Using Flex Gateway to Build Site-to-Site VPN Through CT MPLS IPVPN Connection
01 Introduction

Flex is one of its kind Internet Gateway that provides added flexibility and manageability compared to any other public access Internet Gateways. It is easy to install and manage with multiple customization options for an excellent user experience in high demand public wired and Wi-Fi Internet access. This post explores how to use Flex Gateway to build site-to-site VPN through CT MPLS IPVPN connection.

02 Architecture of Site-to-Site VPN

The example below uses a real customer case study to illustrate the architecture:

The customer wants to connect their overseas data center to Alibaba Cloud through China Telecom (CT) MPLS link. CT is using a Cisco device to connect to Alibaba Cloud VPN Gateway in a VPC network by IPSec VPN connection.

03 Deploy VPN Gateway in VPC network.

Purchase & deploy VPN Gateway

Login to Alibaba Cloud marketplace site using your Alibaba Cloud account. In this tutorial, we will learn how to enable FlexGW VPN as a VPN server in a cloud VPC network.

Search for FlexGW VPN in the search box upon reaching the marketplace webpage:
Choose your preferred Pricing plan:
Choose your existing VPC and vSwitch instance, or keep the default configuration:

### Choose Network Type

<table>
<thead>
<tr>
<th>Network Type</th>
<th>VPC</th>
<th>Classic</th>
</tr>
</thead>
<tbody>
<tr>
<td>[default] vpc-23zro3bm4</td>
<td>[default] vsw-237712f4</td>
<td></td>
</tr>
</tbody>
</table>

Number of available private IP addresses: 4090

**Network Billing Type**
- **Data Transfer**

**Network Bandwidth peak:**
- 50 Mbps
- 100 Mbps
- 200 Mbps
- Public IP (unable to unbind) is distributed by system. If you do not need public IP, please select 0 Mbps bandwidth.
- If you need access public network with Elastic IP, please select 0 Mbps bandwidth, [Create Elastic IP](#).

---

### Choose the Operating System

<table>
<thead>
<tr>
<th>Public Image</th>
<th>Custom Image</th>
<th>Shared Image</th>
<th>Marketplace Image</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Products</strong></td>
<td><strong>Infrastructure &amp; Developer</strong></td>
<td><strong>Collaboration</strong></td>
<td><strong>eCommerce</strong></td>
</tr>
<tr>
<td>Hillstone Virtual NGFW Enterprise Edition</td>
<td>Wowza Streaming Engine 4.x.x</td>
<td>FlexGW IPSec VPN on CentOS</td>
<td></td>
</tr>
<tr>
<td>Hillstone Networks Corp</td>
<td>Wowza Media Systems, LLC</td>
<td>Shanghai Zhuyin Information Technology Co., Ltd.</td>
<td>0.0 USD/hr</td>
</tr>
<tr>
<td>The Hillstone CloudEdge Virtual NGFW Enterprise Edition provides essential NGFW features to Aliciou...</td>
<td>Wowza Streaming Engine is a media server software with ability to deploy on-premises or in the cloud,...</td>
<td>Shanghai Zhuyin Information Technology Co., Ltd.</td>
<td>0.0 USD/hr</td>
</tr>
<tr>
<td>Linux on CentOS</td>
<td>LAMP on Ubuntu 14.04 64bits</td>
<td>Advanced Linux for the Internet (LAMP)</td>
<td></td>
</tr>
<tr>
<td>It is a popular open source web environment consisting of Linux, Nginx, MySQL, and PHP software.</td>
<td>The most popular web service solution stack on the public internet. We, IOS, provide a list of images pr...</td>
<td>Shanghai Zhuyin Information Technology Co., Ltd.</td>
<td>0.0 USD/hr</td>
</tr>
<tr>
<td>Tomcat + Ngnix + My SQL SL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shanghai Zhuyin Information Technology Co., Ltd.</td>
<td></td>
<td></td>
<td>0.0 USD/hr</td>
</tr>
</tbody>
</table>

---

Previous | Next
Confirm your configuration then place your order:

<table>
<thead>
<tr>
<th>Product name</th>
<th>Instance configuration</th>
<th>Payment method</th>
<th>Subscription type</th>
<th>Number</th>
<th>Coupon</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECS</td>
<td>Region: China East 1 (Hangzhou)</td>
<td>Subscription</td>
<td>1 month(s)</td>
<td>1 unit(s)</td>
<td>Credit: $2,558.32 credit left (…</td>
<td>$0.00 USD</td>
</tr>
<tr>
<td>Marketplace Image</td>
<td>Image Name: FlexGW IPsec VPN on CentOS v2.5</td>
<td>Pay-As-You-Go</td>
<td>-</td>
<td>-</td>
<td>$0.00 USD</td>
<td>Hour</td>
</tr>
</tbody>
</table>

Price: $0.00 USD
Original Price: $32.98 USD
Saving: $32.98 USD

End User License Agreement

ECS Service Terms

General Terms

Place Order

Configure the VPC network environment and enhance the security protection

Go back to the ECS console and check that your ECS instance is up and running:

Change the default security group rules to enhance your application security.
Using Flex Gateway to Build Site-to-Site VPN Through CT MPLS IPVPN Connection

Add security group rules

- **NIC:** Internet
- **Rule direction:** Inflow
- **Authorization policy:** Allow
- **Protocol type:** TCP
- **Port range:** 22/22
  - The value range is 1-65535. E.g., "1/200", "80/80".
- **Authorization type:** Address field access
- **Authorization object:** 0.0.0.0/0
  - Please familiarize yourself with setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial
- **Priority:** 1
  - The priority value falls in between 1 - 100. Default value is set to 1 which is also the highest priority value.

Add security group rules

- **NIC:** Internet
- **Rule direction:** Inflow
- **Authorization policy:** Allow
- **Protocol type:** TCP
- **Port range:** 443/443
  - The value range is 1-65535. E.g., "1/200", "80/80".
- **Authorization type:** Address field access
- **Authorization object:** 0.0.0.0/0
  - Please familiarize yourself with setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial
- **Priority:** 1
  - The priority value falls in between 1 - 100. Default value is set to 1 which is also the highest priority value.
Using Flex Gateway to Build Site-to-Site VPN Through CT MPLS IPVPN Connection

05 Configure for Flex Gateway 2.5.0

Login

Login to the FlexGW portal (https://[your_ip_address]) with your ECS account root/[password]:

![Login Form]

Please familiarize yourself with setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial

The priority value falls in between 1 - 100. Default value is set to 1 which is also the highest priority value.
Create a VPN tunnel

Create an appropriate VPN tunnel by providing the necessary details:

**Flex Gateway 2.5.0**

- Tunnel id: CT_Aliyun
- IKE Version: IKEV1
- Auto Start: Manual
- Negotiation Mode: Active
- DPD action: None
- IKE encryption algorithm: 3DES
- IKE integrity algorithm: MD5
- IKE DH algorithm: Group 2 modp1024
- ESP encryption algorithm: 3DES
- ESP integrity algorithm: SHA1

**Save and finish the configuration.**

Check the tunnel list:
Click the “Connect” button and find the status updated from ‘Offline’ to ‘Online’.

**Notes:**
- **Local ID:** You must put this into the ECS public IP, not as an arbitrary ID name.
- **Local Subnet:** This is one of the several subnet CIDR addresses (separated by commas), corresponding to vSwitch CIDR. You cannot merge multiple CIDRs to a bigger CIDR address. For example, do not merge "10.6.10.0/24, 10.6.20.0/24, 10.6.30.0/24" to "10.6.10.0/16".
- **Remote Subnet:** This is one of the several subnet CIDR addresses, corresponding to customer side subnet CIDR. Similar to Local Subnet, you cannot merge multiple CIDR addresses to a bigger one.

### 05 Configure the Route table

In order to route all packages from VPC to customer side vlan, we have to add one route rule entry for each remote subnet.

The following is an example of the situation of routing several customer subnets (192.168.0.0/16 and 10.0.0.0/8). Click ‘Add Route’ and add two route items to VPC routing list.

![Image of route table configuration]

### 06 Conclusion

With that, we have successfully set up all resources and configurations with the link successfully connected. The tutorial expounded on how to use Flex Gateway to build site to site VPN easily and effectively.