



SonicWALL ViewPoint

POLICY UND MANAGEMENT

Die umfassende Reporting-Lösung für Netzwerke

Ein detaillierter Überblick über Vorgänge und Aktivitäten im Netzwerk, wie etwa Sicherheitsbedrohungen, Bandbreitenbelegung sowie die Anwendungs- und Internetnutzung durch die Mitarbeiter, ist für heutige Unternehmen nahezu unverzichtbar. Um größtmögliche Sicherheit zu gewährleisten, Bandbreiten sinnvoll zuzuweisen und für künftige Anforderungen planen zu können, benötigen IT-Administratoren ein intelligentes Tool, das Ereignisse und Aktivitäten im gesamten Netzwerk umfassend und übersichtlich abbildet.

Mit seinem komfortablen webbasierten Reporting stellt SonicWALL® ViewPoint™ eine ideale Ergänzung zu den übrigen Sicherheitsprodukten und Services von SonicWALL dar. Umfassende Reporting-Funktionen liefern ein detailliertes Bild vom Zustand des Netzwerks, inklusive Daten zu Leistung und Sicherheit. Durch die benutzerdefinierte Übersichtsanzeige und eine Vielzahl unterschiedlicher historischer Reports behalten Unternehmen aller Größenordnungen mit SonicWALL ViewPoint den Überblick über Netzwerkauslastung, Security-Aktivitäten sowie über die Web- und Anwendungsnutzung.

SonicWALL ViewPoint kann als Software-Anwendung auf einem Windows® Server von einem Drittanbieter oder als SonicWALL Virtual Appliance in einer VMware®-Umgebung installiert werden. Der Datenverkehr über kabelgebundene oder drahtlose LAN-, WAN- bzw. VPN-Netze wird auf Grundlage der von den SonicWALL Appliances übermittelten Daten und Ereignisse grafisch dargestellt. Darüber hinaus liefert SonicWALL ViewPoint benutzerdefinierte und zeitgesteuerte Reports in verschiedenen exportierbaren Formaten, mit denen sich Organisationen auf Compliance-Audits vorbereiten können.

Funktionen und Vorteile

Große Auswahl an übersichtlichen Reports zu Firewall-Angriffen, Bandbreitennutzung, Websitebesuchen, Anwendungsnutzung und Benutzeraktivitäten macht die Mitarbeiterproduktivität transparent und identifiziert potenziell schädliches Verhalten.

360°-Reporting bietet eine individuell anpassbare Ansicht mit mehreren Übersichtsreports auf einer Seite. Damit können Benutzer wichtige Kennzahlen zum Netzwerk leicht auffinden und Daten aus mehreren Berichten rasch im Überblick analysieren.

Das **Compliance Reporting** gibt Administratoren die Möglichkeit, Berichte zu erstellen und anzuzeigen, die alle Compliance-Anforderungen erfüllen. Diese Berichte können ad hoc oder auch zeitgesteuert für bestimmte gesetzliche Vorgaben erstellt werden.

Sammelreports zu verschiedenen Bedrohungsarten erlauben das Abrufen von Daten über abgewehrte Angriffe und die sofortige Erkennung von Bedrohungen der SonicWALL Network Security Appliances mithilfe des Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service.

Benutzerbasiertes Reporting bildet lokale Benutzeraktivitäten oder auch Aktivitäten an externen Netzwerkstandorten ab und liefert ein genaueres Bild des Nutzungsverhaltens im gesamten Netzwerk.

Flexible Implementierung in Form von **Software** (Nutzung bestehender Infrastruktur) oder als **Virtual Appliance** (gemeinsame Nutzung von IT-Ressourcen, um die Auslastung zu optimieren, Migrationen zu vereinfachen und Investitionskosten zu senken)

Automatisiertes Scheduling von Reports unterstützt die Übermittlung von Tages-, Wochen- oder Monatsreports per E-Mail sowie die Archivierung der Reports. Mittels unterschiedlicher exportierbarer Formate können Benutzer Daten an das Management weiterleiten oder zum späteren Gebrauch archivieren.

Ortsunabhängiger Zugriff vereinfacht die Abfrage von Daten. Sämtliche Reporting-Funktionen lassen sich von einem beliebigen Standort aus mithilfe eines Standard-Webrowsers anzeigen.

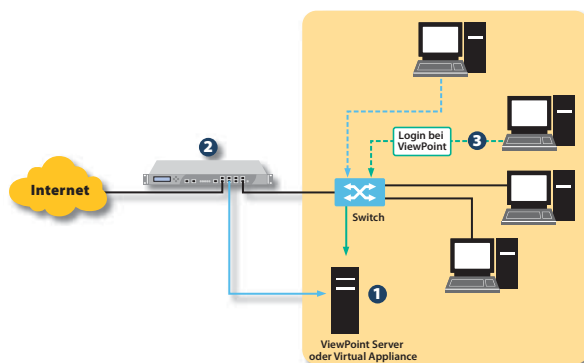
Zusätzliche Analysefunktionen bieten detailliertere Reports zu den unterschiedlichen Arten von Angriffen sowie deren Quellen. Administratoren können so schneller auf externe Bedrohungen reagieren.

Application Control- und SSL VPN-Berichte verbessern die Verwaltung hinsichtlich der Netzwerkeffizienz und -produktivität. Administratoren können Application Control-Berichte, z. B. zu Top-Anwendungen, -Usern und -Regeln, sowie SSL VPN-Berichte zu Top-Usern, Bandbreitenverbrauch, genutzten Ressourcen und Authentifizierungskennzahlen generieren. Detaillierte Informationen können per Drill-Down abgerufen werden. Flexible Implementierung als Software (Nutzung bestehender Infrastruktur) oder Virtual Appliance (gemeinsame Nutzung von IT-Ressourcen, um die Auslastung zu optimieren, Migrationen zu vereinfachen und Investitionskosten zu senken).

- Große Auswahl an übersichtlichen Reports
- 360°-Reporting
- Compliance Reporting
- Sammelreports zu verschiedenen Bedrohungsarten
- Benutzerbasiertes Reporting
- Software- oder Virtual Appliance-Optionen
- Automatisiertes Scheduling von Reports
- Ortsunabhängiger Zugriff
- Zusätzliche Analysefunktionen
- Application Control- und SSL VPN-Berichte

Technische Daten

SonicWALL ViewPoint-Architektur



- 1 Die SonicWALL ViewPoint-Software wird auf einem Netzwerkcomputer mit vorgeschalteter SonicWALL Network Security Appliance installiert.
- 2 Die zentrale SonicWALL Network Security Appliance wird so konfiguriert, dass sie Syslog-Daten an den SonicWALL ViewPoint-Server oder an die Virtual Appliance weiterleitet.
- 3 Der Administrator kann sich über einen Webbrowser bei SonicWALL ViewPoint von unterschiedlichen PCs aus anmelden und Firewall-Übersichtsreports wie „360°“, „Benutzer mit dem höchsten Bandbreitenverbrauch“, „Bandbreite Gesamt“ und „Übersicht Angriffe“ abfragen.

ViewPoint-Reports – Beispiele



„360°“
Benutzerdefinierte Ansichten zeigen mehrere Übersichtsreports in anschaulicher Form.



Web- und Anwendungsnutzung
Mit diesem Report lassen sich sämtliche Aspekte des Internet-nutzungsverhaltens im Netzwerk darstellen. Sie können ablesen, wie lange Mitarbeiter im Internet surfen, Sie erkennen exakt, welche Websites und welche Anwendungen zu welchem Zeitpunkt aufgerufen werden, und sehen verdeckte Nutzungsmuster.



Übersicht Angriffe
Mithilfe der SonicWALL Abo-Services lassen sich Informationen über abgewehrte Angriffe abrufen.



Dienste, Protokolle und Anwendungen
Die Benutzer können den Netzwerkverkehr nach Kategorien aufgeschlüsselt anzeigen. Auf dieser Grundlage können bestimmte Verkehrsarten ausgeschlossen werden, um die Netzwerk-Performance zu verbessern.

Mindestanforderungen an das System

Betriebssystem

Windows Server 2003 32 Bit und 64 Bit (SP2), Windows Server 2008 SBS 64 Bit, Windows Server 2008 Standard 32 Bit und 64 Bit (SP1), Windows XP Professional 32 Bit (SP3), Windows Vista 32 und 64 Bit (SP1), Windows 7 32 Bit und 64 Bit.

In allen Fällen läuft SonicWALL ViewPoint als 32 Bit-Anwendung.

Hardware für ViewPoint-Server

x86-Umgebung: Mindestens 3 GHz Single-CPU-Intel-Prozessor, 2 GB RAM und 100 GB freier Festplattenspeicher

Java

Java-Plug-In Version 1.5 oder höher

Unterstützte SonicWALL Appliances

SonicWALL Network Security Appliances: E-Class NSA-Serie, NSA-Serie, TZ-Serie, PRO-Serie, SonicWALL CSM Appliances, SonicWALL SSL VPN Appliances

Unterstützte Webbrowser

Microsoft® Internet Explorer 6.0 oder höher, Mozilla Firefox 2.0 oder höher

Unterstützte SonicWALL-Firmware

SonicWALL Network Security Appliances:

E-Class NSA-Serie, NSA-Serie: SonicOS Enhanced 5.0 oder höher

PRO-Serie: SonicOS Enhanced 3.2 oder höher

TZ-Serie: SonicOS Standard 3.1 oder höher und SonicOS Enhanced 3.2 oder höher

SonicWALL CSM Appliances: SonicWALL 2.0 oder höher

SonicWALL SSL VPN Appliances: SonicWALL SSL VPN für KMUs Firmware 2.0 oder höher, SonicWALL Aventail E-Class SSL VPN Firmware 9.0 oder höher

Virtual Appliance

Hypervisor: VMware ESX und ESXi

Installiertes Betriebssystem: Gehärtetes SonicLinux

Appliance-Kapazität: 250 GB – 950 GB

Zugewiesener Speicher: 3 GB

VMware-Kompatibilitätsrichtlinien für Hardware:

<http://www.vmware.com/resources/compatibility/search.php>

Weitere Informationen zu den Policy- und Management-Tools von SonicWALL, wie z. B. ViewPoint, erhalten Sie auf unserer Website unter <http://www.sonicwall.com/products/mgmt.html>

SonicWALL-Lösungen für umfassende Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT

SonicWALL ViewPoint

01-SSC-2902 ViewPoint für TZ-Serie und SSL-VPN 200
01-SSC-2901

SonicWALL ViewPoint für NSA-Serie, PRO-Serie, SSL-VPN 2000 und 4000
01-SSC-2902

SonicWALL ViewPoint für E-Class NSA-Serie
01-SSC-2905

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

