

EJERCICIO 3

1. OBJETIVO:

En el presente ejercicio se procederá a configurar un acceso remoto a dos estaciones las cuales van a tener un Firewall SIEMENS Scalance SC646 (Estación 1) y otra un Firewall Scalance S615 (Estación 2). Ambas establecerán un túnel VPN contra un servidor SIEMENS SINEMA RC ubicado en una DMZ en las instalaciones de la compañía. Finalmente habrá un usuario que podrá establecer una comunicación contra el equipo SINEMA RC y a través de él poder alcanzar los equipos que se encuentran detrás de los equipos Scalance.

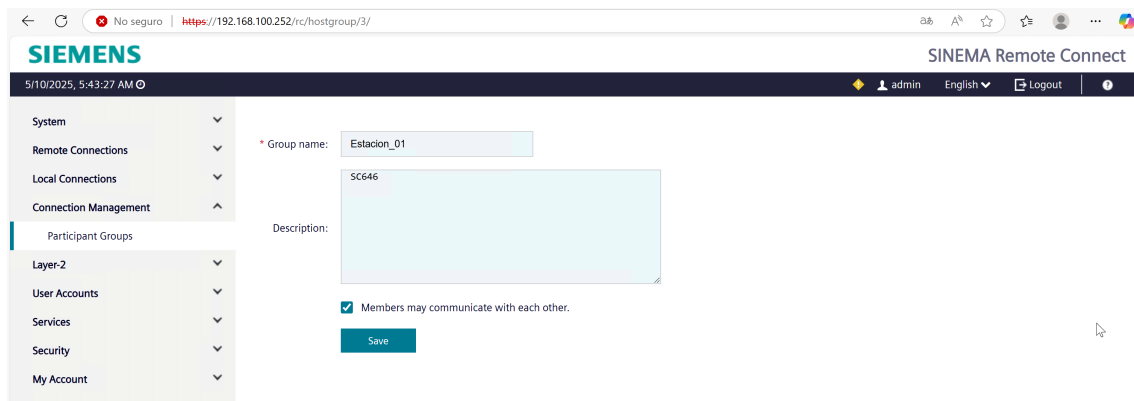
2. PASOS A SEGUIR:

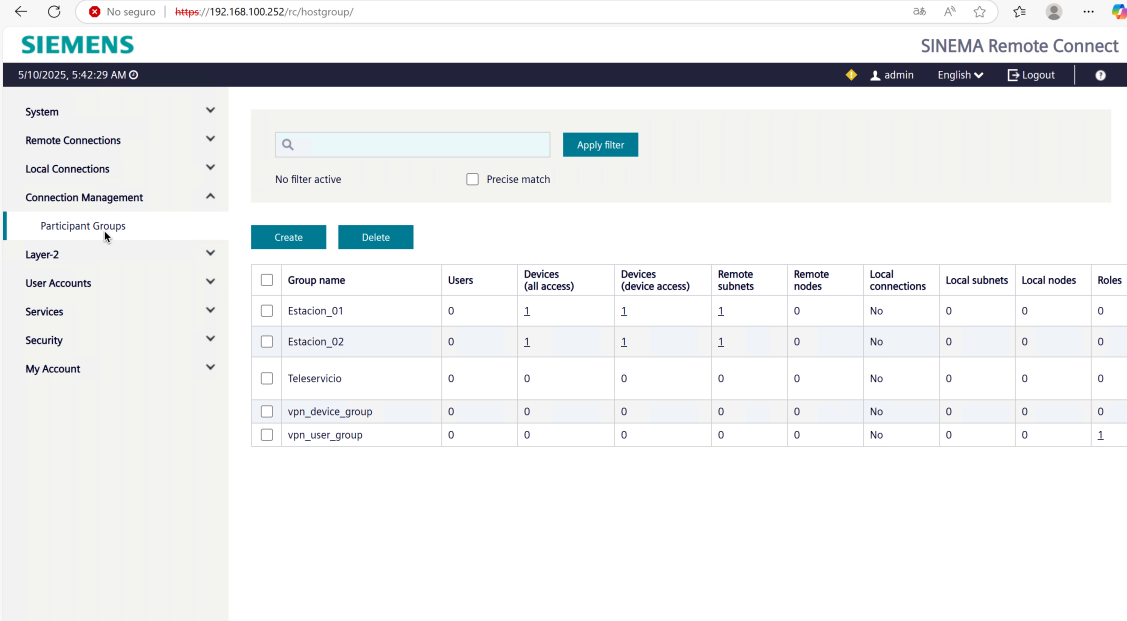
En primer lugar, configuraremos nuestro sistema SINEMA RC para que acepte las conexiones de los equipos SCLANCE SC646 y S615.

Nos conectaremos a la dirección IP 192.168.100.252 mediante HTTPS y los autenticaremos con admin/lcslab2025\$lcslab2025\$.

Allí nos dirigiremos a “Connection Management – Participant Groups” y crearemos tres grupos a los cuales llamaremos:

- “Estación_01” para el equipo SC646.
- “Estación_02” para el equipo S615.
- “Teleservicio01” para el usuario “vpn01”.
- “Teleservicio02” para el usuario “vpn02”.
- Los miembros de ese grupo podrán conectarse a otros del mismo grupo.





SIEMENS SINEMA Remote Connect

5/10/2025, 5:42:29 AM

admin English Logout

System
Remote Connections
Local Connections
Connection Management
Participant Groups
Layer-2
User Accounts
Services
Security
My Account

Search: [] Apply filter

No filter active ☐ Precise match

Create Delete

<input type="checkbox"/>	Group name	Users	Devices (all access)	Devices (device access)	Remote subnets	Remote nodes	Local connections	Local subnets	Local nodes	Roles
<input type="checkbox"/>	Estacion_01	0	1	1	1	0	No	0	0	0
<input type="checkbox"/>	Estacion_02	0	1	1	1	0	No	0	0	0
<input type="checkbox"/>	Teleservicio	0	0	0	0	0	No	0	0	0
<input type="checkbox"/>	vpn_device_group	0	0	0	0	0	No	0	0	0
<input type="checkbox"/>	vpn_user_group	0	0	0	0	0	No	0	0	1

Luego daremos de alta ambos equipos. Para ello nos dirigiremos a “Remote Connections – Devices” y allí seleccionaremos “Create”.

Cumplimentaremos de la siguiente manera:

- Nombre del dispositivo: SC646 y S615, respectivamente.
- Contraseña: lcslab2025\$
- Fabricante: Siemens
- Modelo: SC600 y SC615, respectivamente.
- Protocolo de la VPN: OpenVPN
- Tipo de conexión: Permanente.
- Respecto a las configuraciones de Grupo “añadiremos” el grupo al que pertenece cada uno de los equipos.
 - Todos los accesos.
 - Todos los dispositivos.

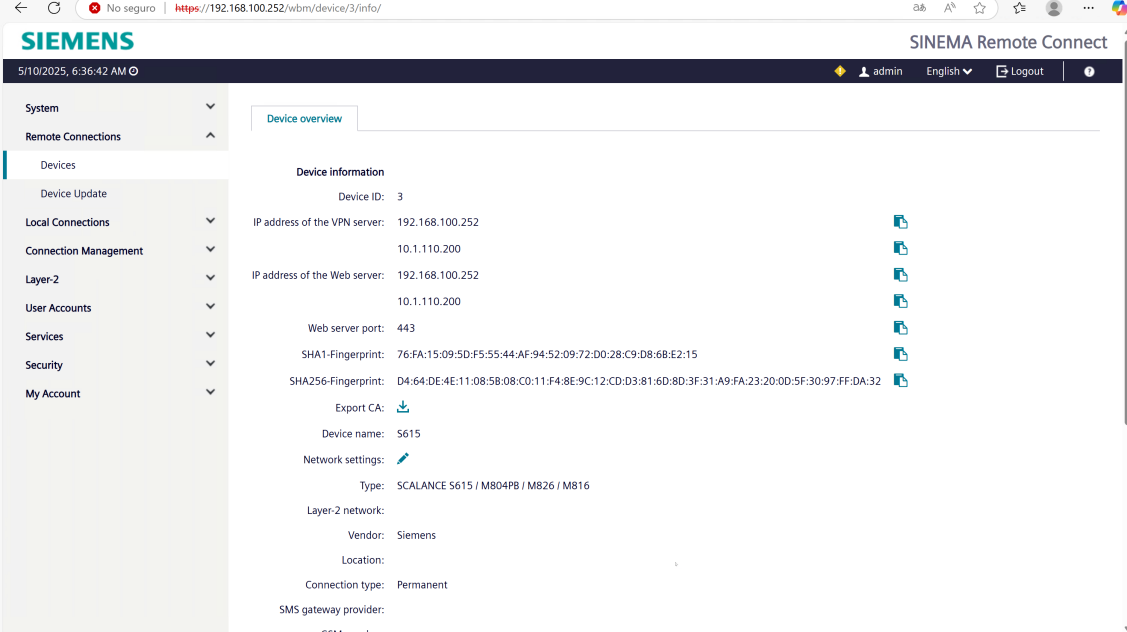
Seleccionaremos “Next” y accederemos al menú de “Network Settings”.

Allí indicaremos:

- Que es un dispositivo tipo “Puerta de Enlace”.
- Añadiremos la red de la instalación, es decir donde estarían los equipos finales. Le daremos el nombre “LAN_Estación01” y “LAN_Estación02”, respectivamente.
- Añadiremos los grupos participantes a los que pertenecen cada uno de los equipos.

Sobre cada uno de los equipos y en el icono “Information” nos fijaremos en las características del equipo y además nos descargaremos el certificado del servidor

seleccionando el icono a la derecha de “Export CA”. Esto nos descargará el certificado del servidor que será empleado por el dispositivo para verificar el certificado de éste. También aparecerá el “Device ID” que emplearemos para autenticar el dispositivo en el servidor SINEMA RC.

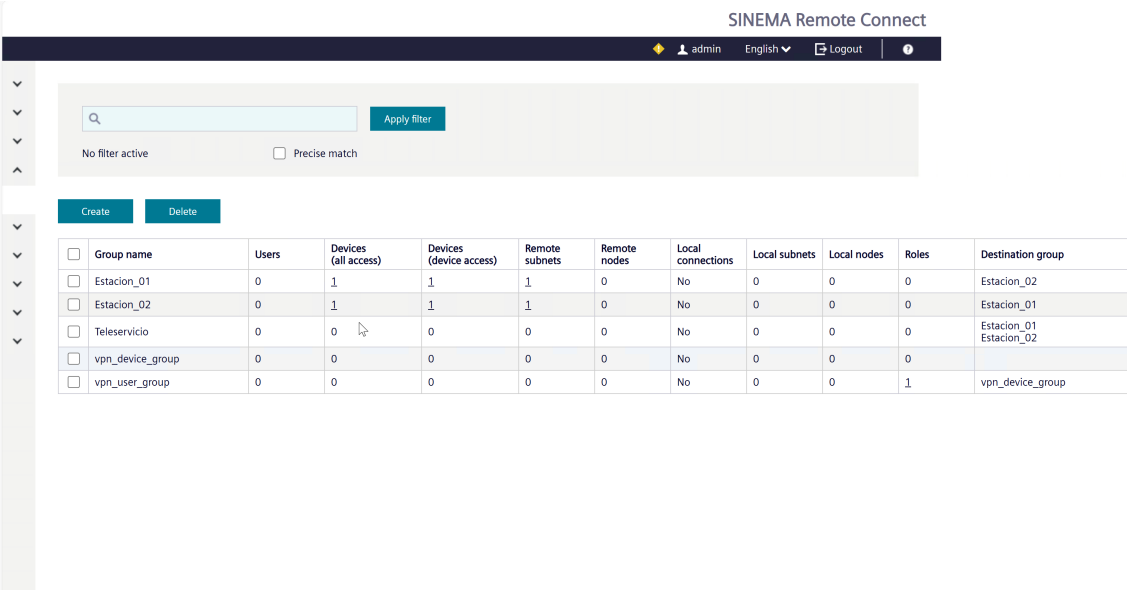


The screenshot shows the SINEMA Remote Connect web interface. The left sidebar contains a menu with options: System, Remote Connections, Devices, Device Update, Local Connections, Connection Management, Layer-2, User Accounts, Services, Security, and My Account. The main content area is titled "Device overview" and displays "Device information" for Device ID: 3. The information includes:

- IP address of the VPN server: 192.168.100.252
- 10.1.110.200
- IP address of the Web server: 192.168.100.252
- 10.1.110.200
- Web server port: 443
- SHA1-Fingerprint: 76-FA:15:09:5D:F5:55:44-AF:94:52:09:72:D0:28:C9:D8:68:E2:15
- SHA256-Fingerprint: D4:64:DE:4E:11:08:5B:08:C0:11:F4:8E:9C:12:CD:D3:81:6D:8D:3F:31:A9:FA:23:20:0D:5F:30:97:FF:DA:32
- Export CA: (Download icon)
- Device name: S615
- Network settings: (Edit icon)
- Type: SCALANCE S615 / M804PB / M826 / M816
- Layer-2 network:
- Vendor: Siemens
- Location:
- Connection type: Permanent
- SMS gateway provider:
- GSM number:

Volveremos a “Connection Management – Participant Groups” para establecer la asociación entre los “Grupos de Participantes”. Es decir, vamos a permitir que:

- Desde la Estación 1 se pueda llegar a la Estación 2.
- Desde la Estación 2 se pueda llegar a la 1.
- Y los usuarios VPN pueden llegar a ambas.



The screenshot shows the SINEMA Remote Connect web interface, specifically the "Participant Groups" section. The top bar includes a search filter and an "Apply filter" button. Below the filter, there are "Create" and "Delete" buttons. The main content is a table with the following columns: Group name, Users, Devices (all access), Devices (device access), Remote subnets, Remote nodes, Local connections, Local subnets, Local nodes, Roles, and Destination group.

Group name	Users	Devices (all access)	Devices (device access)	Remote subnets	Remote nodes	Local connections	Local subnets	Local nodes	Roles	Destination group
<input type="checkbox"/> Estacion_01	0	1	1	1	0	No	0	0	0	Estacion_02
<input type="checkbox"/> Estacion_02	0	1	1	1	0	No	0	0	0	Estacion_01
<input type="checkbox"/> Teleservicio	0	0	0	0	0	No	0	0	0	Estacion_01 Estacion_02
<input type="checkbox"/> vpn_device_group	0	0	0	0	0	No	0	0	0	
<input type="checkbox"/> vpn_user_group	0	0	0	0	0	No	0	0	1	vpn_device_group

A continuación, crearemos los usuarios que se conectarán por VPN a los equipos que estén en las respectivas redes locales de cada uno de los equipos, SC646 y S615.

Iremos a “User Accounts – User & Roles” y crearemos un usuario con las siguientes características:

- Nombre: “vpn01” y “vpn02”.
- Nombres: “Jhonny” y “Thomas”
- Apellidos: “Mentero” y “Potes”.
- Método de autenticación: Contraseña.
- “Next”.
- No podrá hacer ninguna operación desde el equipo SINEMA RC.
- “Next”.
- Van a pertenecer al Grupo de Servicio Remoto, esto es “Teleservicio”.
- Dejaremos pasar el tráfico vía cortafuegos a la IP de equipo virtual para que se pueda conectar por RDP y S7.
- La contraseña será “lcslab2025\$lcslab2025\$”

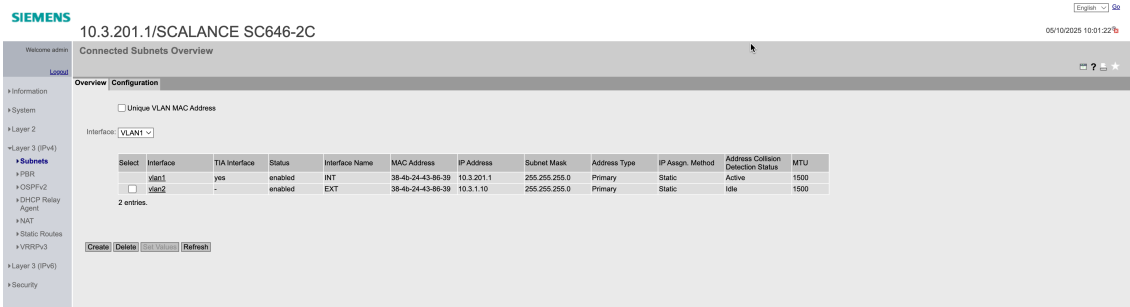
A continuación, deberemos configurar los equipos para que establezcan el túnel VPN contra el equipo SINEMA RC.

Para ello accederemos a las direcciones IP 10.3.201.1 y 10.3.202.1 mediante HTTPS para proceder a la configuración. El usuario será admin/lcslab2025\$.

Luego iremos a “System – Load & Save” y cargaremos cada una de las configuraciones de cada uno de los equipos denominadas “config_SCALANCE_S600.conf” y “config_SCALANCE_SC646.conf”. Para ello localizaremos “Config”, seleccionaremos “Load” y una vez finalizado el equipo se reiniciará.

Volveremos acceder a la configuración del equipo:

- En “Layer 3 – Subnets” asignaremos las direcciones IP 10.3.1.10 y 10.3.2.10 a las “VLAN2” de cada uno de los equipos.
- En “Layer 3 – Static Routes” Configuraremos una ruta por defecto que apunte a las direcciones IP 10.3.1.1 y 10.3.2.1 como siguiente salto.



10.3.201.1/SCALANCE SC646-2C

Connected Subnets Overview

Overview | Configuration

☐ Unique VLAN MAC Address

Interface: **VLAN1**

Select	Interface	TIA Interface	Status	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assign. Method	Address Collision Detection Status	MTU
<input type="checkbox"/>	VLAN1	yes	enabled	INT	38-4b-24-43-88-39	10.3.201.1	255.255.255.0	Primary	Static	Active	1500
<input type="checkbox"/>	VLAN2	-	enabled	EXT	38-4b-24-43-88-39	10.3.1.10	255.255.255.0	Primary	Static	Idle	1500

2 entries.

Create Delete Edit Refresh

SIEMENS 10.3.201.1/SCALANCE SC646-2C

Welcome admin | Logout

Static Routes

Changes will be saved automatically in 52 seconds. Press 'Write Startup Config' to save immediately.

Destination Network:
Subnet Mask:
Gateway:
Administrative Distance: 1

Select	Destination Network	Subnet Mask	Gateway	Interface	Administrative Distance	Status
0 entries.						

Create Delete Refresh

Information
System
Layer 2
Layer 3 (IPv4)
Subnets
PBR
OSPFv2
DHCP Relay Agent
NAT
Static Routes
VRRPv3
Layer 3 (IPv6)
Security

Realizar un “ping” continuo a la dirección IP del PLC simulado en la Estación contraria, esto es 10.3.201.10 y 10.3.202.10.

¿Comunica? ¿Si? ¿No? ¿Porqué? Si la respuesta es sí, continuar.

Hacer un “Tracert” nuevamente a la misma IP y tomar nota del resultado, sobre todo las direcciones IP.

Luego procederemos a cargar el certificado de la CA. Para ello iremos a “System – Load & Save” y localizaremos el apartado “X509Cert” y allí seleccionaremos el que hemos elegido en los pasos previos.

SIEMENS 10.3.201.1/SCALANCE SC646-2C

Welcome admin | Logout

Load and Save via HTTP

Changes will be saved automatically in 52 seconds. Press 'Write Startup Config' to save immediately.

HTTP / TFTP / SFTP / Passwords

Update

Type	Description	Load	Save	Delete
Firmware	Firmware Update	Load	Save	Save

Configuration

Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	Save
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	Save
ConfigPackBackup	ConfigPackBackup	Load	Save	Delete
FirewallNATConfig	FirewallNATConfig	Load	Save	Save
LoginWelcomeMessage	Login Welcome Message	Load	Save	Delete
RunningCLI	Show running-config at CLI settings	Load	Save	Save
RunningSINEMAConfig	SINEMA Running Configuration	Load	Save	Save
Script	Script	Load	Save	Save
SINEMAConfig	SINEMA Offline Configuration	Load	Save	Save
Users	Users and Passwords	Load	Save	Save
WBMfav	WBM favourite pages	Load	Save	Delete

Certificate & Key

Type	Description	Load	Save	Delete
HTTPSCert	HTTPS Certificate	Load	Save	Delete
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	Load	Save	Delete
SSHPrivateKeyRSA	SSH Private Key (RSA)	Load	Save	Delete
X509Cert	X509 Certificates	Load	Save	Save

Service & Log

Type	Description	Load	Save	Delete
Debug	Debug Information for Siemens Support	Load	Save	Delete
Logfile	Event Log (ASCI)	Load	Save	Save
StartupInfo	Startup Information	Load	Save	Save

Information

Type	Description	Load	Save	Delete
MB	SCALANCE S600 MSPS MB	Load	Save	Save

License

Type	Description	Load	Save	Delete
LicenseConditions	ZIP File with Open Source Software License Conditions	Load	Save	Save

Refresh

Information
System
Layer 2
Layer 3 (IPv4)
Layer 3 (IPv6)
Security
Users
Passwords
AAA
Certificates
Firewall
IPsec VPN
OpenVPN
Brute Force Prevention

Luego iremos a “Security – Certificates” para verificar que está correcto.

SIEMENS 10.3.201.1/SCALANCE SC646-2C

Welcome admin | Logout

Certificates Overview

Overview Certificates

Select	Type	Filename	State	Subject DN	Issuer DN	Issue Date	Expiry Date	Used
<input type="checkbox"/>	CA Cert	CA_174060_SINEMA_RC.crt	valid	CN=CA.174060.SINEMA.RC	CN=CA.174060.SINEMA.RC	05/08/2025 16:04:47	05/08/2035 16:04:47	Sinema RC

1 entry

Delete Refresh

Information
System
Layer 2
Layer 3 (IPv4)
Layer 3 (IPv6)
Security
Users
Passwords
AAA
Certificates
Firewall
IPsec VPN
OpenVPN
Brute Force Prevention

¿Aparece como válido el certificado? Si es que es inválido, ¿Cuál puede ser la razón?

Una vez solventado iremos a “System -SINEMA RC” y procederemos a introducir los parámetros necesarios para establecer la VPN.

- IP del servidor: 192.168.100.252.
- Puerto: 443
- Método de verificación del servidor: Certificado.
- Seleccionar el certificado cargado previamente.
- Identificador del equipo: El generado por el servidor SINEMA RC como “Device ID”.
- Contraseña: La asignada a cada equipo, “Icslab2025\$Icslab2025\$”.
- Tipo de comunicación: OpenVPN.
- Tipo: Permanente.

Luego seleccionamos “Set Values”.

Activamos la casilla “Enable SINEMA RC”.

Nuevamente “Set Values”.

A continuación, iremos al servidor SINEMA RC y verificaremos que los equipos están “Online”.

Si pasados unos segundos no se establece la comunicación verificar pasos previos.

Una vez los dos equipos estén “online” repetir el “ping” y el “tracert”.

¿Es el mismo resultado? ¿Si? ¿No? ¿Porqué?

Nos conectaremos vía clave o wifi a algunas de las redes disponibles.

Luego desde un PC abriremos el software SINEMS RC Client. Una vez allí crearemos un perfil con los parámetros de nuestro servidor SINEMA RC:

English | i ?

Account | **Server Profiles** | Settings

Add/edit server profiles

Create

<input type="checkbox"/>	Server name	Server URL	Username
--------------------------	-------------	------------	----------

SINEMA RC Server:
SINEMA RC Server name: icslab
SINEMA RC Server URL: 192.168.100.252
SINEMA RC username: vpn01
Login method: Username / Password
Comment:

Save Cancel

Show log files Exit

Guardamos los cambios y volvemos a la pestaña “Account” donde deberemos configurar la contraseña y seleccionar “Login”

English | i ?

Account | **Server Profiles** | Settings

SINEMA Remote Connect Login
SINEMA RC Server name: icslab - vpn01
SINEMA RC Server URL: 192.168.100.252
Login method: Username / Password
SINEMA RC username: vpn01
SINEMA RC password: *****

Log in

Show log files Exit

Validados correctamente accederemos a la siguiente pantalla.

Session Timeout: 11:59:20 Renew English Logout ?

Account Server Profiles Settings

SINEMA Remote Connect Account

SINEMA RC URL: [192.168.100.252](#) VPN address: - **OFFLINE** **Connect**
 Logged in as: [vpn01](#) NAT status: None

Device list

All Search Search Refresh Connect all devices

Device name	VPN address	Subnet name	Remote subnet (Port)	Virtual subnet	Node name	Node address (Port)	Node virtual address	Status	Location	Allow communication
S615	172.29.0.3	LAN_S6...	10.3....					ONLINE	🏠 📱	NO YES
SC646		Estacio...	10.3....					ONLINE	🏠 📱	NO YES

Show log files Exit

En la parte superior seleccionaremos “Connect” para establecer el túnel VPN contra el SINEMA RC. Esto no permitirá aún poder establecer las comunicaciones con los equipos “detrás” de los firewall SCALANCE SC646 y S615.

Para ello deberemos en la parte inferior seleccionar “YES” en la columna “Allow Communication” en la columna correspondiente.

Session Timeout: 11:58:10 Renew English Logout ?

Account Server Profiles Settings

SINEMA Remote Connect Account

SINEMA RC URL: [192.168.100.252](#) VPN address: 172.29.0.4:5443 (TCP) **CONNECTED** **Disconnect**
 Logged in as: [vpn01](#) NAT status: None

Device list

All Search Search Refresh Connect all devices

Device name	VPN address	Subnet name	Remote subnet (Port)	Virtual subnet	Node name	Node address (Port)	Node virtual address	Status	Location	Allow communication
S615	172.29.0.3	LAN_S6...	10.3....					ONLINE	🏠 📱	NO YES
SC646		Estacio...	10.3....					ONLINE	🏠 📱	NO YES

Show log files Exit

Podremos comprobar la conectividad haciendo un ping continuo a las direcciones IP 10.3.201.10 y 10.3.202.10.

Para visualizar el tráfico generado por la VPN podrán conectarse a los respectivos cortafuegos en la dirección IP 10.3.1.1 y 10.3.2.1 en el apartado “Log and Report” y “Fortiview”. Las credenciales deber admin31/admin31.

Luego podremos abrir el simulador Snap7 para establecer comunicación con el PLC virtualizado y abrir una sesión de Escritorio Remoto contra cada una de las respectivas IPs.

También desde esos mismos equipos podremos realizar un ping desde y hacia cada uno de ellos.

1. ACTIVIDADES ADICIONALES:

- a. Que el usuario vpn01 solo tenga acceso al equipo SC646 y el vpn02 al S615.