

# CIO SURVIVAL GUIDE

FEBRUARY 2008 ■ ISSUE 005

HANDBOOK TO UNIFIED THREAT MANAGEMENT

MALWARE

SPAM

VIRUS

A special supplement with

**NetworkWorld**  
MIDDLE EAST

IN CO-OPERATION WITH

**FORTINET**  
REAL TIME NETWORK PROTECTION

# NEXT GEN SECURITY

The essential guide  
to UTM

CASE STUDY

UAE Central Bank PAGE 18

SPECIAL FOCUS

Cybercrime PAGE 12



SPECIALIST VAD  
SECURITY AND MOBILITY



### UTM

- UTM GLOBAL LEADER (IDC REPORT)
- WIRE SPEED FIREWALL UP TO 70 GBPS
- WIRE SPEED IPS UP TO 15 GBPS
- WIRE SPEED ANTI VIRUS UP TO 4.2 GBPS
- ASIC-BASED ARCHITECTURE
- FLASH-BASED APPLIANCE WITH NO HARD DISK
- CENTRALIZED MANAGEMENT AND REPORTING APPLIANCE
- BUILT-IN VIRTUAL FIREWALL / SSL
- MMS SCANNING AND GPRS FIREWALL FOR TELECOM AND ISP
- OVER 4, 000 HAPPY CUSTOMERS ACROSS THE GCC

### EMAIL SECURITY

- CAN BE DEPLOYED IN TRANSPARENT, GATEWAY AND EMAIL SERVER MODE
- INBOUND / OUTBOUND EMAIL INSPECTION
- IMAGE & PDF ATTACHMENT INSPECTION
- EMAIL ARCHIVING
- EXTREMELY AFFORDABLE EMAIL SOLUTION

### NAC (NETWORK ACCESS CONTROL)

- MONITORS & SECURES PORTS INDIVIDUALLY
- POLICY ENFORCEMENT
- IDENTITY AND ACCESS MANAGEMENT
- QUARANTINES INFECTED COMPUTERS FROM LAN
- NO AGENT

CONSULT

SUPPLY

INSTALL

SUPPORT

# THINKING INSIDE THE BOX

Are there unified threat management (UTM) firewalls with the chops to provide the perimeter security functions that an enterprise needs? After all, enterprises generally employ best-of-breed security products, not the all-in-one devices popular with the small and medium business set. It seems finally UTMs, the Swiss Army Knives of security and networking, are winning favour as easy-to-manage boxes among enterprise IT managers.

Appliances and UTMs are the tip of the hardware spear, with faster and more capable hardware supporting a wider mix of embedded software applications. Today, UTMs come with antispam, antivirus, intrusion-detection, firewall and packet inspection, and antispymware capabilities, as well as VPN connections, Wi-Fi access points and more.

The march of Moore's Law adds more capability and value to these appliances for customers lacking a best-of-breed requirement, and the life-cycle, cost-of-ownership advantages for the appliances are compelling. Now, instead of jumping between separate security tools and management UIs, admins need only go to one place to manage and monitor these systems. Updates are scheduled and initiated from a single console, reports are viewed from one appliance, and policy is managed from one device.

By moving all of these security services into a single device, UTM appliances are supposed to reduce the admin's workload; ease-of-use is one of the main selling points. A well-crafted UI can make short work of checking for signature updates, recent activity, and alerts. Pundits are predicting that UTM appliances will become the dominant security delivery technology in the next two to three years. Users will do well to keep a sharp eye on the rapidly changing vendor landscape in order to keep track of their options. Flip the pages to plow through the hottest technologies and trends in the UTM marketplace – all in one place.

# CIO SURVIVAL GUIDE

**CEO and Publisher**  
Managing Director  
and Associate Publisher  
Managing Editor  
Editor  
Chief Designers  
Designer

Dominic De Sousa  
Amit Pateria  
Kavitha Rajasekhar Vivek  
Jeevan Thankappan  
Denis Fuentes, Ulysses Galgo  
Mark Cantalejo

**Sales Director**  
IT Manager  
Webmasters

Sreejith Nambiar  
Nadeem Hood  
Tristan Troy Maagma,  
Elizabeth Reyes  
James P. Tharian  
subscribe@cpidubai.com  
Miti Agarwal

**Production**  
Subscription  
Marketing Manager

Published by



**Head Office**  
PO Box 13700  
Dubai, UAE  
Tel: +971 4 3515316  
Fax: +971 4 3598486  
Web: www.cpidubai.com

Regional partner of

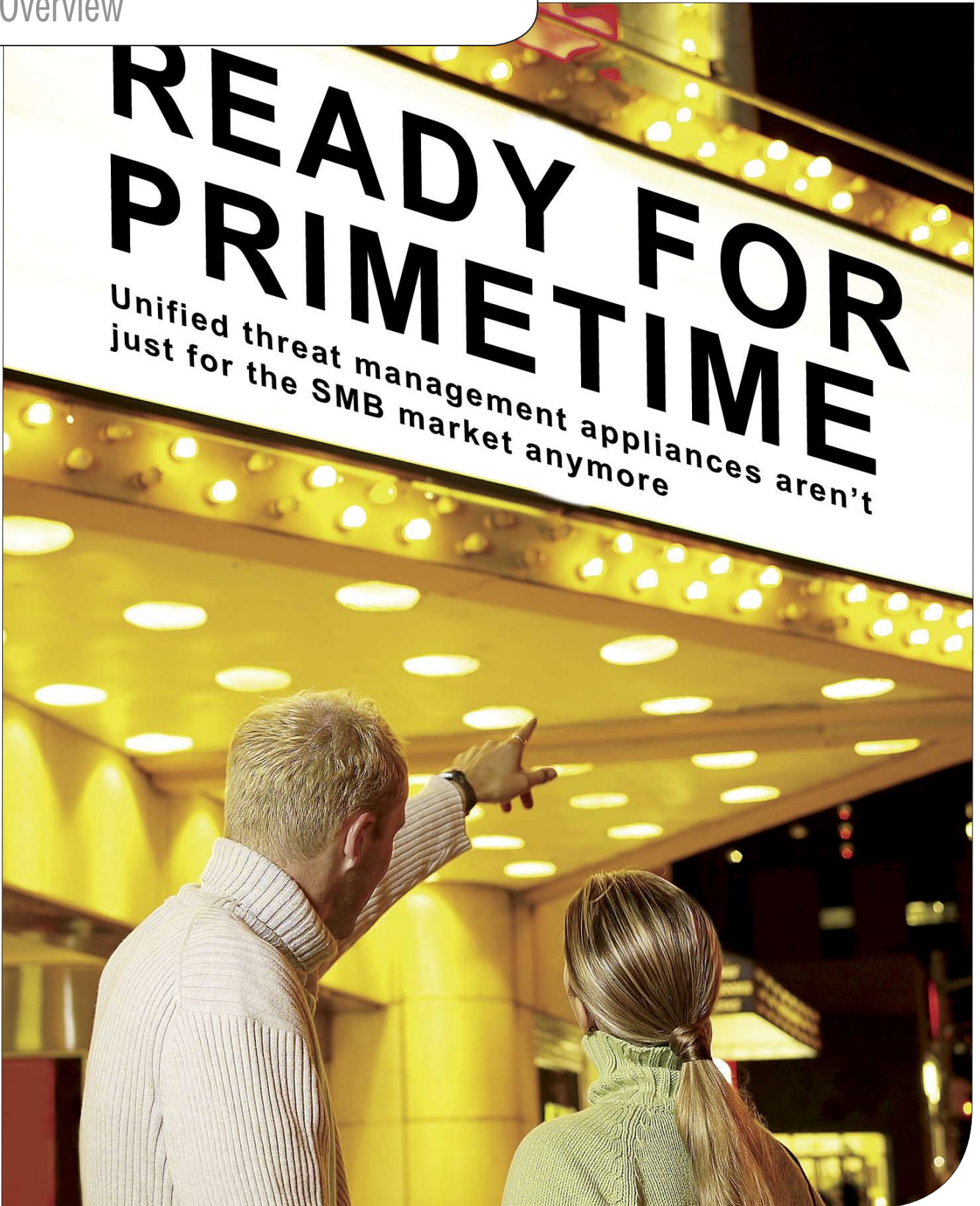


© Copyright 2008 CPI.  
All rights reserved.  
While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.



# READY FOR PRIMETIME

Unified threat management appliances aren't  
just for the SMB market anymore



IT managers at small and midsize businesses like unified threat management appliances - firewalls that layer on antimalware protection, content filtering, antispam and intrusion prevention - because deploying a single, multi-function device reduces costs and simplifies configuration.

However, deciding whether and where to deploy UTM appliances in a large enterprise is a more complicated and difficult decision. The idea of a single point through which all traffic flows as an obvious locus for threat mitigation doesn't work when a network has dozens, hundreds or thousands of distinct locations. Also, because performance is a critical issue in large networks, savvy network managers often seek to distribute threat protection rather than centralise it, simply to reduce the likelihood of a performance bottleneck.

Similarly, the style and quality of threat mitigation features one commonly sees in an SMB UTM may not be of interest to an enterprise, where requirements are more exacting and security architectures are more complex. For example, the antispam features and functionality in UTM firewalls pale compared with those in stand-alone enterprise-class dedicated antispam/antivirus appliances.

With such dramatic differences between SMB and enterprise requirements, is there a place for enterprise UTM firewalls? The answer is definitely "yes," for these three reasons: reduced

complexity, simplified management and increased flexibility.

### Reduced complexity

Enterprise network managers have long sought to include additional threat protection, especially intrusion detection/prevention systems (IDS/IPS) functions, both at the core and at the perimeters of their networks. However, the complexity of dropping standalone IDS/IPS boxes into a network has made them wary.

Building the "firewall sandwich," with load balancers surrounding a core of clustered firewalls, is well understood, but trying to scale that sandwich up with another layer of protection dramatically increases architectural complexity and potential instability.

A simple sandwich is considered science by network architects, but adding layers takes it from craft to art, dramatically increasing the difficulty of the project and opening a window for failure and problems. It's like adding just one more piece of cheese to that Dagwood sandwich: Not only will you be unable to get it in your mouth, but the whole thing may fall apart on your plate.

Enterprise UTM with integrated IDS/IPS can give network managers additional security throughout the network without the massive increase of complexity that stand-alone IPS devices would create.

### Simplified management

It's pleasant to imagine the concept of a single

UTM console that can handle everything from IP routing to IDS alerts, but enterprise security teams often want different management systems for a reason: different people are responsible for different kinds of threats and configuration.

Nevertheless, some level of management integration can reduce the task of handling these different functions. For example, every management console must have different network objects in it that are used to define policy: here are my mail servers, here are my users, this is the guest network, here is where the Internet is.

Each time those same objects must be typed into a different management system, and each time these objects are updated and adjusted, there is an opportunity for human error or miscommunication to create a security hole. A single management console that shares objects across different functions simplifies the complex task of management.

This single management view is especially valuable when firewall, VPN and IDS/IPS are considered together because all three of these functions act on the same policy. Each of these functions needs to have some view of the topology of the network, what applications are running on different servers and what different groups of users are allowed to do. Completely separate management for all three functions makes coordinated policy maintenance difficult, if not impossible.

A single UTM-ready management console realistically enables a fine-tuning of policy across all three functions, increasing total security.

### Increased flexibility

Enterprise security architects generally scoff at the plethora of features, such as antivirus, antispam, antimalware and antiphishing, that are being built into SMB UTM devices. With a "best of breed" mentality and correspondingly large budgets, they are barely interested in activating IPS features in their existing firewalls. However, there are always specific situations where the ability to turn on, for example, antivirus, may be a huge benefit.

Having additional security features latent in large firewalls that can be activated with the click of a mouse gives the network manager increased flexibility, which is of significant value. For example, blocking incoming viruses in a UTM firewall may be a life-saver when the normal antivirus appliances suddenly stop working because of hardware, software or update failure.

Or consider the requirements of a guest user network: Most enterprises have chosen HTTP proxies to provide content filtering and antiphishing protection but may want to let guest users choose a different kind of protection and not take on the support burden of making sure they're properly working with the enterprise proxy. It may be simpler and more effective to enable these features in a UTM firewall for those networks. The flexibility to bring security services in and out of the equation quickly using a UTM firewall supports threat response requirements - even if those features are rarely used.

**A single UTM-ready management console realistically enables a fine-tuning of policy across all three functions, increasing total security.**

# THWARTING BLENDED THREATS



Appliances and UTMs are the tip of the hardware spear, with faster and more capable hardware supporting a wider mix of embedded software applications. Today, UTMs come with antispam, antivirus, intrusion-detection, firewall and packet inspection, and antispyware capabilities, as well as VPN connections, Wi-Fi access points and more.

**U**nified threat management appliances provide increased intelligence to detect network threat activity through the correlation and analysis of data from various security engines. This approach provides an alternative to a piecemeal implementation of separate systems.

IDC established this product category, with a minimum feature set that includes a firewall, intrusion detection/protection system (IDS/IPS) and antivirus

capabilities. Many UTM appliances have been expanded to include VPNs, antispam, antispysware and Web content filtering.

Most of these security capabilities operate at the application layer to detect spam, viruses, worms and other sophisticated forms of

sensitive applications, such as VoIP, the total latency can quickly exceed the recommendation for these mission-critical applications. UTM solutions help overcome latency issues by reassembling the data once for multiple security features rather than reassembling

UTM market:

1. All firewalls are for unified threat management. There is little distinction between a UTM firewall and a "normal" firewall nowadays. The firewall vendor community has made the transition so that all current products include the

software was not originally designed to meet the needs of UTM. For example, without disk space, a UTM firewall can't provide a spam and virus quarantine. Or, without a link to the corporate directory, user personalisation and differentiation on settings can't occur. While established vendors are not moving quickly in this area, new products are coming to market that reflect a rethinking of software and hardware requirements for a UTM firewall that provide better coverage on the threat mitigation side of the house.

**With its integration of multiple security engines into a single appliance, UTM makes it easier for administrators to enforce detailed security policies throughout the enterprise.**

attack, as well as potentially offensive or unauthorized content. Therefore, every UTM appliance must be able to perform deep packet inspection from Layers 3 through 7. Some threats can span several packets, requiring a multipacket payload-reassembly mechanism to thwart them in real time.

Despite the security integration advantages offered by UTM appliances, their complex packet-processing requirements raise concerns about performance. For this reason, UTM systems should deploy some means of hardware acceleration.

The performance issue has two dimensions: throughput and latency. Hardware acceleration affords improvement in both dimensions, and some UTM systems can achieve a throughput of up to 70Gbps with a total latency of less than 50 msec.

Performance also can be a problem with stand-alone systems. Individually, they can offer satisfactory throughput with sufficiently low latency, but when implemented in a serial fashion, as required by the piecemeal defense-in-depth approach, the latency is cumulative.

Because many enterprise networks now support delay-

the content for each security feature individually.

With its integration of multiple security engines into a single appliance, UTM makes it easier for administrators to enforce detailed security policies throughout the enterprise. It also makes it possible to detect blended threats that employ a combination of attacks (such as a mix of viruses, worms, Trojans and denial-of-service attacks) crafted to circumvent a single line of defense.

With UTM solutions, the integrated security engines work together, enabling the system to inspect real-time traffic – whether as packets or entire files - from multiple vantage points. For example, a seemingly harmless e-mail message may pass through an antivirus system. But the message may contain an HTML-based attachment that ultimately points to a Trojan. Because a UTM solution can use a combination of antispam, antivirus, antispysware and other security engines, it can detect such blended threats more readily.

The combination of multiple security engines within a UTM solution establishes a new approach for the detection and remediation of blended threats. These are some of the top trends in the enterprise

option to include some UTM features. While very high-end devices may not include much beyond embedded intrusion-prevention systems and VPN, the term "UTM firewall" has become redundant. If it's a modern-day firewall, it does more than simply block or allow traffic.

2. Conversely, UTM doesn't necessarily include the firewall. Whether it's a public relations ploy or a search for more customers, the UTM market has expanded to include products that don't actually have a firewall inside. Several vendors have brought products to market that have weak or nonexistent firewalls, yet a strong suite of threat mitigation features, including antivirus, antimalware, content filtering and traffic analysis. By combining these everything-but-the-firewall features into a single system, such vendors are focusing on the threat mitigation features and can design hardware that fits those requirements best to bring a very strong offering to the table.

3. New products have new architectures. Most UTM firewalls do a poor job at certain functions - antispam and antivirus are the best examples - because the underlying hardware and

4. Vendor business models are evolving. UTM changes the model from a capital-focused one to a service-focused one. This means that firewalls will get even less expensive - but only be really useful when under a support agreement that provides constant updates. In fact, small-to-midsize-business-sized software-based firewalls are coming to market for "free," based on the idea that they will generate revenue through support and subscription fees. It worked for razors; it can work for firewalls.

5. Network managers remain skeptical. While vendors are packing features into products and offering them at attractive prices, network managers are still hesitating to enable threat mitigation features. The UTM sweet spot is networks in SMBs with no dedicated security staff. While you'd think that enabling UTM features is a no-brainer on these new devices, fears of false positives and bad experiences with performance slow-downs keep many of these devices running in firewall-only mode. Enterprise network managers are even further behind than their small-business brethren in deploying UTM features such as IPS in high-end devices.

# HOW TO SELECT ENTERPRISE UTM FIREWALLS

UTM appliances come in different shapes, sizes and speeds. Here is how to find the right fit in a crowded and disparate security market.

Selecting UTM firewalls in an enterprise environment is more work than just picking a standard firewall, because the “UTM” moniker doesn’t offer much information about what the firewall actually does. When evaluating enterprise UTM firewalls, there are four key issues to consider: performance, UTM feature set, network integration and management. Many of these overlap traditional firewall requirements but must be considered in the light of specific needs for very high-reliability, high-performance, enterprise-class products.

Performance is the key starting point for UTM firewalls, because the UTM features exact such a heavy performance cost. Without accepted metrics on how to measure UTM firewall performance, network managers are left to

determine how fast a UTM device will go by turning it on and putting it in the middle of their network. No matter what you do, don’t skip this step or some reasonable approximation in a test lab. The performance of UTM devices is very dependent on exact configuration and traffic flows, and without some testing, you could easily end up with a device that can’t handle the loads you throw at it.

UTM firewalls that let you scale up without a forklift upgrade, either by upgrading in the chassis or by adding systems in an active/active load balancing configuration, are especially attractive when the performance card is on the table. But it’s better to start with a system that can run as fast as you need the day you turn it on, and save upgrading for another year.

UTM features are near the top of the list for selection

## UTM Do’s and Don’t’s

- Avoid UTM appliances that rely on hard disk
- Go ASIC-based
- Check for TCO for 3 years
- Do not size up the appliance based on the number of users only
- Stay away from per-user licensing scheme.

criteria. The idea seems simple enough: If you want antivirus, it should do antivirus. But within UTM firewalls, there’s considerable variation in how a simple feature such as antivirus is implemented. For example, not every firewall can examine every protocol for virus signatures, and even those that do cover the top protocols can’t always be configured to work on non-standard ports. One firewall we tested only looks for

viruses in certain defined Multi-purpose Internet Mail Extensions types as a way to keep performance peak, opening the potential for future exploits to slip directly past. A critical exercise before buying is understanding exactly what coverage is included and how that coverage relates to your own traffic patterns and requirements.

A small number of UTM firewalls offer a choice in threat mitigation products, such as

multiple antivirus vendors, but most lock you into a single vendor. While antivirus (as an example) is considered a commodity service, other services, such as IPS and antimalware, are in more active development - which makes the choice of vendor and consistency of implementation significantly more important.

Network integration includes the aspects of a UTM firewall that let it sit securely within an existing network. For example, enterprise UTM firewalls are more likely to need some support for dynamic routing protocols such as Open Shortest Path First to integrate within an existing infrastructure. Virtual LAN support, high port density, WAN support and expandability of interfaces over time are all similar network integration features. While most of these also are relevant in a pure enterprise firewall without UTM features, the tendency to use UTM firewalls as points of consolidation of security control raises their importance.

Another aspect of network integration includes the equipment and interfaces required for high availability and scalability. If you've got a specific set of load balancers or switches, the UTM firewalls have to be able to integrate with that equipment with a minimum of re-engineering and additional equipment. Similarly, with the additional requirements for active/active clustering that UTM performance brings, full support for upward scalability should be considered a UTM evaluation criterion.

Management is one of the most difficult parts of a UTM firewall to evaluate, because you don't know how good or bad the management is until you've had lots of experience with the product. While most management systems strive for glitzy interfaces for the novice, the real evaluation comes with consistent and continued use.



Unfortunately, by that time, it's too late to choose another product.

In UTM products, one of the most important features of management is the ability to bring UTM features into play in a flexible and controlled way. For example, a management system that requires all traffic to flow through the IPS, or none of it, is not suitable for an enterprise UTM device. At the same time, the management system must allow for different profiles for the same UTM feature. For example, an IPS might be configured in a liberal way for internal users browsing the Internet, while turned up to strict levels for guest users coming from a different subnet.

While UTM management

systems will be mostly of interest to the security manager, there are aspects of configuration that will fall to a desktop manager (such as antivirus) or network manager (such as dynamic routing). Separating function and privilege level horizontally and vertically across the domain of management is difficult. However, if your UTM deployment will have people from three (or more) teams peering into the same management system, features in this area can be critical to successful long-term operation.

Though, some vendors have taken advantage of the enormous boon that Intel has provided in low-cost, high-performance CPUs that

are aimed at general-purpose computing, it's good idea to go for ASIC-based UTMs, as they are blazingly fast. The argument here is that in addition to traditional network functions, ASICs will also perform well for specific application functions, including inspecting incoming Web connection for http-based threats. It's also equally important to choose flash-based security platforms than hard disk based ones. The rationale for flash-based security platform is that it offers higher reliability and a longer mean time between failures (MTBF) as compared to disk-based ones because they do not rely on spinning media for operations.

# TIPS ON DEPLOYING ENTERPRISE UTM

Deploying enterprise UTM has its own pitfalls. Here are some tips to help you avoid those issues in your network.

### 1. Check performance carefully

Performance is one of the biggest gotchas in UTM devices: As you turn on features, performance can drop dramatically - or not at all. Security product vendors don't hide these performance costs, but they don't make it easy for you to understand what the impact of enabling different UTM features will be on your system performance. Make sure you know exactly what your UTM configuration will be, and test it to be sure that performance matches your requirements. Speed drops of 75% to 90% are common with a single check box. Be sure you also have plenty of headroom. IPS rules, for example, will only get more complex over time, so your IPS will get slower and slower over time.

### 2. Don't shortchange management

UTM firewalls have a lot to



say, with each layer of the firewall logging information about the traffic flowing through it. Enterprises are increasingly being asked to capture and retain these voluminous firewall logs for months or years. Make sure you plan for a dedicated management server with plenty of disk space, memory and CPU power to handle these chatty boxes. Although some enterprise vendors still allow management to be handled via a Web GUI or through a management server running co-resident with a firewall, don't be tempted to skip a properly separated and sized management system.

### 3. Verify high-availability and scalability features

As firewalls take on more functions and become more central to correct network operation, ensuring high availability and scalability also is more important. Because performance is more likely to be a bottleneck in UTM, active/active configurations are more attractive than active/passive - but such configurations are more difficult to build and test. Simulating all the different failures, and making sure that you test them in all the different states of the cluster, can be a five-day and not a five-minute job. We also found that

not every feature in our UTM devices works in the same way. For example, the basic firewall and VPN functions are usually shared cleanly across a cluster, but dynamic routing may not be as well thought out. If the VPN tunnels stay up across an individual device failure but the cluster doesn't know how to route the packets, that's not "highly available."

### 4. Complex configurations are hard to verify

During our testing, we found that the firewalls often were not doing what we thought we had asked for, especially in the area of UTM add-ons such as antivirus and IPS. You should be prepared for a second round of training on system management and configuration, because what you thought you knew about your enterprise firewall may not be enough to get a proper UTM configuration in place. Even if you think you know what you're doing, it's valuable to run simple tests to validate that the protections you've asked for are actually activated. The terminology and protocol coverage varies wildly across different products, and a simple check box for a UTM feature may need an hour of testing to understand.



## The best practices for network security

We all face it - the daily barrage of spam, now infested with zero-day malware attacks, not to mention the risks of malicious insiders, infected laptops coming and going behind our deep packet-inspecting firewalls and intrusion-prevention systems. Some even have to worry about how to prove steps of due care and due diligence towards a growing roster of regulatory compliance pressures.

What can you do under so much extreme pressure to make 2008 a better year, not a year loaded with downtime, system cleanup and compliance headaches? While recent security concepts, such as unified threat management or network admission control are emerging as the essential security tools you should budget for, it's

also appropriate to focus on best practices. We've come up with what we would consider some of the best network security practices.

Here's our best practice list, in order of importance:

- 1) Roll out corporate security policies
- 2) Deliver corporate security awareness and training
- 3) Run frequent information security self-assessments
- 4) Perform regulatory compliance self-assessments
- 5) Deploy corporate-wide encryption
- 6) Value, protect, track and manage all corporate assets
- 7) Test business continuity and disaster recovery planning



# THE ECONOMICS OF CYBERCRIME

Hackers are no longer motivated by notoriety - it's now all about the money.

**C**ybercrime has become a profession; a business model – and the demographic of your typical mastermind cybercriminal is changing rapidly from lone bedroom-bound geek to the type of

organised gangsters more traditionally associated with drug-trafficking, extortion and money laundering.

It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes.

In fact, to make more money than can be made mass producing and selling Class A Heroin (and with far less risk), the only time the criminal need leave his/her PC is to collect their cash. Sometimes, they don't even need to do that...

In all industries, efficient business models depend upon horizontal separation of production processes, professional services, sales channels etc. (each requiring specialised skills and resources), as well as a good deal of trade at prices set by

the market forces of supply and demand. Cybercrime is no different; it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.

The rise of cybercrime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency.

The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill. The most straightforward is to buy the 'finished product', in this case we'll use the example of an online bank account. The product takes the form of information necessary to gain authorised control over a bank account with a six-figure balance. The cost to obtain this information? \$400 (cybercriminals always deal in terms of dollars). It seems like a small figure, but for the work involved and the risk incurred it's very easy money for the criminal who can provide it. Also remember that this is an international trade; many cyber-criminals of this ilk are from poor countries in Eastern Europe, South America or South-East Asia.

The probable marketplace for this transaction will be a hidden IRC (Internet Relay Chat) chatroom. The \$400 fee will most likely be exchanged in some form of virtual currency such as e-gold. E-gold accounts are unregulated, registered offshore and can be set up online and transferred to 'real money' accounts anonymously.

Not all cyber-criminals operate at the coalface, and certainly don't work

exclusively of one another; different protagonists in the crime community perform a range of important, specialised functions.

Gaining control of a bank account is increasingly accomplished through phishing. There are other cybercrime techniques, but space does not allow their full explanation. All of the following phishing tools can be acquired very cheaply: a scam letter and scam page in your chosen language, a fresh spam list, a selection of php mailers to spam-out 100,000 mails for 6 hours, a hacked website for hosting the scam page for a few days, and finally a stolen but valid credit card with which to register a domain name. With all this taken care of, the total costs for sending out 100,000 phishing emails can be as little as \$60. This kind of 'phishing trip' will uncover at least 20 bank accounts of varying cash balances; giving a 'market value' of anything between \$200-\$2,000 in e-gold if the details were simply sold to another cyber-criminal. The very worst-case scenario is a 300% return on the investment, but it could be ten times that.

Better returns can be accomplished by using 'drops' to cash the money. The risks are high though; drops may take as much as 50% of the value of the account as commission, and instances of 'ripping off' or 'grassing up' to the police are not uncommon. Cautious phishers often separate themselves from the physical cashing of their spoils via a series of 'drops' that do not know one another. However, even taking into account the 50% commission, and a 50% 'rip-off' rate, if we assume a single stolen balance of \$10,000-\$100,000, then the phisher is still looking at a return of between 40 and 400 times the meagre outlay of



his/her phishing trip.

The alarming efficiency of cyber-crime can be illustrated starkly by comparing it to the illegal narcotics business. One is faster, less detectable, more profitable (generating a return around 400 times higher than the outlay) and primarily non-violent. The other takes months/years to set-up or realise an investment, is cracked down upon by all almost all governments internationally, fraught with expensive overheads, and extremely dangerous.

On top of viruses, worms, bots and Trojan attacks, organisations in particular are contending with social engineering deception and traffic masquerading as legitimate applications on the network. In a reactive approach to this onslaught, companies have been layering their networks with stand alone firewalls, intrusion prevention devices, anti-virus and anti-spyware

solutions in a desperate attempt to plug holes in the armoury. They're beginning to recognise it's a failed strategy. To fight cyber-crime, there needs to be a tightening of international digital legislation and of cross-border law enforcement co-ordination. But there also needs to be a more creative and inventive response from the organisations under threat. Piecemeal, reactive security solutions are giving way to strategically deployed multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organisations can consolidate their security capabilities into a commonly managed appliance. These measures combined, in addition to greater user education are the best safeguard against the deviousness and pure innovation of cyber-criminal activities.



This article is based on a paper entitled "Dirty Money on the Wires: The Business Models of Cyber Criminals" that was written by Guillaume Lovet, EMEA Threat Response Team Leader at Fortinet

# BEYOND UTM

## The value of a purpose-built network security platform

**T**oday's organizations must account for more points of entry into their networks, more types of resources that require protection, and substantially greater diversity of the threats seeking to exploit any weaknesses that may be present.

A corresponding implication then is that taking an approach to information security that is heavily dependent on point products is also no longer sufficient. Indeed, real-world experience has clearly demonstrated that given the conditions discussed above, the cost and complexity of such a strategy will quickly become overwhelming, not to mention counterproductive.

Therefore, many organisations have selectively implemented and continue

to consider unified threat management (UTM) devices as a means to restore balance to their overall security solution.

To be clear, there is little doubt that the reductions in cost and complexity and improvement in effectiveness that result from having a wide range of security capabilities available in a single device are advantageous. However, it should be equally clear that "actual results will vary". After all, not all UTM technology is created equal. Gains will inevitably vary considerably from one product to the next based on a range of possible differences, such as: the source, quality, and comprehensiveness of the individual security and networking components; the degree of functional integration; the degree of management

unification; and the suitability and capabilities of the underlying hardware.

In contrast, it is only with a purpose-built network security platform—as defined by this paper—that organisations will be assured of maximum security effectiveness, minimum cost of ownership, and the greatest degree of flexibility and overall performance.

### What is a purpose-built network security platform?

For all intents and purposes, a purpose-built network security platform is effectively an advanced UTM solution—one that employs an optimized design to ensure that organizations can maximize the associated gains. Jumping right in, the three high-level requirements that define a purpose-built network security

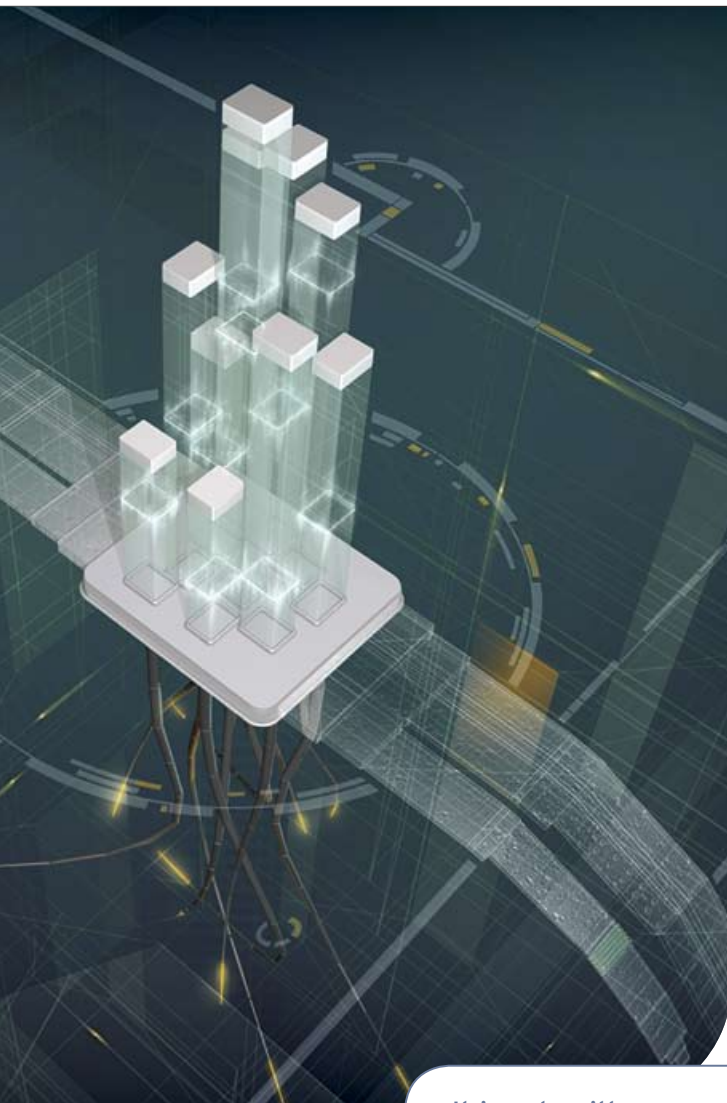
platform are that it must be a turn-key system, it must have capabilities that are tightly integrated yet remain modular, and, it must be based on engineered hardware.

### A turn-key system

To qualify as a turn-key system, a given offering must incorporate all of the elements required to have a complete solution. For starters, this entails having a pre-packaged device that combines hardware, network security operating system, and all requisite security software.

Details on what all of the above qualifications actually entail can be gleaned from the following descriptions of each of the high-level components that comprise a turn-key system in this context.





#### Hardware

This component is covered in detail in its own section later in the paper, but basically entails having hardware that is engineered specifically to ensure maximum performance for the supported security and networking features.

#### Network security operating system

This is an easy component to overlook. In general, beyond merely being present, an ideal operating system should exhibit three key characteristics. First, it should be hardened. To maximize system security and reliability, all unnecessary services should be eliminated, or at least turned off, and all “weak” services should be strengthened or, better

yet, replaced with hardened alternatives.

Second, the operating system should be pre-tuned. Similar to hardening, this process also involves trimming and modifying services, but in this case the objective is to help maximise performance of the supported applications. Speaking of applications, the third necessary characteristic is the incorporation of an extensive set of networking capabilities (i.e., service-oriented applications), including support for: multiple routing protocols (e.g., RIP, OSPF, BGP), translation techniques (e.g., NAT, PAT), switching, VLANs, traffic prioritisation, virtual systems, and failover and

clustering.

#### Integrated, modular capabilities

The next high-level requirement that defines a purpose-built network security platform is that it must exhibit significant degrees of integration, yet still be modular in nature. Clearly, both parts of this requirement start to get to the heart of the issue of “how a solution is built”. Sensible integration is one of the keys to obtaining optimal performance, and is also the essential element for enabling the combination of individual countermeasures to effectively be greater than the sum of the parts.

#### Integrated processing

Actually, this is just another way of saying that, to the extent it makes sense, redundant processing should be eliminated by having different capabilities “share” the execution of common routines. For example, “cracking packets” multiple times, once

for each countermeasure, would be highly inefficient.

That said, not all processing can/should be consolidated since some countermeasures rely on fundamentally different inspection techniques (e.g., processing for a firewall rule set proceeds progressively until a match is made, whereas processing against a threat database is typically exhaustive).

#### Integrated management

This is a particularly significant item, especially since it is one of the most common shortcomings of many conventional UTM products. To start with, it includes integrated policy. This way

all of the settings pertaining to a given domain can easily be established, as well as subsequently modified, in a single place.

#### Engineered hardware

The third and final high-level requirement that defines a purpose-built network security platform is that it must be based on engineered hardware. In general, what this means is having hardware that guarantees sufficiently high performance based on it being “matched” to the specific security software, networking services, and implementation scenarios that it is intended to support.

#### Conclusion

Over the past few years, it has become quite clear that security strategies based predominately on point products are not sustainable. Ongoing changes to the threat and technology landscapes ensure that the resulting, cobbled-together “solutions” inevitably lead to mounting capital and operational costs and, somewhat ironically, to diminishing levels of effectiveness. Faced with this situation, organisations are seeking ways to reduce the complexity, improve the effectiveness, and enhance the operational efficiency of their network-based security defenses.

On the surface, conventional UTM technology seems well suited to these requirements. However, the UTM market is quite crowded and the corresponding products vary considerably in terms of quality and overall effectiveness. Fortunately, organisations can cut through the confusion by embracing purpose-built network security platforms instead. By featuring integrated yet modular capabilities and engineered hardware, these turn-key systems effectively guarantee maximum gains in terms of security effectiveness, operational efficiency, and total cost of ownership.

**It is only with a purpose-built network security platform that organisations will be assured of maximum security**

# ERECTING BARRIERS

The multipurpose security appliances that consolidate firewall/VPN, content filtering, intrusion prevention and more into a single box are winning favour as easy-to-manage devices. Patrice Perche, VP of EMEA, Fortinet, talks about the market drivers and his company's plans for the region.

**NWME: What kind of potential market opportunity do you see in the Middle East and how committed are you to this region?**

**Perche:** The Middle East is strategic for us and we are fully committed to reinforcing our presence in that region. We started making business here two years ago and enjoyed phenomenal growth thanks to the work achieved by our partners, who have done an excellent job in providing support to our customers in the region. In 2007, we took Fortinet to the next level of development by having dedicated resources with Bashar Bashaireh, as the regional manager, and opening our own office.

Overall, the Middle East is a great place to do business in right now and provides us with many business opportunities. So far, we've seen a strong demand for unified security in verticals such as finance, education and telecommunications. Companies from those sectors have been our primary customers but there's a big opportunity in the enterprise market, meaning large companies, and the government sector. We enjoy great success in those

verticals in many countries across the world, and we're starting to see some success in the Middle East as well.

**NWME: What is driving the uptake of UTM appliances in the region?**

**Perche:** In recent years, the development of "blended threats", meaning malicious software that combines attack characteristics from different categories, has amplified. The uptake of UTM technologies and products owes much to the emergence of those blended threats.

In parallel, the success of UTM is also driven by the fact that many companies realized that choosing to layer their networks with stand-alone firewalls, intrusion prevention devices, anti-virus and anti-spyware solutions in a desperate attempt to plug holes in the armoury is a failed strategy. Piecemeal, reactive security solutions are giving way to strategically deployed, integrated multi-threat security systems, which provides multiple layers of protection, such as the integration of firewall with AV, IPS, web content filtering, etc.

At last, another major driver in the region is OPEX. With UTM, instead of having



Patrice Perche, VP of EMEA, Fortinet

to install, manage and maintain disparate devices, organisations can consolidate their security capabilities into a commonly managed appliance. Choosing point solutions means managing multiple devices, multiple licenses, multiple

software upgrades, etc. With a single security platform to deal with the impact on operating expenditure can be enormous and with total cost of ownership reduced budgets are being freed up for other projects.

The best security

**In the Middle East in particular, we see that a large proportion of our sales throughout the region have been for the deployment of chassis-based UTM appliances for medium to large enterprises throughout every verticals.**

solution isn't the largest, most expensive or widely distributed. After all, information is most secure when it is protected via an intelligent approach. Unified security dramatically reduces infrastructure complexity and deployment cost.

**NWME: What are the major threats that Fortinet as a vendor has identified?**

**Perche:** The major threat to Fortinet's continued growth in the Middle East is to not be perceived as a strong local security player or fully committed to this region. Many other companies have suffered from what was perceived as a lack of commitment to the region and that is why it is critical for us to invest in local presence. As I said earlier, we have now opened our own offices in Dubai and heavily invested to ensure there is a local support infrastructure in place.

Our customers in the Middle East often ask about Fortinet's investment in the long term. So, we prove them by our decisions and investments that we are strongly committed to growing our business in the region.

**NWME: So far, UTM's have been popular only with SMBs. Are you also planning to tap the enterprise market, where requirements are more exacting and security architectures are more complex?**

**Perche:** I agree that UTM has been first adopted by SMBs that were looking for a simple security solution to effectively protect themselves against

Internet threats. However, UTM appliances are definitely adopted by the high-end market and at Fortinet, over 60% of our customers are actually large enterprises, telco carriers and global MSSPs. Fortinet does not have the positioning of vendors such as Sonicwall, which is only selling to SMBs. Our strategy is to be recognized as one of the top global security players and for that high-end selling is critical.

In the Middle East in particular, we see that a large proportion of our sales throughout the region have been for the deployment of chassis-based UTM appliances for medium to large enterprises throughout every verticals, including service providers, telco carriers and the industry sector that have identified the need to protect their infrastructures from increasingly sophisticated threats. Using more and more bandwidth-hungry applications, these enterprises require exceptionally fast network security performance and that's why they choose our FortiGate multi-threat security appliances. Our security devices, based on ASIC-accelerated hardware, can provide the high-end 10GigE performance and reliability that these organizations need. Also, our management and reporting tools are critical for these large enterprises that are looking for granular control as well as ease and efficiency in management and maintenance.

Also, virtualised security is becoming a key requirement for MSSPs, carriers and large enterprises. In fact, the need

for securing and segmenting networks and applications increases. Virtualisation provides a method for allowing this type of segmentation, while also consolidating multiple networking devices, reducing network hardware and switch ports, and decreasing operational data center costs.

Fortinet is the only vendor to provide complete virtualized UTM. We can virtualise, or "divide," our FortiGate multi-threat security appliances into multiple, separately provisioned and managed instances through integrated virtual domain, or VDOM, functionality. This is a key competitive advantage that allows us to bring integrated security to the high-end market as well.

**NWME: What are the key issues to consider while evaluating enterprise UTM's?**

**Perche:** Not all UTM technology is created equal. Gains will inevitably vary considerably from one product to the next based on a range of possible differences, such as: the source, quality, and comprehensiveness of the individual security and networking components; the degree of functional integration; the degree of management unification; and the suitability and capabilities of the underlying hardware.

Fortinet has created its purpose-built network security platform from the ground up and we own 100% of our technology. By featuring integrated yet modular capabilities

and engineered hardware, our systems effectively guarantee maximum gains in terms of security effectiveness, operational efficiency, and total cost of ownership. Also, the fact that our platform are based on ASIC acceleration allows us to provide very strong performance, which is a key differentiator, as most UTM solutions will suffer from their lack of performance in comparison with point security solutions.

Also, when evaluating enterprise UTM, I would advise companies to look at certification as it represents third-party validation. Fortinet solutions have received a great amount of industry certifications including: FIPS 140-2, Common Criteria EAL4+ and multiple ICSA Labs Certifications including SSL-TLS (VPN), IPSec, Network IPS, Antivirus, and Firewall. The FortiGate product portfolio is one of the few UTM systems certified by the independent NSS test labs for UTM.

**NWME: What kind of products and solutions can we expect from Fortinet in the future?**

**Perche:** Fortinet will keep focusing in providing higher performance for the best levels of security and costs. In this arena, you should expect the launch of new high-end products for this year. In parallel, we are working on systems that combine high-performance switching, multi-threat security and granular access controls. In fact, we believe that the future of security vendors is in the development of more flexible products that combine security with networking. We launched the FortiGate-224B, the first in a line of unified security and networking platforms, in February last year and other products will follow.

# STRATEGIC SECURITY

The UAE Central bank has beefed up security for its electronic payment network with a multi-threat security appliance from Fortinet, safeguarding confidential data.

**U**AE Central Bank, plays a vital role in the United Arab Emirates (UAE) national economy as it directs monetary, credit and banking policy and supervises its implementation by all banks operating in the UAE. The Central Bank's main responsibilities include the definition and implementation of the banking, credit and monetary policy. It also provides the core payment systems in the UAE.

Given its role, it was crucial for UAE Central Bank to look for a security solution that could help protect its main services. Those include its Image Check Clearing System, which is the electronic system the Central Bank will use to clear all checks that are deposited through

banks in UAE; its reporting services, which are an essential part of their role as supervisor of financial institutions in the UAE; and, its email servers confined in a closed internal network.

UAE Central Bank tendered their security and performance needs. To find a solution that would meet their security and performance requirements. After evaluating several security vendors' solutions, the UAE Central Bank

chose Fortinet's FortiGate-800 integrated security appliances and worked with Fortinet on the implementation.

"We handle a lot of very confidential and time sensitive data for which security is absolutely essential. So, when we decided to move our existing services and systems online for more efficiency, we had to ensure that not only our data would be protected but also that

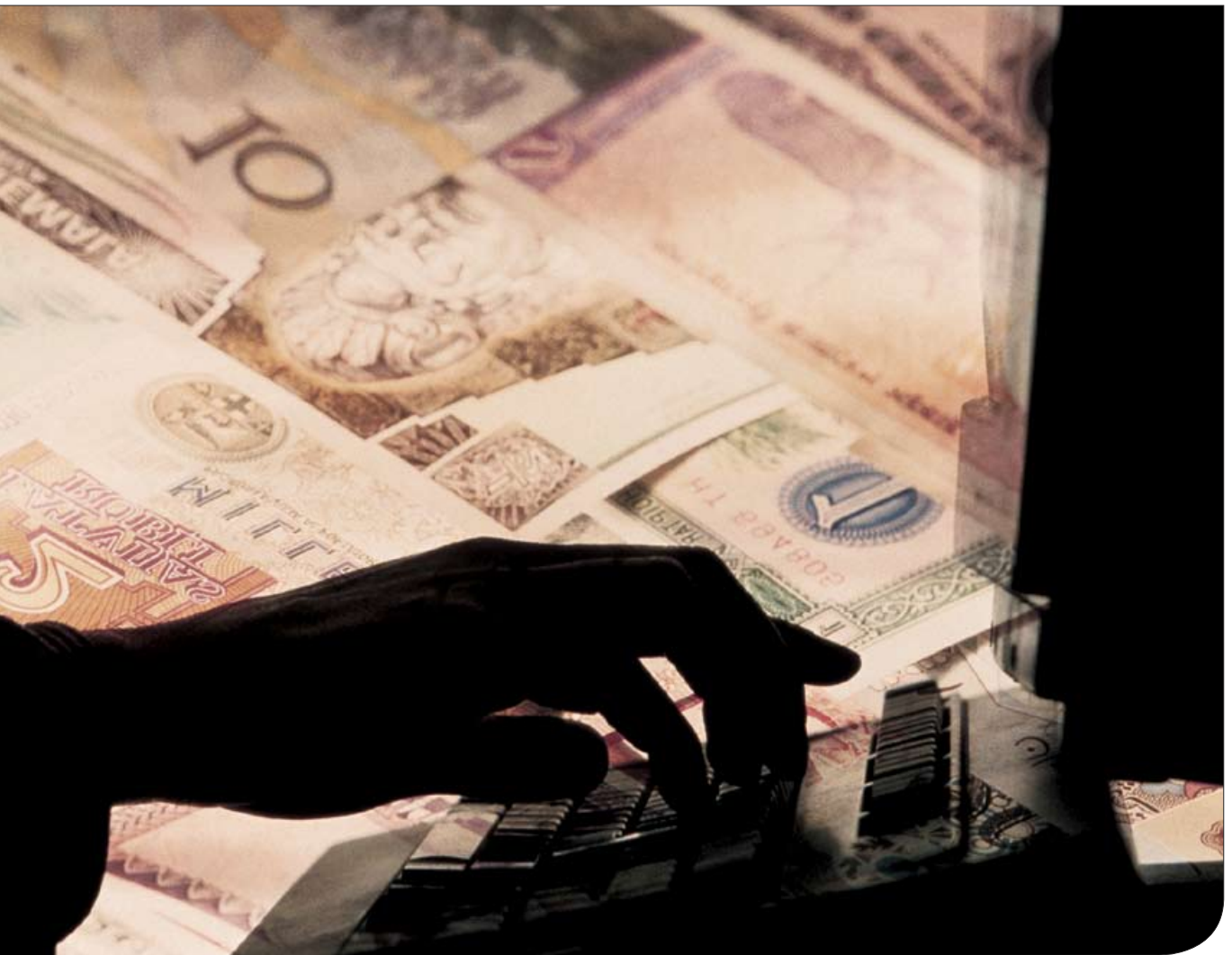


**"We handle a lot of very confidential and time sensitive data for which security is absolutely essential. So, when we decided to move our existing services and systems online for more efficiency, we had to ensure that not only our data would be protected but also that our network would maintain its high performance, delivery throughput and high availability"**

**- Bob Thomson, senior manager, IT projects at UAE Central Bank**

our network would maintain its high performance, delivery throughput and high availability. Fortinet's FortiGate-800 systems provided the performance, flexibility and security we were looking for," said Bob Thomson, Senior Manager, IT projects at UAE Central Bank.

Alireza Bozogmir, Fortinet Product Manager, Secureway, added, "We always work closely with our clients to provide



the right solutions. We recommended Fortinet's integrated network security appliances to the UAE Central Bank because we needed a solution that was reliable and could fulfill the bank's need for a highly available and flexible security solution for its new Image Check Clearing System offering to the banks across the country."

Fortinet's enterprise-class security appliances have been deployed as part of the Central Bank's primary firewall and antivirus solution to help safeguard data, online transactions and

communications. UAE Central Bank deployed two FortiGate-800 multi-threat security appliances in a cluster at its central office in Abu Dhabi for automatic back-up without downtime and one FortiGate-200 appliance at its Dubai office, which works as the bank's disaster recovery center. Fortinet's security appliances are also providing granular security through multi-zone capabilities, allowing administrators to segment their network into zones and create specific policies between zones.

"Between the high

sensitivity of financial data and the banking industry's inevitable evolution towards online communications, financial institutions have more stringent network security requirements than ever," said Bashar Bashaireh, Middle East Regional Manager at Fortinet. "Many enterprises, such as UAE Central Bank, realize that in-depth defense is what's needed to help prevent network compromise and choose FortiGate systems to help effectively protect themselves against blended security threats coming from both external and internal sources."

### Executive summary

**Challenges** - Protecting the sophisticated electronic check-image exchange system. Securing confidential data and communications without sacrificing network performance.

**Solution** - Fortinet's FortiGate-800 integrated security appliances.

**Benefits** - Greater security against blended threats, both external and internal. Granular security through multi-zone capabilities.

# RAISING THE BAR

The UAE University has revamped its security infrastructure, taking a layered approach to whip blended threats

**T**he UAE University has nine separate campuses mostly based in Al Ain with one in Abu Dhabi. Each college campus has its dedicated on-site IT support that can escalate a problem to the central helpdesk, which, in turn, refers it to either the Applications Division or to the central Infrastructure and Core Technologies Division. The Applications Division handles all software related issues whereas the Infrastructure and Core Technologies Division deals with all other issues related to the IT infrastructure in the UAEU.

"IT works in layers, and we are focused on providing good quality IT services and infrastructure to our end users, meaning the students and staff of the University," said Manmohan Singh, Director of Infrastructure & Core Technologies at UAE University.

On the security front, the Infrastructure and Core Technologies Division at UAEU realized that its existing security set up had some limitations in terms of hardware and support. The previous firewall and Content Services Switch (CSS) had reached end of life and end of support since 2003. Support in terms of spares, telephone



support, new patches and software updates were unavailable and the University had no form of monitoring, reporting or alert. This put the University at very high risk and UAEU therefore decided to replace its existing firewall and security setup with a complete security solution, which would provide multiple layers of protection aka Unified Threat Management (UTM).

Hani Sultan, Security Project Manager, UAEU, said, "The previous Cisco Intrusion Detection System (IDS) was out of date and not functioning. The university

constantly experienced worm and virus infections that were attacking servers, consuming network bandwidth and causing considerable network downtime. That's why we wanted to replace the outdated broken intrusion monitoring system with new UTM technology, which would provide complete online protection to the university users."

UAEU also had no SMTP gateway. Internet users were directly connected to the University's internal email server, which made it vulnerable to attacks, spoofing and mailbox hijacking.

So, as part of its continued overhaul of its IT infrastructure, the university decided to upgrade and update its security implementations, including setting up proper security standards, in order to be able to provide free access to learning tools through the Internet to its staff and students without jeopardising the integrity of its network and other services.

To provide true protection against the Internet threats and other malware, UAEU was looking for a solution that would allow the migration of its 20,000+ mail users to a proactive anti-virus, anti-spam service for both its outgoing and incoming mail, with a managed service that was easy to configure and that provided direct user

UAEU evaluated several security products and solutions in the market and found that Fortinet's range of security appliances provided all the features they were looking for without affecting the overall network performance. So, the university opted for two FortiGate-3600A multi-threat security systems for its firewall needs and two FortiGate-1000A appliances to provide all the built-in network-level and content-level threat protection. Combined with multi-gigabit performance, all the FortiGate appliances ensure security and throughput.

In order to effectively combat spam within the academy and secure its internal email server, UAEU deployed two FortiMail-2000A multi-layered, email security platforms. This deployment provided Secure Messaging Platform (SMTP Gateway) to provide optimum configuration flexibility with enterprise-class Antispam and Antivirus features to secure mission critical email applications. This gives its 20,000+ users authenticated access to their mails and prevents spam and spoofing.

On top of the deployment of those security appliances, UAEU wanted to be able to get a comprehensive view of its network usage and security information. The University therefore deployed Fortinet's FortiAnalyzer, which securely aggregates and

time network log records, as well as a comprehensive report and analysis of network usage and security information, supporting its need for discovering and addressing vulnerabilities across dispersed FortiGate systems. FortiAnalyzer also provides advanced security management functions such as quarantine archiving, event correlation, vulnerability assessments, traffic analysis, and content archiving.

The FortiGate integrated security appliances provide antivirus, antispam and firewall proactive protection for both UAEU internal (for data centre, to protect server, our resources) and external communications, deploying multiple DMZs- for SSL VPN, VOIP. FortiAnalyzer provided centralized logging and correlations for its systems and devices, providing essential tools and reports for troubleshooting.

In addition, FortiMail was deployed for both UAEU's incoming and outgoing mail. Despite a total of over 20,000 users, many of whom are using the email services simultaneously, UAEU managed to migrate its system from a Cisco configuration to Fortinet's FortiMail within 36 hours with a record down time of less than one minute, including providing a managed service that provided transparency and direct interface to its users.

"We found the Fortinet solutions easy and flexible to deploy," continued Singh. "We were able to activate as many or as few applications as we needed. Besides, unlike Symantec, FortiMail has provided us with excellent results by reducing spam and viruses. We feel we have more control and, using Fortinet, we have succeeded in protecting the entire network from all types of Internet threats."

**As part of its continued overhaul of its IT infrastructure, the university decided to upgrade and update its security implementations, including setting up proper security standards, in order to be able to provide free access to learning tools through the Internet to its staff and students without jeopardising the integrity of its network and other services.**

interface. At the network level, the university wanted a high-performance firewall solution with multiple DMZ's.

Security Project Managers at

analyzes log data from the FortiGate security appliances deployed throughout its network. FortiAnalyzer provides UAEU with real-

# ON THE FRONT LINE

The Kuwait-based FASTtelco has bolstered its managed security services to SMB users by deploying a multi-threat security platform

**F**AST Telecommunication (FASTtelco) is the leading telecommunications service provider in Kuwait servicing business and consumer sectors, with a nation wide network. FASTtelco delivers business grade data communication services including IP-VPN, Internet, ISDN, IP Centrex, data center and collocation services and managed services. On the consumer front, the provider's services include dial and broadband Internet for residential applications. FASTtelco's services are delivered using direct fiber optics, xDSL, leased lines and latest WiMAX.

FASTtelco identified an

increasing demand from the SMB market for managed security services, specifically ones relating to the protection of their network from Internet threats. The service provider foresaw this demand as an opportunity to introduce network security as a managed service that would enable them to deliver clean Internet to all types of businesses.

The service provider started to look for a multi-threat security platform that would allow them to protect small and medium businesses in Kuwait while optimizing their operational data center costs.

"We have evaluated security solutions from various vendors but very few had solutions specifically

tailored to the needs of MSSPs." said Omar Kaaki, General Manager of FASTtelco. "The ability of the FortiGate solution to virtually segment each customer's connection and customize its configuration and profile to access all or several of the security applications we offer was decisive in our choice. FortiGate's multi-threat security platform is definitely a great option for large data center deployments such as ours."

FASTtelco chose to rely on Fortinet's FortiGate-3600A multi-threat security platform for its new managed security services. The security appliance is set up with virtual domains in order to – from one same hardware platform – isolate the security services provided to each end customer and separate the management of these virtual services from one hardware platform.

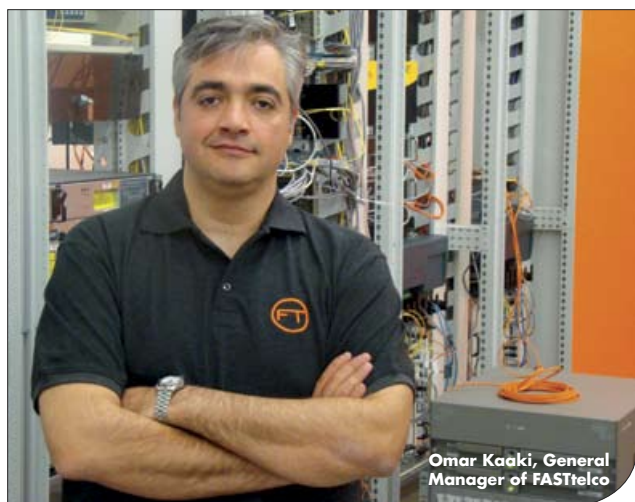
"Fortinet played a significant role directly and through its partner providing consultancy, project management and support services," continued Kaaki.

FortiGate-3600A provides FASTtelco with ten gigabit Ethernet interfaces and up to 6 Gbps throughput, delivering comprehensive network and content protection through the integration of eight essential security applications

and services - including antivirus, firewall, VPN, intrusion prevention (IPS), anti-spam, anti-spyware, Web filtering and traffic shaping. The systems are kept up to date automatically by Fortinet's FortiGuard subscription services, which provide continuous updates to ensure protection against the latest viruses, worms, Trojans, and other threats.

"The business of ISPs in the region has evolved and most of these are now looking for additional value-added services to offer their customers, especially at the corporate level," said Bashar Bashaireh, Middle East Regional Manager at Fortinet. "Managed security services have gained momentum in the Middle East and are poised to grow in the region. FASTtelco is one of the first to offer such a service in Kuwait their SMB customers can be confident that they now have a very cost-effective, secure network solution in place."

FASTtelco is now concentrating on educating the market on the advantages of managed security systems. Expansion of their security services is of course planned but, for the service provider, education is critical and is today's priority.



Omar Kaaki, General Manager of FASTtelco

## INCREASE YOUR SECURITY, NOT YOUR BUDGET



A scant decade ago, packet-filter firewalls were sufficient to protect against virtually all threats coming from the Internet. Today however,

the number, variety and sophistication of Internet threats against businesses have multiplied exponentially, but your day to day operation of security shouldn't.

These "Uber" – UTM devices will have implications for a variety of sectors, with three notable incarnations. The carrier and service provider would deploy them in an effort to filter out malicious traffic from their backbones offering their customers "clean pipes".

This is an idea that has been floating about for some years now, in which carriers should try, as far as possible, to remove viruses, Trojans, worms and malware from their networks, but which is, so far, not a reality for many reasons, including cost, skills and in many

cases, political will.

The second incarnation is within the enterprise core. Where advanced UTM devices would segment and protect every department and ultimately every device, truly hardening the internal network for the first time. And finally, at the small or remote office, the greatest benefit will be realised.

A single appliance will take the place of not only the numerous security devices needed to filter and protect, but also the router and switch.

Just imagine the complication of configuring stand-alone firewall, VPN, AV, IPS, Web Filtering and Anti Spam in HA mode. A rack full of products but even the top system integrators in town shy away from supporting you.

The UTM concept will assist end users to simplify their designs, have in-house skill sets, decrease the renewal cost, consolidate management and reporting and more importantly maintain their focus on other parts of security cycle.



Note: This article was contributed by **Bashar Bashaieh**, Middle East Regional Manager, Fortinet. He can be contacted at [bbashaieh@fortinet.com](mailto:bbashaieh@fortinet.com) Tel: +971 4 3757612

### 8 THINGS OTHER UTM VENDORS DON'T WANT YOU TO KNOW:

- 1) Their hardware is not an appliance, it's just a pizza-box server
- 2) Their hardware is not a purpose-built UTM and can decrease through-put performance
- 3) Their UTM is based on widely used OS which is hardened, but not proprietary
- 4) They have OEM agreement with third party vendors and do not own the technology
- 5) They all use Hard Disks in their UTM appliances which is the no.1 reason for failure.
- 6) Their centralized management solution is incapable of managing OEM products on their appliances (Third party restriction)
- 7) They cannot generate consolidated reports (Third party restriction)
- 8) Future support is not available when they switch OEM agreements.



# FORTINET. **FIRST FOR UNIFIED SECURITY.**

Best of breed security products have a lot in common. But you expect more.

In a world where your security strategy needs to cope with increasingly aggressive blended threats, demanding regulatory requirements and constantly changing business circumstances - complexity is your single biggest risk.

That's why Fortinet is becoming first choice for unified security with more enterprises every day. The outstanding performance of Fortinet solutions has attracted numerous industry accolades and an unprecedented seven ICSA certifications. For defense in depth, you need strength in breadth.

Fortinet protects your business communications by integrating firewall, VPN, antivirus, web filtering, P2P and IM control, IPS, anti-spam, anti-spyware, anti-phishing and QoS onto one high performance ASIC accelerated platform. Deployed as the one unified security solution, Fortinet is the core of your security strategy - reducing complexity and cost, while increasing protection, reliability and performance.

To test us against any solution for your next security project, contact our partner today and find out why Fortinet is first for unified security.

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

FORTINET. **FIRST FOR UNIFIED SECURITY.**

**FORTINET**<sup>™</sup>  
REAL TIME NETWORK PROTECTION

**SECURE  
WAY**

NETWORK DISTRIBUTORS

**SPECIALIST VAD  
SECURITY AND MOBILITY**

Al Thuraya Tower 2, Suite 1105, Dubai Internet City,  
P.O. Box 500640, Dubai, UAE, [www.secureway.ae](http://www.secureway.ae)  
+971 4 3757612 [fortinet@secureway.ae](mailto:fortinet@secureway.ae)