

IA local para PyMEs · 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.

Qué se construye en este módulo

Malla privada: nunca se abren puertos

Levantar una malla
entre dos equipos

Proxy inverso y autenticación cen- tralizada

Un solo punto de en-
trada con identidad

Acceso remoto del implementador

Soporte remoto audi-
table y revocable

3.1 · Malla privada: nunca se abren puertos

Malla privada: 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.

En una tabla

Opción	Qué es
Servicio gestionado de malla (plan gratuito para pocos equipos)	el plano de control lo opera el proveedor; los datos van directamente al cliente; los datos van directamente al cliente; los datos van directamente al cliente
Plano de control autoalojado compatible	el mismo cliente, servicio de terceros
WireGuard a mano	túneles configurados manualmente

El comando, copiable

```
# 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>
```

Si no corre desde cero con un comando, no entra al curso.

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.

3.2 · Proxy inverso y autenticación centralizada

Proxy inverso y autenticación centralizada

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).

En una tabla

Pieza	Función	Opciones típicas
Proxy inverso	TLS, enrutamiento por nombre, cabeceras	uno con certificados a y configuración corta uno más configurab nginx)
Proveedor de identidad (SSO)	usuarios, grupos, MFA, sesiones	un proveedor autoa <i>forward auth</i> (Authenti o uno completo (Keyc
<i>Forward auth</i>	el proxy pregunta al SSO antes de dejar pasar cada petición	lo traen los tres proxie

El comando, copiable

```
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
```

Si no corre desde cero con un comando, no entra al curso.

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 podrá

3.3 · Acceso remoto del implementador

Acceso remoto del implementador

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.

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.

Entregables del módulo

- captura de status con los equipos, salida del nmap con todo cerrado, y la ACL en `labs/03-01/acl.md`.
- Caddyfile, `docker-compose.yml`, y los tres usuarios creados (gerente, contadora, vendedor) con sus grupos.
- `runbook-acceso.md` + `revocar.sh` probado.

Nunca se abren puertos.