



## ADVANCED VPN IPSEC

This is a VPN connection that connects the client's network with their cloud at Gigas via the internet by placing a device (FW, Router, VPN Appliance, UTM, etc.) at each point to allow an IPSec tunnel to be created between them. The VPN's most important features are:

- Performance bandwidth to 80Mbps\*
- Possibility of activating up to three IPSec tunnels sharing maximum traffic (e.g.: 1 tunnel: 80 Mbps, 2 tunnels: 40Mbps/tunnel, 3 tunnels: 25 Mbps/tunnel)
- Nat Traversal functionality (NAT-T)
- Highly compatible with any IP with the following protocols/ports: UDP/500, UDP/4500, ESP...
- Supports IKE v1 and v2
- Supports multiple encryption modes: key size up to 256 bits, with different AES modes, 3DES, SHA-2, authentication with shared RSA keys, etc.
- The traffic generated by the VPN does not consume the transfer contracted by the client with their Cloud Datacenter
- Automatic provision and management can be carried out on Gigas' control panel
- Automatic configuration using a form with handbooks and examples of configurations.

### ADVANTAGES

- » **Secure access from businesses to Gigas' cloud**
- » **Management of up to three independent tunnels at no extra cost**
- » **Provisions in real time**
- » **Automatic configuration**
- » **Free transfer**
- » **Free 30-day trial**

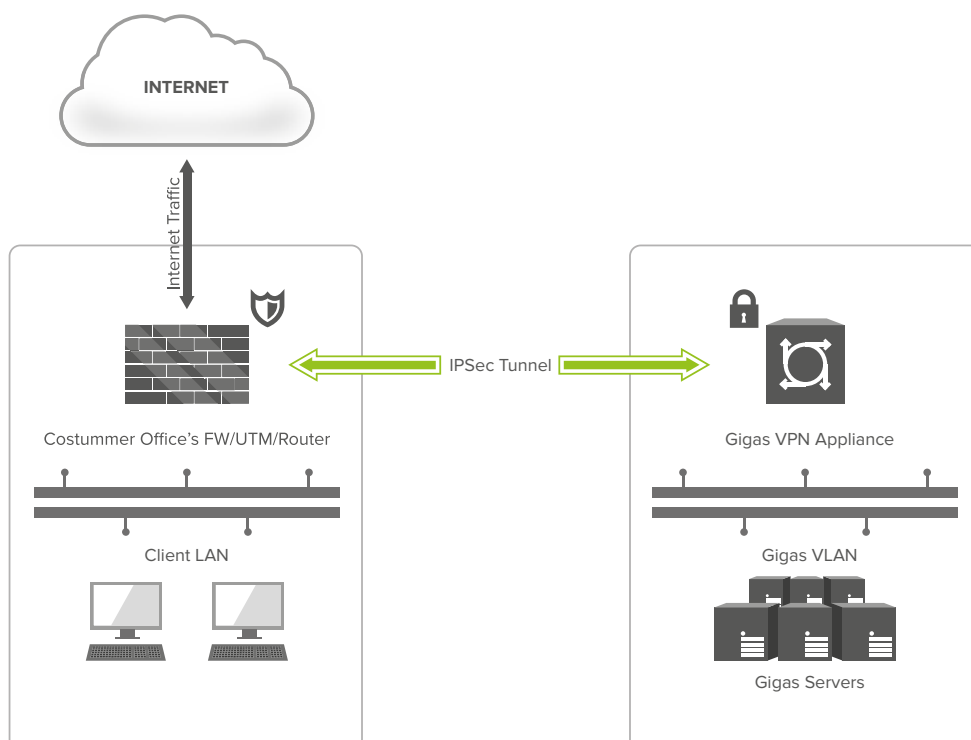
Client-side, the topology is completely seamless for Gigas: having a fixed public IP as a starting point for the tunnel and a device capable of lifting the tunnel is enough and allows the client to choose how and from which part of their network to connect.

In general, there are two types of scenarios: a basic scenario and an advanced scenario.

\*80 Mbps speed for VPNs provisioned in Madrid or Miami. In the case of VPNs provisioned in Chile, the speed will be 80 Mbps for national traffic and 10 Mbps for international traffic

### Basic scenario

This is a simple structure with a single FW/router or UTM to get the client's traffic to the internet and simultaneously raise an IPSec tunnel to their cloud with Gigas. This model only requires that the client's output device to the internet has a feature enabling IPSec tunnels to be activated.

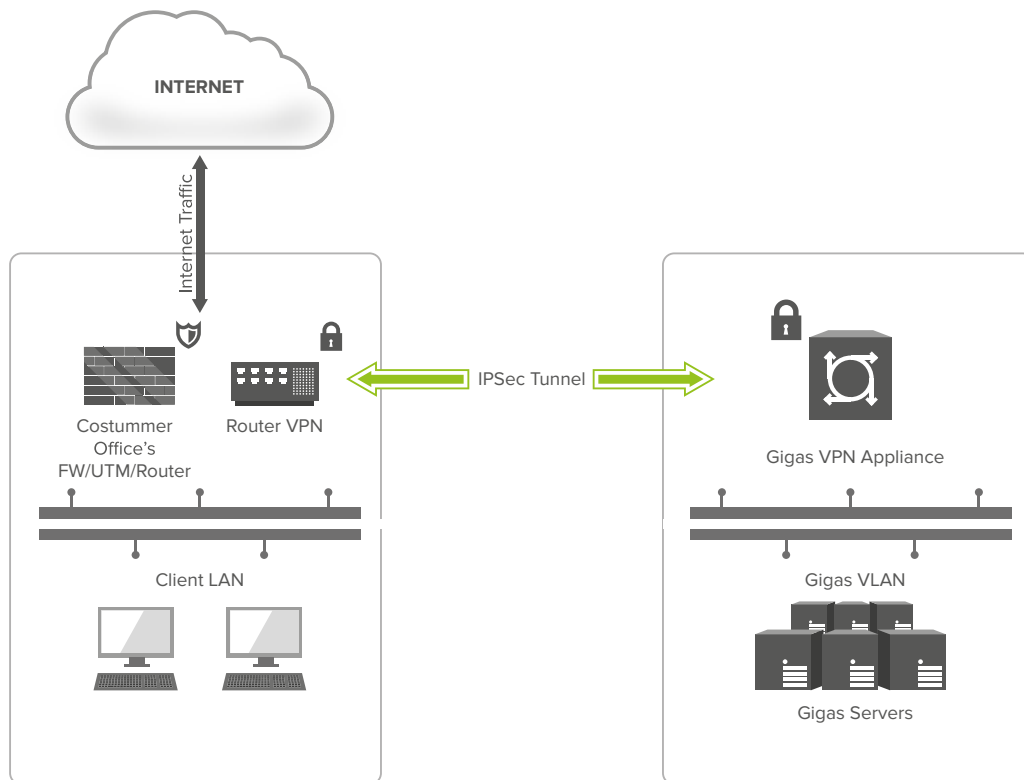




### Advanced scenario

This is a complex network structure where the placement of the VPN router is important. This network model requires determining in which part of the client's network the VPN router should be placed. It is advisable to place it in the nearest part of the network element that connects it to the internet (e.g. the DMZ). This configuration (called "on a stick") prevents traffic sent to the client's cloud from interfering with other communication traveling through the network.

It is therefore necessary to have a device to start the IPSec tunnel. This scenario can be of use if the equipment that links the client to the internet does not have an IPSec feature. By adding a UTM/router to the DMZ, a tunnel can be raised that adds a static route from the client's PCs to send VPN traffic via the new gateway.



#### España

Av. de Fuencarral 44, Edificio Gigas 28108 Alcobendas Madrid +34 91 769 60 00

#### Colombia

Carrera 7 No 67 - 39 Piso 4 Bogotá +57 1 381 9640 Carrera 43ª, San Fernando Plaza Medellín +57 420 40594

#### Chile

Av. Vitacura 2670, Piso 15 Las Condes Santiago +56 228 986 006

#### Perú

Av. Santo Toribio 115 San Isidro Lima 27 +51 1 641 9555

#### Panamá

Tower Financial Center Pl. 35 Calle 50 Panamá +507 836 6999 00

#### México

Av. Presidente Masaryk 29, 1er P. Col. Chapultepec Morales Ciudad de México 1157 52 55 8526 2500