



## VPN IPSEC AVANZADA

Se trata de una conexión VPN que conecta la red del cliente con su red cloud en Gigas a través de internet, colocando en cada punto un dispositivo (FW, Router, Appliance VPN, UTM...) que permita establecer un túnel IPsec entre ellos. Las características más importantes de la VPN son:

- Rendimiento de ancho de banda hasta 80Mbits\*
- Posibilidad de activar hasta tres túneles IPsec compartiendo el tráfico máximo (ej: 1 túnel:80 Mbits, 2 túneles: 40Mbits/tunel, 3 túneles: 25 Mbits/tunel).
- Funcionalidad Nat Transversal (NAT-T)
- Amplia compatibilidad, alcanzando cualquier IP con los protocolos/puertos: UDP/500, UDP/4500, ESP...
- Soporte para IKE v1 y v2
- Soporte de múltiples modos de cifrado: llaves de hasta 256 bits, con AES en diferentes modos, 3DES, SHA-2, autenticación con compartición de llaves RSA, etc.
- El tráfico generado por la VPN, no consume la transferencia contratada por el cliente con su Cloud Datacenter
- Provisión automática y gestión desde el panel de control de Gigas.
- Configuración automática mediante formulario con manuales y ejemplos de configuración.

## BENEFICIOS

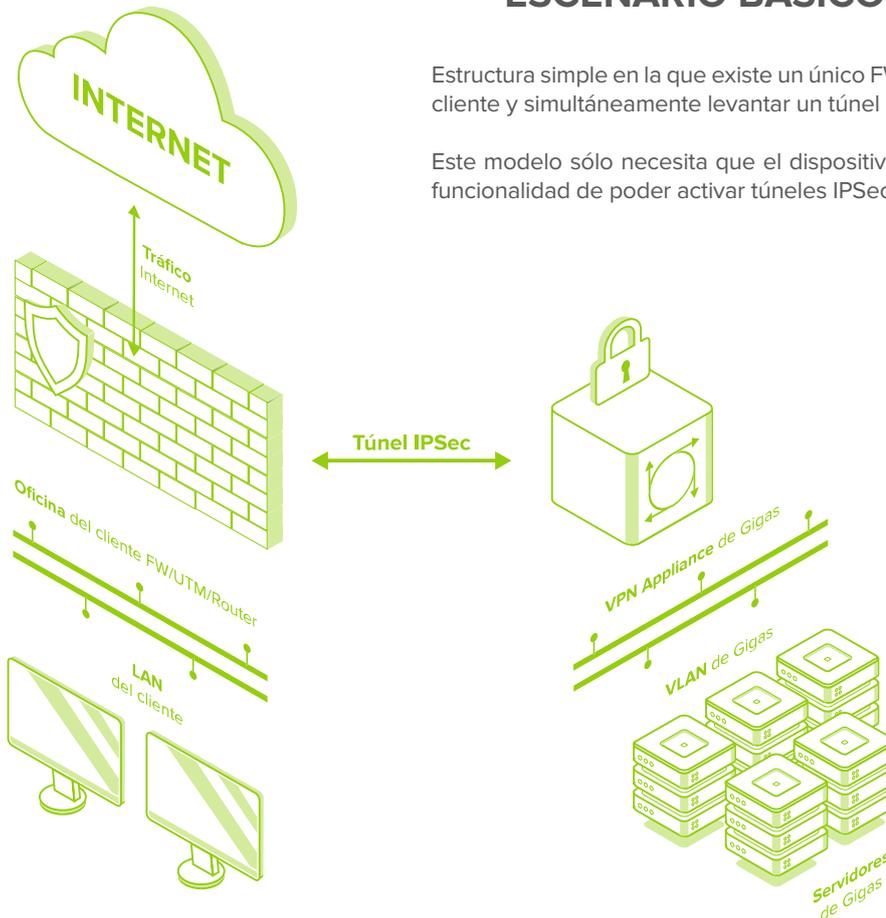
- Acceso seguro desde las corporaciones al cloud Gigas
- Gestión de hasta tres túneles independientes sin coste adicional
- Provisionamiento en tiempo real
- Configuración automática
- Transferencia gratuita
- Trial gratuito durante 30 días

En la parte del cliente, la topología es completamente transparente para Gigas: con disponer de una IP fija pública como punto de inicio del túnel y un dispositivo capaz de levantar el túnel es suficiente, permitiendo al cliente elegir cómo y desde que parte de su red conectar.

Por lo general, podemos encontrar dos tipos de escenarios: el escenario básico y el escenario avanzado.

\*Velocidad de 80Mbits para VPNs provisionadas en Madrid y Miami. En el caso de VPNs en Chile, la velocidad será de 80Mbits para tráfico nacional y de 10Mbits para tráfico internacional

## ESCENARIO BÁSICO



Estructura simple en la que existe un único FW/router o UTM para sacar el tráfico a Internet del cliente y simultáneamente levantar un túnel IPsec hacia su cloud en Gigas.

Este modelo sólo necesita que el dispositivo de salida a Internet del cliente disponga de la funcionalidad de poder activar túneles IPsec.



## ESCENARIO AVANZADO

Se trata de estructuras de red complejas, donde la colocación del router VPN adquiere cierta importancia. En este modelo de red, será preciso determinar en qué parte de la red del cliente colocar el router VPN. Lo recomendable sería situarlo en la parte más próxima al elemento de red que le conecte con Internet (la DMZ por ejemplo). Esta configuración (llamada "On a stick") tiene como objetivo que se envíe el tráfico con destino al cloud del cliente sin interferir en cualquier otra comunicación que viaje por la red.

Por tanto, será necesario disponer de un dispositivo para iniciar el túnel IPSec. Este escenario puede ayudar si el equipo que saca a Internet al cliente no tiene funcionalidad IPSec. Añadiendo un router/UTM en la DMZ podremos levantar el túnel añadiendo una ruta estática en los PCs del cliente para enviar el tráfico VPN por la nueva puerta de enlace.

