CyberInova®

INOVAMESH AT A GLANCE (EXTENDED DESCRIPTION)

AGILE SECURITY SOLUTION FOR DYNAMIC MESH

JULY 2023

CYBERINOVA QUICK INTRO

CyberInova®

- Cyberinova is a cyber security startup that designs, develops and deploys innovative cybersecurity solutions
- Cyberinova founders have more than 100 years of combined experience in advanced IT technologies, cyber security, cloud solutions, IT operations and commercial acumen.
- Our founders are former Unisys Italia employees with advanced knowledge of Unisys Stealth
- We have a growing demand for IoT security solutions
    - Engagement with Stealth Leadership since early 2021 to become a channel partner for Stealth in Italy
    - Our prospects appreciated the Stealth solution but deemed it expensive and complicated
    - We developed InovaMesh as a simple IoT segmentation and SASE solution
        - To date we have two InovaMesh deployments (references available)
        - Unisys Cybersecurity Innovation Team tested InovaMesh solution in December 2021

WHY INOVAMESH - AN INNOVATIVE APPROACH

- Never as today the increasing moving of data and information due to digitalization and remote working request high protection to the integrity and the access of a system. Threads like data theft, alteration of the structure, impossibility of access, smarter ackers, for a company can mean risk to stop and block entire manufacturing process, workflow, good delivery, with high costs and losses at different levels.
- The Cloud Security Alliance (CSA) delineated new defensive strategies from aggression on the network with a new concept, called Software Defined Perimeter (SDP), based on the Zero Trust Network Access (ZTNA) , a security framework where access is continuously verified.
- Based on SDP/ZTNA concepts and exclusive capabilities like mesh network with Dynamic Overlay Control (DYNOC©, a CyberInova® patent pending Id #102023000017760 technology) with InovaMesh® our aim is to enhance the way people connect, to deliver the most agile, safe, and efficient cybersecurity structure.
- **This is the reason why we designed InovaMesh®.**

INOVAMESH - THE AGILE SECURITY SOLUTION

CyberInova®

- The innovative cyber security strategy
  - InovaMesh® is an application framework based on idea that no device or user can be trusted, regardless of whether they are inside or outside the network perimeter.
- A one-to-one relationship between user and the data to access
  - InovaMesh® replaces centralized security controls with distributed software agents that operate under the control of the application manager and provide access to the application infrastructure only after identify verification. These agents create encrypted connections between requesting systems and application infrastructure, with a one-to-one relationship between them.
  - InovaMesh® IoI
    - An all-in-one device that protects IoT devices providing micro-segmentation, isolation, alert and monitoring.

InovaMesh® is the Agile Security Solution.

INOVAMESH – BENEFITS FOR CUSTOMERS

CyberInova®

- Trought micro-segmentation InovaMesh® removes implicit trust and implements micro-perimeter (SDP) preventing techniques of hacking, as lateral movement which can be possible with traditional VPNs.
- It's a SaaS solution (Software as a Service) accessible by client software agents and/or in version with its hardware client.; any apparatus can be connected via LAN/WAN to InovaMesh®. (Windows, mac OS, Linux, iOS, Android etc..).
- Extremely easy installation, require no change to existing infrastructure.
- Replace traditional VPNs with a superior segmentation solutions in term of security, scalability, easy of installation, management and TCO (Total Cost of Ownership).
- Use modern encryption and communication protocols providing superior performance and security and integrate firewall with the granular access control (IP, ports, services)
- Strong identity control and integration with standard Identity and Access Management (IAM)
- SDK to build agent for a variety of Operating Systems and Hardware architectures.

INOVAMESH SUITE

CyberInova®

- Three Integrated Solutions:
  - InovaMesh Remote Worker: an all-in-one device that provides remote/home users with microsegmentation and isolation replacing traditional VPN
  - InovaMesh IoT: an all-in-one device that protects IoT devices by providing microsegmentation, isolation, alert and monitoring
  - InovaMesh SDK: Go SDK library to consume the InovaMesh APIs

INOVAMESH DESIGN PRINCIPLES

CyberInova®

- Cloud native solution based on microservices
  - Small, independents services that communicate over well-defined APIs (RESTful)
  - Leverage microservices and cloud-platforms
- Easy to install (zero-touch configuration).
- Running on COTS devices with low powers, memory and storage (ARM, MIPS processors)
  - Ability to run cheap devices
  - Not linked to a specific device: if it supports Linux (e.g. OpenWRT) we can use it
- Separation of Data Plane from Control Plane
- Zero Trust Network Access principles

INOVAMESH KEY FEATURES

CyberInova®

- Replaces traditional VPNs with a superior segmentation solution in terms of security, scalability, ease of installation, management and TCO (Total Cost of Ownership)
- Requires no changes to existing infrastructure
- Uses modern encryption and communication protocols providing superior performance and security
- Integrated Host Firewall with the granular access control (IP, service, ports)
- Go SDK to build agents for a variety of Operating Systems and hardware architectures.

INOVAMESH KEY FEATURES (CONT)

CyberInova®

- All the components are available for inspection and assurance

- Strong identity control
  - Integration with the customer's existing Identity Provider
  - Standard supported are SAML2, OAuth2 or OpenID Connect
  - Integrates 2FA if required

- Granular access filter based on security groups

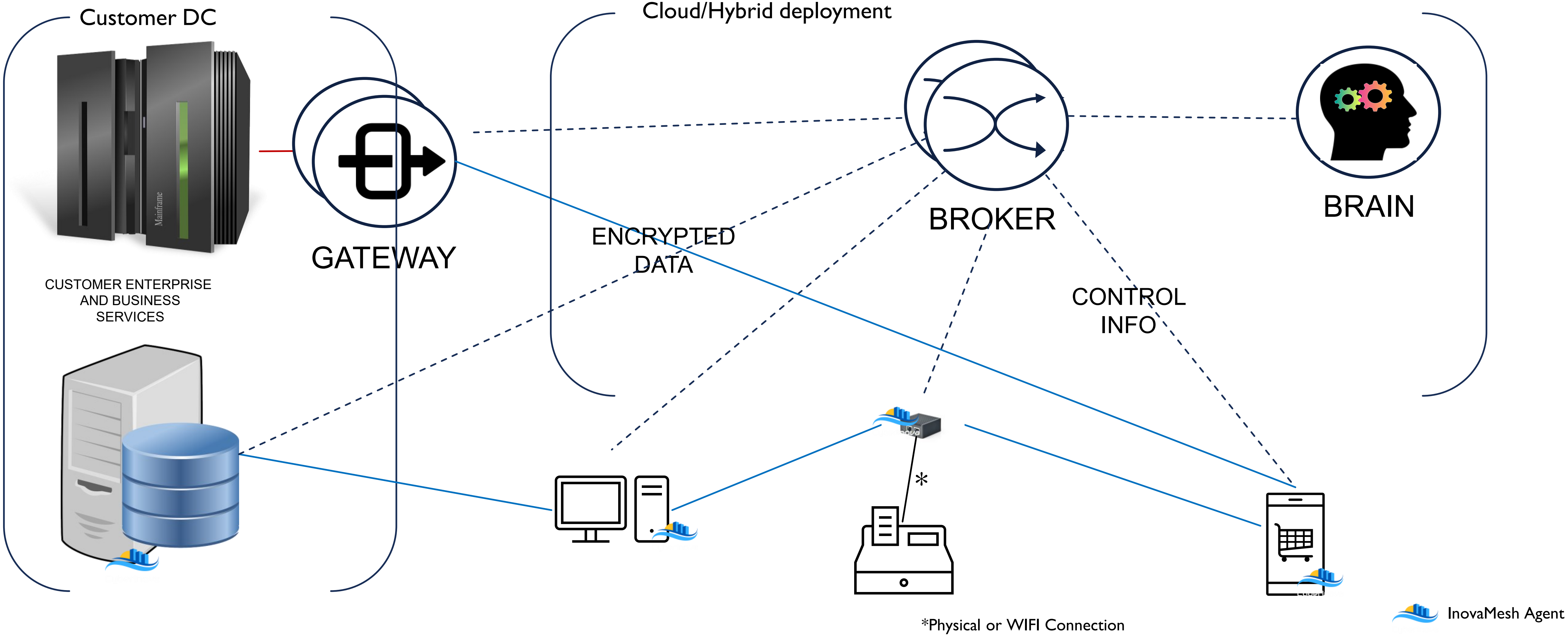
- Captures and organizes the IP traffic that crosses the mesh by recording it locally and at the same time sending it to the ELK (Elasticsearch Logstash Kibana) for auditing and troubleshooting

INOVAMESH FEATURES

CyberInova®

Feature	InovaMesh
Network Segmentation	Yes
Private Virtual Network Mesh	Yes
Active Mesh Isolation	Yes
Running on amd64,arm,arm64,mips,mips64,riscv64,ppc64	Yes
Cloaking (hide device from rest network)	Yes
Support Android and iOS	Yes
Isolation (blocking device internet access)	Yes
Layer 3 Filtering and Access Control	Yes
User Portal	Yes
Active Directory Based Access Control	Yes
Support SAML, OpenID, OAuth2	Yes
Code available for inspection and assurance	Yes
Self-hosted (private)	Yes
Cloud-hybrid hosted	Yes

INOVAMESH OVERVIEW



*Physical or WIFI Connection

HOW IT WORKS: DATA LAYER

CyberInova®

- InovaMesh uses Nebula* by Slack to create a private isolated and encrypted mesh groups (similar to Unisys Stealth COIs):
  - Nebula is a scalable overlay networking tool with a focus on performance, simplicity and security
  - It has been deployed to over 50,000 devices around the world
  - It runs on Linux, macOS, Windows, iOS, and Android
  - Incorporates: Encryption , Security groups , Certificates and Tunnelling
  - Clients can have their own dedicated implementation
    - Note: this is very important: other similar solutions use "cloud" distributed systems (beacons and relays) owned and operated by a 3rd party. This means that it is not possible to separate traffic between different customers or perform a real pen test (e.g. ZeroTier)
    - We are open to full code inspection and independent security assessment

*An in-depth analysis can be found at https://www.diva-portal.org/smash/get/diva2:1528480/FULLTEXT01.pdf

HOW IT WORKS: DATA LAYER (CONT)

- Nebula by Slack HQ is Opensource under MIT license
  - Commercial Use
  - Modification
  - Distribution

- Defined Networking in Santa Monica provides Nebula commercial support (like RedHat for Linux)

- As of December 2021, Defined Networking has received $15M in funding and it is valued at $65M

- Cyberinova is discussing a partnership agreement for the support (under NDA terms)

INOVAMESH DATA LAYER: NEBULA

CyberInova®

- Nebula is a mutually authenticated peer-to-peer software-defined network based on the Noise Protocol Framework.
- Nebula uses certificates to assert a node's IP address, name, and membership within user-defined groups.
- Nebula's user-defined groups allow for provider agnostic traffic filtering between nodes.
- Discovery nodes allow individual peers to find each other and optionally use UDP hole punching to establish connections from behind most firewalls or NATs.
- Users can move data between nodes in any number of cloud service providers, data centres, and endpoints, without needing to maintain a particular addressing scheme.
- Nebula uses Elliptic-curve Diffie-Hellman (ECDH) key exchange and AES-256-GCM in its default configuration.
- Nebula was created to provide a mechanism for groups of hosts to communicate securely, even across the internet, while enabling expressive firewall definitions similar in style to cloud security groups.

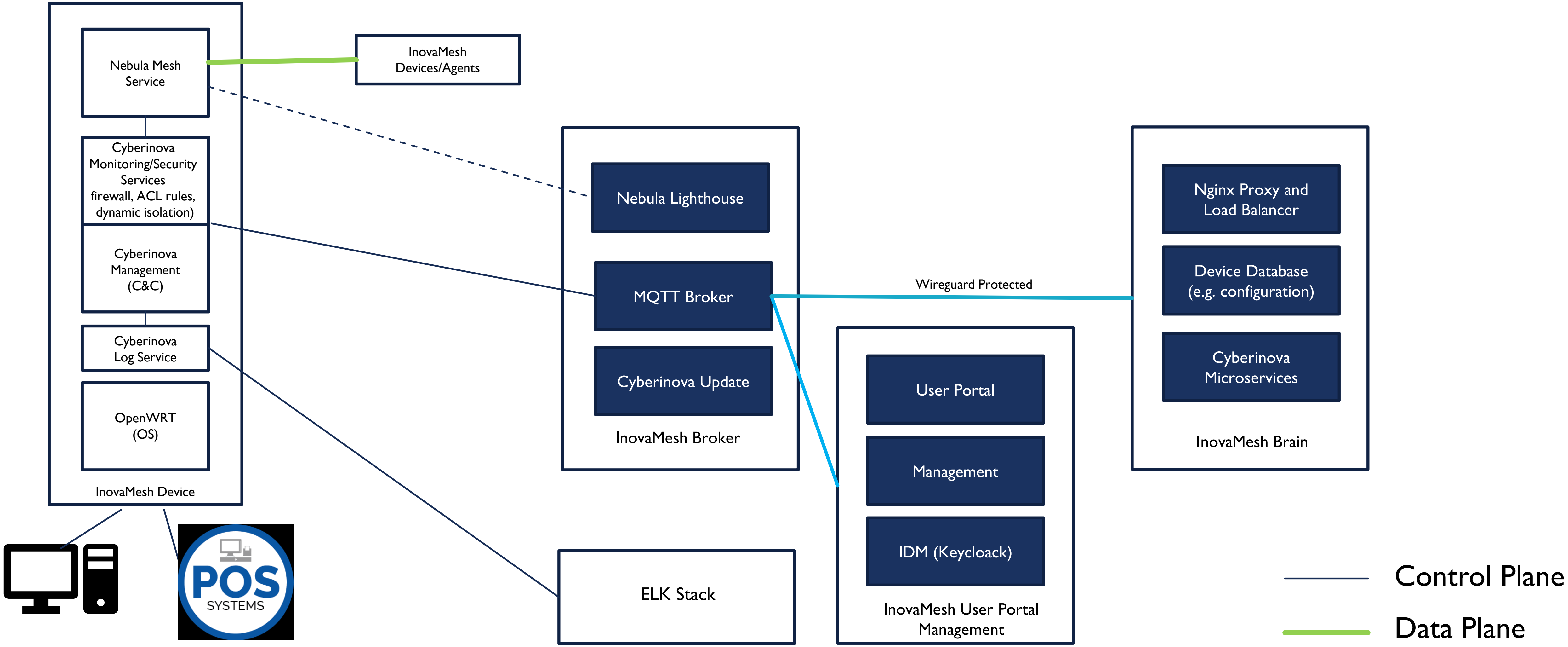
INOVAMESH DEVICE SECURITY

- The security of the Operating System
- All hardware devices qualified by CyberInova have Linux based operating systems.
- The security of the Linux system firewall built into the kernel (iptables).
- The security of the Data Layer.
- Encryption of the certificates and configuration are encrypted on the device and in transit.
- Serial numbers are unique and calculated at every boot: the solution prevents two devices with the same ID and only one device can write/read to its own MQTT topic.

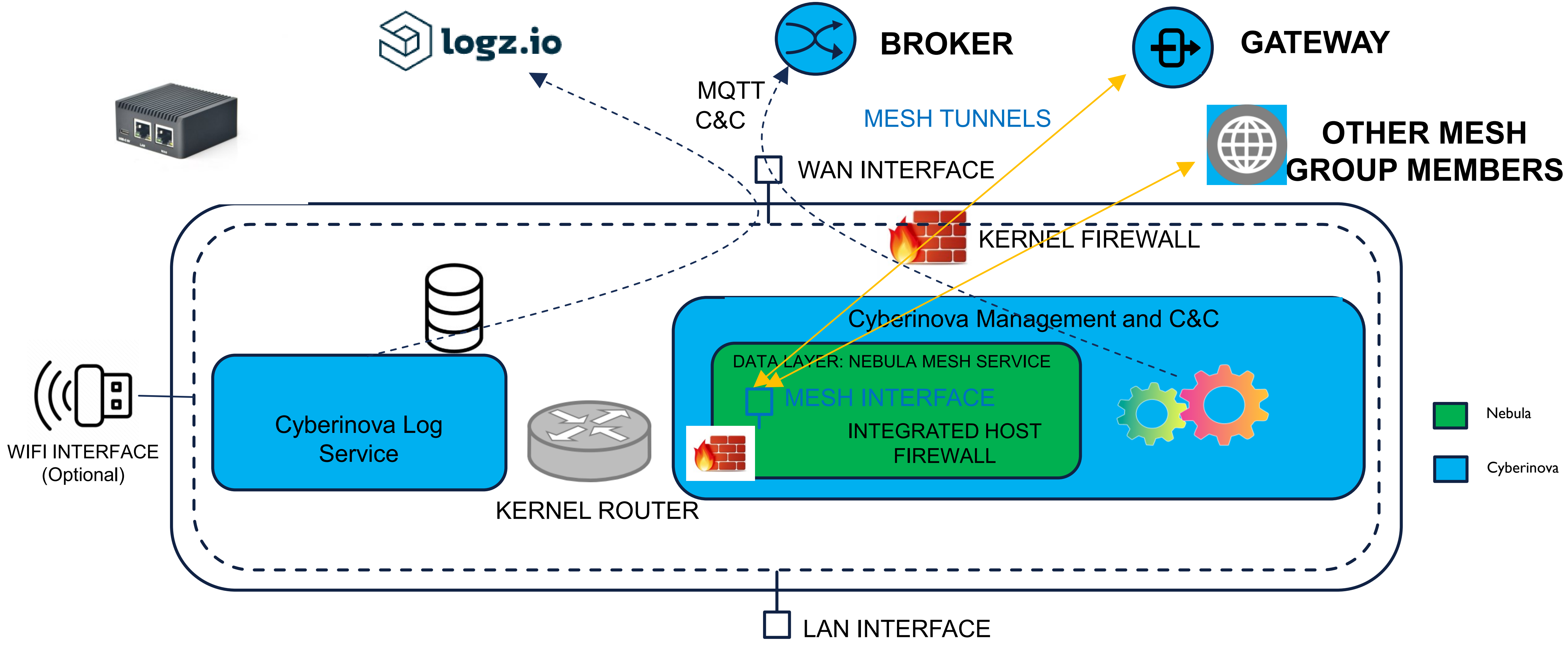
HOW IT WORKS: CONTROL LAYER

- The Control Layer is Cyberinova's intellectual property:
  - Orchestration and the management of the mesh technology (Nebula)
  - Zero-touch configuration of the device
  - Active Mesh Isolation
  - Autoenrollment, registration and activation of the device/agent
  - Monitoring and control (e.g. update)
  - Dynamic configuration (e.g. group management, access rule, routing)
  - Deployment management
  - Integration with Identity Management solutions (e.g. AD, SSO)
  - Automatic Nebula certificate management
  - Additional security features such as the encryption of the Nebula certificates and configuration in transit and at rest

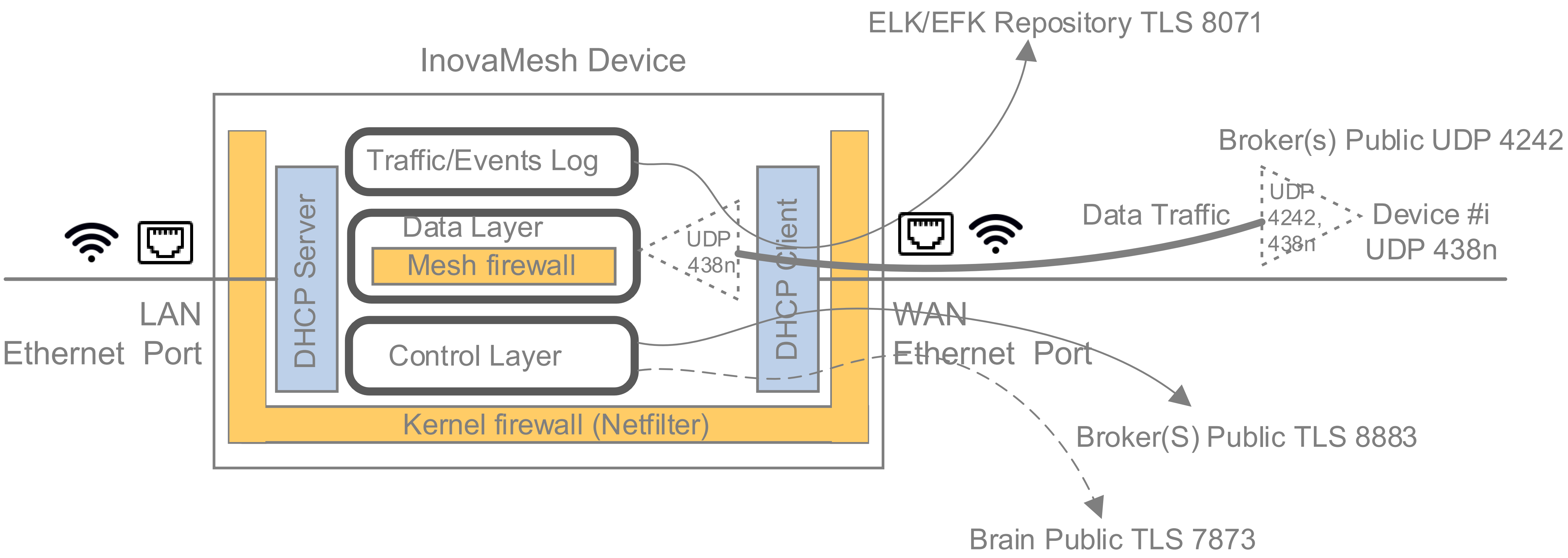
INOVAMESH: ARCHITECTURE OVERVIEW



INOVAMESH DEVICE – MAIN FLOW



INOVAMESH DEVICE – CLIENT FLOW



INOVAMESH COMPONENTS

CyberInova®

- InovaMesh Brain:
    - The "Heart" of the system
    - Written in Node.js (efficient performance, easy deployment process, ability to handle multiple requests and scale smoothly)
    - Some of the microservices:
        - Start/Stop mesh
        - User enrolment/activation
        - Device enrolment/activation
        - Nebula enrolment/activation
        - Group management
- Communicates only with the Broker over a secure (Wireguard) connection
- Can be hosted in our cloud (as a service) or at the Service Integrator cloud/DC, or customer cloud/DC
- Code available for inspection and assurance

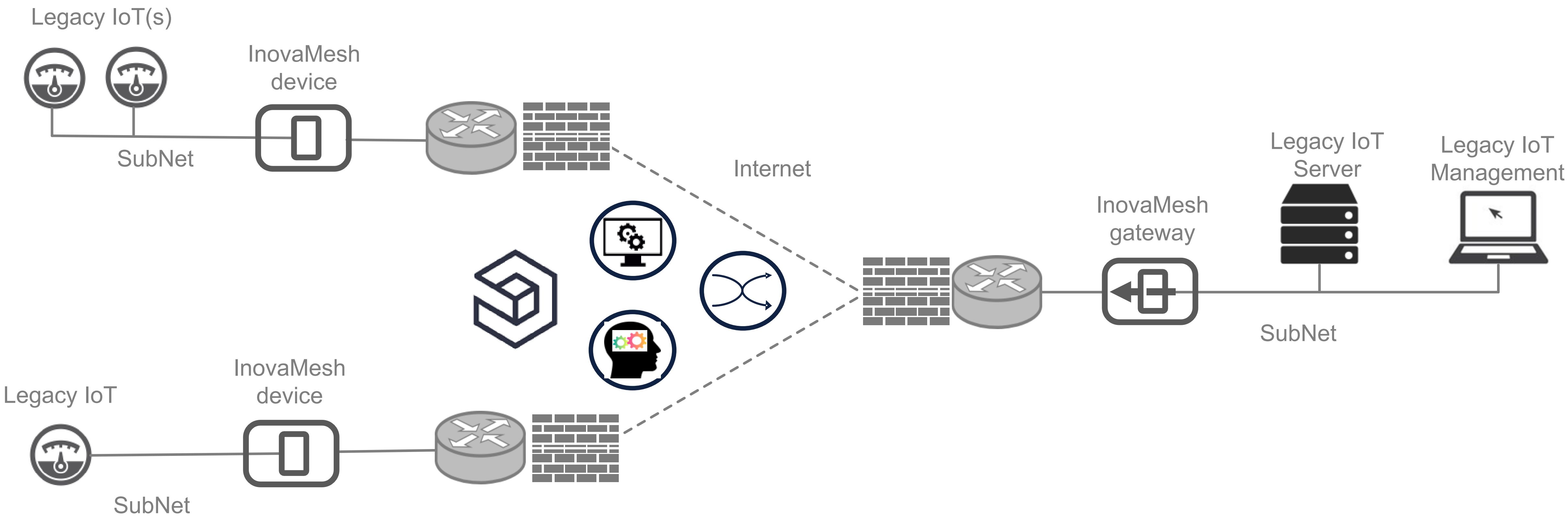
INOVAMESH: COMPONENTS

CyberInova®

- InovaMesh Broker:
  - Connections from behind most firewalls or NAT
  - Based on the facto IoT messaging protocol MQTT (Mosquitto Eclipse server)
  - All communication encrypted and mutually authenticated
  - Lighthouse for Nebula mesh
- InovaMesh ELK stack
  - Collect stats about mesh usage and traffic (metadata): time mesh started stopped, user/device link, data rate and amount of data transfer, IP addresses, protocols and ports
  - Offered as a managed service (by Cyberinova), or for integration with Client Solutions
  - Can be replaced by other log management /aggregation services
- InovaMesh Agent/Device
  - Nebula Service (create the mesh) (written in Go)
  - Cyberinova agent: Management and C&C (command and control) (Written in Go)
  - Cyberinova Log Service (Written in Go)

INOVAMESH DEVICE – LEGACY IOT USE CASE

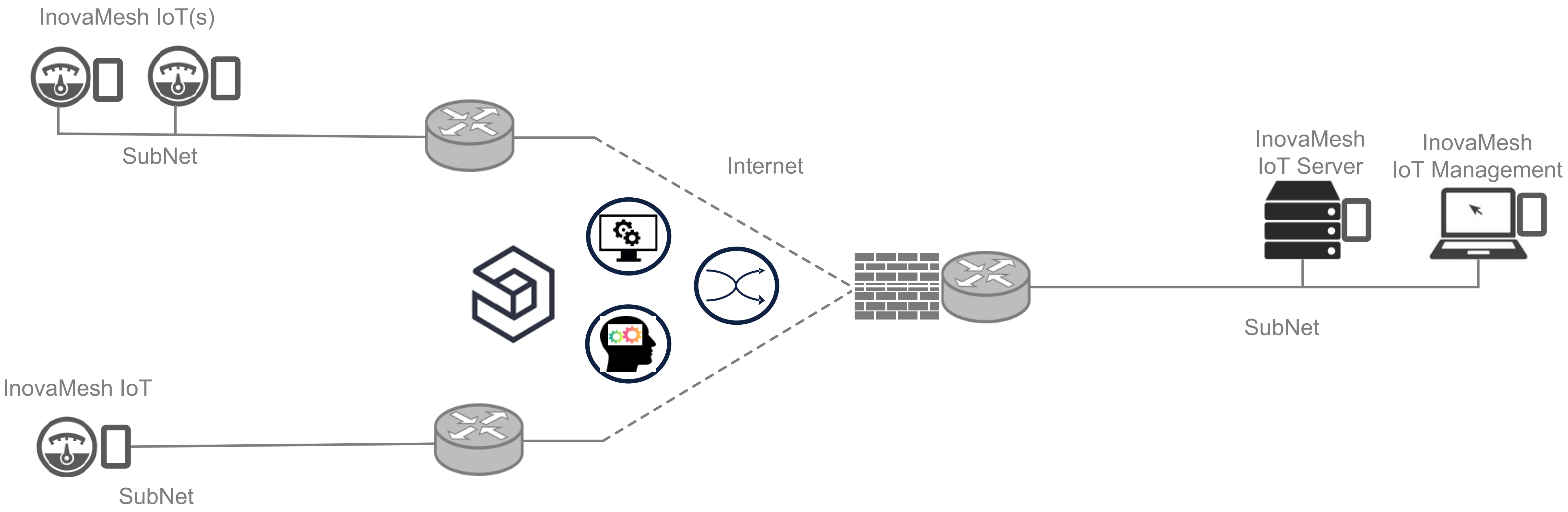
Possible use case of legacy IoT(s), InovaMesh devices and server(s)



INOVAMESH DEVICE – EMBEDDED IOT USE CASE

CyberInova®

Possible use case of Industry 4.0. IoT(s) with InovaMesh embedded and server(s)



INOVAMESH: SOME CERTIFIED DEVICES

CyberInova®

Model	Manufacturer	SoC	O.S.
GL-AR750S	GL.iNet	Qualcomm QCA9563, single-core @775MHz ARM Cortex A7 32bit	OpenWRT
GL-B1300	GL.iNet	Qualcomm IPQ4028, quad-core @717MHz ARM Cortex A7 32bit	OpenWRT
RUTX08	Teltonika Networks	Qualcomm IPQ4018, quad-Core @717 MHz ARM Cortex-A7 32bit	RutOS
NanoPi R1	FriendlyElc	Allwinner H3, quad-core @1.2GHz ARM Cortex-A7 32bit	OpenWRT
NanoPi NEO3	FriendlyElc	Rockchip RK3328, quad-core @2,4 ARM GHz Cortex-A53 64bit	OpenWRT
NanoPi R2S	FriendlyElc	Rockchip RK3328, quad-core @2,4 GHz ARM Cortex-A53 64bit	OpenWRT
Hypervisor	Microsoft, VMware etc	Intel i9-9980HK, octa-core @2.40GHz x86 64bit	OpenWRT, Linux

INOVAMESH ROADMAP AND STATUS

CyberInova®

- We have successfully completed two POCs (references available)
  - Largest IT Service provider to Italian Local Government administration (>50 devices, distributed sites across EU)
  - West-Sud uses InovaMesh for his developers in smart working connections

- Planned POC with a critical infrastructure energy provider

- InovaMesh is at the Minimum Viable Product stage

- Future Product development includes:
  - Management portal for Brain configuration
  - Expand functionalities of User Portal (e.g. WIFI set-up for WIFI to WIFI connection)
  - Dockerizing the Brain and Broker inside Kubernetes

THANKS FOR YOUR ATTENTION

CyberInova®