RETAIL USE CASE: NEVER-BEFORE-SEEN THREATS

Stopping New and Emerging Threats at a Distributed Enterprise

HIGHLIGHTS

Industry

Retail

The Challenge

A retail chain needed to upgrade its capacity to detect and mitigate new and emerging threats. The IT organization was faced with deploying advanced security tools to hundreds of sites, while protecting an ecommerce website and applications in the cloud.

The Solution

An integrated set of security solutions from SonicWall, including next-generation firewalls sized to each location, a web application firewall, advanced threat protection, a virtual firewall for applications in the cloud, and centralized management.

Security Benefits

- Detect never-before-seen threats and zero-day attacks
- Protect remote storefronts, ecommerce applications, and data on public cloud platforms

Operational Benefits

- Easily deploy security solutions to hundreds of remote locations with no on-site technical support
- Provide high availability and meet SLAs for critical applications

Business Benefits

- Avoid disastrous data breaches
- Confidently leverage new ecommerce and cloud technologies
- Address PCI DSS requirements

The Business

A retail chain includes a headquarters operation with administrative staff, a data center, two distribution centers, an e-commerce website for online shoppers, and several hundred physical storefronts.

The company recognized that technology is a key competitive weapon. To increase revenue, it was expanding its ecommerce activities and adding instore customer service applications. To streamline operations, it was moving mission-critical applications to cloud platforms.

As with other distributed organizations, security was a top-of-mind consideration that required careful consideration and planning. The threat landscape was evolving constantly, with zero-day exploits and ransomware attacks appearing daily. These attacks could cripple the entire operation for hours, days, weeks or possibly months.

The marching orders for the IT organization: upgrade security so key technology initiatives can continue without increasing risk (but don't overrun your budget).

Challenges for IT

Security Issues

Faced with this mandate, leaders of the IT organization identified primary security and operational challenges.

The security team was uneasy about the ability of the organization's cybersecurity defenses to detect and respond quickly to new and emerging advanced threats. Concerns were fueled by:

- The explosive growth of never-before-seen threats and zero-day attacks: Last year, SonicWall discovered 153,909 `never-before-seen' malware variants in 2019 — attacks that traditional sandboxes likely missed[1]
- New techniques to evade conventional firewalls and anti-virus tools, including malicious PDF and Office files and the use of TLS/SSL encryption to hide 3.7 million cyberattacks[2]

The team had to protect a wide range of data in an extremely diverse set of environments, including:

- Confidential information on employee desktop PCs, laptops and mobile devices
- Credit card data in ecommerce applications on web servers in the headquarters data center
- Customer information on systems in the stores
- Financial data and employee information in accounting and human resources applications the company is now running on public cloud platforms

Operational Concerns

IT managers had operational concerns as well. For example, they would need to deploy and manage security tools in hundreds of stores, most with no local technical support. They had to ensure that security tools wouldn't cause network bottlenecks that would degrade the performance of critical applications. They also had to strengthen their compliance with Payment Card Industry Data Security Standard (PCI DSS) and other industry and government standards.

Turning to a New Approach

The leaders of the IT organization concluded that a new approach to protecting networks and data was required. This approach would need to incorporate:

- Innovative technologies to detect never-before-seen threats and block zero-day attacks
- An integrated set of tools capable of protecting a wide variety of environments, including a large data center and small storefronts, on traditional servers and virtual environments on cloud platforms
- An architecture supporting high availability and excellent performance for mission-critical in-store applications
- Centralized "single-pane-of-glass" management for security tools

A SonicWall Solution

The retail chain determined that it could achieve its goals by leveraging SonicWall's product line of integrated security and networking products. The solution had five integrated components:

1. Next-generation firewall (NGFW) appliances to protect each site against network-based threats
2. A web application firewall (WAF) to protect the ecommerce websites from application-level attacks

This is a composite use case that explores how a variety of retail companies and other distributed enterprises have responded to security and operational challenges. Most of these challenges are faced by all organizations with multiple locations, from small restaurant chains to multinational conglomerates.

[1] *SonicWall: 2020 SonicWall Cyber Threat Report.*
[2] *Ibid.*

3. A cloud-based advanced threat protection (ATP) platform to identify and block zero-day attacks and other never-before seen threats
4. A virtual next-generation firewall to protect company applications running on public and private cloud platforms
5. A cloud management portal to provide centralized management and analytics for all the SonicWall security infrastructure

1. Next-Generation Firewalls, Sized for Each Location

Next-generation firewalls are a fundamental component of any enterprise security infrastructure. The security and operations teams noted several characteristics of SonicWall's NGFW product lines that made them an excellent fit for the retailer's environment:

- Scalability upwards, to high-end appliances capable of supporting the chain's headquarters and data center
- Scalability downwards, to entry-level unified threat management (UTM) firewalls that could protect small sites such as small storefronts in a cost-effective manner
- A high-throughput hardware architecture that enables SonicWall's mid-range and high-end NGFWs to scan thousands of encrypted and unencrypted connections without sacrificing network performance
- To minimize latency, unique Reassembly-Free Deep Packet Inspection (RFDPI) technology that performs single-pass, stream-based analysis with no buffering or proxying
- To work with high-speed and wireless networks, high port density, including 10-GbE, 5-GbE and 2.5-GbE interfaces on high-end units and support for high-speed 802.11ac Wave 2 wireless connections on all models

The teams decided to deploy pairs of high-end NS*a* 9450 NGFW appliances for the headquarters and the attached data center, mid-range NS*a* 5650 NGFW appliances at the distribution centers, and entry-level TZ300P and TZ600P UTM firewalls for the distributed stores. The pair of units in each location were in a high-availability configuration to ensure reliable, continuous connections to the internet (see Figure 1.)

Three additional characteristics of the SonicWall NGFWs also captured the teams' attention.

First, SonicWall's entry level TZ300P and TZ600P UTM firewalls included several features particularly well suited for small distributed sites like retail stores, notably:

- Easy deployment and management, through simplified configuration and management through SonicWall's centralized management portal
- Power over Ethernet (PoE) and PoE+ ports, to reduce the cost and complexity of connecting devices such as point of sale kiosks, printers, intelligent lighting controllers, cameras, and wireless access points

Second, related to the all-important goal of stopping never-seen-before threats, SonicWall next-generation firewalls are integrated with the company's cloud-based Capture Advanced Threat Protection (ATP) sandboxing service (discussed below). In a typical scenario, when files enter the enterprise network the SonicWall next-generation firewall at the gateway:

1. Blocks traffic from botnets and millions of known malicious websites
2. Decrypts SSL/TLS network traffic to reveal encrypted files
3. Submits copies of suspicious files to Capture ATP, holds the files at the gateway, and only releases the files into the network when the sandbox renders a verdict of "good"

This integration and the way tasks are divided between the firewalls and the cloud-based sandbox ensure that all potential malware files are evaluated with minimal impact on the network and computer users.

Third, SonicWall next-generation firewalls have software-defined wide area network (SD-WAN) capabilities built in. SD-WAN features can optimize the use of both low-cost internet connections (broadband, 3G/4G/5G/LTE, fiber) and expensive but reliable carrier networks (MPLS, T1) between sites. The benefits of SD-WAN capabilities include:

- Reducing WAN costs by substituting internet connections for carrier network links.

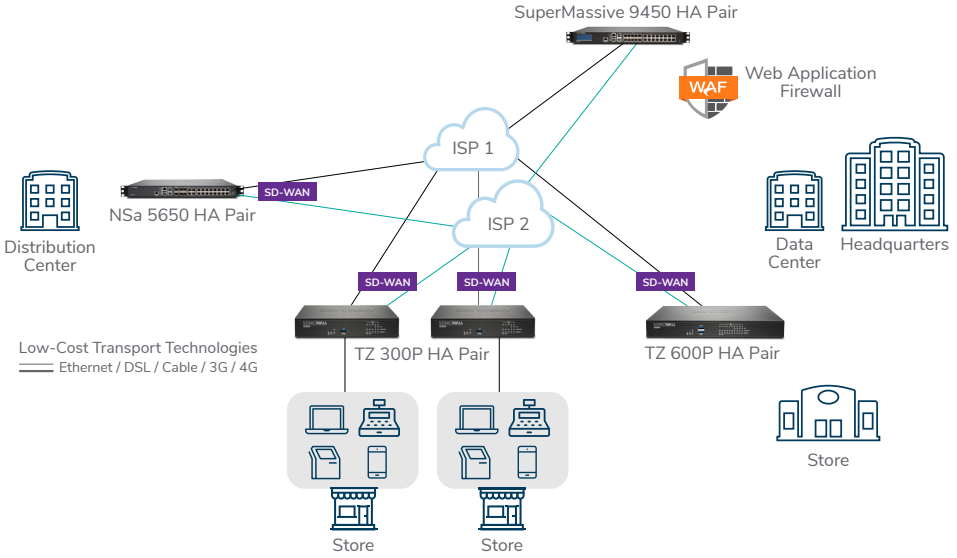

Figure 1: An overview of the initial deployment, featuring high-end, mid-range and entry level next-generation firewall appliances in high-availability pairs with SD-WAN enabled transport at each location, and a web application firewall protecting ecommerce applications in the data center

- Increasing application performance and quality through load balancing, intelligent failover, and the ability to give critical applications priority use of the links with the most available capacity and the least jitter and packet loss.
- Improving flexibility by making it easy to add WAN capacity as business needs change.

2. A Web Application Firewall to Protect eCommerce Applications

The ecommerce and security teams decided to protect the chain's online activities with a SonicWall Web Application Firewall (WAF). This solution (see Figure 1) uses both signature-based and application-profiling deep-packet inspection engines to protect against typical web application attacks, as well as denial-of-service (DoS) attacks and context-aware exploits.

The WAF could accelerate web application performance by providing caching and compression, offloading SSL transactions from web servers, and performing Layer-7 load balancing across clustered web servers.

The SonicWall WAF could help the retailer comply with the standards like the PCI DSS by using data masking and page-blocking techniques to prevent the unauthorized sharing of protected information.

The WAF integrates with the Let's Encrypt Certificate Authority (CA) service, so websites can automatically be provisioned at no cost with SSL/TLS certificates from a trusted source. This would help the chain deliver greater security to website visitors and elevate their SEO placement.

Finally, the WAF is fully integrated with SonicWall Capture ATP, described below.

3. Capture ATP with RTDMI to Defeat Unknown Threats

The company's security team singled out SonicWall's Capture ATP service as an essential weapon for detecting and blocking emerging threats and zero-day attacks.

Exploits detected by Capture ATP include:

- Malicious Flash-based Office documents
- Dynamic Data Exchange (DDE) based exploits and malware inside Office files
- Malicious Office and PDF files containing executables
- Shellcode-based malicious Office and PDF files
- Macro-based malicious Office documents
- PDF documents containing "JavaScript infectors"
- "Phishing style" malicious PDF documents leading to phishing and malware hosting websites

Capture ATP is a cloud-based multi-engine sandbox that analyzes suspicious code to help discover and block newly developed malware from entering enterprise networks (see Figure 2). It works in conjunction with SonicWall next-generation firewalls, WAFs, wireless access points, endpoint security platforms, email security solutions and other SonicWall products.

Capture ATP:

- Compares suspected code with millions of code sequences used in known malware
- Uses Real-Time Deep Memory Inspection™ (RTDMI) to executes the code in each file in multiple sandbox engines in parallel, to discover never-before-seen malware and ransomware

Many sandboxing services can be fooled by techniques such as obfuscating malicious code, hiding code in obscure file types, 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.

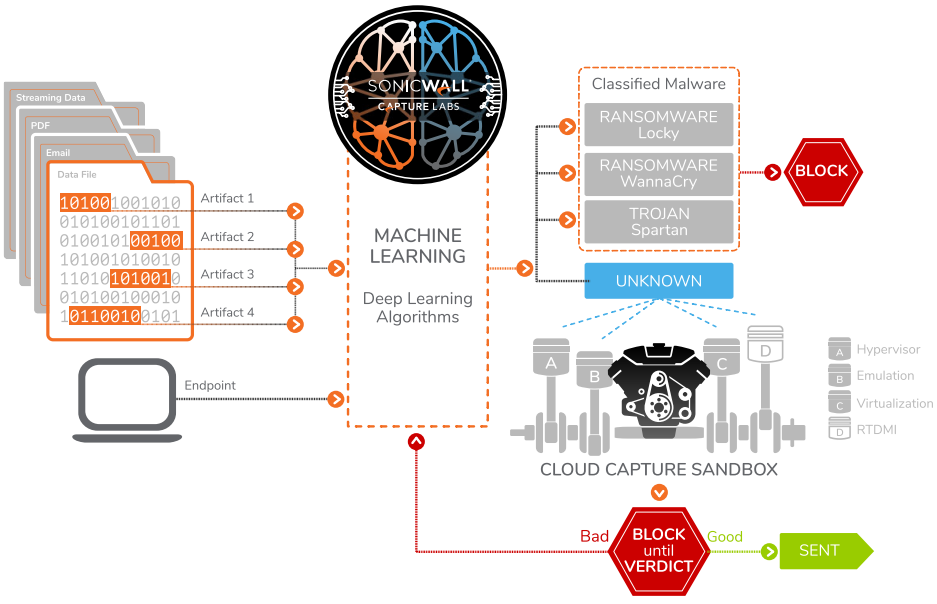

Figure 2: Capture ATP uses machine learning and Real-Time Deep Packet Inspection (RTDPI) to detect never-before-seen malware

Identifying Zero-Day Attacks in Real Time (Before VirusTotal)

The SonicWall RTDMI engine looks inside multiple layers of packaging and obfuscation to find well-entrenched malware that conventional anti-malware solutions don't uncover. It identifies zero-day attacks in real time, often before they are listed in industry malware search portals. Recent examples include:

- The RTDMI engine identified a new malware campaign using malicious Microsoft Office document files. The files contained VBA macro code that decrypts a URL hidden inside an embedded form in the document and downloads a ransomware payload. SonicWall provided customers with a list of indicators of compromise (IOCs) immediately, before the threat was listed in VirusTotal or ReversingLabs
- The RTDMI engine detected a surge in archive files containing an obfuscated JavaScript file that used PowerShell.exe to execute a downloader that downloaded a variant of the popular ransomware family "GandCrab." This complex threat had not been posted on any of the popular threat intelligence portals

These steps occur very fast – in a few seconds at most – so good files are released quickly.

Capture ATP with RTDMI has successfully detected many of the newest and most insidious forms of malware and ransomware, some of which are listed above.

4. A virtual Firewall to Protect Applications in the Cloud

The retail chain recently moved some of its key applications to the Amazon Web Services (AWS) and Microsoft Azure cloud platforms. Unfortunately, conventional firewalls and most security tools have no visibility into network traffic between virtual machines in private clouds or into traffic between zones on public cloud platforms.

However, the company's security team noticed that a SonicWall's Network Security virtual (NSv) series virtual firewall can run on AWS and Azure platforms and help protect applications running there. It can monitor traffic between virtual machines and across zones, block communication between applications and external malicious websites, and stop many types of attacks on virtual workloads, including cross-virtual-machine attacks and side-channel attacks.

The virtual firewall will allow the chain to take advantage of the scalability and flexibility of AWS and Azure without compromising security (Figure 3).

5. Centralized Management and Advanced Analytics

The IT organization was very concerned about the risks of supporting too many security and network tools in too many locations (sometimes known as "tool sprawl"). Because it must support security tools in hundreds of locations

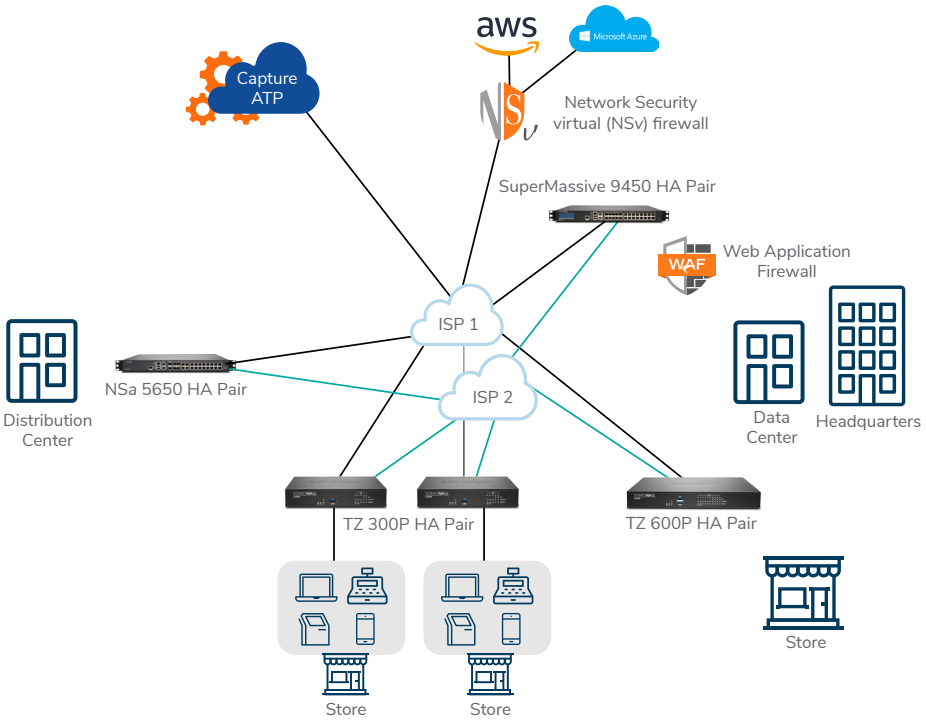

Figure 3: An overview of the deployment including the Capture ATP platform and an NSv firewall in the cloud

SONICWALL®

that lack on-site technical support, central management was also a major consideration.

Fortunately, SonicWall offers its customers access to the 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.

The Capture Security Center will enable the security and operations staffs to:

- Deploy and manage all SonicWall products from the data center with zero-touch provisioning, allowing them to operationalize firewalls at remote locations in minutes with a simple four-step process (register, connect, power-up, and manage)
- Use SonicWall's risk metering to perform real-time analysis of the company's security posture, identify gaps in current defenses, run what-if scenarios to test defensive layers, and identify new defensive strategies to counter threats
- Identify and respond to security incidents faster, using a broad range of security and network data
- Address firewall change management and auditing requirements of industry standards such as PCI DSS

Improved compliance with PCI DSS and Other Standards

The IT organization found that the SonicWall solutions strengthened their compliance with PCI DSS standards.

PCI DSS includes multiple requirements related to **building and maintaining a secure network, protecting cardholder data,** and **implementing strong access control measures.** SonicWall's next-generation and web firewalls allowed administrators to better segment and control access into and out of the POS network in each store that handled credit card data. For example, it was easy to create and enforce policies that restricted access to the POS network to a minimal number of applications and users, and to deny all outbound traffic from the POS networks to the internet (a PCI requirement they had never been able to meet consistently before).

PCI DSS also includes strong mandates to **maintain a vulnerability management program** and **protect all systems against malware.** SonicWall's firewalls greatly strengthened the chain's capabilities in this area through gateway malware detection, intrusion prevention capabilities, SSL/TLS traffic decryption, deep packet inspection, and cloud-based sandboxing with RTDMI.

PCI DSS also requires that organizations handling credit card data **regularly monitor and test networks** and **maintain an information security policy.** With SonicWall's Capture Security Center, administrators were able to continuously monitor their networks' security posture and produce reports to address firewall change management and auditing requirements.

Down the Road

The IT organization is evaluating additional SonicWall security solutions for implementation in the future. The options include:

- SonicWave wireless access points to protect data on the wireless networks in the chain's offices and stores
- SonicWall Email Security Appliances to stop email-based attacks
- SonicWall Cloud App Security, a Cloud Access Security Broker (CASB) that helps ensure the secure use of software-as-a-service applications such as Office 365, G Suite, Dropbox, Box, Slack, and Salesforce
- Capture Client to detect malware and attacks on endpoints

Conclusions: Making a Distributed Enterprise More Secure and More Efficient

Since deploying the five integrated security solutions from SonicWall, the executives and the IT organization of the retail chain have enjoyed a variety of benefits.

Security benefits have included:

- Faster and more accurate detection of never-before-seen threats and zero-day attacks
- Better protection against web-based attacks on ecommerce applications
- A single, integrated set of tools providing security for traditional servers in the data center, virtual environments on cloud platforms, and systems and devices in the stores

Operational benefits have included:

- Rapid deployment of security solutions to hundreds of remote stores with no on-site technical support
- The ability to make fast adjustments to the security infrastructure, so applications can be rolled out and reconfigured quickly
- High availability and high quality of service for critical applications

Business benefits have included:

- Reduced risk of potentially disastrous data breaches
- Lower network costs
- Confidence to leverage new technologies for ecommerce, in-store customer service, and cloud computing

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 trial www.sonicwall.com/freetrial.

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