



- **Experiencia sencilla "tipo oficina" desde cualquier lugar**
- **Fácil de implementar, gestionar y controlar**
- **SonicWALL Aventail Unified Policy**
- **Acceso seguro a cualquier aplicación**
- **Control de Split Tunneling**

### Experiencia sencilla "tipo oficina"

Hoy en día, las empresas dependen cada vez más de los empleados remotos que desempeñan su labor en oficinas domésticas, de los partners externos que utilizan la extranet y de los ejecutivos que trabajan en sus dispositivos gestionados mientras viajan. Estos usuarios necesitan contar con un acceso completo a las aplicaciones críticas de negocio (incluidas las aplicaciones "back-connect", como soft phones VoIP y asistencia técnica remota) como si estuvieran en la oficina. Los administradores de TI se enfrentan al reto de proporcionar a los usuarios un acceso completo, ofreciendo al mismo tiempo la máxima seguridad de escritorio, detección de cortafuegos personales y control de Split Tunneling.

SonicWALL® Aventail® Connect Tunnel™ ofrece a los usuarios de las soluciones SonicWALL Aventail E-Class SSL VPN una experiencia "tipo oficina" sencilla y segura. Connect Tunnel es un cliente que se puede poner a disposición a través de la Web. Permite a los usuarios de escritorios y portátiles remotos autorizados acceder de forma segura a todos los recursos de la red corporativa desde cualquier lugar. Connect Tunnel ofrece el método más sencillo y completo de acceso remoto seguro. Además, proporciona un elevado nivel de seguridad para los usuarios de WLAN y viajeros de negocios que necesiten acceder a todos los recursos desde el exterior de la empresa.

### Prestaciones y ventajas

**Experiencia sencilla "tipo oficina" desde cualquier lugar.** Los usuarios de dispositivos remotos gestionados por el departamento de TI (como PCs de escritorio y portátiles autorizados) pueden trabajar como si estuviesen en la oficina, ya que disfrutan del mismo acceso a los recursos de red que los usuarios de la LAN corporativa. Connect Tunnel ofrece el máximo nivel de transparencia y una facilidad de uso inigualable. Incluye inicio de sesión único, detección automática de red e integración con marcadores de terceros. Los usuarios remotos no tienen que preocuparse por cómo acceder a los recursos requeridos: solo tienen que hacer clic en un icono del dispositivo remoto gestionado por el departamento de TI y autenticarse de forma automática para acceder a la red a través de Internet. Basándose en políticas administrativas, la tecnología SonicWALL Aventail Smart Access™ determina e implementa automáticamente el método de acceso remoto más adecuado para acceder a los recursos corporativos que el usuario necesite.

**Fácil de implementar, gestionar y controlar.** Los administradores pueden instalar Connect Tunnel en dispositivos gestionados sin ninguna dificultad, implementar nuevas versiones de forma automática y modificar la configuración sin necesidad de mayor intervención. El cliente ligero Aventail Connect Tunnel puede preinstalarse en un dispositivo gestionado, o implementarse mediante una única descarga desde un portal Web. Este cliente ligero tan fácil de implementar constituye la alternativa ideal a las VPN IPsec con "cliente pesado".

**SonicWALL Aventail Unified Policy™.** Centraliza el control de todos los usuarios, grupos, recursos y dispositivos, permitiendo a los administradores establecer rápidamente una norma para todos los objetos. Gracias a SonicWALL Aventail End Point Control™ podrá identificar y reforzar las políticas de

seguridad para todos los dispositivos Windows®, Macintosh® y Linux®, detectando automáticamente criterios como el software antivirus, cortafuegos personales, aplicaciones, directorios, nombres y tamaños de archivos, marcas de hora, así como versiones, dominios o entradas del registro de Windows.

**Acceso seguro a cualquier aplicación** (como p. ej. VoIP y asistencia técnica remota). La arquitectura única de SonicWALL Aventail Smart Tunneling™ combina el control a nivel de aplicación de la tecnología SSL con las amplias posibilidades de acceso de un túnel de nivel 3. De esta forma, los usuarios gozan de una variedad de aplicaciones sin precedentes con soporte para los protocolos UDP, TCP y IP, control granular y bidireccional del acceso para todo tipo de aplicaciones, incluyendo las aplicaciones "back-connect", como VoIP y asistencia técnica remota. Es posible interrogar al dispositivo VoIP y autenticar al usuario antes de establecer la conexión. De este modo, se previenen los ataques de códigos maliciosos.

**Control de Split Tunneling.** Permite al departamento de TI determinar si el usuario debe tener capacidad para iniciar sesión en varias redes durante su sesión VPN. NAT traversal, la detección de proxy, traversal y la adaptación dinámica para reducir los conflictos de direcciones garantizan el acceso universal a las aplicaciones. Connect Tunnel puede integrarse fácilmente con marcadores de Internet y otros productos de software para escritorios. Además, puesto que proporciona acceso completo a las aplicaciones requeridas y ofrece, al mismo tiempo, un alto nivel de control de políticas y seguridad, Connect Tunnel constituye una alternativa sencilla y efectiva a las engorrosas implementaciones IPsec.

**Connect Tunnel**

E-Class EX-750  
01-SSC-7704  
Add-on

E-Class EX-1600  
Incluido

E-Class EX-2500  
Incluido

**Cómo funciona SonicWALL Aventail Connect Tunnel**

El cliente ligero SonicWALL Aventail Connect Tunnel puede preinstalarse en un dispositivo gestionado por el departamento de TI o descargarse desde un portal Web. Una vez instalado el cliente Connect Tunnel, el usuario ya no necesita la página Web ni el portal para acceder a los recursos de red para los que está autorizado y disfrutar de una experiencia "tipo oficina". Con solo hacer clic en el icono SonicWALL Aventail Connect en su escritorio, el usuario puede autenticarse automáticamente y acceder a la red mediante Internet desde el dispositivo gestionado.

Especificaciones técnicas	Explorador	Notas
<b>Sistema operativo</b> <b>Windows Vista®</b> <b>Windows XP Pro, SP2</b> <b>Windows 2000 Pro, SP4</b> <b>Windows XP Home, SP2</b>	No disponible	Se requieren derechos de administrador de Windows para la instalación
<b>Plataforma de Windows Server:</b> <b>Windows 2003 Server</b> <b>Windows 3000 Server, SP4</b>	No disponible	Se requieren derechos de administrador de Windows para la instalación
<b>Macintosh OS X v 10.5</b>	No disponible	Se requieren derechos de administrador para la instalación No soporta End Point Control Macintosh OS X v 10.5 solo se ha probado en ordenadores Intel
<b>Kernel de Linux 2.4.20 o posterior</b>	Mozilla Firefox 2.0  (Mozilla Firefox 1.5)	Se requieren derechos de administrador para la instalación Solo se requiere explorador para la detección de proxy No soporta End Point Control

Si desea obtener más información sobre las soluciones SonicWALL Aventail E-Class SSL VPN, visite [www.sonicwall.com](http://www.sonicwall.com).

**Soporte de ventas España**

Teléfono gratuito: 900.811.056

Teléfono: +31 (0) 411.617.815

Correo electrónico:

[sales\\_support-europe@sonicwall.com](mailto:sales_support-europe@sonicwall.com)

**Soporte de ventas Europa – otros países**

Teléfono: +31 (0) 411.617.811

Correo electrónico:

[sales\\_support-europe@sonicwall.com](mailto:sales_support-europe@sonicwall.com)

**Oficina en Portugal/España**

Teléfono: +34.653.94.82.87

Correo electrónico:

[spain@sonicwall.com](mailto:spain@sonicwall.com)

PROTECCIÓN AL SERVICIO DE SU NEGOCIO™