



- **Increases productivity and return on investment**
- **Lowers IT overhead and total cost of ownership**
- **Easy-to-use from any end point**
- **Robust mobile solution**
- **Access to all application platforms**
- **Supports VoIP and remote help desk**
- **Eliminates routing conflicts**
- **Single access gateway**
- **Rapid set-up and deployment**
- **Easy-to-control with Unified Policy Management**

#### Easy, Secure and Clientless Remote Access for the Enterprise

With maturing mobile technologies, booming global markets and heightened focus on disaster preparedness, remote access control has become a business imperative. IT is now mandated with providing secure remote access that is easy for users and cost-effective to implement. Client-based VPNs can be cumbersome to use and manage. SonicWALL® Aventail® E-Class SSL VPN solutions deliver a complete remote access control solution, without escalating infrastructure costs or complexity. SonicWALL Aventail E-Class SSL VPNs provide complete application access with full security, control of the end point and unified policy management. This easy-to-use, easy-to-control solution increases productivity by providing employees and extranet business partners with secure, clientless access to the resources they need from any device, anywhere, with the unmatched security of SSL VPN.

This solution is a part of SonicWALL's new E-Class—a line of premium, enterprise-class solutions offering outstanding protection and performance while delivering elegant simplicity and unparalleled value. The E-Class portfolio of products and services includes a comprehensive line of network security, e-mail security and secure remote access solutions.

#### Features and Benefits

**Increases productivity.** SonicWALL Aventail E-Class SSL VPNs work in more places, including home PCs, kiosks, PDAs and unmanaged devices over wired and wireless networks. SonicWALL Aventail SSL VPNs make your users more productive by providing easy access to more applications from more environments—including Windows, Linux, Macintosh and mobile devices—than any other secure access solution.

**Lowers IT overhead and total cost of ownership.** SonicWALL Aventail E-Class SSL VPN lowers IT costs by enabling network managers to easily deploy and manage a single secure access gateway that extends remote access via SSL VPN for both internal and external users to all network resources—including Web-based, client/server and host-based applications. SonicWALL Aventail SSL VPNs are clientless or use lightweight Web-delivered clients, reducing management overhead and support calls.

**Easy-to-use from any end point.** SonicWALL Aventail E-Class SSL VPN technology provides transparent access to network resources from any network environment or device. A SonicWALL Aventail SSL VPN provides a single gateway for all access and a common user experience across all platforms—including Windows®, Windows Vista, Windows Mobile, Linux® and Macintosh®—from managed or unmanaged devices. An award-winning anti-spam engine coupled with end-to-end attack monitoring ensures the most effective and current protection from spam attacks.

**Robust mobile solution.** SonicWALL Aventail E-Class SSL VPNs provides the most robust secure access solutions for mobile PDAs and smartphones, featuring Session Persistence across office, home or mobile IP addresses without re-authentication.

**Access to all application platforms.** SonicWALL Aventail Smart Tunneling™ delivers fast and easy access to all applications—whether they are Web-based, client/server, server-based or host-based—over a unique architecture that combines the application layer control of SSL with the reach of a Layer 3 tunnel.

**Supports VoIP and remote help desk.** SonicWALL Aventail Smart Tunneling™ provides granular, bidirectional access control for back-connect applications like VoIP and remote help desk.

**Eliminates routing conflicts.** Adaptive addressing and routing dynamically adapts to networks, eliminating addressing and routing conflicts common with other solutions.

**Single access gateway.** SonicWALL Aventail E-Class SSL VPNs give network managers a single secure access gateway for all users, internal and external, to all resources with complete control.

**Rapid set-up and deployment.** All SonicWALL Aventail E-Class SSL VPNs are easily set-up and deployed in just minutes. SonicWALL Aventail's Set-up Wizard provides an easy "out-of-the-box" experience with rapid set-up and deployment.

**Easy-to-control with Unified Policy Management.** SonicWALL Aventail Unified Policy™ offers easy object-based policy management of all users, groups, resources and devices, while enforcing granular control based on both user authentication and end point interrogation. Policy Zones can ensure unauthorized access is denied, or quarantined for remediation.

## Detect the security of any end point

### Robust interrogation for secure control of the end point

Only SonicWALL Aventail End Point Control™ (EPC™) lets you enforce granular access control rules for Windows®, Windows Vista, Windows Mobile, Macintosh® and Linux® end points. EPC combines pre-authentication interrogation to confirm end-point criteria like anti-virus updates. SonicWALL Aventail Policy Zones™ apply detected end point criteria to automated policy enforcement. For example, a user's access may be quarantined—and redirected to remediation instructions—until a security patch is installed. Device Watermarks allow easy access revocation of lost or stolen devices, based upon detection of client certificates. SonicWALL Aventail's Virtual Keyboard stops keystroke sniffers on untrusted end points.

### Advanced EPC for ultimate protection

Optional SonicWALL Aventail Advanced EPC™ combines granular end point control detection with superior data protection. Advanced Interrogator simplifies device profile set-up using a comprehensive predefined list of anti-virus, personal firewall and anti-spyware solutions for Windows platforms, including version and currency of signature file update. Cache Control purges browser cache, session history, cookies and passwords. Secure Desktop creates a virtual encrypted environment that prevents sensitive information from being left behind. SonicWALL E-Class Aventail SSL VPNs also block suspect e-mail attachments in Outlook Web Access or Lotus iNotes, or block access to financial data or patient records. On SonicWALL Aventail SSL VPNs, connections are closed by default, providing "deny all" firewall-style protection.

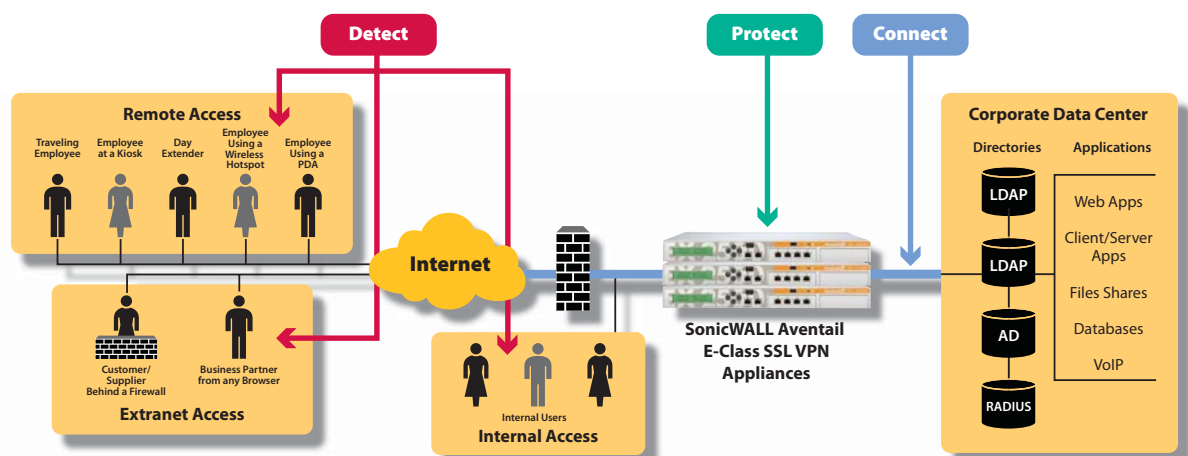
## Protect your enterprise resources with ease

### Streamlined policy management

With its context-sensitive help and Setup Wizard, a SonicWALL Aventail E-Class SSL VPN is easy to set-up and deploy. The extensible, object-based SonicWALL Aventail Unified Policy™ model consolidates control of all Web resources, file shares and client-server resources in a single location, so that policy management can take only minutes. Groups can be populated dynamically based on RADIUS, LDAP or Active Directory authentication repositories, including nested groups. SonicWALL Aventail SSL VPNs support Single Sign-On (SSO) and forms-based Web applications. And users can easily update their own passwords without IT assistance. Also, SonicWALL Aventail Policy Replication lets IT easily replicate policy across multiple appliance nodes, either in the same cluster or in a geographically-distributed fashion.

### Intuitive management and reporting

The SonicWALL Aventail Management Console™ provides a rich, centralized set of monitoring capabilities for auditing, compliance, management and resource planning. Optional Aventail Advanced Reporting™ audits who accessed what enterprise resources, at what time, from which remote location, using standard or custom reports that can be accessed from any Web browser. Visual tools provide real-time information on system state and direct, intuitive options for managing system objects.



- Detect** SonicWALL Aventail's End Point Control detects the identity and security state of the end device
- Protect** SonicWALL Aventail Unified Policy enforces devices access control, ensuring users access only to authorized applications
- Connect** SonicWALL Aventail Smart Access and Smart Tunneling ensure easy, secure user access to all network resources

SonicWALL Aventail E-Class Remote Access Solution provides secure access for all users, devices and applications.

## **Connect users to resources—simply and seamlessly**

### **Broadest application access from the most end points**

SonicWALL Aventail E-Class SSL VPNs deliver intelligent access to Web-based, client/server, server-based, host-based and back-connect applications such as VoIP. SonicWALL Aventail SSL VPNs work seamlessly across Windows, Windows Vista, Windows Mobile, Linux or Macintosh platforms, from desktops, laptops, kiosks, PDAs and smartphones, as well as application-to-application. This significantly increases productivity, while reducing support costs. From the user's perspective, SonicWALL Aventail Smart Access™ dynamically determines and deploys the appropriate access method and security level based on the type and state of the device, user identity and resources needed. Adaptive addressing and routing dynamically adapts to networks, eliminating conflicts. Smart Access streamlines installation and activation of any required agents on Windows devices according to Microsoft standards.

### **Clientless Web-based access or full “in-office” experience**

SonicWALL Aventail E-Class SSL VPNs offer both clientless browser-based access and full access to client/server and legacy applications from Windows, Windows Vista, Windows Mobile, Macintosh and Linux environments. SonicWALL Aventail WorkPlace™ delivers a policy-driven, device-optimized Web portal that provides easy access to Web-based and client/server applications from desktops, laptops, PDAs, smartphones, even from wireless hot spots and kiosks. Users can define shortcuts to frequently-used resources. Workplace can be customized with different logos and color schemes for partners and employees. SonicWALL Aventail WorkPlace access is well-suited for devices not managed by your organization. SonicWALL Aventail Connect™ access delivers an “in-office” experience for Windows, Windows Vista, Windows Mobile, Macintosh and Linux users, enabling full access to client/server and Web-based applications and all other network resources. Enabled through a lightweight, Web-deployable agent, or through an easily-provisioned standard MSI installation, SonicWALL Aventail Connect is ideal for full access from IT-managed devices that require strong desktop security, split-tunneling control and personal firewall detection. SonicWALL Aventail Smart Tunneling™ offers a Layer 3 technology that supports UDP, TCP and IP protocols, and back-connect applications like VoIP. In NAT mode, no set-up of IP address pools is required.

### **A solution customized to your users' needs**

Optional SonicWALL Aventail Native Access Modules™ offer additional native access to Windows Terminal Services, as well as native support for load-balanced Citrix farm environments via the WorkPlace Portal as an alternative to expensive Citrix nFuse implementations. SonicWALL Aventail Host Access Modules™ directly integrate industry-leading AttachmateWRQ terminal emulation with your SonicWALL Aventail E-Class SSL VPN to access a wide range of host-based applications in IBM, UNIX and OpenVMS environments.

### **Most complete access solution for mobile devices**

SonicWALL Aventail SSL VPNs offers Web- and client-based access to critical network resources from any wireless network environment with complete security and control, including Windows Mobile-powered devices, Symbian smartphones, DoCoMo iMode devices and WAP-enabled devices. SonicWALL Aventail SSL VPN solutions provide centralized management of all devices with granular access control and the ability to prohibit access from the device if it's lost or stolen. And with Session Persistence, mobile users can have the flexibility to retain a current session as they switch between networks—on the go between office, commute, home and hotel—without needing to re-authenticate.

### **Reliable high availability and flexibility**

For added reliability, SonicWALL Aventail E-Class SSL VPNs offer active/active high availability (HA) with integrated load balancing and active/active stateful failover on the EX-2500 and EX-1600, eliminating the added cost of a third-party load balancer. And with an optional Aventail Spike License Pack, you can temporarily and cost-effectively increase your remote user count to the maximum capacity of those SonicWALL Aventail appliances for disaster recovery or planned business cycle peaks, whether it's a few dozen or a few thousand additional users.

### **The clear business choice**

SonicWALL Aventail E-Class SSL VPNs include the market-leading EX Series of SSL VPN appliances, offering your business the best solution for secure remote access control. With SonicWALL Aventail, you can enhance your enterprise network security, increase your mobile workforce productivity for greater return on investment (ROI) and reduce IT overhead for a lower total cost of ownership (TCO). SonicWALL Aventail's best-of-breed technology gives you flexible access options for disaster recovery and supports easy audits to help you comply with Sarbanes-Oxley, HIPAA, Basel 2 and other regulatory requirements, even during unexpected business disruptions. And SonicWALL Aventail SSL VPNs make an ideal replacement strategy for IPSec VPNs. From any business perspective, SonicWALL Aventail is the easy choice for secure access.

Specifications

SonicWALL Aventail E-Class SSL VPN Series



SonicWALL Aventail EX-750

- 10 Concurrent User License  
01-SSC-7720
- 25 Concurrent User License  
01-SSC-7732
- 50 Concurrent User License  
01-SSC-7740



SonicWALL Aventail EX-1600

- 5 Concurrent User License\*  
01-SSC-7877
- 25 Concurrent User License  
01-SSC-7884
- 50 Concurrent User License  
01-SSC-7912
- 100 Concurrent User License  
01-SSC-7933
- 250 Concurrent User License  
01-SSC-7947



SonicWALL Aventail EX-2500

- 5 Concurrent User License\*  
01-SSC-7954
- 50 Concurrent User License  
01-SSC-7961
- 100 Concurrent User License  
01-SSC-8017
- 250 Concurrent User License  
01-SSC-8066
- 500 Concurrent User License  
01-SSC-8108
- 1000 Concurrent User License  
01-SSC-8143
- 2000 Concurrent User License  
01-SSC-8164

\*Lab-box, Includes appliance add-ons

For license and support SKUs please visit [www.sonicwall.com](http://www.sonicwall.com)

For more information on SonicWALL's E-Class solutions, please visit [www.sonicwall.com](http://www.sonicwall.com) or [www.aventail.com](http://www.aventail.com).

	EX-750	EX-1600	EX-2500
<b>Performance</b>			
<b>Concurrent users</b>	An ideal solution for a user base of up to 50 concurrent users.	Support for up to 250 concurrent users per node or HA pair	Support for up to 2,000 concurrent users per load-balanced node or HA pair
<b>Hardware</b>			
<b>Form factor</b>		U rack-mount	
<b>Dimensions</b>	17" W x 1.71" H x 15" D (43.18cm W x 4.34cm H x 38.1cm D)	16.8" W x 1.7" H x 13.2" D (4.4cm H x 42.6cm W x 33.4cm D)	17" W x 1.7" H x 19.6" D (43cm W x 4.4cm H x 50 cm D)
<b>Processor</b>	Intel P4 2.4 GHz CPU, 533 MHz FSB, 512 MB DDR RAM	Intel Pentium, 2.4 GHz CPU, 533 MHz FSB, 1 GB DDR RAM	Intel Xeon 2.4 GHz CPU 533 MHz, FSB 2 GB DDR RAM
<b>Network</b>	Two 10/100Base-T Ethernet	Two 10/100 and one 1000Base-T Ethernet, 2 USB Ports, 1 serial bus connection (DB9)	Six 10/100/1000Base-T Ethernet
<b>Power</b>			
Input voltage	100 (5A)/240 (3A) VAC PFC auto-switching	120 (6A) / 240 (3A) VAC auto-switching	120 (6A) / 240 (3A) VAC auto-switching
Output power	200W	185W	300W
Power supply	MTBF 100,000 hours at 40° C (104° F)	MTBF 100,000 hours at 35° C (95° F)	MTBF 100,000 hours at 35° C (95° F)
<b>Environmental</b>			
Operating temperature:	0° - 50° C (32°F to 122° F)	0°C to 40°C (32°F to 104° F)	0°C to 40°C (32°F to 104° F)
Non-operating shock	50g, 11msec	50g, 11msec	50g, 11msec
<b>Regulatory Approvals</b>			
Emissions	FCC Class A, EN, VCCI	FCC Part 15 Class A, CE, C-Tick, VCCI, CCC, BSMI	FCC Part 15 Class A, CE, C-Tick, VCCI, CCC, BSMI
Safety	CAN/CSA, UL, CB Scheme	UL, cUL, CE, TUV, STQC, S, PSB, CCC, BSMI, CB Scheme	UL, cUL, CE, TUV, STQC, S, PSB, CCC, BSMI, CB Scheme
<b>Key Features</b>			
<b>Security</b>			
Encryption	Configurable session length, Ciphers: DES, 3DES, RC4, AES, Hashes: MD5, SHA		
Authentication methods	Server-side digital certificates, Username/password, Client-side digital certificates RSA SecurID and other one-time password tokens, Dual/stacked authentication		
Directories	Microsoft Active Directory, LDAP (Active Directory, Sun iPlanet, etc.), RADIUS; Dynamic groups based on LDAP/AD queries, Certificate revocation lists (CRL)		
Password management	Notification of password expiration and password change from the SonicWALL Aventail WorkPlace portal		
Access control options	User and group, Source IP and network, Destination network, Service/Port (OnDemand and Connect only) Define resources by destination URL, host name or IP address, IP range, subnet and domain, Day, date, time and range, Browser encryption key length, Policy Zones (allows, denies and quarantines access and provides data protection based on end point security profile), File system access controls		
SonicWALL Aventail End Point Control™ (EPC™)	Detection of files, registry keys, running processes and Device Watermarks; Advanced Interrogator: (simplified granular end point detection, including detailed configuration information on over 100 anti-virus, anti-spyware and personal firewall solutions, including McAfee, Symantec, Sophos and Trend) Data Protection: Cache Control (data protection), Secure Desktop (advanced data protection)		
<b>Access and Application Support</b>			
SonicWALL Aventail WorkPlace™ Access (browser-based access)	Clientless access to Web-based resources, Web file access: SMB/ CIFS, DFS, Personal Bookmarks, Multiple optimized WorkPlace portals for different user groups, Access to any TCP- or UDP-based application via the WorkPlace portal (leveraging OnDemand Tunnel agent)		
SonicWALL Aventail WorkPlace Mobile Access	Customized WorkPlace support for mobile phone, smartphone and PDA browsers		
SonicWALL Aventail Connect™ Access	Pre-installed agent provides access to any TCP- or UDP-based application (Windows, Macintosh and Linux support)		
SonicWALL Aventail Connect Mobile™	Lightweight agent provides access to both Web and client/server applications for Windows Mobile Devices		
<b>Management and Administration</b>			
Management	SonicWALL Aventail Management Console (AMC): centralized Web-based management for all access options, End Point Control configuration, access control policies and WorkPlace Portal configuration, easy policy replication across multiple appliances and locations, role-based administration		
Auditing	SonicWALL Aventail Advanced Reporting™, RADIUS auditing and accounting integration		
Monitoring and Logging	User connection monitoring, event alarms, View logs and performance information via the SonicWALL Aventail Management Console, SNMP integration including SonicWALL Aventail-specific SNMP MIB, Support for central SYSLOG server		
<b>High Availability</b>			
High Availability	-	Support for high-availability 2-node clusters with built-in load-balancing and stateful authentication failover	Support for high-availability 2-node clusters with built-in load-balancing and stateful, authentication failover
Clustering	-	-	Support for load-balanced arrays using standard external load balancers

SonicWALL, Inc.

1143 Borregas Avenue  
Sunnyvale CA 94089-1306

T +1 408.745.9600  
F +1 408.745.9300

[www.sonicwall.com](http://www.sonicwall.com)



PROTECTION AT THE SPEED OF BUSINESS™