PROYECTO

TFG

Servidor Web con Acceso Seguro a través de VPN

Autor: Mohammed Maamla Razzak

Titulación: Técnico Superior en Administración de Sistemas Informáticos en Red

Fecha: 20/12/2025	Versión: 1_0

Documentación del producto

Para La documentación del proyecto se presenta como un conjunto de manuales de uso concisos y bien organizados. Estos documentos sirven como herramienta de referencia y formación, garantizando que tanto los usuarios finales como el administrador puedan operar el sistema de manera segura y eficiente.

Manual de Usuario (Empleado Final)

Dirigido a: Empleados, colaboradores y teletrabajadores.

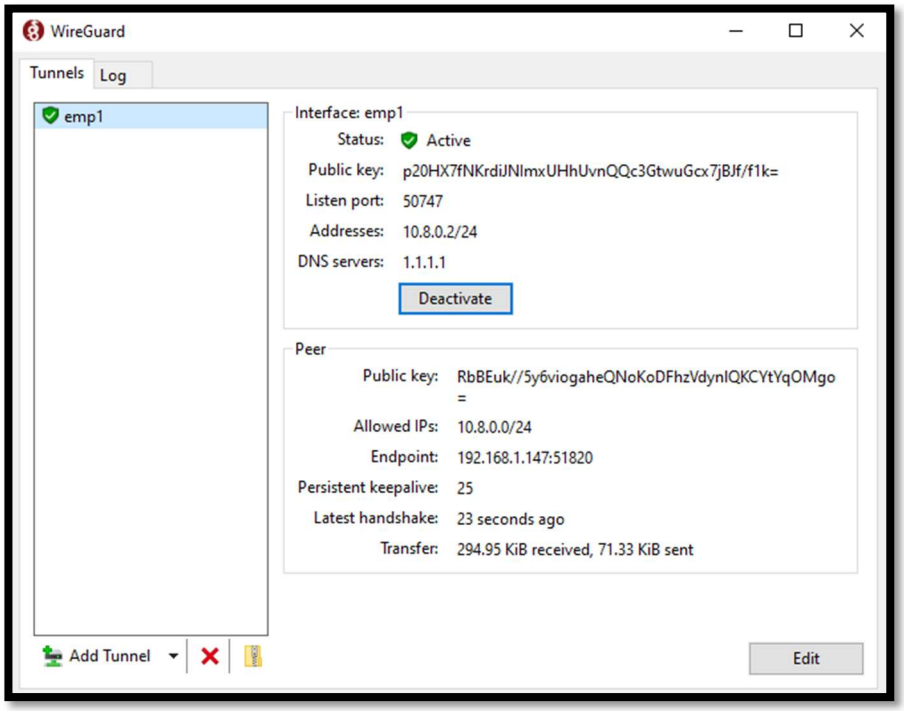
1. Instalación y Conexión al Túnel VPN (WireGuard)

El acceso a la red corporativa es obligatorio a través del túnel VPN.

Instalación: Instalar la aplicación WireGuard en el dispositivo (Windows, móvil, etc.).

Importación del Perfil: El administrador proporcionará un archivo de configuración único (.conf).

Activación: Haga clic en el botón "Activar" o "Connect" para establecer la conexión.



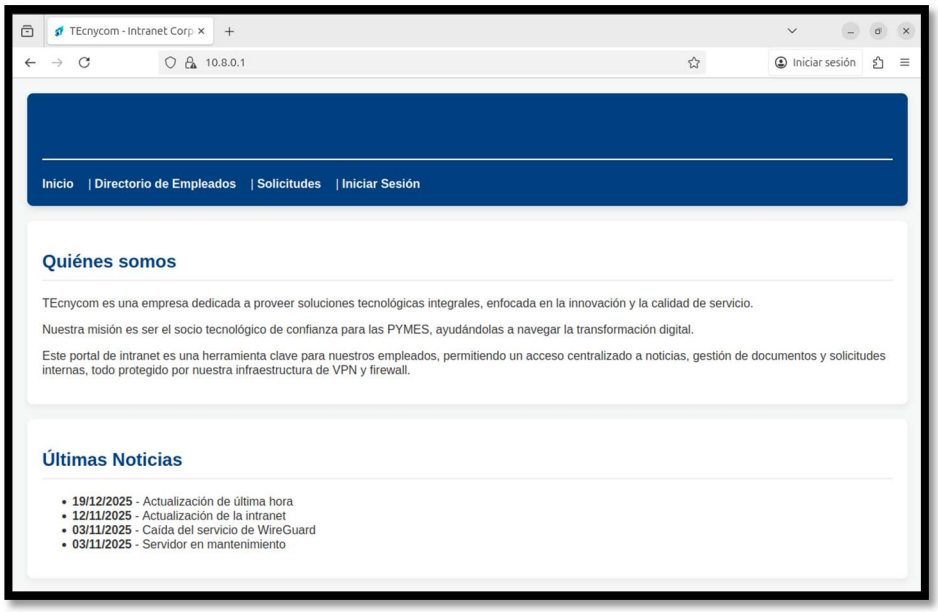
Pie de Imagen: El túnel VPN activo en el cliente Windows (EMP 1), mostrando la conexión cifrada establecida.

2. Acceso a la Intranet Corporativa

Solo con la VPN activa, podrá acceder a la Intranet.

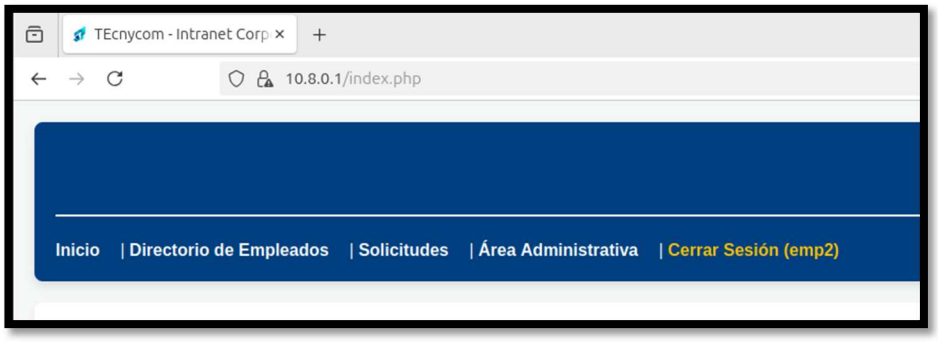
URL Segura: Abrir el navegador e introducir la dirección IP segura del servidor.

Dirección: https://10.8.0.1



Pie de Imagen: La URL de acceso a la Intranet. La conexión es segura (HTTPS) gracias al certificado instalado en el Servidor Central.

Inicio de Sesión: Introducir el usuario y la contraseña proporcionados.



Cierre de Sesión: Cuando finalice, use el enlace "Cerrar Sesión" y desactive el túnel VPN para liberar recursos.

Manual de Administrador (Infraestructura y Servicios)

Dirigido a: Personal técnico responsable de la infraestructura y el mantenimiento diario.

1. Gestión de Usuarios VPN (WireGuard)

A. Alta de Nuevos Empleados (Generación de Claves)

Acceder a la consola del Servidor Ubuntu (SRV1).

Generar un nuevo par de claves privada/pública para los nuevos empleados:

```
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp1_private.key | wg pubkey | sudo tee /etc/wireguard/emp1_public.key
p20HX7fNKrdiJNImxUHhUvnQQc3GtwuGcx7jBJf/f1k=
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp2_private.key | wg pubkey | sudo tee /etc/wireguard/emp2_public.key
NrjUJuY1HpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp3_private.key | wg pubkey | sudo tee /etc/wireguard/emp3_public.key
bBR4t3xyoyazWOeCc/Nr92M1InVLoBIXphIxF0JNmXY=
srv1@srv1:~$ sudo cat /etc/wireguard/emp1_private.key
IJki0cXbJvaovi55ogZDC73/FH3KAsxLKoSTL5e8a1w=
srv1@srv1:~$ sudo cat /etc/wireguard/emp2_private.key
oNvp3b/hk1UABXYcjqgUyi5N2SeS3uEWE/MUq/04r0M=
srv1@srv1:~$ sudo cat /etc/wireguard/emp3_private.key
yMj8FswCS9DFcE0WS9yE2HCggdWUapwqnX3hU0mcrkM=
srv1@srv1:~$ sudo cat /etc/wireguard/emp1_public.key
p20HX7fNKrdiJNImxUHhUvnQQc3GtwuGcx7jBJf/f1k=
srv1@srv1:~$ sudo cat /etc/wireguard/emp2_public.key
NrjUJuY1HpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
srv1@srv1:~$ sudo cat /etc/wireguard/emp3_public.key
bBR4t3xyoyazWOeCc/Nr92M1InVLoBIXphIxF0JNmXY=
srv1@srv1:~$
```

Configuración en el Servidor: Editar el archivo /etc/wireguard/wg0.conf para añadir el nuevo [Peer].

```
  GNU nano 7.2                                                  /etc/wireguard/wg0.conf
[Interface]
Address = 10.8.0.1/24
ListenPort = 51820
PrivateKey = gP4hgRgBXSthnWMGiFYTkDz+PAcWpezEvp+UnwOXW0Q=

#Empleados
[Peer]
PublicKey = p20HX7fNKrdiJNImxUHhUvnQQc3GtwuGcx7jBJf/f1k=
AllowedIPs = 10.8.0.2/32

[Peer]
PublicKey = NrjUJuY1HpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
AllowedIPs = 10.8.0.3/32

[Peer]
PublicKey = bBR4t3xyoyazWOeCc/Nr92M1InVLoBIXphIxF0JNmXY=
AllowedIPs = 10.8.0.4/32
```

Pie de Imagen: Extracto de wg0.conf mostrando la estructura de un nuevo [Peer] con su clave pública y su IP virtual asignada.

Baja de un Empleado

Para revocar el acceso a un usuario, simplemente se debe eliminar su bloque [Peer] completo del archivo /etc/wireguard/wg0.conf y recargar la configuración.

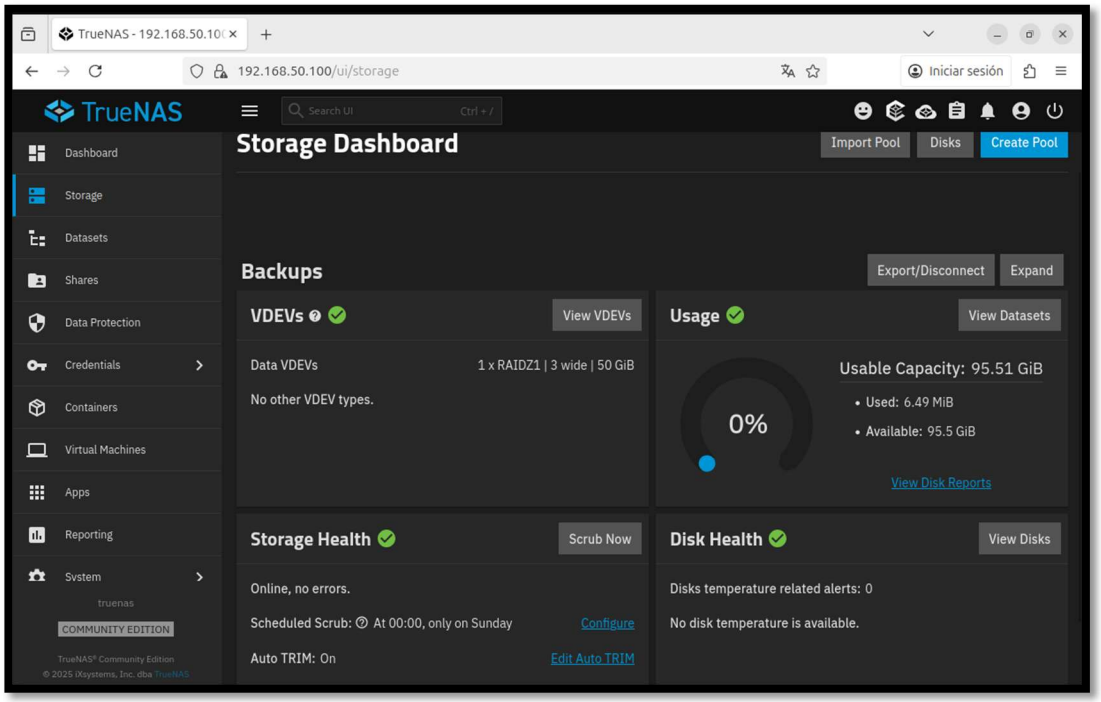
2. Gestión de Almacenamiento (TrueNAS)

Acceso: Acceder a la interfaz web del NAS (IP: 192.168.50.100).

Verificación del Pool (Redundancia): Revisar el Dashboard para confirmar el estado de salud del pool de backups (Backups).

Estado Ideal: ONLINE.

Estado de Advertencia: DEGRADADO (implica que un disco ha fallado y debe ser reemplazado urgentemente).

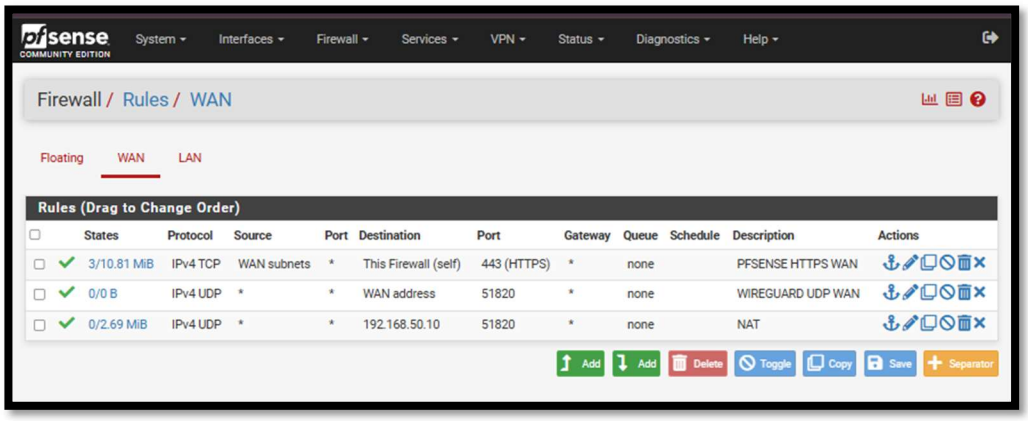


Pie de Imagen: Dashboard del TrueNAS confirmando el estado de salud del Pool de Backups y la configuración RAIDZ1.

3. Verificación de Seguridad Perimetral (pfSense)

El firewall protege la LAN, permitiendo únicamente el tráfico VPN.

Revisión de Reglas: En Firewall → Rules → WAN, confirmar que solo las reglas para el puerto 51820 (WireGuard) y la gestión están activas.



Pie de Imagen: Vista de las reglas de Firewall en pfSense, confirmando la aplicación de la política de mínimo privilegio (solo 51820 abierto).

Manual de Seguridad y Mantenimiento

Dirigido a: Personal técnico.

Objetivo: Establecer una rutina semanal de verificación y auditoría para prevenir fallos y ataques.

1. Rutina de Mantenimiento

Diaria

Auditoría de Backups

Revisar el archivo de log (/var/log/backup_web.log) para confirmar la ejecución del script backup.sh.

Semanal

Estado del RAID

Acceder a TrueNAS y verificar el estado del Pool (ONLINE).

Mensual

Revisión de Logs

Revisar los logs de pfSense (WAN) para identificar patrones de ataque bloqueados.

2. Procedimiento de Recuperación ante Desastres

Si el Servidor Central (SRV1) sufre un fallo total, se sigue este proceso:

Identificación de Fallo: Confirmar que SRV1 está inoperativo.

Recuperación del Backup:

Montar la carpeta NFS del NAS en un nuevo Servidor Ubuntu de reemplazo.

Copiar el último archivo backup_AAAA-MM-DD.tar.gz al nuevo servidor.

Restauración: Descomprimir el archivo en el directorio /var/www/html para restaurar la Intranet a su estado más reciente.

Comando: sudo tar -xzf backup_AAAA-MM-DD.tar.gz

B. Procedimiento en Caso de Fallo del Túnel VPN

Diagnóstico del Firewall: Verificar si el pfSense (192.168.1.147) está accesible.

Diagnóstico del Servicio: En SRV1, verificar que el servicio WireGuard está activo

Comando: sudo systemctl status wg-quick@wg0.

Diagnóstico del Peer: Usar sudo wg para ver si hay algún Latest Handshake de los clientes. Si no hay, la clave pública del cliente podría estar mal configurada.

Mohammed Maamla Razzak

Técnico Superior en Administración de Sistemas Informáticos en Red

2025-2026