



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

Configuración panel OT

2022-2023

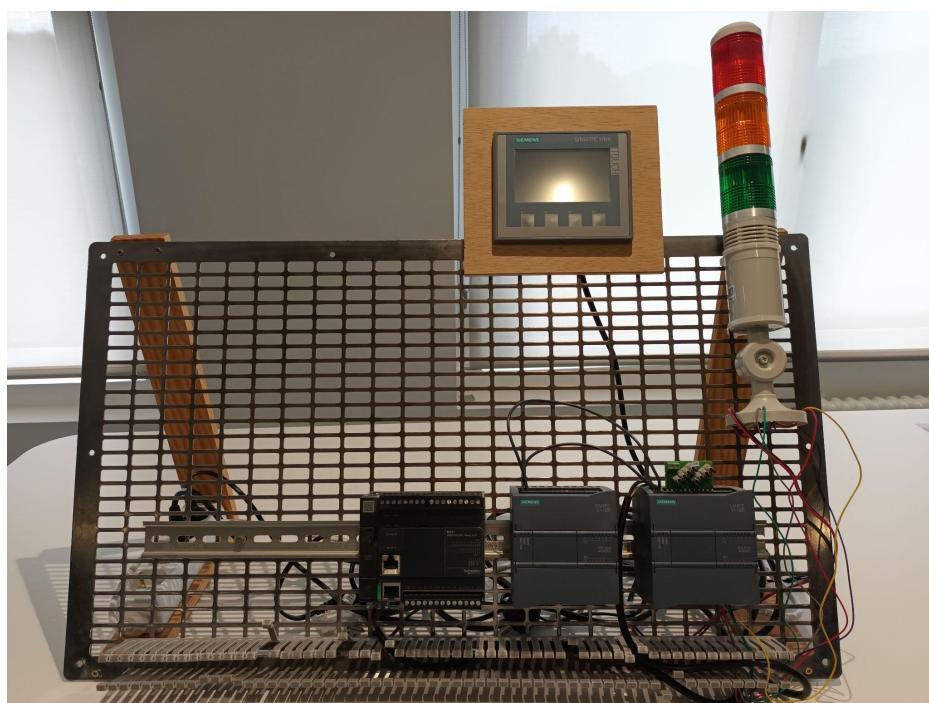


INDICE

1.	<i>Arquitectura del panel OT</i>	1
2.	<i>Acceso a la red Siemens</i>	3
2.1	<i>Configuración switch Scalance XC208</i>	7
2.2	<i>Configuración firewall Scalance S615</i>	8
3.	<i>Acceso a la red Omron ITS200</i>	11
3.1	<i>Configuración switch Phoenix contact</i>	
		13
3.2	<i>Configuración firewall Checkopint</i>	15
4.	<i>Configuración firewall Fortigate 61F</i>	19
5.	<i>Comprobaciones finales</i>	24

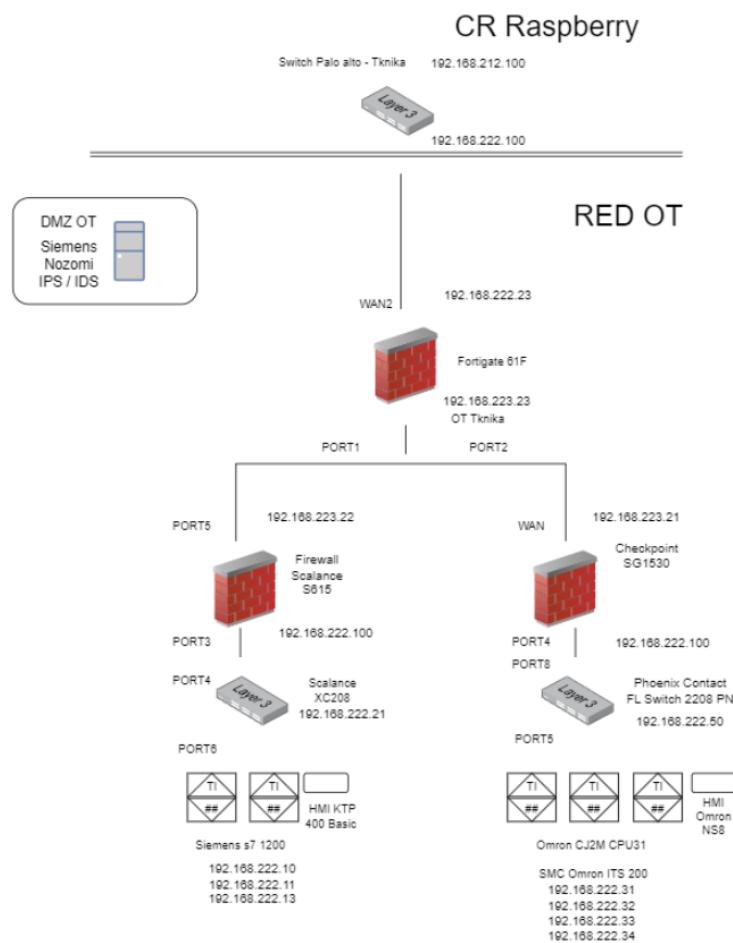
1. ARQUITECTURA DEL PANEL OT

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.



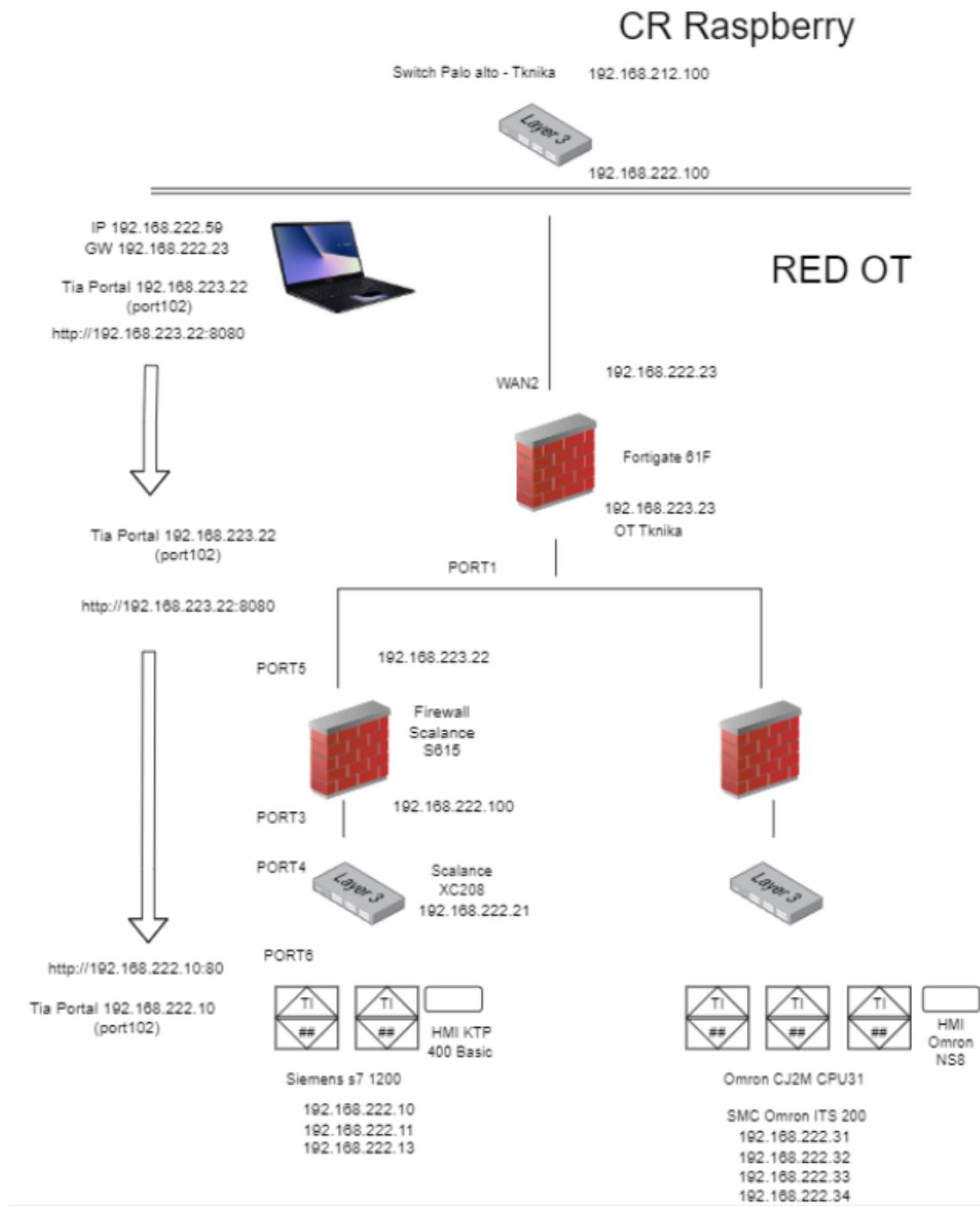
Estos sistemas productivos tienen que ser protegidos con una segmentación adecuada. En la propuesta de segmentación se contemplan 2 subredes cada una protegida por un firewall. El sistema de producción controlado con PLC Siemens se concentra en un switch gestionable Scalance XC208 y se protege con un 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.

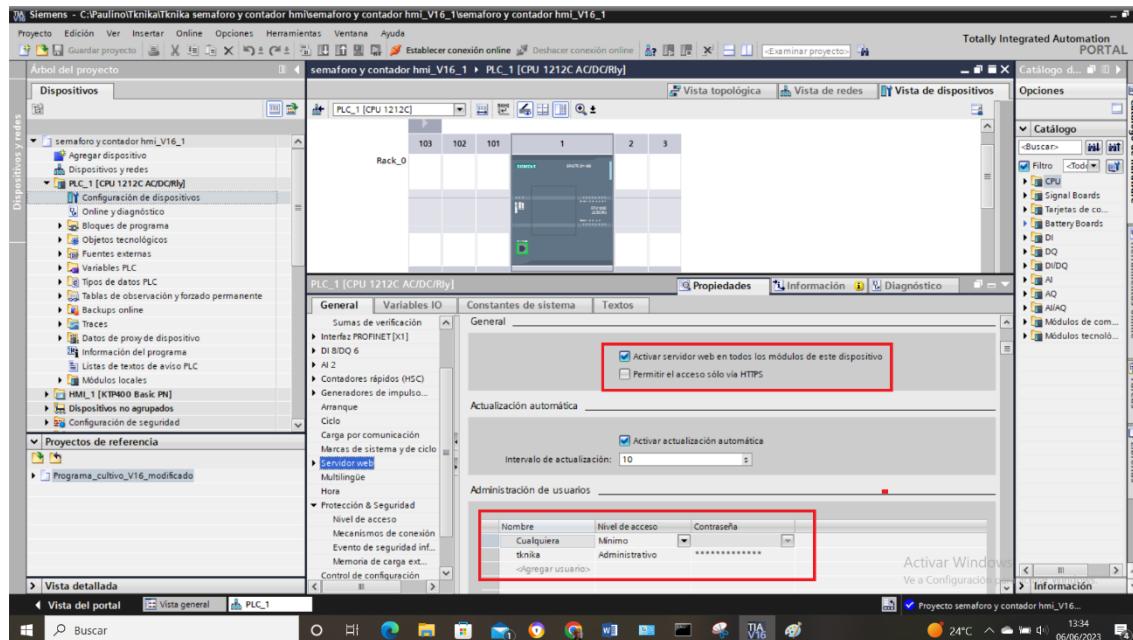


2. ACCESO A LA RED SIEMENS

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.

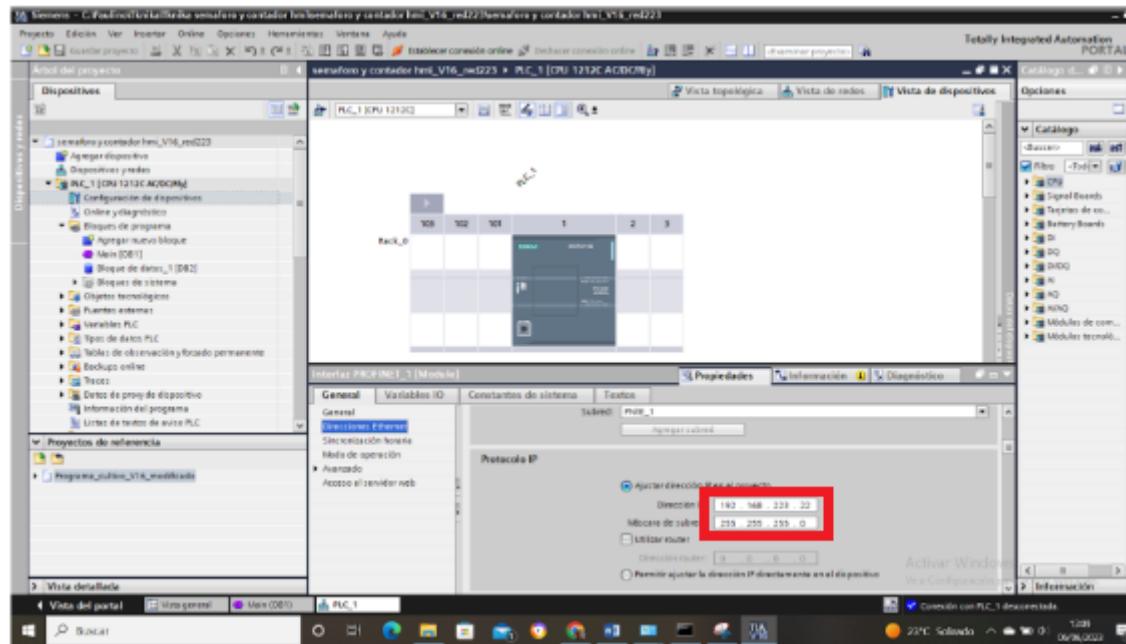


Acceder a través de la IP WAN del cortafuegos <http://192.168.223.22:8080>

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



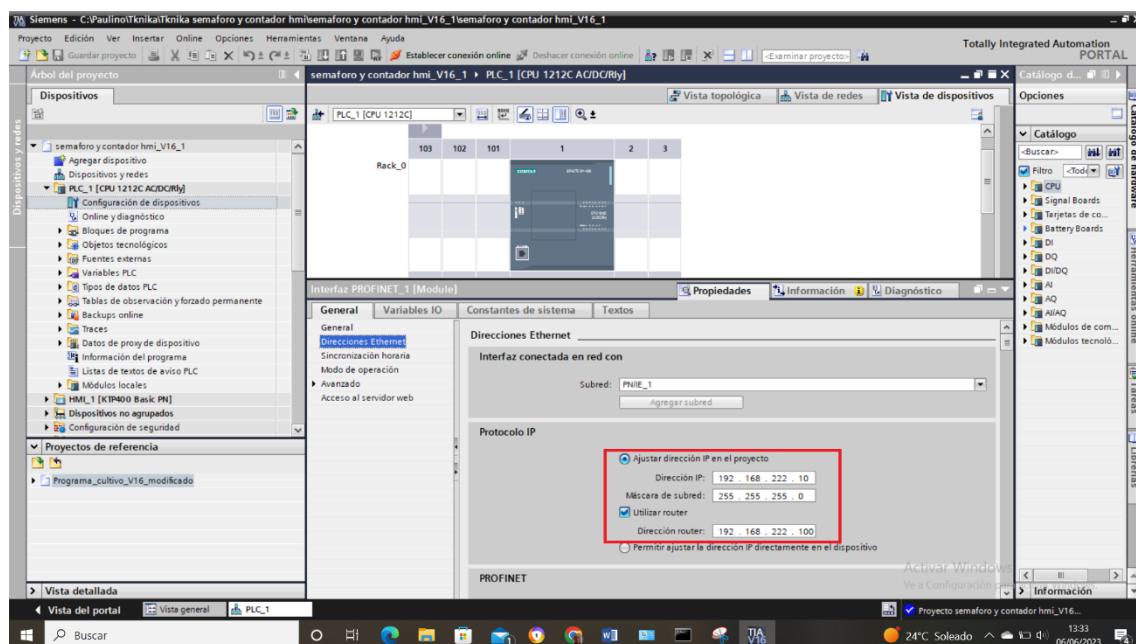
De manera similar accederemos a través de Tia portal. En el proyecto Tia portal configuraremos la IP del PLC apuntando a la IP WAN del cortafuegos. 192.168.223.22 (por defecto puerto 102)



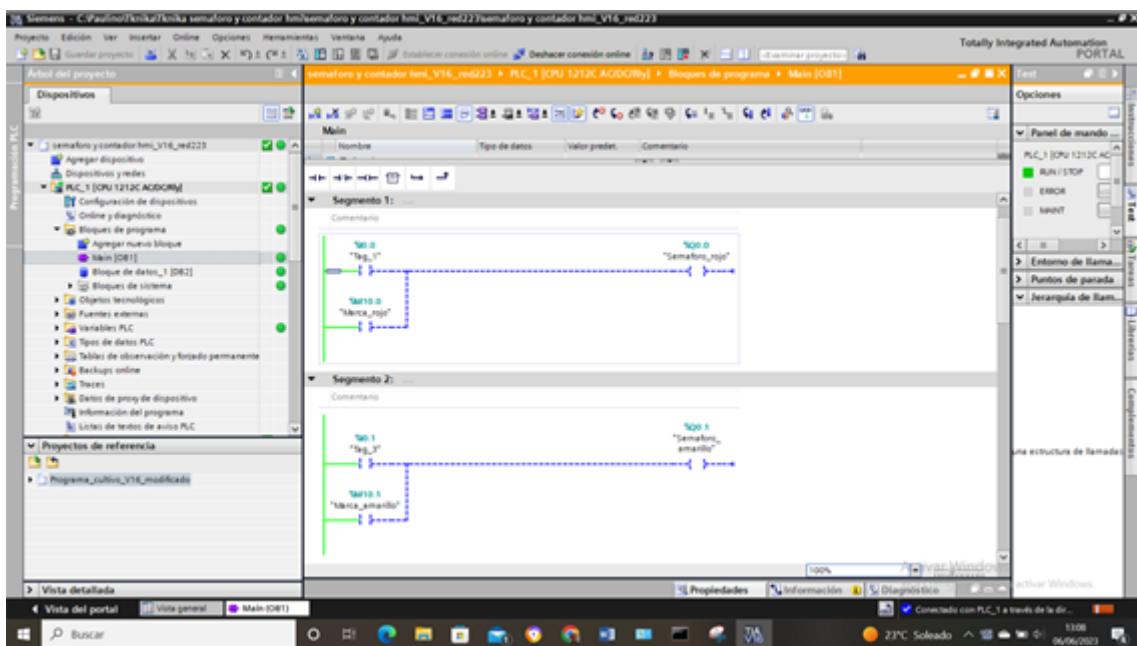
El PLC al estar detrás del cortafuegos en la red interna tendrá cargada una IP local de la red con el gateway de salida apuntando a la IP LAN del cortafuegos.

IP 192.168.222.10

GW 192.168.222.100

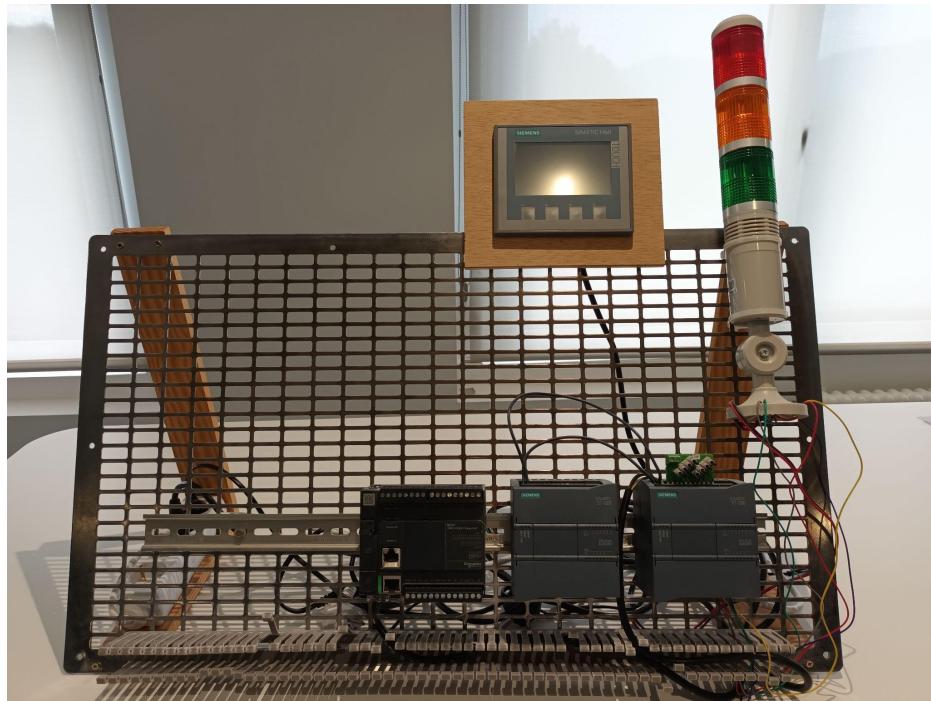


La regla de cortafuegos y la configuración NAPT redirigirán los puertos.



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>

SIEMENS
192.168.222.21/SCALANCE XC208

Welcome admin

Logout

Information

System

Layer 2

Layer 3

Subnets

DHCP Relay Agent

NAT

Security

Connected Subnets Configuration

Overview Configuration Default Gateway

Interface (Name): **vlan1 (vlan1)**

Status: **enabled**

Interface Name: **vlan1**

MAC Address: **d4-f5-27-d2-dc-d4**

DHCP

IP Address: **192.168.222.21**

Subnet Mask: **255.255.255.0**

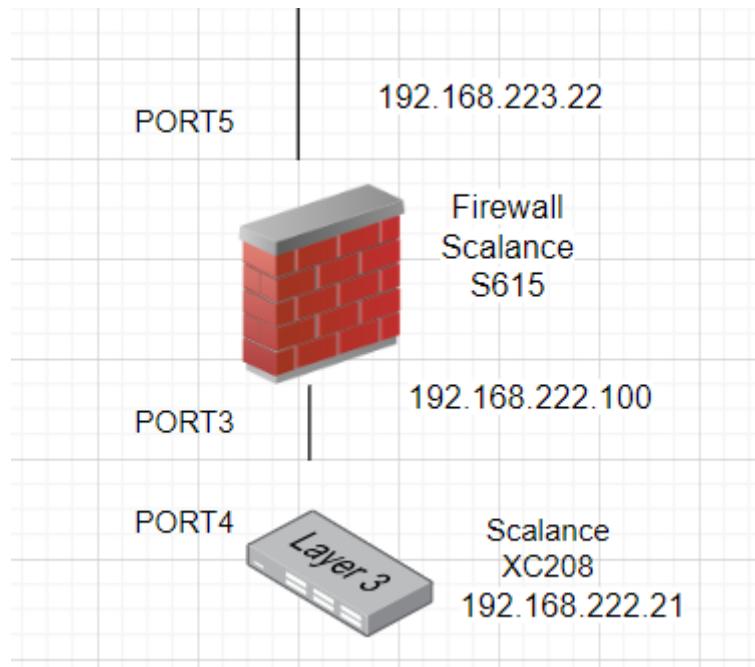
Address Type: **Primary**

TIA Interface

Set Values **Refresh**

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



SIEMENS 192.168.222.100/SCALANCE S615

Welcome admin

[Logout](#)

- ▶ Wizards
- ▶ Information
- ▶ System
- ▶ Interfaces
- ▶ Layer 2
- ▶ Layer 3 (IPv4)
 - ▶ Static Routes
 - ▶ **Subnets**
 - ▶ NAT
 - ▶ VRRPv3
- ▶ Layer 3 (IPv6)
- ▶ Security

Connected Subnets Configuration

[Overview](#) **Configuration**

Interface (Name): **vlan1 (INT)** ▾
Status: **enabled** ▾
Interface Name: **INT**
MAC Address: **d4-f5-27-d6-42-65**
 DHCP
IP Address: **192.168.222.100**
Subnet Mask: **255.255.255.0**
Broadcast IP Address: **192.168.222.255**
Address Type: **Primary**
 TIA Interface
MTU: **1500**

Set Values **Refresh**

Welcome admin

[Logout](#)

- ▶ Wizards
- ▶ Information
- ▶ System
- ▶ Interfaces
- ▶ Layer 2
- ▼ Layer 3 (IPv4)
 - ▶ Static Routes
 - ▶ **Subnets**
 - ▶ NAT
 - ▶ VRRPv3
- ▶ Layer 3 (IPv6)
- ▶ Security

Connected Subnets Configuration

Overview | **Configuration**

Interface (Name): **vlan2 (EXT)** ▾
 Status: **enabled** ▾

Interface Name: EXT
 MAC Address: d4-f5-27-d6-42-69
 DHCP
 IP Address: 192.168.223.22
 Subnet Mask: 255.255.255.0
 Broadcast IP Address: 192.168.223.255
 Address Type: Primary
 TIA Interface
 MTU: 1500

[Set Values](#) | [Refresh](#)

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

Welcome admin

[Logout](#)

- ▶ Wizards
- ▶ Information
- ▶ System
- ▶ Interfaces
- ▶ Layer 2
- ▼ Layer 3 (IPv4)
 - ▶ Static Routes
 - ▶ Subnets
 - ▶ **NAT**
 - ▶ VRRPv3
- ▶ Layer 3 (IPv6)
- ▶ Security

IP Network Address Port Translation (NAPT) (Port Forwarding)

NAT General | **Masquerading** | **NAPT** | **Source NAT** | **NETMAP**

Source Interface: **vlan1 (INT)** ▾
 Traffic Type: **TCP** ▾
 Use Interface IP from Source Interface
 Destination IP Address: 192.168.222.100
 Destination Port: 100
 Translated Destination IP Address:
 Translated Destination Port: 100

Select	Source Interface	Traffic Type	Interface IP	Destination IP	Destination Port	Translated Destination IP	Translated Destination Port
<input type="checkbox"/>	vlan2	TCP	<input checked="" type="checkbox"/>	192.168.223.22	8080	192.168.222.10	80
<input type="checkbox"/>	vlan2	TCP	<input checked="" type="checkbox"/>	192.168.223.22	102	192.168.222.10	102

2 entries.

[Create](#) | [Delete](#) | [Refresh](#)

Welcome admin

[Logout](#)

- ▶ Wizards
- ▶ Information
- ▶ System
- ▶ Interfaces
- ▶ Layer 2
- ▶ Layer 3 (IPv4)
- ▶ Layer 3 (IPv6)
- ▼ Security
 - ▶ Users
 - ▶ Passwords
 - ▶ AAA
 - ▶ Certificates
 - ▶ **Firewall**
 - ▶ IPsec VPN
 - ▶ OpenVPN
 - ▶ Brute Force Prevention

Internet Protocol (IP) Services

General	Predefined	Dynamic Rules	IP Services	ICMP Services	IP Protocols	IP Rules
Service Name: <input type="text"/>						
Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)		
<input type="checkbox"/>	HTTP	TCP	*	80		
<input type="checkbox"/>	TiaPortal	TCP	*	102		
<input type="checkbox"/>	webserver443	TCP	*	443		

3 entries.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Welcome admin

[Logout](#)

- ▶ Wizards
- ▶ Information
- ▶ System
- ▶ Interfaces
- ▶ Layer 2
- ▶ Layer 3 (IPv4)
- ▶ Layer 3 (IPv6)
- ▼ Security
 - ▶ Users
 - ▶ Passwords
 - ▶ AAA
 - ▶ Certificates
 - ▶ **Firewall**
 - ▶ IPsec VPN
 - ▶ OpenVPN
 - ▶ Brute Force Prevention

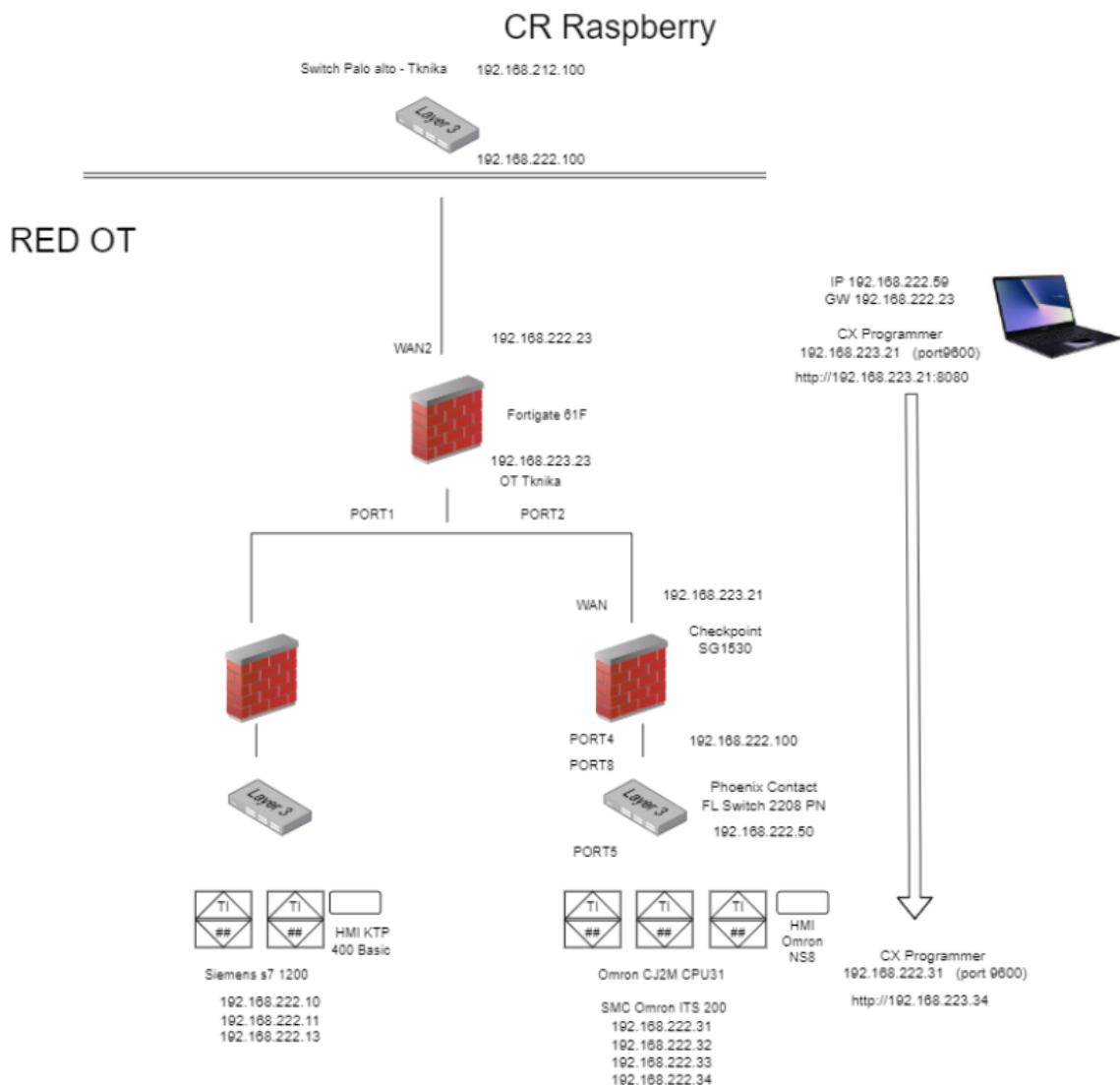
Internet Protocol (IP) Rules

General	Predefined	Dynamic Rules	IP Services	ICMP Services	IP Protocols	IP Rules							
IP Version: IPv4	Rule Set: -	<input checked="" type="checkbox"/> show all	Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence	Acl
2 entries.													
Create Delete Set Values Refresh													

2 entries.

3. ACCESO A LA RED OMRON ITS200

El acceso a la red Omron está configurado de tal manera que las IP de los PLC quedan “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.

← → C □ ▲ No es seguro | 192.168.223.21:8080/monitor.htm

Commissioning SMC International Training

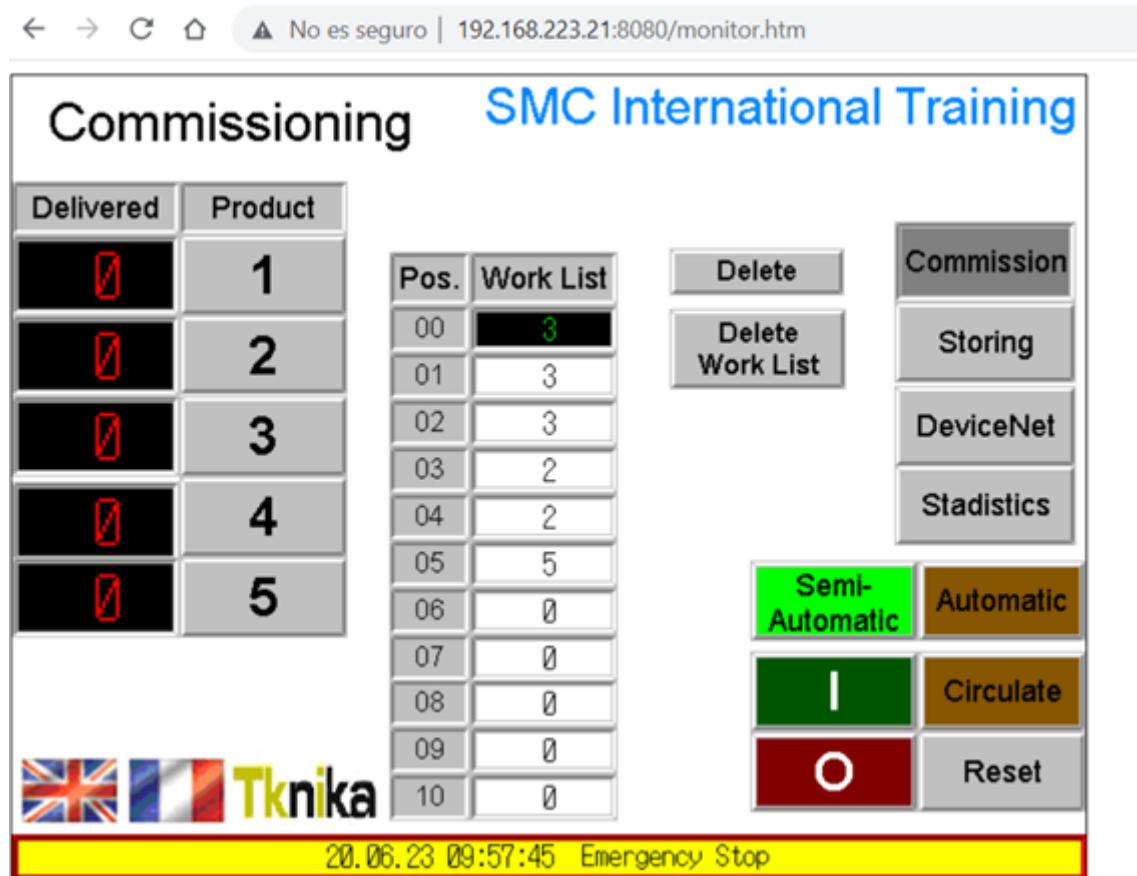
Delivered	Product
0	1
0	2
0	3
0	4
0	5

Pos.	Work List
00	3
01	3
02	3
03	2
04	2
05	5
06	0
07	0
08	0
09	0
10	0

Commission
Storing
DeviceNet
Statistics

Semi-Automatic **Automatic**
I **Circulate**
O **Reset**

20.06.23 09:57:45 Emergency Stop



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



SWITCH2000-dd0ce7 Hello admin

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

Buttons: Apply, Revert, Apply&Save

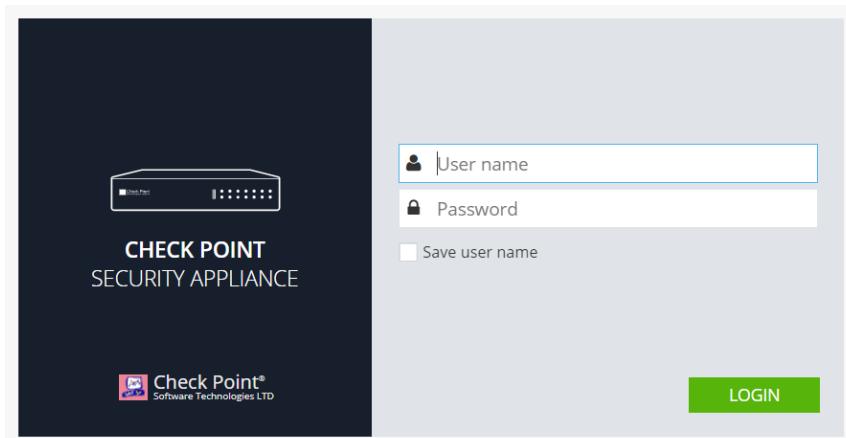
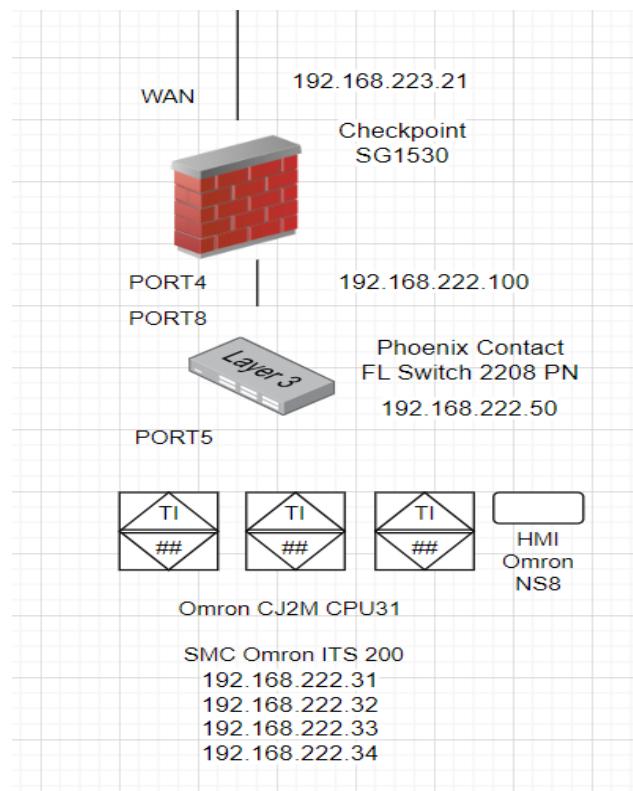
Copyright© by Phoenix Contact GmbH&Co.KG and Other

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)

Internet Configuration

- Connection name: WAN
- Interface: WAN
- Connection type: Static IP
- IP address: 192.168.223.21
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.223.23
- Use connection as VLAN

DNS Server Settings

- First DNS server: 208.91.112.53
- Second DNS server: 208.91.112.52
- Third DNS server: Field is not mandatory

Name	Local IPv4 address	Subnet mask	MAC Address	Status
LAN1 Switch	192.168.222.100	255.255.255.0	00:1c:7f:b1:8e:e1	Cable disconnected
LAN1				Cable disconnected
LAN2				Cable disconnected
LAN3				Cable disconnected
LAN4				100 Mbps/Full duplex
LAN5				Cable disconnected

No.	Destination	Source	Service	Next Hop	Metric	Comment
1	192.168.222.0/24	Any	* Any	LAN1	0	Directly attached network

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

Name	Server Type	IP Address	Ports
Omron_HMI	Web Server	192.168.222.34	TCP: 80, 8080
Omron_PLCL	Custom Server	192.168.222.31	TCP: 9600

Configurar NAT para redireccionamiento puerto 8080 > puerto 80 puerto 9600

> puerto 9600

No.	Original Source	Original Destinati...	Original Service	Translated Sour...	Translated Destin...	Translated Servic...	Comment
1	* Any	192.168.223.21	Port8080	* Original	192.168.223.34	Port80	
2	* Any	192.168.223.21	Omron9600	* Original	192.168.223.31	Omron9600	

Definir políticas de acceso a PLC y HMI

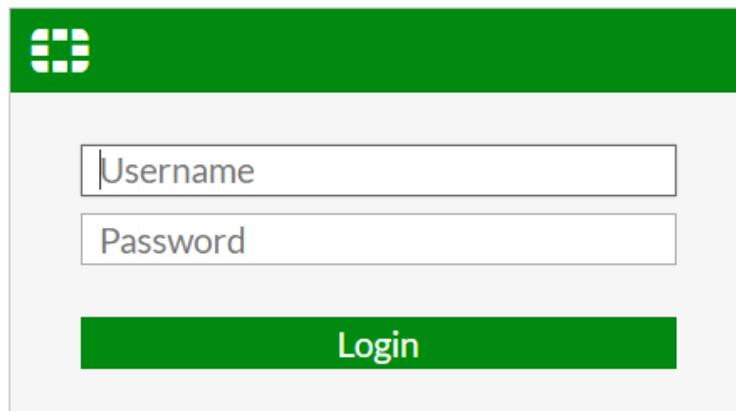
No.	Source	Destination	Action	Log	Comment
1	* Any	Internet	Block	Log	Standard default policy is configured in Firewall blade control page
2	* Any	Internet	Block	Log	Strict default policy is configured in Firewall blade control page

No.	Source	Destination	Action	Log	Comment
1	* Any	Omron_PLC1	Accept	Log	
2	* Any	Omron_HMI	Accept	None	Generated rule: Access policy for Omron_HMI Servers page
3	* Any	Omron_PLC1	Accept	None	Generated rule: Access policy for Omron_PLC1 Servers page
4	* Any	* Any	Block	Log	Default policy is configured in Firewall blade control page

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>



192.168.223.23/ng/system/dashboard/1

FortiGate 61F FortinetOT

Dashboard + Add Widget

Status

System Information

Hostname	FortinetOT
Serial Number	FGT61FTK22061365
Firmware	v6.4.6 build6083 (GA)
Mode	NAT
System Time	2023/06/20 03:34:16
Uptime	00:03:36:02
WAN IP	Unknown

Licenses

- FortiCare Support
- Firmware & General Updates
- IPS
- AntiVirus
- Web Filtering

FortiGate Cloud

Status: Not Activated

Security Fabric

Unable to connect to FortiGuard servers.

Security Fabric Connection is disabled.

Administrators

1 HTTPS	0 FortiExplorer
admin	super_admin

CPU 1 minute

Current usage: 0%

FortiView Sources

FortiView Destinations

FortiView Applications

FortiView Web Sites

FortiView Policies

FortiView Sessions

Security Fabric

Network

System

Policy & Objects

Security Profiles

VPN

User & Authentication

WIFI & Switch Controller

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

The screenshot shows the FortiGate 61F interface configuration. The main menu on the left is under the Network tab, specifically the Interfaces section. The interface list table has columns for Name, Type, Members, IP/Netmask, Administrative Access, DHCP Clients, and DHCP Ranges.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
802.3ad Aggregate	802.3ad Aggregate	a, b	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254
Physical Interface	Physical Interface					
dmz	Physical Interface		10.10.1/255.255.255.0	PING HTTPS FMG-Access Security Fabric Connection		0
wan1	Physical Interface		0.0.0.0/0.0.0	PING FMG-Access		0
wan2	Physical Interface		192.168.222.23/255.255.255.0	PING HTTPS HTTP FMG-Access		2
VLAN Switch	VLAN Switch	internal1, internal2, internal3, internal4	192.168.223.23/255.255.255.0	PING HTTPS SSH FMG-Access		4

The screenshot shows the 'Edit Interface' dialog for the wan2 interface. The interface is defined as a Physical Interface of type WAN. The IP/Netmask is set to 192.168.222.23/255.255.255.0. The 'Addressing mode' is set to Manual. The 'Administrative Access' section includes checkboxes for HTTPS, FMG-Access, HTTP, PING, SSH, RADIUS Accounting, and Security Fabric Connection. The 'Traffic Shaping' section includes an 'Outbound shaping profile' toggle.

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

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	<input checked="" type="checkbox"/> HTTPS	<input type="checkbox"/> HTTP <small>i</small>	<input checked="" type="checkbox"/> PING
	<input checked="" type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
	<input type="checkbox"/> FTP	<input type="checkbox"/> RADIUS Accounting	<input checked="" type="checkbox"/> Security Fabric Connection <small>i</small>

OK Cancel

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

The screenshot shows the Fortinet Fortigate 61F interface. In the left sidebar, under 'Services', the 'Web Access' tab is selected. A new service entry for 'TCP 8080' is being created, highlighted with a red box. The service details are as follows:

Service Name	Protocol	Port	Details	IP/FQDN	Show in Service List	Ref.
TCP 8080	TCP	8080		0.0.0.0	Visible	1

The screenshot shows the Fortinet Fortigate 61F interface. In the left sidebar, under 'Services', the 'Web Access' tab is selected. Two services are listed and highlighted with a red box:

Service Name	Protocol	Port	Details	IP/FQDN	Show in Service List	Ref.
Siemens Port 102	TCP	102		0.0.0.0	Visible	1
Omron Port 9600	TCP	9600		0.0.0.0	Visible	0

Definir políticas de acceso.

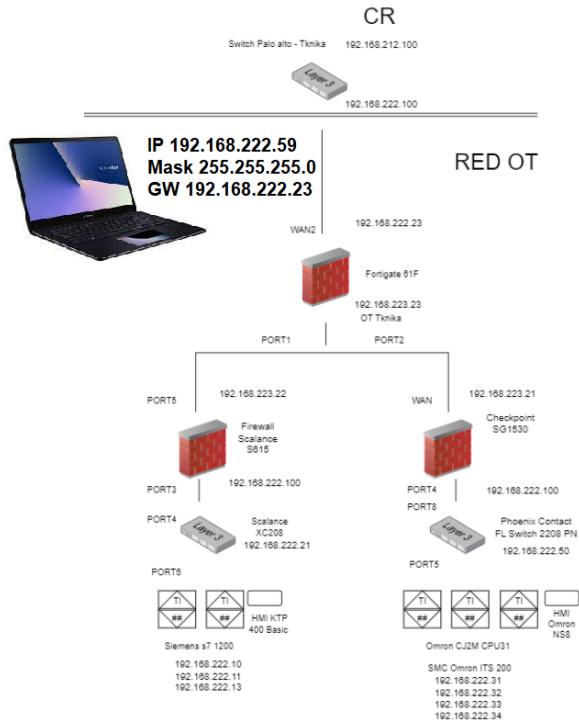
The screenshot shows the Fortinet Fortigate 61F Firewall Policy configuration interface. The 'Firewall Policy' tab is selected. A policy named 'Irteera' is highlighted with a red box. This policy has two rules:

Source	Destination	Action	NAT	Security Profiles	Log	Bytes
all	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
TCP 8080	Siemens Port 102	ACCEPT	Enabled	no-inspection	UTM	4.35 MB

Other policies listed include 'Accesso a OT tknika' and 'Implicit'.

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

← → ⌂ ⌃ ▲ No es seguro | 192.168.223.22:8080/Portal/Portal.mwsl?intro_enter_button=INTRO&PriNav=Start&coming_from_intro=true

SIEMENS S7-1200 station_1 / PLC_1

Nombre de usuario Iniciar

» Página inicial

» Introducción

S7-1200 station_1

SIEMENS SIMATIC S7-1200

MAIN STOP EMERG STOP

PLC1212C AC/DC/RLY

General:

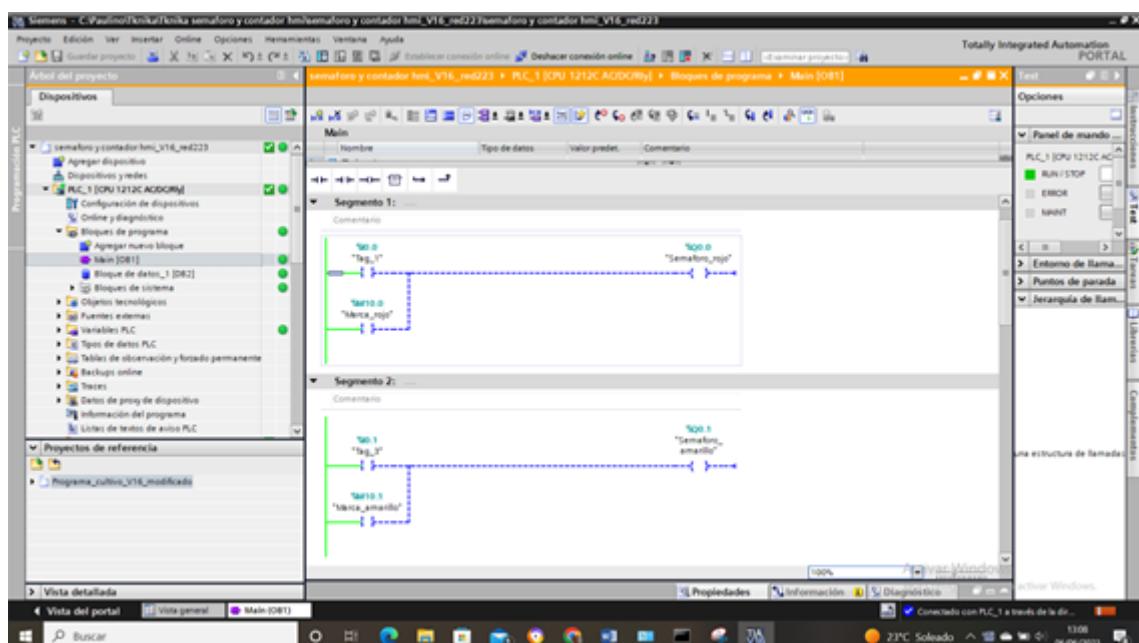
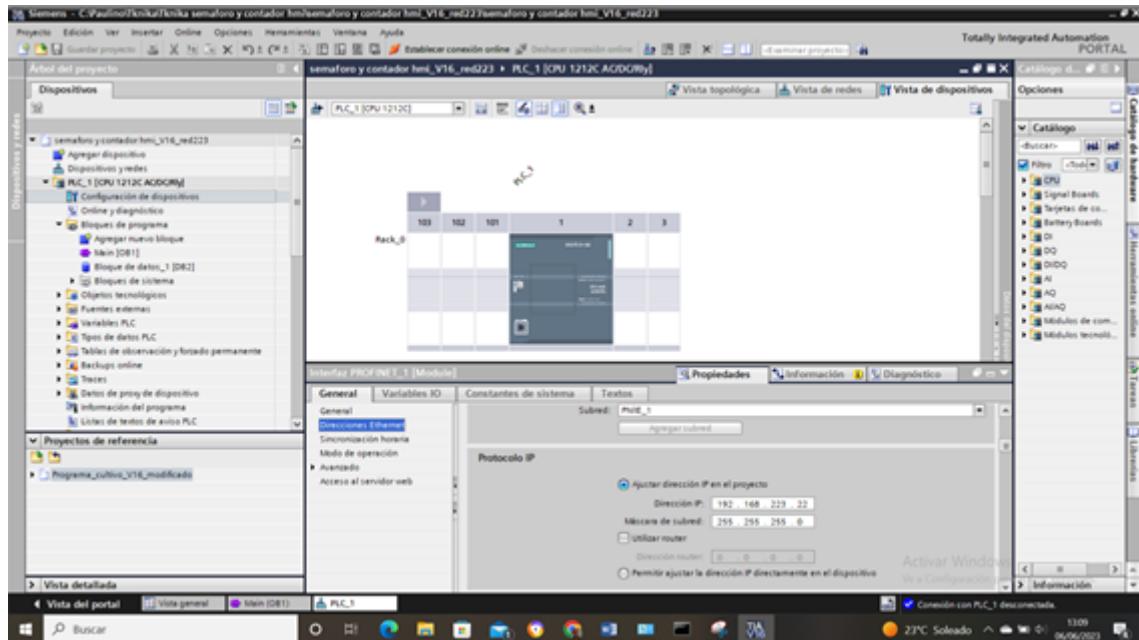
Nombre del proyecto: semáforo y contador hmi_V16_1
TIA Portal: V16

Nombre del equipo: S7-1200 station_1
Nombre del módulo: PLC_1
Tipo de módulo: CPU 1212C AC/DC/RLY

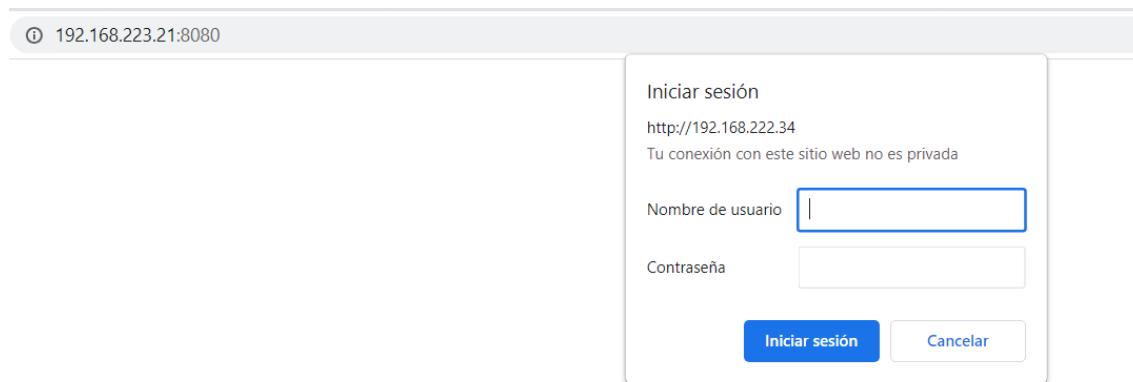
Estado:

Estado operativo: RUN
Estado: Aceptar

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

