Security, Manageability and Scalability for the Distributed Global Network
In recent years, the distributed enterprise has changed dramatically. The traditional model consisted of a central brick-and-mortar headquarters and multiple brick-and-mortar branch locations. While this hub-and-spoke model is still appropriate in certain cases, it no longer reflects the breadth of global business and network opportunities available. Today's modern distributed enterprise is everywhere.

**The everywhere enterprise**

Today's enterprise collaborates globally in real time. Technology trends such as interactive Web 2.0 transactions, high-speed mobile telecommunications and cloud-based Software-as-a-Service (SaaS) applications have opened new channels for conducting many forms of service and retail business at virtually any location from a standard Web browser, offering unprecedented levels of market agility and efficiencies-of-scale:

- Sales and marketing teams engage prospects and customers via Web 2.0, social media, point-of-sale kiosks and interactive displays
- Travelling field reps access CRM, marketing, sales and order entry applications over VPNs or from the Cloud
- Employees, contractors and outsourced specialists work from anywhere in the world, at any time of day or night
- Business is conducted from home offices, home offices and customer, partner and supplier sites
- Executives access network resources from hotel and airline club rooms
- Partners, vendors and consultants access "inside" application resources from "outside" locations, traversing internal and external third-party firewalls
- Core business applications are outsourced to third-party niche specialists and hosted SaaS providers
- Employees and support staff ensure business continuity and service level assurance after natural disasters or unexpected disruptions by working from home or other contingent sites, and accessing network resources over 3G and 4G cellular wireless connections
- Staff and customers access the Internet over wireless local area networks and guest services

Distributed enterprise network traffic no longer consists only of store-and-forward and session-based applications like email, Web pages and traditional client/server applications. It has now expanded to include:

- Web 2.0 applications
- Instant messaging (IM)
- Voice over IP (VoIP)
- Real-time collaboration tools
- Peer-to-peer (P2P) applications
- Wi-Fi and cellular wireless
- IP video surveillance

The business benefits of networking beyond the perimeter and the explosive workforce acceptance of web, mobile and cloud technology have made the traditional hardened perimeter model functionally obsolete.

**Distributed enterprise security and compliance concerns**

With new methods of gaining entry, financially motivated criminal attackers have unleashed ultra-sophisticated threats, increasing the risk of compromised data, systems downtime, reduced productivity, bandwidth consumption and monetary theft. In addition, web-based applications, such as social networking, gaming and streaming media, can diminish productivity and drain bandwidth from other critical applications. Distributed enterprise IT administrators now must address network security in a way that enables and extends business beyond the traditional perimeter.

- WiFi-enabled laptops, ultraportable PDAs and 3G/4G cellular smartphones have overtaken the predominant business role of traditional desktops
- Devices are more commonly located outside the perimeter, in homes, on third-party partner or customer networks, or as public access Internet kiosks in airports, hotels and cafés
- Outside of IT control, devices can be damaged, reconfigured, or lacking fundamental security maintenance and updates
- Mission-critical and sensitive information is stored on remote and mobile endpoint devices
- Employees routinely transport mobile devices off-site, and connect wirelessly over public and private networks
- Employee identities are stolen, hacked, sniffed or inappropriately shared
- Mobile devices get lost, borrowed or stolen
- Public Wi-Fi access must be segmented from sensitive financial or personal information
The impact on IT management

Today, while cyber criminals throughout the world are financially and even politically motivated, distributed enterprise IT administrators must defend their networks within ever-tightening budget restraints. However, implementing a wide array of emerging technologies regionally, nationally or even globally can add significant complexity and overhead costs to IT management.

Overwhelmed IT resources can also be ineffective in sufficiently monitoring, maintaining and updating security defenses. At the same time, governmental and industry regulatory mandates increasingly hold distributed enterprises liable for non-compliance (e.g., PCI, HIPAA or SOX). The cumulative impact on IT management is a growing pressure to spend less while defending against increasingly complex threats.

A comprehensive solution

Historically, distributed enterprises have had to settle for static point solutions that cannot dynamically adapt to continuously shifting threats or easily adjust to new technologies or business demands. These solutions also add complexity and related expense from purchasing, deploying, maintaining and administering separate non-integrated solutions, often from separate vendors. Unfortunately, attempts by some vendors to provide consolidated solutions have failed to effectively reduce complexity and related overhead expense.

Moreover, to sustain profitable growth, any security approach for the distributed enterprise must not only be effective across geographically dispersed areas, but also be able to easily and rapidly scale with enterprise expansion. A comprehensive solution for the distributed enterprise should enable organizations to:

- Deploy security solutions that are smart enough to adapt as the organization evolves—and as threats evolve—both dynamically and globally
- Maintain granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity
- Control, manage and protect their global network easily and automatically
- Receive and share threat and defense data around the world
- Anticipate and stop attacks before they happen
- Secure any user, any device, using any application from anywhere
- Collaborate securely across different networks
- Access any Carrier, SaaS, or Cloud application without diminishing security or performance
- Identify malicious activities on the network in real time
- Ease deployment to seamlessly scale for any distributed enterprise
- Configure firewalls on wireless networks to segment public from private traffic
- Secure reliable high availability over conventional and 3G/4G connections
- Provide optimal economic value and lower TCO

SonicWALL solutions for the distributed enterprise

SonicWALL's end-to-end suite of products and services meet the comprehensive security, manageability and scalability needs of distributed organizations, from end-user desktops, to mission-critical data and servers, to the perimeter gateway, to remote and mobile endpoints and beyond, including:

- Distributed Enterprise Security: gateway firewall, anti-virus, anti-spyware, anti-spam, anti-phishing, intrusion prevention, content filtering, and application intelligence and control
- Distributed Enterprise Management: automated monitoring and alerts; centralized reporting on bandwidth, web usage, productivity, PCI and other mandated regulations; site-to-site and offsite continuous data backup and recovery
- Distributed Enterprise Scalability: hardware, software, and virtual machine deployment options; secure remote access and remote help desk; self-discovering wireless networks; primary and failover support for 3G (and anticipated 4G) connectivity; and integrated dynamic routing

With award-winning product lines for distributed enterprise management, network security, secure remote access, email security, and backup and recovery, SonicWALL® has a solution that can meet the needs and budget of every distributed organization.

- SonicWALL SuperMassive™ E10000 Series is a Next-Generation Firewall platform designed for large networks to deliver scalability, reliability and deep security at multi-gigabit speeds
SonicWALL E-Class Network Security Appliance (NSA) Series solutions are deployable as Unified Threat Management (UTM) or Next-Generation Firewalls, combining powerful deep packet inspection with multiple layers of protection, application intelligence and control, and a suite of high availability features, offering the ultimate choice for larger distributed environments, campus network and data centers.

SonicWALL Network Security Appliance (NSA) Series solutions are deployable as Unified Threat Management (UTM) or Next-Generation Firewalls, adding reliability, functionality and productivity to branch offices, central headquarters sites and distributed mid-sized enterprise networks, while minimizing cost and complexity.

SonicWALL TZ Series solutions are available in Unified Threat Management (UTM) or Next-Generation Firewall configurations, offering standard and self-discovering Wireless-N configurations to instantly ramp-up remote and branch locations, keeping distributed enterprises agile and ahead of emerging Web 2.0 threats.

SonicWALL Global Management System (GMS) provides centralized real-time monitoring and comprehensive policy and compliance reporting for SonicWALL solutions, deployable as software, hardware appliance or as a virtual appliance.

SonicWALL ViewPoint offers an easy-to-use Web-based reporting tool that provides instant insight into distributed network health, performance, productivity and security (deployable as software or a virtual appliance).

SonicWALL Secure Remote Access (SRA) delivers flexible solutions for secure remote access, disaster recovery, and secure extranets across a wide range of endpoint platforms, including Macintosh®, Linux®, Microsoft® Windows 7 and Windows® Mobile, and Google® Android.

SonicWALL Email Security delivers the highest level of protection from inbound and outbound email threats, deployable as software, a hardware appliance or a virtual appliance.

In addition, SonicWALL network security solutions offer SonicWALL Clean Wireless protection, which secures the wireless connection, as well as inspects and encrypts the traffic flowing over the wireless network. When combined with SonicWALL SRA, they create a SonicWALL Clean VPN, which provides a multi-layered approach that enables you to decrypt and decontaminate all authorized SSL VPN traffic before it enters your network environment.

Available on the SonicWALL® NSA 2400MX appliance.