SONICWALL

GOVERNMENT AGENCY USE CASE: SD-WAN

Using A Secure SD-WAN for Reliable, Low-Cost Networking

HIGHLIGHTS

Organization type

Government

The Challenge

Government agencies need to lower network costs of remote offices without compromising security, as well as improving the performance and reliability of new Software-as-a-Service (SaaS) applications and strengthening the protection of wireless networks and web applications.

The Solution

Implementing secure Software-Defined Wide Area Network (SD-WAN) capabilities built into SonicWall next-generation firewalls, as well as advanced security features in those firewalls and other integrated SonicWall solutions.

Financial Benefits

- Additional network capacity through low-cost public Internet services rather than high-cost Multiprotocol Label Switching (MPLS) connections
- Reduced administrative costs with centralized management

Operational Benefits

- Fast, predictable network performance for critical public applications
- Better user experiences for employees and citizens

Security Benefits

- Reduced time to detect and block malware, ransomware, phishing, DoS attacks and other threats
- Better protection for WiFi networks, email, SaaS apps, and other applications

Challenge scenario

A government agency operates out of a main office and 30 district offices. It's public web portal and main applications run on a private cloud in the government data center.

The agency was in the process of deploying new technologies to improve the productivity of its staff and increase engagement with citizens. Initiatives for the coming year included implementing video conferencing centers in each office, expanding the use of SaaS collaboration tools for employees, adding free public WiFi networks in many of its facilities, and deploying new self-service apps on the agency's citizens portal. A team was working on a special project to allow hundreds of agency workers to access critical applications remotely during weather emergencies such as floods and severe winter storms.

At the same time, the CIO was concerned that telecommunications costs for the wide area network (WAN) was consuming too much of the agency's budget. He read that distributed organizations can save up to 60% on WAN costs by moving from MPLS and dedicated links between offices to low-cost public internet services. However, he was aware that using public internet connections would expose the agency's offices to more cyberattacks.

The CIO created a team to evaluate SD-WAN technology to see if it could reduce network and operational costs without compromising security. The team was also charged with determining if an SD-WAN solution could provide additional benefits, such as improving the performance and reliability of the new video conferencing and SaaS applications.

Criteria for Success

The evaluation team decided to assess SD-WAN solutions based on their features in four areas:

1. Advanced SD-WAN capabilities for reliable, high-quality network performance
2. Support for enterprise-grade network security
3. Centralized management and reporting and simple deployment
4. Integration with additional networking and security products

This is a composite use case that explores how a variety of government agencies and other distributed enterprises have responded to security and operational challenges.

The SonicWall Solution

The agency already had SonicWall next-generation firewalls (NGFWs) at many of its locations. The evaluation team realized that the best option would be to implement the SD-WAN features built into those firewalls, and to deploy SonicWall firewalls with those features at the few sites that didn't already have one. An analysis showed the team that this strategy would address all their criteria for success.

1. Advanced SD-WAN Capabilities for Reliable, High-Quality Network Performance

Public internet services are far less costly and much more flexible than MPLS or point-to-point circuits. However, network traffic across the public internet often suffers from jitter, packet loss, and slow performance caused by contention with traffic from other internet users. This was a major concern for the agency, because:

- Predictable high performance is mandatory for critical applications related to public health and safety, emergency preparedness and response, and other time-critical services provided by a health and human services organization.
- Jitter, packet loss, and contention can interfere with employee productivity and disrupt services to citizens, particularly for latency-sensitive applications like voice-over-IP (VoIP), video conferencing and unified communications.

The team discovered that SonicWall SD-WAN technology could improve the performance, predictability and quality of network traffic for high-priority applications through dynamic application-based path selection and other quality of service (QoS) features. Administrators could set up path selection profiles (PSPs) for critical applications that specify minimum criteria for latency, jitter and packet loss. The SonicWall NGFWs then probe available paths between locations and route traffic across the paths that meet or exceed those criteria. If more than one path meet the criteria, the application traffic would be load balanced across them.

The team found that SonicWall SD-WAN technology also provides intelligent failover. If a path becomes unavailable, the traffic it was carrying is quickly re-routed through remaining available paths.

Also, the agency would have the option of increasing performance by deploying SonicWall WAN Acceleration (WXA) appliances at key locations to provide data de-duplication, byte caching, file caching, and protocol optimization.

Team members from the agency's network operations group also noted that SonicWall Analytics could work with flow reporting data captured by the SonicWall devices to help them monitor application traffic and bandwidth utilization in near real time and troubleshoot network problems. They would also be able to identify the applications, websites, and users with the highest bandwidth demands in order to anticipate problems and add bandwidth in advance.

2. Enterprise-Grade Network Security and SD-WAN Delivered in the Same Device

The evaluation team noted that secure SD-WAN technology is a feature of SonicOS. This is the operating system for SonicWall TZ entry-level firewalls and NS*a* and NS*sp* mid-range and high-end NGFWs. Thus, the agency would

not need to worry about integrating a separate SD-WAN appliance with its existing firewalls, or about managing two devices at each location (see Figure 1).

The SonicWall firewalls would provide enterprise-grade network security for each location. They use deep-packet inspection, SSL/TLS decryption, and threat intelligence from the SonicWall Capture Labs Threat Research team to identify and block known malware, traffic from botnets and known malicious websites, and DoS attacks.

The firewalls work with SonicWall's Capture Advanced Threat Protection (ATP) service to detect emerging threats and zero-day attacks. Capture ATP is a cloud-based multi-engine sandbox that analyzes suspicious code. It executes code in multiple parallel sandbox engines and performs Real-Time Deep Memory Inspection™ (RTDMI). Many sandboxing services can be fooled by techniques such as obfuscating malicious code and using very low-level instructions. Capture ATP defeats these and other techniques by using machine learning to quickly identify code similar (but not identical to) known malware, and executing suspicious code all the way down to the level of CPU instructions.

Capture ATP with RTDMI has successfully detected many of the newest and most insidious forms of malware and ransomware, including malicious Office and PDF files containing executables, shellcode, malicious macros, and DDE-based exploits, and "phishing style" PDF documents with links to phishing and malware hosting websites.

The wide range of SonicWall firewalls could help lower capital costs. Each of the agency's small and medium-sized offices could be protected by one very cost-effective unit. This highly scalable system could provide the processing power and network support for the main office.

3. Centralized Management and Zero-Touch Deployment

The agency's security and network teams were concerned about their ability to manage technology in its remote offices, and to collect data from remote locations for analysis. They found that these issues could be addressed with the SonicWall Capture Security Center, a cloud-based security management portal that provides "single-pane-of-glass" visibility, unified management, reporting, and analytics across its product lines.

With the Capture Security Center, the teams could:

- Manage all the SonicWall products from a central location
- View network and security data from all the locations to help troubleshoot network problems and respond to security incidents faster

Because the agency was planning to open new offices and community centers, ease of implementation was also an issue. Administrators were pleased to find that SonicWall firewalls offered a zero-touch deployment option. New firewall appliances can be shipped directly to remote sites. As soon as they are connected to the internet, they are discovered and authenticated, and remotely configured by the Capture Security Center.

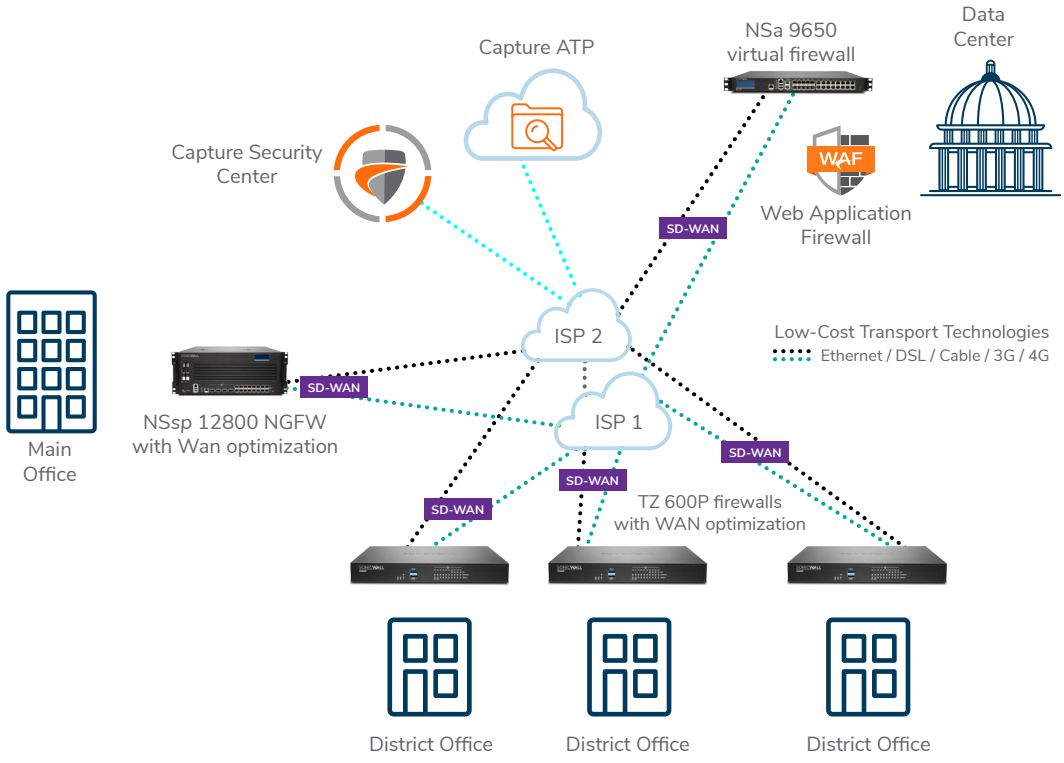

Figure 1: An overview of the deployment, showing entry level and high-end SonicWall firewall appliances with built-in SD-WAN technology, a virtual firewall and a web application firewall, and SonicWall's Capture Security Center for management and Capture ATP advanced threat protection service.

This capability reduces the cost of supporting remote locations and ensures that firewall and SD-WAN configurations are consistent across similar sites. When combined with the availability of fast internet connections, it allows new sites to be securely connected to the network and to SaaS applications in hours, compared with waiting weeks for a new MPLS connection.

4. Integration with Additional Networking and Security Products

The evaluation team also wanted to determine if an SD-WAN solution could be integrated with additional networking and security products, because this would reduce the cost of managing their infrastructure as a whole. It would also make it easier to share data between tools, which would speed up network troubleshooting and security incident response.

They found several SonicWall products that would help with high-priority agency initiatives, as well as improving network management and security overall. In particular:

SonicWave Wireless Access Points (WAPs) would simplify the deployment and management of WiFi networks in its offices and keep employee wireless communications secure and separate from their free public WiFi service.

SonicWall Cloud App Security, a cloud access security broker (CASB), could help enforce the secure use of the agency's SaaS applications, such as Office 365, G Suite, Dropbox and Box.

SonicWall Email Security solutions could strengthen the agencies defenses against ransomware and targeted phishing and business email compromise (BEC) attacks.

SonicWall Secure Mobile Access (SMA) devices could provide advanced authentication, endpoint control and other security services for remote user access. With the optional SonicWall Spike License Pack, SMA could flexibly provide hundreds of agency workers with access to their applications from remote locations as needed during weather emergencies and other events that might disrupt travel.

SonicWall WAF Series web application firewalls could protect the agency's website and self-service citizen apps from sophisticated application-level attacks and employ data leak prevention (DLP) features to prevent hackers from exfiltrating protected personal and health information.

SonicWall Network Security virtual (NSv) virtual firewalls could monitor and protect the agency's application traffic between virtual machine instances running in the private cloud at the state data center.

SonicWall US Government Certifications

SonicWall TZ, NS*a* and SM series products meet a wide range of government certifications, including:

- FIPS 140-2: cryptographic modules
- Common Criteria (ISO/IEC 15408): computer security certification
- U.S. Department of Defense Information Network (DoDIN) firewall/IPS/IDS
- Commercial Solutions for Classified (CSfC): firewall/VPN/IDS/IPS
- IPV6: Ready Logo Phase 2 Core test
- Voluntary Product Accessibility Template (VPAT), Section 508

Deploying a Secure SD-WAN: The Outcomes

After implementing the SD-WAN features built into its SonicWall firewalls, the state agency experienced several positive outcomes.

Financial benefits:

- The ability to add network capacity through low-cost public internet services rather than high-cost MPLS connections
- Reduced administrative costs and effort for providing secure connectivity to remote offices because of centralized management and zero-touch deployments

Operational benefits:

- Fast, predictable network performance for critical public health and safety and emergency response applications
- Better employee and citizen experiences with latency-sensitive applications such as VoIP, video conferencing, and unified communications
- High network availability, even when individual WAN paths fail

Security benefits:

- Reduced time to detect and block malware, ransomware, phishing, DoS attacks, and other threats, through integration with SonicWall's next-generation firewalls and cloud-based advanced threat protection platform
- A simple path to better protecting the agency's WiFi networks, SaaS applications, email, self-service web portals, and applications running on the private cloud in the state data center

Services and Support

Professional Services

Optimize your investment in SonicWall products with professional services delivered by SonicWall Advanced Services Partners that are trained to provide world class professional services for SonicWall customers. From planning

to implementing and optimizing your SonicWall configuration, SonicWall Advanced Services Partners will provide you with peace of mind in knowing that your network and security architecture is providing the most effective protection against today's evolving cyber threats.

Value-Add Support

Customer Success Manager: Provides enterprise environments with a dedicated trusted advisor. Your Customer Success Manager (CSM) acts on your behalf and works with your staff to help minimize unplanned downtime, optimize IT processes, provide operational reports to drive efficiencies and is your single point of accountability for a seamless support experience.

Focused Technical Support (FTS): Provides a named engineering resource to support your enterprise account. Your FTS will know and understand your environment, policies and IT objectives to bring you fast technical resolution when you need support.

SonicWall Live Demo

Experience all SonicWall products and features for yourself in a live, real-time cloud environment. Visit SonicWall's Live Demo portal at for an unguided product demo of your choice.

Free Software Trial

Get a 30-day free trial of available SonicWall software products. Try out first hand in your own proof-of-concept (POC) environment. Request a free trail www.sonicwall.com/freetrial.

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com