ISOLATING THE CELLULAR IOT EDGE FROM HARM

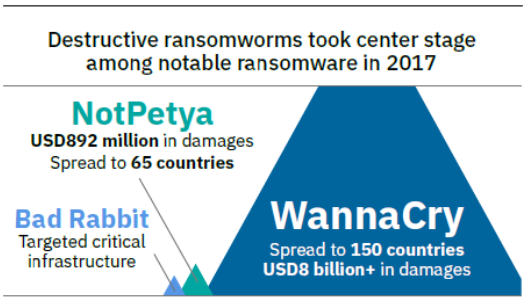
Asavie Application Note

Contents

1. Executive Summary

The internet is a dangerous place. To date, millions of devices have been compromised on the internet edge; the impact is not isolated to only damaging businesses but is also disrupting core internet communication services. These attacks have the propensity to disable even the most secure IoT deployment from communicating with the Microsoft Azure® cloud.

With no other alternative, enterprises are using VPNs over the public internet to protect data in transit between their central business systems and devices in remote locations. The reality is that by attaching a device to the internet, it increases the risk of exposure to seek-and-enslave malware. This has resulted in millions of IoT devices being compromised, the most recent example of which was the Reaper botnet.



Source: IBM X-Force Threat Intelligence Index 2018

At Asavie, we believe industrial devices and business operations should not be exposed to the dangers of the internet. We contend that IoT deployments should be connected in isolated private networks, that provide visibility and control over all data flows originating from the IoT device.

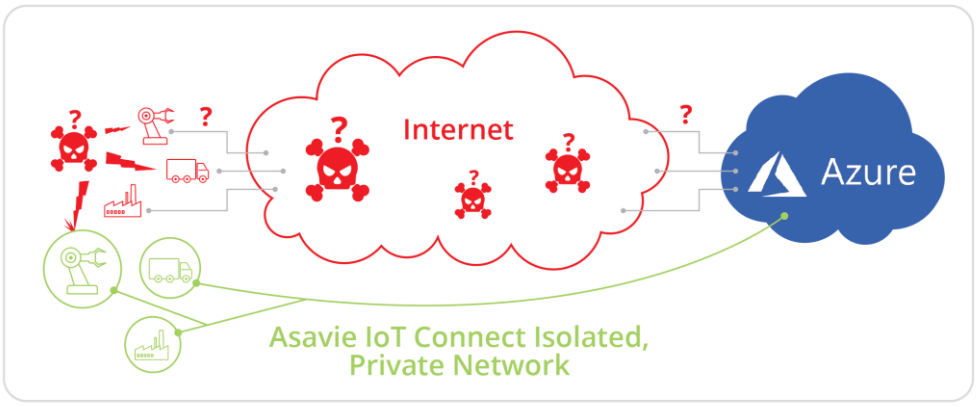


Figure 1 Asavie IoT Connect® private connectivity and virtual security perimeter eliminates exposure to cyber threats

Asavie's software defined IoT connectivity management platform, Asavie PassBridge®, offers private connectivity on demand enabled by Tier 1 mobile network operators such as AT&T, Telenor, Telefonica, Verizon, and Vodafone. Asavie enables enterprises to create dedicated, isolated private networks on demand, that include the controls and insights necessary to assure IoT devices are safe from harm.

Asavie IoT Connect® is a web-based service interface to Asavie PassBridge, enabling the ease of provisioning private networks in minutes versus weeks, that manages device enrolment at any scale from one to tens of thousands, which includes identity management for the Microsoft Azure cloud.

Using Asavie IoT Connect enterprises can simplify secure connectivity and eliminate the exposure to cyber threats. Enabling enterprises with faster times to market and helping to reduce the total cost of ownership for IoT deployments.

2. Isolating cellular IoT edge devices from harm

This application note highlights how Asavie IoT Connect isolates the IoT edge from harm and by doing so eliminates the threat to cybersecurity, enabling enterprises to reduce the total cost of ownership of their IoT deployments.

The application note covers the following key topics:

- Isolated private network for secure data transits from the IoT edge to the Azure cloud
- Seamless IoT edge connectivity - provisioning and chaining the Azure IoT Hub identity to the carrier identity, which is locked to the cellular gateway hardware
- Eliminating security exposures by closing the connectivity gaps
- Visibility and controls of data flows in the private network

Asavie IoT Connect complementing connectivity to Azure IoT Hub

Microsoft Azure facilitates the secure communication of application data from remote devices, irrespective of the underpinning IP network layer connecting the devices to the cloud. Azure enables the encryption of application data, authentication and authorization of the data into the Azure service using secure tokens or digital certificates.

Asavie IoT Connect enables enterprises to provision and manage an isolated private network in minutes, over which the Azure protected data will securely travel. This has the effect of taking IoT devices off the public internet and eliminating their exposure to cyberthreats.

	Layer	Function	Example Protocols
7	Application Layer	network process to application	HTTP, FTP, DNS
6	Presentation Layer	data representation & encryption	XML, JSON, MQTT
5	Session Layer	interhost communication	PAP, PPTP, TLS
4	Transport Layer	end-to-end connections & reliablity	TCP, UDP
3	Network Layer	path determination & logical addressing	IP Addresses
2	Data Link Layer	physical addressing	MAC Addresses
1	Physical Layer	media, signaling, transmission	Ethernet, Bluetooth, Wireless

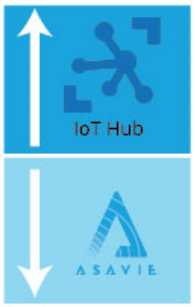


Figure 2: OSI model representation - Asavie IoT Connect enables the secure network layer in which IoT devices can be isolated from cyber threat

Using the Open System Interconnection (OSI) model as a visual representation, Azure IoT Hub enables ease in consuming and securing layers 4 to 7. Asavie complements Azure IoT Hub by enabling a secure network at layer 3 to underpin the security at layers 4 to 7.

2.1. Overview of Asavie IoT Connect

Asavie IoT Connect is a self-service portal, which enables enterprises to provision, manage and define accounts, private networks and security perimeters for their IoT deployment.

Uniquely, Asavie IoT Connect can provision and chain the identity provided by the Azure IoT Hub to a global selection of mobile network operators, which in turn can be locked to the modem identity (IMEI) enabling the concept of a "cloud in a SIM card" (Subscriber Identity Module) for enterprises.

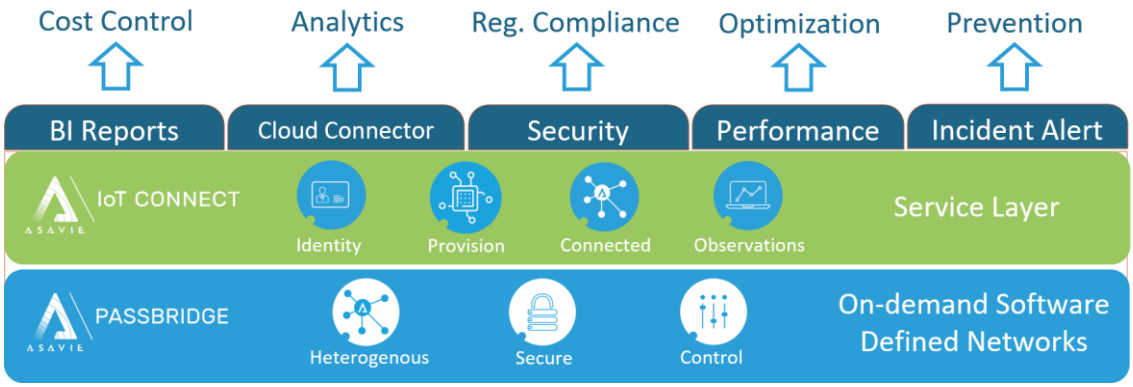


Figure 3 : Asavie "Network as a Service" platform and service architecture

In addition to secure connectivity, Asavie IoT Connect provides enterprises with the following advantages:

- **Eliminating time wasted in manual network builds**
  Network build and change process is reduced from 90+ days to minutes through self-service networks. The network service includes private DNS and authentication of cellular devices into the Asavie private network and auto-provisioned in Azure IoT, enabling a seamless journey to the cloud.
- **Flexibility to grow in line with project needs**
  Scale on-demand with minimal upfront investment using a pay as you go model. Additional features such as data controls, data throttling per device and detailed usage reports, put enterprises in control of all cellular traffic expenditure.
- **Minimizing the impact of device and software constraints**
  Asavie IoT Connect requires no software install or configuration of the device firewall. Asavie IoT Connect blocks all but key data flows originating from the device e.g. build a network that only supports messaging traffic such as MQTTS.
- **Lifetime of security**
  As devices are no longer exposed to the internet, the cyber threat is eliminated and enterprises no longer need to worry about future software patches. In an estate of thousands of IoT devices, this significantly reduces the cost and time-related overheads of update management.

2.2. Asavie PassBridge connectivity platform

Asavie PassBridge is a software defined connectivity platform built on custom off the shelf x86 hardware. The core consists of a resilient, hosted hardware environment operated in multiple global Points of Presence (POP), which is provisioned and managed by the proprietary Asavie PassBridge software stack.

Asavie PassBridge has a distributed software architecture - the orchestration and service layers run in the Azure cloud and the software defined network layer is run in the POP. The Asavie PassBridge software stack is as follows:

- **Service layer** – facilitates the declaration of enterprise tenant - accounts, network, security and charging models, which are pushed to the orchestration layer via the Asavie PassBridge northbound API for implementation.
- **Orchestration layer** – provision enterprise networks on the hardware platform, support authentication and authorization of devices in the enterprise's network, facilitate operational data aggregation.
- **Connectivity layer** – runs the enterprises network with the prescribed virtual networking functions (routing, domain name services, load balancing, firewalling, etc) for data plane transits, controls and security. Management of the secure interconnects that Asavie has in place with Carrier and Internet Service Providers.

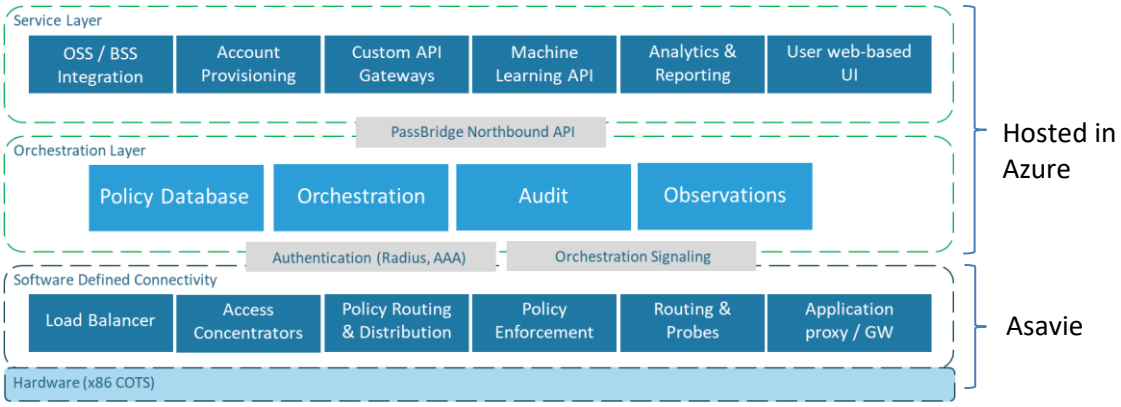


Figure 4: Asavie PassBridge architecture

The enterprise private network is only accessible by devices whose credentials have been provisioned and validated in Asavie PassBridge. Each cellular device's credentials are validated at each attempt to connect with the Asavie PassBridge network. For cellular enabled devices, this implies securely querying the carrier registries, to which Asavie has a private secure connection.

On successful authentication and authorization of a device into the network, traffic will be routed from the carrier network into the Asavie PassBridge POP over a secure link. Depending on the enterprise's declared network configuration, the traffic is assessed against the implicit security policies and routed onwards to the enterprise LAN and/or Azure cloud as prescribed by the enterprise.

3. Bridging the connectivity gap

3.1. Mind the gap!

"Mind the gap!" are visual and audible warnings associated with city transport systems across the globe. When it comes to cellular enabled IoT projects, similar gaps occur at the demarcation points of the service edges. It is through these uncontrolled/open connectivity gaps that devices become exposed to cyberthreats on the internet.

Outlined in the diagram below is a common scenario where the solution architect has scoped an IoT project, selected the cloud service e.g. Azure IoT Hub and deployed sensors/gateway devices with the subscriber identity module (SIM) installed. On successful configuration, data arrives in the Azure cloud as expected.

What remains an unknown, is what else is the gateway communicating with and why? As explained below, this presents an array of issues for the enterprise.

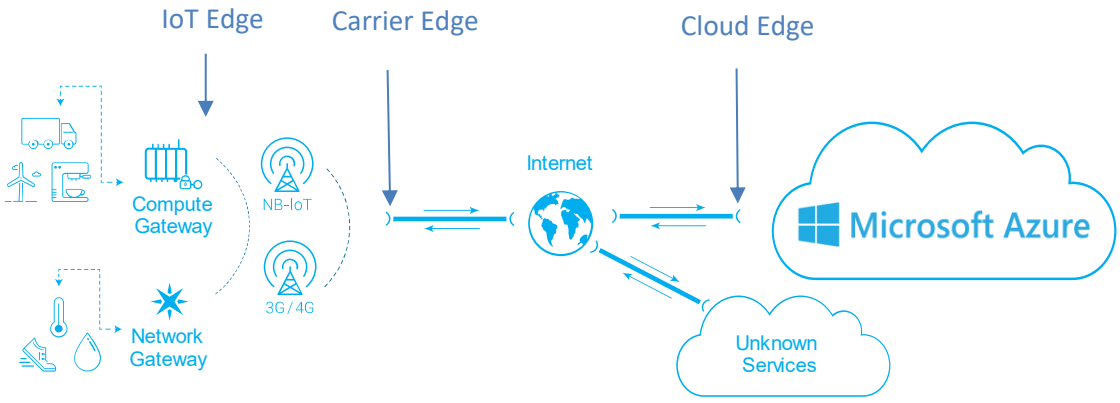


Figure 5 : Demarcation points of service edges

- **Public Internet – Leads to Data Overages**
  As the IoT Edge is connected to the public internet via the carrier edge (as is the case in many MNO/MVNO scenarios), this opens the risk of unknown applications (malicious or not) calling home. For the enterprise with thousands of devices, the challenge is the lack of visibility - to know that these service calls are happening. Ultimately, incurring unnecessary costs on data plans.

  In the worst-case scenario, the enterprise may have to refer to the monthly billing notice, to check if any of the devices are using more data than the others. Potentially, triggering the enterprise to run a firmware over the air (FOTA) update. That is - if they have identified that there is unusual activity causing the unwanted billing overage.

- **Inaccessible IoT Devices Behind the Carrier Edge**

  FOTA creates yet another challenge for the enterprise, as the devices are behind the carrier edge. This means devices are not addressable, making it difficult to push an update out. Enterprises can implement an update trigger methodology to get the device to poll for the update e.g. SMS sent to the device to trigger updates. These updates tend to result in additional engineering efforts and costs, that may not have been scoped or budgeted

for. In addition, project constraints may result in devices that lack the flexibility to run an update.

IoT Hardware & Software Constraints
Project constraints may produce additional challenges for the enterprise in securing the IoT Edge. For example, it may not be possible to place the client end of the TLS connection provided by Azure IoT Hub at the device. Other constraints that may impede firmware updates include:

- lack of hardware to underpin crypto functions or security libraries to securely transfer and validate the firmware package
- limited power source (a battery powered device): which means that software updates cannot be performed e.g. the power to download the update consumes 6 months of lifetime
- the risk of updating software to address a vulnerability outweighs the risk of the update 'bricking' the device

- **Identity Challenge**
  The IoT Edge architecture itself may impede the update process, for example the edge may be composed of a device network behind the cellular gateway, this in turn may result in the IoT devices being assigned an identity in Azure IoT Hub and not the actual cellular gateway. Repeating the challenge highlighted earlier, these devices are not addressable and will need a means by which to trigger the update.

  Fundamentally, enterprises now face an identity gap challenge, in that they need to manage multiple identity systems. For example, a point of sales merchant service provider (POS MSP) looking to deploy 10,000 payment terminals, would have 10,000 identities in the carrier system and 10,000 identities in Azure IoT Hub.

  Overtime, the identity gap may lead to loss of payment terminals, poor quality of service along with a potential loss in revenue, as the asset physical ID (International Mobile Equipment Identity – IMEI), SIM and device ID assigned in Azure IoT Hub are not aligned.

In the following section, we will discuss how enterprises can overcome deployment and update hurdles by using Asavie IoT Connect.

3.2. Identity chaining Azure IoT Hub with carrier SIMs

Asavie IoT Connect bridges the connectivity and identity gap, by leveraging the Asavie PassBridge platform, enterprises get a private network through which the Azure IoT Hub identity, network operator identity and modem identity (IMEI) are managed.

This centralized management of identity simplifies cellular IoT deployments and enables significant advantages over the deployment lifetime:

- **Tamper proof**: no private keys and certs stored on the gateway
- **Faster time to delivery**: ease in rolling out and scaling deployments
- **Reduced total cost of ownership**: eliminating unwanted data flows

By enabling the enterprise to holistically manage the three key identities as one i.e. Azure IoT Hub and carrier SIM, enterprises gain the value of software automation:

- **Software enrolment**: minimizes effort/handling errors when scaling cloud connected devices
- **Access/protocol negotiation (disaggregated from the device)**: eliminating the risk of device lock-out
- **Centralized identity/cert management**: minimizing OTA updates and/or truck rolls to manage devices

Using the Point of Sale MSP example from above, Asavie IoT Connect enables the POS MSP to provision as many network groupings as they need for the 10,000 sales terminals. On enrolling an asset into the private network, there is a call made to auto-provision a device identity in the enterprise Azure IoT Hub. For the POS MSP there is no requirement for a provisioning system, no software needed on the device, enabling faster times to market.

Once the IoT device comes on line, data seamlessly arrives at the Azure IoT Hub. Asavie IoT Connect maps the flows originating from the SIM to the identity created in Azure IoT Hub. In addition, by applying security policies the enterprise can lock down the network and eliminate data communications to unknown sources as indicated in the previous figure 5, thereby saving the enterprise on unnecessary data charges.

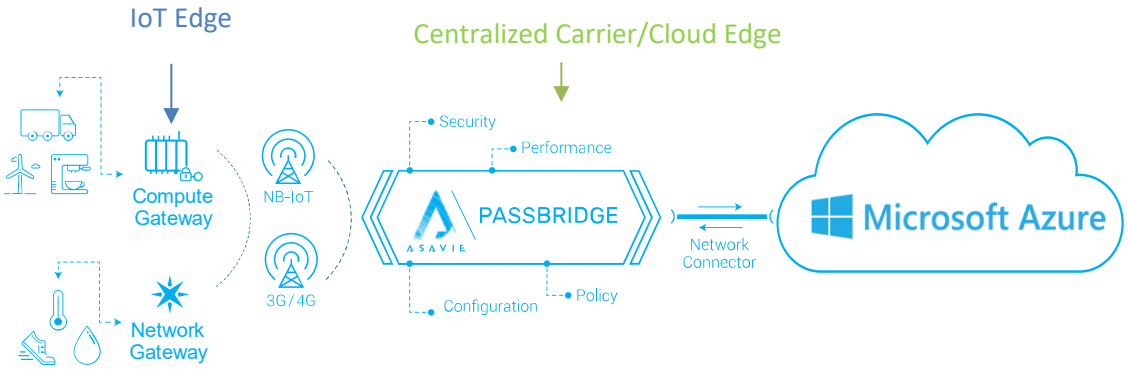


Figure 6 : Asavie PassBridge consolidating and centralizing identity and security management

4. Defense in-depth

4.1. The unknown – unknown?

Enterprises do not get the granular visibility of how data is being consumed from standard carrier IoT service offerings. They receive a reconciled monthly bill which may include unnecessary/unanticipated overages. It is only after the receipt of the monthly bill, that the enterprise may recognize an anomaly. Discovering days/weeks after the fact that the overages may have arisen due to malware that has manifested on the device.

On a weekly basis, Asavie is introduced to customers who have had first-hand experience to security exposures, an example conversation is - “Part of our IoT deployment uses public static IP addresses and was exposed to ‘CVE-2017-6044’, which cost several thousands of dollars in overages – can Asavie help going forward?”.

Security threats are not the only unknown. In the figure below an enterprise’s legitimate application for FOTA failed. As part of the update handling methodology, the developer included loops to request the update package more than once.

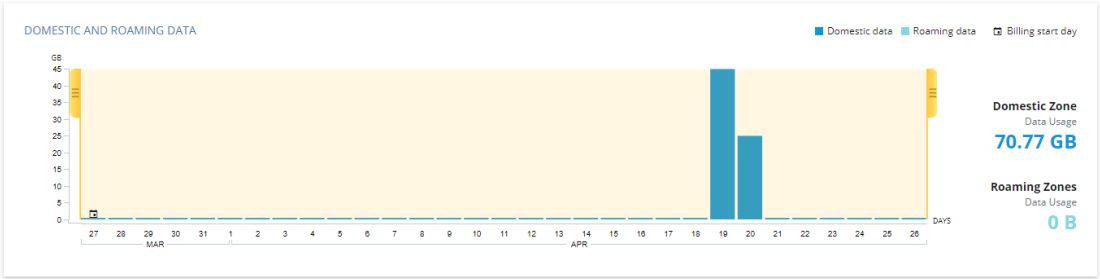


Figure 7 : Asavie IoT Connect daily usage rates, data spikes due to poorly implemented FOTA

As the above example highlights the FOTA update was a legitimate task, the unknown issue was that the update was failing multiple times in the field. The challenge for the enterprise is that a single device could consume the monthly data plan for the entire device fleet, causing a network wide outage.

Continuing with the POS MSP example, not only does this damage the internal revenue stream but results in the potential loss of sales for businesses using the POS MSP systems. This would have a significant impact on trust and brand reputation.

What can be done to protect against the unknown-unknowns?

4.2. Minimizing the risk to exposure

There are many unknowns that can open an IoT deployment to risk. The following sections demonstrate how the network layer enabled by Asavie IoT Connect can minimize and eliminate exposure to the unknown.

Network layer security

Asavie IoT Connect offers dynamic network layer security policy management to provide a consistent foundation of security across the entire cellular IoT deployment estate. The centralized approach eliminates the risk from human error at the pre-deployment configuration stage through to production live deployment.

The enterprise now has the flexibility to open and close connectivity access at will. This has significant advantages over standard private APN offerings from carriers, where adjustments to the security posture are submitted as support tickets. Addressing the ticket can take anything up to several days to implement, which creates an unnecessary window of vulnerability.

Using the POS MSP example, with Asavie IoT Connect the POS MSP is assured that every one of the 10,000 sales terminals going into the field is guaranteed to have the same security posture. The POS MSP gains the control to activate/suspend connectivity to a sales terminal in real-time. This additional security advantage prevents misuse of an asset while in transit from the POS MSP to the end-customer premise.

For projects connecting to Azure IoT Hub or VMs hosted in Azure cloud, the enterprise can white-list the Azure IoT Hub domain and/or the local IP address and port number in use on the hosted VM on which the Asavie agent is installed. The Asavie agent enables VPN connection to the private network, facilitating secure access to the IoT edge gateways.

The Asavie VPN agent and security controls enable enterprises with a secure channel in which FOTA updates can be implemented.

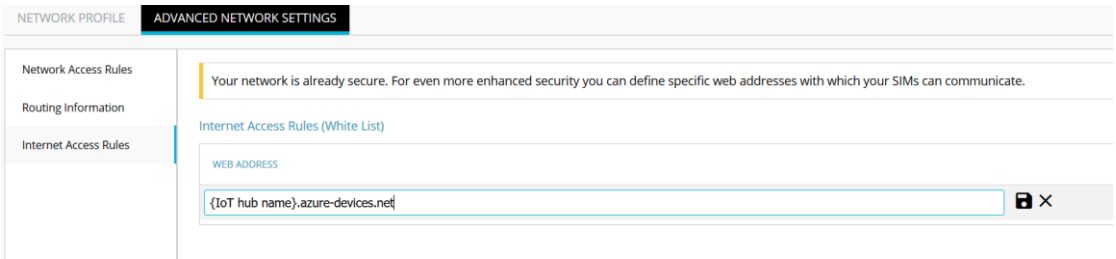


Figure 8 : Whitelisting Azure IoT Hub, assuring cellular devices only connect to the Azure cloud service

Asavie IoT Connect supports bi-directional communication in the private network but by default blocks all in-bound connections, eliminating the exposure of IoT devices with open TCP listening ports to the public internet.

Enterprises can manage gateways via remote access using SSH or Remote Desktop to any gateway that supports that functionality, using an Asavie supplied VPN agent.

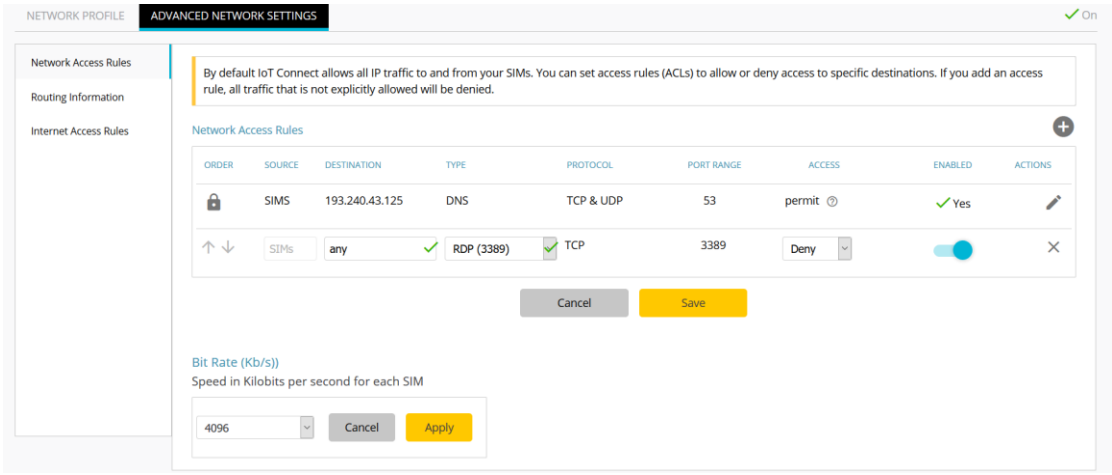


Figure 9 : Dynamic IP access lists, restricting access to all but necessary target destinations

Virtual route controls

Each Asavie IoT Connect managed network supports virtual routing capability enabling enterprises with the flexibility to route traffic as required, without the need to reconfigure devices, eliminating unnecessary FOTA updates.

For example, our POS MSP starts out with Asavie IoT Connect by sending operations data to the Azure IoT Hub and supports secure FOTA updates from an on-premise server using an Asavie agent. A decision is made some time later to move the FOTA service to a VM running in the Azure Cloud. Using Asavie IoT Connect the POS MSP simply enters the route details for the new FOTA service, eliminating the need for device updates on the new location.

Identity chaining

Asavie uses the standard SIM supplied by the carrier to enrol gateways into the private network. There is no manipulation required on the SIM i.e. as a place to store a cert/key, reducing management complexity and overhead for enterprises.

As the identities are managed centrally “off the box”, it means in the event of tampering, that the malicious actor has no means in which to build a toolset e.g. the malicious intent is to poison data in the Azure cloud.

In the event of theft of the gateway, the malicious actor gains no information to the actual target destination for the data flows. Asavie provides a secure domain inside the platform, obfuscating the fact that the gateway is connecting to Azure IoT Hub.

Additional security measures from Asavie IoT Connect include the ability to lock the carrier ID or SIM to the gateway. This locks the Azure IoT Hub identity to the hardware. In the event of a SIM being removed and installed in a different gateway, all communications with Azure IoT Hub will be blocked.

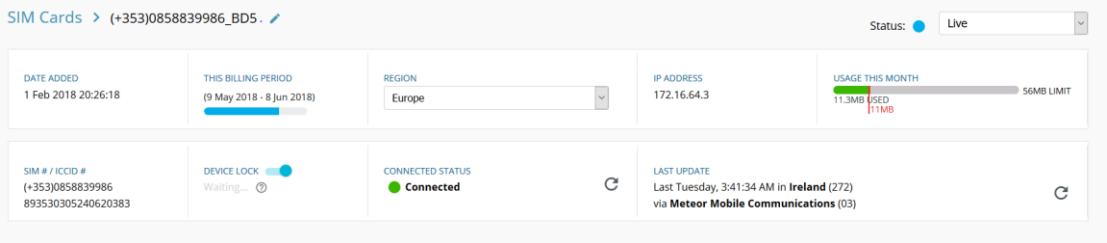


Figure 10 : Asavie IoT Connect Device lock, enabling tamper proof connectivity

An additional advantage of Asavie IoT Connect identity management is in situations where enterprises wish to exchange ownership of a gateway between Azure IoT Hub instances. This requires no certificate/firmware updates on the device. This has significant advantages where a device is in the field and firmware cannot be easily updated.

For example, our POS MSP has multiple business units which manage various regions, sales terminals in one business unit are no longer required and moved to the second business unit. The POS MSP using Asavie IoT Connect can simply move the devices to the new network group with no update required on the device.

5. Actioned Insights

5.1. The perplexity of metrics

Frequently the OT/IT personnel tasked with managing the IoT project post-deployment may not have the complete scope and/or resources necessary to monitor what is happening with the live deployment in the field e.g. is the scaled IoT deployment operating according to the original operational specification, as defined during the Proof of Concept?

With disparate silos of metric sources, log formats and the potential for thousands of lines of entries. It is difficult to interpret what is happening with the IoT deployment. The problem is further exasperated when there is an ask to identify devices that need attention, which can equate to looking for the IP needle in the haystack.

Traditionally, reports offer historical data which is used after the fact that the incident has occurred, which only gets flagged on receipt of the monthly bill. Enterprises need a pro-active approach to the real-time management of IoT deployments.

5.2. Visibility and Insights that matter

Asavie PassBridge's unique position at the network layer provides visibility to the entire end-to-end deployment topology from IoT edge gateways, to the network operator edge and through to the Azure IoT Hub edge, in which it sees all traffic flow requests.

The software approach to intelligence gathering at a network layer, combined with machine learning enables Asavie IoT Connect to:

- control usage and adapt the polices when usage limits are reached
- identify anomalies and notify enterprises
- detect and flag failures associated with critical applications

The visibility and actionable insights available from Asavie help to reduce and eliminate the consumption of metered data that does not deliver value in the IoT operations, helping to reduce the overall total cost of ownership of IoT deployments.

6. Conclusion - Reducing risk in a hyperconnected world

Asavie IoT Connect provides enterprises with private network connectivity for cellular IoT devices. The isolated private network takes IoT edge devices off the public internet, eliminating exposure to cyber threats.

Asavie IoT Connect enables the enrolment and provisioning of Azure IoT identities to reduce the time and effort required in which to deliver scaled IoT deployments. On enrolling a device into the Asavie IoT Connect private network an Azure IoT Hub identity is generated, eliminating the exposure to handling errors. By disaggregating access/protocol negotiation from the device, this prevents the risk of device lock-out to the Azure IoT Hub.

By chaining the carrier identity (SIM) with the Azure IoT Hub identity, Asavie IoT Connect can seamlessly route traffic to the Azure IoT Hub. Asavie IoT Connect requires no software installs and by simplifying the development effort of the IoT Edge device, enterprises minimize the risk of long proof of concept cycles, enabling faster times to production deployment. By centralizing identity/cert management, this minimizes the need for OTA updates and/or truck rolls to manage cellular devices over the operational lifetime.

Asavie IoT Connect provides visibility into every flow generated (malicious or not) in the IoT deployment. This provides enterprises with the capability to manage and control unwanted traffic flows, eliminating the risk of unnecessary data expenditure.

Asavie IoT Connect is sold on a subscription service basis and enables enterprises to easily scale on demand, minimizing upfront costs and ultimately reduces the total cost of ownership over the life of the IoT deployment.

ASAVIE

Asavie Technologies Ltd.
Corporate Headquarters
100 Mount Street Lower,
Dublin 2, D02 TY46, Ireland
P +353 1 6763585
E support@asavie.com
W www.asavie.com