

# SonicWALL VPN Clients

SECURE REMOTE ACCESS

Virtual Private Network (VPN) – Sicherer Remote-Zugriff

- **Erweiterte Sicherheit auf allen Netzwerkebenen**
- **Unkomplizierte VPN-Verwaltung**
- **Hilfreiche Assistenten**
- **Erweiterte Zugriffsmöglichkeiten für produktives Arbeiten**
- **Zuverlässige VPN-Sitzungen**
- **Konnektivität ohne Clients**
- **NetExtender-Technologie**
- **Unterstützung für mobile Geräte**

Um ihre Wettbewerbsfähigkeit in einem globalisierten Umfeld zu sichern, müssen kleine Firmen genauso wie große Unternehmen in der Lage sein, die steigenden Anforderungen von mobilen Arbeitskräften und Mitarbeitern an verteilten Standorten zu erfüllen. Remote Access spielt dabei eine entscheidende Rolle.

Die SonicWALL® VPN Clients bieten eine flexible, benutzerfreundliche und leicht zu verwaltende Virtual Private Network (VPN)-Lösung, die geografisch verteilten und mobilen Benutzern einen sicheren und zuverlässigen Remote-Zugriff auf Unternehmensressourcen bietet – sei es über Breitband, Wireless- oder DFÜ-Verbindungen. Für einen sicheren Remote-Client-to-Host-Zugriff stellt SonicWALL sowohl SSL VPN- als auch IPSec VPN-Verbindungsoptionen bereit. Bei SSL VPN ermöglicht der SonicWALL NetExtender sowohl Thin Client-Konnektivität als auch einen webbasierten clientlosen Remote-Zugriff für Windows-, Windows Mobile-, Mac- und Linux-Systeme. Bei IPSec VPN kann mithilfe des SonicWALL Global VPN Client ein VPN Client auf das Client-System heruntergeladen werden, wodurch eine konventionelle, clientbasierte VPN-Oberfläche geschaffen wird.

## Funktionen und Vorteile

### Erweiterte Sicherheit auf allen Netzwerkebenen.

Hierfür sorgt die Kombination mit einer SonicWALL Network Security Appliance, die den VPN-Verkehr mithilfe der leistungsstarken Deep Packet Inspection-Technologie auf Sicherheitsbedrohungen wie Viren, Würmer, Trojaner und Spyware prüft. Diese kombinierte Lösung ist unter dem Namen SonicWALL Clean VPN\* bekannt.

**Unkomplizierte VPN-Verwaltung.** Das mehrfach ausgezeichnete Global Management System (GMS) von SonicWALL vereinfacht die Verwaltung von SonicWALL VPN Client-Verbindungen.

**SSL VPN für Network Security – NetExtender Konnektivität ohne Client.** Macht vorinstallierte VPN-Clients (Fat Clients) überflüssig. Damit erübrigt sich die aufwändige Installation und Aktualisierung der Clients auf den einzelnen Windows-, Mac- oder Linux-PCs.

**NetExtender-Technologie.** Bietet erweiterte Funktionen, wie z. B. Netzwerkzugriff auf zusätzliche Ressourcen, Services und Anwendungen im Unternehmensnetzwerk.

**Unterstützung für mobile Geräte.** Ermöglicht den Zugriff auf das gesamte Intranet sowie auf Webanwendungen und bietet Remote-Mitarbeitern mehr Flexibilität.

### Global VPN Client

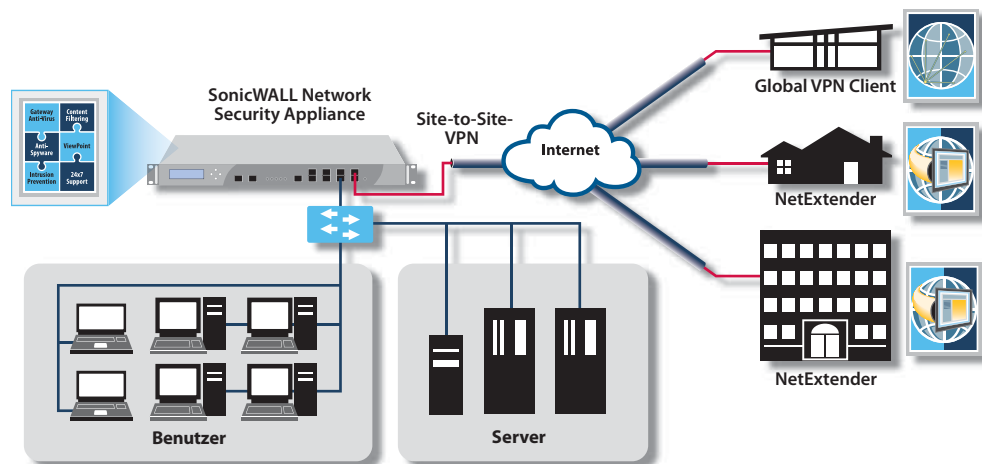
**Hilfreiche Assistenten.** Sorgen für eine schnelle und einfache Implementierung und Konfiguration von VPN-Verbindungen. IPSec VPN-Anwender müssen nur den Domänennamen oder die IP-Adresse des SonicWALL-VPN-Gateways eingeben, um die Konfigurationsregeln für den Global VPN Client automatisch herunterzuladen.

**Erweiterte Zugriffsmöglichkeiten für produktives Arbeiten.** Benutzer können von Microsoft® Windows®-basierten Single- oder Dual-Prozessor-PCs auf das Netzwerk zugreifen. Dabei sorgt der Global VPN Client dafür, dass eingekapselte VPN-Daten beliebige IP-Netzwerke mithilfe von Network Address Translation (NAT) passieren können und erweitert so den sicheren Remote-Zugriff.

**Zuverlässige VPN-Sitzungen.** Gleichzeitige Global VPN Client-Verbindungen lassen sich mit mehreren SonicWALL VPN-Gateways einrichten. Der Global VPN Client unterstützt redundante SonicWALL VPN-Gateways, um den Netzwerkzugriff auf geschäftskritische Ressourcen sicherzustellen, falls das Hauptgateway ausfällt.

\*Clean VPN erfordert einen aktivierten Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention-Abovertrag für die zentrale SonicWALL Network Security Appliance.

# Technische Daten



Comprehensive Gateway Security Suite mit Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention, Application Firewall, Content Filtering, ViewPoint Reporting und 24/7-Support

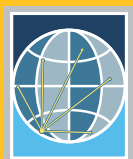


Clean VPN zur Verschlüsselung und Säuberung des Datenverkehrs



## SonicWALL UTM SSL VPN Client

- SonicWALL UTM SSL VPN  
1 Lizenz  
01-SSC-8629
- SonicWALL UTM SSL VPN  
5 Lizenzen  
01-SSC-8630
- SonicWALL UTM SSL VPN  
10 Lizenzen  
01-SSC-8631
- SonicWALL UTM SSL VPN  
25 Lizenzen  
01-SSC-8632
- SonicWALL UTM SSL VPN  
50 Lizenzen  
01-SSC-8633



## SonicWALL Global VPN Client

- Global VPN Client für Windows  
1 Lizenz  
01-SSC-5310
- Global VPN Client für Windows  
5 Lizenzen  
01-SSC-5316
- Global VPN Client für Windows  
10 Lizenzen  
01-SSC-5311
- Global VPN Client für Windows  
50 Lizenzen  
01-SSC-5313
- Global VPN Client für Windows  
100 Lizenzen  
01-SSC-5314
- Global VPN Client für Windows  
1.000 Lizenzen  
01-SSC-2897

Lizenz-Bundles Hardware	SSL VPN Client-Lizenzen gebündelt/max.	GVC Client-Lizenzen gebündelt/max.
TZ 100/TZ 100 W-N	1/5	0/5
TZ 200/TZ 200 W-N	2/10	2/10
TZ 210/TZ 210 W-N	2/10	2/25
NSA 240	2/15	2/25
NSA 2400	2/25	10/250
NSA 3500	2/30	50/1.000
NSA 4500	2/30	500/3.000
NSA 5000	2/30	500/3.000
NSA E5500	2/50	2.000/4.000
NSA E6500	2/50	2.000/6.000
NSA E7500	2/50	2.000/10.000

## Systemanforderungen für NetExtender

<b>Hardware</b>	Appliances der TZ 100-, 200- oder 210-Serie sowie der NSA- oder E-Class NSA-Serie
<b>Firmware/Betriebssystem</b>	Firmware-Version 5.2 oder höher erforderlich Windows 2000, 2003, XP/Vista (32-Bit und 64-Bit) Win Mobile 5 (Pocket PC), Win Mobile 6 (Classic/Professional), MacOS 10.4+ (PowerPC und Intel), Linux Fedora Core 3+ / Ubuntu 7+ / OpenSUSE

## Systemanforderungen für Global VPN Client

<b>Hardware</b>	SonicWALL Network Security Appliance der dritten, vierten oder fünften Generation erforderlich																								
<b>Firmware/Betriebssystem</b>	Firmware-Version 6.4.2 oder höher bzw. SonicOS 3.0 oder höher erforderlich IBM-kompatibler PC mit Intel/AMD-Prozessor																								
	<table border="1"> <thead> <tr> <th></th> <th>32 Bit</th> <th>64 Bit</th> </tr> </thead> <tbody> <tr> <td>XP Professional SP2</td> <td>Ja</td> <td>Ja</td> </tr> <tr> <td>XP Home SP2</td> <td>Ja</td> <td>Nein</td> </tr> <tr> <td>Vista Enterprise SP1</td> <td>Ja</td> <td>Ja</td> </tr> <tr> <td>Vista Business SP1</td> <td>Ja</td> <td>Ja</td> </tr> <tr> <td>Vista Home Basic SP</td> <td>Ja</td> <td>Ja</td> </tr> <tr> <td>Vista Home Premium SP1</td> <td>Ja</td> <td>Ja</td> </tr> <tr> <td>Vista Ultimate SP1</td> <td>Ja</td> <td>Ja</td> </tr> </tbody> </table>		32 Bit	64 Bit	XP Professional SP2	Ja	Ja	XP Home SP2	Ja	Nein	Vista Enterprise SP1	Ja	Ja	Vista Business SP1	Ja	Ja	Vista Home Basic SP	Ja	Ja	Vista Home Premium SP1	Ja	Ja	Vista Ultimate SP1	Ja	Ja
	32 Bit	64 Bit																							
XP Professional SP2	Ja	Ja																							
XP Home SP2	Ja	Nein																							
Vista Enterprise SP1	Ja	Ja																							
Vista Business SP1	Ja	Ja																							
Vista Home Basic SP	Ja	Ja																							
Vista Home Premium SP1	Ja	Ja																							
Vista Ultimate SP1	Ja	Ja																							
<b>Verfügbare Festplattenspeicher</b>	38 MB																								
<b>RAM</b>	512 MB																								
<b>Netzwerkverbindungen</b>	Ethernet-Netzwerk-Schnittstellenkarte mit NDIS-kompatiblen Treiber und/oder DFU-Adapter (internes oder externes Modem, ISDN-Terminal-Adapter) oder WLAN Global VPN Client																								

## Technische Daten für Global VPN Client

<b>IPSec-Modi</b>	ESP (Encapsulated Security Payload)
<b>Verschlüsselungs-algorithmen</b>	DES (56-Bit), 3DES (168-Bit), AES (256-Bit)
<b>Datensicherheit</b>	MD5, SHA-1
<b>Authentifizierung und Schlüsselverwaltung</b>	IKE (Internet Key Exchange)
<b>Benutzer-authentifizierung</b>	RADIUS mit XAUTH, lokaler Benutzer, LDAP, Microsoft Active Directory, Novell eDirectory
<b>Unterstützte Zertifikate</b>	Microsoft, Verisign, Entrust
<b>Unterstützte Standards und RFCs</b>	ESP-Tunnelmodus, IKE (ISAKMP/Oakley): Internet-Schlüsselaustausch mit RFC-Unterstützung (RFC2407-2409), NAT-Traversal (IETF-Drafts), X.509 v3-Zertifikate: (RFC2459), PKCS #7: Cryptographic Message Syntax-Standard (RFC2315), PKCS #12: Personal Information Exchange Syntax-Standard, FIPS Pub 46-1: Datenverschlüsselungsstandard, FIPS Pub 180-1: Secure Hash-Standard, Microsoft Vista 32-Bit

## 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

