



The FactPoint Group: 12 Ways Unified Threat Management Firewalls are Driving Security Consolidation

*UTM devices are engineered to reduce risk,
cost and complexity, ensuring the strongest
defense posture with minimal IT intervention.*

CONTENTS

Introduction	2
What is Unified Threat Management	2
The Demise of the Security Appliance	3
The Changing Security Environment	4
What's Driving Security Consolidation?	4
12 Ways UTM Devices Deliver...	5
- Great productivity by reducing complexity	
- Boost security effectiveness	
- Lower costs	
The Bottom Line on Security Consolidation	7

Tim Clark, Partner
The FactPoint Group
349 First St., Suite A
Los Altos, CA 94022
(650) 233 1748
tclark@factpoint.com

Introduction

Just as virtualization has boosted server consolidation in data centers, so too are technology changes spurring consolidation of single-application security appliances on corporate networks

Instead of one appliance per application, security consolidation aggregates multiple interconnected security applications on a single piece of hardware. This super-appliance goes by the name of Unified Threat Management or UTM.

The point security appliance, once the paradigm for enterprise security with ease, has gone from being part of a solution to becoming part of the problem.

In a simpler time, the security firewall or virtual private network (VPN) appliance was considered an elegant solution. Plug it in, configure it, and let it run. But the standalone security appliance is no longer viewed as a simple, tidy box for a specific security threat.

Changes in both security threats and corporate environments have transformed thinking. Each separate security appliance requires configuration, licensing, license management, specific IT training, and ongoing maintenance with operating system patches, security updates and occasional reboots.

Emerging technologies—such as Voice over IP (VoIP), Wi-Fi, Skype, Web 2.0, Facebook and other social networking tools—create more points of entry into corporate networks and expand potential targets for malicious hackers.

The logic of server consolidation—fewer boxes, less hardware and lower costs—is likewise squeezing out the standalone security appliance, where more point solutions mean more costly management.

However, security consolidation via UTMs represents not just a better security and convenience but also opportunities: An opportunity to reduce network traffic, an opportunity to ease integration of VoIP and Web 2.0 applications, and an opportunity to boost IT productivity.

UTM devices are engineered to reduce risk, cost and complexity, ensuring the strongest defense posture with minimal IT intervention. Compare that to the expense and intricacy of sourcing, installing, integrating and maintaining multiple standalone security appliances from different vendors. Unifying security applications on UTMs gives enterprise administrators better control of their networking infrastructure and allows them to safeguard the corporate network more efficiently.

“A lot of companies have disparate solutions. They buy their firewall from one company, their VPN from another, their intrusion prevention from someone else. That increases the amount of management and maintenance time, and it's more difficult for IT departments. Instead of having just one management console, you can have quite a few. I've spoken with clients that have used consolidated security platforms to go from 10 devices down to just one or two.”

—*Candice Lou, research analyst, Info-Tech*

What is Unified Threat Management?

Researcher IDC defines Unified Threat Management as “security appliance products [that] include multiple security features integrated into one box.” The minimum set of security applications has grown over time but today includes network firewall, virtual private network (VPN), intrusion detection and prevention (IDP), content filtering, anti-spam and anti-spyware. Web application firewalls, data leak prevention (DLP), gateway anti-virus (AV) and enforced desktop anti-virus are included in some UTM devices, and some also handle network management functions such as load-balancing.

How effective is UTM? In a September 2008 report, Aberdeen Group¹ reported that top-notch companies are reaping significant benefits from UTM, measured in the previous 12 months, compared to laggards. Such benefits include:

- 20% reduction in actual threat /vulnerability related incidents
- 14% reduction in audit deficiencies
- 11% reduction in unscheduled downtime
- 5% reduction in total associated staff

Perhaps it's no surprise, then, that the UTM market has been blossoming, according to a 2008 report from Frost & Sullivan:² "The UTM market will mushroom from the present \$1.6 billion [2008] to \$6.9 billion in 2014—an annual compounded growth of 23%," as Processor magazine reported.³

As often occurs when technologies converge, some controversy has emerged over the question whether the "security jack-of-all-trades," as Info-Tech dubs it, is better than best-of-breed point solutions that address specific threats. However, the sheer number of security threats argues against the non-scalable approach of adding a new best-of-breed appliance for every new threat.

The Demise of the Security Appliance

Security appliances have fallen out of favor for several reasons. First, companies experienced a proliferation of security appliances (and associated management headaches) as they added new appliances to protect against new security threats. Consolidating onto UTM devices with the capability to effectively host as many as 10 security services thus reduces the number of devices to manage.

Second, corporations today face complex compliance requirements, not only from government but industry-specific dictates. For compliance, reporting is critical and compiling data from multiple security appliances, each with its own reporting systems, can be a pain. "With SonicWALL, compliance has basically been taken care of," said Jeff Arnts, IT development manager at AltaOne credit union in Ridgecrest, Calif., whose credit union uses SonicWALL's UTM solution. "The NCUA [regulator National Credit Union Administration] auditors have never cited any vulnerability."

In addition, the economic downturn has slowed (or reversed) growth in IT budgets, not just for hardware and software but also for information security personnel. By providing a single management console over a host of security services, UTM's ease the IT manpower crunch.

¹"UTM: Like a Box of Chocolates," Derek Brink, Aberdeen Group, September 2008.

<http://www.aberdeen.com/summary/report/benchmark/4872-RA-unified-threat-management.asp>,

²"World Unified Threat Management," Frost & Sullivan, November 2008.

<http://www.frost.com/prod/servlet/report-homepage.pag?repid=N48C-01-00-00-00&ctxst=FcmCtx1&ctxht=FcmCtx2&ctxhl=FcmCtx3&ctxixpLink=FcmCtx4&ctxixpLabel=FcmCtx5>

³"Consolidated Security Platforms," by William Van Winkle, May 8, 2009, Processor magazine, Sandhills Publishing Company U.S.A.

The Changing Security Environment

The trend toward UTM, sometimes called multi-function security devices, has accelerated as security threats have evolved. Computer crime, once little more than a game, has become a lucrative business for organized criminals. The profit motive—for stealing identities or personally identifiable information—has substantially boosted the volume, diversity and sophistication of threats. Beyond organized crime, persistent reports suggest that hackers tied to foreign governments have successfully targeted both civilian and military infrastructures.

Beyond external threats of cyberwar and cybercrooks, the IT infrastructures of many organizations have changed in fundamental ways. Virtualization—of servers, storage, desktops, even network resources—is all the rage, even if some CIOs still don't virtualize their mission-critical systems. IT departments increasingly support wireless access in corporate offices, campuses and beyond, raising the bar for secure connections to users at insecure endpoints. Increasingly interconnected corporate systems mean that a break-in could allow an attacker access to a broad range of systems and data. These internal systems are increasingly open to suppliers, resellers and other partners, who must be monitored for malware and limited in access.

The recent enthusiasm for cloud computing is forcing IT departments to redefine security when applications, corporate data, shared platform services or Infrastructure as a Service put critical resources outside the company. Cloud applications such as sales force automation, hosted email and email security are already mainstream, and Amazon Web Services, which offer processing and storage in the cloud, is finding rapid if early adoption. Like UTMs, cloud solutions require little IT management.

In addition to up-and-coming technologies such as VoIP or social networking, even new software applications, licensed or proprietary, can add security uncertainty, as do upgrades to existing applications. All these factors expand potential targets for malicious hackers to attack.

What's Driving Security Consolidation?

Amid these changes in corporate networks, the old-school security appliance struggles to hold its own. Where once a single security appliance at the corporate gateway provided adequate protection, today security requires many outward-facing, single-application appliances plus more at key intersections inside the corporate network.

Factor in the growing demand for more bandwidth within the enterprise. Companies must continually upgrade their network infrastructure or risk deteriorating performance. Bringing new applications on line boosts network demand. As enterprises respond by adding more bandwidth, a new opportunity arises that both reduces the complexity of the network infrastructure and provides greater, more effective security.

This fresh security approach is called Unified Threat Management or UTM. In addition to the ever-increasing hunger for bandwidth, a variety of market and security trends are raising the visibility (and attractiveness) of these multi-function devices.

Not only are computer criminals becoming more organized, their attacks are growing more sophisticated. Increasingly individual attacks combine several types of malware—a piece of spam carries a virus that sends the user's machine to an infected Web site that downloads code onto the user's PC that lets attackers return later to steal corporate data. A multi-function device such as a UTM can better defend against these hybrid attacks.

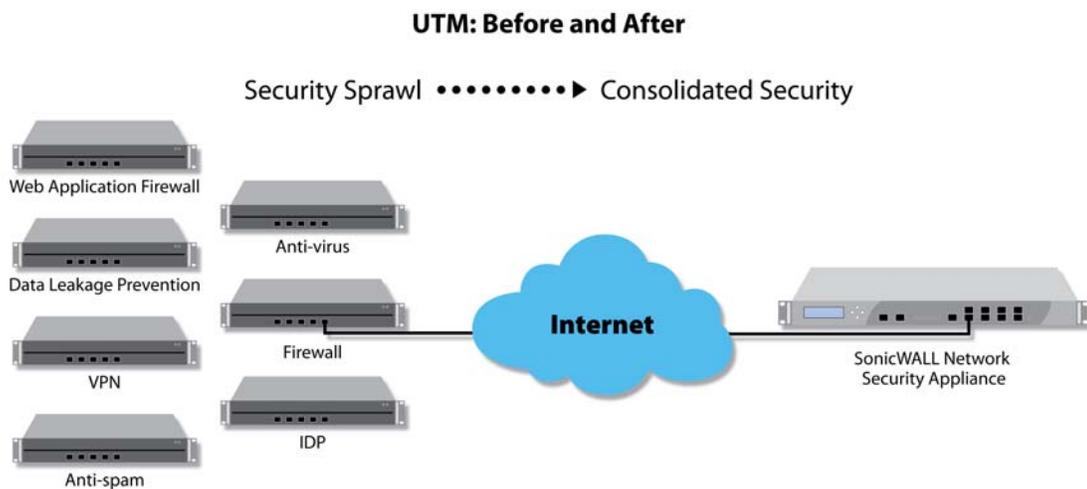
The St. Louis-based Donald Danforth Plant Science Center, a nonprofit agriculture research institute, was beset by malicious SQL injection attacks that defaced its Web site plus an increase in virus, spam and spyware attacks. "One guy would pass it on to the next, and suddenly we'd be troubleshooting 10 machines tracking it down," said Jeremy Tate, senior technical analyst at Danforth Center. "Not only were all my daily activities put on hold, but our scientists were kept from doing research or writing grants. It was a serious

impact on productivity.” Danforth’s well-researched solution: SonicWALL E-Class Network Security Appliance (NSA) E6500 and SonicWALL Email Security.

“SonicWALL helped me write a little script for the Application Firewall feature that immediately stopped the SQL injection,” said Tate, who also configured the E6500 for firewall, intrusion prevention, virus protection and anti-spyware. “The spyware detection has been absolutely fantastic. I can honestly say that since we’ve put it in place, we haven’t had a problem with inbound spyware.”

12 Ways UTM Devices Deliver...

Overall, the benefits of consolidating security devices can be grouped into three categories: Greater productivity, more effective security and lower costs.



Great productivity by reducing complexity

1. **A single, consolidated management console** for multiple security applications makes security administrators more productive. So does a UTM dashboard’s capability of managing separate or remote security domains from a central location. At Carriage Services, Inc., a chain of funeral homes and cemeteries, some 1,000 employees at 173 locations in 29 states run on SonicWALL VPNs that are supported by a single SonicWALL Global Management System (GMS) console at Houston headquarters. “I’ve got the console at my home, so in a disaster scenario, I can manage the entire network from there,” said Jeff Parker, manager of offsite systems.
2. **Simplify ongoing management tasks:** With security consolidation, fewer devices to manage means less management. Jim Walker, owner of Jet Plumbing and Drain Services in Sparks, Nev., reduced weekly administration time on his network from four hours to 10 minutes after installing a SonicWALL TZ 180 Wireless UTM along with a SonicWALL Email Security (ES) 200. The anti-spam engine eliminated 1.4 million spam message over the first weekend it was deployed.
3. **Simplify infrastructure:** Consolidated security devices means IT departments must manage fewer software components, systems, ports, network devices and vendor relationships. JFG Systems, in Carson City, Nev., previously had dedicated two firewall appliances to support more than 100 small

and mid-sized clients. With one SonicWALL NSA 4500 configured for load balanced high-availability, "We've got it down to one device to manage our gateway and maintain our security separations," says Ron Baker, JFG president and architect.

4. **Lower operator training requirements.** Instead of training for each legacy security appliance, a single UTM device requires one training to address multiple security applications.

Boost security effectiveness

5. **Better integration** in consolidated devices produces better security in two ways. First, sharing data easily among security services improves countermeasures. Second, the UTM runs on a single hardened operating system with fewer vulnerabilities to exploit.
6. **Adding new applications** to the UTM helps plug security holes from innovative new practices such as mobile users or protecting new applications. When Glentel, a Canadian telecommunications firm with more than 242 locations, decided to convert to VoIP for its internal communications, its existing SonicWALL PRO and TZ appliances already had built-in VoIP capabilities. "When we started looking at different VoIP solutions, some required us to forego our existing infrastructure with their proprietary platforms," said Glentel's Frank Chay, director of information technology and services. "That was not in the cards." SonicWALL UTMs are also easily deployed to new locations, without restarting, and can be managed centrally with SonicWALL's GMS console.
7. **Stopping blended attacks** that utilize multiple threats is more effective because data can be shared more quickly by security applications within a single device.
8. **Better support for remote users.** Bennett Office Technologies in Willmar, Minn., provides network management services for banks, casinos, healthcare facilities and other clients in Western Minnesota. It upgraded its primary security firewall to a SonicWALL NSA 240 and added other SonicWALL products. "Using our SonicWALL SSL VPN, we can provide support without driving to a remote business location," said Tim Starkenburg, network engineer for Bennett. "We can cover a larger geographic area and provide faster, more qualified service than local competitors."

"Having a comprehensive set of management features that are flexible yet efficient is instrumental not only to establishing and maintaining effective defenses but also to achieving significantly greater cost savings."—Mark Bouchard, Missing Link Security Consulting Inc.

Lower costs

9. **Lower upfront costs** result from consolidating security because UTMs use less hardware. The result: Reduced capital expenditures, or, in CFO language, more productive use of capital. "For what comes standard on SonicWALL appliances, we would pay thousands of dollars more for competitive products," said Geoffrey Sherman, associate technology director at RVM, a New York-based, full-service document management firm for law firms and corporations. "Because the solutions were so affordable, we saw a return on our investment shortly after the solutions were deployed."
10. **Investments protected** because new security services can be turned on in an existing UTM device as security needs change or legacy security appliances reach end of life.

11. **Lower power and cooling** bills because fewer appliances draw less power and put off less heat, giving UTM's a "green" tinge. JFG Systems, for example, reduced demand on server room HVAC and lowered power bills when it consolidated from two SonicWALL UTM devices to the more powerful SonicWALL NSA 4500.
12. **Limit security appliance sprawl** by freeing up space in crowded data centers.

The Bottom Line on Security Consolidation

The most important way information security organizations can save money in 2008 is by leveraging the convergence of established security functions into network- or host-based security platforms that provide multiple layers of security in a single product to protect against an evolving multitude of network and content threats.

—*Gartner Inc.*⁴

Unified Threat Management devices have been in the market for several years, and best practices for security consolidation are beginning to emerge. They include:

- **Replace security appliances gradually**, as existing security solutions become outdated (end of life), with Unified Threat Management devices that include the option of turning on additional modules in the future.
- **Validate ease of management of the UTM appliance**—not all UTM's have tightly integrated management of various security applications. At Potomac Hospital in Virginia, Tony Davis, network systems manager, estimates that using SonicWALL's UTM firewalls, wireless access points and other technology takes roughly 25% of the time it took to maintain his previous solutions. IT productivity is a key benefit.
- **Check for adequate throughput in UTM devices**, which may mean looking to multi-core devices. Some security applications, especially those involving encryption, require heavy processing loads, so putting too many on an under-powered UTM box can hamper performance, especially over high-bandwidth networks. "The SonicWALL NSA E550 gave us all the throughput we wanted," said Bryan Nash, SVP of IT at McHenry Savings Bank, a community bank in Illinois. "Even when we turn on all the security functions, including Gateway Anti-Virus and Intrusion Prevention, we see no degradation in network speed, and no hiccups."
- For the best UTM protection, look to products with **real-time threat detection engines**. These should include dynamic spam and virus updates to keep up with the latest threat signatures.
- To **avoid single points of failure**, a common critique of consolidated security, consider solutions that include additional security engines from other vendors for superior protection. SonicWALL, for example, has its own anti-virus engine but also bundles McAfee for additional protection.
- **Insist on enterprise-class UTM management that is centralized, consolidated and simplified.**⁵ Requirements include manage multiple UTM devices simultaneously, a single management system for all countermeasures, intuitive ease of use for all lifecycle management functions (i.e., configuration, monitoring, troubleshooting, and reporting). With these features, consultant Mark Bouchard of Missing

⁴ "Cost Cutting While Improving IT Security," Gartner Inc., March 2008.

⁵ "Management Considerations for Enterprise-Class UTM," by Mark Bouchard, Missing Link Security Services, 2007. <http://www.sonicwall.com/us/products/resources/188.html>. Other Missing Link white papers on other technical aspects of UTM are available at the same URL.

Link Security Services LLC argues, UTM can boost operational efficiency and enforce security policies consistently across applications.

- **Evaluate how competing UTM devices are updated to keep abreast with evolving threats.** Not all mechanisms are created equal; businesses, for example, may not want to settle for mechanisms based on threats to consumer users of the Internet. The SonicWALL GRID Network collaboratively gathers, analyzes and vets cross-vector threat information from millions of business-oriented sources around the world. Reputation-based threat protection information is then distributed securely, anonymously and in real time to improve the overall effectiveness of SonicWALL security solutions.
- Security consolidation is not just **safer and a convenience but an opportunity** to reduce network traffic, integrate VoIP and other applications, and boost IT productivity.

About SonicWALL

SonicWALL is committed to improving the performance and productivity of businesses of all sizes by engineering the cost and complexity out of running a secure network. For more information, visit the company Web site at <http://www.sonicwall.com/>. Information on SonicWALL's UTM products is available at http://www.sonicwall.com/us/products/UTM_Firewall_VPN.html

About the FactPoint Group

The FactPoint Group (www.factpoint.com) is a Silicon Valley-based market research, publishing and consulting firm specializing in the early adoption of new technologies. The FactPoint Group has been producing world class research, analysis, and consulting since 1993 and continues to help its clients sell and use new technology solutions. FactPoint partner Tim Clark previously was a senior editor with CNET News.com, where he covered Internet security.