SECURE REMOTE ACCESS | **SonicWALL E-Class Secure Remote Access for the Enterprise**

- **Increases productivity and return on investment**
- **Lowers IT overhead and total cost of ownership**
- **Easy-to-use from any endpoint**
- **Robust mobile solution**
- **Access to all application platforms**
- **Remote support**
- **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 to use and cost-effective to implement. Client-based VPNs can be cumbersome to use and manage. SonicWALL® Aventail® E-Class Secure Remote Access (SRA) solutions deliver a complete remote access control solution, flexibly deployable as a hardware or as a virtual appliance, without escalating infrastructure costs or complexity. SonicWALL Aventail E-Class SRA provides complete application access with full security, endpoint control 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 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, email security and secure remote access solutions.

Features and Benefits

Increases productivity. SonicWALL Aventail E-Class SRA works in more places, including home PCs, kiosks, PDAs and unmanaged devices over wired and wireless networks. SonicWALL Aventail SRA makes your users more productive by providing easy access to more applications from more environments—including Windows®, Linux®, Mac OS and mobile devices—than any other secure access solution.

Lowers IT overhead and total cost of ownership. SonicWALL Aventail E-Class SRA 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, host-based and back-connect applications like VoIP. SonicWALL Aventail SRAs are either clientless or use lightweight Web-delivered clients, reducing management overhead and support calls.

Easy-to-use from any endpoint. SonicWALL Aventail E-Class SRA 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, Apple® Mac OS, iPhone®, iPad™, Google Android™ and Linux—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 SRA 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.

Remote support. SonicWALL Virtual Assist enables technicians to provide secure on-demand assistance to customers while leveraging the existing infrastructure.

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 SRA gives network managers a single secure access gateway for all users, internal and external, to all resources with complete control. Administrators have even greater control over portal access, content and design with the newly-enhanced SonicWALL WorkPlace Portal.

Rapid set-up and deployment. All SonicWALL Aventail E-Class SRAs are easily setup and deployed in just minutes. The redesigned SonicWALL Aventail's Set-up Wizard provides an easy, intuitive "out-of-the-box" experience with rapid set-up and deployment. Improved management workflow makes it much easier to understand and manage policy objects.

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 quarantine for remediation.

SONICWALL®

Detect the security of any endpoint

Robust interrogation for secure control of the endpoint

Only SonicWALL Aventail End Point Control™ (EPC™) lets you enforce granular access control rules for Windows®, Windows Vista, Windows 7, Windows Mobile, Apple Macintosh iPhone, iPad and Linux endpoints. EPC combines pre-authentication interrogation to confirm endpoint criteria like anti-virus updates. SonicWALL Aventail Policy Zones™ apply detected endpoint 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. Device Identification enables administrators to tie the serial or equipment ID number for a Windows or Apple iPhone device to a specific user or group. SonicWALL Aventail's Virtual Keyboard stops keystroke sniffers on untrusted endpoints. SonicWALL Recurring EPC performs endpoint scans at user login and at administrator-defined intervals to ensure the ongoing integrity of any endpoint.

Advanced EPC for ultimate protection

Optional SonicWALL Aventail Advanced EPC™ combines granular endpoint 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, Macintosh and Linux platforms, including version and currency of signature file update. Cache Control purges browser cache, session history, cookies and pass-words. Secure Desktop creates a virtual encrypted environment that prevents sensitive information from being left behind. SonicWALL E-Class Aventail SRAs also block suspect email 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.

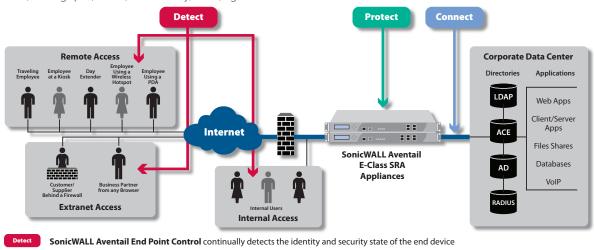## Protect your enterprise resources with ease

Streamlined policy management

With its context-sensitive help and Setup Wizard, a SonicWALL Aventail E-Class Secure Remote Access appliance 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, ACE, LDAP or Active Directory authentication repositories, including nested groups. SonicWALL Aventail SRAs 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. One-Time Password (OTP) support provides a built-in method to generate and distribute secondary factors, for easy and cost-effective two-factor authentication. Administrators can associate OTPs by Realm for greater flexibility in authentication control.

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. Enhanced user monitoring features streamline auditing and troubleshooting of current and historical user activity. Administrators can easily view or filter activity by user, time, throughput, realm, community, zone, agents or IP address.

Detect **SonicWALL Aventail End Point Control** continually 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 Secure Remote Access solutions provide secure access for all users, devices and applications.

Connect users to resources—simply and seamlessly

Broadest application access from the most endpoints

SonicWALL Aventail E-Class Secure Remote Access appliances deliver intelligent access to Web-based, client/server, server-based, host-based and back-connect applications such as VoIP. SonicWALL Aventail SRAs work seamlessly across Windows, Windows Vista, Windows 7, Windows Mobile, Apple Macintosh iPhone and iPad or Linux 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. Zone-based provisioning enables administrators to extend control over what access agents are deployed based upon the remote user's End Point Control classification. 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 Secure Remote Access appliances offer both clientless browser-based access and full access to client/server and legacy applications from Windows, Windows Vista, Windows 7, 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 hotspots 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 7, Windows Mobile, Apple Macintosh, or 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. Virtual Hosts provide clientless access to a wide range of complex Web applications, including those using Flash and JavaScript.

Most complete access solution for mobile devices

SonicWALL Aventail Secure Remote Access appliances 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 SRA 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 Secure Remote Access appliances offer active/active high availability (HA) with integrated load balancing and active/active stateful failover on the SRA EX7000 and EX6000, 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 Secure Remote Access appliances include the award-winning EX Series of SSL VPN appliances, offering your business the best solution for secure remote access control. With SonicWALL, 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's best-of-breed technology gives you flexible access options for disaster recovery and supports easy audits to help you comply with FIPS, Sarbanes-Oxley, HIPAA, Basel 2 and other regulatory requirements, even during unexpected business disruptions. And SonicWALL Aventail E-Class SRA appliances make an ideal replacement strategy for IPSec VPNs. From any business perspective, SonicWALL is the easy choice for secure access.

Specifications

SonicWALL Aventail E-Class SRA Series

E-Class SRA EX6000

SRA EX6000 Appliance
01-SSC-9601

Lab Box User License*
01-SSC-9610

25 Concurrent User License
01-SSC-9612

50 Concurrent User License
01-SSC-9614

100 Concurrent User License
01-SSC-9616

250 Concurrent User License
01-SSC-9618

E-Class SRA EX7000

SRA EX7000 Appliance
01-SSC-9602

Lab Box User License*
01-SSC-9610

50 Concurrent User License
01-SSC-9614

100 Concurrent User License
01-SSC-9616

250 Concurrent User License
01-SSC-9618

500 Concurrent User License
01-SSC-9647

1,000 Concurrent User License
01-SSC-9649

2,000 Concurrent User License
01-SSC-9651

5,000 Concurrent User License
01-SSC-8470

*Includes appliance add-ons

E-Class SRA Virtual Appliance

E-Class SRA Virtual Appliance
01-SSC-8468

10 Concurrent User License
01-SSC-9611

25 Concurrent User License
01-SSC-9612

50 Concurrent User License
01-SSC-9614

For license and support SKUs please visit www.sonicwall.com

	EX6000	EX7000
Performance		
Concurrent users	Support for up to 250 concurrent users per node or HA pair	Support for up to 5,000 concurrent users per load-balanced node or HA pair
Hardware		
Form factor	U rack-mount	U rack-mount
Dimensions	17.0 x 16.75 x 1.75 in (43.18 x 42.54 x 4.44 cm)	17.0 x 16.75 x 1.75 in (43.18 x 42.54 x 4.44 cm)
Processor	Intel Celeron 2.0 GHz 1 GB DDR533	Intel Core2 Duo 2.1 GHz 2 GB DDR533
Network	4 Stacked PCIe GB	6 Stacked PCIe GB
Power	Fixed Power Supply	Dual Power Supply, Hot Swappable
Input voltage	120 (6A) / 240 (3A) VAC auto-switching	120 (6A) / 240 (3A) VAC auto-switching
Input rating	100-240 VAC, 1.2 A	100-240 VAC, 1.5 A, 50-60 Hz; or -36 - -72 VDC, 3.2 A*
Output power	185W	300W
Rated power	100W	130W
Power supply	MTBF 100,000 hours at 35° C (95° F)	MTBF 100,000 hours at 35° C (95° F)
Environmental	WEEE, EU RoHS, China RoHS	WEEE, EU RoHS, China RoHS
Operating temperature:	0°C to 40°C (32°F to 104° F)	0°C to 40°C (32°F to 104° F)
Non-operating shock	110g, 2msec	110g, 2msec
Regulatory Approvals		
Emissions	FCC, ICES, CE, C-Tick, VCCI; MIC	FCC, ICES, CE, C-Tick, VCCI; MIC
Safety	TUV/GS, UL, CE PSB, CCC, BSMI, CB Scheme	TUV/GS, UL, CE PSB, CCC, BSMI, CB Scheme

Key Features

Security	
FIPS certification	Yes
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)

Access and Application Support	
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

Management and Administration	
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

High Availability			
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

E-Class SRA Virtual Appliance	
Hypervisor	ESG™ and ESX™ (version 4.0 and newer)
Operating System Installed	Hardened SonicLinux
Allocated Memory	2 GB
Applied Disk Size	80 GB
VMware Hardware Compatibility Guide	http://www.vmware.com/resources/compatibility/search.php

*Based on installing DC conversion kit in the field

For more information on SonicWALL's E-Class solutions, please visit **www.sonicwall.com**.

SonicWALL's line-up of dynamic security solutions

NETWORK SECURITY

SECURE REMOTE ACCESS

WEB AND E-MAIL SECURITY

BACKUP AND RECOVERY

POLICY AND MANAGEMENT

SonicWALL, Inc.
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600   F +1 408.745.9300
www.sonicwall.com

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™