

Especificación Técnica VPN B2B Administrada

Servicio de acceso seguro e interconexión con terceros

Documento	Especificación técnica genérica
Versión	1.0
Clasificación	Pública
Aplicación	Clientes, partners y terceros autorizados

Propósito. Definir el marco técnico, funcional y operativo del servicio VPN B2B Administrada de Nettix, incluyendo sus principios de arquitectura, controles de seguridad, criterios de interoperabilidad y responsabilidades generales, con el objetivo de facilitar integraciones seguras, consistentes y gobernadas con clientes y terceros.

Este documento está diseñado para publicación general. Los parámetros específicos de cada integración se documentan en un anexo técnico privado por cliente o tercero.

1. Descripción del servicio

VPN B2B Administrada es un servicio de Nettix orientado a habilitar conectividad segura entre usuarios, sistemas o aplicaciones de un cliente y redes o servicios de terceros. La plataforma actúa como punto de control y tránsito seguro, aplicando autenticación, segmentación, políticas de mínimo privilegio, registro de eventos y túneles cifrados hacia los destinos autorizados.

El servicio puede combinar acceso remoto para usuarios con interconexiones Site-to-Site hacia partners, proveedores, clientes corporativos u otras organizaciones que requieran conectividad IPsec.

2. Principios de diseño

Mínimo privilegio: Cada integración limita el acceso a orígenes, destinos, protocolos y servicios expresamente autorizados.

Segmentación: Las integraciones se mantienen lógicamente separadas y no habilitan acceso implícito a otras redes o clientes.

Modelo de servicio administrado: La plataforma es operada integralmente por Nettix bajo procesos, controles y responsabilidades definidos. Los clientes y terceros interactúan mediante interfaces, parámetros de integración y capacidades de servicio claramente establecidos.

Trazabilidad: Se mantienen registros operativos y de seguridad suficientes para soporte, auditoría y resolución de incidentes.

Interoperabilidad: La interconexión con terceros utiliza estándares ampliamente soportados, principalmente IPsec e IKEv2. Los mecanismos de acceso remoto para usuarios o sistemas autorizados se implementan de acuerdo con los requisitos del servicio.

3. Arquitectura lógica

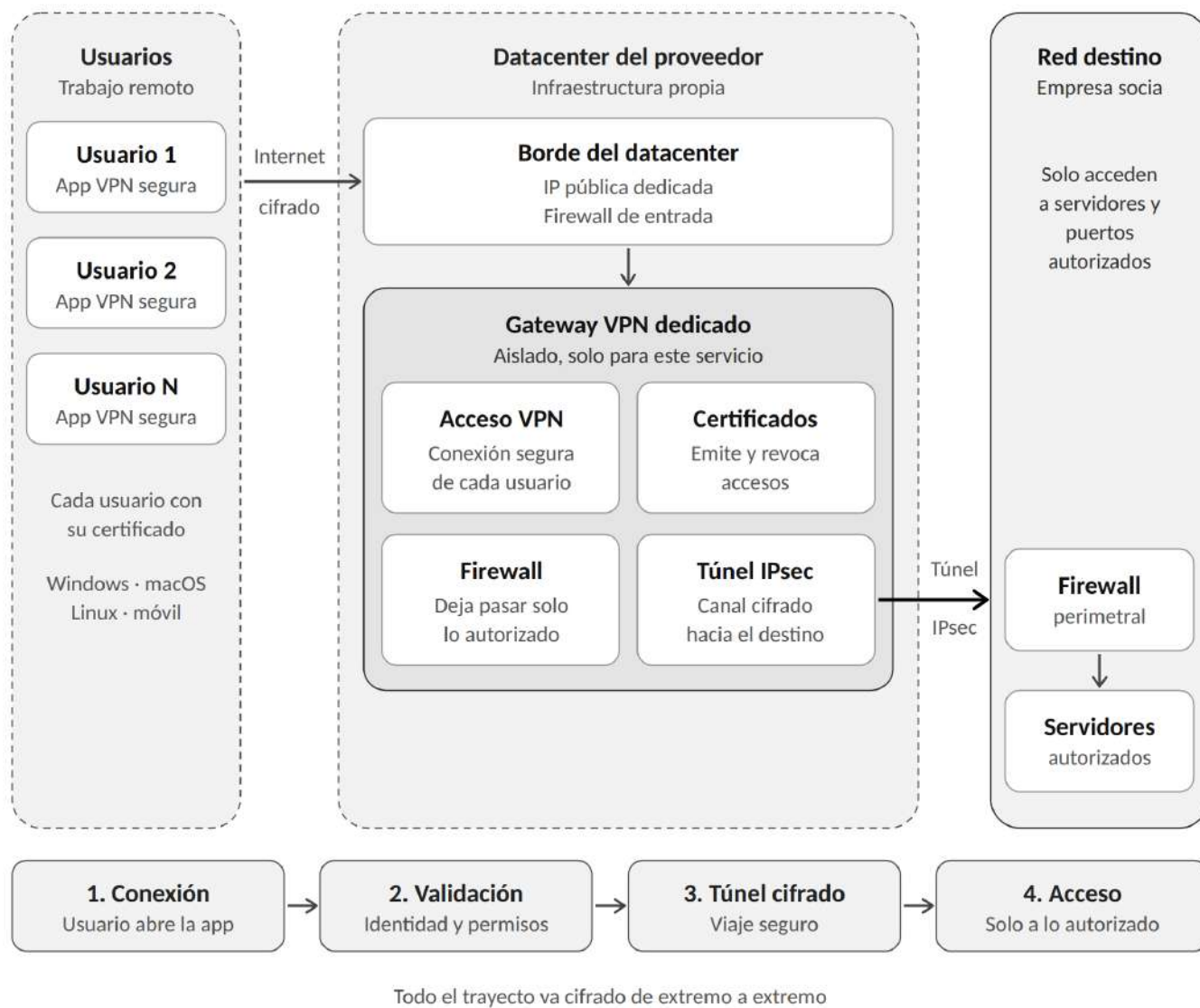


Figura 1. Arquitectura lógica de referencia del servicio.

4. Componentes funcionales

Componente	Función	Información de integración
Acceso remoto seguro	Permite a usuarios o sistemas autorizados ingresar al entorno de servicio mediante un canal cifrado.	Se documentan el método de acceso y los requisitos de autenticación aplicables.
Gateway de seguridad	Aplica políticas, terminación de túneles, encaminamiento controlado y separación lógica.	Se documentan sus funciones, interfaces y parámetros relevantes para la integración.
Control de acceso	Restringe comunicaciones por origen, destino, protocolo y servicio.	Se documenta la matriz de permisos de cada integración.
Túnel B2B	Interconecta la plataforma Nettix con un tercero mediante VPN Site-to-Site.	Se documentan los parámetros necesarios para la interoperabilidad.
Registro y monitoreo	Genera evidencia operativa y de seguridad asociada a conexiones y eventos relevantes.	Las capacidades de trazabilidad y monitoreo se definen de acuerdo con el alcance operativo y contractual del servicio.

5. Flujo de comunicaciones

1. Un usuario, sistema o aplicación autorizado establece una conexión segura hacia la plataforma Nettix.
2. El gateway de seguridad valida la política aplicable y permite únicamente el tráfico expresamente autorizado.
3. Cuando el destino pertenece a un tercero interconectado, el tráfico se encamina por el túnel B2B correspondiente.
4. El túnel Site-to-Site cifra la comunicación hasta el gateway remoto.
5. El tercero entrega el tráfico únicamente a los hosts o redes definidos para la integración.
6. Las conexiones relevantes quedan sujetas a controles de registro, monitoreo y soporte.

6. Controles de seguridad

- Cifrado de comunicaciones en tránsito.
- Autenticación individual o por sistema, según el tipo de acceso.
- Políticas de mínimo privilegio por integración.
- Segmentación lógica entre clientes, servicios e interconexiones.
- Control explícito de rutas y destinos autorizados.
- Registro de eventos de conexión y seguridad.
- Revocación de accesos y credenciales cuando corresponda.
- Parámetros criptográficos definidos de acuerdo con la compatibilidad y políticas de cada tercero.

7. Interoperabilidad VPN Site-to-Site

La plataforma está diseñada para interoperar con gateways empresariales que implementen estándares IPsec. Los valores concretos se acuerdan por integración y se consignan en un anexo técnico.

Parámetro	Criterio general
Intercambio de claves	IKEv2 preferido
Cifrado	AES con longitudes de clave acordes a la política del tercero
Integridad	SHA-2 u otro algoritmo mutuamente soportado
Autenticación	Clave precompartida o certificado, según el caso
Traffic selectors	Definidos explícitamente por red o host autorizado
PFS / DH	Configurado de acuerdo con los requisitos de la integración
Lifetimes	Acordados con el gateway remoto
NAT-T	Disponible cuando la topología de red lo requiera
DPD / recuperación	Soportado según la implementación y parámetros acordados

8. Acceso remoto

Cuando una solución requiera acceso de usuarios finales, Nettix puede proporcionar un canal de acceso remoto seguro. La tecnología concreta se administra como parte del servicio y puede evolucionar sin modificar la interfaz B2B del tercero, siempre que se mantengan los requisitos de seguridad y compatibilidad definidos.

Los usuarios reciben únicamente las rutas y permisos necesarios para las aplicaciones o destinos autorizados. No se presupone conectividad entre usuarios ni acceso general a redes internas.

9. Registro, monitoreo y soporte

- Supervisión del estado de los túneles y de eventos operativos relevantes.
- Registros de conexiones y eventos de seguridad según la política del servicio.
- Capacidad de diagnóstico coordinado con el tercero durante incidentes de interoperabilidad.
- Cambios de configuración sujetos a control operativo y validación técnica.

10. Modelo de responsabilidad

Parte	Responsabilidades generales
Nettix	Operación de la plataforma administrada, gateway de seguridad, controles de acceso, túneles bajo su gestión, registro y soporte.
Cliente	Definir usuarios, sistemas, aplicaciones y destinos que requieren acceso; aprobar la matriz de permisos y notificar altas/bajas.
Tercero / partner	Operar su gateway remoto, publicar los recursos autorizados y proporcionar los parámetros necesarios para la interoperabilidad.

11. Documentación específica por integración

Cada interconexión se complementa con un anexo técnico específico que documenta los parámetros necesarios para su implementación, validación, operación y soporte.

- Identificación de los gateways que participan en la conexión.
- Direcciones públicas necesarias para establecer el túnel.
- Redes o hosts incluidos en el dominio de cifrado.
- Parámetros IKE/IPsec acordados.
- Matriz de origen, destino, protocolo y servicio.
- Sentido permitido de las comunicaciones.
- Contactos técnicos y procedimiento de coordinación.

12. Gobernanza técnica del servicio

El servicio VPN B2B Administrada se gestiona bajo un modelo de operación centralizada en Nettix, con definición de responsabilidades, controles de seguridad, procedimientos de cambio y criterios de interoperabilidad.

La documentación del servicio establece las interfaces, capacidades y parámetros necesarios para su evaluación, integración y operación. Los elementos particulares de cada interconexión se formalizan mediante anexos técnicos específicos, permitiendo mantener una separación clara entre la definición del servicio, la configuración de cada cliente y la operación de la plataforma.

Cuando una integración, evaluación de seguridad o proceso de auditoría requiera información técnica adicional, esta se proporciona de acuerdo con el propósito, alcance y responsabilidades correspondientes.

13. Alcance de la documentación pública

La documentación pública del servicio se concentra en los elementos necesarios para comprender, evaluar e integrar la solución: arquitectura lógica, controles de seguridad, mecanismos de acceso e interconexión, criterios de interoperabilidad, responsabilidades operativas y capacidades de monitoreo.

Los componentes propios de la plataforma —como la topología física, redes de administración, inventario de infraestructura, direccionamiento interno, mecanismos de gestión y procedimientos operativos— se administran dentro del modelo de servicio de Nettix y no forman parte de la interfaz técnica requerida por clientes o terceros.

Asimismo, la información asociada a otros clientes, así como credenciales, secretos, claves privadas y material criptográfico, se mantiene separada de la documentación pública como parte de las prácticas de seguridad y gobernanza del servicio.

14. Resumen de capacidades

Capacidad	Disponibilidad
Acceso remoto seguro	Sí, cuando forma parte del alcance contratado.
VPN Site-to-Site	Sí, mediante estándares IPsec.
Múltiples integraciones B2B	Sí, con segregación lógica y políticas independientes.
Control por origen/destino/servicio	Sí.
Trazabilidad	Sí, dentro del alcance operativo y contractual.
Arquitectura administrada	Sí; la infraestructura subyacente es gestionada por Nettix.

Documento de referencia pública. Los parámetros contractuales, niveles de servicio, direccionamiento y configuración específica se formalizan en la propuesta comercial y/o anexo técnico correspondiente.