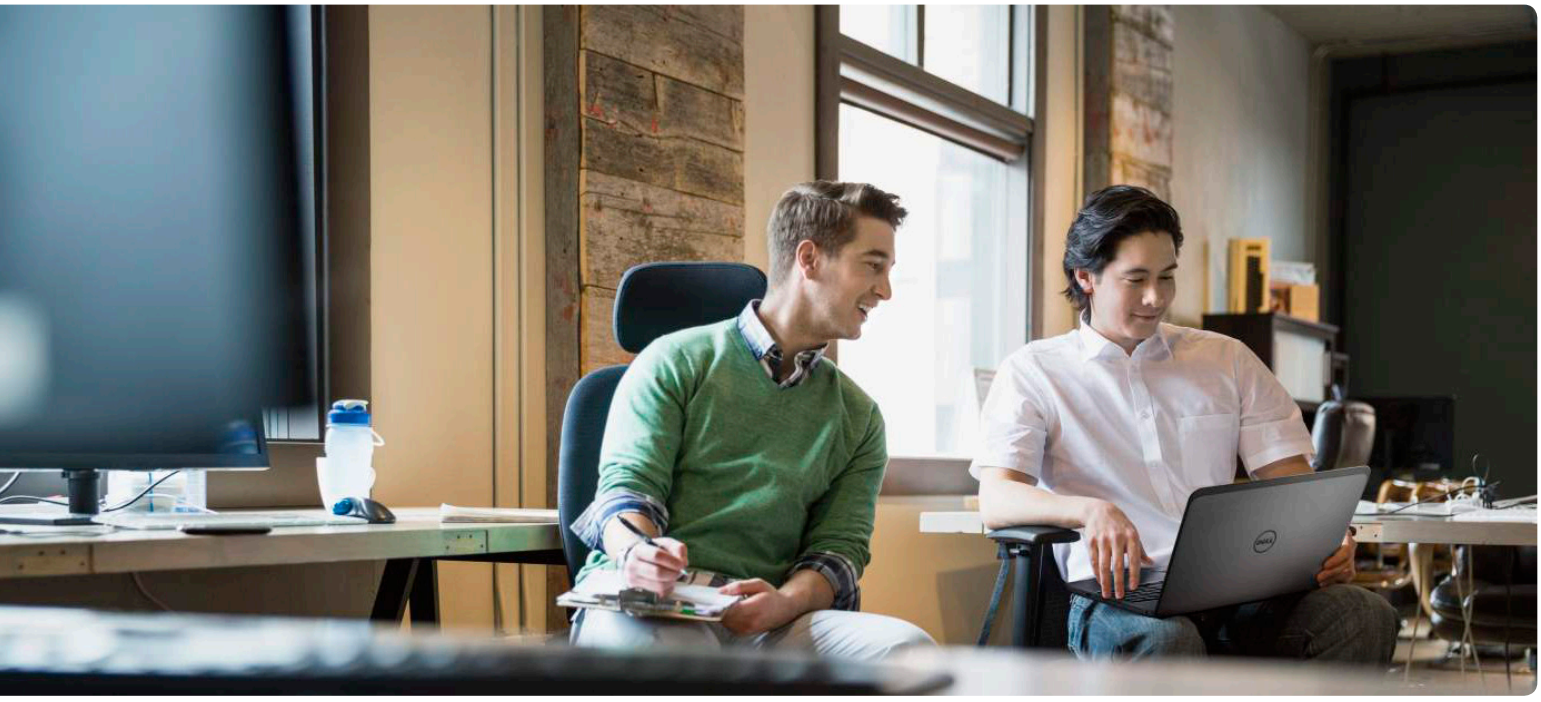
The Distributed Enterprise and the SonicWALL TZ — Building a Coordinated Security Perimeter



Abstract

Branch offices, retail stores, remote sites and mobile workers in distributed enterprises need to be connected to headquarters. But as the network continually stretches to encompass them, it becomes more difficult for IT to manage, secure and maintain compliance companywide. The coordinated security perimeter is a model that gives the distributed enterprise the central management and secure wireless connectivity it needs to defend itself against unceasing attacks on the network.

This paper describes the main pain points of network security in the distributed enterprise. Readers will learn what goes into the coordinated security perimeter and discover the role of the SonicWALL TZ series of firewalls in building up the perimeter around their own organizations.

Introduction

Businesses that run branch offices, remote sites and retail stores physically distribute their networks far beyond headquarters, and mobile workers virtually distribute them even farther. With the distributed enterprise comes the urgent need to build a coordinated security perimeter that protects the network at all the points where data enters and exits.

This paper describes the coordinated security perimeter, a model for extending protection for enterprise networks far beyond the safe confines of headquarters through central management and secure wireless connectivity. Readers will see how a next-generation firewall stores and manages security rules centrally and the SonicWALL TZ, a firewall with integrated wireless controller, executes those rules at the perimeter.

Businesses evolve almost as quickly as security does, but threats evolve more quickly than either businesses or security.

Security is not keeping up

As cybercrime and network attacks have become commonplace, security is always just playing catch-up. One headline, "Is insecurity the new normal?[1]" typifies the cyber-siege mentality of both businesses and consumers.

In its analysis of 63,000 events — including 1,367 confirmed data breaches — Verizon reported that Web app attacks, cyber-espionage and point-of-sale (POS) intrusions accounted for more than 70 percent of incidents across 95 countries.[2]

Threats evolve quickly. Cyber-vandals were once content to deface a website or promote an agenda. Then cybercrime emerged with the objective of obtaining money and information. Cyber warfare has emerged as the battleground of hacktivists and nation-states attempting to disrupt economic activity and affect infrastructure. Businesses — especially small businesses — evolve almost as quickly as security does, but threats evolve more quickly than either businesses or security.

Pain points of network security in the distributed enterprise

Consider several facts of network security life in the distributed enterprise:

- Throughput/security trade-off — The falling costs of broadband connectivity and online storage prompt a company to move more data to and from its network. But as rates of throughput increase, its five-year-old firewall becomes a bottleneck. The company now needs 1 Gbps firewall performance it cannot afford, so it lives with the trade-off between throughput and security, often turning off security features to achieve performance.
- PCI DSS — Retailers collecting credit card information must comply with Payment Card Industry Data Security Standards (PCI DSS). To build and maintain a secure network, the first requirement is to "install and maintain a firewall configuration to protect cardholder data."[3] The second requirement is to "not use vendor-supplied defaults for system passwords and other security parameters." While neither of these poses a stiff challenge to IT administrators at retail locations, they become two more items for central IT to verify for compliance.
- Ever-widening perimeter — Mobile workers, telecommuters and long supply chains continue to extend the perimeter farther from headquarters to employee homes and remote offices, decreasing the control IT has and increasing the organization's vulnerability.
- Mixture of firewalls — To reduce that vulnerability, remote sites buy, install and configure firewalls. However, the feature sets vary from one firewall manufacturer/model to another, resulting in a companywide patchwork of incompatible management consoles, security policies, signatures and update schedules.
- Wireless integration — Most remote sites use multiple wireless access points to give users flexibility in the workplace, and many sites in hospitality and retail use them to keep customers in the store spending money. But a wireless controller adds to the cost of remote site infrastructure, and if it is not integrated with the firewall, it may introduce yet more vulnerability at the perimeter.

Thus, the main source of network security pain is not the expansiveness of the distributed enterprise, but the lack of coordination between headquarters and the remote sites on the perimeter.

For example, assume that headquarters establishes a policy blocking access to video-sharing sites between 9:00 a.m. and 5:00 p.m. and implements it on the central firewall. How can it implement the policy across firewalls from different vendors at remote sites? At best, IT can

[1]*Elizabeth Weise, "Is insecurity the new normal?" USA Today, June 11, 2014*
[2]*"2014 Data Breach Investigations Report," Verizon Enterprise, April 2014*
[3]*PCI Security Standards Council, "PCI Quick Reference Guide," December 2009*

remotely manage the firewalls, but that requires manually configuring each of them for every policy change. At worst, IT must phone or send email with the policy and hope that each firewall supports rules and that each site has somebody who knows how to configure it.

Such a disjointed approach to security is a management headache because of the complexity of administering different firewalls. It is a compliance headache in that IT cannot easily and reliably report on policies at the perimeter. And it is a security headache because it results in inconsistent rules and inconsistent levels of safety.

The future of network protection lies in building a coordinated security perimeter that reduces vulnerability at the farthest reaches of the distributed enterprise's network.

What goes into the coordinated security perimeter?

Building security out that far entails not only hardware and software, but also centralization.

Assume an extreme case of a distributed enterprise in which one company with remote sites acquires another company with remote sites, and their networks and security levels are different. A coordinated security perimeter means centralizing these three elements:

1. Policies — Headquarters must consistently apply security policies and any internal practices required for compliance.
2. Interface — Applying those policies requires that IT administrators in headquarters and in remote locations use the same interface and terminology when they talk to one another. That goes beyond knowing SPI, DMZ, NAT and a few other acronyms to being certain that the firewall in each location implements security in the same way with the same interface.
3. Security features — The feature set of all firewalls should provide the same or complementary protection, in the following order:
   a. Content filtering, to block malicious code from risky websites that users visit
   b. Intrusion prevention, in case code slips through and probes the system for vulnerabilities like outdated signatures and runtime libraries
   c. Anti-malware, to keep downloaded executables from exploiting vulnerabilities and spreading through the network
   d. Application intelligence and control, to prevent rogue applications from impairing network efficiency

This hierarchical approach of security features working at each step goes a long way toward managing threats and keeping the network secure, but it is necessary for all firewalls to support the approach.

Centralizing these elements offers relief from management headaches, security headaches and compliance headaches companywide. Centralization is also the distributed enterprise's assurance that a strong, coordinated security perimeter is in place as far as its network extends.

SonicWALL TZ and the coordinated security perimeter for the distributed enterprise

The SonicWALL TZ series of firewalls is part of a tightly coupled security solution. It recognizes the need that many organizations have for central management and secure wireless connectivity. The TZ series addresses the distributed enterprise's biggest pain points in network security:

- As data moves faster, enterprises must have a firewall that can keep up. TZ products offer increased core count and core speed for performing Reassembly-Free Deep Packet Inspection® (RFDPI) on all traffic moving through the firewall without compromising throughput.
- All TZ products include a setup wizard that forces a change to the factory-default username and password, setting the organization up for PCI DSS compliance from the outset.
- The TZ series is suitably compact and affordable for remote sites, branch offices,

The future of network protection lies in building a coordinated security perimeter that reduces vulnerability at the farthest reaches of the distributed enterprise's network.

All SonicWALL products share the code base and the SonicOS security engine that earned the Dell SonicWALL E10800 a "Recommended" rating by NSS Labs.

retail locations and small office/home office (SOHO), offering protection at all points along the security perimeter.

- A perimeter with no firewalls is bad, but a perimeter with a hodgepodge of mismatched firewalls is not much better. All TZ firewalls provide the same level of security effectiveness found in SonicWALL enterprise products to keep policies, signatures and updates in sync companywide.
- The integrated wireless controller brings firewall security to wireless connectivity, allowing the creation and management of one set of policies for employees with trusted levels of access and another for visitors with only guest-level access. In several of the TZ firewalls, the wireless controller is compatible with SonicPoint 802.11ac access points.[4]

The TZ series is designed for central management and secure wireless in the distributed enterprise, coordinating network security at the perimeter with the corporate firewall. IT administrators companywide enjoy a consistent user interface that simplifies remote site management. All SonicWALL products share the code base and the SonicOS security engine that earned the Dell SonicWALL E10800 a "Recommended" rating by NSS Labs.

The Global Management System (GMS) is designed to centralize configuration and monitoring of every SonicWALL firewall in the distributed enterprise. From headquarters, IT administrators can see activity, push policies and updates, and examine threat detection on any TZ located at any site worldwide (see Figure 1). For new points on the perimeter, administrators can use GMS to image new TZ firewalls with the same policies and rules. As threats evolve and security needs change, GMS enables organizations to centralize management at headquarters, keep all remote sites in sync with the main firewall and enforce the same level of security at every point on the perimeter.

The SonicWALL TZ supports the hierarchical approach to security by progressively applying content/URL filtering, intrusion prevention, anti-malware and application intelligence/control to defend against attacks.

Benefits all around the distributed enterprise

Central management and secure wireless connectivity yield benefits all across the organization.

- IT has more control. Consistent UI and mode of operation in SonicWALL mean

Figure 1: SonicWALL TZ and the coordinated security perimeter for the distributed enterprise

[4]802.11ac is supported on the TZ300, TZ400, TZ500 and TZ600 models.

Share:

that IT does not need to remotely manage a variety of appliances or give different instructions for different products. IT can assure itself of security at the perimeter by uniformly inspecting all information that flows into and out of the network.

- The enterprise keeps up with demands for higher throughput. The SonicWALL TZ supports gradually escalating network speeds while adequately blocking a rising tide of attacks.
- Branch offices and remote sites speak the same language as headquarters. When local administrators work in the same TZ interface and security engine as corporate IT, the risk to the perimeter from miscommunication diminishes. Local staff installing a TZ firewall imaged at headquarters can be certain that their security is on par with that of the central firewall.
- Remote workers become part of the perimeter. A remote employee or telecommuter working behind a TZ is far less likely to infect the enterprise network with malware, especially when the firewall is centrally configured and controlled.
- Mobile workers stay secure as they move among access points. The SonicWALL VPN is based on a proprietary app designed to deliver security updates quickly and eliminate the variability of general VPN clients.
- Customers, visitors and guests enjoy secure Wi-Fi securely provided by the enterprise. When retail and hospitality companies deploy TZ firewalls to fulfill the customer expectation for high-speed wireless, they build loyalty to their brand without incurring security risk on the perimeter.

Conclusion

For distributed enterprises such as retail chains, banks and health care companies, cyberattacks at the perimeter have become a worrisome threat to headquarters. Yet customers, suppliers and employees stretch the perimeter as the business continually extends to branch offices, remote sites and SOHO. Although inconsistency among the firewalls deployed companywide makes network security elusive, the coordinated security perimeter is a strong model for defending against attacks everywhere.

SonicWALL TZ firewalls connected to a main SonicWALL firewall at headquarters offer the central management and secure wireless connectivity necessary to build a coordinated security perimeter for the distributed enterprise. With a consistent set of rules, a consistent level of anti-malware and a consistent user interface across the organization, security changes from a business inhibitor to a business enabler.

Local staff installing a TZ firewall imaged at headquarters can be certain that their security is on par with that of the central firewall.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

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

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.