SonicWall Secure SD-Branch

Branch Reimagined Securely

ABSTRACT

SonicWall SD-Branch reinvents branch connectivity. SonicWall SD-Branch solution secures connectivity and improves user experience at branch offices through an integrated platform that combines SD-LAN, SD-WAN and security for distributed enterprises. This platform enables branch offices to take advantage of cheaper connectivity to connect HQ and branches, enable BYOD, adopt SaaS applications, and scale easily with rise in mobile devices. SD-Branch enables branches to be deployed swiftly with Zero-Touch Deployment and delivers unified visibility and threat detection from a single pane of glass. It is an end-to-end security solution that simplifies deployment, management and troubleshooting.

Introduction

As examined in our Executive Brief, traditional methods of deploying and maintaining security at branch sites has become ineffective, expensive and unmanageable. Distributed enterprises struggle with securing branch sites due to increased exposure points, limited resources and rising costs. This all contributes to a growing cybersecurity business gap.

SonicWall sees SD-Branch as a cornerstone of boundless security for the hyper-distributed era. An effective solution combines the agility of SD-Branch with end-to-end security, network segmentation and compliance. This enables unified policies across the network ecosystem, providing granular security controls to identify and prevent today's stealthiest and never-before-seen attacks from compromising your network.

The SonicWall SD-Branch Solution

Evolution of technology at the branch is essential. With digital transformation, traditional branches cannot keep up with increasing demands from multiplying mobile and IoT devices, driving increased adoption of cloud and SaaS applications. The increase in data demands more MPLS bandwidth. In conjunction, providing the necessary bandwidth over legacy WAN technologies is expensive and hard to roll out without on-site personal.

With the proliferation of devices, management and security becomes a challenge. These devices need different policies and having a unified policy across your LAN and WAN becomes critical for enforcement and visibility. Managing all this from a single pane of glass is needed to further provide rich analytics and real-time stats.

As the cloud adoption picks up, WAN connectivity across the branches must be redesigned intelligently so as to leverage cheaper internet links over more expensive MPLS links. This can be done with SD-WAN technology which brings about operational agility and cost savings. This technology allows organizations and enterprises with branch locations

SOLUTION BRIEF

to build highly available and higher-performance WANs. By using low-cost internet access (broadband, 3G/4G/LTE), organizations can cost-effectively replace expensive WAN connection technologies such as MPLS using SD-WAN.

Identifying and proactively preventing advanced threats at the gateway is essential to ensure security of the organization. Next-generation firewalls with advanced threat protection secures your branch locations and headquarters from the most deadly attacks. Ensure these firewalls can provide real-time detection and prevention to maintain a strong security posture. Combine the next-gen firewalls with secure wireless access points to create a unified solution that protects network and data from the latest threats over both wired and wireless connections. The clients connecting to these secure networks can further be protected by installing endpoint clients on them. With roll-back capability these endpoints can be restored to their original state, in case of compromise. Further, cloud apps can be secured with Cloud App Security. The solution provides complete end-to-end security covering edge, access to endpoint security.

Organizations can rapidly deploy and roll out these devices with Zero-Touch Deployment capability, eliminating or reducing the need for IT personnel to visit multiple branch locations to configure and deploy these solutions. This streamlines into Single Pane of Glass (SPOG) management of all devices including support services from a single vendor.

The solution elements consist of SPOG management with Zero-Touch Deployment capability, next-generation firewalls with Secure SD-WAN, switches, access points, endpoint and cloud app security. When network requirements change, any of the network function can be upgraded or downgraded accordingly. With the flexibility that Software Defined-Branch (SD-Branch) offers, organizations can be more secure, agile, seamless and cloud-centric.

Unified Security Posture

Purchasing an end-to-end security solution simplifies deployment, management and troubleshooting. It further enables to pass compliance checks and reduce operational costs. The SD-Branch solution unifies elements.

It is ideal for distributed networks such as retail locations where firewall and wireless access points can be bundled, extending the security of the wired network to wireless. Security can be further extended to end devices that are connecting to the network with endpoint security.

Cloud Management

Manage all SonicWall products from a SPOG management via the SonicWall Capture Security Center (CSC) cloud-management platform for easy management and simplified analytics to troubleshoot better. Capture Security Center is a scalable cloud security management system that features single-sign-on and 'single-pane-of-glass' management. It integrates the functionality of the Capture Cloud Platform to deliver robust security management, analytics, and real-time threat intelligence for your entire portfolio of network, email, mobile, and cloud security resources.

Zero-Touch Deployment (ZTD)

Quickly scale the SD-Branch solution globally across hundreds of locations with ZTD and cloud management. SonicWall ZTD allows organizations to quickly and securely configure firewalls, switches and APs at new locations without requiring advanced and costly on-site personnel. Once new products are brought online in remote locations, administrators can manage local and distributed networks through CSC.

SONIC**WALL**®

Secure SD-WAN

SD-WAN transforms the WAN edge at the branch. SonicWall delivers comprehensive, industry-leading security solutions that simplify SD-WAN deployments. Our Secure SD-WAN technology is built into SonicOS, the operating system for SonicWall next-generation firewalls, so there's no need to purchase separate and costly SD-WAN appliances and licenses. The Secure SD-WAN solution incorporates multi-WAN transport, load balancing, dynamic path selection, advanced routing, WAN acceleration and much more.

Next-generation Firewalls

SonicWall next-generation firewalls offers real-time, automated threat prevention in superior hardware and virtual platforms. These next-generation firewalls have earned the "recommended rating" from NSS labs 6 times. It is specially designed to combat advanced threats with award-winning multi-engine sandboxing and other advanced threat prevention technologies.

Network Access Switches

SonicWall network access switches provides seamless integration and management with SonicWall security solution. They provide true Zero-Touch Deployment and provisioning capability along with segmentation, security and compliance. Available in 7 models, they are offered as 8, 24, 48-port, non-PoE or PoE variants.

Secure WiFi

SonicWave wireless access points (APs) are built on the latest 802.11ac wave 2 technology to enhance WiFi user experience and provides advanced security on the network— even where firewalls are not deployed. The SonicWave APs provide investment protection by having the flexibility to manage these APs from the cloud or through the firewalls. Wireless expansion at any location is achieved instantaneously using Zero-Touch Deployment and mesh technology. It is available as indoor and ruggedized outdoor models.
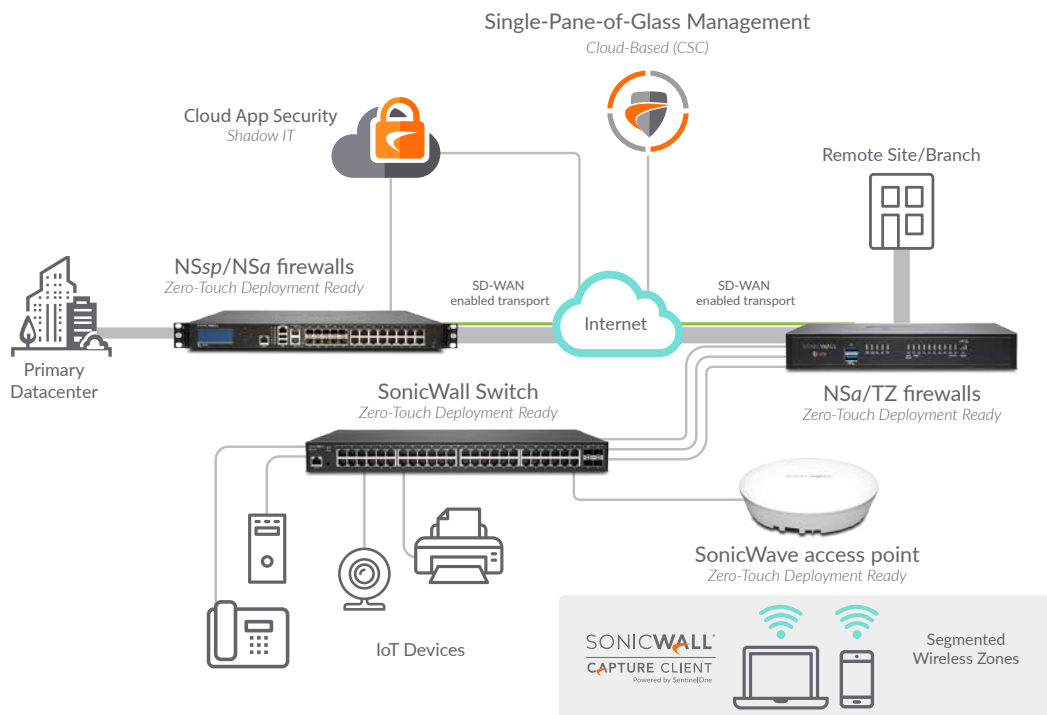
Endpoint Security

SonicWall Capture Client delivers endpoint security. This unified endpoint client platform provides multiple endpoint protection capabilities, including next-generation malware protection, support for visibility into encrypted traffic and rollback protection.

Cloud App Security (CAS)

The data of the users within the cloud applications are further protected with CAS, which provides next-gen cloud app security for email, messaging, file sharing, file storage etc. This enables organizations adopting SaaS applications, to deliver seamless user experience and best-in-class security with SonicWall CAS.

Learn more about SonicWall Secure SD-Branch at www.sonicwall.com/solutions/use-cases/secure-sd-branch.

Single-Pane-of-Glass Management
Cloud-Based (CSC)

Cloud App Security
Shadow IT

Remote Site/Branch

NS*sp*/NS*a* firewalls
Zero-Touch Deployment Ready

SD-WAN
enabled transport

SD-WAN
enabled transport

Internet

Primary
Datacenter

SonicWall Switch
Zero-Touch Deployment Ready

NS*a*/TZ firewalls
Zero-Touch Deployment Ready

SonicWave access point
Zero-Touch Deployment Ready

IoT Devices

SONICWALL
CAPTURE CLIENT
Powered by SentinelOne

Segmented
Wireless Zones

SONICWALL®

Learn more about how SonicWall Secure SD-Branch improves user experience and secures connectivity at branch offices.

www.sonicwall.com/solutions/use-cases/secure-sd-branch

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SONICWALL®

SolutionBrief-SecureSDBranch-US-JK-6395