

## Neue Anwendungen für den Einzelhandel auf der Grundlage sicherer IP- und Wireless-Technologien

*Durchgängige VPN-Konnektivität,  
umfassende Wireless-Sicherheit und  
zentrale Verwaltung ermöglichen neue  
POS-Anwendungen und steigern die  
Produktivität von POS-Systemen*

### INHALT

IP- und Wireless-Anwendungen für gesteigerte Produktivität	2
Sicherheitsrisiken von Breitband- und Drahtlos-Netzwerken	3
Zusätzliche Netzwerk-Aspekte	6
SonicWALL-Lösungen zum Schutz von POS-Anwendungen	8
Resümee	12

*Angesichts verschärfter Wettbewerbsbedingungen setzen Einzelhandelsunternehmen zunehmend auf neue Technologien, um Produktivität und Umsatz zu erhöhen und gleichzeitig Kosten zu senken. IP- und Wireless-Anwendungen bieten dem Einzelhandel praxiserprobte Lösungen. Gute Beispiele sind hier internet- und wirelessfähige POS-Systeme, browserbasierte Supply Chain-Anwendungen, drahtlose Handheld-Geräte und Service-Terminals. Die neuen Lösungen beschleunigen die Datenübertragung und verbessern den Informationsfluss, so dass der Einzelhandel von einer höheren Kundenzufriedenheit und einer Steigerung der Rentabilität profitiert.*

*Um IP- und Wireless-Anwendungen erfolgreich einsetzen zu können, müssen Einzelhandelsunternehmen die Herausforderungen dieser Technologien meistern. So müssen Geschäftsprozesse auch bei einem Netzausfall unterbrechungsfrei weiterlaufen und sensible Kunden- und Geschäftsinformationen effektiv geschützt werden. Auch die weit über das Netzwerk verteilten POS-Geräte sollten sich schnell und einfach einrichten und verwalten lassen.*

*Das vorliegende Whitepaper erläutert, wie sich Einzelhandelsunternehmen mithilfe neuer Anwendungen klare Wettbewerbsvorteile verschaffen können. Außerdem beleuchtet es verschiedene Sicherheitsaspekte und zeigt, in welcher Weise die POS-Lösungen von SonicWALL die genannten Anforderungen erfüllen und Einzelhandelsunternehmen konkrete Wettbewerbsvorteile eröffnen.*

## IP- und Wireless-Anwendungen für gesteigerte Produktivität

Einzelhandelsunternehmen setzen vermehrt auf IP-basierte Systeme und erweitern sie nach und nach mit Wireless-Technologien. Die Vorteile liegen auf der Hand: Nicht nur Front Office- und Back Office-Anwendungen lassen sich so optimieren, auch der Kundenservice und die Umsatzchancen können verbessert werden.

Front Office-Anwendungen wie beispielsweise IP-basierte Zahlungsabwicklung per Kreditkarte und temporäre Wireless POS-Terminals beschleunigen Transaktionen und erhöhen gleichzeitig die Kundenzufriedenheit. Durch Back Office-Anwendungen wie etwa internetbasierte Bestellungsabwicklung, Mitarbeiterportale und Bestandsverwaltung über Wireless-Verbindungen lassen sich Geschäftsabläufe effizienter gestalten und die Kosten deutlich senken.

### Front Office-Anwendungen

- **IP-Zahlungsabwicklung per Kreditkarte** – Dank internetbasierter Zahlungsabwicklung per Kreditkarte können Kosten reduziert und Transaktionen deutlich beschleunigt werden.
- **Kundenbindungsprogramme** – Neue POS-Systeme akzeptieren nicht nur Kreditkarten, sondern auch Kundenkarten und Geschenkgutscheine und bieten Käufern so eine größere Auswahl an Zahlungsmöglichkeiten. Außerdem erleichtern sie die Durchführung von Kundenbindungsprogrammen.
- **Mobile Aufnahme von Bestellungen** – Mit drahtlosen Handheld-Geräten können Servicekräfte in Restaurants Bestellungen am Tisch aufnehmen und Zahlungen abwickeln. Dadurch wird der Service verbessert und das Risiko von Kreditkartenbetrug reduziert.
- **“Line-busting”** – Mit drahtlosen Anwendungen können Transaktionen direkt beim Kunden abgewickelt und Wartezeiten an der Kasse verkürzt werden. Verkaufsmitarbeiter scannen die Ware des Kunden mit einem Handheld-Computer. Anschließend erhält der Kunde eine Plastikkarte oder einen Ausdruck mit Barcode, den er bei Zahlung an der Kasse vorlegt.
- **Temporäre POS-Terminals** – Drahtlose POS-Terminals eignen sich für den Einsatz in Einkaufspassagen oder auf Messen, um zeitlich befristete Verkaufsaktionen zu unterstützen.
- **Wireless-Hotspots** – Wireless Hotspots bieten Kunden einen bequemen öffentlichen Internet-Zugang. Restaurants, Coffee-Shops und Buchläden verbessern dadurch die Kundenzufriedenheit und können zusätzliche Umsätze generieren.
- **Service-Terminals** – An Service-Terminals können Kunden Geschenklisten einsehen und Artikel online im Katalog nachschlagen, während sie sich in der Verkaufsfiliale aufhalten.

## Back Office-Anwendungen

- **Internetbasierte Bestellungsabwicklung** – Internetbasierte Anwendungen zur Abwicklung von Bestellungen straffen die Lieferkette, steigern die Effizienz, erhöhen die Margen und senken die Kosten.
- **Mitarbeiterportale** – Über Internet-POS-Terminals können Mitarbeiter direkt auf Personal-Funktionen zugreifen (z.B. webbasierte Schulungen, Online-Formulare und Bonus-Informationen).
- **Bestandsverwaltung** – Drahtlose Handheld-Geräte erlauben eine regelmäßige Bestandsaufnahme und ermöglichen die Echtzeit-Abfrage wichtiger POS-Zahlen (z.B. Transaktionen, kumulierte Werte oder Lagerbestände).
- **Schwierig anzubindende Standorte** – Drahtlose POS-Terminals eignen sich besonders gut für Außenflächen und Gebäude, bei denen die Verkabelung problematisch ist.
- **Mobiler Zugang für Filialbetreuer** – Für leitende Mitarbeiter, die regelmäßig zwischen verschiedenen Verkaufsfilialen unterwegs sind, kann ein Wireless-Zugriff für wichtige Unternehmensressourcen eingerichtet werden.

Alle genannten Anwendungen setzen eine geschützte Netzwerkinfrastruktur voraus, die eine sichere, schnelle und zuverlässige Konnektivität zwischen den Verkaufsfilialen sowie Wireless-Konnektivität in den einzelnen Filialen bereitstellt.

- **Verbindungen zwischen Verkaufsfilialen** – Die meisten Einzelhandelsunternehmen ersetzen die konventionelle Datenübertragung über das WAN wie DFÜ und Frame Relay nach und nach durch Breitband-VPNs (Virtual Private Networks) (siehe **Verwendung von Breitband im Einzelhandel**). Breitband bietet kleinen, unabhängigen Händlern und großen Einzelhandelsketten gleichermaßen High-Speed-Konnektivität zu erschwinglichen Preisen. In Verbindung mit sicheren VPN-Technologien für den Datenaustausch über das Internet stellt Breitband eine besonders attraktive Option dar.

- **Drahtlose Konnektivität** – Um die Vorteile der neuen drahtlosen Anwendungen nutzen zu können, benötigen Einzelhandelsunternehmen ein sicheres Wireless-Netzwerk, das sensible Daten bei der Übermittlung über Radiowellen umfassend schützt.

### Verwendung von Breitband im Einzelhandel

Bis vor einigen Jahren vertrauten die meisten Einzelhandelsunternehmen bei der Internetanbindung ihrer POS-Systeme entweder auf DFÜ oder auf Frame Relay. Mittlerweile stellen jedoch viele auf Breitband-VPN über DSL oder Kabelmodem um. Breitband verbessert die Performance von POS-Anwendungen und sorgt für eine deutliche Senkung der Verbindungskosten.

Breitband im Vergleich mit Frame Relay:

- Verursacht nur einen Bruchteil der Kosten
- Bietet einen höheren Durchsatz

Breitband im Vergleich mit DFÜ:

- Reduziert den Zeitaufwand bei Kreditkartenzahlungen auf wenige Sekunden
- Verbessert die Zuverlässigkeit von POS-Abfragen und Zahlungsabwicklungen per Kreditkarte
- Macht Ausgaben für teure Fernverbindungen und zusätzliche Telefonleitungen überflüssig
- Bietet Bandbreite für zukünftige Anwendungen

## Sicherheitsrisiken von Breitband- und Drahtlos-Netzwerken

Breitband und Drahtlos-Netzwerke sind von Natur aus unsicher, weil Informationen über das Internet bzw. über Radiowellen versendet werden. Zu den Sicherheitsrisiken von Breitband- und Wireless-Verbindungen zählen der Diebstahl von Kundeninformationen, Viren, Würmer sowie der Missbrauch von Netzwerkressourcen. Diese Bedrohungen können Produktivitätseinbußen und – bei Netzwerkausfällen – Umsatzverluste nach sich ziehen. Daneben können sie rechtliche Probleme verursachen, wenn vertrauliche Kundeninformationen in die falschen Hände gelangen.

**Einzelhändler benötigen Lösungen, um ihre Kunden und ihr Unternehmen vor folgenden Sicherheitsrisiken zu schützen:**

**Hacker-Angriffe**

Viele Unternehmen stellen von DFÜ oder Frame Relay auf Breitband um, weil sie die Vorteile einer schnellen und kostengünstigen Verbindung nutzen wollen. Wenn die Breitbandverbindung aber nicht ausreichend gesichert ist, stellt sie eine Gefahr für die betroffenen POS-Systeme dar. Mögliche Folgen sind Diebstahl von Firmen- oder Kundeninformationen, die Beschädigung wichtiger Unternehmensdatenbanken sowie die unrechtmäßige Nutzung von Internetdiensten – alles Eingriffe, die den täglichen Geschäftsablauf empfindlich stören können.

Daher sollten Einzelhandelsunternehmen ihre Internetverbindung unbedingt mit einer Firewall absichern und für die Übertragung sensibler Daten über das Internet mit einem Virtual Private Network (VPN) (siehe Abb. 1) arbeiten. Um den Sicherheitsanforderungen von VISA und Mastercard (siehe **Sicherheit von Kreditkartendaten**) gerecht zu werden, benötigen Einzelhändler VPN-Verschlüsselung.

**Sicherheit von Kreditkartendaten**

Bestimmte Kreditkartenprogramme verlangen von Einzelhändlern den Einsatz von VPNs. Um eine einheitliche Vorgehensweise bei der Umsetzung dieser Sicherheitsanforderungen zu ermöglichen, haben sich die Kartenorganisationen Visa und MasterCard auf gemeinsame Standards geeinigt. Diese tragen die Bezeichnung „Payment Card Industry (PCI) Data Security Standards“ und haben Gültigkeit für die gesamte Kartenzahlungsbranche. Alle Organisationen, die vertrauliche Kontoinformationen und persönliche Daten speichern, verarbeiten oder übermitteln, müssen bestimmte grundlegende Sicherheitsanforderungen erfüllen. Zu diesen Anforderungen gehören die Installation einer Firewall, die Verschlüsselung von Daten im VPN-Tunnel, sowie die Installation bzw. die regelmäßige Aktualisierung von Antiviren-Software.

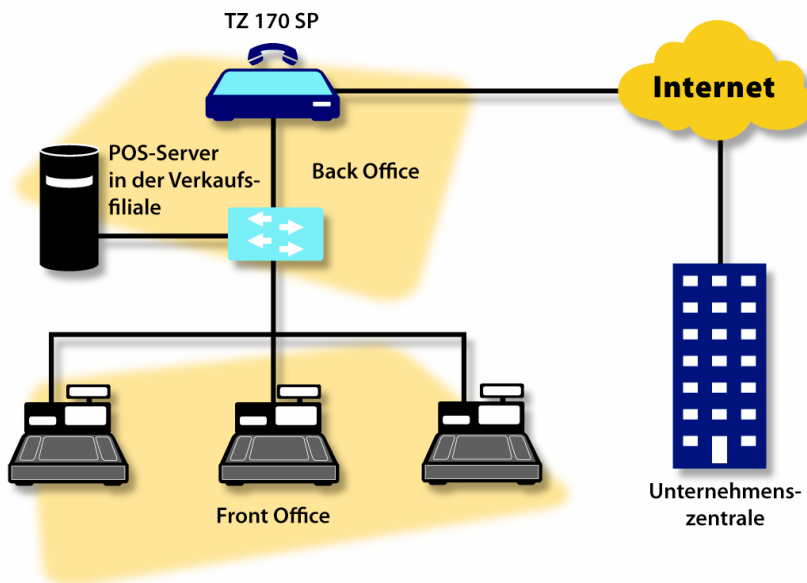


Abb. 1  
Virtual Private Network

## Viren und Würmer

Einzelhandelsunternehmen verwenden immer häufiger Standard-Betriebssysteme wie Windows und Linux. Für Viren-Programmierer sind Microsoft-Produkte aufgrund ihrer Verbreitung besonders attraktiv, während es Hacker gleichermaßen auf Microsoft- wie auf Linux-Systeme abgesehen haben, weil diese bekannte Schwachstellen aufweisen. Wie auf der Microsoft Security Website (<http://www.microsoft.com/security/protect/>) erläutert wird, müssen bei solchen Standard-Betriebssystemen sowohl Antivirenschutz-Lösungen als auch Firewalls installiert werden, um den möglichen Schaden durch Würmer in Grenzen zu halten.

Viren und Würmer befallen besonders häufig:

- **POS-Terminals** – Moderne POS-Terminals basieren auf Standard-Betriebssystemen und weisen damit dieselben Sicherheitsschwachstellen auf wie andere Anwendungen in Firmennetzwerken. Da POS-Systeme absolut geschäftskritische Anwendungen sind, können sich Einzelhändler keine Ausfälle durch Viren leisten.
- **Laptops von Filialbetreuern** – Laptops von Filialbetreuern sind besonders anfällig für Viren, da sie mobil eingesetzt werden und häufig auf unterschiedliche ungeschützte Netzwerke zugreifen. Außerdem besteht die Gefahr, dass Filialbetreuer, die sich vom Privatcomputer aus in Restaurantfilialen, Verkaufsstellen oder an ihrem Büro-Computer einloggen, unabsichtlich Viren über das ungesicherte Heimnetzwerk übertragen.

## Sicherheitsrisiken für Drahtlos-Netze

Wireless-Netzwerke sind noch anfälliger für Hacker-Angriffe als kabelgebundene Netze, weil Daten über Radiowellen übertragen werden und mit einfachen Mitteln abgefangen werden können. Wenn das Wireless-Netzwerk einer Verkaufsstelle oder eines Restaurants nicht abgesichert ist, können Hacker sogar von einem nahe gelegenen Parkplatz aus die Daten abfangen.

Es ist keine Seltenheit, dass Wireless-Netzwerke überhaupt nicht geschützt sind oder dass sie auf unsichere Methoden wie MAC-Adressen-Filterung oder WEP (Wired Equivalent Privacy) zurückgreifen. WEP verwendet einen gemeinsamen Schlüssel für alle Benutzer und wird deswegen häufig zur Zielscheibe für Sicherheitsbedrohungen. Mit frei verfügbaren Tools wie AirSnort oder WEPCrack können Hacker diese Schlüssel in wenigen Stunden umgehen.

## Zusätzliche Netzwerk-Aspekte

### Business Continuity

Sind IP-Anwendungen fest in das Netzwerk eines Einzelhändlers integriert, können Verbindungsausfälle Umsatzeinbußen und Produktivitätsverluste verursachen. Da Breitbandverbindungen durchaus ausfallen können, ist es wichtig, dass Unternehmen sowohl über eine Hauptverbindung, als auch über eine nahtlose Backup-Option verfügen. Als redundante Verbindung kann beispielsweise eine zweite Breitband-Verbindung oder eine DFÜ-Telefonleitung dienen (siehe Abb. 2). Um eine größtmögliche Business Continuity zu gewährleisten, sollten POS-Lösungen Ausfälle der Hauptverbindung erkennen und automatisch die Backup-Verbindung aktivieren. Außerdem sollte die Verbindung automatisch auf die Hauptverbindung zurückgesetzt werden, sobald diese wieder verfügbar ist.

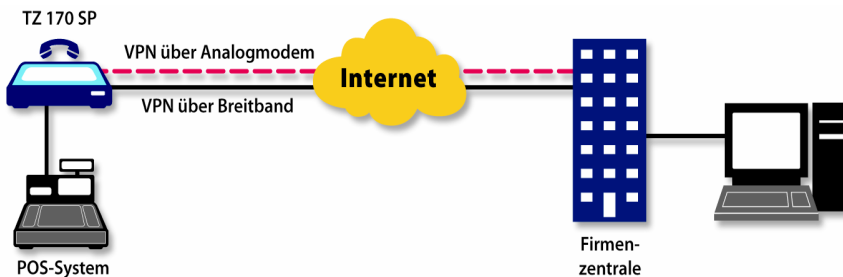


Abb. 2  
Redundante  
Verbindungs-  
optionen

### Zentrale Steuerung und Verwaltung

Einzelhandelsunternehmen betreiben oft mehrere Tausend weit verteilte Verkaufsstellen. Bei derart komplexen Netzwerken ist eine einfache und zentralisierte Verwaltung von enormer Bedeutung. Wenn die Aktualisierung von Anti-Virus- und Content Filtering-Software, die Neukonfigurierung von Hardware sowie die Bereitstellung neuer Anwendungen manuell erfolgt, kann dies sehr zeitaufwändig und kostspielig werden. Außerdem können bei einer manuellen Verwaltung schnell Ungenauigkeiten und Fehler passieren. Daher sollten Einzelhandelsunternehmen Tools zur automatisierten Netzwerkverwaltung verwenden. Idealerweise sollten dabei Protokolle von allen Geräten an einen zentralen Punkt im Unternehmens-LAN weitergeleitet werden, so dass Vireninfektionen und Hacker-Angriffe an der Peripherie zentral erfasst werden können.

## Privates Surfen im Internet

Auch wenn privates Surfen am Arbeitsplatz nicht unbedingt ein Sicherheitsrisiko darstellt, kann es zu Produktivitätseinbußen und unter Umständen auch zu rechtlichen Problemen führen. Versäumen es Unternehmen, den Zugriff der Mitarbeiter auf unerwünschte Websites zu verhindern, kann dies rechtliche Folgen haben – etwa wenn Kollegen oder Kunden mit anstößigen Inhalten auf dem Rechner eines Mitarbeiters konfrontiert werden. Unternehmen können den Zugriff auf Websites mithilfe einer Content Filtering-Lösung selektiv steuern. So ist es beispielsweise möglich, den Zugriff auf Mitarbeiterportale oder Websites mit geschäftsrelevanten Informationen freizugeben und ansonsten alle Websites zu sperren.

Beim Thema Sicherheit steht für den Einzelhandel viel auf dem Spiel. Zwar liegen die Vorteile von Breitband und Drahtlos-Netzen auf der Hand, doch gleichzeitig bringen diese Technologien Risiken mit sich. Sicherheitslücken etwa können zu Produktivitätseinbußen, Umsatzverlusten und rechtlichen Problemen führen. Daher sollten Sicherheitslösungen nicht länger als eine nachträgliche Ergänzung betrachtet werden, sondern von Anfang an in das Netzwerk integriert und flächendeckend angewendet werden. Dabei sollte auf einfache Verwaltungs- und Aktualisierungstools geachtet werden.

## SonicWALL-Lösungen zum Schutz von POS-Anwendungen

SonicWALL bietet integrierte, flexible und leicht verwaltbare Sicherheitsplattformen für POS-Netzwerke. Mit den Security-Lösungen von SonicWALL kann der Einzelhandel Produktivitätsvorteile durch Echtzeit-POS-Anwendungen für IP- und Wireless-Netzwerke nutzen. Gleichzeitig werden vertrauliche Daten geschützt und eine unterbrechungsfreie Konnektivität gewährleistet.

### SonicWALL TZ 170-Serie

#### *Leistungsstarker und praxiserprobter Schutz für kleine Netzwerke*

Die TZ 170 bildet das Herzstück der SonicWALL TZ 170-Serie und bietet soliden und bewährten Netzwerkschutz für kleine Netzwerke, etwa zur Anbindung von POS-Systemen im Einzelhandel und in der Gastronomie. Das skalierbare und kostengünstige Gerät bietet eine große Auswahl an integrierten Sicherheits- und Verfügbarkeits-Funktionen und wächst mit den Bedürfnissen Ihres Netzwerks mit.

Funktionen und Vorteile der SonicWALL TZ 170:

- Leistungsstarke Deep Packet Inspection Firewall zum Schutz vor aktuellen Bedrohungen
- IPSec VPN (Virtual Private Networking) für einen sicheren Datenaustausch über das Internet
- Unterstützung einer zweiten Backup-Breitbandverbindung, die WAN-Redundanz und Lastverteilung gewährleistet
- Hilfreiche Konfigurationsassistenten, mit denen sich selbst die kompliziertesten Aufgaben problemlos bewältigen lassen
- Support für erweiterte Security Services, um umfassende Sicherheit auf allen Netzwerkebenen sicherzustellen
- Support für das ausgezeichnete Global Management System (GMS) mit umfassenden Überwachungs-, Verwaltungs- und Reportingtools

Drei weitere Modelle der SonicWALL TZ 170-Serie bieten zusätzliche Hardware-Konfigurationsmöglichkeiten.

### SonicWALL TZ 170 SP

#### *Integrierte Failover-Funktion auf eine Backup-Breitbandverbindung oder ein integriertes Analogmodem für geschäftskritische POS-Anwendungen*

Die SonicWALL TZ 170 SP ist eine umfassende Sicherheitslösung mit High-Performance VPN-Konnektivität und einer ICASA-zertifizierten Deep Packet Inspection Firewall. Dank Failover-Funktionen auf eine Backup-Breitbandverbindung sowie auf ein integriertes v.92-Analogmodem kann die TZ 170 SP Ausfälle der Breitbandverbindung problemlos überbrücken.

Die TZ 170 SP prüft kontinuierlich den Verbindungsstatus sowie eine Heartbeat-Verbindung zu einem Remote-Gerät, um die Netzwerkverfügbarkeit zu überwachen. Sobald eine der beiden Verbindungen als inaktiv gemeldet wird, führt das Gerät ein automatisches Failover auf die Backup-Breitbandverbindung oder das integrierte Analogmodem durch. Ist die primäre Breitbandverbindung wieder in Betrieb, erkennt die TZ 170 SP die wiederhergestellte Verbindung und wechselt zur ursprünglichen Verbindung zurück. So haben Einzelhandelsunternehmen ständigen Zugriff auf geschäftskritische Daten bei bestmöglicher Performance. Geschäftsunterbrechungen durch Verbindungsausfälle werden vermieden, während gleichzeitig sichergestellt ist, dass die Mitarbeiter produktiv und unterbrechungsfrei arbeiten können.

Die Appliance ist mit einer konfigurierbaren Toll-Saver-Software ausgestattet, mit der sich die Kosten für analoge Backup-Verbindungen reduzieren lassen. Die Verbindung wird beispielsweise automatisch beendet, wenn innerhalb eines bestimmten Zeitraums keine Aktivitäten gemeldet werden. Stehen wieder Daten zur Übertragung an, wird sie wiederhergestellt. Verkaufsstellen im Einzelhandel, die über keine Breitbandverbindung verfügen, etwa, weil diese für sie keine Vorteile bietet, können das Analogmodem auch als primäre Verbindung verwenden.

## SonicWALL TZ 170 Wireless

### *Sichere Wireless-Plattform nach 802.11b/g für drahtlosen Datenaustausch im Einzelhandel*

Die SonicWALL TZ 170 Wireless bietet sichere Konnektivität über drahtlose und kabelgebundene Verbindungen für POS-Kassen und -Selbstbedienungsterminals sowie für Wireless-Laptops und Handheld-Geräte. Teure und unflexible Verkabelungslösungen werden damit überflüssig.

Die TZ 170 Wireless sorgt für größtmögliche Sicherheit in drahtlosen Netzwerken und enthält einen Wireless Access Point nach 802.11b/g mit integrierter Deep Packet Inspection Firewall und VPN Appliance. Da für alle drahtlosen LAN- bzw. WLAN-Netzwerke IPSec VPNs verwendet werden, können sichere Tunnel eingerichtet werden, die sensible Kunden- und Geschäftsinformationen verschlüsseln.

SonicWALL Wireless Guest Services eignen sich besonders für Einzelhandelsunternehmen, die Gastbenutzern einen drahtlosen Netzwerkzugang bieten und gleichzeitig ihr internes Netzwerk schützen möchten. Mit dieser Funktion lassen sich separate Zugangszonen für Wireless-Gastbenutzer einrichten, die vom geschäftskritischen POS-Netzwerk abgetrennt sind. Mit der TZ 170 Wireless und der TZ 170 SP Wireless kann zu diesem Zweck ein separater Gastservice eingerichtet werden, bei dem Gastbenutzer – unabhängig von der Konfiguration – nur über einen WAN-Port mit Internetanbindung kommunizieren, aber keine Verbindung zum LAN-Port herstellen können (siehe Abb. 3).

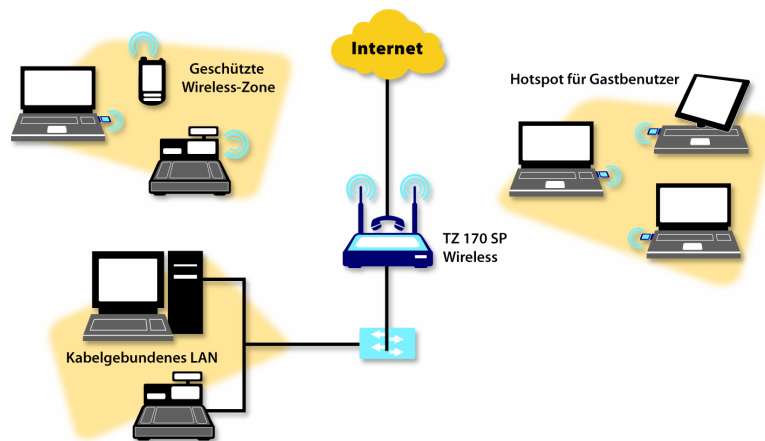


Abb. 3  
Wireless Guest Services

## SonicWALL TZ 170 SP Wireless

### *Leistungsfähige Plattform mit sicherer Wireless-Konnektivität und integrierter automatisierter Failover-Funktion*

Als leistungsfähige Sicherheitsplattform für drahtlose und kabelgebundene POS-Netzwerke im Einzelhandel kombiniert die SonicWALL TZ 170 SP Wireless zuverlässige Wireless-Konnektivität mit den verschiedenen Failover-Optionen der TZ 170 SP.

## SonicWALL PRO-Serie

### *Leistungsstarke skalierbare Lösungen für Unternehmenszentralen und größere Verkaufsstellen im Einzelhandel*

Die Appliances der SonicWALL PRO-Serie kommen normalerweise in der Zentrale eines Einzelhandelsunternehmens zum Einsatz und dienen als zentraler Hub für den Datenaustausch in weit verteilten Netzwerken. Die Appliances sind skalierbar und können bis zu 4.000 Verkaufsstellen unterstützen. Außerdem bieten die flexiblen High-Performance-Produkte der PRO-Serie eine hohe Netzverfügbarkeit und garantieren so den konstanten Zugriff auf geschäftskritische Ressourcen.

Die PRO-Serie bietet mehrere konfigurierbare Schnittstellen zur Segmentierung des Netzwerks sowie zwei WAN-Optionen und spezielle Failover-Ports. Mit der neuesten SonicOS-Firmware ausgestattet, verfügt die PRO-Serie zudem über flexible Konfigurationsoptionen, um selbst komplexeste Anforderungen in IP-Netzwerken zu erfüllen.

### Erweiterte Security Services

Dank erweiterter Funktionen bieten die Sicherheitsplattformen von SonicWALL umfassenden Schutz auf mehreren Ebenen. Die Security Services lassen sich je nach Erfordernis durch weitere Funktionen ergänzen und sind fest in den SonicWALL-Sicherheitsplattformen integriert. Sämtliche Komponenten der Sicherheitslösung werden dabei über eine gemeinsame Benutzeroberfläche verwaltet, so dass die TOC niedrig bleiben.

#### SonicWALL Complete Anti-Virus

##### *Umgehender Virenschutz für Windows-basierte POS-Systeme*

Viele Einzelhandelsunternehmen stellen ihre POS-Systeme auf Standard-Betriebssysteme wie Microsoft Windows um und sind damit anfälliger für Virenangriffe. SonicWALL Complete Anti-Virus wurde gemeinsam mit McAfee® entwickelt und bietet unmittelbaren Schutz vor Viren, die sich schnell ausbreiten und Windows-basierte POS-Systeme zum Erliegen bringen können. Eine speziell entwickelte und zum Patent angemeldete Anti-Virus-Architektur sorgt für die automatisierte Anwendung von Antiviren-Regeln. Die POS-Systeme werden dabei automatisch mit der neuesten Antiviren-Software sowie den neuesten Signaturdateien aktualisiert, bevor der Datenverkehr über eine SonicWALL-Appliance weitergeleitet wird. Complete Anti-Virus enthält außerdem eine Rapid E-Mail Attachment Blocking-Funktion, die gezielt infizierte E-Mail-Dateianhänge in den entscheidenden ersten Stunden vor der Veröffentlichung neuer Virensignaturen sperrt.

#### Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service (GAV)

##### *Schutz vor komplexen Angriffen über die Anwendungsebene*

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service (GAV) vereint eine konfigurierbare ultra-leistungsstarke Deep Packet Inspection Engine mit einer dynamisch aktualisierten Datenbank, die über 1.800 Signaturen zu Sicherheitsschwachstellen enthält. Auf diese Weise bietet der Service umfassenden Schutz vor komplexen Bedrohungen auf der Anwendungsebene, wie beispielsweise Software-Schwachstellen durch Pufferüberläufe, Würmer, Trojaner, Backdoor-Angriffen sowie Peer-to-Peer- und Instant Messaging-Anwendungen. Mit seiner leistungsstarken Performance, seinen innovativen Features und seinen umfassenden Management-Funktionen bietet der SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service (GAV) soliden Netzwerkschutz bei geringen Total Cost of Ownership.

## SonicWALL Content Filtering Service (CFS)

*Kontrolliert den Zugriff auf Webinhalte, um die Produktivität zu steigern und rechtliche Probleme zu vermeiden*

Mit dem SonicWALL Content Filtering Service (CFS) können Einzelhandelsunternehmen ihren Mitarbeitern und Kunden Zugriff auf geschäftsrelevante Websites bieten und gleichzeitig Websites sperren, die anstößige Inhalte enthalten oder die Produktivität beeinträchtigen. SonicWALL CFS enthält eine leistungsstarke Rating- und Caching-Architektur sowie eine Datenbank mit über vier Millionen ständig aktualisierten Einträgen zu Websites, Domänen und IP-Adressen. Außerdem können Einzelhandelsunternehmen die Content Filtering-Lösung an ihre speziellen Anforderungen anpassen und bestimmte Websites freigeben oder sperren. Unternehmen, die ihren Kunden Internetzugang in öffentlichen Bereichen zur Verfügung stellen, bietet der Content Filtering Service von SonicWALL zusätzlichen Schutz vor rechtlichen Problemen.

## SonicWALL Global Management System (GMS)

*Skalierbare und zentralisierte Verwaltungs- und Reportinglösung*

Mit dem SonicWALL Global Management System (GMS) können Einzelhandelsunternehmen alle SonicWALL Internet Security Appliances zentral überwachen und verwalten – egal ob es sich um einige wenige oder mehrere Tausend Appliances handelt (siehe Abb. 4).

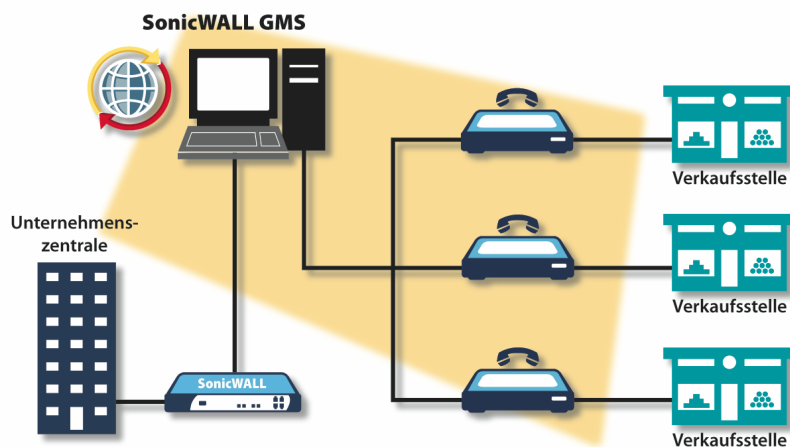


Abb. 4  
Global Management  
System

SonicWALL GMS ermöglicht es, VPN-Tunnel, Sicherheitsregeln und andere Konfigurationsoptionen schnell und unkompliziert in den einzelnen Verkaufsstellen bereitzustellen. Administratoren können neue Sicherheitsregeln und Firmware-Upgrades für alle oder nur für bestimmte Verkaufsstellen verteilen, indem sie zusätzliche Sicherheitsfunktionen zu Remote-Appliances hinzufügen. SonicWALL GMS erlaubt außerdem eine umfassende Verwaltung der erweiterten SonicWALL Security Services wie etwa SonicWALL Complete Anti-Virus und SonicWALL Intrusion Prevention Service. Um eine optimale Netzwerk-Performance zu gewährleisten, kann der Administrator bei der Verteilung von Sicherheitsregeln und Firmware-Updates auf Zeiten mit niedrigerem Netzwerkverkehr ausweichen.

Unternehmen können außerdem mit GMS von SonicWALL unterschiedliche Verwaltungsberechtigungen vergeben und so Verwaltungsaufgaben auf mehrere Netzwerkadministratoren aufteilen. Protokolle und Reports zu Nutzungstrends, Security-Events und anderen Funktionen erleichtern zusätzlich die Überwachung des Netzwerks.

## Resümee

Durch den Einsatz IP-basierter Produktivitätsanwendungen können Einzelhandelsunternehmen die Servicequalität und die Produktivität ihrer POS-Systeme verbessern und sich gleichzeitig vom Wettbewerb differenzieren. Um diese Anwendungen nutzen zu können, müssen Verkaufsstellen und Restaurants mit einem Breitband- oder Wireless-Internetzugang ausgestattet sein. Zudem muss das gesamte Netzwerk umfassend abgesichert werden, um vertrauliche Informationen vor Viren, Würmern und anderen Bedrohungen zu schützen.

SonicWALL bietet als einziger Hersteller eine durchgängige Lösung, die speziell auf die Anforderungen von POS-Umgebungen und Einzelhandelsunternehmen abgestimmt ist. Integrierte Failover-Funktionen, Erweiterte WLAN-Sicherheitsfunktionen mit 3DES/AES-Verschlüsselung und eine einfache webbasierte Verwaltungsschnittstelle für alle Remote-Appliances garantieren nicht nur stabile VPN-Verbindungen und den Schutz vertraulicher Informationen, sondern sorgen auch für eine zentralisierte Steuerung und eine hohe Skalierbarkeit. Je nach Bedarf und Unternehmensgröße bietet SonicWALL dabei unterschiedliche Firewalls für die VPN-Anbindung in der Unternehmenszentrale, die sich bei wachsenden Anforderungen problemlos skalieren lassen.

Alle SonicWALL Appliances unterstützen die SonicWALL-Services Anti-Virus (zur Neutralisierung von Viren und Würmern), Content Filtering (zur Steigerung der Mitarbeiterproduktivität und zum Schutz vor rechtlichen Problemen) sowie Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention (zum Schutz vor den immer komplexeren Bedrohungen auf der Anwendungsebene). Darüber hinaus bieten alle Lösungen ein hohes Maß an Kosteneffizienz und Benutzerfreundlichkeit – zwei Kriterien, die für Einzelhandelsunternehmen und Gastronomiebetreiber von großer Bedeutung sind.

Weitere Informationen über die Sicherheitslösungen von SonicWALL erhalten Sie telefonisch unter +49 (0)89 4545946, per E-Mail unter [germany@sonicwall.com](mailto:germany@sonicwall.com) oder bei Ihrem autorisierten SonicWALL-Händler.