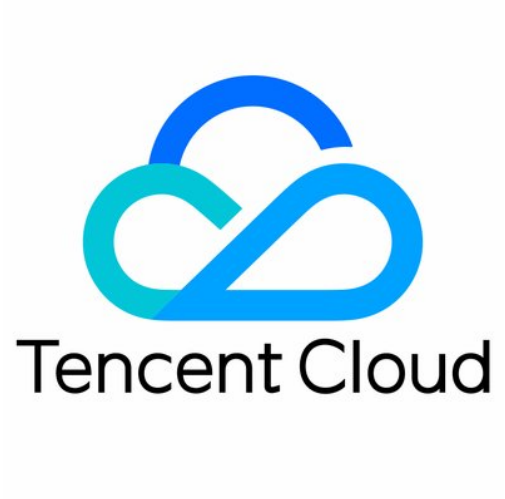
VPN Connections

Practical Tutorial

Product Documentation



Contents

Practical Tutorial
- IPsec VPN
  - Connect via Direct Connect or VPN Connection to Interconnect the Primary and Replica Links for Redundant Communication (Auto-Switch)
  - Hybrid Cloud Primary/Secondary Communication (DC and VPN)
  - Connecting IDC to CCN
  - Local Gateway Configurations
    - Configuring a Cisco Firewall
  - Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery
  - Dedicated Private Network Traffic Encrypted Via a Private Network VPN Gateway
    - Solution Overview
    - Dedicated Private Network Traffic Encrypted Via a Private Network VPN Gateway
  - Establishing a VPN Connection between Tencent Cloud and Azure China
  - Establishing Connection Between IDC and Cloud Resources (Dynamic BGP)
- SSL VPN
  - Connecting Client to VPC
  - SSL VPN Access Control Guide（okta）

Practical Tutorial
IPsec VPN
Connect via Direct Connect or VPN Connection to Interconnect the Primary and Replica Links for Redundant Communication (Auto-Switch)

Last updated：2024-05-24 10:53:09

If your business is deployed in both a local IDC and a Tencent Cloud VPC, you can connect them via direct connect or VPN connection to interconnect the cloud and local services. To improve the business high availability, set up both direct connect and VPN connection businesses. Combined with CCN, configure them as the primary and replica links for redundant communication.

Note

Currently, the routing priority feature is in beta testing. If needed, you may Contact Us.

Currently, the routing priority cannot be adjusted in the console. If you want to adjust the routing priority, you may Contact Us.

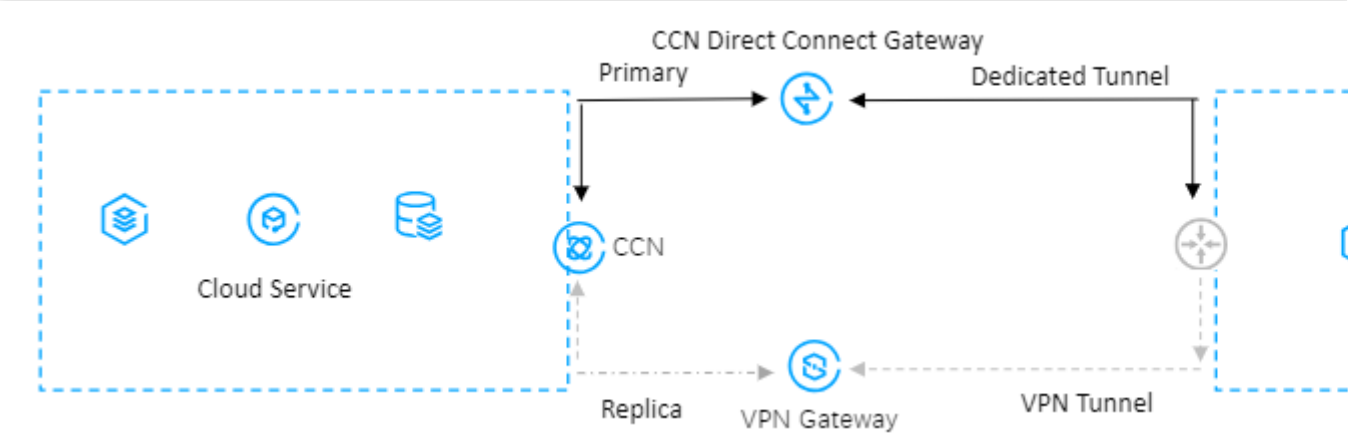
When configuring primary and replica routings, the mask length of the direct connect IP range must be longer than that of the VPN IP range.

Business Scenario

As shown below, you have deployed businesses in VPC and IDC. To interconnect them, user need to deploy network connection services for high-availability communications. When a fault occurs, business will be automatically switched. The deployment plan is as follows:

Direct Connect (primary): The local IDC is connected to a CCN-type direct connect gateway through the connection to establish the local and cloud business communication. When the connection link is normal, all data traffic between the IDC and the VPC is forwarded through the connection.

VPN Connection (replica): A CCN-type VPN security tunnel is established between the local IDC and the cloud VPC to establish the local and cloud business communication. When the direct connect link is abnormal, traffic will be forwarded using this link to ensure the business availability.



Prerequisites

Your local IDC gateway device should support the IPsec VPN feature, and can act as a user-side VPN gateway, to create a IPsec tunnel communication with the cloud-side VPN device.
The IDC-side gateway device has configured with a static IP.
A CCN instance has been created with ECMP and routing overlap features enabled. For more details, contact Technical Support.
The dynamic BGP propagation feature has been enabled on the direct connect. For more details, contact Technical Support.

Directions

Step One: Connecting IDC to Cloud Migration Through Direct Connect

1. Log in to the DC Console. Click connection in the left sidebar, and click **Create** to set up a connection. For details, see Applying for Connection.
2. Click Direct Connect Gateway in the left sidebar, and click **Create** to establish a CCN-type direct connect gateway. After creation, publish the IP range directed to CCN on the details. For detailed operations, see Creating a Direct Connect Gateway, Publishing IDC IP Ranges to CCN.
3. Click **Dedicated Tunnels** > **Exclusive Dedicated Tunnels** in the left sidebar, then click **Create** to set up an exclusive dedicated tunnel. Here, you will need to configure the tunnel name, select the direct connect type, the created direct connect gateway, and interconnect IP for both Tencent Cloud-side and user-side. Choose static routing for the routing method, and fill in the IDC communication IP range. Upon configuration, you can download the configuration guide and complete the setup on the IDC device. For detailed operations, see Exclusive Virtual Interface.

Note

For more detailed configurations, see Migrating IDC to the Cloud Through CCN.

Step Two: Connecting IDC to Cloud Migration Through a VPN Connection

1. Log in to the VPN Gateway Console. Click **Create**. For creating a CCN-type VPN Gateway, see Creating a VPN Gateway. After creation, associate a CCN instance on the details page. For detailed steps, see Associating a CCN Instance.
2. Click Customer Gateway in the left sidebar, and configure the customer gateway (i.e., the logical object of the IDC-side VPN gateway). Enter the public network IP address of the IDC-side VPN gateway. For example, 202.xx.xx.5. For detailed operations, see Creating Customer Gateways.
3. Click VPN Tunnel in the left sidebar, and click **Create** to set up a VPN tunnel. Follow page instructions to configure SPD policy, IKE, IPsec parameters. For detailed configuration information, see Creating a VPN Tunnel.
Configure the VPN tunnel information on the local gateway device at IDC. The configuration here needs to be consistent with the VPN tunnel information in Step 3. Otherwise, the VPN tunnel cannot connect properly.
Configure the routing pointing to the customer gateway in the routing table tab of the gateway.

Note

For more detailed configurations, see Connecting IDC to CCN.

Step Three: Configuring Alarms

You can configure an alarm policy to detect exceptions in the links in time. When a link has an exception, alarm notifications are sent to you automatically via emails and SMS messages. This makes you aware of the risks in advance.

1. Log in to the TCOP Alarm Policy Console.
2. Click **Create**, and enter the policy name. Choose private network/network probe for the policy type, and choose a specific network probe instance for the alarm object. Configure trigger conditions and notifications and click **Complete** to finish.

Step Four: Switching Primary and Replica Routing

When an anomaly alarm for the direct connect gateway's primary path is received, your traffic will automatically be switched to the replica routing on the VPN gateway.
If the primary direct connect returns to normal, you will need to manually switch the traffic back to the direct connect gateway.

Hybrid Cloud Primary/Secondary Communication (DC and VPN)

Last updated：2024-01-09 14:20:07

If your business is deployed in both a local IDC and a Tencent Cloud VPC, you can connect them via Direct Connect or VPN. To improve the business availability, you set up both DC and VPN connections and configure them as the primary and secondary linkage for redundant communication. This document guides you through how to configure the DC and VPN connection as primary/secondary linkages to connect your IDC to the cloud.

Note:

Currently, the route priority feature is currently in beta testing. To use this feature, please submit a ticket.

The next hop type determines the route priority in the VPC route table. The default route priority sequence from high to low is CCN, direct connect gateway, VPN gateway, and others.

Currently, the route priority in the console cannot be adjusted. If you want to adjust the route priority, please submit a ticket.

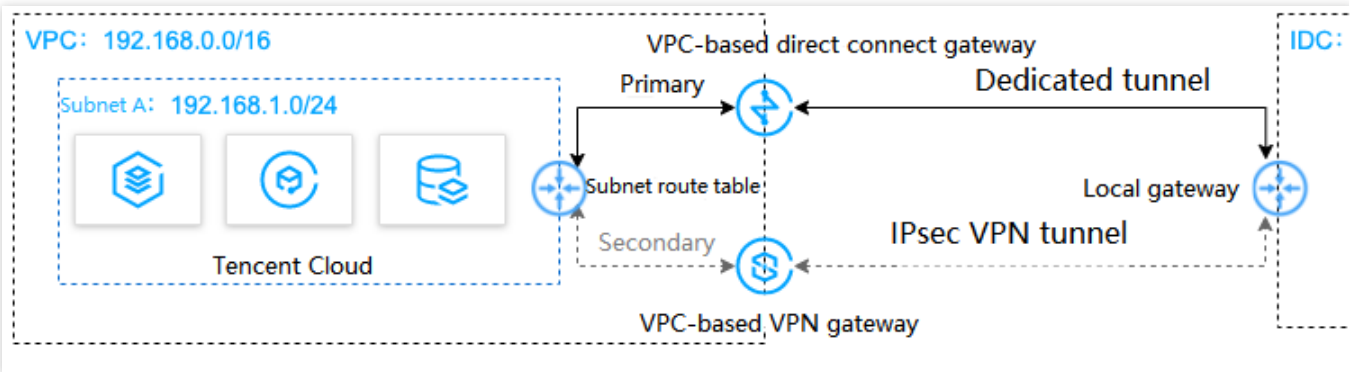
Currently, automatic switching is not supported. When a fault occurs, you must manually switch the route in the VPC.

Scenarios

You have deployed businesses in a Tencent Cloud VPC and an IDC. To interconnect them, you need to configure network connection services for high-availability communications as follows:

Direct Connect (primary): connects the local IDC to a VPC-based direct connect gateway through a connection. When the connection linkage is normal, all data traffic between the IDC and the VPC is forwarded through the connection.

VPN connection (secondary): establishes an IPsec VPN tunnel to interconnect the local IDC and the Tencent Cloud VPC. When the connection linkage fails, traffic will be forwarded using this linkage to ensure the business availability.



Prerequisites

Your local IDC gateway device should support the IPsec VPN feature and can act as a customer gateway to create a VPN tunnel with the VPN gateway.
The IDC gateway device has configured with a static IP address.
Sample data and configuration:

Configuration item			Sample value
Network	VPC information	Subnet CIDR block	192.168.1.0/24
		Public IP of the VPN gateway	203.xx.xx.82
	IDC information	Subnet CIDR block	10.0.1.0/24
		Public IP of the gateway	202.xx.xx.5

Directions

Step 1: Connect IDC to VPC through Direct Connect

1. Log in to the Direct Connect console and click **Connections** on the left sidebar to create a connection.
2. Click **Direct Connect Gateway** on the left sidebar and then click **+New** to create a direct connect gateway. In this example, we create a standard direct connect gateway that connects to a VPC. If the IP range of your IDC conflicts with the IP range of the VPC, you can create a direct connect gateway of the NAT type.
3. Click **Exclusive virtual interface** on the left sidebar and then click **+New** to create a dedicated tunnel. Enter a tunnel name and select the connection type and the direct connect gateway instance that is created. Configure the IP addresses on the Tencent Cloud and IDC sides, select the static route, and enter the IDC IP range. After the configuration is complete, click **Download configuration guide** and complete the IDC device configurations as instructed in the guide.
4. In the route table associated with the VPC subnet for communication, configure a routing policy with the direct connect gateway as the next hop and IDC IP range as the destination.

Note:
For detailed configurations, see Getting Started.

Step 2: Connect IDC to VPC through a VPN connection

1. Log in to the VPN Gateway console and click **+New** to create a VPN gateway for which the value of **Associate Network** is **Virtual Private Cloud**.
2. Click **Customer Gateway** on the left sidebar and then click **+New** to configure a customer gateway. A customer gateway is a logical object of the VPN gateway on the IDC side. Enter the public IP address of the VPN gateway on

the IDC side, such as `202.xx.xx.5` .

3. Click **VPN Tunnel** on the left sidebar and then click **+New** to complete configurations such as SPD policy, IKE, and IPsec.

4. Configure the same VPN tunnel as the step 3 on the local gateway device of the IDC to ensure a normal connection.

5. In the route table associated with the VPC subnet for communication, configure a routing policy with the VPN gateway as the next hop and IDC IP range as the destination.

Note:

For detailed directions, see Connecting VPC to IDC (Route Table).

Step 3: Configure network probes

Note:

After the first two steps, there are two VPC routes to IDC. That is, both direct connect gateway and VPN gateway act as the next hop. By default, the direct connect gateway route has a higher priority, making it the primary path and the VPN gateway the secondary path.

To stay on top of the primary/secondary connection quality, configure two network probes separately to monitor the key metrics such as latency and packet loss rate and check the availability of primary/secondary routes.

1. Log in to the VPC console.

2. Click **+New** to create a network probe. Enter a probe name and destination IP, select a VPC and a subnet, and then set **Source Next Hop** to direct connect gateway.

3. Repeat the step 2 and set the **Source Next Hop** to VPN gateway. After the configuration is complete, you can check the probed network latency and packet loss rate of the direct connect gateway and VPN connection.

Note:

For detailed configurations, see Network Probe.

Step 4: Configure an alarm policy

You can configure an alarm policy for linkages. When a linkage has an exception, alarm notifications are sent to you automatically via emails and SMS message, alerting you of the risks in advance.

1. Log in to the TCOP console and go to the Alarm Policy page.

2. Click **Create**. Enter a policy name, select VPC/Network Probe for the policy type, and specify the network probe instances as the alarm object. Then, configure trigger conditions, alarm notifications, and other information and click **Complete**.

Step 5: Switch between primary and secondary routes

After receiving the exception alarms about the direct connect gateway, you need to manually disable the primary route, and forward traffic to the secondary route VPN gateway.

1. Log in to the VPC console and go to the Route Tables page.

2. Locate the route table associated with the VPC subnet for communication, click the **ID/Name** to enter its details page. Click


to disable the primary route with the CCN as the next hop. Then the VPC traffic destined to IDC will be forwarded to the VPN gateway, instead of the direct connect gateway.

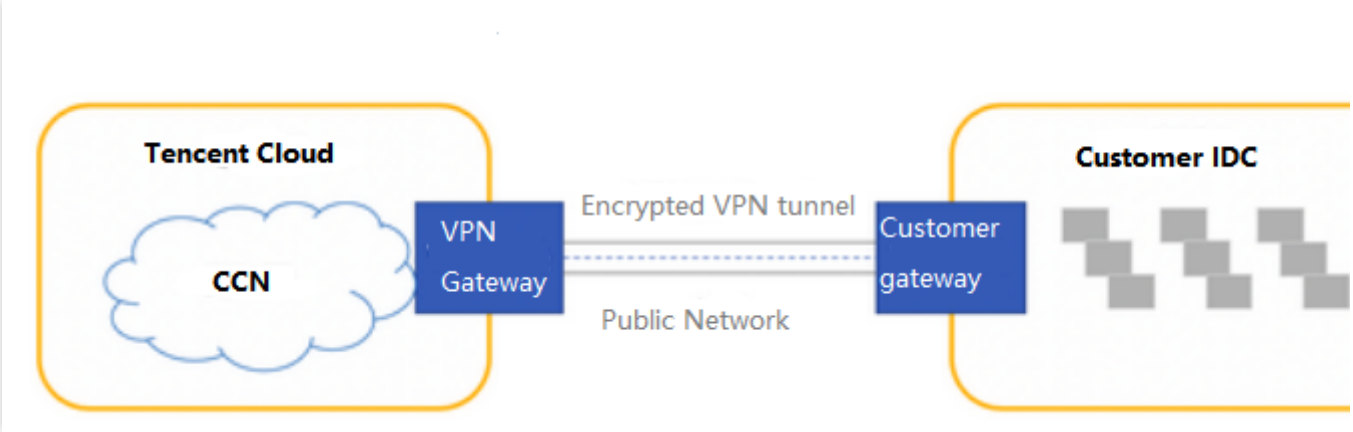
Connecting IDC to CCN

Last updated：2024-01-09 14:20:07

The VPN gateway for CCN can be associated with the Cloud Connect Network (CCN) to establish an encrypted communication between the IDC and CCN. This document introduces how to associate the VPN gateway for CCN with CCN.

Background

A VPN gateway for CCN can be associated with CCN and create multiple encrypted VPN tunnels. Each VPN tunnel can connect one local IDC.



The steps to associate the VPN gateway for CCN with CCN are as follows:

1. Create a VPN gateway for CCN: a VPN gateway is an egress gateway used by CCN along with the customer gateway to establish VPN connections.
2. Associate CCN instances: associate the VPN gateway for CCN with CCN instances.
3. Create a customer gateway: a customer gateway is a logical object used with a Tencent Cloud VPN gateway to record the fixed public IP address of the IPsec VPN gateway on the IDC side. A VPN gateway can establish encrypted VPN tunnels with multiple customer gateways.
4. Create a VPN tunnel: VPN tunnel supports IPsec encryption protocol, which ensures secure data transmission.
5. Configure the VPN gateway route: configure the VPN gateway route to the customer gateway.
6. Configure the IDC devices: configure the VPN tunnel for Tencent Cloud on the local gateway of the IDC.
7. Enable the IDC IP range: add the IDC IP range of the SPD policy to CCN.

Directions

Step 1: create a VPN gateway for CCN

1. Log in to the VPC console.
2. Choose **VPN Connection** > **VPN Gateway** in the left sidebar.
3. On the **VPN Gateway** page, specify **Region** in the topbar and click **+New**.
4. In the **Create VPN Gateway** pop-up window, specify the gateway name (for example, TomVPNGw), associated network, bandwidth cap, and billing method, and then click **Create**. After the VPN gateway is created, the system randomly assigns the gateway a public IP address such as `203.195.147.82` .

Note:

To create a VPN gateway for CCN in the specified availability zone, please submit a ticket.

Parameter	Configuration
Gateway name	Enter the VPN gateway name (up to 60 characters)
Region	Display the region of the VPN gateway
AZ	Select the availability zone of the current gateway
Protocol Type	IPSec and SSL protocols are supported.
Bandwidth cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Associated Network	Select CCN.
Tag	Tags mark VPN gateway resources so that these resources can be queried and managed efficiently. Tag is not a required configuration. You can decide whether to configure it according to your demand.
Billing Mode	Bill-by-traffic mode is supported. This billing mode is applicable to scenarios with significant bandwidth fluctuations.

Step 2: associate CCN instances

You can associate an existing CCN instance by the following steps:

1.1 Return to the **VPN Gateway** page, click the ID of an existing VPN gateway for CCN in the list to view its details.

1.2 On the **Basic Information** tab, click

next to **Network**, select a CCN instance you want to associate from the drop-down list, and then click **Save**.

You can associate a new CCN instance by the following steps:

1.1 Click **CCN** in the left sidebar.

1.2 On the **CCN** page, specify **Region** in the topbar and click **+New**.

1.3 In the pop-up window, complete the following configurations and then click **OK**.

1.1 Enter the name and description for the CCN instance. Select its billing mode, service quality, and bandwidth limit mode.

1.1.1 Select **VPN Gateway** under **Associate with Instance**, and specify the region and ID of an existing VPN gateway for CCN.

Step 3: create a customer gateway

1. Log in to the VPC console.
2. Choose **VPN Connection** > **Customer Gateway** in the left sidebar.
3. On the **Customer Gateway** page, specify **Region** in the topbar and click **+New**.
4. In the **Create Customer Gateway** pop-up window, enter the name and public IP of the customer gateway on the IDC side, and click **Create**.

Step 4: create a VPN tunnel

1. Log in to the VPC console.
2. Choose **VPN Connection** > **VPN Tunnel** in the left sidebar.
3. On the **VPN Tunnel** page, specify **Region** in the top bar and click **+New**.
4. Configure the basic information about the VPN tunnel as prompted.

Note:

IDC IP ranges in each rule cannot overlap.

Rules for tunnels in the same gateway cannot overlap.

Peer IP ranges in the SPD policy can be added to CCN.

5. Configure DPD and health check options.

DPD: By default, DPD is enabled. Retain the default settings. To modify the settings, check the parameters on the page.

Health check: By default, health check is disabled. Retain the default settings.

6. (Optional) Configure IKE parameters. Click **Next** if no advanced configuration is required.
7. (Optional) Configure IPsec parameters. Click **Completed** if no configuration is required.
8. Click **Create**. After the VPN tunnel is created, go back to the VPN tunnel list page. In the **Actions** column of the VPN tunnel, choose **More** > **Download config file** to download the configuration file.

Step 5: configure the VPN gateway route

After the VPN tunnel configuration is complete, configure the VPN gateway route to the customer gateway.

1. Choose **VPN Connection** > **VPN Gateway** in the left sidebar to go to the **VPN Gateway** page. Locate the VPN gateway that you created, and click the value in the **ID/Name** column to enter the gateway details page.
2. Click the **Route Table** tab and click **Add a route**.
3. Configure the policy of routing from the VPN gateway to the customer gateway.

Configuration	Description

Item	
Destination	Enter the IDC IP range configured in the customer gateway for the public access.
Next Hop Type	The default value is VPN Tunnel.
Next Hop	Select a VPN tunnel that has been created.
Weight	Enter an integer within 0-100. The smaller the value, the higher the priority.

4. Click **OK**.

Step 6: configure the IDC devices

After the VPN gateway and VPN tunnel are configured on Tencent Cloud, you must configure the VPN tunnel on the local gateway of the IDC. For more information, see Local Gateway Configurations.

Step 7: enable IDC IP ranges

Note:

This step is applicable only to VPN gateways v1.0 and v2.0.

If you use a VPN gateway v3.0 for CCN and have associated the gateway with a CCN instance, the routing policy in which the next hop is **CCN** will be automatically obtained and displayed in the route table. The routing policy configured on the VPN gateway is also automatically synchronized to CCN.

For VPN gateways v1.0 and v2.0, enable the IDC IP ranges as follows:

1. Log in to the VPC console.
2. Choose **VPN Connection** > **VPN Gateway** in the left sidebar.
3. Click the **ID**/**Name** of the VPN gateway for CCN in the list to view its details.
4. Click the **IDC IP Range** tab, and enable the IP range as needed.

Result Validation

1. Log in to the VPC console.
2. Select **Cloud Connect Network** in the left sidebar to go to the **CCN** page.
3. In the list, click the **ID**/**Name** of the CCN instance associated with the VPN gateway for CCN to view its details.
4. Click the **Route table** tab. If the table shows that the enabled IP range is in the **Valid** state and **Next hop** is a VPN gateway for CCN, the CCN instance is associated.

Local Gateway Configurations
Configuring a Cisco Firewall

Last updated：2024-01-09 14:20:07

To connect your IDC to a Tencent Cloud VPC via IPsec VPN connection, you need to configure the VPN on the gateway device of your local IDC after configuring the VPN gateway on Tencent Cloud. This document introduces how to configure the VPN on a Cisco firewall of the local IDC.

Note:

This document introduces the common configurations of Cisco ASA firewalls.

Replace all the IPs, ports, and other parameters given in this document with your actual values for configurations.

Prerequisites

You have created a VPN connection as instructed in Creating VPN Gateways in a Tencent Cloud VPC, and configured the VPN tunnel as instructed in Creating VPN tunnel.

Data Preparations

The following table describes the IPsec VPN configuration data.

Configuration item			Sample value
Network	VPC information	Subnet CIDR block	10.1.1.0/24
		Public IP of the VPN gateway	159.xx.xx.242
	IDC information	Private CIDR block	172.16.0.0/16
		Public IP of the gateway	120.xx.xx.76
IPsec VPN connection	IKE	Version	IKEV1
		Identity verification method	Pre-shared key
		PSK	tencent@123
		Encryption agorithm	AES-128
		Authentication algorithm	MD5

		Negotiation mode	main
		Local ID	IP address: 120.xx.xx.76
		Remote ID	IP address: 159.xx.xx.242
		DH group	DH2
		IKE SA lifetime	86400
	IPsec	Encryption algorithm	AES-128
		Authentication algorithm	MD5
		Packet encapsulation mode	Tunnel
		Security protocol	ESP
		PFS	disable
		IPsec SA lifetime (in seconds)	3600 s
		IPsec SA lifetime (in KB)	1843200 KB
Firewall	Interface	Nameif	outside

Directions

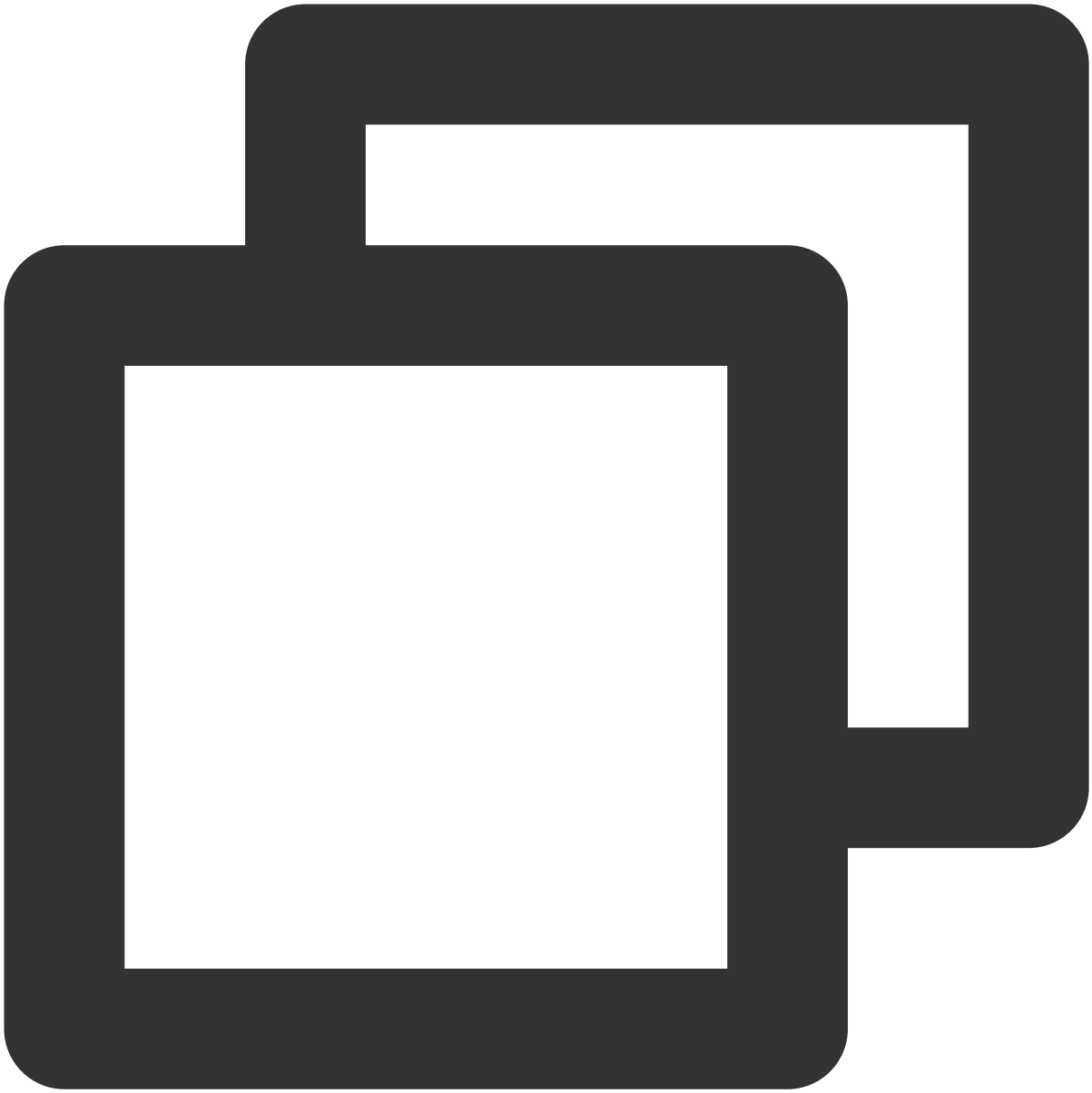
SPD policy-based VPN (IKEv1)

Route-based VPN (IKEv1)

SPD policy-based VPN (IKEv2)

Route-based VPN (IKEv2)

1. Log in to the command-line interface of the firewall device.

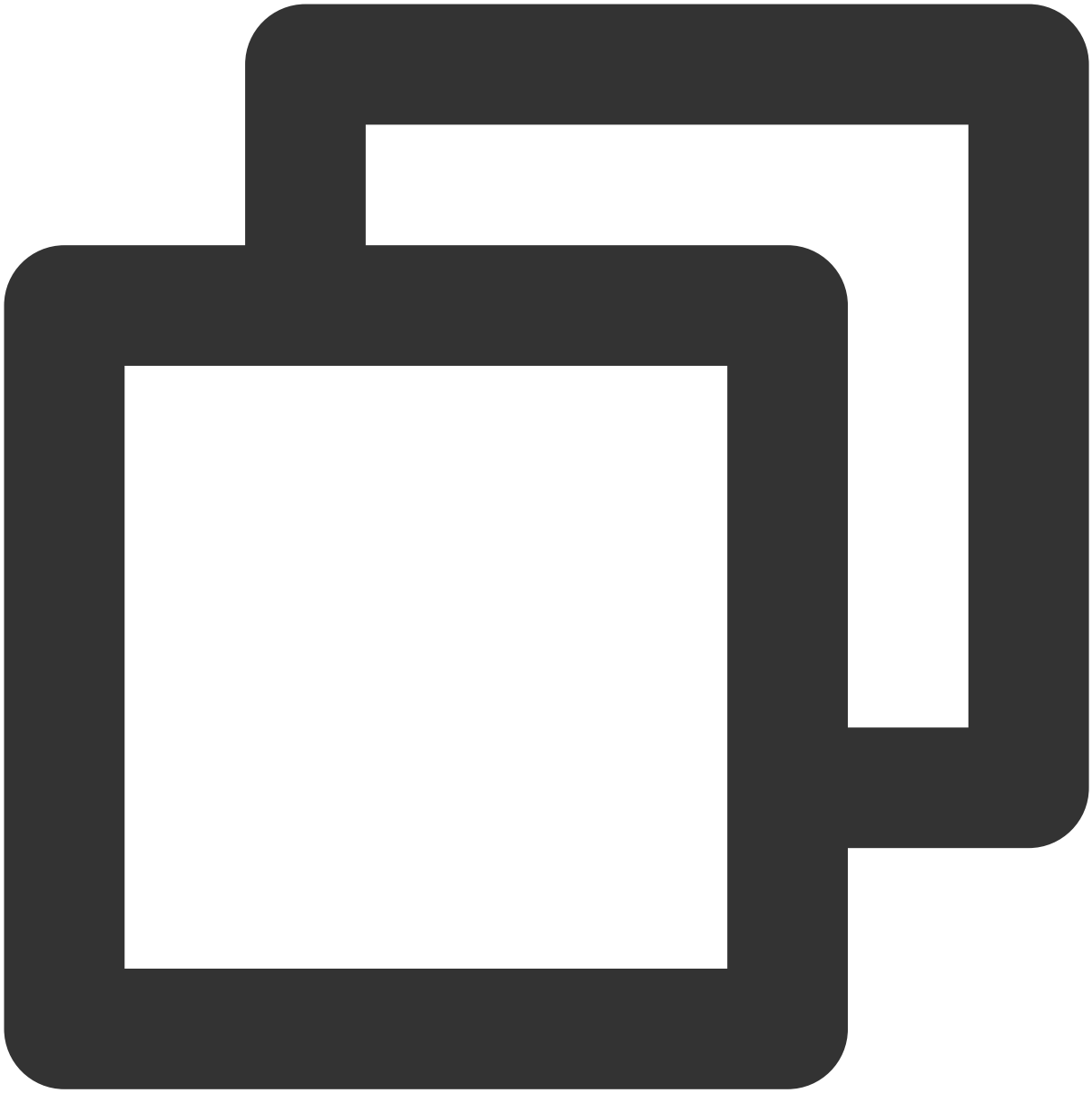


```
   ssh -p admin@10.XX.XX.56

# Use the SSH command to log in to the configuration interface of the firewall.

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

# Enter the username and password to enter the user mode.
```

```
ASA>
ASA> en
Password:

# Input “enable” and its password to enter the privileged EXEC mode in which you ca

ASA# conf t
ASA(config)#

# Input "config ter" to enter the global mode in which you can configure the firewa
```

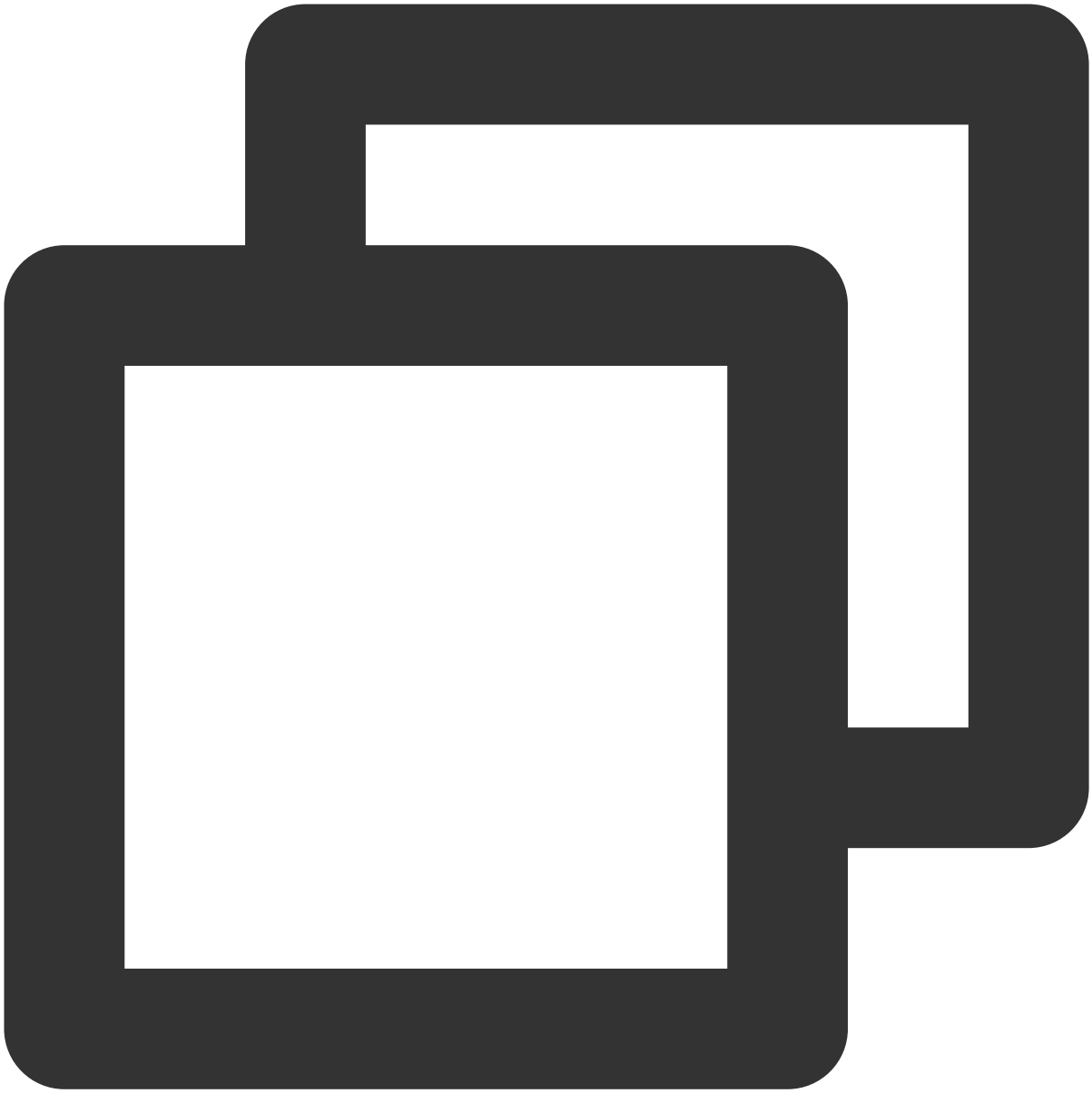
2. Configure the firewall interface.

In the global mode, configure the firewall interface that connects to Tencent Cloud.



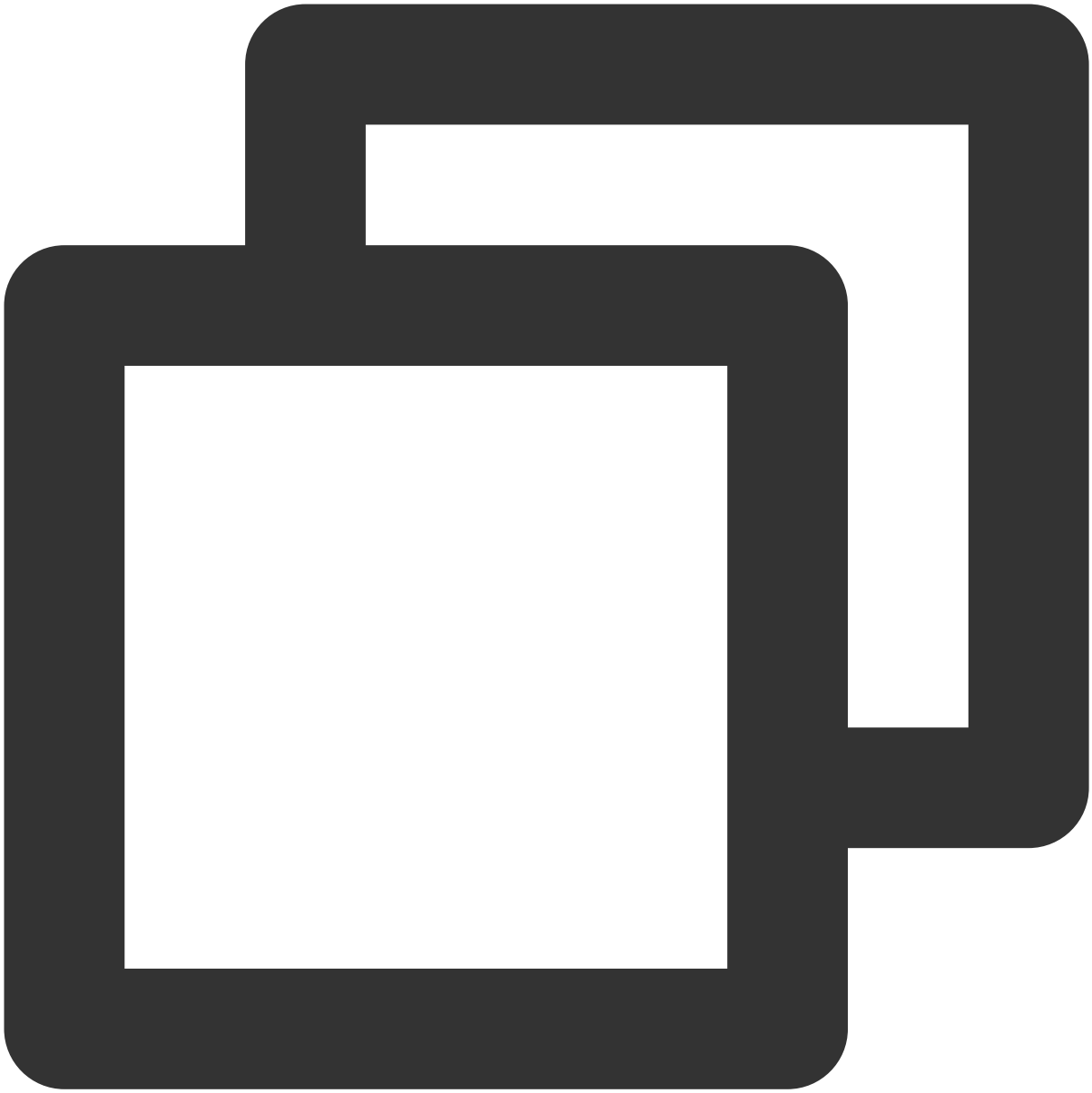
```
interface GigabitEthernet0/0
nameif outside  # Specify the security domain of the interface.
security-level 0  # Specify the security domain level of the interface.
ip address 120.XX.XX.76 255.255.255.252  # Configure the local public IP address
```

3. Configure an ISAKMP policy.



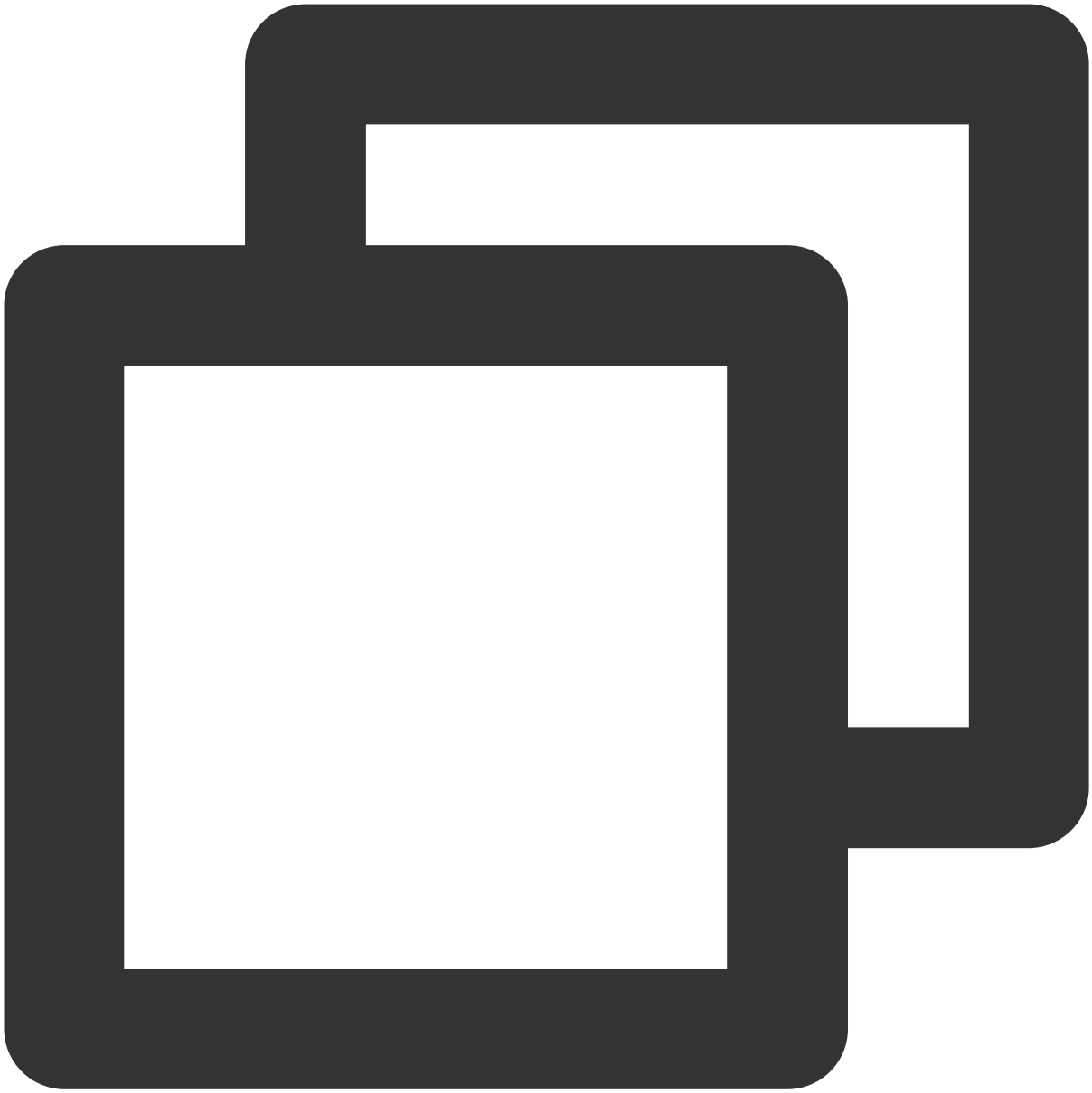
```
crypto ikev1 enable outside  # Enable IKE on the "outside" interface.
crypto ikev1 policy 10  # Define the phase 1 negotiation policy for IKEv1. Enter
authentication pre-share  # Set the authentication method to authentication via
encryption AES-128  # Specify the packet encapsulation encryption algorithm for
hash MD5  # Set the hash algorithm to “MD5” for the IKE policy. It defaults to "
group 2  # Use Diffie-Hellman group 2 for the IKE policy. It defaults to "group
lifetime 86400  # Specify the SA lifetime. It defaults to "86400" seconds.
```

4. Configure the pre-shared key.



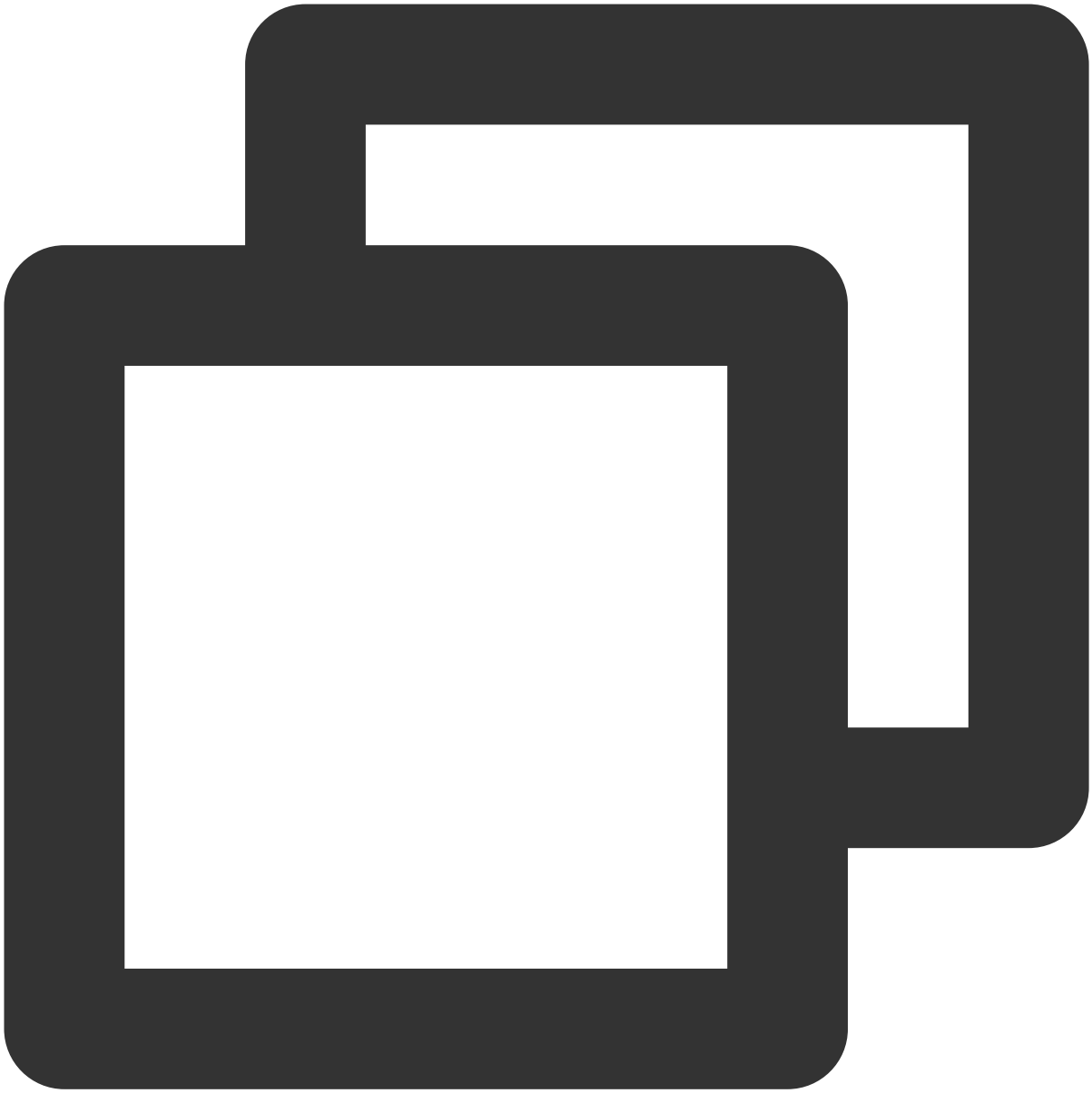
```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # Create a point-to-point IPsec tunne
tunnel-group 159.XX.XX.242 ipsec-attributes  # Configure the tunnel group attrib
ikev1 pre-shared-key tencent@123  # Enter letters, numbers or strings as the key
```

5. Configure the IPsec security protocol.



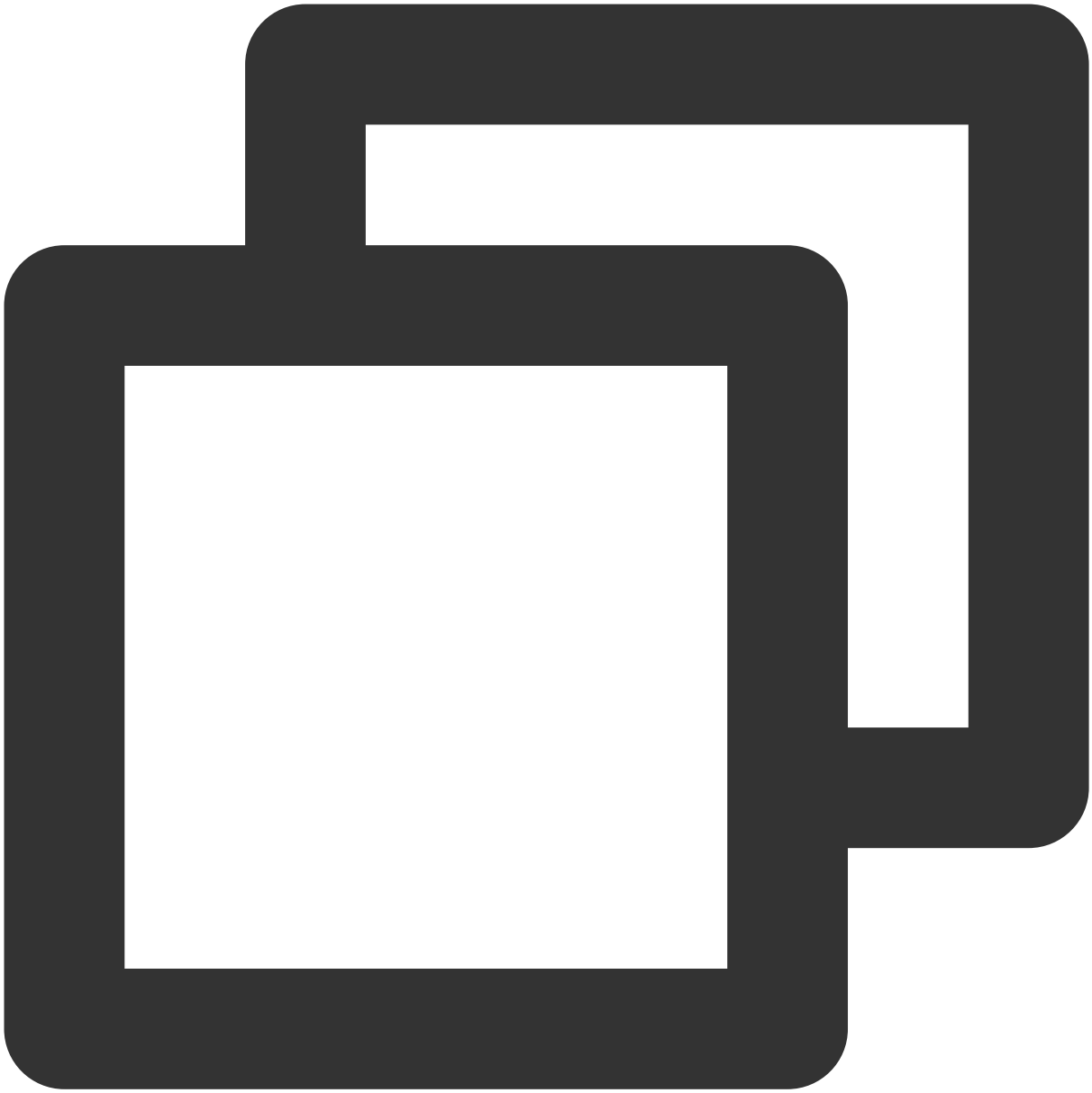
```
    crypto ipsec ikev1 transform-set TS esp-aes esp-md5-hmac  # Specify the encrypti
```

6. Configure ACL.



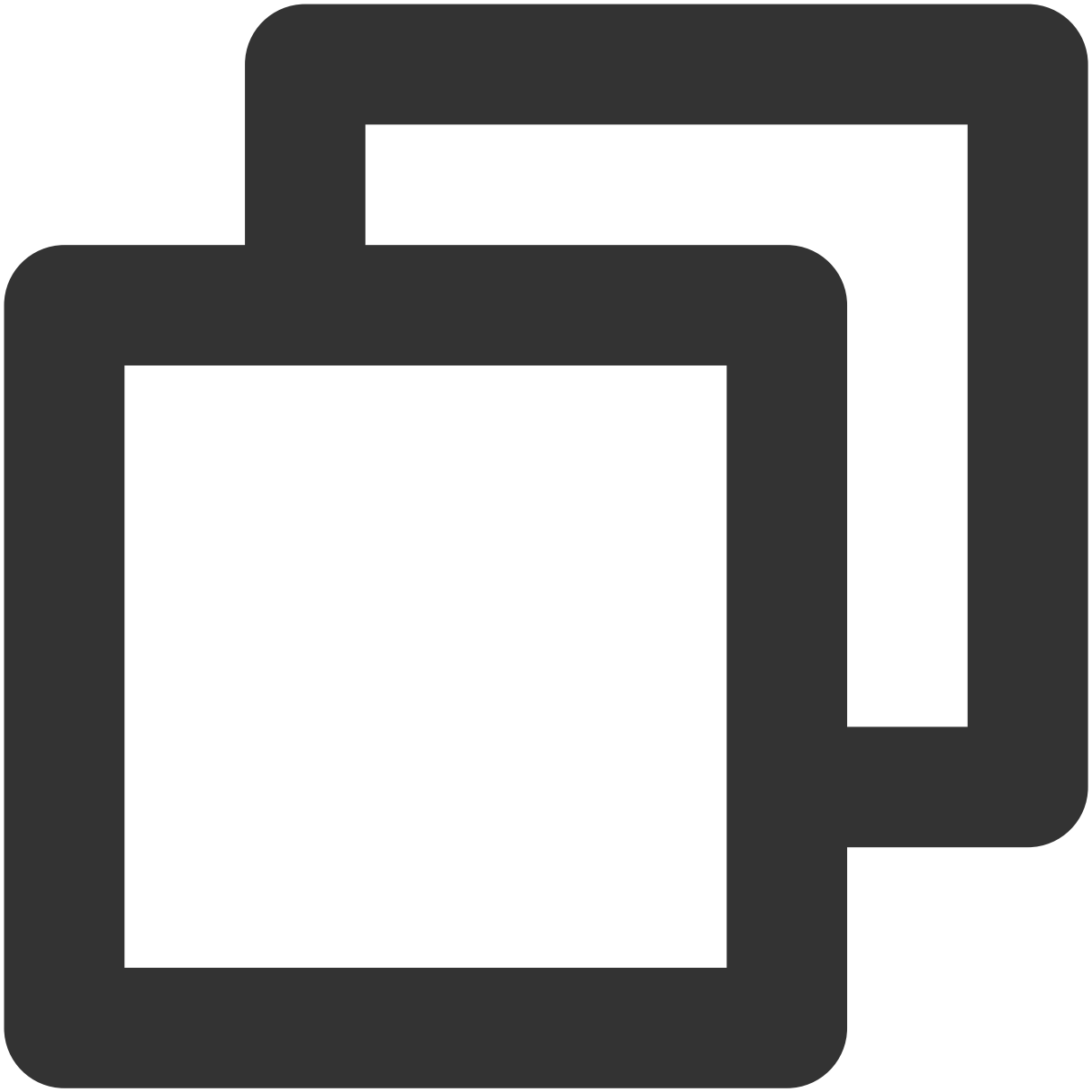
```
access-list INTERESTING extended permit ip 172.XX.XX.0 255.255.0.0 10.1.1.0 255.
```

7. Configure an IPsec policy.



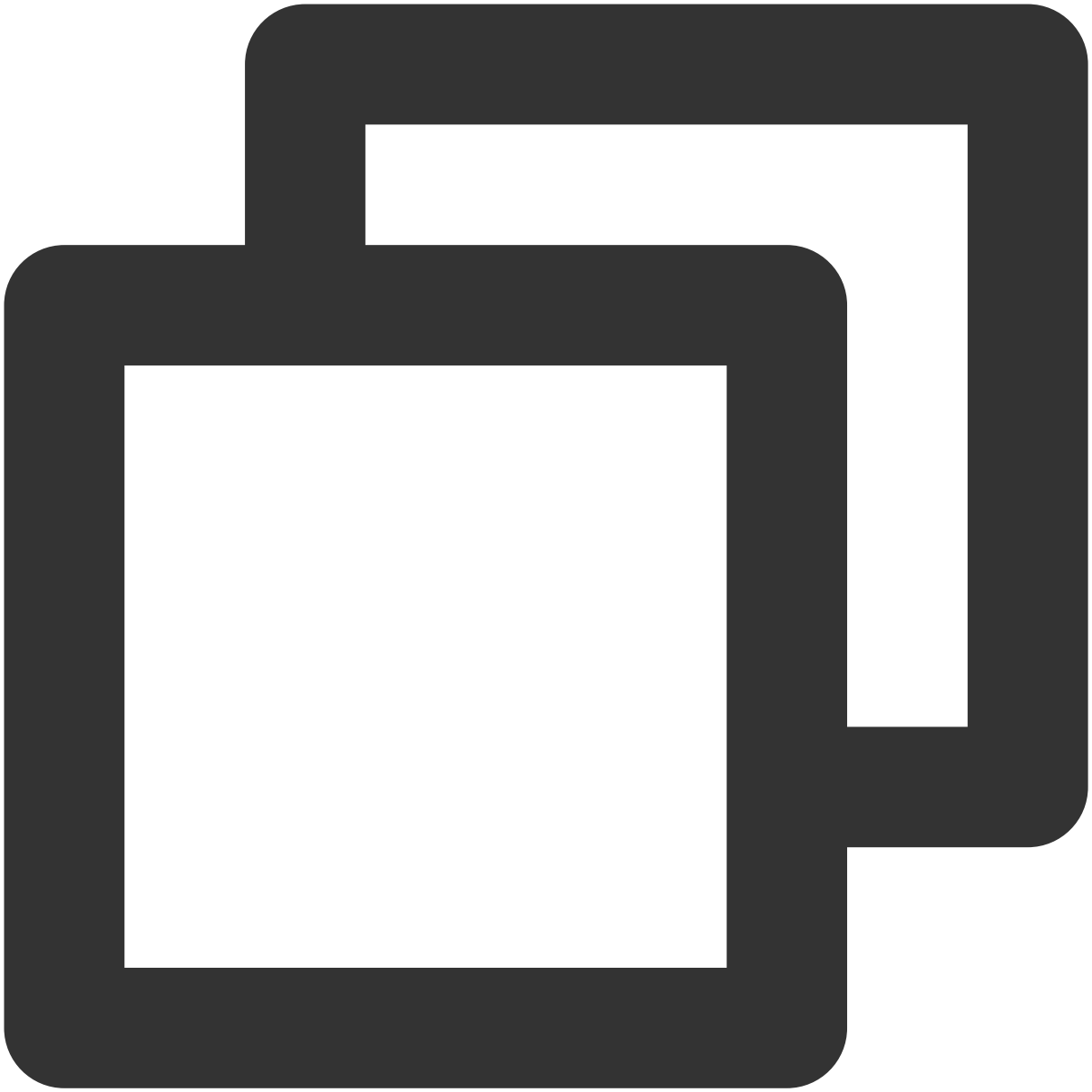
```
crypto map CMAP 1 match address INTERESTING  # Use ACL to allow the packets that
crypto map CMAP 1 set peer 159.XX.XX.242  # Set the public IP address of the des
crypto map CMAP 1 set ikev1 transform-set TS  # Configure an IKEv1 protocol for
crypto map CMAP 1 set security-association lifetime seconds 3600  # Configure a
```

8. Apply the IPsec policy.



```
rypto map CMAP interface outside  # Apply the crypto map configured in the previ
```

9. Configure static routes.

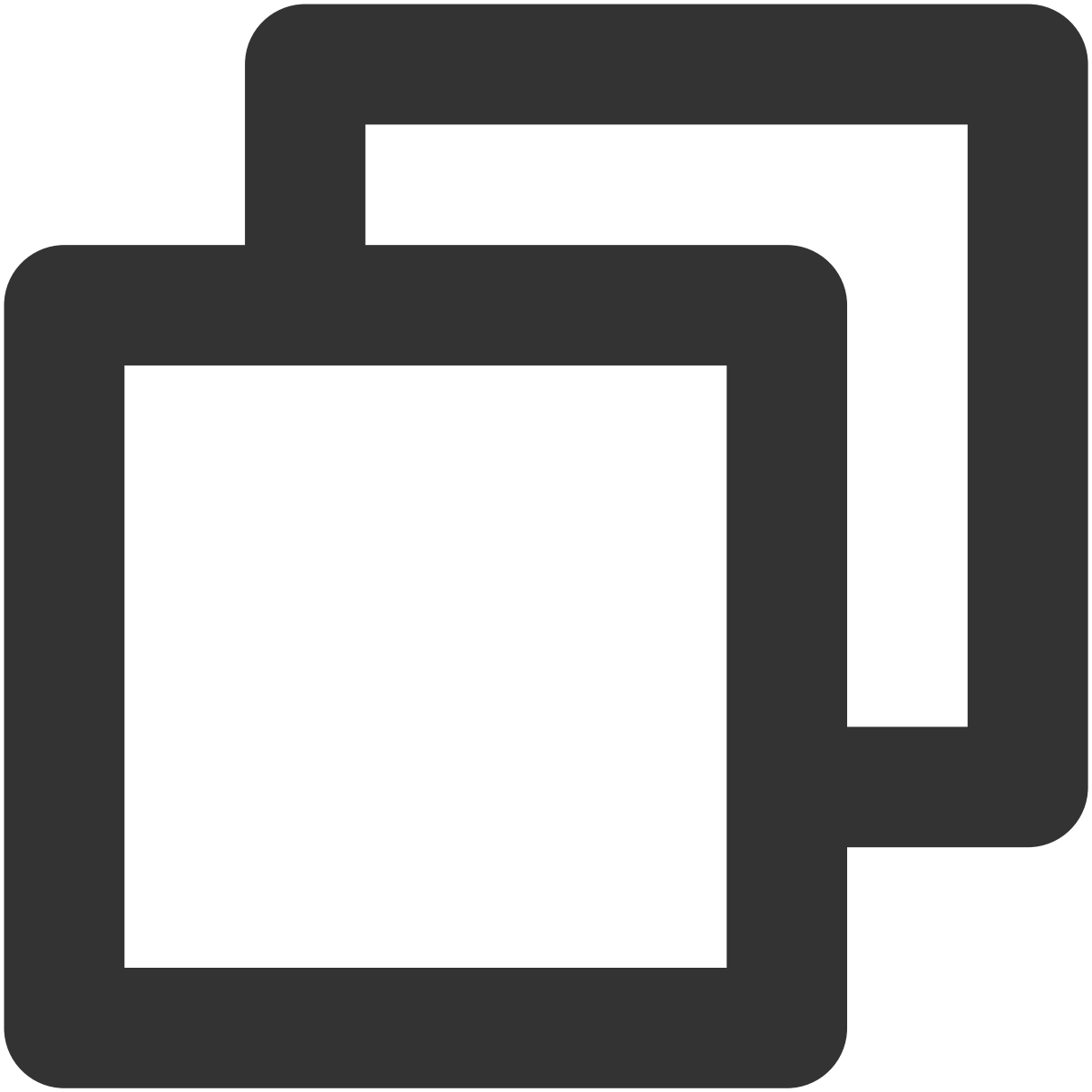


```
route outside 10.1.1.0 255.255.255.0 159.XX.XX.242 1  # Route the data of the IP
```

10. Test the VPN connectivity.

You can use the `ping` command to test the VPN connectivity.

1. Log in to the command-line interface of the firewall device.

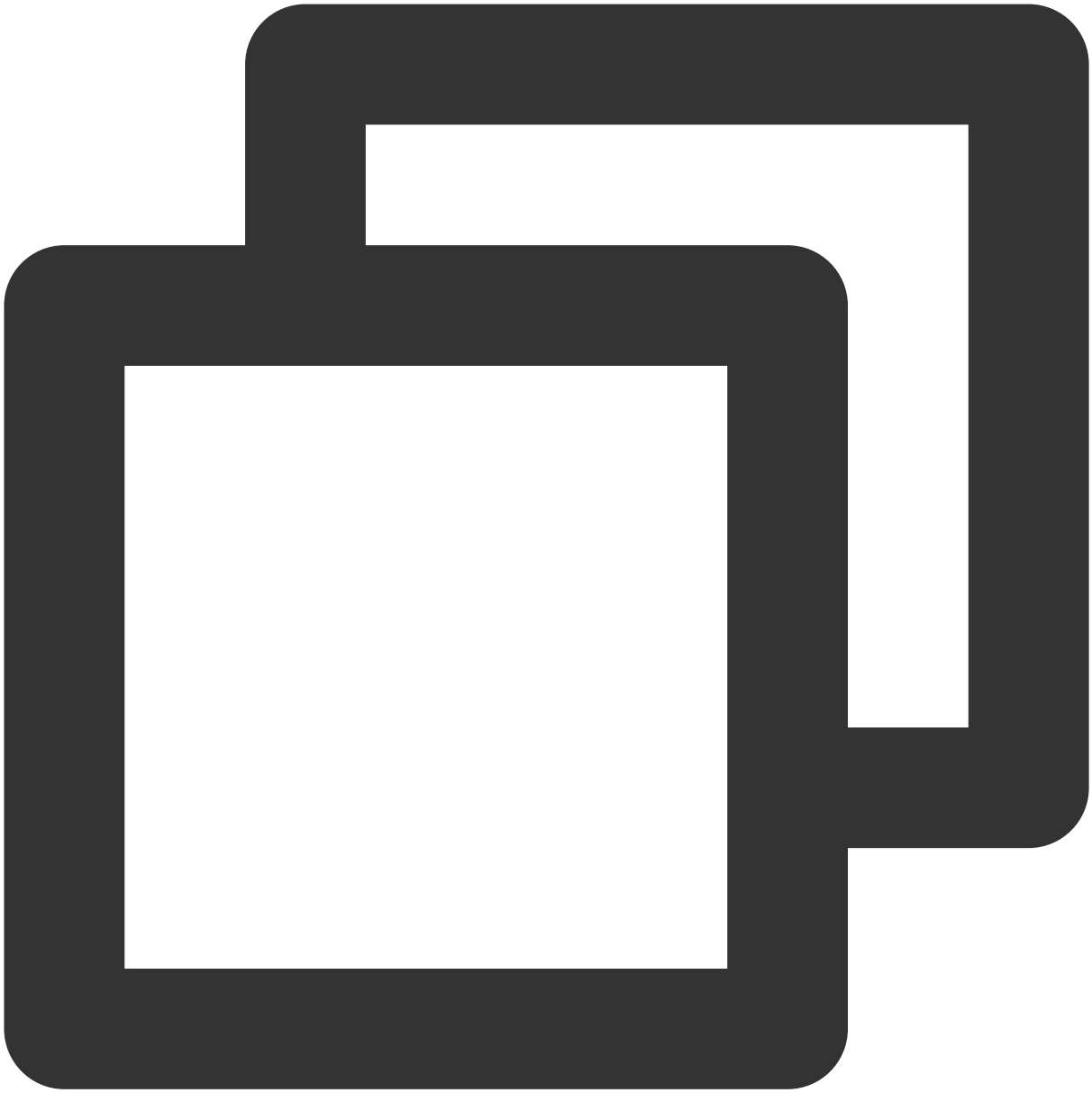


```
   ssh -p admin@10.XX.XX.56

# Use the SSH command to log in to the configuration interface of the firewall.

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

# Enter the username and password to enter the user mode.
```

```
ASA>
ASA> en
Password:

# Input "enable" and its password to enter the privileged EXEC mode in which you ca

ASA# conf t
ASA(config)#

# Input "config ter" to enter the global mode in which you can configure the firewa
```

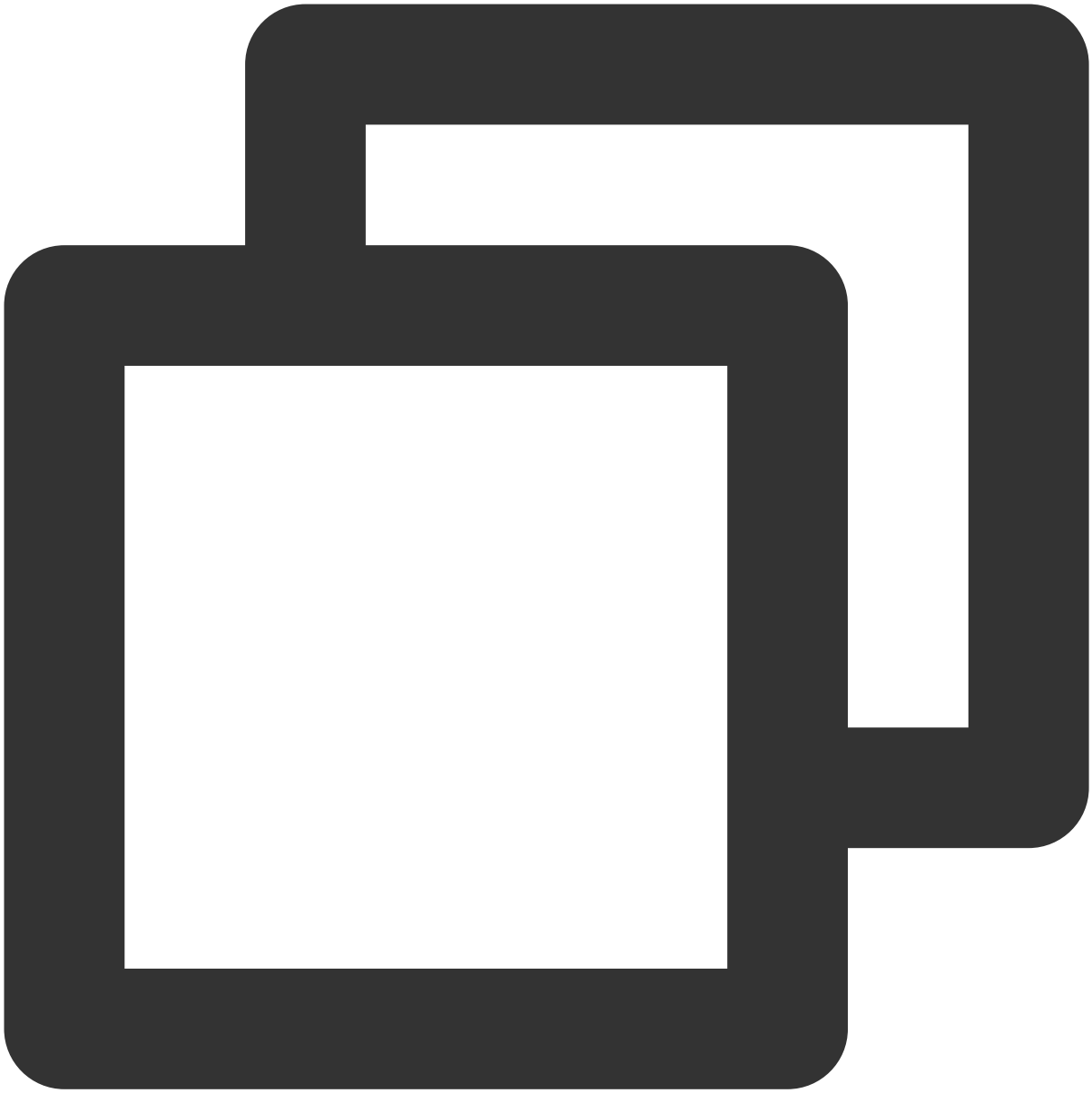
2. Configure the firewall interface.

In the global mode, configure the firewall interface that connects to Tencent Cloud.



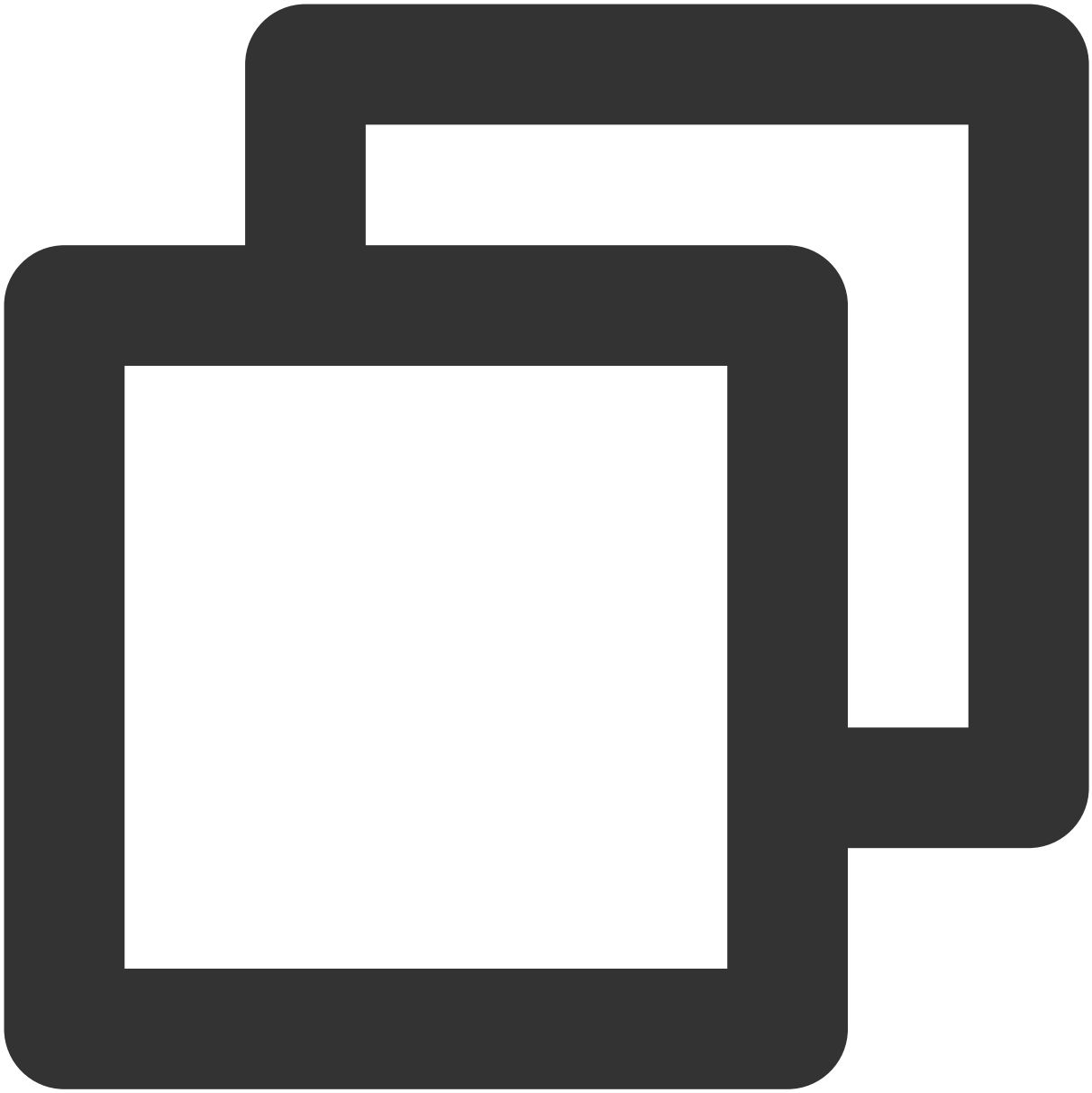
```
interface GigabitEthernet0/0
nameif outside  # Specify the security domain of the interface.
security-level 0  # Specify the security domain level of the interface.
ip address 120.XX.XX.76 255.255.255.252  # Configure the local public IP address
```

3. Configure an ISAKMP policy.



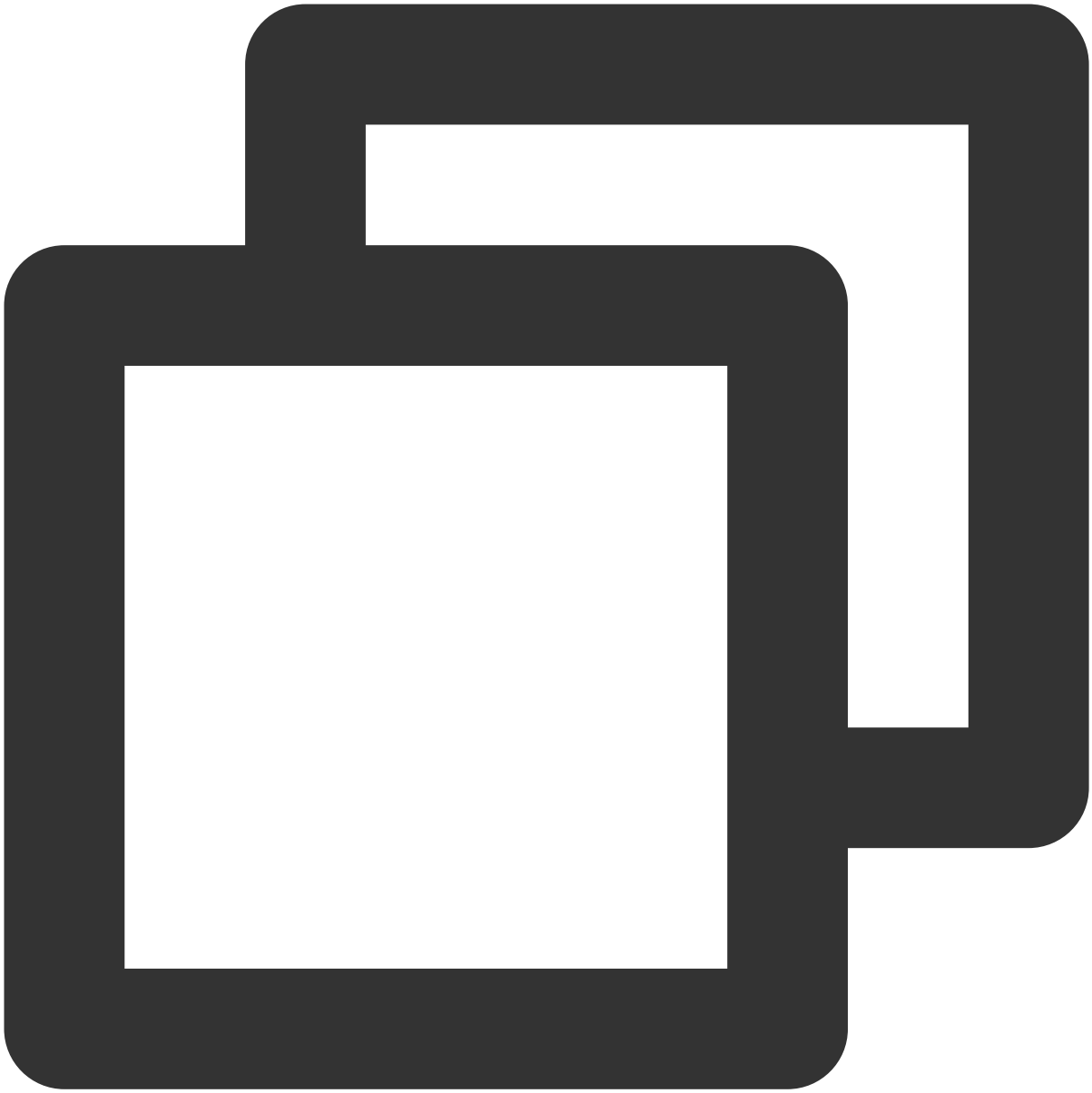
```
crypto ikev1 policy 10  # Define the phase 1 negotiation policy for IKEv1. Ente
authentication pre-share  # Set the authentication method to authentication via
encryption AES-128  # Specify the packet encapsulation encryption algorithm for
hash MD5  # Set the hash algorithm to “MD5” for the IKE policy. It defaults to
group 2  # Use Diffie-Hellman group 2 for the IKE policy. It defaults to "group
lifetime 86400  # Specify the SA lifetime. It defaults to "86400" seconds.
```

4. Configure the pre-shared key.



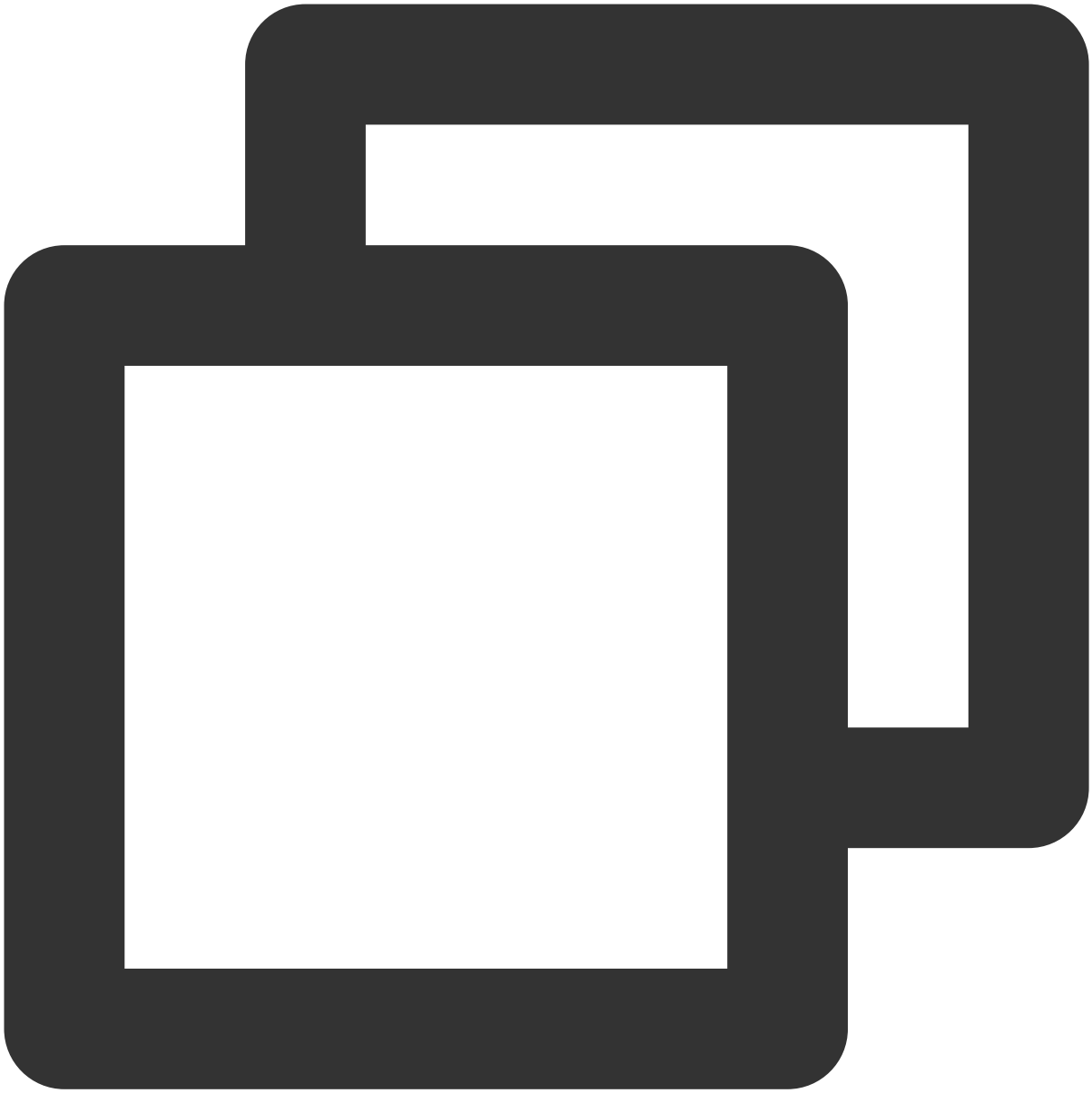
```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # Create a point-to-point IPsec tunne
tunnel-group 159.XX.XX.242 ipsec-attributes  # Configure the tunnel group attrib
 ikev1 pre-shared-key tencent@123  # Enter letters, numbers or strings as the ke
```

5. Configure the IPsec security protocol.



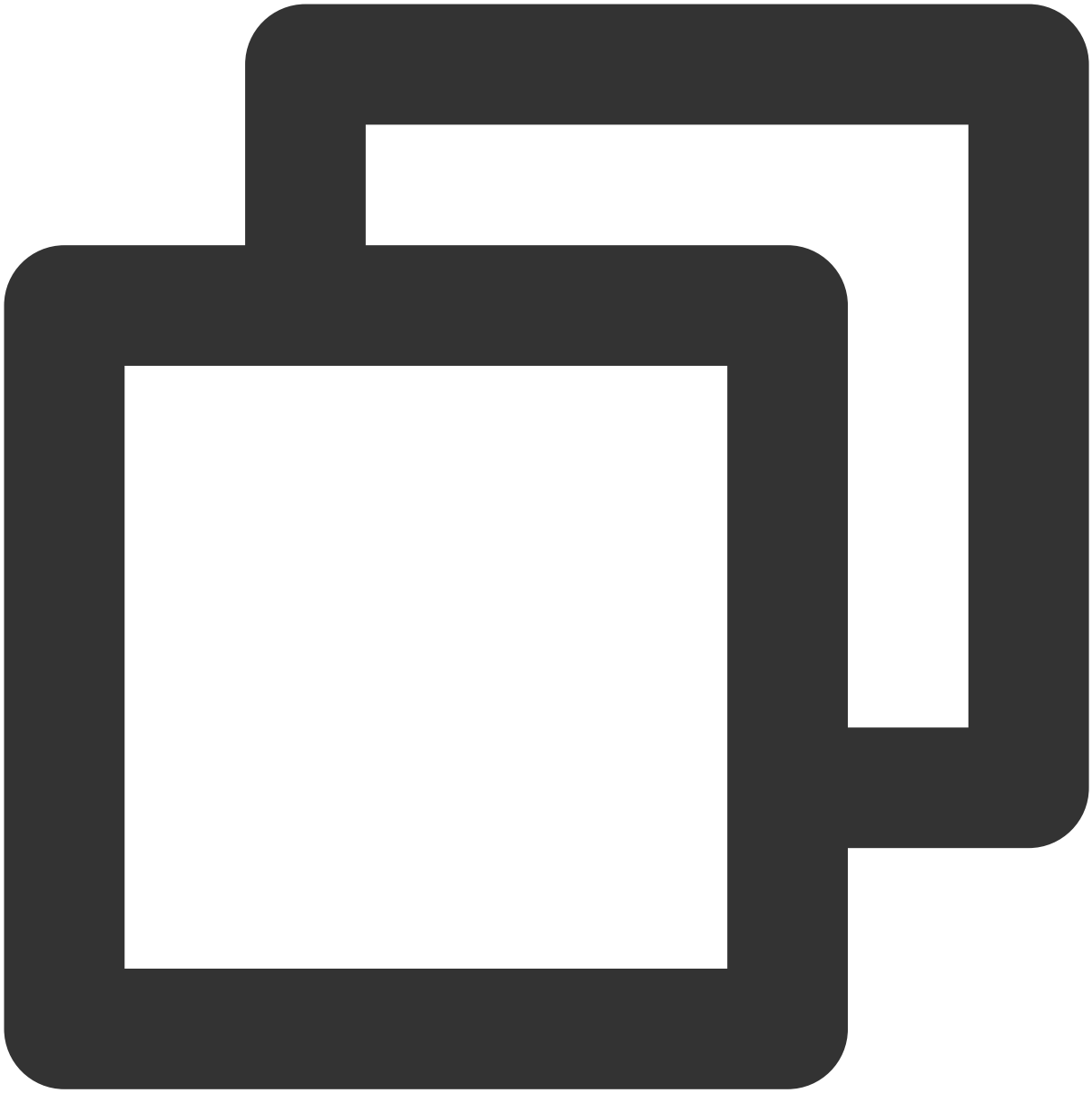
```
    crypto ipsec ikev1 transform-set TS esp-aes esp-md5-hmac  # Specify the encrypti
```

6. Configure an IPsec policy.



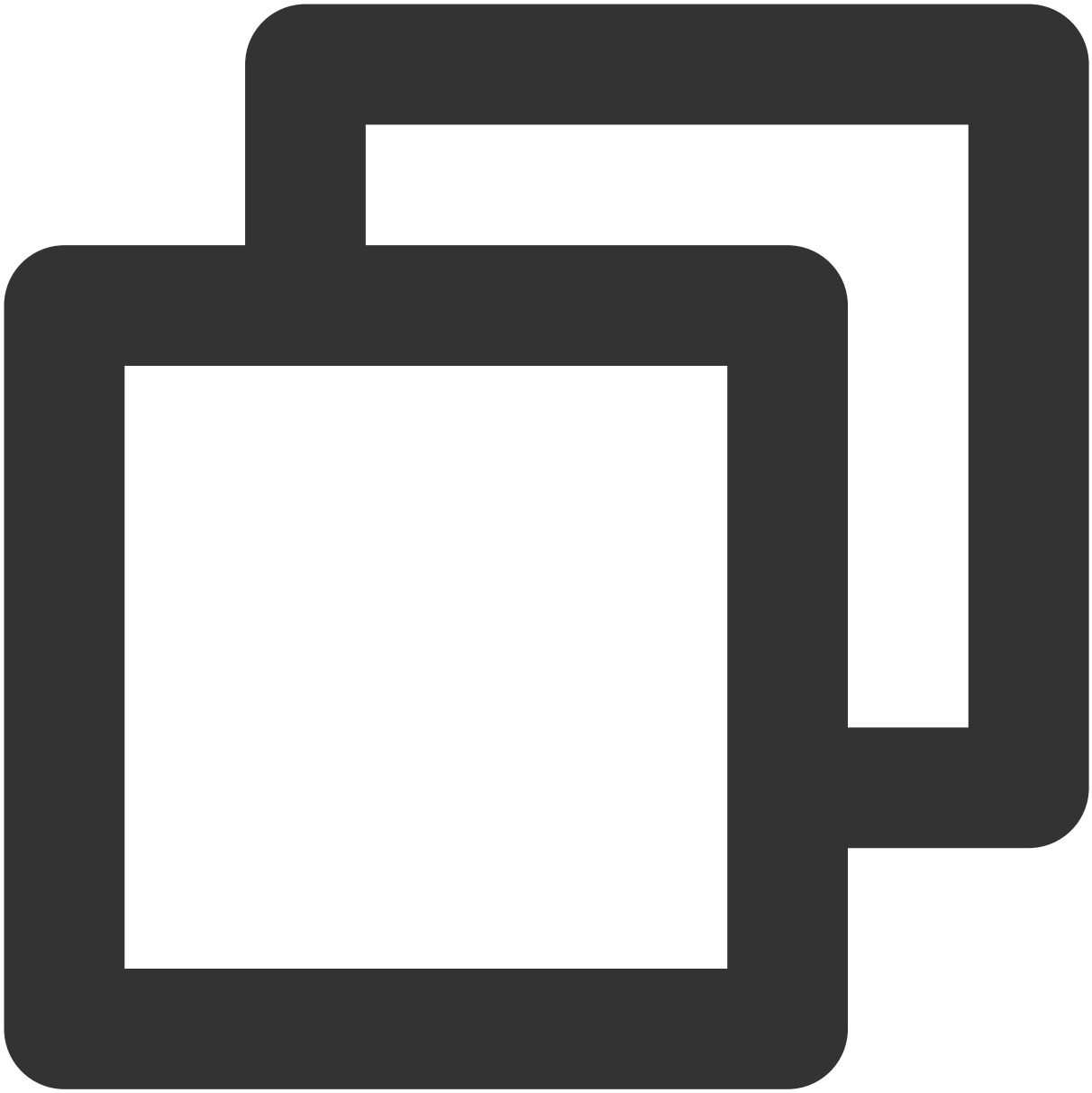
```
crypto ipsec profile PROFILE1
set ikev1 transform-set TS  # Specify an IKEv1 IPSec proposal policy for the cry
set security-association lifetime kilobytes 1843200  # Specify the data stream i
set security-association lifetime seconds 3600  # Set the SA lifetime. The defau
```

7. Apply the IPsec policy.



```
interface Tunnel100
tunnel source interface outside  # Configure the source VPN that comes from the
tunnel destination 159.XX.XX.242  # Configure the public IP address of the desti
tunnel mode ipsec ipv4  # Configure the protocol for the tunnel interface.
tunnel protection ipsec profile PROFILE1  # Use the IPsec policy to protect data
```

8. Configure static routes.

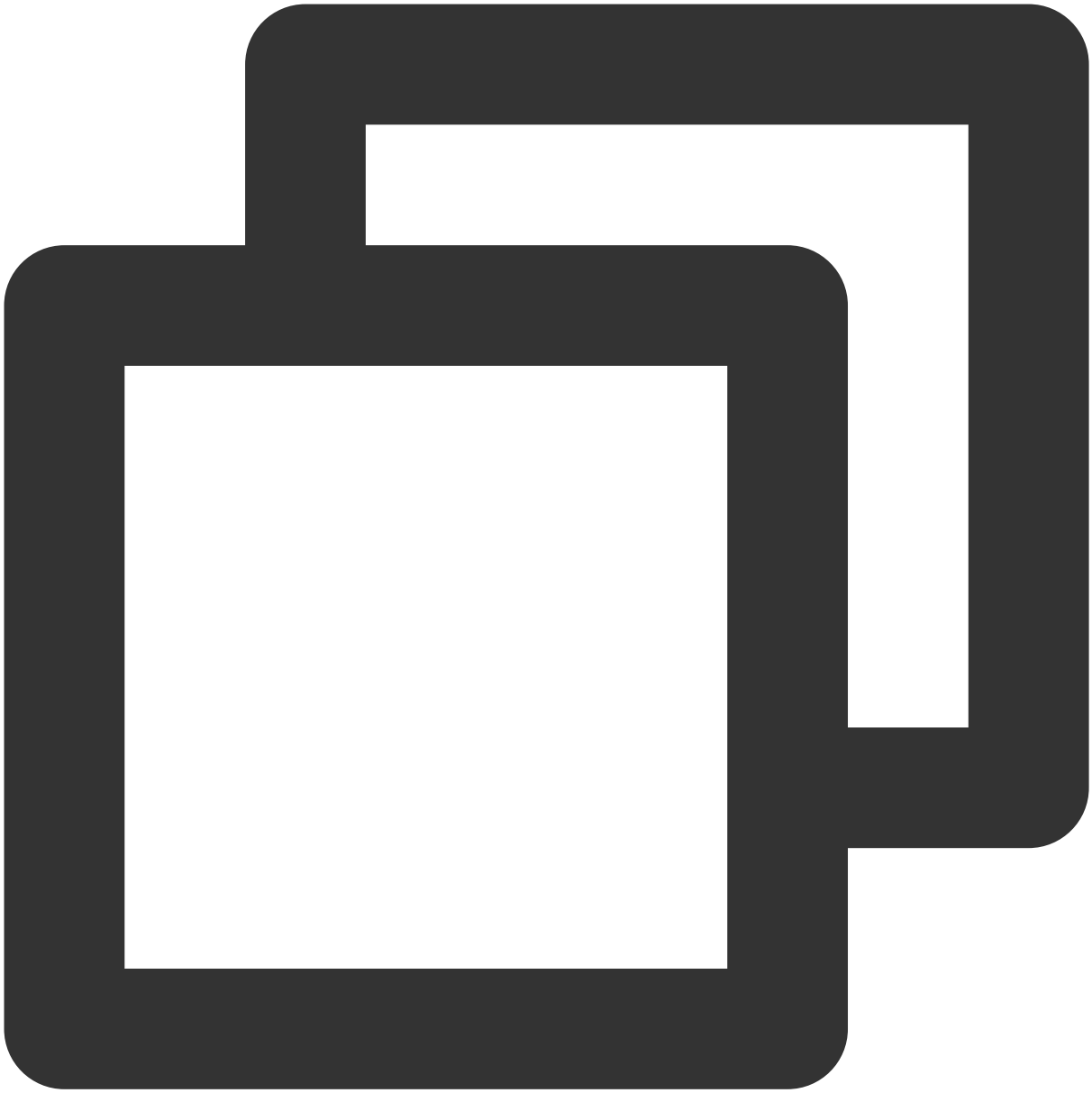


```
route vti 10.1.1.0 255.255.255.0 159.XX.XX.242   # Route the packets to be encry
```

9. Test the VPN connectivity.

You can use the `ping` command to test the VPN connectivity.

1. Log in to the command-line interface of the firewall device.

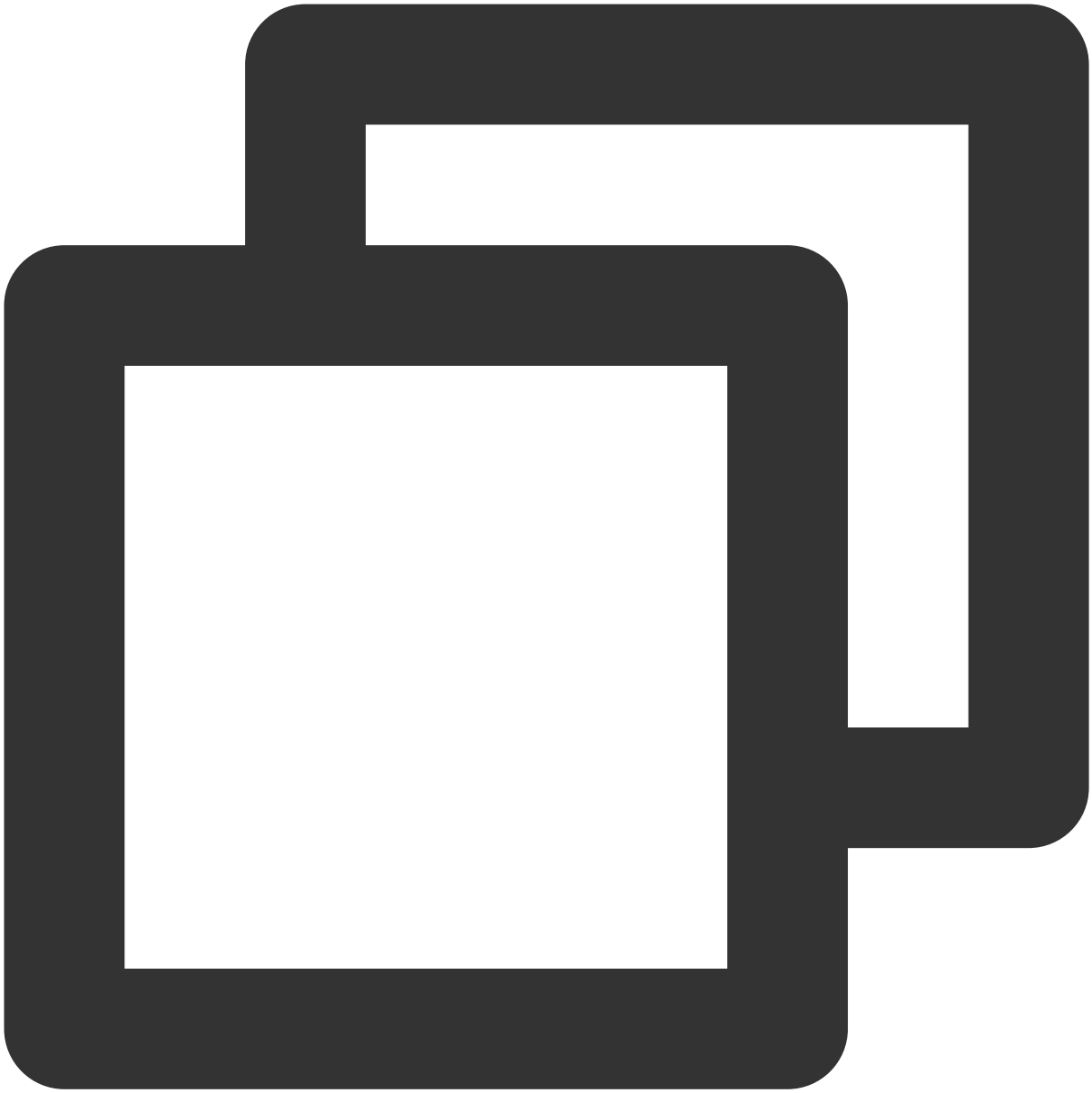


```
   ssh -p admin@10.XX.XX.56

# Use the SSH command to log in to the configuration interface of the firewall.

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

# Enter the username and password to enter the user mode.
```

```
ASA>
ASA> en
Password:

# Input "enable" and its password to enter the privileged EXEC mode in which you ca

ASA# conf t
ASA(config)#

# Input "config ter" to enter the global mode in which you can configure the firewa
```

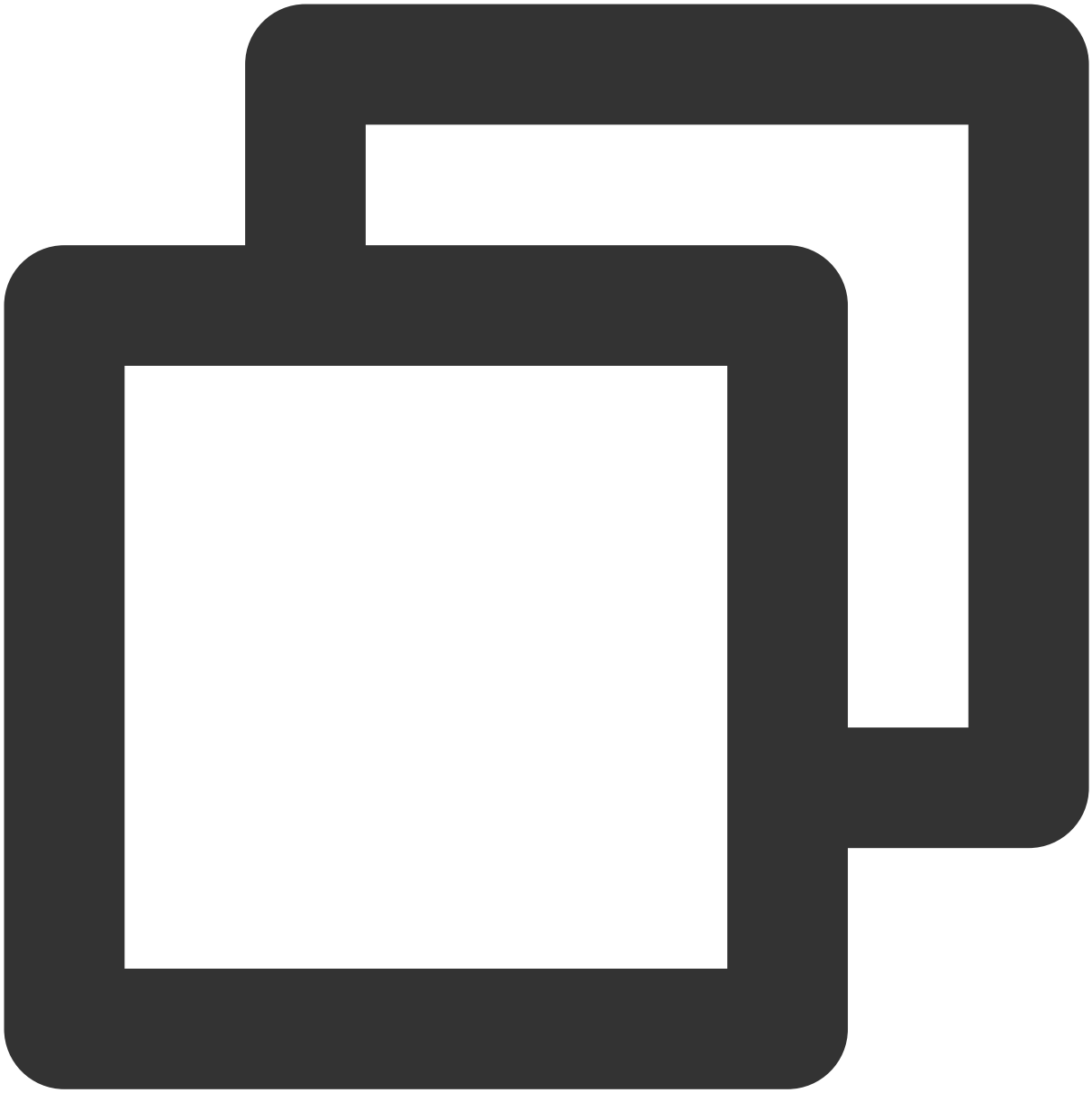
2. Configure the firewall interface.

In the global mode, configure the firewall interface that connects to Tencent Cloud.



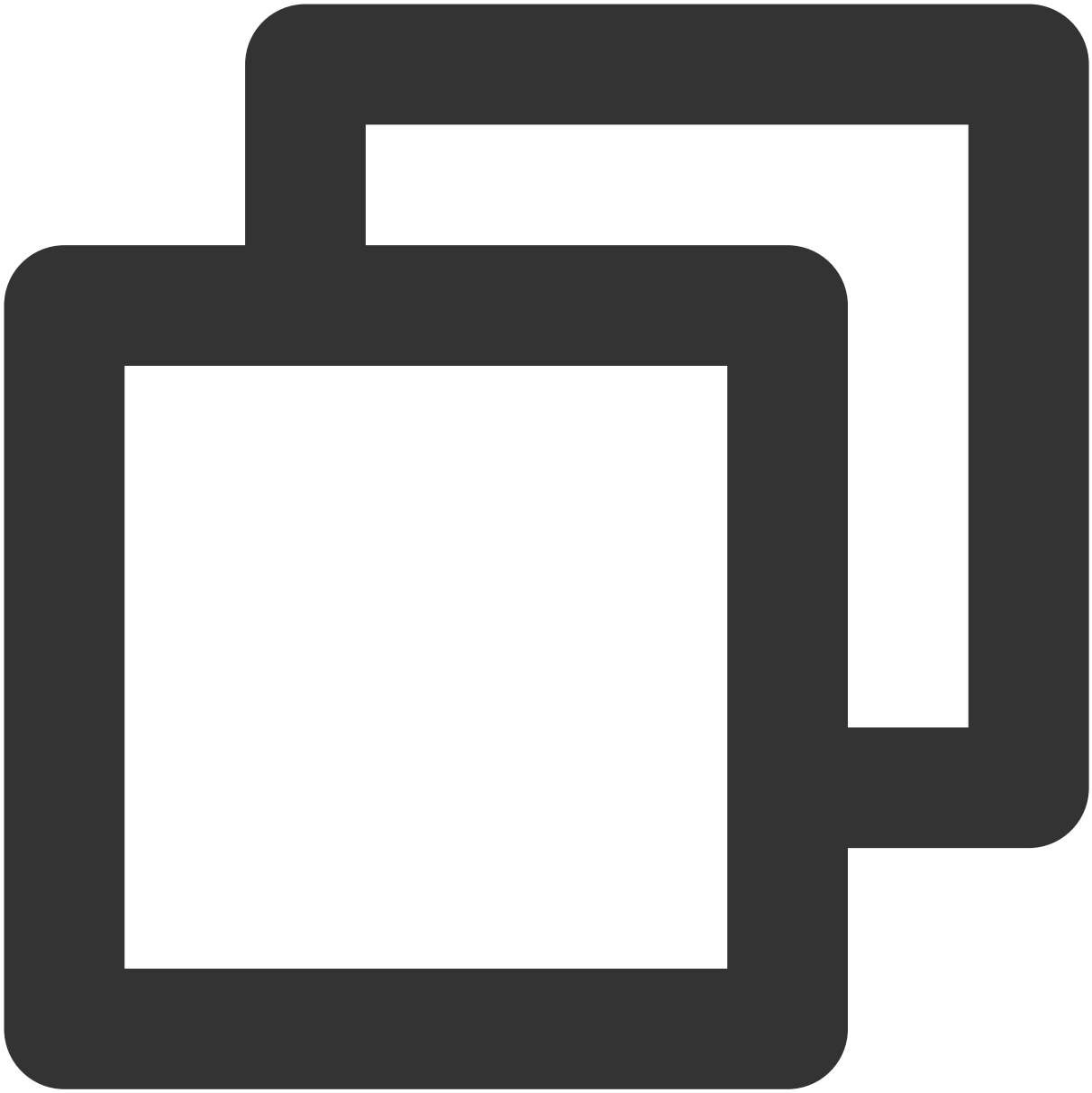
```
interface GigabitEthernet0/0
nameif outside  # Specify the security domain of the interface.
security-level 0  # Specify the security domain level of the interface.
ip address 120.XX.XX.76 255.255.255.252  # Configure the local public IP address
```

3. Configure an ISAKMP policy.



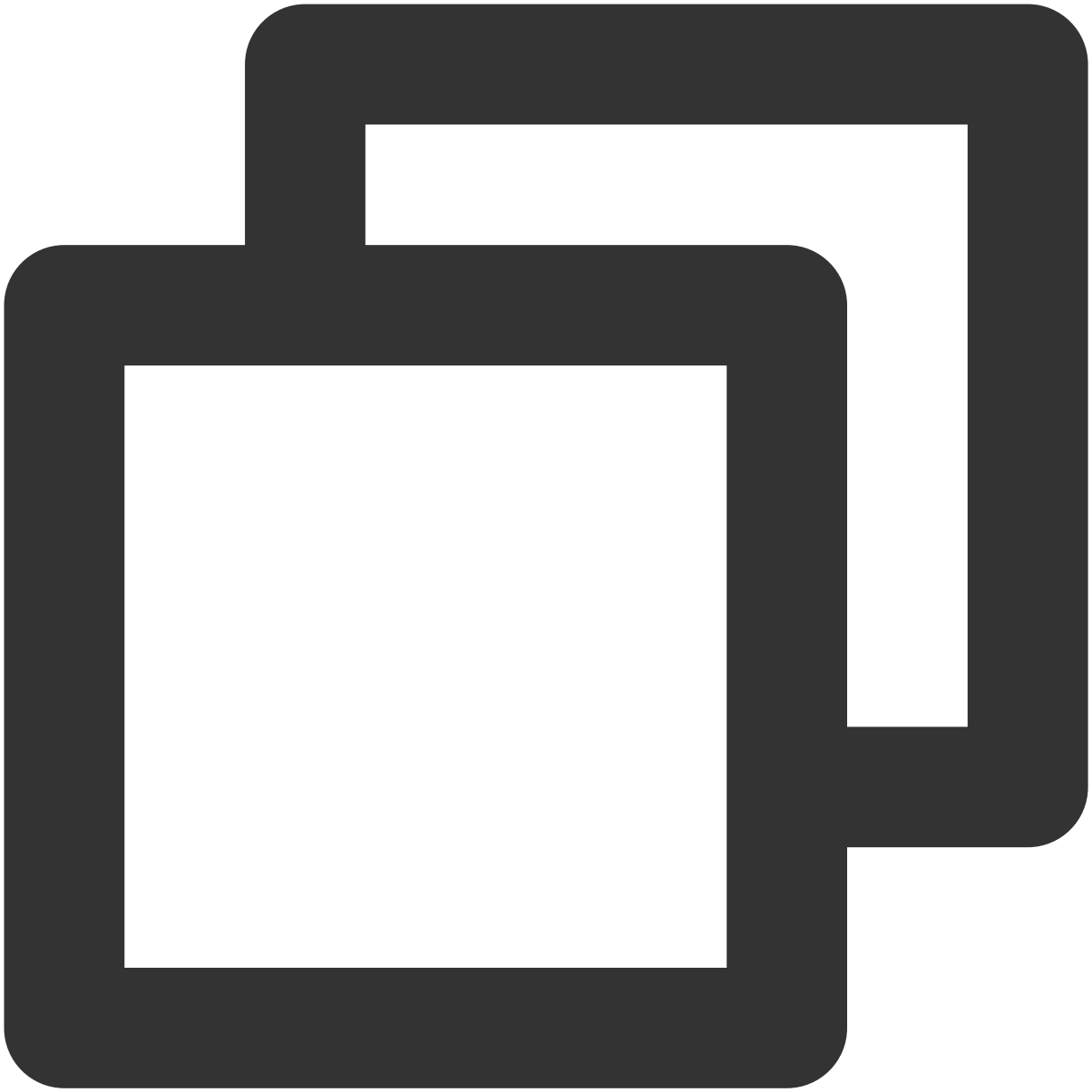
```
crypto ikev2 enable outside  # Enable IKEv2 on the "outside" interface.
crypto ikev1 policy 10  # Define the phase 1 negotiation policy for IKEv2. Enter
authentication pre-share  # Set the authentication method to authentication via
encryption AES-128  # Specify the packet encapsulation encryption algorithm for
integrity MD5  #   # Set the hash  algorithm to “MD5” for the IKE policy. It def
group 2  # Use Diffie-Hellman group 2 for the IKE policy. It defaults to "group
prf sha # Set the encryption algorithm.
lifetime seconds 86400  # Set the SA lifetime. It defaults to 86400s.
```

4. Configure a group policy.



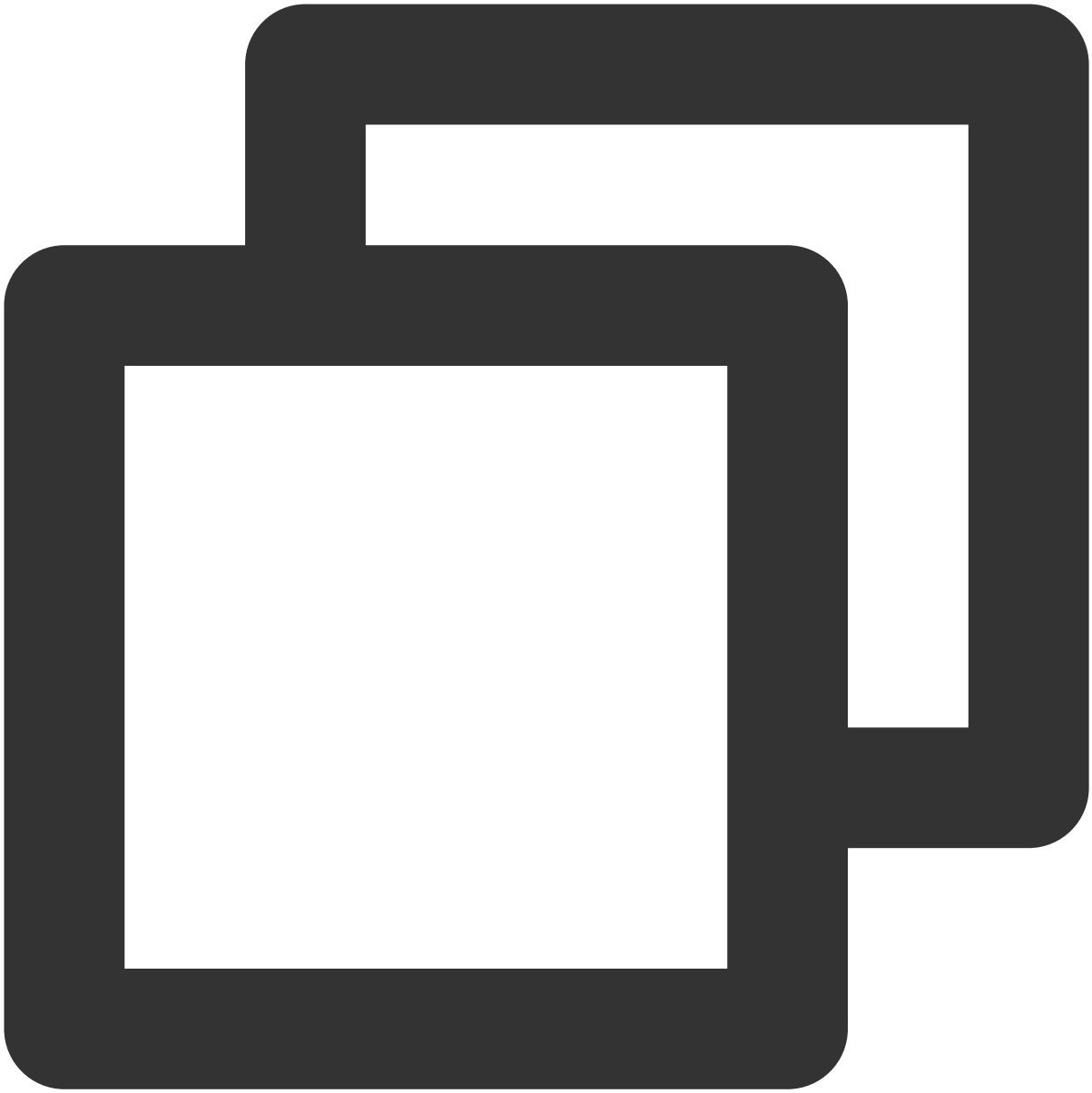
```
group-policy group_policy internal  # Set a group policy for devices.
group-policy group_policy attributes  # Set the group policy attributes.
vpn-tunnel-protocol ikev2 # Set IKEv2 protocol for vpn-tunnel.
```

5. Configure the pre-shared key.



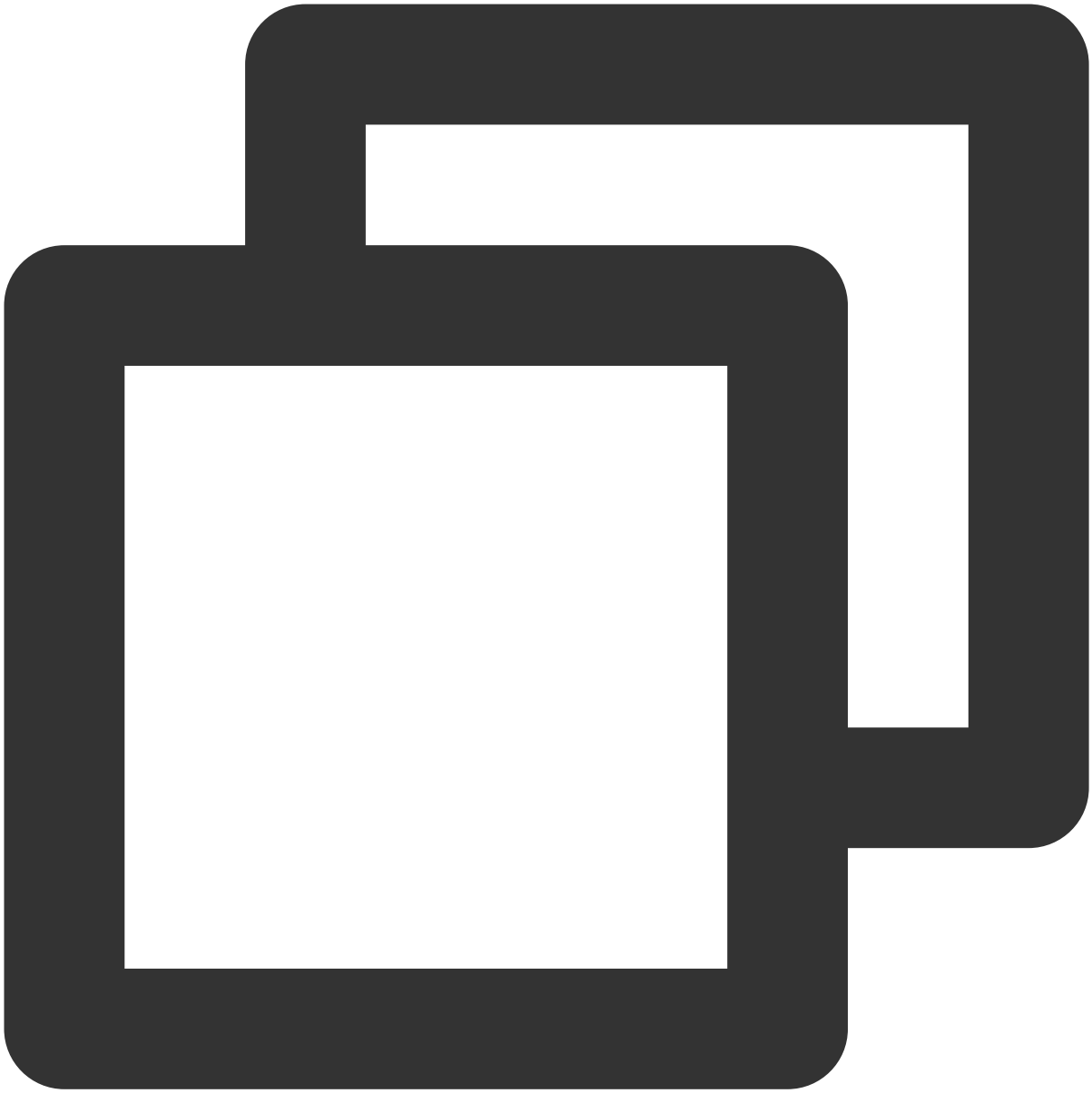
```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # Create a point-to-point IPsec tunne
tunnel-group 159.XX.XX.242 general-attributes default-group-policy group_policy
tunnel-group 159.XX.XX.242 ipsec-attributes  # Configure the tunnel group attrib
ikev2 remote-authentication pre-shared-key tencent@123
ikev2 local-authentication pre-shared-key tencent@123 # Enter letters, numbers o
```

6. Specify the IPsec protocol.



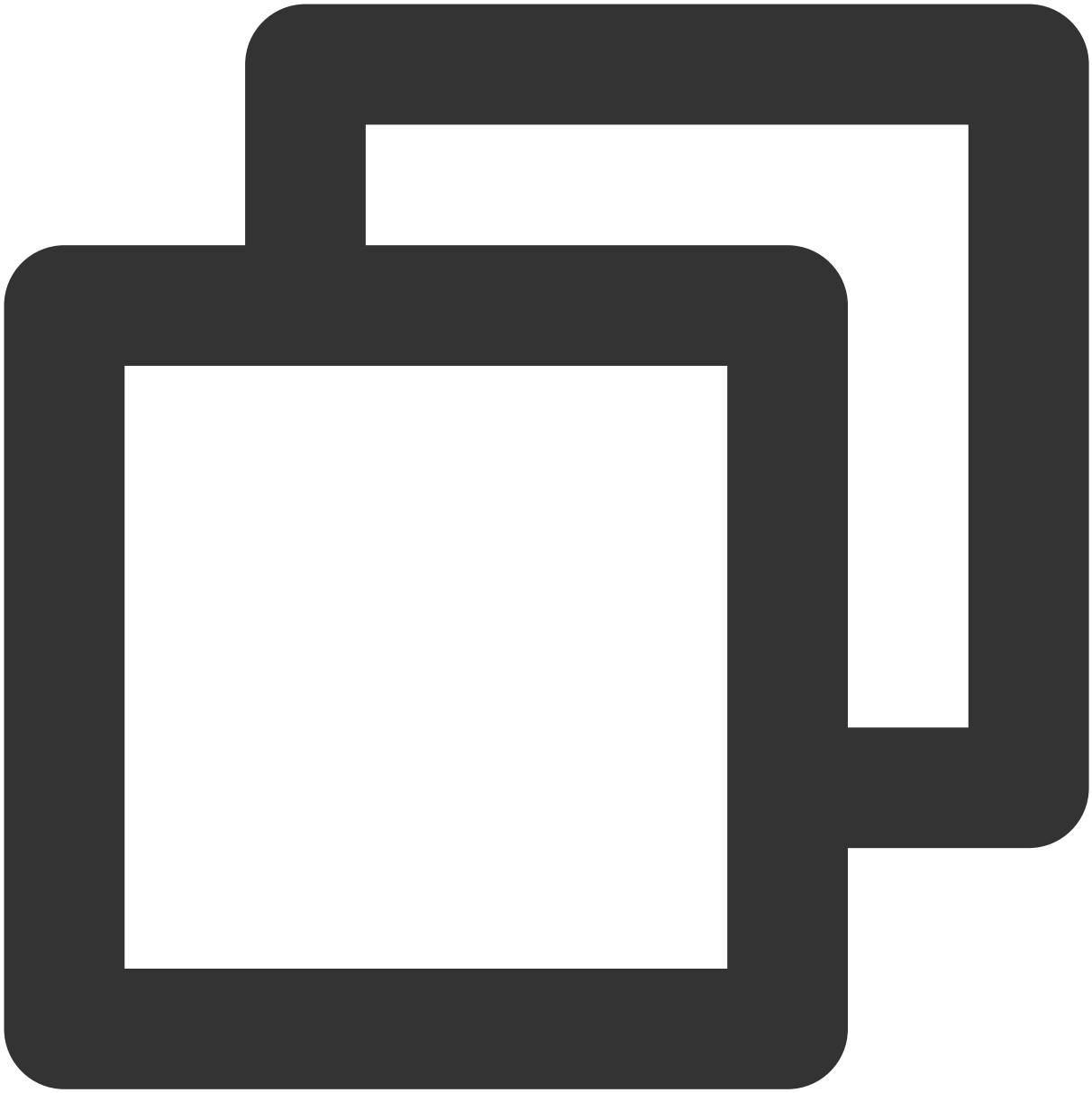
```
crypto ipsec ikev2 ipsec-proposal ikev2_proposal  # Specify the encryption algor
protocol esp encryption aes-128  # Configure an encryption algorithm.
protocol esp integrity sha-1 # Configure an integrity checking algorithm.
```

7. Configure ACL.



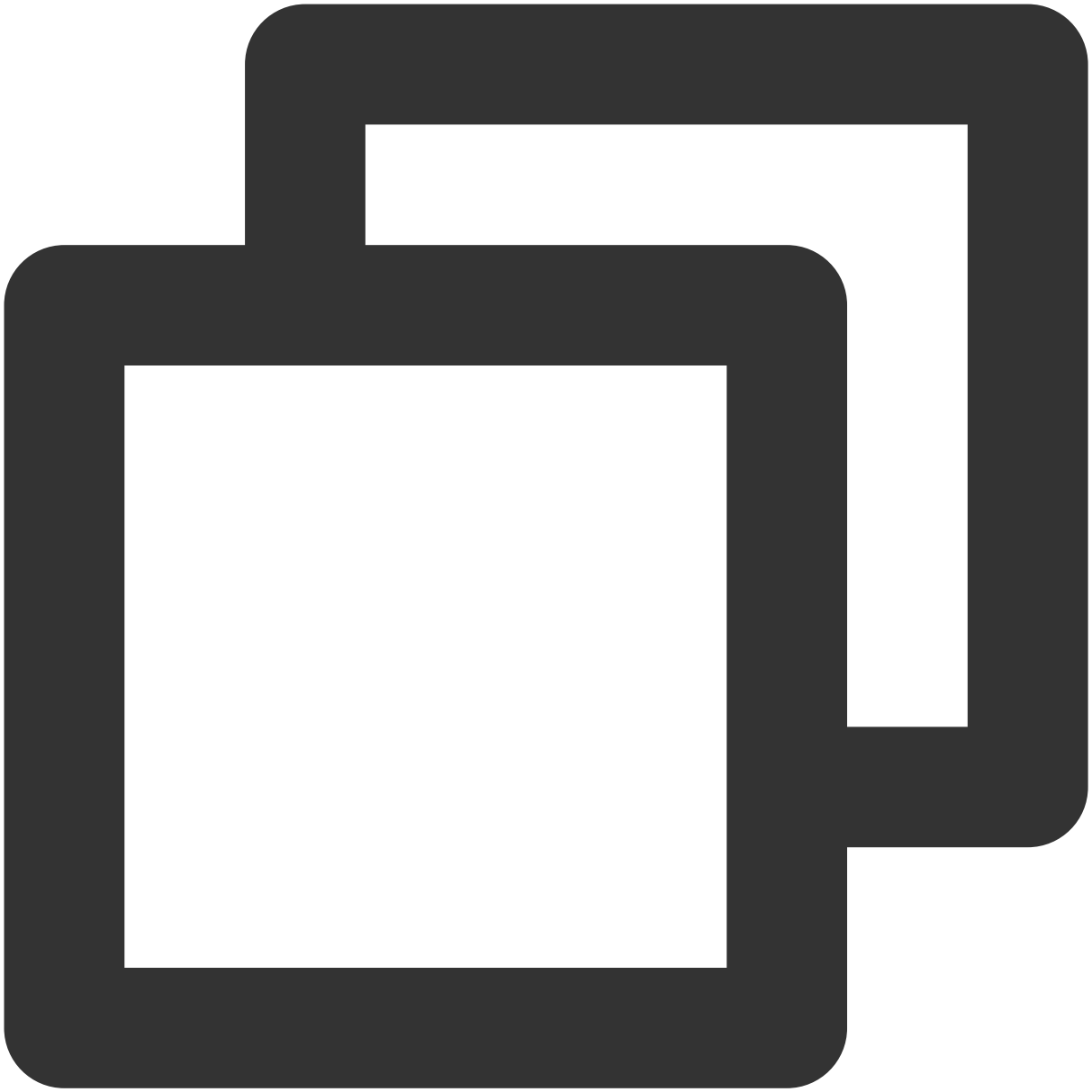
```
access-list INTERESTING extended permit ip 172.XX.XX.0 255.255.0.0 10.1.1.0 255.
```

8. Configure an IPsec policy.



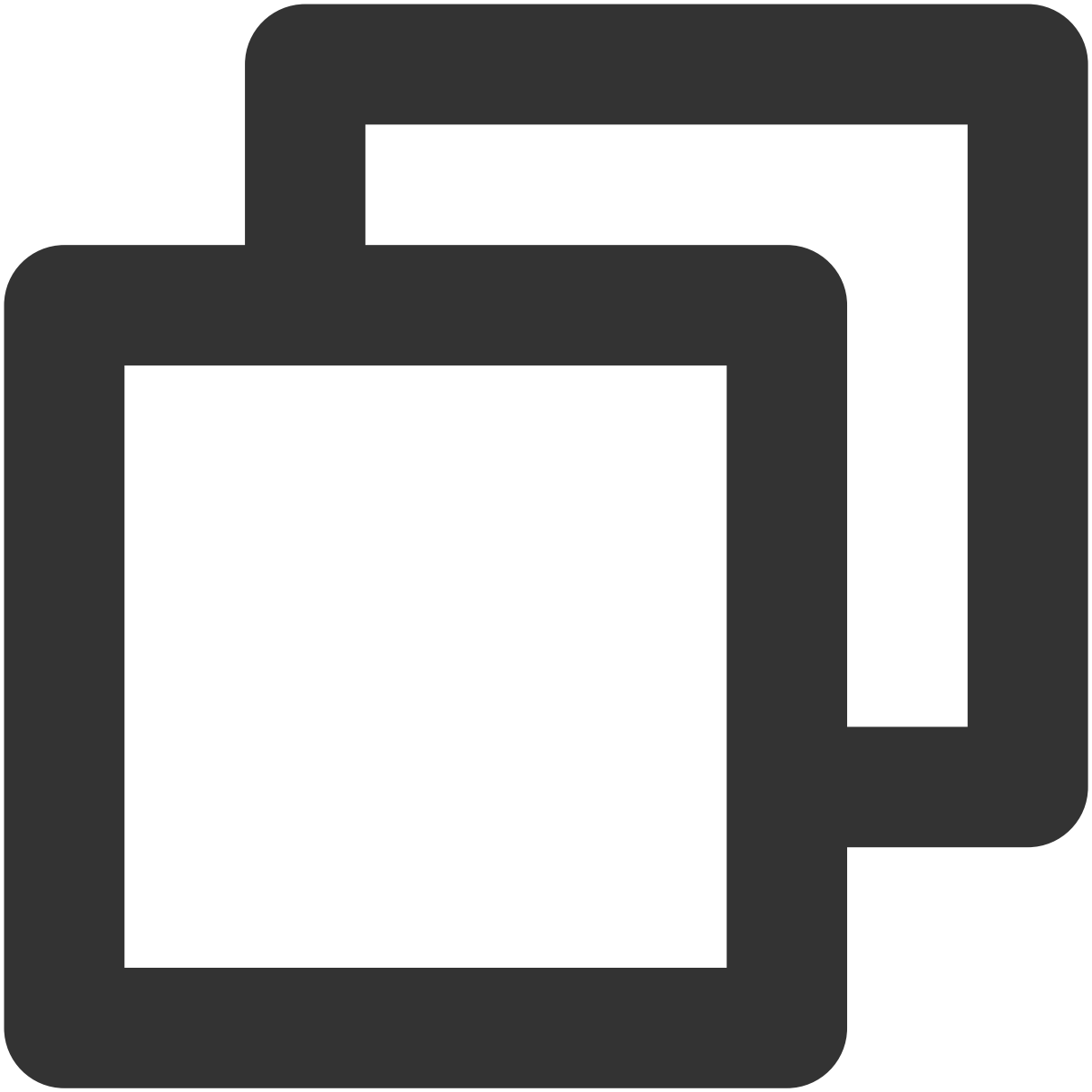
```
crypto map CMAP 1 match address INTERESTING  # Use ACL to allow the packets that
crypto map CMAP 1 set peer 159.XX.XX.242  # Set the public IP address of the des
crypto map CMAP 1 set ikev2 ipsec-proposal ikev2_proposal # Configure an IKEv2 p
crypto map CMAP 1 set security-association lifetime seconds 3600 # Configure a S
crypto map CMAP 1 set security-association lifetime kilobytes 1843200  # Specify
```

9. Apply the IPsec policy.



```
    rypto map CMAP interface outside  # Apply the crypto map configured in the previ
```

10. Configure static routes.

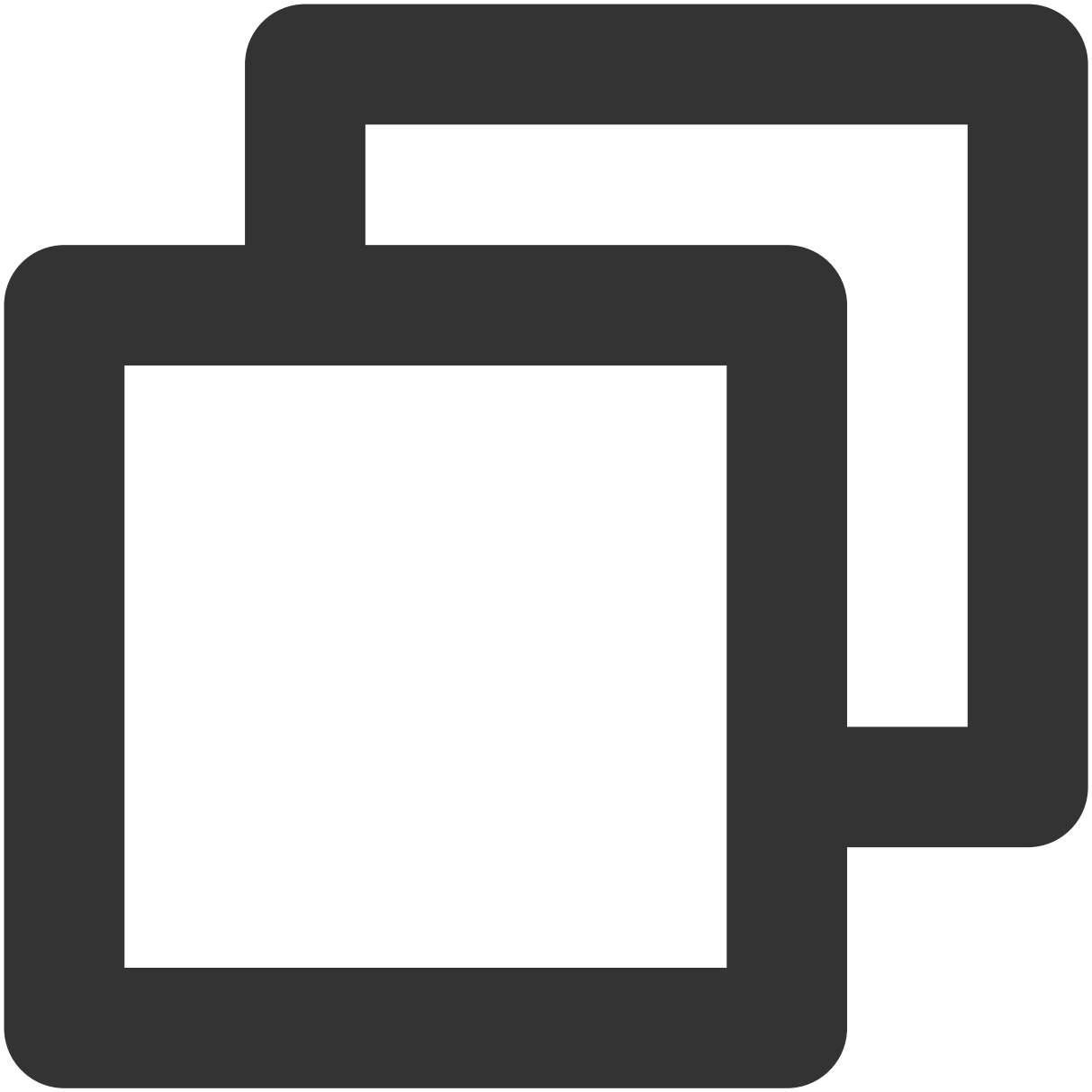


```
route outside 10.1.1.0 255.255.255.0 159.XX.XX.242 1  # Route the data of the I
```

11. Test the VPN connectivity.

You can use the `ping` command to test the VPN connectivity.

1. Log in to the command-line interface of the firewall device.

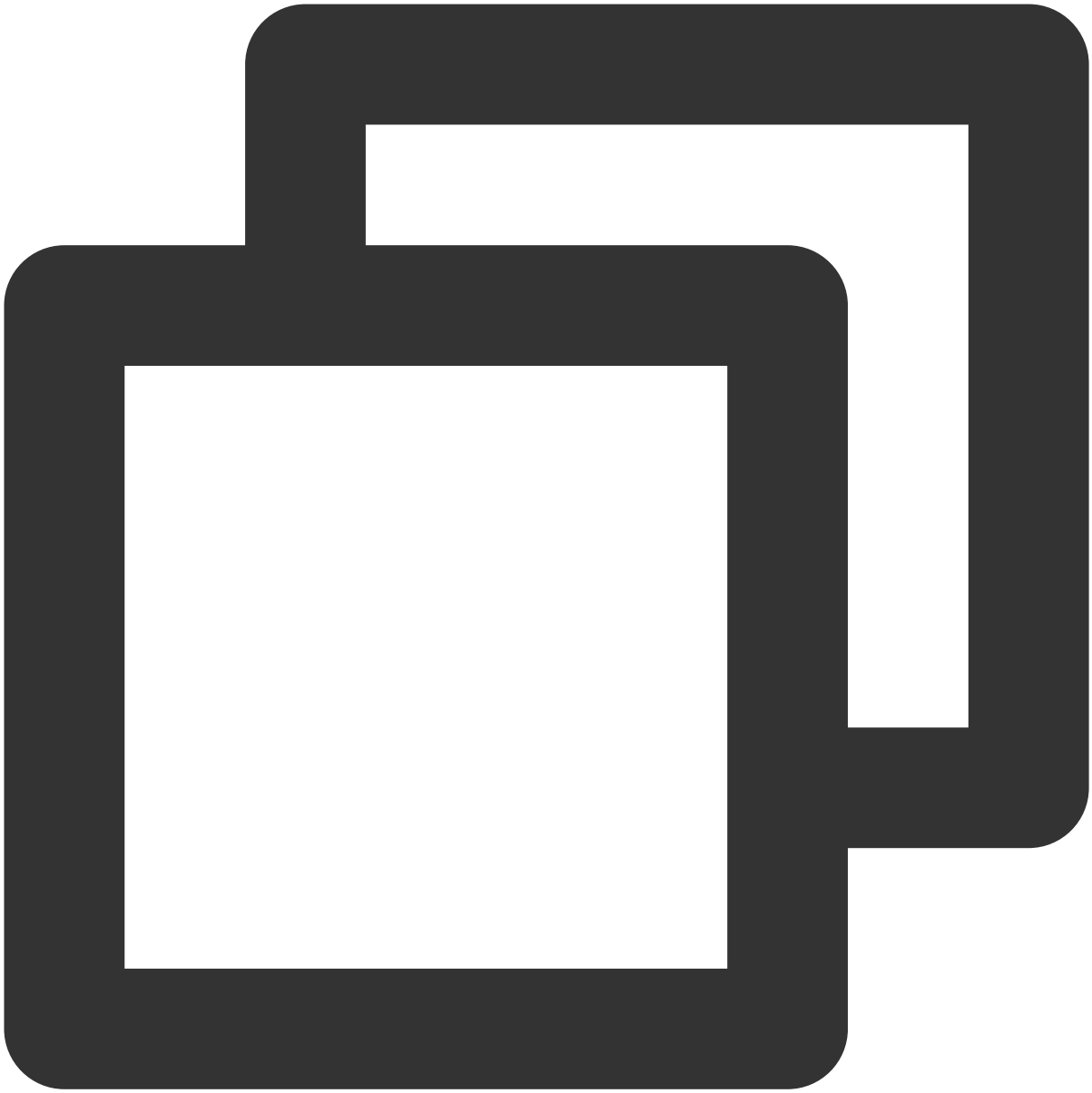


```
   ssh -p admin@10.XX.XX.56

# Use the SSH command to log in to the configuration interface of the firewall.

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

# Enter the username and password to enter the user mode.
```

```
ASA>
ASA> en
Password:

# Input "enable" and its password to enter the privileged EXEC mode in which you ca

ASA# conf t
ASA(config)#

# Input "config ter" to enter the global mode in which you can configure the firewa
```

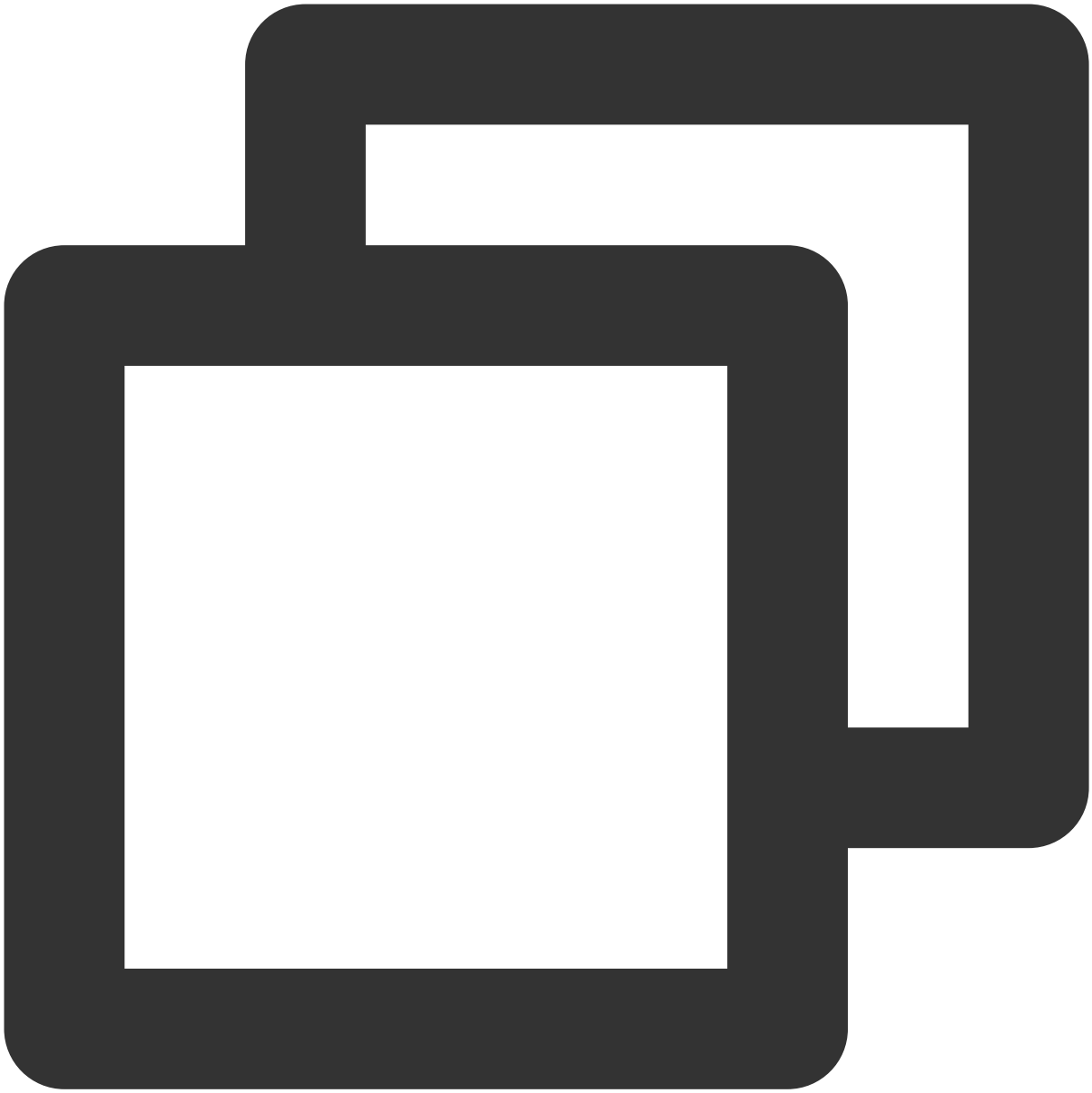
2. Configure the firewall interface.

In the global mode, configure the firewall interface and tunnel interface used to connect Tencent Cloud.



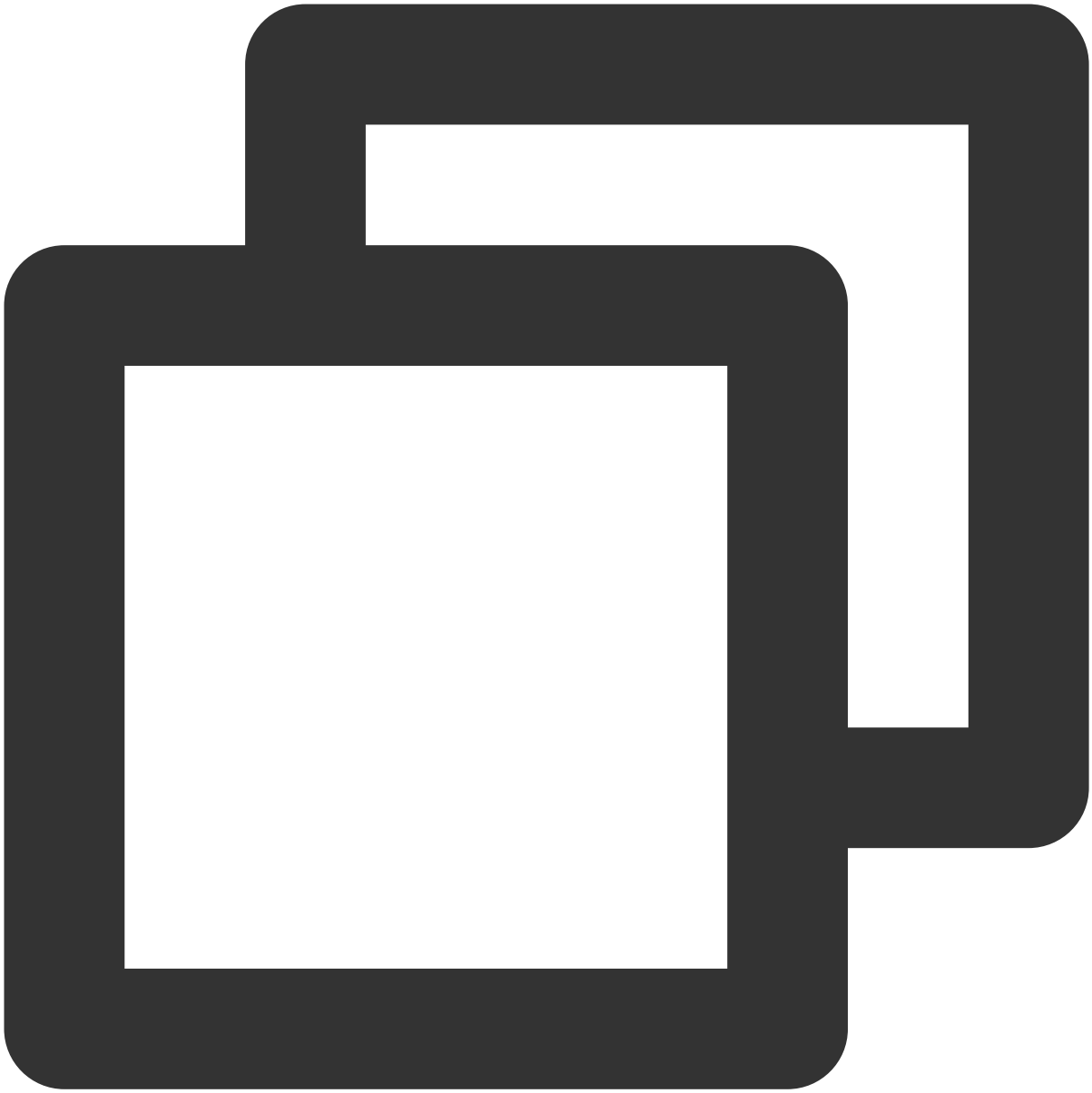
```
interface GigabitEthernet0/0
nameif outside  # Specify the security domain of the interface.
security-level 0  # Specify the security domain level of the interface.
ip address 120.XX.XX.76 255.255.255.252  # Configure the public IP address of th
interface Tunnel100
nameif vti
ip address 172.XX.XX.2 255.255.255.0 # Set an IP address to activate the tunnel
```

3. Configure an ISAKMP policy.



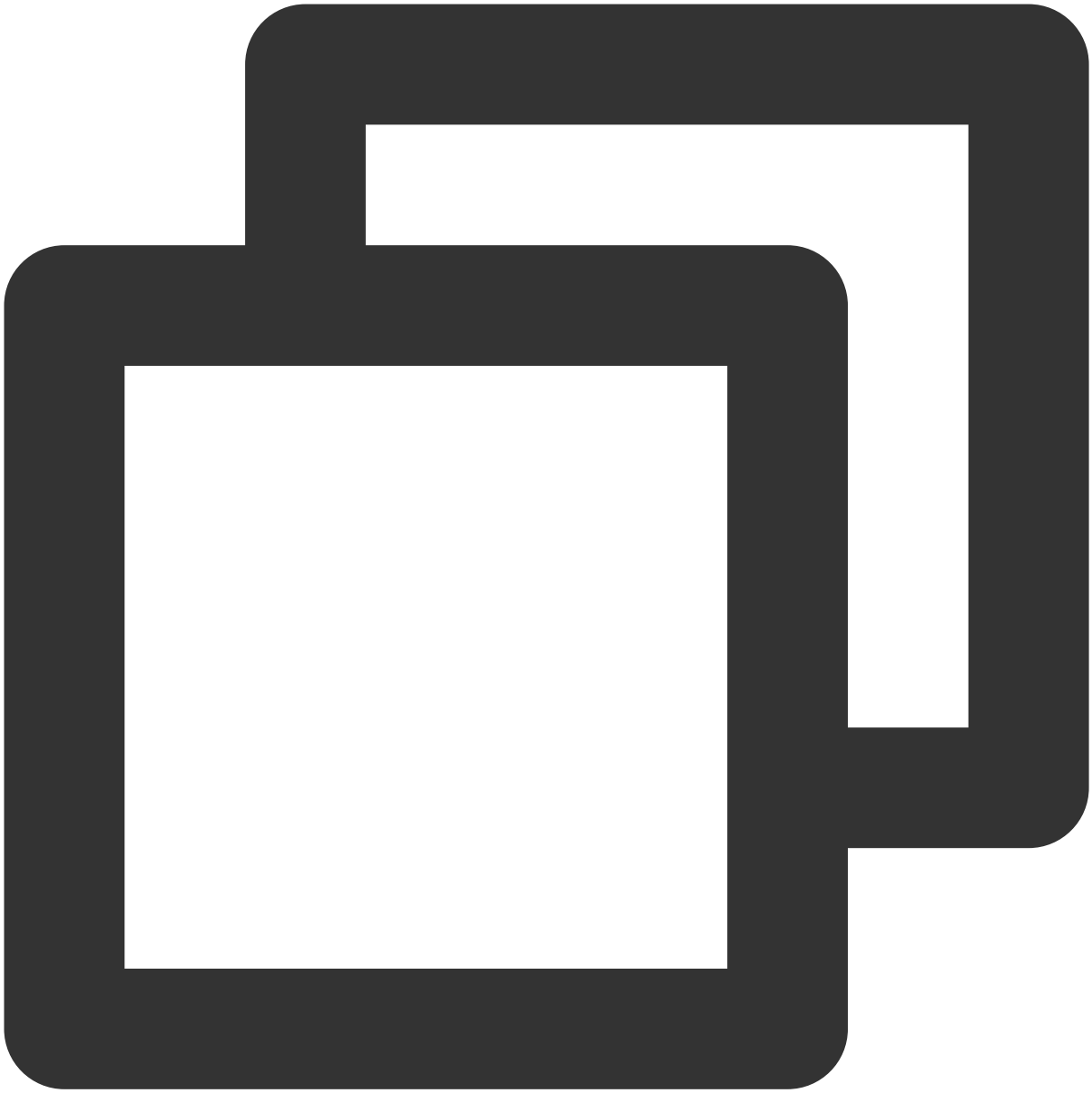
```
crypto ikev2 policy 1  # Define the phase 1 negotiation policy for IKEv2. Enter
encryption AES-128  # Set "AES-128" as the packet encapsulation encryption algor
integrity MD5  /# Set the hash algorithm to “MD5” for the IKE policy. It default
group 2  # Use Diffie-Hellman group 2 for the IKE policy. It defaults to "group
prf sha # Configure the encryption algorithm.
lifetime seconds 86400  # Configure the SA lifetime (namely, lifecycle). It defa
```

4. Configure a group policy.



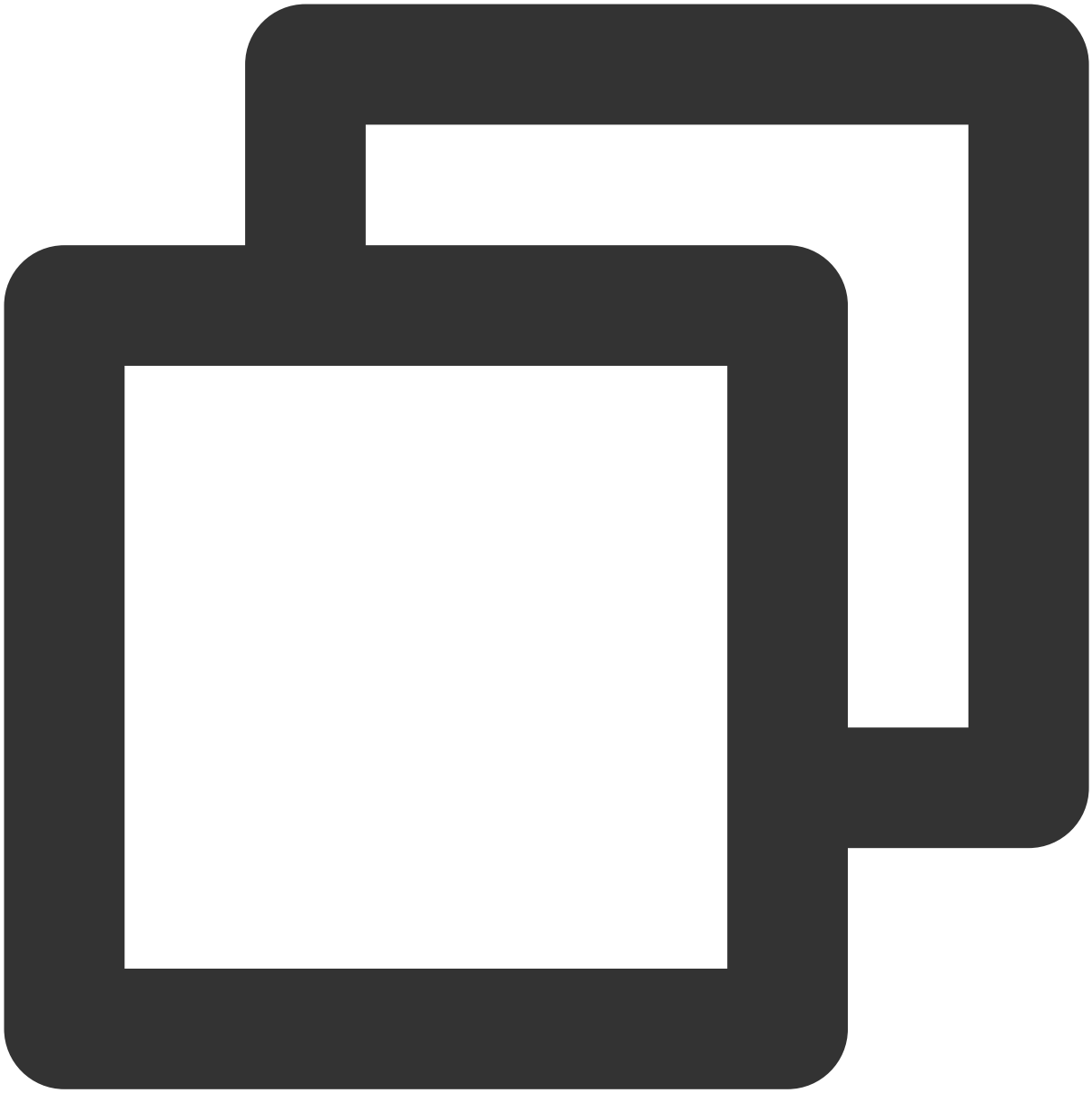
```
group-policy group_policy internal  # Set a group policy for devices.
group-policy group_policy attributes  # Set the group policy attributes.
vpn-tunnel-protocol ikev2 # Set IKEv2 protocol for vpn-tunnel.
```

5. Configure the pre-shared key.



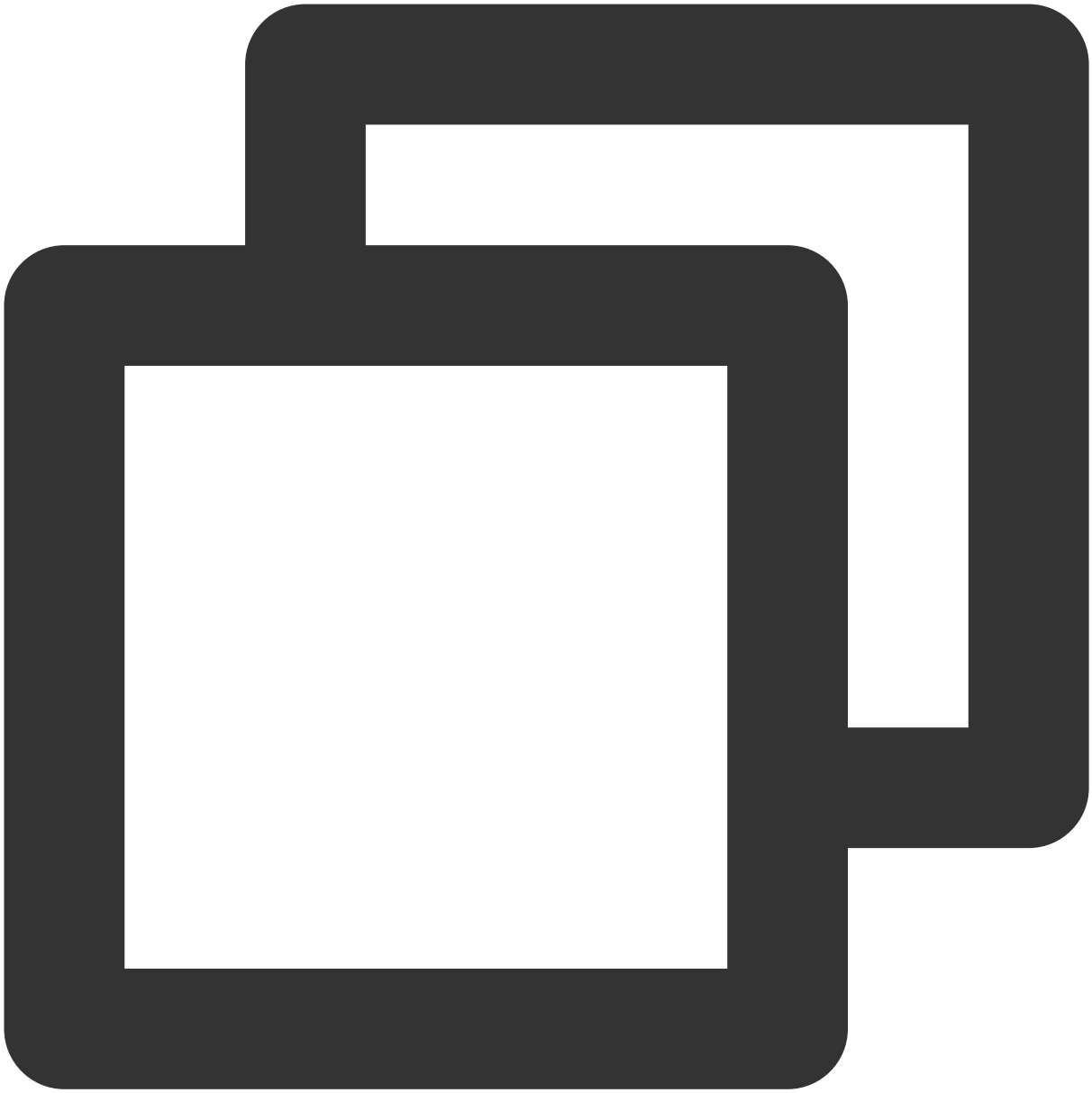
```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # Create a point-to-point IPsec tunne
tunnel-group 159.XX.XX.242 general-attributes default-group-policy group_policy
tunnel-group 159.XX.XX.242 ipsec-attributes  # Configure the tunnel group attrib
ikev2 remote-authentication pre-shared-key tencent@123
ikev2 local-authentication pre-shared-key tencent@123 # Enter letters, numbers o
```

6. Specify the IPsec protocol.



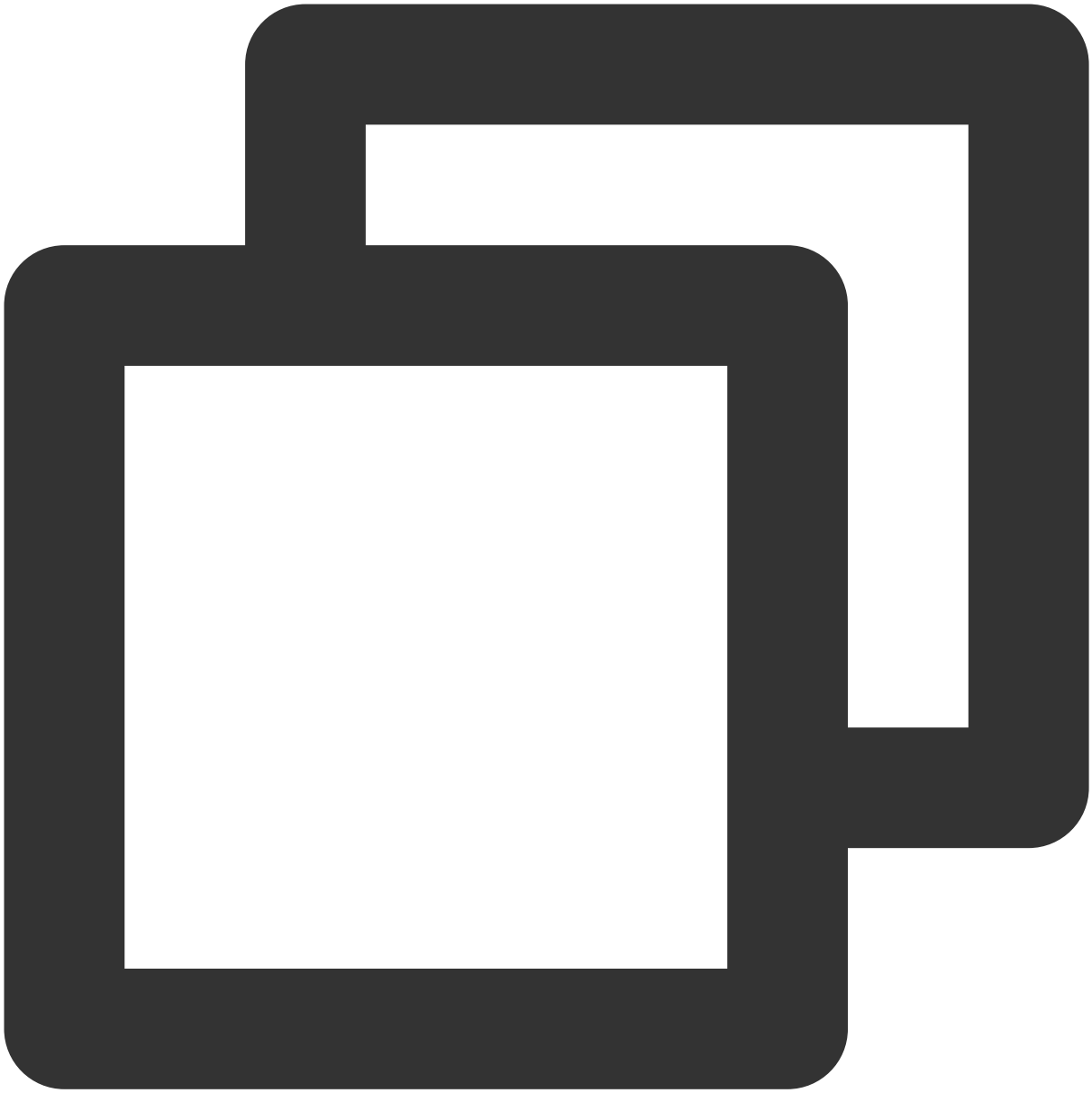
```
crypto ipsec ikev2 ipsec-proposal ikev2_proposal  # Specify the encryption algor
protocol esp encryption aes-128  # Specify an encryption algorithm.
protocol esp integrity sha-1 # Specify an integrity checking algorithm.
```

7. Configure an IPsec policy.



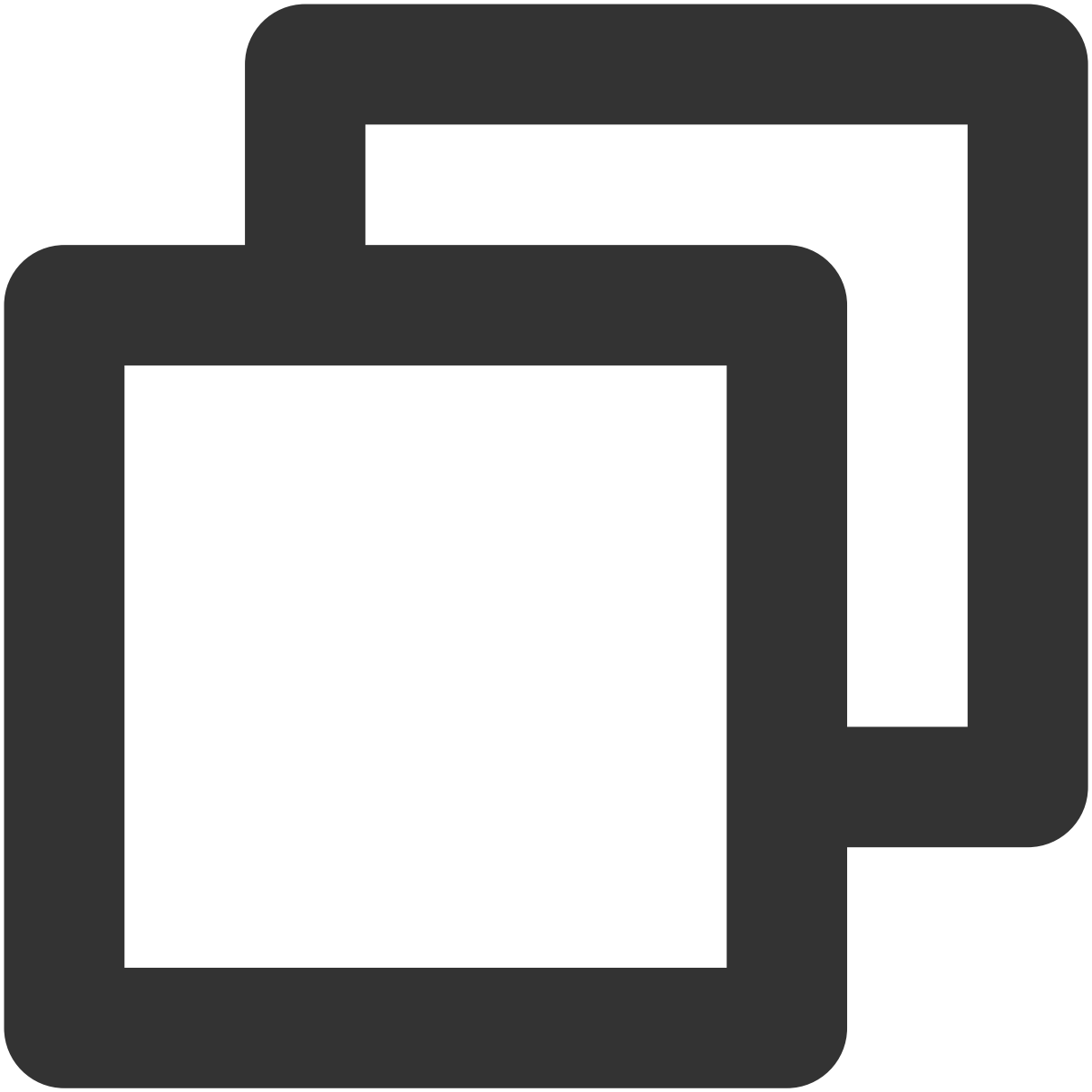
```
crypto ipsec profile PROFILE1
set ikev2 ipsec-proposal ikev2_proposal  # Configure an IKEv2 protocol for the c
set security-association lifetime kilobytes 1843200  # Specify the data stream i
set security-association lifetime seconds 3600  # Set the SA lifetime. The defau
```

8. Apply the IPsec policy.



```
interface Tunnel100
tunnel source interface outside  # Configure the source VPN that comes from the
tunnel destination 159.XX.XX.242  # Configure the public IP address of the desti
tunnel mode ipsec ipv4  # Configure the protocol for the tunnel interface.
tunnel protection ipsec profile PROFILE1  # Use the IPsec policy to protect data
```

9. Configure static routes.



```
    route vti 10.1.1.0 255.255.255.0 159.XX.XX.242   # Route the packets to be encry
```

10. Test the VPN connectivity.

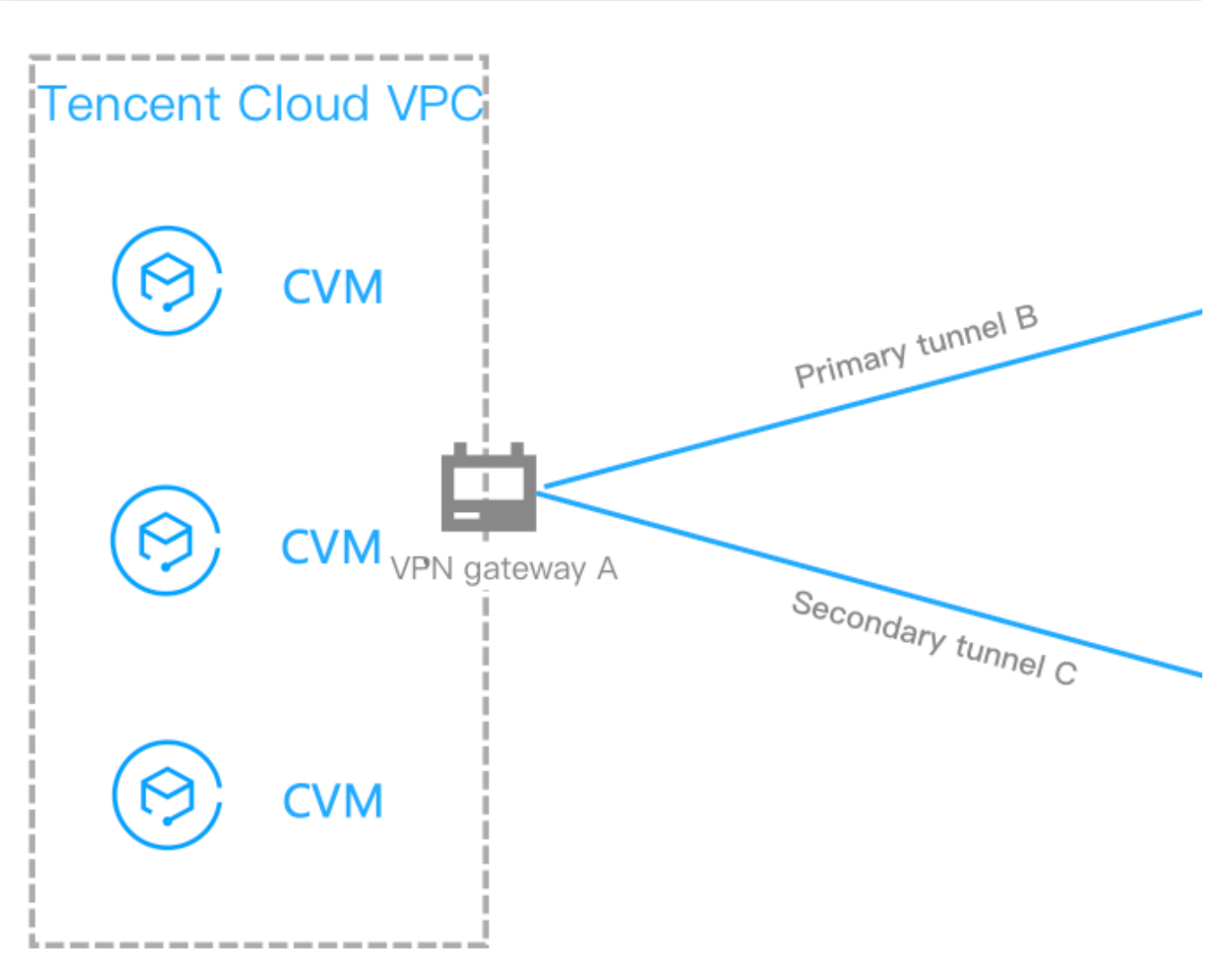
You can use the `ping` command to test the VPN connectivity.

Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery

Last updated：2024-01-09 14:20:07

A Tencent Cloud VPN connection features high availability. If the customer IDC connects to Tencent Cloud via primary/secondary VPN tunnels, when the primary tunnel fails, the business will be automatically switched over to the secondary tunnel, thus ensuring business sustainability and improving reliability. This document describes how to connect an IDC to a single Tencent Cloud VPC and implement primary/secondary disaster recovery.

Disaster Recovery Solution



The customer IDC only needs to interconnect with a single Tencent Cloud VPC. In the IDC, you can deploy two IPsec VPN devices that respectively create IPsec VPN tunnels with Tencent Cloud VPN gateway for VPC. Then, configure two routes to the same destination in the VPN gateway route table, and set the priority to control the primary/secondary tunnels. In case of failure, the routes can be switched over automatically.

Prerequisites

You have created a Tencent Cloud VPC.

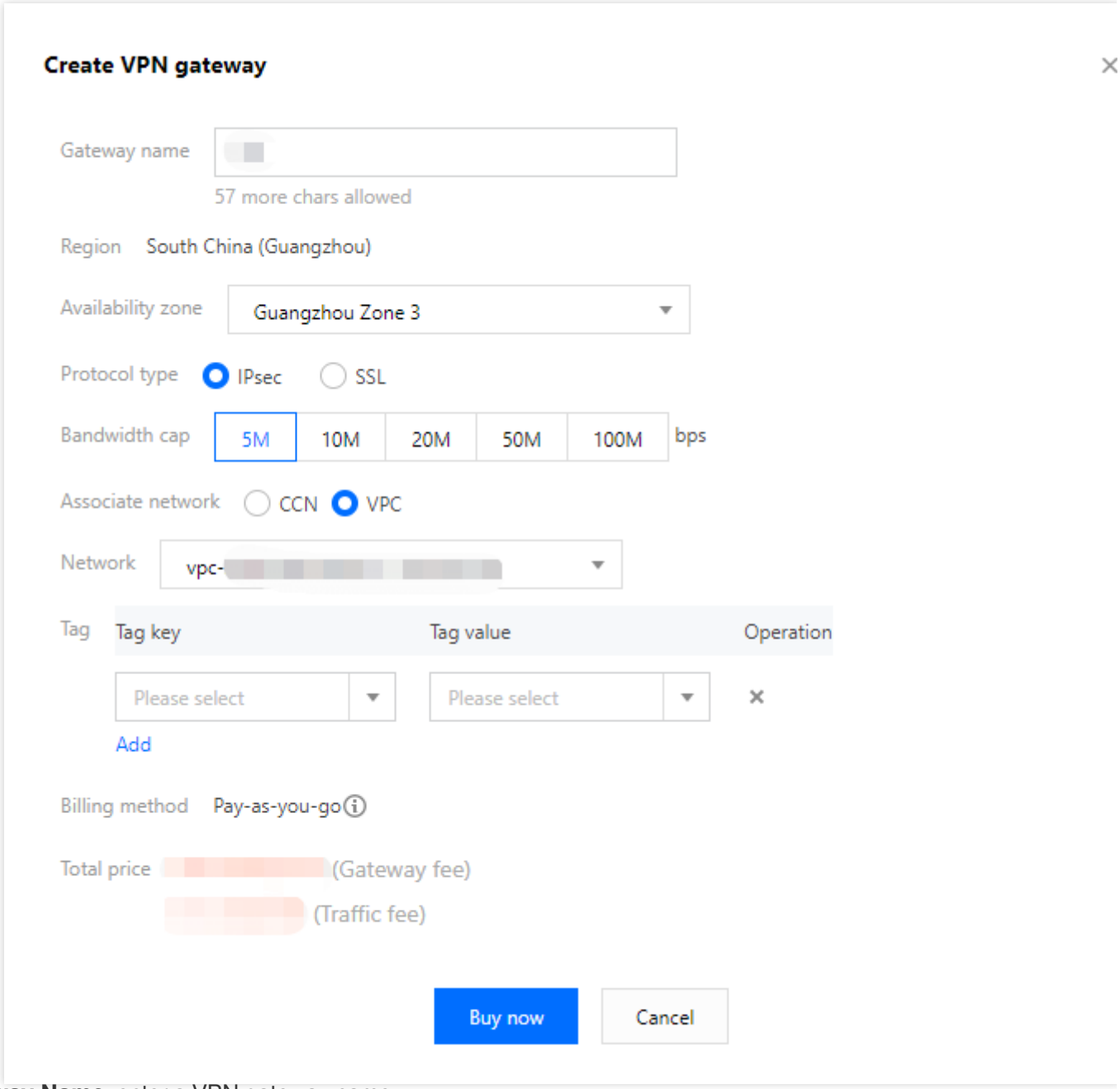
Directions

Step 1: create a VPN gateway A

Note:

This document takes creating a VPN gateway v3.0 as an example.

1. Log in to the VPC console.
2. Select **VPN Connection** > **VPN Gateway** on the left sidebar to access the **VPN Gateway** page.
3. Click **+New**.
4. Configure the following gateway parameters in the pop-up window.



Gateway Name: enter a VPN gateway name.

Associated Network: select **Virtual Private Network**.

Bandwidth Cap: choose the maximum bandwidth that meets the application requirements.

Billing method: supports pay-as-you-go.

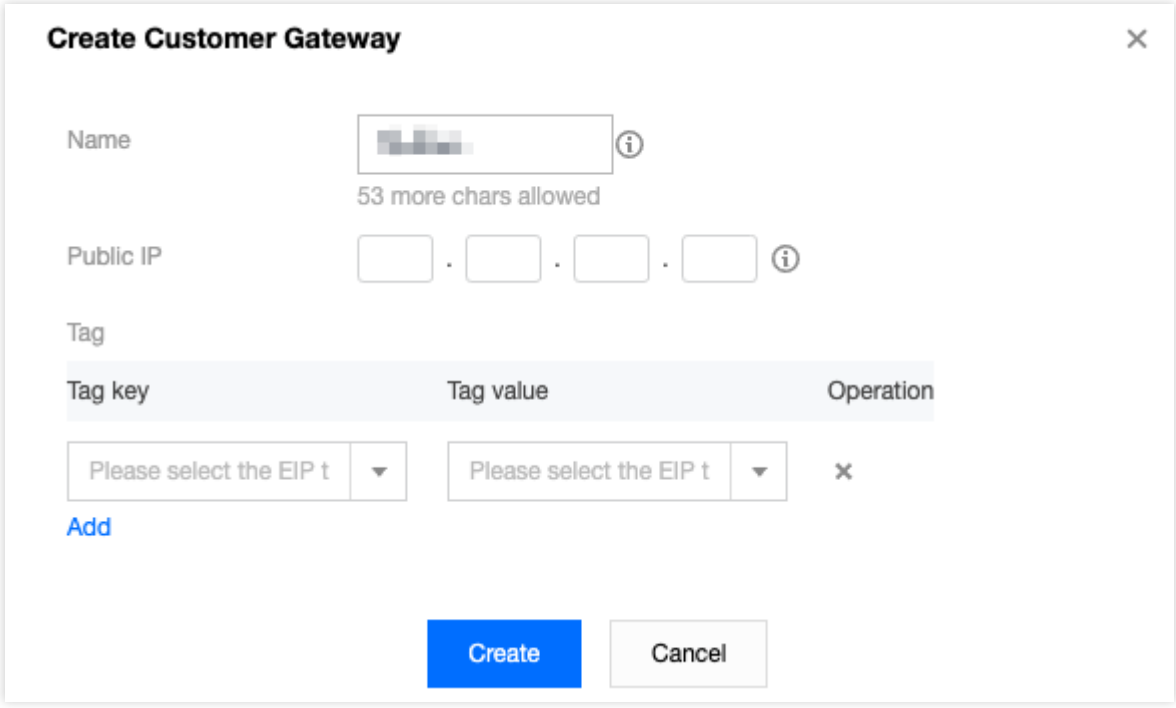
Leave the other parameters empty or keep their default settings.

5. After configuring gateway parameters, click **Create** to create a VPN gateway.
It takes about 1-2 minutes to complete creating a VPN gateway. Each running VPN gateway will be assigned with a public IP.

Step 2: create customer gateways

Creating a customer gateway D

1. Select **VPN Connection** > **Customer Gateway** on the left sidebar to access the **Customer Gateway** page.
2. Choose the region and click **+New**.
3. Enter the name and public IP of the customer gateway. Public IP refers to the static public IP of the VPN gateway device on the customer IDC side. You can optionally set tags.



Name: enter a customer gateway name.
Public IP: enter the public IP address of the VPN gateway on the IDC side.
4. Click **Create**.

Creating a customer gateway E

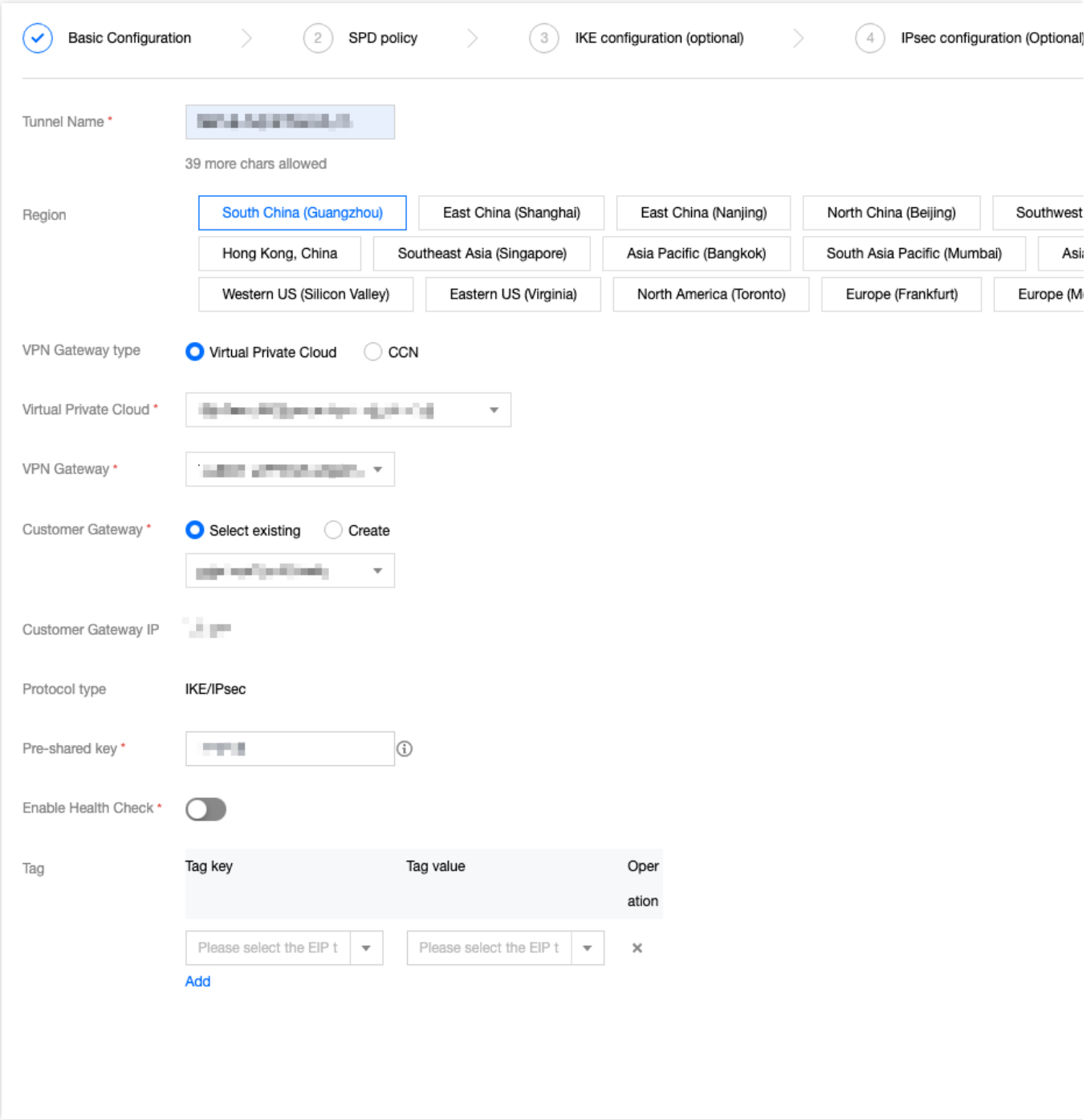
Repeat the step 1-4 of creating a customer gateway D.

Step 3: create primary and secondary VPN tunnels

After creating the VPN gateway and customer gateways, create two VPN tunnels (primary and secondary) that respectively connect the VPN gateway to customer gateways.

Creating a primary tunnel B

1. Select **VPN Connection** > **VPN Tunnel** on the left sidebar to access the **VPN Tunnel** page.
2. Choose the region and click **+New**.
3. Complete the configurations of the VPN tunnel as instructed in Creating VPN Tunnel. The SPD policy specifies a customer IP range `0.0.0.0/0` .



4. Click **Create**.

Creating a secondary tunnel C

Repeat the step 1-4 of creating a primary tunnel B. The SPD policy specifies a customer IP range `0.0.0.0/0` .

Step 4: configure IDC devices

After the first 3 steps, the VPN gateway and VPN tunnel on the Tencent Cloud are configured. Then, you need to configure the VPN tunnel on the local gateway of the IDC. For detailed directions, see Local Gateway Configurations. The local gateway refers to the IPsec VPN device on the IDC side. The public IP of this device is recorded in the "customer gateway" created in step 2.

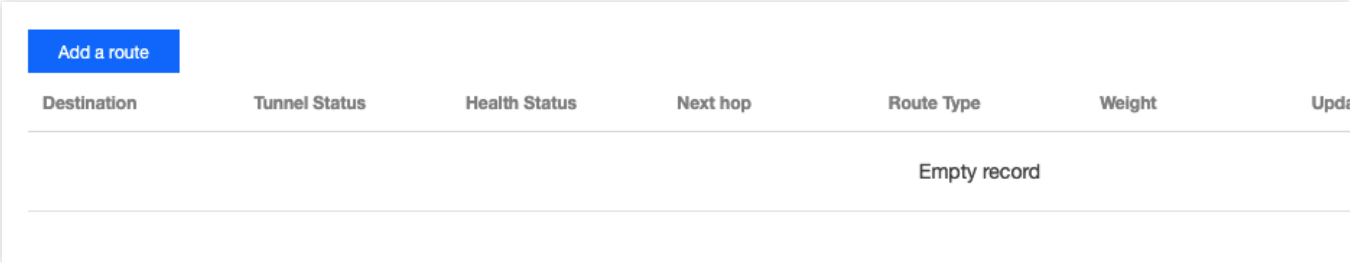
Note:

Configure both VPN gateways connected with the primary and secondary tunnels on the IDC side.

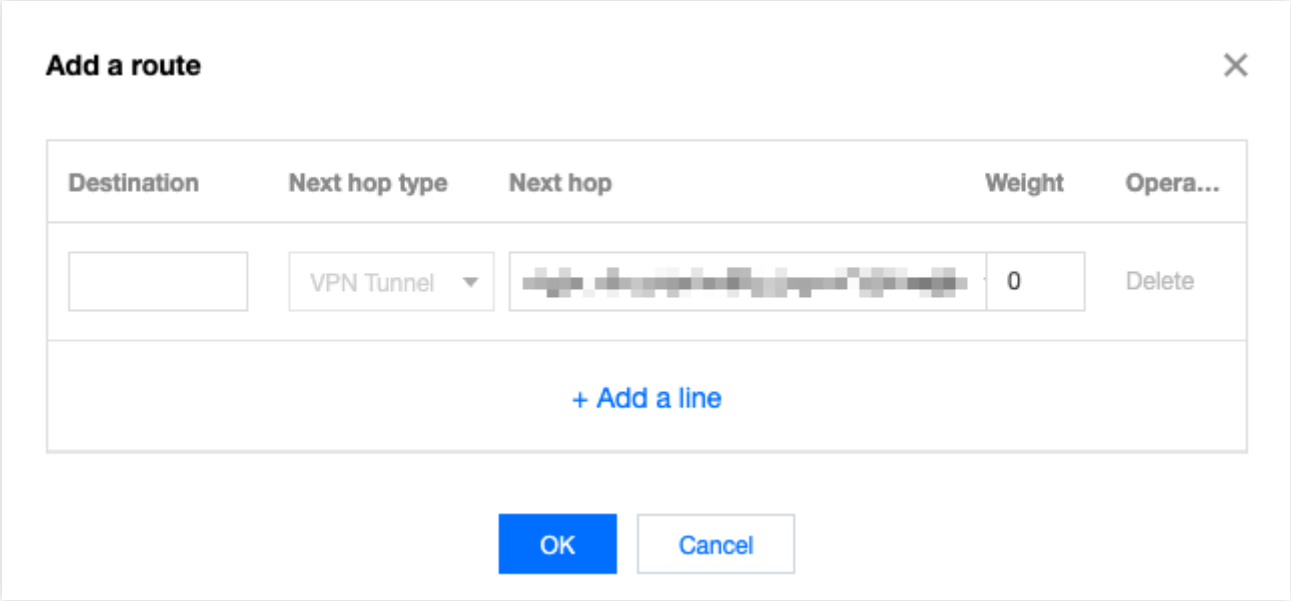
Step 5: configure the VPN gateway routes

After configuring the primary and secondary VPN tunnels, you need to configure the VPN gateway routes to VPN tunnels in the VPN console.

1. Select **VPN Connection** > **VPN Gateway** on the left sidebar to access the **VPN Gateway** page. Locate the VPN gateway A created in the step 1, and click the **ID/Name** to enter its details page.
2. Select the **Route Table** tab and click **Add a route**.



3. Configure the routing policy of the VPN gateway A to the customer gateways D and E, which specifies the routing and forwarding rules of traffic in the VPN tunnels B and C.



Configuration Item	Description
Destination	Enter the IDC IP range that provides the public access.
Next hop type	It defaults to **VPN Tunnel**.
Next hop	Select a VPN tunnel that has been created.
Weight	Enter “0” for the tunnel B. Enter “100” for the tunnel C. The smaller the value, the higher the priority.

4. Click **OK**.

Step 6: configure health checks for tunnels

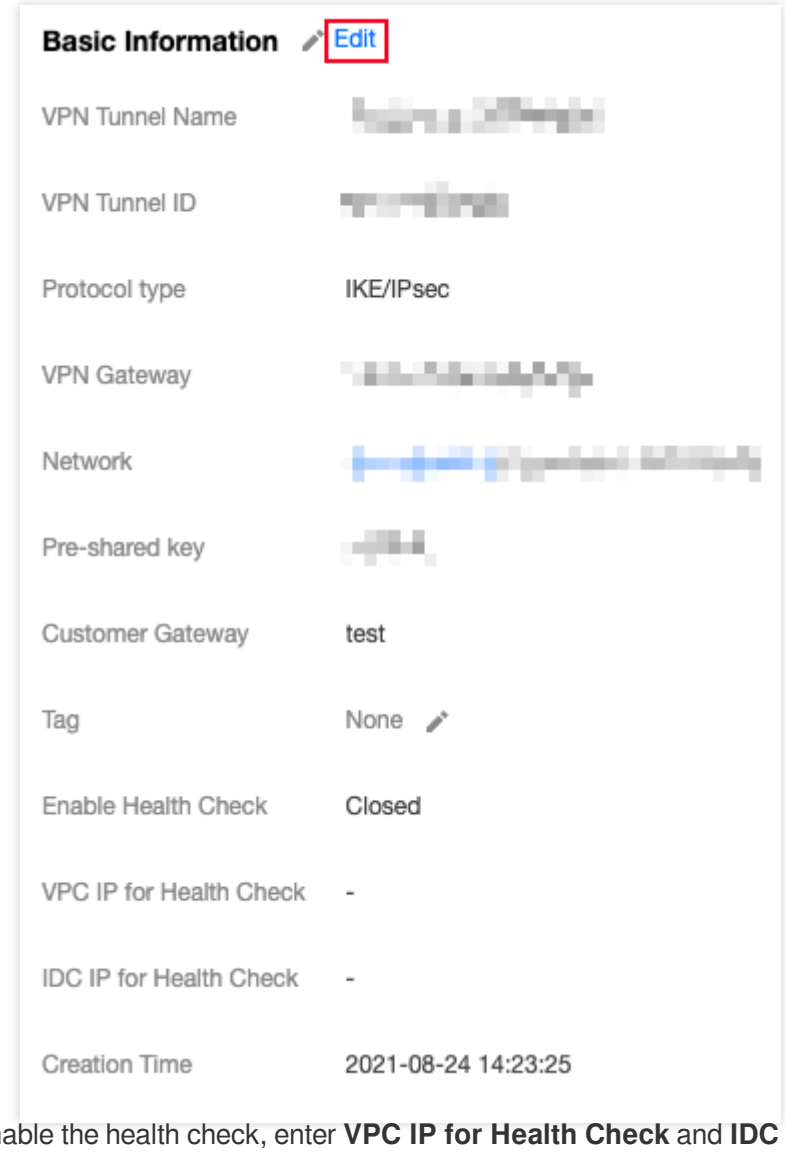
After configuring the VPN gateway routes, configure health checks for both the primary and secondary tunnels.

Note:

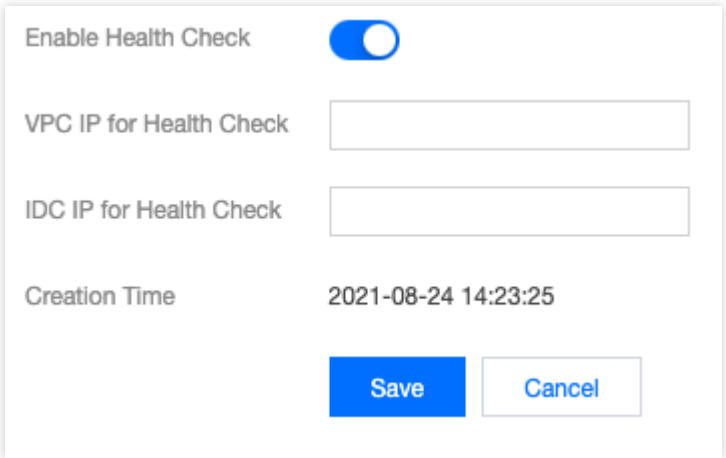
Your business may be interrupted for 1-2 seconds when the health check triggers the primary/secondary tunnel switchover.

Configuring a health check for the primary tunnel B

1. Select **VPN Connection** > **VPN Tunnel** on the left sidebar to access the **VPN Tunnel** page. Locate the VPN tunnel B and click the **ID/Name** to enter its details page.
2. Click **Edit** on the **Basic Information** page.



3. Enable the health check, enter **VPC IP for Health Check** and **IDC IP for Health Check**, and click **Save**.



Note:

VPC IP refers to the Tencent Cloud IP address that sends the access request to the IDC for a health check. This IP does not fall within a VPC CIDR block.

IDC IP refers to the IDC IP address that responds to the health check request of Tencent Cloud. Use an IP different from the VPC IP to avoid conflict.
If an IP address responds to the Tencent Cloud access request delivered via the tunnel, it means the tunnel is healthy.

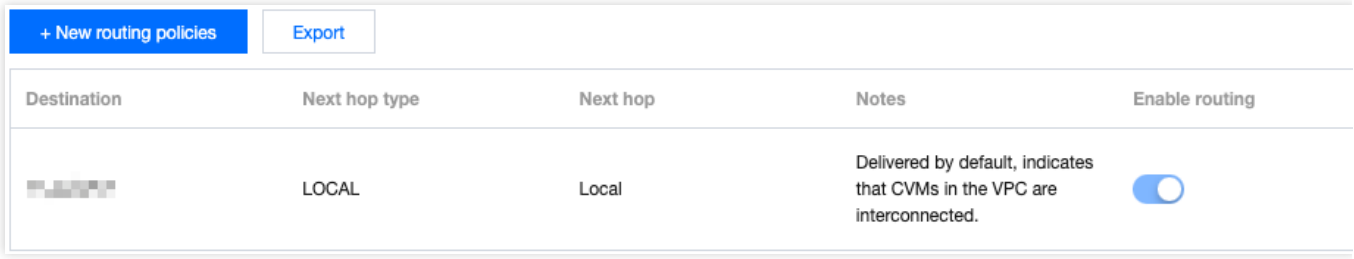
Configuring a health check for the secondary tunnel C

Repeat the step 1-3 of configuring a health check for the primary tunnel B, with a different health check IP address.

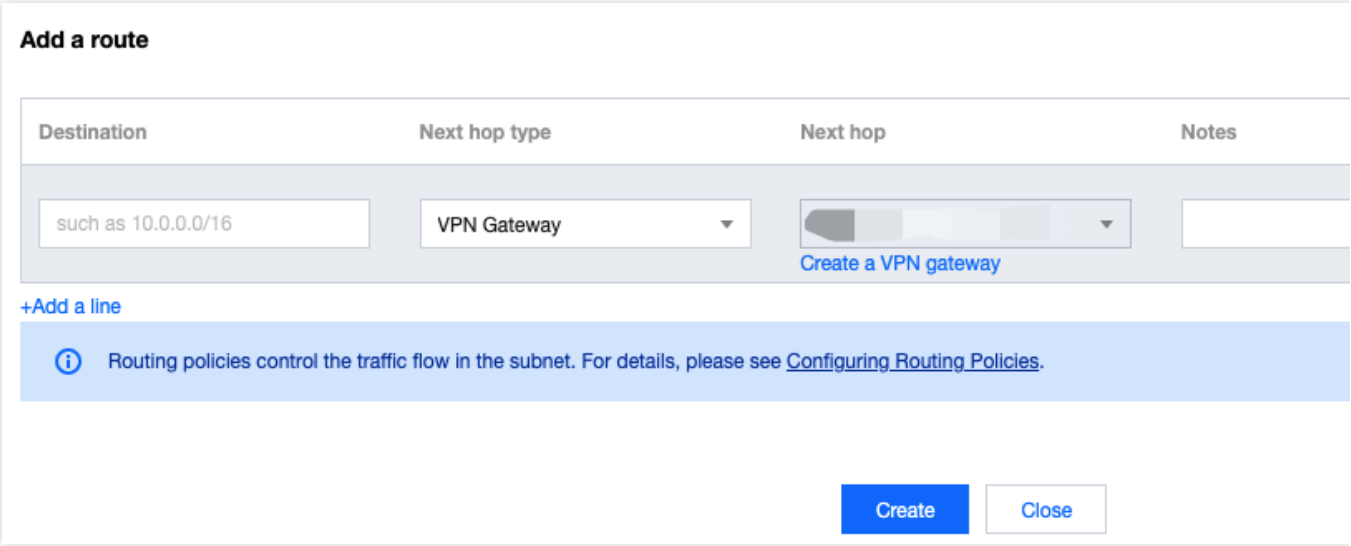
Step 7: configure the VPC routing policy

Now, you need to configure a VPC routing policy to direct the subnet traffic to the VPN gateway, thus enabling the subnet IP ranges to communicate with IDC IP ranges.
1. Log in to the VPC console.
2. Click **Subnet** on the left sidebar, and choose the corresponding region and VPC. Click the associated route table of the subnet to go to the details page.

3. Click **+New routing policies**.



4. In the pop-up window, enter the destination IP range, select **VPN Gateway** for the **Next hop type**, search for the VPN gateway just created and select it for the **Next hop**, and click **Create**.



Step 8: activate a VPN tunnel

You can use the CVM in the VPC to ping an IP address in the customer IP range to activate the VPN tunnel. If the pinging succeeds, the VPC and IDC can communicate with each other.

When the VPN route table finds the route of the primary tunnel B is unreachable, the traffic will be automatically forwarded to the VPN tunnel C to ensure high business availability.

Dedicated Private Network Traffic Encrypted Via a Private Network VPN Gateway Solution Overview

Last updated：2024-08-15 16:11:51

Note:

VPN gateway IP address belongs to the tenant's VPC.

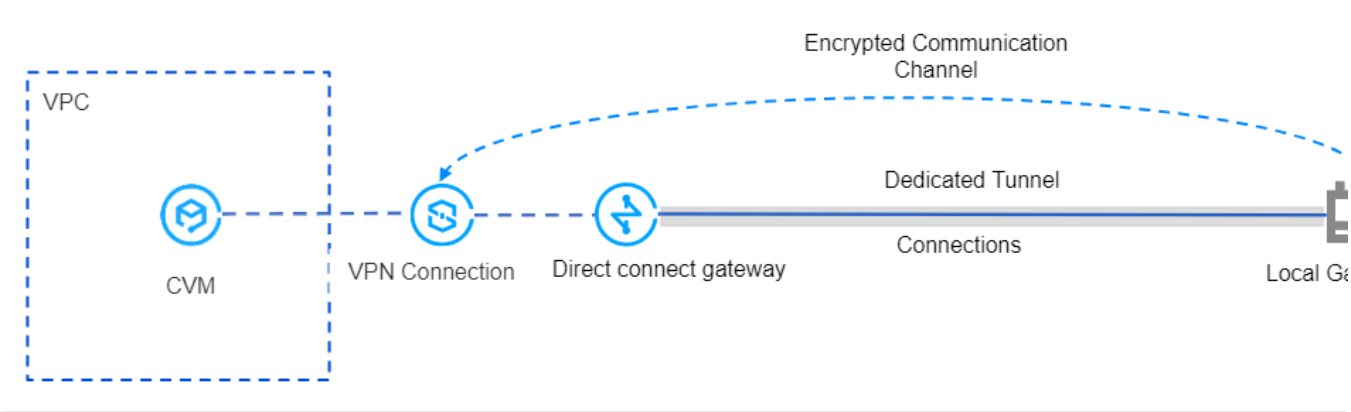
VPN currently only supports the VPC-type VPN. The CCN-type VPN gateway is not supported at the moment.

VPN does not currently support the dynamic BGP.

If you need to use a VPN, please submit a ticket for consultation.

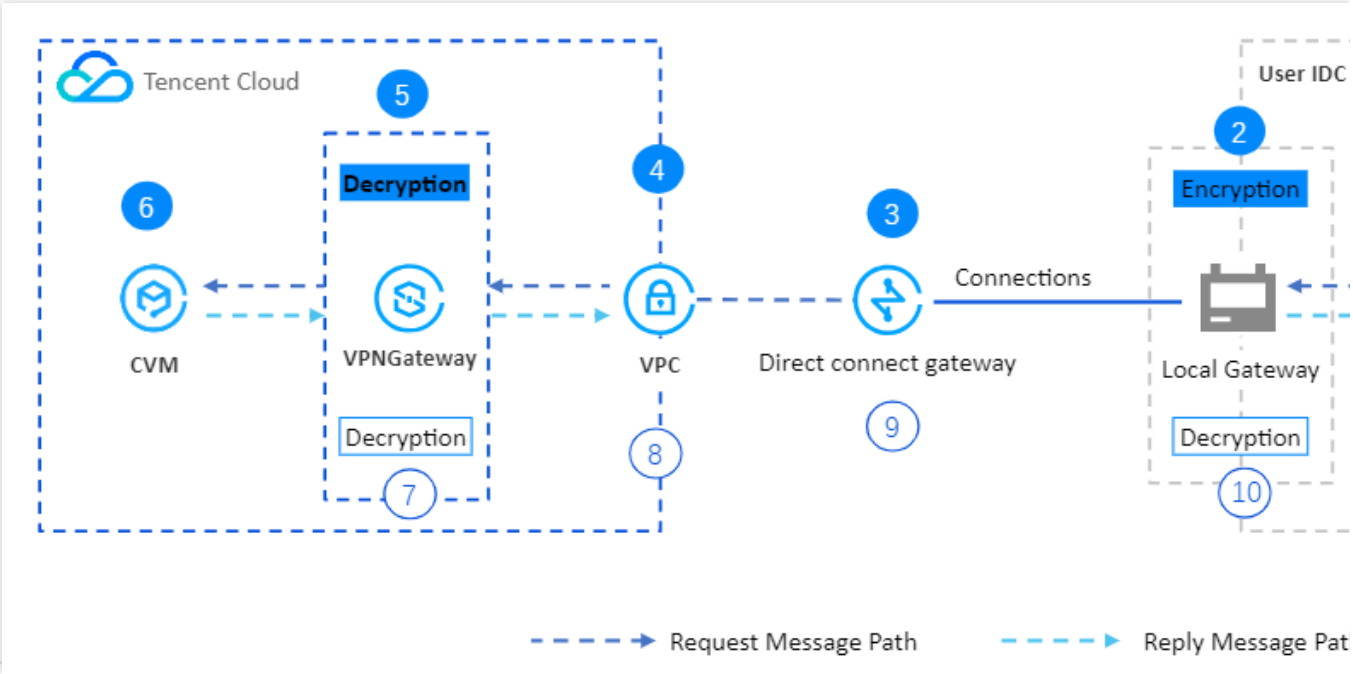
Scenario Description

After the communication through private network is established between the local IDC and the VPC on the cloud via a connection, the VPN gateway can establish an encrypted communication tunnel with the local gateway device through the existing private network connection. You can steer the traffic between the local IDC and VPC that needs to communicate with each other into the encrypted communication tunnel through the relevant route configuration, achieving the encrypted communication of private network traffic.



Principles of Encrypted Private Network Traffic Communication

For your convenience, the following specific instance illustrates the process of encrypted VPN traffic communication.



Serial Number	Forwarding Object	Description
①	User IDC Server	The client initiates an access request, and the request message is routed to the IDC local gateway.
②	IDC Local Gateway	The local gateway encrypts and encapsulates the request message. After encapsulation, it forwards the request message to the direct connect gateway on the cloud based on the configured route.
③	Direct Connect Gateway	After receiving the encapsulated request message, the direct connect gateway forwards it to the VPC.
④	VPC	After receiving the encapsulated request message, the VPC forwards the request message to the VPN gateway.
⑤	VPN Gateway	1. The VPN gateway receives the encapsulated request message and decrypts it. 2. After decrypting the request message, the VPN gateway traverses the route table based on the destination IP address in the request message, then forwards the request message to the CVM.
⑥	CVM	1. After receiving the decrypted request message, the CVM responds by sending a response message to the client. 2. The CVM queries the route table based on the destination IP address of the response message and forwards the response message to the VPN gateway.
⑦	VPN Gateway	1. After receiving the response message, the VPN gateway encrypts it. 2. Based on the encrypted destination IP address of the response message, the VPN gateway queries the routing table and forwards the response message to

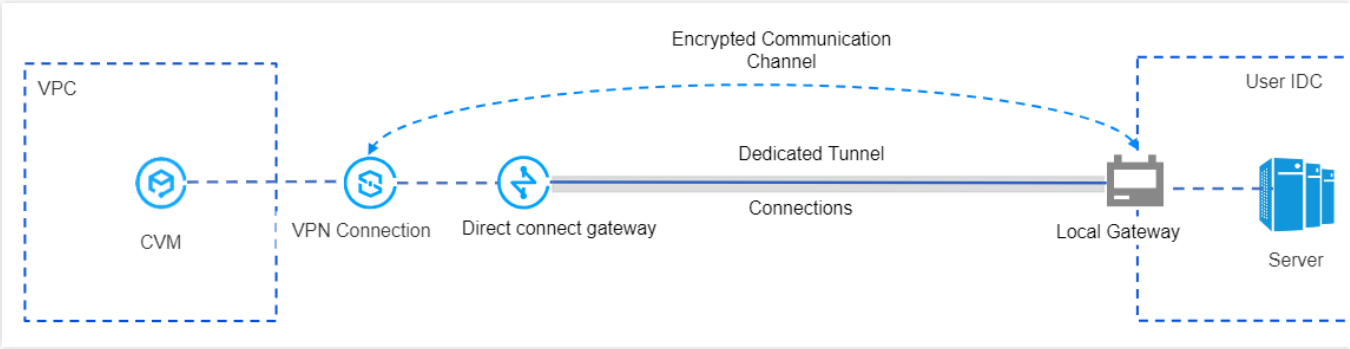
		the VPC.
⑧	VPC	After receiving the encrypted response message, the VPC queries the route table and forwards the encrypted response message to the direct connect gateway.
⑨	Direct Connect Gateway	After receiving the encrypted response message, the direct connect gateway queries the route table and forwards the encrypted response message to the IDC local gateway.
⑩	IDC Local Gateway	1. After receiving the response message, the IDC local gateway decrypts it. 2. The local gateway device queries the routing table based on the destination IP address decrypted from the response message and forwards the response message to the server.

Dedicated Private Network Traffic Encrypted Via a Private Network VPN Gateway

Last updated：2024-08-15 16:12:01

After the communication through private network is established between the local IDC and the VPC on the cloud via a connection, the VPN gateway can establish an encrypted communication tunnel with the local gateway device through the existing private network connection. You can steer the traffic between the local IDC and VPC that needs to communicate with each other into the encrypted communication tunnel through the relevant routing configuration, achieving the encrypted communication of private network traffic.

Service Scenario



Use Limits

VPN currently only supports the VPC-type VPN. The CCN-type VPN is not supported at the moment.
VPN does not support the dynamic BGP routing at this time.
It is only supported in VPN version 4.0.

Network Planning

Configuration Object	IP Range Planning	IP Addresses and Description

VPC	10.7.0.0/16	CVM:10.7.6.10 VPN gateway IP address: 10.7.6.15 **Note:** VPN gateway IP address belongs to the tenant's VPC.
Direct Connect Gateway	195.168.0.0/29	VLAN ID:1234 Tencent Cloud boundary IP address 1: 195.168.0.3/29 Tencent Cloud boundary IP address 2: 195.168.0.2/29 Customer boundary IP address: 195.168.0.1/29.
Local Gateway	195.168.0.0/24	Local gateway IP address connected to VPN on the cloud: 195.168.0.6 IP range connected to the direct connect gateway on the cloud: 195.168.0.1/29
Local IDC Server	133.168.0.0/16	Client IP address: 133.168.0.3/32

Prerequisites

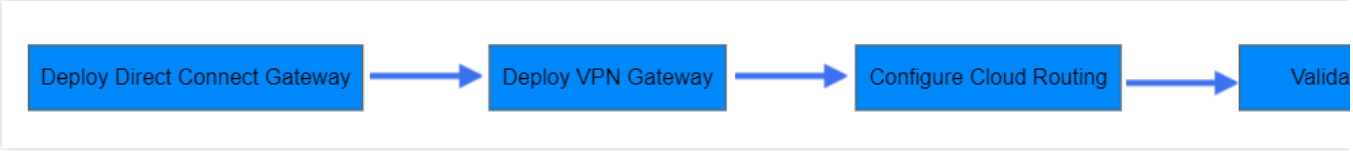
You have created a VPC network.

The connection has been constructed and is connected.

You have applied for VPN access permissions. If you need to use it, please submit a ticket to apply.

IDC side device is ready.

Configuration Process



Step One: Deploying Direct Connect Services

Step 1. Creating a VPC-Type Direct Connect Gateway

1. Log in to the Direct Connect console, and click **Direct Connect Gateway** in the left sidebar.
2. On the **Direct Connect Gateway** page, select the region and VPC at the top, and then click **Create**.
3. In the **Create a Direct Connect Gateway** dialog box, configure the gateway details, and then click **Confirm**.

Field	Meaning
Name	Enter a name for the direct connect gateway.

Availability Zone	Select the availability zone in the region.
Associated Network	Select VPC.
Network	Associate with the created VPC instance, for example, vpc-xxx.

Step 2. Creating a Dedicated Tunnel of Direct Connect

1. Log in to the DC - Dedicated Tunnels console.
2. Click **Dedicated Tunnels** > **Exclusive Private Tunnel** in the left sidebar. At the top of the page, click **Create** and configure Name, Direct Connect Type, Access Network, Region, Associated Direct Connect Gateway, and other basic name configurations. After completion, click **Next**.

Field	Meaning
Dedicated Tunnel Name	Dedicated Tunnel Name.
Direct Connect Type	Select "My Direct Connect"
Connection	Select a connection that is ready.
Access Network	Select VPC.
Gateway Region	Select the region where the target VPC instance is located, such as Guangzhou.
Direct Connect Gateway	Associate the private line gateway created in step 1.

3. Configure the following parameters on the **Advanced Configuration** page.

Field	Meaning
VLAN ID	Configure the planned VLAN, for example, 1234. One VLAN corresponds to one tunnel, with a value range of [0-3,000).
Bandwidth	The maximum bandwidth of a dedicated tunnel cannot exceed the bandwidth of the associated connection. Under the billing model of post-95 monthly payment, the "Bandwidth" parameter does not represent the billing bandwidth.
Tencent Cloud Boundary IP Address 1	Configure the planned connection's Tencent Cloud side boundary interconnect IP address, for example, `195.168.0.3/29` Do not use the following IP ranges or network addresses: `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`.

Tencent Cloud Boundary IP Address 2	Configure the planned standby boundary interconnect IP address, for example, `195.168.0.2/29`. If the primary boundary IP address becomes unavailable due to failure, the standby IP address is automatically activated to ensure the normal service operation. If the Tencent Cloud boundary IP address mask is set to 30, 31, then configuring the Tencent Cloud standby boundary IP address is not supported.
User Boundary IP Address	Configure the cloud IP on the IDC side for direct connect interconnection, for example, `195.168.0.1/29`.
Routing Mode	Select BGP Routing.
Health check	Health check is enabled by default. For details, see Dedicated Tunnel Health Check.
Check Mode	Select the BFD mode.
Health Check Interval	Interval between two health checks.
Number of Health Checks	Switch the route if the health check fails consecutively for the specified number of times.
BGP ASN	Enter the BGP neighbor ASN on the CPE side. Note that the cloud platform ASN is 45090. If this field is left empty, a random ASN will be assigned.
BGP Key	Enter the MD5 value of the BGP neighbor, which defaults to "tencent". If it is left empty, no BGP key is required. It cannot contain the following six special characters: ? & space " \\ +.

4. Click **Submit**.

Step 2: Deploy VPN Service

Step 1. Create a VPC VPN Gateway

1. Log in to the Virtual Private Cloud.
2. In the left directory, select **VPN Connection** > **VPN Gateway** to enter the management page.
3. On the VPN gateway management page, click **New**.
4. In the **Create VPN Gateway** dialog box, configure the gateway parameters as follows.

Parameter Name	Parameter Description
Billing Mode	Select billing by traffic. Monthly subscription is not supported for VPC VPNs currently.
Gateway Name	Enter the VPN gateway name (up to 60 characters).
Region	Display the region of the VPN gateway.

Protocol Type	Select IPsec.
Network Type	Select "VPC".
Associated Network	Select "VPC". Currently, CCN is not supported by VPC VPNs.
Cloud Subnet	Select the subnet created on the VPC side. The VPC VPN gateway IP address is assigned to the tenant's VPC from this subnet.
Bandwidth Cap	Select 5 Mbps.
Network	Select the VPC to be associated with the VPN gateway only when the associated network is a VPC.
Tag	Tags are identifiers for VPN gateway resources, designed to facilitate quicker querying and management of these resources. This configuration is optional and can be defined as needed.

5. After completing the gateway parameter settings, click **Create** to initiate the creation of the VPN gateway.

Step 2. Create a Peer Gateway

1. In the left navigation bar, select **VPN Connection** > **Peer Gateway**.
2. On the **Peer Gateway** management page, select the region, then click **Create**.
3. Enter the name of the peer gateway. For the VPC IP, enter the VPC IP of the local gateway device on the IDC side (195.168.0.6).
4. Click **Create**.

Step 3. Create a VPN Tunnel

1. In the left navigation bar, select **VPN Connection** > **VPN Tunnel**.
2. On the **VPN Tunnel** management page, select the region, and click **New**.
3. Enter the VPN tunnel information on the pop-up page.

This section only introduces the key parameter configurations. For other parameter configurations, refer to Create VPN Tunnel.

Parameter Name	Parameter Description
Tunnel Name	Enter the tunnel name.
Network Type	Select a VPC.
VPC	Select a VPC instance that has been created.
VPN Gateway	Select the VPC VPN gateway created in Step 1.

Peer Gateway	Select the peer gateway created in Step 2.
Pre-shared Key	Set it to 123456.
Negotiation Type	Select "Traffic Negotiation".
Communication Mode	Select "Destination Routing".
Advanced Settings	Select the current default value.

4. Click **Create**.

Step 4: IDC Local Configuration

After the first three steps are completed, the configuration of the VPN gateway and VPN tunnel on the cloud platform has been completed. It is necessary to continue configuring the VPN tunnel information for the other side on the local gateway at the IDC side. For details, refer to Local Gateway Configurations. The "Local Gateway" on the IDC side refers to the IPsec VPN device on the IDC side, and its VPC IP is recorded in the "Peer Gateway" in Step 2.

Step 3: Configure Cloud Routing

After the above configuration is completed, an encrypted communication tunnel can be established between the local gateway device and the VPN gateway. You will also need to configure routes for the cloud network instance to direct cloud and on-premises traffic into the VPN's encrypted communication tunnel.

Step 1. Configure Custom Routing for the Cloud VPC

1. Log in to the VPC Console.
2. In the left directory, click **Subnet**, select the corresponding Region and VPC, and then click on the subnet's associated Route Table ID to display the Details page.
3. Click **Create Routing Policy,** and configure the route to the VPN gateway in the pop-up box.

Parameter Name	Description
Destination Address	Enter the local IDC network segment, for example, '133.168.0.3/32'.
Next Hop Type	Select "VPC VPN Gateway".
Next Hop	Select the VPN gateway created in Step 1 in Step 2 Deploy VPN Service, that is, vpngw-xxxx.

4. Click **+ Add New Line** to configure routing policies to the Direct Connect Gateway.

Parameter	Description

Name	
Destination Address	Enter the VPN IP address of the Local Gateway device, for example '195.168.0.6'.
Next Hop Type	Select **Direct Connect Gateway**.
Next Hop	Select the Direct Connect Gateway created in Step 1 Create VPC Direct Connect Gateway, that is, dcg-xxxx.

5. Click **Create**.

Step 2: Configure VPN Gateway Routing

Note:

To direct VPC traffic to the on-premises network through the VPN gateway-based encrypted communication tunnel, you need to add a route in the VPN gateway for the local IDC network segment.

1. In the left navigation bar, click **VPN Connection** > **VPN Gateway**.
2. On the **VPN Gateway** management page, select the region and VPC, and then click the VPN Gateway instance ID to display the details page.
3. On the **Instance Details** page, click the **Route Table** tab, and then click **Add Route** to configure a routing policy.

Note:

When a new route is added to the VPN Gateway route table, the list by default displays all VPN tunnels under the VPN Gateway (that is, all SPD policy-based and route-based VPN tunnels under the VPN gateway).

Configuration Item	Description
Destination	Enter the local IDC network segment, for example, '133.168.0.3/32'.
Next Hop Type	Not selectable, and defaults to "VPN Tunnel".
Next Hop	Select the VPN Tunnel created when deploying the VPN.
Weight	Set the tunnel's weight to 0. 0: High priority. 100: Low priority.

4. After configuring the routing policy, click **Confirm**.

Step 4: Verify Traffic

After the above configurations are completed, encrypted VPC network communication can be established between the local IDC and the VPC. Test the VPC network connectivity between the local IDC and the VPC and verify that the

traffic is encrypted through the VPN gateway.

1. Testing connectivity

Log in to the CVM instance and use the **Ping** command to access servers within the local IDC network segment.

2. Encryption verification

In the VPN Console, check the VPN tunnel traffic monitoring. The presence of traffic indicates successful encryption.

Establishing a VPN Connection between Tencent Cloud and Azure China

Last updated：2024-01-09 14:20:07

We recommend establishing a VPN connection between two public clouds to transmit traffic over a private network. This improves network security and reduces risk exposure.

Note:

To establish a VPN connection, you need to create Tencent Cloud services and Azure China cloud resources. Therefore, the steps outlined in the tutorial may not be up to date.

The tutorial is provided by a Tencent Cloud service user and is for study and reference only.

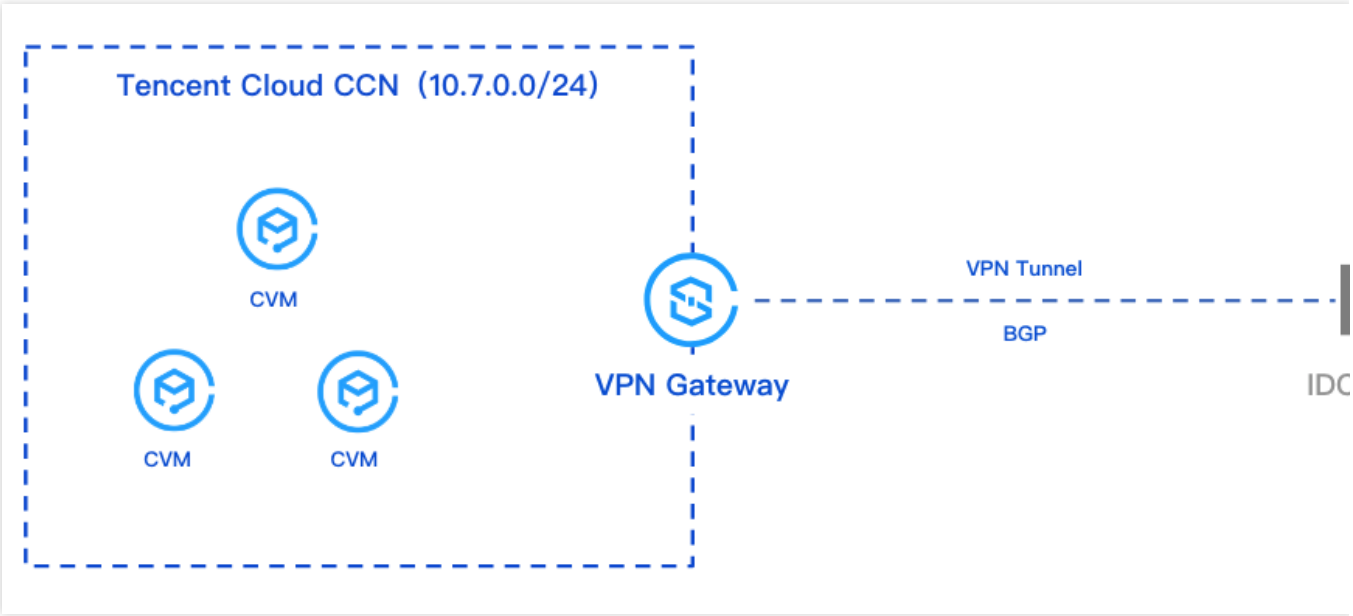
Establishing Connection Between IDC and Cloud Resources (Dynamic BGP)

Last updated：2024-04-10 15:29:15

This document introduces how to establish business communication between IDC and cloud resources using the dynamic BGP of VPN.

Business Scenario

Some business of the users is deployed on the cloud, and VPN is used to connect IDC and cloud networks, and the communication is through BGP.



Operation Process

1. Creating a Cloud Connect Network instance.
2. Creating a CCN type VPN gateway and bind it with the created Cloud Connect Network instance.
3. Creating the customer gateway and specify the ASN on the IDC side.
4. Creating the VPN tunnel and configure the BGP parameters.
5. Local configuration on the IDC side.

Directions

This guide only covers the essential configuration steps and parameters during the operation process. See the specific operational documents for details of other parameters.

Step 1: Creating a Cloud Connect Network Instance

You need to create the required Cloud Connect Network instance on the Cloud Connect Network console. For specific operations, see Creating a CCN Instance.

Step 2: Creating a IPSec VPN Gateway

1. Log in to the VPN Gateway Console, and on the VPN gateway page, click **Create**.
2. Configure CCN type gateway parameters on the VPN Purchase Page.
Region: Select Seoul.
Network type: Select Cloud Connect Network.
Bandwidth: Select 200 Mbps or higher.
BGP ASN: The default ASN of VPN Gateway on the side of Tencent is 64551, with a permissible range of 1 - 4294967295, excluding 139341, 45090, and 58835.
3. On the VPN gateway details page, bind the Cloud Connect Network instance created in Step 1.

Step 3: Creating a Customer Gateway

1. Log in to the Customer Gateway Console, and click **Create** on the Customer Gateway page on the right side.
2. On the **Create Customer Gateway** page, configure the public IP address for internet access and the planned ASN on the IDC side. For more details, see Creating Customer Gateway.

Step 4: Creating a BGP Route-Based VPN Tunnel

1. Log in to the VPN Tunnel Console, click **Create** on the VPN tunnel page on the right side.
2. On the new VPN tunnel creation page, configure the basic tunnel parameters based on actual conditions, and proceed with further configuration after completion.

Parameter	Description
Network Type	Select Cloud Connect Network.
VPN Gateway	Select a Cloud Connect Network type VPN gateway configured with ASN.
Customer Gateway	Select the customer gateway configured with ASN.
Communication Mode	Select dynamic BGP routing.
BGP Neighbor	BGP tunnel IP range for intercommunication between the cloud and the user, the IP range must be within the range of `169.254.128.0/17` .

Cloud BGP Address	BGP IP Address for interconnection between the cloud and the user.
User BGP Address	Unmodifiable and automatically assigned user BGP interconnection address. After manual modification of the cloud BGP address is completed, this parameter automatically updates.

Step 5: IDC Local Gateway Configuration

After you complete the first 4 steps, the configuration of the cloud-based VPN Gateway and VPN Tunnel is already completed. It is necessary to continue configuring the VPN Tunnel information on the Local Gateway on the IDC side. For details, see Local Gateway Configurations.

Note：

The "local gateway" on the IDC side refers to the IPsec VPN device on the IDC side. The public IP of this device is recorded in the created "customer gateway".

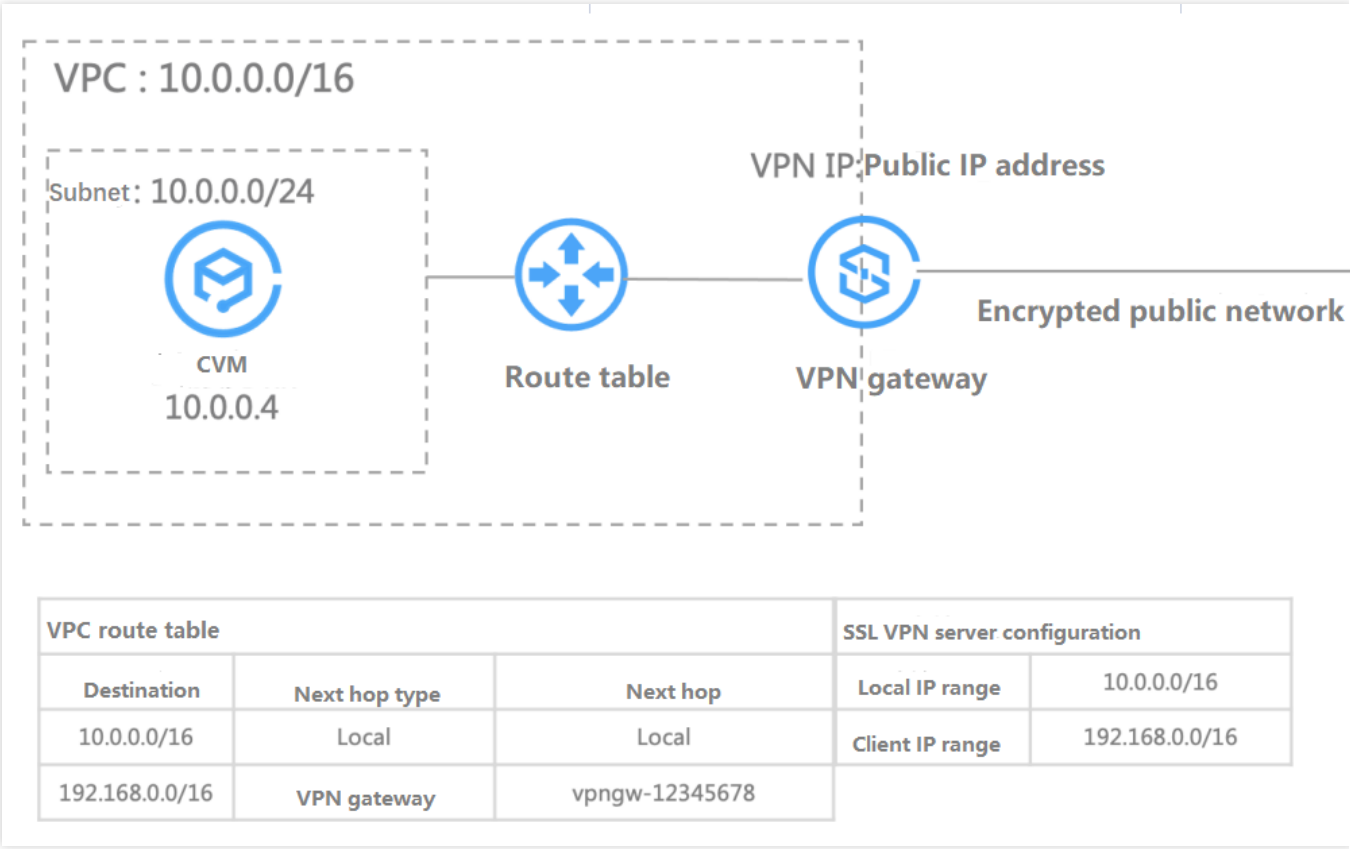
SSL VPN
Connecting Client to VPC

Last updated：2024-01-09 14:20:07

This document describes how to connect to a VPC over an SSL VPN connection on a Windows, macOS, or Linux client.

Background

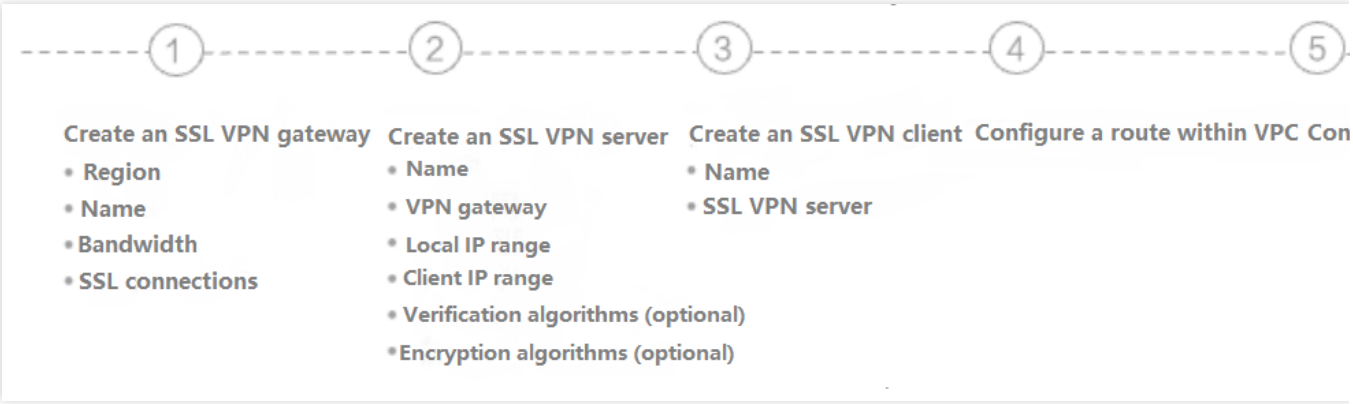
This document takes the scenario below as an example to describe how to connect to a VPC over an SSL VPN connection on a Windows, macOS, or Linux client.



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	192.168.0.0/16
192.168.0.0/16	VPN gateway	vpngw-12345678		

Configuration

The process of connecting to a VPC over an SSL VPN connection on the client is as follows:



Step 1: Create an SSL VPN Gateway

1. Log in to the VPC console.
2. Select **VPN Connections** > **VPN Gateway** on the left sidebar to enter the admin page.
3. Click **+New**.
4. In the **Create VPN gateway** pop-up window, configure the following gateway parameters.

Parameter	Configuration
Gateway name	Enter the VPN gateway name (up to 60 characters).
Region	Display the region of the VPN gateway.
AZ	Select the availability zone of the current gateway.
Protocol Type	Select SSL.
Bandwidth cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Associated Network	Select VPC.
Network	Select the VPC associated with the VPN gateway
SSL VPN Connections	Select the number of clients that you want to connect. An SSL client allows connection from only one user.
Billing Mode	The SSL VPN gateway is pay-as-you-go by default.

5. Click **Create**.

Step 2. Create an SSL VPN Server

1. Log in to the VPC console.
2. Select **VPN Connections** > **SSL VPN Server** on the left sidebar to enter the admin page.

Note:

A VPN gateway can be associated with only one SSL VPN server. For more information, see Use Limits.

3. Click **+New**.
4. In the **Create an SSL VPN server** pop-up window, configure the following parameters.

Parameter	Configuration
Name	Enter the SSL VPN server name (up to 60 characters).
Region	Display the region of the SSL VPN server.
VPN gateway	Select an existing VPN gateway.
Server IP range	Tencent Cloud IP ranges accessed by mobile clients.
Client IP Range	Enter the IP range that is assigned to the mobile client for communication. The IP range must not conflict with the VPC CIDR block of Tencent or your local IP range.
Protocol	Transmission protocol of the server.
Port	Enter the SSL VPN server port used for data forwarding.
Verification algorithm	Supported authentication algorithms: SHA1 and MD5.
Encryption algorithm	Supported encryption algorithms: AES-128-CBC, AES-192-CBC, and AES-256-CBC.
Compressed	No.

5. Click **Create**.

Step 3. Create an SSL VPN Client

1. Log in to the VPC console.
2. Select **VPN Connections** > **SSL VPN Client** on the left sidebar to enter the admin page.
3. Click **+New**.
4. Configure the following parameters in the pop-up window.
5. Click **Create**. When **Certificate Status** changes to **Available**, the client is created.

6. On the SSL VPN client page, find the newly created client certificate and click **Download the configuration** in the **Operation** column.

Note:

An SSL client allows connection from only one user.

Step 4. Configure a Route within the VPC

1. Log in to the VPC console.
2. Click **Route Tables** on the left sidebar to enter the admin page.
3. In the list, click the ID of the target route table to enter its details page. You can also create a route table as instructed in Creating Custom Route Tables.
4. Click **+ New routing policies**. In the pop-up window, configure the routing policy.

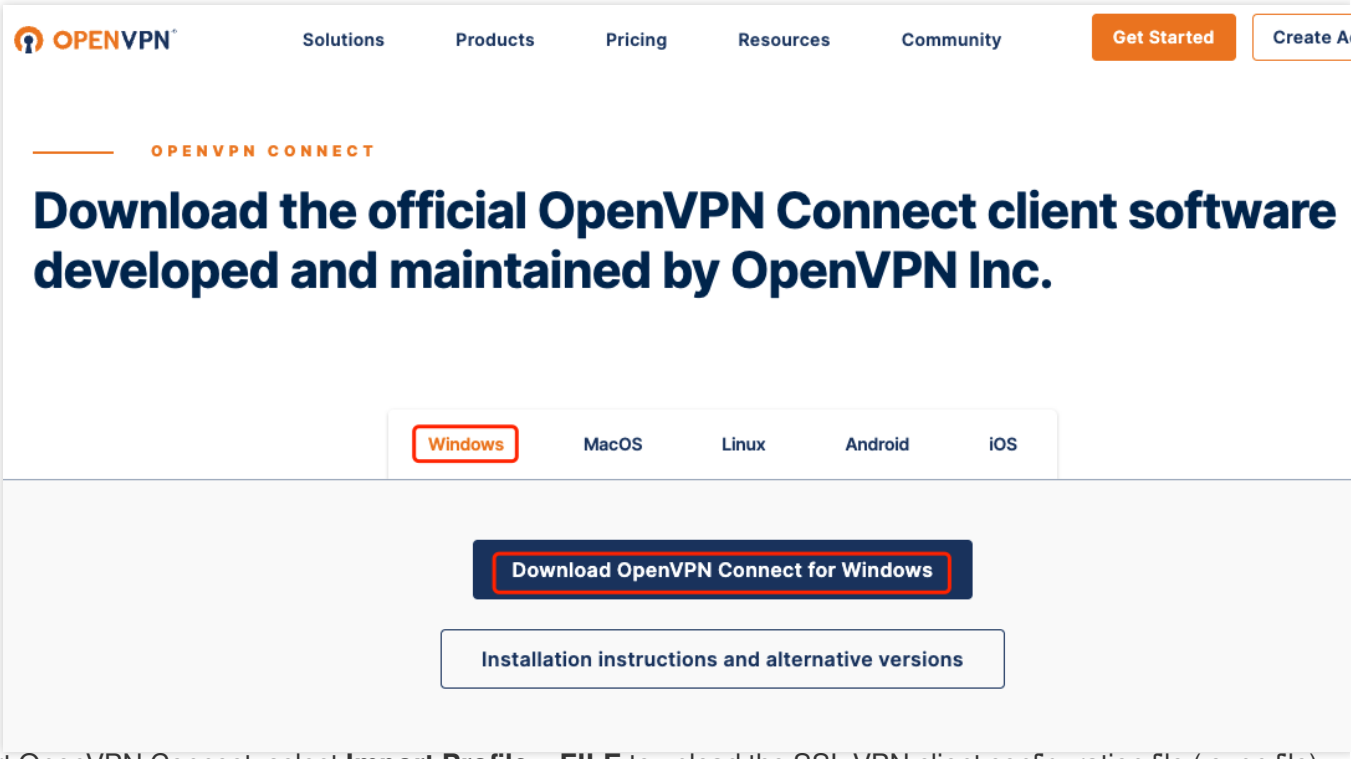
Parameter	Configuration
Destination	Enter the client IP range that is configured in Step 2: Create an SSL VPN Server.
Next Hop Type	Select VPN Gateway.
Next Hop	Select an existing SSL VPN gateway.

Step 5. Configure the Client

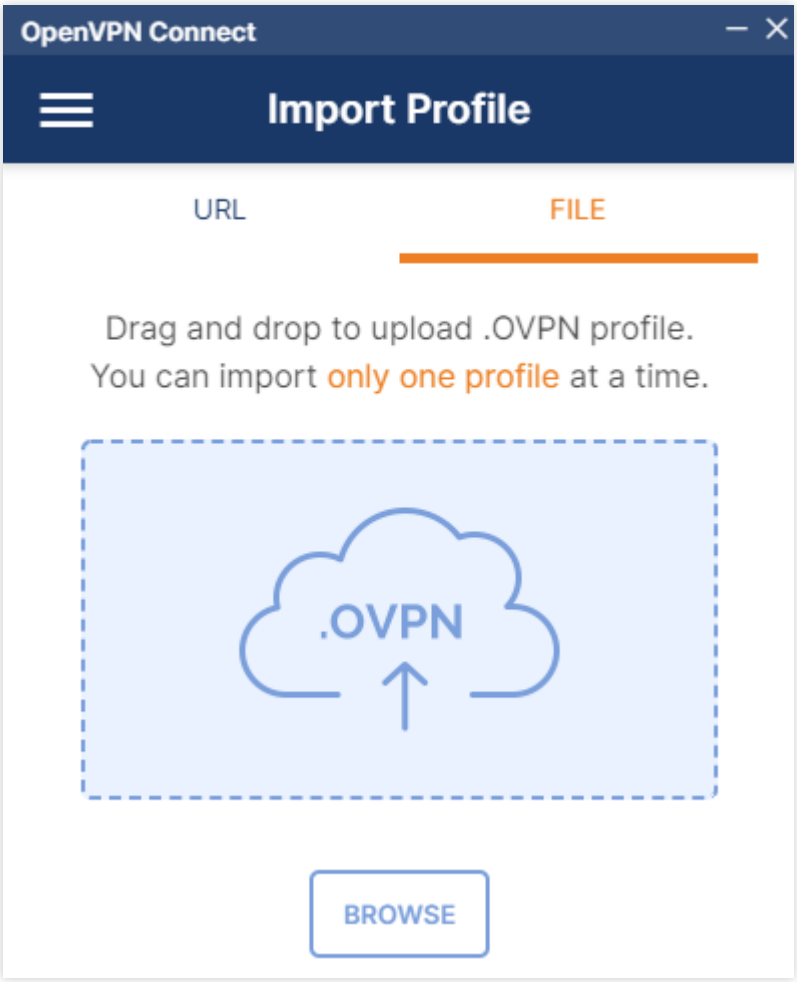
This section describes how to configure Windows, macOS, and Linux clients.

Windows client

1. Download OpenVPN Connect for Windows from the OpenVPN website and install OpenVPN Connect.

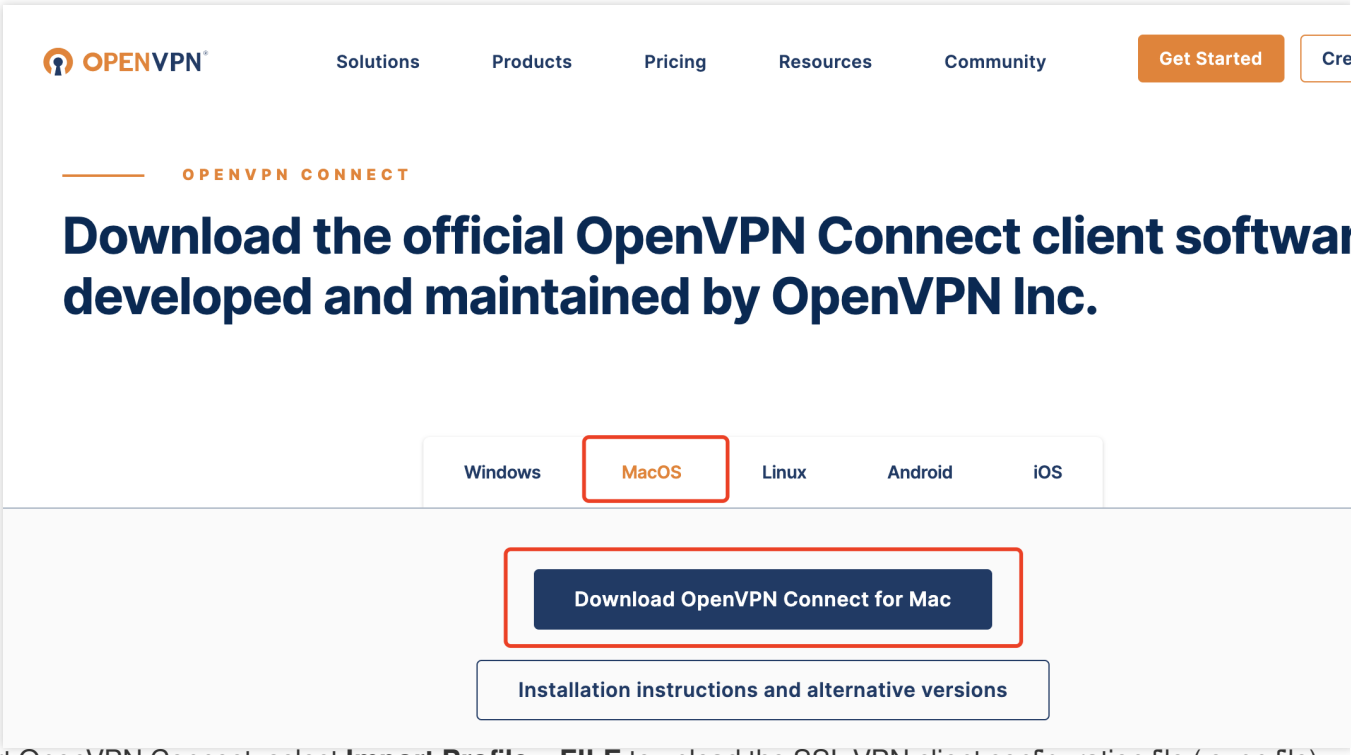


2. Start OpenVPN Connect, select **Import Profile** > **FILE** to upload the SSL VPN client configuration file (.ovpn file) downloaded in Step 3.



macOS client

1. Download OpenVPN Connect for macOS from the OpenVPN website and install OpenVPN Connect.

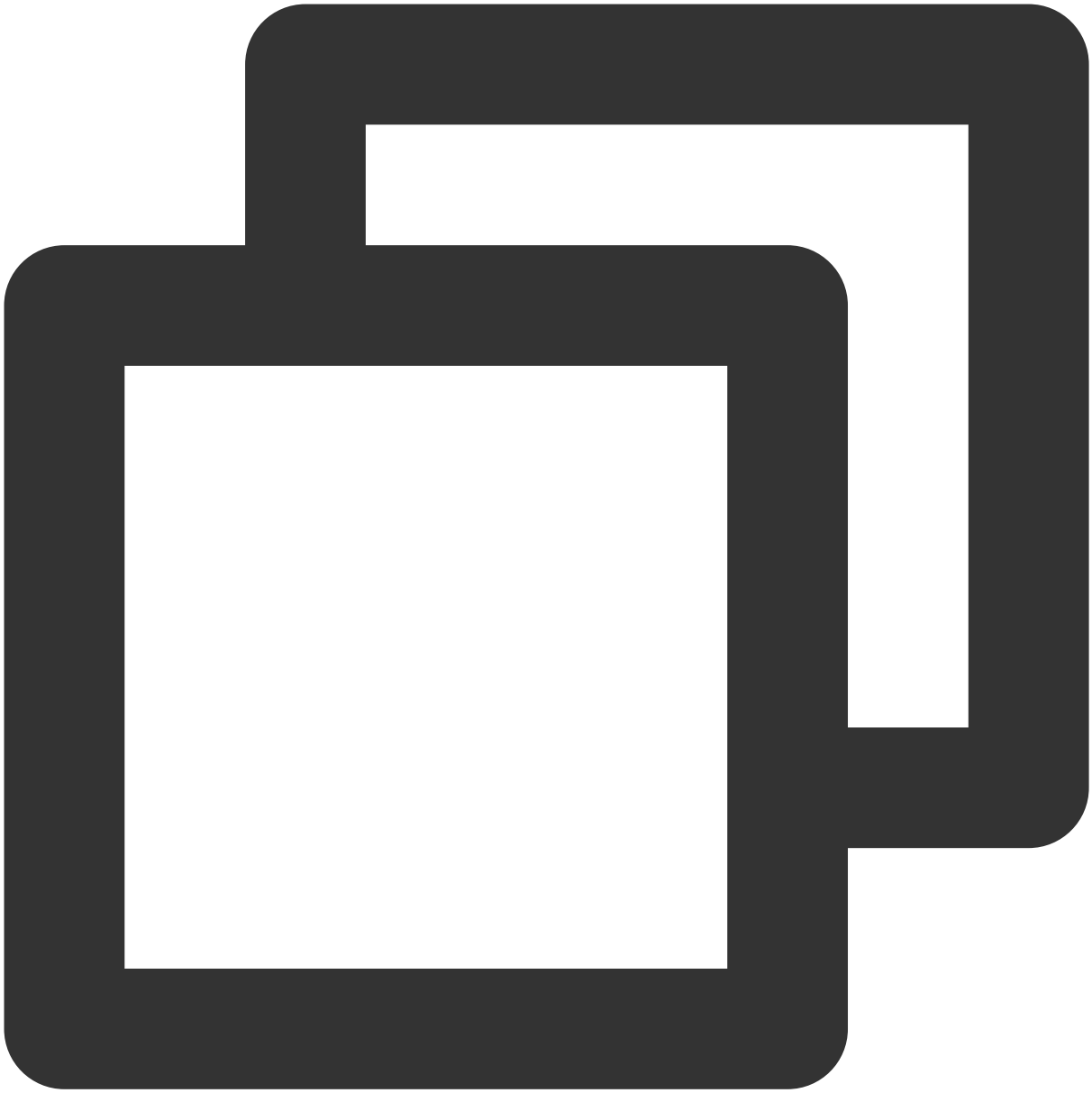


2. Start OpenVPN Connect, select **Import Profile** > **FILE** to upload the SSL VPN client configuration file (.ovpn file) downloaded in Step 3.

Linux client

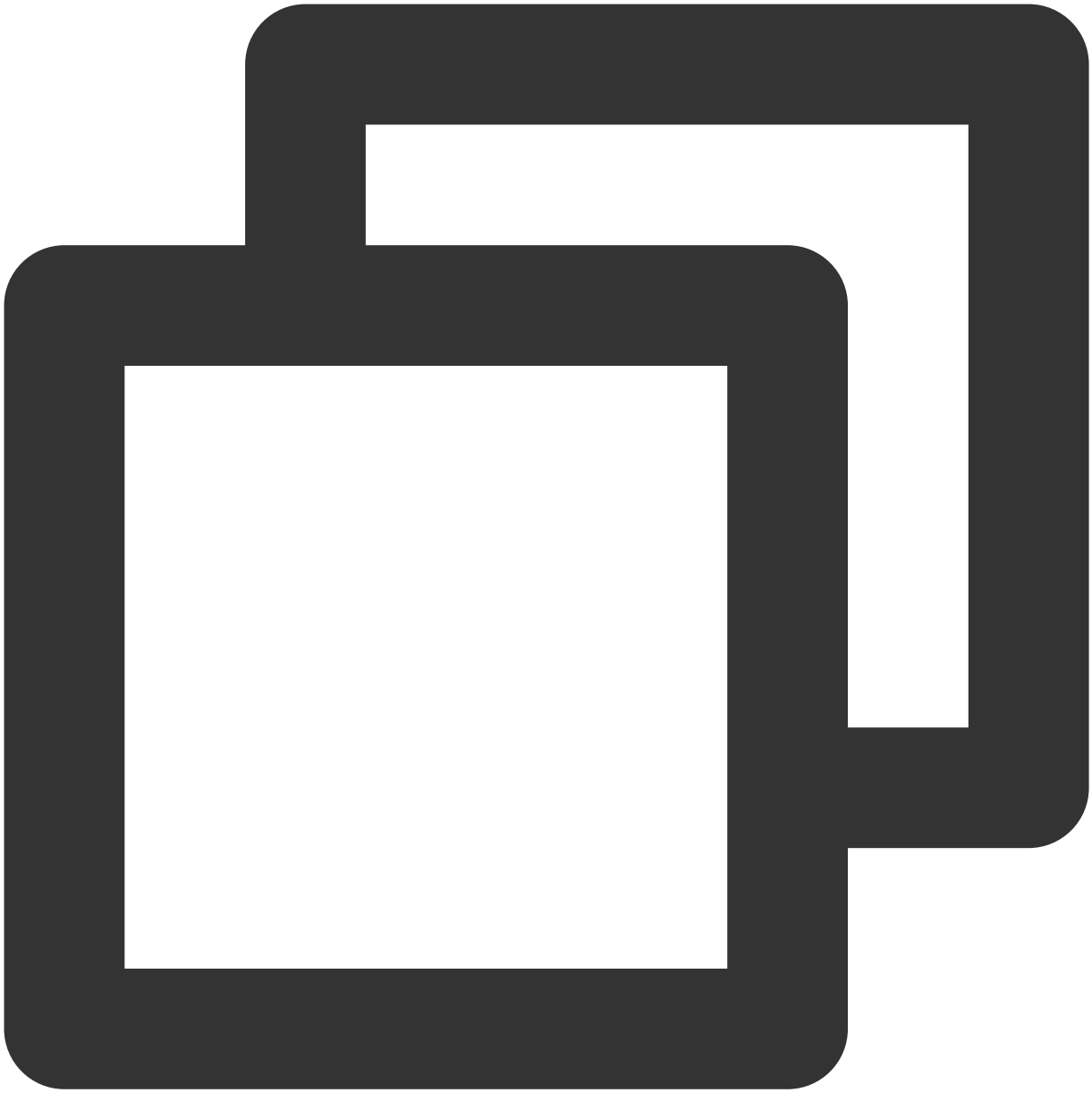
1. Open the command line window.
2. Run the following command to install OpenVPN Connect.

CentOS distribution



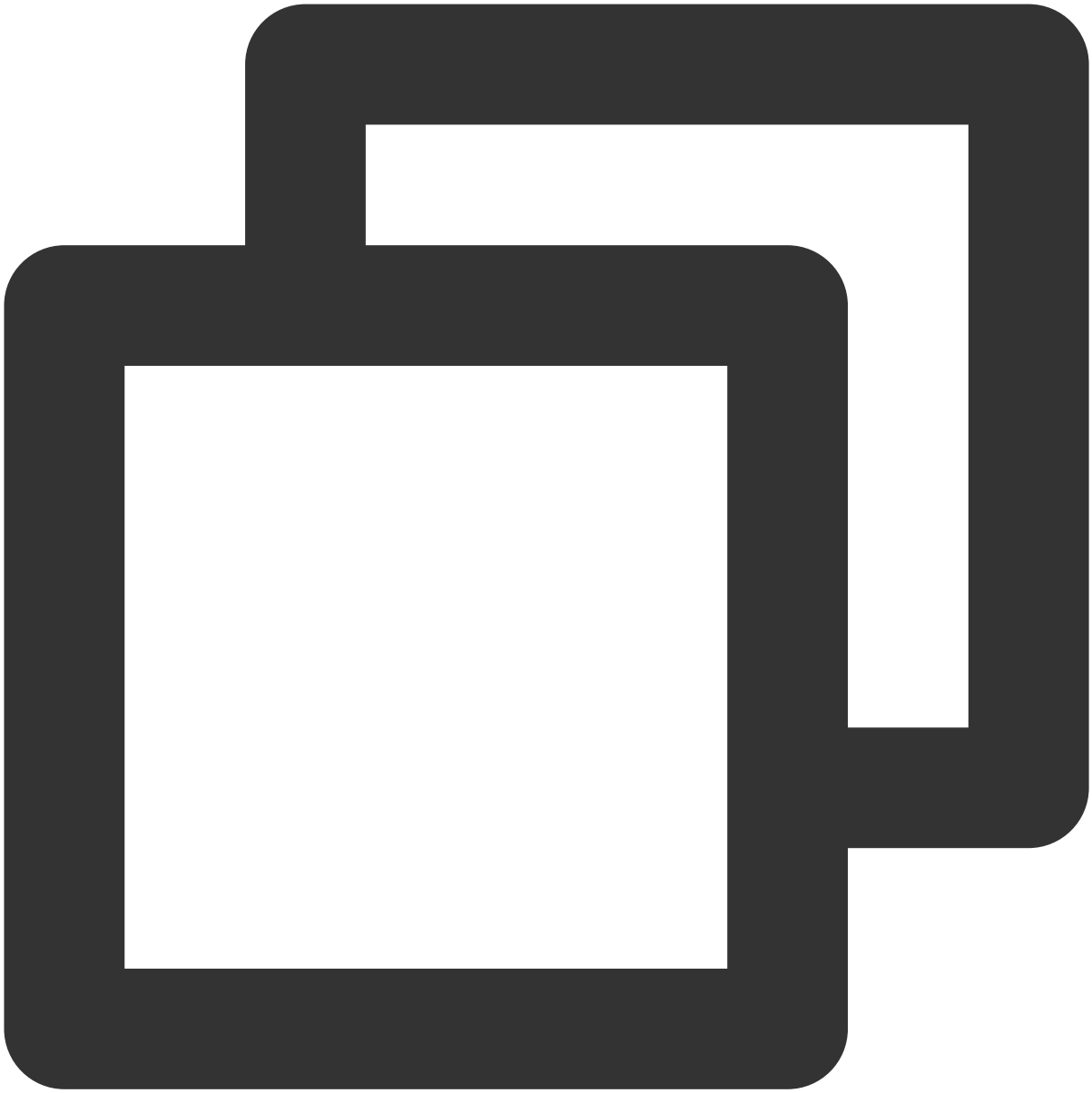
```
yum install -y openvpn
```

Ubuntu distribution



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

3. Extract the SSL VPN client certificate from the package downloaded in step 3 and copy it to the `/etc/openvpn/conf/` directory.
4. Enter the `/etc/openvpn/conf/` directory and run the following command to establish a VPN connection:



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

Step 6. Test the Connectivity

After establishing the SSL VPN connection between Tencent Cloud and the client, you can use `ping` to test the connection.

For example, you can use the CVM in the VPC to `ping` an IP address in the client IP range. If the ping is successful, the VPC and the client can communicate with each other.

SSL VPN Access Control Guide（okta）

Last updated：2024-05-24 10:58:52

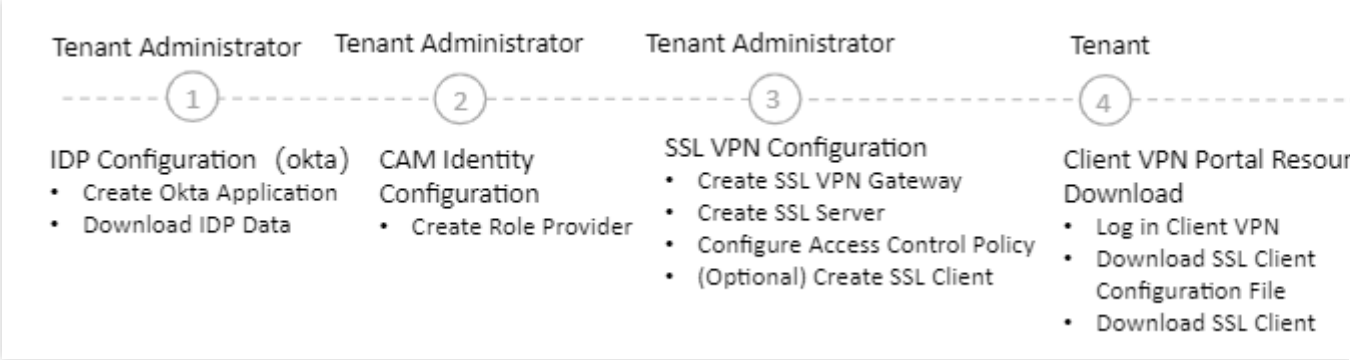
This document explains how to use a third-party IDP (Okta) and SSL VPN to implement access control. This will enhance the security of your businesses.

Note:

Currently, the SSO authentication feature grayscale, is only available in the São Paulo region. If needed, you can Submit a Ticket.

Supports mainstream third-party IDPs based on SAML2.0, such as Okta.

Operation Process



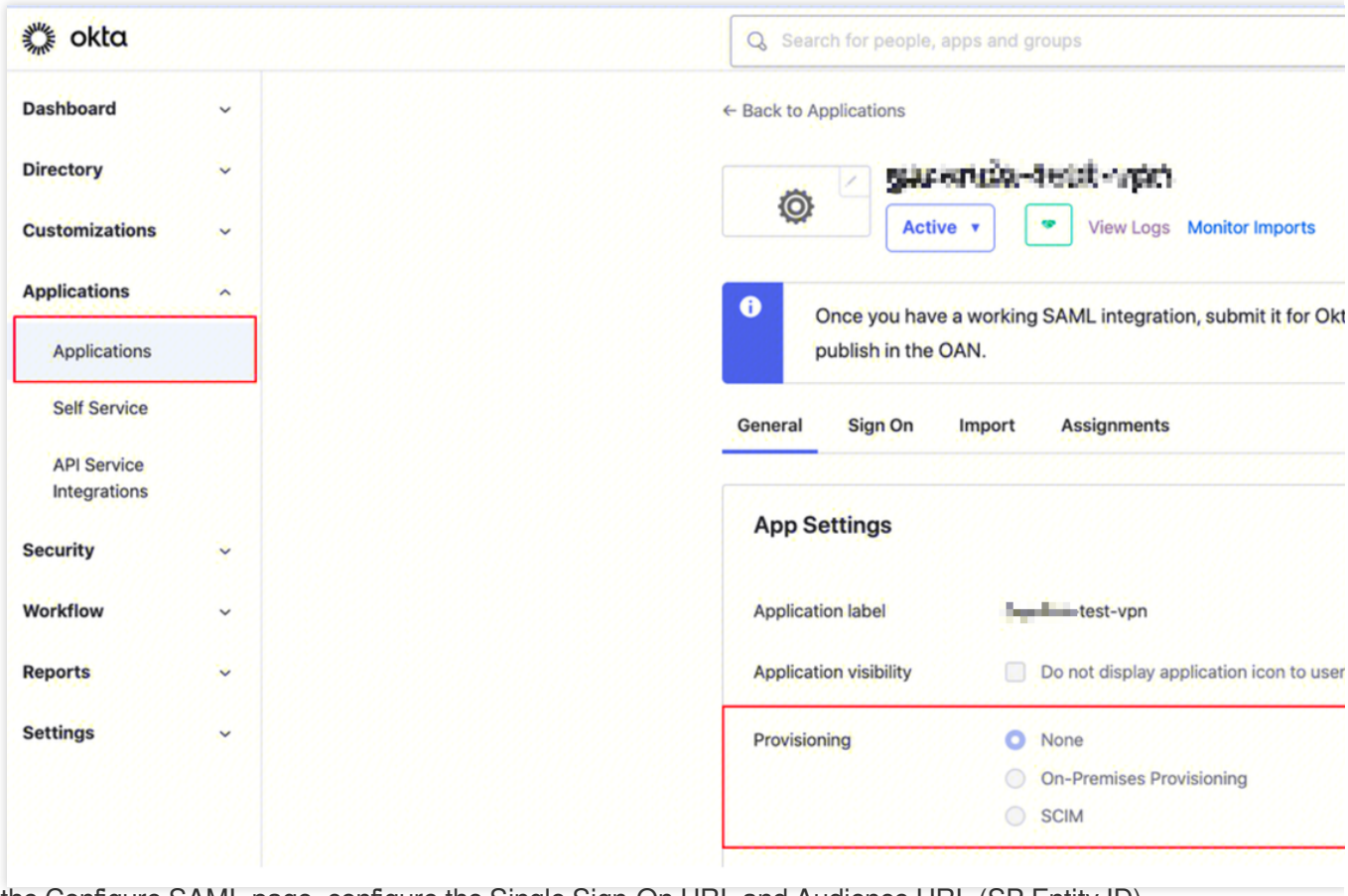
Step 1: (Tenant Admin) IDP Configuration (Okta)

Okta is a third-party IDP system. This node only introduces key parameter configuration. For specific directions of Okta, see the Okta official website or the Okta Single Sign-On.

Configure the trust relationship between Okta and Tencent Cloud to trust each other through this directions.

1. Log in to the Okta official website, and create an Okta application.

2. Go to the Applications page. Click on the application name, and click **Edit** on the General tab.

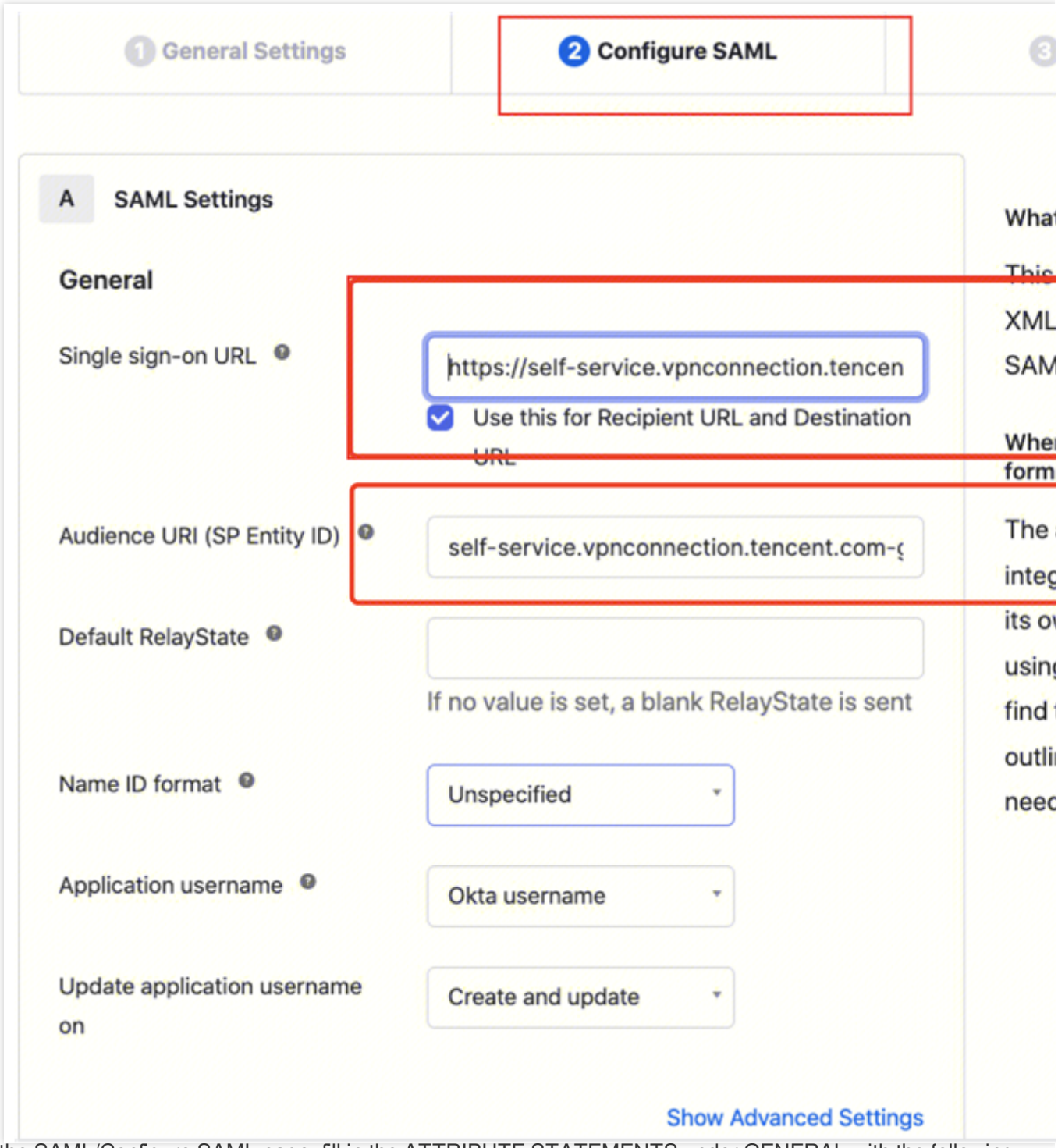


3. On the Configure SAML page, configure the Single Sign-On URL and Audience URL (SP Entity ID).

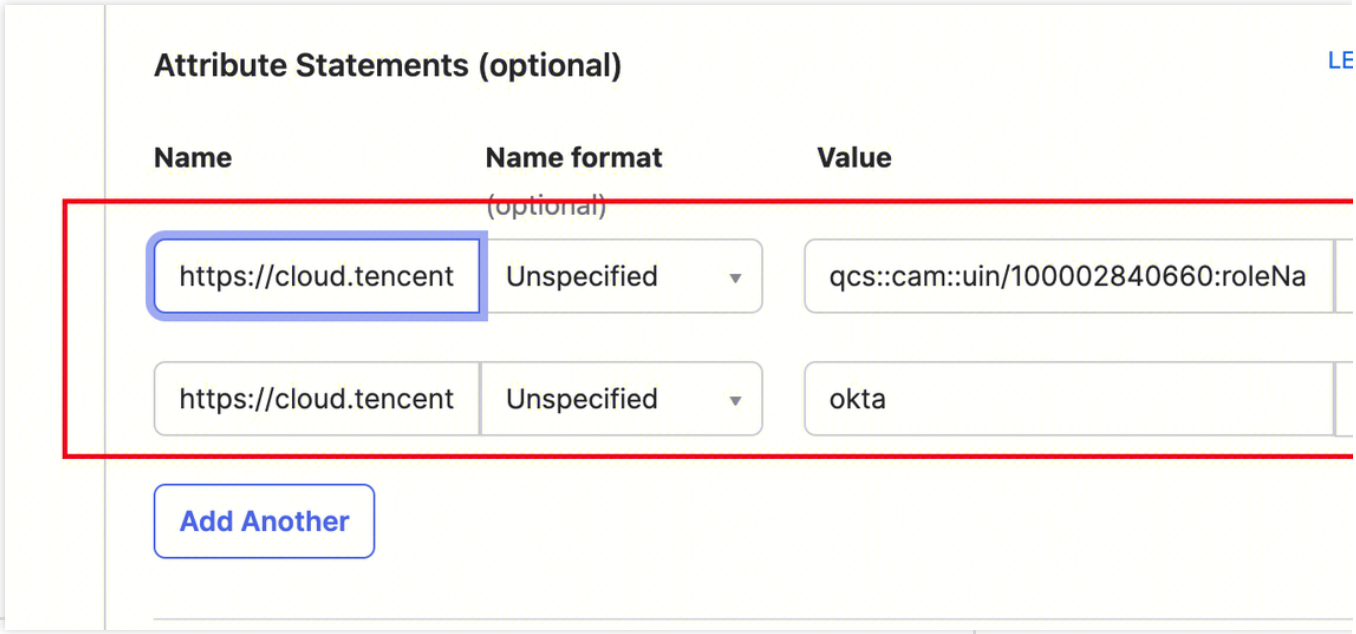
Note:

Single Sign-On URL: `https://self-service.vpnconnection.tencent.com/api/auth/sso-v2/saml` . This is a fixed value.

Audience URI (SP Entity ID): Tencent Cloud Client VPN Self-Service Portal.

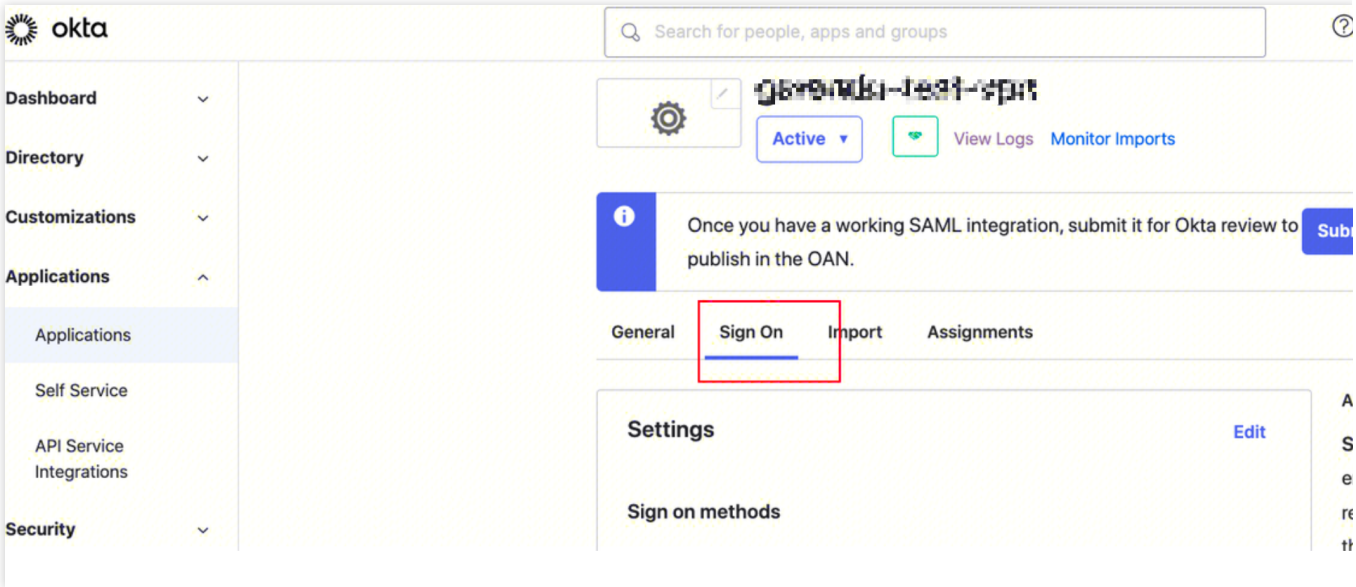


4. On the SAML/Configure SAML page, fill in the ATTRIBUTE STATEMENTS under GENERAL with the following information.

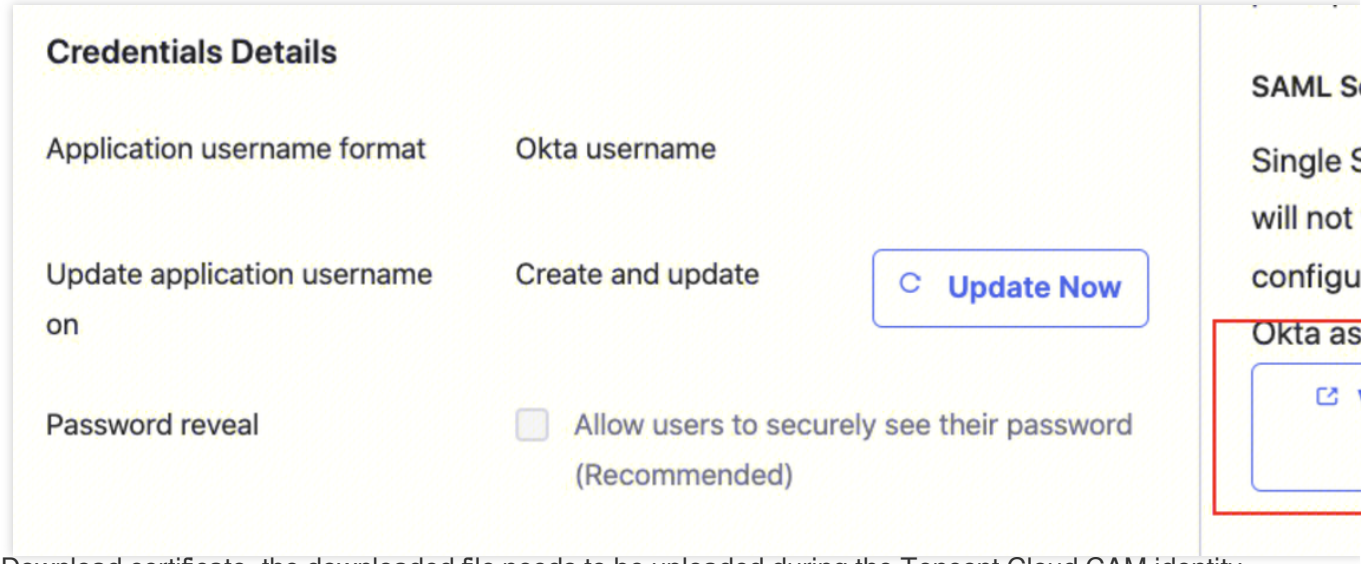


Name	Value
`https://cloud.tencent.com/SAML/Attributes/Role`	qcs::cam::uin/{AccountID}:rol provider/{ProviderName}
`https://cloud.tencent.com/SAML/Attributes/RoleSessionName`	okta

5. Go to the Sign on tab to generate and download the IDP's SAML-Metadata file.



Click View SAML setup instructions.

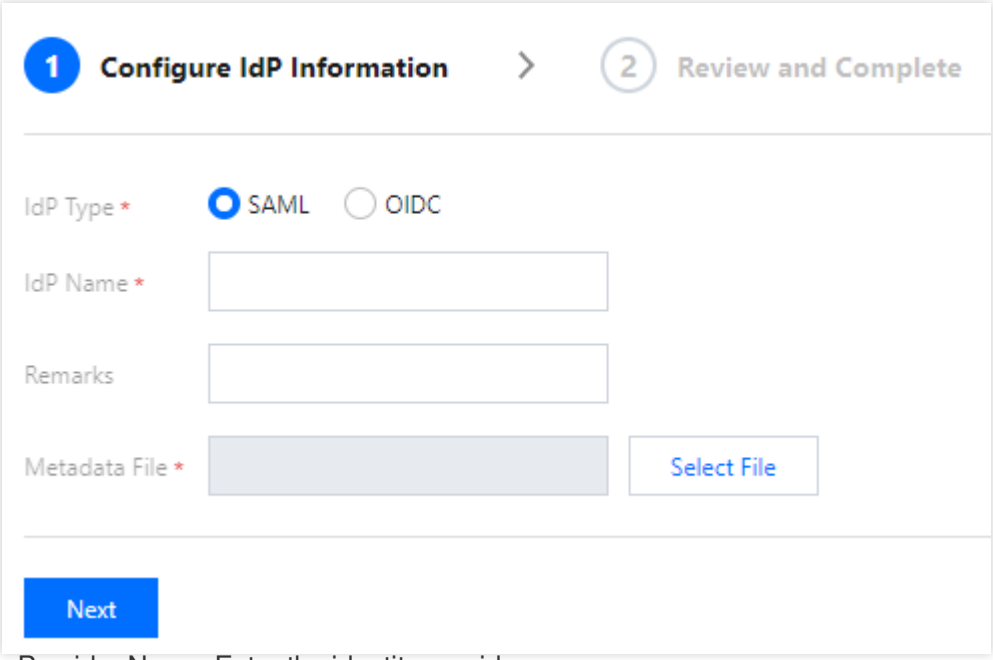


Click Download certificate, the downloaded file needs to be uploaded during the Tencent Cloud CAM identity configuration.

Step 2: (Tenant Admin) Creating a SAML IdP

1. Log in to the CAM Console. Go to the Identity Providers > Role-based SSO page. Click **Create IdP**.

2. On the Create Identity Providers page, choose the provider type as SAML and configure the provider information. Click **NEXT**.



Identity Provider Name: Enter the identity provider name.

Remark Info: Enter your memo information for the current identity providers.

Metadata Documentation: Refers to the file downloaded in Step 1: (Tenant Admin) IDP Configuration (Okta). You need to upload the SAML-Metadata documentation downloaded in the IDP configuration to the Metadata Documentation. If Metadata Documentation content validation is successful, a successful upload is allowed.

Step 3: (Tenant Admin) VPN Resource Configuration

Create an SSL VPN Gateway

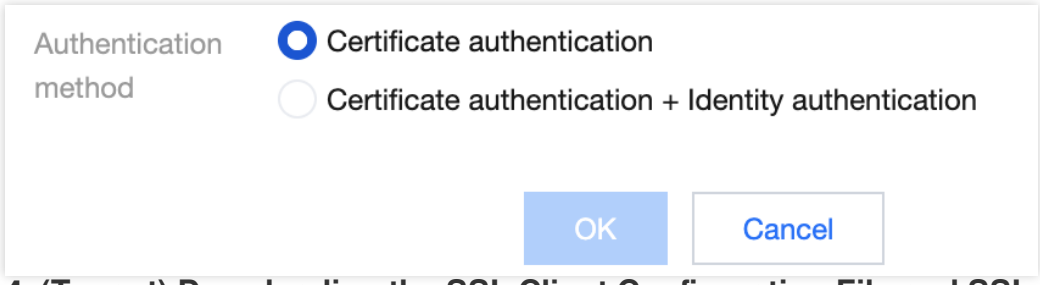
1. Log in to VPC Console. Choose **VPN Connections** > **VPN Gateway** in the left sidebar to enter the management page.
2. On the VPN Gateway Management page, click **New**. On the pop-up **Create VPN Gateway** page, configure the SSL VPN gateway according to the interface parameters.

Creating the SSL VPN Server

1. Choose **VPN Connections** > **SSL VPN Server** in the left sidebar to enter the management page.
2. On the SSL VPN server management page, click **Create**. In the pop-up **Create SSL VPN Server** dialog box, configure the SSL VPN server according to the interface parameters.

Authentication Method: By default, this method allows the SSL VPN server to be fully accessed by SSL clients.

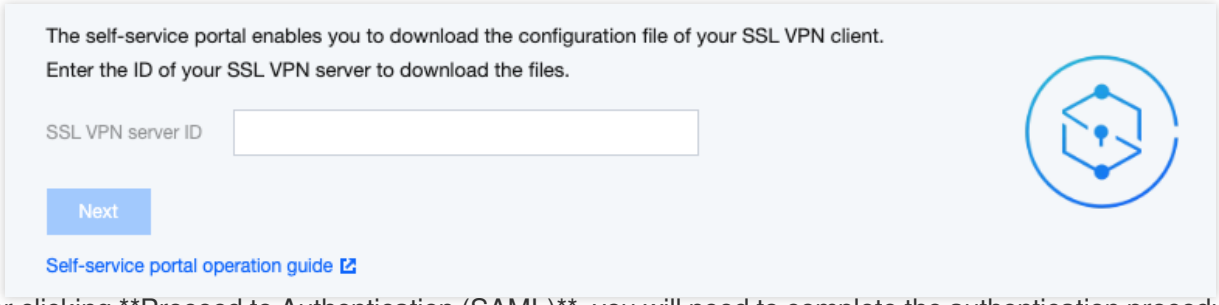
Identity Provider: The current provider is Tencent Cloud CAM. For more details, see Cloud Access Management usage instructions.



Step 4: (Tenant) Downloading the SSL Client Configuration File and SSL Client on the Client VPN Portal

1. Access the Tencent Cloud Client VPN Self-Service Portal through your local browser.
2. Enter the created SSL VPN Server ID in the input box on the row where the SSL VPN Server ID is located. Click **Next** to begin SSO authentication.

If you do not have or are unsure of the SSL VPN server ID, you can contact the tenant administrator to obtain it.



3. After clicking **Proceed to Authentication (SAML)**, you will need to complete the authentication procedure specified by your administrator.

If you do not have an account or encounter any problems during the authentication log-in process, contact your tenant administrator. Once you complete the authentication and successfully logged in, you will automatically log in to your business system.

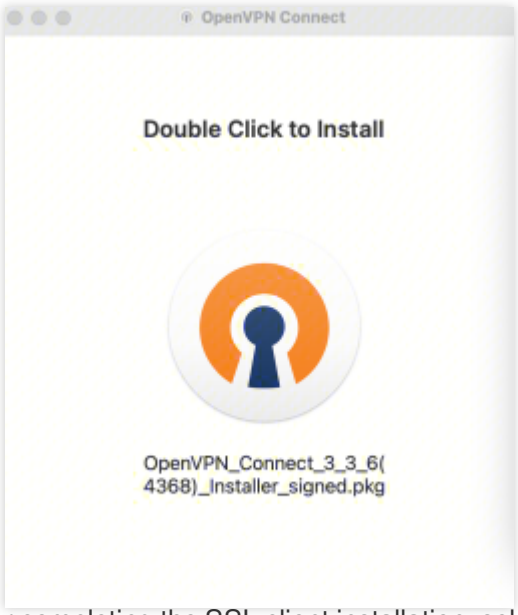
4. In the **Download SSL Client Configuration File** section, find the client configuration file you need to download and click **Download**.

Step 5: (Tenant) SSL Client Installation and Connection

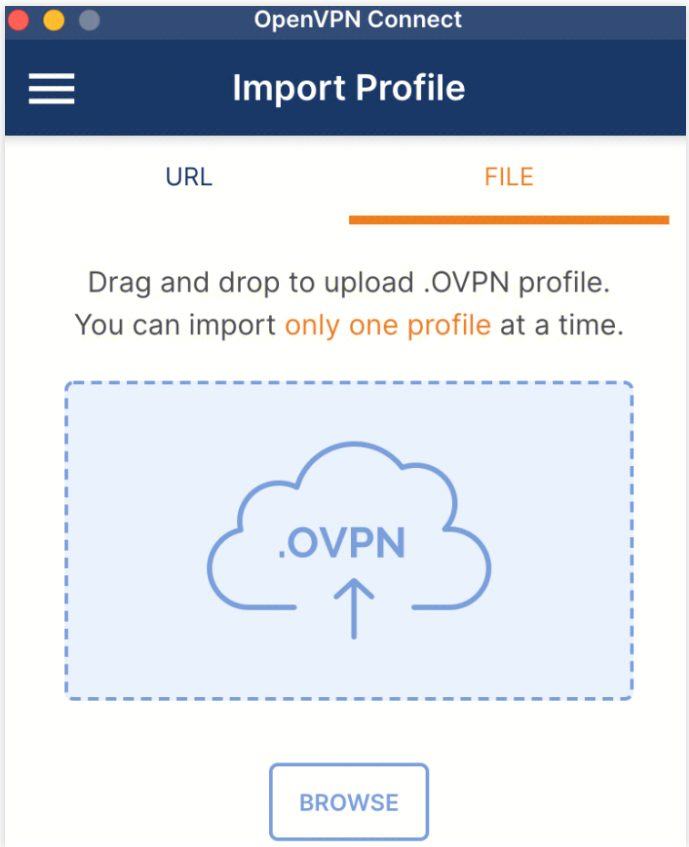
Note:

Use version 3.4.0 or later for the OpenVPN client.

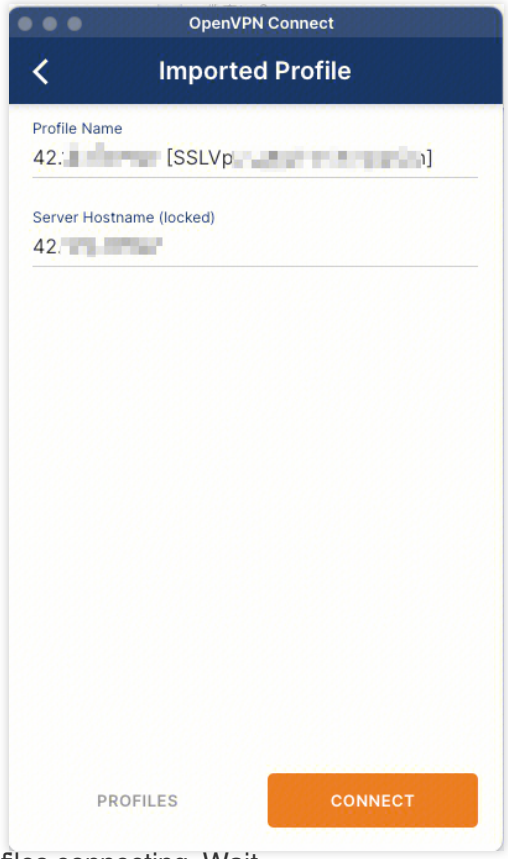
1. Decompress the installation package locally and double-click the installer to install the client as prompted.



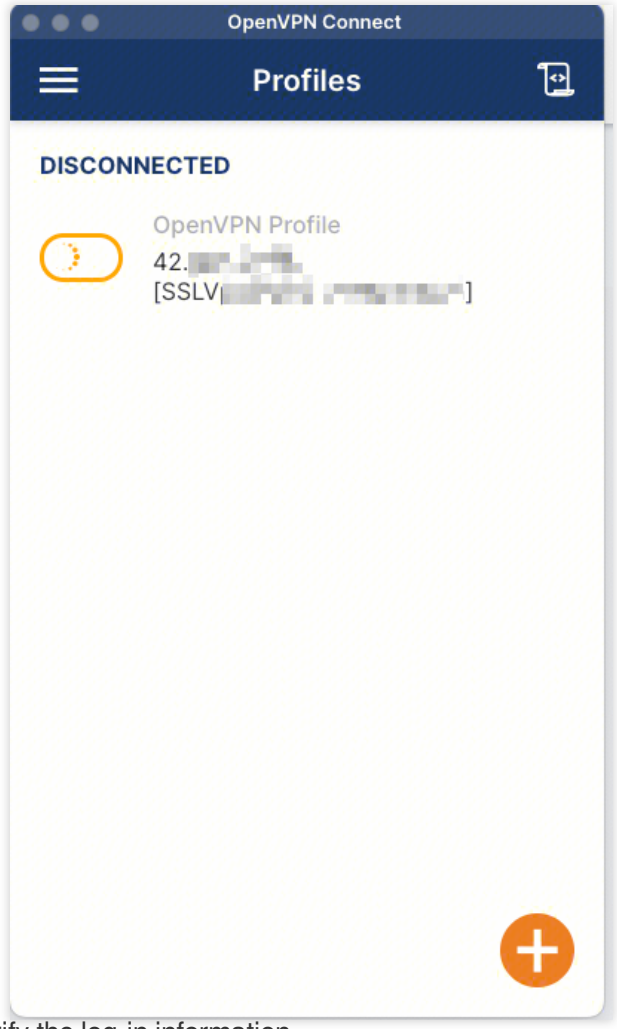
2. After completing the SSL client installation, select the FILE page in the Import Profile menu to upload the downloaded SSL client configuration file (in .ovpn format).



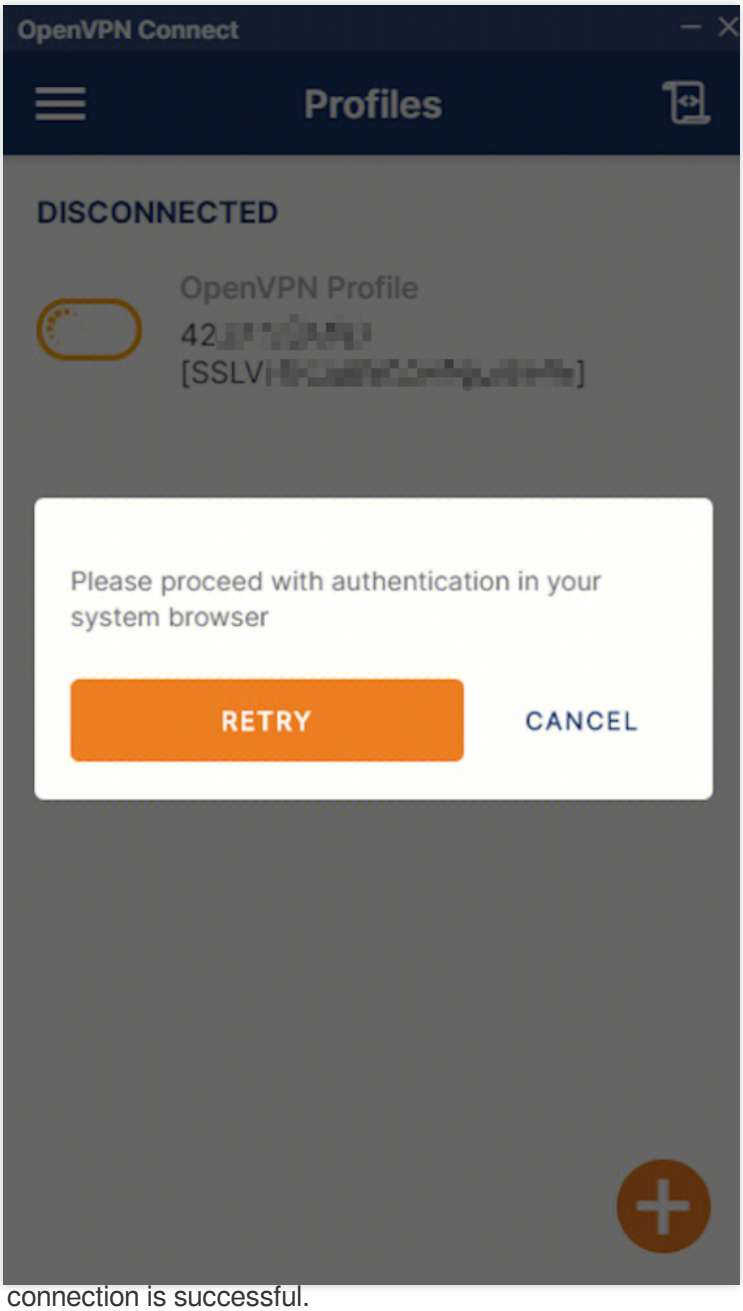
3. After successful upload, select connect to establish the connection.



4. Profiles connecting. Wait.



5. Verify the log-in information.



6. The connection is successful.