



É uma ligação VPN que liga a rede do cliente à sua rede na cloud da Oni através da internet, colocando em cada ponto um dispositivo (FW, Router, Appliance VPN, UTM ...) que permite estabelecer um túnel IPSec entre eles. As características mais importantes da VPN são:

- Largura de banda até 80Mbits *
- Possibilidade de ativar de um a três túneis IPSec partilhando o tráfego máximo (ex: 1 túnel: 80 Mbits, 2 túneis: 40 Mbits / túnel, 3 túneis: 25 Mbits / túnel).
- Funcionalidade Nat Transversal (NAT-T)
- Ampla compatibilidade, atingindo qualquer IP com os protocolos / portas: UDP / 500, UDP / 4500, ESP ...
- Suporte para IKE v1 e v2
- Suporte a vários modos de criptografia: chaves até 256 bits, com AES em modos diferentes, 3DES, SHA-2, autenticação com partilha de chave RSA, etc.
- O tráfego gerado pela VPN não consome a transferência contratada pelo cliente com seu Cloud Datacenter
- Provisão e gestão automáticos através do painel de controle.
- Configuração automática via formulário com manuais e exemplos de configuração

BENEFÍCIOS

- » Acesso seguro de empresas à cloud ONI
- » Gestão de três túneis independentes, sem custos adicionais
- » Provisão em tempo real
- » Configuração automática
- » Transferência gratuita
- » Trial gratuito durante 30 dias

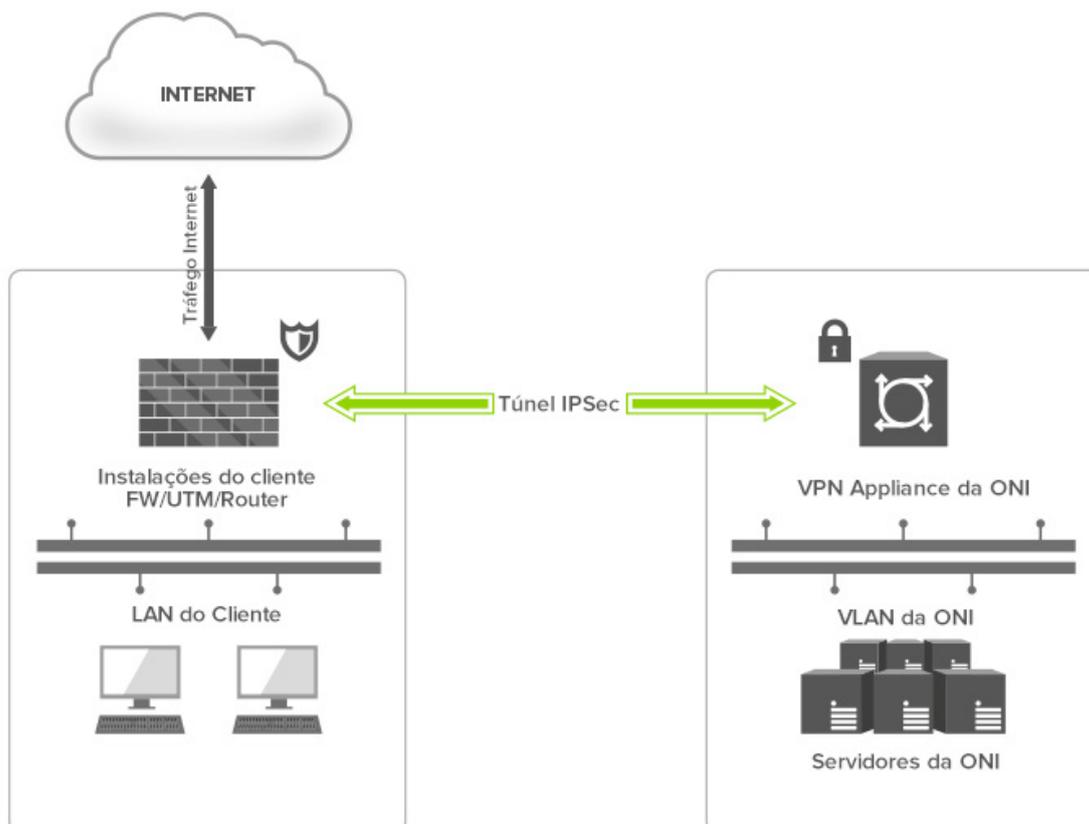
Do lado do cliente, a topologia é totalmente transparente para a ONI: basta ter um IP público fixo como ponto de partida do túnel e um dispositivo capaz de o estabelecer, permitindo ao cliente escolher como e de que parte da sua rede ligar.

Geralmente, podemos encontrar dois tipos de cenários: o cenário básico e o cenário avançado.

* Velocidade de 80Mbits para VPNs fornecidos em Madrid e Miami. No caso das VPNs no Chile, a velocidade será de 80Mbits para o tráfego nacional e 10Mbits para o tráfego internacional

Cenário básico

Estrutura simples na qual existe um único FW / router ou UTM para obter o tráfego de Internet do cliente e simultaneamente construir um túnel IPSec para sua nuvem na ONI. Este modelo requer apenas que o dispositivo de saída da Internet do cliente tenha a funcionalidade para ativar túneis IPSec.





Cenário avançado

Estruturas de rede complexas, nas quais o posicionamento do router VPN assume importância relevante. Neste modelo de rede, será necessário determinar em que local da rede do cliente deve colocar o router VPN. Será aconselhável colocá-lo na parte mais próxima do elemento de rede que o liga à Internet (a DMZ, por exemplo). Essa configuração, denominada “On a stick”, tem como objetivo enviar tráfego para a cloud do cliente sem interferir com qualquer outra comunicação que circule pela rede

Resumindo, ao adicionarmos um router / UTM na DMZ, poderemos construir e gerir o túnel IPSec, adicionando uma rota estática nos PCs dos clientes, para enviar tráfego VPN através do nosso Gateway, sem dependermos da capacidade dos equipamentos do cliente terem ou não esta funcionalidade.

