LÖSUNGSPROFIL

SonicWall Secure SD-Branch

Neudefinition der Sicherheit für Filialen

Zusammenfassung

SonicWall SD-Branch ist die Neudefinition der Filialen-Konnektivität. Die SonicWall SD-Branch Lösung sichert die Konnektivität und transformiert die Benutzererfahrung in den Filialen von verteilten Unternehmen durch die Bereitstellung einer integrierten Plattform, die SD-LAN, SD-WAN und Sicherheit kombiniert. Diese Plattform ermöglicht den Filialen, für die Konnektivität mit dem Unternehmenssitz und mit anderen Filialen günstigere Verbindungen zu nutzen, BYOD zu aktivieren, SaaS-Anwendungen einzusetzen und ihre Lösung problemlos im Einklang mit der steigenden Anzahl mobiler Geräte zu skalieren. SD-Branch erlaubt eine rasche Einbindung mittels Zero-Touch Deployment und ermöglicht einheitliche Transparenz und Bedrohungsschutz über eine zentrale Benutzeroberfläche. Zugleich vereinfacht diese End-to-End Security-Lösung die Implementierung und Fehlerbehebung.

Einführung

Wie in unserem Lösungsprofil dargestellt, sind herkömmliche Methoden zur Bereitstellung und Aufrechterhaltung von Sicherheit in Filialen unwirksam, zu teuer und unüberschaubar geworden. Für verteilte Unternehmen ist die Sicherung ihrer Filialen aufgrund der steigenden Anzahl potentieller Schwachstellen, begrenzter Ressourcen und steigender Kosten oft eine große Herausforderung. Dies trägt letztendlich zu einer wachsenden Cybersicherheitslücke im Unternehmen bei.

SonicWall sieht SD-Branch als Eckpfeiler für die grenzenlose Sicherheit in unserem hyperverteilten Zeitalter. Eine effektive Lösung kombiniert die Agilität von SD-Branch mit End-to-End-Sicherheit, Netzwerksegmentierung und Compliance. Dies ermöglicht die Durchsetzung einheitlicher Regeln im gesamten Netzwerk-Ökosystem und bietet granulare Sicherheitskontrollen zur Erkennung und Verhinderung von komplexen und noch nie dagewesenen Attacken, bevor diese Ihr Netzwerk kompromittieren.

Die SD-Branch Lösung von SonicWall

Die Weiterentwicklung der Technologie auf Filialebene ist heute wichtiger denn je. Herkömmlich ausgestattete Filialen können mit dem mit der digitalen Transformation einhergehenden rasch ansteigenden Anzahl der mobilen und IoT-Geräten nicht Schritt halten und wenden sich verstärkt Cloud- und SaaS-Anwendungen zu. Für diese gesteigerten Datenmengen wird wesentlich mehr MPLS-Bandbreite benötigt. Die Bereitstellung der notwendigen Bandbreite über herkömmliche WAN-Technologien ist jedoch sehr teuer und erfordert meist den Einsatz von IT-Fachkräften vor Ort.

Mit der rasch ansteigenden Anzahl von Geräten werden Verwaltung und Sicherheit zur Herausforderung. Für diese Geräte sind andere Regeln erforderlich und für die Durchsetzung und Gewährleistung der Transparenz muss eine einheitliche Richtlinie für das gesamte LAN und WAN vorhanden sein. Alle diese Einrichtungen müssen über eine zentrale Benutzeroberfläche verwaltbar sein, die auch umfassende Analysen und Echtzeitstatistiken liefert.

Mit zunehmendem Einsatz von Cloud-Technologie ist für die WAN-Konnektivität filialenübergreifend eine intelligente Architektur erforderlich, um neben den teuren MPLS-Verbindungen auch billigere Internetverbindungen nutzen zu können. Dazu ist der Einsatz der SD-WAN-Technologie erforderlich, wobei zugleich betriebliche Agilität und Kosteneinsparungen erzielt werden. Diese Technologie ermöglicht Organisationen und großen Unternehmen mit vielen Filialen den Aufbau von hochverfügbaren, leistungsstarken WANs. Durch Verwendung eines kostengünstigen Internetzugangs (Breitband, 3G/4G/LTE) können Unternehmen teure WAN-Verbindungstechnologien wie MPLS durch kostengünstige SD-WAN ersetzen.

Die Identifizierung und proaktive Abwehr von komplexen Bedrohungen am Gateway sind voraussetzend für die Gewährleistung der Sicherheit einer Organisation. Next-Generation-Firewalls bieten Schutz vor komplexen

SD-Branch-Markt steigt auf

3 Mrd. USD

bis 2022

Quelle: Network World

Sparen Sie bis zu

70 %

bei einer SD-WAN-Implementierung

Quelle: SD-WAN-Ressourcen

Bedrohungen und schützen Ihre Filialen und Ihren Hauptsitz auch vor den bösartigsten Angriffen. Diese Firewalls müssen Echtzeiterkennung und -abwehr bieten, damit ein hohes Sicherheitslevel aufrechterhalten werden kann. Durch die Kombination von Next-Gen-Firewalls mit sicheren Wireless Access Points kann eine einheitliche Lösung für den Schutz des Netzwerks und der Daten vor den neuesten Bedrohungen über drahtlose und kabelgebundene Verbindungen geschaffen werden. An den mit diesen sicheren Netzwerken verbundenen Clients können zusätzlich Endpunkt-Clients installiert werden, um einen noch umfassenderen Schutz zu ermöglichen. Dank der integrierten Roll-Back-Funktion können diese Endpunkte im Fall einer Kompromittierung jederzeit in ihren Originalzustand zurückgesetzt werden. Darüber hinaus können Cloud-Anwendungen mit Cloud App Security geschützt werden. Die Lösung bietet End-to-End-Sicherheit, vom Netzwerkrand bis zum Zugang und zu den Endpunkten.

Zero-Touch Deployment-fähige Geräte lassen sich von Unternehmen schnell von zentraler Stelle aus implementieren und einführen, sodass IT-Fachkräfte nicht mehr an zahlreiche Standorte fahren müssen, um diese Lösungen zu konfigurieren und einzubinden. Über eine Single-Pane-of-Glass (SPOG) Managementkonsole können alle Geräte, einschließlich unterstützender Dienste eines Anbieters zentral verwaltet werden.

Diese Lösung umfasst verschiedene Elemente, wie SPOG-Verwaltung mit Zero-Touch Deployment-Fähigkeit, Next-Generation-Firewalls mit Secure SD-WAN, Switches, Access Points sowie Endpunkt- und Cloud-App-Security. Wenn sich die Netzwerkanforderungen ändern, kann jede Netzwerkfunktion problemlos per Upgrade oder Downgrade angepasst werden. Mit der von Software Defined-Branch (SD-Branch) ermöglichten Flexibilität können Organisationen agiler, offener und cloudzentrischer handeln.

Einheitliches Sicherheitslevel

Mit dem Erwerb einer End-to-End Security-Lösung werden Implementierungen, Verwaltungsaufgaben und Fehlerbehebung vereinfacht. Des Weiteren wird sichergestellt, dass Compliance-Prüfungen bestanden und Betriebskosten gesenkt werden. Die SD-Branch Lösung sorgt für einheitliche Elemente.

Sie eignet sich ideal für verteilte Netzwerke, wie z. B. an Filialstandorten des Einzelhandels, wo Firewalls und Wireless-Access-Points gebündelt und die Sicherheit von kabelgebundenen Netzwerken auf drahtlose Netzwerke erweitert werden kann. Mittels Endpoint Security kann die Sicherheit auch auf die mit dem Netzwerk verbundenen Endgeräte erweitert werden.

Cloud-Management

Alle SonicWall Produkte können auf der SonicWall Cloud-Management-Plattform Capture Security Center (CSC) über eine zentrale Benutzeroberfläche, die auch Analysen und Fehlerbehebungsfunktionen bereitstellt, verwaltet werden. Das Capture Security Center ist ein skalierbares Cloud-Security-Managementsystem, das sowohl Single-Sign-On als auch Single-Pane-of-Glass-Verwaltung bietet. Es integriert die Funktionalität der Capture Cloud Plattform, um ein robustes Sicherheitsmanagement, Analytics-Funktionen und Echtzeit-Bedrohungsinformationen für Ihr gesamtes Portfolio an Netzwerk-, E-Mail-, mobilen und Cloud-Sicherheitsressourcen bereitzustellen.

Zero-Touch-Deployment (ZTD)

Mit ZTD und Cloud-Management lässt sich die SD-Branch Lösung schnellstens an Hunderten von Standorten weltweit implementieren. SonicWall ZTD ermöglicht Organisationen eine schnelle und sichere, Konfiguration von Firewalls, Switches und APs an neuen Standorten, ohne die Kosten für den Einsatz von IT-Fachkräften vor Ort. Nachdem neue Produkte an den externen Standorten online geschaltet wurden, können Administratoren die lokalen und verteilten Netzwerke über das CSC verwalten.

Sicheres SD-WAN

SD-WAN transformiert den WAN-Netzwerkrand der Filialen. SonicWall liefert umfassende, branchenführende Security-Lösungen, mit denen die SD-WAN-Implementierung vereinfacht wird. Unsere Secure SD-WAN-Technologie ist bereits in SonicOS, dem Betriebssystem der SonicWall Next-Generation-Firewalls integriert. Das bedeutet, dass keine zusätzlichen teuren SD-WAN-Appliances und Lizenzen erworben werden müssen. Die Secure SD-WAN Lösung umfasst Multi-WAN-Transport, Lastverteilung, dynamische Pfadauswahl, komplexes Routing, WAN-Beschleunigung und vieles mehr.

Next-Generation-Firewalls

SonicWall Next-Generation-Firewalls bieten automatischen Bedrohungsschutz in Echtzeit, der in hochwertige Hardware- und virtuelle Plattformen integriert ist. Diese Next-Generation-Firewalls erhielten von NSS Labs bereits zum sechsten Mal die Bewertung „Empfohlen“. Sie wurden speziell für die Abwehr von komplexen Bedrohungen entwickelt und bieten preisgekrönte Multi-Engine-Sandboxing sowie andere komplexe Bedrohungsschutztechnologien.

Network Access Switches

SonicWall Network Access Switches lassen sich nahtlos mit der SonicWall Security Lösung integrieren und verwalten. Sie ermöglichen echtes Zero-Touch Deployment mit Bereitstellung sowie Segmentierung, Security und Compliance. Die 7 Modelle sind als 8-, 24-, 48-Port-Ausführung sowie ohne PoE oder mit PoE erhältlich.

Sicheres WLAN

SonicWave Wireless Access Points (APs) bauen auf die neueste 802.11ac Wave 2 Technologie auf, wodurch die WLAN-Benutzererfahrung optimiert und umfassende Sicherheit im Netzwerk ermöglicht wird — auch wenn keine Firewalls implementiert wurden. Die SonicWave APs sorgen für den Schutz Ihrer Investition, da sie flexibel von der Cloud aus oder durch die Firewalls verwaltet werden können. An jedem beliebigen Standort kann das WLAN sofort mittels Zero-Touch Deployment und Mesh-Technologie erweitert werden. Es werden Modelle für die Verwendung in Gebäuden und robuste Versionen für die Installation im Freien angeboten.

Endpunktsicherheit

SonicWall Capture Client sorgt für die Endpunktsicherheit. Diese einheitliche Endpunkt-Client-Plattform bietet mehrere Schutzfunktionen an Endpunkten, einschließlich Malwareschutz der nächsten Generation, Unterstützung für Sicht auf verschlüsselten Verkehr und Rollback-Schutz.

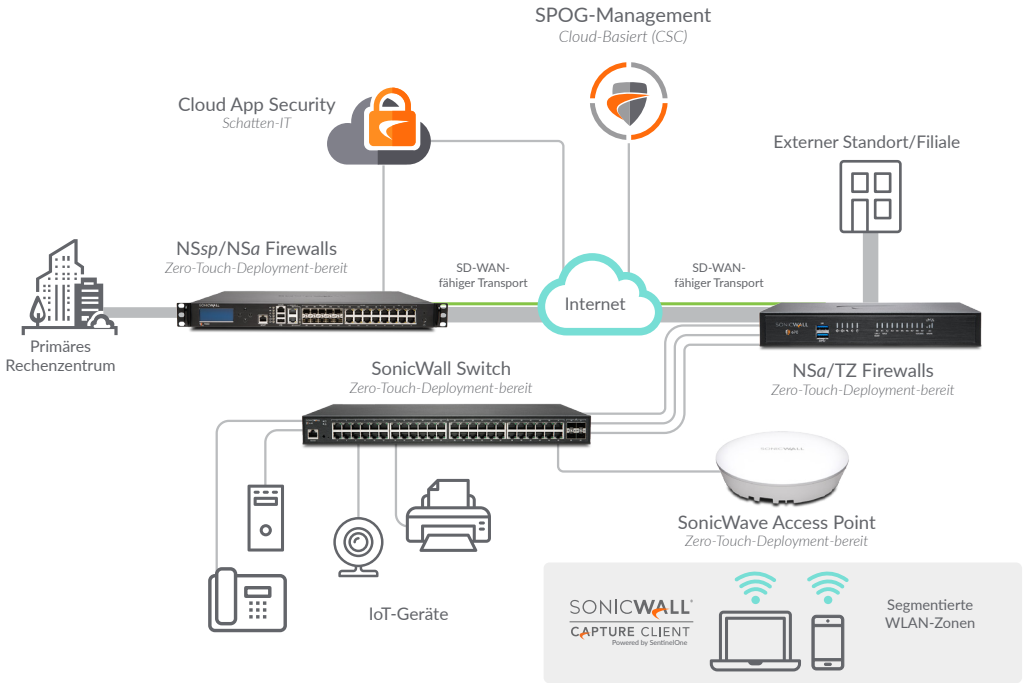
Cloud App Security (CAS)

Die in den Cloud-Anwendungen enthaltenen Benutzerdaten werden durch CAS zusätzlich geschützt, indem Next-Gen-Cloud App Security für E-Mail, Messaging, File-Sharing, Dateispeicherung usw. bereitgestellt werden. Mit SonicWall CAS können Organisationen unbedenklich SaaS-Anwendungen annehmen und eine nahtlose Benutzererfahrung und Best-in-Class Security bieten.

Weitere Informationen über SonicWall Secure SD-Branch finden Sie hier.

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

© 2020 SonicWall Inc. ALLE RECHTE VORBEHALTEN.

SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber. Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte. MIT AUSNAHME DER IN DEN LIZENZBESTIMMUNGEN FÜR DIESES PRODUKT DARGELEGTEN REGELUNGEN ÜBERNEHMEN SONICWALL UND/ODER DEREN TOCHTERGESELLSCHAFTEN KEINERLEI HAFTUNG UND LEHNEN SÄMTLICHE AUSDRÜCKLICHEN, STILLSCHWEIGENDEN ODER GESETZLICHEN GEWÄHRLEISTUNGEN IM ZUSAMMENHANG MIT IHREN PRODUKTEN AB, INSBESONDERE DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG. EINE HAFTUNG VONSEITEN DER SONICWALL UND/ODER DEREN TOCHTERGESELLSCHAFTEN FÜR DIREKTEN UND INDIREKTEN SCHADENSERSATZ, ERSATZ FÜR FOLGESCHÄDEN, SCHADENSERSATZ MIT ABSCHRECKUNGSWIRKUNG, BESONDEREN SCHADENSERSATZ ODER ERSATZ FÜR NEBEN- UND FOLGEKOSTEN (INSBESONDERE SCHADENSERSATZ FÜR ENTGANGENEN GEWINN, UNTERBRECHUNG DER GESCHÄFTSTÄTIGKEIT ODER DATENVERLUST), DER SICH AUS DER VERWENDUNG ODER DER NICHT MÖGLICHEN VERWENDUNG DIESES SCHRIFTSTÜCKS ERGIBT, IST GRUNDSÄTZLICH AUSGESCHLOSSEN, SELBST WENN SONICWALL BZW. DIE MIT IHR VERBUNDENEN GESELLSCHAFTEN VON DER MÖGLICHKEIT DIESER SCHÄDEN UNTERRICHTET WURDEN. SonicWall und/oder deren Tochtergesellschaften geben keine Gewährleistung in Bezug auf die Genauigkeit oder Vollständigkeit der Inhalte dieses Dokuments und behalten sich jederzeit das Recht auf stillschweigende Änderung der Spezifikationen und Produktbeschreibungen vor. SonicWall Inc. und/oder deren Tochtergesellschaften übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

SolutionBrief-SecureSDBranch-US-VG-1981