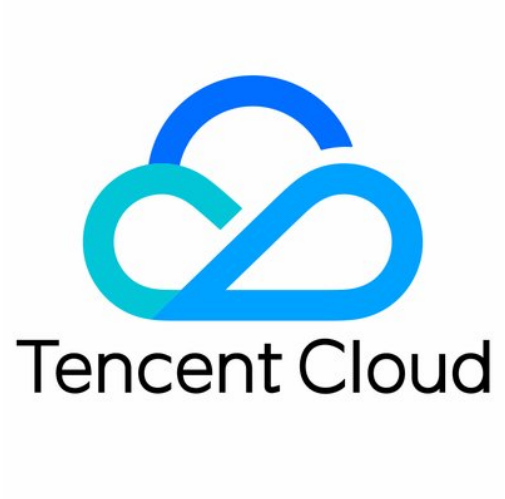
Direct Connect

Practical Tutorial

Product Documentation



Contents

Practical Tutorial
Connecting a Local IDC to CVM by Using a VPC NAT Gateway and Direct Connect

Last updated：2024-01-13 16:02:36

This document describes how to achieve resource access between an Internet Data Center (IDC) and VPC by using Direct Connect and the SNAT and DNAT features of a VPC NAT gateway.

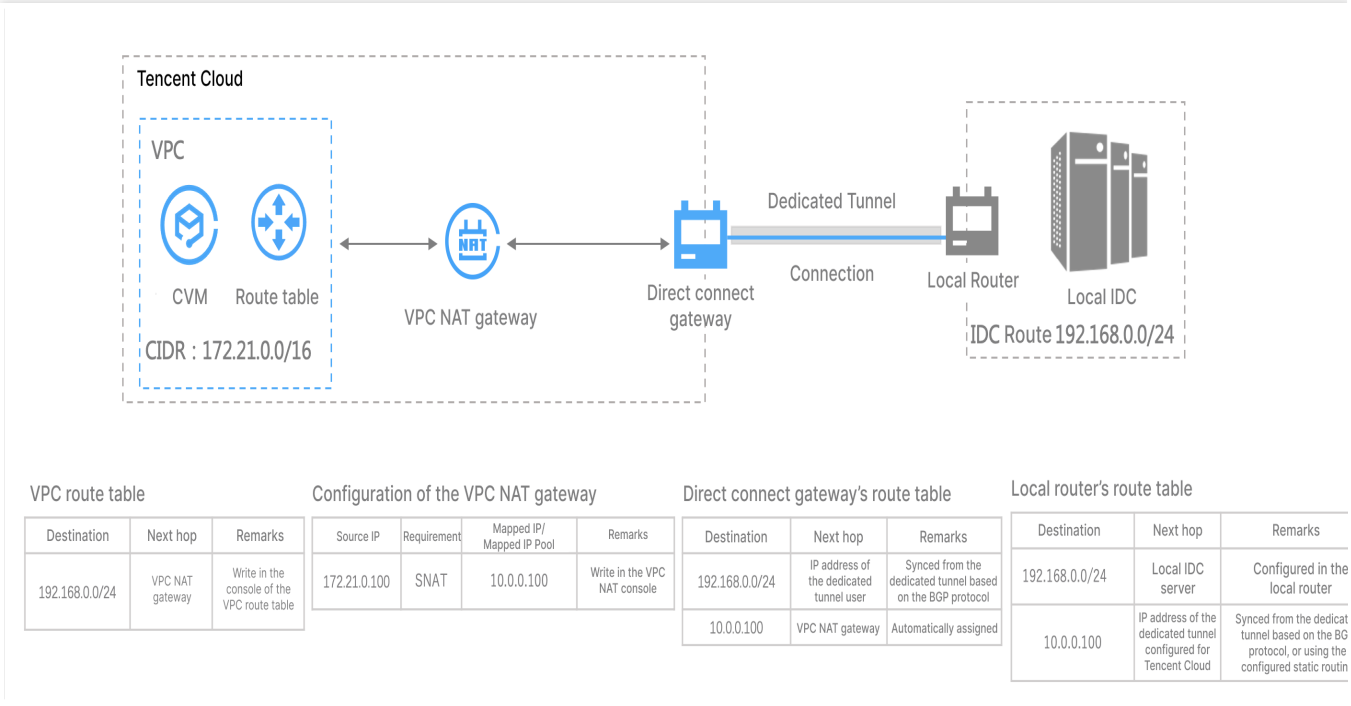
Note:

V3R2 NAT direct connect gateway is in beta testing. To use this feature, please submit a ticket.

VPC NAT gateway is in beta testing. To use this feature, please submit a ticket.

Scenarios

You can use Direct Connect and a VPC NAT gateway to build direct connections for resource access between Tencent Cloud and your IDC without causing conflicts between specified IP addresses.



VPC route table

Destination	Next hop	Remarks
192.168.0.0/24	VPC NAT gateway	Write in the console of the VPC route table

Configuration of the VPC NAT gateway

Source IP	Requirement	Mapped IP/ Mapped IP Pool	Remarks
172.21.0.100	SNAT	10.0.0.100	Write in the VPC NAT console

Direct connect gateway's route table

Destination	Next hop	Remarks
192.168.0.0/24	IP address of the dedicated tunnel user	Synced from the dedicated tunnel based on the BGP protocol
10.0.0.100	VPC NAT gateway	Automatically assigned

Local router's route table

Destination	Next hop	Remarks
192.168.0.0/24	Local IDC server	Configured in the local router
10.0.0.100	IP address of the dedicated tunnel configured for Tencent Cloud	Synced from the dedicat tunnel based on the BG protocol, or using the configured static routin

Prerequisites

You have built a connection. For more information, see Applying for Connection.
You have created a VPC.

Notes

You must configure network address mappings for the NAT gateway.
When you configure routing rules for a VPC NAT gateway, SNAT-Local-Layer-3, SNAT-Local-Layer-4, and DNAT-Peer-Layer-4 rules are mapped automatically. Peer-Layer-3 rules cannot be mapped. In addition, VPC CIDR is not published by default. Therefore, if you specify only Peer-Layer-3 rules, you must manually configure VPC CIDR routing for your IDC. We recommend that you use a Peer-Layer-3 rule with a Local-Layer-3 or Local-Layer-4 rule.

Directions

Step 1: Create a VPC NAT gateway

1. Log in to the NAT Gateway console.
2. In the left sidebar, choose **NAT Gateway** > **VPC NAT Gateway**, select the region and the VPC in which the gateway resides, and click **Create**.
3. Specify parameters and click **Activate now**. See the following figure:

Note:
For more information about the configuration, see NAT Gateway.

Step 2: Create an NAT direct connect gateway

1. Log in to the **Direct Connect Gateway console**.
2. In the **Create a direct connect gateway** window, enter a gateway name, select the zone, select **NAT** for **Associated Network**, and select an NAT instance to which the direct connect gateway associates.
3. Agree to the redundant gateway cleanup agreement and click **OK**.

Note:
For more information about parameter configuration, see Creating a Direct Connect Gateway

Step 3: Create a dedicated tunnel

The tunnels created on the connections vary depending on the access method. You can create tunnels of one of the following types as needed:
The tunnels created on your own connections are exclusive dedicated tunnels, which are applicable to scenarios with requirements for high-bandwidth access and exclusive access. For details, see Exclusive Dedicated Tunnel.
The tunnels created on our partners' connections pre-established in Tencent are shared dedicated tunnels, which are applicable to scenarios where there is no need for high-bandwidth access and the cloudification time is short. For

details, see Shared Dedicated Tunnel.

Step 4: Configure SNAT and DNAT routing rules for the VPC NAT gateway

1. Log in to the NAT Gateway console and click **VPC NAT Gateways** in the left sidebar. On the page that appears, click the ID of the created VPC NAT gateway.
2. On the details page of the VPC NAT gateway, configure SNAT and DNAT rules on the **SNAT** and **DNAT** tabs respectively. This document uses SNAT rules as an example.
3. On the **SNAT** tab, click **Create**. On the **Create SNAT rule** page, select **Layer-3** for **Mapping type**, enter the VPC IP address in the **Source IP** field, and enter an IP address or IP address pool in the **Mapped IP**/**Mapped IP pool** field as needed.

You can click **+ New line** to configure multiple SNAT routing rules.

4. Click **OK**.

Note:

For more information about parameter configuration, see Operation Overview.

Step 5: Configure routing policies in the VPC route table

1. Log in to the VPC console and go to the Route Tables page.
2. On the **Route tables** page, find the route table corresponding to your VPC and click the table name.
3. On the details page of the route table, click **+ New routing policies**. In the pop-up window, configure the routing policy.

Specify the IP range of your IDC for **Destination**, **VPC NAT gateway** for **Next hop type**, and the name of the VPC NAT gateway created in Step 1 for **Next hop**.

Note:

For more information about other VPC routing policies, see Managing Routing Policies.

Step 6: Configure the local IDC

Download the CPE configuration guide and follow the instructions for configuration.

Note:

For more information about parameter configuration, see Exclusive Virtual Interface.

Step 7: Test connectivity

Test whether CVM instances and your local IDC are connected.

1. Log in to an CVM instance in your VPC.
2. Run the ping command to test the IP address of the server in your local IDC. If ICMP packets are returned, the CVM instance is connected to the IDC.

Run the packet capture command on the server in your local IDC. You can see that the source IP address of the packets is the specified IP address after SNAT.

Note:

If no packets are returned, perform the following operations for troubleshooting:

Check the VPC route table. Ensure that you have specified the VPC NAT gateway for next hop. For more information, see Step 5.

Check whether you have configured an SNAT or DNAT rule. If no rules are configured, the connection fails. For more information, see Step 4.

Ensure that the status of the dedicated tunnel is **Connected**. The BGP status of Dedicated Tunnel 2.0 must be **established**.

If you have tried all above operations and the issue persists, please submit a ticket.

3. Log in to the server in your local IDC and run the `ssh root@NAT IP` command.

If packets are returned, the connection succeeds.

Hybrid Cloud Primary/Secondary Communication (DC and VPN)

Last updated：2024-01-13 16:12:04

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 in beta testing. To use this feature, 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 cannot be adjusted in the console. If you want to adjust the route priority, submit a ticket.

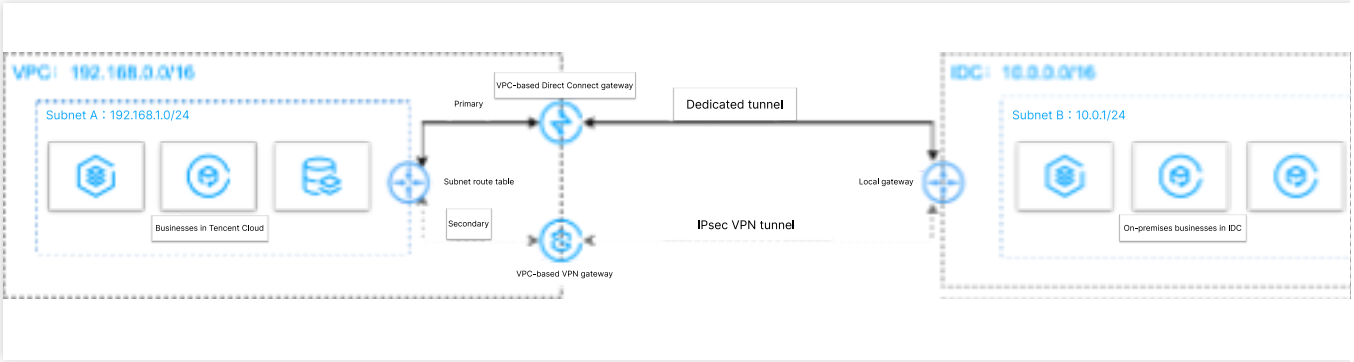
Currently, automatic switching is not supported. When a fault occurs, you must manually switch the route in the VPC.

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

Flowchart

1. Connect IDC to VPC through Direct Connect
2. Connect IDC to VPC through a VPN connection
3. Configure network probes
4. Configure an alarm policy
5. Switch between the primary and secondary routes

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** in 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 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 Tencent Cloud Observability Platform 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.

Best Practices on Direct Connect High Availability and Hybrid Cloud Network

Last updated：2024-01-13 16:02:36

Tencent Cloud direct connect maximizes the high availability of business in various failure scenarios, such as port exception/fiber optic component failure, network device failure, failure of data center at the access point etc. It provides four-line dual access point (recommended), two-line dual access point, two-line single access point and other network architectures, where, the four-line dual access point network architecture provides higher level of Tencent Cloud Direct Connect Service Level Agreement. In this document, we take four-line dual access point architecture as an example to describe the high availability design and practices of Tencent Cloud direction connect.

Network Architecture with High Availability

User IDC accesses at least two Tencent Cloud direct connect access points through connections to achieve high availability and load balancing at the physical level.
Direct connect gateway integrates with DSR clusters based on DSR system design. It acts as the bridge between Tencent Cloud and IDC to form a virtual dedicated tunnel together with the local router at IDC side and achieve resources intercommunication via Tencent Cloud VPC or CCN.
DSR clusters provide two Tencent Cloud border IP addresses to implement active-active routing system at the control plane. Thus, the local router on IDC side has created BGP neighbor adjacency with the two clusters respectively via BGP protocol to effectively ensure high availability of business in case of DSR cluster upgrade or single cluster failure and avoid impact on business caused by single BGP neighbor adjacency interruption and route convergence.
Meanwhile, DSR adjusts and removes exceptional service nodes dynamically through real-time monitoring mechanism in the cluster to ensure the availability of single cluster. It adopts large-scale cluster scaling technique to enable horizontal scaling among multiple clusters for the business to ensure availability across clusters.

Hot switching in case of failure

Switching in case of connection failure

The system switches the traffic to connection 2 automatically when it detects a failure in connection 1 to ensure normal operation of the business. The traffic will be switched back automatically when the failure is recovered.

Switching in case of exchange failure

The system switches the traffic to connection 2 automatically when it detects a failure in exchange 1 to ensure normal operation of the business. The traffic will be switched back automatically when the failure is recovered.

Switching in case of DSR failure

The system switches the traffic to connection 2 automatically when it detects a failure in the DSR cluster to ensure normal operation of the business. The traffic will be switched back automatically when the failure is recovered.

Switching in case of access point failure

The system switches the traffic to access point 2 automatically when it detects a failure in access point 1 to ensure normal operation of the business. The traffic will be switched back automatically when the failure is recovered.

Switching in case of over capacity

According to capacity planning, the usage of each connection is not allowed to be over 50%. If the usage of connection 1 is over 50%, the system will switch traffic to connection 2 automatically. Then, the traffic will be switched back to connection 1 when the usage is below 50%.

Limits and Suggestions for Practices

Network layer (dedicated tunnel)

BGP IP needs to be configured on both Tencent Cloud side and the user IDC side to establish a session, and BGP session must be kept in active-active status.
See the figure below for the configuration on Tencent Cloud side. For more information, see Exclusive Virtual Interface-Advanced Configuration.
BFD and NQA needs to be provided for health check to ensure robustness of the tunnel. For more information on the configuration of health check, see Health Check for the Dedicated Tunnel.

Physical layer (connection)

On the IDC side, users can use the same port of an edge device to connect primary/secondary connections to ensure high availability of the connections, or use two edge devices to connect primary/secondary connections.

Migrating Cross-Region Dedicated Tunnel to CCN

Last updated：2024-11-05 09:46:38

Background

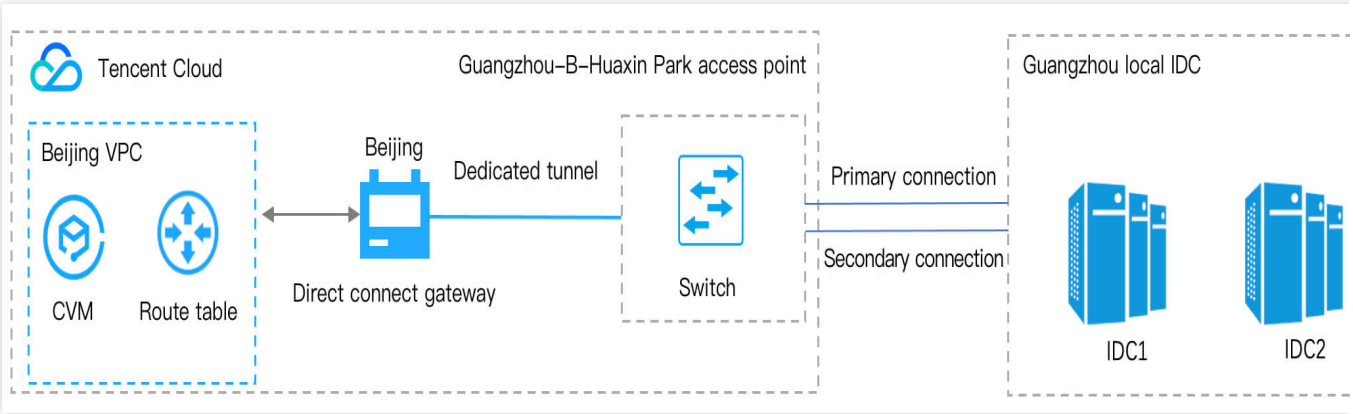
We plan to end the **cross-region dedicated tunnel** service of Direct Connect on December 31, 2022 (cross-region dedicated tunnel creation was not supported any more starting from September 2021). To ensure more stable and high-quality network operation of your business, your cross-region dedicated channels will be serviced by Tencent Cloud's Cloud Connect Network (CCN). For more information, see here. This document introduces how to migrate your cross-region dedicated channels to CCN.

Migration Scenario and Solution

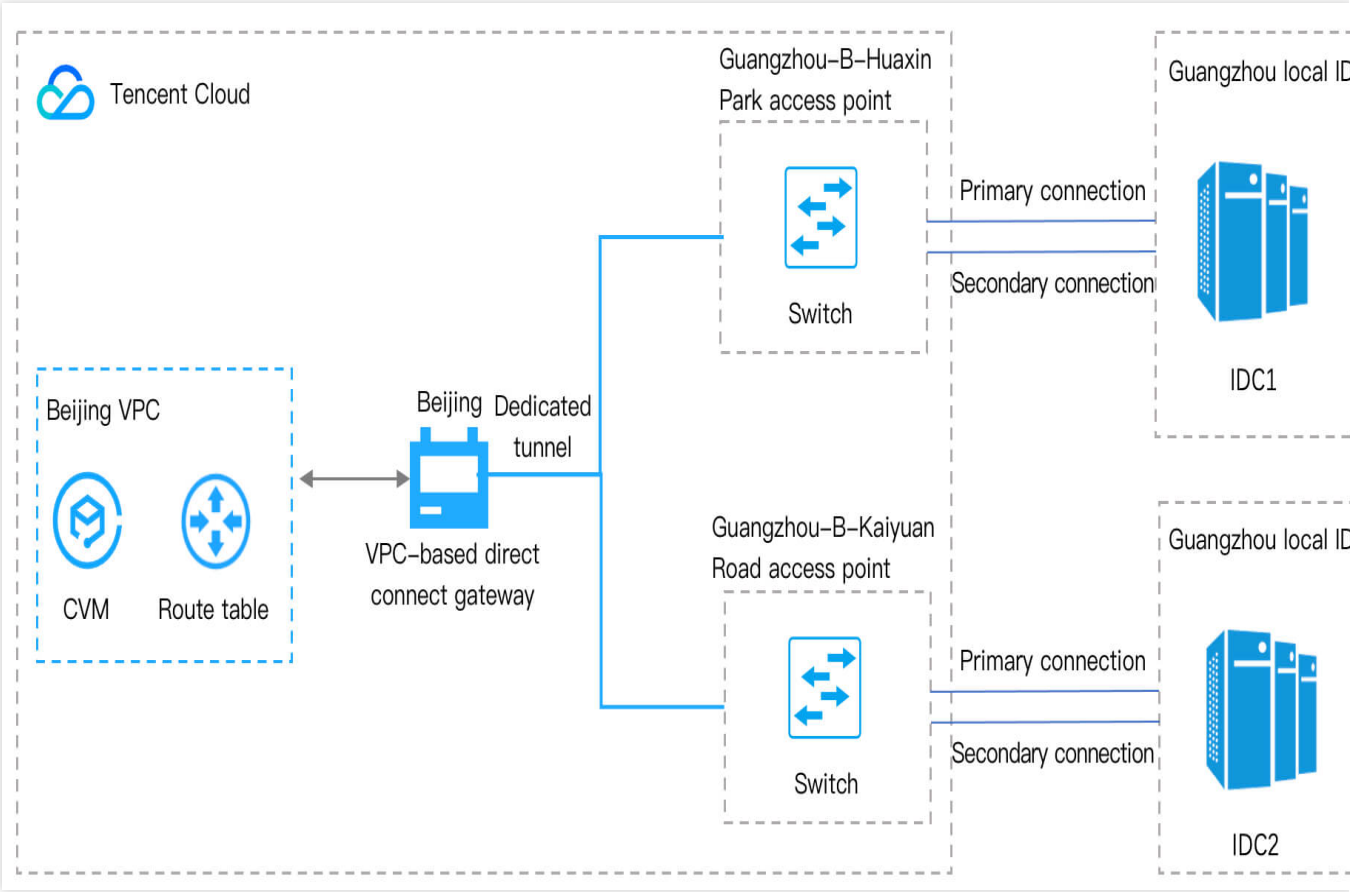
According to the region attributes of local IDCs, the scenarios for migrating cross-region dedicated channels to CCN are divided into two types, and the migration scheme varies according to the scenario.

Scenario 1: Local IDCs are deployed in the same region

Local IDCs connect to Tencent Cloud through a single access point



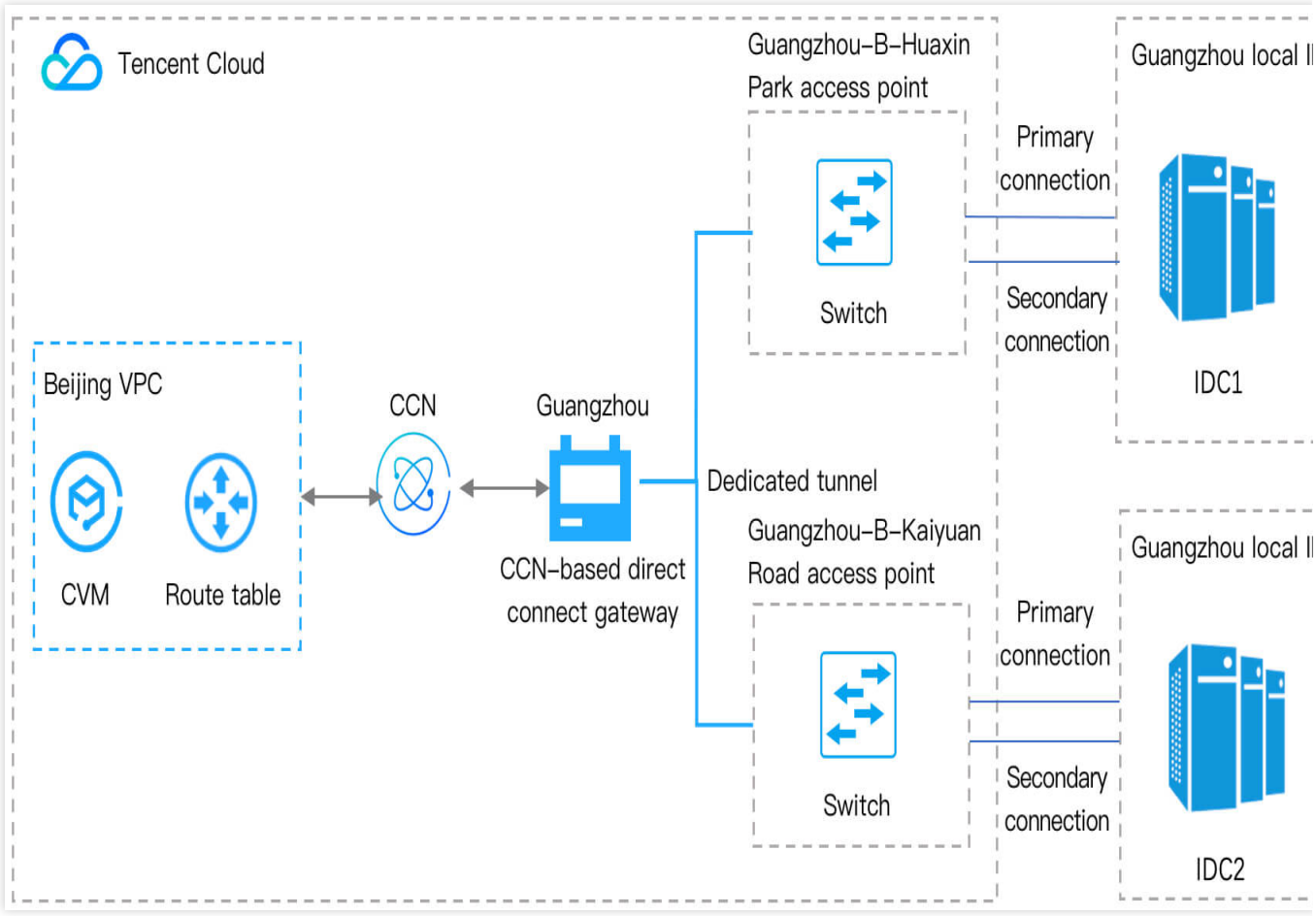
Local IDCs connect to Tencent Cloud through multiple access points



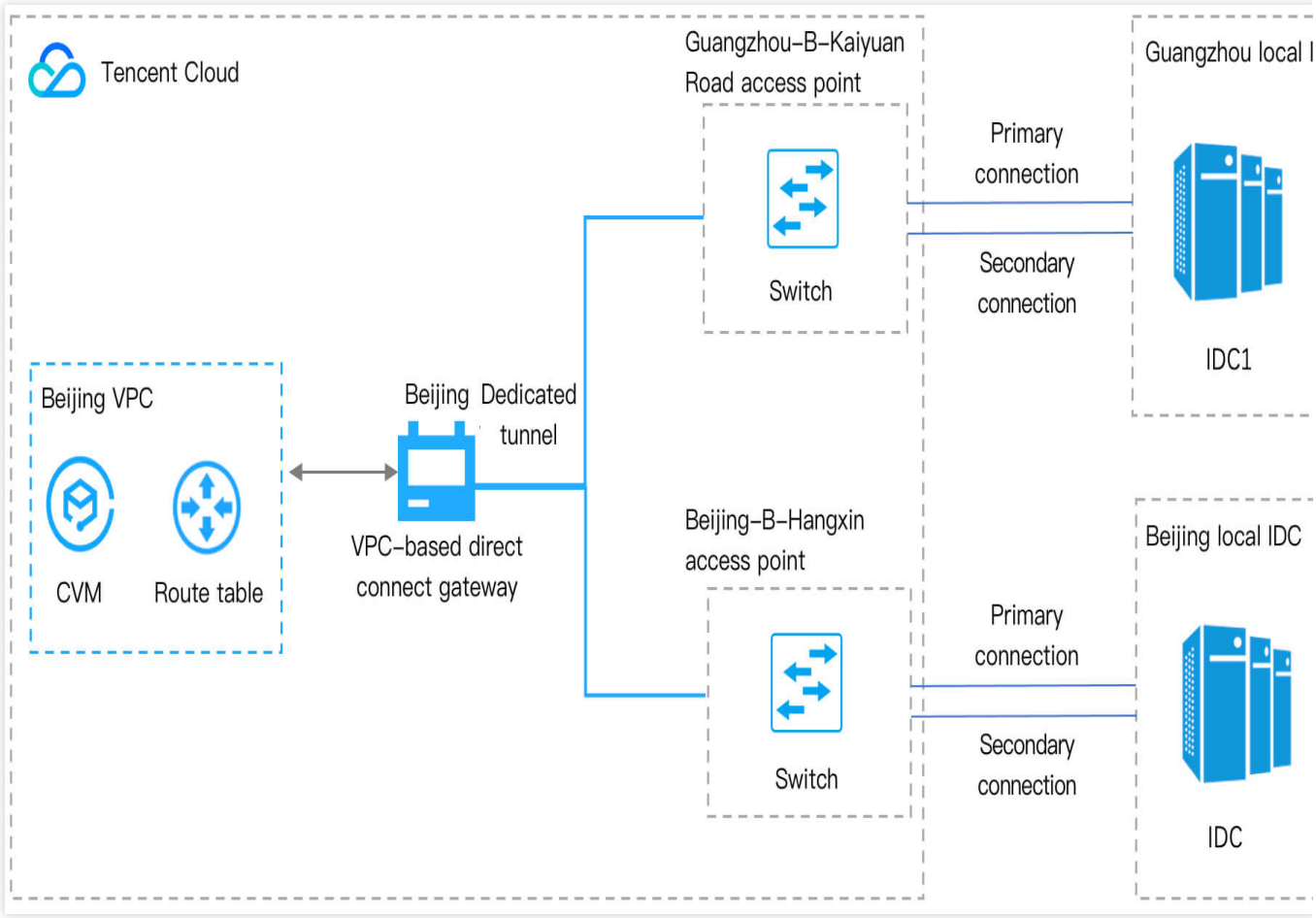
Solution

In a scenario where local IDCs are deployed in the same region, you need to create a CCN-based direct connect gateway and dedicated tunnel in the region where the connection access points reside. For more information, see Migration Process.

The switching aims to implement cross-region resource interconnection based on CCN, and the target networking after the switching is as follows.



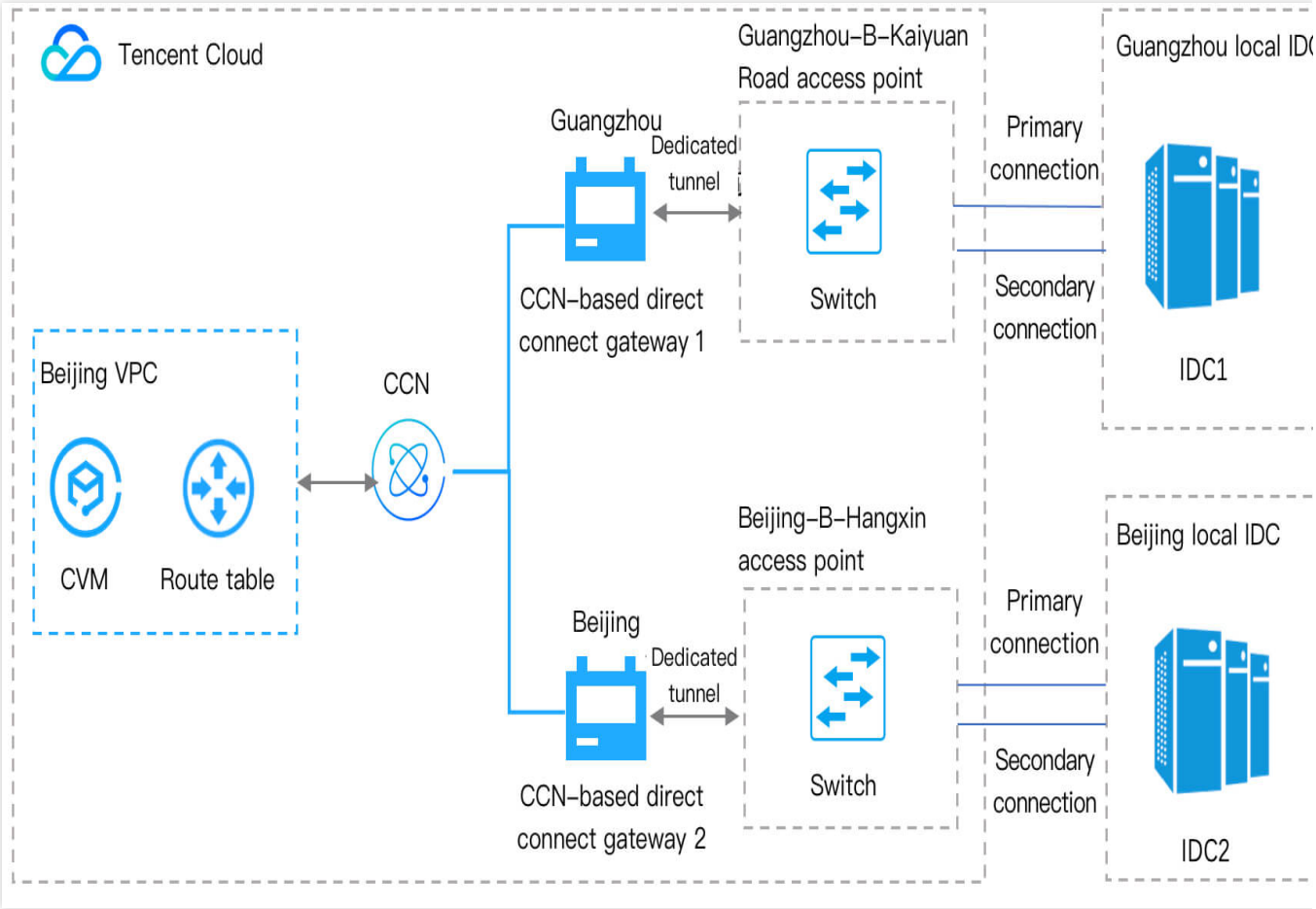
Scenario 2: Local IDCs are deployed in different regions



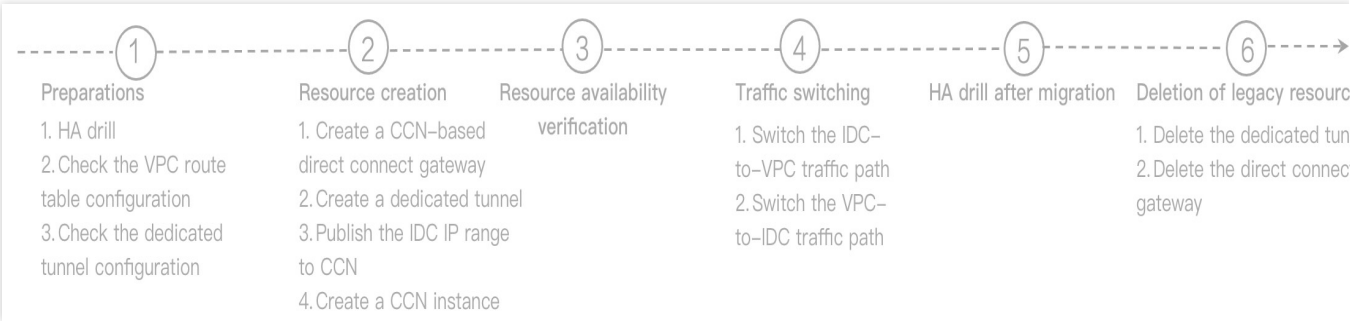
Solution

In a scenario where local IDCs are deployed in different regions, you need to create a CCN-based direct connect gateway and dedicated tunnel in each of the regions where the connection access points reside. For more information, see Switching Process.

The switching aims to implement cross-region resource interconnection based on CCN, and the target networking after the switching is as follows.



Migration Process



1. Preparations

1.1 Perform a high-availability (HA) drill: Before migrating cross-region dedicated tunnels to CCN, you are advised to perform an HA drill to ensure the HA of your business.

1.2 View the VPC route table configuration: View and note down the route table configuration, such as the VPC region and next hop, of the VPC where your current cross-region dedicated tunnel resides.

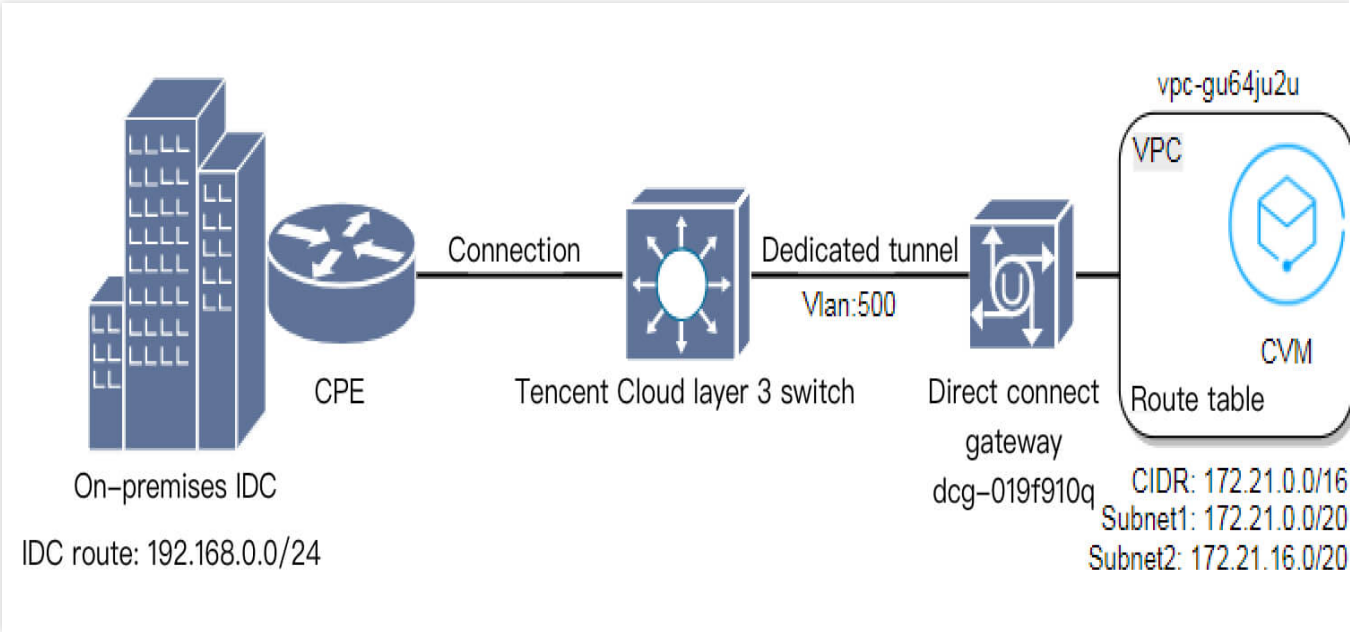
1.3 View the dedicated tunnel configuration: View and note down your current cross-region dedicated tunnel configuration, such as the dedicated tunnel ID, network region, peer IPs, and BGP ASN.
2. Resource creation
2.1 Create CCN-based direct connect gateways: According to your migration scenario, create CCN-based direct connect gateways for CCN interconnection.
2.2 Create CCN dedicated tunnels: After creating CCN-based direct connect gateways, you need to create corresponding CCN dedicated tunnels to connect the access points and gateways.
2.3 Publish IDC IP ranges to CCN: The direct connect gateways created in step 2.1 "Create CCN-based direct connect gateways" publish the IDC IP ranges obtained to CCN to enable the routes from IDCs to CCN.
2.4 Create a CCN instance: On the CCN side, create a CCN instance to mount the direct connect gateways.
3. Resource availability verification
On the Direct Connect side, check whether the basic configuration of the Direct Connect resources created in Resource creation. For example, check the connectivity of dedicated tunnels, BFD parameter settings, and whether direct connect gateways can obtain IDC routes.
4. Traffic migration
Note:
This step is to migrate your real traffic to CCN, and your business will be interrupted for a short time. We recommend performing the migration during off-peak hours. If you have any questions, submit a ticket.
4.1 Switch the IDC-to-VPC traffic path.
4.2 Switch the VPC-to-IDC traffic path.
5. HA drill after migration
To ensure the HA of your business, you are advised to perform an HA drill again after the business runs stably after traffic switching.
6. Deletion of legacy resources
After your business runs stably for about a week, delete the legacy direct connect gateway and dedicated tunnel.

Notes

If your current cross-region dedicated tunnel meets any of the following cases, submit a ticket before migration:
Your business is using a NAT direct connect gateway.
The BGP/BFD multi-hop feature is enabled for the dedicated tunnel.
The BGP route quota (100 routes by default) has been adjusted for the dedicated tunnel.
The static route quota (20 routes by default) has been adjusted for the dedicated tunnel.
`Local Preference` has been adjusted for the dedicated tunnel.
The direct route redistribution feature is enabled for the dedicated tunnel (if this feature is enabled, you can directly access IPs over the dedicated tunnel from a VPC).
Other special networking scenarios or requirements.

Migration Example

This example shows how to migrate business from a local IDC to the cloud by using a connection. The topology is as follows:



Preparations

1. (Optional) Perform an HA drill.

To ensure business availability and rollback capability during switchover, you are advised to perform a fault redundancy drill before the switchover. That is, perform a primary/secondary connection and loaded line switchover to ensure business availability. Perform subsequent cutover operations after the drill is completed.

2. View the VPC route configuration.

2.1 Log in to the VPC console.

2.2 Click **Route Table** in the left sidebar, select the VPC region, select the VPC, and click the **route table ID**.

2.3 On the page displayed, you can view the VPC route table configuration details.

3. View the dedicated tunnel configuration.

3.1 Log in to the Direct Connect console.

3.2 Click **Exclusive virtual interface** in the left sidebar, and click the **dedicated tunnel ID** to enter the dedicated tunnel details page.

4. Click the **Advanced Configuration** tab to view the advanced configuration of the dedicated tunnel.

Based on the preceding information, VPC traffic destined for 192.168.0.0/24 will be routed to the direct connect gateway dcg-019f9l0q based on the VPC route table policy.

Resource creation

Step 1. Create CCN-based direct connect gateways

1. Log in to the **Direct Connect Gateway console**.
2. In the upper-left corner of the **Direct Connect Gateway** page, select the region where the connection access point resides.
3. Click **+ New**, enter the direct connect gateway name, and set **Associate Network** to **CCN**. This document uses "dcg-dx8kvqto" as an example. Note that CCN-based direct connect gateways currently do not support the NAT type. For more information, contact your Tencent Cloud rep or submit a ticket for consultation.
4. Click **OK**.

Note:

The CCN-based direct connect gateway and the connection access point must be in the same region.

Step 2. Create CCN dedicated tunnels

1. Log in to the Direct Connect console.
2. Choose **Exclusive virtual interface** in the left sidebar and click **+ New**.
3. On the **Basic configuration** page, set parameters as needed. This document uses "test" as an example.

Note:

Connections: Use the original connection whose ID is `dc-dqggvxad` .

Access Network: Select **CCN**.

Direct Connect Gateway: Select the CCN-based direct connect gateway "dcg-dx8kvqto" created in step 1.

4. Click **Next**. On the **Advanced configuration** page displayed, enter the VLAN ID. This document uses "501" as an example.

Note:

1. **VLAN ID** must be the new ID.
2. Cloud peer IP1/IP2 and CPE peer IP must be new interconnection IPs.

5. Click **Next**, configure the IDC device, and click **Submit**.

Step 3. Publish IDC IP ranges to CCN

1. Log in to the Direct Connect Gateway console. Click the ID of the direct connect gateway created in Step 1 to enter the details page of the direct connect gateway instance. Click the **Publish IP Range** tab and click **Create**.
2. On the page displayed, enter the IDC IP range and click **Save**. This document uses "192.168.0.0/24" as an example.
3. After successful saving, you can view the newly added IDC IP range.

Note:

1. You can use either the custom mode (formerly named "Static") to add an IDC IP range or the auto-propagation mode (formerly named "Dynamic") to publish an IDC IP range.
2. If you use the auto-propagation mode to dynamically report routes, the report delay is about one minute during the convergence process.
3. To use the auto-propagation mode to sync IDC routes, submit a ticket.

Step 4. Create a CCN instance

1. Log in to the CCN console, click **+ New**, set parameters as needed, and click **OK**. This document uses "ccn-msg8kju5" and "vpc-gu64ju2u" as examples.
2. After the CCN instance is created, click the CCN instance ID on the CCN list page to enter the CCN instance details page. This document uses "ccn-msg8kju5" as an example.
3. On the CCN instance details page, click the bandwidth management tab and purchase cross-MLC-border bandwidth traffic.
4. Click **Route Table**.

Note:

For traditional dedicated tunnels, VPCs publish CIDR blocks to IDCs but publish VPC subnets to CCN instances.

Resource availability verification

After resource creation, you need to verify the basic configuration and business availability on the Direct Connect side.

1. Verify the dedicated tunnel connectivity.
 On the customer-premises equipment (CPE), check whether the BGP neighbor adjacency is established successfully.
2. Verify the BFD parameter settings.
 On the CPE, check whether the BFD session is created and whether parameters are correctly set.
3. Verify whether the direct connect gateway receives route entries from IDCs properly.
 On the direct connect gateway details page, check whether IDC routes to the cloud are correctly synced to the direct connect gateway.

Traffic switching

Switch the IDC-to-VPC traffic path

1. Log in to the CCN console.
2. Click the test CCN instance ("ccn-msg8kju5" in this example) to enter the instance details page. Click the **Associated Instances** tab, click **Add an instance**, and set parameters as needed. This document uses "Direct Connect Gateway", "Beijing", and "dcg-dx8kvqto" as examples.
3. Click **OK**. The instance whose ID is dcg-dx8kvqto is successfully associated with the CCN instance.
4. Click **Route Table**. The route table of the CCN instance is as follows.

Note:

1. If the dedicated tunnel uses the static routing mode, and you want to switch IDC-to-VPC traffic to a CCN dedicated tunnel path, you only need to direct CPE routes to the new sub-interface CCN dedicated tunnel.
2. If the dedicated tunnel uses the BGP routing mode, there are two cases if you switch to CCN:
2.1 If the direct connect gateway was created after September 15, 2020, the CCN instance sends a VPC CIDR block to the direct connect gateway, and the original cloud tunnel also sends a VPC CIDR block to the IDC, the local router obtains the VPC CIDR block based on the BGP protocol. You need to manually enable or disable the VPC or direct

connect gateway route in the CCN instance to control the IDC-to-VPC traffic path. For more information, see Direct Connect Gateway Overview.
2.2 If the direct connect gateway is created before September 15, 2020, the CCN instance sends a subnet CIDR block to the direct connect gateway, and the local router obtains the subnet CIDR block based on the BGP protocol. The original cloud tunnel sends a VPC CIDR block to the IDC, and the local router obtains the VPC CIDR block based on the BGP protocol. According to the rule where the route with the longest mask will be matched, IDC-to-VPC traffic will be automatically switched to the CCN instance. For more information, see Direct Connect Gateway Overview.

Switch the VPC-to-IDC traffic path

1. Click the route table whose ID is `rtb-2kanpxjb` and view the VPC route table policy changes. The VPC can automatically sync the CCN route table, and equivalent routes added later are disabled by default. The original dedicated tunnel is still used as the VPC-to-IDC traffic path.
2. Disable the routing policy of the original direct connect gateway and enable the routing policy where the next hop is CCN.Now, the VPC-to-IDC traffic path is switched to the CCN dedicated tunnel.

Note:

When changing the routing policy, the VPC-to-IDC traffic is interrupted. To ensure business security, you need to perform the operation in a time window where the business can be interrupted.
To perform a smooth switchover, perform the steps below:
2.1 Split the IDC route into two detailed routes: In this example, split 192.168.0.0/24 into 192.168.0.0/25 and 192.168.0.128/25.
2.2 Add the two detailed routing policies to the VPC route table.
2.3 The VPC-to-IDC traffic will choose the 25-bit mask detailed routing policy. Now, the routing policy where the next hop of the destination IP range 192.168.0.0/24 is the direct connect gateway is invalid, and you can disable or delete the routing policy.
2.4 Enable the routing policy where the next hop is the CCN IP range 192.168.0.0/24 in the VPC route table. Then, the VPC-to-IDC traffic still chooses the detailed route routing policy of the original direct connect gateway.
2.5 Disable or delete the routing policies of the detailed routes one by one. Then the VPC-to-IDC traffic will be switched to the CCN tunnel accordingly.

HA drill after migration

After the preceding steps, the cross-region dedicated tunnel business is completely switched over to the CCN instance. After observing the business for a period of time, you can perform a fault redundancy drill to ensure HA of the primary/secondary connections and loaded connections.

Deletion of legacy resources

After the HA test, observe the business for about one week. If the network is stable, delete the legacy dedicated tunnel and direct connect gateway resources.

Migrating IDC to the Cloud Through CCN

Last updated：2024-11-05 09:46:38

Step 1: Create a CCN-based Direct Connect Gateway

1. Log in to the VPC console and click **Direct Connect Gateway** on the left sidebar.
2. Click **+New**.
3. In the pop-up window, enter a gateway name, select **CCN** for **Associate Network**, leave **CCN instance** empty, and click **OK**.

Step 2: Add an IP Range to Publish to the Direct Connect Gateway

1. Locate the direct connect gateway just created and click the **ID/Name** to access its details page.
2. Select the **Publish IP Range** tab.
3. Click **Create** and enter a published IP range.

Step 3: Create a CCN Instance

For more information , see Creating a CCN Instance.

Step 4: Create a Dedicated Tunnel to Connect the CCN-based Direct Connect Gateway

1. Log in to the Direct Connect console and click **Dedicated Tunnels** on the left sidebar.
2. Click **+New**.
3. In the pop-up window, enter relevant information as prompted. Select **CCN** for **Access Network** and then select the CCN-based direct connect gateway just created.

Step 5: Associate a Network Instance

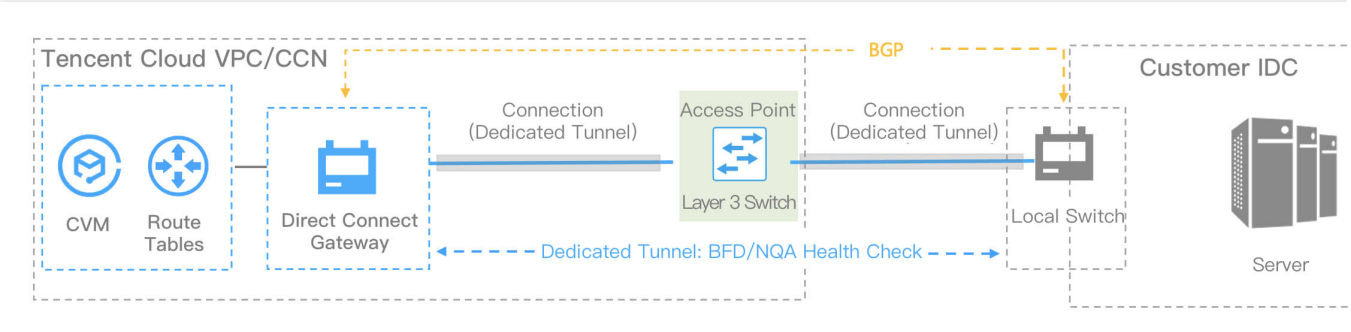
Associate the network instances (including VPC and direct connect gateway) with the CCN instance for interconnection. For detailed directions, see Associating Network Instances.

Accelerating Routing Convergence Through BGP+BFD (Layer 3)

Last updated：2024-11-05 09:46:38

This document describes how to accelerate routing convergence between customer IDC and private network by initiating BGP routing protocol on the local IDC switch and configuring bidirectional forwarding detection (BFD) on Tencent Cloud direct connect gateway.

Background



Note:

In a connection using static routes, we recommended that you use static routes and BFD/NQA to achieve route convergence.

The connection connects the IDC switch and the layer 3 network sub-interface of Tencent Cloud switch, thereby connecting IDC and Tencent Cloud network.

Implement mutual access to resources through VPC/CCN.

Implement routing convergence through BGP+BFD/NQA.

Prerequisite

You have built a VPC as instructed in Building Up an IPv4 VPC.

You have applied for a connection as instructed in Applying for Connection and completed the preparatory construction.

Configuration Guide

Step 1. Create a direct connect gateway

For more information, see Creating a Direct Connect Gateway.

Step 2. Create a dedicated tunnel

The tunnels created on the connections vary depending on the access method.
The tunnels created on your own connections are exclusive dedicated tunnels, which are applicable to scenarios with requirements for high-bandwidth access and exclusive access. For more information, see Exclusive Virtual Interface.
The tunnels created on our partners' connections pre-established in Tencent are shared dedicated tunnels, which are applicable to scenarios where there is no need for high-bandwidth access and the cloudification time is short. For more information, see Shared Dedicated Tunnel.

Step 3. Configure health check

For more information, see Dedicated tunnel health check.

Step 4. Completing the IDC local configuration as instructed in Huawei NE Series Routers

This document takes Huawei CE switch as an example. For other local configurations, see Huawei NE Series Routers.
If you can't implement the layer 3 sub-interface connection due to special reasons, you can try layer 2 sub-interfaces. For details, see Mode 2.

(Recommended) Mode 1: Layer 3 sub-interface+BGP

```
# Set sub-interfaces for layer 3 connection
interfaces
<interface_number>.<sub_number>
description <interface_desc>
dot1q termination vid <vlan id>
ip address <subinterface_ipaddress>
<subinterface_netmask>
speed <interface_speed>
duplex full
undo negotiation auto
commit
# Set eBGP
bgp <as_number>
router-id <route_id>
peer <bgp_peer_address> as-number
<bgp_peer_as_number>
peer <bgp_peer_address> password cipher
<bgp_auth_key>
peer <bgp_peer_address> description
<bgp_desc>
ipv4-family unicast
peer <bgp_peer_address> enable
```

```
commit
# Set BFD configuration of eBGP
bgp <as_number>
router-id <route_id>
peer <bgp_peer_address> bfd min-tx-interval
1000 min-rx-interval 1000 detect-multiplier 3
```

Mode 2: Layer 2 Vlanif interface+BGP (It is recommended to disable STP for layer 2 interfaces)

```
# Set ports
interfaces
<interface_number>
description
<interface_desc>
port link-type
trunk
undo shutdown
speed
<interface_speed>
duplex full
undo negotiation
auto
stp disable ** (****Disable****stp****STP****)**
commit
# Set virtual tunnels
vlan
<subinterface_vlanid>
description
<subinterface_desc>
# Set logic interfaces
interface Vlanif
<subinterface_vlanid>
description <subinterface_desc>
ip address
<subinterface_ipaddress> <subinterface_netmask>
# Configure interface VLAN
interfaces
<interface_number>
port trunk
allow-pass vlan <subinterface_vlanid>
commit
# Set eBGP
bgp
<as_number>
router-id
<route_id>
peer
```

```
<bgp_peer_address> as-number <bgp_peer_as_number>
peer
<bgp_peer_address> password cipher <bgp_auth_key>
peer
<bgp_peer_address> description <bgp_desc>
ipv4-family
unicast
peer
<bgp_peer_address> enable
# Set BFD configuration of eBGP
bgp <as_number>
router-id <route_id>
peer <bgp_peer_address> bfd min-tx-interval
1000 min-rx-interval 1000 detect-multiplier 3
commit
```

How to Set Keepalive and Holdtime Parameters

After establishing a BGP connection between two peers, the two peers periodically send keepalive messages to the peer to maintain the validity of the BGP connection. If a router does not receive a keepalive message or any other type of packet from the peer within the specified holdtime, the BGP connection is considered to have been interrupted and thus the BGP connection is interrupted.

The keepalive-time and hold-time values are determined through negotiation between the two peers. The smaller hold-time value in the Open message of both peers is the final hold-time value. The smaller value between **the result of the negotiated hold-time value divided by 3** and the locally configured keepalive-time value is used as the final keepalive-time value.

When the BGP connection is established, the recommended holdtime is 180 seconds (default value used by most vendors).

If the configured holdtime is less than 30 seconds, the linkage may interrupt the neighbor session in normal cases, and linkage jitter detection is required. You are advised to enable BFD to improve convergence performance.

IDC Local Configuration
BGP Routing Configuration Guide
Huawei NE Series Routers

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
undo shutdown
speed <interface_speed>
duplex full
undo negotiation auto
commit

# Set virtual tunnels
interfaces <interface_number>.<subinterface_number>
description <subinterface_desc>
vlan-type dot1q <subinterface_vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>
commit

# Set eBGP
bgp <as_number>
router-id <route_id>
peer <bgp_peer_address> as-number <bgp_peer_as_number>
peer <bgp_peer_address> password cipher <bgp_auth_key>
```

```
peer <bgp_peer_address> description <bgp_desc>
ipv4-family unicast
peer <bgp_peer_address> enable
commit

# Configure BFD for eBGP
bgp <as_number>
router-id <route_id>
peer <bgp_peer_address> bfd min-tx-interval <time value> min-rx-interval <time
value> detect-multiplier <value>
```

Huawei CE Series Switches

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC. Using the layer-3 sub-interfaces to connect to Tencent Cloud is recommended.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
undo portswitch
undo shutdown
speed <interface_speed>
duplex full
undo negotiation auto
commit

# Configure virtual tunnels (layer 3 sub-interfaces)
interface  <interface_number>.subinterface-number
description <subinterface_desc>
dot1q termination vid <vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>

# Set eBGP
bgp <as_number>
#router-id <route_id>
peer <bgp_peer_address> as-number <bgp_peer_as_number>
peer <bgp_peer_address> password cipher <bgp_auth_key>
peer <bgp_peer_address> description <bgp_desc>
ipv4-family unicast
peer <bgp_peer_address> enable
```

```
commit

# Configure BFD for eBGP
bgp <as_number>
router-id <route_id>
peer <bgp_peer_address> bfd min-tx-interval <time value> min-rx-interval <time
value> detect-multiplier <value>
```

H3C S Series Switches

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC. Using the layer-3 sub-interfaces to connect to Tencent Cloud is recommended.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
port link-mode route
undo shutdown
speed <interface_speed>
duplex full

# Configure layer 3 sub-interfaces
interface  interface-number.subnumber
description <vlan_description>
dot1q termination vid <vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>
bfd min-transmit-interval <value> //BFD parameter
bfd min-receive-interval <value>  //BFD parameter
bfd detect-multiplier <value>  //BFD parameter


# Set eBGP
bgp <as_number>
#router-id <route_id>
peer <bgp_peer_address> as-number <bgp_peer_as_number>
peer <bgp_peer_address> password cipher <bgp_auth_key>
peer <bgp_peer_address> description <bgp_desc>
```

```
# Configure BFD for eBGP
peer <bgp_peer_address> bfd
```

Juniper MX Series Routers

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
set interfaces <interface_number> description <interface_desc>
set interfaces <interface_number> vlan-tagging
set interfaces <interface_number> link-mode full-duplex
set interfaces <interface_number> speed <interface_speed> // Whether this
command can be configured depends on whether the module supports it
set interfaces <interface_number> gigether-options no-auto-negotiation // This
command is recommended to be used in combination with
Usage
commit

# Configure virtual tunnels
set interfaces <interface_number> unit <subinterface_number> vlan-id
<subinterface_vlanid>
set interfaces <interface_number> unit <subinterface_number> description
<subinterface_desc>
set interfaces <interface_number> unit <subinterface_number> family inet
address
<subinterface_ipaddress>/<subinterface_netmask>
commit

# Set eBGP
set protocols bgp group ebgp type external // Define protocol group. Changing
ebgp name is allowed.
```

```
set protocols bgp group ebgp neighbor <bgp_peer_address> loacal-as <as_number>
// If not configured, the global AS number will be used
 by default (set routing-options autonomous-system XX)
set protocols bgp group ebgp neighbor <bgp_peer_address> peer-as
<bgp_peer_as_number>
set protocols bgp group ebgp neighbor <bgp_peer_address> authentication-key
<bgp_auth_key>
set protocols bgp group ebgp neighbor <bgp_peer_address> description
<bgp_peer_desc>
commit

# Configure BFD for eBGP
set protocols bgp group ebgp neighbor <bgp_peer_address> bfd-liveness-detection
minimum-interval <value>
```

Cisco ASR Series Routers

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
no shutdown
speed <interface_speed>
duplex full
no negotiation auto
commit

# Configure virtual tunnels
interfaces <interface_number>.<subinterface_number>
description <subinterface_desc>
encapsulation dot1q <subinterface_vlanid>
ipv4 address <subinterface_ipaddress> <subinterface_netmask>
bfd interval <value> min_rx <value> multiplier <value> //BFD parameter
commit

# Set eBGP
router bgp <as_number>
#bgp router-id <router_id>
neighbor <bgp_peer_address>
remote-as <bgp_peer_as_number>
password encrypted <bgp_auth_key>
description <bgp_peer_desc>
remote-as <bgp_peer_as_number> fall-over bfd //Configure BFD for BGP
```

```
commit
```

Cisco C Series Switches

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC. Using the layer-3 sub-interfaces to connect to Tencent Cloud is recommended.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
no shutdown
no switchport
speed <interface_speed>
duplex full
no negotiation auto
end

# Configure layer 3 sub-interfaces
interface  interface-number.subnumber
description <vlan_description>
encapsulation dot1q <vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>
bfd interval <value> min_rx <value> multiplier <value> //BFD parameter
end

# Set eBGP
router bgp <as_number>
bgp router-id <router_id>
neighbor <bgp_peer_address> remote-as <bgp_peer_as_number>
neighbor <bgp_peer_address> password encrypted <bgp_auth_key>
neighbor <bgp_peer_address> description <bgp_peer_desc>
```

```
neighbor <bgp_peer_address> activate
neighbor <bgp_peer_address> fall-over bfd single-hop //Configure BFD for BGP
```

Cisco Nexus Series Switches

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC. Using the layer-3 sub-interfaces to connect to Tencent Cloud is recommended.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
no shutdown
no switchport
speed <interface_speed>
duplex full
no negotiation auto
end

# Configure layer 3 sub-interfaces
interface  interface-number.subnumber
description <vlan_description>
encapsulation dot1q <vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>
bfd interval <value> min_rx <value> multiplier <value> //BFD parameter
end
# Set eBGP
router bgp <as_number>
bgp router-id <router_id>
neighbor <bgp_peer_address>
  remote-as <bgp_peer_as_number>
  password encrypted <bgp_auth_key>
  description <bgp_peer_desc>
```

```
neighbor <bgp_peer_address> fall-over bfd single-hop //BFD configuration
commit
```

Static Routing Configuration Guide
Huawei NE Series Routers

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
undo shutdown
speed <interface_speed>
duplex full
undo negotiation auto
commit

# Configure virtual tunnels
interfaces <interface_number>.<subinterface_number>
description <subinterface_desc>
vlan-type dot1q <subinterface_vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>
commit

# Configure NQA detection for static routes
nqa test-instance <admin-name>< test-name>
 test-type icmp  //Default detection type
 destination-address  x.x.x.x (nexthop-address ) //Detection address
 interval seconds <value> //Detection interval
 timeout <value> //Timeout period
 probe-count <value> //Number of packets per detection
```

```
 frequency <value> //Detection frequency
 start now


# Configure static routing
# Configure global static routes
ip route-static <ip-address> <mask | mask-length> <nexthop-address> track nqa
<admin-name>< test-name>
//<ip-address>Destination IP ranges for users to access Tencent network
services
such as ip route-static 172.16.0.192 255.255.255.192 10.128.152.1 track nqa
user test


# Configure static routes for users to access Tencent Cloud in VRF mode
ip route-static <vpn-instance vpn-instance-name> <ip-address> <mask | mask-
length> <nexthop-
address> track nqa  <admin-name>< test-name>
such as ip route-static vpn-instance GLOBAL 9.0.0.0 255.0.0.0 10.128.152.1
track nqa user test
commit
```

Huawei CE Series Switches

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC. Using the layer-3 sub-interfaces to connect to Tencent Cloud is recommended.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
undo portswitch
undo shutdown
speed <interface_speed>
duplex full
undo negotiation auto
commit

# Configure virtual tunnels (layer 3 sub-interfaces)
interface  <interface_number>.subinterface-number
description <subinterface_desc>
dot1q termination vid <vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>

# Configure NQA detection for static routes
nqa test-instance <admin-name>< test-name>
 test-type icmp  //Default detection type
 destination-address  x.x.x.x (nexthop-address ) //Detection address
 interval seconds <value> //Detection interval
 timeout <value> //Timeout period
 probe-count <value> //Number of packets per detection
 frequency <value> //Detection frequency
```

```
 start now


# Configure static routing
# Configure global static routes
ip route-static <ip-address> <mask | mask-length> <nexthop-address>track nqa
<admin-name>< test-name>//<ip-address>
Destination IP ranges for users to access Tencent network services
such as ip route-static 172.16.0.192 255.255.255.192 10.128.152.1 track nqa
user test

# Configure static routes for users to access Tencent Cloud in VRF mode
ip route-static <vpn-instance vpn-instance-name> <ip-address> <mask | mask-
length> <nexthop-
address>track nqa  <admin-name>< test-name>
such as ip route-static vpn-instance GLOBAL 9.0.0.0 255.0.0.0 10.128.152.1
track nqa user test
commit
```

H3C S Series Switches

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
port link-mode route
undo shutdown
speed <interface_speed>
duplex full

# Configure layer 3 sub-interfaces
interface  interface-number.subnumber
description <vlan_description>
dot1q termination vid <vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>

# Configure NQA detection for static routes
nqa entry <admin-name> < test-name>
type icmp-echo  //Default detection type
destination-address  x.x.x.x (nexthop-address ) //Detection address
interval seconds 2 //Detection interval
frequency <value> //Detection frequency
history-record enable
probe count  <value> //Number of packets per detection
probe timeout <value> //Timeout period

# Configure Track
```

```
track <number> nqa entry  <admin-name>< test-name> //Associate Track with NQA

# Configure static routing
ip route-static <Destination_IP_address> <Mask_of_the-IP_address>
<VLAN_interface> track <number>
```

Juniper MX Series Routers

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
set interfaces <interface_number> description <interface_desc>
set interfaces <interface_number> vlan-tagging
set interfaces <interface_number> link-mode full-duplex
set interfaces <interface_number> speed <interface_speed> // Whether this
command can be configured depends on whether the module supports it
set interfaces <interface_number> gigether-options no-auto-negotiation // This
command is recommended to be used in combination with
Usage
commit

# Configure virtual tunnels
set interfaces <interface_number> unit <subinterface_number> vlan-id
<subinterface_vlanid>
set interfaces <interface_number> unit <subinterface_number> description
<subinterface_desc>
set interfaces <interface_number> unit <subinterface_number> family inet
address
<subinterface_ipaddress>/<subinterface_netmask>
commit

# Configure static routing
# Configure a static route to the user IP globally
set routing-options static route <customer_prefix/mask> next-hop
<customer_interface_ip>
```

```
# Configure BFD for the static routes. To configure RPM for the static routes,
consult equipment vendors.
set routing-options static route <customer_prefix/mask>bfd-liveness-detection
minimum-interval <value>

such as set routing-options static route 1.1.1.0/24 next-hop 192.168.1.2 bfd-
liveness-detection minimum-interval 1000

# Configure a static route to the user IP in VRF mode
set routing-instances <vrf_name> routing-options static route
<customer_prefix/mask> next-hop
<customer_interface_ip>
such as set routing-instances cap routing-options static route 1.1.1.0/24 next-
hop 192.168.1.2
commit
```

Cisco ASR Series Routers

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
no shutdown
speed <interface_speed>
duplex full
no negotiation auto
commit

# Configure virtual tunnels
interfaces <interface_number>.<subinterface_number>
description <subinterface_desc>
encapsulation dot1q <subinterface_vlanid>
ipv4 address <subinterface_ipaddress> <subinterface_netmask>
commit

# Configure IP SLA (NQA)
ip sla <operation-number>
icmp-echo x.x.x.x<nexthop_address> source-ip x.x.x.x <source_address>
frequency <value> //Set a detection frequency
timeout <value> //Set a timeout period
ip sla schedule <operation-number> life forever start-time now
en

# Configure Track-associated IP SLA
```

```
track <operation-number> ip sla <operation-number> reachability
end

# Configure static routing
router static
vrf <vrf-name> //If no VRF is specified, the static route is in the default VRF
mode.
  address-family <ipv4 | ipv6> unicast
  <ip-prefix/netmask> <next_hop_ip> <interface_number> <description_text>
<distance> <tag tag_value> track <operation-number>
commit
```

Cisco C Series Switches

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC. Using the layer-3 sub-interfaces to connect to Tencent Cloud is recommended.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
no shutdown
no switchport
speed <interface_speed>
duplex full
no negotiation auto
end

# Configure layer 3 sub-interfaces
interface  interface-number.subnumber
description <vlan_description>
encapsulation dot1q <vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>
end

# Configure IP SLA (NQA)
ip sla <operation-number>
icmp-echo x.x.x.x<nexthop_address> source-ip x.x.x.x <source_address>
frequency <value> //Set a detection frequency
timeout <value> //Set a timeout period
ip sla schedule <operation-number> life forever start-time now
end
```

```
# Configure Track-associated IP SLA
track <operation-number> ip sla <operation-number> reachability
end

# Configure static routes and associate track
ip route <ip_prefix> <netmask> <interface_number | vlan_id> <next_hop_ip> <name
nexthop_name> <distance> <tag tag_value> track <operation-number>
```

Cisco Nexus Series Switches

Last updated：2024-11-05 09:46:38

Direct Connect connects Tencent Cloud with the user IDC with a dedicated physical line. After configuring the Direct Connect gateway and dedicated tunnel on the Tencent Cloud side, users need to configure routes on the local IDC. Using the layer-3 sub-interfaces to connect to Tencent Cloud is recommended.

Note:

This document only introduces the local routing configurations associated with Tencent Cloud Direct Connect. For other information, please see the local router documentation or consult your router provider.

Routing Configuration

Note:

It's recommended that you use the default configurations of `Keepalive` and `holdtime` for the BGP connection between the two peers. The `holdtime` is three times the interval at which keepalive messages are sent. The recommended `holdtime` value is 180s.

```
# Configure ports
interfaces <interface_number>
description <interface_desc>
no shutdown
no switchport
speed <interface_speed>
duplex full
no negotiation auto
end

# Configure layer 3 sub-interfaces
interface  interface-number.subnumber
description <vlan_description>
encapsulation dot1q <vlanid>
ip address <subinterface_ipaddress> <subinterface_netmask>
end

# Configure IP SLA (NQA)
ip sla <operation-number>
icmp-echo x.x.x.x<nexthop_address> source-ip x.x.x.x <source_address>
frequency <value> //Set a detection frequency
timeout <value> //Set a timeout period
ip sla schedule <operation-number> life forever start-time now
end
```

```
# Configure Track-associated IP SLA
track <operation-number> ip sla <operation-number> reachability
end

# Configure static routes and associate track
ip route <ip_prefix/netmask> <interface_number | vlan_id> <next_hop_ip> <name
nexthop_name><distance> <tag tag_value> track <operation-number>
```

Establishing Direct Connect Between Tencent Cloud and Various Cloud Vendors Through Equinix
Creating a Virtual Network Device of Equinix

Last updated：2024-11-05 09:46:38

If your Equinix Fabric account does not have a port in the region to be connected, follow the steps in this document to create a virtual device.
If your Equinix Fabric account has a port in the region to be connected, you can skip this document and directly "Create a Connection from Equinix to AWS Cloud".

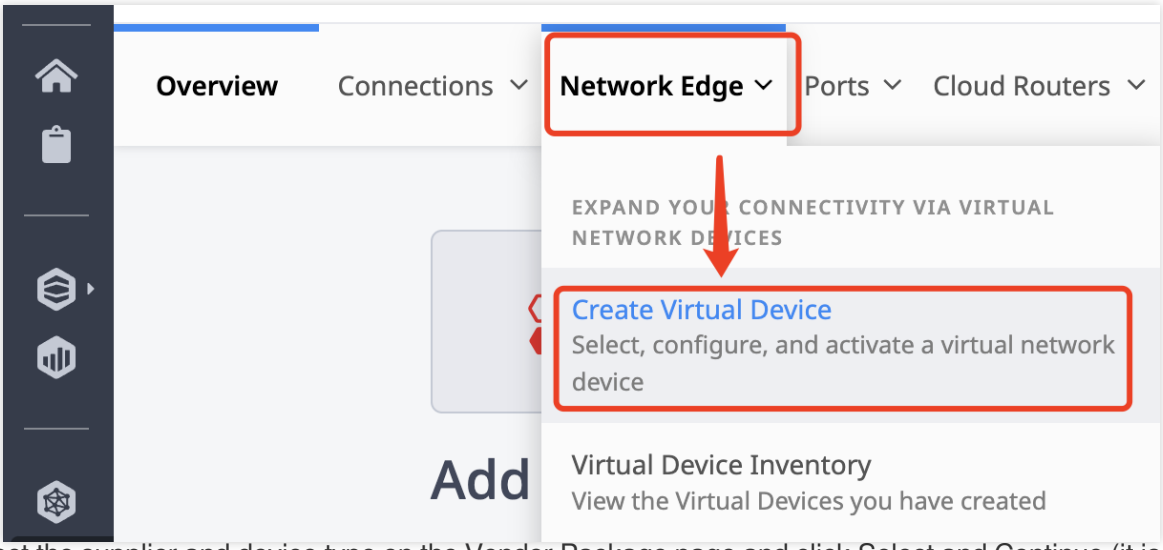
Prerequisites

You already have an Equinix Fabric account.
If you do not have an account, you can contact sales personnel via the Equinix page or create one. If you have any questions about using the page, you can contact Equinix sales personnel for guidance or reach out to Equinix Online Service for support.

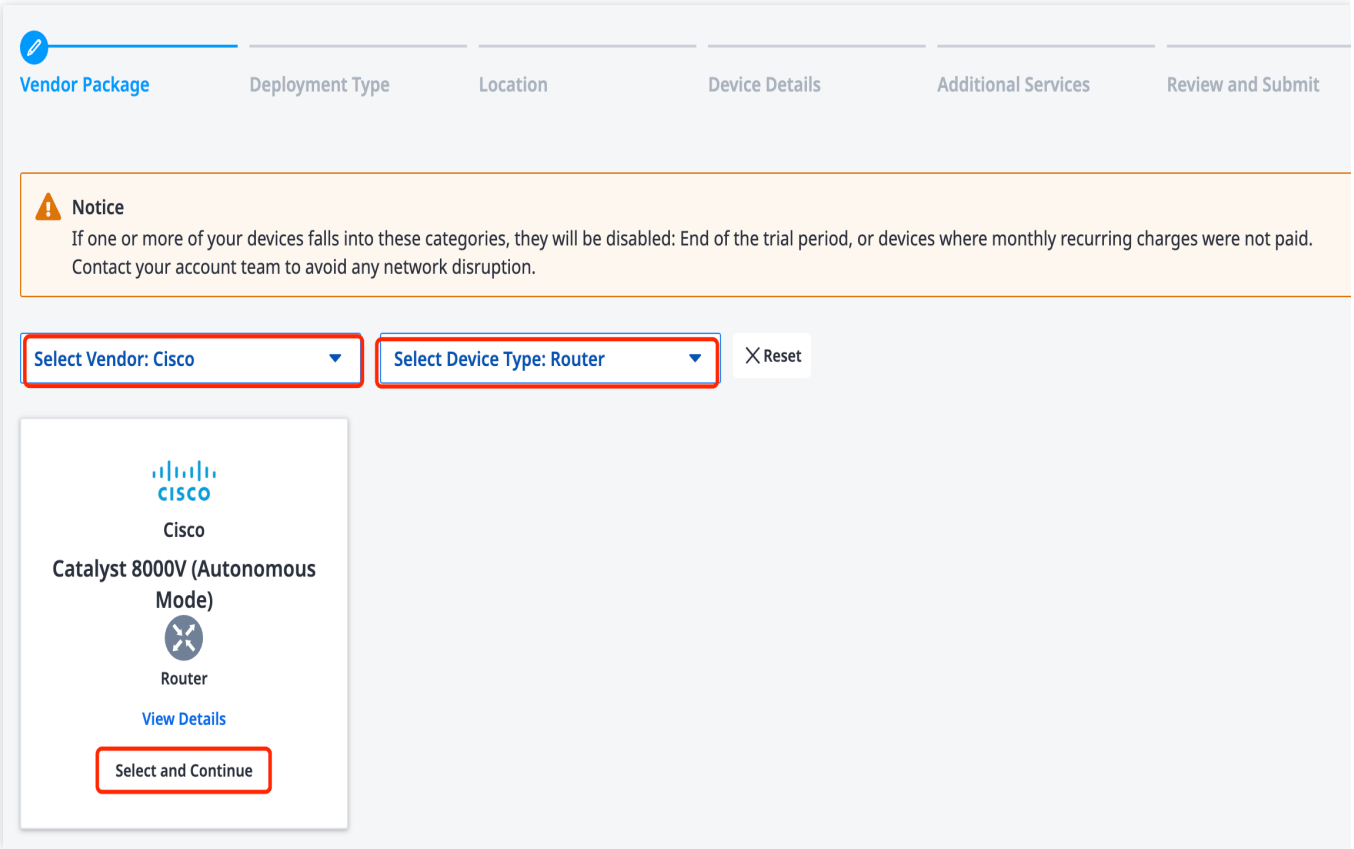
Directions

Placing an Order on the Equinix Side

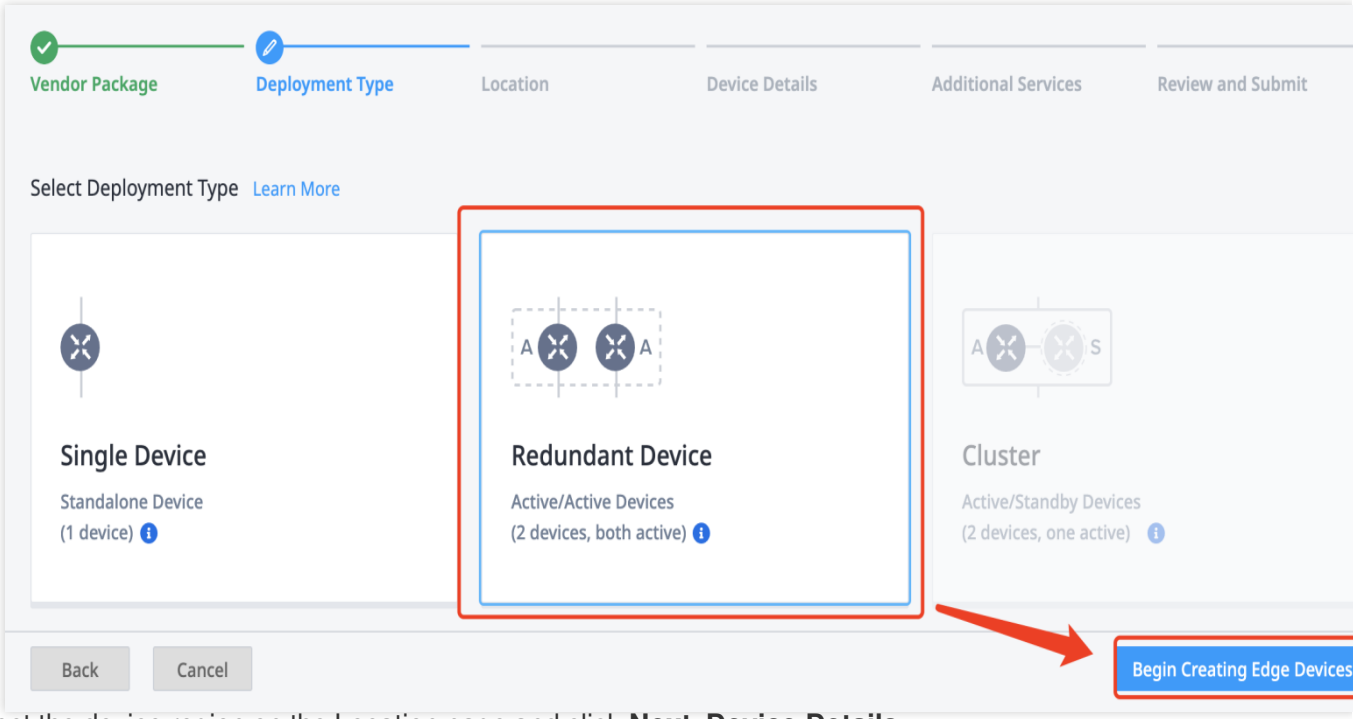
1. Log in to Equinix Fabric.
2. Select Create Virtual Device from the Network Edge menu.



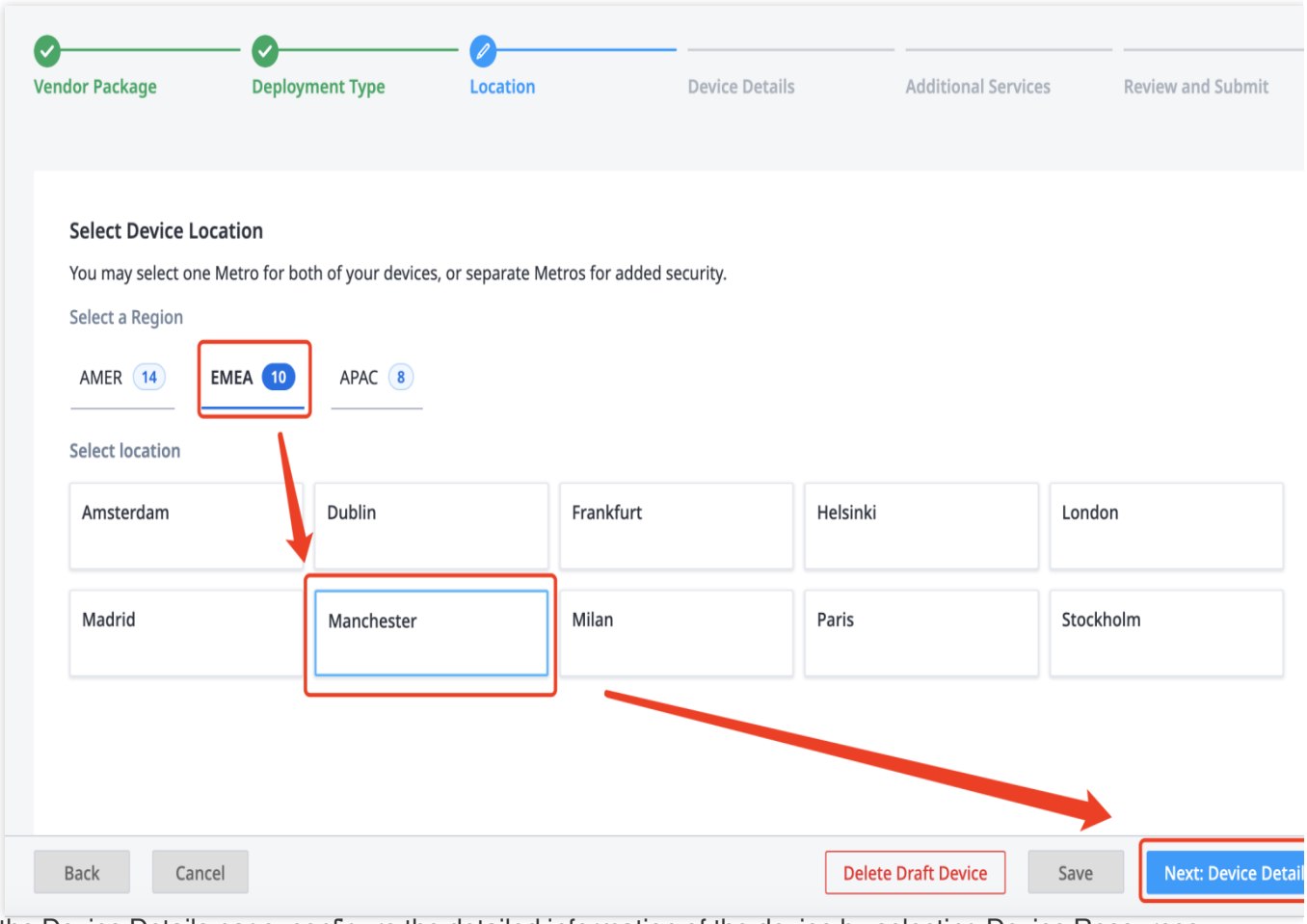
3. Select the supplier and device type on the Vendor Package page and click Select and Continue (it is recommended to use Cisco 8,000 V virtual router, which provides a standard configuration process).



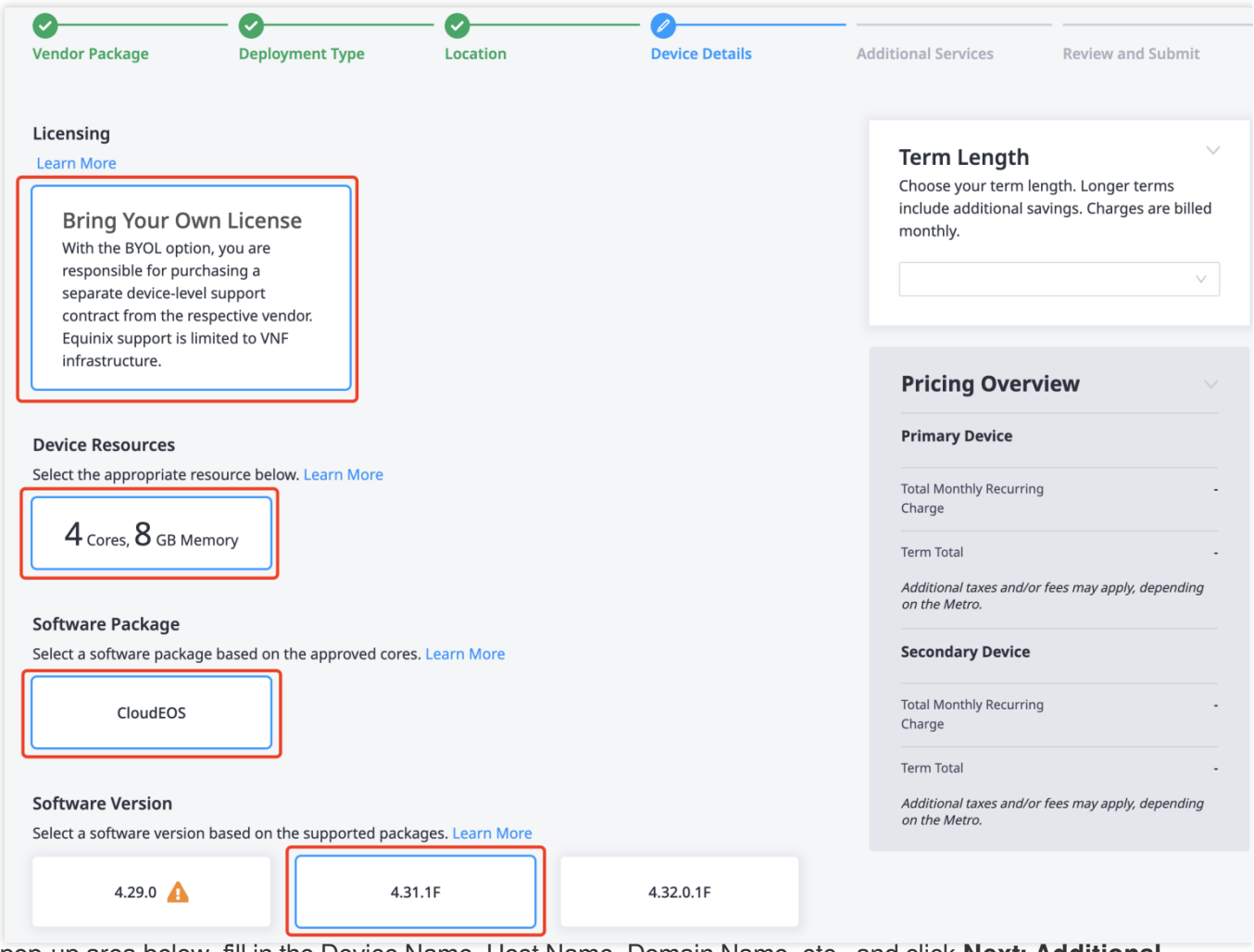
4. Select the deployment type on the Deployment Type page and click **Begin Creating Edge Devices**.



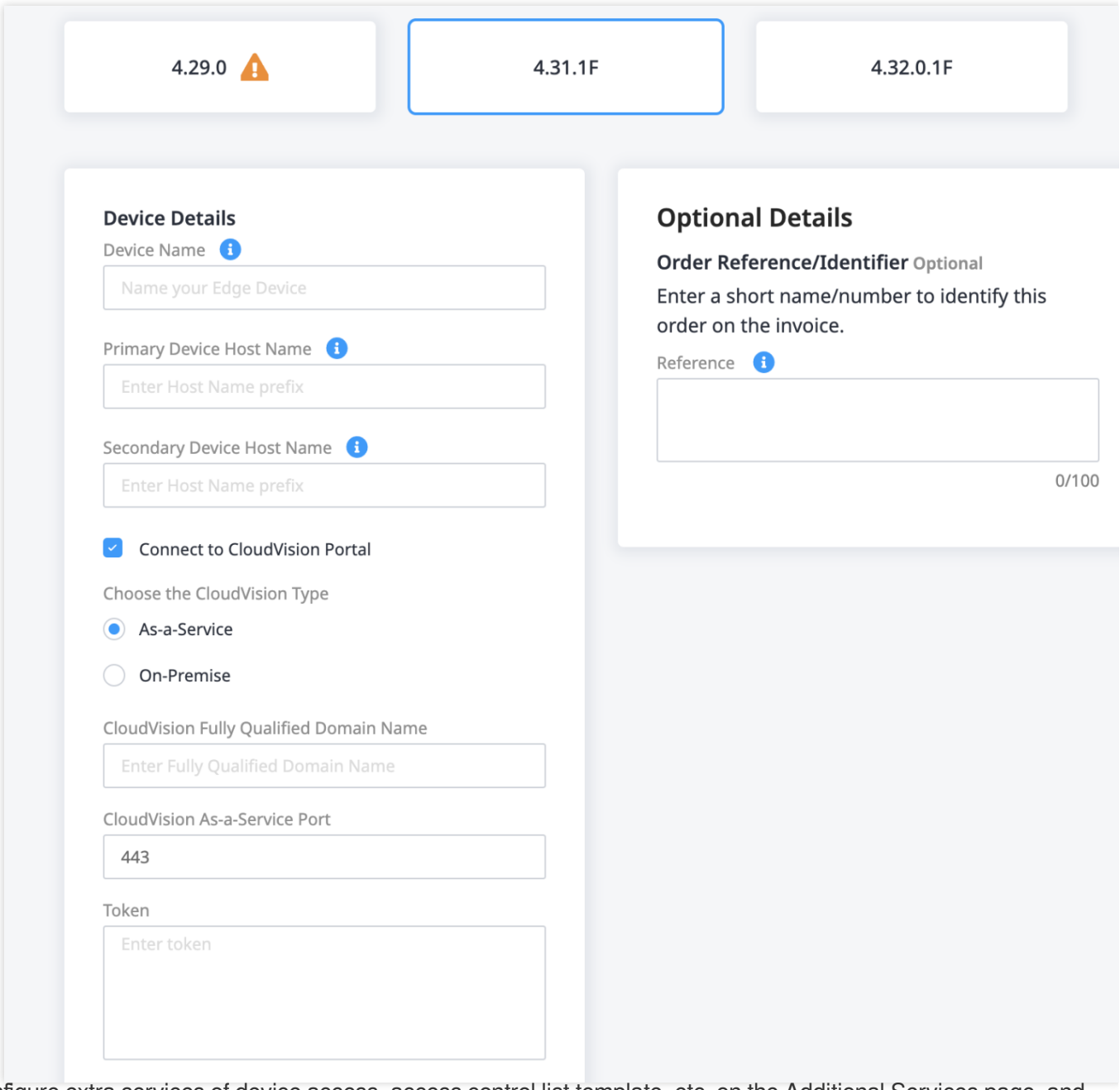
5. Select the device region on the Location page and click **Next: Device Details**.



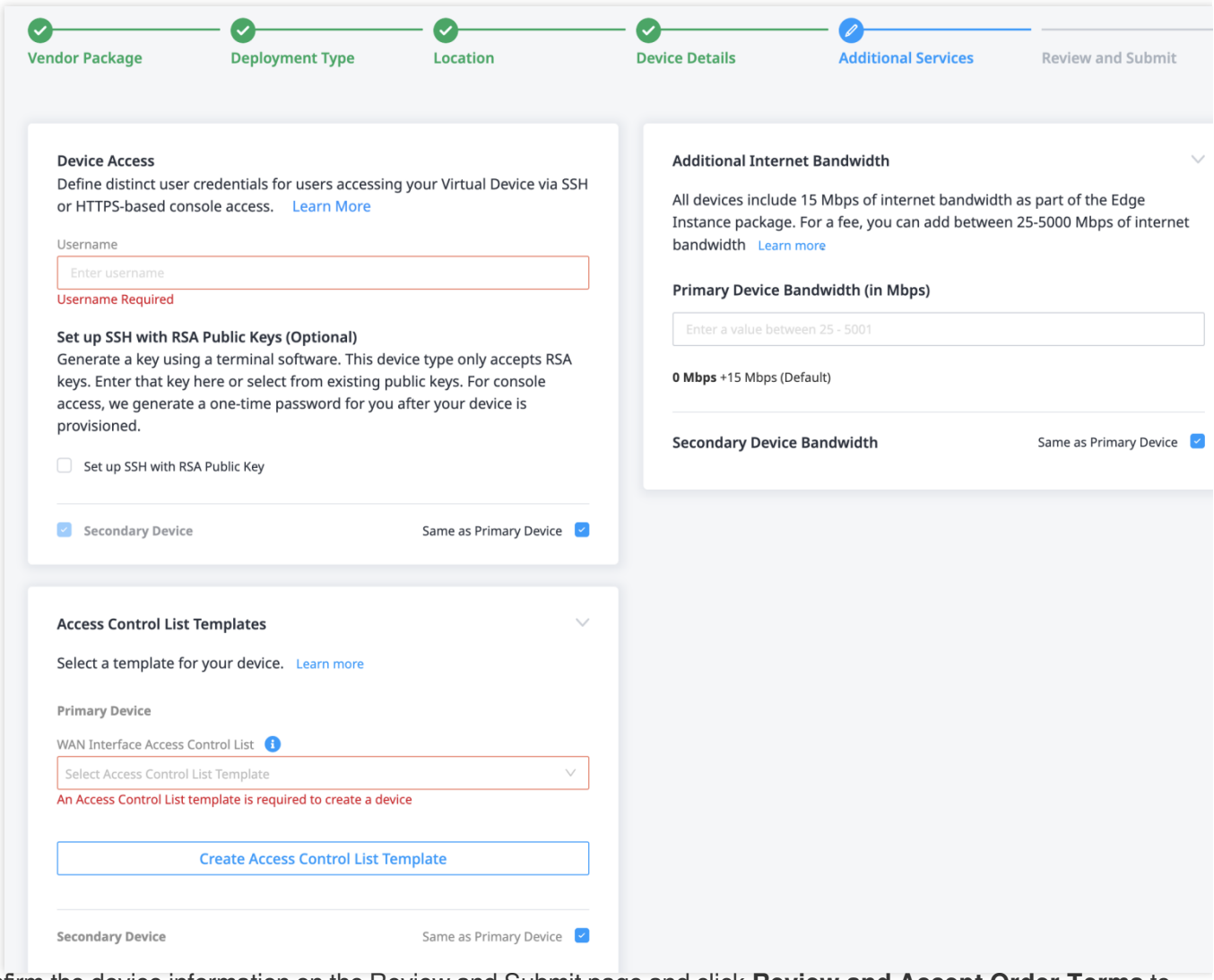
6. On the Device Details page, configure the detailed information of the device by selecting Device Resources, Software Package and Software Version.



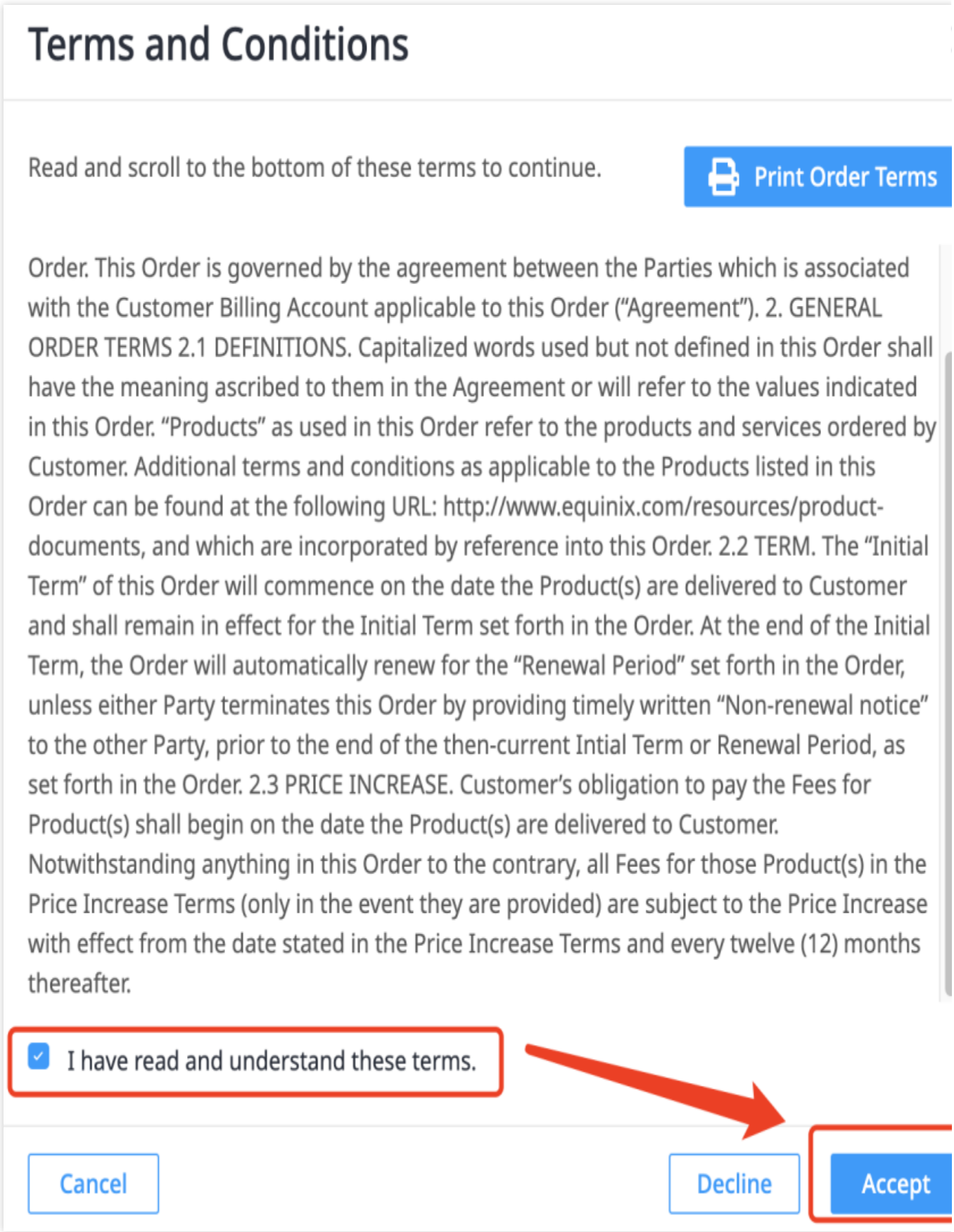
In the pop-up area below, fill in the Device Name, Host Name, Domain Name, etc., and click **Next: Additional Services**.



7. Configure extra services of device access, access control list template, etc. on the Additional Services page, and click **Next: Review**.

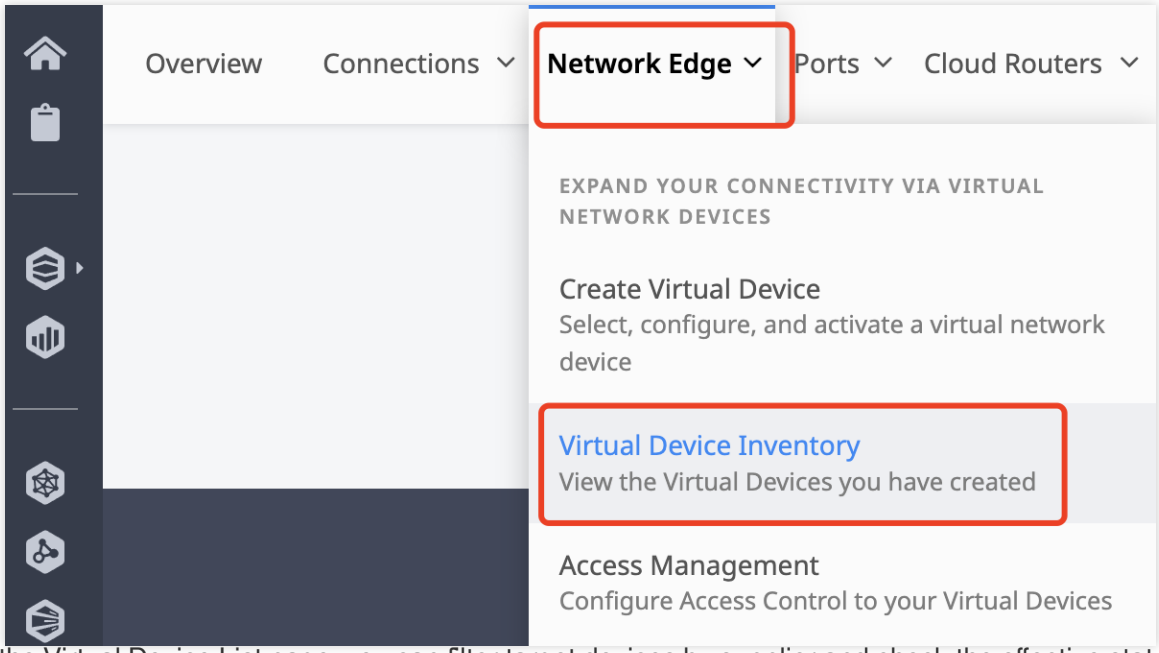


8. Confirm the device information on the Review and Submit page and click **Review and Accept Order Terms** to review the order terms in the pop-up text box. After reading and understanding these terms, check **I have read and understand these terms** and click **Accept**. Then click **Create Virtual Device**. The virtual device will be created.

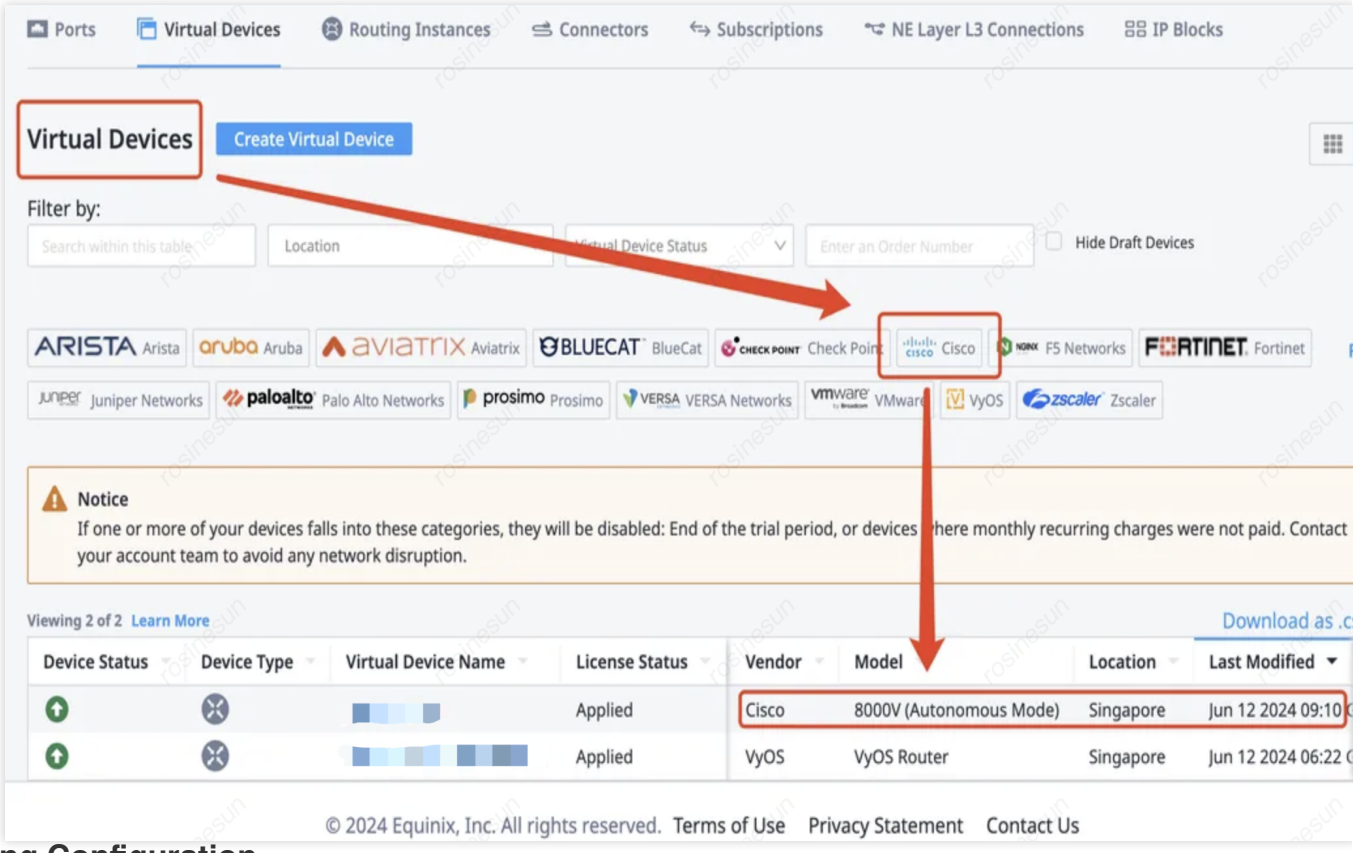


Viewing Status of the Virtual Device

1. Select Virtual Device Inventory from the Network Edge menu.

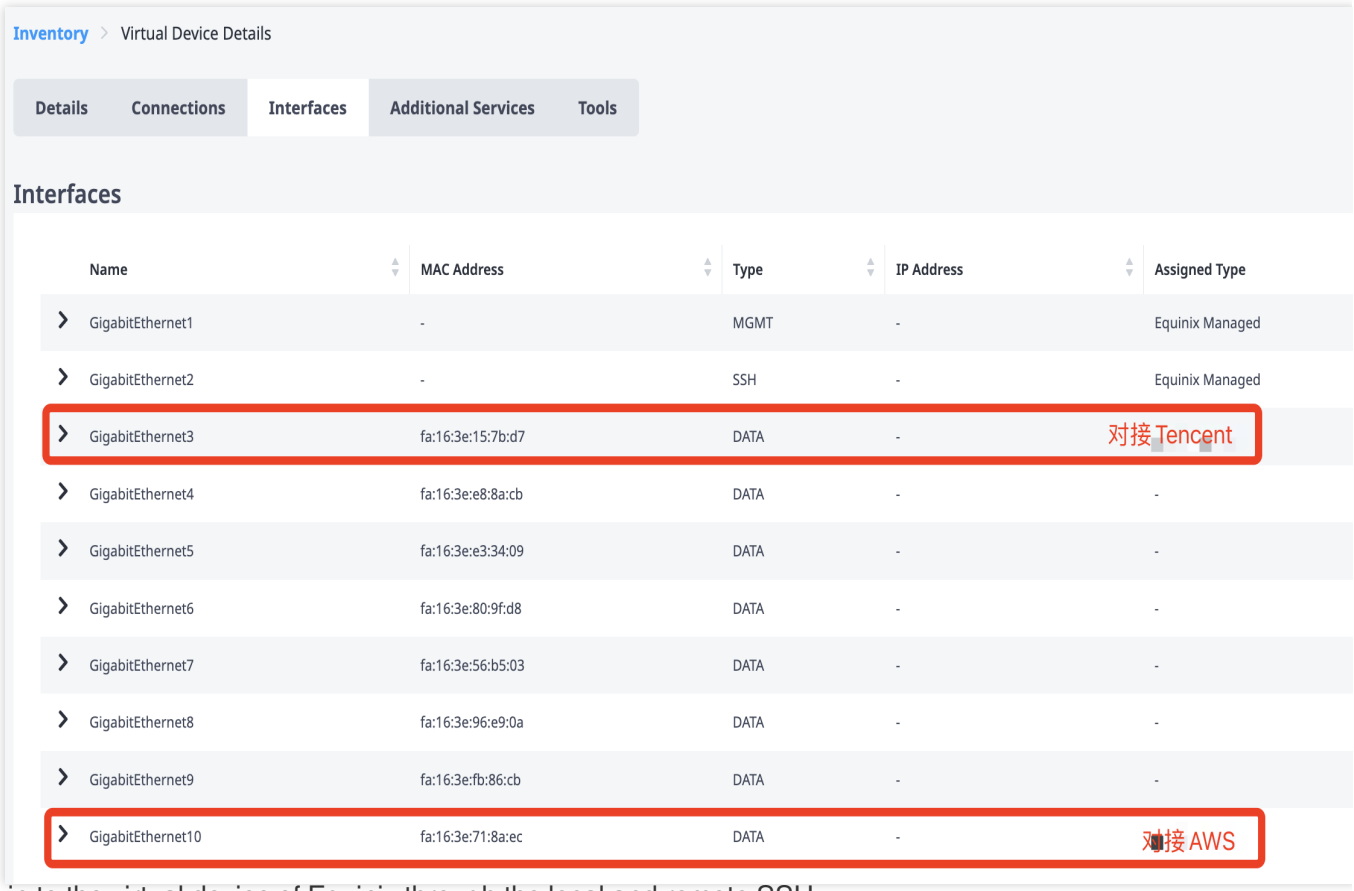


2. On the Virtual Device List page, you can filter target devices by supplier and check the effective status of the device.

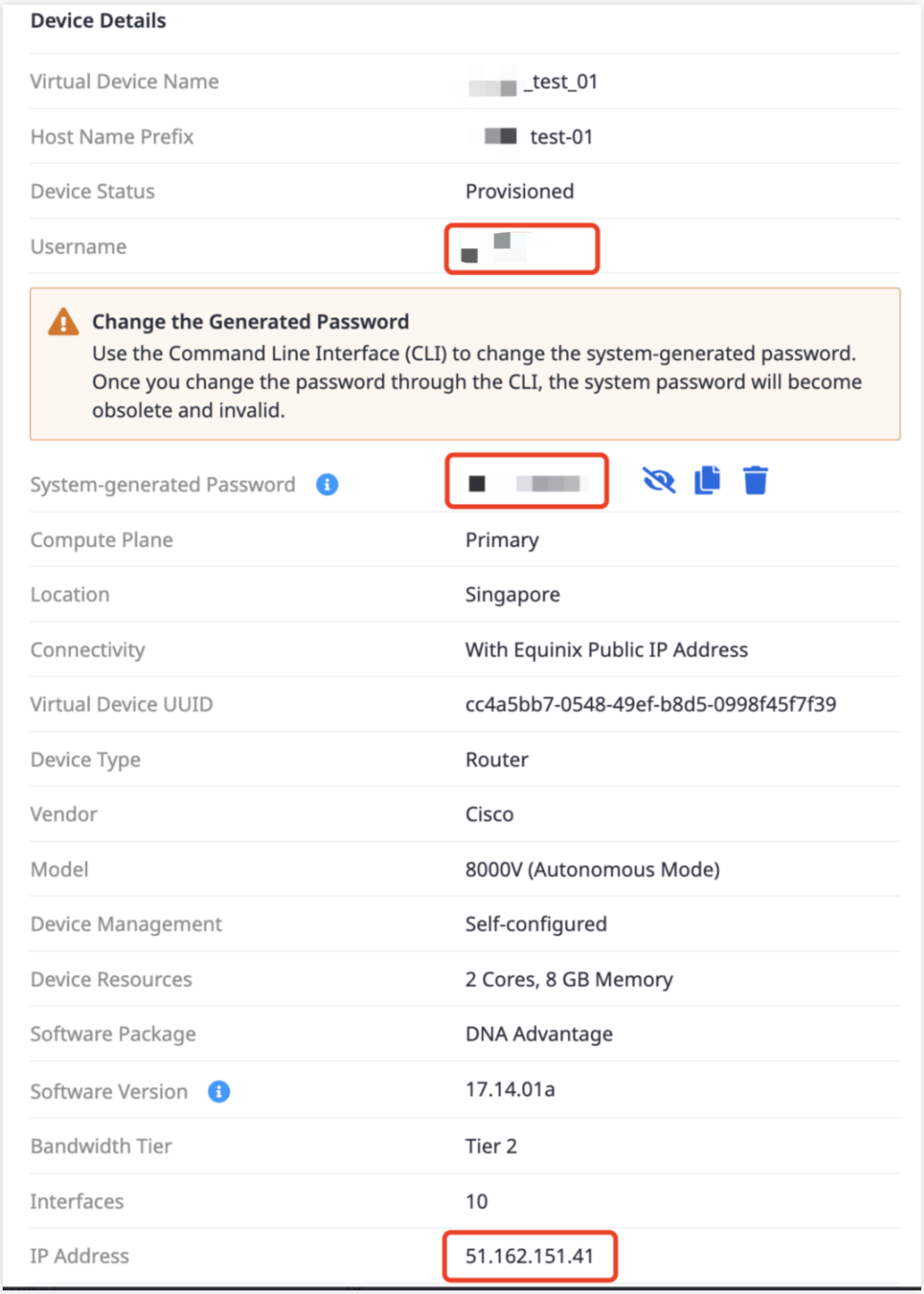


Issuing Configuration

1. Enter the virtual device interface to view the two ports corresponding to connection. For example, for the connection to Tencent Cloud, the port GigabitEthernet3 of the virtual device will be used, and for the connection to AWS Cloud, the port GigabitEthernet10 will be used.

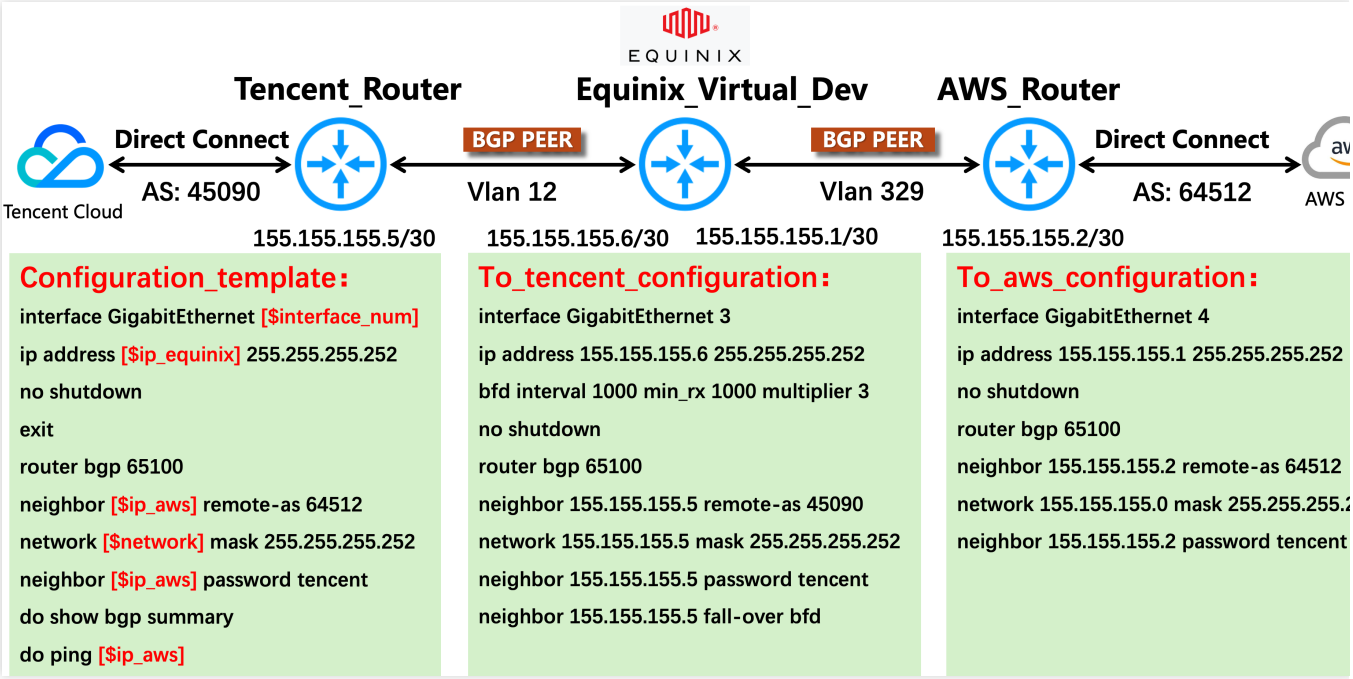


2. Log in to the virtual device of Equinix through the local and remote SSH.



```
(base) jiafengliu@YANISLIU-MB1 ~ % ssh yanisliu@51.162.151.41
The authenticity of host '51.162.151.41 (51.162.151.41)' can't be established.
RSA key fingerprint is SHA256:V6iYumdWVYNsUeu9vvn4hnW4+LbqtpQyYpkbWkwGpy0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '51.162.151.41' (RSA) to the list of known hosts.

============================================================

Access to this system is limited to authorized users for
             company business purposes only.

     WARNING: All unauthorized access is prohibited.

============================================================
(yanisliu@51.162.151.41) Password:



yaisliu-test-01#
```

3. After logging in to the virtual device through the remote SSH, manual configuration of the Layer 3 interconnection is required, and the configuration templates and examples are as follows:



Creating a Connection from Equinix to AWS Cloud

Last updated：2024-11-05 09:46:38

Prerequisites

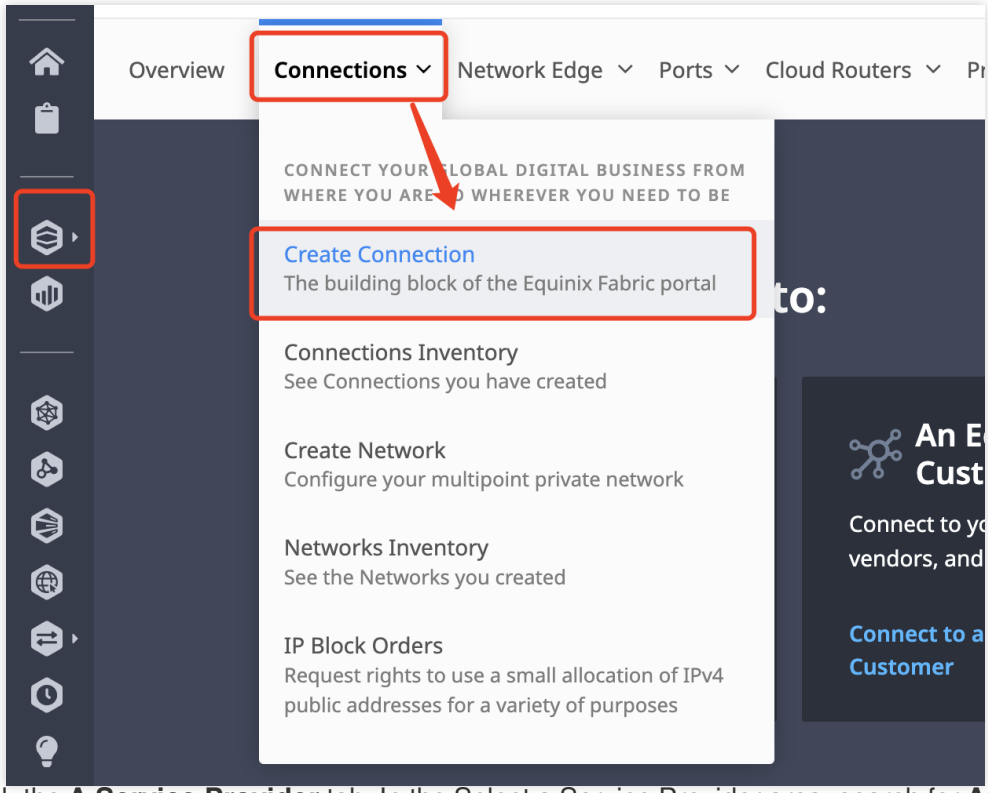
You already have an Equinix Fabric account. If you do not have one, you can contact sales personnel via the Equinix page or create one. If you have any questions about using the page, you can contact Equinix sales personnel for guidance or reach out to Equinix Online Service for support.
You already have an AWS account.
Your Equinix Fabric account has a port in the region to be connected.

Directions

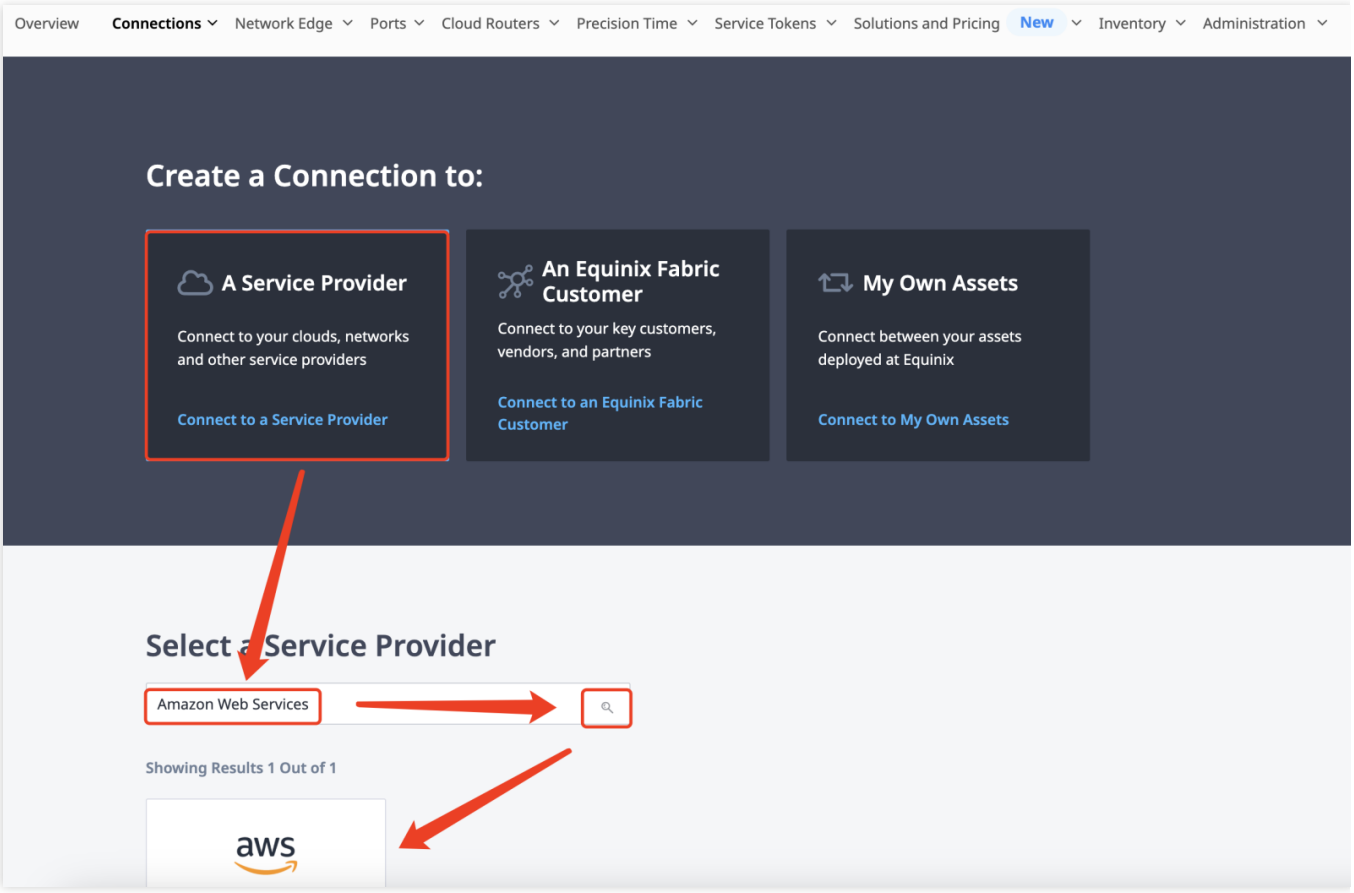
Placing an Order on the Equinix Side

Step 1: Selecting a Service Provider

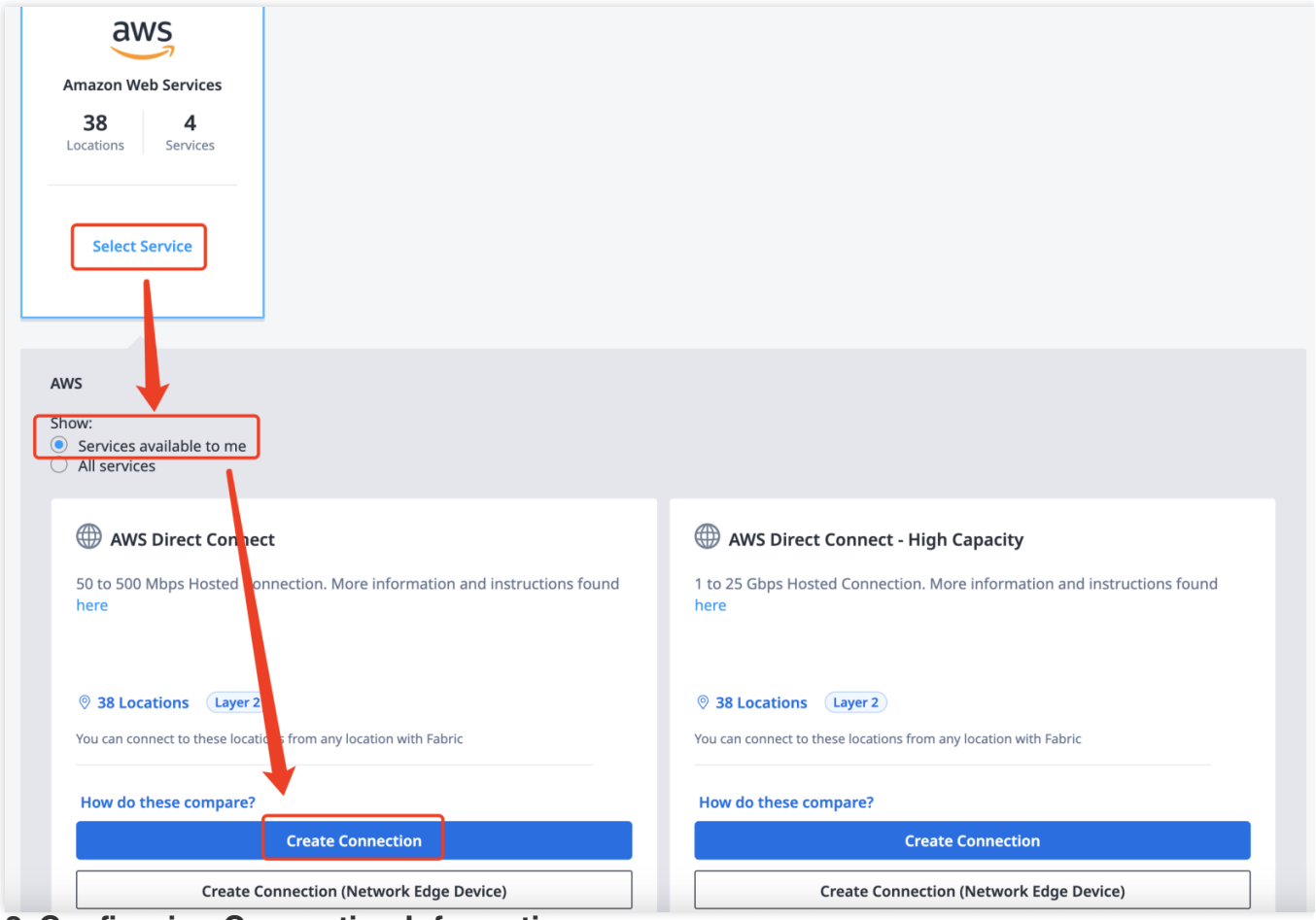
1. Log in to Equinix Fabric.
2. Select **Create Connection** from the Connections menu.



3. Click the **A Service Provider** tab. In the Select a Service Provider area, search for **Amazon Web Services** in the search box and the **Amazon Web Services** selection box will appear.

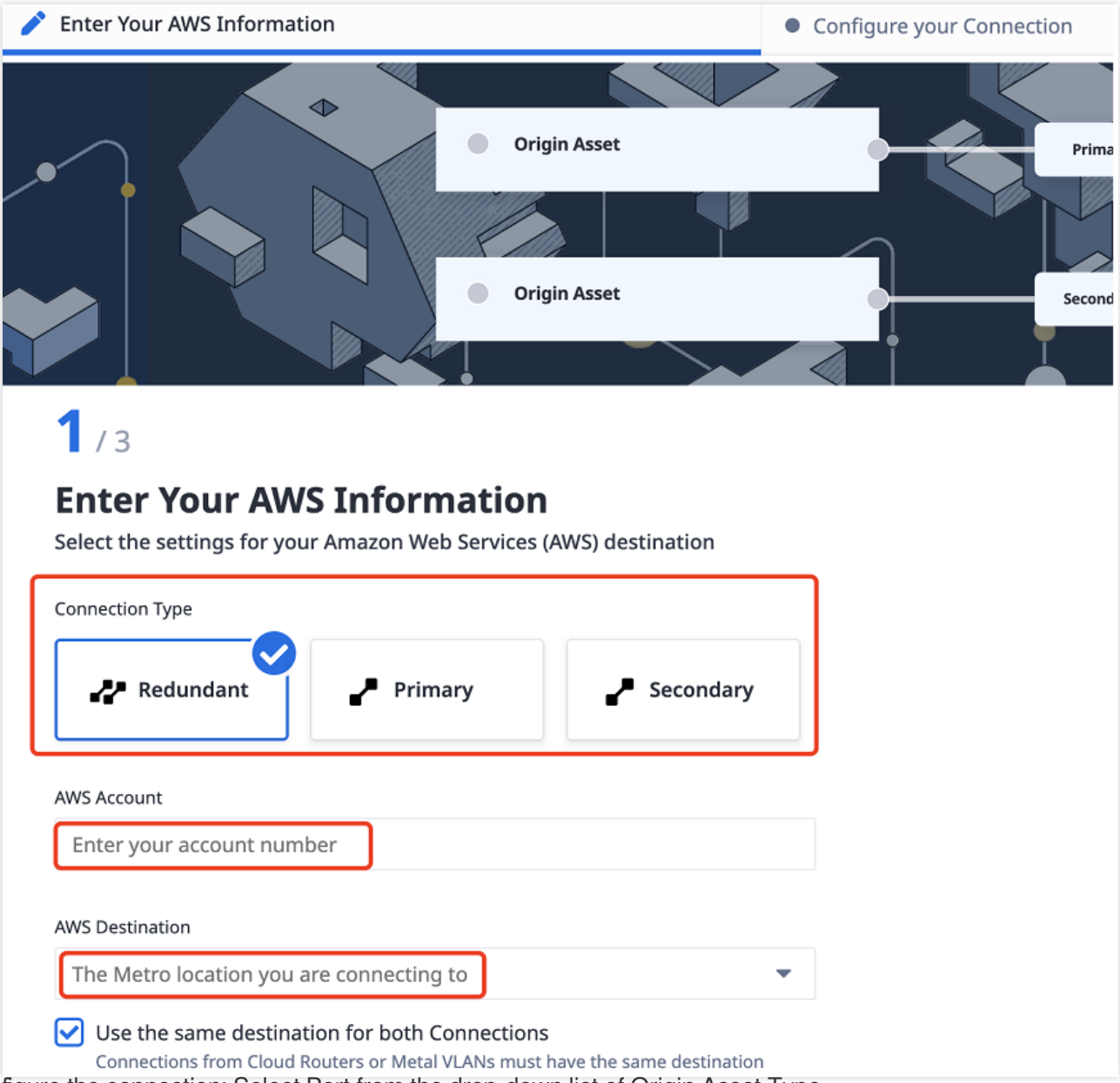


4. In the **Amazon Web Services** selection box, click **Select Service**. In the pop-up window, select the service type **Services available to me**, choose the appropriate service and click **Create Connection**.



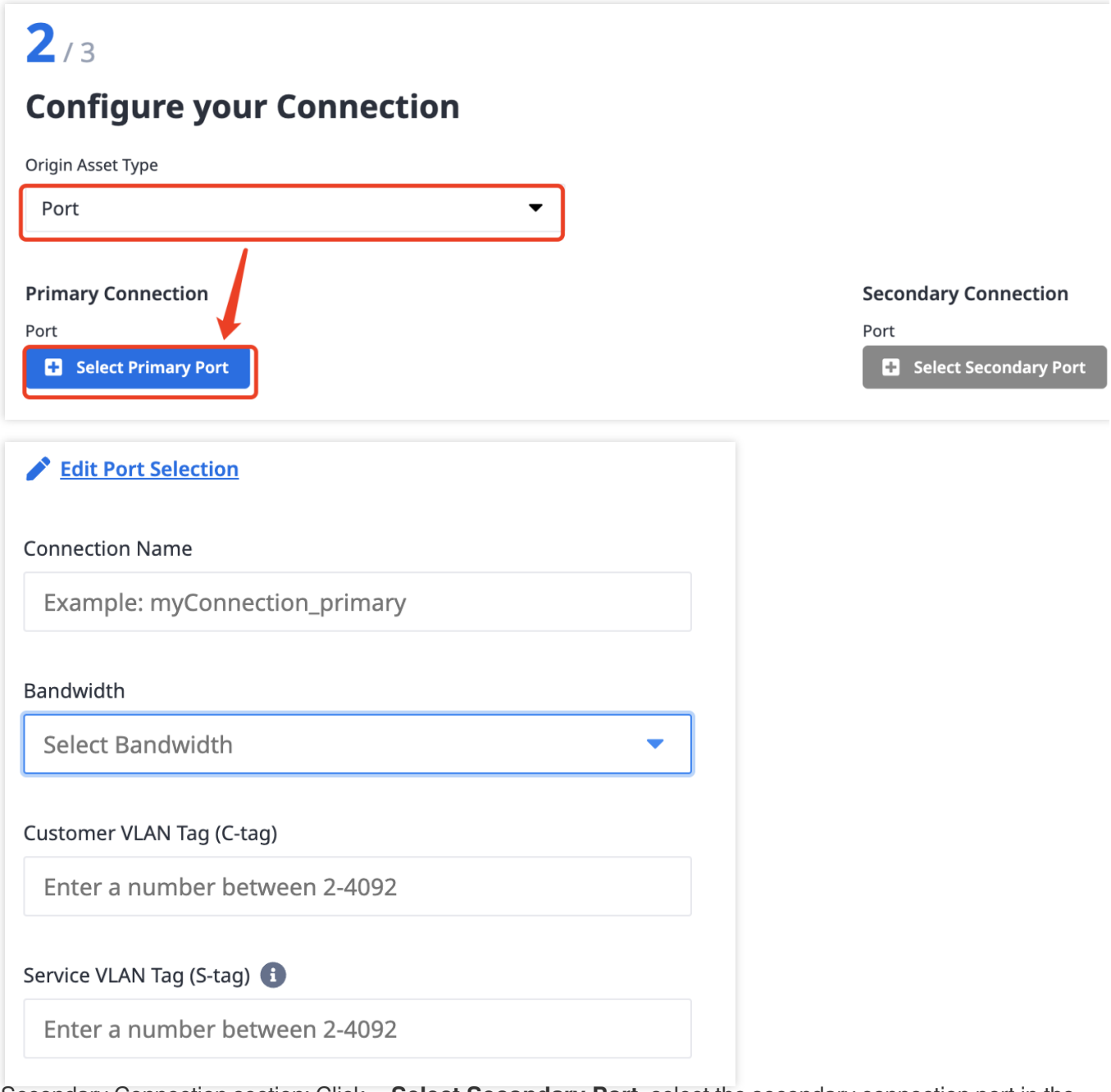
Step 2: Configuring Connection Information

1. Enter the AWS information: connection type, AWS account ID and AWS destination, and then click **Next**.

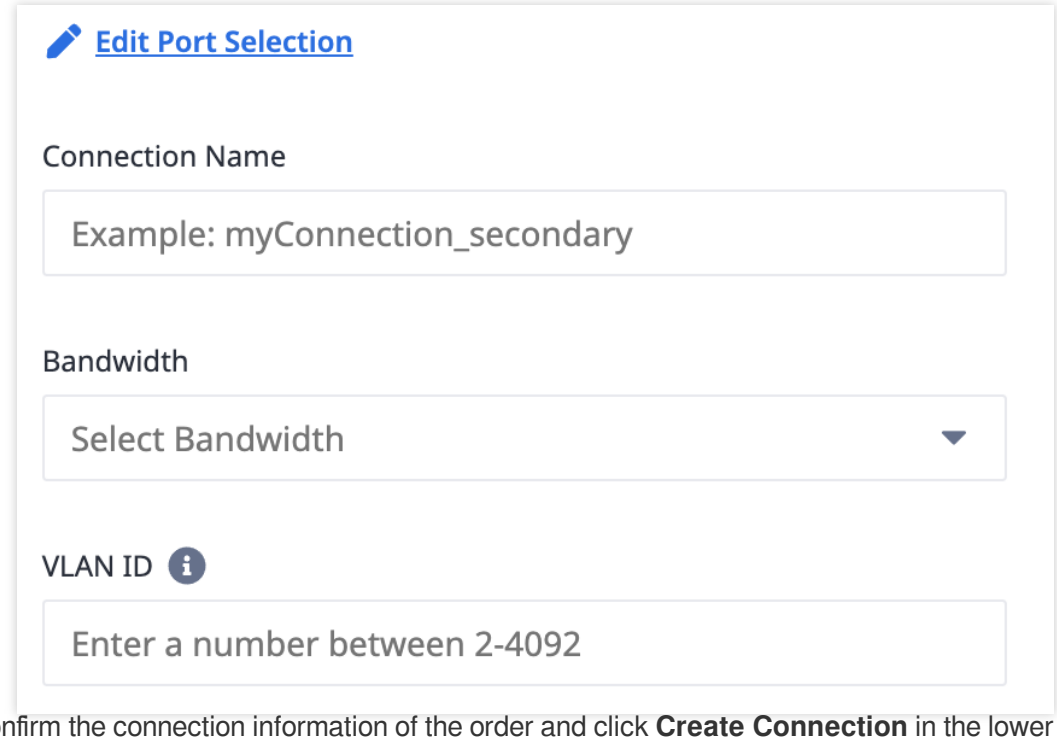


2. Configure the connection: Select Port from the drop-down list of Origin Asset Type.

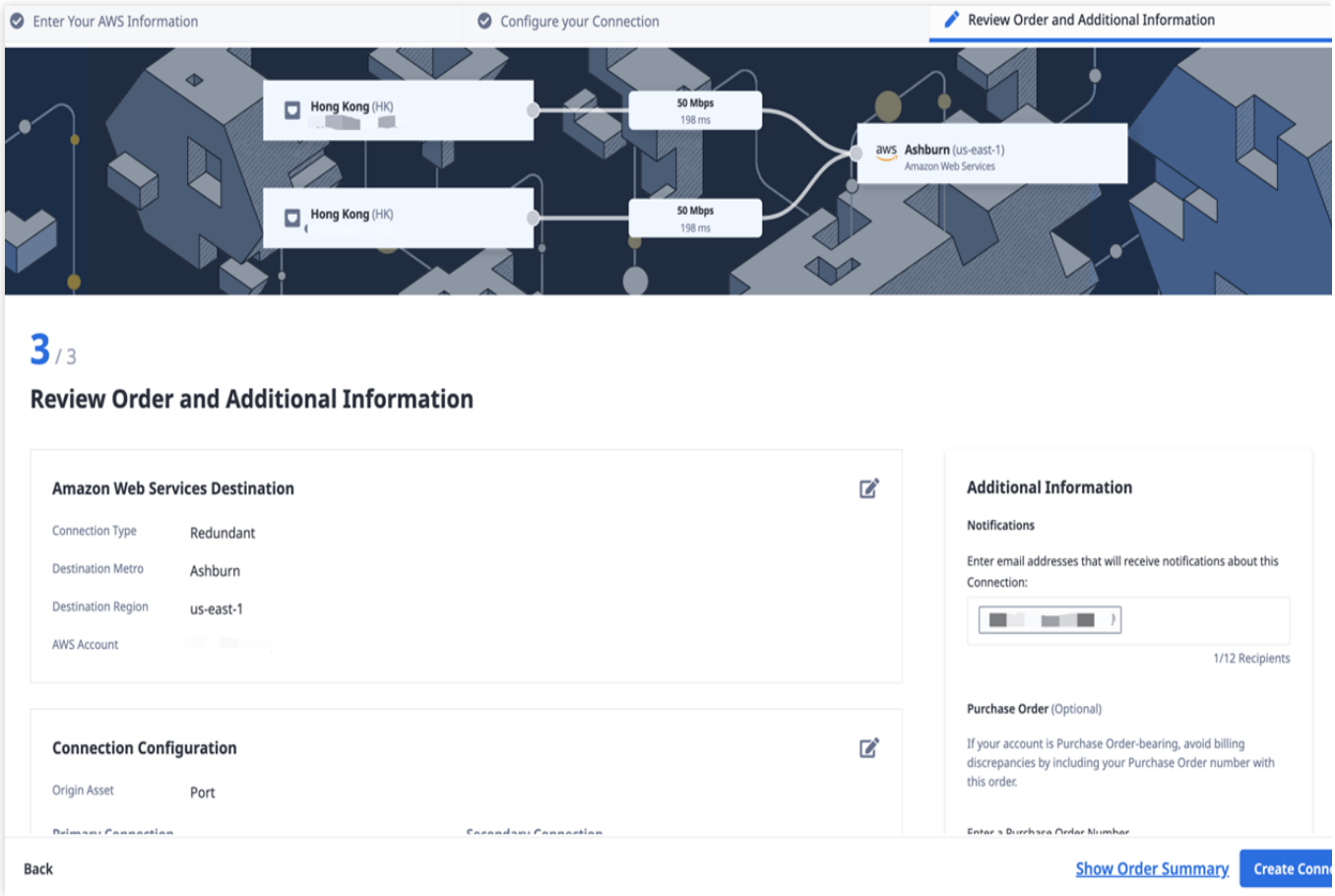
In the Primary Connection section: Click **+ Select Primary Port**, select the connection port in the pop-up window on the right and click **Select Port** in the lower right corner. Then enter the primary connection name, select the bandwidth and enter the customer VLAN ID and service VLAN ID.



In the Secondary Connection section: Click **+ Select Secondary Port**, select the secondary connection port in the pop-up window on the right and click **Select Port** in the lower right corner. Then enter the secondary connection name, select the bandwidth and enter the customer VLAN ID and service VLAN ID. After completing the form, click **Next**.



3. Confirm the connection information of the order and click **Create Connection** in the lower right corner.



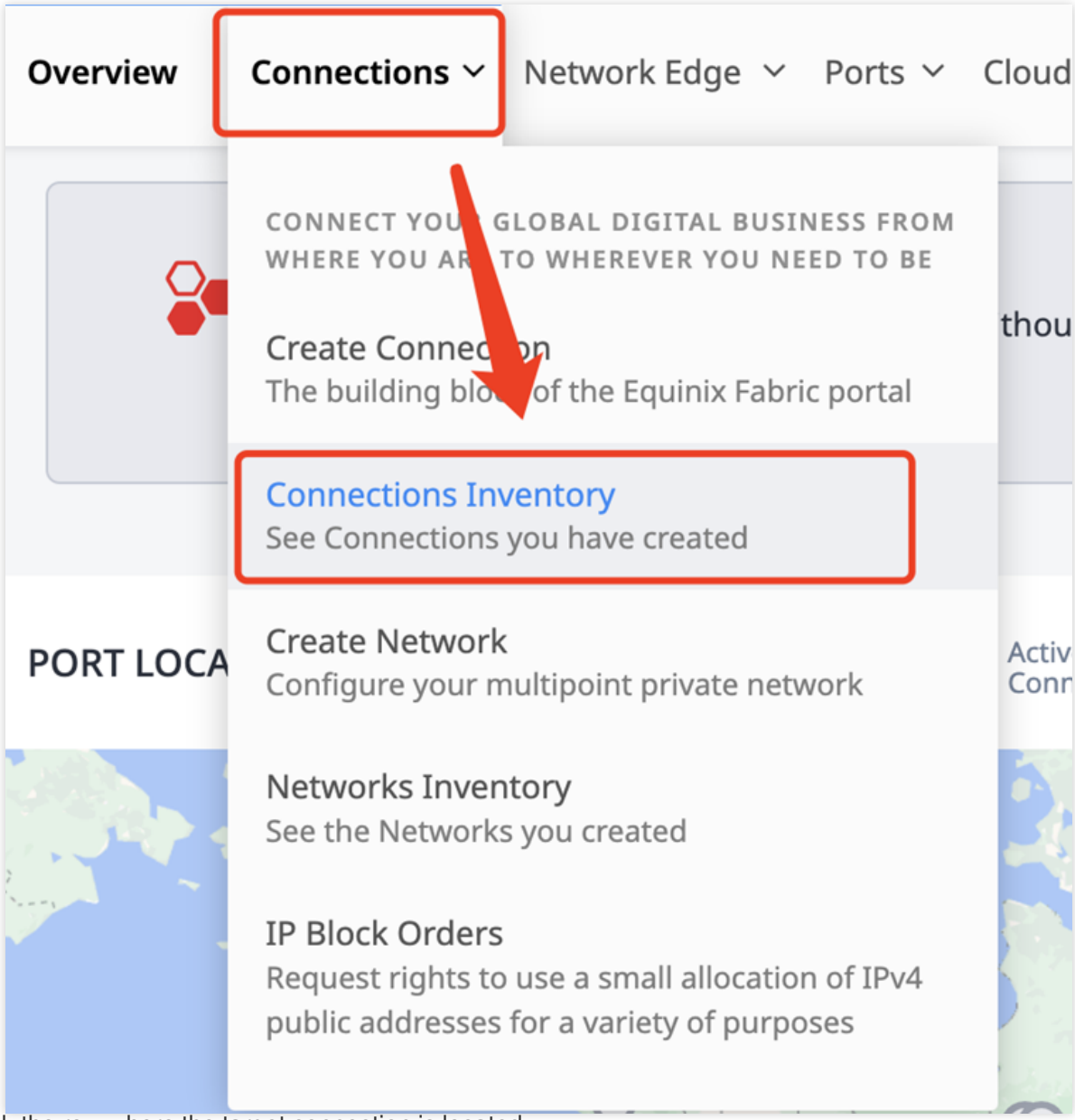
Confirming Connection

Step 1: Confirming an Order on the AWS Side

1. Log in to the Direct Connect console of AWS Cloud and click Connection in the left navigation bar to enter the connection list page.
2. Select the target connection and click View Details. Then select the Charge Confirmation checkbox and click **Accept**.

Step 2: Accepting Connection on the Equinix Side

1. In the drop-down list of Connection, select **Connections Inventory**.



2. Click the row where the target connection is located.
3. Click **Accept**.
4. Enter the Amazon access key and click **Submit**.