VELOS IOT INTEGRATION MODELS

velosiot.com

Velos IoT

@ velos-iot

Table of Contents

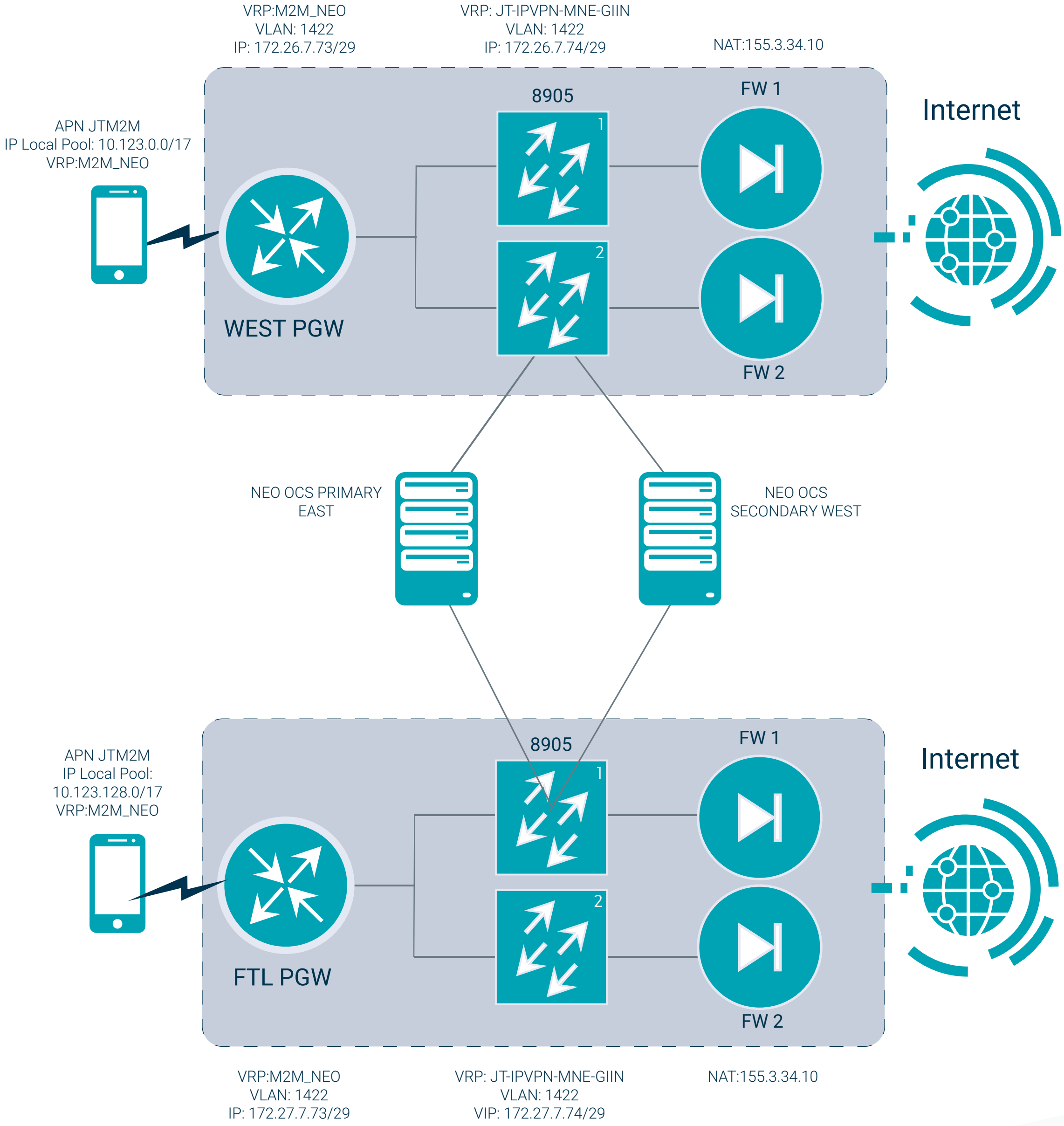
M2M Classic Model

M2M classic is our default model allowing customers to have an open internet connection.

The device should be configured with the APN "*jtm2m*" and once this device is attached to a visiting network, the data session will pass over the IPX (IP Exchange) and reach the JT Mobile Core.

The PGW (packet gateway) will accept this data request and establish a session back to the device. This session will then pass through the JT 8905 switches and onto our firewalls where it will be NAT-ed out to the internet.

This APN has no restrictions on the firewall so it can access any site on the web. It's a fully geo-redundant solution with the platform mirrored in Jersey and Guernsey.

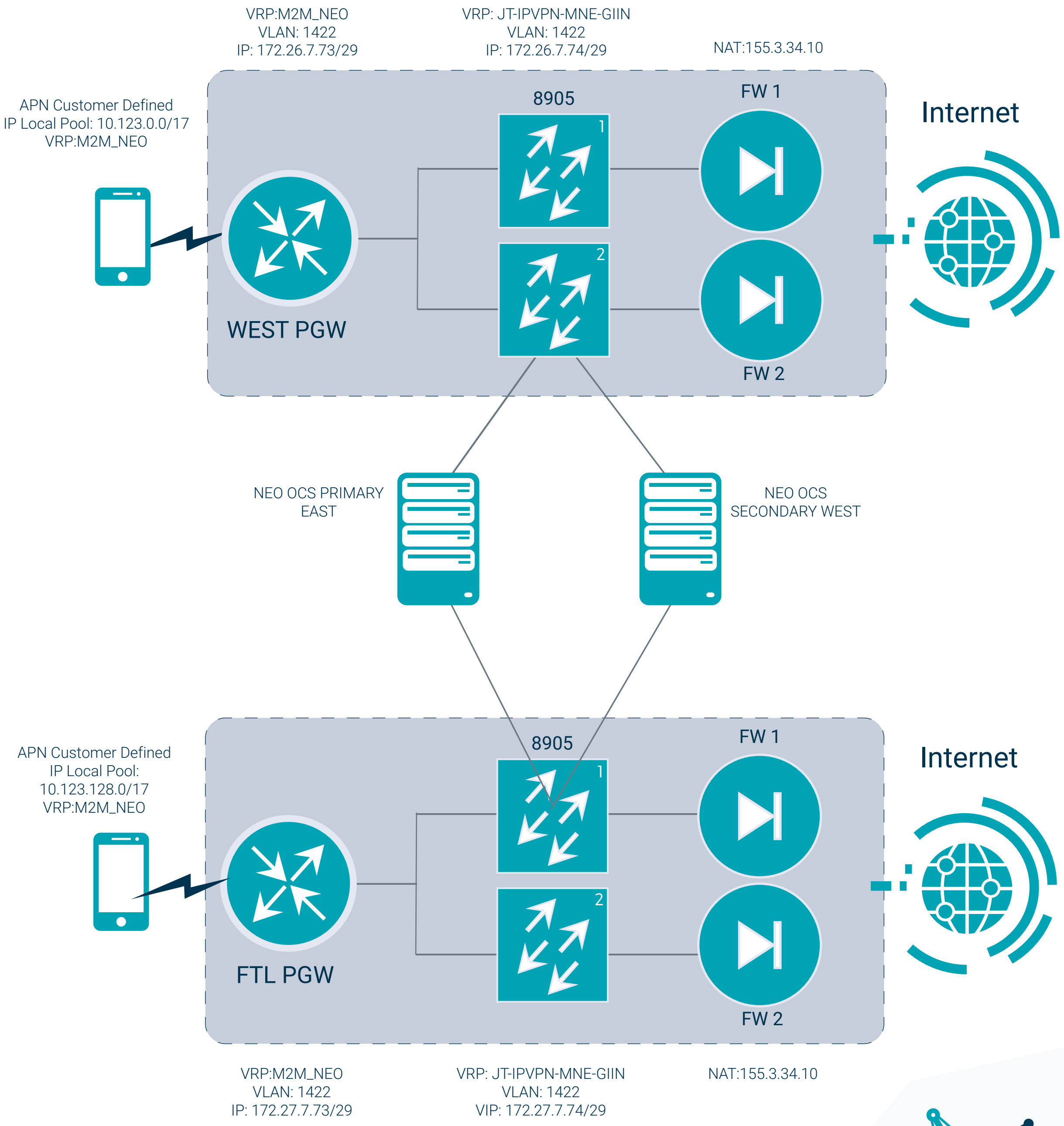


Custom Classic Model

The Custom Classic model gives our customers a custom-built APN that has open access to the Internet.
The device should be configured with the APN that the customer has requested and once this device is attached to a visiting network, the data session will pass over the IPX (IP Exchange) and reach the JT Mobile Core.

The PGW (packet gateway) will accept this data request and establish a session back to the device. This session will then pass through their 8905 switches and onto our firewalls where it will be NAT-ed out to the internet.

This APN has no restrictions on the firewall so it can access any site on the web. It’s a fully geo-redundant solution with the platform mirrored in Jersey and Guernsey.



Custom Classic Restricted Model

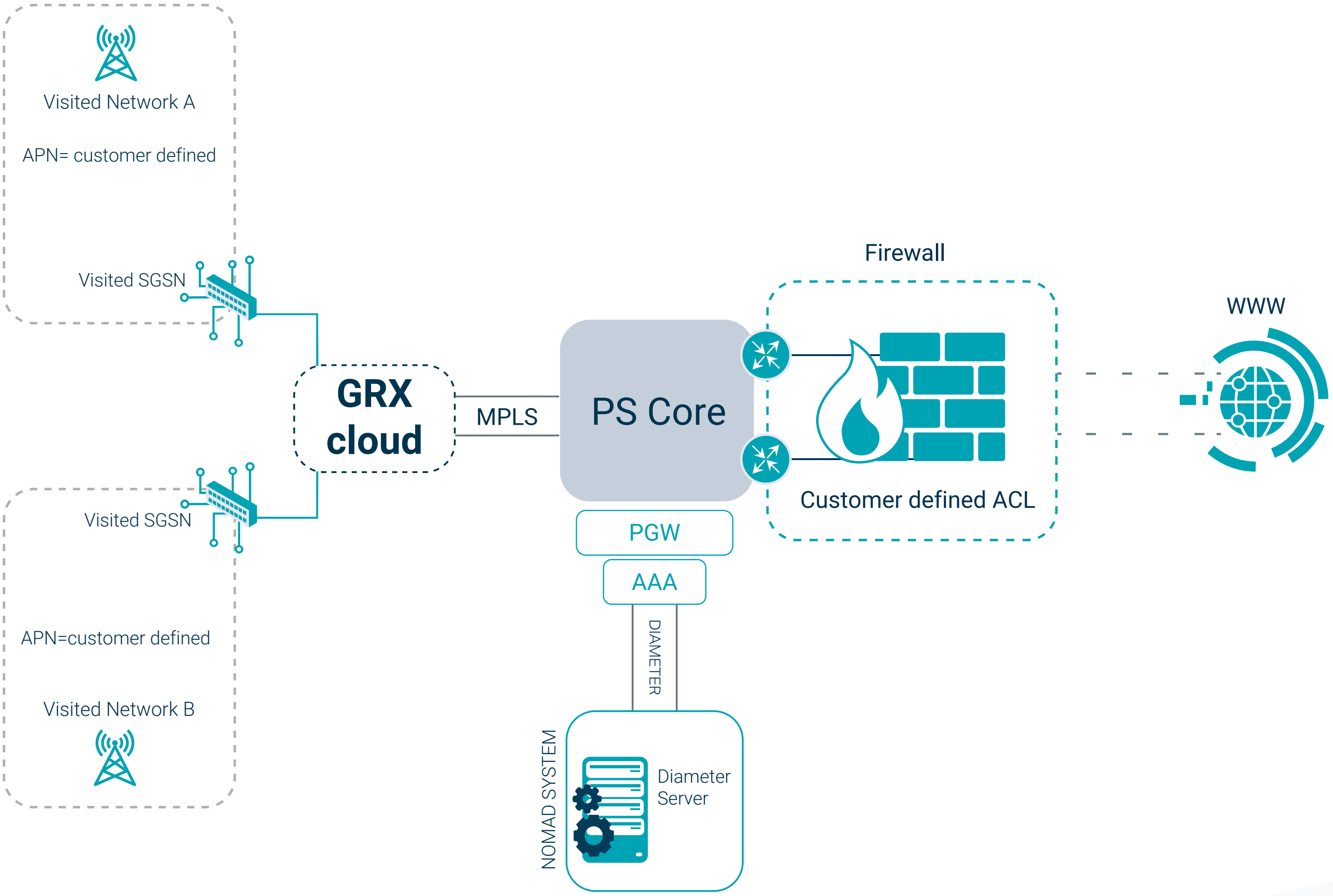
Classic restricted model allows customers to have a custom APN that is then passed through an ACL (access control list) on the firewall and this list can permit or deny anything that the customer requests. Some common scenarios are:

Allow certain IPs and deny everything else
Allow certain TCP / UDP ports and deny everything else
A mixture of the two
Please note fqdn (a domain name) is not supported

The device should be configured with the custom configured APN and once this device is attached to a visiting network, the data session will pass over the IPX (IP Exchange) and reach the JT Mobile Core.

The PGW (packet gateway) will accept this data request and establish a session back to the device. This session will then pass through their 8905 switches and onto our firewalls where it will follow the ACL rules that have been configured.

It's a fully geo-redundant solution with the platform mirrored in Jersey and Guernsey.



Fixed Private IP Standard

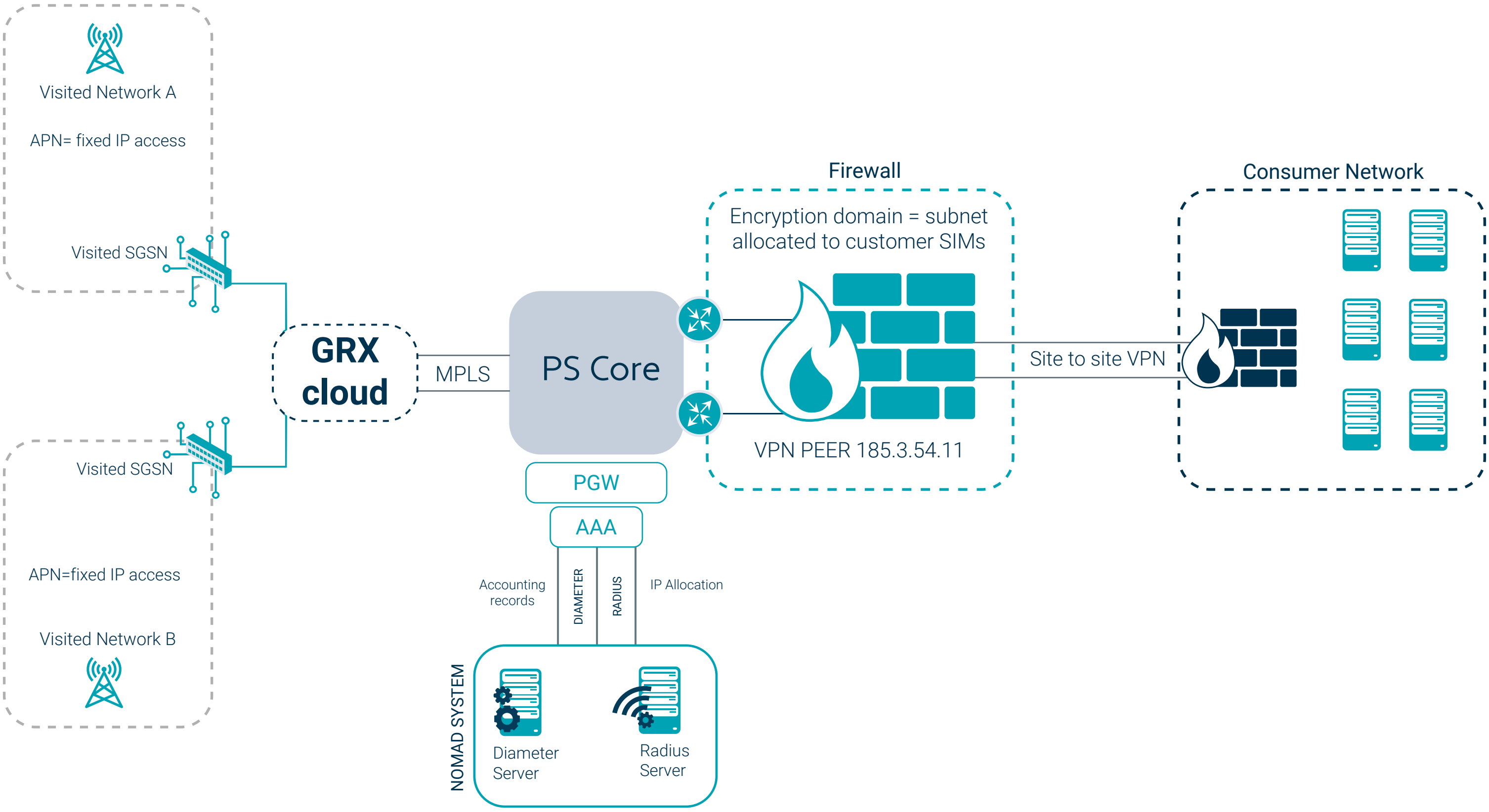
The Fixed Private IP Standard model allows customers to have a default APN that gives the device a fixed private IP address every time it opens a data session.

There would be a VPN between Velos IoT and the customer where the data would pass through. The main advantage of this model is that it allows the customer to be able to communicate with the device giving you two-way communication.

The device should be configured with the default APN "*fixedipaccess*" and once this device is attached to a visiting network, the data session will pass over the IPX (IP Exchange) and reach the JT Mobile Core. The PGW (packet gateway) will accept this data request and then do a radius authentication to Nomad where it is then assigned the same IP each time.

This session will then pass through their 8905 switches and onto the firewall where all traffic will be passed over the VPN back to the customer.

There are two firewalls on the Velos IoT side and if one should fail then the other firewall will take over.



Fixed Private IP Custom

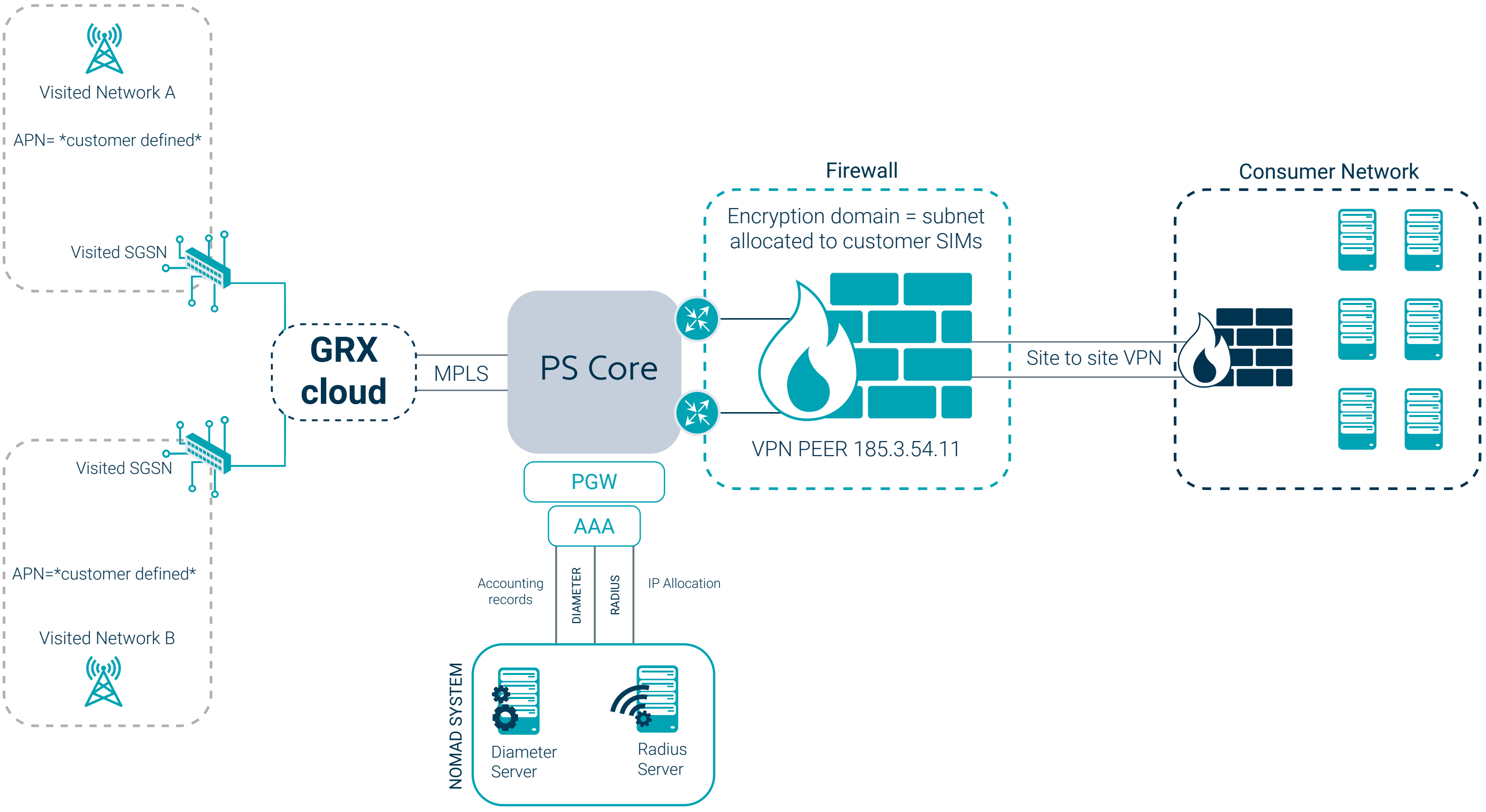
Fixed Private IP Standard model allows customers to have a custom APN that gives the device a fixed private IP address every time it opens a data session.

There would be a VPN between Velos IoT and the customer where the data would pass. The main advantage of this model is that it allows the customer to be able to communicate with the device giving you two-way communication.

The device should be configured with the custom configured APN and once this device is attached to a visiting network, the data session will pass over the IPX (IP Exchange) and reach the JT Mobile Core. The PGW (packet gateway) will accept this data request and then do a radius authentication to Nomad where it is then assigned the same IP each time.

This session will then pass through the JT 8905 switches and onto the firewall where all traffic will be passed over the VPN back to the customer.

Redundancy is achieved by configuring a second VPN which will incorporate GRE/BGP routing.

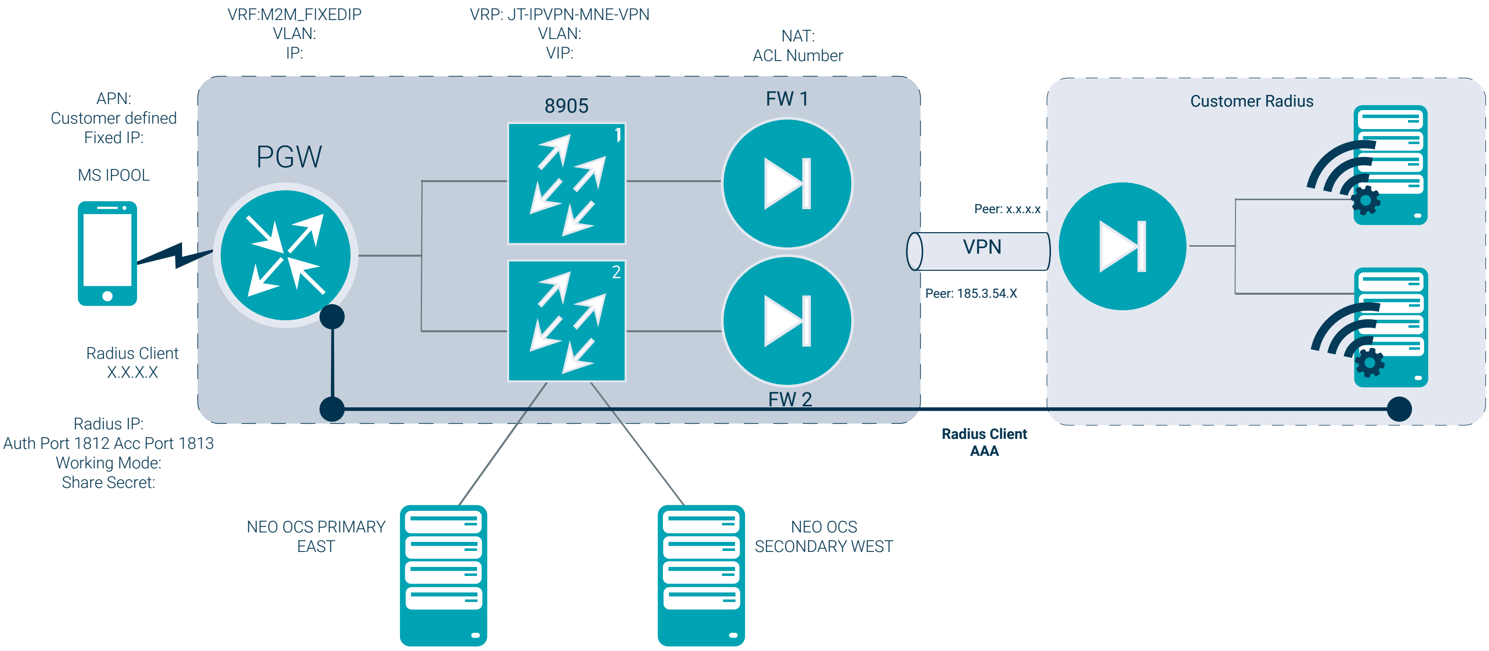


Fixed Private IP Custom With Customer Radius Server

This model works like the slide before where the customer will have a custom APN and when the sim card does a data request is does a radius authentication and get allocated the same IP every time and this is then passed down the VPN/IPSec tunnel to the customers network.

The only difference with this integration is that the customer has their own radius server so instead of the radius authentication being passed to Nomad it is passed through the dedicated radius link between Velos IoT and the customer.

The only thing to bear in mind with this is that the private IP subnet that the customer allocates as their SIM IP pool must not clash with anything on Velos IoT network.



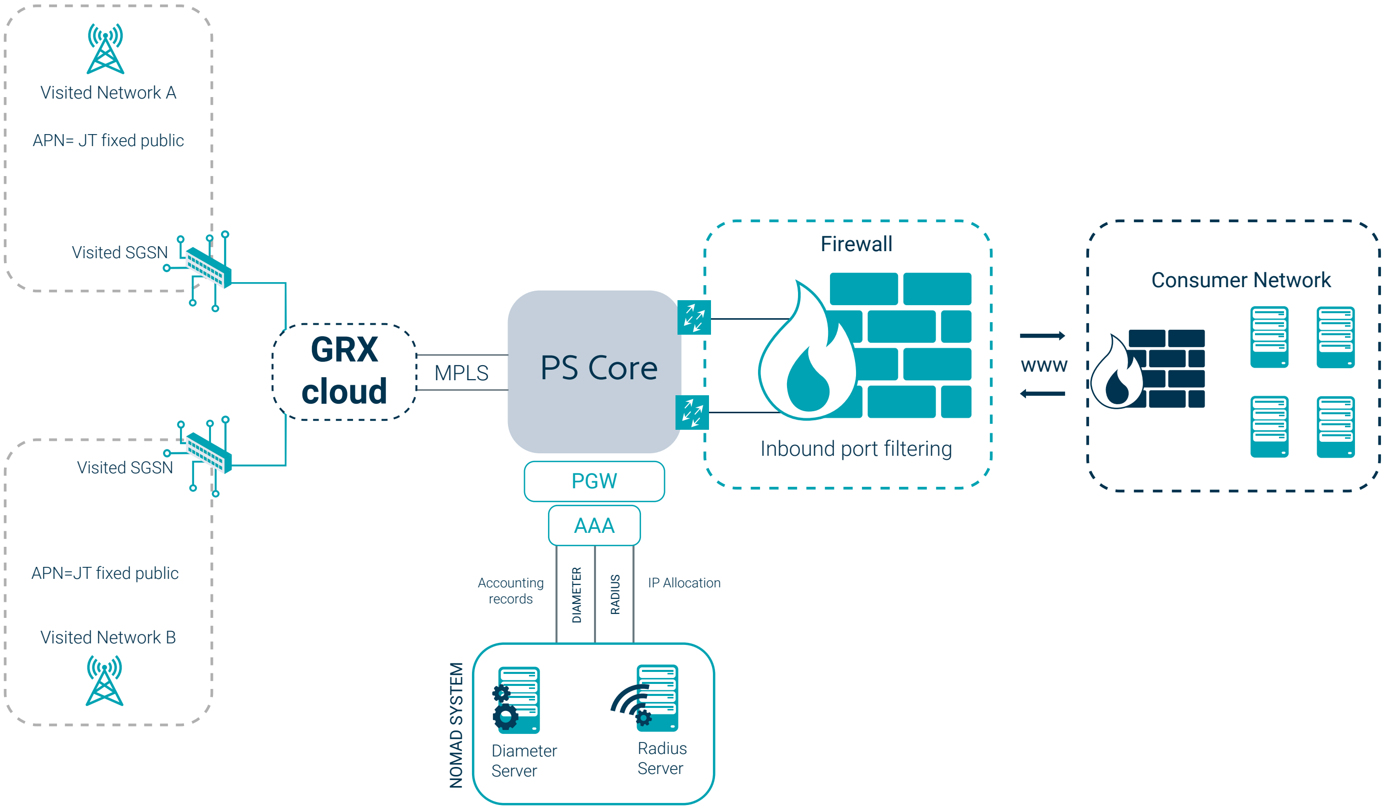
Fixed Public IP Standard

Fixed Public model allows customers to have a default APN that gives the device a fixed public IP address every time it opens a data session.

The main advantage of this model is that it allows the customer to be able to communicate with the device giving you two-way communication.

No VPN is needed for this solution as connectivity to the device is done over the internet to the Public IP. The device should be configured with the default APN "*jtfixedpublic*" and once this device is attached to a visiting network, the data session will pass over the IPX (IP Exchange) and reach the JT Mobile Core.

The PGW (packet gateway) will accept this data request and then do a radius authentication to Nomad where it is then assigned the same Public IP each time.



IMSI Donation

Transit model is where the customer has their own infrastructure and are purely using Velos IoT as an IMSI donor to give the customer reach to our roaming partners.

Integration will involve having a VPN between both networks that will pass the signalling and diameter traffic to the customers network. This VPN can be replaced by a direct connect circuit which gives better reliability and performance.

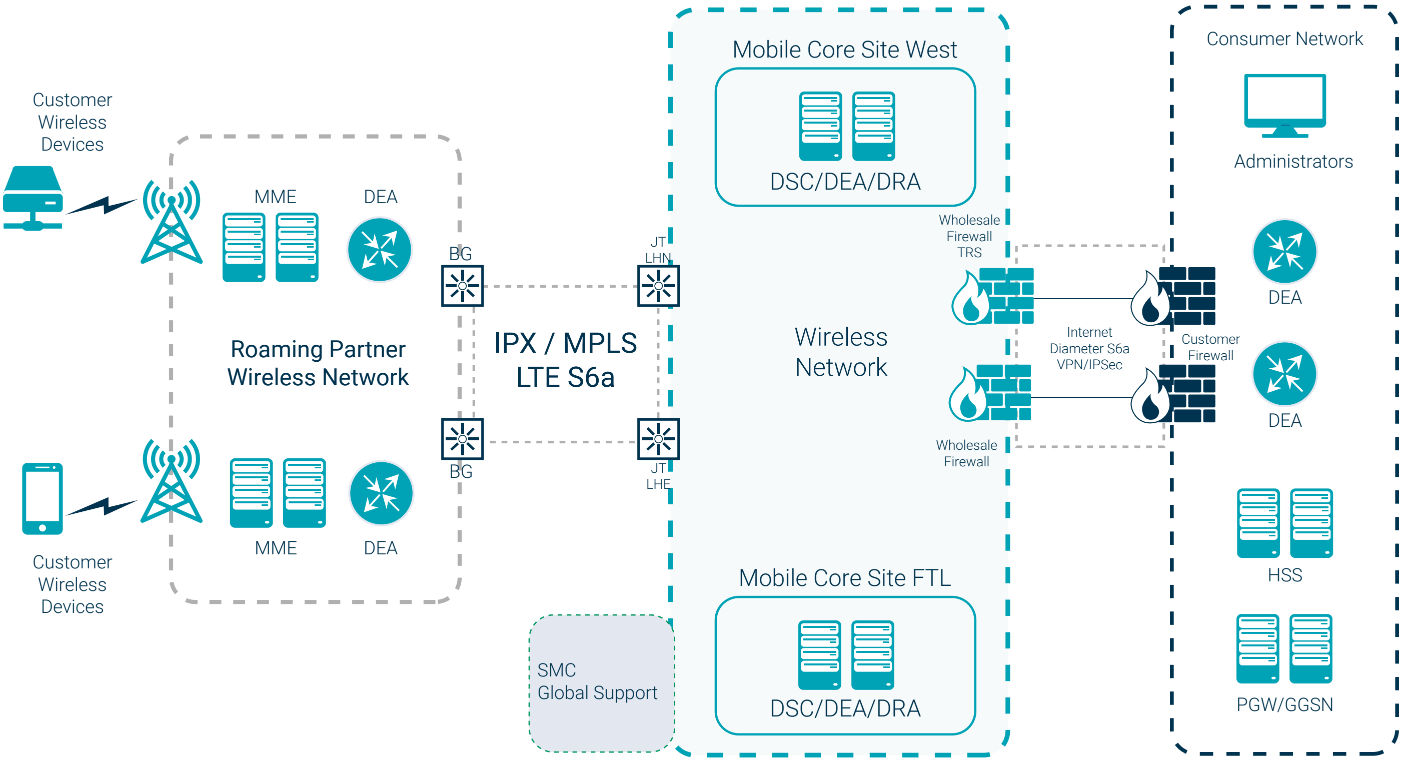
The customers IP Backbone addressing would need to go onto Velos IoT IR21 so that Velos IoT roaming partners can configure their networks to allow these IPs to access their network.

Main integration milestones would be:

VPNs between networks
SIGTRAN links between STPs
S6a links between DRAs for diameter
DNS configuration for APNs
AoB – TAP/CDR billing, testing

As the customer owns their own network, they will be responsible for redundancy within their network.

For the interconnect there would be two VPNs configured for resiliency and this reliability can be further improved by adding direct connects which will come at a cost to the customer.



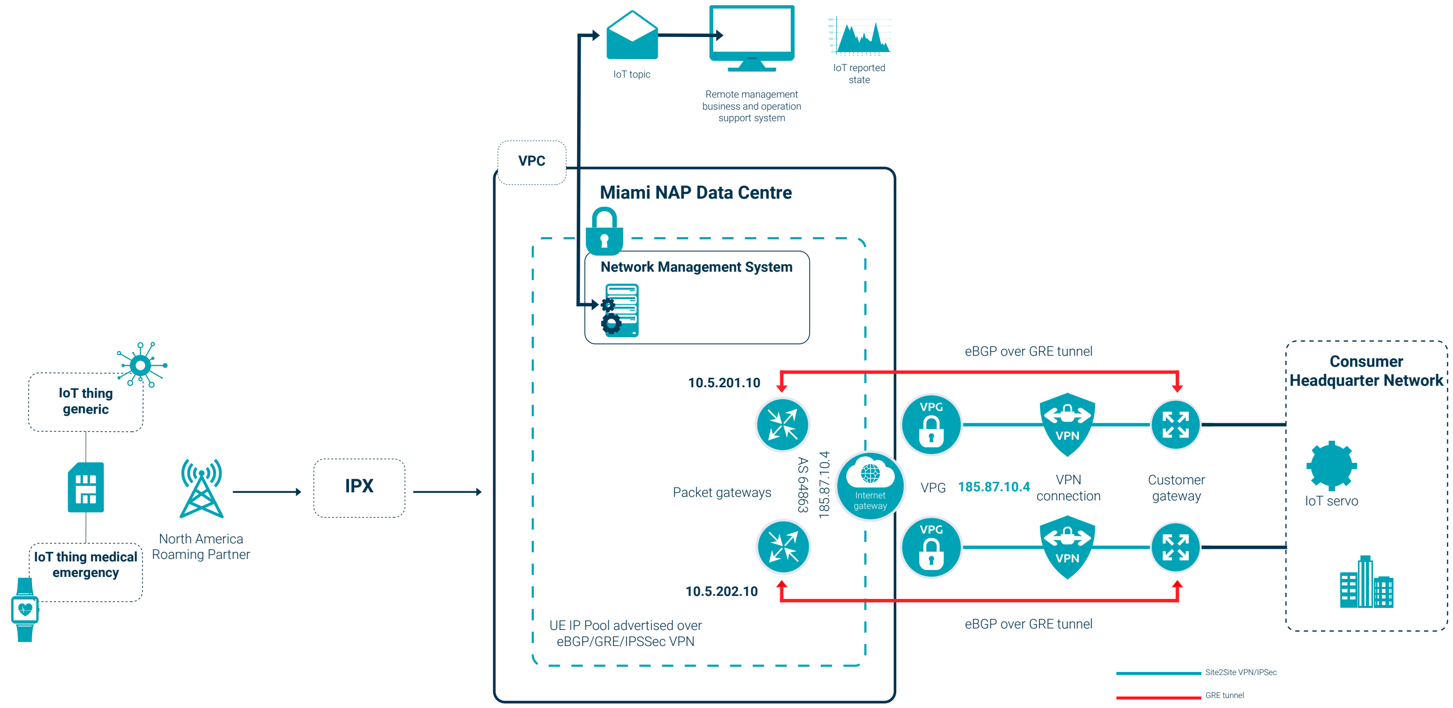
Accelerate

With customers striving for lower latency times to improve device performance Velos IoT have provided a PoP (point of presence) in Miami which allows our data traffic to stay in the US rather than transit all the way to Jersey to and then back again. As an example of the benefit from having this PoP:

Usual round trip US-based SIM to Jersey – 300ms
US SIM to US PoP – 90ms

Customers based in North, Central and South America would gain from these time improvements. Another benefit from this solution is that sensitive data information remains in the US.

To provide full resiliency the customer will need two network devices to configure VPN tunnels. They will also need to support GRE/BGP which provides the routing and failover.

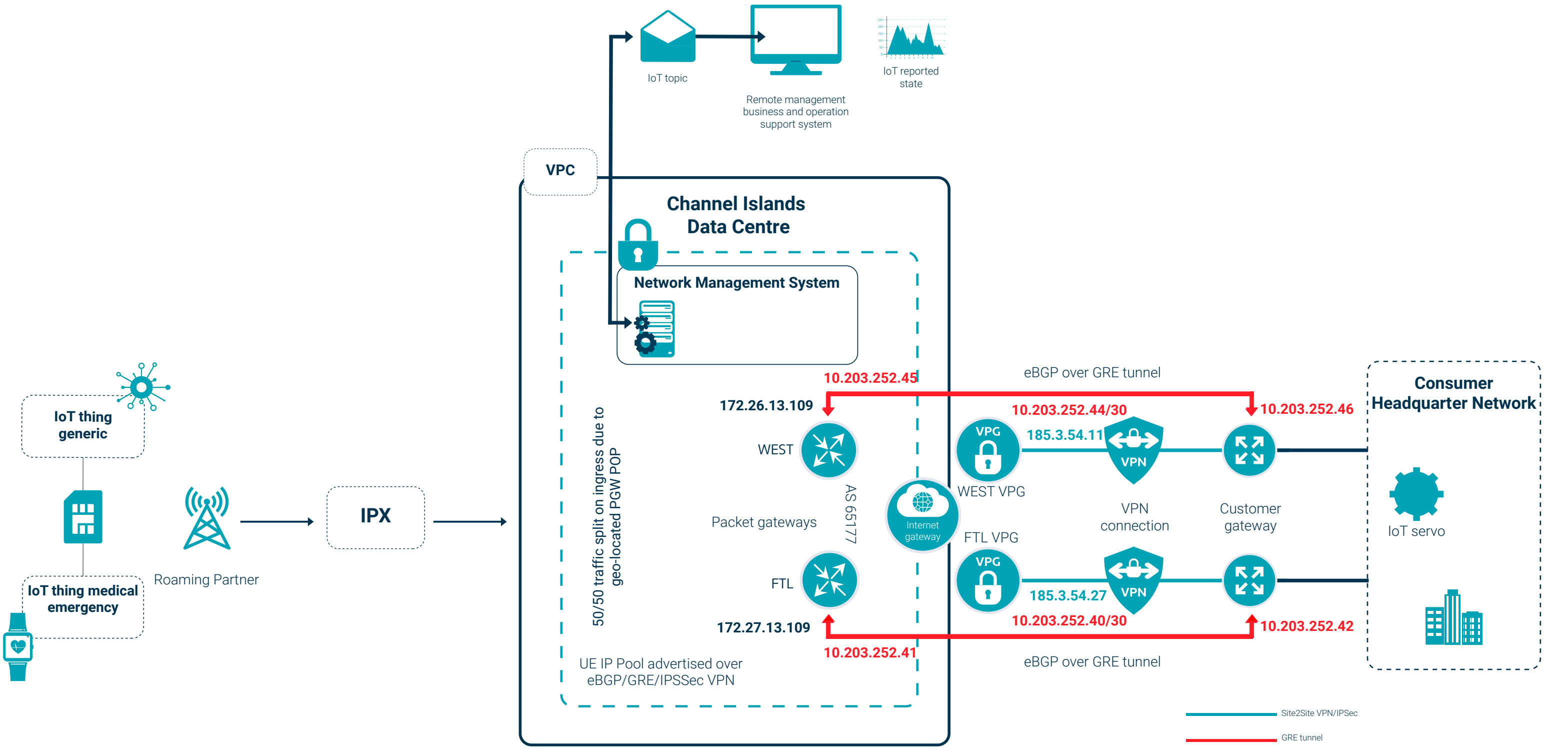


CI Enhanced

This model shows how we can offer an enhanced resilient model for Fixed IP customer that lives on the JT Core.

Previously for a our Fixed IP models we could only offer one IPSec tunnel that had two Firewalls supporting the tunnel in the Velos IoT network. If one Firewall failed then the other would take over but if the IPSec tunnel failed then the customer would experience down time.

To provide full resiliency the customer will need two network devices to configure VPN tunnels. They will also need to support GRE/BGP which provides the routing and failover.



eUICC

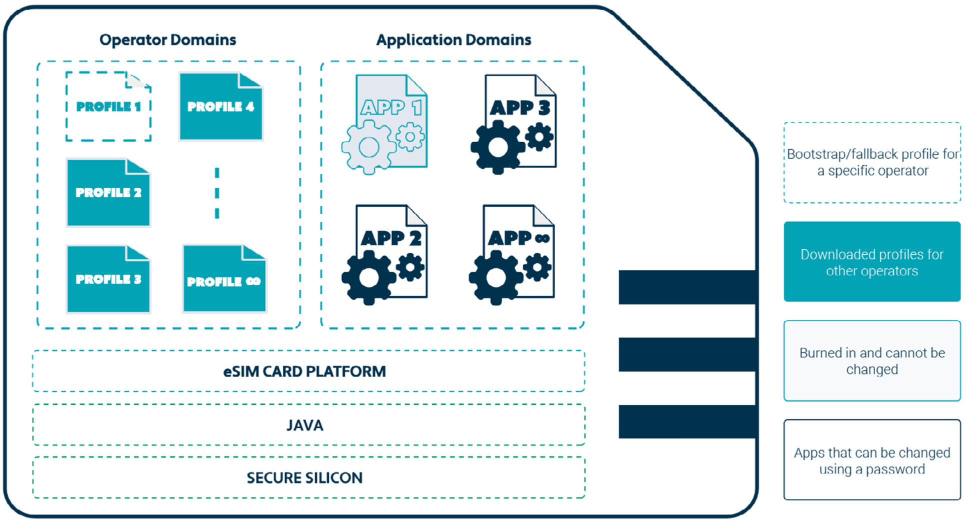
eSIM & eUICC represent the most radical change in over two decades of GSM connectivity in terms of how customers can select and change service provider profiles based on the criteria or business rules of their choosing.

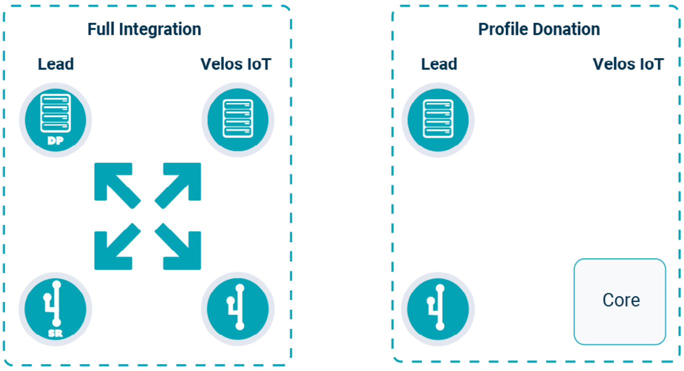
What is an eSIM Profile?
An eSIM Profile is an essential part of eSIM technology. An eSIM Profile is the Operator Profile that allows connectivity to that Operator's network. An eSIM can support multiple eSIM Profiles, which can be downloaded over the air to the eSIM when the eSIM in the field. Only one eSIM Profile can be in use at any one point in time. The eSIM Profile can be used as a bootstrap profile, a fallback profile or a production profile.

What is an eSIM Bootstrap Profile?
An eSIM Bootstrap Profile comes pre-installed on the device. This allows the device to connect to any available network, wherever it is in the world—without any configuration required and works "out-of-the-box". The eSIM Bootstrap Profile is the profile that is used to be able to connect to any network to be able to download new profiles.

What is an eSIM Fallback Profile?
An eSIM Fallback Profile is an eSIM Profile that has been designated to be used if none of the other eSIM Profiles can get connectivity. This allows devices to recover from situations where a profile can not get connected to a specific operator.

What is an eSIM Production Profile?
An eSIM Production Profile is a profile selected for operational or product use. This eSIM Production Profile is typically the one that will be downloaded to the eSIM once the device is used in its usual geography. It is usually a profile that is local to the country.


Operator Domains
Application Domains
PROFILE 1
PROFILE 4
PROFILE 2
PROFILE 3
PROFILE ∞
APP 1
APP 3
APP 2
APP ∞
eSIM CARD PLATFORM
JAVA
SECURE SILICON
Bootstrap/fallback profile for a specific operator
Downloaded profiles for other operators
Burned in and cannot be changed
Apps that can be changed using a password



Edge Data Center Locations

London Equinix Hex	
Address	LD8 6/7/8/9 Harbour Exchange Square, London E14 9GE, United Kingdom
Node	Cisco-uk.hbx.lcr01
Rack Info	Floor 7, Rack 7CF21

Paris Equinix Aubervilliers	
Address	PA 6 10 rue Waldeck Rochet Building 520 93300, Aubervilliers France
Node	Cisco-fr.aub.lcr01
Rack Info	Zone 3, Z3-G6

London Telehouse East	
Address	Tele-house East Coriander Ave, London E14 ZAA, United Kingdom
Node	Cisco-uk.the.lcr01
Rack Info	2nd Floor, TMF51, Rack J2

London Equinix Powergate	
Address	LD 9 Unit 2 Powergate Site, Park Volt Avenue, London NW10 6PW, United Kingdom
Node	Cisco-uk.pwg.lcr02
Rack Info	Zone 3, Z3-G6

London Telehouse North	
Address	Tele-house North Coriander Ave, London E14 ZAA, United Kingdom
Node	Cisco-uk.thn.lcr01
Rack Info	4th Floor, TFM4, Rack C4

Reach your full potential with Velos IoT

Formerly JT IoT, Now a combined global business with Velos IoT, Top Connect and NextM2M. Velos IoT is a leading IoT connectivity solutions provider with over ten years of best industry knowledge and strong financial stability.

We provide resilient global IoT connectivity with over 600 networks in over 200 countries and territories managed through a world-class connectivity management platform to over 17 million cellular devices worldwide. Whether you are a growing business or a global enterprise, we have a fully scalable business model that can be adapted to your specific business needs.

Start your IoT journey with us, **contact an IoT expert today**.

velos

velosiot.com

Velos IoT

@ velos-iot