The Benefits of SIMETRY's Private APN

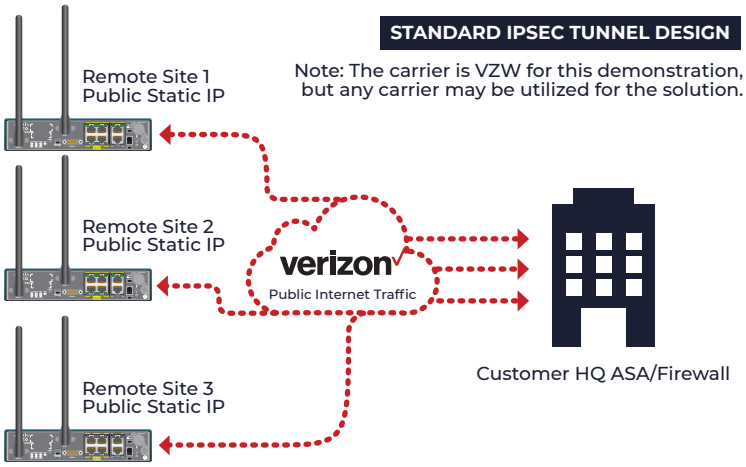
SIMETRY

Standard IPsec Tunnel Design

The most widely used and accepted form of connecting your remote traffic to a central demarcation is the use of IPsec. An IPSec tunnel allows for the implementation of a virtual private network (VPN) to securely extend connectivity beyond its own network to customers, partners, and suppliers. While this is a secure common practice, IPSec can be difficult to manage at scale.

Because every remote endpoint of an IPsec deployment has potential connectivity issues from packet loss, general network outages, latency, and network saturation; IPsec remote endpoints require manual intervention from IT network support teams to restore services. This can be labor intensive and time-consuming depending on the remote accessibility of the device and if local intervention is required to restore services. Furthermore, IPsec deployments require Public IP addressing to establish a secure tunnel between endpoints. While the use of Public IP addresses is very common in computer networking, you must maintain a high-level cyber security posture that is evergreen to new vulnerabilities that may compromise networks via Public IP addressing assigned to devices.

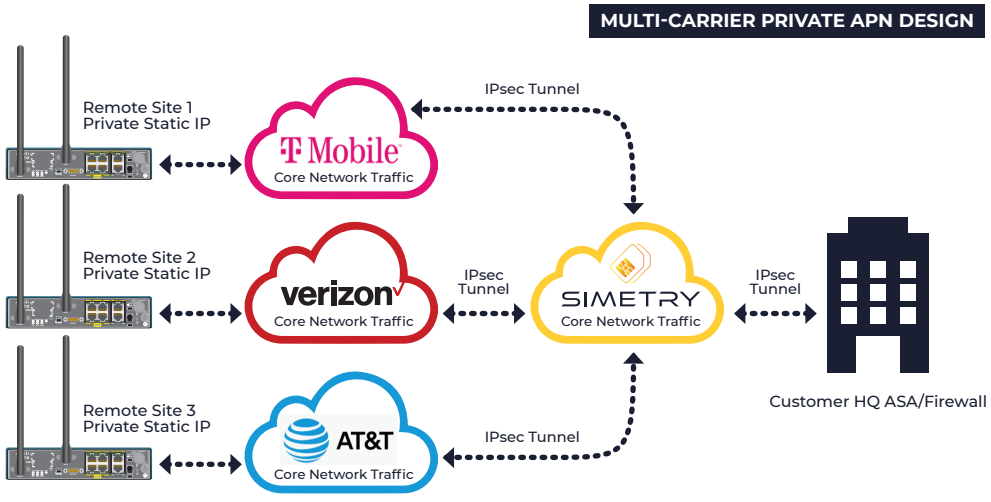
Lastly, with the turnover rate in the US averaging between 12%-15% annually, organizations must ensure credentials, configurations, and other proprietary configurations are constantly updated. In fact, 52% of businesses admit that employees are their biggest weakness in IT security due to simple careless actions. While deployments of IPsec tunnels on the remote endpoints are acceptable and common, the constant cyber-attacks on Public IP addresses, the burden of being ever vigilant of new vulnerabilities and maintaining best security practices, all while dealing with turnover and careless IT security practices makes managing a large-scale IPsec build-out for organizations difficult and potentially high-risk.



SIMETRY's Private APN

So, what is a private APN? APN stands for Access Point Name. It's a gateway between a cellular network and the Internet. With the APN settings in place, your device builds a connection to a carrier's gateway. Part of this process involves the carrier using a defined APN network to choose the assigned IP address(s) and security settings where applicable. To mitigate the risks of a standard IPsec design for IoT devices, SIMETRY has built a robust and secure private APN infrastructure with redundant interconnects to all the major carriers in the United States. SIMETRY's private APN's are pre-built and ready for use today, which will greatly reduce your mean time to deployment.

Your network will be assigned a secure private subnet and the remote devices will be assigned Private Static IP addressing, which is not accessable from the public internet. Once your network traffic is securely routed from the Mobile Network Operator (MNO) to SIMETRY over your private APN, SIMETRY can securely route the traffic to any cloud environment, data center infrastructure, or simply send the traffic to our internet gateways. This means you have full control of your remote network traffic with access to all major carriers, while consolidating the management of hundreds, if not thousands, of IPsec tunnels by simply managing a single redundant secure VPN tunnel with SIMETRY.



simetry.com/private-apn
1-833-SIMETRY
sales@simetry.com