用户端互通的 BGP 隧道网段，该网段必须在 `169.254.128.0/17` 范围内。
云端 BGP 地址	云上与用户互联的 BGP IP 地址。
用户端 BGP 地址	不可修改，自动分配的用户端 BGP 互联地址。 云端 BGP 地址手动修改后，该参数随之自动更新。

步骤五：IDC 本地网关配置

完成前4步后，云上 VPN 网关和 VPN 通道的配置已经完成，需要继续在 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。

说明：

IDC 侧的“本地网关”即为 IDC 侧的 IPsec VPN 设备，该设备的公网 IP 记录在创建好的“对端网关”中。

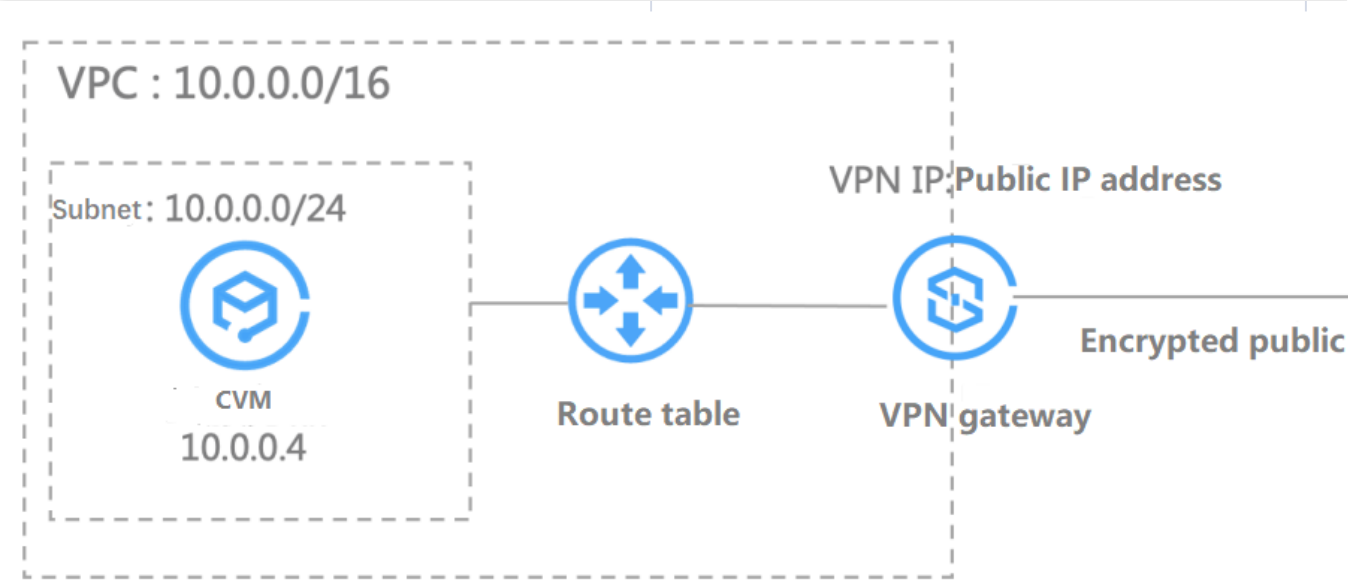
SSL VPN
建立客户端与 VPC 连接

最近更新时间：2024-01-09 14:41:10

本文为您介绍 Windows、MAC 和 Linux 客户端如何通过 SSL VPN 连接 VPC。

背景信息

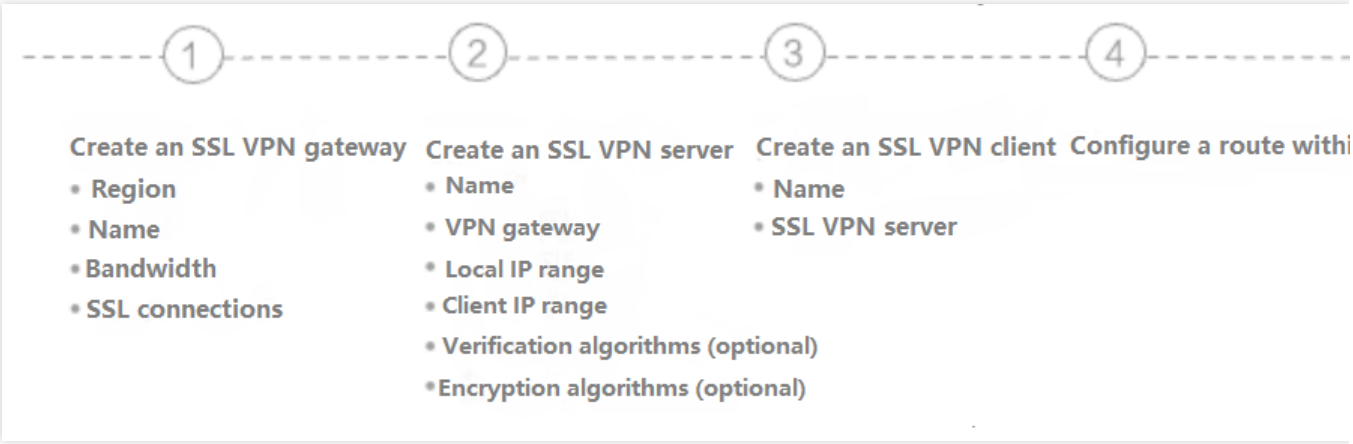
本文以下图场景为例，为您介绍 Windows、MAC 和 Linux 客户端如何使用 SSL VPN 连接VPC。



VPC route table			SSL VPN server configuration	
Destination	Next hop type	Next hop	Local IP range	10.0.0.0/16
10.0.0.0/16	Local	Local	Client IP range	192.168.0.0/1
192.168.0.0/16	VPN gateway	vpngw-12345678		

配置流程

客户端通过 SSL VPN 连接 VPC 流程图如下所示：



步骤1：创建 SSL VPN 网关

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	选择当前网关所在的可用区。
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。
所属网络	选择 VPN 网关将要关联的具体私有网络。
SSL 连接数	连接客户端的数量，一个 SSL 客户端仅允许一个用户连接，不支持一个 SSL 客户端连接多个客户。
计费方式	SSL VPN 默认为按流量计费。

5. 完成网关参数设置后，单击**创建**。

步骤2：创建 SSL 服务端

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。

说明：

一个 VPN 网关仅支持关联一个SSL 服务端，详情请参见 使用限制。

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。
本端网段	客户移动端访问的云上网段。
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。

5. 完成网关参数设置后，单击**创建**。

步骤3：创建 SSL 客户端

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。
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。
6. 在 SSL 客户端页面，找到已创建的客户端证书，然后在操作列单击**下载配置**。

说明：

一个 SSL 客户端仅允许一个用户连接，不支持一个 SSL 客户端连接多个客户。

步骤4：配置 VPC 内路由

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. 在列表中，单击需要修改的路由表 ID，进入详情页，若需新建路由表，可参考 创建自定义路由表。
4. 单击**新增路由策略**，在弹出框中，配置路由策略。

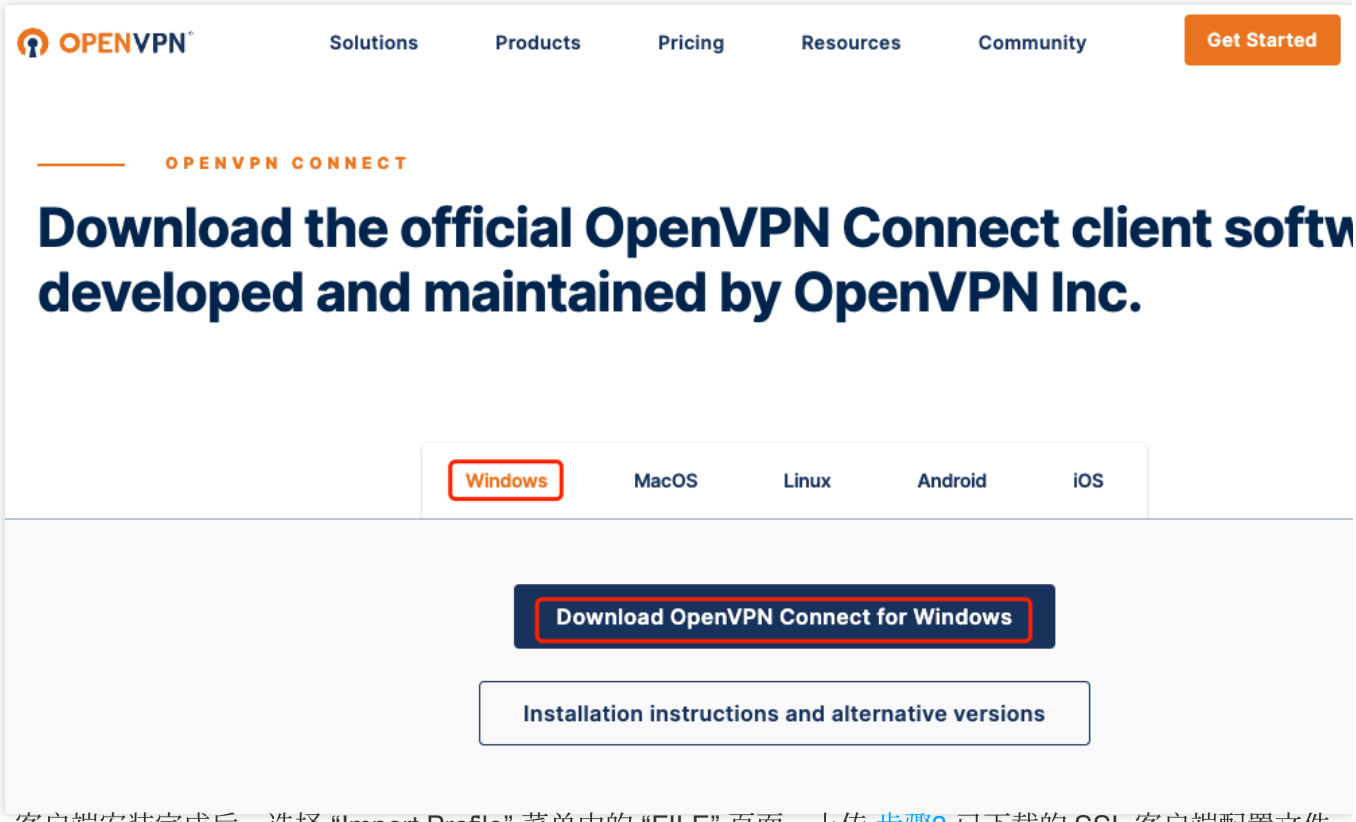
参数名称	参数说明
目的端	请填写 步骤2：创建 SSL 服务端 中创建时配置的客户端网段。
下一跳类型	选择 VPN 网关。
下一跳	下一跳选择创建好的具体 SSL VPN 网关实例。

步骤5：配置客户端

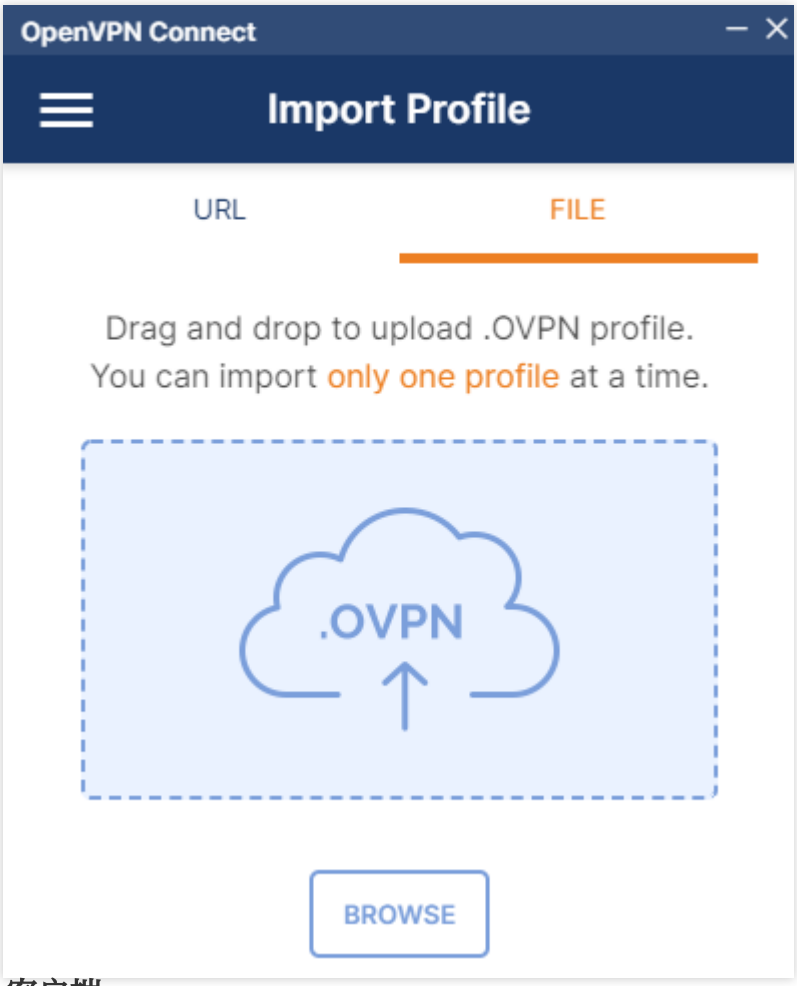
以下内容为您介绍如何配置 Windows、MAC 及 Linux 客户端。

Windows 客户端

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

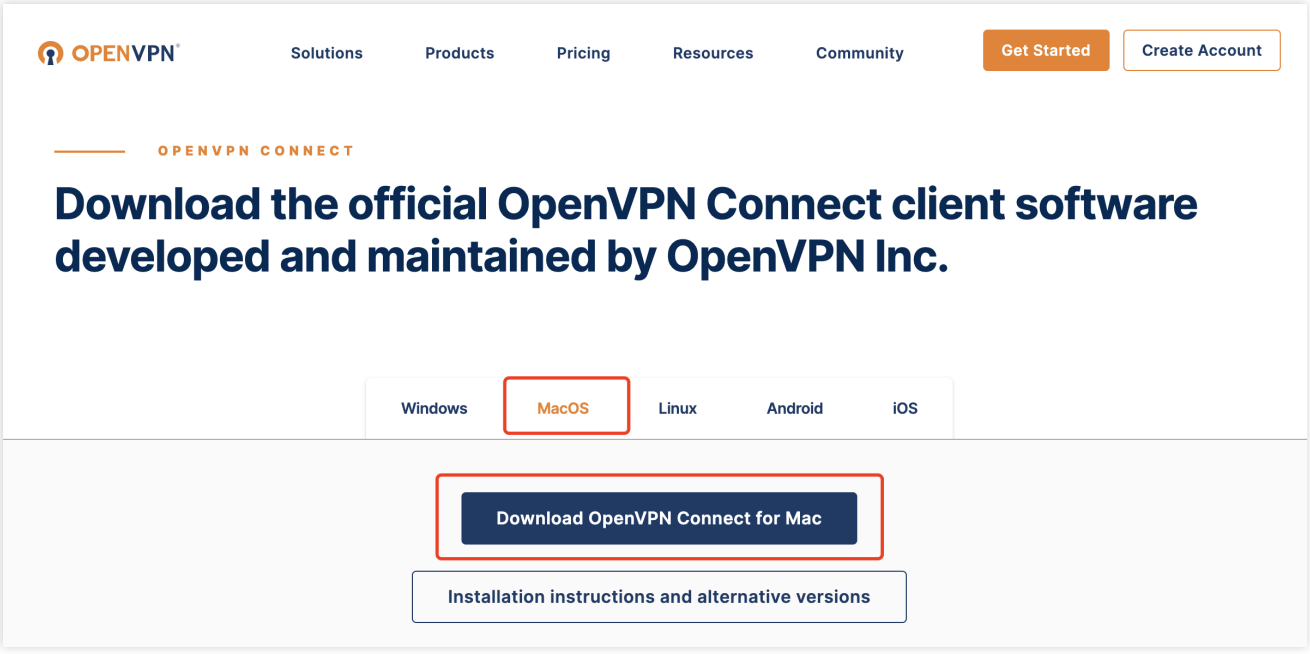


2. SSL 客户端安装完成后，选择 “Import Profile” 菜单中的 “FILE” 页面，上传 步骤3 已下载的 SSL 客户端配置文件（.ovpn 格式）。

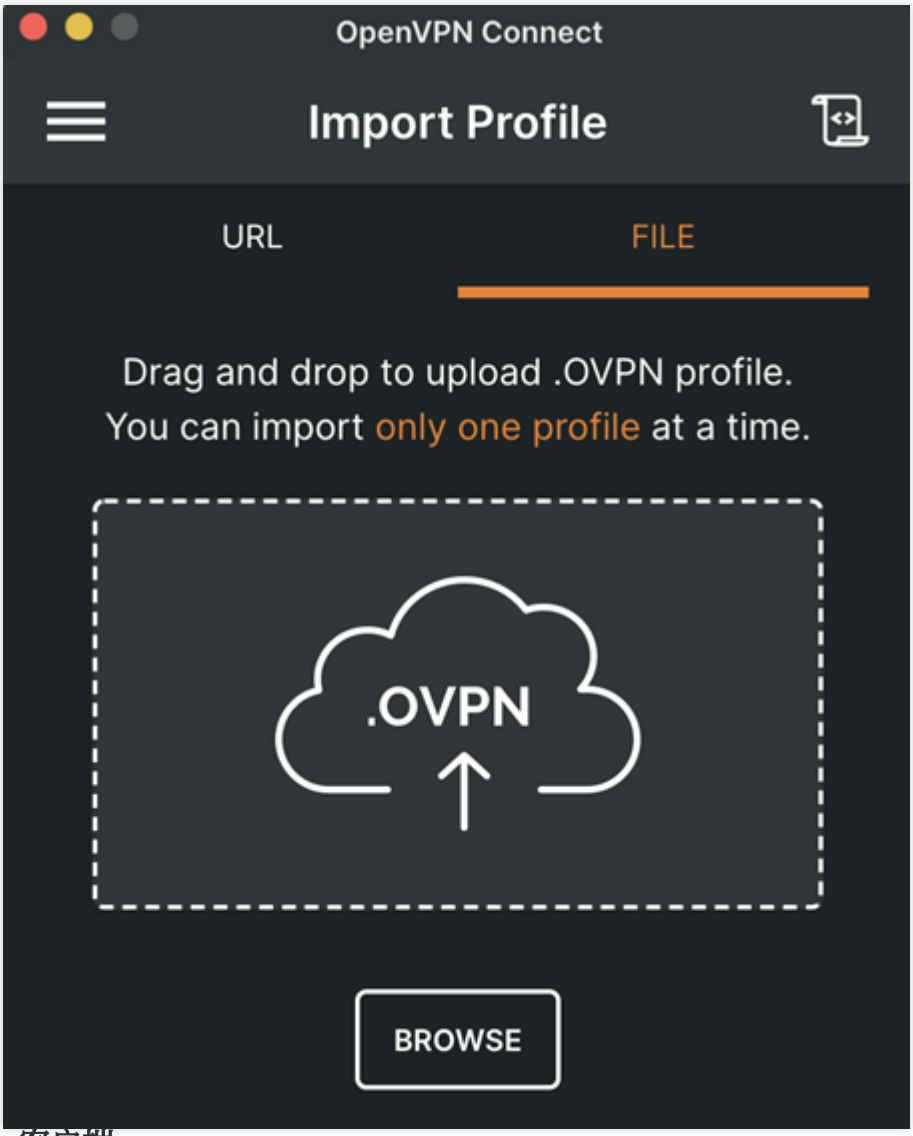


MAC 客户端

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



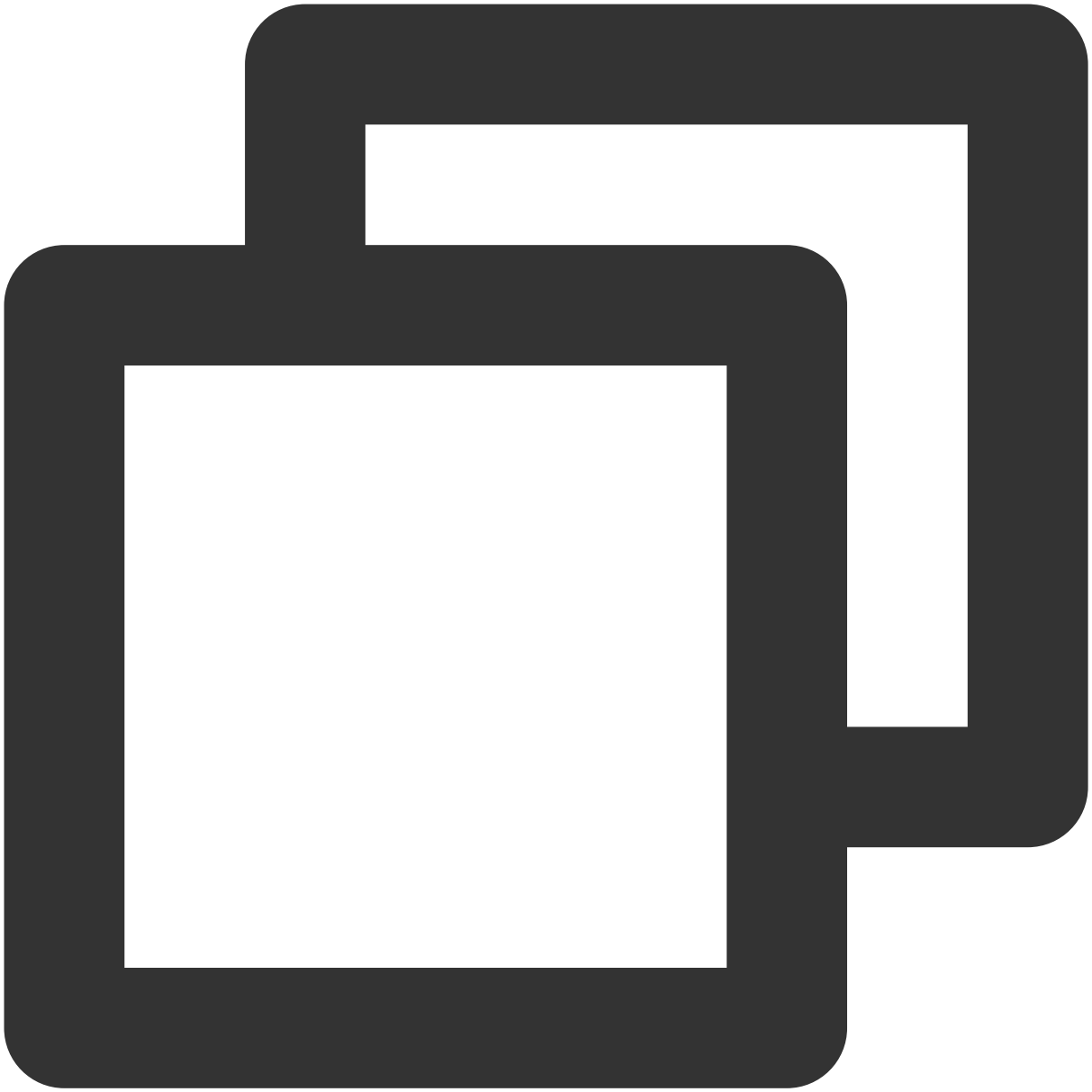
2. SSL 客户端安装完成后，选择 “Import Profile” 菜单中的 “FILE” 页面，上传 步骤3 已下载的 SSL 客户端配置文件（.ovpn 格式）。



Linux 客户端

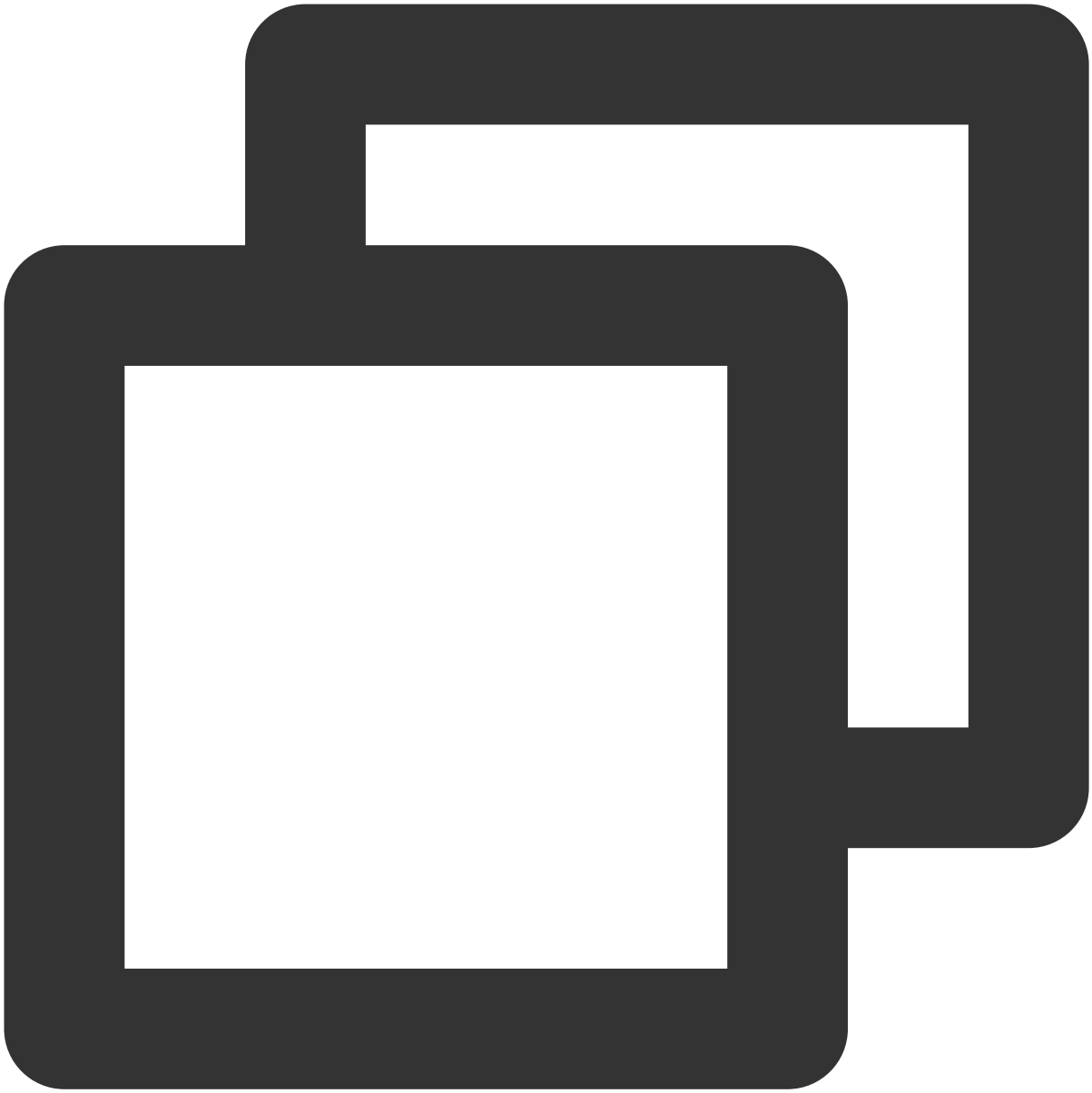
1. 打开命令行窗口。
2. 执行以下命令安装 OpenVPN 客户端。

centos 发行版



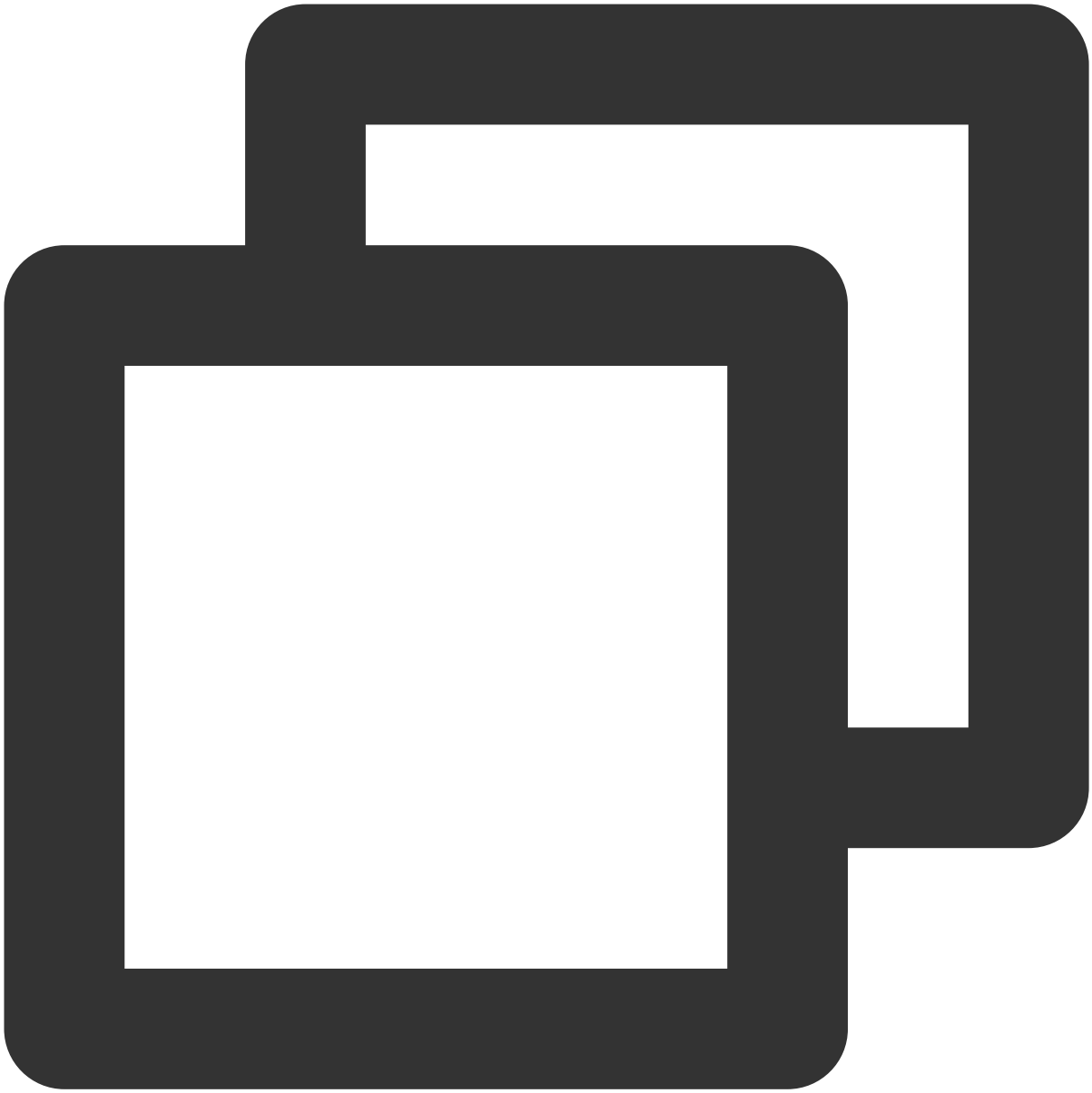
```
yum install -y openvpn
```

ubuntu 发行版



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

3. 将 步骤3 已下载的 SSL 客户端证书解压拷贝至/etc/openvpn/conf/目录。
4. 进入/etc/openvpn/conf/目录，执行以下命令建立 VPN 连接。



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

步骤6：测试连通性

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 客户端网段中的 IP，可以 ping 通表示 VPC 和客户端可以正常通信。

SSL VPN 访问控制实践指引（okta）

最近更新时间：2024-05-24 10:58:47

本文介绍如何使用第三方 IDP（okta）和 SSL VPN 实现访问控制，提升您业务的安全性。

说明：

目前 SSO 身份认证功能灰度中，当前仅支持圣保罗地域，如有需要，请提交 工单申请。

支持基于 SAML2.0 的主流第三方 IDP，如 Okta。

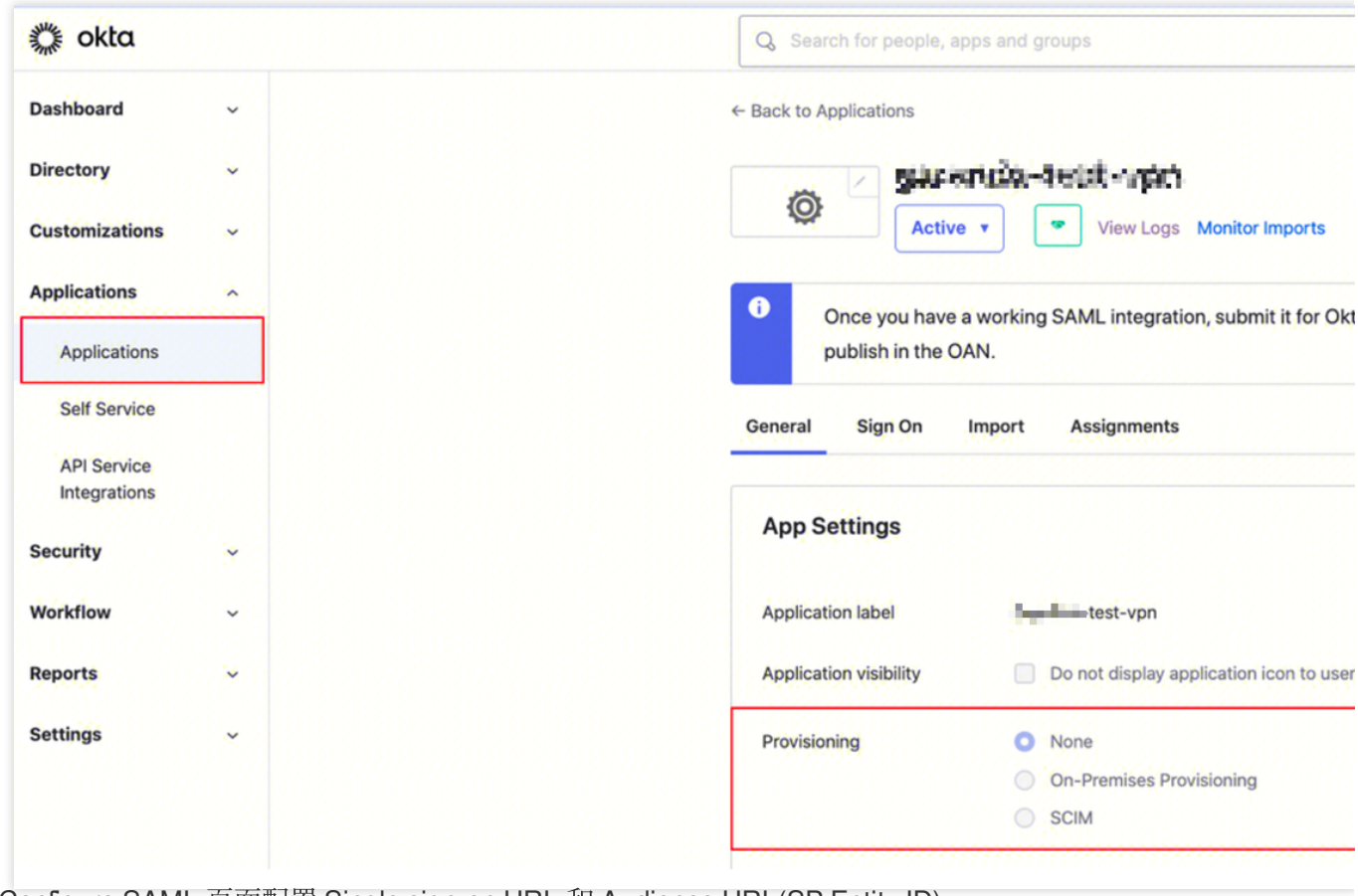
操作流程

步骤1：（租户管理员）IDP 配置（okta）

Okta 为第三方 IDP 系统，本节点仅介绍重点参数配置，Okta 具体操作步骤请查看 Okta 官网或者 okta 单点登录腾讯云指南。

通过本步骤配置 Okta 和腾讯云之间的信任关系使之相互信任。

1. 登录 Okta 官网，并创建 Okta 应用程序。
2. 进入 Applications 页面，并单击应用名称，然后在 General 页签单击 **Edit**。

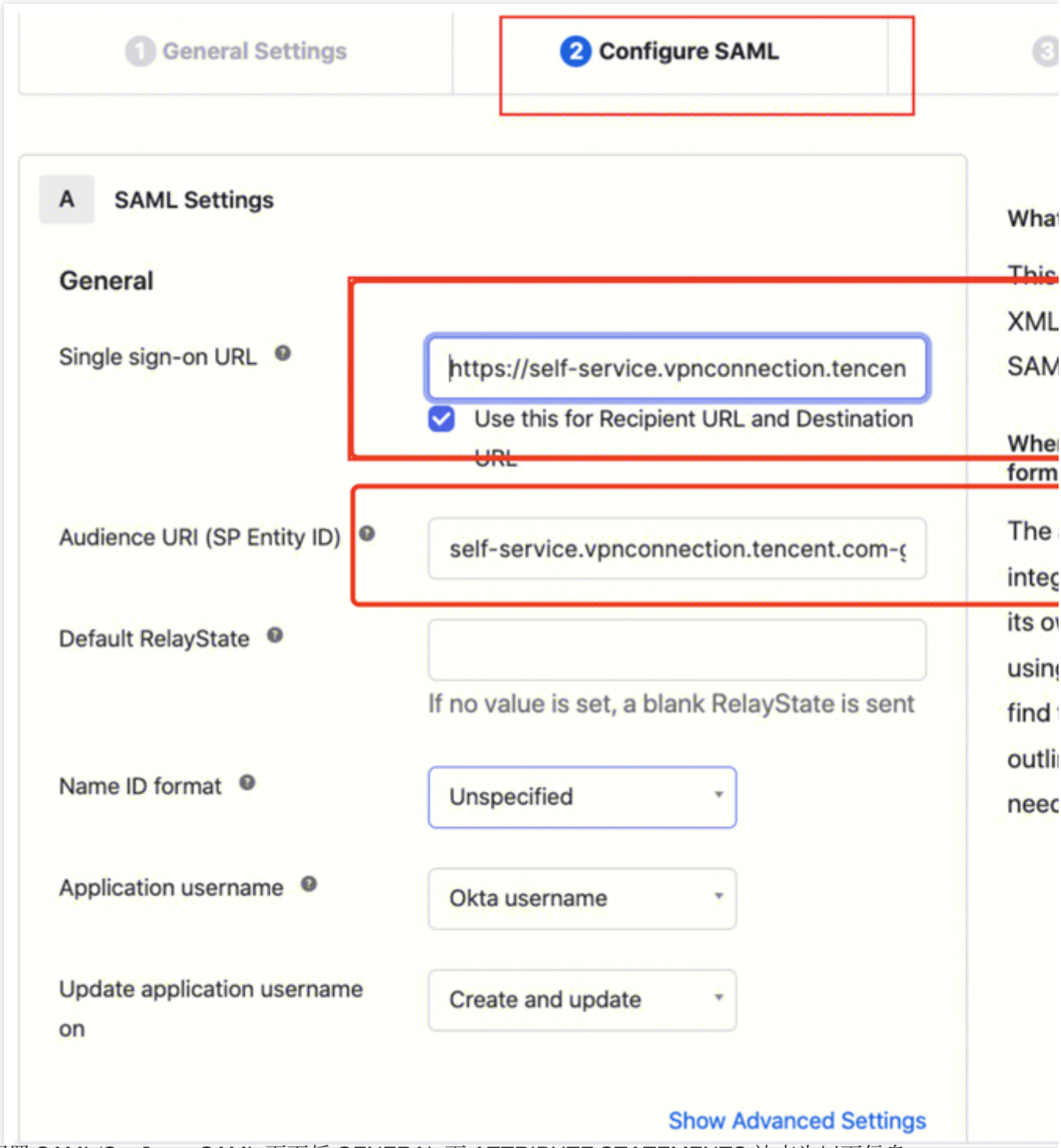


3. 在 Configure SAML 页面配置 Single sign-on URL 和 Audience URL(SP Entity ID)。

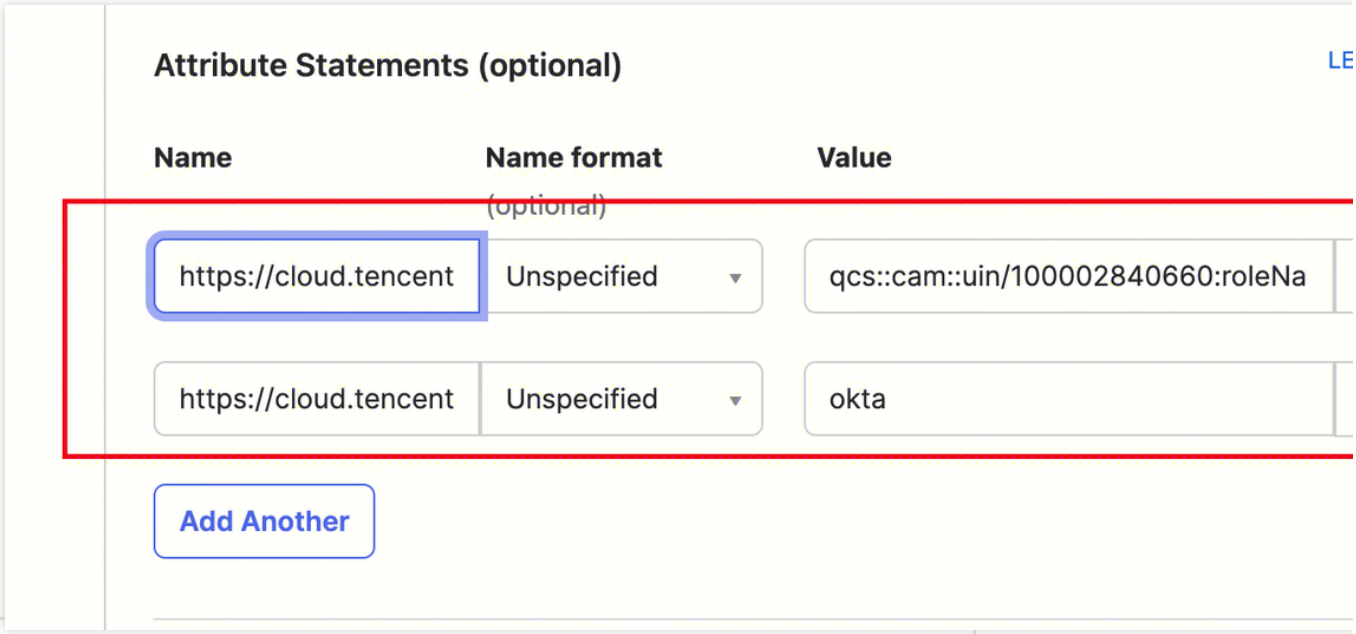
说明：

Single sign-on URL：`https://self-service.vpnconnection.tencent.com/api/auth/sso-v2/saml`，此项为固定值。

Audience URI (SP Entity ID)：腾讯云 Client VPN 自助服务门户。

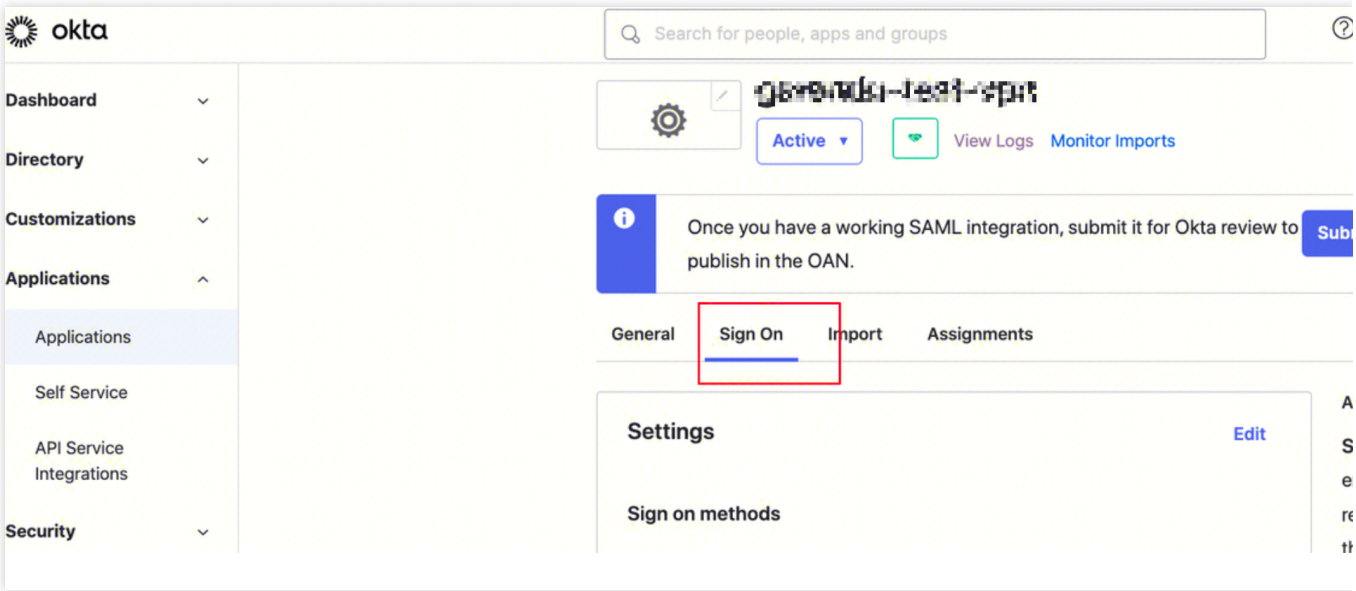


4. 在配置 SAML/Configure SAML 页面将 GENERAL 下 ATTRIBUTE STATEMENTS 补充为以下信息。

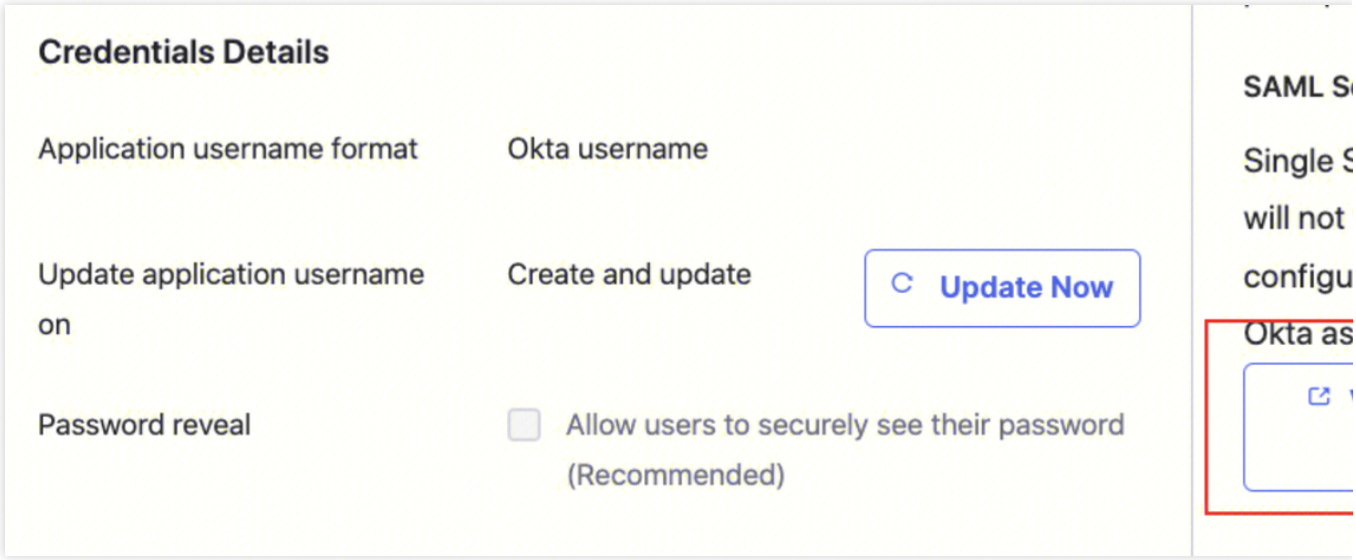


Name	Value
`https://cloud.tencent.com/SAML/Attributes/Role` :	qcs::cam::uin/{AccountID}:rol provider/{ProviderName}
`https://cloud.tencent.com/SAML/Attributes/RoleSessionName`	okta

5. 在 Sign on 页签获取生成并下载 IDP 的 SAML-Metadata 文件。

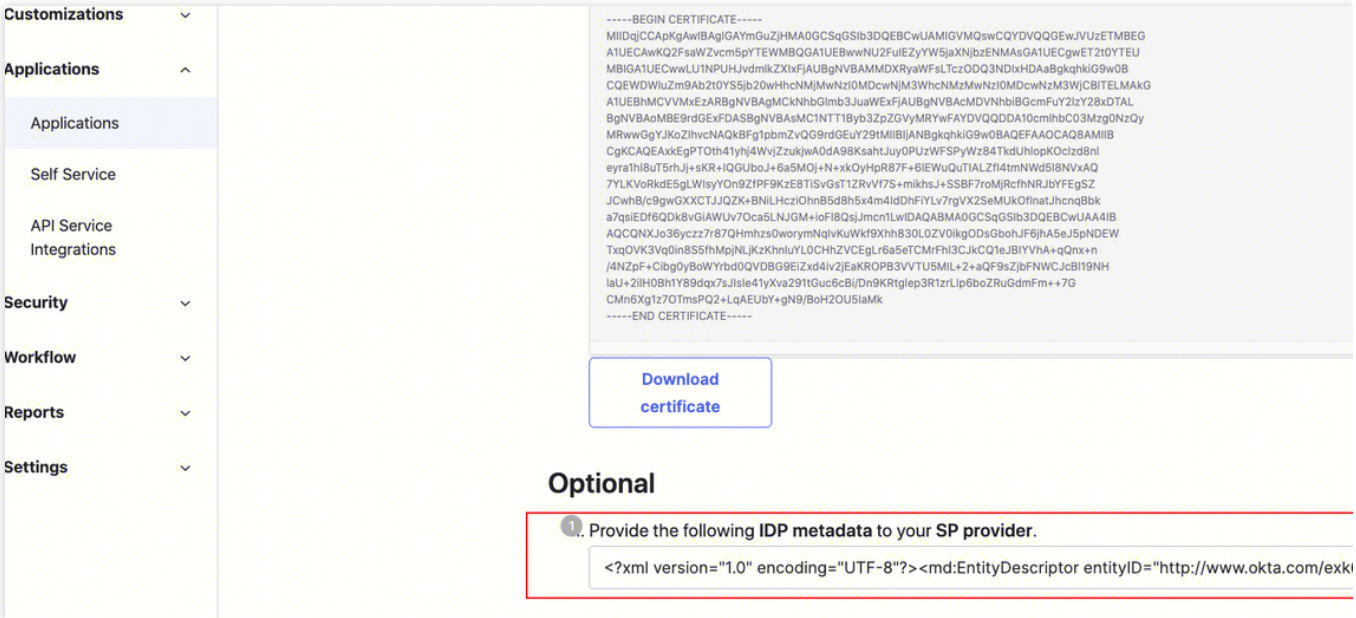


单击 View SAML setup instructions.



单击 Download certificate

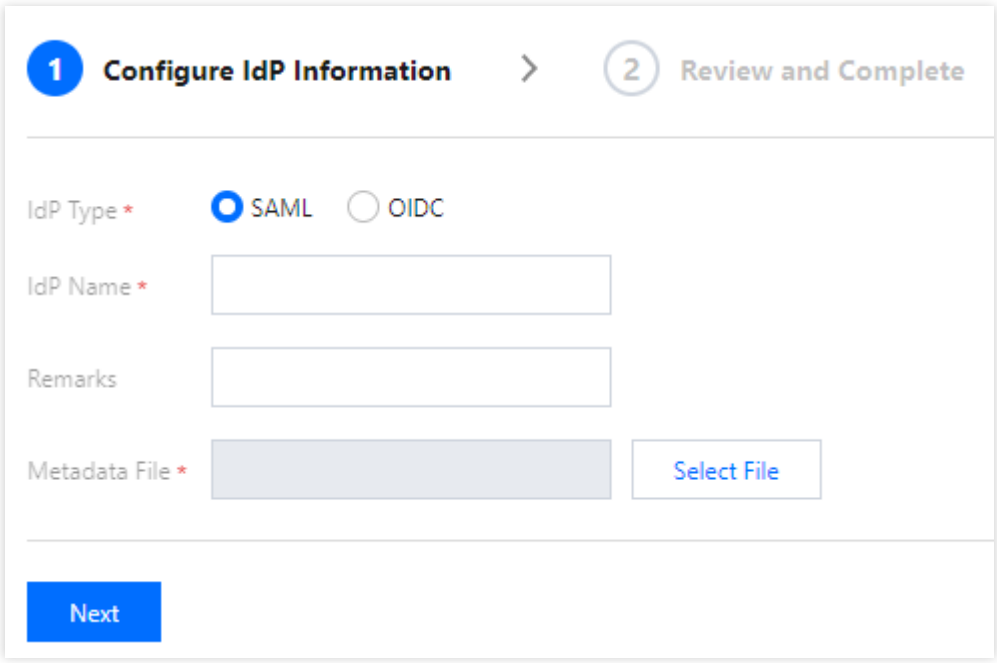
，下载好的文件需要在腾讯云 CAM 身份配置时上传，



步骤2：（租户管理员）CAM 身份配置

1. 登录访问管理（CAM）控制台，进入 身份提供商 > 角色SSO 页面，单击**新建提供商**。

2. 在新建身份提供商页面，选择提供商类型为 SAML 并配置提供商信息，单击**下一步**。



身份提供商名称：输入身份提供商名称。

备注信息：输入您对当前身份提供商的备忘信息。

元数据文档：即 步骤1：（租户管理员）IDP 配置（okta） 中下载的文件。您需要在元数据文档上传 IDP 配置中下载的 SAML-Metadata 数据文档，元数据文档内容检验合法即可上传成功。

步骤3：（租户管理员）VPN资源配置

创建 SSL VPN 网关

1. 登录 私有网络控制台，在左侧导航栏中选择 **VPN 连接** > **VPN 网关**，进入管理页。
2. 在 VPN 网关管理页面，单击**新建**，并在弹出的**新建 VPN 网关**页面，依据界面参数配置 SSL VPN 网关。

创建 SSL 服务端

1. 在左侧导航栏中选择 **VPN 连接** > **SSL 服务端**，进入管理页。
2. 在 SSL 服务端管理页面，单击**新**建，在弹出的**新建 SSL 服务端**对话框中，依据界面参数配置 SSL 服务端。

认证方式：该认证方式默认 SSL 服务端可被 SSL 客户端全量访问。

身份提供商：当前身份提供商为腾讯云 CAM，详情可查看 身份提供商 使用说明。

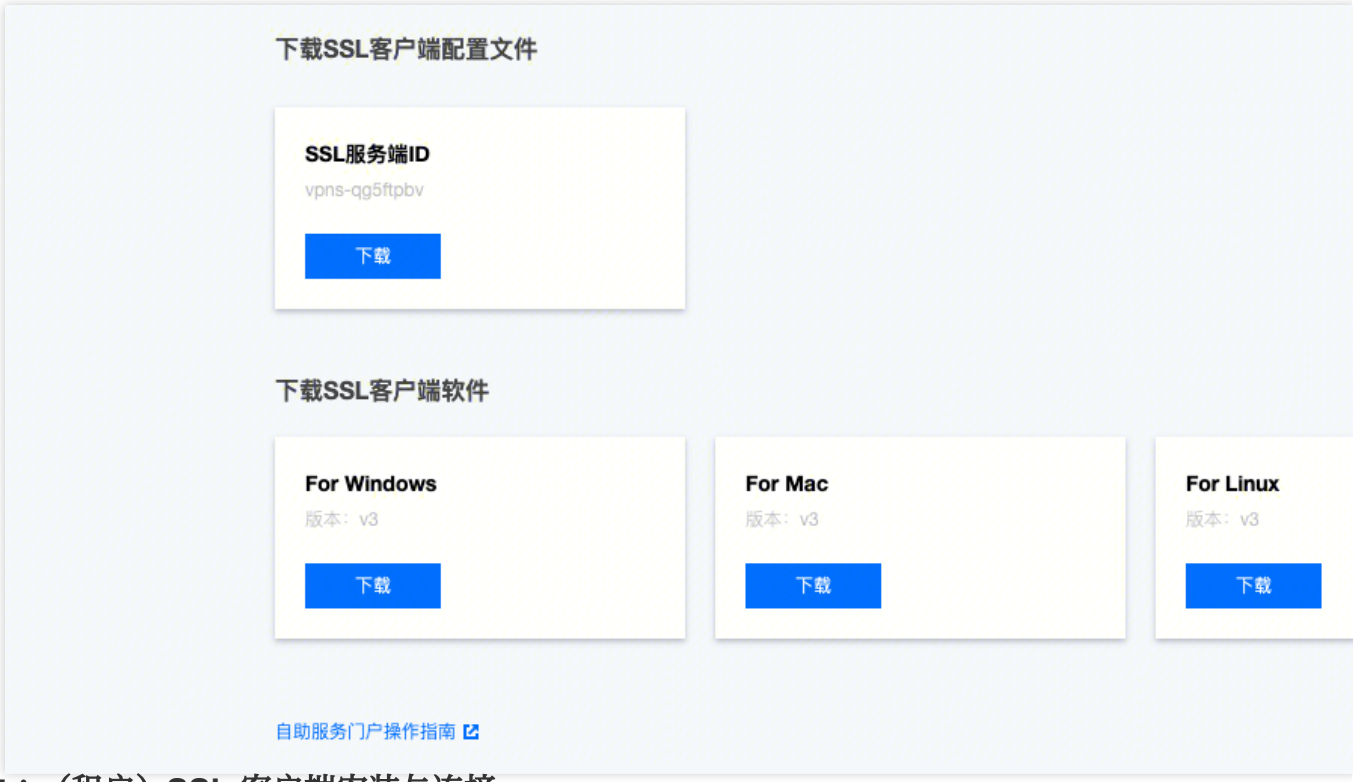
步骤4：（租户）在 Client VPN 门户下载 SSL 客户端配置文件和 SSL 客户端

1. 通过您本地浏览器访问 腾讯云Clinet VPN 自主服务门户。
2. 在 SSL 服务端 ID 所在行的输入框中输入创建好的 SSL 服务端 ID，然后单击**下一步**，开始 SSO 认证。

如果您没有或者不确定 SSL 服务端 ID，可联系租户管理员获取。

3. 单击**跳转进行认证（SAML）**后，您需要完成您的管理员指定的认证程序。
如果您没有账号或在认证登录过程中遇到其他问题，请联系您的租户管理员。在您完成认证并成功登录后，将自动登录您的业务系统。

4. 在**下载SSL客户端配置文件**区域找到您需要下载的客户端配置文件，单击**下载**。

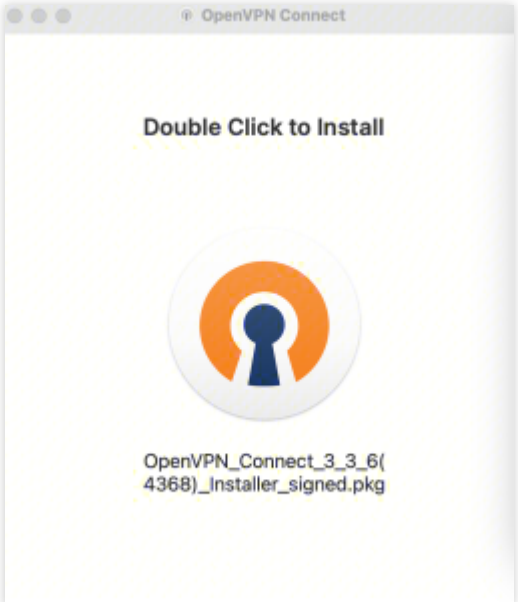


步骤5：（租户）SSL 客户端安装与连接

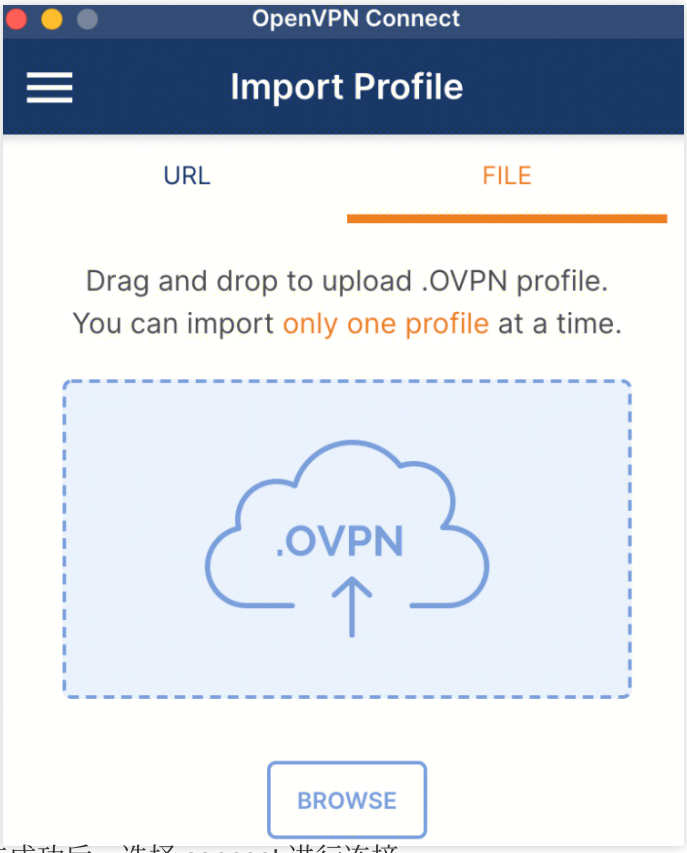
说明：

客户端 OpenVPN 请使用3.4.0及以上版本。

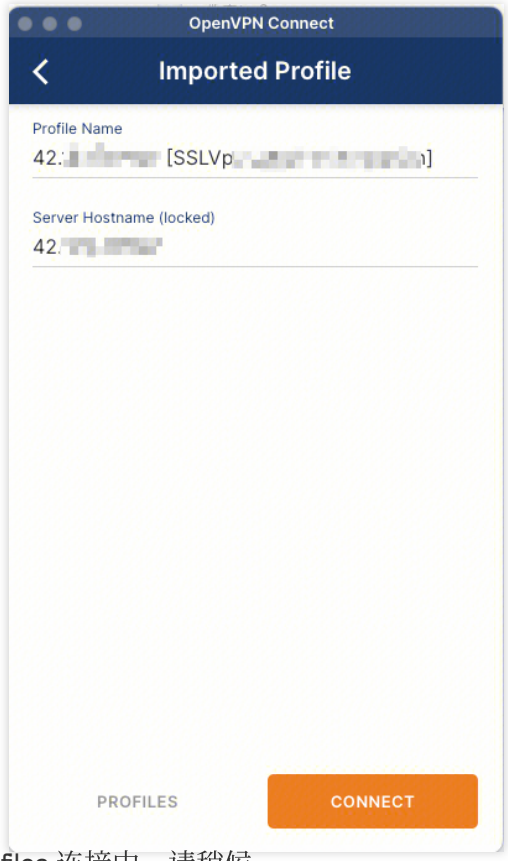
1. 在本地解压安装包，双击安装程序依据界面提示进行安装。



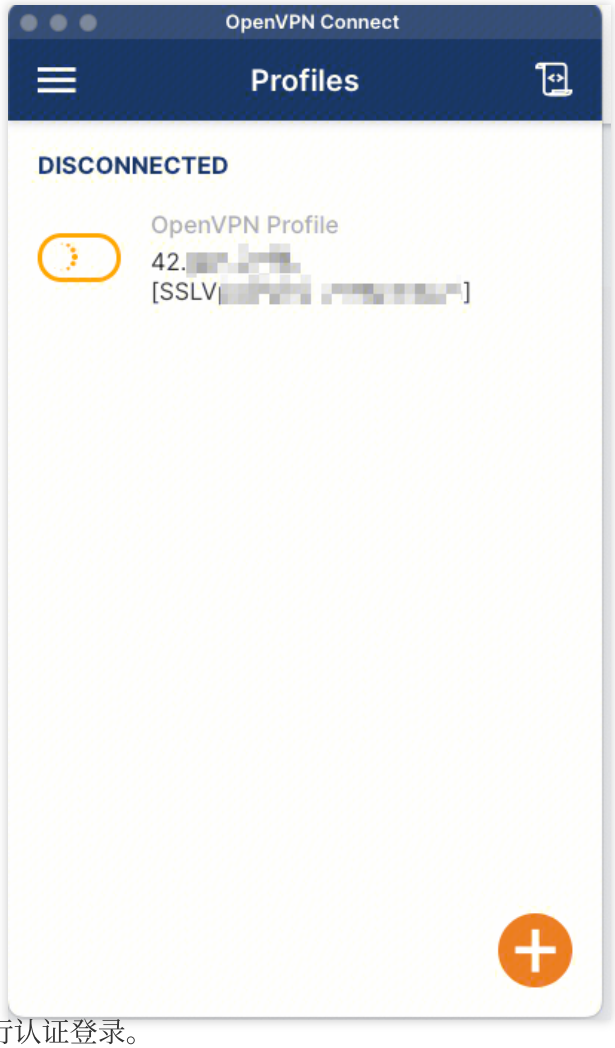
2. SSL 客户端安装完成后，选择“Import Profile”菜单中的“FILE”页面，上传已下载的 SSL 客户端配置文件（.ovpn 格式）。



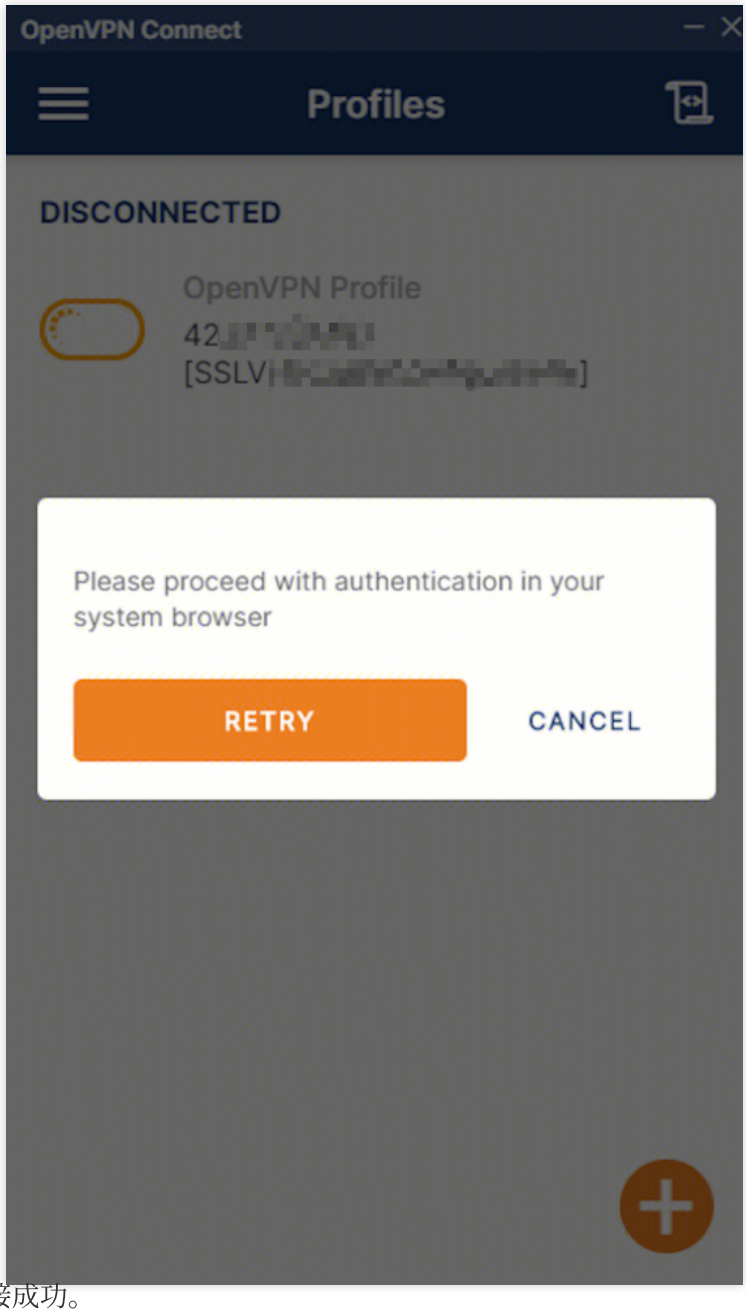
3. 上传成功后，选择 connect 进行连接。



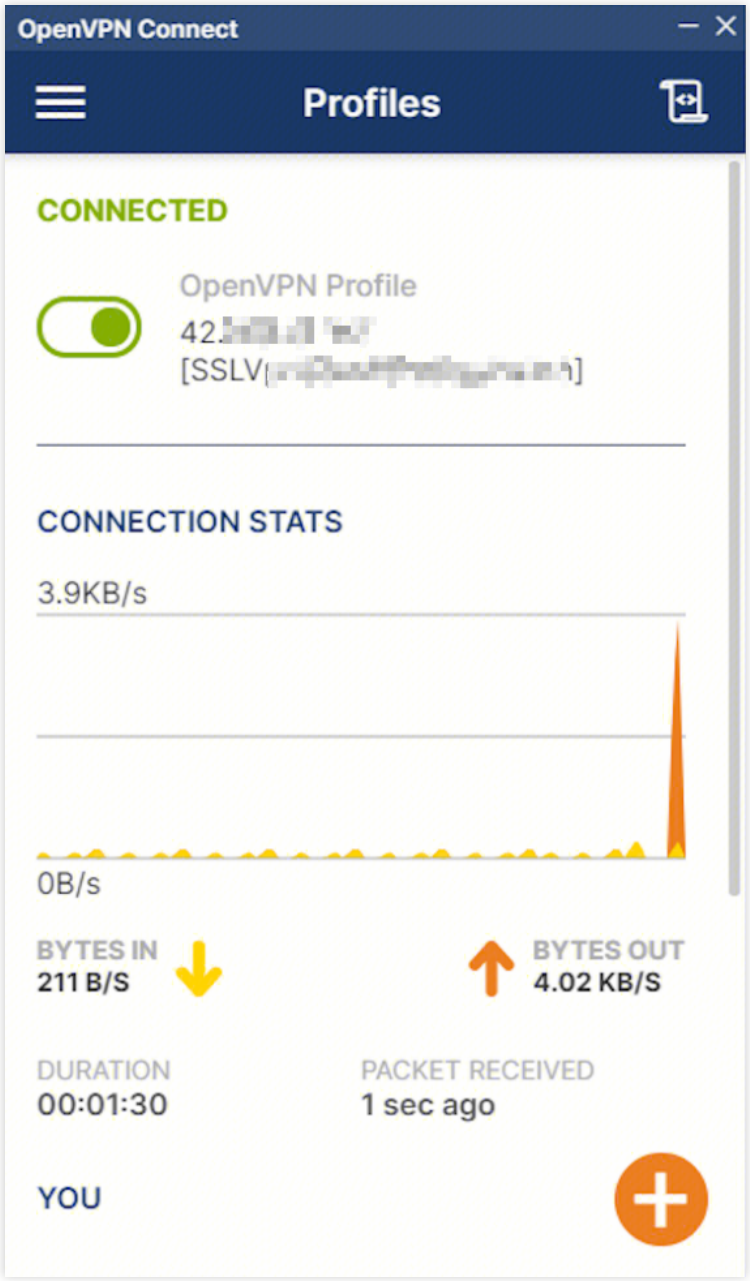
4. Profiles 连接中，请稍候。


OpenVPN Connect
Profiles
DISCONNECTED
OpenVPN Profile
42.
[SSLV

5. 进行认证登录。


OpenVPN Connect
Profiles
DISCONNECTED
OpenVPN Profile
42
[SSLV
Please proceed with authentication in your system browser
RETRY
CANCEL

6. 连接成功。


OpenVPN Connect
Profiles
CONNECTED
OpenVPN Profile
42.
[SSLV
CONNECTION STATS
3.9KB/s
0B/s
BYTES IN
211 B/S
BYTES OUT
4.02 KB/S
DURATION
00:01:30
PACKET RECEIVED
1 sec ago
YOU