SonicWALL® Scrutinizer

MANAGEMENT UND REPORTING

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

- **Granulare Analyse und Berichte**
- **Erweiterte Problembehebung**
- **Leistungsstarke Visualisierung**
- **Verbesserte Forensik-Funktionen**
- **Analyse des Anwendungsverkehrs**
- **Unterstützung von Fremdanbieter-Produkten**
- **Personalisierbare Warnmeldungen**
- **Flexible Verwaltung**

Unternehmen sehen sich heute mehr denn je gezwungen, die Produktivität zu steigern, ihre Investitionen zu optimieren und Kosten (wie z. B. die monatlichen Internet-Gebühren) zu senken. Gleichzeitig nimmt der Datenverkehr durch die private Nutzung von Web 2.0- und Social Media-Anwendungen drastisch zu und verursacht erhebliche Bandbreiten- und Produktivitätsverluste. Mit veralteten Überwachungs- und Reporting-Tools lassen sich zwar Ports und Protokolle überwachen, nicht aber der Anwendungsverkehr, der Firewalls, Router und Switches passiert. Deshalb werden Bedrohungen von infizierten Hosts im Netzwerk nicht immer entdeckt. Auch Managed Service Provider (MSPs) und Value Added Reseller (VARs) müssen den Servicenutzen für den Kunden transparent machen und gleichzeitig den Kosten- und Zeitaufwand für die Verwaltung der einzelnen Konten unter Kontrolle behalten.

SonicWALL® Scrutinizer ist ein herstellerunabhängig einsetzbares Analyse-, Visualisierungs- und Reporting-Tool, mit dem Sie aktuelle und historische Netzwerkperformancedaten erfassen und Probleme beheben können. Das Tool hilft Unternehmen und Service Providern, ihre Produktivität zu steigern, und unterstützt eine große Auswahl an Routern, Switches und Firewalls sowie zahlreiche Datenfluss-Reporting-Protokolle.

Scrutinizer kann mit den Netzwerkprodukten zahlreicher Anbieter eingesetzt werden. In Kombination mit einer SonicWALL Next-Generation Firewall bietet das Tool zur Analyse des Anwendungsverkehrs ganz besondere Vorteile. Wie keine andere Lösung liefert Scrutinizer präzise Daten zur Anwendungsverkehrsanalyse und nutzt dabei die von den SonicWALL Firewalls exportierten IPFIX- oder NetFlow-Daten. Das Tool kann die häufigsten Anwendungen, Client-Anwendungskommunikation, Flows, Protokolle, Benutzer, Domänen, Länder und Subnetze identifizieren. NetFlow/IPFIX wird auch von einigen anderen Firewall-Anbietern unterstützt, doch nur SonicWALL bietet derart detaillierte Informationen zum Anwendungsverkehr.

Zum Funktionsumfang von Scrutinizer gehören eine Deep-Packet-Analyse, automatisierte Reporting-Funktionen mit proaktiver Jitter-/Latenz-Überwachung, Alarmmeldungen bei verdächtigen Aktivitäten und individuell anpassbare Dashboards. Darüber hinaus bietet das Tool historisches und erweitertes Reporting, eine rollenbasierte Verwaltung, erweiterte Analyse- und schwellenwertbasierte Alarmfunktionen[1] sowie zahlreiche spezielle Features für MSPs und ISPs[2].

Funktionen und Vorteile

Granulare Analyse und Berichte. Erlauben eine unkomplizierte visuelle Darstellung der häufigsten Hosts, Protokolle, Ports, Anwendungen, Verkehrsdaten und Client-Anwendungskommunikation für alle Netzwerkbereiche und alle Geräte. Dank flexibler Analyseoptionen lassen sich Trends in Bits, Bytes, Paketen oder Prozentzahlen der verbrauchten Gesamtbandbreite darstellen. Scrutinizer unterstützt sowohl IPFIX als auch Flexible NetFlow für die Bereitstellung umfassend personalisierbarer Berichtsvorlagen und kann alle Flow-Aufzeichnungen beliebig lange speichern.

IPFIX liefert detailliertere Informationen und ermöglicht eine **erweiterte Fehlerbehebung** bei Kapazitätsengpässen, Latenz, Jigger, Active Timeouts, häufiger Client-Anwendungskommunikation, häufigen Host-Flows, Host-Aufkommen, Adresspaar-Aufkommen, MAC-Adressen, VLANs und Domänen.

Leistungsstarke Visualisierungstools. Auflistung der häufigsten Schnittstellen für alle Router, Switches und Firewalls zur Darstellung von Echtzeit- oder archivierten Anwendungsverkehrsdaten mit interaktiven Diagrammen, Tabellen und Google® Maps sowie mit einer innovativen Matrix-Ansicht zur Darstellung von Flow-Feldern und Netzwerk-Karten zur Visualisierung der relevanten Flow-Daten.

Verbesserte Forensik-Funktionen. Erkennung und Alarmierung bei unerlaubten Anwendungen, böswilligem Datenverkehr, bekannten infizierten Internet-Hosts, fehlerhaften Flow-Sequenznummern, DNS-Cache Poisoning, unberechtigten IP-Adressen, DHCP- und Mail-Servern, Port-Scanning, übermäßigem Multicast-Verkehr, HTTP-Hijacking und DDOS-Angriffen.

Analyse des Anwendungsverkehrs. Verbindet führende Next-Generation Firewalls mit der Scrutinizer-Software zu einer einzigartigen Lösung. Die Firewall überträgt IPFIX-Daten in Echtzeit an die Traffic Analyzer-Erfassungsanwendung, wo der Administrator die Nutzungsdaten nach Anwendung und Benutzer untersuchen, Daten nach bestimmten Zeitspannen einsehen und viele weitere Optionen nutzen kann. NetFlow/IPFIX wird auch von anderen Firewall-Anbietern unterstützt, doch nur SonicWALL bietet derart detaillierte Informationen zum Anwendungsverkehr.

Unterstützung von Fremdanbieter-Produkten. Sorgt für Kompatibilität mit Hunderten von Routern, Switches und Firewalls unabhängig vom Hersteller, so dass Tausende von Schnittstellen gleichzeitig überwacht werden können.

Personalisierbare Warnmeldungen. Können bei Schnittstellenzugriffen, unfertigen Flows, bedenklichen Aktivitäten sowie bei Voice- und Video-Qualitätsproblemen ausgelöst werden und zeigen an, wie viele andere Alarme der Host bereits ausgelöst hat.

Flexible Verwaltungsfunktionen. Erlauben die Erstellung individuell anpassbarer Dashboards nach Anmeldung, gruppen- und anmeldungsbasierter Berechtigung, um auf die Flows bei bestimmten Router-, Switch- und Firewall-Schnittstellen zuzugreifen. MSPs können Stylesheets ganz unkompliziert entsprechend dem Corporate Branding ändern.

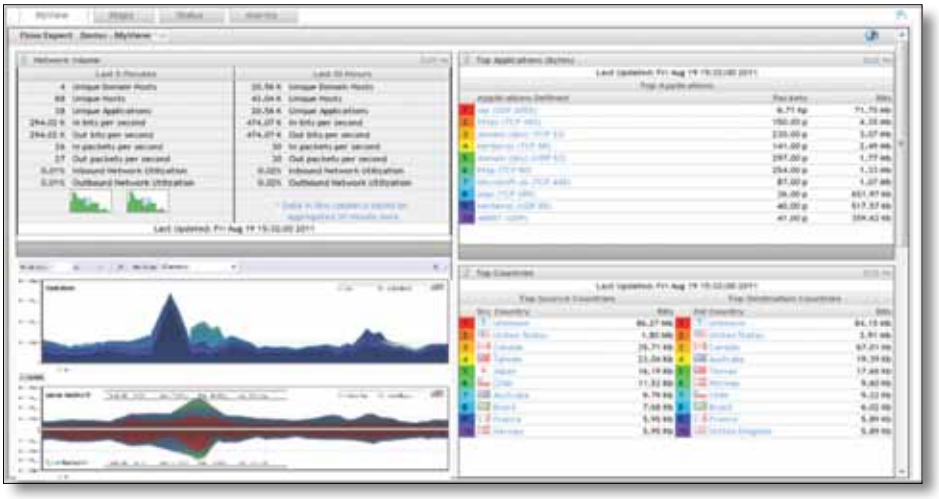
[1] Für dieses Feature ist das Flow Analytics-Modul erforderlich
[2] Im Service Provider-Modul verfügbar

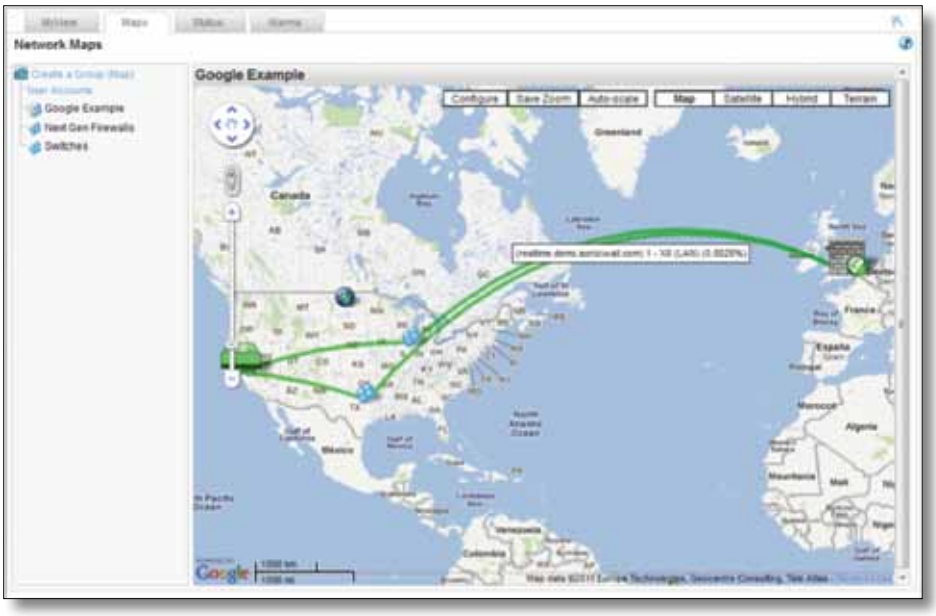
SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Personalisierbares Dashboard

Das individuell anpassbare Benutzer-Dashboard bietet einen schnellen und aussagekräftigen Einblick in die Netzwerkperformance. Dashboards können pro Benutzer erstellt werden, um ohne großen Aufwand die häufigsten Anwendungen, die Netzwerkauslastung oder individuelle Mashups anzuzeigen, die für bestimmte Benutzer relevant sind.



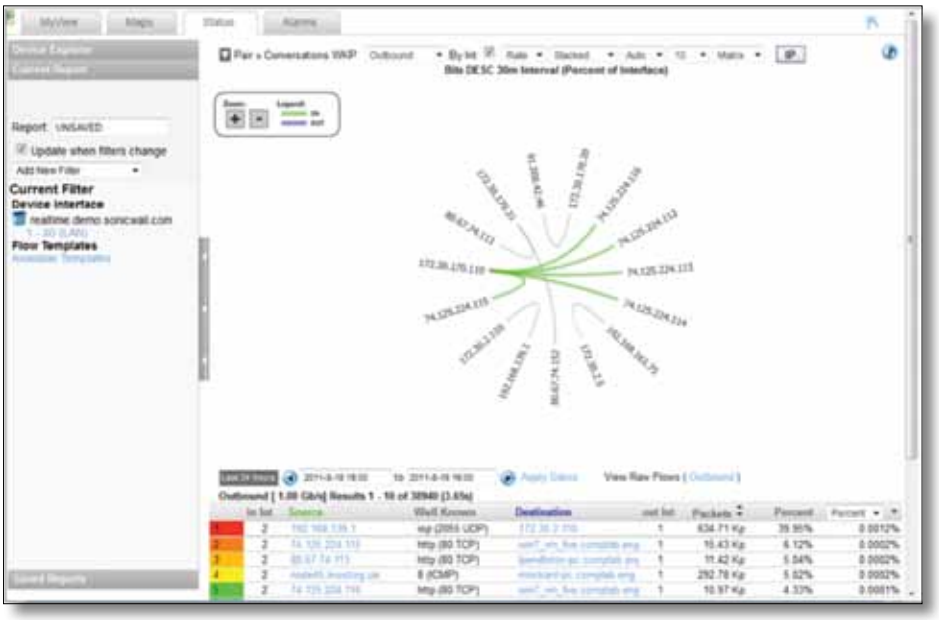


Google Maps

Die Integration von Google Maps erlaubt eine umfassende Sicht auf das gesamte Netzwerk – auch über geografische Grenzen hinweg! Die Verbindungen sind farbig gekennzeichnet und werden auf der Grundlage ihres aktuellen Status angezeigt, so dass die Behebung von Fehlern zum Kinderspiel wird.

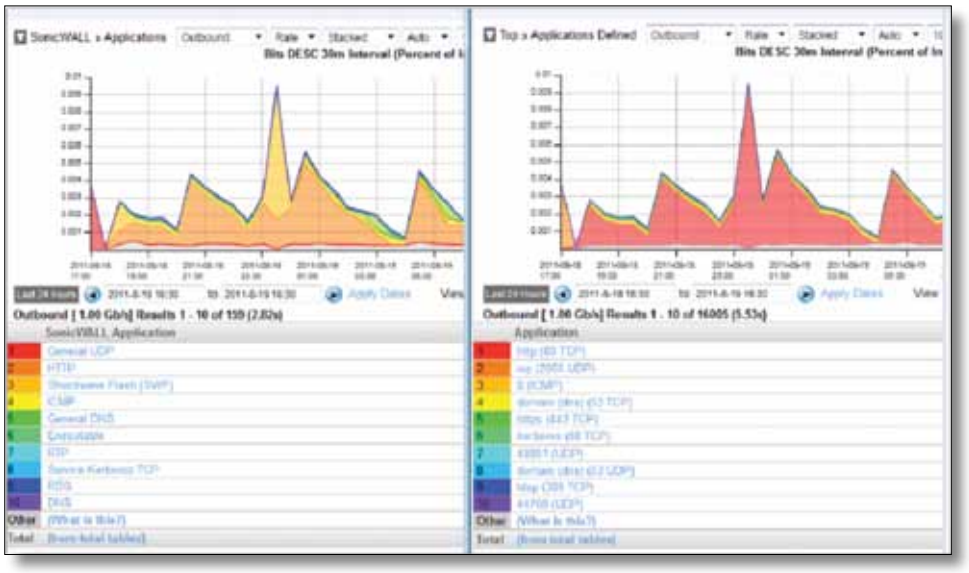
Matrix-Ansicht

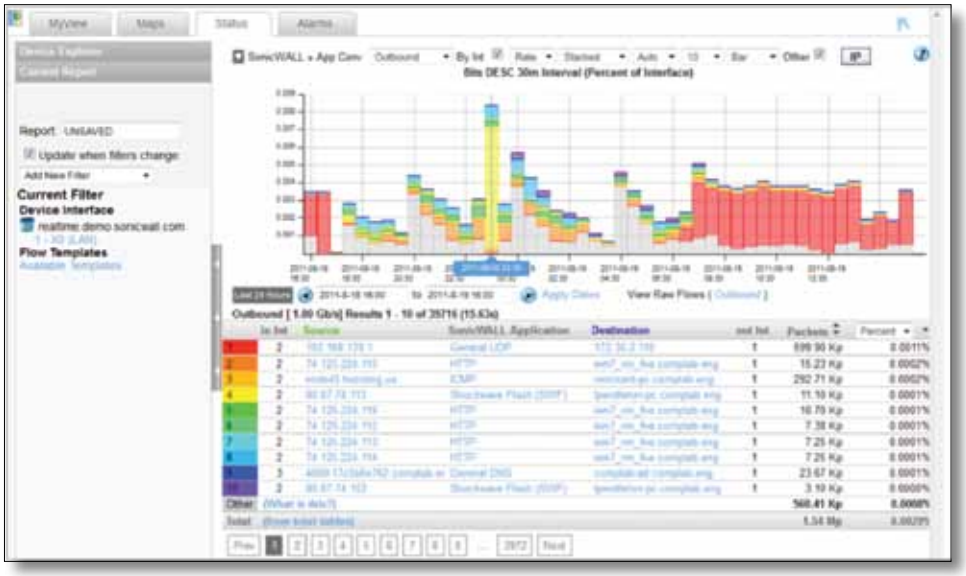
Die innovative „Matrix"-Ansicht bietet eine aussagekräftige Visualisierung der Client-Anwendungskommunikation im gesamten Netzwerk. Host-Host-Verbindungen lassen sich einfach identifizieren, da man die Verbindungen sehen kann, während sie aufgebaut werden.



SonicWALL-Vorlagen

Individuelle SonicWALL-Vorlagen liefern zusätzliche Details und genaue Einblicke in den Datenverkehr im Netzwerk. In der linken Hälfte der Abbildung sehen Sie SonicWALL IPFIX mit Vorlagen, rechts eine herkömmliche Anwendungsverkehrsanalyse.



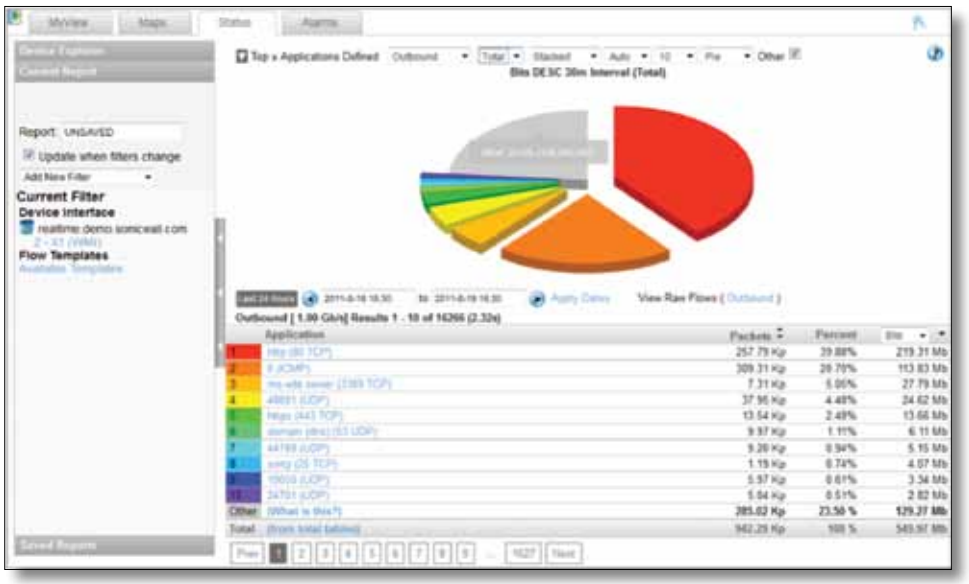


Client-Anwendungskommunikation

Der Anwendungsverkehr lässt sich einfach nach einem bestimmten Zeitbereich aufschlüsseln, um Nutzungsspitzen zu erkennen. Aussagekräftige Netzwerkperformance-Daten machen die Statistiken zur Anwendungsnutzung noch anschaulicher.

Angaben zu Anwendungen

Schlüsseln Sie den Anwendungsverkehr in mehrere verschiedene Ansichten auf, um den Datenverkehr nach Paketzahl, Bits, Bytes oder als Prozentzahl des gesamten Verkehrs innerhalb einer bestimmten Zeitspanne anzuzeigen.



Funktionen und technische Daten

Empfohlene Implementierung

Hardware
x64 Quad Core 2 GHz
8 GB RAM
50 GB HDD (IDE oder SATA)

Betriebssystem
Windows Server 2008 64-Bit (R2) [alle Editions]

Mindestanforderungen

Hardware
x64 Dual Core 2,2 GHz
4 GB RAM
50 GB HDD (IDE oder SATA)

Betriebssystem
Windows Server 2008 64-Bit (SP2) [alle Editions]
Windows Vista 64-Bit Professional oder Enterprise

SonicWALL Scrutinizer mit Flow Analytics

5 Nodes
01-SSC-4002

25 Nodes
01-SSC-4003

Unlimitiert
01-SSC-4004

Add-On-Module

Managed Service Provider-Modul

5 Nodes
01-SSC-4515

25 Nodes
01-SSC-4516

Unlimitiert
01-SSC-4521

Cisco Advanced Reporting-Modul
01-SSC-4536

Hinweis: Informationen zu verfügbaren Node Upgrade-Optionen und Support-SKUs erhalten Sie unter **www.sonicwall.com**

	Kostenfreier Scrutinizer	Scrutinizer mit Flow Analytics-Modulen	Scrutinizer mit Flow Analytics- und Service Provider-Modulen
Kapazität und Visualisierung			
Archivierte Daten	Bis zu 24 Stunden	Unbegrenzt	Unbegrenzt
Plattform für Trendanalyse bei Kombination mit Berichtsarchivierung	Bis zu 24 Stunden	■	■
Auflistung der häufigsten Schnittstellen für alle Router, Switches und Firewalls	Auf 5 Schnittstellen begrenzt	■	■
Kompatibel mit zahlreichen Anbietern	■	■	■
Kapazitäten für 20.000 Flows pro Sekunde mit v8.X	■	■	■
Unterstützung für über 1.000 Exporter und über 1.000 Schnittstellen	■	■	■
Integration mit Google Maps	■	■	■
Flexibles Reporting			
Zeitliche Planung für den Berichtversand per E-Mail		■	■
Daten lassen sich mithilfe von Filtern ein- und ausschließen	■	■	■
Möglichkeit zum Umbenennen von Vorlagen für zukünftige Anwendung	■	■	■
Definierbare vorgegebene Startseite pro Kunden-Login	■	■	■
Definition von Anwendungsgruppen mit Port- und IP-Adressbereichen	■	■	■
Datendarstellung in Bits, Bytes, Paketen oder Prozentzahlen	■	■	■
Genaue Darstellung mit FlowView bis auf die Empfangssekunde	■	■	■
Bericht pro Schnittstelle über häufigste Hosts, Protokolle, Anwendungen, Client-Anwendungskommunikation etc.	■	■	■
Filter-Speichermöglichkeit bei individuellen Berichten		■	■
Trends für ein- und ausgehende Daten oder für beide Richtungen gleichzeitig in allen Berichten	■	■	■
Möglichkeit zum Hinzufügen mehrerer Schnittstellen für mehrere Router, Switches oder Firewalls in einem einzigen Bericht	■	■	■
Filtern nach sämtlichen exportierten Feldern (z. B. MAC-Adresse, VLAN, Latenz) in den Vorlagen	■	■	■
Einfache Identifizierung häufiger Anwendungen im Netzwerk über zahlreiche Netzwerkgeräte hinweg		■	■
MPLS-Reporting nach Subnetzen		■	■
Reporting und Trends zu Microsoft® Exchange-Protokollen		■	■
Speicherung aller Einträge und aller Flows so lange wie nötig, ggf. ohne Zeitbeschränkung		■	■
Erstellung von Berichten über die häufigsten Länder, Domänen oder Subnetze		■	■
SonicWALL-spezifische Reporting-Vorlagen		■	■
Individuelle Abrechnungslösungen bei übermäßiger Nutzung und zur Fakturierung			■
Warnmeldungen			
Warnmeldungen bei gespeicherten Filtern, hoher Schnittstellenaktivität, unfertigen Flows und potenziell schädlichen Aktivitäten		■	■
Im Scrutinizer gespeicherte Berichte können mit einem Schwellenwert zum Auslösen eines Alarms konfiguriert werden		■	■
Eindeutiger Index pro Alarm (zeigt, wie viele andere Alarme der Host ausgelöst hat)		■	■
Administratoren können die Servicequalität proaktiv überwachen und werden automatisch über Qualitätsprobleme beim Voice/Video-Verkehr benachrichtigt		■	■
Fehlerbehebung			
Erstklassiges Fehlerbehebungstool, mit dem sich Performanceprobleme erkennen lassen	■	■	■
Latenz/Jitter-Analyse nur mit nProbe	■	■	■
Suche nach bestimmten Hosts oder Ports	■	■	■
Kapazitätsplanungstool für Systemadministratoren, um die Nutzung während Spitzenzeiten zu ermitteln		■	■
Host-Flows (Flow-Aufkommen pro Host oder Aufkommen der Unique Hosts)		■	■
Adresspaar-Aufkommen (Aufkommen einmaliger Absender-Ziel-Adresspaare)		■	■
Nutzung von IPFIX-Statistiken für einen besseren Einblick in VoIP-Kennzahlen (Codec, Anrufer-ID, Dauer, Ursprung, Ziel, etc.)		■	■
Sicherheit			
Konfigurierbarer Zeitrahmen für DNS Caching	■	■	■
Filtermöglichkeit nach Host-Host und Subnet-Subnet	■	■	■
Möglichkeit, den Datenverkehr anhand von TCP-Flags zu filtern	■	■	■
Nachverfolgung der Flow-Sequenznummer, Trendermittlung bei den Ergebnissen und Anzeigen von Problemen	■	■	■
Erkennung und Warnung bei gesperrten Anwendungen (z. B. BitTorrent P2P, FTP, YouTube, Facebook, Skype)		■	■
Erkennung und Warnung bei böswilligem Datenverkehr (z. B. Würmer oder Viren), bekannten infizierten Internet-Hosts, illegalen IP-Adressen, übermäßigem Multicast-Verkehr, HTTP-Hijacking, DNS-Cache Poisioning, unberechtigten DHCP-Servern, DDoS-Angriffen etc.		■	■
Erkennung und Warnung bei Scanning: SYN, NULL, FIN, XMAS etc.		■	■
Verwaltung			
Personalisierbare MyView-Dashboards pro Anmeldung	■	■	■
Gruppenbasierte Benutzerrechte	■	■	■
Konfiguration von Berechtigungen nach Anmelde-Konto für den Zugriff auf Flows bestimmter Router-, Switch- oder Firewall-Schnittstellen			■
Stylesheets zur einfachen Modifizierung mit zahlreichen Standardeinstellungen zum Ändern der Farbe, Schrift und Logos, um die Marketinganforderungen des Service Providers zu erfüllen			■
Unterstützte Protokolle und andere technische Daten			
Personalisierbare Schnittstellennamen und Möglichkeit, Standard-SNMP-ifAlias-Namen zu ändern	■	■	■
Personalisierbare Schnittstellengeschwindigkeit sowohl in ein- als auch ausgehender Richtung mit unterschiedlichen Werten	■	■	■
Identifizierung der Schnittstellennamen mit NetFlow oder SNMP	■	■	■
Integration mit sämtlichen Fremdanbieter-NMS-Lösungen	■	■	■
LDAP-Unterstützung	■	■	■
Erkennen von Flows bei unbegrenzten UDP-Ports	■	■	■
IPv6-Unterstützung	■	■	■
Unterstützung für NetFlow v1, v5, v6, v7, v9, jFlow, sFlow (v2, v4, v5), SNMP(v1, v2, v3) und IPFIX	■	■	■
Nexthop-Filter	■	■	■
FnF NBAR- und IPFIX-Unterstützung zum Durchführen von Deep Packet Inspection, um Layer 7-Anwendungsverkehr zu identifizieren		■	■
DNS-Auflösung wird automatisierter und konstanter Prozess		■	■

SonicWALL-Lösungen für dynamische Sicherheit

NETWORK SECURITY | SECURE REMOTE ACCESS | WEB & E-MAIL SECURITY | BACKUP & RECOVERY | POLICY & MANAGEMENT

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®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

©2010 SonicWALL und das SonicWALL-Logo sind eingetragene Marken von SonicWALL, Inc. Dynamic Security For The Global Network ist eine Marke von SonicWALL, Inc. Alle anderen hier erwähnten Produktnamen sind Eigentum der jeweiligen Inhaber. Änderung technischer Daten und Produktbeschreibungen ohne vorherige Ankündigung vorbehalten. 10/10 SW 1083