SonicWALL® | Aventail™
E-CLASS SSL VPN

SECURE REMOTE ACCESS

SonicWALL Aventail Connect Tunnel

- **Easy "in-office" experience from anywhere**
- **Easy-to-deploy, -manage and -control**
- **SonicWALL Aventail Unified Policy**
- **Secure access to any application**
- **Split tunnel control**

Easy "In-Office" Experience

Today, more and more business is being done remotely by home office workers, traveling executives with managed laptops and extranet partners. These mission-critical users need the same full access to key business applications—including back-connect applications like VoIP soft phones and remote help desk—as if they were in the office. The challenge for IT is to provide full access while ensuring strong desktop security, split-tunneling control and personal firewall detection.

SonicWALL® Aventail® Connect Tunnel™ offers SonicWALL Aventail E-Class SSL VPN users an easy and secure, "in-office" experience alternative. Connect Tunnel is a Web-deployable client that provides users of authorized remote desktops and laptops with secure everywhere access to the entire corporate network. Connect Tunnel delivers the easiest, most complete method of secure remote access available, and is ideal for providing strong security for wireless Local Area Network (LAN) users and road warriors who need full access away from the office.

Features and Benefits

Easy "in-office" experience from anywhere provides remote users of IT-managed devices (such as authorized desktops and laptops) with the same access to network resources as they would have on the office LAN—for a complete "in-office" experience. Connect Tunnel delivers the highest level of transparency and unmatched ease-of-use for the user, including single sign-on, network auto-discovery and integration with third-party dialers. Users don't have to think about how to gain full access to their resources. With a click of an icon on the IT-managed remote device, the user can automatically authenticate to the network over the Internet. SonicWALL Aventail Smart Access™ technology automatically determines and deploys the right remote access method to the corporate resources that the user needs, based on administrative policy.

Easy-to-deploy, -manage and -control, with administrators easily installing Connect Tunnel on managed devices, and automatically updating new versions and making configuration changes without further intervention. The lightweight Aventail Connect Tunnel client can be preinstalled on an IT-managed device, or deployed via a one-time download from a Web portal, offering an ideal easy-to-deploy alternative for "fat client" IPSec VPNs.

SonicWALL Aventail Unified Policy™ centralizes control of all users, groups, resources and devices, allowing administrators to quickly set policy with a single rule across all objects. Using SonicWALL Aventail End Point Control,™ you can identify and enforce security policy for all Windows,® Macintosh® and Linux® devices, by automatically detecting such criteria as anti-virus software, personal firewalls, applications, directories, file names and sizes, timestamps, or Windows versions, domains, and registry entries.

Secure access to any application—including VoIP and remote help desk—using SonicWALL Aventail Smart Tunneling™ technology, a unique architecture that combines the application layer control of SSL with the application reach of a Layer 3 tunnel. This provides users unparalleled application breadth, including support for UDP, TCP and IP protocols, as well as granular bi-directional access control for any applications, including back-connect applications like VoIP and remote help desk. A VoIP device can be interrogated and the user authenticated before connection, preventing the threat of malware attacks.

Split tunnel control enables IT to control a user's ability to log onto multiple networks while on the VPN. NAT traversal, proxy detection, traversal and dynamically adaptive mitigation of address conflicts ensure universal application access. Connect Tunnel is easily integrated with Internet dialers and other desktop software products. And since users get full access to the applications they need, along with complete policy control and security, Connect Tunnel also provides an easy and effective alternative to cumbersome IPSec deployments.

SONICWALL®
PROTECTION AT THE SPEED OF BUSINESS™

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

E-Class EX-1600
Included

E-Class EX-2500
Included

How SonicWALL Aventail Connect Tunnel Works

The lightweight SonicWALL Aventail Connect Tunnel client can be preinstalled on an IT-managed device, or downloaded from a Web portal. Once the Connect Tunnel client is installed, the user no longer needs to access a Web site or portal to gain access to all their authorized network resources, and have a complete "in-office" experience. With a click on the SonicWALL Aventail Connect icon on the desktop, the user can automatically authenticate and get access from the IT-managed device to the network over the Internet.

Specifications Operating System	Browser	Notes
Windows Vista® **Windows XP Pro, SP2** **Windows 2000 Pro, SP4** **Windows XP Home, SP2**	N/A	Windows administrator rights required for installation
Windows Server Platform: **Windows 2003 Server** **Windows 3000 Server, SP4**	N/A	Windows administrator rights required for installation
Macintosh OS X v 10.5	N/A	Administrator rights required for installation No support for End Point Control Macintosh OSX v 10.5 has been tested only on Intel computers
Linux kernel 2.4.20 or later	Mozilla Firefox 2.0 (Mozilla Firefox 1.5)	Administrator rights required for installation Browser required only for proxy detection No support for End Point Control

For more information about SonicWALL Aventail E-Class SSL VPN solutions, please visit **www.sonicwall.com.**

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

SONICWALL®
PROTECTION AT THE SPEED OF BUSINESS™