

THE EVOLUTION OF UTM

FORTINET™

REAL TIME NETWORK PROTECTION

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 threats against business networks have multiplied, and firewalls and antivirus software on desktops are no longer sufficient. The evolution of security systems and software to the present Unified Threat Management (UTM) appliance-type solutions is really a history of an "arms-race" between hackers, crackers and virus authors, and security vendors. Every time a new vulnerability is detected, new security mechanisms and measures are developed and put in place, but then some new way of getting past the defenses or attacking the security measure is developed. In recent years, the development of "blended threats", malicious software that combines attack characteristics from different categories, have been developed. Examples of these are Trojans with embedded spam engines, or viruses with spyware payloads. The development of UTM technologies and products owes much to the emergence of these blended threats.

THE ENEMY WITHIN

While UTM devices have so far been effective at stopping many external threats at the network edge, threats that originate internally are still difficult to defend against. Studies have shown that a significant part of network incidents are caused by disgruntled employees, and security administrators have tried to deal with this possibility by segmenting their networks to try to contain problems or isolate critical business information resources, such as the company database server or mail server. While this strategy may be effective against certain kinds of targeted internal attacks, there is another issue emerging: with more

companies issuing notebook computers to employees, there is an increasing risk that these notebooks may get infected or compromised, say while the employee is traveling and connecting via an unsecured wireless hotspot. An infected notebook computer connecting back within the corporate network would have circumvented the gateway defenses and may potentially infect all the computers on that network segment.

Although the focus of most security products thus far has been protecting the "choke-points" of the network, the "blurring" of the network edge, which is the result of a more mobile workforce, will eventually require security vendors to think also about protecting each network node. This is where I see the next stage in the evolution of security.

SECURITY WITHIN THE NETWORK VS. NETWORK SECURITY

A series of developments in network security are leading to the emergence of a comprehensive solution that could make the network itself so resilient that it is impervious to most attacks. A key component of this solution is evolving from the product vendors that are most often associated with UTM, Unified Threat Management.

Two major drivers have pushed internal network security to a crisis point. These are:

Cyber crime. As criminals, who have thrived on identity theft and extortion, become more and more successful they are casting their nets wider and wider. They are now targeting specific companies and web sites that offer rich opportunities because they generate valuable transactions or are repositories for large collections of personal data such as credit card or bank accounts.

Malicious insiders. The number of tools and techniques available to the average end user for hacking, scanning, and exploiting network resources has increased dramatically. Over time the number of insider incidents that lead to real losses of either information or business resources will only go up. The LAN access point must be treated as a security perimeter in order to protect the organization from attacks coming from that quarter.

There are myriad entries in the UTM pantheon ranging from Linux servers running separate security applications to hardware chassis designed to house multiple servers, all the way to purpose-built security platforms with deep packet inspection capabilities that allow continuous scanning of all traffic to provide protection at the content layer.

The components that comprise true UTM capability have always included:

Firewalling. The ability to enforce a connection based policy along with requirements for SSL and IPSec VPN.

Intrusion prevention (IPS) has seen a dramatic uptake because it can counter the spread of worms and block some targeted attacks. Yet a common concern raised by enterprises IT administrators over IPS is that it creates a "clean" side and a "dirty" side within the network. In other words machines on the same LAN segment as an infected machine would be at risk. In order to be completely effective IPS would have to sit in front of every end point device.

In-line Anti Virus has become a driver in the security appliance space because the volumes of unwanted or infected email, IM, and P2P files are impacting the ability of their respective servers to handle them.

URL Content Filtering was initially not associated with security. But as more web sites began to contain malicious content it became a critical component of end user defense.

And of course, the combined functionality of these UTM features has brought even greater benefit as attacks that combine elements of malicious software with network attacks over new protocols are countered by an integrated appliance.

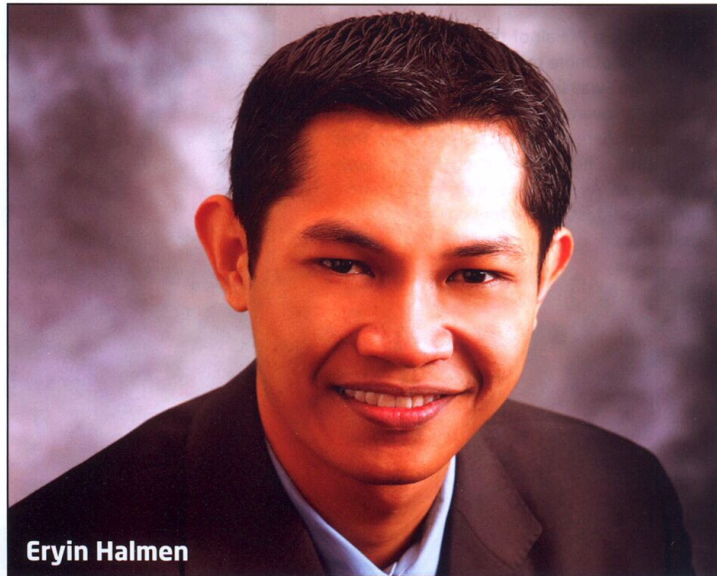
The next evolution in these combined function security appliances is the addition of networking capability. Routing protocols such as OSPF, RIP, and BGP provide the architectural flexibility that many enterprises demand without the expense of designing, configuring, and maintaining separate routers and load balancers. In many cases a UTM can be deployed without the need for a router at all, thus enhancing its value proposition.

Internal segmentation has always been problematic. As a mechanism for containing threats or isolating parts of the network, it seems more like an expensive kludge rather than an elegant solution. The level of policy setting required is too granular, and requires a breadth of skills that most administrators in all but the largest companies lack. When the requirements for implementing this are quantified, it can seem either too expensive or simply beyond the capabilities of SMBs to competently implement.

As UTM has shown, aggregation and integration of security functions can be an effective and economical solution - both in terms of money and effort - for corporate networks of any size. There is an opportunity, therefore, for security vendors to develop solutions that secure the network fabric by combining the functions of network switch, IPS, AV, firewall and router. In other words, collapsing the switch and router into the traditional UTM security appliance.

THE PROPOSED SOLUTION

This solution relies most heavily on a switched network architecture. These



Eryin Halmen

usually involve core switches as well as access switches. Virtual LANs (VLANs) would be used to provide granularity down to the device where needed. The switch enforces policy based on layer 2 and 3 information. Data streams that are normal and therefore allowed would be filtered by additional IPS functionality. The IPS filtering ideally is performed directly within the switch. Connections to the Internet and third parties would be made with firewall capabilities also embedded in the switch. This next generation UTM security device would also provide additional network segmentation such as for Transaction Zones and departmental barriers.

There will be three major incarnations of these super-UTM devices. The carrier and service provider would deploy them in an effort to filter out malicious traffic from their backbones. They would then be able to offer their customers "clean pipes". This is an idea that has been floated 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 some cases, political will.

The second incarnation is within the enterprise core where these advanced UTM devices would segment and protect every department and ultimately every device. Truly hardening the internal network for the first time.

And at the small office, or remote office the greatest benefit will be realized. 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.

This concept takes UTM far beyond its birth as a simple security platform. The industry will see some major dislocations as security devices begin to harbor networking features. Traditional router and switch vendors will find that their products, built on speed and simplicity, are not able to accommodate deep packet inspection and granular defense. Security vendors that specialized in firewalls or IPS will find that they are being supplanted by more flexible products that combine security with networking.

This article was contributed by Mr. Eryin Halmen, Country Sales Manager of Malaysia & Brunei, Fortinet Malaysia Sdn Bhd.