WAI

GUÍA DE CONECTIVIDAD

Conectar tu base de datos a la plataforma WAI

Opciones de conectividad, características técnicas y modelo de seguridad para establecer la conexión entre tus bases de datos y la plataforma WAI.

AUDIENCIA: **Equipos de seguridad, sistemas y arquitectura**

VERSIÓN: **Mayo 2026**

NATURALEZA: **Documento descriptivo · No prescriptivo**

CONTENIDO

Índice

Si el índice aparece vacío al abrir el documento, sitúa el cursor sobre él y pulsa F9 para actualizarlo.

1. Objetivo 3
2. Garantías comunes a todas las opciones 4
3. Las cuatro opciones, en una tabla 5
4. Detalle de cada opción 6
Opción A — Base de datos expuesta a Internet 6
Descripción 6
Prerrequisitos 6
Características de seguridad 6
Información operativa 6
Opción B — Base de datos pública con whitelist por IP 7
Descripción 7
Prerrequisitos 7
Características de seguridad 7
Información operativa 7
Opción C — Túnel SSH a través de un bastión 8
Cómo funciona, en términos de negocio 8
Descripción técnica 8
Prerrequisitos 8
Características de seguridad 8
Información operativa 9
Opción D — Tailscale (solución enterprise) 10
Cómo funciona, en términos de negocio 10
Descripción técnica 10
Prerrequisitos 10
Posicionamiento enterprise 10
Modelo de seguridad 11
Modos de despliegue 11
Compatibilidad de instalación 12
5. Comparativa consolidada de seguridad 13
6. Información operativa para el equipo técnico 14
7. Glosario 15

1. Objetivo

WAI necesita leer datos de la base o las bases de datos que el cliente designe para analizarlos, generar dashboards, ejecutar agentes de negocio, detectar incidencias y materializar acciones automáticas.

Para hacerlo se requieren dos elementos:

- Una **conexión de red** entre la plataforma WAI y la base de datos.
- Unas **credenciales** de un usuario con los permisos mínimos necesarios (típicamente solo lectura).

Este documento describe las cuatro alternativas que se pueden usar para establecer la conexión de red. La función de WAI es proporcionar información completa sobre cada una; la elección depende de la política de seguridad interna, la infraestructura existente y las preferencias operativas del cliente.

2. Garantías comunes a todas las opciones

Las cuatro opciones se implementan respetando estos principios sin excepción:

- **Cifrado en tránsito**. Mediante TLS o WireGuard en todos los flujos.
- **Principio de mínimo privilegio**. WAI nunca solicita credenciales administrativas; el cliente crea un usuario aplicativo con los permisos estrictamente necesarios.
- **Credenciales cifradas en reposo**. Gestionadas en la plataforma a través de un secrets manager. Nunca se almacenan en repositorios ni en texto plano.
- **Revocación inmediata**. El cliente puede cortar el acceso en cualquier momento cerrando el firewall, eliminando el usuario o desactivando el túnel.
- **Auditoría completa**. WAI puede entregar registros de qué se consultó, cuándo y desde qué proceso.

3. Las cuatro opciones, en una tabla

#	Opción	Esfuerzo cliente	Esfuerzo WAI	Aislamiento de red
A	Base de datos expuesta a Internet	Bajo	Bajo	Bajo
B	Base de datos en Internet con firewall a IP de WAI	Bajo-Medio	Bajo	Medio
C	Túnel SSH a través de un bastión	Medio	Medio	Medio-Alto
D	Tailscale (solución enterprise)	Bajo-Medio	Bajo	Alto

Las secciones siguientes describen cada opción en detalle, con sus características, sus prerrequisitos y sus garantías de seguridad.

4. Detalle de cada opción

Opción A — Base de datos expuesta a Internet

Descripción

La base de datos del cliente es accesible directamente desde Internet mediante un endpoint público. WAI se conecta a ese endpoint utilizando las credenciales facilitadas. No existen restricciones adicionales de red por encima de las del propio motor.

Prerrequisitos

- La base de datos cuenta con un endpoint accesible públicamente desde Internet.
- El motor de base de datos admite cifrado TLS en sus conexiones.
- El cliente puede provisionar un usuario aplicativo con los permisos mínimos necesarios.

Características de seguridad

Capa	Característica
Cifrado en tránsito	TLS nativo del motor de base de datos
Autenticación	Usuario y contraseña
Restricción por origen	No aplica
Restricción por destino	No aplica
Trazabilidad	Logs propios del motor de base de datos
Revocación	Rotación o desactivación del usuario por parte del cliente

Información operativa

WAI necesita del cliente el endpoint público, el puerto, el nombre de la base de datos y un usuario con permisos mínimos. La conexión se establece con cifrado TLS activado.

Opción B — Base de datos pública con whitelist por IP

Descripción

La base de datos sigue teniendo un endpoint público, pero el firewall o Security Group del cliente solo permite conexiones entrantes desde la IP fija de salida de WAI. Cualquier intento desde otra IP es rechazado a nivel de red antes de llegar al motor.

Prerrequisitos

- La base de datos cuenta con un endpoint accesible desde Internet.
- El cliente puede gestionar reglas de firewall o Security Group sobre el segmento de red donde reside la base de datos.
- El motor de base de datos admite cifrado TLS en sus conexiones.

Características de seguridad

Capa	Característica
Cifrado en tránsito	TLS nativo del motor de base de datos
Autenticación	Usuario y contraseña
Restricción por origen	Sí, por IP de WAI a nivel de firewall
Restricción por destino	Implícita (solo la base de datos permitida)
Trazabilidad	Logs propios del motor + logs del firewall del cliente
Revocación	Eliminación de la regla de firewall por el cliente

Información operativa

WAI proporciona al cliente la IP fija de salida que debe permitirse en el firewall. El cliente añade una regla que admita conexiones entrantes únicamente desde esa IP, hacia el puerto estándar del motor de base de datos elegido. WAI recomienda forzar TLS a nivel de motor si este lo permite.

Opción C — Túnel SSH a través de un bastión

Cómo funciona, en términos de negocio

> *Imagina que tu base de datos vive en un edificio sin entrada directa desde la calle. El bastión SSH es una garita de seguridad situada en la entrada del recinto: solo quien tiene la llave correcta puede pasar por ella, y sólo desde ella se accede al interior. WAI atraviesa esa garita mediante una conexión cifrada (SSH), y desde dentro establece una segunda conexión, también cifrada, hasta la base de datos. En ningún momento la base de datos queda expuesta a Internet, y todo lo que entra por la garita queda registrado.*

Descripción técnica

La base de datos vive en una red privada sin acceso desde Internet. El cliente dispone de un servidor bastión con SSH expuesto que sí tiene conectividad interna hacia la base de datos. WAI se conecta primero al bastión por SSH y, a través de esa conexión cifrada, abre un túnel hasta la base de datos interna.

Prerrequisitos

- Existe un servidor bastión SSH operativo, accesible desde Internet, con conectividad interna hacia la base de datos.
- El cliente mantiene el bastión: parches, hardening, auditoría de accesos.
- El cliente puede crear un usuario SSH dedicado para WAI y gestionar claves públicas autorizadas en ese usuario.
- El bastión admite conexiones SSH (TCP/22) entrantes desde la IP fija de salida de WAI.

Características de seguridad

Capa	Característica
Cifrado en tránsito	Doble: SSH (transporte) + TLS del motor (aplicación)
Autenticación	Clave pública SSH (sin password) + usuario/contraseña del motor
Restricción por origen	Sí, IP de WAI a nivel de bastión
Restricción por destino	El bastión solo enruta al host/puerto de la base de datos
Trazabilidad	Logs SSH del bastión + logs del motor
Revocación	Eliminación de la clave pública en el bastión

Información operativa

El cliente provisiona un usuario SSH dedicado en el bastión, instala la clave pública que WAI proporciona, y configura el firewall del bastión para aceptar SSH solo desde la IP de WAI. WAI realiza la conexión usando autenticación por clave pública; nunca por contraseña.

Opción D — Tailscale (solución enterprise)

Cómo funciona, en términos de negocio

> *Imagina una red privada virtual que solo conecta unos pocos dispositivos previamente autorizados, como una sala con acceso por reconocimiento facial. La plataforma WAI y la base de datos del cliente se reconocen entre sí mediante una identidad criptográfica única — no por dirección IP, que podría falsificarse — y a partir de ese momento pueden hablarse como si estuvieran en la misma red local.*
>
> *Ningún dispositivo no autorizado puede entrar, ni siquiera escuchar el tráfico, porque toda comunicación va cifrada extremo a extremo. Y lo más importante: el cliente no abre ningún puerto en su firewall. Es el dispositivo del cliente el que sale hacia la red privada, no Internet la que entra hacia el cliente. Esto elimina por completo la superficie de ataque desde fuera.*

Descripción técnica

Tailscale es una solución enterprise de red privada Zero Trust basada en el protocolo WireGuard, el estándar moderno de VPN incorporado al kernel Linux mainline desde 2020 y avalado por auditorías criptográficas independientes. Crea conexiones peer-to-peer cifradas entre los nodos autorizados del cliente y de WAI, gestionando las identidades, claves y reglas de acceso desde un plano de control centralizado.

Prerrequisitos

- El cliente puede instalar un agente ligero (~30 MB) en un servidor de su red, junto a la base de datos. Si la base de datos está en un appliance donde no es viable instalar software adicional, se puede utilizar un servidor auxiliar como Subnet Router.
- El servidor donde se instala el agente puede establecer conexiones salientes hacia Internet (típicamente UDP/443 o UDP/41641, sin necesidad de reglas entrantes).
- La política interna del cliente admite el uso de software de terceros con cumplimiento SOC 2 Type II e ISO 27001.

Posicionamiento enterprise

- **Cumplimiento**: SOC 2 Type II e ISO 27001 a nivel proveedor (Tailscale Inc.). Informes disponibles a petición.
- **Adopción**: utilizado en producción por organizaciones como Mercado Libre, Instacart, Bloomberg, Roblox y entidades financieras europeas. Referencias públicas: tailscale.com/customers.
- **Arquitectura criptográfica**: publicada y revisada independientemente. Detalles: tailscale.com/security.
- **Soberanía del dato**: Tailscale coordina la conexión pero no procesa el contenido del tráfico. El cliente conserva la titularidad completa de sus datos.

- **Self-hosted opcional**: para clientes que requieren control total del plano de control existe la alternativa autohospedada Headscale.

Modelo de seguridad

Capa	Característica
Cifrado en tránsito	WireGuard end-to-end (ChaCha20-Poly1305) + TLS del motor
Autenticación	Identidad criptográfica por dispositivo, no por IP
Restricción por origen	Por identidad criptográfica del dispositivo autorizado
Restricción por destino	Declarativa mediante ACL: dispositivo + puerto exactos
Puertos abiertos en el cliente	Ninguno (solo conexiones salientes)
Trazabilidad	Admin console centralizada: logins, conexiones, cambios de ACL
Revocación	Inmediata desde el admin console (menos de un minuto)

Modos de despliegue

El cliente elige entre dos modelos según su preferencia operativa:

1. **Tailnet gestionado por WAI** (modo llave en mano). WAI provee las credenciales de invitación y opera el tailnet. El cliente solo instala el agente. WAI puede conceder acceso de lectura al admin console al cliente.
2. **Tailnet del cliente**. Si el cliente ya utiliza Tailscale, basta con invitar al nodo de WAI al tailnet existente con los tags apropiados.

En ambos modos, las ACLs garantizan que WAI solo accede a lo que esté explícitamente permitido.

Compatibilidad de instalación

El agente Tailscale es compatible con todos los entornos habituales. WAI acompaña al equipo técnico del cliente durante la instalación; los enlaces a la documentación oficial son los siguientes:

Entorno	Documentación oficial
Linux (Ubuntu, Debian, RHEL, CentOS, otros)	tailscale.com/kb/1031/install-linux
macOS	tailscale.com/kb/1016/install-macos
Windows	tailscale.com/kb/1022/install-windows
Docker	tailscale.com/kb/1282/docker
Kubernetes (operator)	tailscale.com/kb/1236/kubernetes-operator
Subnet Router	tailscale.com/kb/1019/subnets

El tiempo medio de instalación es de 5 a 15 minutos, según el entorno.

5. Comparativa consolidada de seguridad

La tabla siguiente resume, capa por capa, las características de las cuatro opciones para facilitar la comparación directa.

Capa	A. Pública	B. Whitelist IP	C. SSH Tunnel	D. Tailscale
Cifrado en tránsito	TLS	TLS	SSH + TLS	WireGuard + TLS
Restricción por IP de origen	No	Sí	Sí	Sí (por identidad criptográfica)
Restricción por destino	No	Implícita	Implícita	Sí, declarativa por ACL
Sin puertos abiertos en el firewall del cliente	No	No	Solo SSH	Ninguno
Trazabilidad centralizada	Limitada	Limitada	Logs del bastión	Admin console
Revocación inmediata	Rotar contraseña	Borrar regla firewall	Borrar clave SSH	Un clic en admin console
Esfuerzo de operación a largo plazo	Bajo	Bajo	Medio	Bajo
Compatible con BD sin IP pública	No	No	Sí	Sí
Identidad criptográfica por dispositivo	No	No	No	Sí
Cumplimiento del proveedor (SOC 2 / ISO 27001)	N/A	N/A	N/A	Sí

6. Información operativa para el equipo técnico

Dato	Valor
IP pública fija de salida de WAI (opciones A, B y C)	188.245.116.72
Estabilidad de la IP de salida	IP fija; cambios notificados con 30 días de antelación
Cifrado en tránsito	TLS 1.2+ en todos los flujos; WireGuard usa ChaCha20-Poly1305
Cifrado en reposo de credenciales	AES-256 a través de secrets manager
Auditorías independientes del proveedor Tailscale	SOC 2 Type II, ISO 27001 (informes a petición)
Plano de control Tailscale	Multi-región; self-hosted disponible vía Headscale

Materiales que WAI entrega al equipo técnico del cliente según la opción elegida:

- Bloque de ACL listo para pegar (opción D).
- Clave pública SSH para añadir al bastión (opción C).
- Lista de IPs y FQDN de origen y destino a configurar en firewalls (opciones A, B, C).
- Runbook de instalación específico del entorno elegido.

7. Glosario

- **ACL (Access Control List)** — documento de reglas que define qué dispositivo puede conectar a cuál y por qué puerto.
- **Bastión** — servidor intermedio con SSH expuesto, utilizado para acceder a recursos internos sin exponerlos directamente.
- **CIDR** — notación para expresar un rango de direcciones IP.
- **DMZ** — zona desmilitarizada, segmento de red expuesto a Internet con servicios públicos.
- **End-to-end (E2E)** — el tráfico va cifrado desde el origen hasta el destino, sin que ningún intermediario pueda leerlo.
- **FQDN** — nombre DNS completo de un dispositivo.
- **MagicDNS** — función de Tailscale que asigna un FQDN a cada dispositivo del tailnet automáticamente.
- **Subnet Router** — nodo Tailscale que anuncia un rango CIDR de una red interna, evitando instalar el agente en cada máquina.
- **Tag** — etiqueta criptográfica asignada a un dispositivo, contra la que se escriben las reglas de ACL.
- **Tailnet** — red privada virtual provista por Tailscale; cada organización tiene el suyo.
- **WireGuard** — protocolo de VPN moderno, simple y auditado; incorporado al kernel Linux desde 2020.
- **Zero Trust** — modelo de seguridad en el que ningún tráfico se considera confiable por defecto; todo se autentica e identifica explícitamente.

Documento mantenido por el equipo WAI · Mayo 2026 · Para casos de uso no contemplados en este documento, el equipo de WAI diseña una solución a medida.