ASAVIE

Secure Termination of Mobile and IoT Traffic in your Cloud or On-premise

Up to now, to secure access to the enterprise private network required a mobile based VPN client / digital credential per device. This required enterprise IT to install software on each mobile and assign unique digital credentials, with the additional cost of a credential life-cycle management solution.

At scale this becomes cumbersome and is tedious to maintain. Furthermore, current mobile VPN clients are less than optimal for IoT. The result is the use of disparate solutions to connect enterprise mobiles and IoT, creating potential security gaps within the enterprise.

Simplifying Secure Access with Asavie

Asavie securely connects mobile devices to a private mobile network, from which traffic can be routed and aggregated through a secure IPsec tunnel that can be terminated in both the corporate network and/or in the cloud.

Asavie's site-to-site IPsec reduces IT admin complexity by eliminating the need to install a VPN client per device and the need for unique credentials per enterprise mobile or IoT device.

The managed service offering caters for all fleet sizes, allowing enterprises to focus on what matters - running a safe and trusted business at any scale.

How are devices protected?

Asavie's private network IPsec termination offers the highest level of security, availability, reliability and redundancy.

The true end-to-end private network supports:

1. Device authentication into a dedicated private mobile network using RADIUS
2. Private static IP address assignment for mobile devices
3. Route based IPsec for ease of managing traffic destined for an IPsec tunnel
4. Security policies to regulate traffic in the end-to-end network
5. Industry standard compatible IPsec e.g. IKEv2, authentication - SHA, encryption - AES-256bit
6. Visibility and policy management for all device traffic

Cellular Devices

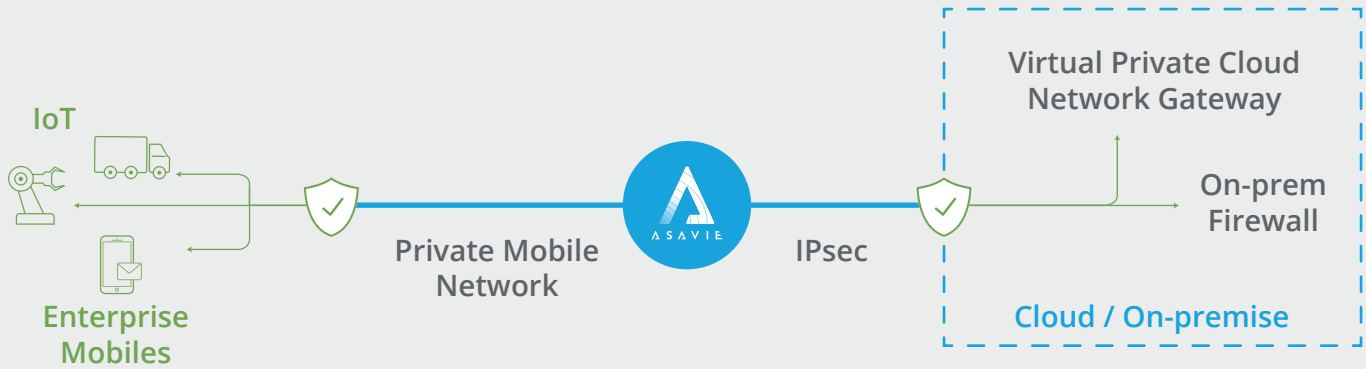


Figure 1: Asavie private networks with routed IPsec VPN, for true end-to-end trusted networks

Asavie's private mobile network service is unique, as it requires no additional software on the mobile device. Furthermore, IT admins get complete visibility and control of all mobile traffic, which includes traffic requests not destined for the IPsec tunnel.

High Availability (HA)

Multi-site fail-over including dead peer detection, support for HA of multi-cloud and on-premise termination.

Static Private IP Addresses

A self-defined, scalable pool of private IP addresses, that are unreachable from the internet, at no extra cost.

Visibility and Control

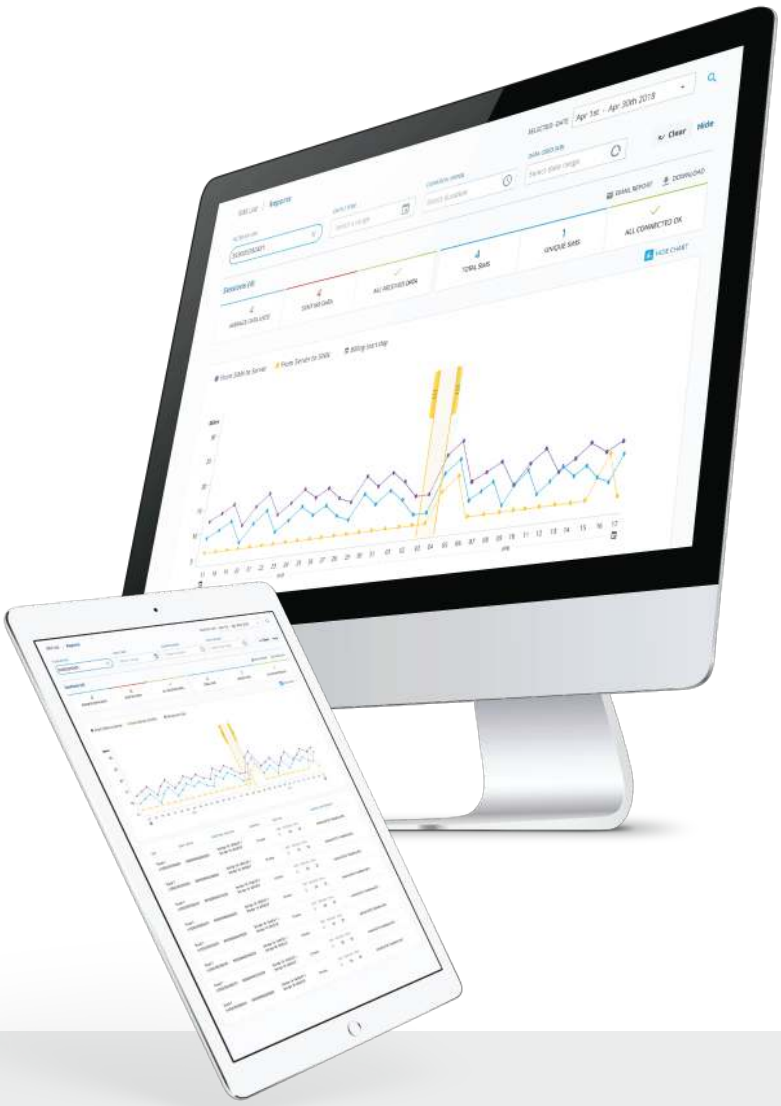
Gain visibility into every byte of data that mobile devices send, enhance security whilst lowering mobile expenditure.

No Software on the Mobile

With no software to install on the device and integrations with leading MDM/EMM solutions, IT admins can efficiently and effortlessly roll-out and manage the service to the entire enterprise mobile fleet.

Managed as a Service

Reduce IT burden with access to a support team dedicated to helping you succeed with your business connectivity needs.



Simplifying Complexity

Re-use existing security infrastructure and simplify secure access for mobile and IoT fleets, using just one set of IKE and SHA credentials.

Self-serve Portal

The intuitive web portal allows IT admins to manage secure connectivity from anywhere, with real-time policy settings.

Stay on Point

With no VPN clients on mobile devices and reduced maintenance effort, IT admins can focus on strategic business objectives.

ASAVIE