

## Reducing Total Cost of Security Ownership

*Reducing the total cost of security to ensure the greatest possible return on technology investments.*

### CONTENTS

Demand for Cost-effective Security	2
Reducing Costs of Operational Performance	3
Reducing Costs of Implementation	4
Reducing Costs of Management	5
SonicWALL Solutions	5
Conclusion	6

## Abstract

At a time when value is paramount, IT must lower the total cost of security and ensure the greatest possible return on its technology investments. SonicWALL® contends that IT must consider reducing costs in each aspect of their security technology, particularly the individual costs associated with operational performance, implementation and management. In order to keep a technologically competitive edge while cutting costs, a status quo approach is no longer sufficient. Through deliberate comparison, it is clear that SonicWALL offers an effective alternative with which to significantly reduce the total cost of security ownership.

## Demand for Cost-effective Security

During uncertain economic times, executives and shareholders demand greater accountability from IT on staffing and technology expenditures, and pull in the reins on discretionary budgets. Today, it is mandatory for IT to lower the total cost of security and ensure the greatest possible return on its technology investments.

Simultaneously, with the explosive pace of innovation in media, applications, platforms, connectivity and bandwidth, business users are demanding more from technology than ever before in order to derive competitive advantages in the marketplace. To gain an edge, businesses expect technology to help them to be first to market with flexible offerings that respond to the needs of customers. Breakthroughs in technology can help companies get business done anywhere, anytime, in larger volumes and at an increasingly faster pace.

Despite their advantages, however, these emerging technologies tend to be prone to vulnerabilities that can be readily exploited by professional attackers. No longer simply students out for the prestige of showing they could compromise a system, today's exploit developers are backed by profit-driven criminal organizations that seek to gather login credentials to financial sites for financial theft, identity theft, and pump-and-dump stock schemes. In response to skyrocketing increases in malicious attacks, industry and government regulators require ever-tighter security in order for IT to meet compliance or else face stiff penalties.

The explosive availability of bandwidth is one case in point. A T1 connection, typically costing \$3,000 a few short years ago, might now be available for \$300 per month—or one tenth the cost, and there are other options available for even less. While this increase in bandwidth potentially gives businesses ten times the available throughput per dollar, it also gives hackers ten times the bandwidth in which to hide malware and other attacks. IT must now manage and secure ten times the flow of traffic previously traversing the network, without a corresponding increase in budget, staffing or invested infrastructure performance. At a time when value is paramount, IT is faced with doing more with less.

While it has been said that nobody gets fired for buying a status quo solution, in order to keep a technologically competitive edge while cutting costs, a status quo approach is no longer sufficient. Instead of locking up or restructuring infrastructure at the demand of proprietary vendors, IT must maintain the flexibility to consider alternative innovative solutions that can engineer the costs out of technology without sacrificing levels of expected security and performance.

When comparing security solutions, of course, there are more costs for IT to consider than just sticker price. Secondary costs include: bottlenecks to network throughput and business productivity, losses due to security insufficiencies resulting in breaches or regulatory noncompliance, technical staffing costs required for implementation and administration, restricted integration or scalability and even energy consumption. Whichever solutions are applied, in order to reduce the total cost of security, IT must consider potential cost reductions in each aspect of their security technology, particularly the individual costs associated with operational performance, implementation and management.

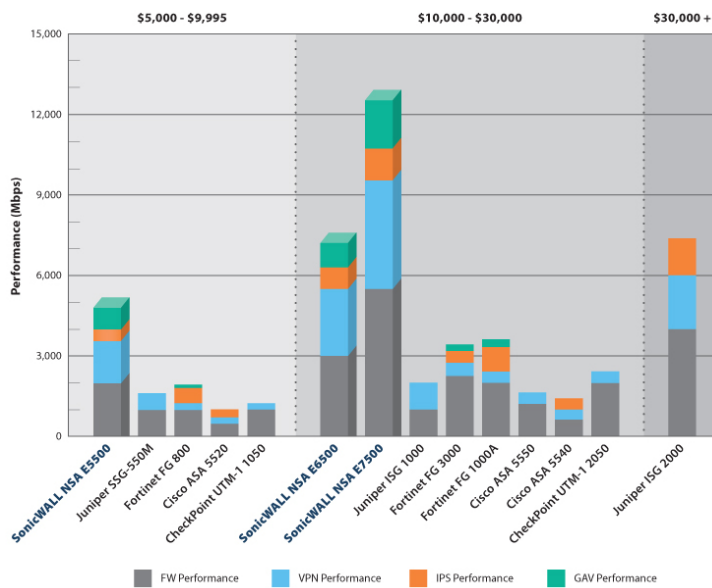
## Reducing Costs of Operational Performance

Still, no security solution is worth the price if it cannot deliver the operational performance needed to add business value. A security solution should not come at the cost of transactional downtime, restricted communications, reduced productivity or overburdened IT resources. Rather, it should be engineered to eliminate bottlenecks and streamline processes to deliver protection transparently to business operations. In order to add substantive value, a solution must perform its security tasks without complicating management, and thus allow an organization to enhance productivity and focus on its core business. In short, a solution shouldn't cause denial-of-service—it should prevent it.

Unified Threat Management (UTM) solutions offer an example. While malicious attacks can penetrate stateful packet inspection firewalls, early attempts at deep packet inspection with UTM often resulted in significant performance reduction. Today, certain solutions have been engineered using innovative technology such as multi-core processing and Reassembly-Free Deep Packet Inspection (RFDPI) to break through these restrictions, while others have not. The chart below compares the performance of several enterprise-class network security solutions.<sup>1</sup>

### Comparative Enterprise UTM Performance (Mbps)

Performance: SonicWALL E-Class NSA Series vs. Competition



<sup>1</sup>Competitive performance data sources:

- Check Point Network Security data sheet (April 18, 2008 P/N 502887);
- Cisco Models Comparison ([http://www.cisco.com/en/US/products/ps6120/prod\\_models\\_comparison.html](http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html));
- Fortinet Unified Threat Management (<http://www.fortinet.com/doc/FortinetMatrix.pdf>);
- Juniper Networks SSG 140 data sheet (100181-007 Feb 2008);
- Juniper Networks SSG 300 Series data sheet (100203-005 Feb 2008);
- Juniper Networks SSG 500 Series data sheet (100143-007 Jan 2008);
- Juniper Networks ISG Series data sheet (110036-017 Apr 2008);
- Nokia IP390 data sheet (NI3 062 041).

This sampling demonstrates the wide performance variance between solutions. Not only can solutions offer differing layers of UTM protection (e.g., Gateway Anti-Virus, Intrusion Protection, etc.), but their scanned traffic throughput varies significantly: the highest-rated throughput is roughly twelve times higher than the lowest-rated throughput.

However, raw performance does not necessarily directly equate to value. A fundamental benchmark for cost-to-performance in a security solution is the number of megabits of traffic analyzed per second compared to total cost. The chart below compares the cost-to-performance value of the same network security solutions.<sup>2</sup>

**Comparative Cost of Performance (\$/Mbps) for Enterprise Class UTM**

Vendor	Model	Firewall	VPN	IPS	GAV	Overall Average
Checkpoint	UTM-1 2050	7.75	38.75	--	--	6.46
	UTM-1 1050	12.50	6.66	--	--	12.50
Cisco	ASA 5550	18.33	51.76	--	--	13.54
	ASA 5540	26.15	52.29	37.77	--	11.93
	ASA 5520	24.44	48.89	29.33	--	10.48
Fortinet	FG 3000	8.89	37.73	49.99	79.98	5.83
	FG 1000A	7.50	37.49	15.00	74.98	4.17
	FG 800	10.00	49.98	16.66	66.63	5.13
Juniper	ISG 2000	11.00	22.00	31.43	--	5.95
	ISG 1000	25.00	25.00	--	--	12.50
	SSG-550M	10.50	21.00	--	--	7.00
SonicWALL	NSA E5500	5.00	6.66	18.17	13.33	2.08
	NSA E6500	4.67	5.60	16.46	15.55	1.93
	NSA E7500	4.54	6.25	20.83	13.89	2.00

Once again, it is significant to note that among different solutions the results can vary widely: the highest overall average cost-to-performance figure is nearly seven times the cost of the lowest figure (*highlighted above*). Through deliberate comparison, it is clear that SonicWALL solutions now offer an effective alternative with which to significantly reduce security costs associated with operational performance.

## Reducing Costs of Implementation

Reducing the upfront implementation costs associated with acquisition and deployment makes an immediate impact on budgetary targets, and therefore is frequently a determining factor in whether a particular solution ultimately receives approval for go-ahead. Proprietary “status” brands also inherently carry an additional sticker shock, and generally should be avoided in preference of alternative solutions that can deliver equivalent or greater effectiveness at a lower price point.

To reduce acquisition costs, therefore, IT must seek out vendors who are best able to integrate cost-efficiencies into manufacturing their solutions that can reduce overall acquisition costs, without decreasing value. For instance, SonicWALL leverages non-proprietary, industry-standard platforms and commercially-

<sup>2</sup> Megabit-per-second costs are listed in US\$ based upon published list price and performance data as cited above. Categorical UTM component feature performance figures are calculated independently at total UTM solution list price divided by maximum throughput in Mbps per individual component. Overall Average \$/Mbps figure is calculated at total UTM solution list price divided by total UTM throughput.

available chipsets, while adding value by applying superior software intelligence to increase performance and security. Acquisition costs may also be lowered by selecting vendors who can take advantage of the economies of scale associated with an extensive and efficient distribution network.

Deployment of overly complex proprietary solutions can also add to implementation costs. IT departments are stretched to accomplish faster speed-of-deployment with fewer staff. Every extra minute spent learning, installing, configuring and integrating a security solution takes IT resources away from other mission-critical and revenue-generating projects, and keeps employees, partners and customers waiting to access the resources they need.

## Reducing Costs of Management

Businesses no longer need to view security as an arcane mystery that warrants an overpriced, difficult-to-manage solution. In the past, security was perceived as highly complex, demanding an overly esoteric and expensive response requiring closed black boxes and high-priced consultants. If corporate IT wished to be directly involved, technicians needed to overcome steep learning curves to master proprietary console commands on a seemingly endless number of individual administrative interfaces. Over time, however, IT managers have deployed multiple generations of firewalls, and have now become well versed in a wide range security technology issues, such as secure remote access, e-mail productivity, data retention, regulatory compliance, data leakage and business continuity. Unfortunately, there remain certain vendors who still continue to increase the cost and complexity of their solutions, without correspondingly increasing value in relative performance and security.

IT now has the option to consider innovative, alternative solutions that are engineered to simplify managing and administering security. For example, as security threats have become more sophisticated, IT has matured away from complex single-point solutions that respond to individual threats (e.g., viruses, worms, malware, Trojans, spam) as they arise. Instead, IT has shifted toward a simpler-yet-comprehensive Unified Threat Management (UTM) approach.

Additionally, solutions that adopt a unified management approach can often reduce administrative costs by providing the capability for a centralized management interface that applies intuitive object-based models and flexible reporting capabilities. Global management and reporting helps prevent costs incurred from regulatory noncompliance, particularly where it can provide proactive alerts, real-time monitoring, and historic trending analysis across multiple security components. Costs can also be reduced by solutions that automate management tasks.

## SonicWALL Solutions

SonicWALL has an established record of relentlessly engineering the cost out of high-performance secure networking to provide a value alternative to status quo solutions. SonicWALL is uniquely positioned in the industry to eliminate costs out of building and running secure networks through strategically reducing:

- **Operational Performance Costs** by delivering elegant, high-utility, real time threat and data protection solutions in a security-as-service model;
- **Implementation Costs** by integrating leading-edge software intelligence with ultra high-performance state-of-the-art commercially available chipsets delivered on industry standard hardware platforms, providing solutions that simplify complex setup while seamlessly fitting into the most demanding network infrastructures;
- **Management Costs** by delivering globally-managed, centrally-administered products and dynamic security service offerings.

And yet, SonicWALL solutions do not sacrifice performance for cost-efficiency. SonicWALL streamlines business security, freeing resources to enhance productivity and profitability, by integrating dynamically intelligent services, software and hardware into a comprehensive offering of high-performance security solutions, including:

- **Unified Threat Management (UTM)** that applies a multi-tiered proactive network security defense featuring ultra-high-performance multi-core platforms and a patented Reassembly-Free Deep Packet Inspection technology (U.S. Patent 7310815) to deliver real-time detection and protection through a suite of services including gateway anti-virus, anti-spyware, intrusion prevention, anti-spam and content filtering.
- **Secure Remote Access** featuring SonicWALL SSL VPN and award-winning SonicWALL Aventail E-Class SSL VPN technology, which enables remote and mobile employees, partners and customers to access mission-critical resources with granular policy control, endpoint interrogation, clientless Web deployment, and unified policy management.
- **E-mail Security and Anti-Spam** providing inbound protection against spam, viruses, phishing and other e-mail threats as well as outbound protection from confidential information leaks.
- **Continuous Data Protection (CDP)** offering automatic, real-time tape-free data backup and recovery for network servers, laptops and PCs.
- **Global Management System (GMS)** enabling IT to manage a few or thousands of SonicWALL appliances from a central location, along with real-time ViewPoint reporting

## Conclusion

The cost of security should be measured not only by list price, but in the sum total of operational performance, implementation, and ongoing management costs. IT is no longer shackled to proprietary vendors and arcane solutions, but can now intelligently select solutions that provide the greatest overall value, while retaining the utmost security and performance. As a relentless innovator in the secure infrastructure market, SonicWALL is committed to improving the performance and productivity of businesses by engineering the cost out of building and running secure networks.