



**The SonicWALL Approach to Consolidating Network Security Infrastructure and Cutting Costs**

### Introduction

Unrelenting pressure to do more with less has IT departments worldwide embracing techniques and technologies that help achieve consolidation, such as having fewer centralized data centers and using virtualization products to significantly reduce server count. The same pressure applies to information security. Consolidation is an appropriate response. By taking advantage of modern Unified Threat Management (UTM) solutions, organizations can substantially reduce the cost and complexity of their security infrastructure while not only maintaining its effectiveness but actually boosting it. UTM also frees up resources to help address other, emerging business-critical issues and projects.

This brochure identifies the substantial benefits available to organizations that elect to replace their ever-increasing collection of network security point products with consolidated UTM devices. It further explains the combination of innovative features/functions and robust, platform-level capabilities that enable customers of SonicWALL® UTM products to maximize their gains due to consolidation.

### The Network Security Challenge

These days the mandate to do more with less is essentially pervasive. And perhaps for no domain is this mandate more applicable than for network security. After all, budgets are coming under fire at the same time that risks are on the rise.

### Budgets are Down

Consistent with a relatively recent trend, most projections forecast that IT security budgets will continue a period of moderate contraction in the coming years or, at best, remain stable. This is due in part to the weakened state of the worldwide economy and the associated challenges this presents to the majority of businesses. However, the economy is not the only factor contributing to a the downward trend for security budgets.

Another contributing factor is that within many organizations, management has become a bit complacent. They see there's been no major, network-based attack in the news recently and feel that making further investments in network security is not really necessary.



### Risks are Up

Contrary to what complacent managers would have everyone believe, the risks facing today's IT-enabled businesses are actually on the rise.

- There has been a substantial increase in the volume, diversity, sophistication, and elusiveness of threats, as attacks on individuals and corporations alike have evolved from little more than a game to a lucrative, albeit illegal, business.
  - The surface area open to attack continues to expand as organizations, in order to remain competitive, steadily adopt emerging technologies, buy or build new applications, and upgrade the ones they already have.
  - Similarly, the points of entry for threats are multiplying as businesses strive to improve their bottom line by embracing greater degrees of user mobility, interconnectivity, and third-party access to networked systems.
- Organizations also must demonstrate compliance with the mounting collection of legislation and industry regulations to avoid punitive penalties and, more importantly, damage to their reputations.

The net result is that organizations clearly can't afford to stand by and do nothing when it comes to network security – but neither can they afford to incur the expense of continuing to pursue a conventional strategy based on implementing an ever-expanding collection of point products. Fortunately, there is an alternative that is not only affordable but also highly effective.

### **The Response: Unified Threat Management-enabled Consolidation**

For most IT departments, consolidation is already a familiar concept. Indeed, many shops have projects already underway to reduce the number of servers, data centers, or different types of storage solutions they need to operate. These organizations may even consider consolidation a business imperative.

In any event, UTM devices are effectively an application of the same concept of consolidation to the discipline of network security. The goal with UTM is to simplify an organization's network defenses despite all of the factors that are causing the security problem to grow in both scope and complexity. At a high level, this is accomplished by combining multiple countermeasures that provide protection against multiple types of threats operating across multiple layers of the computing stack in a single physical device. Ideally, this UTM solution is suitable for deployment in multiple locations on an organization's network.

Putting aside for now the detailed requirements that must also be addressed to yield a product that is appropriate for enterprise-class deployments, the result with UTM is a solution that conveys a remarkable number of benefits – particularly relative to traditional, point-product based approaches to network security.

### **Reduced Cost of Ownership**

Taking advantage of UTM appliances to replace or obviate the need for further point products will substantially reduce both the capital and operating expenditures associated with an organization's network security infrastructure. Savings in this regard can be attributed to:

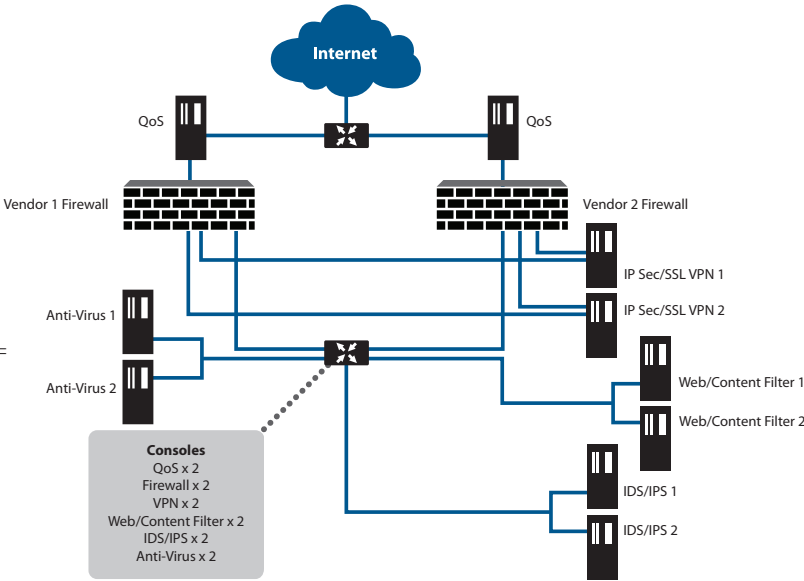
- Being able to purchase considerably fewer products, as well as associated management systems and server hardware
- Possibly having less and simpler network infrastructure (e.g., switches, routers, and load balancers) as a result of needing to plug fewer devices into fewer ports
- Requiring less power (providing a "green" solution) and consuming less data center space
- Reducing requirements for operator training
- Requiring considerably less effort for ongoing management tasks such as policy configuration, event analysis, and reporting due to having a single, integrated management console
- Having fewer software components, systems, network devices, and vendor relationships to maintain



The precise savings that can be achieved is difficult to predict due to the number of factors involved. However, it is not uncommon to see an aggregate recovery of 50% or more – a level that is fairly easy to attain when you consider the following example.

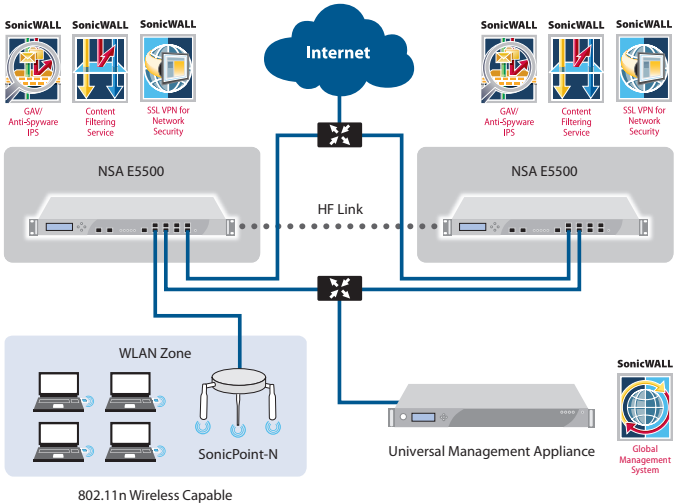
**Before:**

- 4 Consoles
- 12 Appliances/Servers
- 250 watts/appliance x 12 = 3,000 watts
- Training = 7 vendors x \$2,500 = \$17,500



**After:**

- 2 x SonicWALL NSA E5500
- 1 x SonicWALL UMA EM5000 (includes 10 nodes)
- 81 watts/SonicWALL NSA appliance x 2 + 125 watts x 1 = 286 watts
- Training = 2 vendors x \$2,500 = \$5,000



Another consideration in this regard is the number and types of locations where Unified Threat Management appliances can be used. In particular, with multi-gigabit processing capabilities, modern UTM products are actually well suited for providing comprehensive protection not just at Internet boundaries, but on internal networks as well – for example, between different zones or as a gateway to a data center. On an absolute basis, this increases the potential for reduced cost of ownership even further.

**Enhanced Security**

Another advantage that Unified Threat Management has over point products is the potential to deliver superior stopping power. Because UTM is a consolidated solution with a much lower cost of ownership, it may very well enable some organizations to engage a greater set of countermeasures than would otherwise be within their means.

Further gains are also possible based on having both integrated processing and integrated management capabilities. By internally sharing and correlating the findings of individual countermeasures and then facilitating a coordinated response, UTM solutions can efficiently achieve a level of effectiveness that would otherwise require a substantial amount of manual integration among disparate products. Similarly, having integrated management means that all of the security settings pertaining to a given domain can be established and maintained in a single place – a characteristic which inherently helps minimize an all-too-common occurrence with point products where miscommunication and/or misconfiguration basically allows threats “to slip through the cracks.”

### **Additional Considerations**

In addition, UTM has a handful of other value propositions that should be acknowledged, including:

- Its capacity to reduce infrastructure complexity
- The corporate goodwill that embracing a “green” solution can yield
- The investment protection that comes from having a modular and extensible solution where additional capabilities can be “turned on” as needed

The good news is that most of the benefits discussed above can be attained, at least to some degree, with pretty much any UTM solution. What sets SonicWALL apart, however, is the emphasis placed on enabling enterprises to *maximize* these gains. Specifically, we allow our customers to pursue a much greater degree of consolidation and, therefore, achieve a much greater return than would be possible with competing UTM products by:

- Providing a broader set of countermeasures and related networking capabilities
- Ensuring the quality and robustness of the platform on which they operate

### **SonicWALL Goes Above and Beyond the Competition**

The vast majority of UTM products provide little more than a core set of traditional security tools, such as stateful packet firewall, IPSec VPN, intrusion detection/prevention, and anti-virus capabilities. Some of the better ones may incorporate anti-spyware and Web/URL filtering as well. In contrast, SonicWALL introduces the potential for even greater degrees of consolidation by also delivering several sets of capabilities that are fairly unique within the UTM market.

### **Integrated Clean VPN**

IPSec VPN technology is considerably less well-suited to enabling remote access by individual and mobile users than it is to the scenario of establishing secure, site-to-site connectivity between multi-person offices. The problem lies in the effort required to pre-distribute, pre-install, and subsequently manage the requisite client component (i.e., VPN agent). SonicWALL has addressed this shortcoming by provisioning its UTM appliances with integrated SSL VPN capabilities. With this Clean VPN feature set:

- Users can remotely connect to network resources by accessing a personalized portal from any Web browser
- Administrators are freed from having to install and maintain another piece of client software given that SonicWALL network security appliances automatically push the NetExtender thin client to remote users’ PC, Mac, or Linux-based computers once they access the portal
- A Web-based graphical user interface makes configuration of all SSL VPN parameters a simple, straightforward exercise
- All traffic coming into the network via the SSL VPN gets processed by the UTM appliance’s deep packet inspection engine, providing advanced protection against viruses, spyware, and other forms of malware

Plus, there is the consolidation benefit. For some organizations the availability of an integrated SSL VPN will obviate the need to maintain a separate, dedicated secure remote access device at their branch, regional, and possibly even headquarters locations.

### Application Firewall + Embedded QoS

Whereas most UTM products rely on stateful packet filtering (a technology focused primarily on providing network-layer protection), SonicWALL UTM appliances are also provisioned with an Application Firewall. As a result, IT departments have two formidable sets of capabilities at their disposal. First, they can configure 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 whatever content is deemed inappropriate.

The second set of capabilities ties in SonicWALL's onboard quality of service (QoS) feature set, which includes industry standard 802.1p and Differentiated Service Code Points (DSCP) Class of Service (CoS) indicators. Combined with the in-depth application awareness afforded by the SonicWALL Application Firewall, the net

result is the ability to control bandwidth usage in a highly granular manner. For instance, VoIP, multimedia services, and business-critical applications can be configured to receive priority treatment and have guaranteed bandwidth allotments. Alternately, the bandwidth available to less desirable, user-centric applications such as YouTube or Facebook can be restricted by enforcing a customizable upper limit.

Once again, there is also considerable potential for consolidation. The presence of these capabilities in SonicWALL UTM appliances will, in many instances, eliminate the need to implement separate bandwidth management products or separate application-specific security gateways, such as those used to control instant messaging (IM) and peer-to-peer (P2P) file sharing.

### Clean Wireless

Widespread use of wireless local area networks (WLAN) technology within enterprise networks continues to be constrained by lingering concerns about security; the cost and complexity of deployment and ongoing management; performance limitations; and the ability to adequately support a modern portfolio of bandwidth-hungry, latency-sensitive applications. Clean Wireless is the SonicWALL response to this situation. One of the key facets of Clean Wireless is the inclusion of a wireless access switch/controller (WAC) in our UTM appliances<sup>1</sup>. Not only does this eliminate the need for yet another, separate, standalone device, but it also yields two critical advantages in the areas of WLAN security and performance.

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).

Clean Wireless also enables use of the UTM's bandwidth management capabilities to granularly control how wireless bandwidth, which is a relatively limited commodity, can be used. This way administrators can ensure that critical or sensitive applications have the resources they need to perform adequately.

*"We are extremely pleased with our NSA 2400 from SonicWALL. It was up and running less than 4 hours following the catastrophic failure of our previous firewall, has been very reliable, and is a breeze to administer. It's met all of our needs from a security perspective and even allowed us to eliminate a couple of network devices, a switch and a router."*

**Robert Smith**  
Director of Information Technology  
Linda Hall Library – Kansas City, MO

<sup>1</sup> For a detailed explanation of the full solution, users are referred to the Clean Wireless data sheet and the associated white paper Secure Wireless Made Easy – Selecting a Next-Generation Solution for Pervasive WLAN Implementations, both of which are available at [www.sonicwall.com](http://www.sonicwall.com).

## Comprehensive Anti-Spam Service

Anti-spam is another area where SonicWALL provides a unique opportunity for consolidation. For competing UTM products that actually include anti-spam functionality, it is usually a fairly rudimentary capability based on little more than the implementation of real-time black lists (RBL). In contrast, SonicWALL's Comprehensive Anti-Spam Service filters email traffic by employing multiple, complementary layers of inspection and analysis.

- SMTP traffic arriving at the external interface of SonicWALL network security appliances is first checked using traditional IP reputation techniques, such as RBLs. This helps remove messages from known bad senders as well as those associated with directory harvest, denial-of-service, and backscatter attacks.
- Email traffic is then inspected using SonicWALL's proprietary GRIDprint technology. GRIDprints are security signatures that are automatically generated and distributed to SonicWALL devices based on real-time analysis of data collected from the SonicWALL GRID Network, consisting of over 4 million business endpoints, hundreds of millions of messages and billions of reputations votes.
- With 80-85% of all bad messages having already been eliminated by this point – at the connection level no less – SonicWALL's cloud-based Advanced Content Management (ACM) service is engaged to clean up the rest. ACM applies Adversarial Bayesian Analysis featuring over a dozen inspection techniques including advanced text and image parsing, lexicographical distancing, gibberish detection, and multi-layer antivirus protection.

In addition, the Comprehensive Anti-Spam Service is:

- Easy to install – it can be initiated with a single mouse click, with no need to redirect MX records or reconfigure network settings
- Easy to manage – an integrated, single point of management, configuration, and reporting reduces weekly administrative effort to only a few minutes per week
- Easy to use – quarantine mail boxes can be configured and customized for per-user processing of suspected junk mail
- Thorough and transparent – Unlike with many competing products, any size message can be scanned and all actions taken by the reputation service are logged

The result is an economical yet powerful approach that is well-suited to smaller organizations that require anti-spam coverage but otherwise do not need the full set of advanced functionality typical of a dedicated email security gateway. Of course larger organizations may also find it useful, particularly as an affordable, extra layer of protection when trying to establish a defense-in-depth strategy for email security.

## Ensuring All of the Right Pieces are in Place ... And Then Some

The presence of numerous security and networking capabilities in a single device is not sufficient. The effectiveness of a UTM solution as a means for achieving consolidation also depends on the strength of the underlying platform: all of the components that comprise a complete solution and the details of how they are brought together. No meaningful gains will be possible unless the UTM solution can perform all desired functions at a high rate of throughput and with minimal latency. This can only occur if unless it can be efficiently managed and fits seamlessly into an organization's computing environment.



In this regard, some of the leading features and characteristics that ensure SonicWALL network security appliances are appropriate not just for SMBs, but for larger enterprises as well. These are identified in the table below.

#### **Powerful performance**

- SonicWALL UTM products have been purpose-built and optimized from the start to be multi-function security devices, as opposed to starting with a firewall, switch, or router and bolting on a bunch of security countermeasures
- SonicWALL high-capacity UTM devices feature a specialized multi-core processing and inspection architecture
- Besides the anti-spam and bandwidth management capabilities to pre-filter traffic and reduce processing load, SonicWALL UTM products also feature innovative and efficient processing and inspection techniques such as Reassembly-free Deep Packet Inspection™ technology

#### **Maximum manageability**

- By using the SonicWALL Global Management System, all lifecycle management functions are centralized, consolidated, and simplified; policy development is straightforward, yet granular and flexible; and role-based administration is fully supported
- Dynamic threat protection, content filtering, and application control services are continually updated on a 24x7 basis to maximize security and minimize administrative effort

#### **Comprehensive compatibility**

- With more than a dozen network security appliances to choose from, organizations are assured of being able to select units that are well-aligned with their needs from the perspective of price/performance and functionality
- Numerous features and selectable options are typically available for items such as IP address assignment, NAT, VLANs, routing, QoS, user authentication, VoIP, load balancing, high availability, event logging, VPN encryption, and WLAN security

### **Maximize Your Consolidation Benefits with SonicWALL**

Consolidation is a proven and highly effective strategy for reducing IT complexity and cutting costs. In the case of network security, using modern UTM appliances in place of a disparate collection of point products can also convey the added benefit of enhancing an organization's defenses – not to mention its compliance with an ever-growing volume of information privacy, security, and governance regulations. The extent to which these and other associated benefits will be realized, however, depends on the scope and utility of the specific security and networking capabilities that are included, along with the strength of the underlying platform on which they run.

SonicWALL provides businesses with the opportunity to maximize their gains when pursuing a UTM-enabled, network security consolidation initiative, because the SonicWALL portfolio of network security appliances

- Include support for the full range of traditional security capabilities, such as stateful packet inspection, IPSec VPN, intrusion prevention, anti-virus, anti-spyware, and content filtering
- Include support for an unrivaled set of advanced capabilities, such as integrated SSL VPN, an application firewall, onboard QoS, an embedded wireless access controller, and comprehensive anti-spam
- Are based on an enterprise-class platform featuring robust capabilities in the crucial areas of performance, manageability, and network compatibility

For further information on SonicWALL's extensive portfolio of Unified Threat Management network security appliances including *Application Firewall*, *Clean VPN*, *Clean Wireless* and *Comprehensive Anti-Spam Service*, please refer to [www.sonicwall.com](http://www.sonicwall.com).

#### **SonicWALL, Inc.**

1143 Borregas Avenue  
Sunnyvale CA 94089-1306

T +1 408.745.9600  
F +1 408.745.9300

[www.sonicwall.com](http://www.sonicwall.com)



PROTECTION AT THE SPEED OF BUSINESS™