



# SonicWALL Analyzer

MANAGEMENT UND REPORTING

Analyse-, Visualisierungs- und Reporting-Tool  
zur Überwachung des Anwendungsverkehrs

- **Umfassende grafische Reports**
- **Next-Generation Syslog Reporting**
- **Ereignisberichte zu SonicWALL SRA und CDP**
- **Übergreifende zeitgesteuerte Berichte**
- **360°-Reporting**
- **Compliance Reporting**
- **Sammelreports zu verschiedenen Bedrohungsarten**
- **Benutzerbasiertes Reporting**
- **Ortsunabhängiger Zugriff**
- **Zusätzliche Analysefunktionen**

Die private Nutzung von Webanwendungen wie Webmail, Facebook®, Instant Messaging oder BitTorrent am Arbeitsplatz beeinträchtigt nicht nur die Produktivität der Mitarbeiter, sondern auch die Übertragungsgeschwindigkeit und die Sicherheit im Firmennetzwerk. IT-Abteilungen benötigen hier eine Lösung, die das Sicherheitsbewusstsein schärft, die optimale Nutzung des Netzwerks sicherstellt und eine intelligente Verwaltung von Anwendungen ermöglicht. Darüber hinaus sollte die Lösung auch Forensik-Analysefunktionen bieten und eine kostengünstige Fehlerbehebung erlauben. Die meisten Analyse- und Reporting-Tools haben jedoch keine übersichtlichen Visualisierungsfunktionen und sind umständlich in der Handhabung.

Mit SonicWALL® Analyzer verfügen Administratoren über ein anwenderfreundliches, webbasiertes Analyse- und Reporting-Tool, das aktuelle sowie historische Einblicke zum Zustand, zur Leistung und zur Sicherheit des Netzwerkes bietet. Analyser unterstützt Firewalls, Backup- und Recovery-Produkte und Secure Remote Access-Lösungen von SonicWALL. Unternehmen jeder Größe profitieren beim Einsatz des Analyser-Tools von der gesteigerten Produktivität sowie der verbesserten Bandbreitennutzung und einem erhöhten Sicherheitsbewusstsein. SonicWALL verbindet in seinem Produkt Funktionen zur externen Analyse des Anwendungsverkehrs mit den detaillierten Daten, die von den eigenen Firewalls generiert werden, und bietet damit als einziger Firewall-Hersteller eine Komplettlösung in diesem Bereich.

## Funktionen und Vorteile

**Umfassende grafische Reports.** Berichte zu Firewall-Angriffen, zur Bandbreitennutzung und zum Anwendungsverkehr machen die Mitarbeiterproduktivität transparent und identifizieren potenziell schädliche Netzwerkaktivitäten.

**Next-Generation Syslog Reporting.** Entscheidende Verbesserungen der Architektur ermöglichen eine schnellere Datenzusammenfassung, sodass Berichte zu ankommenden Syslog-Meldungen annähernd in Echtzeit erstellt werden können. Durch den direkten Zugriff auf die zugrunde liegenden Rohdaten werden zusätzlich umfassende granulare Kontrollmöglichkeiten und ein individuell anpassbares Reporting unterstützt.

**Ereignisberichte zu SonicWALL Secure Remote Access (SRA) und Continuous Data Protection (CDP).** Bieten anhand von Next-Generation Syslog-Daten aussagekräftige Informationen zum Zustand und zum Verhalten der jeweiligen Appliance.

**Übergreifende zeitgesteuerte Berichte.** Von einem zentralen Zugangspunkt aus kann auf sämtliche zeitgesteuerte Berichte zugegriffen werden. Die einzelnen Berichte können dabei Diagramme und Tabellen für mehrere verschiedene Geräte enthalten. Die Berichte können zeitgesteuert erstellt werden und in unterschiedlichen Formaten an einen oder mehrere E-Mail-Adressaten versendet werden.

**360°-Reporting.** Bietet individuell anpassbare Ansichten mit mehreren Übersichtsreports auf einer Seite. Benutzer können damit wichtige Kennzahlen zum Netzwerk leicht auffinden und Daten aus mehreren Berichten rasch im Überblick analysieren.

**Compliance Reporting.** Gibt Administratoren die Möglichkeit, Berichte zu erstellen, die alle Compliance-Anforderungen erfüllen. Die Berichte können hierbei ad hoc oder auch zeitgesteuert für bestimmte gesetzliche Vorgaben erstellt werden.

**Sammelreports zu verschiedenen Bedrohungsarten.** Hierin werden Daten zu abgewehrten Angriffen erfasst. Bedrohungen, die von den SonicWALL-Firewalls und dem SonicWALL Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service erkannt wurden, können unmittelbar dargestellt werden.

**Benutzerbasiertes Reporting.** Bildet Aktivitäten einzelner Benutzer auf lokaler Ebene oder an externen Netzwerkstandorten ab und liefert damit noch genauere Einblicke zum netzwerkweiten Verkehr – und dabei speziell zur Anwendungsnutzung, zu besuchten Websites, Backup-Aktivitäten und VPN-Verbindungen pro Benutzer.

**Ortsunabhängiger Zugriff.** Vereinfacht das Reporting und bietet Administratoren über einen Standard-Webbrowser Analysedaten zu jedem beliebigen Standort.

**Zusätzliche Analysefunktionen.** Bieten detaillierte Reports zu bestimmten Arten von Angriffen oder Eindringversuchen sowie Angaben zur Ursprungsadresse. Administratoren können so schneller auf externe Bedrohungen reagieren.

**SONICWALL**®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

# Technische Daten



- Analyzer für die TZ-Serie  
01-SSC-3378
- Analyzer für NSA 240, NSA 2400  
01-SSC-3379
- Analyzer für NSA 3500  
01-SSC-3380
- Analyzer für NSA 4500  
01-SSC-3381
- Analyzer für die E-Class NSA- und  
SuperMassive™ E10000-Serie  
01-SSC-3382
- Analyzer für CDP 210  
01-SSC-3383
- Analyzer für CDP 220  
01-SSC-3384
- Analyzer für CDP 5040B  
01-SSC-3385
- Analyzer für CDP 6080B  
01-SSC-3386
- Analyzer für SRA 1200  
01-SSC-3387
- Analyzer für SRA 4200  
01-SSC-3388
- Analyzer für die E-Class SRA-Serie  
01-SSC-3389

## SonicWALL Analyzer



Netzwerkverkehrsstatistiken, etwa zu den am häufigsten besuchten Websites, lassen sich einfach und bequem abrufen. Mithilfe von Drill-Down Reporting-Funktionen können Daten nach Details wie Standortname, IP-Adresse, Website-Kategorie oder Anzahl der Verbindungsversuche sortiert werden.



Dank der integrierten granularen Reporting-Funktionen lassen sich Verkehrsdaten für die am häufigsten verwendeten Anwendungen im Netzwerk anzeigen. Die wichtigsten erkannten bzw. gesperrten Anwendungen können dabei einfach nach Kategorie, Zeitraum oder Aufrufer identifiziert werden.

### Systemvoraussetzungen

<b>Betriebssystem</b>	Windows Server 2003 64 Bit (SP2) Windows Server 2008 SBS 64 Bit (R2) Windows Server 2008 Standard 64 Bit (R2) Windows Vista Pro 64 Bit (SP1) Windows 7 Pro 64 Bit (SP1) SonicWALL Analyzer wird dabei jeweils als 32-Bit-Anwendung ausgeführt.
<b>Hardware für Analyzer Server</b>	Mindestanforderungen: Single Core 3-GHz-x86-Prozessor, 4 GB RAM, 100 GB HDD
<b>Java</b>	Java SE Runtime Environment 1.6 oder höher
<b>Internet-Browser</b>	Microsoft® Internet Explorer 8.0 oder höher Mozilla Firefox 6.0 oder höher Google Chrome ab Version 13.0 Wird nur unter Microsoft Windows-Plattformen unterstützt

### Virtual Appliance

Hypervisor:	VMware ESX und ESXi
Installiertes Betriebssystem:	Gehärtetes SonicLinux
Appliance-Kapazität:	250 GB, 950 GB
Zugewiesener RAM:	4 GB
VMware-Kompatibilitätsrichtlinien für Hardware:	Siehe <a href="http://www.vmware.com/resources/compatibility/search.php">www.vmware.com/resources/compatibility/search.php</a>



Die Überwachung verwalteter SonicWALL Appliances wird dank der intuitiven grafischen Berichte zum Kinderspiel. Auffälligkeiten im Netzwerkverkehr lassen sich anhand der Nutzungsdaten für bestimmte Zeiträume, Aufrufer, Antwortstellen oder Services identifizieren. Die Berichte können anschließend in MS Excel oder PDF exportiert bzw. direkt am Drucker ausgegeben werden.



Threat Management-Funktionen sind beim Analyzer standardmäßig vorhanden; die wichtigsten Netzwerkbedrohungen lassen sich nach Ziel, Aufrufer oder Bedrohungsart anzeigen. Ebenfalls enthalten sind umfassende Berichtsfunktionen, wie z. B. beim Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service.

### Unterstützte SonicWALL Appliances

SonicWALL Network Security Appliances (NSA): E-Class NSA-, NSA-, TZ- und PRO-Serie<sup>1</sup>  
SonicWALL Continuous Data Protection  
SonicWALL Content Security Manager (CSM)  
SonicWALL E-Class und SMB Secure Remote Access (SRA)<sup>2</sup>

### Unterstützte SonicWALL-Firmware

SonicWALL E-Class NSA- und NSA-Serie: SonicOS Enhanced 5.0 oder höher  
SonicWALL PRO-Serie: SonicOS Enhanced 3.2 oder höher  
SonicWALL TZ-Serie: SonicOS Standard 3.1 bzw. Enhanced 3.2 oder höher  
SonicWALL CSM-Serie: SonicWALL 2.0 oder höher  
SonicWALL SRA für KMUs: Firmware 2.0 oder höher  
SonicWALL E-Class SRA-Serie: Firmware 9.0 oder höher

<sup>1</sup> Bestehende SonicWALL XPRS/XPRES2-, SonicWALL SOHO2-, SonicWALL Tele2- und SonicWALL Pro/Pro-VX-Modelle werden nicht unterstützt.

<sup>2</sup> Nur neuere Aventail E-Class SRA Appliances mit 12-stelligen Seriennummern im Hexadezimalformat



**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)

### SonicWALL-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™