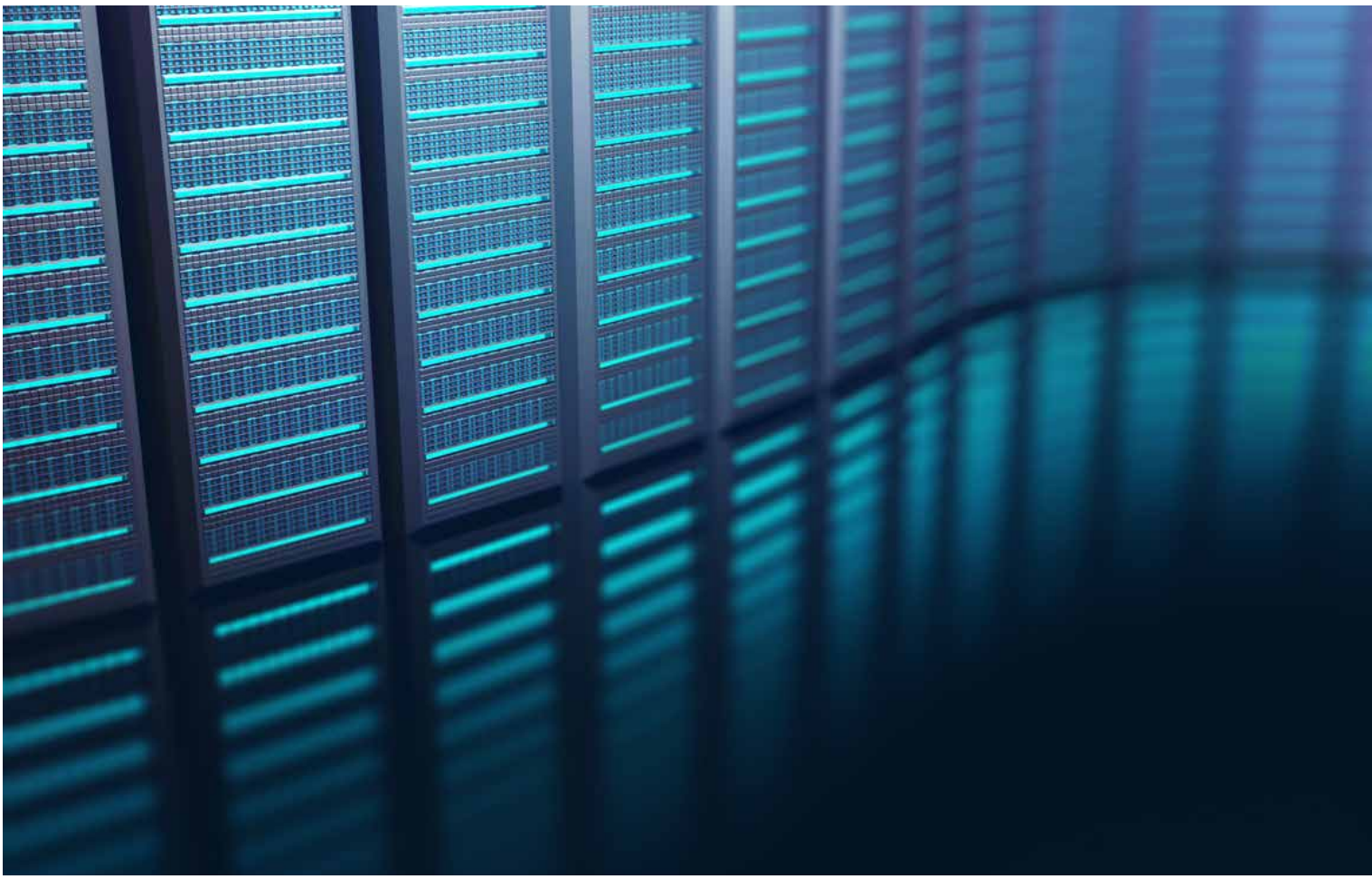
SonicWall-Produktüberblick



Überblick

Für Organisationen ist es heute extrem wichtig, ihre Systeme, Benutzer und Daten möglichst effizient zu schützen, ohne dabei die Netzwerkleistung zu beeinträchtigen. Unsere kabelgebundenen und drahtlosen Sicherheitslösungen werden von mehr als 250.000 Kunden in 200 Ländern eingesetzt – von kleinen und mittleren Firmen bis hin zu größeren Unternehmen, öffentlichen Einrichtungen, Einzelhandelsfirmen, Organisationen aus den Bereichen Bildung und Gesundheitswesen sowie von Serviceprovidern.

SonicWall bietet umfassende, aufeinander abgestimmte Produktlinien für diese Bereiche:

- Netzwerksicherheit
- Zugriffssicherheit
- E-Mail-Sicherheit
- Sicherheitsmanagement und Reporting

Netzwerksicherheit

SonicWall ist einer der führenden Anbieter von Next-Generation Firewalls (NGFWs). Die bewährte SonicOS-Firmware bildet das Herzstück jeder SonicWall NGFW. SonicOS basiert auf unserer skalierbaren Multicore-Hardware-Architektur und unserer patentierten* Single-Pass-Reassembly-Free Deep Packet Inspection® (RFDPI)-Engine, die den gesamten Verkehr unabhängig von Port oder Protokoll prüft und die Latenzzeiten auf ein Minimum begrenzt.

Unsere NGFWs scannen jedes einzelne Paket und jedes einzelne Byte und bieten gleichzeitig die hohe Leistung und die geringe Latenz, die Netzwerke mit hoher Auslastung benötigen. Im Gegensatz zu den Produkten anderer Anbieter ermöglicht die Single-Pass-RFDPI-Engine gleichzeitige Multi-Threat- und Anwendungsprüfungen sowie die Analyse von Dateien beliebiger Größe ohne „Packet Reassembly". Auf diese Weise lässt sich die moderne, ultraskalierbare Sicherheitsarchitektur der SonicWall NGFWs an die Anforderungen wachsender und verteilter Unternehmensnetzwerke und von Datencentern anpassen.

SonicWall NGFWs bieten eine Reihe zuverlässiger Funktionen, darunter:

- Capture Cloud-basiertes Multi-Engine-Sandboxing
- API gegen Bedrohungen
- Entschlüsselung und Prüfung von verschlüsseltem Verkehr
- Intrusion Prevention Service (IPS)
- Malware-Schutz
- Application Intelligence, Anwendungskontrolle und -visualisierung in Echtzeit
- Website/URL-Filtering (Content Filtering)
- Virtual Private Networking (VPN) über SSL oder IPSec
- Wireless-Sicherheit
- Stateful Failover/Failback

Unsere Firewalls bieten darüber hinaus schnelle Reaktionszeiten und einen kontinuierlichen Schutz vor Zero-Day-Bedrohungen durch das Capture Labs-Research-Team. Dieses hochkarätige Team sammelt, analysiert und prüft vektorübergreifend Informationen zu Bedrohungen aus einer Vielzahl von Bedrohungsdatenquellen, darunter eine Million Sensoren innerhalb des Capture Threat-Netzwerks weltweit.

SonicWall SuperMassive Series

Die SonicWall SuperMassive 9000 Series-NGFW-Plattform bietet großen Netzwerken höchste Skalierbarkeit, Zuverlässigkeit und Sicherheit bei Multi-Gigabit-Geschwindigkeiten.

NSS Labs hat unsere Firewalls einem der strengsten Praxistests für NGFWs unterzogen. Dabei erzielte SonicWall herausragende Ergebnisse bei Schutzfunktionen, Performance, Skalierbarkeit, Zuverlässigkeit und TCO. Die Firewalls von SonicWall setzen Maßstäbe bei der High-Performance-Anwendungskontrolle und Bedrohungsabwehr in den unterschiedlichsten Implementierungsszenarien – von kleinen Unternehmen bis hin zu großen Datencentern, Netzbetreibern und Serviceprovidern.

Die SuperMassive 9000 Series bietet die hohe Servicequalität und unterbrechungsfreie Netzwerkverfügbarkeit und Konnektivität, die heute von Unternehmen, Behörden und Universitäten mit 10/40-GBit/s-Infrastrukturen erwartet wird. Dank ihrer hohen Kerndichte und ihrem kompakten 1-HE-und 2-HE-Format sparen die SuperMassive 9000-Firewalls nicht nur Platz im Rack, sondern auch Strom- und Kühlungskosten.

**U.S.- Patente 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723*

SONICWALL®

SonicWall Network Security Appliance (NSA) Series

Die SonicWall Network Security Appliance (NSA) Series ist eine der sichersten und leistungsstärksten NGFW-Produktreihen. Sie gewährleistet kompromisslose Business-Class-Sicherheit und -Leistung und basiert auf der gleichen Architektur wie die SuperMassive Series, das Flaggschiff unserer NGFWs, die ursprünglich für die anspruchsvollsten Telekommunikationsanbieter und Unternehmen weltweit entwickelt wurde. Gleichzeitig steht sie für das exzellente Preis-Leistungs-Verhältnis und die hohe Benutzerfreundlichkeit, die man von SonicWall erwartet.

Nach jahrelanger Forschung und Entwicklung wurde die NSA Series von Grund auf für verteilte Unternehmen, kleine bis mittelgroße Firmen, Zweigniederlassungen, Schulen und Behörden konzipiert. Die NSA Series basiert auf einer revolutionären, ultraskalierbaren Multicore-Architektur und einer patentierten RFDPI-Single-Pass-Engine. Sie gewährleistet höchste Sicherheit, Leistung und Skalierbarkeit sowie eine extrem hohe Anzahl an Verbindungen pro Sekunde und bietet die meisten gleichzeitigen Verbindungen und die geringsten Latenzzeiten ihrer Klasse – ganz ohne Einschränkungen bei der Dateigröße.

SonicWall TZ Series

Die SonicWall TZ Series umfasst extrem zuverlässige und sichere Unified Threat Management (UTM)-Firewalls, die speziell für kleine und mittlere Unternehmen (KMUs), den Einzelhandel, Behörden sowie für verteilte Enterprise-Netzwerke mit Außenstellen und Zweigniederlassungen konzipiert wurden. Mit ihren äußerst wirksamen Anti-Malware-, Intrusion Prevention-, Content/URL Filtering- und Anwendungskontrollfunktionen für kabelgebundene und drahtlose Netzwerke setzen sich die Appliances klar von Produkten für den Consumer-Bereich ab. Darüber hinaus bieten sie umfassende Unterstützung für mobile Plattformen wie Laptops, Smartphones und Tablet-PCs. Dank Deep Packet Inspection (DPI) mit ultraschneller Performance können Unternehmen ihre Produktivität erheblich verbessern, ohne von den Netzwerkengpässen gebremst zu werden, die bei anderen Produkten häufig auftreten.

Wie bei allen SonicWall-Firewalls überprüft die TZ Series die gesamte Datei (auch TLS-/SSL-verschlüsselte Dateien), um einen vollständigen Schutz zu gewährleisten. Darüber hinaus bietet die TZ Series Application Intelligence and Control, detaillierte Analysen des Anwendungsverkehrs und Reporting, Internet Protocol Security (IPsec) und SSL VPN, mehrfaches ISP-Failover, Lastverteilung, optional integriertes Highspeed-802.11ac-WLAN sowie Netzwerksegmentierung und erfüllt außerdem die Anforderungen an PCI-Compliance. In Kombination mit den Switches der Dell X-Series sorgen die Firewalls der TZ Series für die nötige Flexibilität, die Unternehmen brauchen, um sicher wachsen zu können – ohne dabei die Komplexität zu erhöhen.

SonicWave Wireless Network Security Series

Mit seiner innovativen SonicWall Wireless Network Security-Lösung macht SonicWall den Datenaustausch in drahtlosen Netzwerken sicher, einfach und erschwinglich. Die Lösung kombiniert leistungsstarke SonicWave Series 802.11ac Wave 2-Wireless Access Points mit den führenden SonicWall-Firewalls, um das hohe Maß an Sicherheit und Performance zu erreichen, das man von kabelgebundenen Netzwerken kennt. Für Performance und Schutz der Enterprise-Klasse sorgen Intrusion-Prevention, TLS-/SSL-Entschlüsselung und -Prüfung, Anwendungskontrolle sowie Content-Filtering.

Die SonicWave Wireless Network Security Series bietet weit mehr als gewöhnliche Secure Wireless-Produkte. Mithilfe der RFDPI-Technologie gewährleistet unsere Lösung doppelte Sicherheit: Sie schützt drahtlose Netze durch die Verschlüsselung von Wireless-Datenverkehr und eliminiert Netzwerkbedrohungen. SonicWall sorgt dabei für niedrige TCO, da die kostspielige Implementierung und Verwaltung einer separaten Wireless-Lösung parallel zum kabelgebundenen Netz entfällt.

Die TZ Series bietet eine umfassende Sicherheitsplattform zum Schutz von KMUs und Verkaufsfilialen.

SONICWALL®

SonicWall WAN Acceleration Appliance (WXA) Series

Mit der SonicWall WAN Acceleration Appliance (WXA) Series wird die WAN-Anwendungsperformance und Benutzererfahrung in kleinen und mittleren Unternehmen mit Remote-Standorten und Zweigniederlassungen erheblich verbessert. Die WXA Series reduziert den Datenverkehr um ein Vielfaches, weil nach dem erstmaligen Transfer nur noch neu hinzugekommene oder geänderte Daten im Netzwerk übertragen werden. Zudem deduplizieren die WXA-Lösungen die über das WAN transportierte Daten. Hierfür „merken" sie sich, welche Daten bereits übertragen wurden, und ersetzen erneut gesendete Bytefolgen durch eine Kennung. Auf diese Weise verringern sie die Anwendungslatenz und sparen Bandbreite. Zu den weiteren Beschleunigungsfeatures zählen Data-Caching, Datendeduplizierung, Metadata-Caching, HTTP (Web)-Caching und Funktionen zur Komprimierung während der Übertragung.

Bei den WXA-Lösungen handelt es sich nicht um Standalone-Produkte, sondern um integrierte Add-Ons zu den Firewalls der SonicWall SuperMassive 9000, NSA und TZ Series. Die integrierten Lösungen sparen Platz und sorgen für eine effizientere Bereitstellung und Konfiguration. Außerdem ermöglichen sie ein besseres Routing und Management und lassen sich u. a. mit VPNs integrieren. Bei Implementierung mit einer SonicWall-NGFW mit Application Intelligence and Control Service bieten die WXA-Lösungen einen doppelten Vorteil: Sie priorisieren den Anwendungsverkehr und reduzieren gleichzeitig den Datenverkehr zwischen Standorten. Auf diese Weise sorgen sie für eine optimale Netzwerk-Performance.

Weitere Informationen zu den Netzwerksicherheitsprodukten von SonicWall erhalten Sie unter: www.sonicwall.com/de-de/products.

Network Security Services und Zusatzprodukte

Die Network Security Firewall Services und Zusatzprodukte von SonicWall bieten großen wie kleinen Organisationen einen extrem effektiven, erweiterten Schutz, um die Abwehr von Sicherheitsbedrohungen zu unterstützen, die Sicherheitskontrolle zu verbessern, die Produktivität zu steigern und Kosten zu senken.

Unsere Services und Zusatzprodukte umfassen:

- TotalSecure-Bundle – Firewall plus Comprehensive Gateway Security Suite-Bundle (Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence, Content/Web Filtering und 24/7-Support)
- Advanced Gateway Security Suite-Bundle – Capture Advanced Threat Protection, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Content/Web Filtering und 24/7-Support
- Gateway Security Services – Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Application Intelligence and Control
- Capture Advanced Threat Protection (ATP)
- Content Filtering Services
- Enforced Client Anti-Virus und Anti-Spyware-Software
- Comprehensive Anti-Spam Service
- Deep Packet Inspection von SSL-verschlüsseltem Verkehr (DPI SSL)
- Application Intelligence and Control
- Intrusion Prevention System (IPS)

Weitere Informationen zu unseren Network Security Services und Zusatzprodukten erhalten Sie unter: www.sonicwall.com/de-de/products/firewalls/security-services.

Zugriffssicherheit

SonicWall SMA bietet ein einheitliches Secure Access Gateway, um Mobilität, BYOD und Cloud-Migration optimal umzusetzen. Unsere Lösung erlaubt es Organisationen, jederzeit, überall und auf sämtlichen Geräten Zugang zu geschäftskritischen Unternehmensressourcen bereitzustellen. Mit ihrer Regel-Engine zur granularen Zugriffskontrolle, kontextsensibler Geräteauthentifizierung, VPN auf Anwendungsebene und einer erweiterten Authentifizierung mit Singe-Sign-on unterstützt SMA moderne BYOD- und Mobilitätsstrategien in hybriden IT-Umgebungen.

Darüber hinaus reduziert SMA mit Funktionen wie Geo-IP- und Botnet-Erkennung, Web Application Firewall und integrierter Capture ATP-Sandbox die Angriffsfläche für Bedrohungen.

Mobilität und BYOD

Für Organisationen, die auf BYOD, flexible Arbeitszeiten und Offshore-Entwicklung setzen wollen, ist SMA die perfekte Lösung. SMA reduziert die Angriffsfläche für Bedrohungen und sorgt so für erstklassige Sicherheit. Gleichzeitig unterstützt die Lösung die neuesten Verschlüsselungsalgorithmen und Chiffrierverfahren und macht Organisationen so noch sicherer. Mit SonicWall SMA können Administratoren einen sicheren mobilen Zugriff bereitstellen und rollenbasierte Berechtigungen definieren. Auf diese Weise erhalten Endbenutzer einen einfachen und schnellen Zugriff auf die benötigten Unternehmensanwendungen, -daten und -ressourcen. Gleichzeitig schützt die Einführung sicherer BYOD-Regeln Unternehmensnetzwerke und -daten vor unberechtigtem Zugriff und Malware.

Migration in die Cloud

Organisationen, die ihre Daten in die Cloud verlagern, bietet SMA eine Single-Sign-on (SSO)-Infrastruktur mit einem zentralen Webportal zur Authentifizierung der Anwender in einer hybriden IT-Umgebung. SMA sorgt für einen einheitlichen und nahtlosen Zugriff, ganz gleich, ob sich die Unternehmensressourcen im lokalen Netzwerk, im Web oder in einer gehosteten Cloud befinden. Darüber hinaus ist es nicht nötig, sich die vielen unterschiedlichen Anwendungs-URLs zu merken und unzählige Lesezeichen zu pflegen. Mit Workplace, einem zentralen Zugriffsportal, können Anwender über eine einzige URL mit einem Standard-Webbrowser auf alle geschäftskritischen Anwendungen zugreifen. SMA bietet Federated SSO sowohl für in der Cloud gehostete SaaS-Anwendungen, die SAML 2.0 nutzen, als auch für lokal gehostete Anwendungen, die RADIUS oder Kerberos einsetzen. Zusätzliche Sicherheit bietet die Integration unterschiedlicher Authentifizierungs-, Autorisierungs- und Abrechnungsserver sowie führender Multi-Faktor-Authentifizierungstechnologien (MFA). Secure SSO wird erst dann auf autorisierten Endpunktgeräten bereitgestellt, nachdem der Health Status sowie die Einhaltung von Compliance-Vorgaben geprüft wurden.

Managed Service Provider

Managed Service Providern sowie Organisationen mit Datacentern bietet SMA eine sofort einsatzbereite Lösung, um ein hohes Maß an Business-Continuity und Skalierbarkeit zu gewährleisten. Die SMA-Lösung von SonicWall unterstützt bis zu 20.000 gleichzeitige Verbindungen auf einer einzigen Appliance und lässt sich durch intelligentes Clustering für Hunderttausende von Anwender nach oben skalieren. Dank Active-Active-HA-Clustering (Global High Availability) und integriertem dynamischen Load Balancer (Global Traffic Optimizer), der den globalen Datenverkehr bedarfsgerecht dem am besten geeigneten Datencenter in Echtzeit zuweist, lassen sich Kosten für Datencenter einsparen. SMA bietet Service-Verantwortlichen diverse Tools, um die erforderlichen Dienste ohne jegliche Ausfallzeiten bereitzustellen und selbst anspruchsvollste SLAs zu erfüllen.

SonicWall SMA ist ein einheitliches Secure Access Gateway, mit dem Organisationen jederzeit, überall und auf sämtlichen Geräten Zugang zu geschäftskritischen Unternehmensressourcen bereitstellen können.

SMA-Appliances

SonicWall SMA lässt sich als High-Performance-Appliance oder Virtual Appliance (gemeinsame Nutzung der IT-Ressourcen zur Optimierung der Auslastung, Vereinfachung der Migration und Senkung der Investitionskosten) implementieren. Die Hardware-Appliances basieren auf einer Multicore-Architektur, die dank SSL-Beschleunigung, VPN-Durchsatz und leistungsstarken Proxys eine hohe Performance zur Bereitstellung eines zuverlässigen und sicheren Zugriffs bieten. In stark regulierten und staatlichen Organisationen ist SMA mit FIPS 140-2 Level 2-Zertifizierung verfügbar. Die virtuellen SMA-Appliances bieten den gleichen zuverlässigen und sicheren Zugriff auf gängigen virtuellen Plattformen wie Hyper-V und VMware. Egal, ob Sie physische Appliances, virtuelle Appliances oder eine Kombination aus beidem implementieren möchten – SMA lässt sich nahtlos in Ihre bestehende IT-Infrastruktur einbinden.

Management und Reporting

SonicWall bietet eine intuitive webbasierte Verwaltungsplattform, um das Appliance-Management zu optimieren, und stellt umfassende Reporting-Funktionen bereit. Die benutzerfreundliche Oberfläche sorgt für Klarheit bei der Verwaltung mehrerer Appliances. Eine einheitliche Regelverwaltung hilft Ihnen, Zugriffsregeln und -konfigurationen zu erstellen und zu überwachen. Dabei werden Ihre Benutzer, Geräte, Anwendungen, Daten und Netzwerke anhand eines einzigen Regelwerks verwaltet. Routineaufgaben lassen sich automatisieren und Aktivitäten planen. Auf diese Weise werden Sicherheitsteams von redundanten Aufgaben befreit und können sich auf strategische Sicherheitsaufgaben wie z. B. die Reaktion auf Vorfälle konzentrieren.

Ihre IT-Abteilung kann so die Erwartungen der Anwender optimal erfüllen und den für das jeweilige Anwenderszenario sichersten Zugriff bereitstellen. Sie können aus einer Reihe clientloser, webbasierter Secure Access-Möglichkeiten für Servicepartner oder externe Vertragspartner und einem konventionelleren, clientbasierten Full-Tunnel-VPN-Zugriff für Führungskräfte wählen. Egal, ob fünf Anwender auf Daten aus dem gleichen Datencenter oder Tausende von Anwender auf Ressourcen in global verteilten Datencentern zugreifen müssen – SonicWall SMA hat die passende Lösung für Sie, um einen zuverlässigen und sicheren Zugriff bereitzustellen.

Weitere Informationen über die Mobile Security-Produkte von SonicWall erhalten Sie unter: www.sonicwall.com/de-de/products/remote-access.

SONICWALL

E-Mail-Sicherheit

So wichtig E-Mails für die geschäftliche Kommunikation sind, so groß sind auch der Schaden und die Produktivitätsverluste, die sie verursachen können – etwa wenn E-Mail-basierte Bedrohungen wie Ransomware, Phishing, Business-E-Mail-Compromise (BEC), Spoofing, Spam und Viren Ihre Mailserver und Posteingänge überfluten. Darüber hinaus sind Unternehmen laut Gesetz verpflichtet, vertrauliche Daten zu schützen, einen sicheren Austausch sensibler Kundendaten oder vertraulicher Informationen über E-Mail zu gewährleisten und zu verhindern, dass vertrauliche Daten in fremde Hände geraten. Ob es sich bei Ihrer Organisation um eine kleine oder mittelständische Firma mit Wachstumspotenzial, ein großes Unternehmen mit verteilten Netzwerken oder einen Managed-Service-Provider (MSP) handelt – Sie brauchen eine kostengünstige Lösung für E-Mail-Sicherheit und -Verschlüsselung, die so skalierbar und flexibel ist, dass sie mit Ihrem Unternehmen mitwächst und sich dezentral – z. B. entsprechend Ihren Organisationseinheiten und Domänen – verwalten lässt.

Darüber hinaus setzen immer mehr Organisationen auf Microsoft Office 365, um Kosten und Ressourcen effektiv zu managen. Da Office 365 mit Sicherheitsfunktionen zur Bekämpfung raffinierter E-Mail-Bedrohungen ausgestattet ist, benötigen Organisationen eine E-Mail-Sicherheitslösung der nächsten Generation, die sich nahtlos mit Office 365 integrieren lässt und Schutz vor den neuesten raffinierten Bedrohungen bietet.

SonicWall Email Security-Appliances

SonicWall Email Security lässt sich einfach installieren, verwalten und kostengünstig von 10 bis auf 100.000 Postfächer erweitern. Die Lösung kann als Hardware Appliance, als Virtual Appliance (gemeinsame Nutzung von IT-Ressourcen) oder als für Microsoft Windows Server oder Small Business Server optimierte Software implementiert werden. Die physischen SonicWall Email Security Appliances sind ideal für Organisationen, die eine dedizierte lokale Lösung benötigen. Unsere mehrschichtige Lösung bietet umfassenden Schutz vor ein- und ausgehenden E-Mail-Bedrohungen und umfasst mehrere Hardware Appliance-Optionen, die sich für bis zu 10.000 Benutzer pro Appliance skalieren lassen. Darüber hinaus eignet sich SonicWall Email Security als virtuelle Appliance oder Software-Anwendung perfekt für Organisationen, bei denen Flexibilität und Agilität im Zuge der Virtualisierung eine große Rolle spielen. Die Lösung kann im Hochverfügbarkeits- bzw. Split-Modus konfiguriert werden, um die Anforderungen großer Implementierungen zentral und effektiv zu erfüllen.

Die E-Mail-Sicherheitslösung von SonicWall verwendet Technologien wie Advanced Reputation Management, Advanced Content Management, Adversarial Bayesian Filtering und einen Support-Vector-Machine-Algorithmus, um soliden Schutz vor ein- und ausgehenden Bedrohungen zu garantieren.

- Integration mit Multi-Engine Capture ATP-Sandbox
- Mehrere AV-Engines: SonicWall Capture Labs, McAfee®, Kaspersky™ und Cyren
- Konfigurierbare Einstellungen wie Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) und Domain-based Message Authentication, Reporting & Conformance (DMARC)
- Reputationsprüfung nicht nur der IP-Adresse des Absenders, sondern auch von Betreff und Inhalt der Nachricht sowie von eingebetteten Links und Anhängen
- Nahtlose Integration mit Office 365
- Add-On für Verschlüsselung und Compliance

Die Email Security-Lösung lässt sich intuitiv, schnell und einfach verwalten. Dabei können Sie die Spamverwaltung problemlos an die Endbenutzer delegieren und dabei trotzdem die volle Kontrolle über die Sicherheitsfunktionen behalten. Dank der nahtlosen Multi-LDAP-Synchronisierung ist die Verwaltung von Benutzer- und Gruppenkonten ein Kinderspiel. Die Lösung bietet außerdem eine einfache Integration für Office 365, um raffinierte E-Mail-Bedrohungen abzuwehren.

Bei großen verteilten Umgebungen können Sie dank Mandantenfähigkeit Subadministratoren einsetzen, um die Einstellungen in mehreren Organisationseinheiten (wie z. B. Unternehmensabteilungen oder MSP-Kunden) innerhalb einer einzigen Email Security-Implementierung zu verwalten.

SonicWall Hosted Email Security Service

Vertrauen Sie auf gehostete Services, die sich schnell bereitstellen und leicht verwalten lassen, um Ihre Organisation vor E-Mail-basierten Bedrohungen wie Ransomware, Zero-Day-Bedrohungen, Spear Phishing und BEC zu schützen und gleichzeitig E-Mail-Compliance-Richtlinien und gesetzliche Vorgaben einzuhalten. Da physische und virtuelle Appliances mit identischen Features ausgestattet sind, erhalten Sie mit unserer gehosteten Lösung den gleichen erweiterten Schutz vor E-Mail-Bedrohungen. SonicWall™ Hosted Email Security bietet erstklassigen Cloud-basierten Schutz vor ein- und ausgehenden Bedrohungen – und das zu erschwinglichen, kalkulierbaren und flexiblen monatlichen oder jährlichen Abonnementkosten. Gleichzeitig können Sie den vorab fälligen Kosten- und Zeitaufwand für die Implementierung sowie die laufenden Verwaltungskosten minimieren.

SonicWall bietet VARs und MSPs jetzt eine bessere Möglichkeit, wettbewerbsfähig zu bleiben, ihre Umsätze zu steigern und gleichzeitig Risiken, Verwaltungsaufwand und laufende Kosten zu minimieren. SonicWall Hosted Email Security umfasst MSP-freundliche Features wie z. B. flexible Kaufoptionen, automatisiertes Provisioning, Office 365-Integration und Funktionen für die zentrale Verwaltung mehrerer Abonnenten. Mit SonicWall Hosted Email Security profitieren VARs und MSPs von einer gehosteten E-Mail-Sicherheitslösung eines führenden Sicherheitsanbieters.

Weitere Informationen über die E-Mail-Sicherheitsprodukte von SonicWall erhalten Sie unter: www.sonicwall.com/de-de/products/secure-email.

SONICWALL®

Sicherheitsmanagement, Reporting und Analysen

SonicWall ist überzeugt, dass ein vernetzter Ansatz beim Sicherheitsmanagement nicht nur essentiell für gute präventive Sicherheitspraktiken ist, sondern auch die Grundlage für eine einheitliche Security-Governance-, Compliance- und Risikomanagement-Strategie bildet. Mit den Management-, Reporting- und Analyselösungen von SonicWall profitieren Organisationen von einer integrierten, geschützten und erweiterbaren Plattform, um über ihre kabelgebundenen, drahtlosen und mobilen Netzwerke hinweg eine starke, einheitliche Strategie zur Abwehr und Reaktion auf Sicherheitsbedrohungen zu realisieren. Organisationen, die sich voll und ganz für eine solche gemeinsame Plattform entscheiden, profitieren von wertvollen Erkenntnissen rund um die Sicherheit. Auf diese Weise können sie fundierte Entscheidungen treffen und schnell handeln, um Zusammenarbeit, Kommunikation und Wissen im gemeinsamen Sicherheitsframework voranzutreiben.

SonicWall Global Management System

Anders als bei einem weniger effizienten gerätebasierten isolierten Ansatz lassen sich mit der SonicWall Global Management System (GMS)-Lösung Netzwerksicherheitsoperationen einheitlich auf Geschäftsprozesse und Servicelevel abstimmen. Mit der als Software oder virtuelle Appliance verfügbaren GMS-Lösung können Organisationen jeder Größe und Art die Verwaltung ihrer Sicherheitsappliances unkompliziert konsolidieren, Verwaltung und Fehlerbehebung vereinfachen und alle betrieblichen Aspekte der Sicherheitsinfrastruktur föderieren. Unter anderem bietet GMS zentralisierte Richtlinienverwaltung und -durchsetzung, Echtzeit-Ereignisüberwachung, granulare Datenanalysen und Berichte sowie Audit-Trails über eine einheitliche Enterprise-Plattform.

Dank Workflow-Automatisierung können Organisationen mit GMS zudem auch alle Änderungen an ihren Firewalls effektiv verwalten. Dieser interne, automatisierte Prozess ermöglicht es, eine strenge Vorgehensweise für die Konfiguration, den Vergleich, die Validierung, die Prüfung und die Genehmigung von Regeln vor der Implementierung durchzusetzen. Auf diese Weise werden die Richtigkeit und Einhaltung von Regeländerungen sichergestellt. Die Freigabegruppen sind flexibel. Sie erlauben die Einhaltung unternehmenseigener Sicherheitsregeln sowie die rechtzeitige Implementierung geeigneter Firewall-Regeln entsprechend den neuesten Compliance-Vorgaben.

SonicWall Cloud GMS

Cloud GMS ist eine offene, skalierbare Cloud-basierte Sicherheitsmanagement-, Überwachungs-, Reporting- und Analyseplattform, die sich kosteneffizient als Software-as-a-Service (SaaS) bereitstellen lässt. Sie ist für Organisationen jeder Größe und für die unterschiedlichsten Anwendungsszenarien ausgelegt – auch für verteilte Unternehmen und Serviceprovider, die sich aufgrund der Kosteneffizienz für Cloud-Computing entscheiden. Cloud GMS ist die ideale Cloud-basierte Sicherheitsmanagement-Plattform, um nachhaltige, aufeinander abgestimmte Sicherheitsmaßnahmen über alle Netzwerke hinweg umzusetzen.

Kunden profitieren mit Cloud GMS von ultimativer Transparenz und Flexibilität und können das gesamte SonicWall Network Security-Ökosystem schneller, gezielter und genauer verwalten – und zwar standortunabhängig und von einem zentralen Ort aus. Mit einer unternehmensweiten Sicht auf die Sicherheitsumgebung und Echtzeit-Sicherheitsdaten für die zuständigen Mitarbeiter können Organisationen die richtigen Entscheidungen für Sicherheitsregeln und -kontrollen treffen und ihr Sicherheitskonzept stärken.

Serviceprovidern erleichtert Cloud GMS die Verwaltung der einzelnen Sicherheitsprozesse für mehrere Clients. Mit Cloud GMS können MSP/MSSPs die Flexibilität ihrer Sicherheitsservices steigern und gleichzeitig die Betriebskosten und den Aufwand für Infrastrukturen reduzieren, die sich in ihrem alleinigen Besitz befinden.

SonicWall Analyzer

Analyzer ist ein benutzerfreundliches webbasiertes Analyse- und Reporting-Tool zur Überwachung des Anwendungsverkehrs, das aktuelle und historische Daten zum Zustand sowie zur Performance und Sicherheit des Netzwerkes liefert. Das Tool unterstützt SonicWall Firewalls und Secure Mobile Access-Geräte und nutzt Analysedaten zum Anwendungsverkehr, um Berichte zu Security Events zu erstellen. Mit dem Analyzer-Tool profitieren Unternehmen jeder Größe von einer höheren Produktivität, einer besseren Bandbreitennutzung und einem optimierten Sicherheitsbewusstsein. Analyzer ist als Windows-Anwendung sowie als virtuelle Appliance verfügbar.

Weitere Informationen zu den Management- und Reporting-Produkten von SonicWall erhalten Sie unter: www.sonicwall.com/de-de/products/firewalls/management-and-reporting.

SONICWALL®

SonicWall Enterprise Services

Setzen Sie Ihre SonicWall Network Security-Lösung noch besser ein und erhalten Sie in jeder Situation den Support den Sie benötigen – rechtzeitig und zuverlässig. Mit dem Enterprise Support und den Professional Services von SonicWall holen Sie langfristig garantiert mehr aus Ihrer Lösung heraus.

Global Support Services

Holen Sie sich Unterstützung, damit Ihr Geschäft reibungslos läuft:

Technischer Support

- **8/5** – Montag bis Freitag von 8.00 bis 17.00 Uhr für nicht kritische Umgebungen.
- **7/24** – Unterstützung rund um die Uhr (einschließlich an Wochenenden und Feiertagen) für geschäftskritische Umgebungen.

Value-add-Support

- Mit **Premier Support** erhalten Unternehmen einen dedizierten Technical Account Manager (TAM) für ihre IT-Umgebung. Ihr TAM agiert als vertrauenswürdiger Berater in Ihrem Auftrag. Er arbeitet mit Ihren Mitarbeitern zusammen, um ungeplante Ausfallzeiten zu minimieren, IT-Prozesse zu optimieren, Betriebsberichte bereitzustellen und so für effizientere Prozesse zu sorgen. Darüber hinaus ist er Ihr zentraler Ansprechpartner und sorgt für ein nahtloses Support-Erlebnis.
- Mit einem **Dedicated Support Engineer (DSE)** steht Ihnen ein konkreter Support-Techniker für Ihre Enterprise-Umgebung zur Seite. Ihr DSE macht sich mit Ihrer IT-Umgebung, Ihren Regeln und Richtlinien sowie Ihren IT-Zielen vertraut, um im Bedarfsfall technische Probleme schnell zu lösen.

Global Professional Services

Sie benötigen Unterstützung, um die beste Sicherheitslösung für Ihr Unternehmen zu finden und diese anschließend in Ihrer bestehenden Infrastruktur einzurichten? Lassen Sie uns das für Sie übernehmen. Mit Global Professional Services erhalten Sie einen zentralen Ansprechpartner für all Ihre Implementierungs- und Integrationsanforderungen. Wir unterstützen Sie mit maßgeschneiderten, speziell auf Ihre individuelle IT-Umgebung abgestimmten Services und unterstützten Sie in den folgenden Bereichen:

- **Planung:** Analyse Ihrer Firewall-Anforderungen
- **Implementierung/Bereitstellung:** Bewertung und Bereitstellung Ihrer Lösung
- **Wissensvermittlung:** Nutzung, Verwaltung und Wartung Ihrer Lösung
- **Migration:** Minimierung von Unterbrechungen und Gewährleistung der Business-Continuity

Die SonicWall Enterprise Services sind für die SuperMassive/NSAs/TZ Series/ SRA/SMA/Email Security/GMS-Lösungen verfügbar.

Weitere Informationen erhalten Sie unter: https://www.sonicwall.com/de-de/support.

Fazit

Mehr Informationen über die Sicherheitsprodukte von SonicWall

Integrieren Sie Ihre Hardware, Software und Services für einen erstklassigen Schutz. Weitere Informationen erhalten Sie unter www.sonicwall.com/de-de/customers/contact-sales. Mehr zu unseren Kauf- und Upgrade-Optionen finden Sie unter www.sonicwall.com/how-to-buy. Außerdem können Sie die SonicWall-Lösungen selbst unter www.sonicwall.com/trials ausprobieren.

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
1033 McCarthy Blvd
Milpitas, CA 95035

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com