

SonicWALL Application Intelligence & Visualization

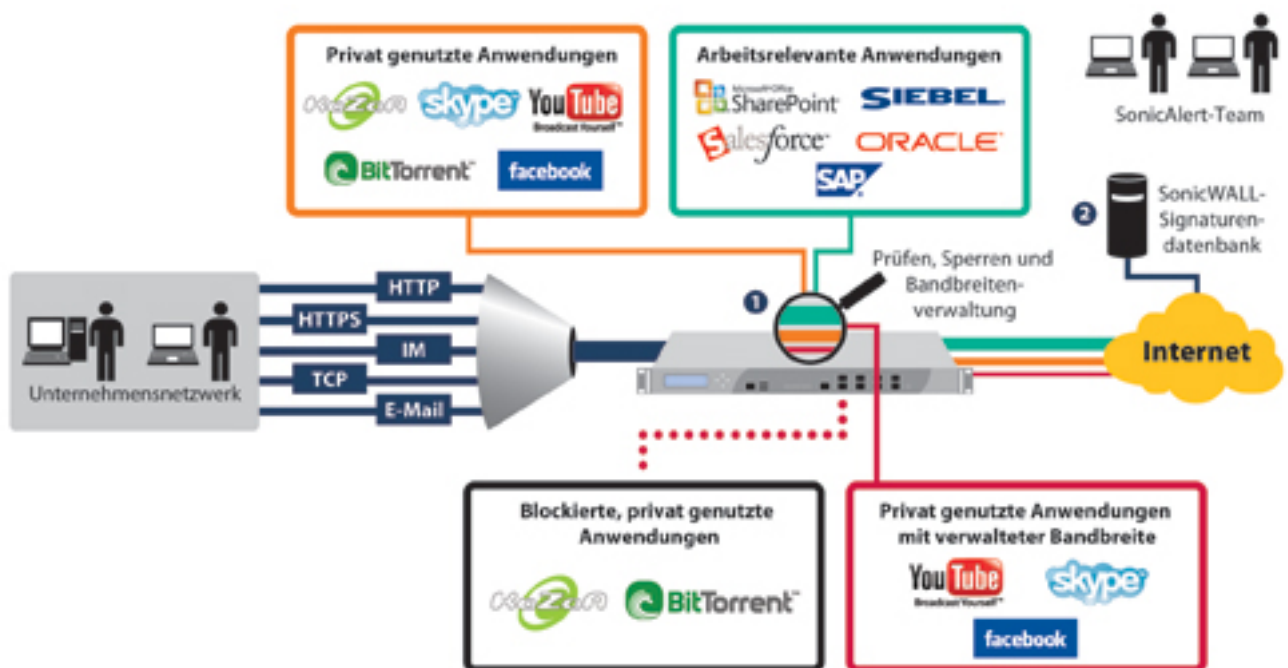
Zugriffskontrolle auf Anwendungsebene und Schutz vor Datenlecks

Wie Application Intelligence die Netzwerksicherheit im Zuge von Web 2.0, Cloud Computing und Mobility sicherstellt.

Webbasierte Anwendungen bilden das Kernstück innovativer Web 2.0-, Cloud Computing- und Mobilitätsinitiativen, mit denen die Produktivität gesteigert, die Zusammenarbeit verbessert, Abläufe rationalisiert und Kosten reduziert werden können. Doch immer noch ignorieren viele Unternehmen die erhöhten Risiken die diese Technologien mit sich bringen.

Mit **SonicWALL® Application Intelligence** werden die Netzwerksicherheits-Appliances von SonicWALL um Funktionen zum Schutz, zur Verwaltung und Kontrolle des Datenverkehrs in der Anwendungsschicht erweitert – neben dem Schutz gegen herkömmliche Bedrohungen in der Netzwerkschicht. Im Gegensatz zu Appliances, die nur auf Anwendungskontrolle setzen, bietet SonicWALL eine nahtlose Integration von Application Intelligence mit Intrusion Prevention und branchenführendem Firewall-Schutz – und damit eine einheitliche und umfassende Netzwerksicherheitslösung, die sich zudem einfach bereitstellen und verwalten lässt.

SonicWALL Deep Packet Inspection Architektur mit Application Intelligence:



- **Leistungsstarke Engine** sucht nach Anwendungen unabhängig von Port, Protokoll oder HTTPS/SSL-Verschlüsselung
- Kontinuierlich **aktualisierte Datenbank** mit tausenden von Anwendungssignaturen
- **Automatisierte Anwendungsprüfung** in kabelgebundenen und drahtlosen Netzwerken

- **Application Intelligence-Logging und Reporting** mit GMS oder ViewPoint möglich

Die wichtigsten Vorteile von SonicWALL Application Intelligence auf einen Blick:

(1) Skalierbarkeit:

Prüfung einer unbegrenzten Zahl gleichzeitiger Downloads mit beliebiger Größe

(2) Visualisierung und Kontrolle von Anwendungen:

Ermöglicht das regelbasierte Blockieren oder Einschränken spezifischer Anwendungen wie z. B. bandbreitenintensiver Audio/Video-Streaming- und Peer-to-Peer-Programme, unzulässiger ausführbarer Dateien (z. B. EXE, PIF, SRC, VBS), nichtautorisierter Web 2.0-Websites, Browser oder Instant Messaging-Clients.

(3) Schutz von Anwendungen vor Bedrohungen:

Sorgt auch bei andauernden, insbesondere auf Cloud-basierte Anwendungen abzielenden Angriffen für stabile Performance.

(4) Anwendungsbasierte Bandbreitenverwaltung:

Sorgt für Quality of Service (QoS), indem bestimmten geschäftskritischen Anwendungen, Benutzergruppen oder Tageszeiten dedizierte Durchsatzraten zugewiesen werden.

(5) Anwendungsbasierter Schutz vor dem Abfangen von Daten:

Erkennt und verhindert, dass sensible, vertrauliche oder mit einem Wasserzeichen versehene Daten über FTP-Server oder als Anhang über öffentliche Webmail-Dienste wie Hotmail® oder Google Mail® oder über unternehmensinterne E Mail-Dienste wie SMTP und POP3 unautorisiert das Unternehmensnetzwerk verlassen.