ADVANCED VPN
/ technical datasheet

a gigas group company

ADVANCED VPN IPSEC

This is a VPN connection that connects the client's network with their cloud at ONI 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 80Mbits*
- Possibility of activating up to three IPSec tunnels sharing maximum traffic (e.g.: 1 tunnel: 80 Mbits, 2 tunnels: 40Mbits/tunnel, 3 tunnels: 25 Mbits/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 ONI' control panel
- Automatic configuration using a form with handbooks and examples of configurations.

ADVANTAGES

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

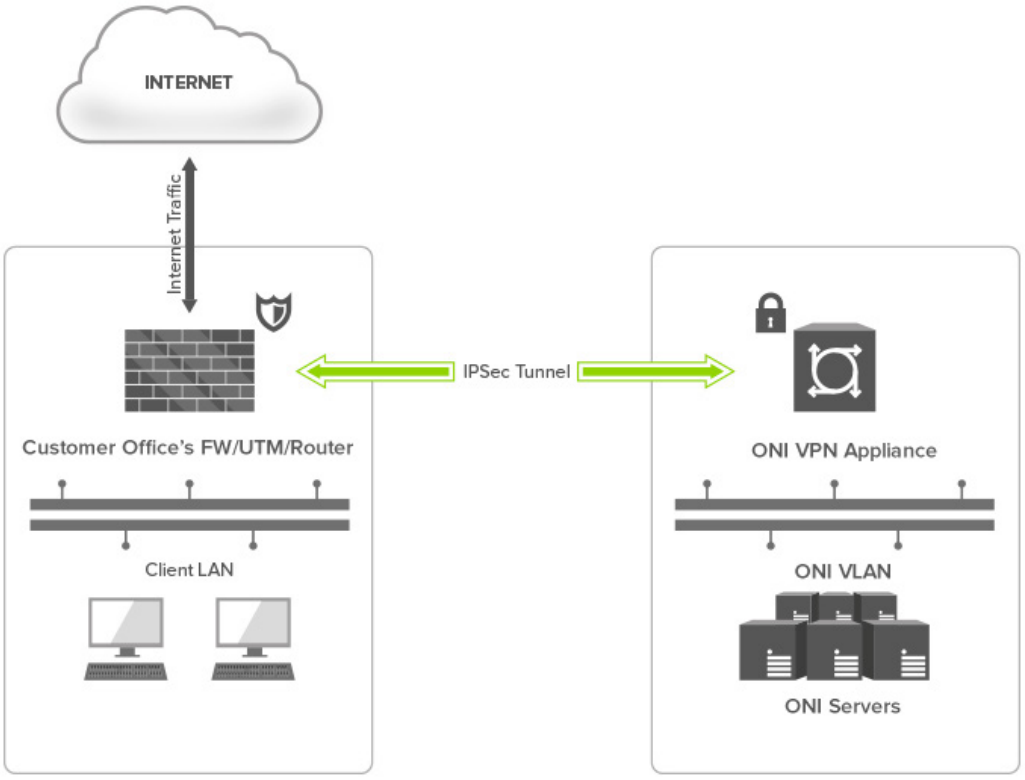
Client-side, the topology is completely seamless for ONI: having a fixed public IP as a starting point for the tunnel and a device capable of lifting the tunnel is enough and allows the client to choose how and from which part of their network to connect.

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

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