Manual VPN
Huawei Cloud

Índice

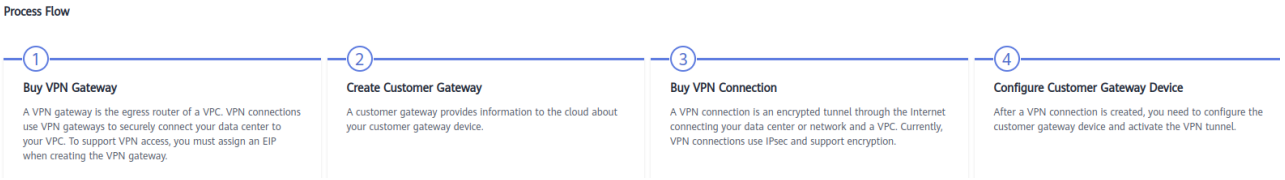
1. Introducción a Huawei Cloud

Puede utilizar el servicio VPN para conectar su centro de datos local a su VPC en la nube y añadir más capacidad de computación a su red aprovechando la escalabilidad y elasticidad de la nube.

Una conexión VPN entre su centro de datos y la VPC puede utilizarse para ampliar fácilmente la capacidad y el alcance de los servicios del centro de datos.

Las conexiones VPN encriptadas se crean a través de Internet para lograr unas comunicaciones seguras, fiables y rentables.

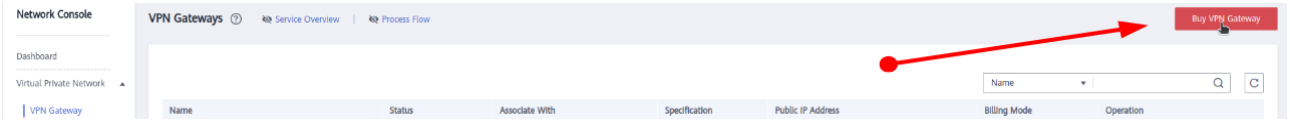
2. Flujo de Proceso para Creación de VPN



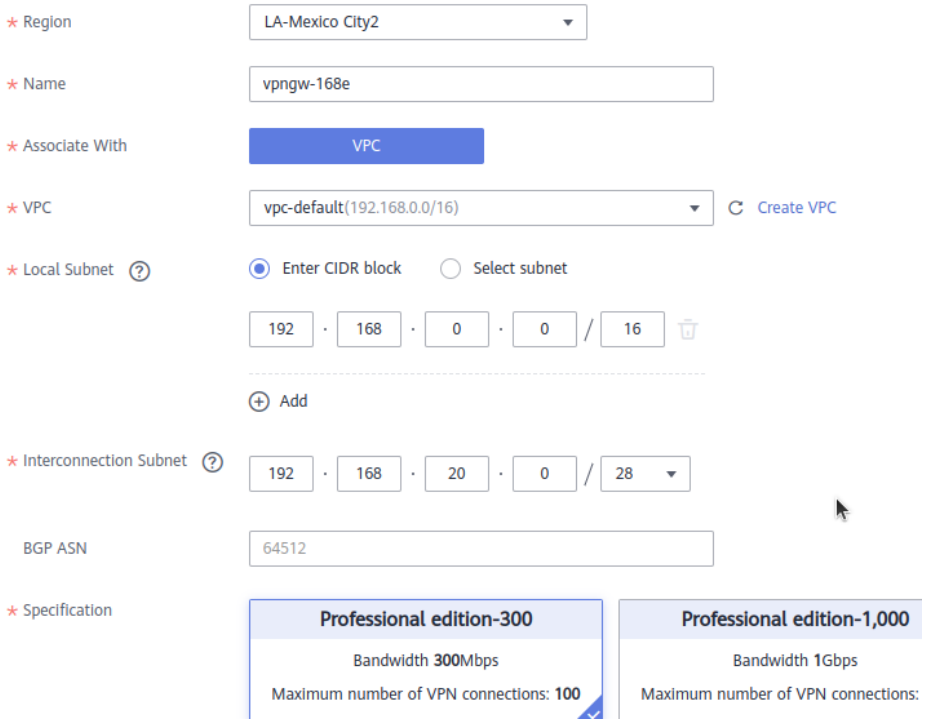
1) Creación del VPN Gateway
    a) Un VPN Gateway es el Router de salida de una VPC. Las conexiones VPN utilizan VPN Gateways para conectar de forma segura su centro de datos con su VPC. Para admitir el acceso a la VPN, debe asignar un EIP al crear el VPN Gateway.
2) Creación del Customer Gateway
    a) Un Customer Gateway provee la información hacia la nube acerca de su dispositivo en el Customer Gateway.
3) Creación de la Conexión de la VPN
    a) Una conexión VPN es un túnel cifrado a través de Internet que conecta su centro de datos o red y una VPC. Actualmente, las conexiones VPN utilizan IPsec y admiten el cifrado.
4) Configuración del Customer Gateway
    a) Una vez creada la conexión VPN, hay que configurar el dispositivo de la pasarela del cliente y activar el túnel VPN.

3. Creación del VPN Gateway

1. En la sección de “VPN Gateway” ubicada en “Virtual Private Network”, dar click en el botón rojo “Buy VPN Gateway”.



   a. Región (Ejemplo: Mexico City 2)
   b. Nombre (Ejemplo: Alias-STP)
   c. Asociación con (VPC)
   d. VPC (la VPC será en la que se albergarían los servidores de sus servicios)
   e. Subred Local (Subredes VPC que necesitan comunicarse con una red de cliente a través de conexiones VPN. El valor por defecto es una subred VPC, Ejemplo: 192.168.0.0/16, normalmente la comunicación con STP es Host-to-Host, es decir, IPs puntuales /32)
      1. En este apartado, puedes “Seleccionar Subred” que hayas agregado previamente.
   f. Subred de Interconexión (Subred VPC para la VPN Gateway, que no puede traslaparse con las subredes VPC en uso, Ejemplo: 192.168.20.0/28)



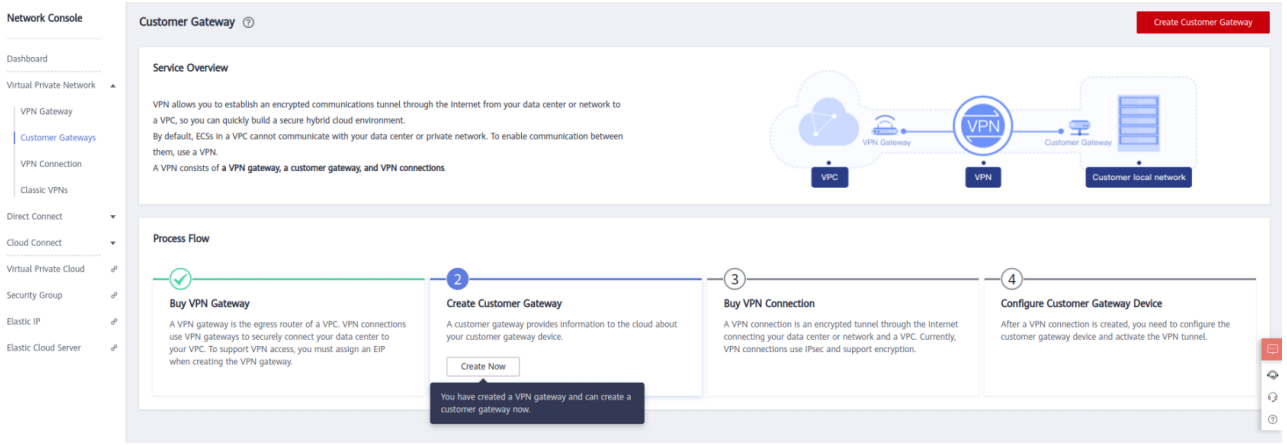
Vista de ejemplo en los parámetros previamente comentados.

Posteriormente, se configuran los apartados de los “grupos EIP (Elastic public IP)” que es enteramente a elección del cliente, ya que depende de las necesidades que se tengan.

Para continuar con el proceso, es necesario dar click en el botón rojo “Next” en la parte inferior izquierda de la pantalla.Y posteriormente se desplegarán los detalles del VPN Gateway creado.

4. Creación del Customer Gateway

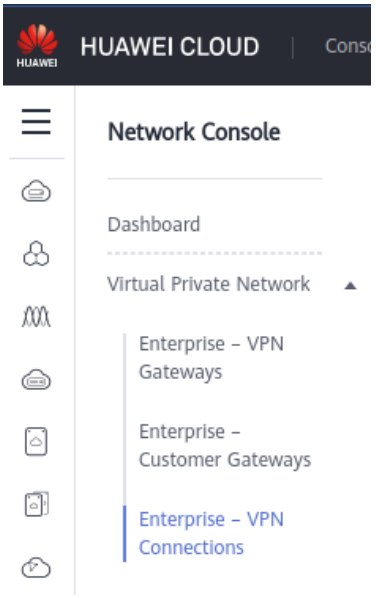
Como siguiente paso, en el apartado “Dashboard”, seleccionar “Customer Gateway” y posteriormente dar click en “Create Customer Gateway”.



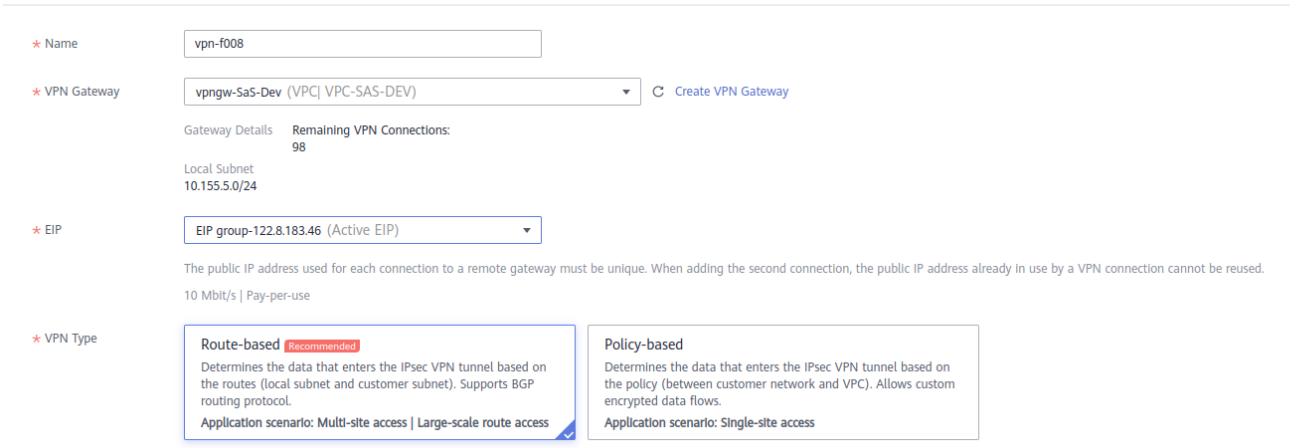
Aparecerá un recuadro con el “Nombre” que habrá que especificar como identificador, posteriormente en “Routing Mode” seleccionar “Static” por lo que en el apartado “Public IP Address” **hay que escribir la IP Pública proporcionada por STP en el “Formato de Alta de VPN”** en el apartado “Peer Remoto” de STP.

5. Conexión VPN-Gateway/VPN-Connections

En el “Network Console”, al desplegar “Virtual Private Network” aparece el botón “Enterprise - VPN Connections”, en esta pantalla, presionar el botón rojo “ Buy VPN Connection ” de la parte superior derecha.



En la siguiente pantalla nos aparecerá la configuración de esta conexión.

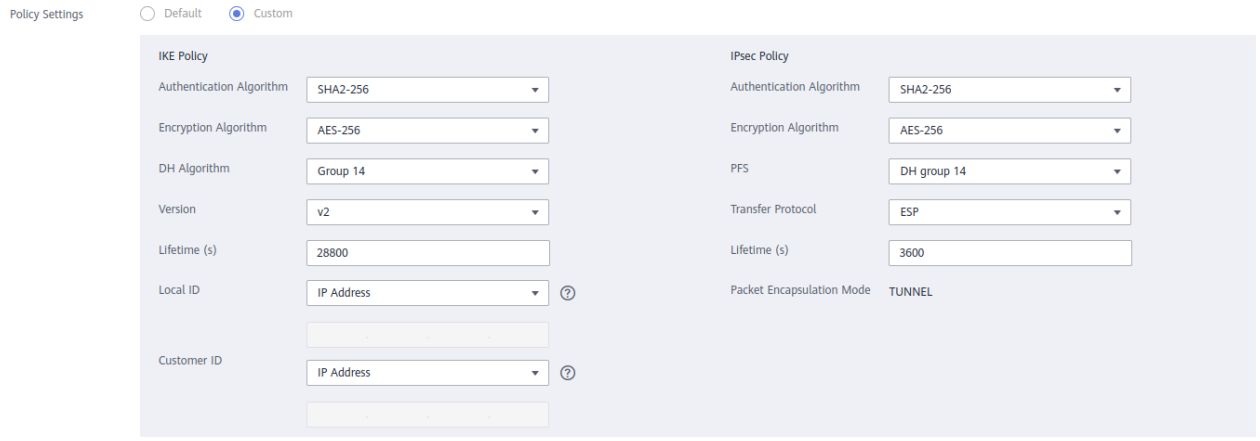


Name: Nombre representativo de la conexión.
VPN Gateway: Se utiliza el Gateway creado en los pasos anteriores.
Gateway IP address/EIP: Peer Local de la VPN que deberá ser compartido con STP mediante el "Formato de Alta de VPN".
Customer Gateway: Peer Remoto de la VPN que se encuentra en el "Formato de Alta de VPN" compartido por STP.
VPN Type: "Static Routing"/"Route Based".
Customer Subnet: Apartado de Redes Remotas (IPs /32) que se encuentra en "Dominios de Cifrado" en el "Formato de Alta de VPN".
Interface IP Address Assignment: Se recomienda usar la opción "Automatically Assign".
PSK: Llave pre-compartida, normalmente el equipo de VPNs de STP la comparte mediante una liga con un archivo encriptado por contraseña, esta se comparte una vez se proporciona el "Formato de Alta de VPN" mediante el ticket. En caso de ser generada de otra forma, favor de aclararlo durante alguna sesión o el hilo de correos del ticket.

Policy Settings: "Custom".

- **Authentication Algorithm (para IKE Policy e IPSec Policy)**: "SHA2-256" (viene especificado en el "Formato de Alta de VPN").
- **Encryption Algorithm (para IKE Policy e IPSec Policy):** "AES-256" (viene especificado en el "Formato de Alta de VPN").
- **DH Algorithm:** "Grupo 14" - **PFS:** "DH Grupo 14"
- **Version:** "v2" - **Transfer Protocol:** "ESP"
- **Lifetime (s) de IKE Policy**: "28800" - **Lifetime (s) de IPSec Policy:** "3600"
- **Local ID:** "IP Address"
- **Customer ID:** "IP Address"

Una vez terminada esta configuración, dar click en el botón  de la parte inferior derecha.



5. Aspectos importantes

- Por lo visto y por experiencia, Huawei Cloud al generar la VPN genera la ruta estática automáticamente, pero puede ocasionar algún problema y en situaciones muy específicas, que sea necesaria la intervención o cambio en dicha configuración.
- La mayoría de las situaciones hemos notado que al realizar pruebas de conectividad, no se terminan de concretar de STP -> Cliente, por lo que recomendamos realizar ping o pruebas de conectividad Cliente -> STP. Esto puede ayudar ya que “habilita” el túnel al existir tráfico en el túnel.
- Comúnmente es necesaria la configuración de “Security Groups” que se encuentra en el apartado “Elastic Cloud Server” -> “Cloud Server Console” -> “Security Groups”. Aquí se especifican las políticas de entrada o salida (Inbound/Outbound Rules) de su red de servidores.

6. Documentación relevante

- https://support.huaweicloud.com/intl/es-us/bestpractice-vpn/vpn_05_0001.html
- https://www.huaweicloud.com/intl/es-us/product/vpn.html
- https://support.huaweicloud.com/intl/es-us/vpn/index.html