LO ESENCIAL · Módulo 3 · Red y acceso

Nunca se abren puertos. Malla privada, proxy inverso, una sola identidad, y acceso remoto del implementador que se puede revocar.

3.1 · Malla privada: nunca se abren puertos

Objetivos

- Levantar una malla entre dos equipos
- Acceder desde fuera sin exponer nada

La regla: nunca se abren puertos

Un puerto abierto al internet es una puerta a la calle con un letrero. Los robots la encuentran en minutos. En este curso **ningún** servicio se expone: los equipos hablan entre sí por una **malla privada** (una VPN entre pares), y quien no está en la malla no ve nada. Ni el proxy, ni el SSO, ni el asistente.

Una malla privada moderna se apoya en **WireGuard** (protocolo de VPN incluido en el núcleo de Linux) y le añade lo que WireGuard no trae: descubrimiento de pares, atravesar NAT sin abrir puertos, identidad por usuario y listas de control de acceso.

Opciones `[VOLÁTIL — verificado: 2026-09]`

Opción	Qué es	Cuándo
Servicio gestionado de malla (plan gratuito para pocos equipos)	el plano de control lo opera un tercero; los datos van directo entre pares	arrancar rápido;
Plano de control autoalojado compatible	el mismo cliente, servidor propio	cuando el client por terceros
WireGuard a mano	túneles configurados uno por uno	dos o tres equip máximo manten

El **criterio**: ¿quién más puede ver que la ferretería existe? Con la gestionada, el proveedor sabe qué equipos se conectan (no qué dicen). Con la autoalojada, nadie. El cliente decide con esa frase delante.

PROCEDIMIENTO · **Laboratorio 3.1 · dos equipos, una malla, cero puertos**

Se hace con el nodo de servicios (mini PC) y el portátil del implementador.

```
# En cada equipo: instalar el cliente de la malla elegida y unirlo con la identidad del
    usuario.
# El comando exacto cambia con la herramienta; el resultado no: cada equipo recibe una IP
    privada
# estable (100.x.y.z o similar) alcanzable solo desde la malla.
<cliente-de-malla> up
<cliente-de-malla> status        # debe listar el otro equipo y su IP de malla
ping -c 3 <ip-de-malla-del-mini-pc>
```

Después, la prueba de la regla:

```
# Desde un equipo FUERA de la malla (datos móviles del celular), la IP pública de la
    oficina:
nmap -Pn -p 22,80,443,8080 <ip-publica-oficina>
# Lo que debe ver: todos "filtered" o "closed". Ninguno "open".
```

ACL mínima (la sintaxis varía; la idea no): el grupo `empleados` llega al proxy en el puerto 443 del nodo de servicios y a nada más; el grupo `implementador` llega además al SSH de los tres nodos; el NAS solo acepta al nodo de servicios y al espejo de backups.
Entregable: captura de `status` con los equipos, salida del `nmap` con todo cerrado, y la ACL en `labs/03-01/acl.md`. Commit: «Capa 3.1: malla privada».
Nada: la malla no depende del cómputo. Es la misma en A, B y C.

Cuándo NO usar esto **Malla privada: nunca se abren puertos**

- No use la malla para «compartir el asistente con el público»: eso es otro producto, con otra seguridad, y no es el de este curso.
- No ponga el plano de control autoalojado si nadie va a actualizarlo: un plano de control viejo es peor que uno gestionado al día.

PRÁCTICA · **Práctica**

1. ¿Qué ve un atacante que escanea la IP pública de la ferretería? ¿Y uno que robó el portátil del vendedor con la malla activa? (Respuesta: el módulo 3.2 y el bloqueo del disco.)
2. Escriba la ACL para un cuarto grupo: `contador-externo`, que solo debe ver la colección «contabilidad» a través del proxy.

Referencias

1. WireGuard — sitio y documentación: https://www.wireguard.com/

2. Donenfeld, J. A. (2017). *WireGuard: Next Generation Kernel Network Tunnel.* NDSS.

3. Documentación de la herramienta de malla elegida (gestionada o autoalojada) — se referencia en `labs/03-01/acl.md` con fecha. `[VOLÁTIL — verificado: 2026-09]`

3.2 · Proxy inverso y autenticación centralizada

> Objetivos
>
> - Un solo punto de entrada con identidad
> - Poner SSO delante de un servicio

Una puerta, una recepción

Dentro de la malla hay varios servicios: el asistente, el panel de trazas, el gestor de documentos, quizá una interfaz de chat. Sin un **proxy inverso**, cada uno tiene su puerto, su certificado y su forma de pedir contraseña. Con él, hay **una sola dirección** (`https://asistente.el-tornillo.interno`) y **una sola identidad** (SSO).

Piezas `[VOLÁTIL — verificado: 2026-09]`

Pieza	Función	Opciones típicas
Proxy inverso	TLS, enrutamiento por nombre, cabeceras	uno con certificados automáticos y configuración corta (Caddy) o uno más configurable (Traefik, nginx)
Proveedor de identidad (SSO)	usuarios, grupos, MFA, sesiones	un proveedor autoalojado con *forward auth* (Authentik, Authelia) o uno completo (Keycloak)
Forward auth	el proxy pregunta al SSO antes de dejar pasar cada petición	lo traen los tres proxies

Criterio: tres empleados no justifican un proveedor de identidad pesado. Uno ligero con grupos y MFA basta; lo importante es que **cada servicio reciba de la cabecera quién es el usuario y a qué grupos pertenece**, porque el módulo 6 va a filtrar por eso antes de recuperar.

PROCEDIMIENTO · Laboratorio 3.2 · proxy + SSO delante de un servicio

```
cd ~/labs/el-tornillo && mkdir -p labs/03-02 && cd labs/03-02
cat > Caddyfile <<'EOF'
asistente.el-tornillo.interno {
    tls internal
    forward_auth sso:9000 {
        uri /outpost.goauthentik.io/auth/caddy
        copy_headers X-Authentik-Username X-Authentik-Groups
    }
    reverse_proxy asistente:8080
}
EOF
# docker-compose.yml con tres servicios: proxy (Caddy), sso (proveedor elegido), asistente
docker compose up -d
```

Prueba:

```
curl -k -I https://asistente.el-tornillo.interno/      # sin sesión → 302 al SSO
# iniciar sesión en el navegador como "contadora" (grupo: contabilidad)
# el asistente debe recibir: X-Authentik-Username: contadora  X-Authentik-Groups:
    contabilidad
```

Lo que debe ver: sin sesión, redirección al SSO; con sesión, el servicio de prueba imprime el usuario y sus grupos leídos **de la cabecera**. Nunca vuelve a pedir contraseña por su cuenta.
Entregable: `Caddyfile`, `docker-compose.yml`, y los tres usuarios creados (gerente, contadora, vendedor) con sus grupos. Commit: «Capa 3.2: proxy y SSO».
Nada: corre en el nodo de servicios. Es idéntico en A, B y C.

Cuándo NO usar esto **Proxy inverso y autenticación centralizada**

- No exponga el proxy fuera de la malla «para probar»: la regla de la lección anterior no tiene excepciones de prueba.
- No confíe en la cabecera de usuario si el servicio es alcanzable **sin pasar por el proxy** (por ejemplo, por su puerto interno): cualquier equipo de la malla podría inventarla. El servicio solo escucha al proxy.

PRÁCTICA · Práctica

1. ¿Qué pasa si la contadora está en dos grupos (contabilidad, gerencia)? ¿Cómo lo lee el asistente?

2. Diseñe la ACL del proxy: el panel de trazas solo para `gerencia` e `implementador`.

Referencias

1. Caddy — documentación de `forward_auth`: https://caddyserver.com/docs/
2. Authentik — documentación: https://docs.goauthentik.io/ · Authelia: https://www.authelia.com/
3. OWASP — *Top 10 for Large Language Model Applications* (LLM01, LLM06 sobre acceso y datos): https://owasp.org/www-project-top-10-for-large-language-model-applications/

3.3 · Acceso remoto del implementador

> Objetivos
>
> - Soporte remoto auditable y revocable
> - Escribir el runbook de acceso y de revocación

El acceso más peligroso es el suyo

Quien implementa tiene, durante meses, más poder sobre los datos del cliente que el propio gerente. Ese acceso hay que **diseñarlo** como se diseña el de cualquier otro usuario: con identidad propia, límites, registro y —sobre todo— una forma de **quitarlo** que no dependa de usted.

Principios

Principio	Cómo se aplica
Identidad propia	usuario `implementador` en el SSO, en su propio grupo; nunca la cuenta del gerente ni `root` compartido
MFA obligatoria	para el implementador antes que para nadie
Acceso por la malla, con ACL	SSH a los nodos solo desde el grupo `implementador`; sin puertos abiertos (3.1)
Llaves, no contraseñas	SSH con llave; la llave pública queda documentada; la privada nunca sale de su equipo
Registro	cada sesión SSH y cada acción administrativa queda en el registro del sistema, que el cliente puede leer
Acotado en el tiempo	acceso permanente solo mientras haya contrato de mantenimiento; se renueva, no se hereda
Revocable sin usted	el gerente puede quitarle el acceso con un procedimiento de una página, sin llamarlo

El runbook de acceso (lo que se entrega)

`labs/03-03/runbook-acceso.md`:

1. **Quién tiene acceso** y a qué (tabla: persona, cuenta, grupo, alcance).
2. **Cómo se da acceso** a un técnico nuevo (crear usuario en el SSO, añadir al grupo, añadir llave SSH, anotar en la tabla).
3. **Cómo se revoca** — el procedimiento que el gerente ejecuta solo: "`bash # en el nodo de servicios, como administrador local del cliente ./revocar.sh implementador # deshabilit el usuario en el SSO, quita la llave SSH de los # tres nodos, expulsa el equipo de la malla, deja registro `"
4. **Cuenta de emergencia** («rómpase el vidrio»): un usuario administrador local, con contraseña en sobre cerrado en la caja fuerte del cliente, que **no** usa el SSO. Se prueba una vez al trimestre y se rota después de cada uso.
5. **Qué se registra** y dónde se consulta.

> PROCEDIMIENTO · **Laboratorio 3.3**
>
> Escriba `revocar.sh` para su malla y su SSO, córralo contra un usuario de prueba, y verifique que el usuario revocado **no** puede entrar por ninguna de las tres vías (malla, SSO, SSH). Anote la prueba en el runbook.
> **Entregable:** `runbook-acceso.md` + `revocar.sh` probado. Commit: «Capa 3.3: acceso del implementador».
> Nada. Es igual en A, B y C.

Cuándo NO usar esto **Acceso remoto del implementador**

- No dependa de «yo me porto bien». El cliente no puede auditar intenciones; sí puede auditar registros.
- No conserve una puerta trasera «por si el cliente se equivoca». Si la necesita, es que la entrega (módulo 14) quedó incompleta.

PRÁCTICA · **Práctica**

1. El cliente termina el contrato un viernes por la noche. Liste, en orden, lo que hace el gerente el sábado para que usted ya no tenga acceso.
2. ¿Qué queda registrado si usted entra un domingo a las 2 a. m.? ¿Quién lo ve el lunes?

Referencias

1. NIST SP 800-53 Rev. 5 — controles de acceso (familia AC) y auditoría (AU): https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
2. OpenSSH — autenticación por llave y `AuthorizedKeysCommand`: https://www.openssh.com/manual.html
3. Módulo 14 de este curso — la entrega y el plan de continuidad.