Access Server / Ficha técnica - Abril 2025

Access Server

Access Server es una solución de software VPN segura, escalable y fácil de implementar, ya sea en la nube o en sus propias instalaciones. Proporciona acceso remoto protegido a su red y recursos empresariales, e incorpora funciones esenciales de acceso basado en el modelo de confianza cero (ZTNA).

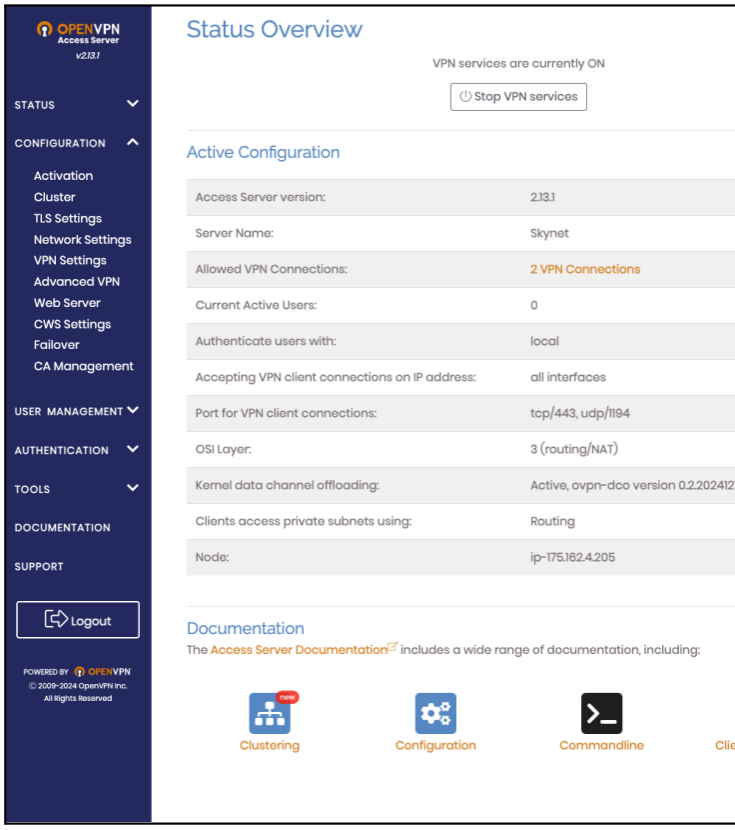
Permite que su personal —ya sea remoto, híbrido o presencial— trabaje de forma segura desde cualquier lugar, otorgando a su empresa mayor flexibilidad sin comprometer la seguridad. Puede gestionar el acceso remoto con permisos granulares y aplicar principios de confianza cero, garantizando que solo se otorgue acceso con privilegios mínimos y desde dispositivos y ubicaciones de confianza.

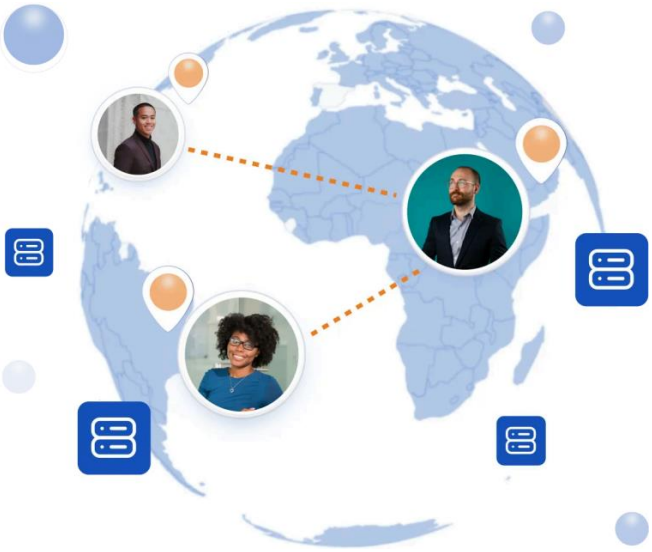
Además, Access Server ayuda a proteger los datos sensibles aislando sus aplicaciones SaaS críticas de Internet, haciéndolas accesibles únicamente a través de la VPN. Esto reduce eficazmente la superficie de ataque y neutraliza credenciales robadas o filtradas.

Para reforzar aún más la seguridad, Access Server ofrece compatibilidad con múltiples métodos de autenticación, una infraestructura PKI X.509 integrada para el aprovisionamiento de certificados y diversas herramientas para una verificación de identidad robusta.

A diferencia de las soluciones VPN heredadas basadas en hardware, Access Server elimina la complejidad y el alto costo de las redes seguras, gracias a sus opciones de implementación flexibles, licenciamiento accesible e interfaces web intuitivas tanto para administradores como para usuarios.

Con alta escalabilidad y soporte para funcionalidades ZTNA, Access Server es la solución de seguridad de red ideal para acompañar a su empresa en cada etapa de su crecimiento, permitiendo una operación segura y eficiente.





¿Cómo funciona Access Server?

Access Server es un software de servidor VPN que puede desplegarse tanto en la nube como en entornos locales, utilizando hardware estándar o máquinas virtuales. Es posible instalar múltiples instancias de Access Server en configuración de clúster de alta disponibilidad, lo que permite equilibrar la carga de conexiones y el tráfico de datos entre varios nodos para mayor resiliencia y rendimiento. Gracias a sus últimos desarrollos, Access Server también es capaz de gestionar el cifrado a nivel de núcleo (kernel), lo que maximiza la velocidad de transmisión de datos sin comprometer la seguridad.
Habilitar el acceso remoto es sencillo: basta con instalar Access Server en su red corporativa para que su equipo pueda conectarse de forma segura a las aplicaciones y recursos empresariales. Los usuarios solo necesitan la aplicación OpenVPN Connect en sus dispositivos para establecer la conexión.
Access Server es compatible con una amplia variedad de sistemas operativos: Windows, macOS, Linux, ChromeOS, iOS y Android.

Características	¿Qué es?
Administración simple y opciones de instalación flexibles	
Interfaz web administrativa	Interfaz intuitiva para gestionar configuraciones de red, controles de acceso, usuarios, grupos, ajustes de autenticación y más.
Interfaz de línea de comandos	Herramientas completas en línea de comandos para gestionar todos los aspectos de su Access Server.
Instalación offline / en red aislada	Flexibilidad para instalar Access Server en una LAN sin conexión a Internet. (Contacte a soporte de OpenVPN para la activación offline con su clave de licencia fija).
Disponibilidad en la nube	Imágenes preconfiguradas disponibles para Amazon Web Services, Google Cloud, DigitalOcean, Microsoft Azure, Oracle Cloud e IBM Cloud, lo que permite una implementación rápida y escalable.
Compatibilidad con virtualización	Imágenes preconfiguradas disponibles para Docker, Microsoft Hyper-V y VMWare ESXi, facilitando la implementación rápida y escalable.
Compatibilidad con sistemas operativos Linux	Compatible con Red Hat Enterprise Linux, Debian y Ubuntu.
Compatibilidad con bases de datos	Compatible con MySQL (por defecto utiliza base de datos SQLite).
Compatibilidad con cliente OpenVPN Connect	Los clientes OpenVPN Connect están disponibles para Android, iOS, Windows y macOS.
Incorporación sencilla	
Interfaz web del cliente	Interfaz simple para que los usuarios descarguen el cliente OpenVPN Connect junto con su perfil de conexión, gestionen sus perfiles y actualicen sus contraseñas.
Instalador incluido de OpenVPN Connect	Archivos de instalación que configuran OpenVPN Connect v3 con el perfil de conexión precargado. (Puedes generarlos desde la línea de comandos y distribuirlos a usuarios de Windows y macOS).
Distribución de perfiles de conexión por URL	Permite a los usuarios obtener su perfil ingresando la URL del servidor en la app Connect o haciendo clic en una URL personalizada. (Estas URLs se pueden generar desde la interfaz web de administración o CLI).
Soporte para archivo de configuración global	Archivo único que configura automáticamente la app Connect de los usuarios con los ajustes, perfiles y proxies preferidos, facilitando la gestión de dispositivos móviles.
Conectividad	
Data Channel Offload (DCO)	Aumenta la velocidad y el rendimiento de las conexiones VPN al trasladar el cifrado y descifrado del canal de datos al espacio del núcleo del sistema.
Compatibilidad con el protocolo OpenVPN	Utiliza el protocolo OpenVPN, ampliamente soportado por equipos de red. Es compatible con firewalls y funciona en modos TCP y UDP. Su naturaleza de código abierto facilita auditorías y revisiones.
Soporte completo para aplicaciones TCP, UDP, IP	Compatible con cualquier aplicación que se comunique mediante TCP o UDP, lo que garantiza que Access Server pueda proteger todo el tráfico de red que su organización necesita.
Alta disponibilidad y redundancia	
Agrupación de servidores (Server Clustering)	Aumenta la disponibilidad y la capacidad de carga al distribuir el tráfico de datos entre múltiples nodos de Access Server, lo que permite una escalabilidad horizontal y le ayuda a satisfacer las necesidades de una fuerza laboral en crecimiento.
Modo de conmutación por error (Failover Mode)	Ejecuta un segundo servidor en espera que puede asumir automáticamente si falla el servidor principal, ayudando a minimizar el tiempo de inactividad. Ambos servidores deben operar en una red de área local (LAN).

Características	¿Qué es?
Autenticación	
Compatibilidad con SAML	Centraliza la gestión de usuarios y proporciona acceso seguro y sencillo mediante inicio de sesión único (SSO), reduciendo la necesidad de múltiples credenciales y mejorando la experiencia del usuario.
Compatibilidad con LDAP, RADIUS y PAM	Gestiona y aplica autenticación de usuarios de forma coherente en todos los sistemas y servicios, desde dispositivos locales hasta la red corporativa, garantizando el acceso seguro a los recursos privados.
Compatibilidad con scripts post-autenticación	Amplía las capacidades integradas de Access Server utilizando Python3 para incluir MFA personalizado, verificaciones ZTNA, asignaciones automáticas de grupos (mediante LDAP, SAML o RADIUS), entre otros.
Autoridad certificadora y PKI X.509 incorporadas	Emite, gestiona e inspecciona certificados X.509 tanto para el Access Server como para los clientes, a fin de verificar identidades antes de establecer una conexión.
Compatibilidad con PKI externa	Permite la integración con otros sistemas de gestión de PKI X.509, como OpenSSL o Microsoft AD CS, para crear y distribuir pares de certificado/clave para el servidor y los clientes.
Autenticación multifactor (MFA)	Añade una capa adicional de seguridad mediante MFA a través de una app de autenticación (por ejemplo, Google Authenticator, Duo) u otros plugins generadores de TOTP.
Múltiples métodos de autenticación	Habilita diferentes sistemas de autenticación según el grupo o usuario, lo que permite aplicar validaciones más estrictas para usuarios en roles críticos que acceden a datos altamente sensibles.
Seguridad	
Verificación de postura del dispositivo *(vía script post-autenticación)***	Bloquea conexiones desde dispositivos con direcciones MAC o UUID no registradas, o con aplicaciones no compatibles (incluida la versión), para hacer cumplir la postura de dispositivo aprobada.
Verificación de contexto de ubicación *(vía script post-autenticación)***	Bloquea intentos de conexión desde direcciones IP no registradas para aplicar políticas de acceso basadas en ubicación y reducir el impacto de credenciales comprometidas.
Seguridad del canal de control	Soporta TLS-Crypt v2 por defecto para ofrecer resistencia a ataques post-cuánticos a nivel de TLS.
Cifrado del canal de datos	Soporta AES-256-GCM como cifrado por defecto para el canal de datos, y puede configurarse para incluir otros algoritmos como Chacha20-Poly1305 según prioridad.
Cumplimiento FIPS	Cumple con FIPS usando configuraciones por defecto y soporta modo FIPS (Red Hat, Ubuntu).
Control de acceso	Define qué usuarios y grupos tienen acceso a qué recursos, incluyendo redes, servicios IP y otros usuarios o grupos.
Renovación automática de certificado de CA	Genera automáticamente un nuevo certificado de CA cada año para evitar interrupciones de conexión por certificados expirados en los perfiles de usuario recién descargados.
Múltiples perfiles de usuario por cuenta	Evita interrupciones de conexión permitiendo a los usuarios tener perfiles adicionales, de los cuales al menos uno debe coincidir con el certificado de CA más reciente.
Política de bloqueo por fallos de autenticación	Previene ataques de fuerza bruta bloqueando automáticamente al usuario tras múltiples intentos fallidos. El umbral de intentos y la duración del bloqueo son personalizables.
Cifrado de servicios web	Protege el tráfico de la interfaz web de cliente y administración mediante certificados SSL autofirmados. (Puedes instalar certificados válidos para evitar advertencias del navegador y mejorar la seguridad).
Soporte para scripts del lado del cliente *(Windows y macOS)*	Permite ejecutar tareas automáticamente cuando el usuario se conecta (por ejemplo, al abrir el navegador o iniciar un programa).

Características	¿Qué es?
Enrutamiento simplificado	
Split-tunneling	Permite que el tráfico con destino a internet público evite pasar por la VPN, lo que ayuda a mejorar la velocidad de red, reducir la latencia y disminuir la carga en el Access Server.
Acceso de menor privilegio (ZTNA)	Define qué subredes IP o direcciones IP específicas puede acceder un usuario para proteger los recursos sensibles del servidor (incluso se puede restringir el acceso a un puerto específico).
NAT y enrutamiento	Requiere que todas las conexiones con Access Server (configurado en modo NAT) sean iniciadas por los clientes, o permite que tanto los clientes como el Access Server (configurado en modo Routing) inicien conexiones.
Enrutamiento sitio a sitio y punto a sitio	Permite conectar un router (utilizado como puerta de enlace) en una ubicación con el Access Server en otra, extendiendo la red empresarial a oficinas remotas.
Enrutamiento basado en nombres de dominio*	Utiliza nombres de dominio en lugar de subredes IP para simplificar el enrutamiento de red, permitiéndote definir y configurar fácilmente el acceso a tus recursos.
Automatización y registros	
Informes de registro (Log reports)	Muestra conexiones anteriores realizadas al Access Server, junto con metadatos relevantes como identidad del usuario, dirección IP, duración de la conexión y más.
Registro remoto (Remote logging)	Escribe y almacena los datos de registro del Access Server en el daemon syslog local o en un servidor syslog externo, permitiendo una gestión centralizada de registros, auditorías simplificadas y mayor cumplimiento normativo.
API XML-RPC y REST	Se integra con otros sistemas para gestionar programáticamente el Access Server, automatizar flujos de trabajo y más.

*Próximas funciones ** Próximamente más funciones y mejoras

Escucha lo que dicen nuestros clientes

“Tenemos un caso de uso en el que ejecutamos dos VPN en paralelo. OpenVPN supera por completo a nuestro otro servidor VPN en términos de velocidad.

— Thomas A., Presidente

“Access Server combina potencia, versatilidad y seguridad en una solución asequible, resolviendo desafíos clave como la productividad remota, la protección de datos sensibles y la escalabilidad.”

— Richard V., CTO

“Migramos nuestras soluciones VPN hace unos 4 años e identificamos a OpenVPN como la solución ideal para nosotros. Cumplía con muchos de nuestros requisitos, especialmente en lo relacionado con la autenticación en dos pasos (2FA) y el enfoque de confianza cero en el acceso de los usuarios mediante perfiles. El precio también es muy competitivo. El soporte al cliente es muy bueno.”

— Daniel C., Jefe de TI

Vea lo que otros dicen sobre Access Server en G2