

EJERCICIO 1

1. OBJETIVO:

En el presente ejercicio se procederá a configurar un túnel VPN “Sitio a Sitio”. El escenario será el siguiente. Existen 3 planta fotovoltaicas; Planta A (Planta Solar + Centro de Control), B (Planta Solar) y C (Planta solar). La Planta A es la que tiene conexión a Internet mediante tecnología móvil 5G. La Planta A, se comunica con la B y la C mediante radio enlaces privados mediante bandas no licenciadas. La distancia entre ellas es de 70-100 metros con visión directa. La VPN Sitio a Sitio se produce entre las Plantas A y B. Gracias al empleo de este radio enlace se evita que cada planta solar tenga su propio enlace 5G y el consiguiente gasto asociado.

2. PASOS A SEGUIR:

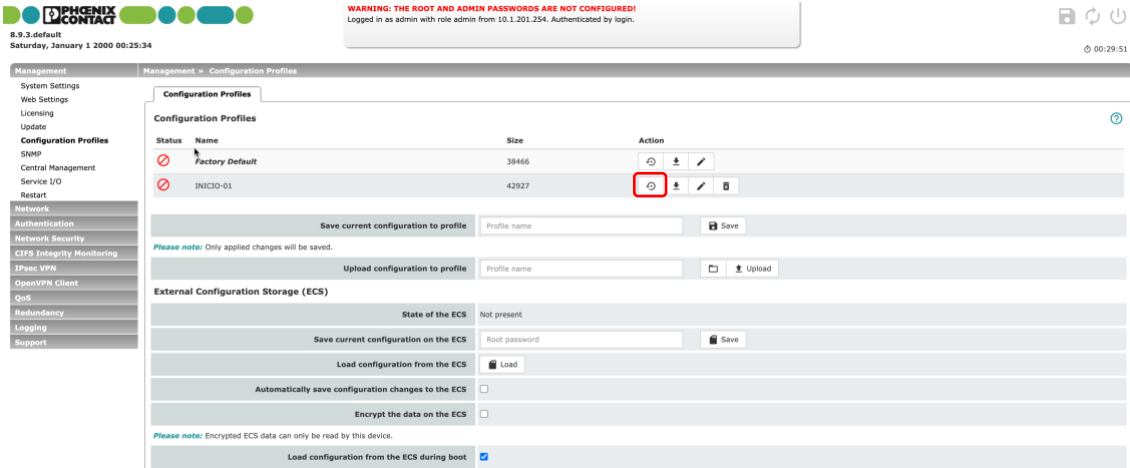
Para ello contamos con dos equipos Router Firewall de fabricante Phoenix Contact.

El equipo “mGuard-01” estará ubicado en la Planta B y el “mGuard-02” en la Planta A.

El equipo mGuard-02 (Planta A) estará esperando las comunicaciones internas que le lleguen desde las diferentes plantas solares, mientras que el mGuard-01 serán los que inicien las comunicaciones (Planta B o C).

Para ello deberemos de conectarnos al mGuard-01 en su interfaz web de gestión segura, HTTPS, que estará en la IP 10.1.201.1 Las credenciales de acceso serán admin/mGuard. De igual modo en la del mGuard-012 en la IP 10.1.202.1.

Allí iremos a “Management – Configuration Profiles” y cargaremos el fichero de configuración titulado como INICIO-01 y pinchando en el icono “Restore Profile” lo cargaremos. Esto borrará cualquier configuración anterior y lo dejará listo para configurar el túnel VPN.

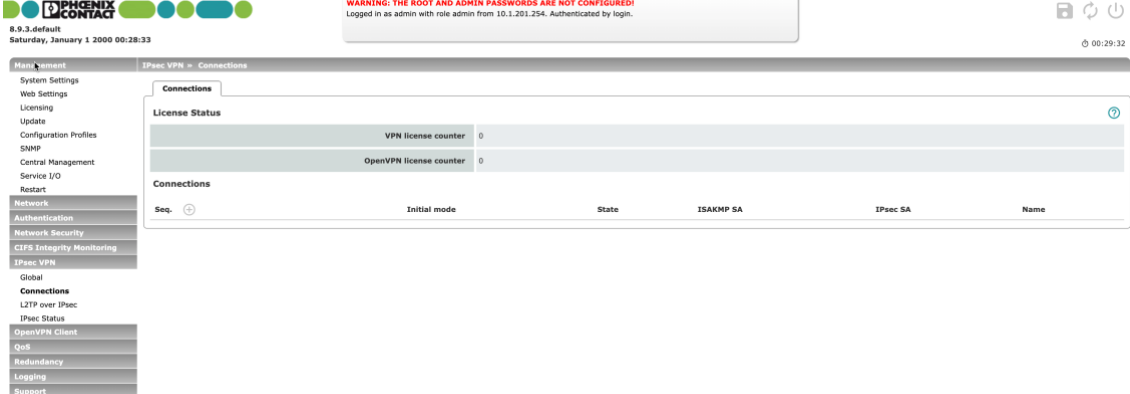


The screenshot shows the web interface of a Phoenix Contact mGuard-01 device. At the top, there is a warning banner: "WARNING: THE ROOT AND ADMIN PASSWORDS ARE NOT CONFIGURED! Logged in as admin with role admin from 10.1.201.254. Authenticated by login." The left sidebar contains a navigation menu with options like Management, System Settings, Web Settings, Licensing, Update, Configuration Profiles, SNMP, Central Management, Service I/O, Restart, Network, Authentication, Network Security, CIFS Integrity Monitoring, IPsec VPN, OpenVPN Client, QoS, Redundancy, Logging, and Support. The main content area is titled "Configuration Profiles" and contains a table with the following data:

Status	Name	Size	Action
	Factory Default	38466	
	INICIO-01	42927	

Below the table, there are sections for "Save current configuration to profile" (with a "Profile name" field and a "Save" button), "Upload configuration to profile" (with a "Profile name" field and an "Upload" button), and "External Configuration Storage (ECS)". The ECS section includes a "State of the ECS" field (set to "Not present"), a "Save current configuration on the ECS" button, a "Load configuration from the ECS" button, and checkboxes for "Automatically save configuration changes to the ECS" and "Encrypt the data on the ECS". A "Please note" message states: "Encrypted ECS data can only be read by this device." At the bottom, there is a checkbox for "Load configuration from the ECS during boot" which is checked.

Luego iremos a el menú IPsec “VPN – Connections” crearemos la que nos unirá con la Planta A.



WARNING: THE ROOT AND ADMIN PASSWORDS ARE NOT CONFIGURED!
 Logged in as admin with role admin from 10.1.201.254. Authenticated by login.

8.9.3-default
 Saturday, January 1 2000 00:28:33

Management > IPsec VPN > Connections

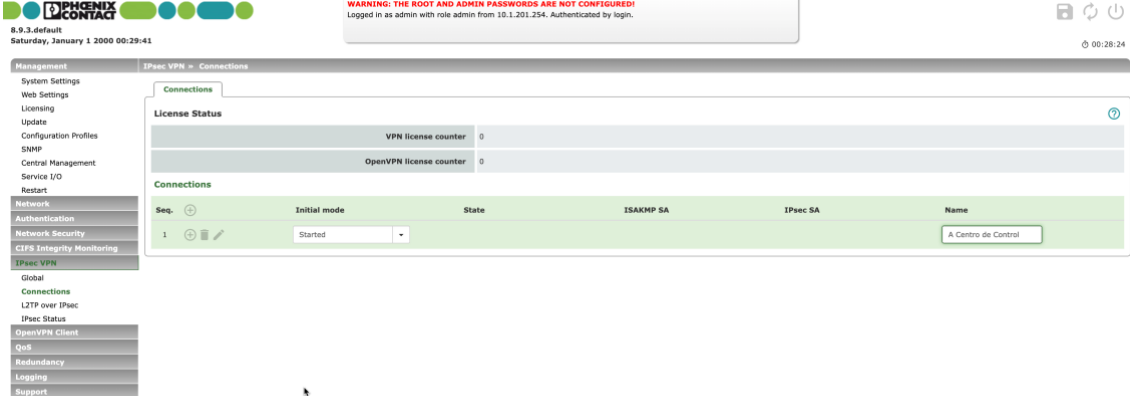
Connections

License Status

VPN license counter	0
OpenVPN license counter	0

Connections

Seq.	Initial mode	State	ISAKMP SA	IPsec SA	Name
------	--------------	-------	-----------	----------	------



WARNING: THE ROOT AND ADMIN PASSWORDS ARE NOT CONFIGURED!
 Logged in as admin with role admin from 10.1.201.254. Authenticated by login.

8.9.3-default
 Saturday, January 1 2000 00:29:41

Management > IPsec VPN > Connections

Connections

License Status

VPN license counter	0
OpenVPN license counter	0

Connections

Seq.	Initial mode	State	ISAKMP SA	IPsec SA	Name
1	Started				A Centro de Control

Una vez allí configuraremos todos los parámetros seleccionando “Edit Row”.

Con los siguientes datos deberemos configurar el túnel VPN:

- La VPN deberá estar iniciada.
- La dirección IP del firewall del otro extremo es la de la interfaz WAN.
- La interfaz que utilizará para establecer el túnel la misma que el punto anterior.
- El inicio de la comunicación será iniciada por este firewall, el mGuard-01.
- La red local que anunciará al otro extremo, el mGuard-02, es la que tiene en la interfaz LAN.
- La red remota a la que queremos llegar es la que tiene el mGuard-02 en su interfaz LAN.
- En ningún caso se hace traducción de nombres de red.
- Las reglas en el cortafuegos serán las que aparezcan por defecto pero se tendrá que loguear todo el tráfico.
- Como método de autenticación se empleará contraseña pre-compartida y ésta será “icslab”.
- El modo ISAKMP será el que no sea vulnerable a ataques.

- Dentro de las opciones IKE tendremos que bajo el menú ISAKMP SA, EL cifrado será AES-256; el algoritmo de HASH será SHA-256 y Diffie-Hellman el Grupo 14.
- En las opciones SA de IPSec el cifrado será el mismo que el anterior y el de HASH SHA-512.

Una vez hecho lo anterior guardaremos los cambios seleccionando “Save” haciendo “Click” sobre el icono de disquete en la esquina superior derecha.

Ahora iremos al mGuard-02 con IP 10.1.202.1 bajo las mismas condiciones que en el caso del mGuard-01 y cargaremos el mismo fichero de configuración.

Configuraremos una VPN de igual manera excepto que:

- La IP remota será la interfaz WAN del mGuard-01.
- El modo conexión será en espera.
- La red local será la del mGuard-02 en su interfaz LAN.
- La red remota será la del mGuard-01 en su interfaz LAN.

Luego en IPSec VPN – IPSec Status tendremos que verificar en ambos extremos que aparece la VPN en “Established”.

Luego iremos a la interfaz web del quipo Fortigate con IP 10.1.1.1 o 10.1.2.1 y loguearnos en su interfaz web con las credenciales user11/user11 y user11/user11; respectivamente.

Desde el PC del alumno o desde el virtual con IP 10.1.202.20 y que podremos acceder por escritorio remoto con credenciales admin/icslab arrancaremos el cliente de Snap7 y conectaremos al PLC de la planta solar fotovoltaica con IP 10.1.201.10.

Trataremos de pararlo y arrancarlo.

Allí en “Log & Report” tendremos que identificar el tráfico IPSec entre las direcciones IP 10.1.1.10 y 10.1.2.10.

¿Cuál es el Log?

¿Qué método está empleando? ¿ESP? ¿AH?

¿Se puede ver los comandos de encendido o apagado? ¿Si? ¿No? ¿Porqué?

Si desde un equipo en la red 10.1.201.0/24 o 10.1.202.0/24 a través del simulador Snap7 accedemos al PLC simulado Siemens S7-315 PLC PN-DP con IP 192.168.100.21 ¿podemos ver el tráfico “S7”?

¿Por qué no va por el túnel IPSec?

3. ACTIVIDADES ADICIONALES:

- a. Acceder a la configuración del Fortigate y crear una regla que permita solo el tráfico entre la dirección IP 10.1.1.10 y 10.1.2.10.
- b. Permitir que el equipo contrario responda a “ping” pero que no te puedas conectar por S7.
- c. Limitar las comunicaciones desde el equipo 10.1.202.10 (Centro de Control) al PLC con IP 10.1.20.10 en los protocolos S7 y RDP.