



- **Erhöhung von Produktivität und ROI**
- **Entlastung der IT-Abteilung und Reduzierung der TCO**
- **Einfaches Handling von allen Endpunkten aus**
- **Robuste Lösung für mobile Anwender**
- **Zugriff auf sämtliche Anwendungsplattformen**
- **Remote Support**
- **Vermeidung von Routingkonflikten**
- **Einheitliches Access Gateway**
- **Schnelle Installation und Bereitstellung**
- **Einfache Kontrolle dank Unified Policy Management**

**Unkomplizierter, sicherer und clientloser Remote-Zugriff für Unternehmen**

Mit der zunehmenden Verbreitung von Mobiltechnologien, der fortschreitenden Globalisierung der Märkte und dem wachsenden Interesse an wirksamen Disaster Recovery-Maßnahmen gewinnt auch der sichere Remote-Zugriff für Unternehmen an Bedeutung. IT-Abteilungen müssen heute zuverlässige Remote Access-Lösungen bereitstellen, die anwenderfreundlich sind und sich kostengünstig implementieren lassen. Client-basierte VPNs sind mitunter in der Handhabung und Verwaltung sehr aufwändig. Die SonicWALL® Aventail® E-Class Secure Remote Access (SRA)-Produkte bieten hier eine Komplettlösung, bei der sich weder die Infrastrukturkosten noch die Komplexität nennenswert erhöhen. Die benutzerfreundlichen und leistungsstarken Appliances lassen sich wahlweise als Hardware- oder Virtual Appliance implementieren und ermöglichen einen uneingeschränkten Anwendungszugriff mit umfassender Sicherheit, effizienter Endpunktkontrolle und einheitlichem Policy Management. Mitarbeiter und Geschäftspartner mit Extranet-Zugang können an jedem Ort und von jedem Gerät aus einen clientlosen und sicheren Zugriff auf die benötigten Ressourcen erhalten und so ihre Produktivität steigern.

Mit der E-Class bietet SonicWALL ein attraktives Paket an Premium-Enterprise-Class-Lösungen, die ein außergewöhnlich hohes Maß an Sicherheit und Performance gewährleisten und dabei äußerst anwenderfreundlich und kosteneffizient sind. SonicWALLs Portfolio an E-Class-Produkten und -Services umfasst eine komplette Auswahl an Network Security-, E-Mail Protection- und Secure Remote Access-Lösungen.

**Funktionen und Vorteile**

**Erhöhte Produktivität.** SonicWALL Aventail E-Class SRA ermöglicht einen flexibleren Remote-Zugriff über kabelgebundene und drahtlose Netzwerke vom Home Office sowie von öffentlichen Terminals, PDAs und nicht verwalteten Geräten. Benutzer können von zahlreichen Umgebungen wie Windows®, Linux®, MacOS oder von mobilen Geräten aus auf eine Vielzahl von Anwendungen zugreifen und so noch produktiver arbeiten.

**Entlastung der IT-Abteilung und Reduzierung der TCO.** Die E-Class SRA Appliances von SonicWALL Aventail helfen IT-Kosten zu senken. Über ein sicheres, einfach zu implementierendes und zu verwaltendes Access Gateway können interne wie externe Benutzer per SSL VPN auf sämtliche Netzwerkressourcen zugreifen – darunter web- und hostbasierte Anwendungen sowie Client-Server- und Back-Connect-Anwendungen wie VoIP. Da die SonicWALL Aventail SRAs keinen Client benötigen bzw. mit einem webbasierten Lightweight-Client auskommen, reduzieren sich auch der Verwaltungsaufwand und Support-Anfragen.

**Einfaches Handling von allen Endpunkten aus.** Die E-Class SRA-Technologie von SonicWALL Aventail sorgt für einen transparenten Zugriff auf Netzwerkressourcen von beliebigen Netzwerkumgebungen und Geräten. Die Appliance dient als Gateway für sämtliche Zugriffe und bietet Benutzern von verwalteten und unverwalteten Geräten unter Windows, Windows Vista®, Windows Mobile, Apple® MacOS, iPhone®, iPad™, Google Android™, Linux und anderen Plattformen eine einheitliche Benutzererfahrung. Eine ausgezeichnete Anti-Spam-Engine und die durchgängige Überwachung von Angriffen garantieren einen effizienten und aktuellen Schutz vor Spam-Angriffen.

**Robuste Lösung für mobile Anwender.** SonicWALL Aventail E-Class SRA bietet einen besonders robusten Remote-Zugriff für PDAs und Smartphones. Dank Session Persistence ist beim Wechsel der IP-Adresse während einer Verbindung keine Neuauthentifizierung erforderlich.

**Zugriff auf sämtliche Anwendungsplattformen.** SonicWALL Aventail Smart Tunneling™ kombiniert die Sicherheit von SSL mit den umfassenden Zugriffsmöglichkeiten eines Layer-3-Tunnels. Die einzigartige Architektur sorgt für einen schnellen und unkomplizierten Zugriff auf

beliebige web-, server- und hostbasierte Anwendungen sowie Client-Server-Applikationen.

**Remote Support.** SonicWALL Virtual Assist ermöglicht es Technikern, den Kunden im Bedarfsfall über die bestehende Infrastruktur sicheren Support zu bieten.

**Vermeidung von Routingkonflikten.** Adressierung und Routing werden dynamisch an das jeweilige Netzwerk angepasst. Die bei anderen Lösungen häufig auftretenden Adress- und Routingkonflikte gehören damit der Vergangenheit an.

**Einheitliches Access Gateway.** Mit den SonicWALL Aventail E-Class SRA-Lösungen können Netzwerkadministratoren den Zugang für interne und externe Benutzer über ein einheitliches sicheres Access Gateway auf sämtliche Ressourcen flexibel steuern. Dank des weiter verbesserten SonicWALL WorkPlace-Portals haben Administratoren jetzt noch mehr Kontrolle über Zugriff, Inhalt und Gestaltung des Portals.

**Schnelle Installation und Bereitstellung.** Die SonicWALL Aventail E-Class SRA Appliances lassen sich in Minutenschnelle installieren und bereitstellen. Der neue intuitive Setupassistent von SonicWALL Aventail bietet maximale Benutzerfreundlichkeit und sorgt für eine schnelle und unkomplizierte Installation und Bereitstellung. Dank der verbesserten Verwaltungsprozesse lassen sich Regelobjekte viel einfacher verstehen und verwalten.

**Einfache Kontrolle dank Unified Policy Management.** SonicWALL Aventail Unified Policy™ bietet ein einfaches objektbasiertes Policy Management für sämtliche Benutzer, Gruppen, Ressourcen und Geräte und ermöglicht eine granulare Kontrolle mittels Benutzerauthentifizierung und Abfrage von Endpunkten. Mithilfe von Policy Zones können Zugriffsversuche komplett oder bis zur Behebung einer möglichen Sicherheitslücke vorübergehend abgewiesen werden.

## Zuverlässige Ermittlung der Sicherheitssituation an Endpunkten

### Effiziente Abfragen für eine sichere Kontrolle von Endpunkten

SonicWALL Aventail End Point Control™ (EPC™) ist die einzige Funktion, mit der sich Zugriffsregeln für Endpunkte unter Windows®, Windows Vista, Windows 7, Windows Mobile, Apple Macintosh iPhone, iPad und Linux gezielt steuern und durchsetzen lassen. Durch eine Abfrage vor der Authentifizierung werden Endpunkte auf Kriterien wie vorhandene Virenschutz-Updates überprüft. SonicWALL Aventail Policy Zones™ nutzt die am Endpunkt ermittelten Kriterien zur Erstellung automatisierter Zugriffsregeln. Wird einem Benutzer der Zugriff verwehrt, erhält er gleichzeitig Hinweise zur Behebung des Problems, beispielsweise durch Installation eines Sicherheitspatches. Dank Device Watermarking kann bei verlorenen oder gestohlenen Geräten der Zugriff einfach auf Grundlage der Client-Zertifikate verweigert werden. Mit der Funktion Device Identification können Administratoren die Serien- oder Geräte-ID-Nummer für ein Windows-Gerät oder Apple iPhone an einen bestimmten Benutzer oder an eine bestimmte Gruppe binden. Die Funktion Virtual Keyboard schließlich bietet wirksamen Schutz vor Keyloggern auf nicht vertrauenswürdigen Endpunkten. SonicWALL Recurring EPC scannt die Endpunktgeräte bei der Anmeldung und in bestimmten Abständen, die vom Administrator festgelegt werden können, um die fortlaufende Integrität sämtlicher Endpunktgeräte zu gewährleisten.

### Größtmöglicher Schutz dank Advanced EPC

Die optionale Komponente Aventail® Advanced EPC™ vereint eine gezielte Endpunkt-Erkennung mit ausgereiften Datenschutzfunktionen. Der Advanced Interrogator erleichtert die Erstellung von Geräteprofilen anhand einer vordefinierten Liste von Anti-Virus-, Anti-Spyware- und Personal Firewall-Lösungen für Windows-, Macintosh- und Linux-Plattformen, wobei auch die Version und Aktualität der Signaturen berücksichtigt werden. Cache Control entfernt Elemente aus dem Cache-Speicher und Sitzungsverlauf des Browsers und löscht Cookies sowie Kennworteingaben. Die Funktion Secure Desktop schafft eine virtuelle verschlüsselte Umgebung und verhindert, dass vertrauliche Informationen auf dem Gerät zurückbleiben. Verdächtige E-Mail-Anhänge in Outlook Web Access oder Lotus iNotes werden von den E-Class SRAs ebenso blockiert wie der Zugriff auf Finanzdaten oder Patientenakten. Für einen umfassenden Firewall-Schutz sind bei den SonicWALL Aventail SSL VPNs standardmäßig alle Ports geschlossen.

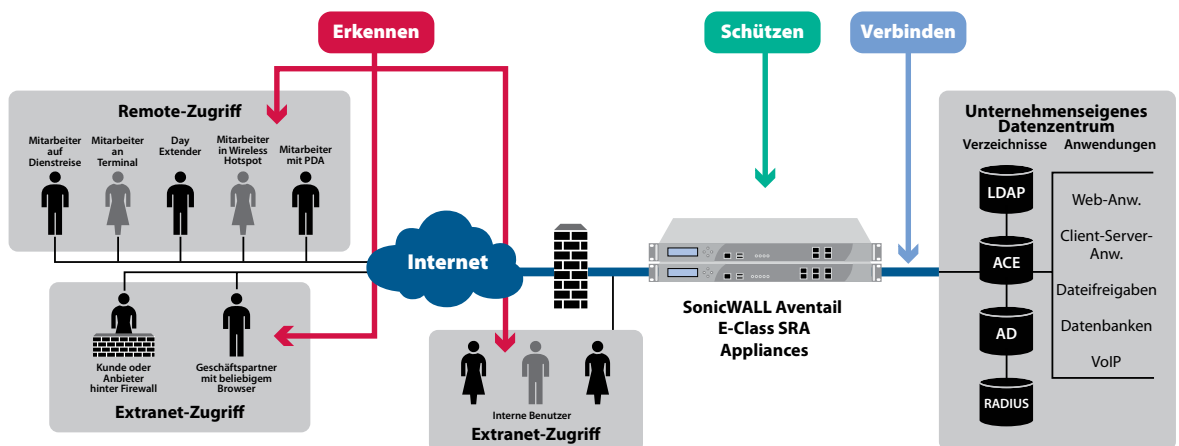
## Einfacher Schutz von Unternehmensressourcen

### Optimiertes Policy Management

Mit ihren kontextspezifischen Hilfsfunktionen und einem Setupassistenten lassen sich die SonicWALL Aventail E-Class Secure Remote Access Appliances denkbar einfach installieren und einsetzen. Über das erweiterbare, objektbasierte SonicWALL Aventail Unified Policy™-Modell werden sämtliche URL- und Client-Server-Ressourcen sowie Dateifreigaben von einem gemeinsamen Punkt aus kontrolliert. Damit beansprucht das Policy Management nur noch wenige Minuten. Auf der Grundlage von Authentifizierungsmethoden wie RADIUS, ACE, LDAP und Active Directory können Benutzer Gruppen dynamisch zugeordnet werden – auch in verschachtelten Gruppen. Die SonicWALL Aventail SRAs unterstützen Single Sign-On (SSO) und Webanwendungen auf Formularbasis. Benutzer können Kennwörter problemlos ohne den IT-Administrator aktualisieren. Mit der Funktion SonicWALL Aventail Policy Replication lassen sich Richtlinien einfach über mehrere Appliance Nodes replizieren – unabhängig davon, ob sich diese im selben Cluster befinden oder geografisch verteilt sind. Die Appliances unterstützen Einmalpasswörter und bieten damit eine integrierte Methode, um Zweifaktoren zu generieren und zu verteilen. Auf diese Weise lässt sich eine unkomplizierte und kosteneffektive Zweifaktor-Authentifizierung durchführen. Administratoren können Einmalpasswörter nach Bereichen zuordnen, um mehr Flexibilität bei der Authentifizierungskontrolle zu gewährleisten.

### Intuitives Management und Reporting

Die SonicWALL Aventail Management Console™ stellt zahlreiche zentralisierte Berichts- und Überwachungsmöglichkeiten für Audits, Compliance, Verwaltung sowie Ressourcenplanung zur Verfügung. Das optionale Aventail Advanced Reporting™ mit seinen Standard- und benutzerdefinierten Reports erfasst sämtliche Zugriffe auf Unternehmensressourcen im Detail. Das Abfragen der Reports ist dabei über jeden beliebigen Webbrowser möglich. Visuelle Tools liefern Echtzeitinformationen zum Systemstatus sowie intuitive Optionen zum Verwalten von Systemobjekten. Erweiterte Funktionen zur Benutzerüberwachung erlauben eine effizientere Überwachung aktueller und historischer Benutzeraktivitäten und erleichtern die Fehlerbehebung. Administratoren können ganz unkompliziert Aktivitäten einsehen oder nach Benutzer, Zeit, Durchsatz, Bereich, Community, Zone, Agents oder IP-Adresse filtern.



- Erkennen** SonicWALL Aventail End Point Control ermittelt kontinuierlich die Identität und Sicherheitssituation des Endgeräts.
- Schützen** SonicWALL Aventail Unified Policy setzt die Zugriffskontrolle für Geräte um und stellt sicher, dass Benutzer nur auf freigegebene Anwendungen zugreifen können.
- Verbinden** SonicWALL Aventail Smart Access und Smart Tunneling sorgen für einen einfachen und sicheren Nutzerzugriff auf sämtliche Netzwerkressourcen.

Die SonicWALL Aventail E-Class Remote Access-Lösungen bieten einen schnellen und sicheren Zugriff für alle Benutzer, Geräte und Anwendungen.

## Einfacher und lückenloser Benutzerzugriff auf Ressourcen

### Umfassender Zugriff auf Anwendungen von den meisten Endpunkten aus

Die SonicWALL Aventail E-Class Secure Remote Access Appliances ermöglichen einen transparenten Zugriff auf web-, server-, hostbasierte und Client-Server-Anwendungen sowie auf Back-Connect-Applikationen wie VoIP. Die SRA Appliances sind plattformübergreifend für Windows, Windows Vista, Windows 7, Windows Mobile, Apple Macintosh iPhone und iPad oder Linux-Plattformen anwendbar und regeln den Zugriff von Desktops, Laptops, öffentlichen Terminals, PDAs und Smartphones sowie zwischen Anwendungen. Auf diese Weise lassen sich gleichzeitig die Mitarbeiterproduktivität steigern und die Supportkosten senken. SonicWALL Aventail Smart Access™ führt eine dynamische Auswahl und Anwendung des geeigneten Zugriffsverfahrens sowie des Sicherheitsniveaus je nach Gerätetyp/-status, Benutzeridentität und benötigten Ressourcen aus. Dank der zonenbasierten Bereitstellung können Administratoren auf der Grundlage der EPC-Klassifizierung des Remote-Benutzers die Kontrolle über die Zugriffs-Agents erweitern. Die Adressierungs- und Routingfunktionen passen sich dynamisch an Netzwerke an, wodurch etwaige Konflikte vermieden werden. Smart Access erleichtert außerdem die Installation und Aktivierung von Agents auf Windows-Geräten gemäß Microsoft-Standards.

### Clientloser, webbasierter Zugriff oder umfassendes „In-Office“-Erlebnis

Die SonicWALL Aventail E-Class Secure Remote Access Appliances bieten einen clientlosen Zugriff via Browser sowie einen vollständigen Zugriff von Windows-, Windows Vista-, Windows 7-, Windows Mobile-, Macintosh- und Linux-Umgebungen auf Client-Server-Anwendungen und Legacy-Applikationen. Mit seinem richtlinienbasierten geräte-optimierten Webportal erlaubt SonicWALL Aventail WorkPlace™ einen einfachen Zugriff auf webbasierte Anwendungen und Client-Server-Applikationen von Desktops, Laptops, PDAs, Smartphones und selbst von Wireless Hotspots und öffentlichen Terminals aus. Über persönliche Shortcuts können Benutzer auf häufig benötigte Ressourcen zugreifen. Daneben lässt sich WorkPlace mit entsprechenden Logos und Farbschemas für Partner und Mitarbeiter personalisieren. SonicWALL Aventail WorkPlace bietet sich insbesondere als Zugriffsoption für Geräte an, die nicht vom Unternehmen verwaltet werden. Der Zugriff über SonicWALL Aventail Connect™ vermittelt Benutzern von Windows, Windows Vista, Windows 7, Windows Mobile, Apple Macintosh sowie Linux den Eindruck, im Büro zu arbeiten und erlaubt uneingeschränktes Arbeiten mit Client-Server- und Web-Anwendungen sowie allen anderen Netzwerkressourcen. SonicWALL Aventail Connect wird über einen webseitig bereitgestellten Lightweight-Agent oder eine Standard-MSI-Installation aktiviert und eignet sich ideal als Zugriffsoption für Geräte, die von der IT-Abteilung verwaltet werden und umfassende Desktop-Sicherheit, Split-Tunnel-Steuerung sowie Personal Firewall-Erkennung benötigen. Die in SonicWALL Aventail Smart Tunneling™ enthaltene Layer 3-Technologie unterstützt die Protokolle UDP, TCP und IP sowie Back-Connect-Anwendungen wie VoIP. Im NAT-Modus müssen dabei keine IP-Adresspools eingerichtet werden.

### Maßgeschneiderte Lösung für die Bedürfnisse der Benutzer

Die optionalen SonicWALL Aventail Native Access Modules™ bieten einen systemeigenen Zugriff auf Windows Terminal Services sowie einen systemeigenen Support über das WorkPlace-Portal für Citrix-Farmen mit Lastverteilung als Alternative zu einer kostenintensiven Citrix nFuse-Implementation. Virtual Hosts bietet einen clientlosen Zugriff auf eine Vielzahl komplexer Webanwendungen wie Applikationen mit Flash und JavaScript.

### Umfassendste Access-Lösung für mobile Endgeräte

Die SonicWALL Aventail Secure Remote Access Appliances bieten umfassende Sicherheits- und Kontrollfunktionen für den web- und clientbasierten Zugriff auf kritische Netzwerkressourcen von beliebigen Wireless-Umgebungen aus (z. B. Windows Mobile-Geräte, Symbian-Smartphones, DoCoMo iMode- und WAP-fähige Geräte). Alle Geräte können zentral mittels granularer Zugriffskontrolle verwaltet werden. Geht ein Gerät verloren oder wurde es gestohlen, kann der Zugriff für dieses Gerät verweigert werden. Dank Session Persistence können mobile Benutzer beim Wechsel zwischen verschiedenen Netzwerken die aktuelle Sitzung ganz normal ohne Neuauthentifizierung fortführen.

### Hochverfügbar, flexibel und zuverlässig

Für ein erhöhtes Maß an Zuverlässigkeit bieten die Aventail E-Class Secure Remote Access Appliances SRA EX7000 und EX6000 Active/Active Hochverfügbarkeitsfunktionen. Das integrierte Load Balancing und Active/Active Stateful Failover machen die Anschaffung eines externen Load Balancers überflüssig. Zudem lässt sich mit einem optionalen Aventail Spike License Pack die Anzahl der Remote-Nutzer vorübergehend auf das vorgegebene Maximum der SonicWALL Aventail-Appliances erhöhen, um den Betriebsablauf auch während eines Katastrophenfalls zu gewährleisten oder um geplante Arbeitsspitzen abzufangen – unabhängig davon, ob es sich nur um ein paar oder um tausende zusätzliche Benutzer handelt.

### Eine klare Entscheidung

Die SonicWALL Aventail E-Class Secure Remote Access Appliances beinhalten die führenden Appliances der EX-Serie und bieten Ihrem Unternehmen die ideale Lösung für einen sicheren Remote-Zugriff. Mit SonicWALL verbessern Sie die Sicherheit Ihres Unternehmensnetzwerks, steigern die Produktivität Ihrer mobilen Mitarbeiter, optimieren den ROI (Return on Investment) und reduzieren gleichzeitig den Aufwand Ihrer IT-Abteilung und damit die TCO (Total Cost of Ownership). Die herausragenden Technologien von SonicWALL bieten flexible Zugriffsoptionen, mit denen Sie auch im Katastrophenfall einen normalen Betriebsablauf gewährleisten können. Darüber hinaus können Sie Ihre Organisation auf die Einhaltung von FIPS, Sarbanes-Oxley, HIPAA, Basel 2 und weiteren behördlichen Vorgaben prüfen – selbst bei unerwarteten Unterbrechungen des Betriebs. Außerdem eignen sich die SonicWALL Aventail E-Class SRA Appliances ideal als Ersatz für IPSec VPNs. Wenn es um einen sicheren Zugriff geht, ist SonicWALL Aventail für jedes Unternehmen die Lösung der Wahl.

Technische Daten

SonicWALL Aventail E-Class SRA-Serie



E-Class SRA EX6000

- SRA EX6000 Appliance  
01-SSC-9601
- Lab Box-Benutzerlizenz\*  
01-SSC-9610
- Lizenz für 25 gleichzeitige Benutzer  
01-SSC-9612
- Lizenz für 50 gleichzeitige Benutzer  
01-SSC-9614
- Lizenz für 100 gleichzeitige Benutzer  
01-SSC-9616
- Lizenz für 250 gleichzeitige Benutzer  
01-SSC-9618



E-Class SRA EX7000

- SRA EX7000 Appliance  
01-SSC-9602
- Lab Box-Benutzerlizenz\*  
01-SSC-9610
- Lizenz für 50 gleichzeitige Benutzer  
01-SSC-9614
- Lizenz für 100 gleichzeitige Benutzer  
01-SSC-9616
- Lizenz für 250 gleichzeitige Benutzer  
01-SSC-9618
- Lizenz für 500 gleichzeitige Benutzer  
01-SSC-9647
- Lizenz für 1.000 gleichzeitige Benutzer  
01-SSC-9649
- Lizenz für 2.000 gleichzeitige Benutzer  
01-SSC-9651
- Lizenz für 5.000 gleichzeitige Benutzer  
01-SSC-8470

\*Inklusive Appliance-Add-Ons



E-Class SRA Virtual Appliance

- E-Class SRA Virtual Appliance  
01-SSC-8468
- Lizenz für 10 gleichzeitige Benutzer  
01-SSC-9611
- Lizenz für 25 gleichzeitige Benutzer  
01-SSC-9612
- Lizenz für 50 gleichzeitige Benutzer  
01-SSC-9614

Weitere Informationen zu Lizenz- und Support-Artikelnummern erhalten Sie unter [www.sonicwall.com/de](http://www.sonicwall.com/de).

|  | EX6000  | EX7000   |
|--|---|--|
| <b>Leistung</b>                          |   |  |
| <b>Gleichzeitige Benutzer</b>            | Unterstützt bis zu 250 gleichzeitige Benutzer pro Node bzw. HA-Paar | Unterstützt bis zu 5.000 gleichzeitige Benutzer pro Node mit Lastverteilung bzw. HA-Paar |
| <b>Hardware</b>                          |   |  |
| <b>Gehäuse</b>                           | 1 HE-Einschub   | 1 HE-Einschub  |
| <b>Abmessungen</b>                       | 43,2 x 42,5 x 4,4 cm  | 43,2 x 42,5 x 4,4 cm   |
| <b>Prozessor</b>                         | Intel Celeron 2,0 GHz<br>1 GB DDR533                                | Intel Core2 Duo 2,1 GHz<br>2 GB DDR533   |
| <b>Netzwerk</b>                          | 4 PCIe GB (gestackt)  | 6 PCIe GB (gestackt)   |
| <b>Leistung</b>                          | Feste Stromversorgung   | Duale Stromversorgung, hot-swappable   |
| Eingangsspannung                         | 120 (6 A)/240 (3 A) VAC<br>Automatische Anpassung                   | 120 (6 A)/240 (3 A) VAC<br>Automatische Anpassung  |
| Eingangsnennspannung                     | 100-240 VAC, 1,2 A  | 100-240 VAC, 1,5 A, 50-60 Hz; oder<br>-36 - -72 VDC, 3,2 A*                              |
| Ausgangsleistung                         | 185 W   | 300 W  |
| Nennleistung                             | 100 W   | 130 W  |
| Stromversorgung                          | MTBF 100.000 Stunden bei 35° C                                      | MTBF 100.000 Stunden bei 35° C   |
| <b>Umgebungsbedingungen</b>              | WEEE, EU RoHS, China RoHS   | WEEE, EU RoHS, China RoHS  |
| Betriebstemperatur                       | 0 bis 40° C   | 0 bis 40° C  |
| Erschütterungsfestigkeit (ausgeschaltet) | 110 g, 2 ms   | 110 g, 2 ms  |
| <b>Erfüllte Normen/Standards</b>         |   |  |
| Emissionen                               | FCC, ICES, CE, C-Tick, VCCI; MIC                                    | FCC, ICES, CE, C-Tick, VCCI; MIC   |
| Sicherheit                               | TÜV/GS, UL, CE<br>PSB, CCC, BSMI, CB Scheme                         | TÜV/GS, UL, CE<br>PSB, CCC, BSMI, CB Scheme  |

Die wichtigsten Funktionen

| Sicherheit                                   |   |
|--|---|
| FIPS-Zertifizierung                          | Ja  |
| Verschlüsselung                              | Sitzungslänge konfigurierbar, Chiffrierverfahren: DES, 3DES, RC4, AES, Hashcodes: MD5, SHA  |
| Authentifizierungsmethoden                   | Digitale Zertifikate auf Serverseite, Benutzername/Kennwort, digitale Zertifikate auf Clientseite, RSA SecurID und andere Einmalpasswort-Tokens, Dual/Stacked Authentication  |
| Verzeichnisse                                | Microsoft Active Directory, LDAP (Active Directory, Sun iPlanet u. a.), RADIUS; dynamische Gruppen auf Basis von LDAP- bzw. AD-Abfragen, Certificate Revocation Lists (CRL)   |
| Passwortverwaltung                           | Benachrichtigung bei Ablauf des Passworts und Passwortänderungen über das SonicWALL Aventail Workplace-Portal   |
| Zugriffssteuerungsoptionen                   | Benutzer und Gruppe, Quell-IP und -Netzwerk, Zielnetzwerk, Dienst/Port (nur OnDemand und Connect), Definieren von Ressourcen nach Ziel-URL, Hostname oder IP-Adresse, IP-Bereich, Subnet und Domäne, Tag, Datum, Uhrzeit und Zeitspanne, Browser-Chiffrierschlüssellänge, Policy Zones (Freigabe/Sperrung/vorübergehende Verweigerung des Zugriffs, Datenschutz gemäß Sicherheitsprofil des Endpunkts), Zugriffskontrolle für das Dateisystem |
| SonicWALL Aventail End Point Control™ (EPC™) | Erkennung von Dateien, Registrierungsschlüsseln, laufenden Prozessen und Device Watermarks; Advanced Interrogator (vereinfachte gezielte Endpunkterkennung inkl. detaillierter Konfigurationsdaten zu mehr als 100 Anti-Virus-, Anti-Spyware- und Personal Firewall-Lösungen von McAfee, Symantec, Sophos, Trend u. a.), Datenschutzfunktionen: Cache Control (Datenschutz), Secure Desktop (erweiterter Datenschutz)                         |

Zugriffs- und Anwendungsunterstützung

|   |  |
|---|--|
| SonicWALL Aventail Workplace™ Access (browserbasierter Zugriff) | Clientloser Zugriff auf webbasierte Ressourcen, Webdateizugriff: SMB/ CIFS, DFS, personalisierte Lesezeichen, mehrere optimierte Workplace-Portale für verschiedene Benutzergruppen, Zugriff auf TCP- oder UDP-basierte Anwendungen über das Workplace-Portal (unter Nutzung des OnDemand Tunnel-Agents) |
| SonicWALL Aventail Workplace Mobile Access                      | Individuelle Workplace-Unterstützung für Mobiltelefon-, Smartphone- und PDA-Browser  |
| SonicWALL Aventail Connect™ Access                              | Zugriff auf beliebige TCP- oder UDP-basierte Anwendungen über vorinstallierten Agent (Unterstützung für Windows, Macintosh und Linux)  |
| SonicWALL Aventail Connect Mobile™                              | Zugriff auf Web- und Client-Server-Anwendungen für Windows Mobile-Geräte über einen Lightweight-Agent  |

Management und Verwaltung

|                                 |  |
|---------------------------------|--|
| Verwaltung                      | SonicWALL Aventail Management Console (AMC): zentralisierte webbasierte Verwaltung für sämtliche Zugriffsoptionen, End Point Control-Konfiguration, Richtlinien für die Zugriffssteuerung, Konfiguration des Workplace-Portals, einfache Replikation von Richtlinien über mehrere Appliances hinweg, rollenbasierte Administration |
| Auditing                        | SonicWALL Aventail Advanced Reporting™, RADIUS-Auditing und Accounting   |
| Überwachung und Protokollierung | Überwachung von Benutzerverbindungen, Ereignisalarme, Abfrage von Protokollen und Performance-Daten über die SonicWALL Aventail Management Console, SNMP-Integration inkl. SonicWALL Aventail-spezifischer SNMP MIB, Unterstützung für zentralen SYSLOG-Server   |

Hochverfügbarkeitsoptionen

|                   |   |  |  |
|-------------------|---|--|--|
| Hochverfügbarkeit | - | Support für hochverfügbare Cluster mit 2 Nodes, integriertem Load Balancing und Stateful Authentication Failover | Support für hochverfügbare Cluster mit 2 Nodes, integriertem Load Balancing und Stateful Authentication Failover |
| Clustering        | - | -  | Support für Arrays mit Load Balancing und externen Standard-Load Balancern                                       |

E-Class SRA Virtual Appliance

|   |   |
|---|---|
| <b>Hypervisor</b>                                     | ESG™ und ESX™ (ab Version 4.0)  |
| <b>Installiertes Betriebssystem</b>                   | Gehärtetes SonicLinux   |
| <b>Zugewiesener Speicher</b>                          | 2 GB  |
| <b>Benötigter Festplattenspeicher</b>                 | 80 GB   |
| <b>VMware-Kompatibilitätsrichtlinien für Hardware</b> | <a href="http://www.vmware.com/resources/compatibility/search.php">http://www.vmware.com/resources/compatibility/search.php</a> |

\*Bei Installation eines Gleichstrom-Conversion Kits vor Ort

Weitere Informationen zu den E-Class-Lösungen von SonicWALL erhalten Sie unter [www.sonicwall.com/de](http://www.sonicwall.com/de).

SonicWALL-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT

SonicWALL Deutschland

Tel: +49 89 4545 946 [www.sonicwall.de](http://www.sonicwall.de)

SonicWALL Schweiz

Tel: +41 44 810 31 35 [www.sonicwall.ch](http://www.sonicwall.ch)

SonicWALL Österreich

Tel: +41 44 810 31 35 [www.sonicwall.at](http://www.sonicwall.at)



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™