



NVR Gateway – Arquitectura de Seguridad y Aislamiento para Acceso Remoto a Grabadores de Video

Resumen ejecutivo

NVR Gateway es una plataforma SaaS de acceso remoto seguro a grabadores de video (NVR), diseñada para entornos empresariales que exigen aislamiento total, trazabilidad absoluta y cero exposición directa de servicios.

Permite conectar, auditar y gestionar accesos a cualquier NVR (Reolink, TP-Link, ZoneMinder, etc.) mediante túneles SSH inversos cifrados, sin abrir puertos en la red local del cliente y sin depender de servicios en la nube de terceros.

Arquitectura de defensa en profundidad (Zero Trust)

1. Autenticación robusta y segmentada

- Dual authentication layer: usuarios NVR y administradores separados en tablas (users vs admin_users).
- Soporte nativo de **TOTP (Time-Based One-Time Password)** compatible con **Microsoft Authenticator**.
- Regeneración segura de claves 2FA con QR dinámico y auditoría de cambios.
- Bloqueo automático tras 3 intentos fallidos con persistencia en base de datos (login_attempts).

2. Control de acceso granular (IP + Módulo)

- **Whitelist de IPs por usuario:** soporte para rangos CIDR (ej. 192.168.1.0/24).
- Permisos por módulo (permisos_usuario_modulo) para usuarios no administradores.
- El usuario admin está técnicamente inmutable (no editable ni eliminable vía interfaz).

3. Firewall perimetral reactivo

- Detección automática de escaneos: 3 intentos con usuario no registrado → bloqueo IP en firewall_perimetral.
- Lista negra persistente con razón y timestamp.
- Bloqueo inmediato en la capa de aplicación antes de cualquier procesamiento.



4. Túnel de acceso remoto seguro

- Agente Windows ligero (NVR_Agent.exe) que inicia un **SSH reverse tunnel**.
- Configuración mediante config.ini descargable desde el panel (sin contraseñas: usa clave pública).
- Heartbeat cada 5 min → estado del túnel visible en tiempo real (agent_status.php).
- Aislamiento completo: cada cliente tiene su propio subdominio, usuario del sistema y base de datos independiente (arquitectura HestiaCP multi-tenant).

5. Auditoría total y no repudio

- **Configuración:** todos los cambios en branding se registran en config_audit_log (quién, qué, cuándo, IP).
- **Permisos:** modificaciones de acceso por módulo en permissions_audit_log.
- **Contraseñas:** cualquier cambio o restablecimiento se audita en password_change_log (método + IP).
- **Accesos:** todos los logins (éxito/fallo) se registran en user_logs y nvr_access_log.

6. Resiliencia y autogestión

- Módulo de recuperación de contraseña por email con token de un solo uso y expiración (1h).
- Validación anti-enumeración: siempre responde el mismo mensaje, independientemente de si el usuario existe.
- Protección contra bots: límite de 1 restablecimiento cada 15 min por usuario.
- Emails corporativos listos para producción (PHPMailer, TLS/SSL, modo prueba).

7. White-label y aislamiento visual

- Personalización total de marca: logo (.webp), fondo (.webp), favicon (.ico), títulos.
- Cambios parciales sin sobrescritura: solo se actualizan los campos modificados.
- Aislamiento visual por cliente: cada subdominio tiene su propia identidad visual sin interferencia.



Stack técnico

- **Backend:** PHP 8 + MySQL (PDO preparado, sin SQLi)
- **Frontend:** HTML5/CSS3/JS vanilla (sin dependencias externas)
- **Seguridad:** TOTP RFC6238, SSH reverse tunnel, HTTPS obligatorio, salida de datos sanitizada
- **Despliegue:** Listo para HestiaCP, Ubuntu 20.04+, sin root requerido
- **Librerías:** PHPMailer, sin frameworks (zero bloat)

NVR Gateway no es un plugin ni un hack: es un **producto SaaS listo para revender**, con arquitectura multi-tenant, defensa en profundidad, y auditoría de nivel forense. Ofrece a partners una solución blanca, técnicamente impecable, que resuelve el problema del acceso remoto seguro **sin comprometer la red del cliente**.

Listo para producción. Listo para white-label. Listo para generar valor.