



# SonicWALL Application Intelligence, Control and Visualization

FIREWALL

**Granulare Überwachung, Kontrolle und Echtzeit-Visualisierung von Anwendungen**

IT-Administratoren stehen heute vor einer echten Herausforderung: Sie müssen die Verfügbarkeit und Effizienz unternehmenskritischer Lösungen gewährleisten und gleichzeitig die Nutzung unproduktiver und oftmals gefährlicher Anwendungen kontrollieren. Das geht nur, wenn die Bandbreite für unternehmenskritische Anwendungen priorisiert und Social Media-Anwendungen oder Spiele in ihrem Verbrauch eingeschränkt oder komplett gesperrt werden. Stateful Packet Inspection-Firewalls, wie sie noch in vielen Unternehmen eingesetzt werden, bieten hier keine Lösung: Da sie lediglich Ports und Protokolle prüfen, sind sie nicht in der Lage, Anwendungen zu identifizieren, geschweige denn, zwischen unbedenklichem und verdächtigem Datenverkehr zu unterscheiden.

SonicWALL® bietet eine umfassende Überwachung und Kontrolle von Anwendungen – und zwar unabhängig vom Port oder Protokoll. Hierfür wird der Netzwerkverkehr auf jedes einzelne Paket und jedes einzelne Byte gescannt und ermittelt, welche Anwendungen von welchem Benutzer verwendet werden. Die Firewalls der nächsten Generation von SonicWALL nutzen eine ständig erweiterte Signaturrendatenbank, die derzeit Tausende von Anwendungen und Millionen von Malware-Bedrohungen erkennt, und sorgen so für einen automatischen, nahtlosen Netzwerkschutz. Die Lösung identifiziert und neutralisiert Malware, Eindringversuche, Datenlecks und Regelverletzungen, bevor dem Unternehmensnetzwerk oder den Benutzern ein Schaden entstehen kann.

SonicWALL Application Intelligence and Control bietet IT-Administratoren eine Reihe neuer, benutzerfreundlicher Verwaltungsfunktionen, die eine gezielte Kontrolle von Anwendungen und Benutzern erlauben. Administratoren können auf einfache Weise Regeln zur Bandbreitenverwaltung erstellen, die für vordefinierte Kategorien (wie Social Media oder Spiele), bestimmte Anwendungen oder einzelne Benutzer bzw. Gruppen gelten. Sobald neue Anwendungen dazukommen, werden die entsprechenden Signaturen auf die Firewalls übertragen. Dort werden die jeweiligen Regeln und Anwendungsobjekte automatisch aktualisiert, ohne dass sich die IT-Abteilung um diese zeitaufwändigen und umständlichen Aufgaben kümmern muss. SonicWALLs Lösungen zur Analyse des Anwendungsverkehrs helfen Administratoren dabei, Netzwerkausfälle und Sicherheitsbedrohungen schneller und effizienter in den Griff zu bekommen und einen unmittelbaren ROI sicherzustellen. Darüber hinaus liefert die Analyse des Anwendungsverkehrs einen umfassenden Einblick in Netzwerk-Ereignisse und -Aktivitäten und sorgt für ein erhöhtes Sicherheitsbewusstsein sowie eine sinnvollere Netzwerknutzung durch die Mitarbeiter.

Die Funktion Application Intelligence and Control ist zusammen mit SonicWALL Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention als 1-, 2- oder 3-Jahres-Abo erhältlich. Außerdem ist sie Bestandteil der SonicWALL Comprehensive Gateway Security Suite-Abos für die Firewalls der TZ 210-, Network Security Appliance (NSA)- und E-Class NSA-Serie.

## Funktionen und Vorteile

**Application Intelligence.** Mithilfe von SonicWALLs Reassembly-Free Deep Packet Inspection™-Technologie wird jedes einzelne Paket überprüft, um zu ermitteln, welche Anwendungen von welchen Benutzern verwendet werden. Eine Signaturrendatenbank gewährleistet dabei einen automatischen und nahtlosen Netzwerkschutz.

**Anwendungskontrolle.** Anhand von flexiblen, konfigurierbaren Regeln lassen sich Anwendungen, Dateien, URLs und E-Mail-Anhänge je nach Typ, Benutzer, Zeitplan, kundenspezifischen Signaturen und anderen Kriterien in der Bandbreitennutzung beschränken oder komplett sperren.

**Anwendungsvisualisierung.** Bietet Echtzeit-Grafiken zu Anwendungen, Bandbreitenverbrauch in ein- und ausgehender Richtung, Benutzern, aktuell aufgerufenen Websites und anderen Parametern. Zusätzlich können die Daten an einen NetFlow/IPFIX-Analyser übertragen werden, um den historischen Netzwerkverkehr offline zu analysieren und Probleme zu identifizieren.

**Analyse des Anwendungsverkehrs.** Liefert einen detaillierten Einblick in aktuelle und historische von der Firewall übermittelte Daten einschließlich Anwendungsaktivitäten nach Benutzer.

**Schutz vor Datenlecks.** Blockiert und kontrolliert die unerlaubte Übermittlung sensibler Daten per FTP-Upload oder als E-Mail-Anhang über private Webmail-Dienste wie Hotmail® oder Gmail® bzw. als SMTP- und POP3-E-Mail über den Firmenaccount.

**Bandbreitenverwaltung auf der Anwendungsebene.** Gewährleistet die erforderliche Servicequalität (QoS) durch Zuordnung fester Durchsatzraten für geschäftskritische Anwendungen oder Benutzergruppen zu bestimmten Tageszeiten.

**Automatisierte Signaturreupdates.** Vereinfachen die Verwaltung und stellen sicher, dass das Netzwerk vor den neuesten Bedrohungen geschützt ist.

**Deep Packet Inspection für SSL-Verkehr.** Dehnt den Schutz auf SSL-verschlüsselten Verkehr aus, ermöglicht eine optimale Einhaltung von Compliance-Vorgaben und bietet Content Filtering sowie Schutz vor Datenlecks. Darüber hinaus können andere Vektoren für Malware eliminiert werden. Verschlüsselter Verkehr wird entschlüsselt, geprüft und transparent für den Benutzer wieder verschlüsselt. Dabei ist eine Konfiguration für ein- und ausgehende Verbindungen möglich.

- **Application Intelligence**
- **Anwendungskontrolle**
- **Anwendungsvisualisierung**
- **Analyse des Anwendungsverkehrs**
- **Schutz vor Datenlecks**
- **Bandbreitenverwaltung auf der Anwendungsebene**
- **Automatisierte Signaturreupdates**
- **Deep Packet Inspection für SSL-Verkehr**

## Next-Generation Firewalls mit Application Intelligence, Control and Visualization

### Identifizierung

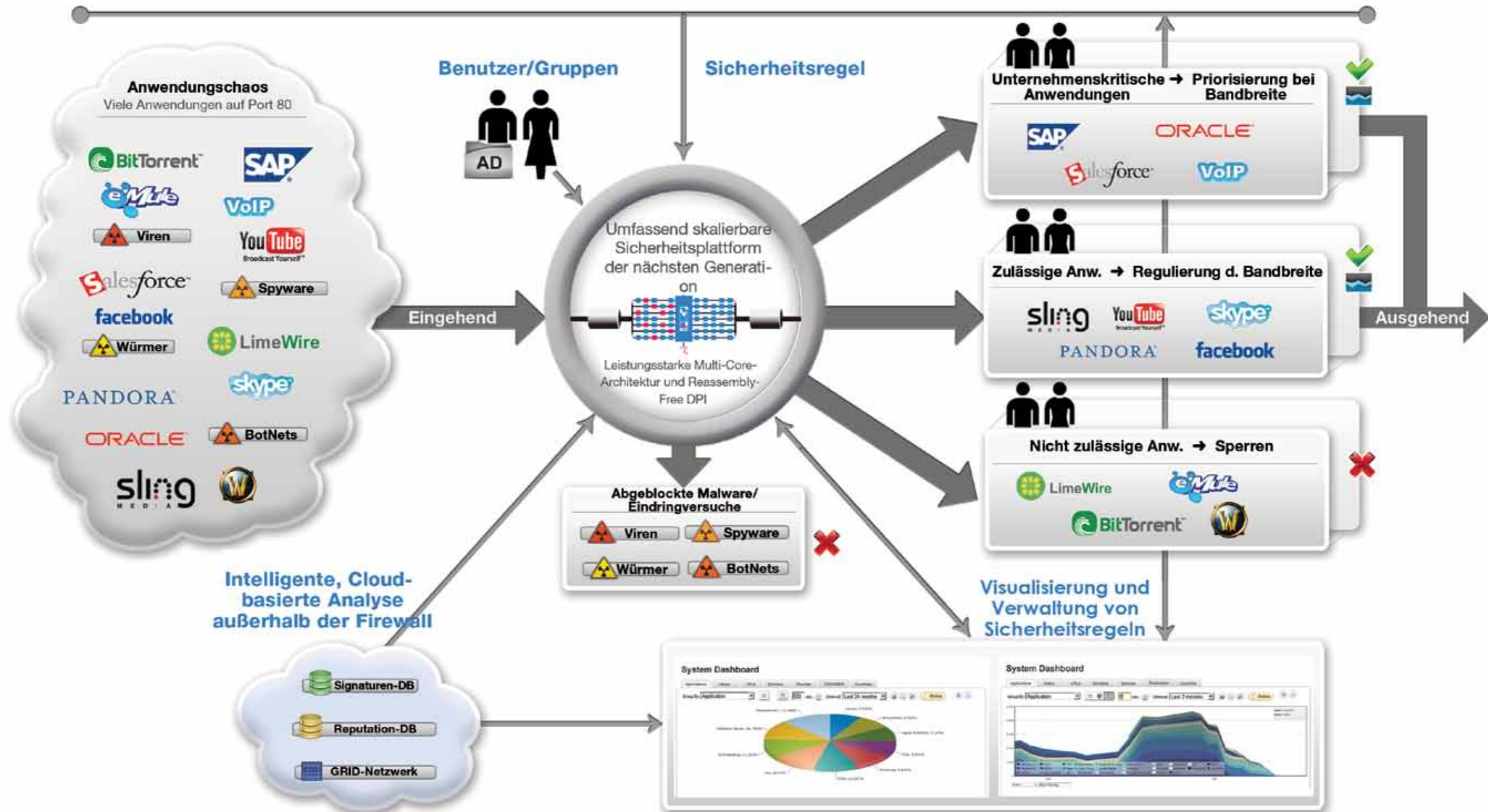
- Nach Anwendung
  - Nicht nach Port und Protokoll
- Nach Benutzer/Gruppe
  - Nicht nach IP
- Nach Content-Kontrolle
  - Nicht nach Dateiname

### Kategorisierung

- Nach Anwendung
- Nach Anwendungskategorie
- Nach Ziel
- Nach Content
- Nach Benutzer/Gruppe

### Kontrolle

- Priorisierung von Anwendungen nach Regel
- Verwaltung von Anwendungen nach Regel
- Blockieren von Anwendungen nach Regel
- Erkennen und Blockieren von Malware
- Erkennen und Verhindern von Eindringversuchen



# Technische Daten



## Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service

NSA E7500 (1 Jahr)  
01-SSC-6130

NSA E6500 (1 Jahr)  
01-SSC-6131

NSA E5500 (1 Jahr)  
01-SSC-6132

NSA 5000 (1 Jahr)  
01-SSC-6159

NSA 4500 (1 Jahr)  
01-SSC-6133

NSA 3500 (1 Jahr)  
01-SSC-6134

NSA 2400 (1 Jahr)  
01-SSC-6135

NSA 250M-Serie (1 Jahr)  
01-SSC-4570

NSA 220-Serie (1 Jahr)  
01-SSC-4612

TZ 210-Serie (1 Jahr)  
01-SSC-6165

Abos auch für mehrere Jahre erhältlich

Die Artikelnummern zu allen Network Security Appliances von SonicWALL finden Sie unter [www.sonicwall.com/de](http://www.sonicwall.com/de).



### SonicWALL Deutschland

Tel: +49 89 4545 946 [www.sonicwall.de](http://www.sonicwall.de)

### SonicWALL Schweiz

Tel: +41 44 810 31 35 [www.sonicwall.ch](http://www.sonicwall.ch)

### SonicWALL Österreich

Tel: +41 44 810 31 35 [www.sonicwall.at](http://www.sonicwall.at)

## Anwendungsvisualisierung

Anhand von Echtzeit-Grafiken zu Anwendungen, Bandbreitenbelegung in ein- und ausgehender Richtung, besuchten Websites und sämtlichen Benutzeraktivitäten kann der Administrator die Vorgaben für Anwendungen anpassen, um die Einhaltung von Sicherheitsregeln sicherzustellen.



## Wichtige Features

### Application Intelligence-Funktionen

- Umfassende Kontrolle durch Prüfung und Kategorisierung des gesamten Verkehrs unabhängig von Ports oder Protokollen
- Funktion zum Schutz vor Datenlecks durch Überwachung von benutzerdefinierten Inhalten
- Bandbreitenverwaltung auf Anwendungsebene mithilfe einer umfangreichen, ständig erweiterten Signaturrendatenbank und wirksamer Regeln
- Vordefinierte und personalisierte Aktionen: Protokollieren, Protokollieren und Blockieren, individuelle Benutzernachrichten, DPI umgehen und Bandbreitenverwaltung
- Deep Packet Inspection von Datenverkehr, der SSL-verschlüsselte Protokolle nutzt

### Signaturen-Datenbank

- Dynamisch aktualisierte Datenbank mit tausenden von Anwendungs- und Content-basierten Signaturen

### Logging und Analyse des Anwendungsverkehrs

- Erweitertes Next-Generation Syslog-Reporting
- Analyse des Anwendungsverkehrs mit SonicWALL Analyzer, Scrutinizer und Global Management System
- Logging mittels Netflow/IPFIX mit Erweiterungen erlaubt zusätzliche „Off-the-Box“-Analyse und Visualisierung des Netzwerkverkehrs.

### Skalierbarkeit

- Prüfung einer großen Zahl gleichzeitiger Downloads mit unbegrenzter Dateigröße

Ausführlichere Informationen zu den Security-Mehrwertdiensten von SonicWALL, wie Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Application Intelligence and Control, Comprehensive Anti-Spam Service, Enforced Client Anti-Virus and Anti-Spyware und Content Filtering Service, finden Sie unter <http://www.sonicwall.com/de>.

### SonicWALL-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT

**SONICWALL**

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™