SOLUTION BRIEF

Aptilo IoT Connectivity Control Service™ (IoT CCS)

Because You Don't Need Another Mobile Core! Mobile Operators Can Leave Their Mobile Core Untouched and Create IoT Connectivity Services Previously Considered Unthinkable

Joint Solution Components

- FortiGate Next-generation Firewall (NGFW)
- Aptilo Networks Carrier-class Systems (CCS)

FORTINET FABRIC-READY

Executive Summary

Fortinet and Aptilo have partnered to deliver a fast, secure, and highly flexible solution for mobile network operators to deliver highly profitable services and keep up with IoT customer demands. The integrated offer, called Internet-of-Things (IoT) CCS, combines the award-winning FortiGate next-generation firewall (NGFW) with Aptilo's carrier-class systems providing mobile network operators (MNOs) with a non-disruptive IoT solution for both existing and next-generation 5G architectures.

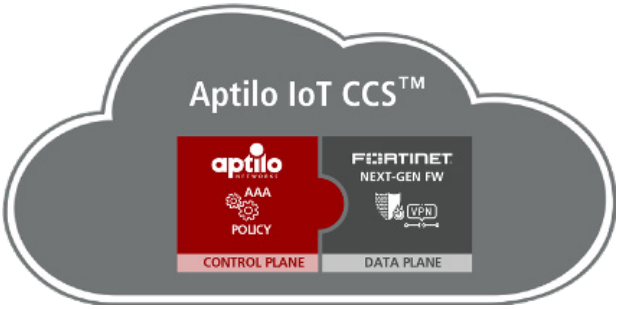
Most mobile operators' core networks are purpose-built for traditional consumer mobile services and a handful of different subscription types. They use a few predefined policies, which are not always suitable for IoT services. IoT customers often need more flexible services and thus their own unique subscriptions; subscriptions with complex, dynamic connectivity, and security policies. Furthermore, IoT business customers want to sit in the driver's seat and manage their own security and policies.

The ability to offer these kinds of instant, customized IoT connectivity services is therefore very challenging. In practice, it is nearly impossible to achieve these kinds of complex services in the current mobile core.

Many IoT customers need secure communications through private access point names (APNs). Handling private APNs is a hassle for mobile operators. It is one thing to create an APN for a utility company with millions of meters, but doing so for thousands of customers in the upcoming IoT mass market? This will just not scale!

To keep up with IoT customers' demands, we have seen mobile operators building a dedicated mobile core just for IoT. But is this really necessary and can the additional cost be justified? Is it even sufficient? One of Aptilo's IoT Connectivity Control Service™ (CCS) customers, a Tier 1 mobile operator, stated that they couldn't get the IoT connectivity management they needed even with a dedicated IoT mobile core. It was not possible to deliver flexible and cost-effective global IoT connectivity services to their customers. And, just think about the additional cost of duplicating mobile core nodes and to scale for capacity in two places.

This is why we created the Aptilo IoT CCS where Aptilo is managing the control plane and Fortinet the data plane.



Joint Solution Description

With Aptilo IoT CCS, which includes Fortinet FortiGate next-generation firewalls (NGFWs) as an integral part, mobile operators can add an IoT connectivity control, and security layer for their IoT services on top of the existing mobile core. Best of all, it will work with the coming service-based 5G core (5GC) architecture. It also adds a lot of value to existing IoT roaming platforms such as Ericsson DCP and SIM connectivity management platforms such as Cisco Jasper. Aptilo IoT CCS is based on Aptilo's IoT Connectivity Management Platform—Aptilo SMP™. It is delivered as a service from Amazon Web Services (AWS), turning it all into an operational expenditure (OpEx).

The Aptilo CCS enables new and innovative IoT services: new kinds of IoT services that you have never seen before—in a matter of days rather than months and to a fraction of the alternative costs.

Aptilo has been working in the control plane of wireless services since 2001. Aptilo is now a member of the Fortinet Fabric-Ready Technology Alliance Partner Program, which harnesses the power of Fortinet open application programming interfaces (APIs) and the ability to deliver simple, more integrated solutions to our joint customers.

"We have selected Fortinet's FortiGate next-generation firewall for its fast and secure architecture built on their custom security ASICs and advanced OS that runs throughout Fortinet's Security Fabric."

Jonas Björklund, CTO, Aptilo Networks

Through the Fortinet FortiGate, Aptilo IoT CCS gets policy enforcement at the edge, routing, virtual private network (VPN) management, device traffic filtering, protection against distributed denial-of-service attacks (DDoS), limitation of the number of transmission control protocol (TCP) connections, and more. The detection of anomalies are also part of the Aptilo IoT CCS security in this tight integration between Aptilo and Fortinet platforms.

The Aptilo CCS multitenancy virtual APN completely removes the complexity with setting up individual private APNs for each customer. A mobile operator only has to connect **one** standard APN to Aptilo CCS to serve **all** customers that are connected to the Aptilo IoT CCS through standard VPNs.

Using the same APN name, mobile operators can add international mobile operator partners to their Aptilo IoT CCS service. Combined with their ability to instantly localize eSIM (eUICC) OTA, operators can offer a truly global connectivity without roaming charges.

Through the Aptilo CCS multitenancy virtual APN, operators can offer a secure international connectivity with optional breakout for selected traffic at the nearest AWS point of presence. This is a unique capability that is virtually impossible to obtain in the standard 3GPP core with home routing as the typical option.

Joint Solution Benefits

- **100% OPEX:** An IoT connectivity control and security layer on top of any existing and future mobile core, delivered as a service from Amazon AWS.
- **Innovation:** Enables creative IoT connectivity services adapted for each business customer. Delivered in days rather than months.
- **Avoiding APN hassles:** Only one standard APN to Aptilo CCS is required to serve all customers which are connected to the Aptilo IoT CCS through standard virtual private networks (VPNs).
- **Self-service:** Mobile operators can provide customer web self-services using Aptilo's extensive representational state transfer (REST) application programming interfaces (APIs).
- **IoT Security:** Mobile operators can offer IoT security as a service powered by Fortinet's comprehensive portfolio of services.
- **Global connectivity:** Mobile network operators can add international mobile operator partners to their Aptilo IoT CCS service and localize the eSIM (eUICC) over the air (OTA). Lower latency is achieved with policy-based traffic breakout at AWS' point of presence.

Diagram of Joint Solution

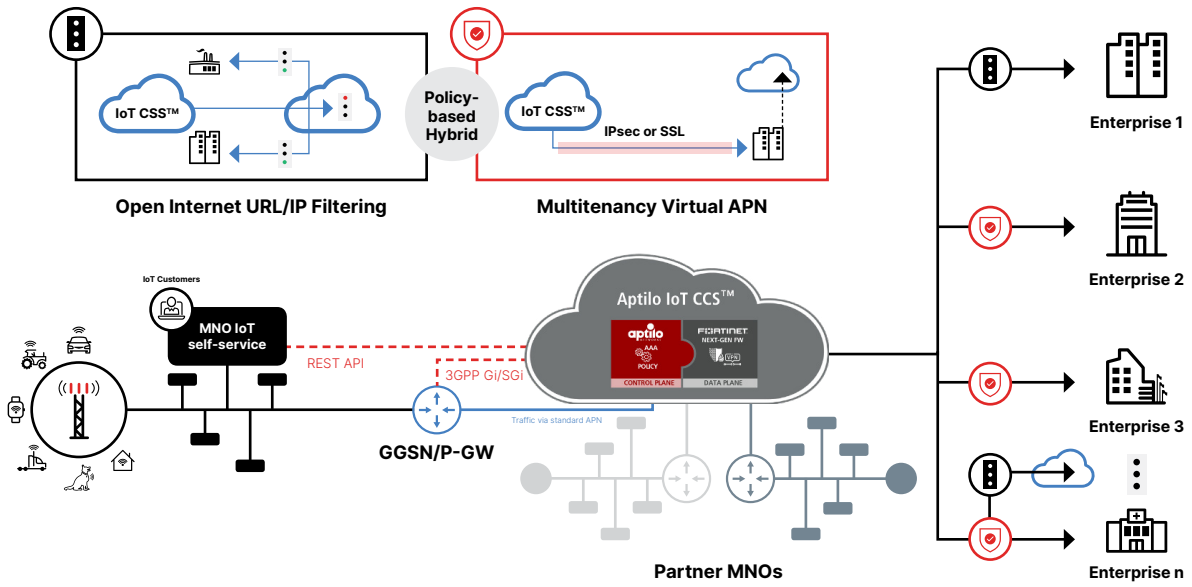


Figure 1: All traffic from MNOs to IoT CCS through single standard APNs. Signaling through standard 3GPP Gi/SGi interface. Customer self-service connected through REST API.

Added Security Also for Small Businesses

Using a secure tunnel, such as a private APN or Aptilo CCS multitenancy virtual APN, is the best practice to protect your IoT devices. But it is not for everyone. For many smaller businesses, setting up a VPN is an insurmountable obstacle. Instead, they take their chances over the open internet.

Not anymore! With Aptilo's and Fortinet's integrated security solution, small businesses can get comprehensive filtering of traffic, sophisticated routing capabilities, and they're also protected by the award-winning FortiGate NGFW. This will dissuade any lurking hackers from targeting them.

Use Case Domestic IoT Connectivity

Let's use a forestry corporation as an example. They are in need of multiple connectivity options for their forestry machines with granular policy control; a secure virtual APN (VPN) to their headquarters for location tracking of vehicles, reporting of cut timber, machinery hours, etc. In addition, a secure virtual APN (VPN) is established to the forestry machine manufacturer for software upgrades and to provide data for predictive maintenance. They also need firewall protected internet access for the machinery operator according to their corporate policies. Aptilo IoT CCS, powered by Fortinet security, enables all this with customer self-management through integration with the mobile operator's customer portal.

Use Case International IoT Connectivity

Another example is a coffee machine manufacturer that rents their machines to coffee shops all over the world. Through the Aptilo CCS multitenancy virtual APN, operators can offer a secure international connectivity for firmware upgrades, billing data, and predictive maintenance. The manufacturer can save significantly in logistics and administration costs. They just need to handle one unified eSIM card and one VPN connection instead of multiple local SIM cards and VPN connections for each local mobile operator. All IoT units in their warehouse can have an identical configuration. The localization OTA happens when the coffee shops switch the coffee machines on for the first time in the destination country. For the manufacturer, this means streamlined logistics and reduced tied-up capital. For the mobile operator, it means a customer stickiness that few services can offer and the possibility to charge a value-based premium.

Let's now apply the international connectivity possibilities using Aptilo IoT CCS on a car manufacturer. They also want to have the logistics gains and secure connectivity for software upgrades. On top of this, they don't want to suffer from the added latency that comes with the typical mobile operator home routing of traffic. Latency is becoming even more important, as low latency is one of the main features in 5G. Here Aptilo CCS comes to the rescue with the potential to route traffic to the nearest AWS point of presence as the car moves across borders.

About Aptilo Networks

Aptilo Networks is a leading provider of carrier-class systems to manage data services with advanced functions for authentication, policy control, and charging.

Learn more at https://www.aptilo.com/cloud/cellular-iot-connectivity-management-and-policy-control/.

May 7, 2021 5:38 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\May\Refresh\Aptilo\sb-FA-aptilo-iot-connectivity-572021\sb-FA-aptilo-iot-connectivity-572021

696318-A-0-EN