

10 Möglichkeiten, wie Sie Ihr Netzwerk sicher optimieren können

Mit SonicWALL Next-Gen Firewall Application Intelligence and Control und der WAN Acceleration Appliance (WXA)-Serie

SONICWALL[®]

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Sichere Netzwerkoptimierung	1
1. Application Intelligence	2
2. Blockieren von unerwünschten Anwendungen	3
3. Bandbreitenverwaltung auf Anwendungsebene	4
4. Datendeduplizierung	5
5. Windows File Share-Beschleunigung	6
6. Protokoll-Optimierung	7
7. Datenkompression	8
8. Verbesserte Sicherheit	9
9. Echtzeit-Visualisierung	10
10. Mühelose Verwaltung	11
Sichere Netzwerkoptimierung mit SonicWALL	12
SonicWALL Next-Generation Firewalls	13
Die SonicWALL WAN Acceleration Appliance-Serie	14
Vereinfachte Implementierung	15
Fazit	16

Sichere Netzwerkoptimierung

Das Web hat sich rasant entwickelt und die Art, wie wir arbeiten, grundlegend verändert. Mit der zunehmenden Verbreitung von Web 2.0- und Social Networking-Anwendungen müssen IT-Verantwortliche völlig neue Herausforderungen bewältigen, um moderne Unternehmensnetzwerke zu schützen, zu kontrollieren und ausreichend mit Bandbreite zu versorgen.

Optimierte Performance

Verbesserte Sicherheit

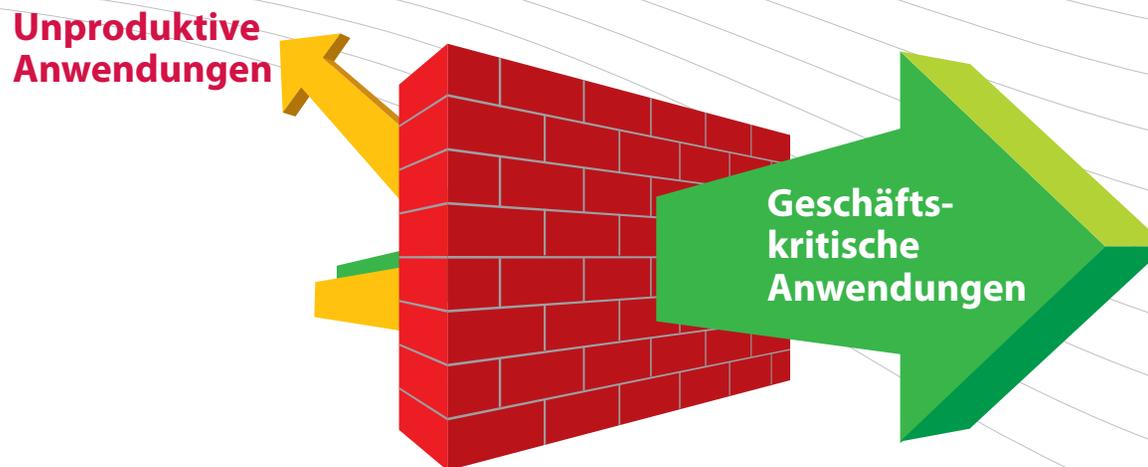
Erhöhte Produktivität

SonicWALLs erweiterte Sicherheitsplattform vereint wie keine andere Lösung zentrale Next-Gen Firewall Application Intelligence, Control and Visualization-Funktionen, Gateway-Schutz und SSL-Inspektion für große Unternehmen sowie WAN-Beschleunigung für verteilte Standorte miteinander. Das reibungslose Zusammenspiel dieser Komponenten sorgt für eine erhebliche Verbesserung der Sicherheit und Kontrolle im Netzwerk. In diesem E-Book zeigen wir Ihnen 10 Möglichkeiten, wie Sie mit den Lösungen von SonicWALL Ihre Performance optimieren, die Sicherheit erhöhen und die Mitarbeiterproduktivität verbessern können, ohne dass Latenzzeiten entstehen.

1. Application Intelligence

Der Anwendungsverkehr in modernen Netzwerken nimmt rasant zu. Bestehende WAN-Lösungen stoßen schnell an ihre Grenzen.

Firewalls mit Application Intelligence filtern nicht arbeitsrelevanten Anwendungsverkehr heraus. So werden einzig die kritischen Anwendungen priorisiert.



Firewalls mit Application Intelligence sind in der Lage, nicht arbeitsrelevante und gefährliche Daten zu visualisieren und herauszufiltern. Datenverkehr von geschäftskritischen Anwendungen wird weitergeleitet.

2. Blockieren von unerwünschten Anwendungen

Die Nutzung nicht arbeitsrelevanter und gefährlicher Anwendungen durch die Mitarbeiter stellt eine zusätzliche Herausforderung für die IT dar.

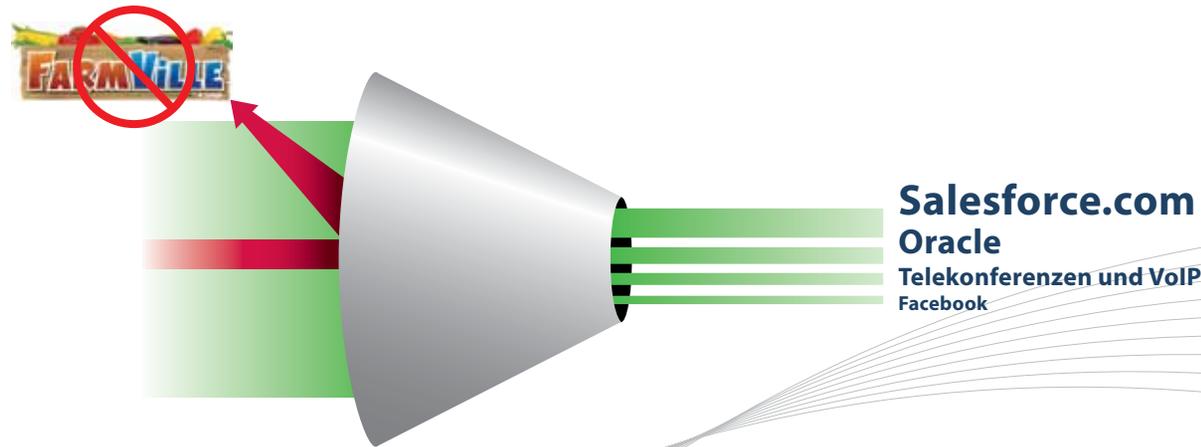


Next-Generation Firewalls mit Application Intelligence and Control können unproduktive oder gefährliche Anwendungen erkennen und blockieren, bevor sie in Ihr Netzwerk gelangen.

Mit Application Intelligence and Control können Administratoren unerwünschte Anwendungsdaten, wie z. B. YouTube, BitTorrent und Facebook Farmville, erkennen und blockieren.

3. Bandbreitenverwaltung auf Anwendungsebene

Kritische Geschäftsanwendungen müssen priorisiert werden. Die Bandbreite für Social Media- und Video-Streaming-Anwendungen hingegen kann nach Bedarf gedrosselt oder komplett blockiert werden.

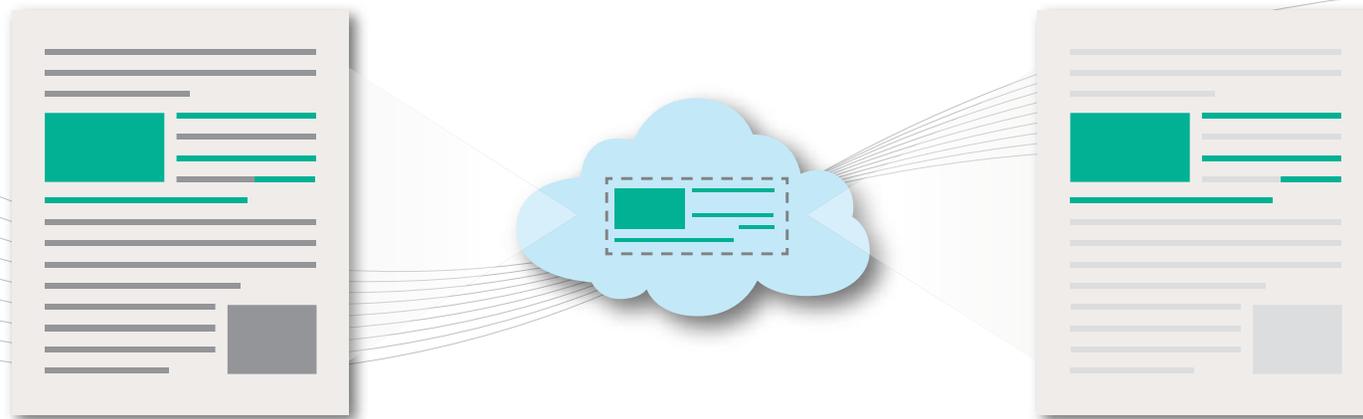


Mit Application Intelligence and Control können Administratoren zwischen produktiven und unproduktiven Anwendungen unterscheiden.

Mit Application Intelligence and Control können Administratoren die autorisierte Nutzung von Anwendungen erlauben (z. B. Facebook für Marketing-Mitarbeiter oder YouTube für Schulungen). Gleichzeitig können sie die private Nutzung bestimmter Applikationen – sogar auf Komponentenebene – sperren (z. B. Farmville auf Facebook). Darüber hinaus können geschäftskritische Anwendungen wie Salesforce.com im Netzwerk priorisiert werden.

4. Datendeduplizierung

Wenn geografisch verteilte Nutzer von Netzwerkanwendungen zusammenarbeiten, werden häufig komplette Dateien mehrmals übertragen, so dass die gleichen Daten immer wieder ausgetauscht werden.



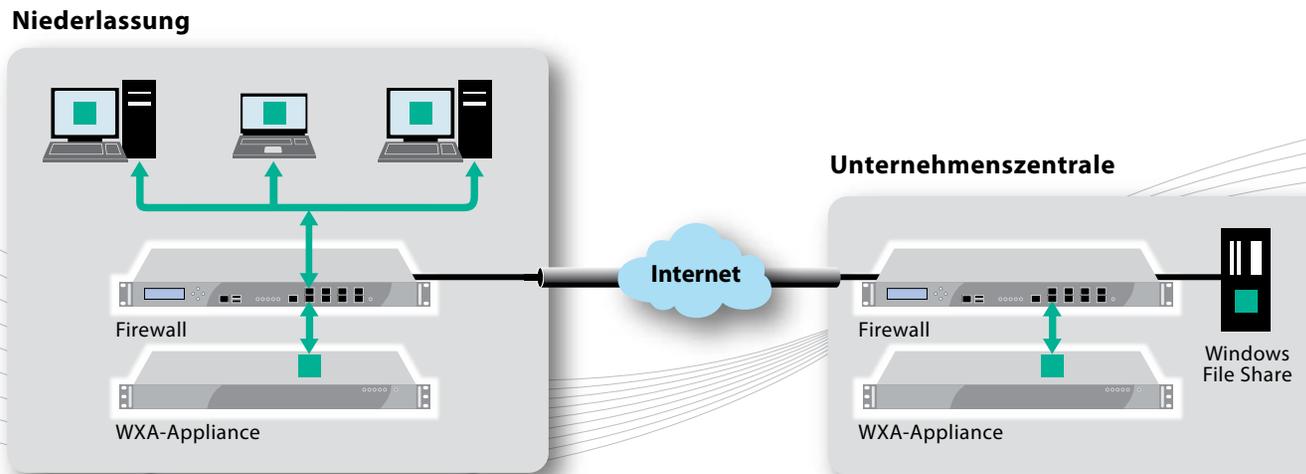
***Datendeduplizierung reduziert den Datenverkehr,
da nur inkrementelle Änderungen übertragen werden.***

Datendeduplizierung mittels Byte- und File-Caching senkt den Bandbreitenverbrauch massiv. Dadurch werden die Antwortzeiten verkürzt, was zu einer besseren Benutzererfahrung für alle Beteiligten führt.

5. Windows File Share-Beschleunigung

Greifen mehrere Benutzer in einem WAN mit Windows® File Sharing (WFS) auf die gleiche Datei zu, kann sich dadurch der Bandbreitenbedarf erhöhen.

Werden ausschließlich die geänderten Daten anstelle der gesamten Datenstrukturen übertragen, profitieren die Nutzer von erheblich kürzeren Antwortzeiten und einem geringeren Bandbreitenverbrauch.

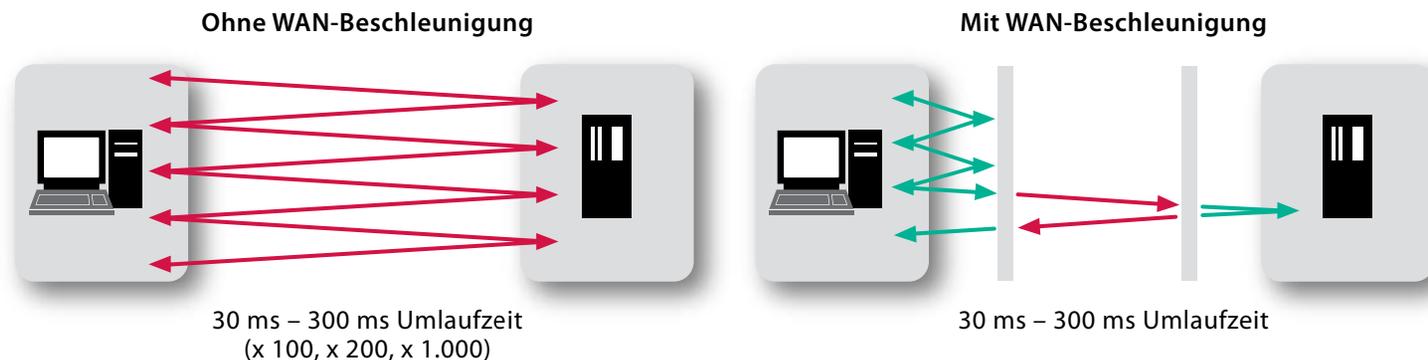


Bei der WFS-Beschleunigung werden die am häufigsten verwendeten Dateien und Metadaten lokal zwischengespeichert, um den redundanten Datenaustausch auf ein Minimum zu reduzieren.

6. Protokoll-Optimierung

Anwendungen, die für eine LAN (Local Area Network)-Umgebung ausgelegt sind, funktionieren über eine WAN-Verbindung aufgrund von Chhattiness oder einer ineffizienten Anwendungskommunikation möglicherweise weniger gut.

Dank Protokoll-Optimierung profitieren Benutzer, die über das WAN auf gemeinsame Ressourcen zugreifen, von einer schnellen LAN-ähnlichen Anwendungsperformance.



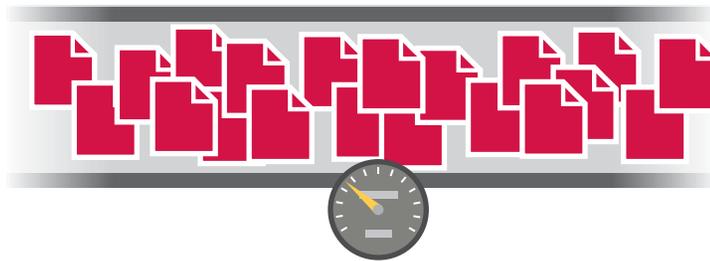
Protokoll-Optimierung verkürzt die Antwortzeiten der Anwendungen beim Zugriff über das WAN.

7. Datenkompression

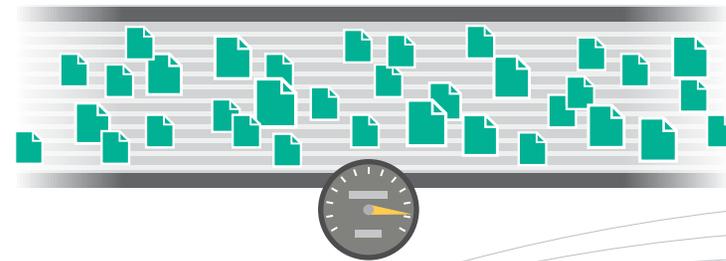
Aufgrund ihrer hohen Komplexität generieren moderne Anwendungen immer mehr Netzwerkverkehr.

Datenkompression sorgt für eine höhere Performance und eine niedrigere Latenz im WAN.

Ohne Datenkompression



Mit Datenkompression

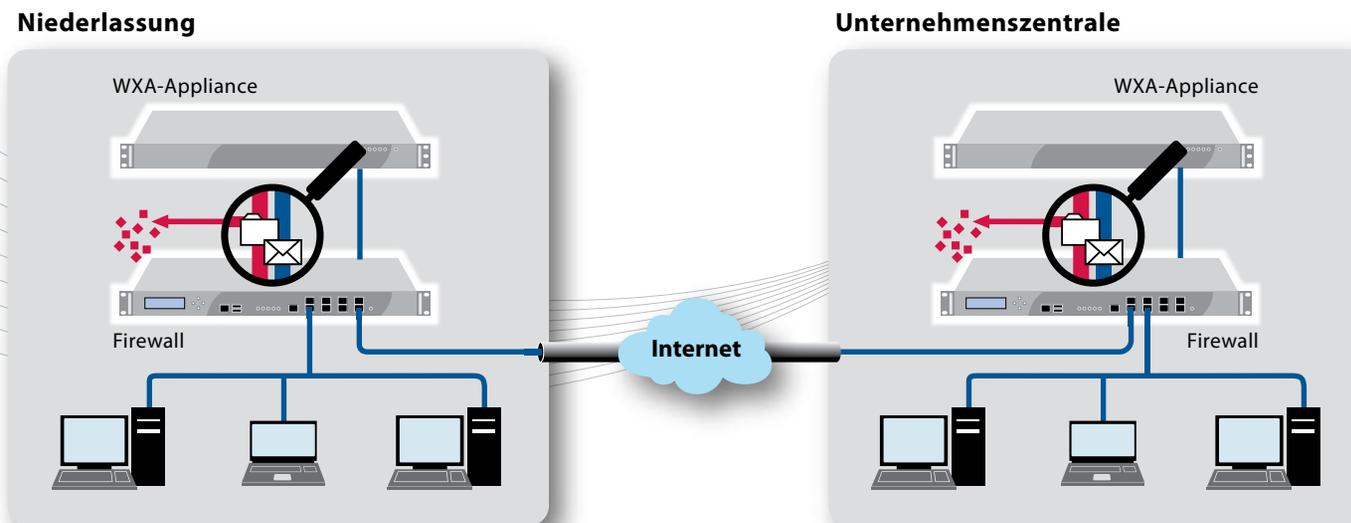


Datenkompression sorgt für eine höhere Performance und eine niedrigere Latenz im WAN.

8. Verbesserte Sicherheit

Bei anderen WAN-Optimierungslösungen muss der Administrator die Lösung innerhalb oder außerhalb der Sicherheitsgrenze implementieren, was das Netzwerk häufig anfällig für Sicherheitsschwachstellen macht. Nicht selten wird durch diese Produkte die Verbreitung von Bedrohungen im Netzwerk sogar noch beschleunigt.

Die SonicWALL Next-Generation Firewalls mit integrierter Reassembly-Free Deep Packet Inspection™ prüfen jedes einzelne Datenpaket für sämtliche Protokolle, um Malware und Eindringversuche abzuwehren, bevor die Daten im WAN beschleunigt werden.



Mit SonicWALL müssen Sie keinen Kompromiss zwischen Sicherheit und Optimierung eingehen.

9. Echtzeit-Visualisierung



Unternehmen benötigen Reporting- und Visualisierungstools, um unerwünschte Netzwerkaktivitäten schnell zu erkennen.

Beschleunigung, ja – aber nicht um jeden Preis!

Die Echtzeit-Visualisierung bietet dem Administrator einen strategischen Einblick in die erzielten Performance-Steigerungen und die damit verbundenen Kosteneinsparungen. Gleichzeitig können Administratoren erkennen, ob unerwünschte oder unsichere Anwendungen genutzt werden und entsprechend reagieren, um das Netzwerk zu schützen bzw. zu steuern und die TCO weiter zu senken.

10. Mühelose Verwaltung

Dank der konsolidierten Administration über eine zentrale Oberfläche lassen sich unsere Lösungen ganz einfach verwalten. Außerdem reduzieren sich Implementierungsaufwand und TCO aufgrund niedrigerer Infrastruktur-, Schulungs- und Administrationskosten.



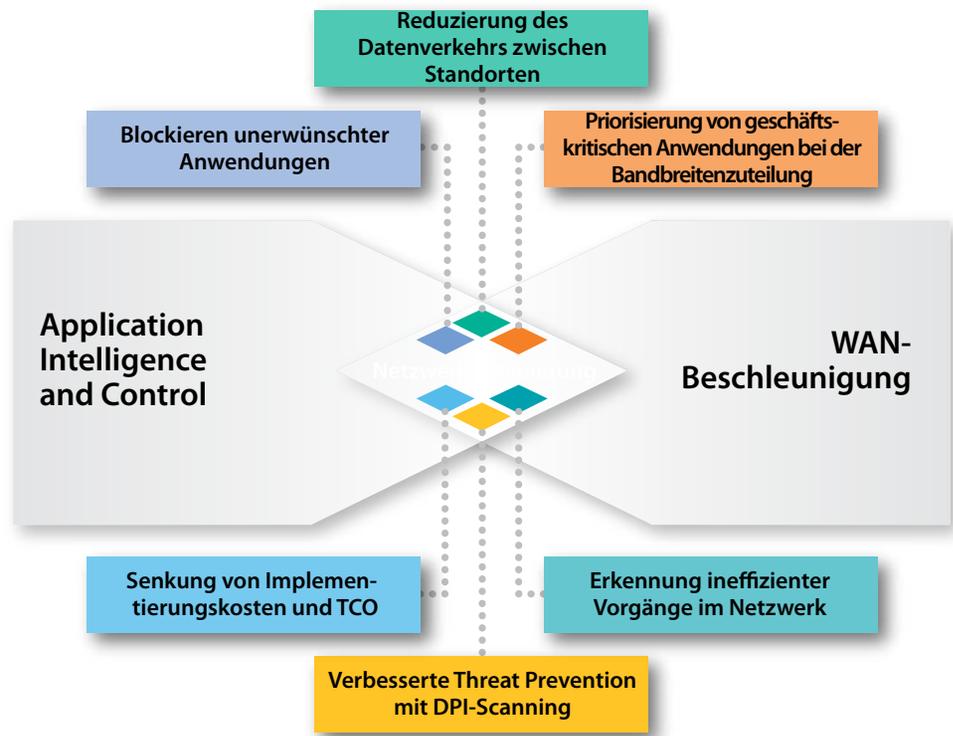
Eine integrierte Plattform ist sicherer und besser zu verwalten als eine zusammengestückelte Lösung.

Mit SonicWALL können Sie die WAN-Beschleunigung und DPI-Prüfung sowie VPN und Application Intelligence and Control über eine einzige Oberfläche verwalten.

Sichere Netzwerkoptimierung mit SonicWALL

SonicWALL bietet Organisationen und Unternehmen ausgereifte Lösungen für eine sichere Netzwerkoptimierung. Wie kein anderer Anbieter bringt SonicWALL dabei zentrale Next-Generation Firewall Application Intelligence, Control and Visualization-Funktionen, Gateway-Schutz und eine Prüfung SSL-verschlüsselter Sitzungen sowie WAN-Beschleunigung für verteilte Netzwerke in einer einzigen Lösung zusammen. Das reibungslose und dynamische Zusammenspiel dieser Komponenten sorgt für eine erhebliche Verbesserung der Sicherheit und Kontrolle im Netzwerk, ohne dass merkliche Latenzzeiten entstehen.

Wir bieten unseren Kunden eine moderne Sicherheitsplattform, mit der sie ihr Netzwerk kontrollieren und vor den ständig neuen Sicherheitsgefahren sowie vor Anwendungsbedrohungen und Bandbreitenverlust schützen können.



SonicWALL Next-Generation Firewalls

SonicWALL Next-Generation Firewalls mit SonicWALL Application Intelligence and Control ermöglichen eine detaillierte Überwachung und Echtzeit-Visualisierung von Anwendungen. So lässt sich die Bandbreite priorisieren und maximale Netzwerksicherheit und Produktivität gewährleisten.

Durch den kombinierten Einsatz der Funktionen Application Intelligence and Control und WAN-Beschleunigung können sie sowohl den Anwendungsverkehr priorisieren als auch den Datenverkehr zwischen den Standorten reduzieren – ein unschlagbarer kombinierter Nutzen.



Das in die SonicWALL Firewalls integrierte Feature nutzt die SonicWALL Reassembly-Free Deep Packet Inspection™-Technologie, um Anwendungen unabhängig von Port oder Protokoll zu identifizieren und zu kontrollieren. Eine ständig wachsende Signaturendatenbank, die Tausende von Anwendungen und Millionen von Malware-Bedrohungen erkennt, verbessert die Sicherheit. Außerdem lassen sich damit die Anwendungen gezielt kontrollieren, die Bandbreite priorisieren oder drosseln und der Zugriff auf bestimmte Websites sperren.

Die SonicWALL WAN Acceleration Appliance-Serie

Die SonicWALL® WAN Acceleration Appliance (WXA)-Serie verbessert die WAN-Anwendungsperformance und Benutzererfahrung in Unternehmen mit Remote-Standorten und Zweigniederlassungen deutlich. Dabei reduziert die WXA-Serie den Datenverkehr massiv, indem nur noch neue oder geänderte Daten im Netzwerk übermittelt werden.



Bei den WXA-Lösungen handelt es sich nicht um Stand-alone-Produkte, sondern um integrierte Add-Ons zu den SonicWALL Next-Generation Firewalls. Dies vereinfacht die Bereitstellung, die Konfiguration, das Routing und die Verwaltung.

Zur SonicWALL WXA-Serie gehören die WXA 500 Live CD, die Hardware Appliances WXA 2000 und WXA 4000 sowie die WXA 5000 Virtual Appliance.

Vereinfachte Implementierung

Die SonicWALL Next-Generation Firewalls bieten Auto-Provisioning und Konfigurationsmanagement für die SonicWALL WAN Acceleration-Serie.

Die Implementierung der WXA-Serie wird deutlich einfacher und erfordert keine erneute Konfiguration des Netzwerks.



Dies erleichtert die Bereitstellung der WXA-Lösungen in verteilten Netzwerken und die Integration mit anderen Komponenten wie z. B. VPNs.

Fazit



Mit den SonicWALL-Lösungen für eine sichere Netzwerkoptimierung erhält Ihr Unternehmen eine erweiterte und konsolidierte Sicherheitsplattform.

Die Integration von Next-Generation Firewall, Deep Packet Inspection, Application Intelligence and Control und WAN-Beschleunigung bietet Ihnen einen effektiven und umfassenden Ansatz, um Ihr Netzwerk sicher zu optimieren.



Weitere Informationen

- Besuchen Sie die Network Optimization Knowledge Site von SonicWALL
- Lesen Sie das Whitepaper "Next-Generation Firewall Market Analysis"

Wenn Sie uns Feedback zu diesem E-Book, anderen E-Books oder Whitepapers von SonicWALL geben möchten, senden Sie eine E-Mail an folgende Adresse: feedback@sonicwall.com.

Über SonicWALL

Geleitet von seiner Vision Dynamic Security for the Global Network entwickelt SonicWALL® intelligente Netzwerk- und Datensicherheitslösungen, die sich dynamisch an die Anforderungen von Organisationen und an die ständig wechselnden Sicherheitsbedrohungen anpassen. Weltweit vertrauen kleine wie große Unternehmen auf die mehrfach ausgezeichneten Hardware-, Software- und Virtual Appliance-Lösungen von SonicWALL, um Anwendungen zu erkennen und zu kontrollieren und um Netzwerke vor Eindringlingen und Malware-Angriffen zu schützen. Weitere Informationen erhalten Sie auf unserer Website unter www.sonicwall.com/de.

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

