



IoT Services: Virtual Private Networks

With the growing emergence of the Internet of Things (IoT), businesses now have ready access to a world of valuable data not previously available. Essentially any physical device can become IoT-enabled by integrating cellular connectivity. However, failure to secure IoT device connectivity increases an organization's risk of a costly and embarrassing data breach.

A KORE VPN (Virtual Private Network) secures these connections by extending your company's private network out to cellular connected devices.

A VPN allows a company's application servers to communicate directly to cellular connected devices without requiring the devices to be directly connected to the Internet with public IP addresses. Additionally, the connection between the devices and the application server is encrypted end-to-end when a VPN is used, so sensitive data is secure while in transit over the Internet. By offloading the encryption function to the network, IoT device computing power is not wasted unnecessarily, as it is oftentimes very limited.



KORE VPN Options

KORE provides a wide range of VPN connectivity options for secure and reliable IoT data routing. KORE's leading solutions provide:

- Rapid and simple deployment
- Support for single-site or multi-site deployments with automatic failover
- Support for dynamic routing
- Protection from Internet-based DDoS and traffic flood attacks
- Standard AES-256 encryption
- 24x7 monitoring & support by KORE's global NOC.

With options available for any budget or need, your business can choose from the following to meet your specific requirements:

Cisco Easy VPN Software Client

The Cisco Easy VPN client can be loaded onto a customer computer to allow it to connect to the KORE IoT network. During the connection negotiation, the Cisco VPN concentrator located in the KORE network will assign the client a pre-determined private IP address which is considered the host IP address. Source and destination routing rules are in place to ensure only application server IP addresses and mobile device IP addresses associated with the customer account are permitted to communicate with each other.

While best suited for testing purposes, KORE's software VPN solution can also be used for smaller IoT application deployments:

Pre-Configured Cisco Router

KORE has partnered with Cisco to provide pre-configured VPN routers. Prior to shipment, KORE's network engineers configure the router for seamless integration into your company's network. Routers can be shipped as a redundant pair with pre-tested failover capability or as a standalone VPN appliance. Packages include a Cisco service agreement, network integration support, and 24x7 VPN tunnel availability monitoring. KORE offers a multitude of hardware options to meet any size IoT solution.

Customer Provided Router

If your organization already has a device that supports IPSec tunnels, it can be used to establish a VPN connection with the KORE network. KORE network engineers will collaborate with your company's technology staff to design a solution that works with your existing equipment. In order to enable VPN tunnel availability monitoring, customers are asked to provide the IP address of a host machine that is reachable through the newly created tunnel.

Cloud-Based Router

KORE can route data directly to your company's Amazon Web Services (AWS) or Microsoft Azure cloud deployment over secure, encrypted VPN tunnels. With this option, you can enable redundant, secure data routing to your AWS or Azure resources with no need for your own network infrastructure.

Custom Solutions

If the customer's solution requirements are not met by any of the above offerings, custom solutions are available. Any custom requirements are evaluated by a KORE sales engineer and network engineer and are quoted on a case-by-case basis.

Reliable Routing Between KORE and Customer Networks Delivers High Availability

BGP-4 queries routers and determines the fastest way to route data over the Internet. By providing multiple routes to georedundant data centers, your organization benefits from reliability, resiliency, and deterministic re-routing services.

Professional Services

KORE's Professional Services provide dedicated consultation, helping with difficult routing demands and special APN requirements. Available on an hourly or per-project basis, our team of experts have a deep knowledge of infrastructure, security and networking disciplines.

Security between the device and the Mobile Network Operator (MNO) network

Data transmitted between a device and the mobile carrier network is encrypted by the network.

Security between the MNO network and the KORE IoT network

The private APN is programmed into the devices and used by the device to indicate to the network its data should be routed to the KORE data center. Data is then routed through the carrier's private network to the KORE data centers via IPsec VPN tunnels and is secured by AES-256 encryption. Mobile device authentication and Mobile IP assignment is performed by RADIUS servers running within the KORE data centers. Each device is assigned a permanently reserved IP address which is unique to the device's SIM number and resident within a specific private mobile device IP range that is associated

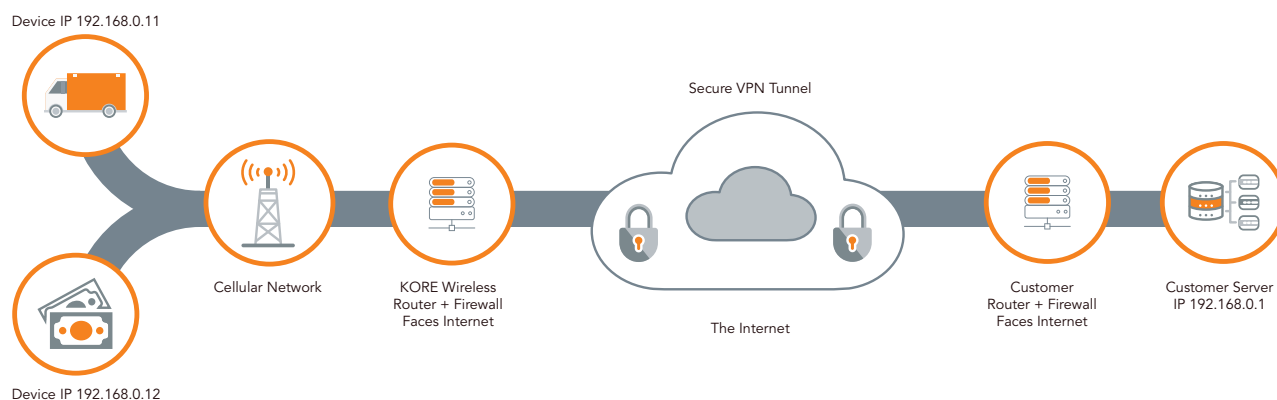
with the customer account. These mobile device IP ranges are specific to each customer account with no overlap permitted between accounts.

Security between the KORE IoT network and the customer network

Data is routed to the customer's data centers via IPsec VPN tunnels. All data transmitted over the VPN tunnel is encrypted by the customer's choice of AES-256 or 3DES encryption. Access Control Lists (ACLs) are used to only permit communication between the private network of the customer and specific mobile device IP ranges associated with the customer's account.

The combination of the dedicated VPN tunnels and ACLs allow KORE to separate the customer's device traffic and create the functional equivalent of a dedicated APN into a Mobile Network Operator (MNO).

Security



KORE VPN Service Options

Service	Description
Cisco Software VPN	Cisco Easy VPN access to KORE network for testing and small production deployments
Monitored Connection: Single-Site	Single-site VPN with KORE provided CPE and 24x7 monitoring
Monitored Connection: Multi-Site	Multi-site, redundant VPNs with KORE provided CPE and 24x7 monitoring
Single-Site VPN	Single-site VPN between KORE and customer provided equipment
Multi-Site VPN	Multi-site, redundant VPNs between KORE and customer provided equipment
Cloud Based Router	Direct routing of the customer traffic by KORE to the customer's AWS or Azure instance
Network Consulting (hourly)	Custom design and setup for specific customer's needs
Network Consulting (project)	Larger project based customization services and consulting

Reach out to KORE today to learn more about how our VPN services can secure and protect your IoT implementation.