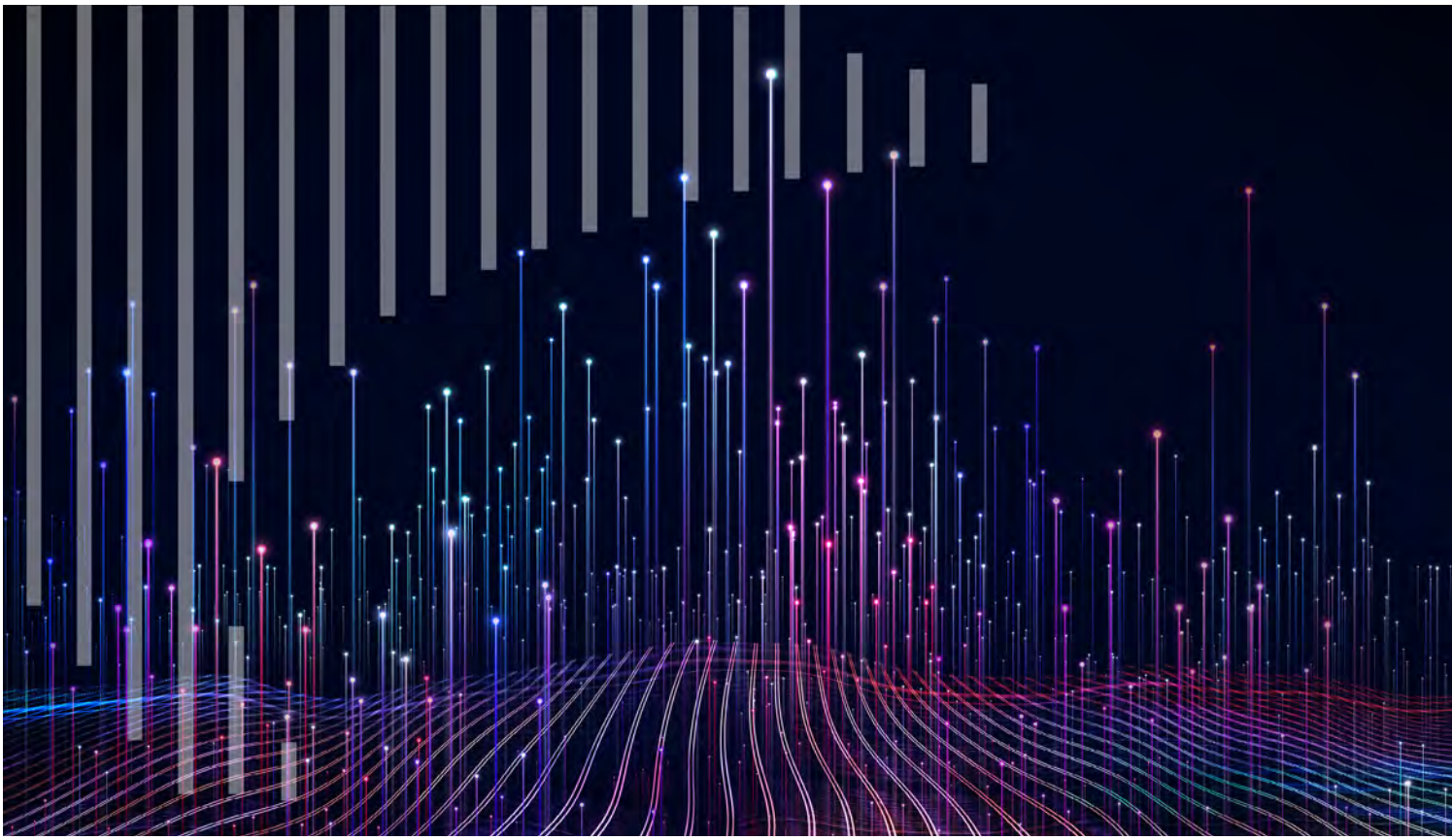
SonicWall-Produktüberblick

Juni 2022



Überblick

Für Organisationen ist es extrem wichtig, ihre öffentlichen/privaten Clouds, Anwendungen, Benutzer und Daten möglichst effizient zu schützen, ohne dabei die Netzwerkleistung zu beeinträchtigen. Die SonicWall Capture Cloud Platform ermöglicht eine enge Integration von Sicherheits-, Verwaltungs- und Analysefunktionen sowie Echtzeitinformationen zu Bedrohungen über das komplette SonicWall-Portfolio an Netzwerk-, Wireless-, E-Mail-, Mobile-, Web- und Cloud-Security-Produkten hinweg. So können kleine und mittlere Firmen, große Unternehmen, öffentliche Einrichtungen, Einzelhändler, Serviceprovider sowie Organisationen aus den Bereichen Bildung und Gesundheitswesen unser umfassendes Sicherheitsökosystem nutzen und gleichzeitig von der Leistung, Agilität und Skalierbarkeit der Cloud profitieren.

Mit der Capture Cloud Platform verfolgen wir die Strategie und die Vision, kontinuierlich Innovationen voranzutreiben und containerisierte As-a-Service-Sicherheitsanwendungen zu entwickeln, die sich spielend leicht programmieren und on demand bereitstellen lassen. Sie umfasst im Wesentlichen die folgenden zentralen Komponenten und Funktionen:

- Netzwerksicherheit
- Sicherheit in kabelgebundenen Netzwerken
- Wireless-Sicherheit
- Endpoint-Security
- WAN-Beschleunigung
- Erweiterte Sicherheitsdienste
- Cloud App Security
- Cloud Edge Secure Access
- Secure Mobile Access
- E-Mail-Sicherheit
- Sicherheitsmanagement, Reporting und Analysen
- Professional Services und Support

Gemeinsam ergeben sie eine geschäftskritische mehrschichtige Cybersicherheitslösung, die neben Bedrohungsinformationen, Analysen und Kollaborationstools auch Management-, Reporting- und Analytics-Funktionen umfasst, die perfekt aufeinander abgestimmt sind.

Netzwerksicherheit

SonicWall ist einer der führenden Anbieter von Next-Generation-Firewalls (NGFWs). Die SonicOS- oder SonicOSX-Firmware bildet das Herzstück jeder Next-Generation-Firewall von SonicWall. SonicOS basiert auf unserer skalierbaren Hardware-Architektur sowie unserer patentierten Real-Time Deep Memory Inspection(RTDMI™)-Technologie und unserer ebenfalls patentierten Reassembly-Free Deep Packet Inspection®(RFDPI)-Single-Pass-Engine, die den gesamten Verkehr unabhängig von Port oder Protokoll prüfen und die Latenzzeiten auf ein Minimum begrenzen.

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 RFDPI-Single-Pass-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 von wachsenden und dezentralen Unternehmensnetzwerken und von Datencentern anpassen.

Die Next-Generation-Firewalls von SonicWall bieten eine Reihe zuverlässiger Funktionen, wie zum Beispiel:

- Capture ATP, eine cloudbasierte Multi-Engine-Sandbox
- SD-WAN
- REST-APIs
- Entschlüsselung und Prüfung von verschlüsseltem Verkehr
- Intrusion-Prevention-Service (IPS)
- Malware-Schutz
- Application-Intelligence, Anwendungskontrolle und Echtzeitvisualisierung
- Website-/URL-Filterung (Content-Filterung)
- Virtual Private Networking (VPN) über SSL oder IPSec
- Wireless-Sicherheit
- Sicherheit für Hybrid-Cloud- und Multi-Cloud-Umgebungen
- Stateful Failover/Failback

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

SonicWall Network Security services platform (NS*sp*) Series

Die SonicWall NS*sp* Series bietet großen Netzwerken höchste Skalierbarkeit, Zuverlässigkeit und Sicherheit bei Multi-Gigabit-Geschwindigkeiten.

Nach umfassenden und wiederholten Tests mit einer 100%igen Erkennungsrate und ohne eine einzige Falschmeldung bescheinigte ICSA Labs den SonicWall-Firewalls in den letzten fünf Quartalen in Folge eine überragende Effektivität. Die Firewalls von SonicWall setzen Maßstäbe bei der High-Performance-Anwendungskontrolle und Bedrohungsabwehr in den unterschiedlichsten Implementierungsszenarien – angefangen bei kleinen Unternehmen bis hin zu großen Datencentern, Netzbetreibern und Serviceprovidern.

Unsere High-End-NS*sp*-Multi-Instance-Firewall etwa bietet die hohe Servicequalität und unterbrechungsfreie Netzwerkverfügbarkeit und Konnektivität, die heute von Unternehmen, Behörden, Serviceprovidern und Universitäten mit 100-/40-/10-GBit/s-Infrastrukturen erwartet wird. Die NS*sp* Series nutzt innovative Deep-Learning-Sicherheitstechnologien in der SonicWall Capture Cloud Platform und bietet so einen bewährten Schutz vor den ausgeklügeltsten Bedrohungen, ohne Abstriche bei der Performance zu machen.

Unified Policy mit SonicOSX 7

Das Unified-Policy-Management-Feature in SonicOSX 7 ermöglicht eine integrierte Verwaltung von Zugriffs- und Sicherheitsregeln über bestimmte High-End-NS*sp*-Firewalls und virtuelle NS*v*-Firewalls von SonicWall hinweg.

Bei der neuen Web-Oberfläche wurde ein komplett anderer Ansatz gewählt. Der Fokus liegt hier auf einem User-first-Design, das ein intuitiveres Set-up kontextbezogener Sicherheitsregeln über praktische Warnmeldungen und durch einfaches Klicken gestattet.

Auch visuell macht das Design mehr her als die klassische Oberfläche. In einer zentralen Firewall-Ansicht erhält der Nutzer Informationen zur Effektivität verschiedener Sicherheitsregeln. Hier besteht die Möglichkeit, die vordefinierten Regeln für Gateway-Anti-Virus, Anti-Spyware, Content-Filterung, Intrusion-Prevention, Geo-IP-Filter und Deep-Packet-Inspection-Prüfung des verschlüsselten Datenverkehrs ganz unkompliziert anzupassen.

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

SONICWALL®

Mit dieser neuen Unified-Policy-Oberfläche bietet SonicWall eine optimierte Erfahrung: Verantwortliche können schneller auf dynamische Traffic-Änderungen reagieren und profitieren insgesamt von einer besseren Sicherheit.

SonicWall Network Security appliance (NS*a*) Series

Die SonicWall Network Security appliance (NS*a*) Series ist eine der sichersten und leistungsstärksten Next-Generation-Firewalls ihrer Klasse. Sie gewährleistet Business-Class-Sicherheit ohne Abstriche bei der Performance und basiert auf derselben Architektur wie die NS*sp* Series – das Flaggschiff unserer Next-Generation-Firewalls –, die für die anspruchsvollsten Unternehmensnetzwerke weltweit entwickelt wurde.

Nach jahrelanger Forschung und Entwicklung wurde die NS*a* Series von Grund auf für verteilte Unternehmen, kleine bis mittelgroße Firmen, Filialen, Bildungseinrichtungen und Behörden konzipiert. Die NS*a* Series kombiniert eine revolutionäre Multicore-Architektur mit cloudbasierter Real-Time Deep Memory Inspection(RTDMI)-Technologie, einer patentierten ultraskalierbaren Engine für die Bedrohungsabwehr. Sie gewährleistet beispiellose Sicherheit, Leistung und Skalierbarkeit und bietet im Vergleich zu anderen führenden Firewall-Herstellern eine hohe Anzahl gleichzeitiger Verbindungen, geringe Latenzzeiten und die meisten Verbindungen pro Sekunde – 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), Einzelhändler, Behörden sowie dezentrale Unternehmen mit Remote-Sites und Filialen konzipiert wurden. Mit ihren äußerst wirksamen Anti-Malware-, Intrusion-Prevention-, Content-/URL-Filtering- und Anwendungskontrollfunktionen für kabelgebundene und drahtlose Netzwerke setzt sich die TZ Series klar von Produkten für den Consumer-Bereich ab. Darüber hinaus bietet sie umfassende Unterstützung für mobile Plattformen wie Laptops, Smartphones und Tablets. 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 und Anwendungskontrolle, detaillierte Analysen und Berichte zum Anwendungsverkehr, Internet Protocol Security (IPsec) und SSL-VPN, mehrfaches ISP-Failover, Lastverteilung und SD-WAN. Dank optionaler integrierter Power-over-Ethernet(PoE)- und Highspeed-802.11ac-Wireless-Technologien können Organisationen ihre Netzwerkgrenzen sicher und einfach erweitern. In Kombination mit den SonicWall-Switches und der einfachen vollautomatischen Implementierung sorgen die TZ-Firewalls dafür, dass Unternehmen sicher und flexibel wachsen können – ohne dabei die Komplexität zu erhöhen.

Bei den TZ-Firewalls der neuesten Generation handelt es sich um die ersten Firewalls mit Desktop-Formfaktor, die Multi-Gigabit(2,5-/5-/10-G)- oder Gigabit-Schnittstellen, sicheres SD-WAN, einen integrierten und erweiterbaren Speicher, TLS-1.3- und 5G-Unterstützung und gleichzeitig eine extrem hohe Performance bieten. Weitere Vorteile sind eine redundante Stromversorgung sowie Unterstützung für 802.11ac Wave 2. Für mittlere Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, bietet die neue Generation der TZ-Firewalls bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.

SonicWall Network Security virtual (NS*v*) Series

Die SonicWall Network Security virtual (NS*v*)-Firewalls nutzen Funktionen für die automatisierte Erkennung und Prävention von Sicherheitslücken in Hybrid- und Multi-Cloud-Umgebungen mit virtualisierten Versionen der SonicWall-Next-Generation-Firewalls. Ausgestattet mit den gleichen umfassenden Sicherheitstools und -services wie eine SonicWall-Firewall, schützt die NS*v* Series Ihre virtuellen und Cloud-Umgebungen effektiv vor Ressourcenmissbrauch, Cross-VM-Angriffen, Side-Channel-Angriffen sowie allen gängigen Netzwerk-Exploits und -Bedrohungen.

Die NS*v* lässt sich einfach in einer mandantenfähigen virtuellen Umgebung – in der Regel zwischen virtuellen Netzwerken (VNs) – implementieren und bereitstellen. Sie richtet Zugriffskontrollen ein, um die Sicherheit von Daten und virtuellen

Maschinen (VMs) zu gewährleisten, und erfasst gleichzeitig den virtuellen Datenverkehr zwischen VMs und Netzwerken für eine automatisierte Prävention von Sicherheitslücken.

Mit Infrastrukturunterstützung für eine Hochverfügbarkeitsimplementierung erfüllt die NS*v* die Software-Defined-Data-Center(SDDC)-Anforderungen an Skalierbarkeit und Verfügbarkeit. Die Firewalls lassen sich spielend leicht als virtuelle Appliances in Private-Cloud-Plattformen wie VMware ESXi, Linux KVM, Nutanix oder Microsoft Hyper-V oder in den Public-Cloud-Umgebungen AWS oder Microsoft Azure implementieren. Die NS*v* Series bietet Organisationen flexible BYOL- und PAYG-Lizenzierungsmodelle. Dabei profitieren sie von allen Sicherheitsfunktionen einer physischen Firewall sowie den operativen und wirtschaftlichen Vorteilen der Virtualisierung.

Einige NS*v*-Firewall-Modelle basieren auf SonicOSX mit Unified Policy. Verantwortliche können damit schneller auf dynamische Traffic-Änderungen reagieren und profitieren so von einer optimierten Erfahrung und einer insgesamt höheren Sicherheit.

Weitere Informationen zu den SonicWall-Firewalls finden Sie unter www.sonicwall.com/products/firewalls/.

Capture Security appliance 1000 (CSa 1000)

Um Datenschutzstandards und andere Vorschriften einzuhalten, brauchen Sie eine budgetfreundliche Plattform zur Bedrohungsanalyse, die von bösartigem Code weder erkannt noch umgangen werden kann. Bei der SonicWall Capture Security appliance (CS*a*) handelt es sich um eine On-Premises-Lösung zur Dateianalyse und Malware-Erkennung auf Basis von SonicWall Real-Time Deep Memory Inspection (RTDMI). Mit RTDMI kann CS*a* eine größere Menge an Malware schneller und effektiver identifizieren. Die geringe Rate an falsch positiven Ergebnissen verbessert die Sicherheit und das Benutzererlebnis.

Dank CS*a* können Sie verborgene Malware über unterschiedliche Dateitypen, Dateigrößen und Betriebsumgebungen hinweg analysieren und so Zero-Day-Bedrohungen zuverlässig erkennen. Die Appliance nutzt speicherbasierte Echtzeit-Prüfmethoden, um Side-Channel-Angriffe zu erkennen und zu stoppen. Sie zwingt Malware dazu, ihre Wirkmechanismen im Speicher offenzulegen. So ist sie in der Lage, die in großer Zahl vorkommenden Zero-Day- und unbekannten Bedrohungen abzuwehren. CS*a* unterstützt geschlossene Netzwerke und kann in Kombination mit den neuesten Next-Generation-Firewalls von SonicWall eingesetzt werden.

Die Implementierung geht schnell und einfach: Nutzer müssen lediglich grundlegende Netzwerk- und Reporting-Einstellungen vornehmen und festlegen, welche Geräte Zugriff bekommen – und schon können sie loslegen. Die CS*a* ist über eine IP-Adresse ansteuerbar und lässt sich daher überall implementieren, solange sie von Geräten erreicht werden kann, die Dateien zur Analyse übermitteln. Eine Implementierung ist auch in geschlossenen oder Air-Gap-Netzwerken möglich.

Sicherheit in kabelgebundenen Netzwerken

SonicWall-Switches ermöglichen Highspeed-Network-Switching mit beispielloser Performance und Manageability. Sie bieten eine hohe Portdichte, optional Power over Ethernet (PoE) sowie einen 1- oder 10-Gigabit-Durchsatz. Ideal für KMUs und Software-Defined-Branch(SD-Branch)-Netzwerke geeignet, ermöglichen sie es Unternehmen jeder Größe, die digitale Transformation voranzutreiben und mit den ständigen Änderungen in der Netzwerk- und Sicherheitslandschaft Schritt zu halten.

Die Verwaltung der SonicWall-Switches erfolgt über SonicWall-Firewalls oder Wireless Network Manager (WNM). WNM sorgt für eine nahtlose und durchgängige Sicherheit in kabelgebundenen und drahtlosen Netzwerken und ermöglicht so ein zentralisiertes Sicherheitskonzept. Dies ermöglicht eine einfachere Implementierung, Verwaltung und Fehlerbehebung und beseitigt Lücken, die bei Switches von Drittanbietern auftauchen könnten. Dank vollautomatischer Implementierung lassen sich die SonicWall-Switches im Handumdrehen über verteilte Filialen hinweg bereitstellen.

Wireless-Sicherheit

Mit seiner innovativen SonicWall Wireless Network Security-Lösung macht SonicWall den Datenaustausch in drahtlosen Netzwerken sicher, einfach und erschwinglich. Die leistungsstarken 802.11ax-Wireless-Access-Points der SonicWave Series lassen sich denkbar einfach über Wireless Network Manager verwalten.

Neben den Highspeed-Wireless-Access-Points und dem cloudbasierten Dashboard umfasst die Wireless-Security-Lösung von SonicWall auch Wi-Fi Planner, ein erweitertes Site-Survey-Tool, mit dem

Administratoren Wi-Fi-Netzwerke effektiv planen und implementieren können. Die Lösung enthält zudem die mobile SonicExpress-App, die ein einfaches Onboarding und Monitoring der Zugriffspunkte gestattet und Administratoren mit Echtzeitinformationen zu Netzwerkstatus und Sicherheit versorgt.

Unsere Lösung geht weit über gewöhnliche Wireless-Security-Produkte hinaus: Sie schützt drahtlose Netzwerke mit den RTDMI- und RFDPI-Technologien und bietet hoch entwickelte Sicherheitsfeatures wie Multi-Engine-Sandboxing, Content-Filterung und Cloud-AV direkt am Access-Point, ohne dass eine Firewall erforderlich ist. Weitere Features wie Intrusion-Prevention, TLS-/SSL-Entschlüsselung und -Prüfung und Anwendungskontrolle sorgen im Netzwerk für zusätzliche Sicherheit und gewährleisten eine hohe Performance der Enterprise-Klasse.

Die SonicWave-APs unterstützen schnelles Roaming, sodass Benutzer nahtlos zwischen verschiedenen Standorten wechseln können. Das funktionsreiche Portfolio umfasst Features für Captive Portal, automatische Kanalauswahl, Spektrumsanalyse, Airtime-Fairness, Bandsteering sowie Signalanalyse-Tools zur Überwachung und Problembehebung.

SonicWall sorgt dabei für niedrige Gesamtbetriebskosten, da die kostspielige Implementierung und Verwaltung einer separaten Wireless-Lösung parallel zum kabelgebundenen Netz entfällt.

Endpoint-Security

In heutigen Unternehmen spielen die Verwaltung und der Schutz von Endgeräten eine entscheidende Rolle. Weil zum einen ein Kommen und Gehen benutzereigener Geräte im Netzwerk herrscht und außerdem viele ungeprüfte Endpunkte von verschlüsselten Bedrohungen betroffen sind, ist es extrem wichtig, diese Geräte zu schützen. Mit der wachsenden Gefährdung durch Ransomware und Anwendungsschwachstellen stehen Endgeräte im Zentrum der heutigen Bedrohungslandschaft.

Oft haben Administratoren Schwierigkeiten mit der Visibilität und der Verwaltung ihrer Sicherheitsplattform. Weitere Herausforderungen sind die konsistente Gewährleistung der Client-Sicherheit und die Bereitstellung benutzerfreundlicher und aussagekräftiger Informationen und Berichte.

Obwohl es bereits seit Jahren Produkte für die Endpunktsicherheit gibt, tun sich Administratoren immer noch in folgenden Bereichen schwer:

- Sicherheitsprodukte auf dem neuesten Stand halten
- Umsetzung von Regeln auf globaler Ebene
- Berichte und Überblick über den Zustand der Nutzergeräte
- Bedrohungen über verschlüsselte Kanäle sowie Bedrohungen, die verschlüsselte Kanäle erzeugen
- Warnmeldungen und Problembehebung
- Katalogisieren von Anwendungen und deren Schwachstellen
- Abwehr hoch entwickelter Bedrohungen wie Ransomware
- Dateilose Angriffe und infizierte USB-Geräte, die den Perimeterschutz umgehen

SonicWall Capture Client ist eine einheitliche Client-Plattform mit zahlreichen Endpoint-Schutzfunktionen. Die Lösung verfügt über eine cloudbasierte Verwaltungskonsole und bietet eine optionale komplette Integration mit SonicWall-Next-Generation-Firewalls, die SonicWall-Kunden eine einheitliche Sicherheitserfahrung bietet. In Kombination mit Enforcement-Funktionen kann SonicWall Capture Client sicherstellen, dass auf den Endgeräten Sicherheitssoftware installiert ist bzw. dass sie über ein eingebettetes SSL-Zertifikat verfügen, um verschlüsselten Verkehr zu prüfen. Um die Prüfung von SSL-Verkehr (DPI-SSL) zu erleichtern und die Benutzererfahrung zu verbessern, ist es mit Capture Client jetzt außerdem viel leichter, SSL-Zertifikate auf Endgeräten durchzusetzen.

Darüber hinaus umfasst Capture Client eine hoch entwickelte Antiviren-Engine, die raffinierteste Malware-Attacken abwehrt und zudem eine Rollback-Option bietet, um den ursprünglichen Zustand vor der Infizierung wiederherzustellen. Capture Client Advanced lässt sich außerdem mit SonicWall Capture Advanced Threat Protection (ATP) integrieren, um verdächtige Dateien zu analysieren und so Angriffe zu stoppen, bevor sie ausgeführt werden.

Administratoren können nun alle Anwendungen auf jedem mit Capture

Client geschützten Endgerät katalogisieren und Berichte zu bekannten Schwachstellen innerhalb des Ökosystems einsehen.

Das globale Dashboard verschafft MSSPs einen Überblick über die Zahl der Infektionen, die vorhandenen Schwachstellen sowie die Capture Client-Version, die bei den einzelnen Nutzern installiert ist. Administratoren können sehen, welche Inhalte und welche Personen am meisten durch die Content-Filterung blockiert werden und welche Geräte online und in Betrieb sind. Mit der globalen Richtlinie können sie eine einzige Grundregel für alle Nutzer anwenden. Damit ist es einfacher, neue Nutzer anzulegen und Schutzmechanismen für neue Bedrohungen über alle Nutzer hinweg zu erstellen, für die diese Regel gilt.

Hier eine Auswahl der SonicWall Capture Client-Features:

- Durchsetzung von Sicherheitsmaßnahmen
- DPI-SSL-Zertifikatsverwaltung
- Kontinuierliche Verhaltensüberwachung
- Hochpräzise Bestimmungen dank maschinellem Lernen
- Mehrschichtige heuristische Techniken
- Informationen zu Anwendungsschwachstellen
- Einzigartige Rollback-Funktionen
- Integration des Netzwerk-Sandbox-Services Capture Advanced Threat Protection
- Globales Dashboard und globale Richtlinie mit Vererbung
- Abgleich verdächtiger Dateien mit der Capture ATP-Datenbank, die Informationen zu gefährlichen und vermeintlichen Bedrohungen enthält (mit nur einem Klick)
- Content-Filtering zur Umsetzung von Webregeln sowie Blockieren bösartiger IP-Adressen, URLs und Domains auf Geräten außerhalb des Netzwerks
- Regelbasierte Gerätesteuerung zum Blockieren potenziell infizierter Speichergeräte

Erweiterte Sicherheitsdienste

Die Network-Security-Firewall-Services von SonicWall ermöglichen kleinen wie großen Organisationen einen extrem effektiven, erweiterten Schutz. Damit können sie Sicherheitsbedrohungen besser abwehren, die Sicherheitskontrolle verbessern, ihre Produktivität steigern und Kosten senken.

SonicWall bietet drei Abopakete für die Firewalls der Gen-7-Series: Threat Protection Services Suite, Essential Protection Services Suite und Advanced Protection Services Suite. Die Threat Protection Services Suite enthält grundlegende Sicherheitsservices zum Schutz von Netzwerken vor Bedrohungen in einem kosteneffektiven Bundle. Das Essential-Bundle bietet essenzielle Sicherheitsdienste zum Schutz vor bekannten und unbekannten Bedrohungen, während Sie mit der Advanced-Suite die Sicherheit Ihres Netzwerks mit zusätzlichen essenziellen Cloud-Security-Services verstärken können.

Die **Threat Protection Services Suite** ist nur für die TZ 270/370/470 Series verfügbar. Sie umfasst Gateway-Anti-Virus, Intrusion-Prevention und Anwendungskontrolle, Content-Filtering-Service, Deep Packet Inspection von TLS-/SSL-verschlüsseltem Verkehr (DPI-SSL) sowie 24/7-Support.

Die **Essential Protection Services Suite** umfasst Capture Advanced Threat Protection mit RTDMI-Technologie, Gateway-Anti-Virus, Intrusion-Prevention und Anwendungskontrolle, Content-Filtering-Service, Comprehensive Anti-Spam Service, Deep Packet Inspection von TLS-/SSL-verschlüsseltem Verkehr (DPI-SSL) sowie 24/7-Support.

Die **Advanced Protection Services Suite** umfasst Capture Advanced Threat Protection mit RTDMI-Technologie, Gateway-Anti-Virus, Intrusion-Prevention und Anwendungskontrolle, Content-Filtering-Service, Comprehensive Anti-Spam Service, Deep Packet Inspection von TLS-/SSL-verschlüsseltem Verkehr (DPI-SSL), 24/7-Support, Cloud-Management, cloudbasiertes Reporting für sieben Tage sowie optionalen Premier Support.

Deep-Memory-Erkennung

Die patentierte SonicWall Real-Time Deep Memory Inspection(RTDMI)-Engine erkennt und blockiert unbekannte Massenmalware proaktiv und in Echtzeit mittels Deep Memory Inspection. Die jetzt mit dem SonicWall Capture Advanced Threat Protection(ATP)-Cloud-Sandbox-Service verfügbare Engine identifiziert und stoppt selbst die gefährlichsten modernen Bedrohungen einschließlich künftiger Meltdown-Exploits.

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Cloud App Security

SonicWall Cloud App Security schützt häufig genutzte SaaS-basierte E-Mail-, Kollaborations- und Produktivitätsanwendungen wie Office 365 E-Mail, SharePoint, OneDrive, G Suite, Dropbox und Box.
Diese Lösung bietet Schutz vor:

- Business-E-Mail-Compromise (BEC)
- Datenverlust (Data Loss Prevention, DLP)
- Feindlicher Kontoübernahme (Account Takeover, ATO)
- Hoch entwickelten Malware- und Zero-Day-Bedrohungen in schädlichen Anhängen und gespeicherten Dateien
- Gezielten Phishing-Angriffen
- Betrugsversuchen

Cloud App Security nutzt erweiterte Funktionen für User-Profiling und Verhaltensanalysen mit über 300 Bedrohungsindikatoren, um festzustellen, ob rechtmäßige Konten von Cyberkriminellen ausgenutzt werden. Mithilfe von ML- und KI-Funktionen blockiert die Lösung Impersonation-Angriffe und durchleuchtet Aktivitäten auch rückwirkend.

Bei SaaS- und Filesharing-Anwendungen wie OneDrive nutzt Cloud App Security die Multi-Engine-Sandbox von SonicWall Capture ATP, um brandneue Malware aufzuspüren. Damit lassen sich Dateien und Daten sowohl rückwirkend als auch in Echtzeit prüfen – im ruhenden Zustand oder während der Übermittlung in einer SaaS-Umgebung, intern oder von Cloud zu Cloud. Das DLP-Feature der Lösung sorgt für einen zusätzlichen Schutz gespeicherter Daten, da der Zugriff nur zugelassenen Anwendungen vorbehalten ist und unautorisierte Daten-Uploads nicht möglich sind.

Als SaaS-Service lässt sich Cloud Security innerhalb weniger Minuten aktivieren und in Betrieb nehmen. Dank unbegrenzter Skalierbarkeit können kleine wie große Organisationen sofortigen Schutz für ihre SaaS-Nutzer hinzufügen – egal ob es wenige Hundert oder Hunderttausende rund um den Globus sind. Jede SaaS-App verfügt über eine separate Policy-Engine mit jeweils eigenen Regeln und Enforcement-Funktionen. Auf diese Weise können Sie je nach Sicherheitsanforderungen für jede SaaS-Anwendung eine spezifische Regel festlegen.

Da mit Cloud App Security weder Hardware noch Software installiert und verwaltet werden muss, entfallen die Investitionskosten, die komplexe Installation und die laufenden Wartungskosten, die bei alternativen On-Prem-Lösungen gang und gäbe sind.

Weitere Informationen über SonicWall Cloud App Security finden Sie unter www.sonicwall.com/cloud-security.

Cloud Edge Secure Access

Zero-Trust-Sicherheit löst traditionelle VPN-Sicherheit ab

Heutige Mitarbeiter möchten flexibel von jedem beliebigen Ort aus arbeiten können – und Organisationen wollen von den Kosteneinsparungen und der operativen Effizienz der Cloud profitieren.

Doch traditionelle VPN-Lösungen wurden nicht für diese neue Realität konzipiert. Die Implementierung einer solchen Lösung kann mehrere Tage oder sogar Wochen dauern. Lieferengpässe könnten die Verfügbarkeit beeinträchtigen und selbst wenn Sie eine Lösung implementiert haben, lassen sich Stillstandzeiten nur schwer planen.

Schlimmer noch: Diese traditionellen Lösungen können Angreifern die Tür zu Ihrem Netzwerk öffnen. Jeder erfolgreiche Log-in ermöglicht Cyberkriminellen einen umfassenden Netzwerkzugriff einschließlich Lateral Movement innerhalb des Netzwerksubnetzes.

Und da der Nutzer-Traffic durch den lokalen VPN-Konzentrator läuft, anstatt direkt zur Cloud übermittelt zu werden, entstehen bei VPN-Lösungen Latenzzeiten, die sowohl die Effizienz als auch die Cloud-Erfahrung von Benutzern beeinträchtigen.

Prognosen von Gartner zufolge werden 60 % der Unternehmen bis 2023 einen Großteil ihrer Virtual Private Networks (VPNs) für den Remote-Zugriff gegen Zero-Trust-Network-Access (ZTNA) austauschen.

Zero-Trust-Netzwerksicherheit zum Schutz wertvoller Ressourcen

Mit Cloud Edge Secure Access bietet SonicWall eine ZTNA-Lösung, die nicht nur diese Probleme behebt, sondern auch eine Vielzahl weiterer Vorteile bietet. Herzstück von SonicWall Cloud Edge Secure Access sind drei wesentliche Funktionen:

- Least-Privilege-Zugriff zum Schutz von Unternehmensressourcen
- Schnelle Selfservice-Implementierung
- Zuverlässiger Zugriff von jedem beliebigen Ort aus direkt über die Cloud

Als cloudnativer Service bietet er eine einfache Network-as-a-Service(NaaS)-Lösung für eine Site-to-Site- und Hybrid-Cloud-Verbindung mit integrierter Zero-Trust- und Least-Privilege-Sicherheit.

- Device Posture Check (DPC) gewährt nur authentifizierten und regelkonformen Geräten einen Zugriff auf das Netzwerk
- Die Richtlinien für die softwaredefinierte Mikrosegmentierung verhindern auf effektive Weise die Ausbreitung von Sicherheitslücken
- Mit Network Traffic Control (NTC), einer Stateful-Firewall-as-a-Service(FwaaS)-Lösung, lässt sich definieren, wer von wo aus auf welche Ressourcen zugreifen darf; auf diese Weise kann ein regelbasierter Schutz realisiert werden

Organisationen können jetzt Remote-Mitarbeitern eine größere Kontrolle bieten und gleichzeitig wertvolle Unternehmensressourcen schützen.

Globaler cloudnativer Service, der sich in Minutenschnelle implementieren lässt

SonicWall Cloud Edge wird von mehr als 30 Points of Presence (PoPs) weltweit unterstützt.

IT-Manager können Filialen an das Unternehmensnetz anbinden und den globalen Service in 15 Minuten implementieren. Endbenutzer können den SonicWall Cloud Edge-Client in nur fünf Minuten installieren und produktiv einsetzen.

Die Infrastruktur basiert auf der Software-Defined-Perimeter(SDP)-Architektur. Diese trennt den zentralisierten Controller von den Gateways, die als Trust-Broker agieren.

Durch Verteilung der SDP-Gateways lässt sich Cloud Edge Secure Access schnell skalieren, was eine hohe Performance und ein bestmögliches Cloud-Erlebnis gewährleistet.

Darüber hinaus ist Cloud Edge Secure Access durch die Trennung von Funktionen immun gegenüber gängigen Cyberbedrohungen wie DDoS, Log4j-Exploits, Angriffen über öffentliche WLAN-Netze, SYN-Flood und Slowloris.

Weitere Vorteile:

- Sicherheit für dezentrale Unternehmen und mobile Mitarbeiter
- Sofortiger, sicherer Zugriff auf filialbezogene Ressourcen und weitere Informationen in Hybrid Clouds
- Umfassende Skalierung – von zehn Nutzern auf Tausende Nutzer
- Unterstützung eines clientlosen Webzugriffs über beliebige öffentliche Geräte
- Leistungsstarke WireGuard-Verschlüsselung
- Cloud-Identity-Provider- und SIEM-Integrationen
- Moderne SSO- und MFA-Integration
- SIEM-Integration
- Mandantenfähigkeit für MSSPs
- Network Traffic Control (NTC) legt fest, wer von wo aus auf bestimmte Netzwerke und Services zugreifen kann, und sorgt so für einen umfassenden Schutz auf Firewall-Ebene
- Device Posture Check (DPC) gewährt nur authentifizierten und regelkonformen Geräten einen Zugriff auf das Netzwerk
- Erhältlich in Asien, Europa, dem Nahen Osten und den USA

Weitere Informationen über SonicWall Cloud Edge Secure Access finden Sie unter www.sonicwall.com/products/cloud-edge-secure-access.

SONICWALL®

Secure Mobile Access

Die SonicWall Secure Mobile Access (SMA) Series bietet ein einheitliches, sicheres Access-Gateway, mit dem sich Herausforderungen rund um Mobilität, Home-Office-Konzepte, BYOD und Cloud-Migration erfolgreich meistern lassen. 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 -chiffren 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). Ein sicherer SSO-Zugriff wird erst dann auf autorisierten Endgeräten gewährt, nachdem der Gerätezustand und die Einhaltung von Compliance-Vorgaben geprüft wurden.

Managed-Service-Provider

Managed-Service-Providern sowie Organisationen mit Datencentern 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 mehr als eine Million Anwender nach oben skalieren. Dank Active-Active-HA-Clustering (Global High Availability) und integriertem dynamischem 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.

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 leistungsstarker Proxys eine hohe Performance sowie einen zuverlässigen und sicheren Zugriff gewährleisten. 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 und Cloud-Plattformen wie Hyper-V, VMware ESX/ ESXi, KVM, AWS und Azure. Egal, ob Sie physische Appliances, virtuelle Appliances oder eine Kombination aus beidem implementieren möchten – SMA lässt sich nahtlos in Ihre bestehende IT-Infrastruktur einbinden.

SMA Web Application Firewall

Die SonicWall SMA100 Series Web Application Firewall (WAF) setzt auf umfassende Abwehrstrategien und eine verbesserte Perimetersicherheit, um Webanwendungen in Private-, Public- oder Hybrid-Cloud-Umgebungen optimal zu schützen. Darüber hinaus bietet sie Webanwendungssicherheit und Schutz vor Informationslecks und ermöglicht gleichzeitig eine schnellere Bereitstellung von Webanwendungen mit Funktionen für Lastverteilung (einschließlich Anwendungserkennung), SSL-Offloading (mehr Resilienz) und eine verbesserte digitale Erfahrung.

Weitere Vorteile sind unter anderem:

- Schutz vor bekannten und Zero-Day-Schwachstellen mit virtuellem Patching und personalisierbaren Regeln

- Schutz vor den neuesten im OWASP aufgelisteten Schwachstellen und Bedrohungen wie SQL-Injection und Cross-Site-Scripting (XSS)
- Unterstützung eines clientlosen Zero-Trust-Zugriffs über einen Webbrowser sorgt für bequeme Nutzung über beliebige öffentliche Geräte
- Hohe Session-Management- und Authentifizierungsanforderungen wie OTP, 2FA und SSO
- Ausfallsicherer Serverschutz vor DoS-/DDoS-Angriffen auf Anwendungen

Management und Reporting

SonicWall bietet eine intuitive webbasierte Verwaltungsplattform, um das Appliance-Management zu optimieren, und stellt umfassende Reporting-Funktionen bereit. Die benutzerfreundliche Oberfläche ermöglicht eine übersichtliche Verwaltung mehrerer Appliances. Dank der zentralen Regelverwaltung können Sie Zugriffsregeln und -konfigurationen auf einfache Weise erstellen und überwachen. Dabei werden Ihre Benutzer, Geräte, Anwendungen, Daten und Netzwerke anhand einer einzigen Regelkonfiguration verwaltet. Routineaufgaben lassen sich automatisieren und Aktivitäten planen. Auf diese Weise werden Sicherheitsteams von redundanten Aufgaben befreit, sodass sie sich stattdessen auf strategische Sicherheitsaufgaben wie z. B. die Reaktion auf Vorfälle konzentrieren können.

Ihre IT-Abteilung kann so die Erwartungen der User 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 wählen oder sich für einen konventionelleren clientbasierten Full-Tunnel-VPN-Zugriff für Führungskräfte entscheiden. Egal, ob es fünf Anwender aus dem gleichen Datencenter oder Tausende von Anwendern in global verteilten Datencentern sind – SonicWall SMA ist die perfekte Lösung für einen zuverlässigen und sicheren Zugriff.

Weitere Informationen zu den Mobile-Security-Produkten von SonicWall finden Sie unter www.sonicwall.com/products/remote-access/.

E-Mail-Sicherheit

E-Mails sind extrem wichtig für Ihre Geschäftskommunikation, doch gleichzeitig sind sie auch der größte Angriffsvektor für Bedrohungen wie Ransomware, Phishing, Business-E-Mail-Compromise (BEC), Spoofing, Spam und Viren. 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 diese Daten in fremde Hände geraten. Ob es sich bei Ihrer Organisation um eine kleine oder mittelständische Firma mit Wachstumspotenzial, ein großes dezentrales Unternehmen 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.

Immer mehr Organisationen setzen auf Microsoft Office 365 und Google G Suite, um Kosten und Ressourcen effektiv zu managen. Diese Produkte enthalten zwar integrierte Sicherheitsfunktionen, doch um hoch entwickelte E-Mail-

Bedrohungen wirklich abwehren zu können, benötigen Organisationen eine E-Mail-Sicherheitslösung der nächsten Generation, die sich nahtlos mit Office 365 und G Suite 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 virtuelle 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 ist SonicWall Email Security als virtuelle Appliance oder Softwareanwendung erhältlich – ideal für Organisationen, die sich die Flexibilität und Agilität der Virtualisierung zunutze machen möchten. Die Lösung kann im Hochverfügbarkeits- bzw. Split-Modus konfiguriert werden, um die Anforderungen großer Implementierungen zentral und effektiv umzusetzen.

Unsere E-Mail-Security-Lösung setzt modernste Technologien wie maschinelles Lernen, heuristische Techniken, Reputations- und Inhaltsanalysen, Time-of-Click-URL-Schutz sowie Sandboxing für Anhänge und URLs ein, um eine umfassende Abwehr von ein- und ausgehenden Bedrohungen sicherzustellen.

Die Lösung umfasst außerdem effiziente E-Mail-Authentifizierungsstandards – wie etwa Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) und Domain-based Message Authentication, Reporting und Conformance (DMARC) –, um Spoofing-Angriffe und E-Mail-Betrug zu stoppen.

- Abwehr hoch entwickelter Bedrohungen, bevor sie im Posteingang landen
- Schutz vor E-Mail-Betrug und gezielten Phishing-Angriffen
- Echtzeitinformationen zu Bedrohungen für topaktuelle Sicherheit
- Schutz für Cloud-E-Mail-Service (Office 365, G Suite)
- Schutz vor Datenverlust bei E-Mails und Einhaltung von Compliance-Vorgaben
- Einfaches Management und Reporting
- Flexible Implementierungsoptionen

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 und G Suite, 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

Mit gehosteten Services, die sich schnell bereitstellen und leicht verwalten lassen, können Sie Ihre Organisation vor E-Mail-Bedrohungen wie Ransomware, Zero-Day-Angriffen, Spear-Phishing und BEC schützen und gleichzeitig E-Mail-Compliance-Richtlinien und gesetzliche Vorgaben einhalten. Da physische und virtuelle Appliances mit identischen Features ausgestattet sind, erhalten Sie mit unserer gehosteten Lösung den gleichen erweiterten Schutz vor E-Mail-Bedrohungen. Darüber hinaus sorgt die Lösung für eine zuverlässige E-Mail-Kontinuität. Dies gewährleistet, dass E-Mails immer zugestellt werden und die Produktivität bei planmäßigen oder unvorhersehbaren Ausfällen lokaler E-Mail-Server bzw. bei Ausfällen eines Cloud-Providers wie Office 365 und G Suite nicht beeinträchtigt wird.

SonicWall Hosted Email Security bietet erstklassigen cloudbasierten 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 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 etwa robuste Mandantenfähigkeit, flexible Kaufoptionen, automatisiertes Provisioning, Office-365-Integration und Funktionen für die zentrale Verwaltung mehrerer Abonnenten.

Weitere Informationen zu den SonicWall Email Security-Produkten finden Sie unter www.sonicwall.com/de-de/products/secure-email.

Sicherheitsmanagement, Reporting und Analysen

SonicWall ist überzeugt, dass ein vernetzter Ansatz beim Sicherheitsmanagement nicht nur essenziell für gute präventive Sicherheitspraktiken ist, sondern auch die Grundlage für eine einheitliche Security-Governance-, Compliance- und Risikomanagement-Strategie bildet. Die Management-, Reporting- und Analyselösungen von SonicWall bieten Organisationen eine integrierte, sichere und erweiterbare Plattform, mit der sie über ihre kabelgebundenen, drahtlosen und Multi-Cloud-Netzwerke hinweg eine robuste und einheitliche Strategie definieren können, um Sicherheitsbedrohungen abzuwehren und angemessen darauf zu reagieren. Organisationen, die sich voll und ganz für eine solche gemeinsam genutzte Plattform entscheiden, profitieren außerdem von wertvollen sicherheitsrelevanten Erkenntnissen. Auf diese Weise können sie fundierte Entscheidungen treffen und schnell handeln, um Zusammenarbeit, Kommunikation und Know-how im gemeinsamen Sicherheitsframework zu fördern.

SonicWall Network Security Management

SonicWall Network Security Manager (NSM) bietet Ihrer Organisation alles, was sie für ein einheitliches Firewall-Management-System braucht. Dank einer umfassenden Transparenz auf Benutzerebene, einer gruppenbasierten Gerätesteuerung und einer unbegrenzten Skalierbarkeit können Sie Ihre SonicWall-Netzwerksicherheitsprozesse zentral bereitstellen und verwalten.

Dazu gehören die Implementierung und Verwaltung aller Firewall-Appliances, Gerätegruppen und Nutzer, die Orchestrierung und Durchsetzung einheitlicher Konfigurationen und Sicherheitsrichtlinien in Ihren SD-Branch- und SD-WAN-Umgebungen sowie eine umfassende Überwachung mit detaillierten Berichten und Analysen über ein dynamisches Dashboard. Besonders praktisch: Mit NSM können Sie all diese Aufgaben über eine einzige anwenderfreundliche cloudnative Konsole erledigen, auf die Sie von jedem Ort aus über beliebige browserfähige Geräte zugreifen können.

Serviceprovidern bietet NSM eine umfassende Verwaltung mehrerer Nutzer sowie eine unabhängige, getrennte Richtlinienkontrolle für alle verwalteten Nutzer. Diese Trennung betrifft alle Management-Features und -Funktionen von NSM, die den Firewall-Betrieb für die einzelnen Anwender regeln. Auf diese Weise können Sie für jeden Nutzer eine Reihe eigener User, Gruppen und Rollen einrichten, um die Gerätegruppenverwaltung, Richtlinien-Orchestrierung und alle anderen administrativen Aufgaben im Rahmen des zugewiesenen Nutzerkontos durchzuführen.

SonicWall Analytics

Mit SonicWall Analytics werden aus Daten Entscheidungen und Maßnahmen, um Sicherheitsprobleme zu lösen und ein erneutes Auftreten zu verhindern.

Dieser robuste Traffic-Monitoring- und -Analyse-Service ermöglicht einen detaillierten Überblick über sämtliche Aktivitäten innerhalb der Netzwerksicherheitsumgebung. Die informationsgestützte Analyse-Engine aggregiert, normalisiert und kontextualisiert Sicherheitsdaten (etwa zum Netzwerkverkehr und den Benutzeraktivitäten), die durch die Firewall und die Wireless-Access-Points fließen. So gewinnen Administratoren nahezu in Echtzeit einen direkten Einblick in die Bedrohungsinformationen zu ihren Netzwerken und Usern.

Dank dieser aussagekräftigen Analysedaten und Berichte verfügen Organisationen über die

[1] NSM SaaS enthält Reporting- und Analyse-Features.
[2] NSM On-Prem erfordert eine separate Installation von SonicWall Analytics On-Prem sowie eine Lizenz für die Reporting- und Analyse-Features.

Erkenntnisse und Fähigkeiten, um sicherheitsbezogene und operative Probleme effizienter zu identifizieren und zu beheben. Sicherheitsteams können durch Drill-down-Funktionen relevante Daten untersuchen und analysieren sowie im Fall von verdächtigen oder riskanten Benutzeraktivitäten und Verhaltensweisen evidenzbasierte Maßnahmen präziser, schneller und mit größerer Transparenz einleiten. Gleichzeitig können sie ihre wertvolle Zeit dazu nutzen, schnelle Reaktionen und Maßnahmen zur Lösung der wichtigsten Sicherheitsrisiken zu orchestrieren, anstatt auf jedes einzelne Ereignis reagieren zu müssen.

Die Integration von Analytics in die Geschäftsprozesse ermöglicht außerdem eine Automatisierung aussagekräftiger Warnmeldungen in Echtzeit, eine proaktive und automatisierte Orchestrierung von Sicherheitsrichtlinien und -kontrollen und eine Überwachung der Ergebnisse zur Gewährleistung der Sicherheit. Auf diese Weise lassen sich Analysen besser operationalisieren.

SonicWall Wireless Network Manager

SonicWall Wireless Network Manager (WNM) integriert die gemeinsame Verwaltung von SonicWave-Access-Points und SonicWall-Switches. Als Teil des SonicWall Capture Security Center-Ökosystems ermöglicht WNM eine hohe Transparenz und eine zentrale Verwaltung über kabelgebundene und drahtlose Netzwerke hinweg.

Der cloudbasierte und nutzerfreundliche WNM vereinfacht den Zugriff, die Kontrolle und das Troubleshooting über ein zentrales Dashboard. Mit WNM können Administratoren einzelne Regeln auf Benutzerebene erstellen und auf verschiedene Standorte und Zonen anwenden oder durch einen Drill-down auf verwaltete Geräte detaillierte Daten aufrufen. WNM ist umfassend skalierbar und lässt sich für einen einzigen Standort oder auch für globale Unternehmensnetzwerke mit Zehntausenden verwalteter Geräte einsetzen.

Vor der Implementierung des Access-Points kann ein Wireless-Site-Survey dabei helfen, eine möglichst hohe Performance und Produktivität sicherzustellen. Das in WNM integrierte Wi-Fi-Planner-Tool ermöglicht die strategische Implementierung von Access-Points, um die Wi-Fi-Benutzererfahrung zu verbessern und kostspielige Fehler zu vermeiden.

Mittels vollautomatischer Implementierung lassen sich die SonicWave-Access-Points und SonicWall-Switches über die mobile SonicExpress-App in nur wenigen Minuten automatisch bereitstellen. Das Provisioning lässt sich spielend leicht auch remote durchführen, was Zeit und Geld spart.

Durch automatische Firmware- und Sicherheitsupdates bleiben verwaltete Geräte immer auf dem neuesten Stand. Da bei einem Internetausfall die Access-Points und Switches ohne WNM weiterlaufen können, ist die Business-Continuity jederzeit gewährleistet.

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

Professional Services und Support

Setzen Sie Ihre SonicWall-Netzwerksicherheitslösung 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 08:00 bis 17:00 Uhr für nicht kritische Umgebungen
- **24/7** – 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 eigener 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 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 NS*sp*/NS*a*/TZ Series sowie SMA/Email Security/GMS verfüg-bar.

Erfahren Sie mehr dazu:
www.sonicwall.com/en-us/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.de. 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 SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

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

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, Kalifornien 95035, USA

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