Consolidated Network Security

FORTINET DELIVERS
NETWORK SECURITY CONSOLIDATION

REAL TIME NETWORK PROTECTION

FURTINET®

Introduction

As an IT professional concerned with network security, you're confronted by a constantly-evolving array of threats and increasing compliance requirements. But you have to balance your ability to manage this dynamic "threat-scape" against many other imperatives, including cost (both CapEx and OpEx), limited data center space, manageability, and, increasingly, environmental concerns. This white paper discusses how network security consolidation using a Unified Threat Management (UTM) platform can help you address these challenges and deliver more effective security, notable cost savings, and a smaller environmental footprint.

The Consolidation Imperative

Driven by space, power, budget, and other constraints, consolidation has become both a tactical and strategic imperative for enterprise IT professionals at all levels, from the CIO on down. The benefits of consolidation, whether physical or virtual, are well known: lower cost, less power consumption, improved manageability, and a better environmental footprint among them.

Most of the buzz about consolidation concentrates on its application to the data center as a whole, or to application servers in particular. But this focus overlooks an area where consolidation offers even more dramatic advantages: network security. Consider that, in the case of application server consolidation, most of the benefits are in some sense peripheral to the fundamental task at hand: the delivery of application services. By contrast, as discussed below, consolidating network security with a UTM platform delivers profound improvements in its ability to accomplish its fundamental task: managing the diverse range of threats that confront enterprise networks.

Consolidating network security also delivers notable cost benefits. According to Gartner, the most important way information security organizations will 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.[1] In fact, Gartner estimates that, by 2010, only 10% of emerging security threats will require tactical point solutions, compared with 80% in 2005.

Thus, network security consolidation is a real bargain: all the benefits that consolidation delivers for other areas of enterprise computing—lower cost, easier management, and many "green" benefits—plus improved security!

The Perfect Storm

Network security consolidation could hardly have arrived at a better time, for IT professionals concerned with security are finding themselves at the center of a perfect storm caused by the convergence of three trends. First, there's the slowing growth of IT budgets. In a recent survey of IT decision makers by Computer Economics, the average expected growth in IT budgets was only 2.5%.[2] And, since IT budgets depend to a large extent on company profits, the rough weather the economy is enduring can only further slow this growth rate.

Second is an unfortunate trend towards complacency about network security and compliance issues, if not among security professionals, then among the executive staff that controls the budget. In a sense, network security has become a victim of its own success in dealing with both new threats and new regulatory mandates like Sarbanes-Oxley. There has been no headline grabbing network-based attack for several years, and so many executives may feel that security has been "taken care of." There is also a related tendency to concentrate on compliance issues at the expense of more traditional security issues, since their bottom-line impact is more readily discerned, and more in line with executive-level concerns.

Third, and perhaps most important, is the increasing complexity of network security: the growing sophistication of threats, an ever-increasing compliance burden, and the vulnerabilities constantly exposed by new applications and technologies. Exploits are no longer so much focused on hacker reputation as on financial gain, and organized crime is moving in to take advantage of network security weaknesses. Of course, where there's profit involved, innovation happens faster, so the scope and power of threats is changing more rapidly. The compliance burden is ever heavier as well, especially given the necessity of being able to prove that all possible steps were taken to protect sensitive data, which requires extensive logging and auditing. To top it all off, the very success of IT in supplying new applications to support business innovation and competitive advantage—not to mention popular applications like Skype and Facebook—has inevitably added new avenues of attack.

Network security consolidation via a UTM platform offers you a way through this storm by delivering more effective security at a lower cost than hard-to-integrate point solutions. As a bonus, it also supports many aspects of corporate green initiatives.

Enhancing Security Through Consolidation

Consolidating your network security enhances security in three ways: better integration, more efficient management, and superior threat intelligence.

Improved Integration

Better integration on both a software and hardware level bolsters security by delivering more complete coverage of threats and improved scalability.

More Complete Threat Coverage

The threats confronting you today are both network and content-based. Network threats include denial of service (distributed denial of service using "zombie" networks being particularly dangerous), eavesdropping and other intrusions and basic worms. These are dealt with using firewalls, Intrusion Prevention Systems (IPS) and VPNs. Content-based threats include more sophisticated worms, viruses, phishing and pharming, spyware, email spam and more, and require content-inspection technologies such as antivirus, antispam, web filtering and the like.

The rising sophistication of attackers, driven in part by the increasing involvement of organized crime, is also boosting the frequency of blended attacks that combine both network and content-level threats. For instance, the malware FunLove included a virus and a worm, while Bagle.H of the FunBag family essentially involved a virus as the payload of a worm. Targeted attacks, which trade speed of propagation for stealthier and thus deeper penetration into valuable resources, use a similar mix. For instance, spy-phishing starts with an email targeted at an audience pre-disposed to use certain web sites and services. It includes a trojan (or a link that will result in one being downloaded) that monitors web traffic, waiting for particular sites to be accessed (e.g., online banking). When this happens, it acquires credentials and other valuable information and then transmits it to a collection site, often via IRC or an encrypted channel.

By enabling knowledge sharing between countermeasures, consolidating your network security with a UTM platform can greatly increase your ability to detect and prevent not only standard attacks but also more sophisticated multi-vector attacks. For instance, a consolidated system that couples a signature-based antivirus engine with a proactive intrusion prevention engine will be far more effective than a single-technique solution. Likewise, integrating web filtering, antivirus and IPS capabilities in a way that allows the various engines to correlate activity can greatly increase the ability to fend off sophisticated attacks. This correlation enables the system to initiate defense during the earliest possible phase of the attack, cutting down the likelihood of success and reducing related damage.

Hardware integration offers additional benefits. A common, hardened network security OS, in which all unnecessary services have been eliminated, and which is tuned for the supported countermeasures, is obviously more secure than multiple operating systems, each with their own vulnerabilities and, in the case of multiple-vendor solutions, varying levels of support. As well, consolidation can eliminate redundant processing by having different capabilities share the execution of common routines. For example, "cracking packets" multiple times, once for each countermeasure, is highly inefficient and causes additional latency in the network. To further reduce latency, purpose-built UTM systems should employ hardware acceleration whenever possible, which also contributes greatly to the scalability of the solution.

Finally, consolidation offers a superior way to incorporate multiple networking capabilities such as multiple routing protocols (e.g., RIP, OSPF, BGP), translation techniques (e.g., NAT, PAT), switching, VLANs, traffic prioritization, virtual systems, failover and clustering. Virtualization is particularly important to unlock further security functionality, such as the ability to create multiple and separate security domains so that resources with different trust levels can be isolated and treated differently.

More Effective Management

Consolidating network security via UTM can greatly improve the productivity of your security professionals by providing unified, centralized management of all the solution's capabilities, which of course is also necessary for scalability. This is an area where a non-consolidated approach is simply incapable of competing. There is certainly no practical way to unify and centralize management of a multi-vendor security solution. And even when a single vendor supplies a solution based on multiple boxes, even if it's called Unified Threat Management, the reality is that such vendors often assemble their offering from a collection of OEM solutions. This is especially likely to be true of vendors who are making the transition from a single-threat offering (e.g., Intrusion Prevention) to Unified Threat Management: they build their UTM offering by adding OEM technologies to their core competency: antivirus from one vendor, Intrusion Prevention from another, and so forth. Such solutions are all too likely to offer a fragmented, partially-unified management approach whose complexity can compromise your ability to monitor and counter network and content-level threats.

By contrast, many security management tasks become easier with a truly consolidated solution. Centralization gives you the ability to remotely manage multiple devices at once and supports other scalability features such as hierarchical policies and flexible grouping capabilities. From a single console you can establish or modify all of the settings pertaining to a given domain, or, as may be desired in the case of role-based administration, globally across all domains. Unified logging and reporting capabilities make compliance audits easier, while the same unification applied to event analysis and correlation not only improves the solution's automatic response to threats, but make forensic analysis quicker and easier. Finally, you can manage all classes of device using a common set of management applications, which is critical to your ability to scale the solution as your enterprise grows.

Superior Threat Intelligence

Consolidation yields superior threat intelligence by making possible the unification of threat research, which is the vendor-based research and development effort that supplies the multi-layered security intelligence necessary for successful threat management. Traditionally there has been something of a rivalry between antivirus and vulnerability researchers. Yet, as attacks become more complex and multi-modal, they demand a hybrid approach to threat research that combines these two disciplines, as well as others. Just as enabling the various countermeasure modules in a UTM solution to share knowledge makes its response to threats more effective, so too an integrated program of research and development across all threat types delivers more accurate countermeasures.

This is another area in which non-consolidated approaches often fall short, and for exactly the same reasons as discussed above under management. Vendors who rely on OEM technology to flesh out their offerings are dependent on the threat research offered by their suppliers. This makes it harder for you to judge the quality of the complete solution, and diffuses the responsibility for the research quality and timeliness. The existence of another link in the transmission chain from research lab to end-users can only make it more difficult to guarantee timely response, and hamper the responsiveness of the vendor's help desk. Because the understanding of various threats is diffused across multiple vendors, no matter how good their specialized knowledge is, the amount of cross-discipline knowledge-sharing is naturally limited, making it harder to understand multi-mode threats or how the various pieces of the solution can most effectively work together to counter them.

By contrast, the threat research behind a truly consolidated UTM solution will comprise an effort by a team of highly-trained researchers experienced in a variety of threats and countermeasures, supported by knowledge-sharing structures and processes designed to highlight the ways in which multi-mode attacks can combine different threats. Likewise, team members charged with developing countermeasures will have a deep understanding of the synergies offered by the internal knowledge sharing of their UTM solution. This makes the detection of new threats, and the development of appropriate countermeasures, faster and more accurate. Such a threat research effort should also be global in nature, include automated feedback from the installed base of appliances as well as a manual means for customers to report new threats, and stress cooperation with major infrastructure vendors. This means that a large installed base is important; smaller vendors simply cannot offer the same degree of coverage.

Reducing Costs Through Consolidation

Network security executives are increasingly facing the same cost imperatives as other areas of information technology: improve services while reducing total cost of ownership (TCO) in terms of operational expenses (OpEx) and capital expenditures (CapEx). In security, as elsewhere in IT, OpEx comprises a much larger portion of the budget.

Many of the benefits of network security consolidation from a CapEx standpoint are obvious. First off, you have a lower up-front cost because you're not purchasing multiple systems, and there's even a minor saving coming from reduced cabling. There's also the fact that in many enterprises, data center space is becoming critically limited, so any potential reduction in rack space is important to help avoid facility expansion. Virtualization also contributes to CapEx reduction, by making it possible to manage multiple security domains without adding more equipment.

Perhaps the most important TCO benefit of a consolidated network security platform involves scalability. It's rare that an enterprise will implement all aspects of UTM immediately. More likely, you'll start consolidating a few security functions -- perhaps firewall, VPN, and IPS, -- then consider adding others in the future, perhaps replacing single-function antivirus, Web filtering or other products near the end of their life.   With a consolidated solution, those capabilities are already there. You don't have to purchase and install more boxes; a simple subscription is usually all that's needed. It's quite similar to the practice of buying dark fiber in excess of today's bandwidth needs and then lighting it up when necessary. Thus, consolidation helps preserve the value of your security investments by making it easier to add new functionality with a minimum capital investment.

Network security consolidation delivers even greater OpEx benefits. As noted above, multiple vendors, or even multiple boxes from a single vendor, impose a greater management burden. This forces your security staff into a reactive mode, with constant fire-fighting leaving them less time for proactive initiatives to support business growth. As well, with a consolidated approach, your training, maintenance, support and threat update subscriptions will not only be less costly, but simpler and more rapid as you will be dealing with only one management interface and one set of updates from one vendor.

Going Green With Consolidation

Environmental consciousness is an issue customers are increasingly considering in the vendors they do business with. For instance, according to IDC, over 50% of customers take the "green" stance of a vendor into consideration when selecting a supplier, and one-third rate the availability of green offerings from an IT supplier as "important" or "very important."[3] This comes right from the top of the management chain as well: green IT is growing in importance for almost 80% of executives. As much as "going green" can help a company's reputation, however, IDC also notes that the number one driver for green IT adoption is the reduction of operational costs.

Consolidation naturally means more efficient power usage by your hardware (e.g., shared power supply and ventilation), especially in the case of chassis and blade-based UTM solutions, and thus lower electrical bills. As an example of the potential cost reduction, consider just a small part of the network security infrastructure: the perimeter defense between the primary Internet gateway and the private network infrastructure. It is common to find a firewall, a VPN concentrator, an intrusion prevention system, a gateway antivirus system, and a web filtering system deployed here in daisy-chain fashion: five devices each providing a single-function security service. Using a very conservative estimation of 300 watts per device, the power consumption for this security infrastructure totals 1500 watts.

By replacing these standalone systems with a consolidated network security system, a single 300-watt system can provide the same functions with only 20% of the recurring power cost. This power reduction also reduces cooling costs in two ways. First, every watt of power consumed by IT equipment requires about 0.8 watts of cooling energy. Second, the smaller physical footprint makes it easier to direct cool air, or apply various forms of per-rack liquid cooling, for more efficient heat transfer.

Overall, lower power consumption means a smaller carbon footprint. There's also the energy reduction across the entire life cycle: more efficient manufacturing and less hardware to recycle at end of life. Even the reduction in cabling needed makes a contribution, as PVC cable cladding has a large environmental footprint both in its manufacture and in its recycling.

Summary

Consolidating your network security with a truly-integrated Unified Threat Management solution gives you better network protection, more efficient use of your capital budget, lower operational expenses by reducing the management burden as well as training, support, and threat update costs, and preserves your investment by allowing you to add robust security functionality with little or no additional hardware. Added to these hard savings are the green benefits of consolidation, most notably a smaller carbon footprint across the entire life cycle of the equipment. In short, network security consolidation offers both economic and reputational advantages that make it one of the best investments IT departments of all sizes can make.

---

[1] Gartner: *Cost Cutting While Improving IT Security,* March 20, 2008

[2] Computer Economics: *Security Technology Spending Declines as Share of IT Budget,* March, 2008

[3] IDC: *The Growing Importance of Green IT: Findings from IDC's U.S. Green IT Survey,* November 2007

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: (Firewall, Antivirus, IPSec, SSL, Network IPS, and Anti-Spyware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com

WPR137-0408-R1