Tknika

Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre

Configuración panel OT

2022-2023

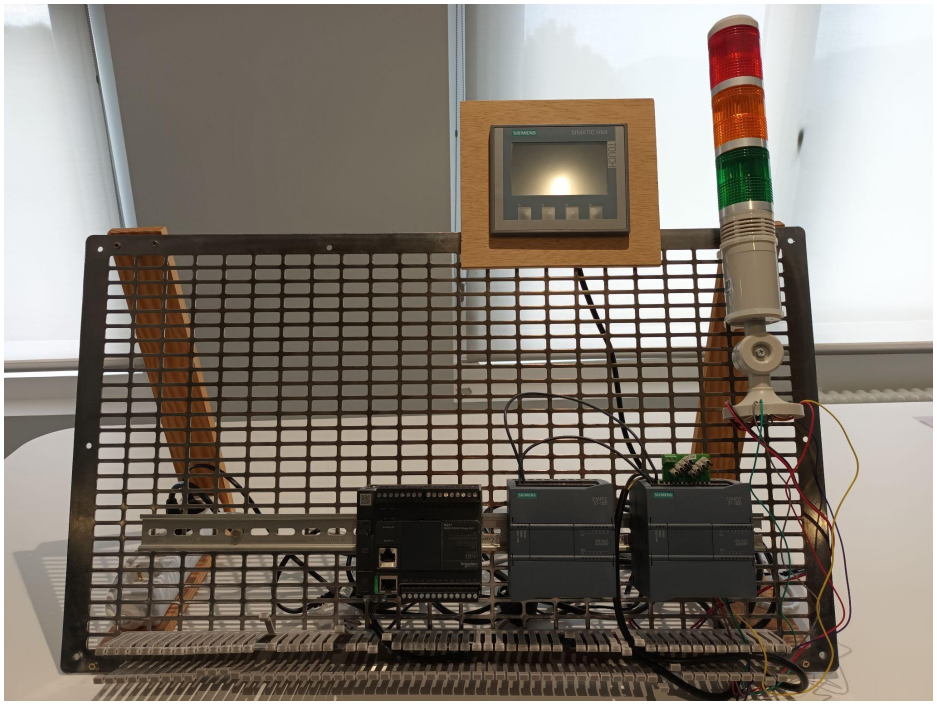
Fp EUSKADI LANBIDE HEZIKETA

EUSKO JAURLARITZA
GOBIERNO VASCO
HEZKUNTZA SAILA
Lanbide Heziketako Saiburuordetza
DEPARTAMENTO DE EDUCACIÓN
Viceconsejería de Formación Profesional

INDICE

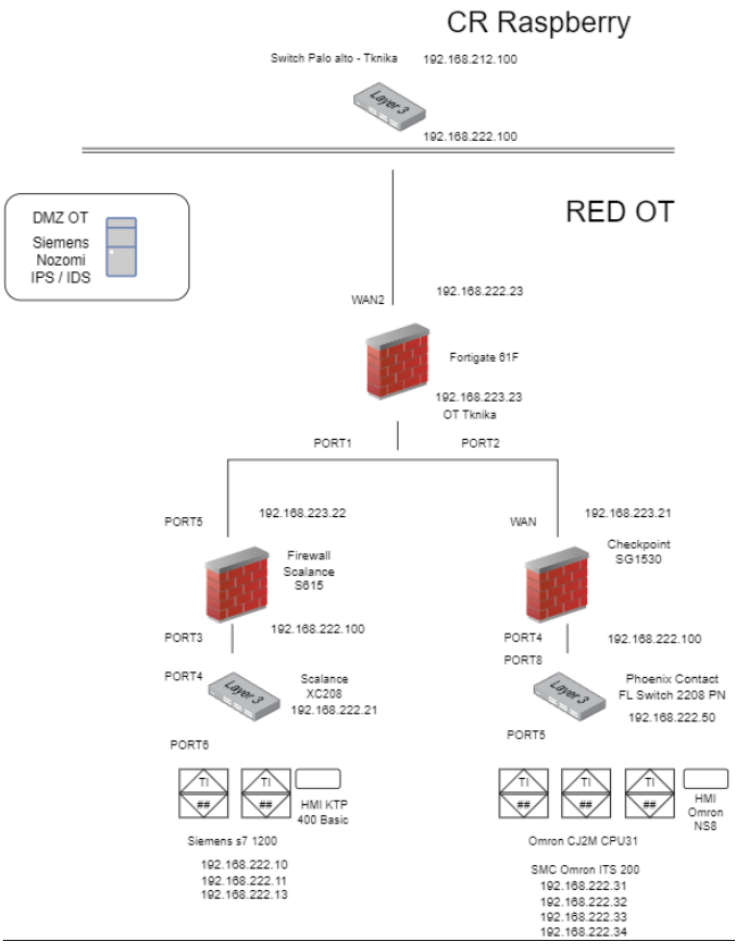
1. ARQUITECTURA DEL PANEL OT

El laboratorio de ciberseguridad de Tknika dispone de una célula de fabricación ITS 200 y un panel con PLC Siemens que simulan 2 sistemas productivos.



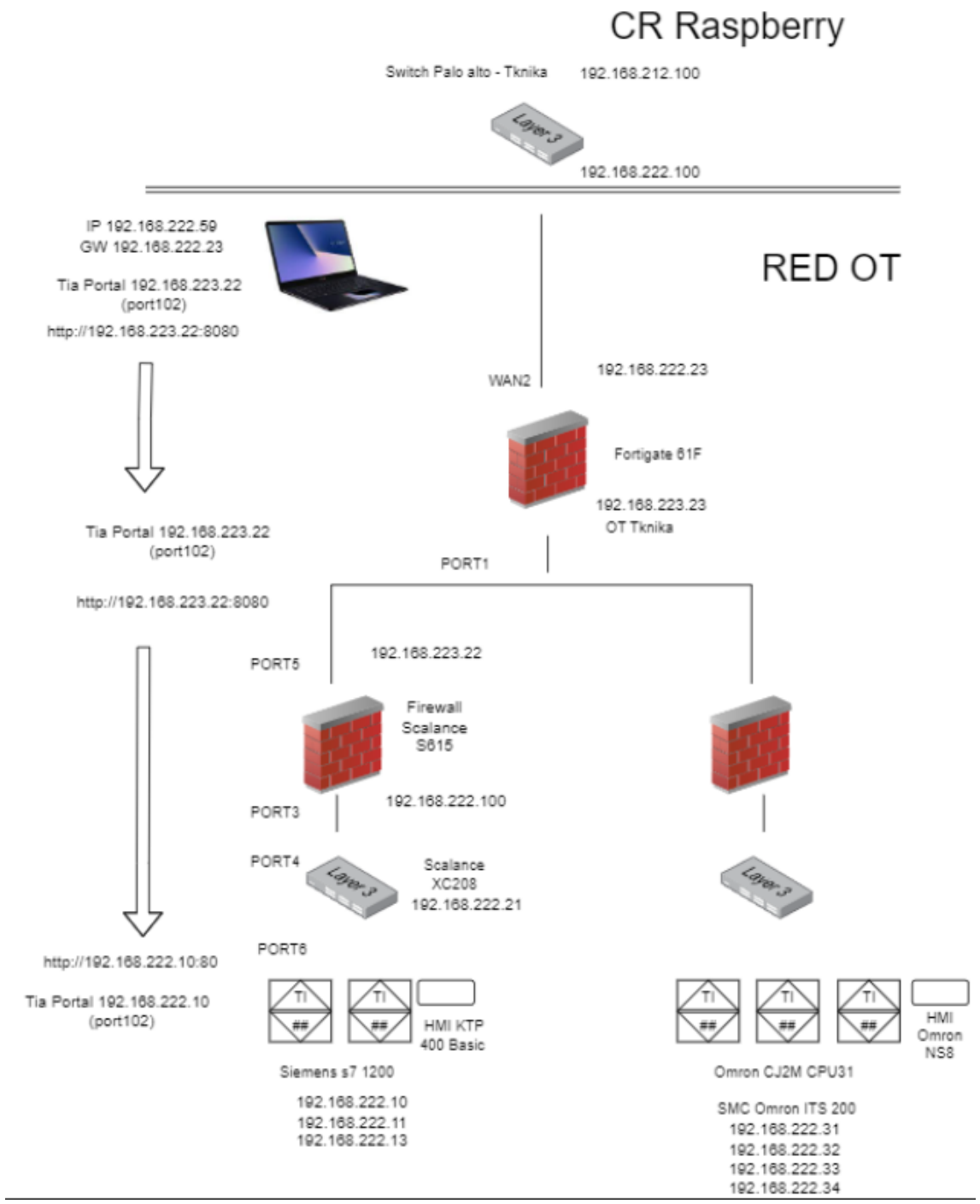
Estos sistemas productivos tienen que ser protegidos con una segmentación adecuada. En la propuesta de segmentación se contemplan 2 subredes cada una protegida por un firewall . El sistema de producción controlado con PLC Siemens se concentra en un switch gestionable Scalance XC208 y se protege con un Firewall industrial Siemens Scalance S615.El sistema de producción ITS 200 controlado con PLC Omron se concentra en un switch gestionable Phoenix Contact y se protege con un Firewall Checkpoint. Ambos segmentos son protegidos por un firewall principal para OT (Fortinet 61F) que enlaza con la red de Tknika, en este caso con el ciberrange.

Se han seleccionado dispositivos de diferentes fabricantes de manera premeditada para conocer diferentes tecnologías de configuración y a la vez dificultar el acceso a un posible atacante al tener que superar barreras con diferentes configuraciones.

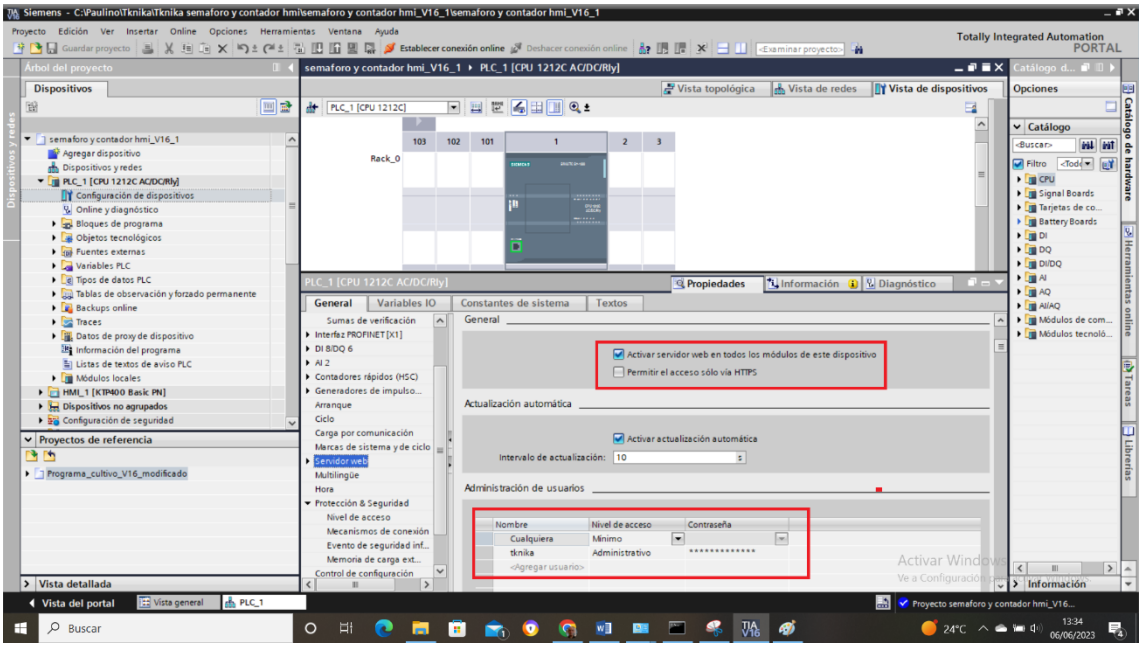


2. ACCESO A LA RED SIEMENS

El acceso a la red Siemens está configurado de tal manera que las IP de los PLC queden "ocultas" detrás del firewall. Para acceder al PLC vía webserver utilizaremos la IP WAN del cortafuegos en su puerto 8080 (http://192.168.223.22:8080) y la configuración del cortafuegos nos redirigirá hacia la IP del PLC y el puerto 80 (http://192.168.222.10).



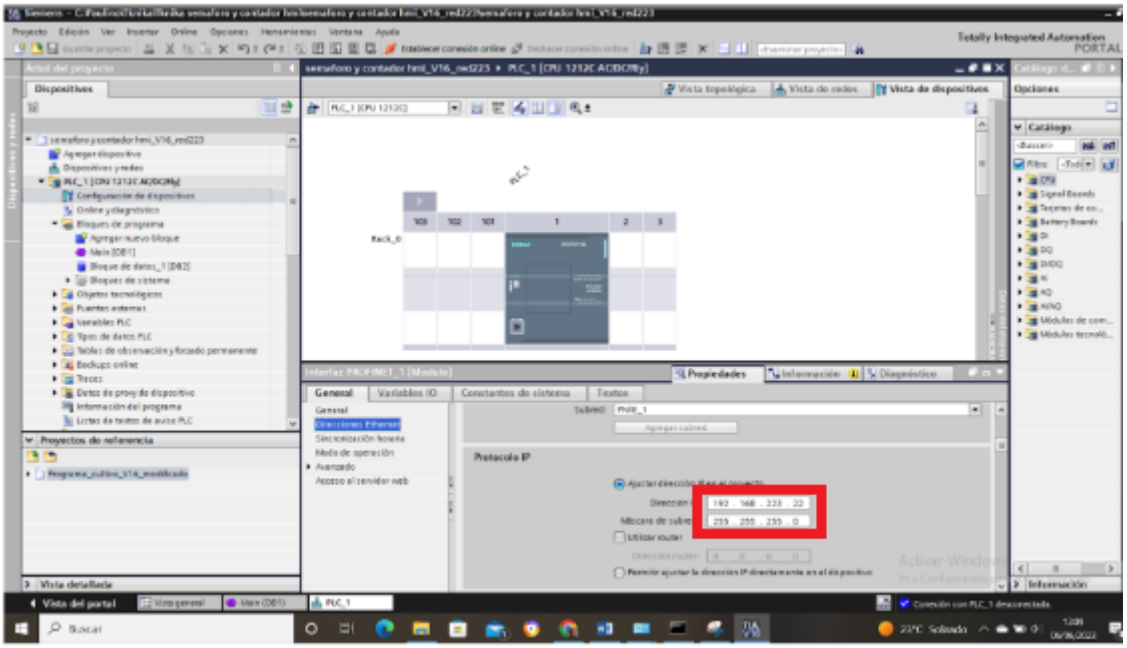
Habilitar el acceso webserver en el PLC con(port 443)/sin (port 80) seguridad y configurar un usuario de acceso.



Acceder a través de la IP WAN del cortafuegos http://192.168.223.22:8080

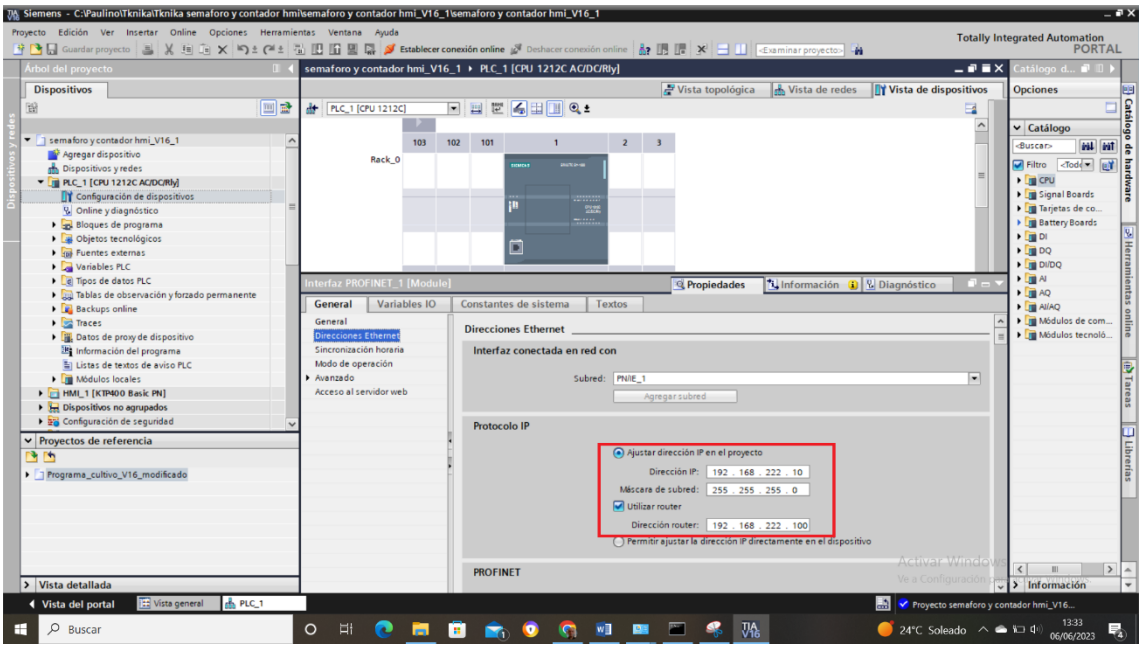
El cortafuegos redirige a la IP del PLC en el servicio port 80 y nos muestra la página del webserver.

De manera similar accederemos a través de Tia portal.En el proyecto Tia portal configuraremos la IP del PLC apuntando a la IP WAN del cortafuegos. 192.168.223.22 (por defecto puerto 102)

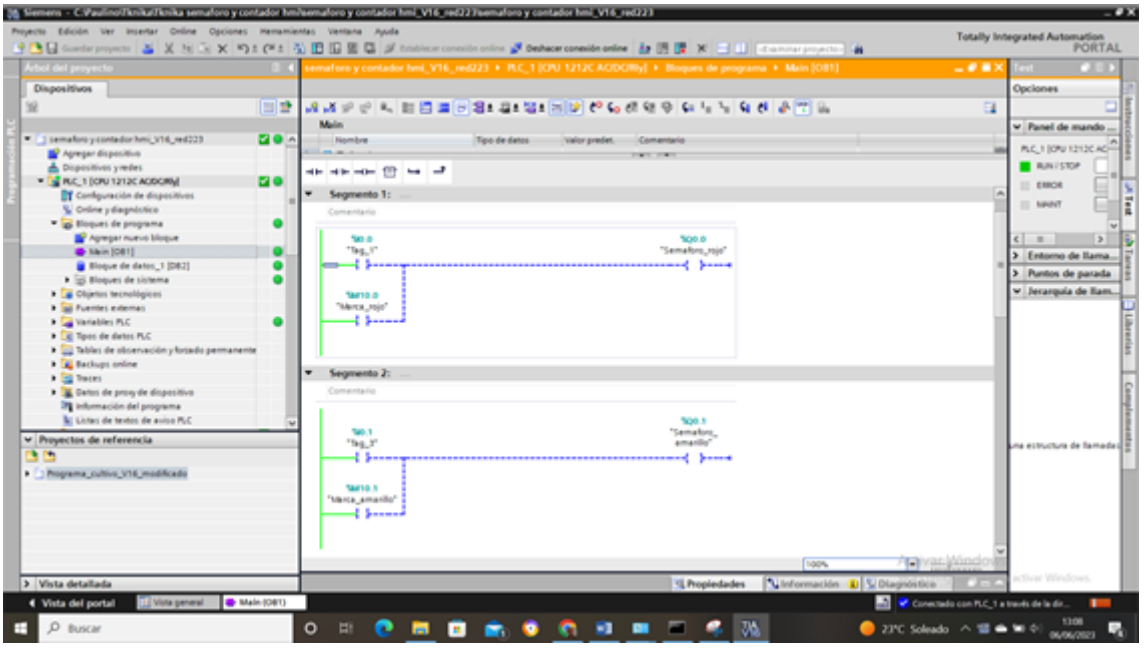


El PLC al estar detrás del cortafuegos en la red interna tendrá cargada una IP local de la red con el gateway de salida apuntando a la IP LAN del cortafuegos.

IP 192.168.222.10 GW 192.168.222.100

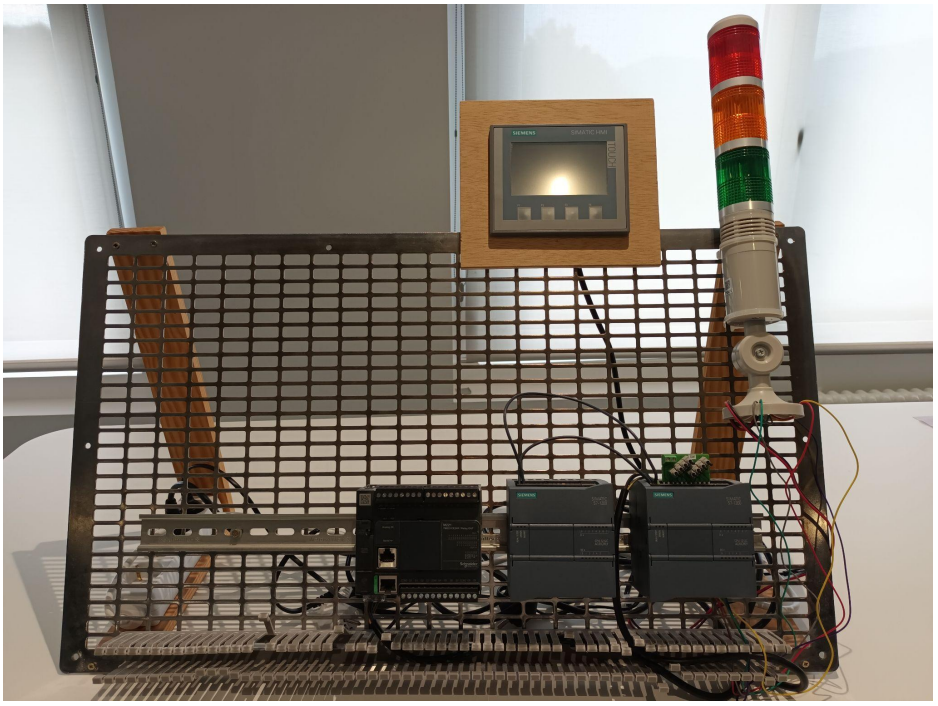


La regla de cortafuegos y la configuración NAPT redirigirán los puertos.

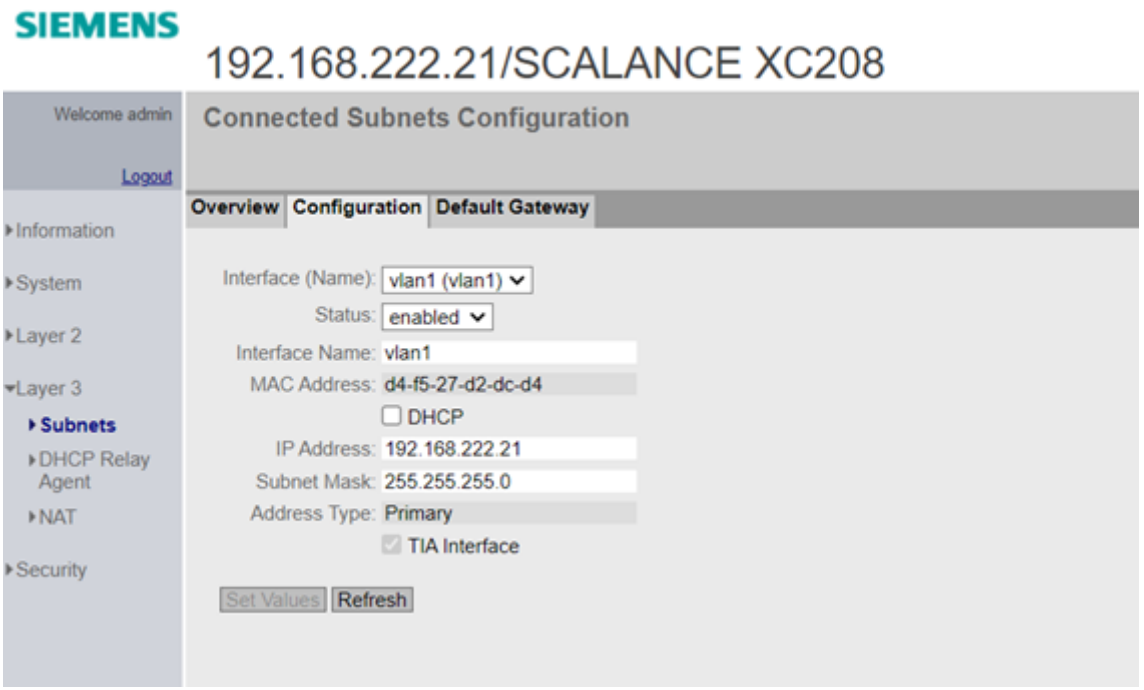

Totally Integrated Automation
PORTAL
Segmento 1:
Segmento 2:

2.1 CONFIGURACIÓN SWITCH SCALANCE XC208

El switch de la red Siemens realiza tareas de concentrador para los PLC Siemens 1(192.168.222.10) , Siemens 2 (192.168.222.11) y la pantalla HMI (192.168.222.13)

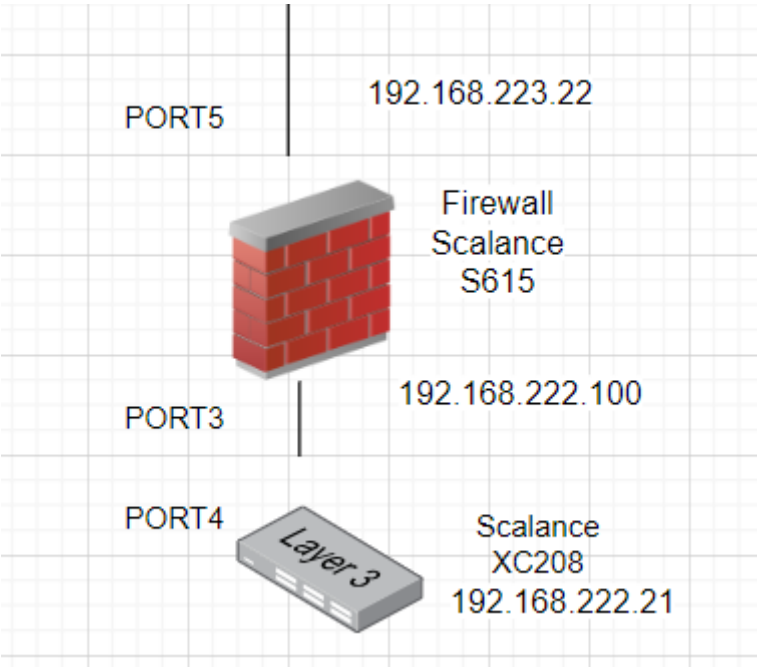


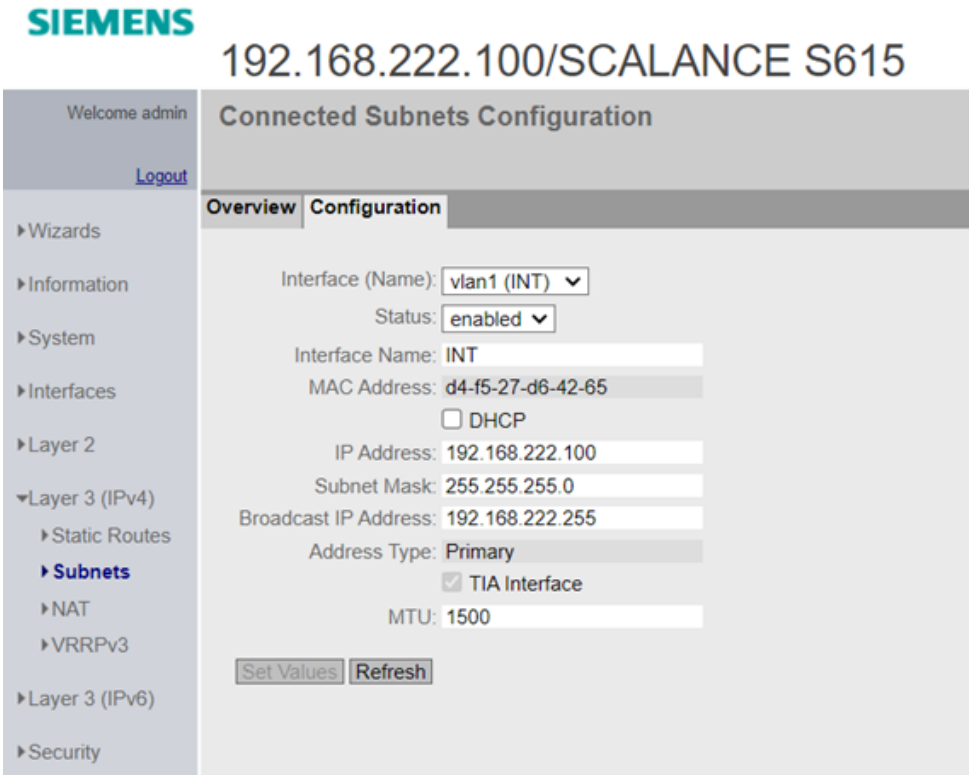
La IP de gestión del switch es https://192.168.222.21

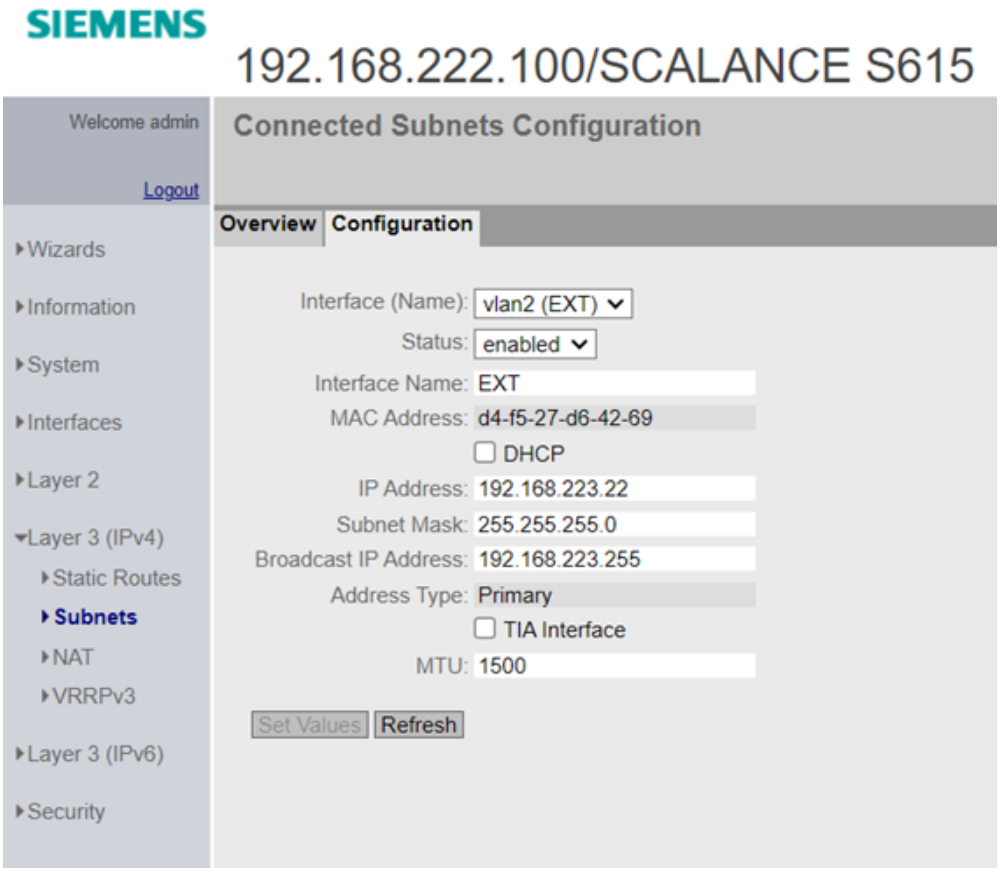


2.2 Configuración firewall Scalance S615

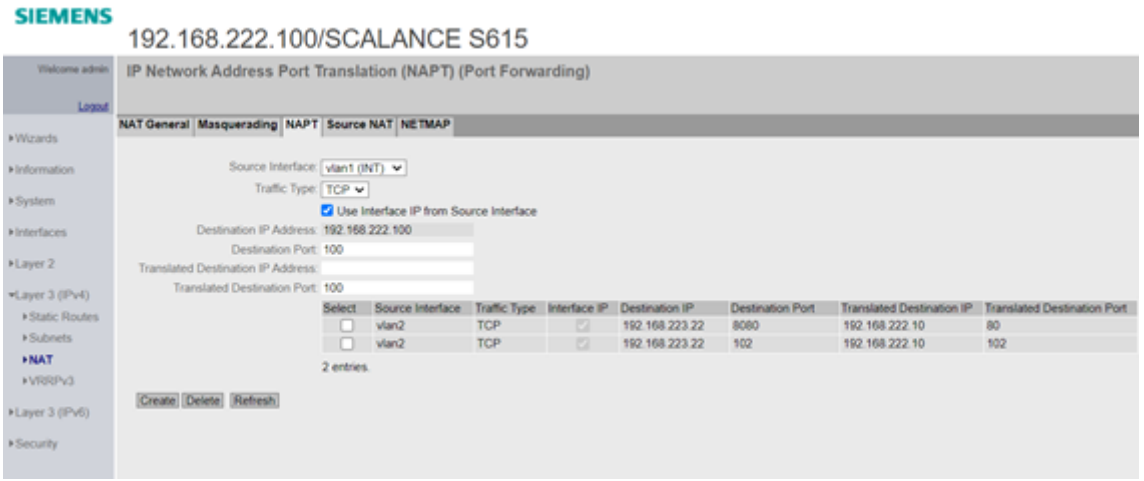
La red Siemens está controlada por un firewall Scalance S615 con 2 subredes, una INT 192.168.222.100 conectada al panel industrial Siemens a través del switch XC208 y una EXT 192.168.223.22 conectada al firewall principal Fortinet

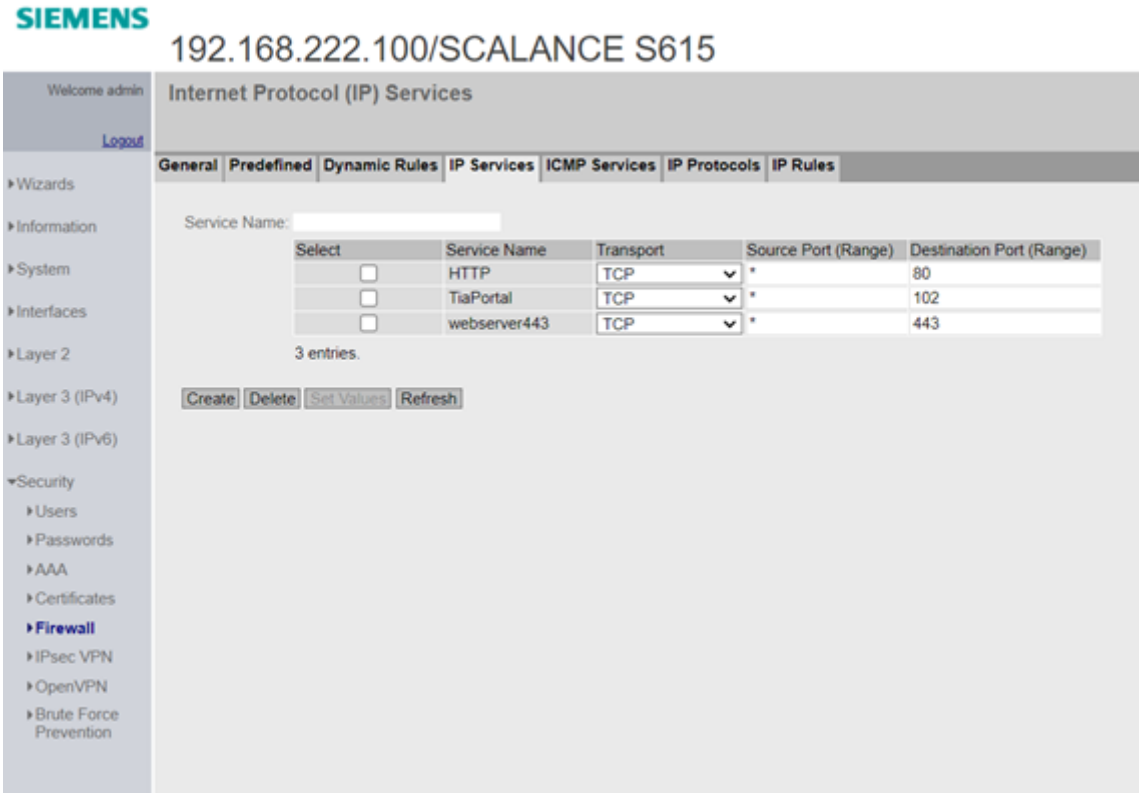


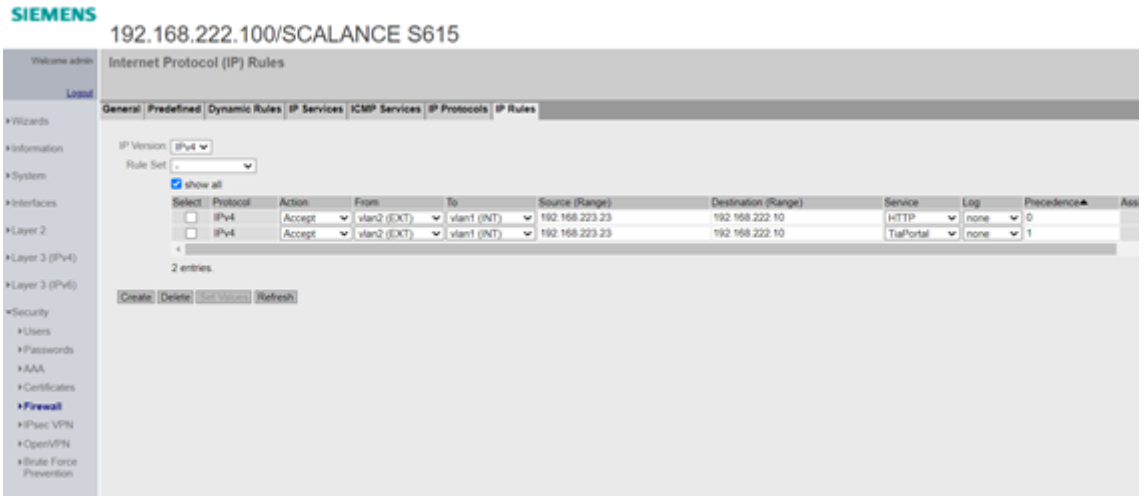




En el cortafuegos hay que configurar por un lado la redirección de puertos NAPT así como las reglas de filtrado.

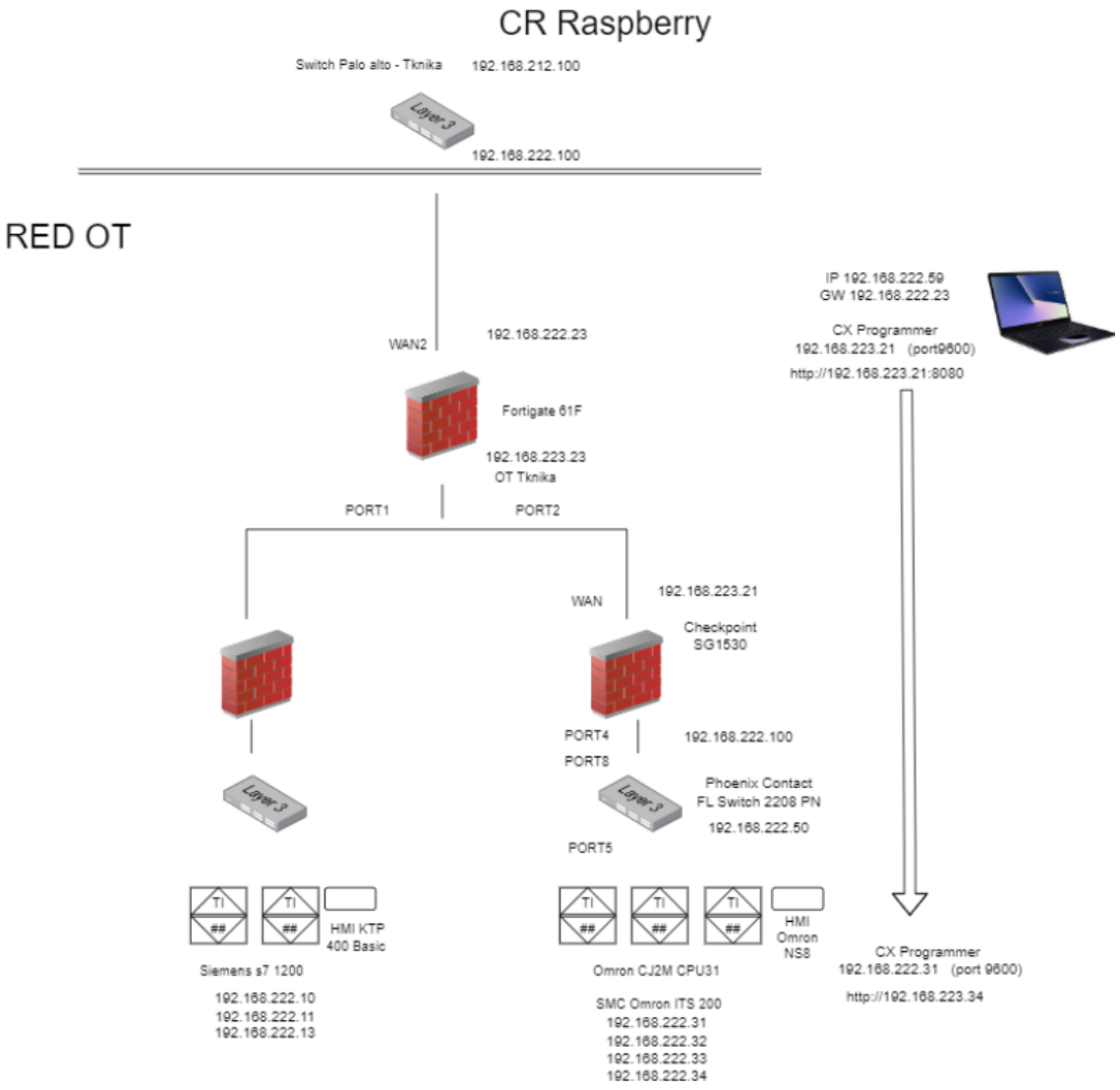



SIEMENS
192.168.222.100/SCALANCE S615
Welcome admin
Logout
Internet Protocol (IP) Services
General
Predefined
Dynamic Rules
IP Services
ICMP Services
IP Protocols
IP Rules
Wizards
Information
System
Interfaces
Layer 2
Layer 3 (IPv4)
Layer 3 (IPv6)
Security
Users
Passwords
AAA
Certificates
Firewall
IPsec VPN
OpenVPN
Brute Force Prevention
Service Name:
Select
Service Name
Transport
Source Port (Range)
Destination Port (Range)
HTTP
TCP
*
80
TiaPortal
TCP
*
102
webserver443
TCP
*
443
3 entries.
Create
Delete
Set Values
Refresh

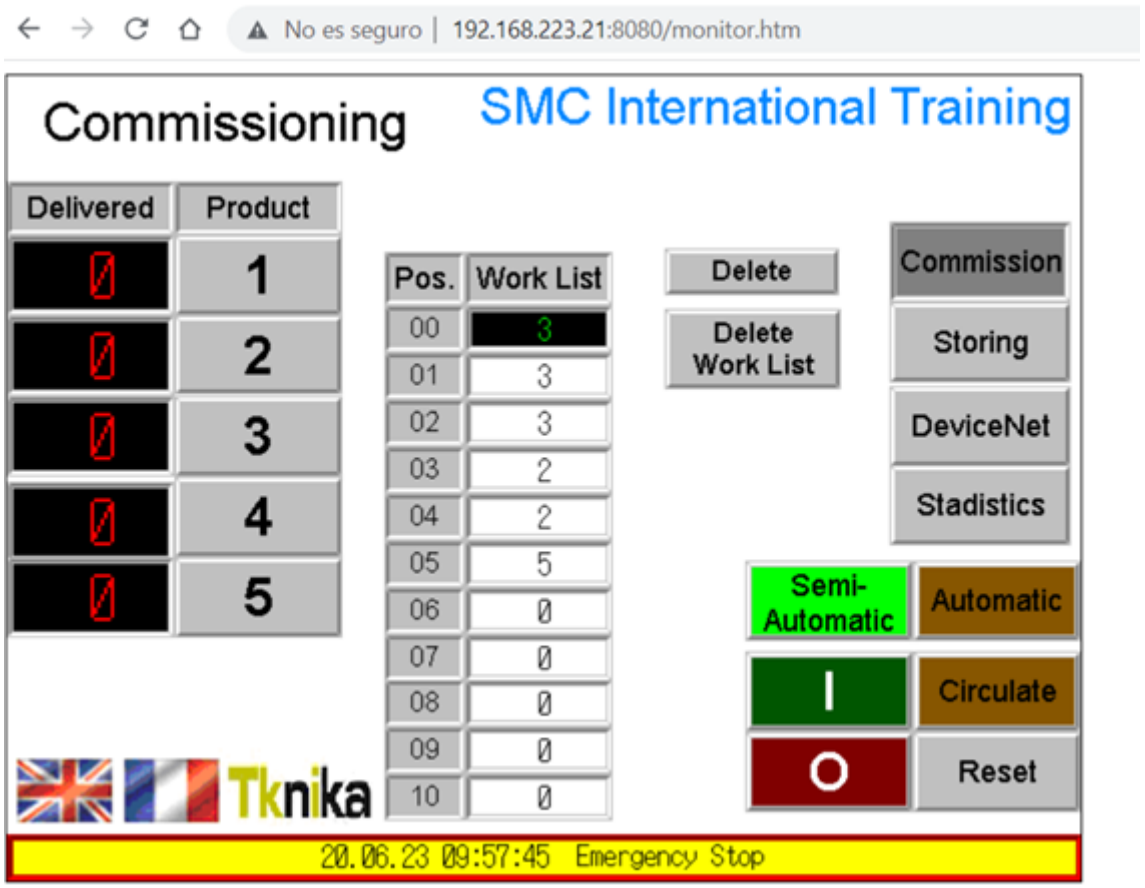

SIEMENS
192.168.222.100/SCALANCE S615
Internet Protocol (IP) Rules
General
Predefined
Dynamic Rules
IP Services
ICMP Services
IP Protocols
IP Rules
IP Version:
Rule Set:
show all
Select
Protocol
Action
From
To
Source (Range)
Destination (Range)
Service
Log
Precedence
IPv4
Accept
vlan2 (EXT)
vlan1 (INT)
192.168.223.23
192.168.222.10
HTTP
none
0
IPv4
Accept
vlan2 (EXT)
vlan1 (INT)
192.168.223.23
192.168.222.10
TiaPortal
none
1
2 entries.
Create
Delete
Set Values
Refresh

3. ACCESO A LA RED OMRON ITS200

El acceso a la red Omron está configurado de tal manera que las IP de los PLC queden "ocultas" detrás del firewall. Para acceder a la pantalla HMI vía web utilizaremos la IP WAN del cortafuegos en su puerto 8080 (http://192.168.223.21:8080) y la configuración del cortafuegos nos redirigirá hacia la IP de la pantalla y el puerto 80 (http://192.168.222.34).



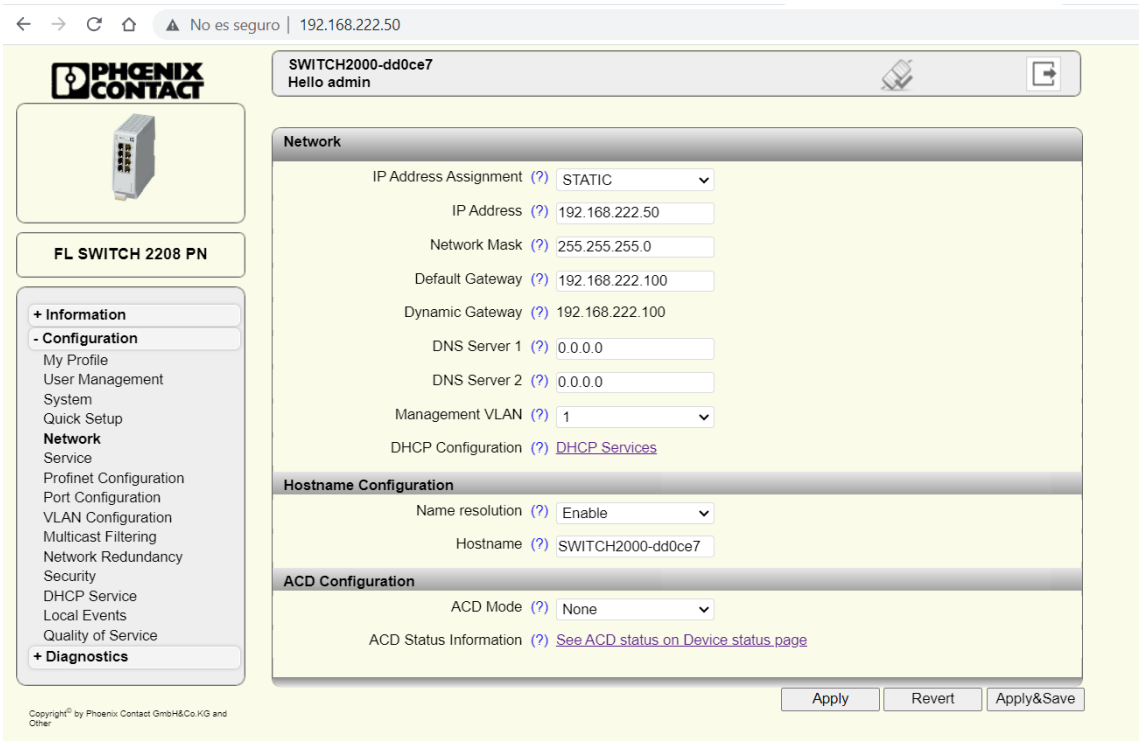
Pantalla HMI Omron 192.168.223.21:8080 que se redirige a 192.168.222.34 en la red interna.



3.1 Configuración switch Phoenix contact

El switch de la red Omron realiza tareas de concentrador para los PLC Omron CJ2M Almacén(192.168.222.31) , Inspección (192.168.222.32) y Clasificación (192.168.222.33) y la pantalla de gestión HMI Omron (192.168.222.34)

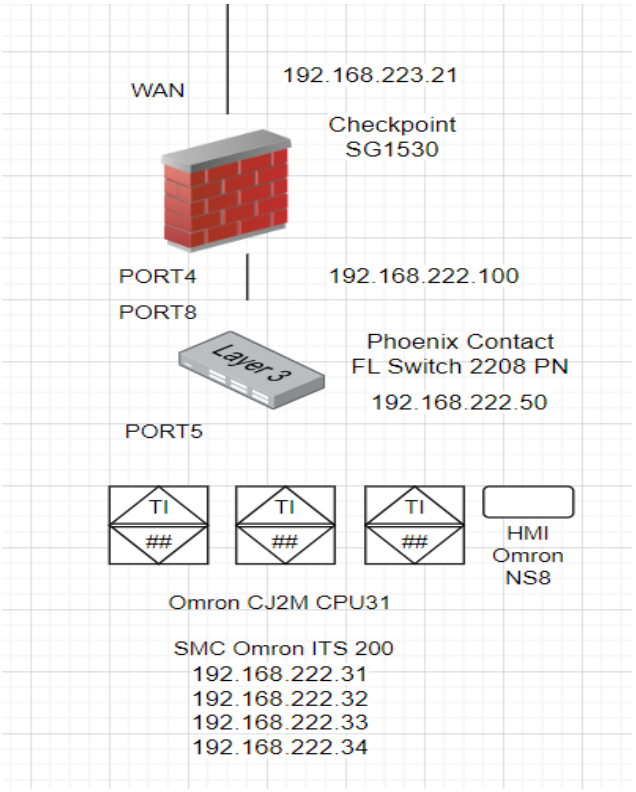
Se gestiona desde la dirección http://192.168.222.50

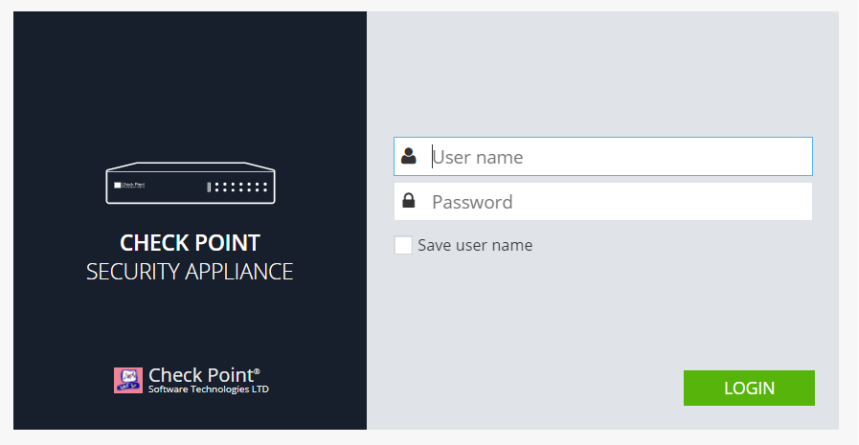

No es seguro | 192.168.222.50
PHOENIX CONTACT
SWITCH2000-dd0ce7
Hello admin
FL SWITCH 2208 PN
+ Information
- Configuration
My Profile
User Management
System
Quick Setup
Network
Service
Profinet Configuration
Port Configuration
VLAN Configuration
Multicast Filtering
Network Redundancy
Security
DHCP Service
Local Events
Quality of Service
+ Diagnostics
Network
IP Address Assignment (?) STATIC
IP Address (?) 192.168.222.50
Network Mask (?) 255.255.255.0
Default Gateway (?) 192.168.222.100
Dynamic Gateway (?) 192.168.222.100
DNS Server 1 (?) 0.0.0.0
DNS Server 2 (?) 0.0.0.0
Management VLAN (?) 1
DHCP Configuration (?) DHCP Services
Hostname Configuration
Name resolution (?) Enable
Hostname (?) SWITCH2000-dd0ce7
ACD Configuration
ACD Mode (?) None
ACD Status Information (?) See ACD status on Device status page
Apply
Revert
Apply&Save
Copyright© by Phoenix Contact GmbH&Co.KG and Other

3.2 CONFIGURACIÓN FIREWALL CHECKPOINT SG1530

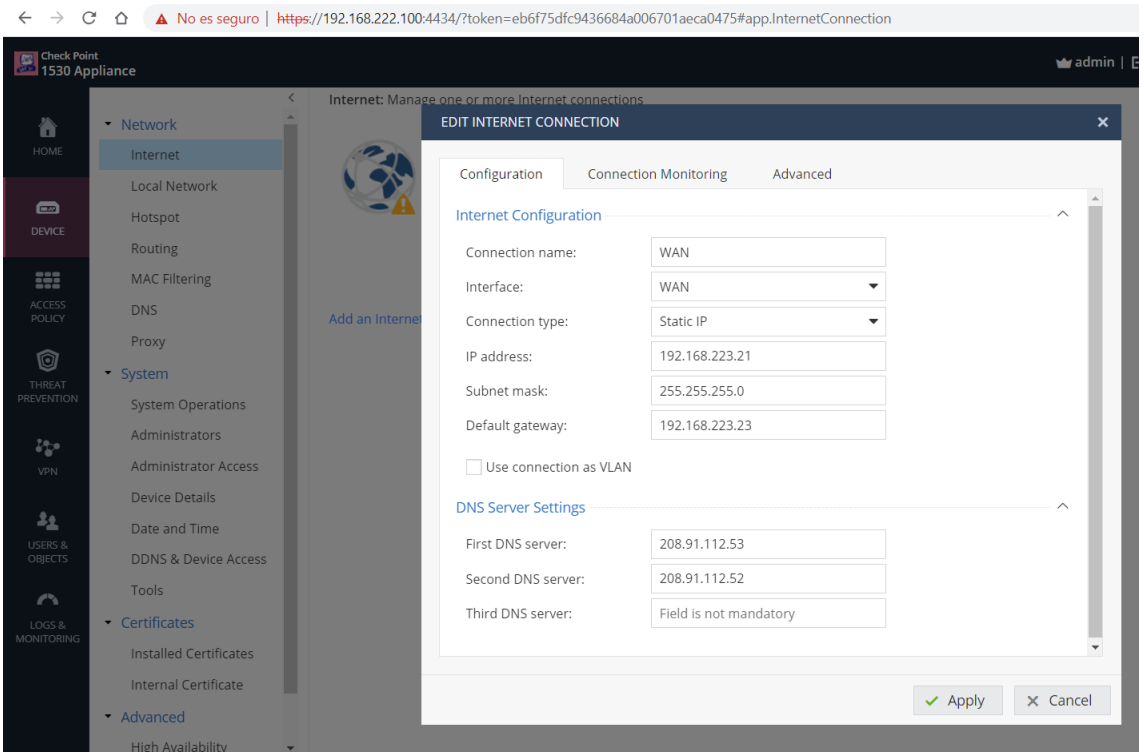
La red Omron está controlada por un firewall Checkpoint SG1530 con 2 subredes, una INT 192.168.222.100 conectada al panel industrial Omron a través del switch Checkpoint y una EXT 192.168.223.21 conectada al firewall principal Fortinet

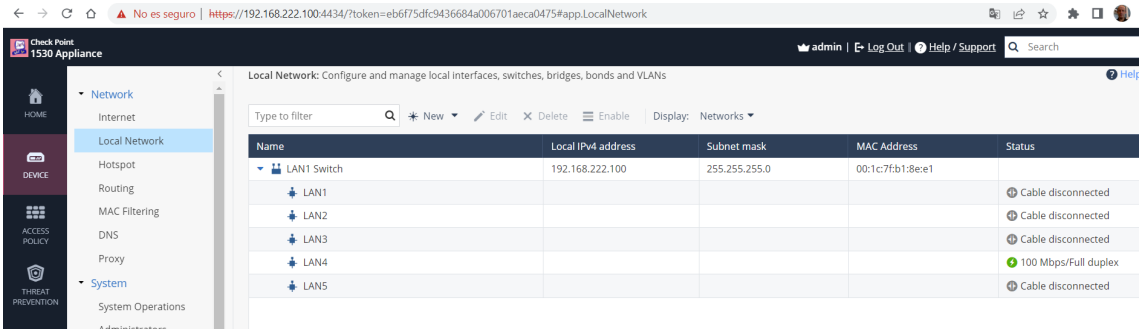
La dirección de gestión es 192.168.222.100:4434 (Atención al puerto)

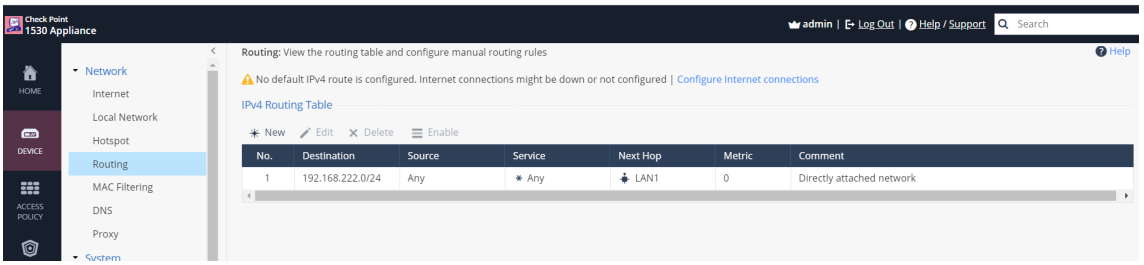




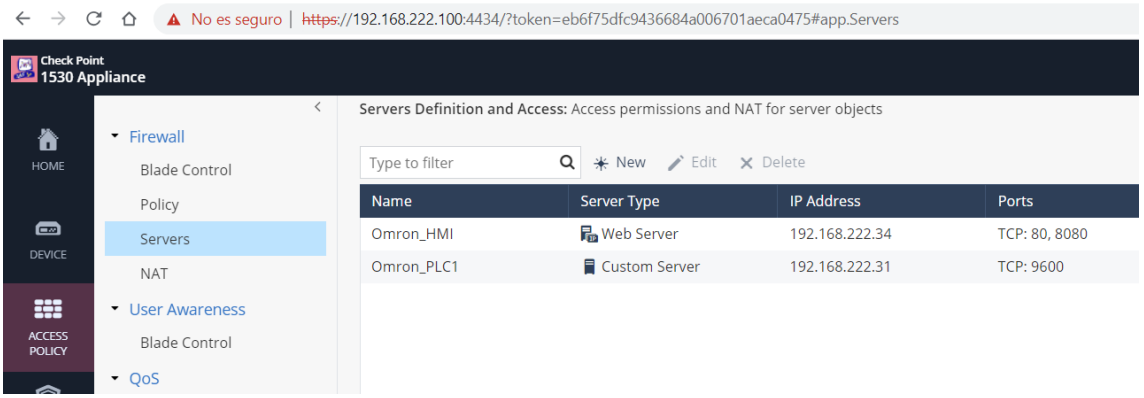
Definir red interna INT (192.168.222.100) y red externa WAN (192.168.223.21)

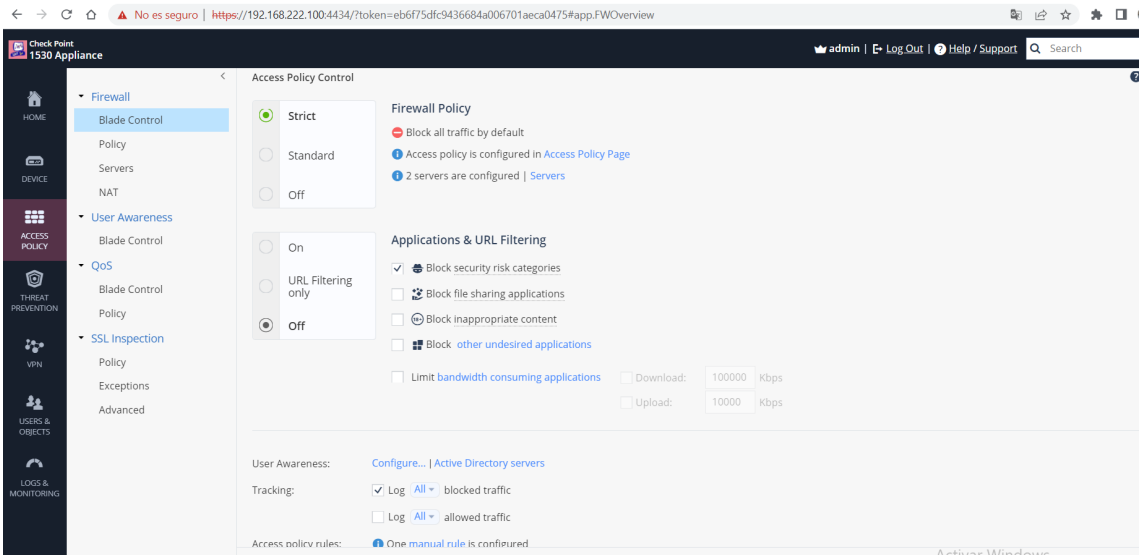




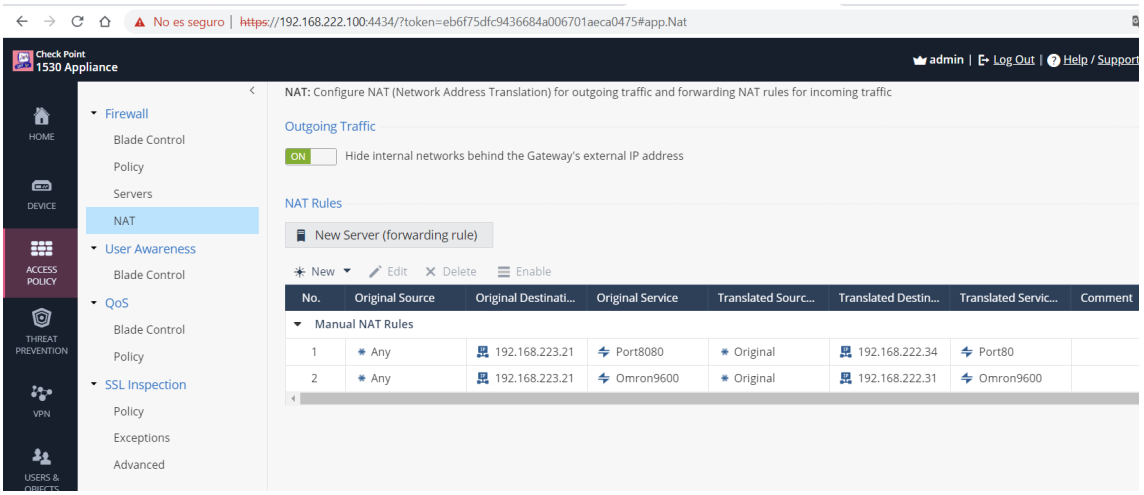


Definir servicios, PLC Omron (port 9600) y pantalla HMI (port 80) en sus respectivos puertos

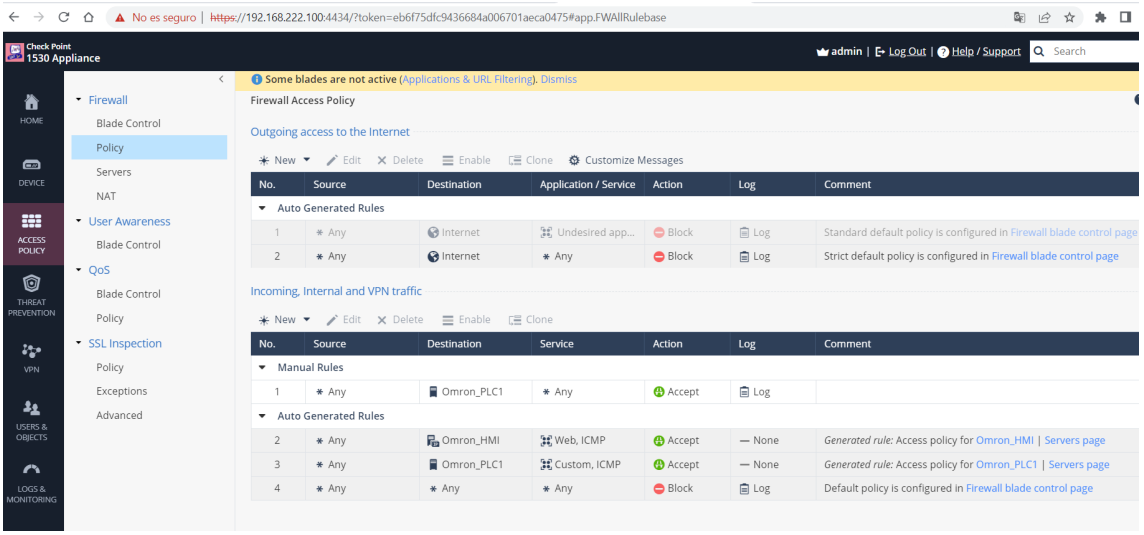




Configurar NAT para redireccionamiento puerto 8080 > puerto 80 puerto 9600 > puerto 9600



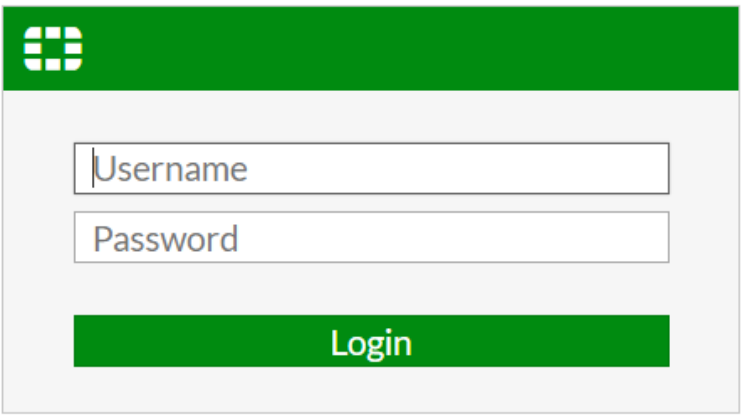
Definir políticas de acceso a PLC y HMI

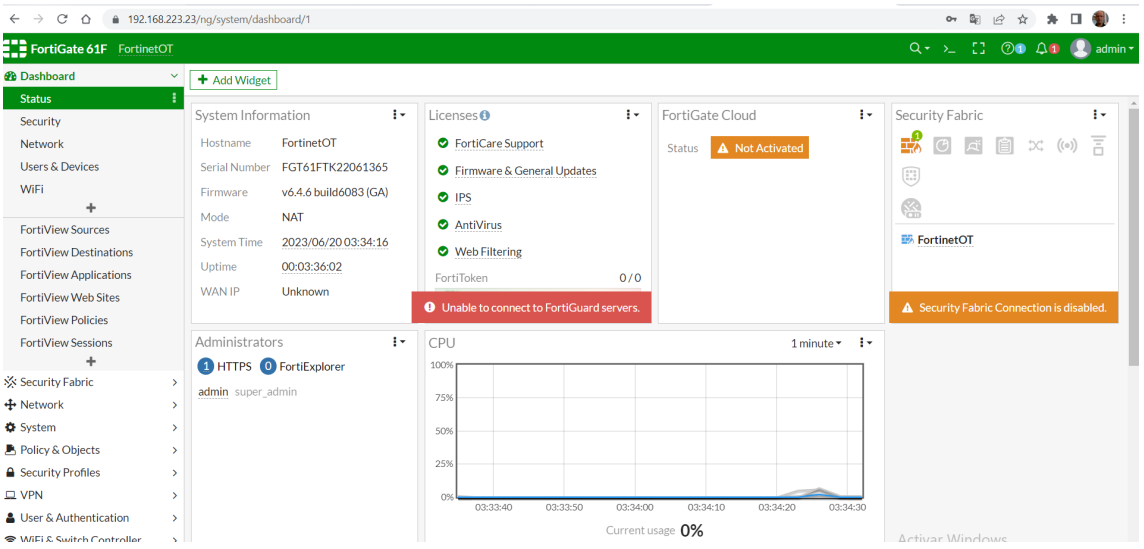


4. Configuración Firewall Fortinet (Fortigate 61F)

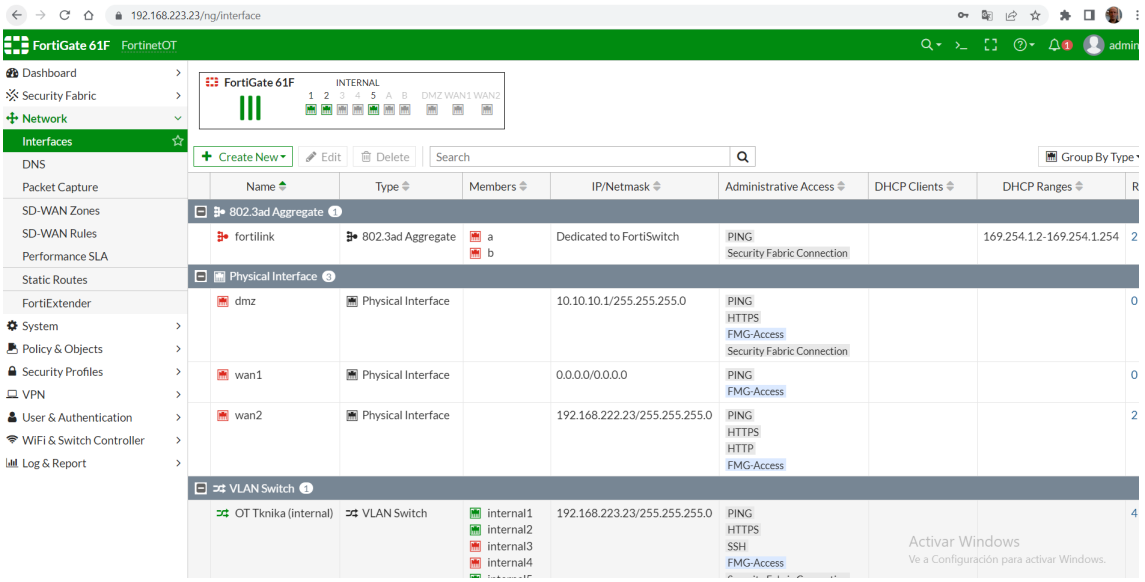
El firewall Fortigate 61S es el primer control de acceso a la red OT y el dispositivo que conecta las redes OT y la red de Tknika (Ciber range)

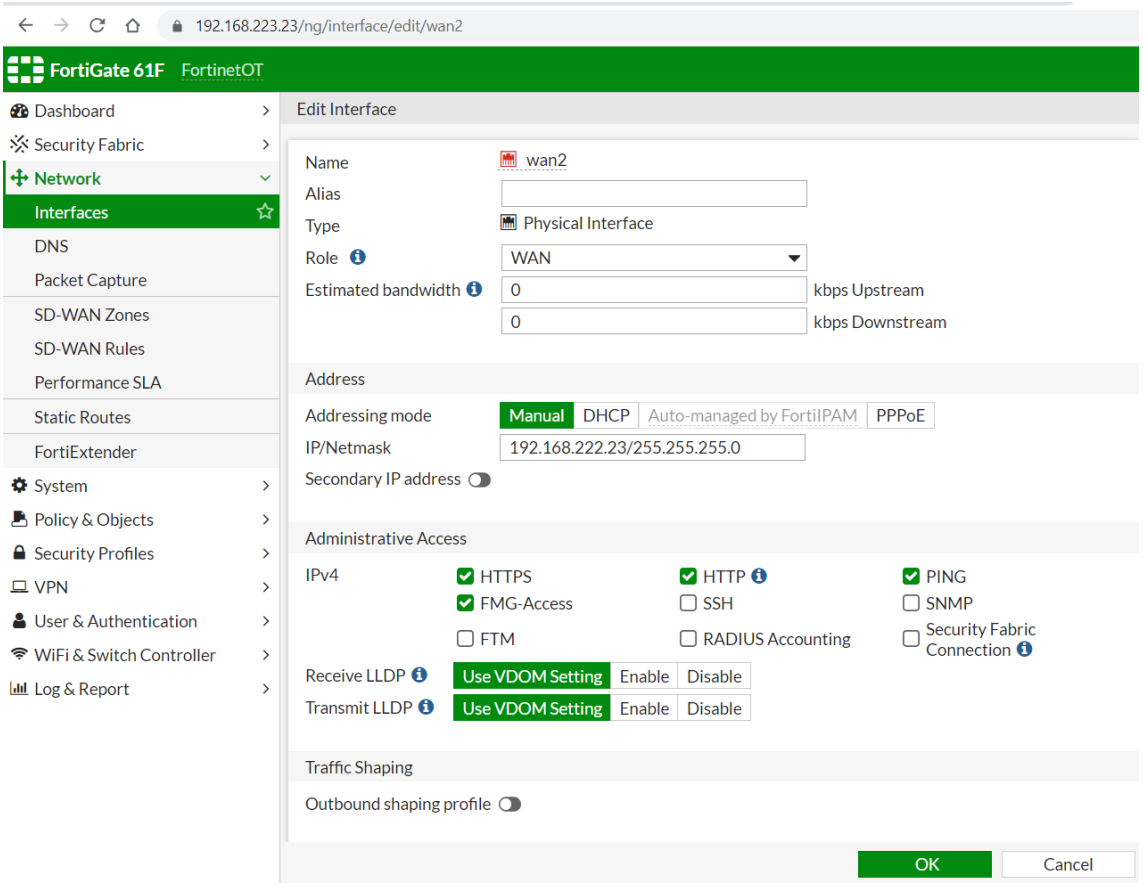
Se gestiona desde https://192.168.222.23

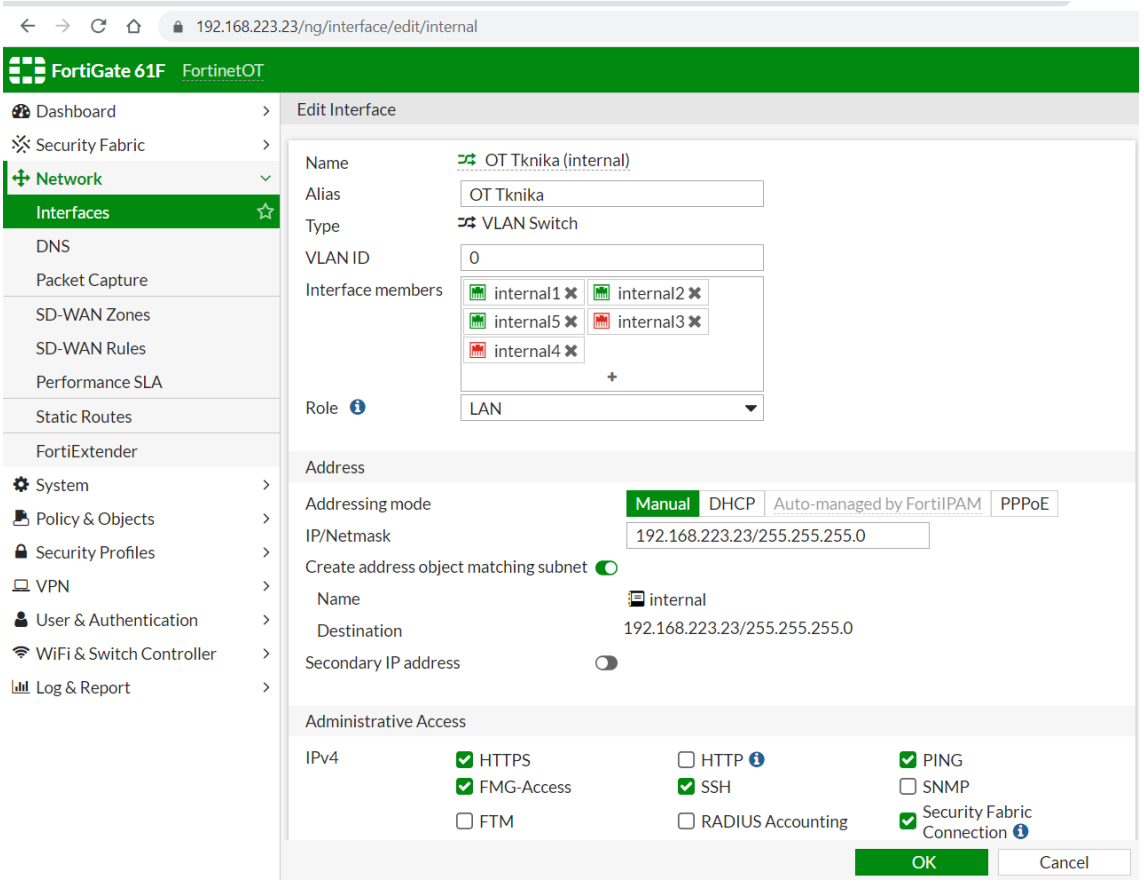




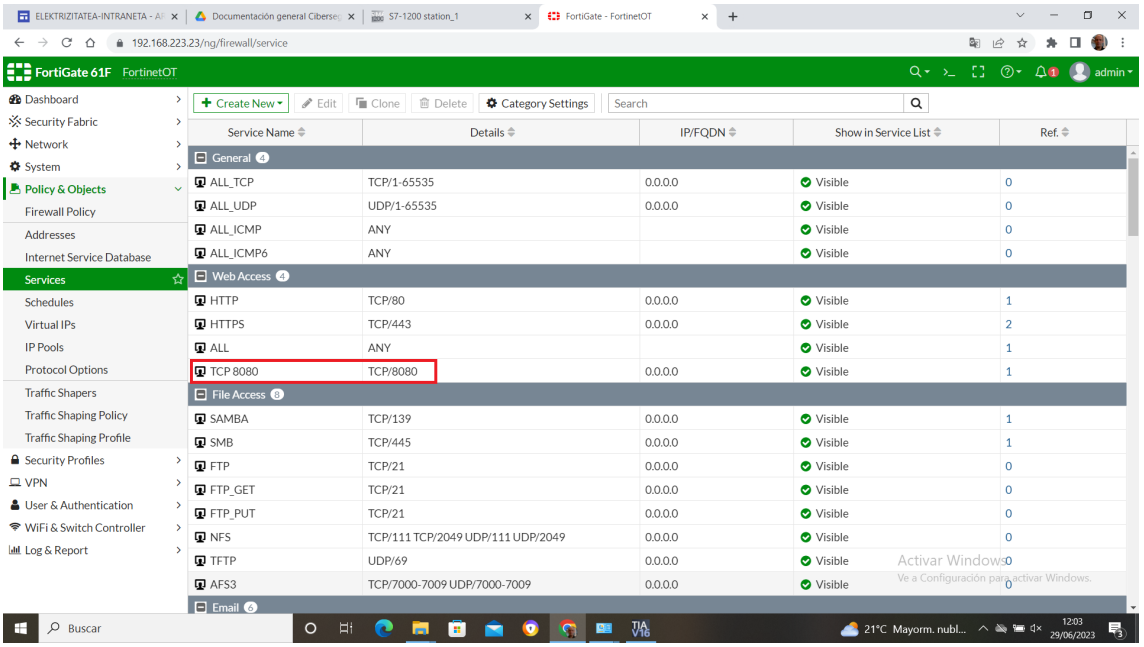
Definir los interfaces WAN2 (192.168.222.23) y LAN interna (192.168.223.23)

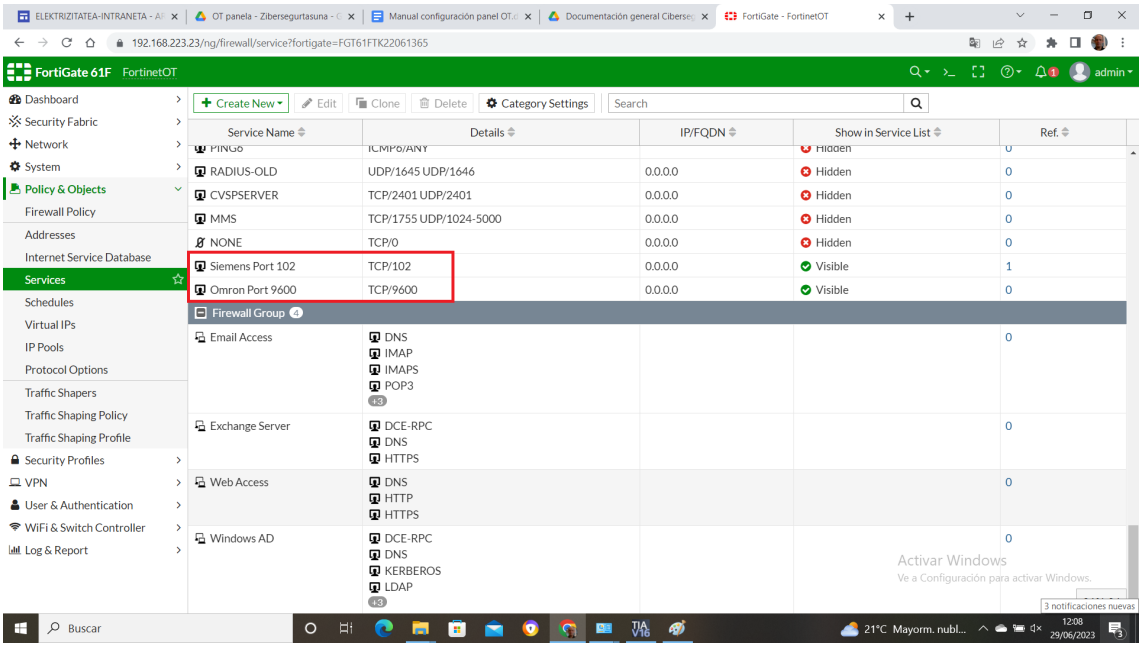




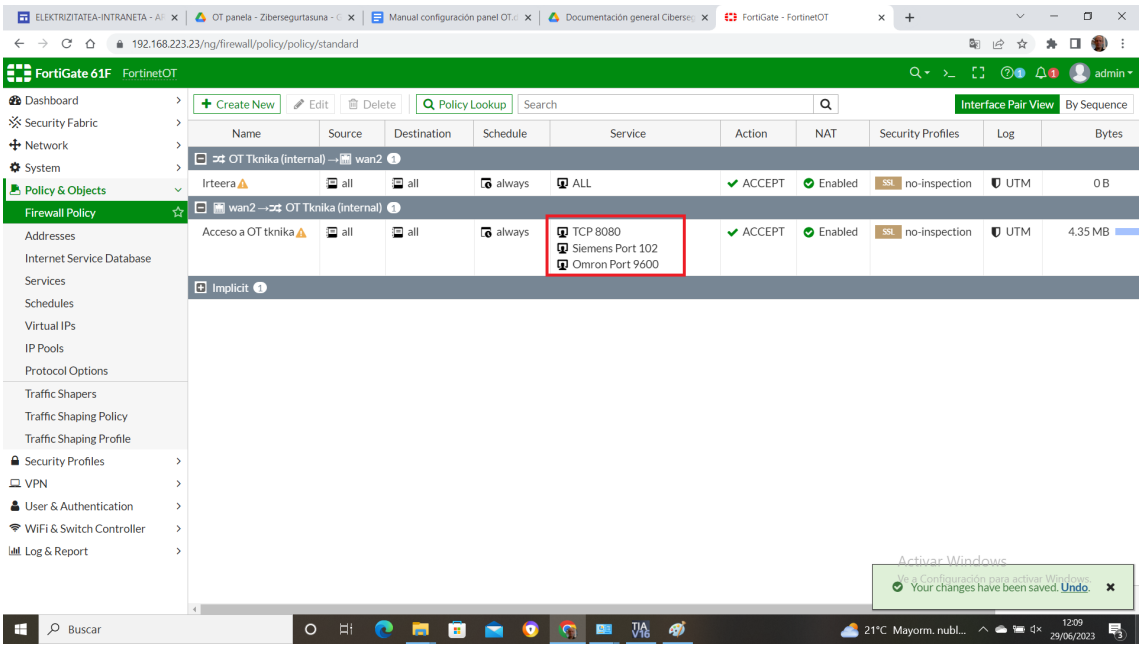

192.168.223.23/ng/interface/edit/internal
FortiGate 61F
FortinetOT
Dashboard
Security Fabric
Network
Interfaces
DNS
Packet Capture
SD-WAN Zones
SD-WAN Rules
Performance SLA
Static Routes
FortiExtender
System
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
Log & Report
Edit Interface
Name
OT Tknika (internal)
Alias
OT Tknika
Type
VLAN Switch
VLAN ID
0
Interface members
internal1
internal2
internal5
internal3
internal4
Role
LAN
Address
Addressing mode
Manual
DHCP
Auto-managed by FortiIPAM
PPPoE
IP/Netmask
192.168.223.23/255.255.255.0
Create address object matching subnet
Name
internal
Destination
192.168.223.23/255.255.255.0
Secondary IP address
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
OK
Cancel

Definir servicios acceso web Port 8080 , Siemens Port 102 y Omron Port 9600



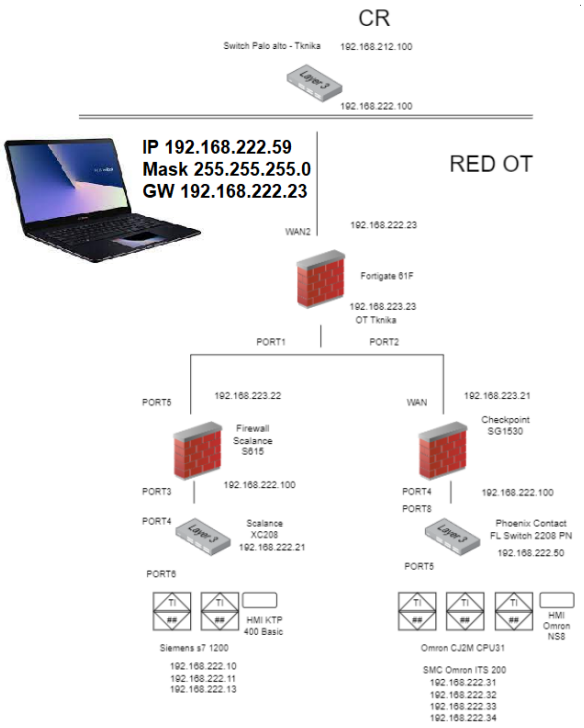


Definir políticas de acceso.

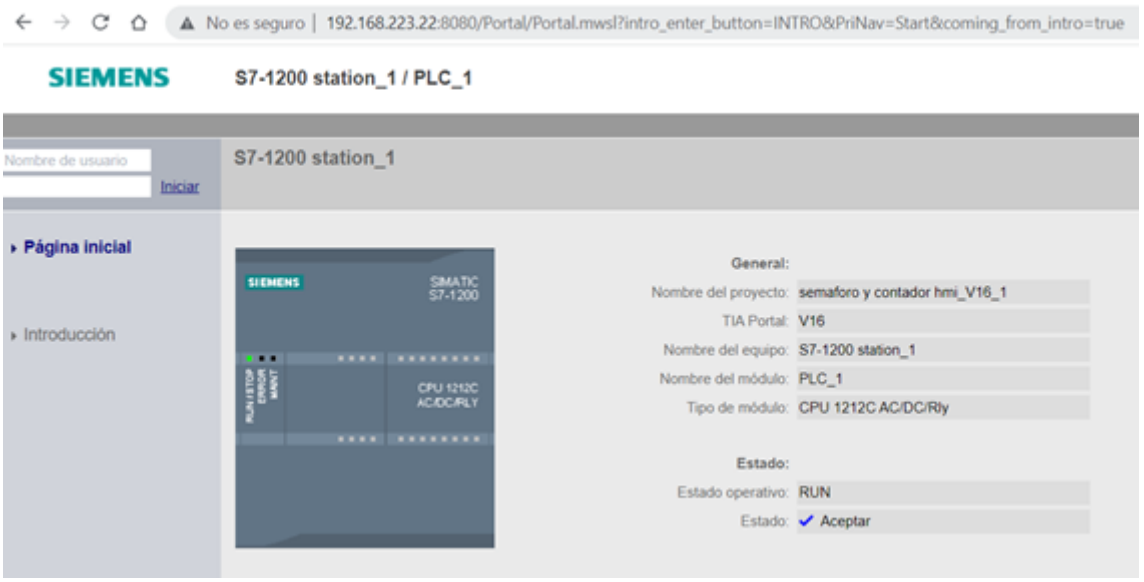


5. COMPROBACIONES FINALES

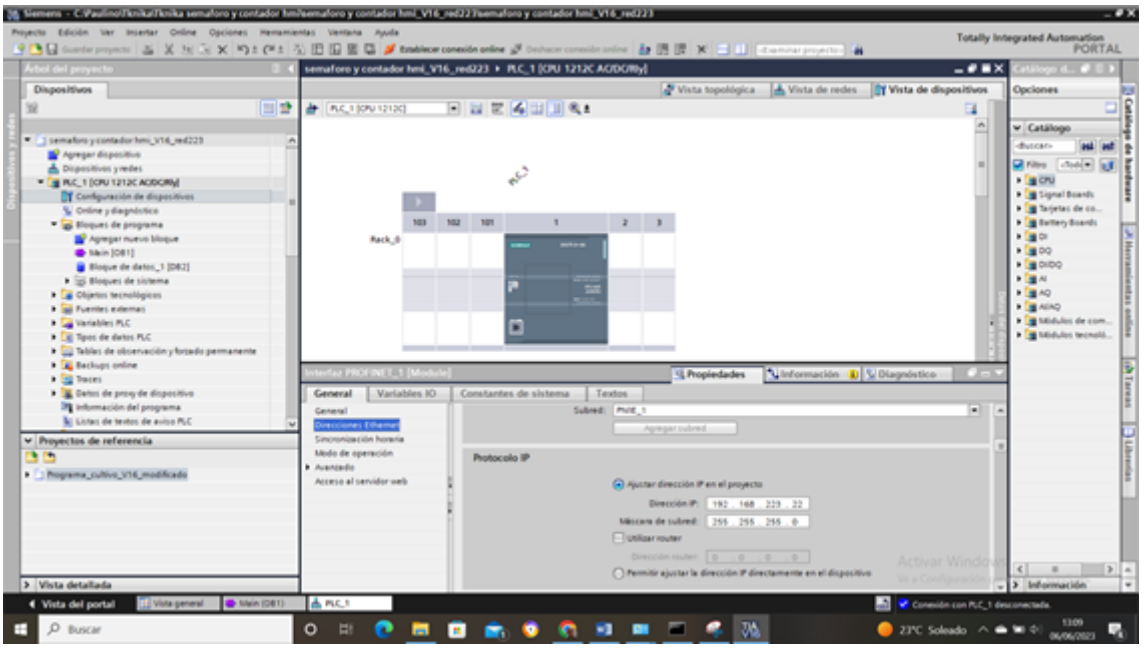
Ubicamos un PC en la parte externa de la red y comprobamos la accesibilidad a todos los servicios configurados.

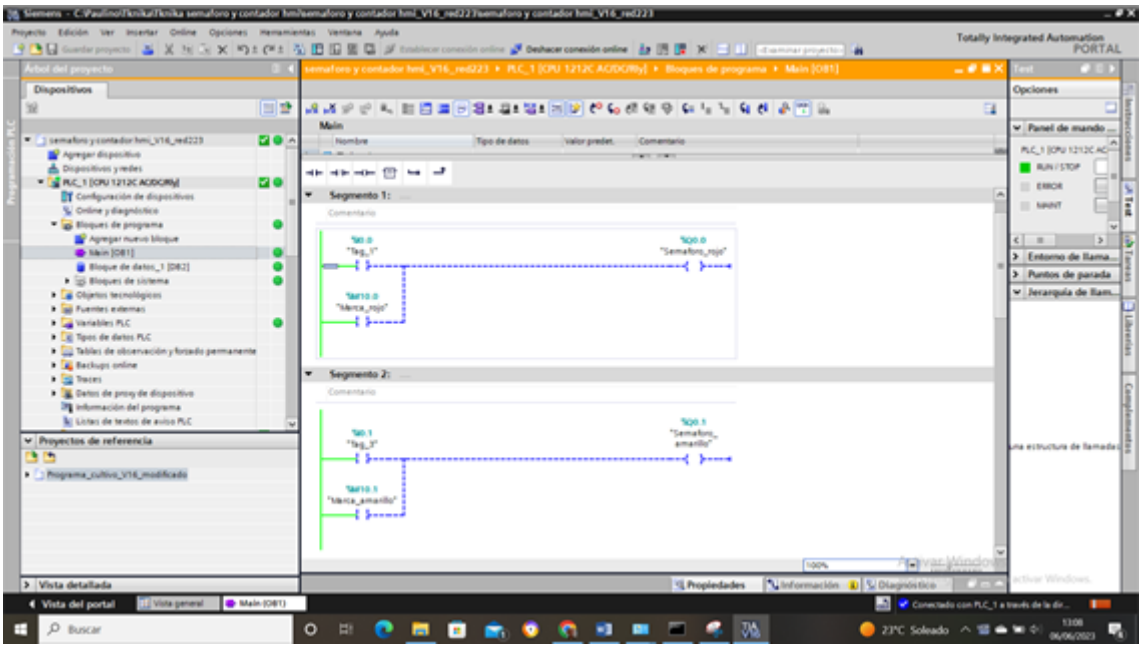


Acceso web al webserver Siemens http://192.168.223.22:8080

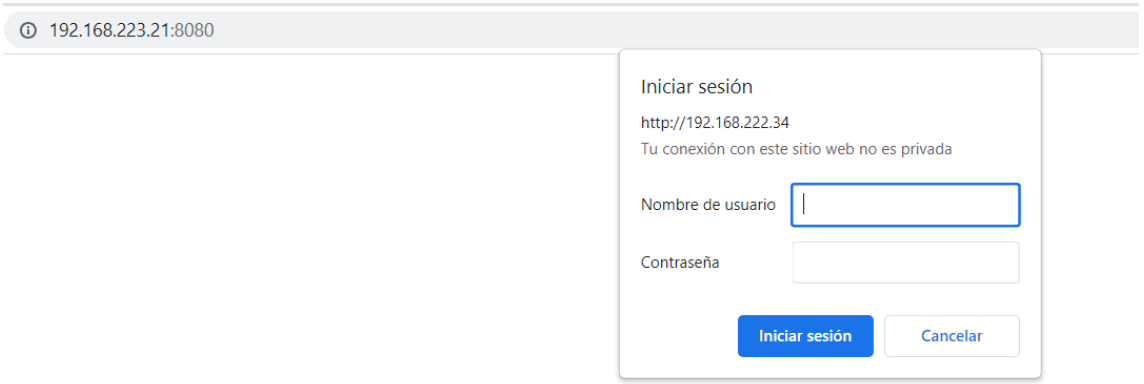


Acceso Tia portal al PLC Siemens en 192.168.223.22





Acceso a la pantalla HMI Omron en http://192.168.223.21:8080



Acceso a los PLC Omron a través del puerto 9600 del firewall Checkpoint

192.168.223.21

No conecta

Tknika

Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre