

# Consolidating SMB Network Security Infrastructure

Ways to Cut Costs and Complexity

**SONICWALL**<sup>®</sup>

PROTECTION AT THE SPEED OF BUSINESS<sup>®</sup>

# Table of Contents

Securing the SMB Network	1
Budgets are down	2
Risks are up	3
Point Solutions: Fragile and Complex	4
The Promise of UTM: Consolidated Security	5
SonicWALL TZ Series: Best-in-Class Consolidated Security	6
SonicWALL NSA Series: Best-in-Class Consolidated Security	7
The SonicWALL Advantage	8
SonicWALL Comprehensive Anti-Spam Service	9
SonicWALL Application Firewall	10
SonicWALL Clean Wireless	11
SonicWALL Clean VPN	12
SonicWALL GRID Network	13
SonicWALL Continuous Data Protection (CDP)	14
Conclusion	15

# Securing the SMB Network

In today's economy, small- to medium-sized businesses (SMBs) and their IT organizations need to do more with less. It is the responsibility of IT to optimize limited resources and garner the greatest return on budgets. Enterprises are already reaping the benefits of consolidation, centralizing data centers and embracing virtualization initiatives.



*The value of economizing through consolidation also applies to information security.*

SMBs have the opportunity to optimize productivity and minimize total cost of ownership (TCO)—while also maximizing security against Web 2.0-based threats—by consolidating multiple security technologies into a single Unified Threat Management (UTM) solution.

# Budgets are down

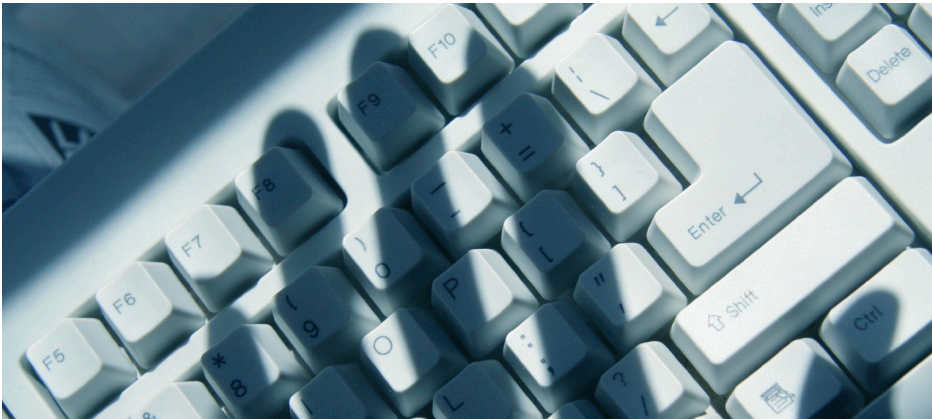
Forecasts show IT security budgets will continue a period of moderate contraction in the coming years or, at best, remain stable, due in part to the weakened state of the worldwide economy and the associated challenges this presents to the majority of businesses.

***Budgets are not the only factor  
weakening network security.***



Many SMBs have become complacent, when they don't see frequent reminders in the form of major, network-based attack in the news. And, they begin to feel that making further investments in network security may not be necessary. When faced with tighter budgets, some SMBs shortsightedly forego necessary security in the name of thrift.

# Risks are up



In reality, the volume, diversity, sophistication, and elusiveness of threats have substantially increased, in addition to the emergence of new Web 2.0 threats from microblogs and social media sites. As companies adopt emerging business technologies, the surface area subject to attack expands. Entry points for threats increase when SMBs rely more on mobility, virtual private networks (VPNs), interconnectivity and third-party access to network resources.

*Contrary to what complacent managers  
would have everyone believe,  
risks are actually on the rise.*

In addition, SMBs must comply with more legislation and industry regulations to avoid penalties or damage to their reputations. Without comprehensive and up-to-date protection, SMBs face malware infections, stifled productivity and regulatory non-compliance.

# Point Solutions: Fragile and Complex

Traditional standalone point products are not the best solution in combating this growing onslaught as they may not work seamlessly together to provide comprehensive protection. Cobbling together multiple security products to defend against the latest emerging threats can actually lead to a fragile “house of card” network resulting in the risk of network downtime, along with increases in cost and complexity.



***IT simply cannot keep up the balancing act.***

Point products demand complex manual integration and countless administrative hours to provide a coordinated defense. Administrators are unable to manage multiple point solutions easily. Each added point product drives up IT costs with separate expenses for staff resource time spent in training, deployment, maintenance and administration.

# The Promise of UTM: Consolidated Security

Multi-layered Unified Threat Management (UTM) solutions enable organizations to deploy broader and better-coordinated security countermeasures, easily and efficiently. However, many UTM products offer only a baseline of core traditional security tools (e.g., stateful packet inspection firewall, site-to-site IPSec VPN, intrusion detection and prevention, and anti-virus capabilities). Some solutions may incorporate anti-spyware and content filtering.

***To live up to its potential, UTM should consolidate all critical advanced features on a single platform.***

Many UTM products do not have the many security tools needed today and tomorrow. Consequently, you would be lacking SSL VPN, secure wireless, anti-spam, and application filtering and would still need to buy, deploy and manage separate appliances, which run counter the more seamless protection and efficient management benefits of consolidation. SonicWALL has overcome the limitations of other UTM offerings by consolidating all critical advanced features onto a single platform.

# SonicWALL TZ Series: Best-in-Class Consolidated Security

The all-new SonicWALL® TZ Series line of network security firewall offerings consolidate a broad range of advanced integrated UTM security services into a single, high-performance platform. Designed to maximize protection and minimize IT resource requirements, SonicWALL network security consolidates critical defenses necessary for protection against the latest advanced including sophisticated Web 2.0 threats. Going well beyond the standard UTM feature offerings, SonicWALL significantly elevates comprehensive protection by delivering a revolutionary set of features that are redefining the UTM market.

*SonicWALL TZ Series solutions deliver*



*consolidated UTM security for the SMB.*

SonicWALL TZ deployments can also be seamlessly integrated with SonicWALL's Continuous Data Protection (CDP) solution. This provides complete SMB protection by combining consolidated network security with easily deployed and managed data backup and recovery.

# SonicWALL NSA: Best-in-Class Consolidated Security

SonicWALL® Network Security Appliance (NSA) line of firewall appliance offerings are engineered to be the most scalable, reliable and highest performing multifunction threat appliances in their class. The NSA Series applies next-generation Unified Threat Management (UTM) against a comprehensive array of attacks, combining intrusion prevention, anti-virus and anti-spyware with the application-level control of SonicWALL Application Firewall.

*SonicWALL NSAs deliver*



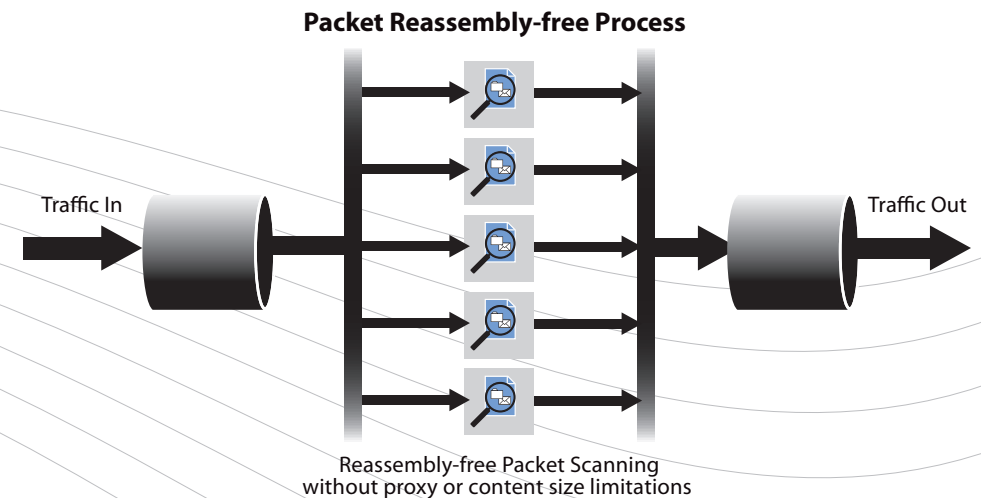
*consolidated UTM security for the SMB.*

SonicWALL NSAs can also be seamlessly integrated with the SonicWALL Global Management System (GMS). GMS provides medium-sized businesses and service providers with a flexible, powerful and intuitive tool to centrally manage and rapidly deploy SonicWALL appliances and security policy configurations.

# The SonicWALL Advantage

SonicWALL reduces the cost, complexity, and risk of a multi-point security solution, by consolidating multiple security technologies in one easily managed, affordable appliance. SonicWALL's high-performance hardware architecture, featuring Reassembly-Free Deep Packet Inspection™ technology in combination with specialized security microprocessors, delivers comprehensive and seamlessly coordinated protection without compromising network throughput.

*SonicWALL's consolidated UTM significantly out-protects other less-sophisticated solutions.*

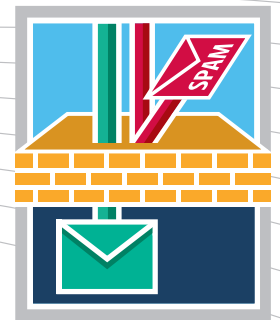


Designed to maximize protection and minimize IT resource requirements, SonicWALL network security consolidates critical defenses to protect against—and stay ahead of—the most advanced threats including sophisticated Web 2.0 threats. Going far beyond standard UTM feature offerings, SonicWALL UTM gives SMBs the ability to capitalize on a full range of UTM protection, including Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Enforced Client Anti-Virus, and Content Filtering. In addition, SonicWALL's new TZ Series and NSA Series also now integrates Comprehensive Anti-Spam Service, Application Firewall, Clean VPN, and Clean Wireless services into its protection capability, further detailed in the following pages.

# SonicWALL Comprehensive Protection

Vital for securing any network against the new more advanced Web 2.0 based threats, the SonicWALL Comprehensive Anti-Spam Service uses real-time sender IP reputation analysis and cloud-based Advanced Content Management techniques to remove spam, phishing and virus laden messages from inbound SMTP-based email before they reach your network.

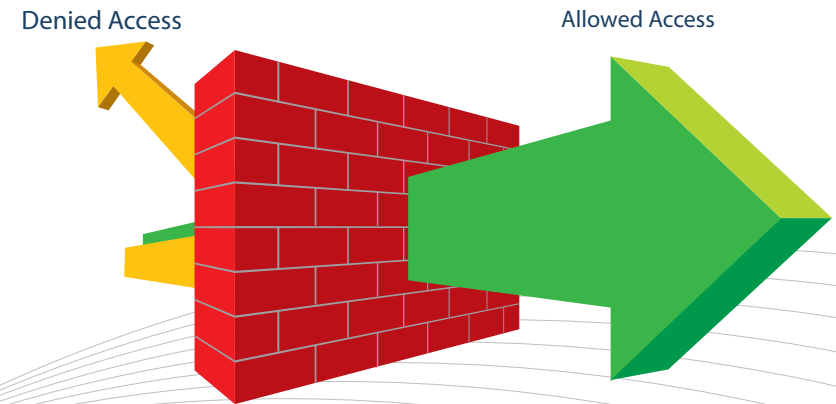
*The SonicWALL Comprehensive Anti-Spam Service  
delivers advanced spam protection  
at the network gateway.*



In just a few clicks, the SonicWALL Comprehensive Anti-Spam Service can instantly start filtering Simple Mail Transfer Protocol (SMTP) email traffic to remove spam, phishing and even virus-laden email. The SonicWALL Comprehensive Anti-Spam Service eliminates the need for less-effective, slow-responding and error-prone real-time blacklist services.

# SonicWALL Application Firewall

Most UTM products rely on stateful packet filtering, which primarily provides network-layer protection. Alternatively, SonicWALL UTM solutions provisioned with Application Firewall provide granular, application-specific policies that allow custom access control based on a wide range of attributes, including the individual user or application that is involved, the IP subnet they are on, and the time of day, week or month. Policies can even be set to restrict the transfer of specific files and documents, as well as to scan email attachments and other types of traffic for inappropriate content.



***SonicWALL Application Firewall extends protection beyond threats to the management and control of data and applications that pass through the network security appliance.***

Integrated with quality of service (QoS) features, Application Firewall can control bandwidth usage in a highly granular manner. For instance, administrators can guarantee priority bandwidth allotments for Voice/video over IP (VoIP), multimedia services, and business-critical applications, while restricting applications such as YouTube, Facebook, Instant Messenger and peer-to-peer file sharing, eliminating the need for separate bandwidth management products or application-specific security gateways.

# SonicWALL Clean Wireless



Clean Wireless delivers the innovative dual protection of high-speed secure wireless combined with high-performance UTM, which are required to both

- 1 Secure the wireless connection and;**
- 2 Inspect and encrypt the traffic flowing over the wireless local area network (WLAN).**

## *SonicWALL Clean Wireless extends UTM firewall security to your WLAN.*

The Clean Wireless solution goes beyond mere secure wireless solutions by enabling wireless networks to be as secure as wired networks using deep packet inspection, delivering greater security, performance, manageability and value to organizations of all sizes. By integrating 802.11n-compatible wireless access points with UTM network security appliances over a central point of management, Clean Wireless can support and enforce one set of security policies over both wired and wireless networks.

# SonicWALL Clean VPN

Today, your office is where you are: at home, at the airport, at a café. Customers, partners and contractors need access to your business from anywhere. In addition, uncertainties ranging from natural disasters, pandemics and terrorism to fires, power outages and hard drive crashes can threaten to disrupt network access. As more users continue to work from home it's more important than ever to allow these users access to internal network resources.

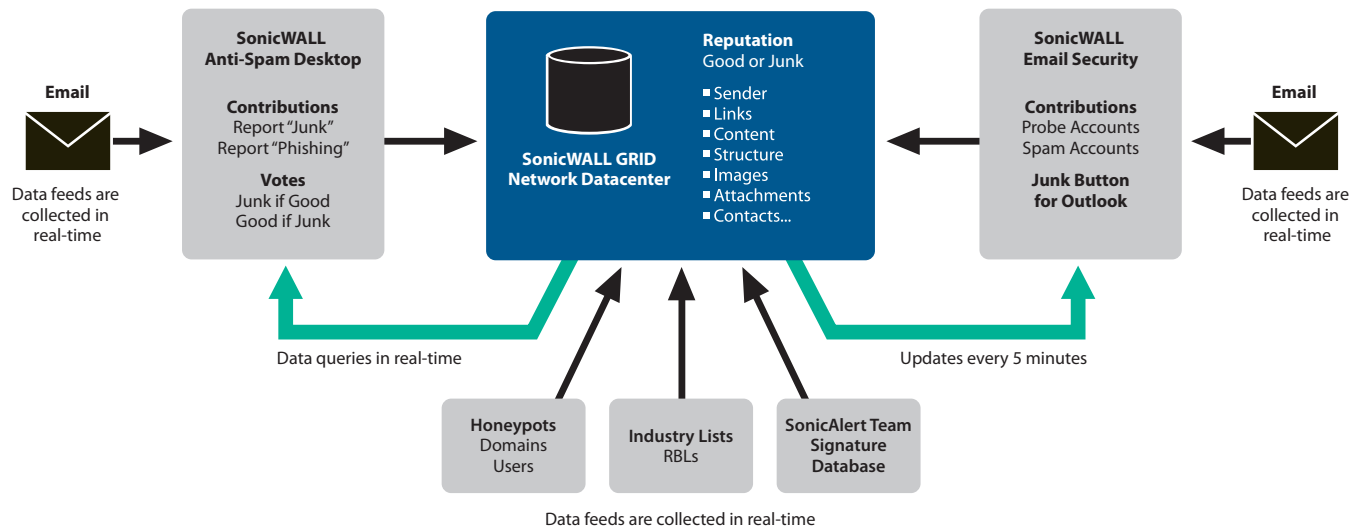


## *SonicWALL Clean VPN extends UTM firewall security to your VPN.*

Clean VPN consolidates the innovative dual protection of both SSL VPN and high-performance UTM. SonicWALL Clean VPN protects the integrity of VPN access by establishing trust for remote users and their endpoint devices, using enforced authentication, data encryption and granular access policy. It also secures the integrity of VPN traffic, establishing trust by cleaning and authorizing all inbound traffic for malware and checking all outbound VPN traffic in real time.

# SonicWALL and its GRID Network

SonicWALL Security leverages its GRID Network which consolidates cross-vector threat information from millions of business-focused sources around the world. Reputation-based threat protection information collaboratively gathered, analyzed, vetted, and then distributed securely, anonymously and in real time to improve the overall effectiveness of SonicWALL security solutions.



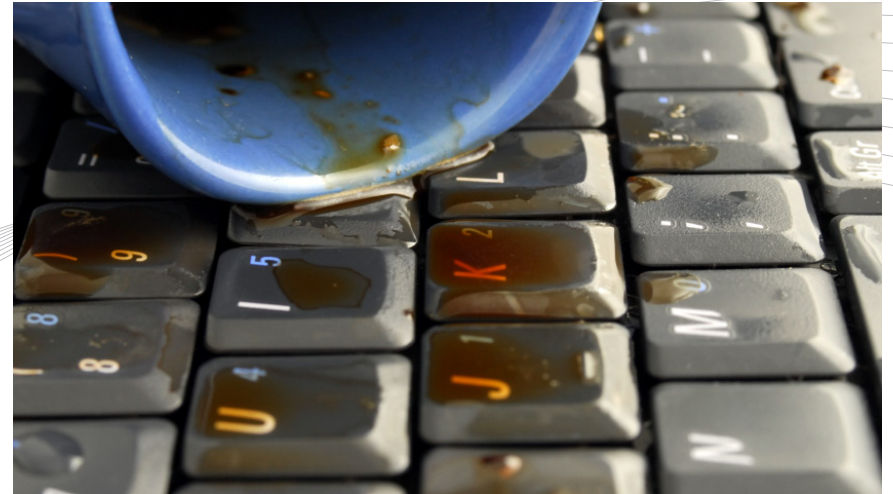
*The GRID's collaborative filtering process to be highly accurate and fully self-correcting.*

SonicWALL is actively developing and expanding the breadth of the information consolidated on the GRID Network, as well as integrating the range of SonicWALL solutions that contribute to and take advantage of this global threat monitoring information, in order to provide businesses with more comprehensive and responsive security solutions.

# SonicWALL Continuous Data Protection (CDP)

Further enhancing the protection of the all-new TZ Series or NSA Series, SonicWALL CDP offers SMBs the only complete end-to-end disk-based backup and recovery solution. SonicWALL CDP consolidates automatic transparent backup, user-directed restore, flexible disaster recovery options and low-touch administration for servers, desktops and mobile laptops.

*CDP offers the only complete end-to-end disk-based backup and recovery solution for SMBs.*



An ideal replacement for tape-based systems, CDP solutions provides foolproof, intuitive continual protection. Extensible across multiple platforms, CDP can instantly recover data, applications or entire workstation or server systems onto original, new or virtual devices.

# Conclusion



In today's economy, SMBs and their IT organizations need to do more with less. It is the responsibility of IT to optimize limited resources and garner the greatest return on corporate budgets. Cobbling together multiple point products and protect against a growing population of sophisticated Web 2.0 threats can result in a fragile "house of cards" network. Leading enterprises are already reaping benefits through consolidation, by centralizing data centers and embracing virtualization initiatives. By consolidating security around SonicWALL Unified Threat Management (UTM), your organization can better protect itself and eliminate the costs, complexity and risks of managing separate point solutions.

### **How Can I Learn More?**

- Download the Whitepaper: "Consolidating Network Security Infrastructure"
- Download the Whitepaper: "The FactPoint Group: 12 Ways UTM's Are Driving Security Consolidation"
- Read more about SonicWALL's Consolidation Solution
- Click here to opt in to receive SonicWALL newsletters

For feedback on this e-book or other SonicWALL e-books or whitepapers, please send an e-mail to [feedback@sonicwall.com](mailto:feedback@sonicwall.com).

**Forward to a Friend**

### **About SonicWALL**

SonicWALL<sup>®</sup> is a recognized leader in comprehensive information security solutions. SonicWALL solutions integrate dynamically intelligent services, software and hardware that engineer the risk, cost and complexity out of running a high-performance business network. For more information, visit the company Web site at [www.sonicwall.com](http://www.sonicwall.com).