# Executive brief: A coordinated security perimeter for distributed enterprise

Understanding the need for central management, secure connectivity and scalable secure switching

## Abstract

This paper describes the coordinated security perimeter, a model for extending protection for enterprise networks far beyond the safe confines of headquarters. This is achieved through central management, secure wireless connectivity and scalable secure switching.

## Introduction

Branch offices, retail stores, remote sites and mobile workers in distributed enterprises need to be connected to headquarters. At the same time, headquarters needs a simple way to maintain security policies across the distributed enterprise. 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.

## Security is not keeping up

As cybercrime and network attacks have become commonplace, security is always just playing catch-up.

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 offices — 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 in both speed and ability to block new threats. 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. 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. The seventh PCI DSS requirement is to "restrict access to cardholder data by business need-to-know." To enhance and maintain security, administrators should consider isolating sensitive business operations by implementing strong access control measures.
- **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 IT control and increasing the organization's vulnerability.
- **Mixture of firewalls** — To reduce that vulnerability, remote sites buy, install and configure firewalls. However, this adds complexity. 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. Compounding the problem, administrators are forced to use additional separate consoles to manage switches, wireless networks and WAN optimization. At the same time, they are often limited by the number of secure ports that can be controlled by each firewall. As a result they have limited flexibility in applying granular security controls.
- **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 consistent networks, resulting in coordination issues between headquarters and remote sites on the perimeter.

There can also be a lack of traffic visibility and control across the distributed network. For example, assume that headquarters establishes a policy blocking access to video-sharing sites between 9 a.m. and 5 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 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 someone who knows how to configure it.

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

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 complexity by integrating functions, and thus reduces vulnerability at the farthest reaches of the distributed enterprise 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 across all remote sites.
2. **Interface** — Applying those policies requires that IT administrators in headquarters and 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

An integrated 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 assurance for the distributed enterprise that a strong, coordinated security perimeter is in place, as far as its network extends.

## Conclusion

For distributed enterprises such as retail chains, banks and healthcare companies, cyber-attacks 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 small offices/home offices (SOHO). Although inconsistency and complexity among the firewalls deployed companywide makes network security elusive, the coordinated security perimeter is a strong model for defending against attacks everywhere.

**Learn more** about securing your distributed enterprise network with the SonicWall TZ Series.

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

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 Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

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**