



- **Unkompliziertes „In-Office“-Erlebnis an jedem beliebigen Standort**
- **Leichte Installation, Verwaltung und Bedienung**
- **SonicWALL Aventail Unified Policy**
- **Sicherer Zugriff auf beliebige Anwendungen**
- **Split-Tunnel-Steuerung**

Unkompliziertes „In-Office“-Erlebnis

Immer mehr Mitarbeiter und Partner arbeiten heute außerhalb der Unternehmensgrenzen. Ob es sich um Führungskräfte mit verwalteten Laptops handelt, die häufig unterwegs sind, um Mitarbeiter im Home Office oder um Partner, die das Extranet nutzen: Sie alle tragen entscheidend zum Erfolg eines Unternehmens bei und benötigen den gleichen uneingeschränkten Zugriff auf wichtige Geschäftsanwendungen (z. B. Back-Connect-Anwendungen wie VoIP Soft Phones oder Remote Help Desk) wie ihre Kollegen vor Ort. Die Herausforderung für IT-Abteilungen besteht darin, diesen Benutzern vollen Zugriff auf wichtige Geschäftsressourcen bereitzustellen und gleichzeitig eine hohe Desktop-Sicherheit, Split-Tunnel-Steuerung und Personal Firewall-Erkennung zu gewährleisten.

SonicWALL® Aventail® Connect Tunnel™ bietet den Nutzern von SonicWALL Aventail E-Class SSL VPN eine unkomplizierte und sichere Alternative mit echtem „In-Office“-Erlebnis. Connect Tunnel ist ein webseitig bereitgestellter Client, der Benutzern von autorisierten Remote-Desktop-PCs und -Laptops einen sicheren und standortunabhängigen Zugriff auf das gesamte Unternehmensnetzwerk ermöglicht. Connect Tunnel ist die unkomplizierteste und umfassendste Secure Remote Access-Lösung auf dem Markt und bietet WLAN-Benutzern und Geschäftsreisenden, die auch außerhalb des Unternehmens vollen Netzwerkzugriff benötigen, ein hohes Maß an Sicherheit.

Funktionen und Vorteile

Unkompliziertes „In-Office“-Erlebnis an jedem beliebigen Standort. Bietet Remote-Benutzern von verwalteten Geräten (z. B. autorisierte Desktop-PCs und Laptops) den gleichen Zugriff auf Netzwerkressourcen, den sie im Unternehmensnetz haben und vermittelt so den Eindruck, im Büro zu arbeiten. Connect Tunnel sorgt für maximale Transparenz und unübertroffene Benutzerfreundlichkeit und bietet neben Single Sign-On eine automatische Netzwerksuche und die Integration von Dialern anderer Anbieter. Remote-Benutzer müssen sich keine Gedanken machen, wie sie vollen Zugriff auf ihre Ressourcen erhalten. Klickt der Benutzer ein Symbol auf dem verwalteten Remote-Gerät an, kann er sich automatisch über das Internet im Netzwerk authentifizieren. Auf der Grundlage von administrativen Regeln erkennt und verwendet die SonicWALL Aventail Smart Access™-Technologie automatisch das geeignete Remote-Zugriffsverfahren für die Unternehmensressourcen, die der Benutzer benötigt.

Leichte Installation, Verwaltung und Bedienung.

Connect Tunnel lässt sich leicht auf verwalteten Geräten installieren. Außerdem werden Updates mit neuen Versionen automatisch durchgeführt und Konfigurationsänderungen ohne weiteres Einschreiten des Administrators vorgenommen. Der Aventail Connect Tunnel-Lightweight-Client kann auf einem verwalteten Gerät vorinstalliert werden oder über einen einmaligen Download von einem Webportal installiert werden und bietet eine ideale Alternative zu „Fat Client“-IPSec VPNs.

SonicWALL Aventail Unified Policy™. Ermöglicht eine zentrale Kontrolle über alle Benutzer, Gruppen, Ressourcen und Geräte, damit einheitliche Regeln schnell und einfach auf alle Objekte angewendet werden können. Mit SonicWALL Aventail End Point Control™ lassen sich alle Windows®, Macintosh®- und Linux®-Geräte identifizieren und Sicherheitsregeln auf diese Geräte anwenden. Ermöglicht wird dies durch

die automatische Erkennung von Kriterien wie z. B. Virenschutz-Software, Personal Firewalls, Anwendungen, Verzeichnisse, Dateinamen und -größen, Zeitstempel oder Windows-Versionen, -Domänen und -Registrierungseinträge.

Sicherer Zugriff auf beliebige Anwendungen

(z. B. VoIP und Remote Help Desk). Die SonicWALL Aventail Smart Tunneling™-Technologie kombiniert die Sicherheit von SSL auf der Anwendungsebene mit den umfassenden Zugriffsmöglichkeiten eines Layer-3-Tunnels. Die einzigartige Architektur bietet Benutzern eine außergewöhnlich große Anwendungsbreite inklusive Unterstützung für UDP-, TCP- und IP-Protokolle sowie eine granulare und bidirektionale Zugriffskontrolle für beliebige Anwendungen (z. B. Back-Connect-Anwendungen wie VoIP und Remote Help Desk). Bevor die Verbindung zugelassen wird, können VoIP-Geräte abgefragt und Benutzer authentifiziert werden, um Malware-Angriffe zu verhindern.

Split-Tunnel-Steuerung.

Mit dieser Funktion kann die IT-Abteilung bestimmen, ob ein Benutzer die Möglichkeit haben soll, sich während der VPN-Sitzung bei mehreren Netzwerken anzumelden. NAT-Traversal, Proxy-Erkennung, Traversal und die adaptiv-dynamische Entschärfung von Adresskonflikten stellen einen umfassenden Anwendungszugriff sicher. Connect Tunnel lässt sich unkompliziert mit Internet-Dialern und anderen Desktop-Softwareprodukten integrieren. Da der Benutzer uneingeschränkter Zugriff auf die benötigten Anwendungen erhält und das System gleichzeitig eine umfassende Regelkontrolle und zuverlässige Sicherheit gewährleistet, bietet Connect Tunnel auch eine unkomplizierte und effektive Alternative zu umständlichen IPSec-Systemen.



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

E-Class EX-1600
Inklusive

E-Class EX-2500
Inklusive

Wie funktioniert SonicWALL Aventail Connect Tunnel?

Der SonicWALL Aventail Connect Tunnel Lightweight-Client kann auf einem verwalteten Gerät vorinstalliert werden oder von einem Webportal heruntergeladen werden. Sobald der Connect Tunnel-Client installiert ist, benötigt der Benutzer keine Website und kein Portal mehr, um auf die freigegebenen Netzwerkressourcen zuzugreifen. Auf diese Weise profitiert er von einem umfassenden „In-Office“-Erlebnis. Mit einem Klick auf das SonicWALL Aventail Connect-Symbol auf dem Desktop kann sich der Benutzer automatisch authentifizieren und von dem verwalteten Gerät über das Internet auf das Netzwerk zugreifen.

Technische Daten		
Betriebssystem	Browser	Hinweise
Windows Vista® Windows XP Pro, SP2 Windows 2000 Pro, SP4 Windows XP Home, SP2	Nicht zutreffend	Windows-Administratorenrechte für die Installation erforderlich
Windows Server-Plattform: Windows 2003 Server Windows 3000 Server, SP4	Nicht zutreffend	Windows-Administratorenrechte für die Installation erforderlich
Macintosh OS X v 10.5	Nicht zutreffend	Administratorenrechte für die Installation erforderlich Kein Support für End Point Control Macintosh OS X v 10.5 wurde nur auf Intel-PCs getestet
Linux-Kernel 2.4.20 oder höher	Mozilla Firefox 2.0 (Mozilla Firefox 1.5)	Administratorenrechte für die Installation erforderlich Browser nur zur Proxy-Erkennung erforderlich Kein Support für End Point Control

Weitere Informationen über die SonicWALL Aventail E-Class SSL VPN-Lösungen erhalten Sie unter www.sonicwall.com/de.

SonicWALL Deutschland

Tel.: +49 89 4545 946
www.sonicwall.de

SonicWALL Schweiz

Tel.: +41 44 810 31 35
www.sonicwall.ch

SonicWALL Österreich

Tel.: +41 44 810 31 35
www.sonicwall.at

SONICWALL®
PROTECTION AT THE SPEED OF BUSINESS™