



SonicWALL Clean Wireless

CLEAN WIRELESS

Leistungsstarke Clean Wireless-Lösungen

- **Umfassende Wireless-Sicherheitsfunktionen**
- **Außergewöhnliche Wireless-Performance**
- **Zentrale WLAN-Verwaltung**
- **Verbesserte Wireless-Zuverlässigkeit**
- **Flexible Wireless-Implementierungsoptionen**
- **Virtual Access Point (VAP)-Segmentierung**
- **Unterstützung zahlreicher Protokolle**
- **Granulare Durchsetzung von Sicherheitsregeln**
- **Optisch dezente Wireless Access Points**
- **FairNet Wireless-Bandbreitenuordnung**

Mit der intensiveren Bandbreitennutzung, dem Wunsch nach nahtlosem Roaming, den erweiterten Netzwerkgrenzen sowie der gestiegenen Anzahl an Verbindungen wachsen die Anforderungen an drahtlose Netzwerke. Gleichzeitig wird die Verwaltung bestehender 802.11-Wireless-Umgebungen erschwert. Viele Unternehmen stehen daher vor einer schwierigen Herausforderung: Sie müssen die Kompatibilität mit alten 802.11-Technologien gewährleisten und gleichzeitig ihr drahtloses Netzwerk durch eine zentrale Verwaltung und Kontrolle über alle WLAN-Nodes hinweg erweitern und optimieren, ohne dabei die Sicherheit zu vernachlässigen.

Die SonicWALL® Clean Wireless™-Lösungen kombinieren High-Performance-802.11n-Technologie mit Netzwerksicherheitsappliances der Enterprise-Klasse, um höchste Wireless-Sicherheit und Performance zu gewährleisten und gleichzeitig die Konfiguration und Verwaltung sämtlicher 802.11-basierter drahtloser Netzwerke zu vereinfachen.

Die Lösung basiert auf IEEE 802.11 a/b/g/n-kompatiblen SonicWALL SonicPoint-N (SonicPoint-Ni Dual-Band, SonicPoint-Ne Dual-Band und SonicPoint-N Dual-Radio) Wireless Access Points und sorgt dafür, dass Anwender in WLANs mit hoher Bandbreite sicher und schneller auf Daten sowie auf Voice- und Video-Ressourcen zugreifen können. Die SonicPoint-N Wireless Access Points lassen sich für Netzwerke jeder Größenordnung skalieren. Sie müssen nicht vorkonfiguriert werden, da sie von einer aktuellen SonicWALL-Firewall zentral konfiguriert und verwaltet werden können, ohne dass ein zusätzlicher Wireless Access Controller erforderlich ist.

Dank nahtloser Integration der Wireless Access Points mit einer erstklassigen Next-Generation Firewall bzw. Unified Threat Management Firewall mit erweiterter Application Intelligence and Control-Technologie werden die drahtlos übermittelten Daten genauso gründlich wie der kabelgebundene Datenverkehr gescannt. Auf diese Weise können IT-Administratoren verteilte High-Performance-Wireless-Netzwerke mit einheitlicher Regelverwaltung in drahtlosen und kabelgebundenen Netzwerken implementieren und unkompliziert verwalten.

Funktionen und Vorteile

Umfassende Wireless-Sicherheitsfunktionen wie Wireless Intrusion Detection Services (WIDS), Wireless Firewall, sicheres Layer 3-Wireless-Roaming, IEEE 802.11d Roaming – auch World Mode genannt – und integrierte Wireless Guest Services (WGS) zur Durchsetzung eines passwortgeschützten Zugriffs für Kunden und andere Gastbenutzer.

Außergewöhnliche Wireless-Performancefunktionen wie 40-MHz-Kanäle und Paket-Aggregation zur Unterstützung von Datenraten bis zu 600 MBit/s. Dank Dual-Radio- und Dual-Band-Unterstützung können wahlweise 2,4-GHz- oder 5,0-GHz-Netzwerke verwendet werden.

Zentrale WLAN-Verwaltung über eine SonicWALL Firewall der SuperMassive™ E10000-, E-Class Network Security Appliance (NSA)-, NSA- oder TZ-Serie, ohne dass die SonicPoint-N-Geräte vorkonfiguriert werden müssen.

Verbesserte Wireless-Zuverlässigkeit. Die Multiple-Input Multiple-Out (MIMO)-Technologie verwendet mehrere Antennen als Sender sowie als Empfänger, um den Durchsatz und die Zuverlässigkeit zu verbessern.

Flexible Wireless-Implementierungsoptionen. Befestigung an der Wand oder an der Decke möglich. Die SonicPoint-N Wireless Access Points können über einen SonicWALL Power over Ethernet (PoE) Injector oder ein entsprechendes Fremdanbietergerät mit Strom versorgt werden, falls Steckdosen schwer zugänglich sind. (Für SonicPoint-Ni Dual-Band und SonicPoint-Ne Dual-Band wird ein Gerät nach IEEE 802.3af PoE benötigt, für SonicPoint-N Dual-Radio ein Gerät nach

IEEE 802.3at PoE.) Die SonicPoint-N Dual-Radio und SonicPoint-Ne Dual-Band Access Points können auch direkt über ein AC-Netzteil versorgt werden.

Virtual Access Point (VAP)-Segmentierung. Erlaubt bis zu acht SSIDs mit dedizierten Authentifizierungs- und Datenschutzeinstellungen bei Nutzung der gleichen physischen Infrastruktur und ermöglicht eine logische Segmentierung von sicherem, drahtlosem Netzwerkverkehr und einen sicheren Kundenzugriff.

Unterstützung zahlreicher Protokolle wie 802.11 a/b/g/n, WPA2 und WPA, so dass Unternehmen Geräte, die keine höheren Verschlüsselungsstandards unterstützen, weiterhin nutzen können. Darüber hinaus ist eine unkomplizierte Migration zu 802.11n möglich.

Granulare Durchsetzung von Sicherheitsregeln. Erlaubt die Implementierung von Firewall-Regeln für den gesamten drahtlosen Datenverkehr und kontrolliert die gesamte drahtlose Client-Datenübertragung zu sämtlichen Hosts im Netzwerk, egal ob kabelgebunden oder drahtlos.

Optisch dezente Wireless Access Points mit LED- und Logo-Abdeckungen, dimmbaren LEDs (außer Betriebsanzeige) und internen Antennen (bei den SonicPoint-Ni-Modellen).

FairNet Wireless-Bandbreitenuordnung. Garantiert jedem Wireless-Benutzer eine Mindestbandbreite, um zu verhindern, dass einzelne Benutzer überproportional viel Bandbreite beanspruchen.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

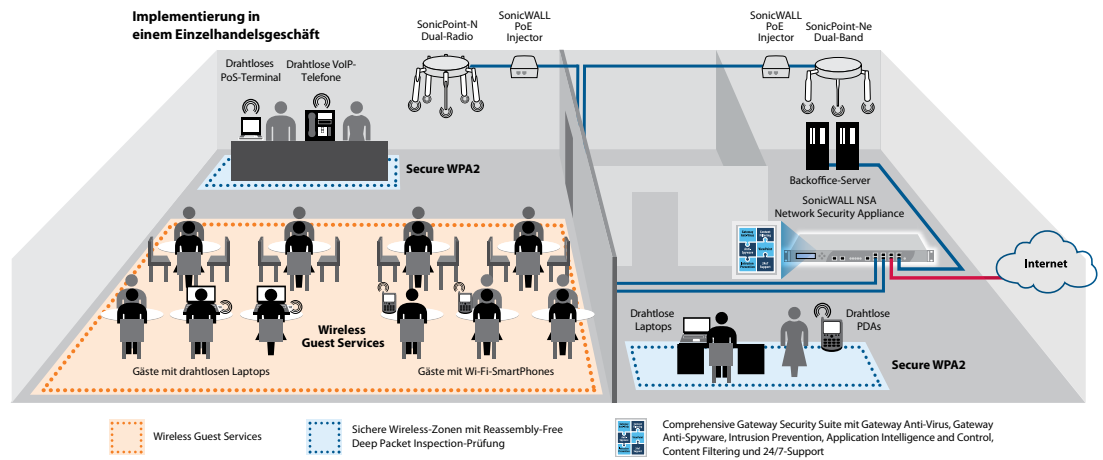
1. Beispiel: Kleines Einzelhandelsgeschäft/Arzt- oder Zahnarztpraxis

Einzelhandelsunternehmen, Arzt- oder Zahnarztpraxen können die SonicPoint-N Wireless Access Points mit Firewall-Lösungen von SonicWALL kombinieren, um schnell zusätzliche Kapazitäten für den drahtlosen Netzwerkzugang zu schaffen. Gleichzeitig erfolgt am Gateway für den Datenverkehr über kabelgebundene und drahtlose Verbindungen eine Reassembly-Free Deep Packet Inspection™ (RFDPI), bevor der Zugriff auf sensible Daten freigegeben wird. Während SonicWALL Wireless Guest Services (WGS) dem Kunden einen passwortgeschützten Internetzugang zur Verfügung stellen, sorgen die SonicWALL Virtual Access Points (VAPs) für eine logische Segmentierung des sicheren drahtlosen Netzwerkverkehrs und ermöglichen einen unbedenklichen Kundenzugriff.

- SonicPoint-N Wireless Access Points mit 802.11n bieten einen schnelleren drahtlosen Zugriff mit größerer Reichweite und höherer Zuverlässigkeit.
- Die SonicPoint-N Wireless Access Points ermöglichen es

Mitarbeitern, über SSL VPN oder WPA2 sicher auf Netzwerkressourcen aus dem Drahtlosnetz zuzugreifen.

- Durch die Übertragung von bis zu acht eindeutigen SSIDs sorgen die VAPs für eine sichere Segmentierung vertrauenswürdiger und nicht vertrauenswürdiger Wireless-Benutzer.
- SonicWALL RFDPI prüft den gesamten drahtlosen Datenverkehr auf Sicherheitsgefahren und Bedrohungen.
- Mit SonicWALL WGS können Kunden drahtlos auf Netzwerkressourcen zugreifen.
- Auto-Provisioning und zentralisierte Verwaltung für alle im Netzwerk implementierten SonicPoint-N Wireless Access Points.
- Bei den SonicPoint-N Dual-Radio Wireless Access Points kann ein Funkkanal speziell für die Erkennung unberechtigter Access Points verwendet werden, während der andere Kanal Wireless-Nutzern zur Verfügung steht, um so die Einhaltung gesetzlicher Vorgaben sicherzustellen.



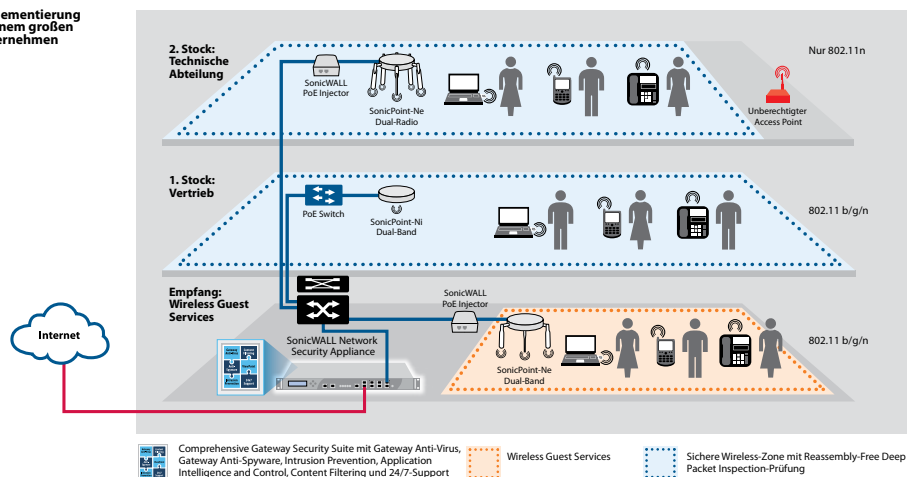
2. Beispiel: Clean Wireless-Lösung

In verteilten Organisationen können sich SonicPoint-N Wireless Access Points automatisch mit einer Firewall von SonicWALL verbinden, um die neuesten Konfigurationen und die aktuelle Firmware via Auto-Provisioning zu erhalten. Auf diese Weise wird eine schnelle Implementierung erreicht. Die SonicWALL Firewalls bieten eine zentrale Wireless-Überwachung und -Verwaltung und senken so die TCO für die Infrastruktur. Die Geräte der SonicPoint-N-Serie bieten integrierte drahtlose Intrusion Detection Systems (IDS), die nach unberechtigten Access Points suchen und unberechtigte Zugriffe verhindern.

- SonicPoint-N Wireless Access Points mit 802.11n bieten einen schnelleren drahtlosen Zugriff mit größerer Reichweite und höherer Zuverlässigkeit.

- Die SonicPoint-N Wireless Access Points erkennen automatisch das zentrale Verwaltungsgateway und erleichtern die Implementierung.
- Die Geräte der SonicPoint-N-Serie ermöglichen es Mitarbeitern, über SSL VPN oder WPA2 sicher auf Netzwerkressourcen aus dem Drahtlosnetz zuzugreifen.
- SonicWALL RFDPI prüft den gesamten drahtlosen Datenverkehr umfassend auf Sicherheitsgefahren und Bedrohungen.
- Durch die Übertragung von bis zu acht eindeutigen SSIDs sorgen die VAPs für eine sichere Segmentierung vertrauenswürdiger und nicht vertrauenswürdiger Wireless-Benutzer.

Implementierung in einem großen Unternehmen



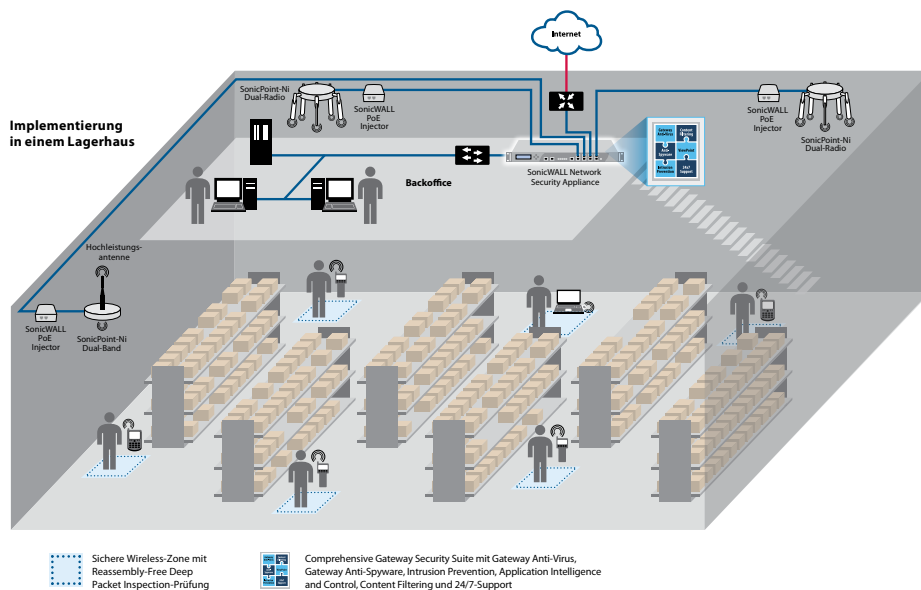
3. Beispiel: Implementierung in einem Lagerhaus

In Lagerhäusern können sich SonicPoint-N Wireless Access Points automatisch mit einer Firewall von SonicWALL verbinden, um die neuesten Konfigurationen und die aktuelle Firmware via Auto-Provisioning zu beziehen. Auf diese Weise wird eine schnelle Implementierung erreicht. Die SonicWALL-Firewalls bieten eine zentrale Wireless-Überwachung und -Verwaltung und senken so die TCO für die Infrastruktur. Die SonicPoint-Ni Dual-Band und SonicPoint-Ne Dual-Band Access Points verfügen über integrierte drahtlose IDS, die nach unberechtigten Access Points suchen und unberechtigte Zugriffe verhindern.

- SonicPoint-N Wireless Access Points mit 802.11n bieten einen schnelleren drahtlosen Zugriff mit größerer Reichweite und höherer Zuverlässigkeit.
- Die SonicPoint-N Wireless Access Points erkennen automatisch

das zentrale Verwaltungsgateway und erleichtern die Implementierung.

- SonicPoint-N Wireless Access Points ermöglichen es Mitarbeitern, über SSL VPN oder WPA2 sicher auf Netzwerkressourcen aus dem Drahtlosnetz zuzugreifen.
- SonicWALL RFDPI prüft den gesamten drahtlosen Datenverkehr umfassend auf Sicherheitsgefahren und Bedrohungen.
- Durch die Übertragung von bis zu acht eindeutigen SSIDs sorgen die VAPs für eine sichere Segmentierung vertrauenswürdiger und nicht vertrauenswürdiger Wireless-Benutzer.
- Die SonicWALL Firewalls bieten Auto-Provisioning und eine zentralisierte Verwaltung für alle im Netzwerk implementierten SonicPoints.



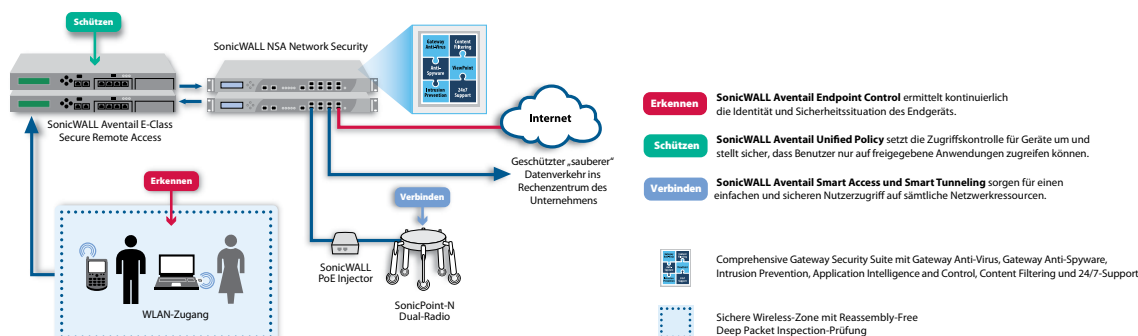
4. Beispiel: Enterprise Wireless-Umgebung und SonicWALL Aventail E-Class Secure Remote Access

In verteilten Wireless-Umgebungen, in denen zusätzliche Endpoint Security und Network Access Control (NAC) erforderlich sind, können Netzwerkadministratoren SonicPoints zusammen mit einer SuperMassive E10000- oder E-Class NSA-Appliance sowie einer SonicWALL Aventail E-Class Secure Remote Access (SRA)-Appliance implementieren. Die kombinierte Lösung bietet nicht nur eine verteilte Wireless-Konnektivität und eine zentrale SonicPoint-Verwaltung, sie führt außerdem Endpunkt-Abfragen durch und setzt Sicherheitsregeln an den Endbenutzergeräten durch, so dass alle Wireless-Systeme über eine ordnungsgemäße Konfiguration verfügen, bevor sie Zugriff auf sichere Netzwerkressourcen erhalten.

- An allen Eingangspunkten werden Sicherheitsregeln durchgesetzt, die eine granulare Zugriffskontrolle für eine effiziente

Zusammenarbeit und Einhaltung von Compliance-Vorgaben ermöglichen.

- Die benutzerfreundliche Lösung bietet schon heute die wichtigsten NAC-Elemente und stellt eine solide Grundlage für zukünftige NAC-Initiativen dar.
- Die SonicWALL 802.11n-Lösungen bieten einen schnelleren drahtlosen Zugriff mit größerer Reichweite und höherer Zuverlässigkeit.
- Durch die Übertragung von bis zu acht eindeutigen SSIDs sorgen die VAPs für eine sichere Segmentierung vertrauenswürdiger und nicht vertrauenswürdiger Wireless-Benutzer.
- Die SonicWALL Firewalls bieten Auto-Provisioning und eine zentralisierte Verwaltung für alle im Netzwerk implementierten SonicPoints.



Technische Daten



SonicWALL SonicPoint-N Dual-Radio mit PoE Injector
01-SSC-9290

SonicWALL SonicPoint-N Dual-Radio 4er Pack ohne PoE Injector
01-SSC-9292

SonicWALL SonicPoint-N Dual-Radio 8er Pack ohne PoE Injector
01-SSC-9294



SonicWALL SonicPoint-Ni Dual-Band mit PoE Injector
01-SSC-8576

SonicWALL SonicPoint-Ni Dual-Band 4er Pack ohne PoE Injector
01-SSC-8589

SonicWALL SonicPoint-Ni Dual-Band 8er Pack ohne PoE Injector
01-SSC-8593



SonicWALL SonicPoint-Ne Dual-Band mit PoE Injector
01-SSC-8578

SonicWALL SonicPoint-Ne Dual-Band 4er Pack ohne PoE Injector
01-SSC-8591

SonicWALL SonicPoint-Ne Dual-Band 8er Pack ohne PoE Injector
01-SSC-8584



PoE Injector 802.3af Gigabit N
01-SSC-5544

	SonicPoint-N Dual-Radio	SonicPoint-Ni Dual-Band	SonicPoint-Ne Dual-Band
Hardware			
Abmessungen	19,1 cm (L) x 19,1 cm (B) x 3,8 cm (H)	15 cm (L) x 15 cm (B) x 3 cm (H)	
Gewicht	0,39 kg	0,27 kg	
Anforderungen an die PoE-Stromversorgung	802.3at /0,35 A	802.3af/0,35 A	
Stromversorgung	PoE und AC-Netzteil	PoE	PoE und AC-Netzteil
Statusanzeigen	Sechs (6) LEDs (WLAN, Link/Act) (LAN, Link/Act), Betrieb, Wrench		
Antennen	Jeweils 3 externe SMA- und RP-TNC-Antennen	Komplett intern	3 externe SMA-Antennen
LAN-Anschlüsse	1 10/100/1000 Autosensing RJ-45-Port für Ethernet und Power over Ethernet (PoE) 1 RJ-45-Konsolenport		
Montage	Kit für Wand- bzw. Deckenhalterung; Logo- und LED-Abdeckung		
Virtual Access Points	Bis zu 8 pro SonicPoint		
Maximale Anzahl verwalteter Geräte			
Security Appliance	Pro WLAN-Schnittstelle	Pro Appliance	
TZ 100/100 Wireless-N	1	1	
TZ 200/200 Wireless-N	2	2	
TZ 210/210 Wireless-N	16	16	
NSA 240	16	16	
NSA 2400/2400MX	32	32	
NSA 3500	48	48	
NSA 4500	64	64	
NSA 5000	64	64	
NSA E5500	96	96	
NSA E6500	128	128	
NSA E7500	128	128	
NSA E8500	128	128	
SuperMassive E10000-Serie	128	128	
Standards			
Erfüllt folgende Normen	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n Draft 2.0, IEEE 802.11i, IEEE 802.3af		
Richtlinien	FCC/ICES CE, G-Tick, RoHS, WEEE		
Sicherheit	UL, cUL, TÜV-GS, CB, CE		
Umgebungsbedingungen			
Temperaturbereich	0 bis 40 °C		
Funkdaten			
Frequenzband	802.11a: 5,180-5,825 GHz; 802.11b/g: 2,412-2,472 GHz; 802.11n: 12-2,472 GHz, 5,180-5,825 GHz		
Verwendete Kanäle	802.11a: USA und Kanada 9, Europa 15, Japan 8, Singapur 9, Taiwan 4 Kanäle 802.11b/g/n: USA und Kanada 1-11, Europa 1-13, Japan 1-14		
Dynamische Frequenzwahl	Unterstützt		
Sendeleistung	Abhängig von den landesspezifischen gesetzlichen Vorgaben		
TPC (Transmit Power Control)	Unterstützt		
Unterstützte Datenraten	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 MBit/s pro Kanal; 802.11b: 1, 2, 5, 11 MBit/s pro Kanal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 MBit/s pro Kanal 802.11n: 6, 9, 12, 18, 24, 36, 48, 54, 72, 84, 150, 300 MBit/s pro Kanal		
Modulationstechnologie	802.11a: OFDM (Orthogonal Frequency Division Multiplexing), BPSK, QPSK, 1-QAM, 64-QAM 802.11b: DSSS (Direct Sequence Spread Spectrum), CCK, DBPSK, DQPSK 802.11g: OFDM (Orthogonal Frequency Division Multiplexing), BPSK, QPSK, 16-QAM, 64-QAM; 802.11n: 802.11n Draft 2.0		
Sicherheit			
Datenverschlüsselung	WPA2; IPSec, 802.11i, WPA; 64/128/152 Bit WEP, TKIP, AES, SSL VPN*		
Authentifizierung			
Authentifizierung	RADIUS, Active Directory, Novell e-Directory, SAMBA, Single Sign-On (SSO)		
PoE Injector			
Hardware			
Anzahl der Anschlüsse	2: 1 Eingang (Daten); 1 Ausgang (Daten und Spannung)		
Abmessungen	31 mm (H) x 58,5 mm (B) x 145 mm (T)		
Gewicht	450 g		
Anschlüsse	Shielded RJ-45, EIA 568A und 568B		
Anzeige	Systemanzeige: Netzspannung (grün); Benutzeranzeige: Kanalspannung aktiv (grün)		
Datenraten	10/100/1000 MBit/s		
Power over LAN-Ausgang			
Pinbelegung/Polarität	4/5 (+), 7/8 (-) T21 210W		
Ausgangsspannung	-48 VDC		
Benutzeranschluss	Min. 15,4 W	Min. 16,4 W	Min. 15,4 W
Notwendige Eingangsspannung			
AC Eingangsspannung	90-264 VAC		
AC-Frequenz	47-63 Hz		
AC-Eingangstrom	0,5 A bei 100-240 VAC		
Standards und Richtlinien			
Standards/Normen	CE, RoHS, WEEE; Elektromagnetische Emission und Immunität; EN 55022, CISPR 22, FCC Part 15 (Class B mit FTP-Kabel); EN 55024, CISPR 24		
Sicherheits-Zertifizierungen	UL 60950-1; EN 60950; IEC 60950-1		
Umgebungsbedingungen			
Umgebungstemperatur bei Betrieb	0-40 °C		
Luftfeuchtigkeit bei Betrieb	Max. 90 %, nicht kondensierend		
Temperatur bei Lagerung	-20 bis 70 °C		
Luftfeuchtigkeit bei Lagerung	Max. 93 %, nicht kondensierend		
Höhe bei Betrieb	-304,8 bis 3048 m		

*Bei Einsatz mit einer SonicWALL Appliance der Secure Remote Access-Serie

Weitere Informationen zu den Clean Wireless-Lösungen von SonicWALL 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-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™