

# Clean Wireless

So werden drahtlose Netzwerke sicherer, leistungsfähiger, kosteneffizienter und einfacher zu verwalten

**SONICWALL**®

PROTECTION AT THE SPEED OF BUSINESS™

# Inhalt

Was hält Unternehmen davon ab, Wireless-Netzwerke einzuführen?	1
Sicherheit von Wireless-Netzwerken	2
Performance von Wireless-Netzwerken	3
Verwaltung von Wireless-Netzwerken	4
Kosteneffizienz von Wireless-Netzwerken	5
SonicWALL® Clean Wireless™	6
Fazit	7

# Was hält Unternehmen davon ab, Wireless-Netzwerke einzuführen?

WLAN-Netze (Wireless Local Area Networks) haben viele Vorteile. Sie ermöglichen flexibles Arbeiten an unterschiedlichen Orten und steigern die Produktivität von Mitarbeitern, Partnern vor Ort, Lieferanten und Gästen. In Geschäften, Wartezimmern von Arztpraxen oder Cafés sorgen WLANs für mehr Komfort, zufriedeneren Kunden, höhere Umsätze und eine engere Kundenbindung. Hinzu kommt, dass WLANs oft günstiger sind als kabelgebundene Netzwerke.



**Obwohl WLANs enorme Vorteile bieten, haben viele Kunden noch Zweifel.**

Die meisten Unternehmen würden Wireless-Technologien am liebsten sofort einsetzen. Doch es gibt Bedenken auf Seiten der IT-Abteilung im Hinblick auf

- die Sicherheit von Wireless-Netzwerken
- die Performance von Wireless-Netzwerken
- die Verwaltung von Wireless-Netzwerken
- der Kosteneffizienz von Wireless-Netzwerken

# Sicherheit von Wireless-Netzwerken



Ausführliche Medienberichte über frühere Sicherheitslücken mit der WEP-Verschlüsselung, über Hacker, die vom Auto aus gezielt nach offenen WiFi-Netzen suchen („War-Driving“) und über andere Methoden zum Knacken von Wireless-Netzen haben zu einem erhöhten Sicherheitsbewusstsein und dem Wunsch nach einer besseren Sicherheitslösung für drahtlose Netze geführt.

***WLANs müssen mindestens genauso sicher sein wie kabelgebundene Netzwerke mit Deep Packet Inspection.***

Um bei der Sicherheit mit kabelgebundenen Netzwerken gleichzuziehen, benötigen WLANs zudem weitere Sicherheitsfunktionen, wie z. B.:

- Unified Threat Management (UTM), um Datenverkehr mithilfe von Intrusion Prevention-, Virenschutz- und Spamschutz-Technologien zu durchsuchen.
- Wireless Intrusion Detection und Prevention (WIDS/WIPS), um unberechtigte Zugriffe und DoS (Denial of Service)-Angriffe zu verhindern.
- Sicherheit auf Anwendungsebene, um die Nutzung von unerlaubten Anwendungen und den Zugriff auf vertrauliche Informationen zu verhindern.
- Funktionen für die Zugriffskontrolle, die den Zugriff davon abhängig machen, ob auf den Endpunkten eine entsprechende Sicherheitssoftware mit den erforderlichen Sicherheitseinstellungen aktiv ist.

# Performance von Wireless-Netzwerken

Ein Wireless-Netzwerk muss latenzkritische Anwendungen wie Voice/ Video over IP (VoIP) unterstützen können und eine adäquate Servicequalität gewährleisten. 802.11n-Implementierungen erreichen zwar Durchsatzraten von bis zu 300 MBit/s, doch bei Einsatz in einer bestehenden 802.11b/g/a-Infrastruktur kann die Leistung deutlich einbrechen.



***Kommen mehr Wireless Services für mehr Benutzer und Anwendungen hinzu, kann die Netzwerk-Performance darunter leiden.***



Ein flexibler Ansatz kann dazu beitragen, Leistungseinbußen zu vermeiden. IT-Manager können beispielsweise:

- den Zugriff auf 802.11n-Clients beschränken.
- Dualband/Dual Radio-Access Points verwenden, um 802.11n Clients auf das 5-GHz-Band zu begrenzen und das 2,4-GHz-Band den 802.11b/g-Endpunkten zu überlassen.
- die Nutzung der verfügbaren Wireless-Bandbreite anhand von Kriterien wie User, Uhrzeit, Datum oder Art der Anwendung steuern

# Verwaltung von Wireless-Netzwerken

Je mehr Wireless Services hinzukommen, desto komplexer werden Implementierung, Konfiguration und laufende Verwaltung der Infrastruktur. Dies gilt besonders für Lösungen mit vielen Funktionen und Features.

*Eine ideale Lösung sollte nicht nur **die Implementierung, sondern auch die laufende Verwaltung vereinfachen.***



Dabei ist eine zentrale Verwaltung erst der Anfang. Zusätzlich sind folgende Verwaltungsfunktionen erforderlich:

- Zuverlässige Überwachungs- und Reporting-Funktionen, um die Fehlersuche, Regelkontrolle und Konfiguration zu vereinfachen.
- Power over Ethernet (PoE) zur einfachen Implementierung von Access Points.
- Auto-Discovery- und Auto-Provisioning-Funktionen zur automatischen Erkennung und Bereitstellung neuer Access Points über zentral definierte und verwaltete Konfigurationen.
- Automatische Verteilung von Firmware und zeitkritischen Patch-Updates.

# Kosteneffizienz von Wireless-Netzwerken

Komplexität kann zu höheren Kosten führen. Um sichere WLAN-Netzwerke zu realisieren, werden häufig zusätzlich zu den bestehenden WPA2- oder WIDS/WIPS-Lösungen separate Firewall-, VPN-, IPS- oder multifunktionale UTM-Geräte hinter dem Wireless Access Switch/ Controller (WAC) implementiert. Doch durch den Einsatz mehrerer Appliances steigen auch die IT-Kosten.

**Moderne Lösungen zeichnen sich durch niedrigere TCO (Total Cost of Ownership) aus, da sie WAC und UTM in einem Gerät kombinieren.**



Eine kombinierte WAC/UTM-Lösung sollte für den jeweiligen Einsatz optimiert sein und die gleiche Funktionalität und Leistung bieten wie Einzelkomponenten. Um Kosten zu sparen, sollte die Wireless-Lösung außerdem folgendes bieten:

- Ein einheitliches Konzept, um Regel- und Objektdefinitionen über eine zentrale Verwaltungsoberfläche zu erstellen.
- Einen PoE-Injector, um teure Erweiterungen des Stromnetzes zu vermeiden.
- Abwärtskompatibilität mit älteren Generationen von Wireless-Clients, um eine maximale Auslastung zu gewährleisten, ohne die Client-Systeme aktualisieren zu müssen.

# SonicWALL Clean Wireless™

SonicWALL® Clean Wireless vereint High-Speed-Wireless-Sicherheit mit leistungsstarkem Unified Threat Management bei Einsatz einer Appliance der SonicWALL TZ-, der NSA (Network Security Appliances)- oder der E-Class NSA-Serie in Verbindung mit SonicPoint-N™ Dual-Band- oder SonicPoint™-Access Points.



**SonicWALL Clean Wireless bietet mehr Sicherheit und Leistung, mehr Kosteneffizienz und eine einfachere Verwaltung.**



Die innovative SonicWALL Clean Wireless-Lösung liefert doppelten Schutz:

- 1** Verschlüsselung und Schutz von Wireless-Datenverkehr in drahtlosen High-Speed-802.11n-Netzwerken.
- 2** Filterung des Datenverkehrs und Reassembly-Free Deep Packet Inspection in Hochgeschwindigkeit, um das Wireless-Netzwerk umfassend vor Viren, Spyware und anderen Bedrohungen zu schützen.

Die SonicWALL Clean Wireless-Lösung sichert das Netzwerk gleich zweifach ab: Sie verschlüsselt den Wireless-Datenverkehr, eliminiert mögliche Bedrohungen und schützt gleichzeitig das drahtlose Netzwerk vor Eindringversuchen. Die SonicWALL Clean Wireless-Lösung bietet dabei viel mehr als normale Sicherheitslösungen. So sorgt sie mit ihrer Deep-Packet-Inspection-Funktionalität dafür, das Wireless-Netzwerke genauso sicher wie ein Kabelnetzwerk sind. Große und kleine Unternehmen profitieren von mehr Sicherheit und Leistung, niedrigeren Kosten und einer einfacheren Verwaltung.

# Fazit

Egal ob im Einzelhandel, im Gesundheitswesen oder in der Industrie – WLANs bieten Unternehmen und Organisationen einen enormen Nutzen. Trotz der Vorteile gab es in der Vergangenheit immer wieder Bedenken von Seiten der IT-Verantwortlichen was die Sicherheit, die Leistung, die einfache Verwaltung und die Kosteneffizienz von Wireless-Netzen betrifft.

***Heute muss sich kein Unternehmen mehr für eindimensionale Secure Wireless-Lösungen entscheiden, die nur auf Verschlüsselungsbasis arbeiten.***

SonicWALL Clean Wireless mit Deep Packet Inspection macht WLANs genauso sicher wie kabelgebundene Netzwerke und bietet doppelte Sicherheit mit High-Speed Secure Wireless- und High-Performance UTM-Schutz. Auf diese Weise sorgt SonicWALL für:

- hohe Wireless-Sicherheit
- hohe Wireless-Performance
- eine einfache Verwaltung von Wireless-Netzwerken
- kosteneffiziente Wireless-Netzwerke

### **Wie erhalte ich weitere Informationen?**

- Laden Sie das Whitepaper „AimPoint Group: Secure Wireless leicht gemacht – Die Auswahl einer WLAN-Lösung der nächsten Generation für durchgehende WLAN-Implementierungen“ herunter.
- Lassen Sie sich unseren SonicWALL-Newsletter zuschicken:

Wenn Sie uns Feedback zu diesem E-Book, anderen E-Books oder Whitepapers von SonicWALL geben möchten, senden Sie eine E-Mail an folgende Adresse: **feedback@sonicwall.com**.

**Weiterempfehlen**

### **Über SonicWALL**

Als führender IT-Sicherheitsanbieter sorgt SonicWALL mit seinen intelligenten und dynamischen Service-, Software- und Hardware-Lösungen für den reibungslosen Betrieb von High-Performance-Unternehmensnetzen und senkt nicht nur die Risiken und Kosten, sondern auch die Komplexität. Weitere Informationen erhalten Sie auf unserer Website unter **www.sonicwall.com/de**.