

Fijoport

The IoT Security Solution



Smart Remote Network Access
& Asset Management

November 2025



Bernardo de la Isla O'Neill – BDM Fijowave
Bernardo.delaislaoneill@fijowave.com

01

Fijowave Company

02

How does Fijoport work ?

03

**Why our customers use Fijoport
Features & Benefits**

04

Fijowave Products & Roadmap

05

Use Cases

06

Appendix



About Fijowave



- Irish company established in 2011

What does Fijoport by Fijowave do?

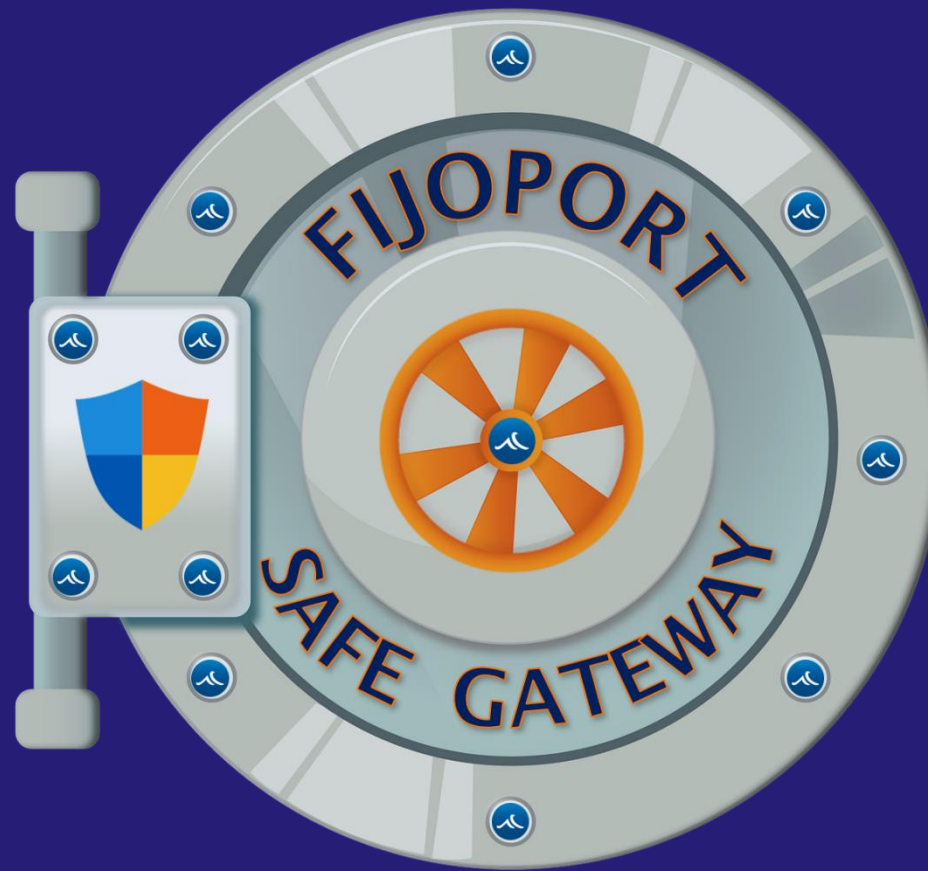
- It provides customers with the ability to **securely** remote access their **IP** devices and **legacy** equipment and **manage** them as if they were directly connected to the units on-site.

Who do we do it for?

- Telecommunications – Carriers, PBX partners
- Manufacturing - Industry 4.0
- Utilities - Electricity sub-stations
- Energy Industry – Renewable energy
- Any Organizations that need 24/7 remote access



How does Fijoport work?



USA



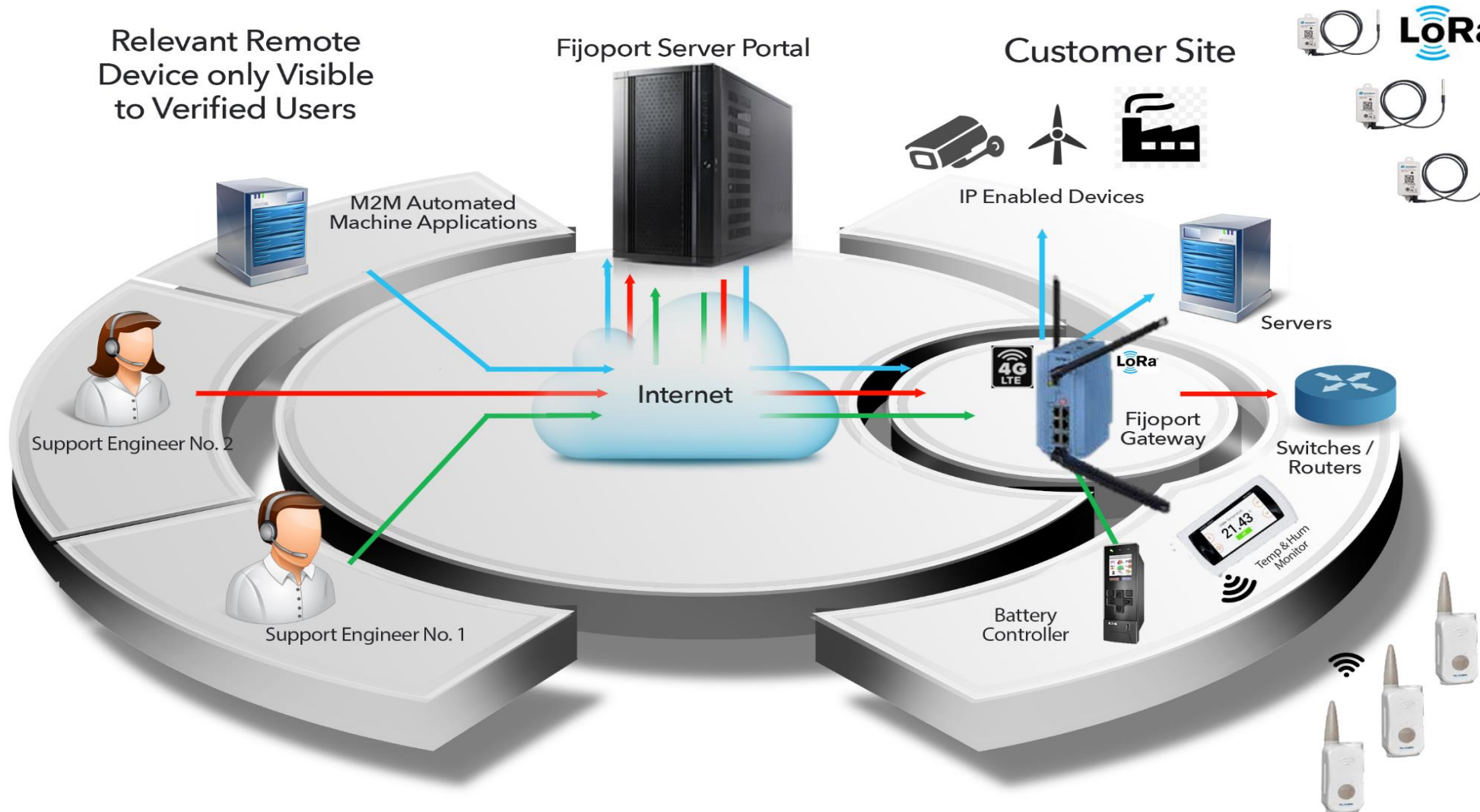
MEXICO



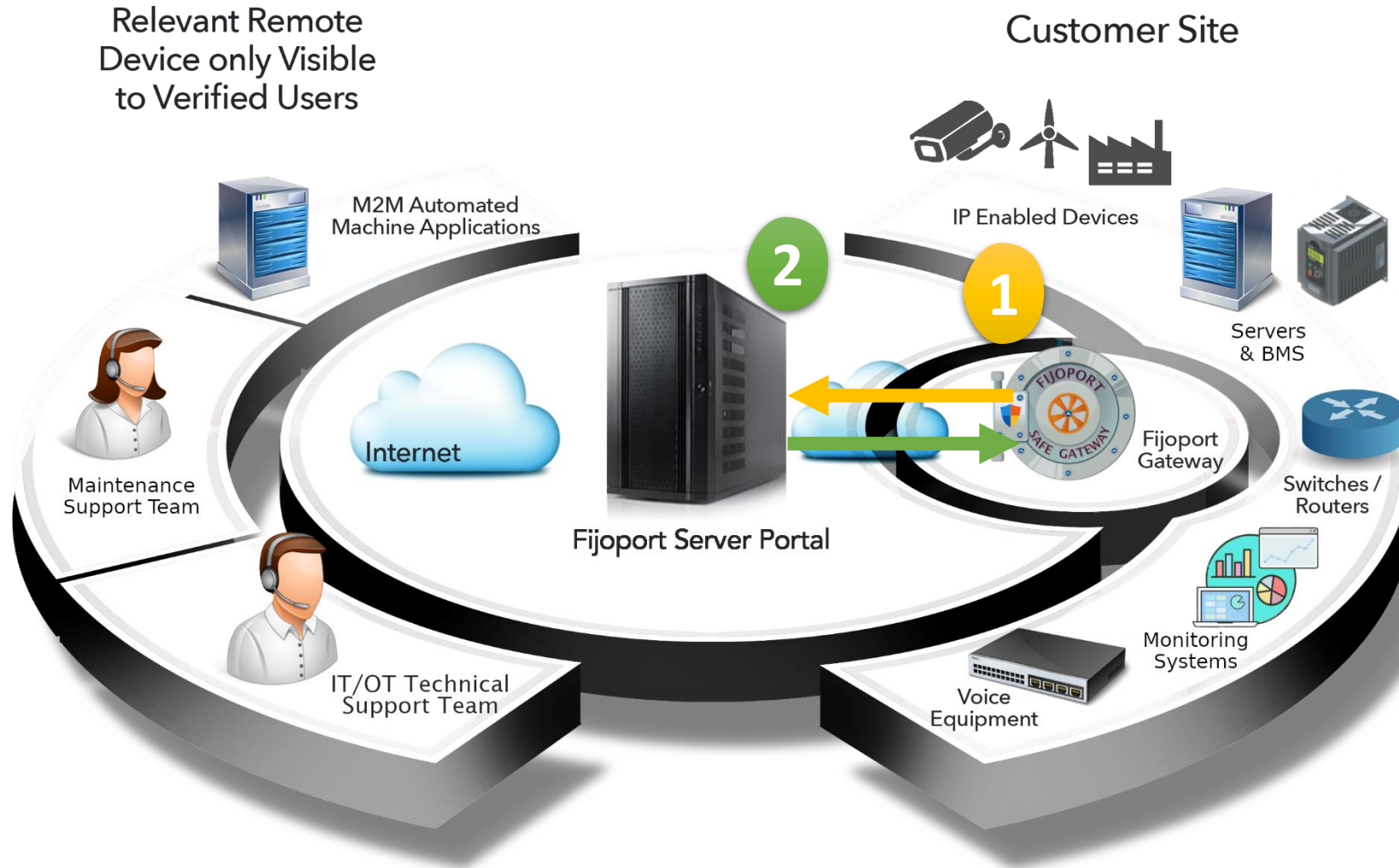
IRELAND



Fijoport Product



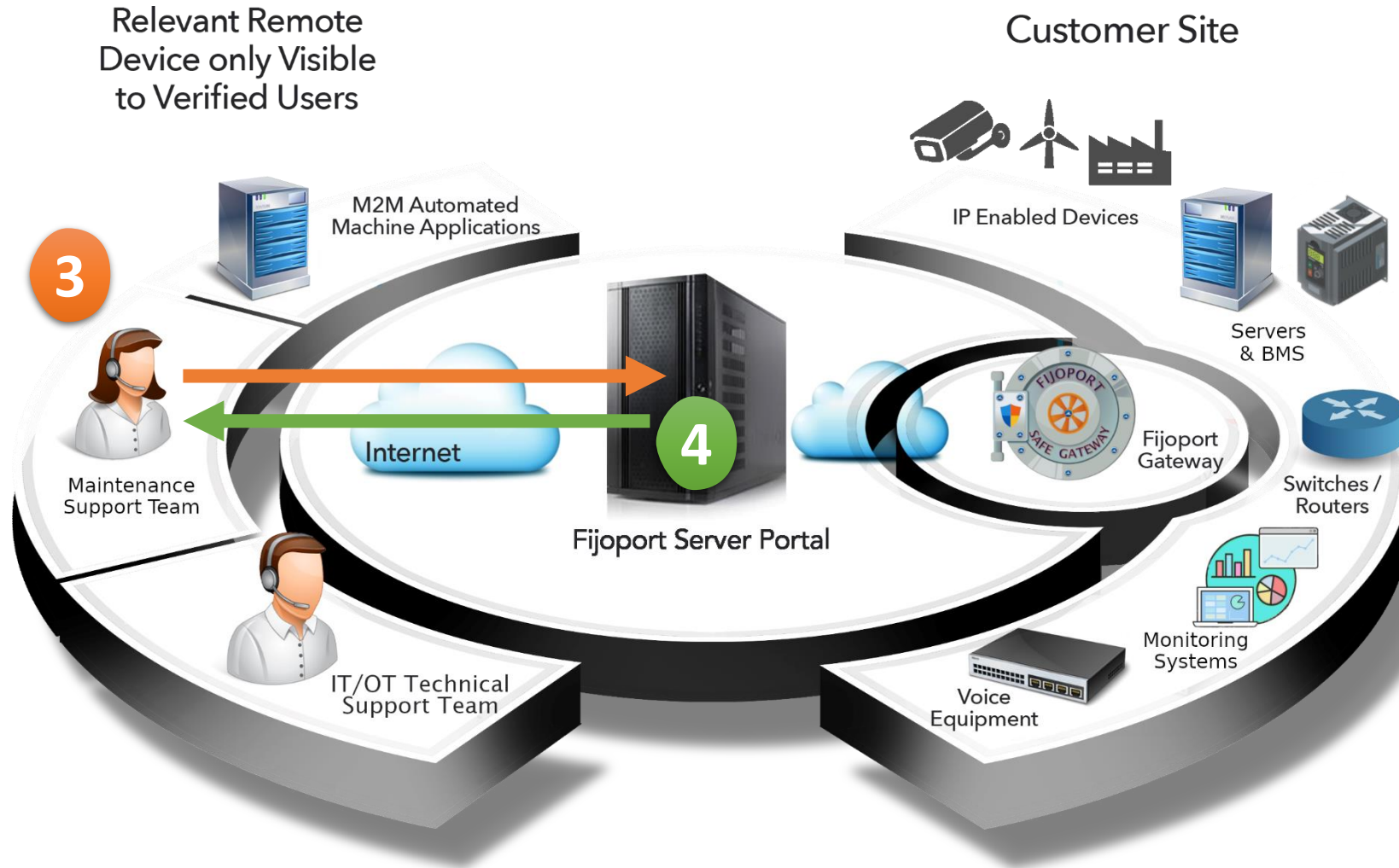
Fijoport Identifies with the server



1. Fijoport outbound connection to Portal server

2. Portal authenticates the Fijoport (RSA public/private keys)

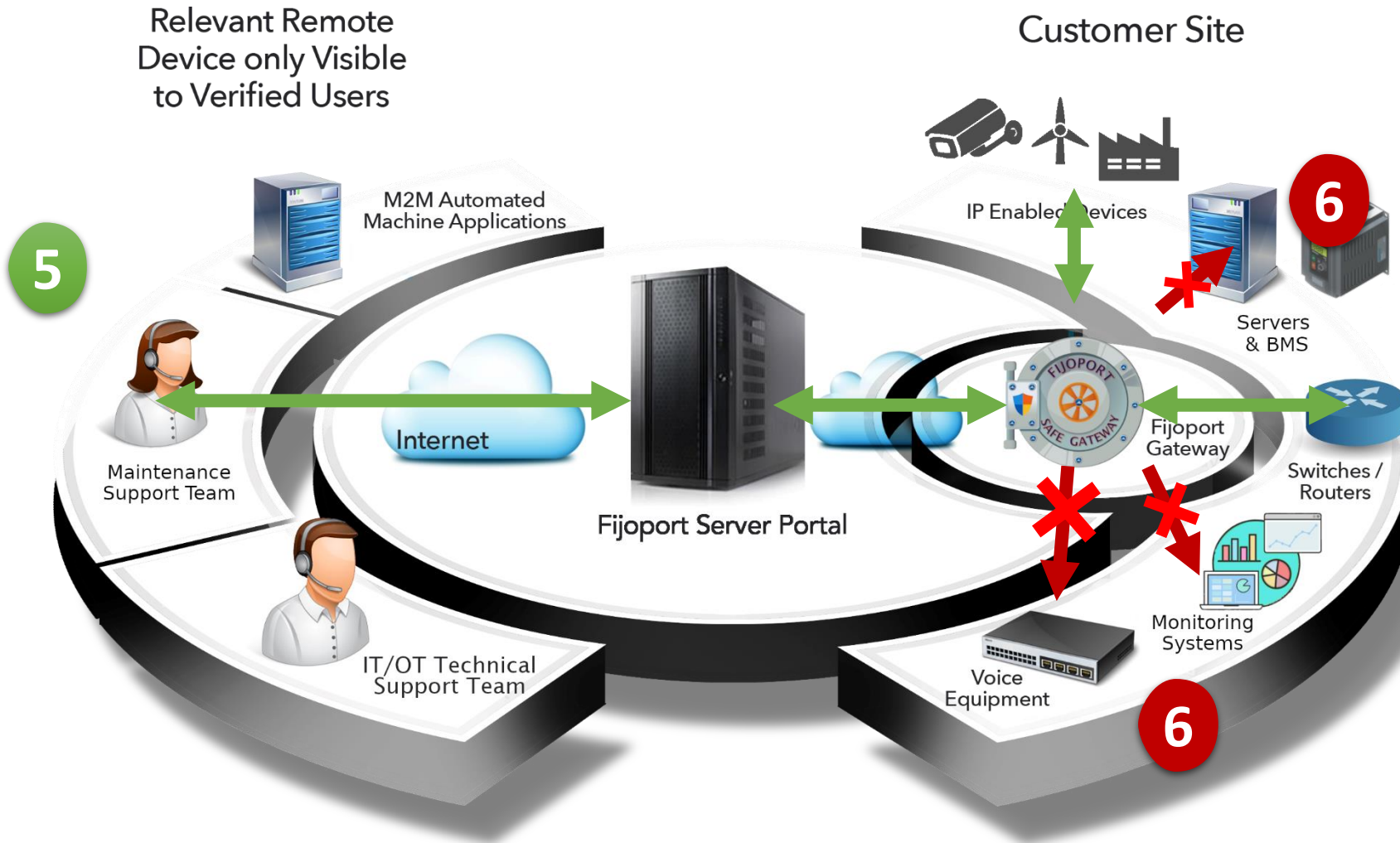
User authenticates with the server



3. User authenticates with the Portal (LDAP, Radius, TACACS+)

4. Access control - administrator decides who can access what devices

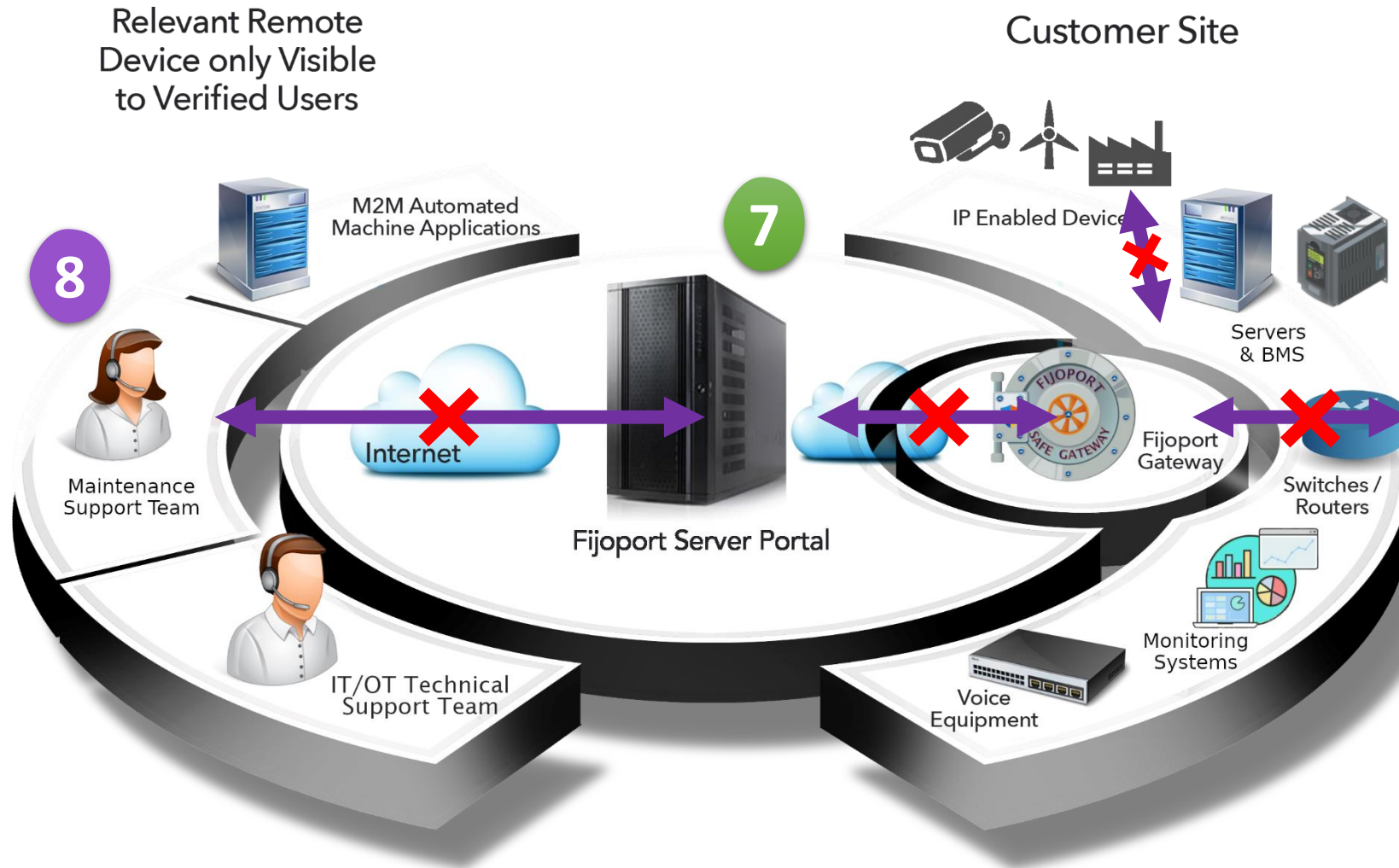
Encrypted tunnel established



5. Upon user request Portal establishes encrypted tunnel to Fijoport (AES)

6. User can access authorized devices only

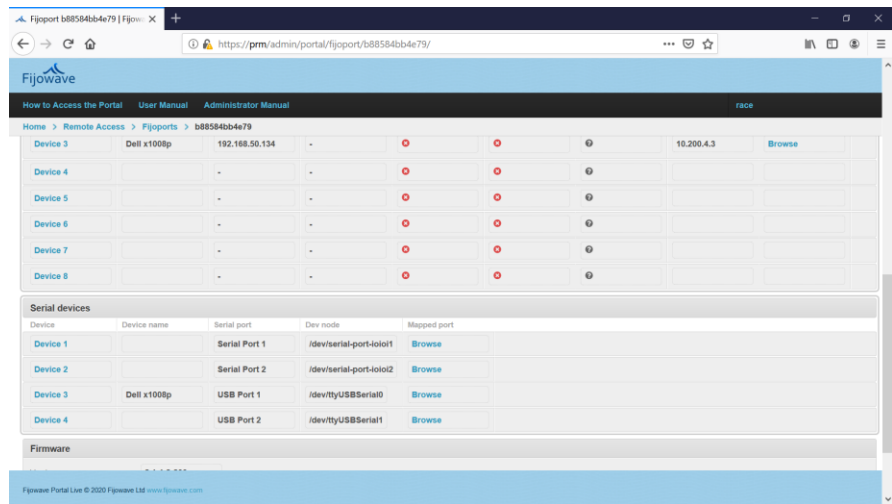
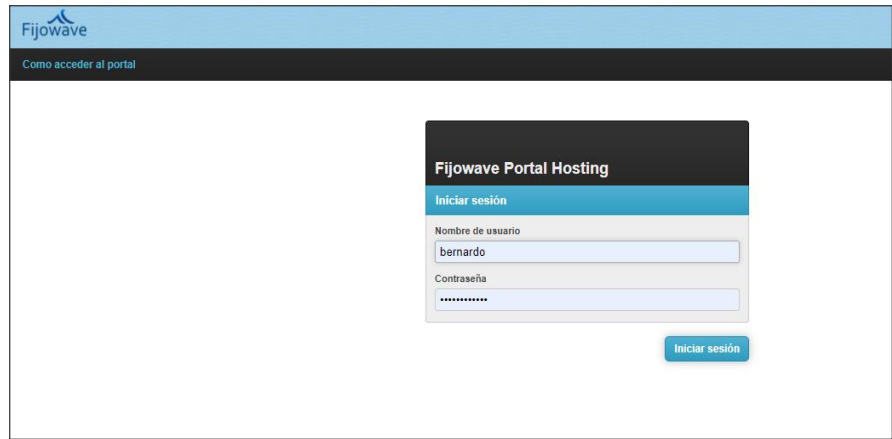
User terminates session



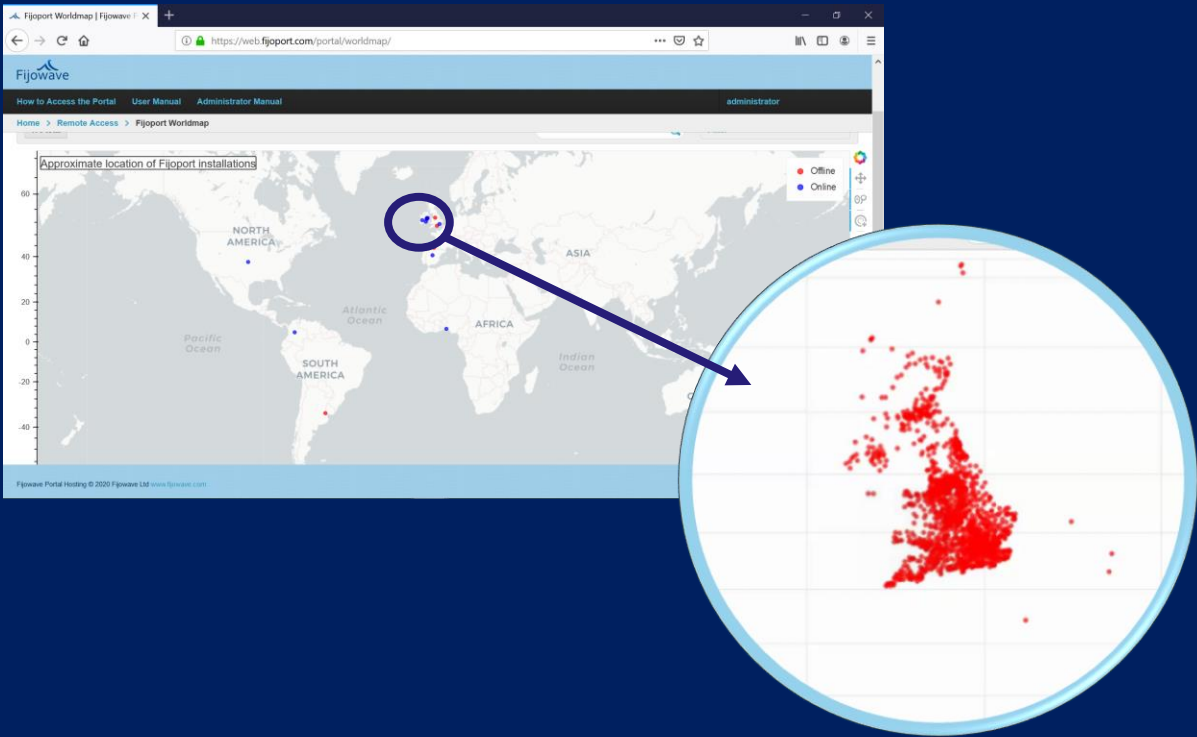
7. Devices or Out-of-band management network ONLY accessible via the Portal

8. IP tunnel is closed when Remote Access Session is completed

User friendly – Web interface portal



Fijoport geographic localization

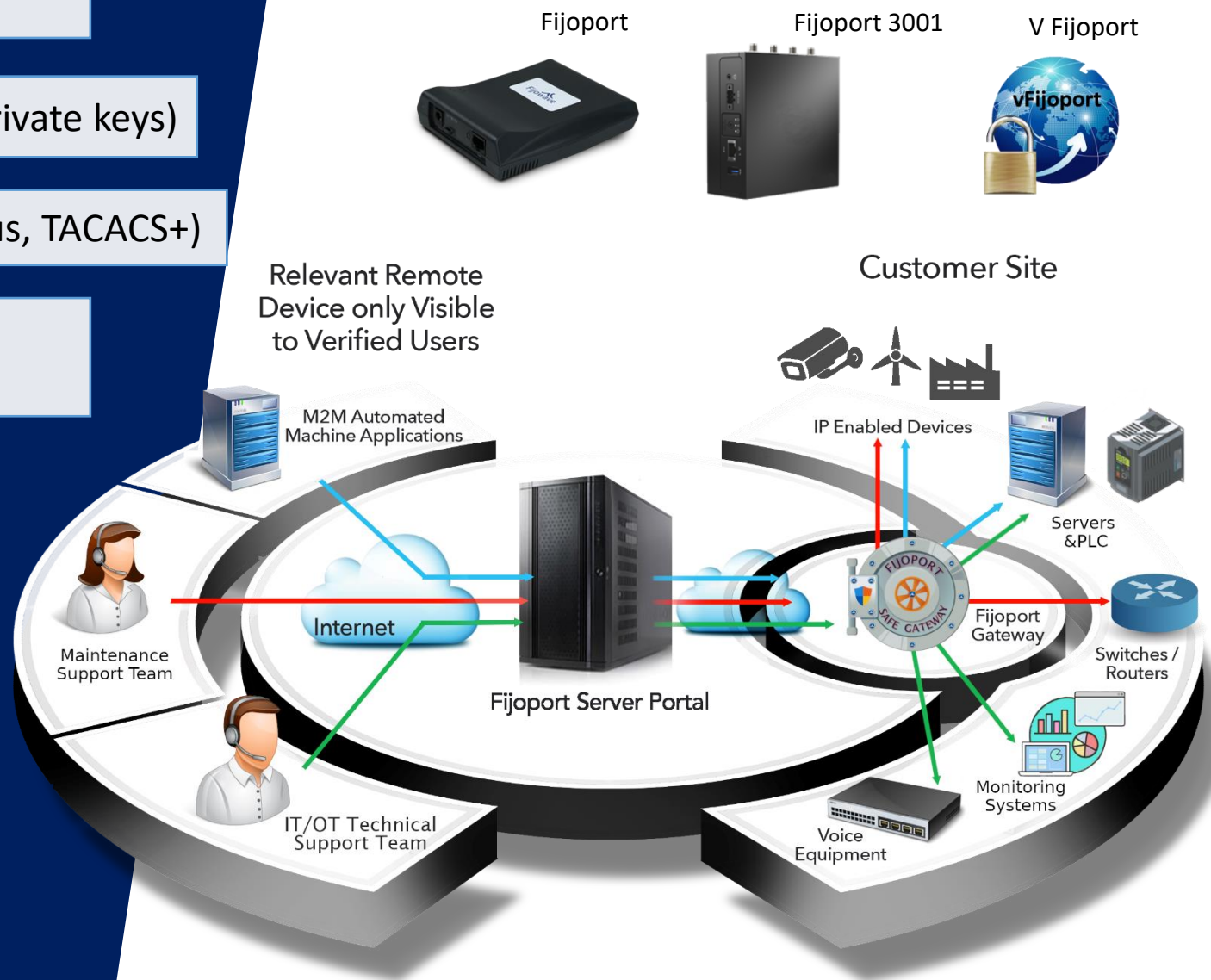


Interactive map locating Fijoports

How does Fijoport work?



- 1 Fijoport outbound connection to Portal server
- 2 Portal authenticates the Fijoport (RSA public/private keys)
- 3 User authenticates with the Portal (LDAP, Radius, TACACS+)
- 4 Access control - administrator decides who can access what devices
- 5 Upon user request Portal establishes encrypted tunnel to Fijoport (AES)
- 6 User can access authorized devices only
- 7 Devices or Out-of-band management network ONLY accessible via the Portal
- 8 IP tunnel is closed when Remote Access Session is completed





Why customers use Fijoport

- ❖ PLUG 'N' PLAY – simple installation, replicability,
- ❖ MULTIPLE CONNECTIONS
 - ❖ IP, LTE & Serial interface for legacy equipment
 - ❖ Can be connected via LAN and Cellular to provide failover (Business Continuity / Disaster recovery)
- ❖ SECURE –
 - ❖ No detectable cyber footprint on site (outbound only effect)
 - ❖ Configurable Remote Access Control List. (per user, per device)
 - ❖ On-demand authorised access via secure VPN session (only via Portal Server).
- ❖ SCALABILITY – Cost competitive from 1 – 1000's of units
- ❖ Operational cost savings & Carbon Footprint reductions
- ❖ SOFTWARE OPTION for Vendor's Hardware.

Fijoport Product Offerings & Roadmap



01

Fijoport - Wired Network

02

Fijoport 3001 - Wired and Mobile

03

Fijoport - Virtual Fijoport (Docker, Vmware, Linux)

04

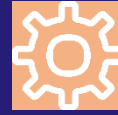
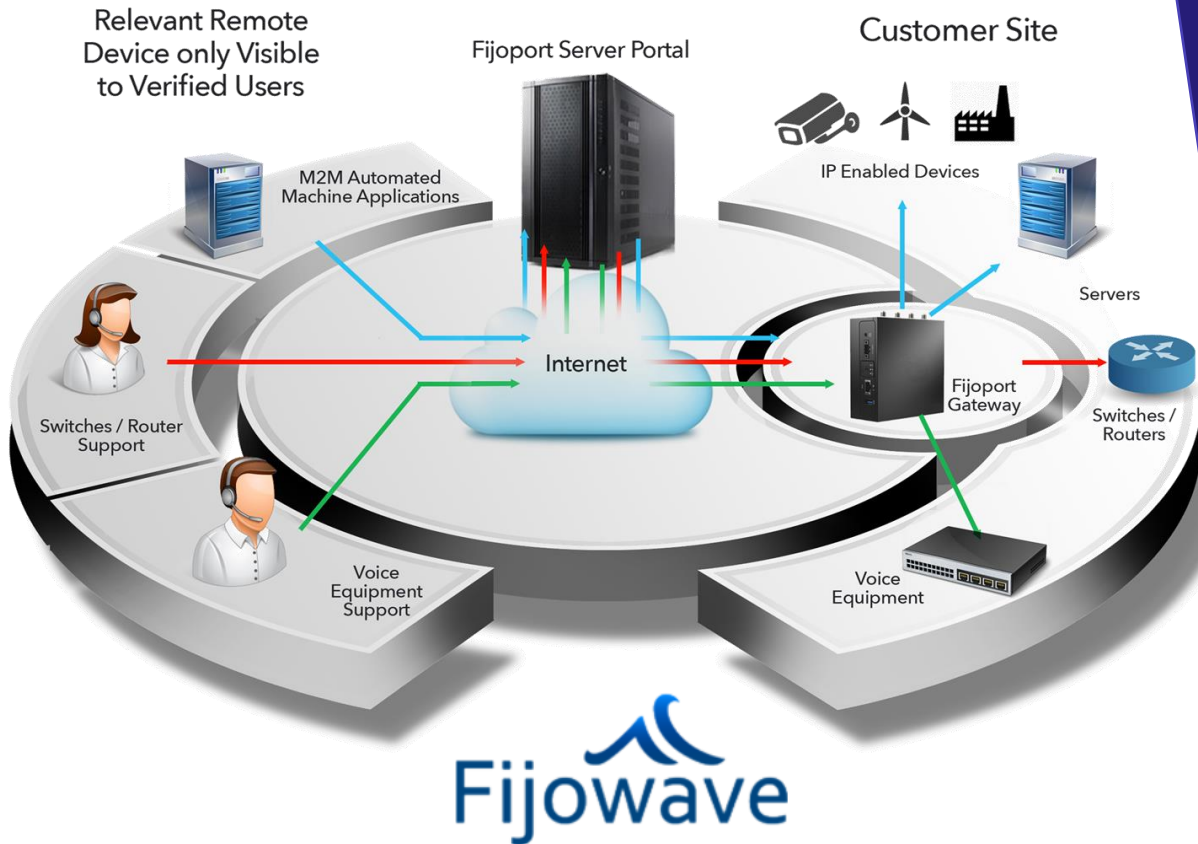
Fijoport - OEM Integration

05

Value Add Applications- Network Health Check, PRM



Summary



Secure Remote Access to IP-enabled (IoT) and Legacy equipment



Scalability from 1 to 1000's of sites



Monitoring (24/7) & Management of Equipment with Dashboard overview and Alerting



AI / Predictive Maintenance



Installation Simplicity – Plug&Play



QUALITY
ISO 9001:2015
NSAI Certified

Use cases

USE CASE – Direct Maintenance & Support



Customer Requirement.

British Telecom (BT), a leading European telco has deployed Fijoport to manage all PBX and SIP Gateways sold by BT to their customers, enabling the monitoring and management of customer sites 24/7 without user intervention at remote site. BT wants to provide its engineers with the ability to remote access IP-enabled equipment on these sites as if they were directly connected to the units on-site. Allowing them to meet its SLA commitments, Increase customer satisfaction and customer retention rates



Key requirements addressed	Additional Benefits
➤ Secure bi-directional encrypted connectivity between user and remote site. ➤ Support for 24/7 maintenance and management of devices without user intervention at remote site. ➤ Control and Management over all user access. ➤ Any access is limited to authorised personnel and all remote sessions are logged and auditable. ➤ Dashboard display of entire network of sites with alerting of fault conditions.	➤ Response times are radically improved while truck roll is reduced. ➤ Simple install procedure, plug and play, fitted in minutes. Can be configured remotely. ➤ Future proofing investment as Fijoport architecture allows easy implementation of new functionality. ➤ Integrated ticketing system allows tracking of engineers' work activity ➤ Increased customer satisfaction and customer retention rate



Zero Trust Architecture: Selector Zero Trust



- Engineer / Operator**
- Requests for access
 - Unattended 24/7

Fijowave
Zero Trust Selector



Portal Server Logout

Current status **CONNECTED**

Connection to portal: Allowed Blocked Allowed

Change the Domain name or IP address and port for the portal server or add a backup server.

Server	IP address	Port
1	f.fijoport.com	
2	176.9.67.54	

Configure Fijoport to connect to the portal through a proxy server.

Use Proxy	Disabled
Proxy Server URL	
Proxy port	

Click Save and then Reset the Fijoport to force immediate reconnection to portal server.

[Return to menu](#) Save Cancel

Powered by Fijowave
www.fijowave.com

- Options to select:**
- Access only
 - Monitoring only
 - Both

Deny access



AVAYA



Allow



IT Site Manager
Fijowave

Remote Access Control Logout

Enter the names and IP addresses of the devices that may be accessed via the portal.

Remote monitoring, access, and available ports may be configured for each device

* = allow all, blank = disallow all, comma separated list of up to 10 allowed ports e.g. 80,443

ID	Description	IP address	Device Type	Permissions	Ports
1	IPO	192.168.54.220		☒ monitoring ☐ access	udp * tcp *
2	Fred	192.168.50.200		☒ monitoring ☒ access	udp * tcp *
3	Dell x1008p	192.168.50.100		☒ monitoring ☒ access	udp * tcp *
4	DECT	192.168.50.217		☒ monitoring ☒ access	udp * tcp *
5				☒ monitoring ☒ access	udp * tcp *
6				☒ monitoring ☒ access	udp * tcp *
7				☒ monitoring ☒ access	udp * tcp *
8				☒ monitoring ☒ access	udp * tcp *

Click Save and this data will be updated on the portal server after the next RAS session.

[Return to menu](#) Save Cancel

USE CASE –Secure Remote Access to Electricity Substation



Customer Requirement.

One of the Fijowave's customers is a leading Irish energy company. They want to provide its engineers and Sub-Contractors with the ability to remotely access IP-enabled equipment and legacy equipment on these sites as if they were directly connected to the units on-site. The energy company requires a solution that provides both in-band and out-of-band remote access and provides full control over User access, Device access and audit logging capabilities. The energy company wants to analyse variations in performance across their entire network of sites .



Key requirements addressed	Additional Benefits
➤ Secure bi-directional encrypted connectivity between user and remote site. ➤ Control and Management over all user access. ➤ Support for 24/7 maintenance and management of devices without user intervention at remote site. ➤ Licensing and Network layer security policies permit only legitimate traffic in the private network. ➤ No software installations required on remote devices being accessed. ➤ Any access is limited to authorised personnel and all remote sessions are logged and auditable. ➤ Dashboard display of entire network of sites with alerting of fault conditions.	➤ Increased network security, eliminating unsolicited access requests. Total control over access permissions. ➤ Response times are radically improved while truck roll is reduced. ➤ Lower cost of total ownership with minimized number of on-site visits for maintenance. ➤ Ability to scale the solution on demand, without the need to re-design the network connectivity. One solution for all sites. ➤ Reduces companies carbon footprint through significant reductions in truck roll. ➤ Simple install procedure, plug and play, fitted in minutes. Can be configured remotely. ➤ Future proofing investment as Fijoport architecture allows easy implementation of new manual or automated functionality.



Appendix

IoT & Asset Management / Monitoring

Why & What's the benefit

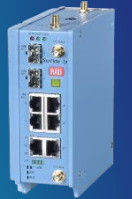


Partners

- Increase revenue Opportunities -
 - Different support package offerings.
- SLA (Service Level Agreements)
 - Reduce Penalties
- Truck Roll.
 - Reduced sites visits & sending the right person & equipment to site if required.
- Optimise resources
 - Allows for different level of expertise work on customer issues simultaneously.
- Predictive Maintenance capability.
 - 24/7 remote access and monitoring allows for AI predictive analysis.
- Customer satisfaction
 - Inform the customer he has an issue and possibly resolve it even before the customer is aware of a problem.
- Reduced carbon Foot print.
- Security updates

End User

- Secure access to Devices & Audit Logs
 - Authorised Users only down to device level
 - Protect devices without username/password options
- SLA (Service Level Agreements)
 - Allows for specification of shorter response times
- Reduced Downtime
 - Cost savings
- Optimise End User resources
 - Efficient use of internal expertise
 - Facilitates remote working
- Predictive Maintenance capability.
 - Reduced Downtime & Schedule maintenance based on performance.
 - Develop your own applications
- Customer satisfaction
 - Early identification and faster response times , reduced downtime costs. Greater flexibility
- Security updates



Fijoport features & benefits



Fijoport features & benefits

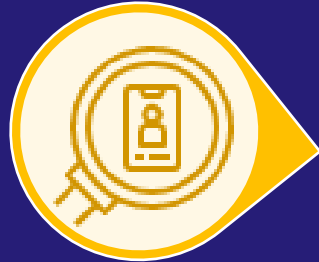
Centralized operations

Alerts of faults sent to the Dashboard, SMS and email



Inventory monitoring

(Licensing, connected phones, hardware and software revisions)



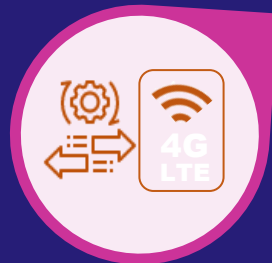
Remote configuration Updates

Deployment of cybersecurity patches



Business continuity

Redundancy –
IoT - Out of band Access 4G LTE



Fijoport



Fijowave



Peace of mind and confidence

One platform management For multi-vendor devices

Switches, firewalls, virtual machines, IP phones, IP DECT, servers, media gateways, SBC – (session border controllers)



Automated advanced 24-7 monitoring control

Alarms sent



Powerful scalability – from 1 to 100,000 devices



Fijoport Advantages

Much more than a VPN

✓ Simple to install

- Plug and play
- IT expertise not required
- Post out fijoport , configure remotely

✓ Same Solution – Small & Large Sites

✓ Centralized administration

- Intelligence in the server
- Centrally monitored and managed
- Separation of concerns

✓ Scalability made simple (1 to 1000's)

- Flexibility No additional rules needed to scale
- No additional approvals required when scaling – same network configuration/design

✓ Allows Secure Access to obsolete operating systems

VS

Standard VPN

⇒ Complex Install

- Time consuming per site
- IT expertise required

⇒ Different VPN configurations for each sites

⇒ Requires both central & per site admin

- Corporate & per site Security Policies
- Public IP Address management per site
- NAT & Firewall rules required per site

⇒ Complex scalability rules

- Limited Flexibility with design
- IT design & approval required when scaling

⇒ Very difficult to provide secure access to obsolete operating systems

Fijoport Advantages

Much more than a VPN

✓ Secure Access to legacy Serial Equipment

✓ Control over set up closedown of VPN's

- Fijoport pre configured with portal server address
- No changes require to inbound firewall or NAT
- Audit logging of connection establishment
- Automatic Shutdown of VPN on inactivity
- Setup requires specific user request
- Bandwidth

✓ Segmentation of User groups

- e.g. IT, OT, Security, Switch, Voice, Legacy user groups
- Managed centrally by Portal administrator, easy to see, manage, add/remove users, access token management)

✓ Network Resilience

- Out of band network access / Failover from Company network

VS

Standard VPN

➔ Access to legacy serial equipment requires additional equipment

➔ Control over set up closedown of VPN's

- Both ends need to be aware of each others public IP address
- Firewall and NAT configuration to allow incoming traffic

➔ Standard VPN's- Segmentation of User groups

- standard VPNs do not have this capability

➔ Reliant on Company Network

Thank You

www.fijowave.com

© Fijowave 2025

Fijoport

La Solución de Seguridad IoT

Acceso Remoto y Cyberseguro
Gestión de Activos inteligente

November 2025



Bernardo de la Isla O'Neill – BDM Fijowave
Bernardo.delaislaoneill@fijowave.com

01

Fijowave

02

¿Cómo funciona Fijoport?

03

¿Porqué nuestros clientes eligen Fijoport?
Funcionalidades y Beneficios

04

Productos Fijowave y hoja de ruta

05

Casos de Uso

06

Apéndice



About Fijowave



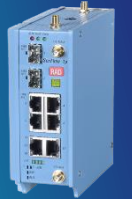
- Compañía Irlandesa establecida en el 2011

¿Que hace Fijoport?

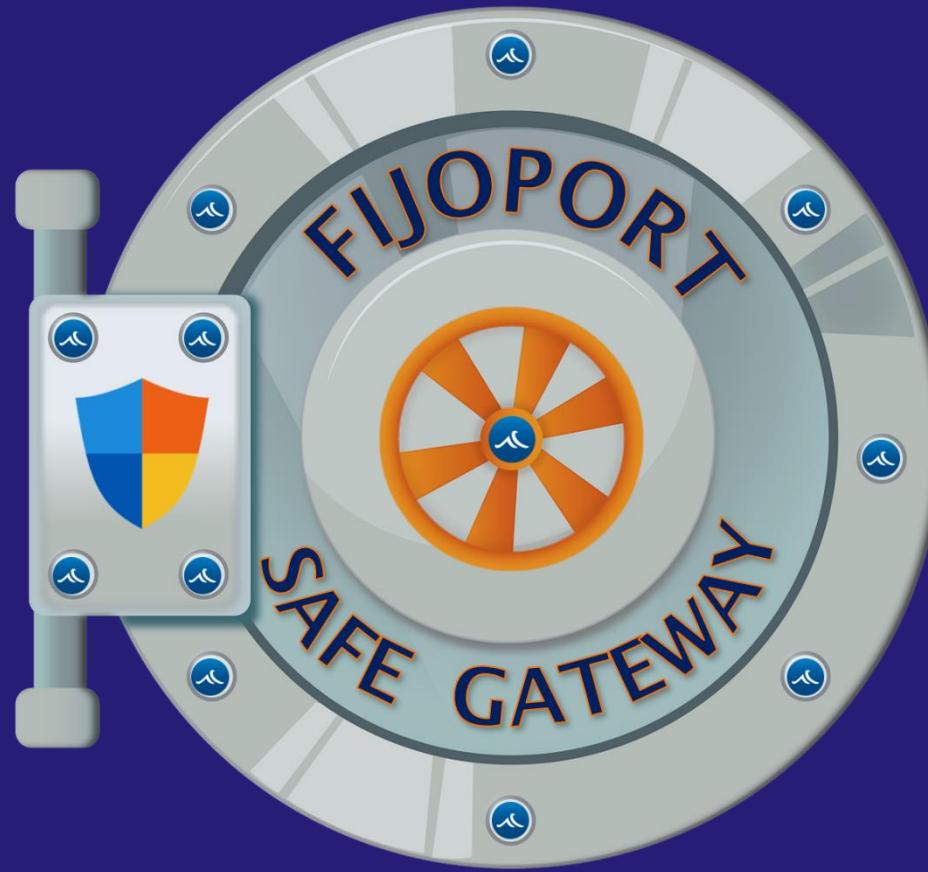
Brinda al usuario la posibilidad de conectarse de manera remota y cibersegura a sus **dispositivos IP y seriales** así como equipos **heredados o legados** como si estuvieran conectados directamente a la unidad en cualquier parte que se encuentren.

Industrias

- Telecomunicaciones – Operaciones Centralizadas
- Industria del sector de transporte
- Industria 4.0 – Producción Industrial
- Monitoreo en plantas de servicio – tratamiento de aguas
- Organizaciones que requieren conexión remota 24/7 – Seguridad
- Industria Energética – Subestaciones eléctricas – Aerogeneradores



¿Cómo Funciona Fijport?



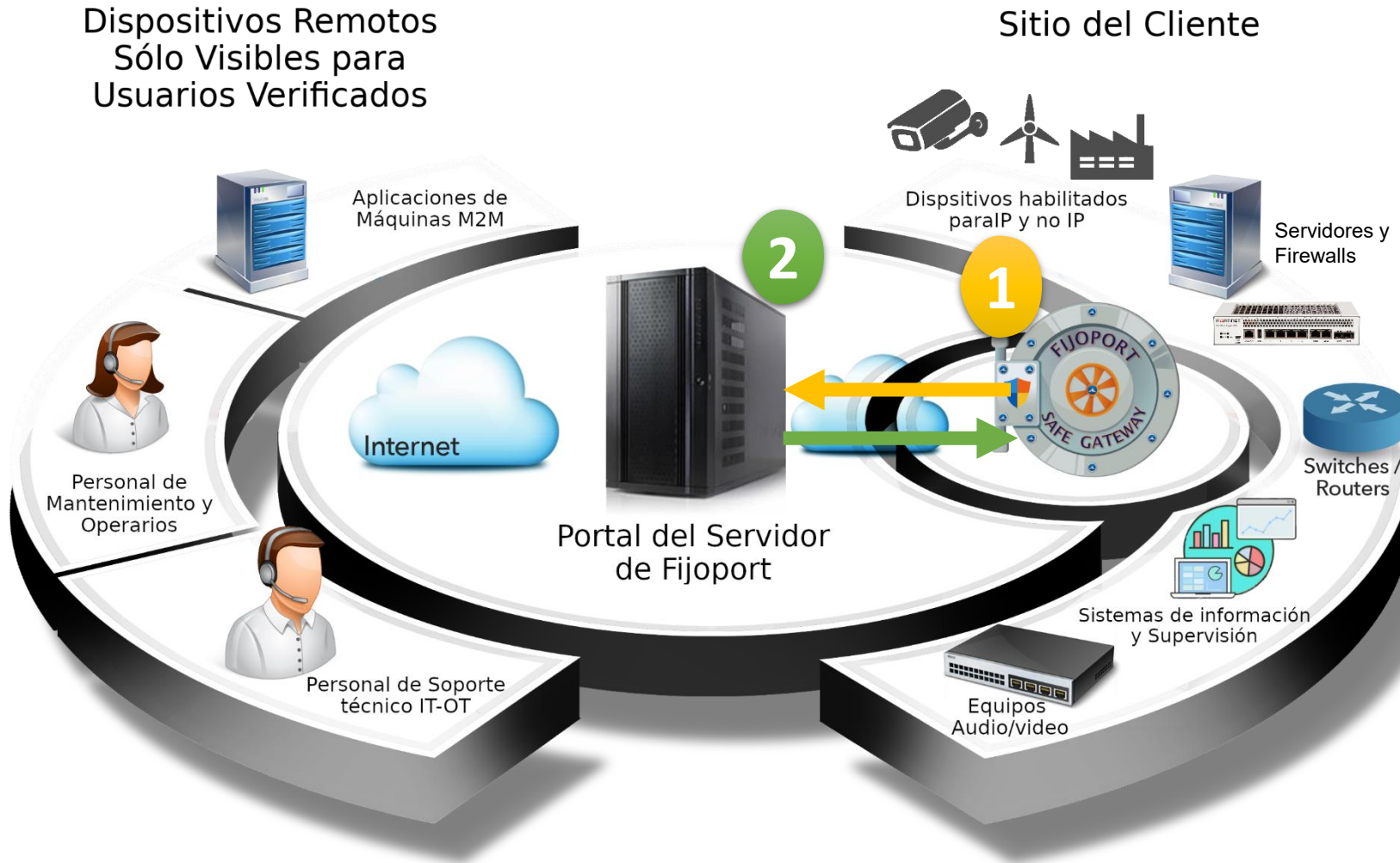
USA



MEXICO



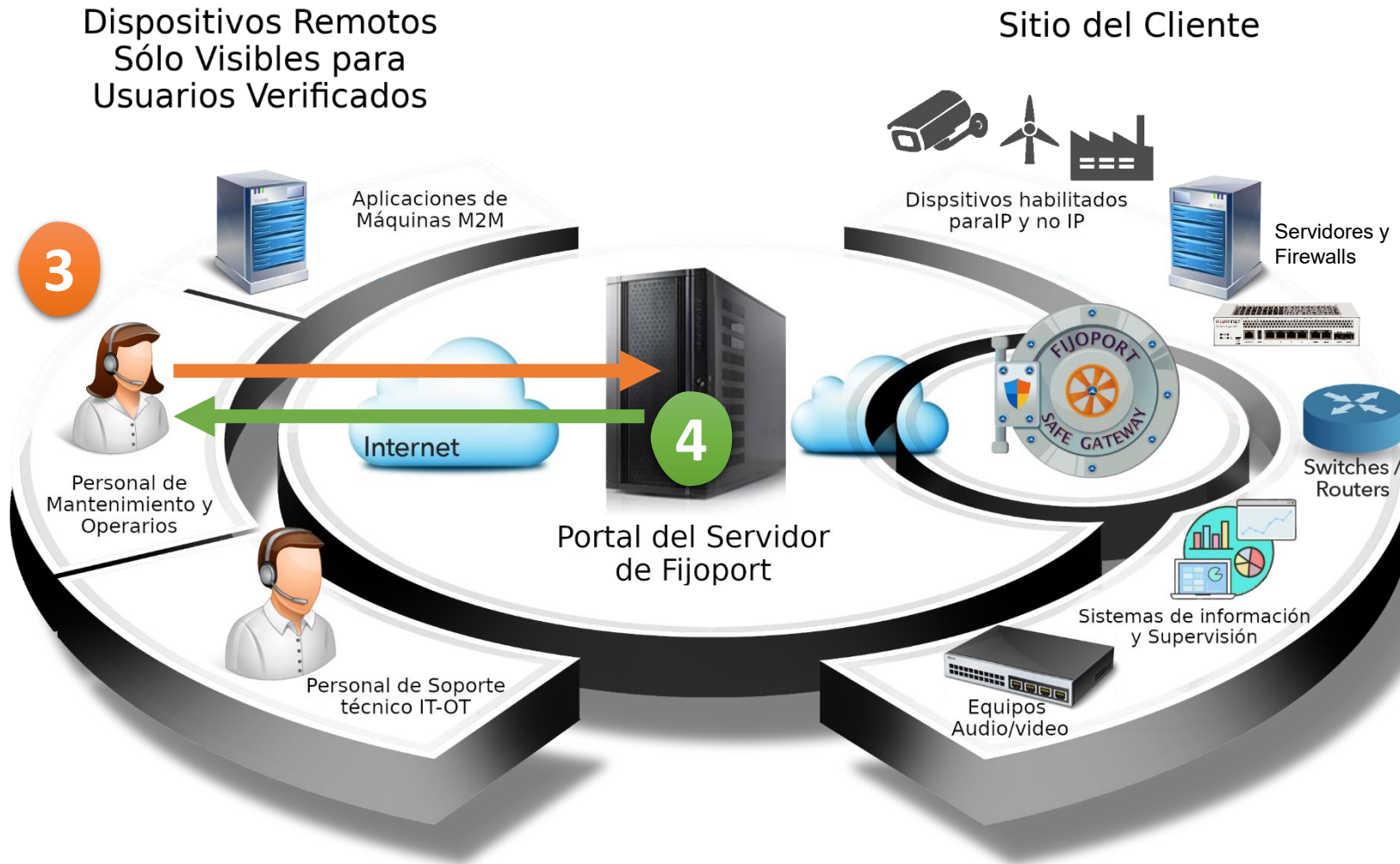
Identificación de Fijoport con el Servidor



1. Fijoport establece una conexión por red o fuera de banda al Servidor del portal

2. El portal autentifica el Fijoport (RSA llaves públicas/privadas)

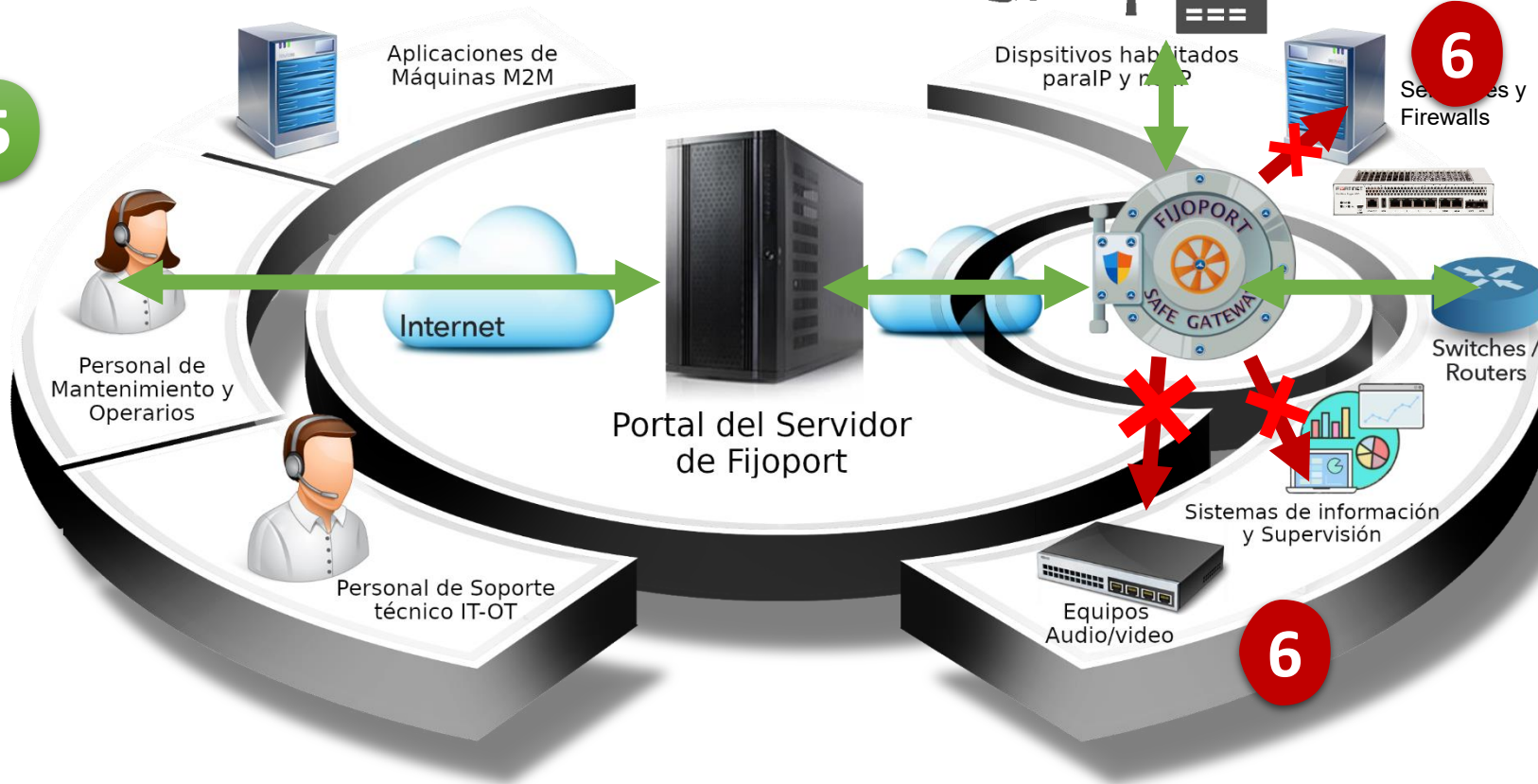
Autenticación del usuario con el Servidor



Túnel encriptado establecido

Dispositivos Remotos
Sólo Visibles para
Usuarios Verificados

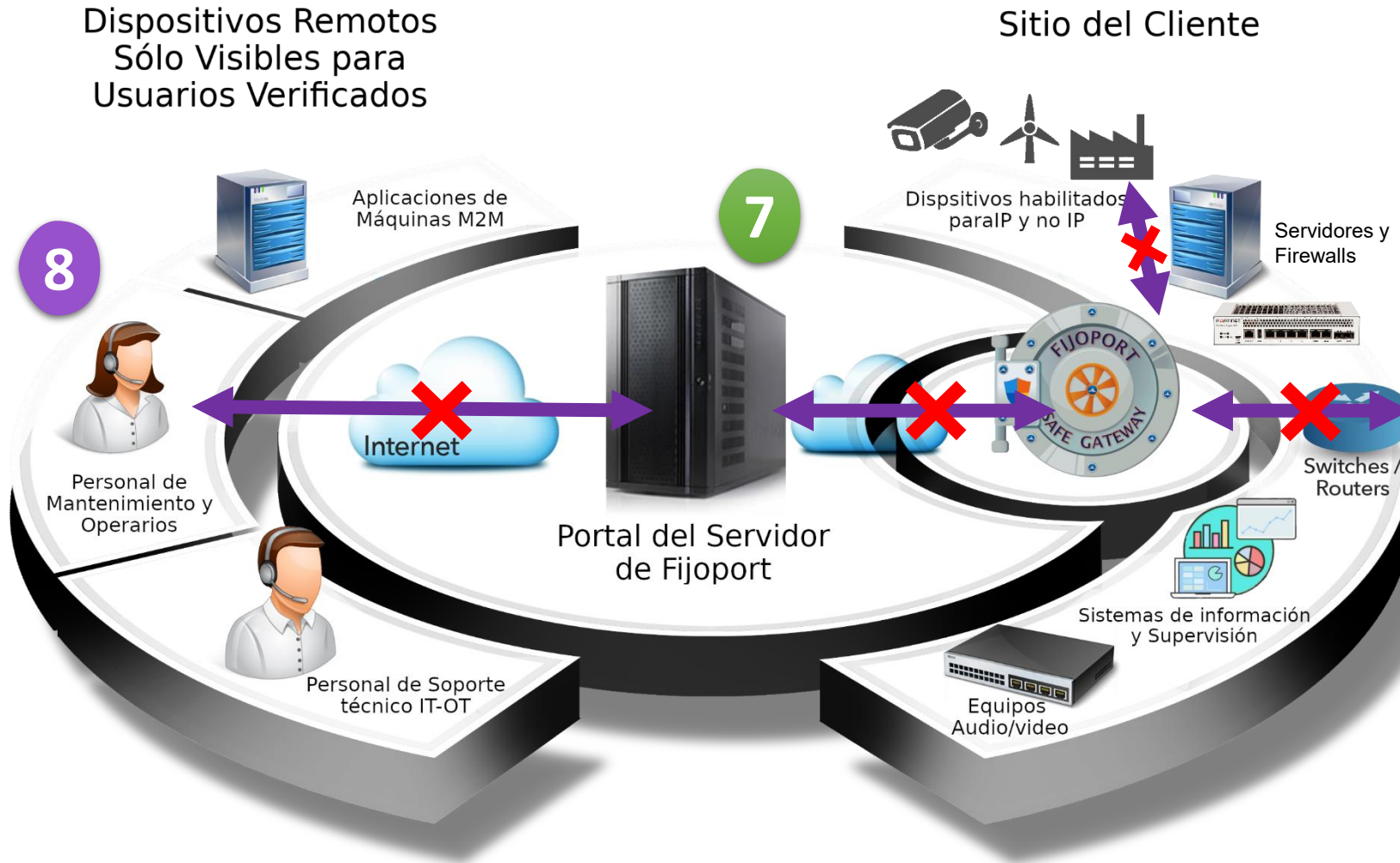
Sitio del Cliente



5. A petición del usuario, el portal establece un túnel encriptado a Fijoport (AES)

6. El usuario puede acceder solamente a dispositivos autorizados

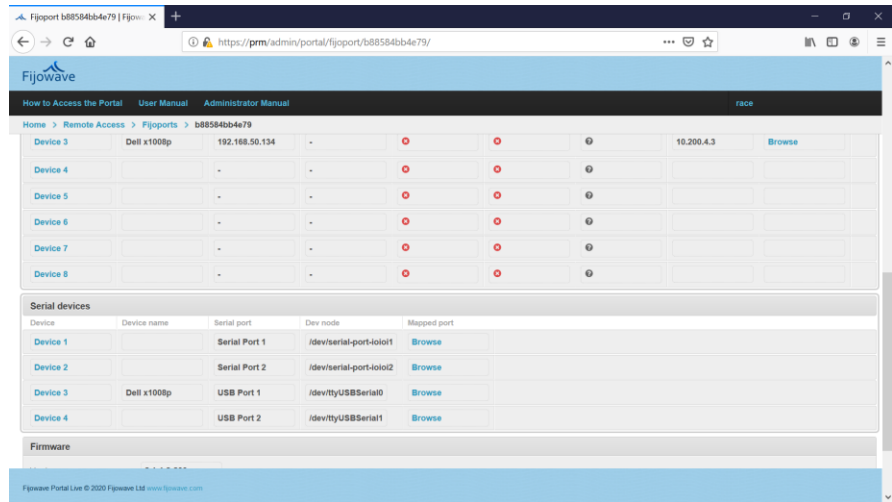
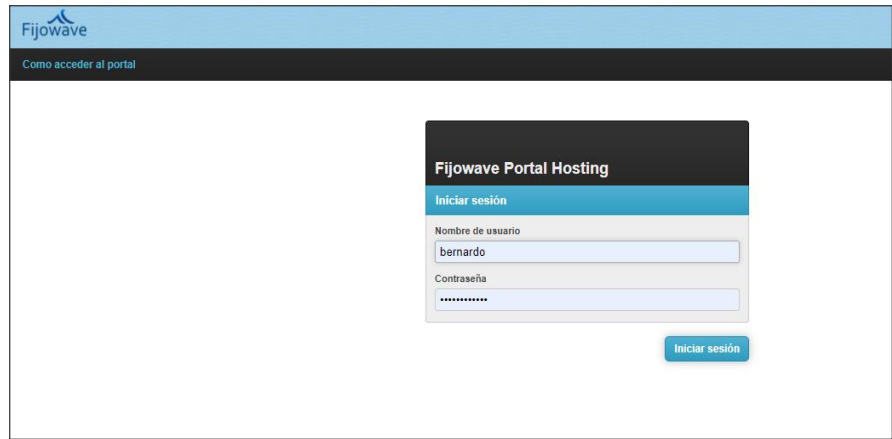
Sesión finalizada por el usuario



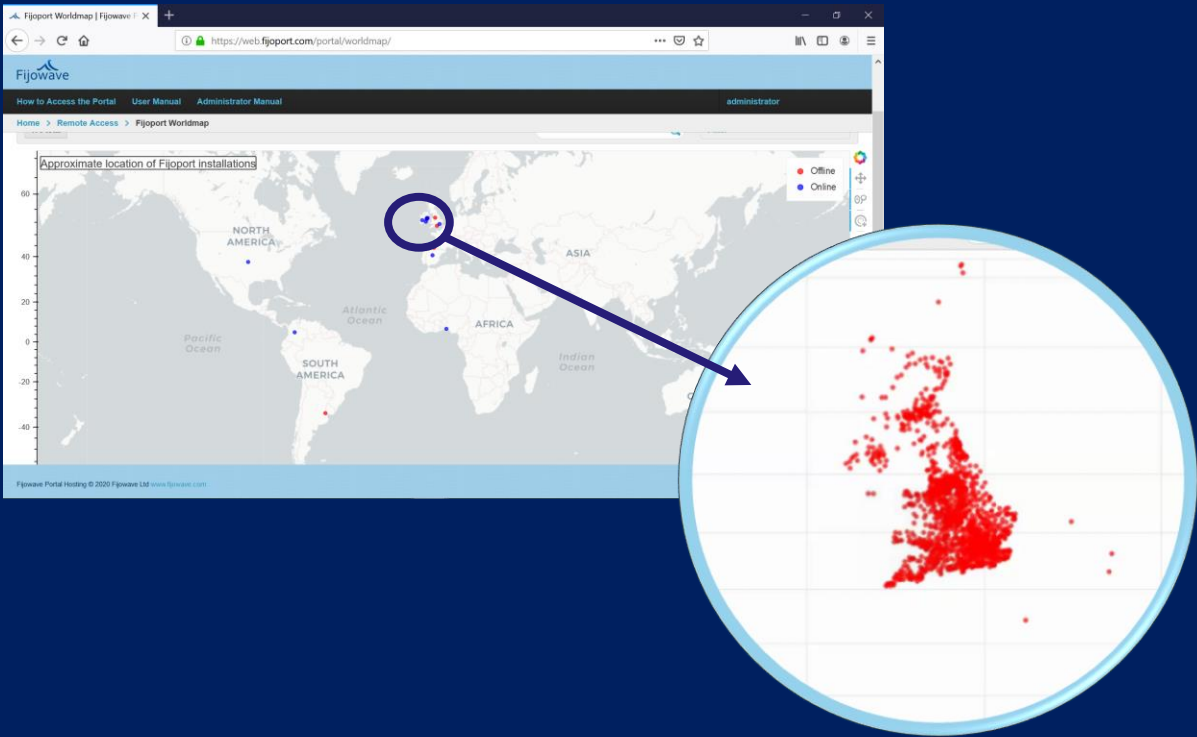
7. El acceso a los dispositivos o la administración fuera de banda se realiza **SOLAMENTE** a través del Portal

8. El tunel IP se Cierra cuando la session de acceso remoto finalice.

User friendly – Web interface portal



Fijoport geographic localization



Interactive map locating Fijoports

¿Cómo funciona Fijoport?

- 1 Fijoport establece una conexión por red o fuera de banda al Servidor del portal
- 2 El portal autentica el Fijoport (RSA llaves públicas/privadas)
- 3 El usuario se autentica con el portal (LDAP, Radius, TACACS+)
- 4 Control de Acceso – el administrador decide quién tiene acceso y a qué dispositivo
- 5 A petición del usuario, el portal establece un túnel encriptado a Fijoport (AES)
- 6 El usuario puede acceder solamente a dispositivos autorizados
- 7 El acceso a los dispositivos o la administración fuera de banda se realiza SOLAMENTE a través del Portal
- 8 El túnel IP se cierra cuando la sesión de acceso remoto finalice.



Fijoport



Fijoport 3001

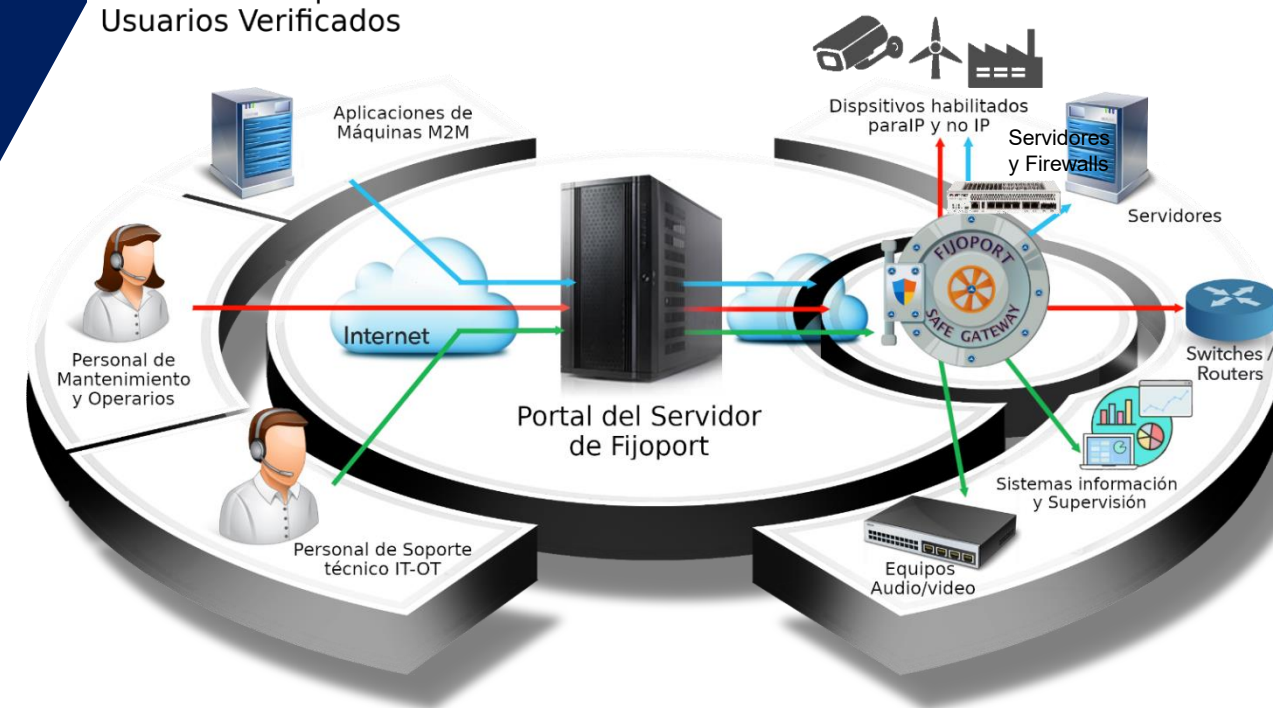


V Fijoport



Dispositivos Remotos
Sólo Visibles para
Usuarios Verificados

Sitio del Cliente





¿Porqué usar Fijoport?

- ❖ Simple de Instalar- Mínima configuración e impacto a la red (Aún sin habilidades específicas de TI).
- ❖ Interfaces IP, USB y puertos Seriales para el control a distancia de equipamiento heredado sin IP (LEGADOS).
- ❖ Ciber-huella no detectable en sitio (solo en fuera de banda)
- ❖ Resilencia – se puede utilizar la red LAN o móvil (para control fuera de banda) o las dos.
- ❖ Lista configurable de Accesos Remotos, Auditable. (por usuario, por dispositivo)
- ❖ Acceso seguro proactivo através de VPN (solo por medio del portal).
- ❖ Opción soft para integración con fabricantes de equipos
- ❖ Software personalizable
- ❖ VFijoport - integración con hardware existente

Soluciones Fijoport & hoja de ruta



01

Fijoport - Red LAN

02

Fijoport 3001 - LAN & 4G/LTE

03

Fijoport - Fijoport Virtual (Docker, Vmware, Linux)

04

Fijoport - Integración OEM

05

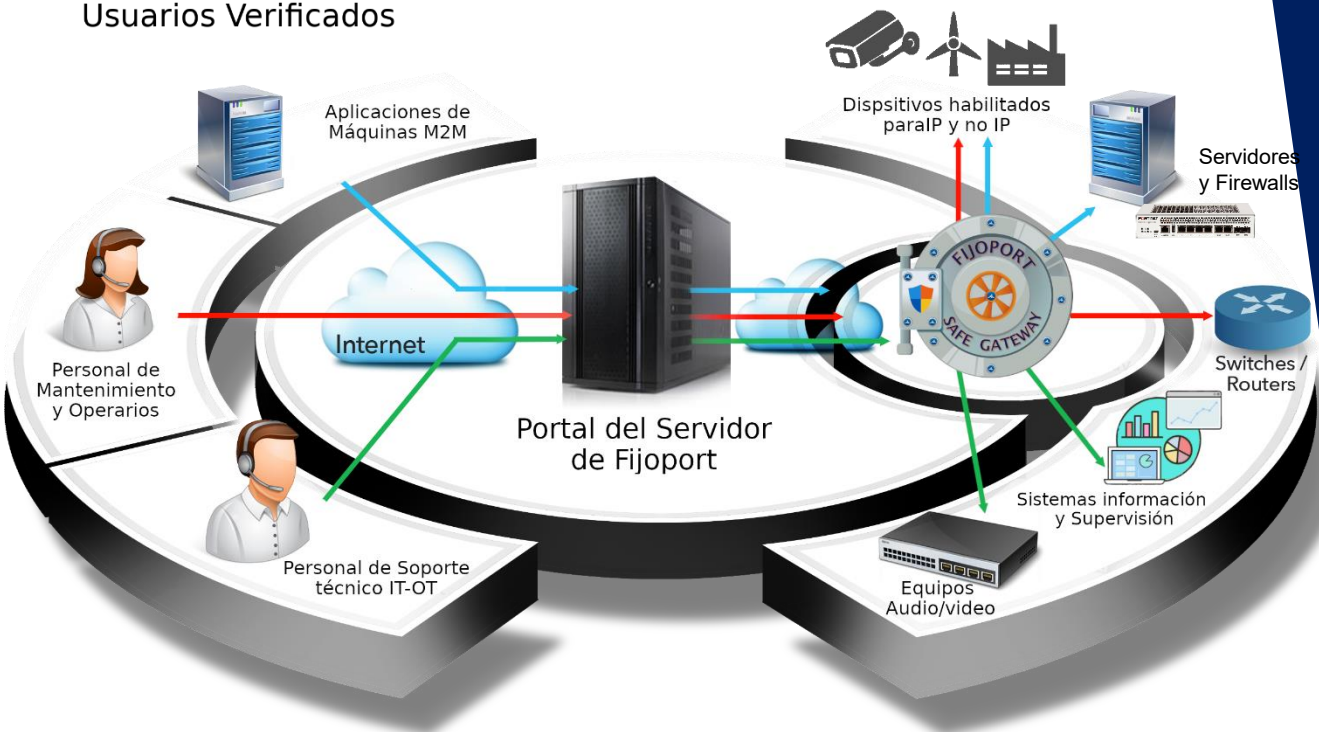
Aplicaciones de valor añadido – Chequeo de estado de red (NH)



¿Qué ofrece Fijoport?

Dispositivos Remotos
Sólo Visibles para
Usuarios Verificados

Sitio del Cliente



Acceso Remoto **Seguro** a
dispositivos IP (IoT)
y equipos no IP (serial)



Escalable de 1 a miles de sitios



Monitoreo (24/7) & Gestión
de dispositivos utilizando el Panel
de control y alertas - **Resilencia**



Instalación **Sencilla** – Plug&Play
Integración de SW en OEM

Casos de Uso

CASO DE USO– Mantenimiento y Soporte directo



Requerimientos del cliente

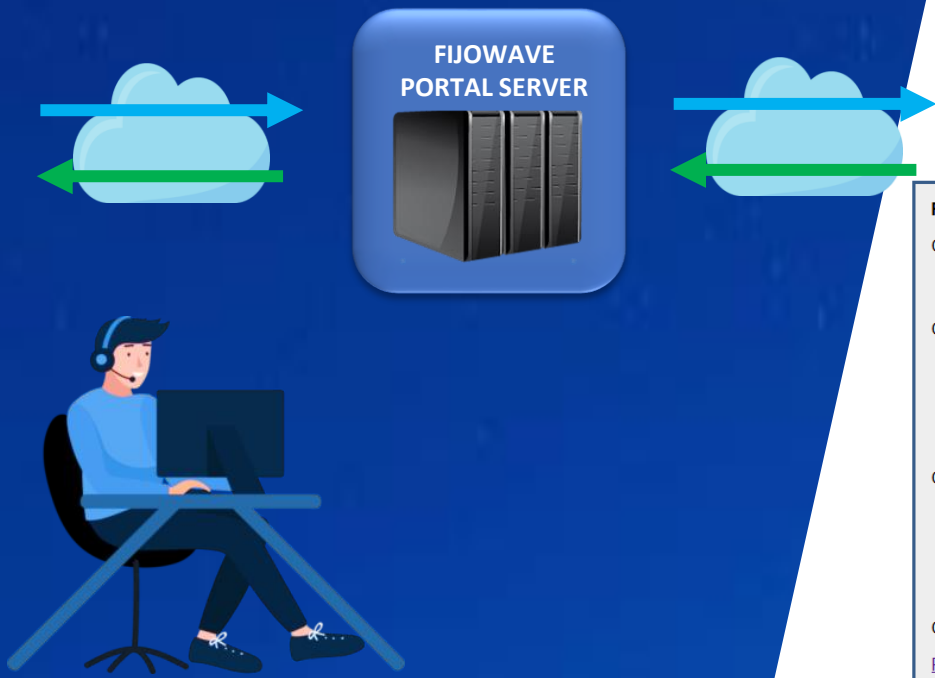
British Telecom (BT), una de las principales empresas de tele-comunicaciones de Europa, ha recurrido al uso de Fijoport para gestionar todas las PBX y Gateways SIP de sus clientes, permitiéndole el monitoreo y la gestión de todos los dispositivos las 24h, sin la necesidad de intervención del usuario en origen. BT quiere dotar a sus ingenieros con la capacidad de acceder remotamente a los equipos habilitados con IP de sus clientes, como si estuvieran conectados directamente a las unidades localmente, permitiéndoles cumplir con mayor eficiencia sus Acuerdos de Nivel de Servicio (SLA), aumentando la satisfacción de los clientes y la tasa de retención de clientes



Requerimientos clave resueltos	Beneficios adicionales
➤ Conectividad segura, bidireccional y encriptada entre usuario y dispositivo remoto. ➤ Soporte para el mantenimiento y administración de dispositivos las 24 horas, sin necesidad de la intervención in situ del usuario. ➤ Control sobre todos los usuarios con acceso. ➤ Cualquier acceso está limitado al personal autorizado, todas las sesiones se guardan automáticamente y son auditable. ➤ Visualización en el Panel de control de toda la red y todos los sitios con alerta de fallos.	➤ Mejora notable en los tiempos de respuesta y reducción del tiempo en desplazamientos. ➤ Sencillo proceso de instalación, plug & play. En pocos minutos está operativo y puede ser configurado de manera remota. ➤ Diseño compatible con futuras mejoras (API). Fijoport permite fácilmente implementar nuevas funcionalidades manuales o automatizadas. ➤ Sistema integrado de asignación de tareas, según cola de trabajo pendiente ➤ Incrementa la satisfacción y retención del cliente.



Arquitectura Zero Trust: Selector Zero Trust



Ingeniero / operador

- Solicitud de acceso
- Acceso desatendido 24/7



Portal Server Logout

Current status CONNECTED

Connection to portal Allowed Blocked Allowed

Change the Domain name or IP address and port or add a backup server.

Server	IP address	Port
1	f.fijoport.com	
2	176.9.67.54	

Configure Fijoport to connect to the portal through a proxy server.

Use Proxy	Disabled
Proxy Server URL	
Proxy port	

Click Save and then Reset the Fijoport to force immediate reconnection to portal server.

[Return to menu](#) Save Cancel

Powered by Fijowave
www.fijowave.com

- Opciones a seleccionar:
- Permiso de acceso
 - Monitoreo
 - Ambos

Bloquear



Permitir



Remote Access Control Logout

Enter the names and IP addresses of the devices that may be accessed via the portal.

Remote monitoring, access, and available ports may be configured for each device

* = allow all, blank = disallow all, comma separated list of up to 10 allowed ports e.g. 80,443

ID	Description	IP address	Device Type	Permissions	Ports
1	IPO	192.168.54.220		☒ monitoring ☐ access	udp *
2	Fred	192.168.50.200		☒ monitoring ☒ access	udp *
3	Dell x100bp	192.168.50.100		☒ monitoring ☒ access	udp *
4	DECT	192.168.50.217		☒ monitoring ☒ access	udp *
5				☒ monitoring ☒ access	udp *
6				☒ monitoring ☒ access	udp *
7				☒ monitoring ☒ access	udp *
8				☒ monitoring ☒ access	udp *

Click Save and this data will be updated on the portal server after the next RAS session.

[Return to menu](#) Save Cancel

CASO DE USO –Gestión de activos en Subestaciones Eléctricas



Requerimiento del cliente

Uno de los clientes de Fijowave es una destacada empresa energética irlandesa. Desean proporcionar a sus ingenieros y subcontratistas la capacidad de acceder de forma remota a equipos habilitados para IP y a equipos heredados en estos sitios como si estuvieran conectados directamente a las unidades en el lugar. La empresa energética requiere una solución que proporcione acceso remoto tanto dentro de banda como fuera de banda, y que ofrezca control total sobre el acceso de usuarios, acceso a dispositivos y capacidades de registro de auditorías. Además, la empresa desea analizar las variaciones en el rendimiento en toda su red de sitios.



Requerimientos clave resueltos	Beneficios adicionales
➤ Una conexión bidireccional, segura y encriptada entre usuario y dispositivo remoto. ➤ Control sobre todos los usuarios con acceso. ➤ Soporte para el mantenimiento y la administración las 24h de todos los dispositivos, sin necesidad de la intervención presencial del usuario. ➤ Acceso mediante licencias y capas de seguridad que solo permiten el tráfico legítimo dentro de la red privada. ➤ No se requiere la instalación de ningún software en los equipos remotos a los que se accede. ➤ Los usuarios solo podrán ver los dispositivos a los que tengan acceso. ➤ Cualquier acceso está limitado al personal autorizado, todas las sesiones se guardan automáticamente y son auditable. ➤ Visualización en el panel de control de toda la red y todos los sitios con alerta de fallos. ➤ Sencillo proceso de instalación, Plug & play. En pocos minutos está operativo y puede ser configurado de manera remota.	➤ Incremento de la seguridad de la red, eliminando peticiones de acceso no deseadas. Control total sobre los permisos de acceso. ➤ La compañía energética puede reaccionar más rápidamente a las solicitudes de soporte técnico, tanto internas como externas. ➤ Los tiempos de respuesta mejoran notablemente, al mismo tiempo que se reduce el tiempo empleado en traslados. ➤ Reducción del coste de mantenimiento de las instalaciones, al reducirse el número de las visitas necesarias. ➤ Mejora la eficiencia operacional y organizativa. ➤ Capacidad de ampliar la solución Fijoport inicial a demanda, sin necesidad de rediseñar la red. Una única solución para todos los sitios. ➤ La solución Fijoport ayuda al compromiso de la empresa con el medio ambiente, al reducir la huella de carbono generada, con la disminución del número de traslados necesarios. ➤ Diseño compatible con futuras mejoras (API). Fijoport permite fácilmente implementar nuevas funcionalidades manuales o automatizadas.



Apéndice

IoT y Gestión de Activos / Monitoreo

Porqué y Beneficios

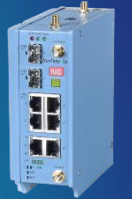


Partners

- Incremento en las ganancias-
 - Ofrecimiento de paquetes de mantenimiento y soporte
- SLA (Service Level Agreements)
 - Reducción en las penalidades
- Uso Vehicular
 - Reducción de visitas a sitio, incremento en la eficiencia sabiendo a qué especialista mandar y que tipo de repuesto
- Optimización de profesionales
 - Permite trabajar de manera simultanea y eficiente en diferentes niveles de problemas.
- Capacidad de Mantenimiento Predictivo
 - El acceso remoto y mantenimiento 24/7 remote permite analisis preventive con IA
- Satisfacción del cliente
 - Informa a nuestro clients de que tiene un problema y muy posiblemente arreglarlo antes de que se entere del mismo
- Reducción de la huella de carbono
- Actualizaciones de Cyber seguridad

Usuarios finales

- Seguridad en los accesos a dispositivos y registros auditables
 - Autorización a dispositivos exclusivo a usuarios
 - Protección de dispositivos que no cuentan con opciones de usuario/contraseña
- SLA (Service Level Agreements)
 - Permite responder de manera mas eficiente
- Reducción en los cortes de inactividad
 - Ahorro en costos
- Optimización de recursos (especialistas)
 - Uso eficiente del expertise interno
 - Facilita el trabajo remoto
- Capacidad de Mantenimiento preventivo
 - Reducción en cortes de inactividad. Agendar mantenimiento basado en el performance.
 - Desarrollo de aplicaciones propias
- Satisfaccion del Cliente
 - Identificación temprana de problemas y una respuesta rápida y eficiente, Flexibilidad y reduccion de cortes de inactividad
- Security updates



Fijoport bondades y funcionalidades

Acceso desatendido

Sin necesidad de una computadora o alguien que haga la conexión



Conexión segura y confiable a través de túneles de seguridad

Característica principal de Cyberseguridad



Estado de red

Fijoport monitorea el estado de red LAN/WAN y así prevenir fallas



Solución de costo efectivo

Maximiza ganancias reduciendo costos de operaciones y transporte



Fijoport

Solución
Todo en
UNO

Fijowave

Instalación plug&play

Conexión DHCP via LAN/WAN port. Sin necesidad de abrir puertos en el Firewall



Personalizado para Avaya

Aprobado y certificado por Avaya



Portal Server



Arquitectura Zero Trust

*Control de Acceso – Acceso a usuarios individuales
Ciber seguridad*



Fijoport bondades y funcionalidades (continuación)

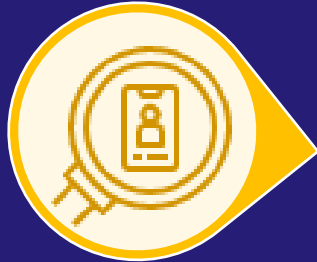
Centralización de Operaciones

Alertas y fallas son direccionados al tablero de control central, SMS y correo electrónico



Inventario monitoreado

(Licencias, revisiones de hardware y software, etc)



Configuración remota y automática de actualizaciones de seguridad

Parches de ciberseguridad



Continuidad de negocio

Redundancia IoT – Accesos fuera de banda 4G LTE



Fijoport



Fijowave



Seguridad y Confiabilidad

Una sola plataforma para proveedores multiples

Switches, firewalls, máquinas virtuales, teléfonos IP, DECT IP, media gateways, controladores de sesión (SBC)



Control y monitorización avanzado 24-7

Control de fallos por alarmas



Escalabilidad de 1 100,000 dispositivos



Ventajas Fijoport

Mucho más que una VPN

- ✓ **Simple de instalar y configurar**
 - Plug and play
 - No requiere de especialistas IT
 - Listo para envío - configuración remota
- ✓ **Misma solución – Pequeños y Grandes sitios**
- ✓ **Gestión de activos centralizada**
 - La inteligencia se encuentra en el portal server
 - Gestion y monitoreo centralizado
 - Configuración de separación de entidades sencilla
- ✓ **Simpleza en la escalabilidad (de 1 a 1000's)**
 - Flexibilidad y sin requerimiento de reglas para escalar
 - Sin requerimientos de certificaciones – mismo diseño de red
- ✓ **Permite Acceso Seguro a Sistemas Operativos Obsoletos**



VPN Acceso remoto

- ⇒ **Instalación compleja**
 - Mucho tiempo en cada instalación
 - Profesionales IT especializados
 - Visita al sitio necesario
- ⇒ **Cada VPN instalada – configuración distinta**
- ⇒ **Se necesita gestión central y por sitio**
 - Políticas de seguridad y por sitio
 - IP Pública por sitio
 - Reglas de NAT y Firewall necesarias por sitio
- ⇒ **Reglas complejas par escalabilidad**
 - Flexibilidad limitada dependiendo del diseño de red
 - Aprobaciones necesarias, certificaciones para escalar
- ⇒ **Complejidad en garantizar acceso seguro a equipos con Sistemas operative obsoleto**

Ventajas Fijoport

Mucho más que una VPN

- ✓ Acceso seguro a equipos legados por medio de puertos serie
- ✓ Control de finalización de sesión de túneles VPN
 - Dirección del Portal Server preconfigurado en Fijoport
 - No hacen falta cambios del NAT o Firewall de entrada
 - Control de Registro de conexiones establecidas
 - Cierre automático del túnel VPN por inactividad
 - Configuraciones específicas requieren usuario (solicitud del parte del usuario)
 - Ancho de banda controlada
- ✓ Segmentación de Usuarios por grupos
 - Ej. Grupos de IT, OT, Seguridad, PBX, Voz, Legados
 - Gestionado de manera centralizada por el portal administrador, fácil uso, fácil de configurar, agregar/remover usuarios, accesos etc)
- ✓ Resiliencia de red
 - Acceso fuera de banda / por fallo en la red corporativa



VPN Acceso remoto

- ⇒ Acceso seguro a equipos legados requieren de equipamiento adicional
- ⇒ Control de finalización de sesión de túneles VPN
 - La IP pública tiene que ser conocida por los dos extremos
 - Reglas de NAT y Firewall a permitir tráfico entrante
- ⇒ Segmentación de Usuarios por grupos
 - VPN del tipo acceso remoto no cuenta con esta funcionalidad
- ⇒ Dependiente de la red corporativa

Gracias

www.fijowave.com

sales@fijowave.com

© Fijowave 2025