www.pipelinepub.com
Volume 18, Issue 9

Reinventing Private APN for IoT

By: Jonas Bjorklund

In our previous article, Hyperscaling IoT Services, we argued why mobile operators should take a hyperscaler approach to enable the agility and global reach needed to provide cellular IoT connectivity services to demanding enterprise customers. We suggested that mobile operators leave their core network untouched and use services built upon hyperscalers such as Amazon Web Services (AWS) to extend their IoT connectivity offering. Here they can add a programmable and flexible layer of policy control, IoT security, and automation on top of their mobile infrastructure.

The good news is that vendors already offer this type of value-added functionality as an OPEX-based IoT connectivity control service (IoT CCS).

Mobile operators offer private APNs to their IoT enterprise customers, with the traffic terminated in an enterprise virtual private network (VPN). An enterprise VPN is a connection that is always on and where all traffic from all IoT devices flows, enabling devices to reach back-end applications and vice versa securely.

With an IoT CCS service, mobile operators can reinvent the concept of a private APN, which has previously been the only (costly) option for enterprises in need of added security and a virtual private network to reach their devices. Now mobile operators can take things one step further by providing a multi-tenant private APN. *Private*, because an enterprise VPN is used between the IoT CCS service and the enterprise network. *Multi-tenant* because mobile operators only have to extend one APN to their instance of the IoT CCS service to serve all of their customers with a secure virtual network.

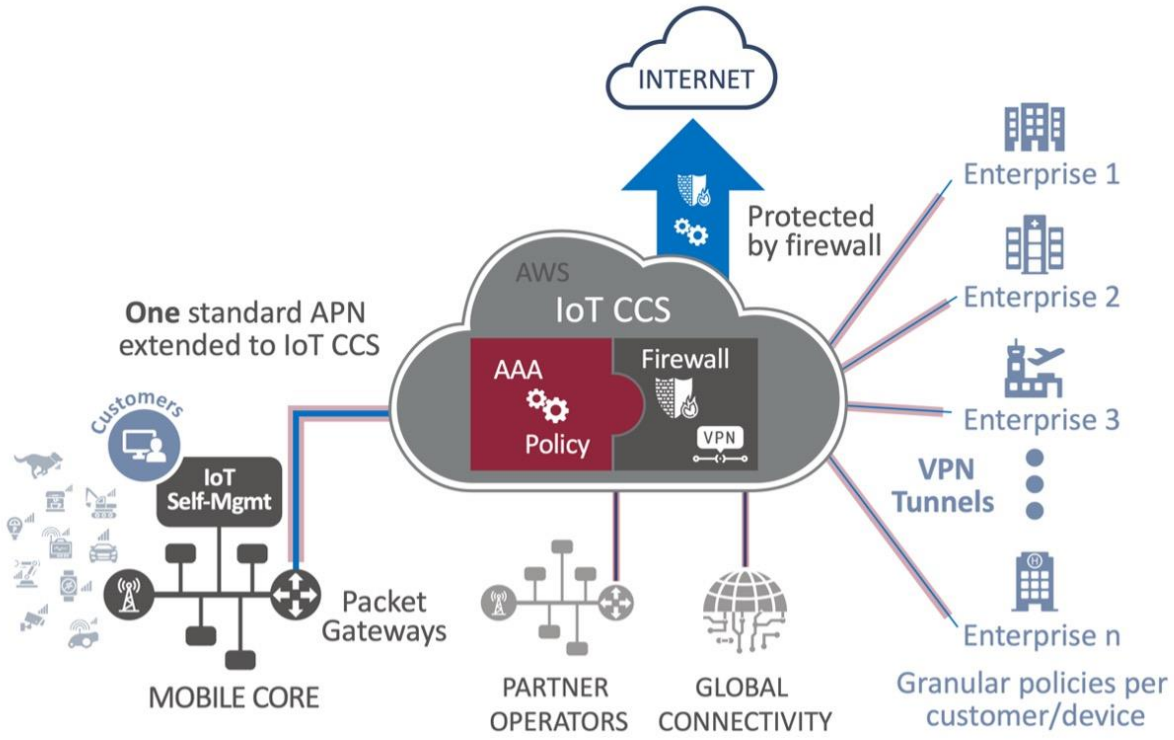

Figure 1: IoT connectivity control services
click to enlarge

Benefits for both mobile operators and IoT customers

An IoT CCS service allows mobile operators to scale by automating frequent processes. For instance, they can use customer self-service with automatic setup, enabling customers to create the VPNs themselves in minutes compared with the weeks, or even months, it can take to do this manually.

Using only one joint APN is also beneficial for mobile operator customers. If the customer needs to change the APN, the IoT device logic may need updating. Updating thousands of devices is not a straightforward operation, especially if they are in remote locations. The IoT CCS service reduces the need for these critical updates because the one APN can point to multiple VPN connections.

Furthermore, what enterprise customers want for their IoT devices is connectivity that provides the same amount of control and security as if they live on their own corporate local area network (LAN). The only problem is that with traditional cellular IoT, devices live on the mobile network. Most customers also require the connectivity to be extended globally. Therefore, a private APN with one mobile operator is simply not

enough. The answer is to utilize an IoT CCS service. It allows operators to easily extend the concept of private APNs to partner networks globally while providing the same firewall security. By adding global MNO partners and connectivity hubs to the IoT CCS service, they will be able to offer their IoT customers a secure global software-defined wide area network (SD-WAN) rather

than a private APN. Customers can get local break-out of the IoT traffic because mobile operators can quickly spin up an IoT CCS instance at any point of presence offered by the hyperscalers.

Such a secure global SD-WAN will match customer needs much better than a private APN as most IoT suppliers are international. IoT customers may also want to include their partner companies in their SD-WAN.

So, the mobile operator must deliver a secure and global SD-WAN for IoT to each customer under one contract and with one customer support.

Enterprises also need this IoT connectivity service to be unified across country borders with devices keeping the same IP address, policies, and security.

One enterprise VPN may not be sufficient, as many customers need to split the IoT traffic from a device into different VPN connections.

For global connectivity, some traffic may need to go out locally, protected by firewalls. Sensitive traffic such as firmware updates and analytics data may need to go securely in the SD-WAN delivered via enterprise VPN tunnels back to the IoT device vendor and their partners.

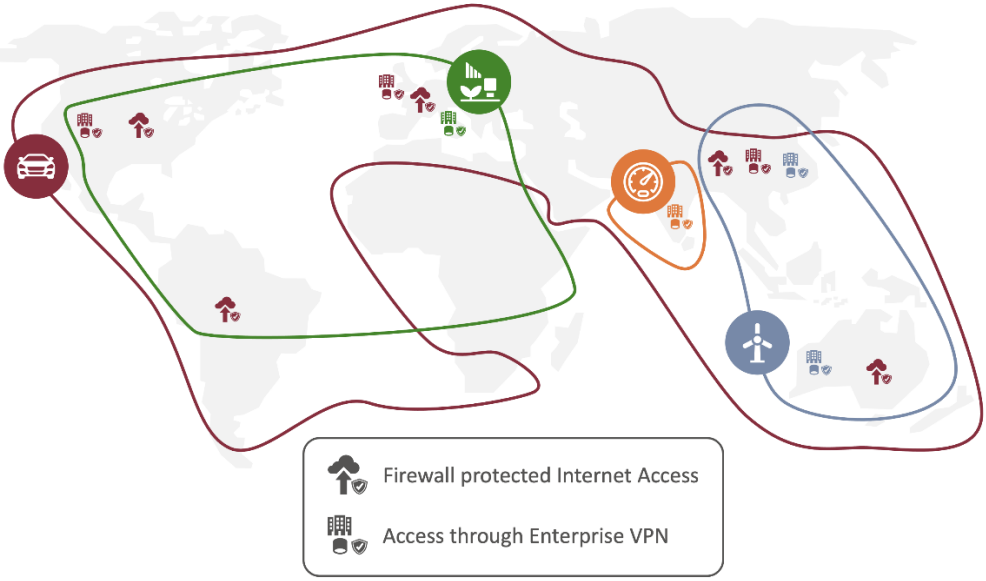

Figure 2: Reinventing IoT connectivity
click to enlarge

The service delivery and control must also be the same, whether the traffic goes through roaming or localization of eSIMs. Localization is a requirement in some markets for legal and commercial reasons. However, when a mobile operator localizes a device using eSIM, they lose control of the device to the local operator.

By connecting the local partner network to their instance of the IoT CCS service, mobile operators can keep control over the IoT device even when it has been localized. The traffic will be home routed by default using the same APN name. If local traffic break-out is required, the mobile operator can establish IoT CCS service nodes at the nearest location offered by the hyperscaler.

Delivering value to the enterprise customer

Usually, operators' mobile core and OSS/BSS teams prioritize stability before being fast on their feet, implementing every change requested by demanding customers.

Mobile operators can free themselves from these limitations with an IoT CCS service. It gives them the freedom to innovate IoT services that were impossible to achieve in a strict 3GPP environment. Mobile operators can easily tailor IoT connectivity services to the specific needs of different customer types. Let's examine a few customer cases and how a hyperscale IoT CCS service can help.

Automotive industry

A modern car is a hub of multiple IoT devices. These devices come from subcontractors of suspension, batteries, brakes, security systems, entertainment systems, and more. They all need private connectivity for firmware upgrades and

predictive maintenance. This is the perfect use case for providing a secure SD-WAN rather than one private APN connection. With an IoT CCS service, the car manufacturer can include partner companies in their SD-WAN to securely deliver their information through VPN. There may also be a need to have localized Internet. An IoT CCS service can potentially route the Internet traffic to the home country's Internet break-out to enable users to, for example, watch their Netflix content while abroad.

The automotive industry generally has skilled IT teams that want to do advanced integrations through APIs. This request is much easier to deliver on through a cloud-based service than trying to integrate with the mobile core. For special cases, mobile operators can even isolate delivery to a separate instance of the IoT CCS service.

Small and medium enterprises (SME)

The SME segment is the direct opposite of a car manufacturer in the sense that these companies may have no IT resources at all, and they might only have a handful of devices.

Take a small taxi and transport company as an example. They may run a few legacy systems that always need to have contact with the cars. These systems might have limited security functions if they have not yet been updated to current security requirements. They could benefit greatly from operator-managed security and delivering their traffic through a managed firewall.

There's a massive volume of potential customers in the SME segment, but each customer does not contribute much revenue. So, this is a volume game where automation is the key. To make it a profitable business, a mobile operator needs to automate the IoT connectivity service delivery to the SME market. Customers must be able to handle their own settings. For self-management to work, service providers must provide a super easy-to-use user interface in a portal or an app, with all the settings customers need.

The flexibility in integrating such user interfaces and the security provided by firewalls make an IoT CCS service ideal for this segment.

Utilities

A customer may need to connect hundreds of thousands, maybe millions, of IoT devices such as electrical meters. The devices are simple and cheap, so they often lack security features. At the same time, these devices have a vulnerable position in people's homes. Thus, they need to be protected by firewalls and have the traffic delivered through enterprise VPNs. An IoT CCS service will potentially also be able to detect anomalies in traffic patterns.

Global transportation and logistics

An IoT CCS service can be a game-changer for global transportation and logistics if combined with the mobile operator's ability to localize eSIM to international partner networks.

First, let's look at an international transportation company with trucks frequently crossing borders. A mobile operator can connect all their partner MNOs to the IoT CCS service. The transport company will get a unified global secure connectivity. Where needed, this can be done without roaming using localization of eSIMs, while the mobile operator maintains the control. The truck will, for instance, maintain its IP address, policies, and security across borders even if the eSIM needs to be localized.

The benefit for global logistics is even higher. Imagine freeing working capital by storing only one version of the IoT device instead of individual versions for each country or region. Doing this under one mobile operator contract and still being able to apply the same security and policies, through the IoT CCS service, across the board is a unique value proposition. Add to this the possibility of allowing some of the traffic to break out in the local country and some routed home in secure VPNs.

In both cases mentioned, the mobile operator must go beyond roaming and localize eSIMs over-the-air (OTA) to local subscriptions. This will eliminate the issue of networks blocking customers' IoT devices due to breaches of regulations and commercial agreements that prohibit permanent roaming.

The cost savings potential

An IoT CCS service is a vital component of what the analyst firm Transforma Insights calls "Hyperscale IoT Connectivity." In this report, the firm states that an enterprise can save on average the equivalent of 27.8 percent of the cost of global IoT connectivity when using a mobile operator that offers hyperscale IoT connectivity. This equates to an astonishing $117 billion globally between 2020 and 2030. Consider this as 117 billion reasons why mobile operators should go hyperscale.