



Accesos Remotos en entornos Industriales

EDORTA ECHAVE GARCÍA

AGENDA

- › **Horario:**
 - › 09:30 a 13:30
 - › 14:30 a 18:30
- › **Día 1:**
 - › Teoría.
 - › Presentación de Laboratorio.
 - › Ejercicios.
- › **Día 2:**
 - › Ejercicios.



Presentación de Equipo

- **Edorta Echave García**
- Técnico en Sistemas Informáticos y Telecomunicaciones
- **Responsable de Ciberseguridad Industrial**, Grupo ARANIA
- **Coordinador del Centro de Ciberseguridad Industrial**, País Vasco
- Desarrollo profesional en entornos IT como OT en el sector de Automoción, Energía, Transporte, Aeronáutica y Manufactura.
- Más de **15 años** de experiencia

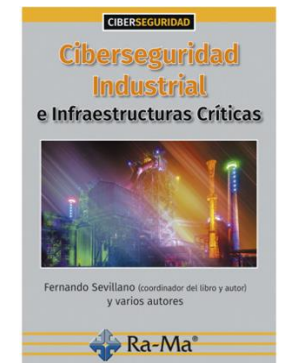


- **Certificaciones y formación** específica sobre tecnología de distintos fabricantes y productos
- **ISA/IEC 62443 Cybersecurity Expert**
- **Miembro ISA**
- Coautor: “**Ciberseguridad Industrial e Infraestructuras Críticas**”
- **Ponente** en eventos de referencia, Advanced Factories, C1b3rwall, Jornadas STIC CCN-CERT, ISA OT Cybersecurity Summit (Bruselas)
- **Profesor Universitario y Colaborador en centros F.P.**
- Autor: <https://enredandoconredes.com>

FORTINET®

SIEMENS

kaspersky





INTRODUCCIÓN

DEFINICIÓN

Acceso Remoto: Capacidad de alcanzar equipos que se encuentren distribuidos geográficamente lo cual nos permite tener acceso a equipos, instalaciones, fábricas, maquinaria o infraestructuras sin necesidad de desplazamiento.

BENEFICIOS

- › Realización de intervenciones sin acudir in-situ.
- › Ahorro en costes.
- › Centralización de recursos.
- › Menor tiempo de respuesta ante fallos o incidencias.
- › Nuevos servicios:
 - › Mantenimiento predictivo.
 - › Tele asistencia deslocalizada.
 - › Captura de datos de proceso.
 - › Gestión de dispositivos.

INCONVENIENTES

- › Aumento del grado de exposición de equipos.
- › Implementar nuevas medidas de seguridad.
- › Costes añadidos:
 - › Dispositivos.
 - › Licencias.
 - › 2FA.
 - › Recursos hardware en sistemas.
 - › Actualizaciones de firmware y software.
- › Modificación de arquitecturas de red.

REQUISITOS

- › Presupuesto.
- › Aumento de medidas en la gestión:
 - › Proveedores.
 - › Usuarios.
 - › Accesos; IP destino, puerto.
 - › Procedimientos de Alta, renovación y baja de accesos.
- › Trabajo conjunto entre Administradores de Sistemas/Red y persona de planta, Producción, Mantenimiento, Ingeniería, I+D+I.

REQUISITOS

- › Homologación de tecnologías.
 - › IPSec, SSL/TLS.
- › Homologación de productos.
 - › Hardware, Software.



TECNOLOGÍAS

TECNOLOGÍA SOFTWARE

- › Mediante un software instalado en un equipo se puede visualizar la pantalla remota en un equipo local.
- › Adicionalmente, transferir ficheros, grabar sesión, 2FA, paneles de control, gestión de activos, instalación de parches, etc.
- › Alta compatibilidad con dispositivos y S.O.
- › Posibilidad de recibir asistencia y un operario pueda ver la pantalla de manera simultánea.
- › Posibilidad de identificarlo en NGFW.
- › Ejemplos, Teamviewer, Anydesk, VNC, Navegadores, RDP, etc.

TECNOLOGÍA VPN, IPSEC

- › Modo Transporte
 - › Solo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP.
- › Modo Túnel
 - › Todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento.

TECNOLOGÍA VPN, IPSEC

- › Protocolo AH (Authentication Headers), proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.
- › Protocolo ESP (Encapsulating Security Payload), proporciona confidencialidad y la opción, altamente recomendable, de autenticación y protección de integridad.
- › Protocolo IKE (Internet Key Exchange), emplea un intercambio secreto de claves de tipo DH para establecer el secreto compartido de la sesión, usándose Criptografía de Clave Pública o precompartida.

TECNOLOGÍA VPN, IPSEC

- › Fase 1
 - › En las negociaciones de Fase 1, los dos puntos intercambian credenciales. Los dispositivos se identifican y negocian para encontrar un conjunto común de configuraciones de Fase 1 que usar. Cuando se concluyen las negociaciones de Fase 1, los dos puntos tienen una Asociación de Seguridad (SA) de Fase 1. Esa SA es válida sólo por un período de tiempo determinado.

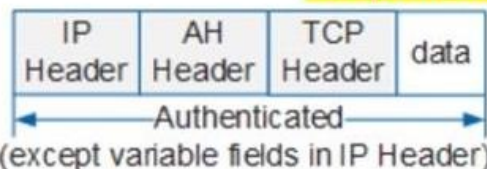
TECNOLOGÍA VPN, IPSEC

- › Fase 2
 - › El propósito de las negociaciones de Fase 2 es establecer la SA de la Fase 2 (a veces llamada IPSec SA). La SA de IPSec es un conjunto de especificaciones de tráfico que informan al dispositivo qué tráfico enviar por la VPN y cómo cifrarlo y autenticarlo. En las negociaciones de Fase 2, los dos puntos concuerdan en un conjunto de parámetros de comunicación.

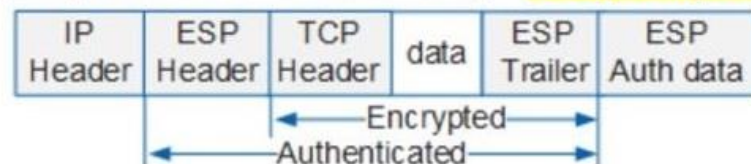
TECNOLOGÍA VPN, IPSEC

IPSEC Transport Mode

AH (Authentication Header)

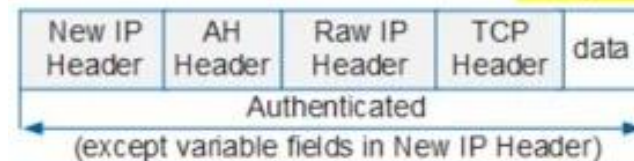


ESP (Encapsulation Security Payload)

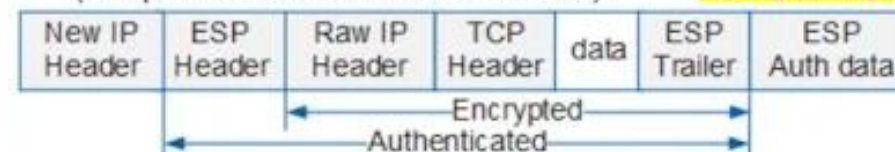


IPSEC Tunnel Mode

AH (Authentication Header)



ESP (Encapsulation Security Payload)



TECNOLOGÍA VPN, SSL/TLS

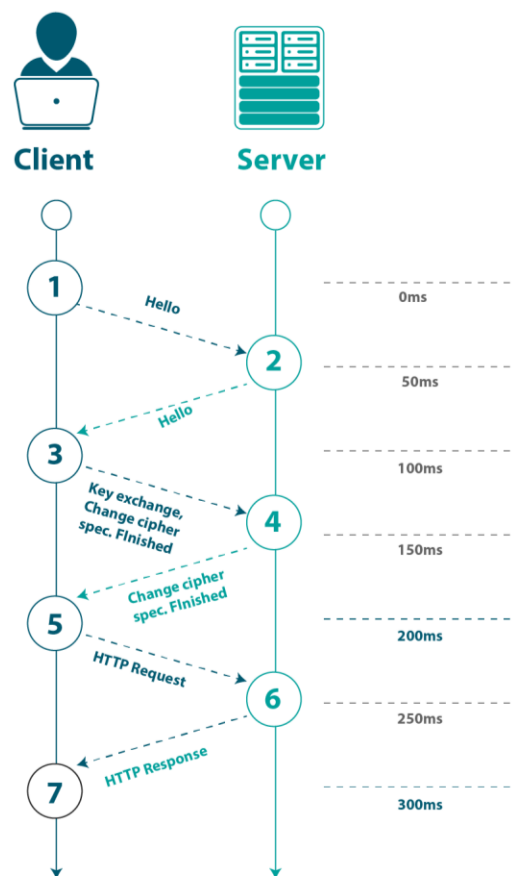
- › Secure Socket Layer / Transport Layer Security.
- › TLS evolución de SSL
- › SSL desactualizado
- › Última versión TLS 1.3
- › Fases:
 - › Negociar entre las partes el algoritmo que se usará en la comunicación.
 - › Intercambio de claves públicas y autenticación basada en certificados.
 - › Cifrado del tráfico basado en cifrado simétrico.

TECNOLOGÍA VPN, SSL/TLS

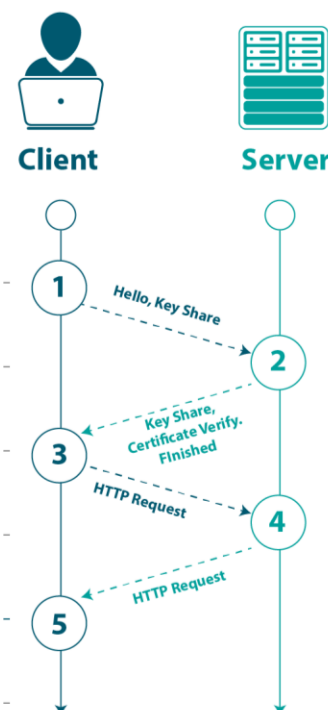
- › Permite la confidencialidad del dato/mensaje, códigos de autenticación de mensajes para integridad y como un producto lateral, autenticación del mensaje.
- › Para criptografía de clave pública: RSA, Diffie-Hellman, DSA o Fortezza
- › Para cifrado simétrico: RC2, RC4, IDEA, DES, Triple DES y AES.
- › Con funciones Hash: MD5 o de la Familia SHA.

TECNOLOGÍA VPN, SSL/TLS

TLS 1.2
(Full Handshake)



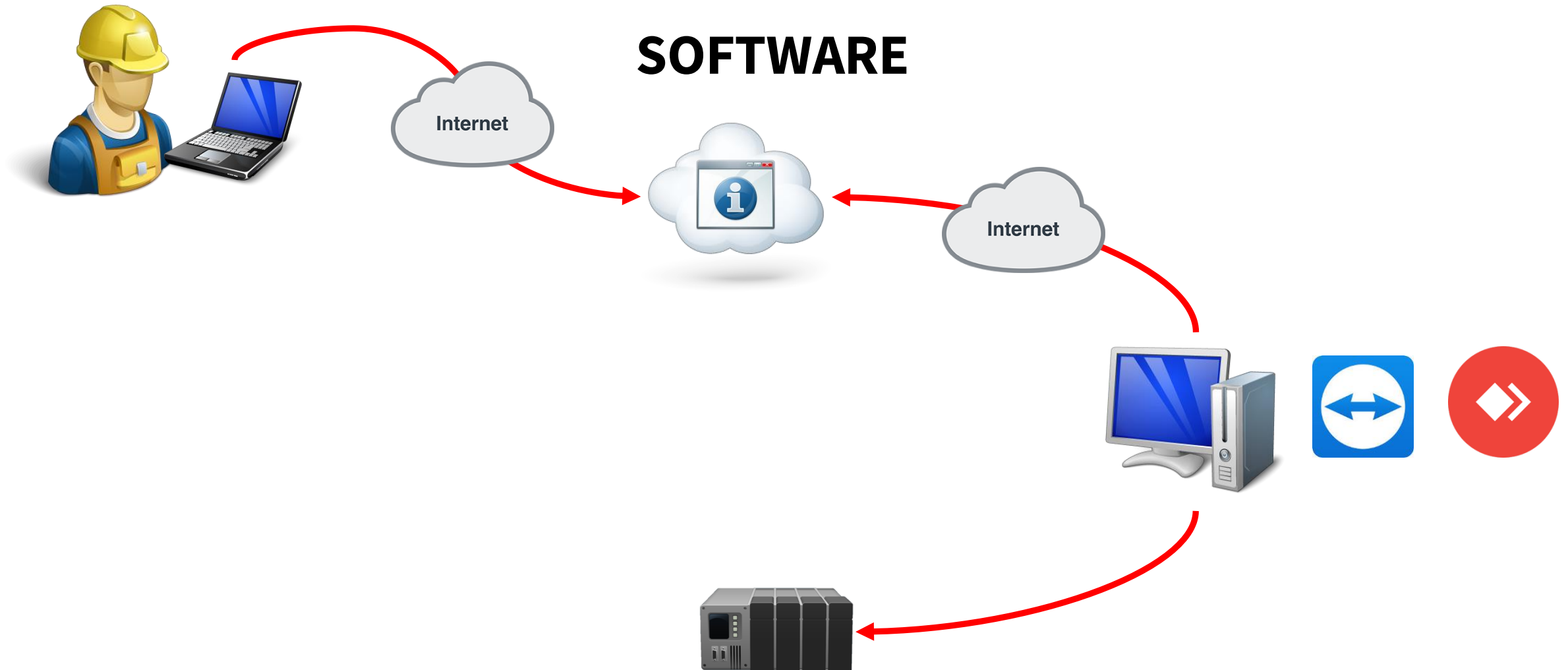
TLS 1.3
(Full Handshake)



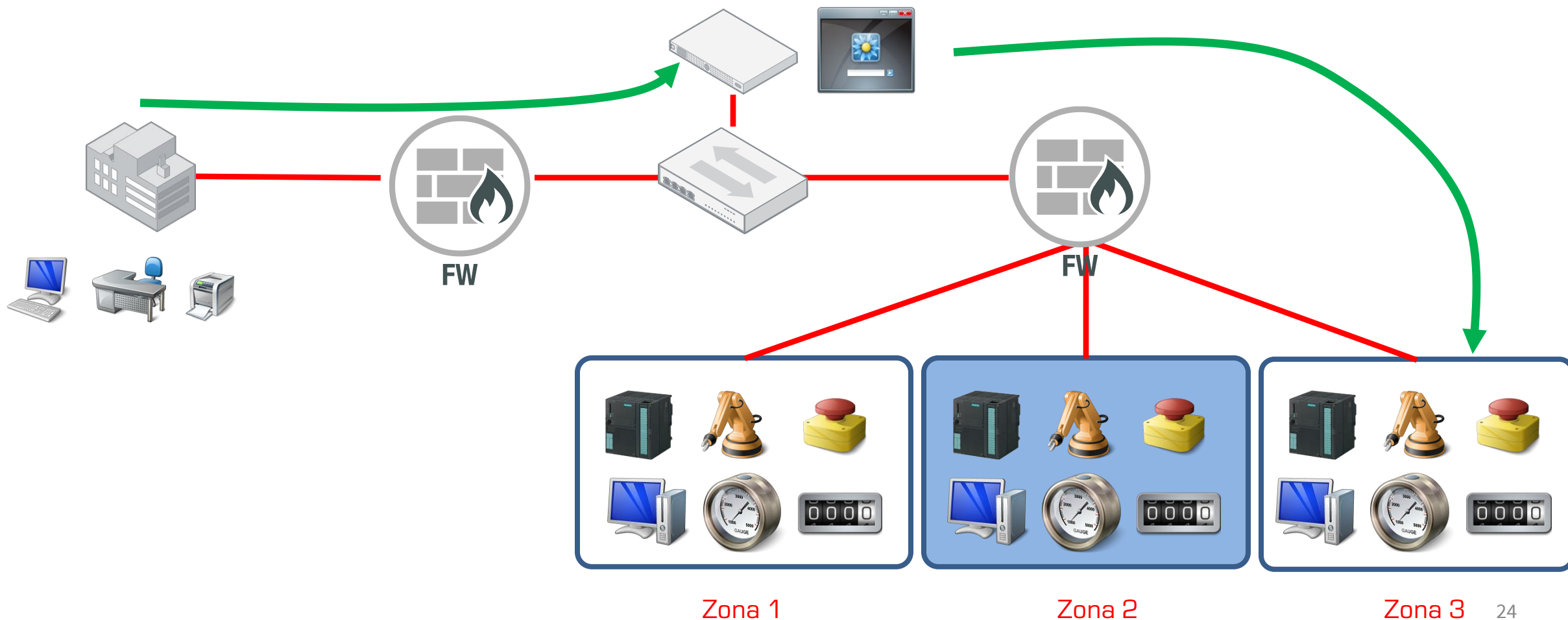


ARQUITECTURAS

SOFTWARE



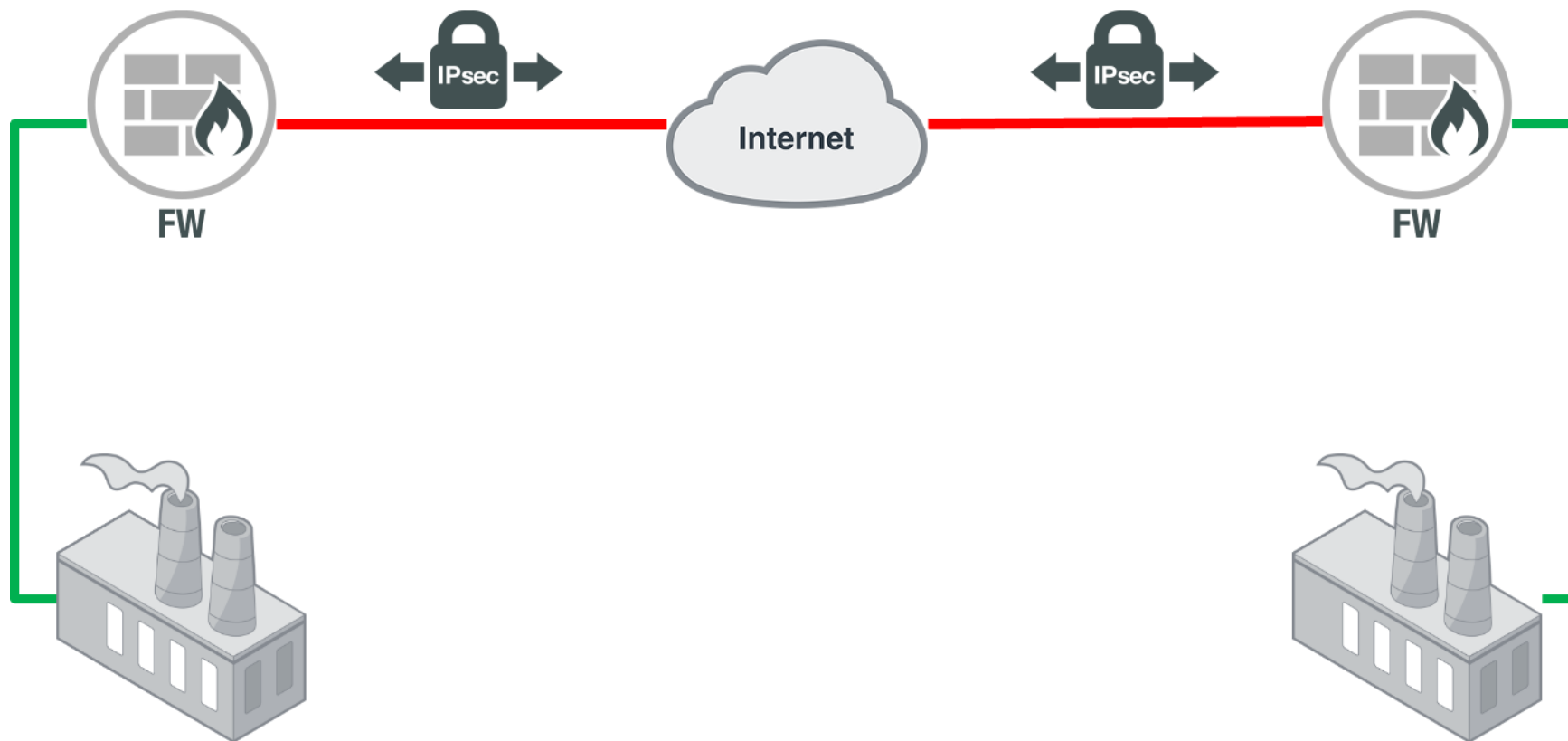
SOFTWARE



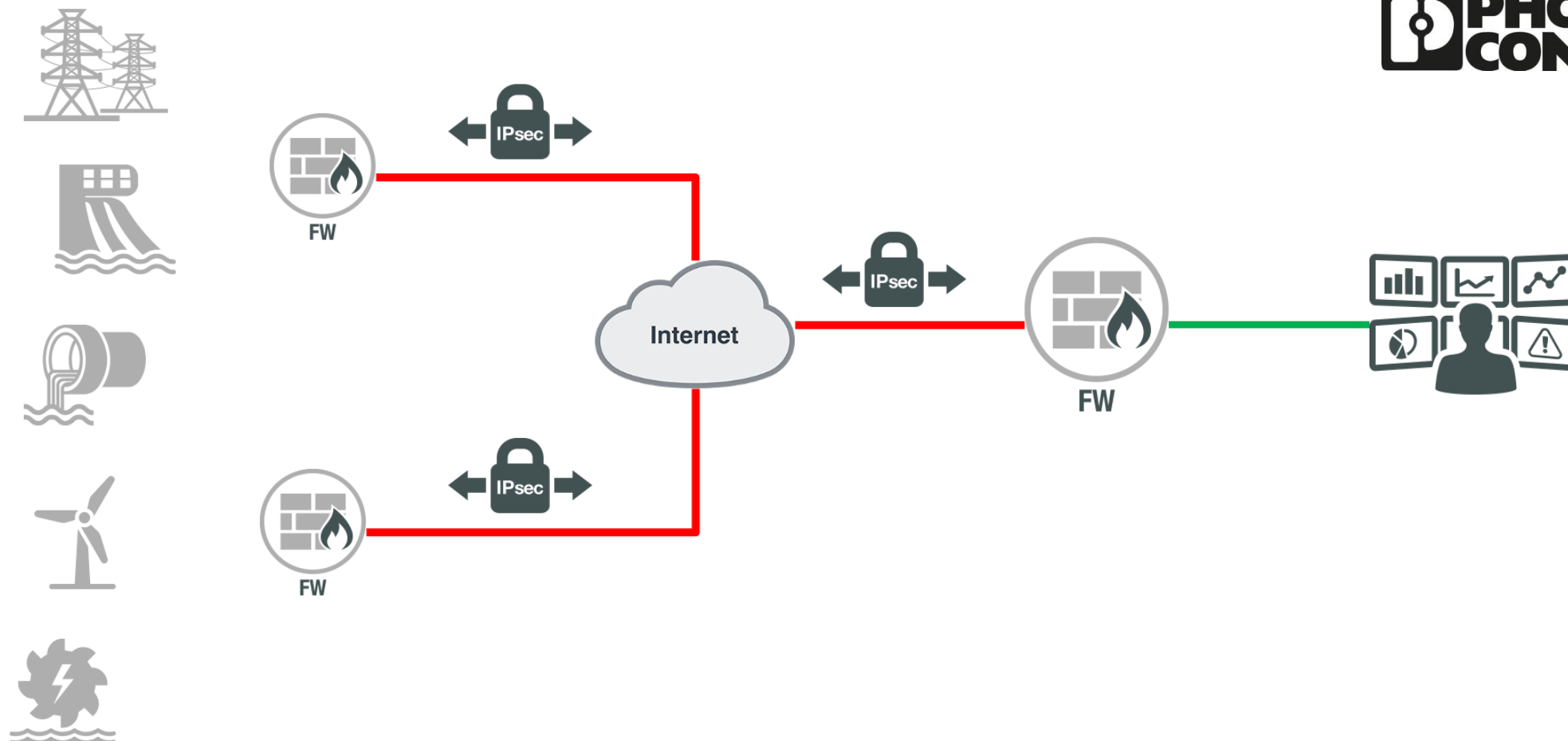
PROS Y CONTRAS

- › Pros
 - › Sencillez de despliegue.
 - › Acceso a equipos en el mismo segmento de red, L2.
 - › Compatibilidad con diferentes S.O.
 - › Simultaneidad visual; Operario planta & Teleservicio.
- › Contras
 - › Falta de logs centralizada.
 - › Acceso a Internet.

SITIO A SITIO



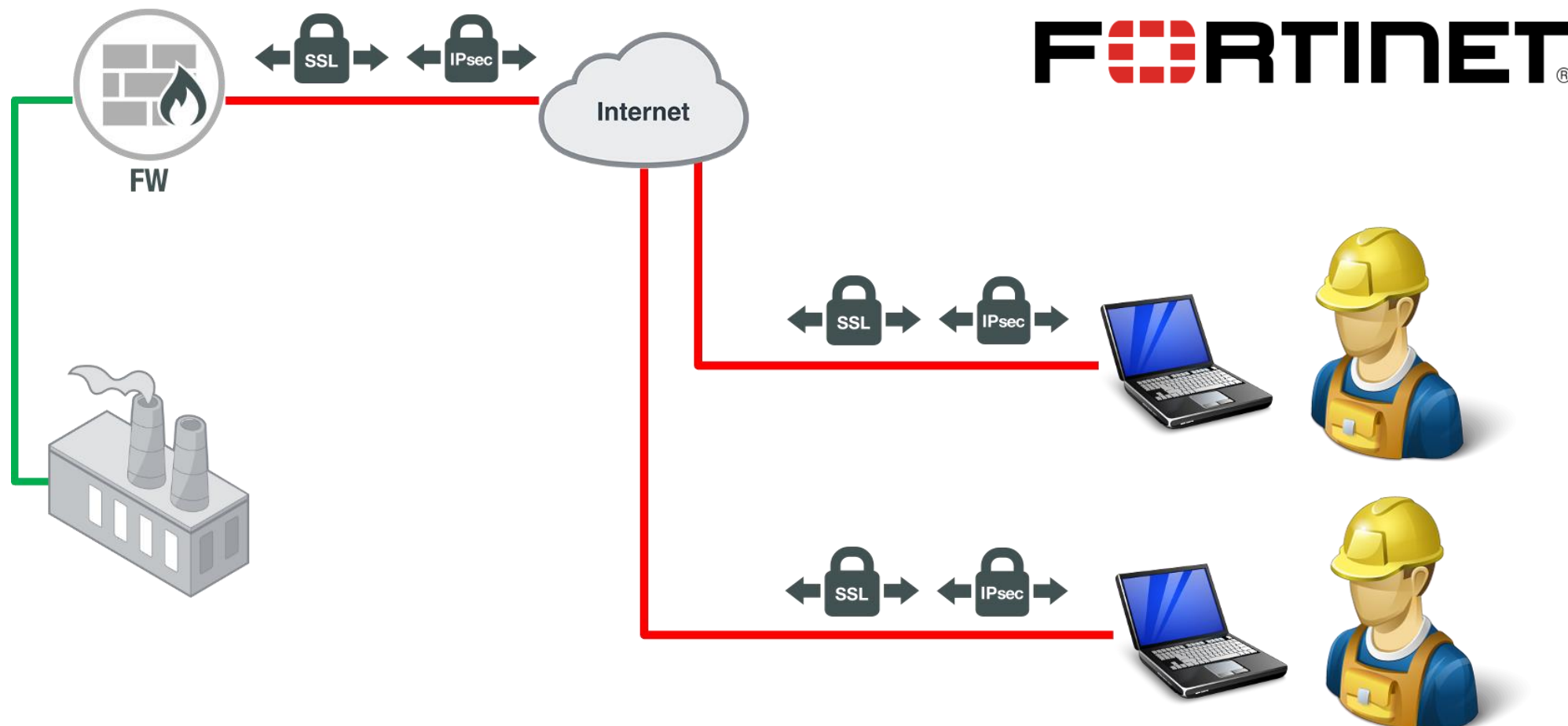
SITIO A SITIO



PROS Y CONTRAS

- › Pros
 - › Consolidación de servicios.
 - › Aplicación de funcionalidades avanzadas.
 - › Empleo de equipos de diferentes fabricantes.
- › Contras
 - › Uso de NAT en caso de duplicidad de direccionamientos.
 - › Variedad de tecnologías.

ACCESO REMOTO

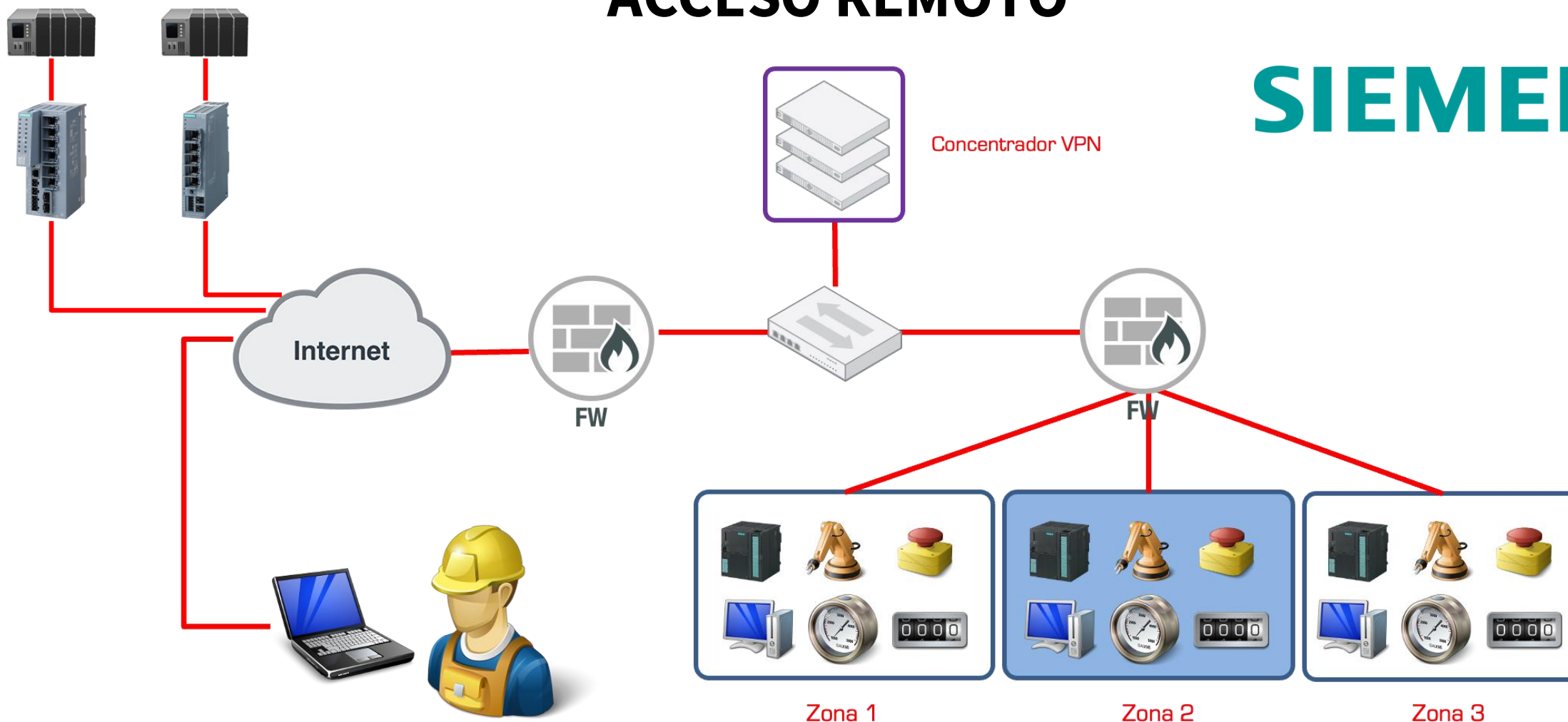


PROS Y CONTRAS

- › Pros
 - › Consolidación de servicios.
 - › Aplicación de funcionalidades avanzadas, DPI, IDS/IPS, 2FA.
 - › Implementar controles sobre equipos finales, PC. S.O.
 - › Todo el tráfico del PC por la sede.
- › Contras
 - › Instalación de cliente en PC, no siempre es posible o existen reticencias. Políticas y variedad de software.
 - › Actualización de cliente software.

ACCESO REMOTO

SIEMENS

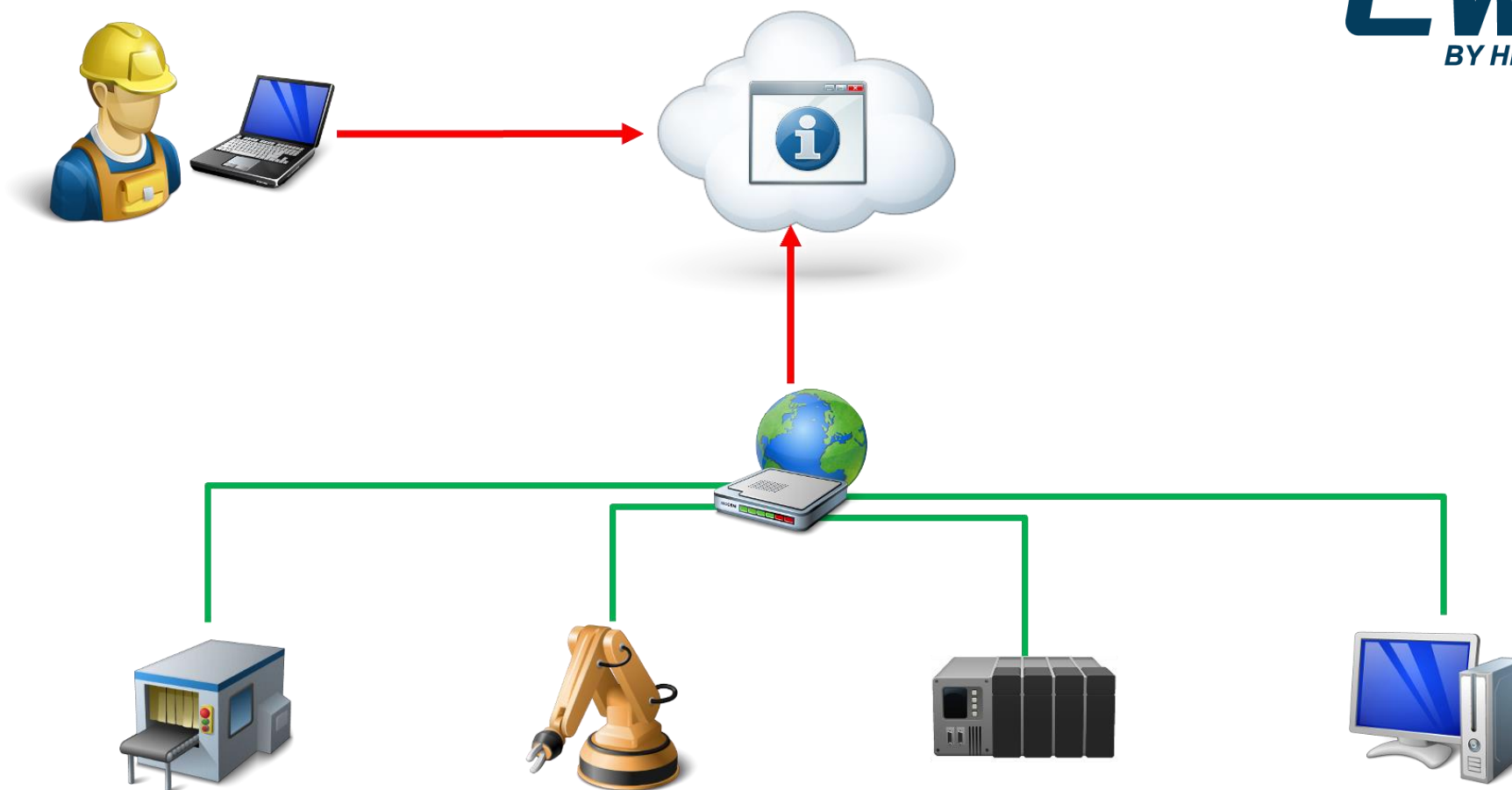


PROS Y CONTRAS

- › Pros
 - › Consolidación de servicios.
 - › Aplicación de funcionalidades avanzadas. DPI, IDS/IPS, 2FA.
 - › Posibilidad de virtualizar concentrador.
- › Contras
 - › Exposición del concentrador.
 - › Soluciones propietarias.

ACCESO REMOTO

EWON[®]
BY HMS NETWORKS



PROS Y CONTRAS

- › Pros
 - › Sencillez en el despliegue.
 - › Recogida de datos.
 - › Acceso por redes móviles.
 - › Posibilidad de interruptor físico.
- › Contrás
 - › Múltiples puntos de entrada a la organización.
 - › Consolidación de logs en sistemas SIEM.

PROS Y CONTRAS

FortiGuard Labs

Research
Services
Threat Intelligence
Support
Resources
About

FORTINET

PSIRT

Out-of-bound Write in sslvpnd

Summary

A out-of-bounds write vulnerability [CWE-787] in FortiOS and FortiProxy may allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.

Workaround : disable SSL VPN (disable webmode is NOT a valid workaround)

Note: This is potentially being exploited in the wild.

Version	Affected	Solution
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above

IR Number
FG-IR-24-015

Published Date
Feb 8, 2024

Updated Date
Jan 15, 2025

Severity
⚠ Critical

CVSSv3 Score
9.6

Impact
Execute unauthorized code or commands


CVE ID
CVE-2024-21762

CVRF
Download

Language

English

PROS Y CONTRAS




[Get support](#)
[Security advisories](#)
[Report vulnerabilities](#)
[Bug Bounty](#)
[Subscribe](#)
[RSS feed](#)

Palo Alto Networks Security Advisories / CVE-2024-3400


CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect


Urgency HIGHEST



Severity 10 - CRITICAL

Response Effort MODERATE	Recovery USER	Value Density CONCENTRATED	Attack Vector NETWORK
Attack Complexity LOW	Attack Requirements NONE	Automatable YES	User Interaction NONE
Product Confidentiality HIGH	Product Integrity HIGH	Product Availability HIGH	Privileges Required NONE
Subsequent Confidentiality HIGH	Subsequent Integrity HIGH	Subsequent Availability HIGH	

CVE **JSON** **CSAF** 



Published **2024-04-12**

Updated **2024-05-03**

Reference **PAN-252214**

Discovered **in production use**

Description

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

Customers should continue to monitor this security advisory for the latest updates and product guidance.

Product Status

RESUMEN

- › Cada solución tiene sus pros y contras.
- › A priori, más recomendable NGFW ya que permite:
 - › Definir un único punto de acceso a la organización. Modelo defendible.
 - › Gestión de identidades centralizada, AD, LDAP, RADIUS...
 - › Aplicación de DPI, IDS/IPS.
 - › Restricciones sobre los equipos de terceros como S.O; presencia de AV.
 - › Posibilidad de métodos robustos como certificados digitales.

RESUMEN

- › En caso de emplear Router-Firewall, normalizar una tecnología.
- › Buscar productos certificados en ISA/IEC 62443-4-1 y 4-2.
- › Contemplar Reglamento de Seguridad en Máquinas (EU) 2023/1230

QUE NO HACER

- › Exposición directa de equipos finales en internet. NAT 1:1, Port-Forwarding...
- › Delegar en terceros el control de accesos.
- › “Te pongo este equipo en máquina que es mejor para ti, me conecto cuando necesites”.
- › “No es mejor para ti, es mejor más cómodo, para el proveedor”.
- › No controlar la vigencia de los accesos.
- › No controlar uso de credenciales.
- › Dar acceso 24X7X365, por defecto.

QUE NO HACER

- › Duplicidad de recursos; Acceso Remoto IT y Acceso Remoto OT.
- › "Permit Any Any".
- › No hacer una gestión de acceso.
- › No actualizar los equipos.

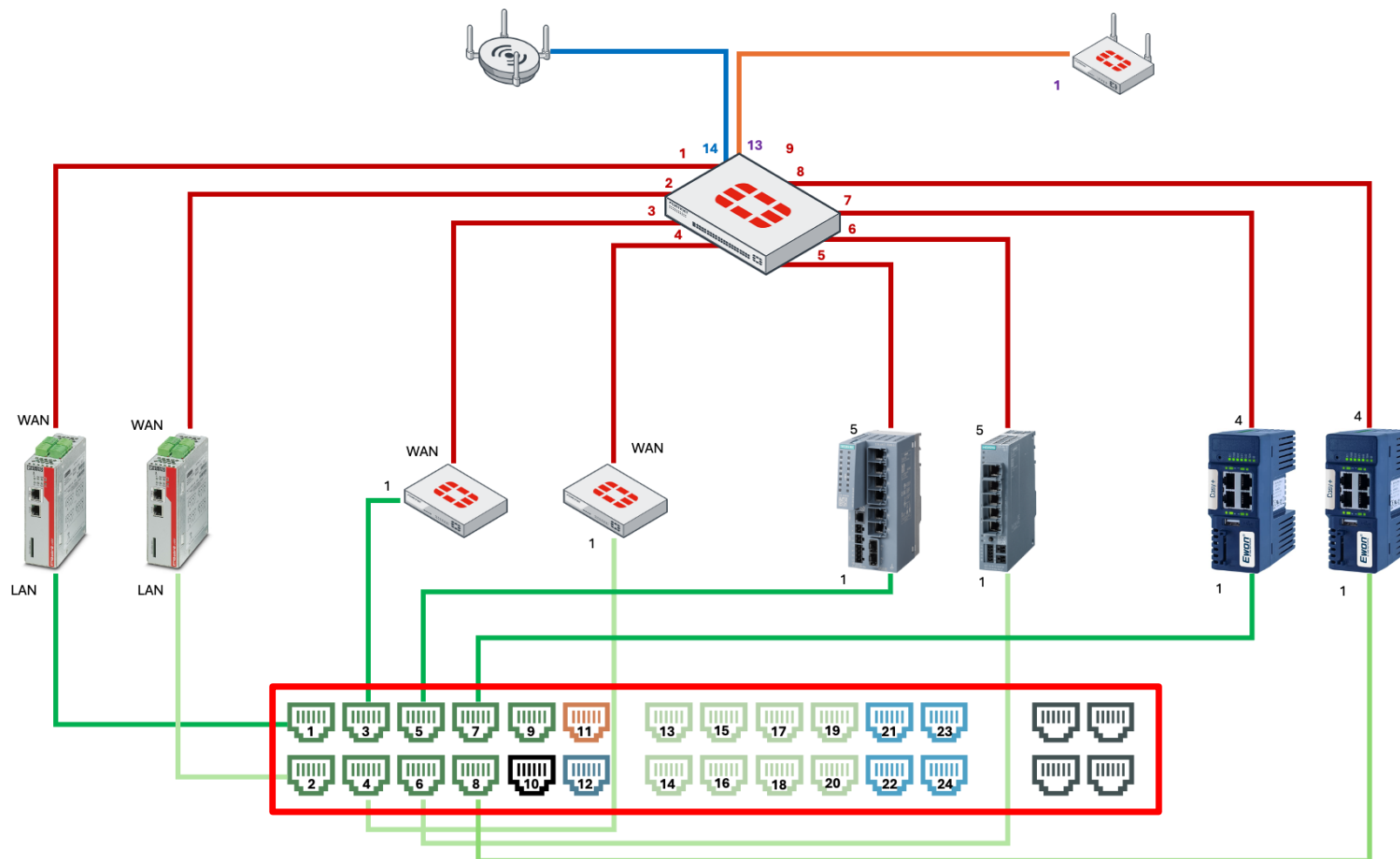


LABORATORIO

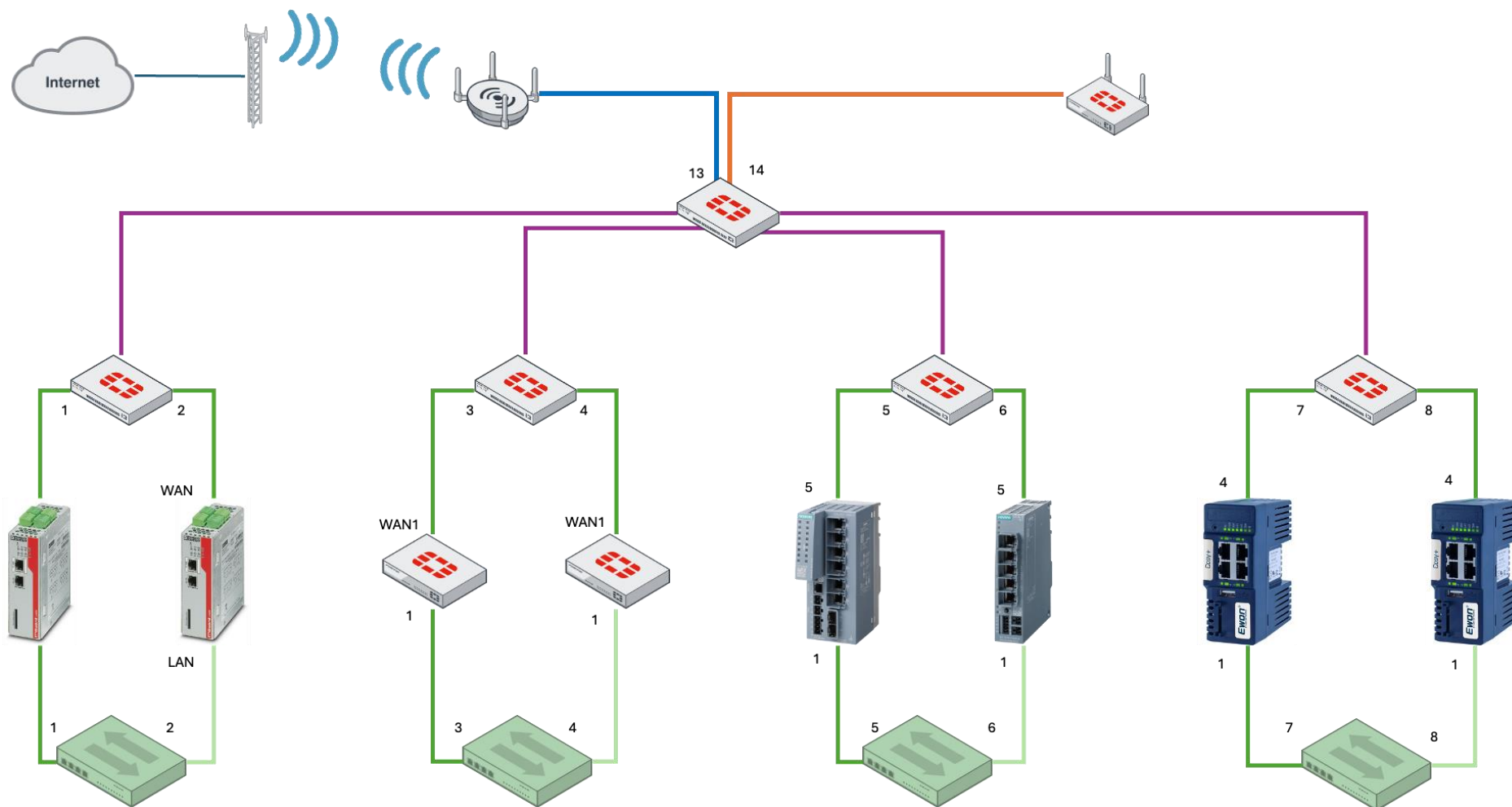
LABORATORIO

- › 4 Escenarios
- › Escenario 1
 - › VPN Sitio a Sitio
- › Escenario 2
 - › Acceso Remoto
- › Escenario 3
 - › VPN Sitio a Sitio Recursos Internos + Acceso Remoto
- › Escenario 4
 - › VPN Sitio a Sitio Recursos de Terceros + Acceso Remoto

LABORATORIO



LABORATORIO



LABORATORIO

10. **X** . **Y** . **Z** / 24

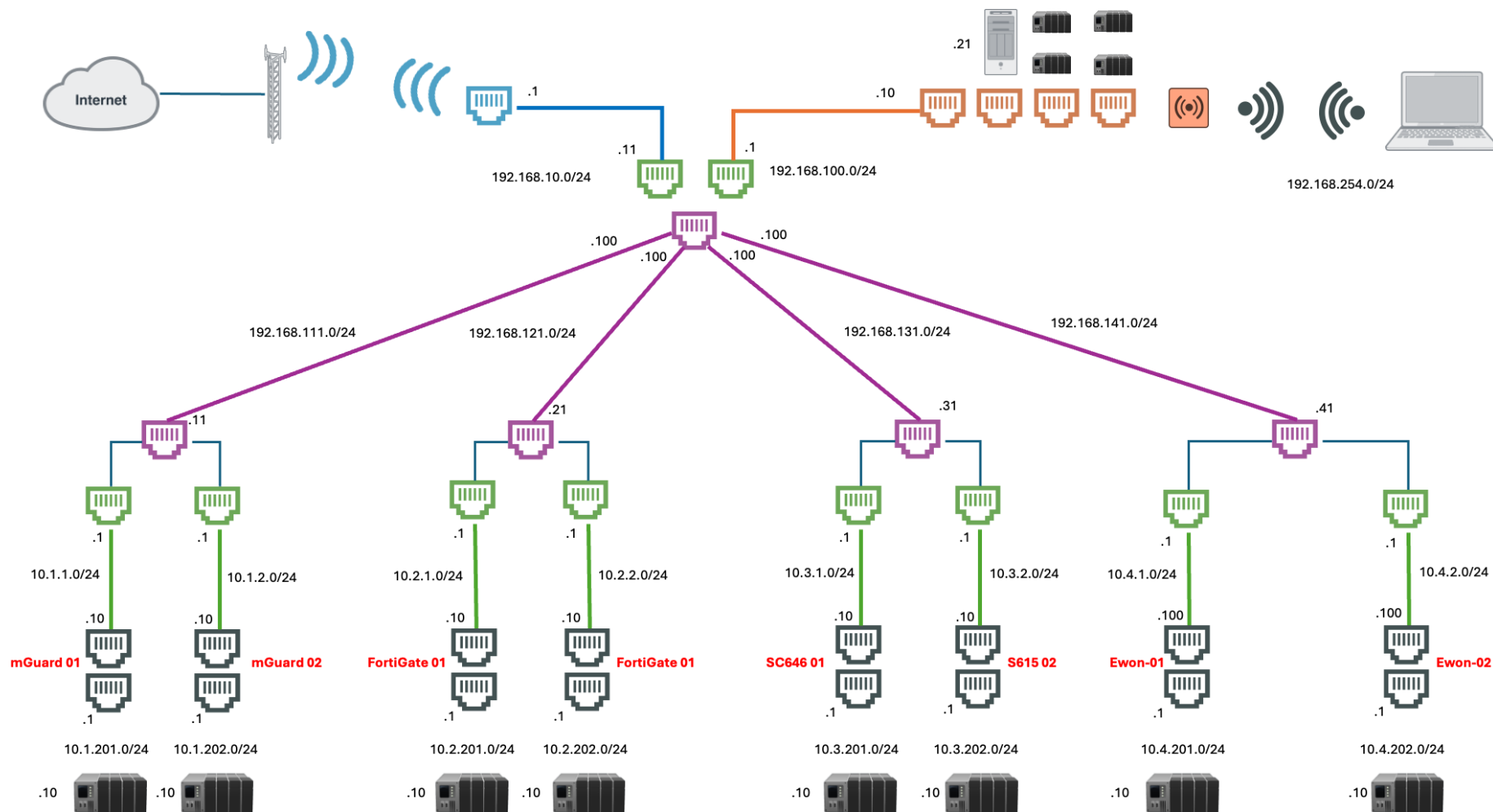
X = Número de escenario.

Y = Segmento de red, un dígito enlace "WAN" tres dígitos "LAN".

2XX, donde: **2** = Red OT; **01**, Primer FW; **02**, Segundo FW

Z = IP del equipo final

LABORATORIO



CONSEJOS

- › Leer primero las guías para ver lo que hay que hacer.
- › Los ejercicios pueden requerir de la colaboración entre los dos grupos.
- › Hay que leer, interpretar y contrastar con lo que aparece en pantalla.
- › Escenario 1: Labor conjunta.
- › Escenario 2: Independiente.
- › Escenario 3: SINEMA RC, en conjunto. Equipos, por separado.
- › Escenario 4: Independiente.



ESCENARIO 1

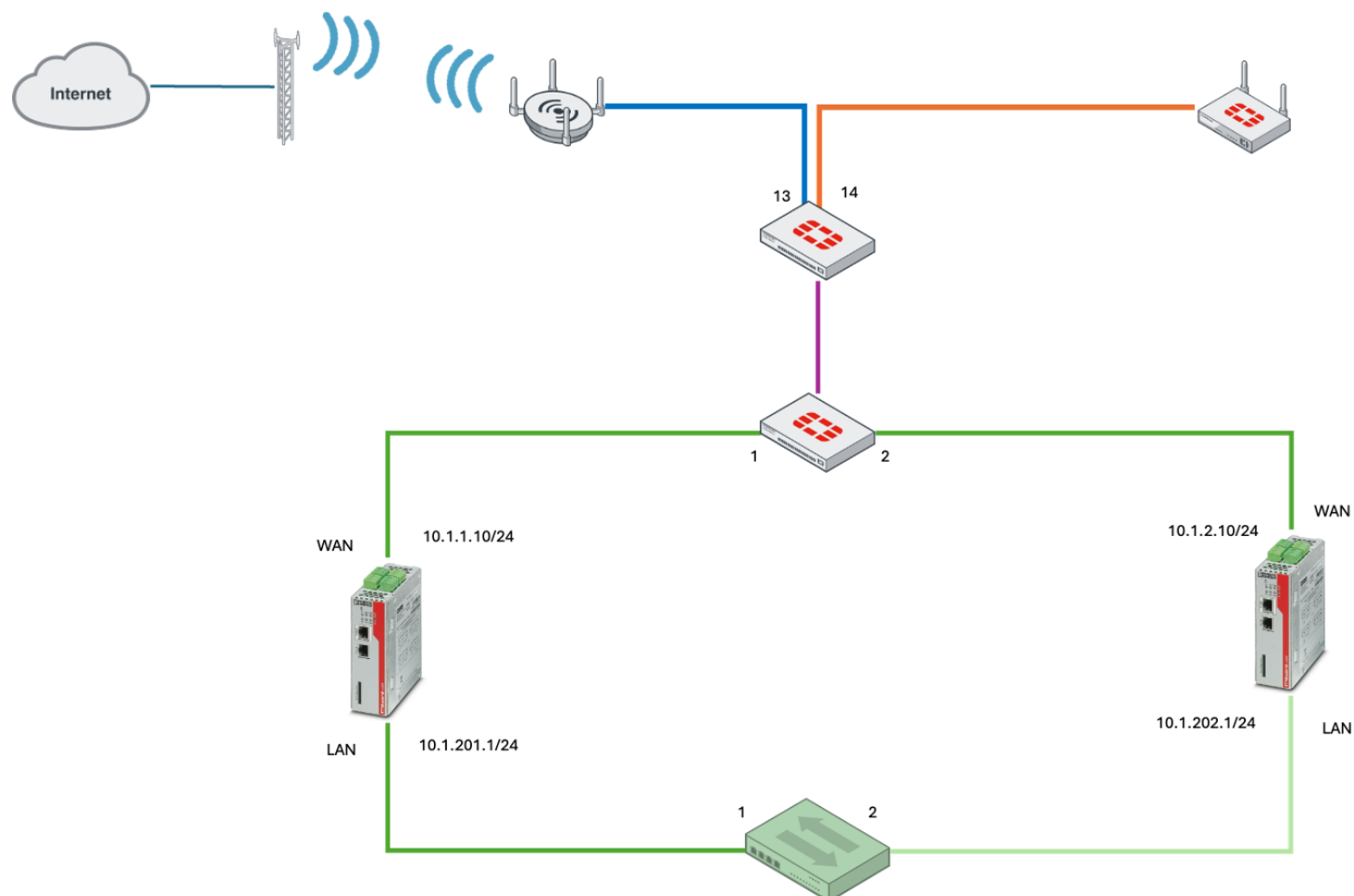
ESCENARIO 1

- › Tecnología: Phoenix Contact
- › Escenario: VPN Sitio a Sitio.
- › Se configurará una VPN Sitio a Sitio mediante protocolo IPSec y equipos “mGuard”.
- › Los equipos tienen dos interfaces de red “WAN” y “LAN”.
- › La VPN se establece mediante la “WAN”.

ESCENARIO 1

- › mGuard-01:
 - › WAN: 10.1.1.10/24
 - › LAN: 10.1.201.1/24
- › mGuard-02:
 - › WAN: 10.1.2.10/24
 - › LAN: 10.1.202.1/24
- › Los alumnos tendrán que conectarse al switch y accediendo a las IP de los mGuard en los puertos LAN hacer la configuración.
- › En la IP 10.1.201.10 y 10.1.202.10 tienen el PLC y WKS.
- › Si emplean su equipo la IP deben de poner la .100.

ESCENARIO 1





ESCENARIO 2

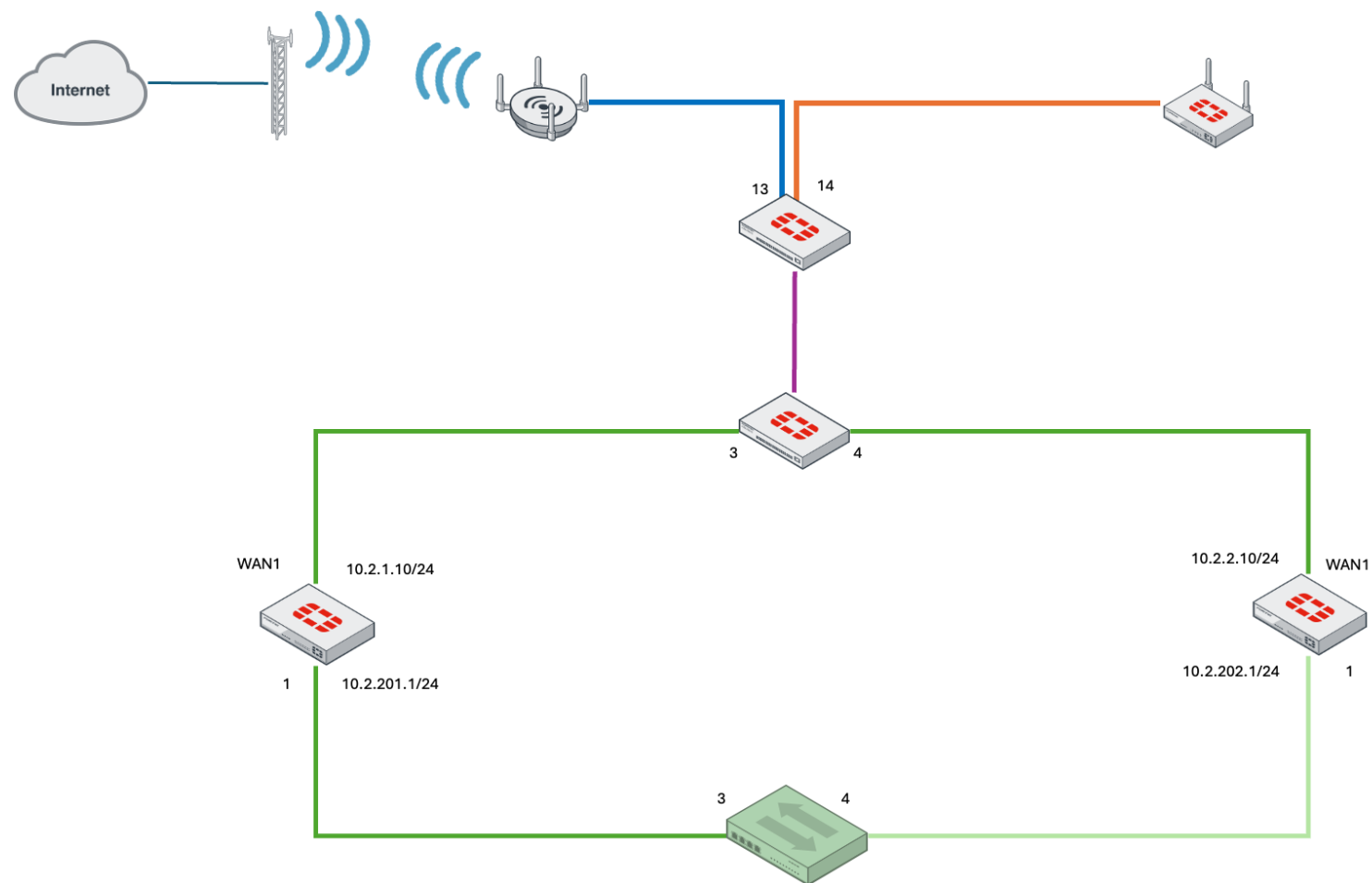
ESCENARIO 2

- › Tecnología: Fortinet.
- › Escenario: Acceso Remoto.
- › Se configurará una VPN de Acceso remoto para un Técnico que da Teleasistencia contra un Firewall Corporativo
- › Los equipos tienen dos interfaces de red “WAN” y “LAN 1”.
- › La VPN se establece mediante la “WAN”.

ESCENARIO 2

- › FGT-01:
 - › WAN: 10.2.1.10/24
 - › LAN: 10.2.201.1/24
- › FGT-02:
 - › WAN: 10.2.2.10/24
 - › LAN: 10.2.202.1/24
- › Los alumnos tendrán que conectarse al switch y accediendo a las IP de los Fortigate en los puertos LAN hacer la configuración.
- › En la IP 10.2.201.10 y 10.2.202.10 tienen el PLC y WKS.
- › Si emplean su equipo la IP deben de poner la .100.

ESCENARIO 2





ESCENARIO 3

ESCENARIO 3

- › Grupo 3:
 - › Tecnología: SIEMENS
 - › Escenario: Acceso Remoto, concentrador VPN On-Site ubicado en una DMZ.
 - › FWs Scalance SC646 y S615 crean una VPN contra el concentrador y el técnico de servicio lo hace por un acceso acceso remoto con usuario y contraseña

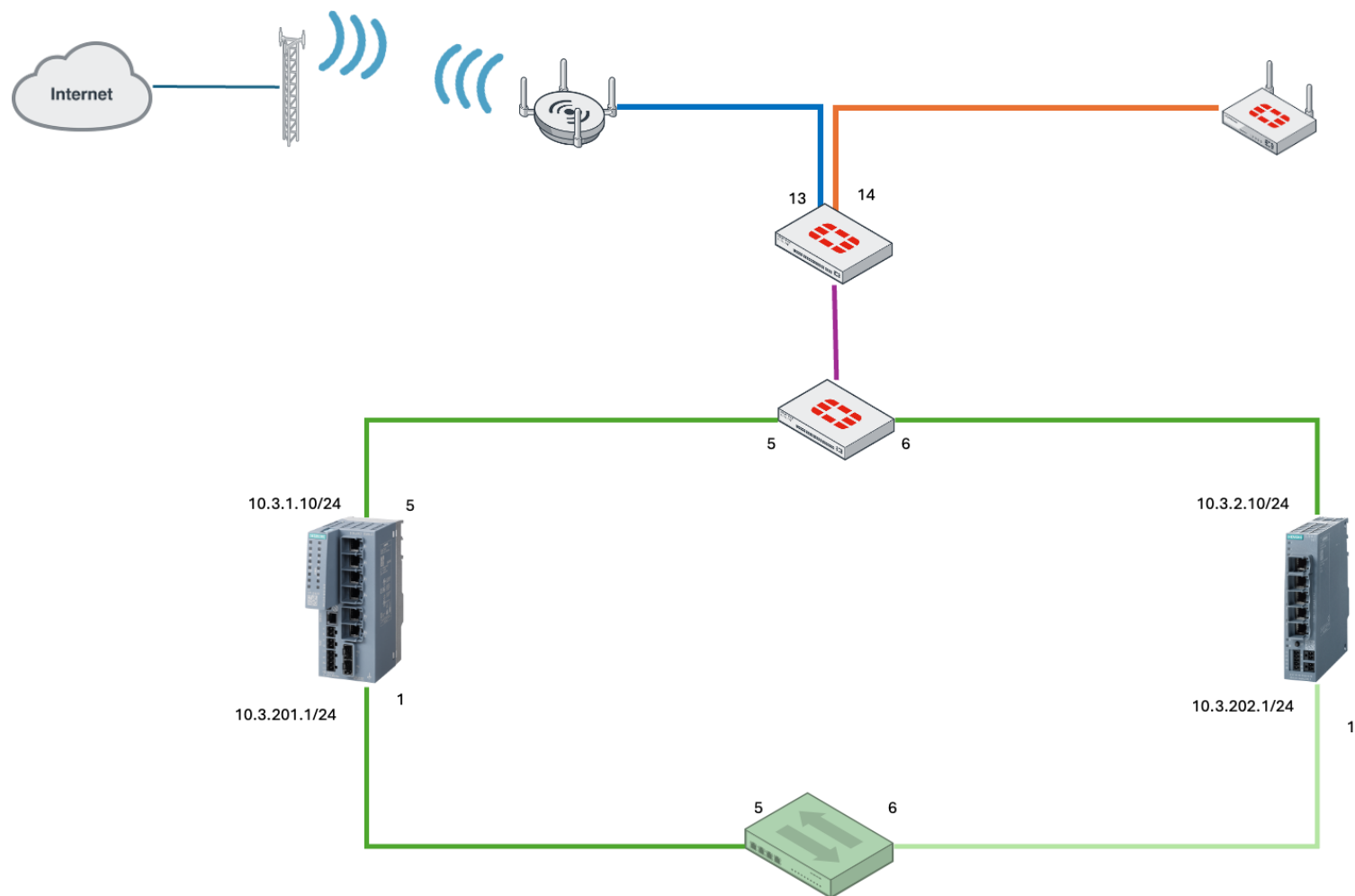
ESCENARIO 3

- › SC-646:
 - › P5: 10.3.1.10/24
 - › P1: 10.3.201.1/24
- › S615:
 - › P5: 10.3.2.10/24
 - › P1: 10.3.202.1/24
- › Los alumnos tendrán que conectarse al switch y accediendo a las IP de los Equipos Scalance en los puertos LAN hacer la configuración.
- › En la IP 10.3.201.10 y 10.3.202.10 tienen el PLC y WKS.

ESCENARIO 3

- › Si emplean su equipo la IP deben de poner la .100.

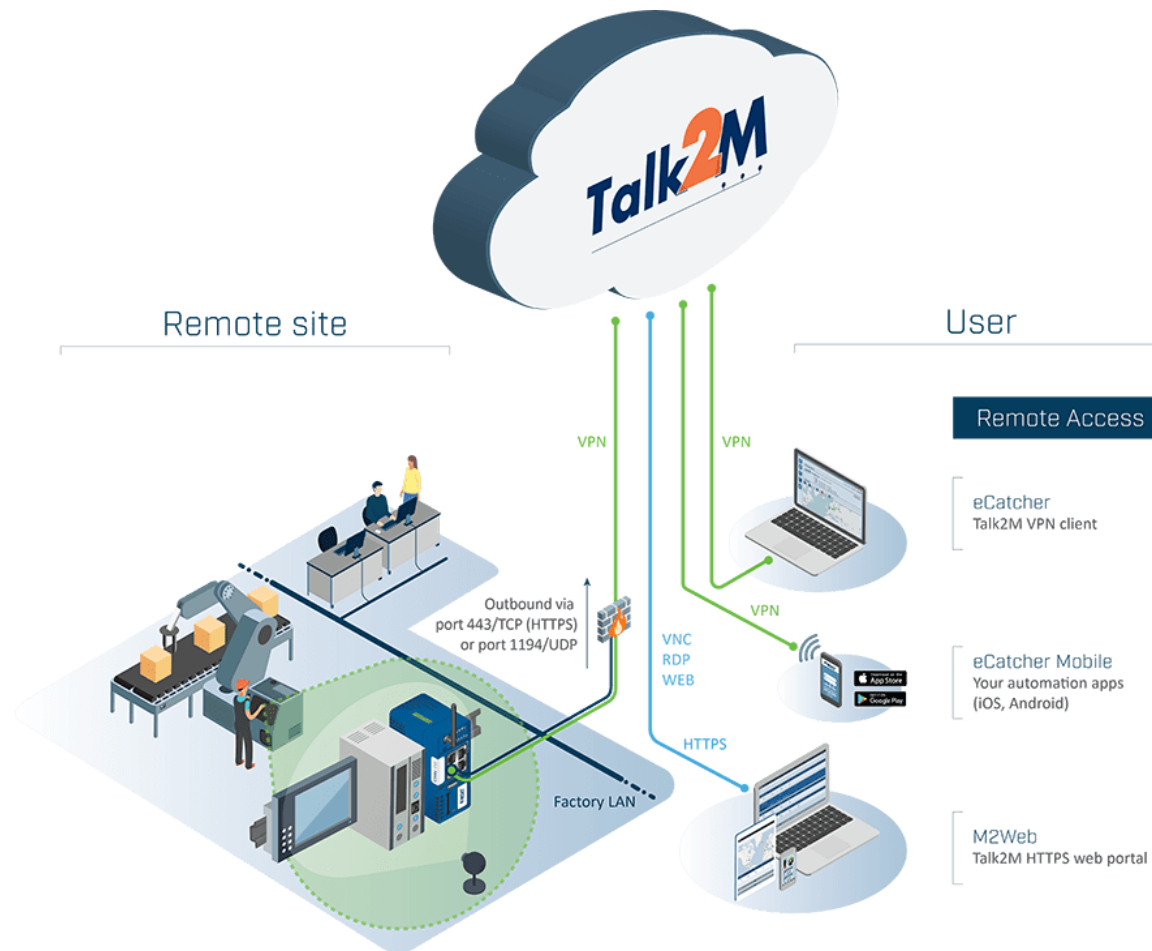
ESCENARIO 3



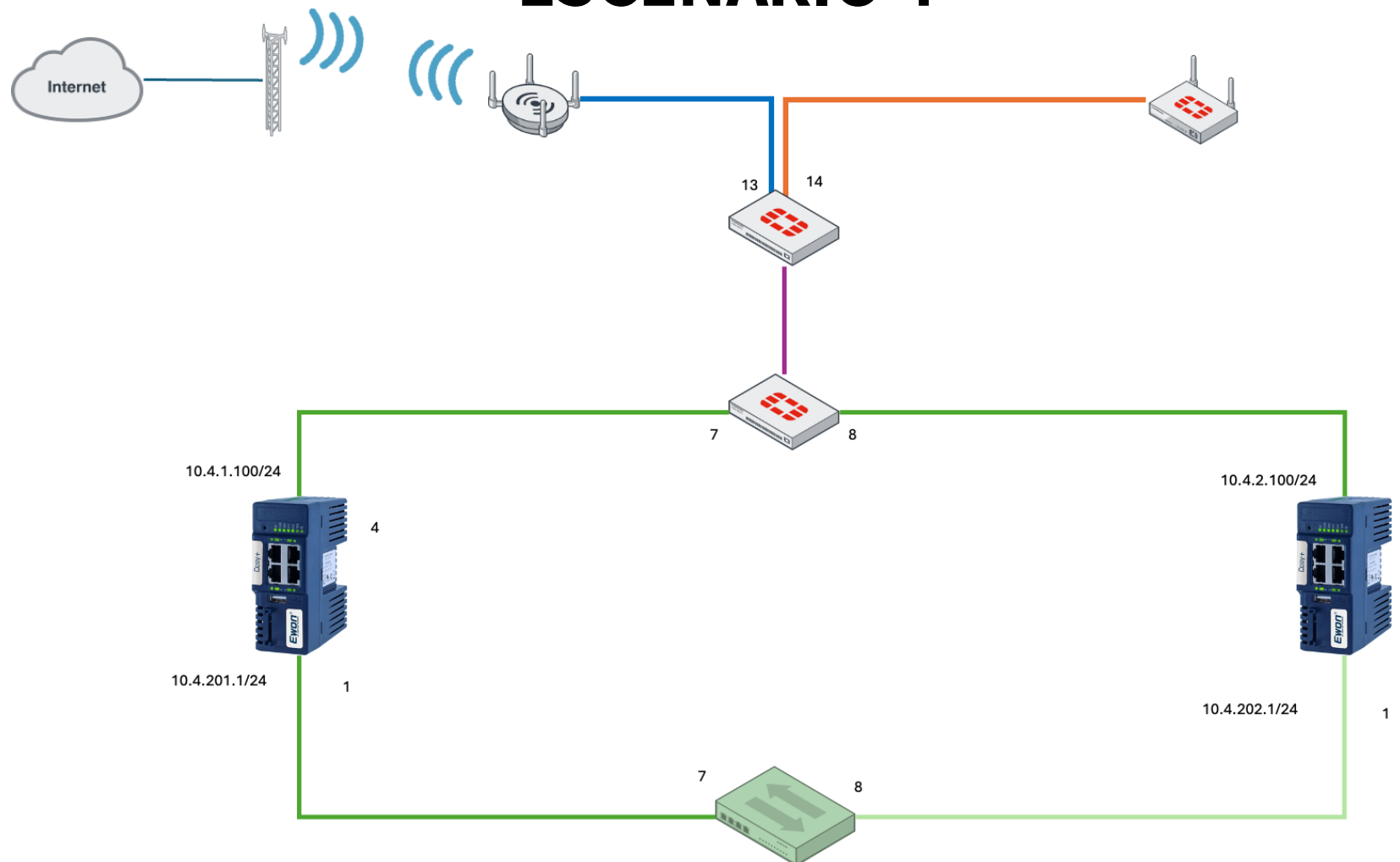


ESCENARIO 4

ESCENARIO 4



ESCENARIO 4



ESCENARIO 4

- › Se configurará una VPN de Acceso remoto a través de la plataforma Cloud Talk2M.
- › Los equipos tienen 4 interfaces, pero usaremos la 1 y 4, LAN y WAN respectivamente.
- › La VPN se establece mediante el 4.
- › Los alumnos deberán configurar los equipos eWon Cosy+ y Flexy para conectarlos a la plataforma Cloud Talk2M.

ESCENARIO 4

- › eWon-01:
 - › WAN: 10.4.1.100/24 (DHCP)
 - › LAN: 10.4.201.1/24
- › eWon-02:
 - › WAN: 10.4.2.100/24 (DHCP)
 - › LAN: 10.4.202.1/24
- › Software eCatcher: para registrar los eWon en la plataforma Talk2M y conectarse a ellos para crear la VPN.
- › Software eBuddy: para identificar el equipo, abrir un navegador para ejecutar los asistentes y realizar la configuración.

ESCENARIO 4

- › Los alumnos deberán configurar los equipos eWon Cosy+ y Flexy para conectarlos a la plataforma Cloud Talk2M.
- › Si emplean su equipo la IP deben de poner la .100.



ESKERRIK ASKO – GRACIAS – THANK YOU

Zamalbide Auzoa z/g - 20100 Errenteria (Gipuzkoa)

T. (+34) 943 082 900

info@tknika.eus

www.tknika.eus

EDORTA ECHAVE GARCÍA



¡ ESKERRIK ASKO !