

Unified Threat Management

Experience the All-in-One

The all-in-one approach of UTM simplifies product selection, product integration, and ongoing support. Besides these, convenience and ease of installation along with lower TCO has made the UTM market very special. In this article, we deal with different aspects of UTM and explore the solutions available in Indian market.



Multiple solutions in one box is not a very new demand but challenging for vendors to meet the demand architecturally with combination of performance and lower price range.

The accelerated demand has opened up a market for new appliances called 'Unified Threat Management' (UTM). The term "Unified Threat Management" was named by Charles Kolodgy of International Data Corporation (IDC) in 2004. Rather than

administer multiple systems that handle anti-virus, content filtering, intrusion detection and spam filtering, companies started to search out a firewall appliance that integrates all of the solutions into a single rack mountable network appliance. The multiple functionality of the Unified Threat Management appliance fueled up the justification for replacing older more basic firewalls.

The Concept

Integrated appliances or UTM are complete solutions that incorporate core

security functions into a single solution to effectively prevent security breaches of the network.

UTM products typically provide all the essential security capabilities a company needs to protect its network, in a single appliance-type device, such as antivirus, firewall, intrusion detection and prevention, etc. For small and medium businesses especially, this "all-in-one" approach conveys several significant benefits over the alternative, "let's get one of each" approach, or point solution approach.

Selecting the latter means you can easily end up purchasing and supporting as many as six devices, all of which have to be configured and managed independently.

Explaining the necessity of the concept, **Vishak Raman, Country Manager, Fortinet India**, says that a single UTM appliance makes it very easy to manage your security strategy, with just one device to worry about, one source of support and

a single way to set-up and maintain every aspect of your security solution. So not only it is a cost-effective option, but day-to-day "running costs" will also be lowered significantly.



Vishal Dhupar, MD, Symantec India, also believes that the integrated security functions can be managed from a single management console included with the appliance. By using this management console, administrators can manage local and remote appliances over the Internet including advanced configurations, rule sets and cluster parameters. This is a cost-effective way of network protection from a single security expert.

The Evolution

When hackers were the primary focus of an IT enterprise, a firewall was sufficient to protect most networks. Then as viruses became more prevalent, corporates took to anti-virus gateways that scanned for viruses followed by Web content filtering, and later, spam filtering. This resulted in a mess of systems that were costly to administer and took up valuable rack space. Journey of UTM started from here.

According to **Digvijaysinh Chudasama, Vice President—Sales, Cyberoam**, first generation UTM appliances were just a loosely bonded combination of various security features. Such UTM appliances compromised granularity of individual

solutions and sacrificed flexibility. They could not handle the dynamic situations—Wi-Fi & DHCP environments and internal threats were not yet given their required importance. Second generation UTM devices had more granular features and focused on the internal threat protection. But to counter new threats like phishing, pharming that attacked individual users for financial gain and to provide protection against threats arising from employee internet usage (either due to employee ignorance or due to malicious intent), there arose a need for identity based security.

The third generation identity based UTM evolved



Solutions in Indian Market

With the growing demand of UTM, Indian market has become a lucrative market for UTM solutions/appliances vendors. Some vendors like Symantec and Juniper, have partnered with each other to bring out powerful solution combining their own technology expertise in their respective domains. With several innovative features and attractive price ranges, vendors have made their solutions available in Indian market. Some of them are here below:

FortiGate-800

The FortiGate-800 or 800F is an ideal solution for high performance antivirus and content filtering gateway, or as a complete network protection solution leveraging firewall, VPN, and IDP capabilities. The FortiGate-800 Antivirus Firewall features 4 10/100/1000 tri-speed Ethernet ports for networks running at gigabit speeds and 4 user-definable 10/100 ports that provide granular security through multi-zone capabilities, allowing administrators to segment their network into zones and create policies between zones. It includes salient features like Network-based Antivirus, Dynamic Intrusion Detection and Prevention, Firewall (ICSA Certified), VPN (ICSA Certified), Transparent Mode and Remote Access.



Check Point UTM-1

Beyond protecting against traditional threats through tightly-integrated security features including a stateful-inspection firewall,



IPSec VPN, gateway antivirus and anti-spyware, and intrusion prevention, Check Point's new UTM-1 product line also features an innovative Web Application Firewall to help protect Web servers, as well as advanced security functions for voice over Internet protocol (VoIP), instant messaging and peer-to-peer networks. Integrated Check Point SmartCenter management delivers centralized, built-in security

then. This latest generation UTM embeds user identity in firewall rule matching criteria, eliminating IP addresses as intermediate components to identify and control the user. This offers instant visibility and proactive controls over security breaches. Also, this delivers complete security in dynamic IP environments like DHCP and Wi-Fi where the user cannot be identified through IP addresses.

Commenting on the evolution of the solution, Vishak Raman says that the goal of UTM is to simplify the overall security solution despite the rising complexity and growing scope of the security problem. The most apparent aspect of this simplification is the physical consolidation of point products into a single product; hence the term unified threat management. Unfortunately, some UTM products have little else to offer.

Today's customer is not satisfied with point solutions or piece-meal solutions. He wants one vendor to be responsible for an end-to-end security solution. Such Integrated Appliances or UTM solutions are flexible enough to operate within current network environments as part of

an overall multi-tier, multi-platform security plan. This makes the security network easily manageable. Vishal Dhupar feels that integrated appliances or UTM solutions also provide the customer with an ideal way to reduce total cost of ownership by eliminating the need to deploy and manage multiple security products manufactured by different vendors. This also helps eliminate the complexity of security management.

Addressing the evolution perspective, **Bhaskar Bakhavatsalu, Country Sales Manager, Check Point Software Technologies, India**, says that the goal of UTM is to simplify the overall security solution despite the rising complexity and growing scope of the security problem. The most apparent aspect of this simplification is the physical consolidation of point products into a single product; hence the term unified threat management. Unfortunately, some UTM products have little else to offer.

TCO Justification

The new UTM approach gives important business advantages and surprisingly significant cost savings. For

example, if we consider the capital expenses and the operating costs of a typical traditional architecture and compare this to the operational costs of UTM solution, the Total Cost of Ownership (TCO) is clearly lower and according to experts a payback in as little as eighteen months is perfectly possible. If the ease of adding in future upgrades, improved availability and efficiency gains are added into the calculation, the payback will be nearer to twelve months. As well as showing good returns at large sites, UTM is ideal for small-to-medium users and large sites linked to branch offices and smaller satellite sites.

The security threat landscape is changing—threat volume is rising, threat-generation time is falling, and threats are becoming more elusive. Additionally,



management without the need for additional hardware or software. UTM-1 also enables secure connectivity for remote workers using integrated SSL VPN technologies, and gives IT administrator's greater visibility into their network infrastructure through comprehensive monitoring and reporting features.

Firebox X Edge from WatchGuard

WatchGuard Technologies has recently announced its Firebox X Edge e-Series line of integrated security appliances. Firebox X Edge e-Series appliances, aimed at businesses with 1-50 users, now support gateway anti-virus, intrusion prevention, spam blocking and enhanced URL filtering, in addition to its proactive application layer firewall and VPN capabilities. Because an intuitive Web-based user interface provides quick, out-of-the-box device configuration for all the necessary small business network security protections, Firebox X Edge is less expensive and less time consuming to administer than using multiple security solutions.



Cyberoam CR1000i and CR1500i Series

Cyberoam CR1000i and CR1500i series are powerful network security appliances delivering dynamic, multi-layered security with a high level of user identity-based granularity. Cyberoam offers user



identity-based firewall, VPN, anti-virus, anti-spam, intrusion detection and prevention—IDP, content filtering over a single platform to provide comprehensive security. In addition, with bandwidth management and Multi-Link Manager, they provide complete security for large enterprises.

more endpoints are having more connections to enterprise networks. The customers are looking for security solutions that will allow them to stay ahead of external threats, internal threats and allow them to track and enforce compliance of all network connections. Elaborating on the justification, Bhaskar Bakthavatsalu says "these solutions save time. They save money. And most important, they secure networks to ensure peace of mind—a benefit any CIO or IT manager can embrace in today's dynamic business environment. Customer should ideally consider each of the key attributes to ensure a secure and manageable framework that will serve the organization now and in the future."

Addressing the TCO issue Vishak Raman says, "UTM appliances are easier to manage because most or all of the security features are on a single box, using a single interface. They require fewer staff than point solutions that may need specialized skills to take care of a single aspect of security. They are frequently cheaper than point solutions because UTM devices sometimes do

away with operating system or per-seat licenses altogether. They offer more value simply because they have more security features on each box."

Agreeing to the justification, Vishal Dhupar says, "As all security functions were previously handled by multiple systems, UTM ensures lower costs. In addition, UTM also offers the advantage of scalability. The TCO factor, however, is one of the biggest evaluation criteria for UTM adoption."

Supporting the TCO justification, Digvijaysinh Chudasama, says, "When compared to the high capital and operating expense involved in deploying multiple stand-alone security appliances, UTMs already offer great cost-efficiency. Where capital expense is concerned, they cost a fraction of the



cost of a host of individual solutions. At the operating expense end too, they offer great cost benefits. They eliminate the need for multiple AMCs, dedicated technical persons to operate multiple solutions, in addition to the need to deal with multiple patches, upgrades and vendors while simplifying operations greatly."

Technical challenges

Some vendors bundle several security software packages into a commodity PC server, and call that a UTM product. In such cases, there may very well be compatibility issues, in addition to performance issues, and these products do not provide the same level of manageability and ease-of-use that other UTM vendors are able to provide.

Although many UTM products claim to fulfill all your "plug-and-play" deployment dreams, many fall short in some important way. Aside from ease of installation, there are three key criteria you should examine when making a purchasing decision:

Each of the components should be "best of breed": Each component of the solution should employ best-of-breed

SonicWALL PRO Series

The SonicWALL PRO Series solves security issues by combining multiple network and security functions including a deep packet inspection firewall, IPSec VPN, layered anti-virus, antispayware, intrusion prevention and Web content filtering capabilities into a single integrated appliance that is easy to manage and deploy. Based on a dynamically updateable platform, PRO Series appliances are automatically updated to ensure zero day protection against a variety of network and application threats. Optimized for advanced networking and ultra reliable operation, they are designed for mission-critical data and network communication deployments. At the core of every PRO Series appliance is SonicOS, SonicWALL's powerful operating system which provides policy-based firewall management over complex deployments and enables complete control over network traffic and application usage. The PRO Series features six models: PRO 1260,

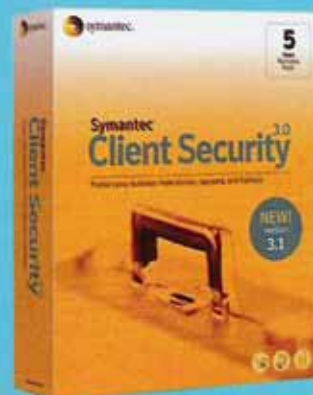


2040, 3060, 4060, 4100 and 5060, designed to meet the network security needs for organizations of all sizes.

Symantec Client Security 3.1

Symantec Client Security 3.1 helps keep client systems safe by providing comprehensive and proactive protection against malware with vulnerability-based detection. Integrated graphical reporting and simplified management of multiple, integrated security technologies allow organizations to maintain control of client systems, minimize productivity disruptions, and enhance client security.

It automatically detects and repairs the effects of spyware, adware, viruses, and other malicious intrusions in real time to help keep client systems safe. Vulnerability-based protection feature of this product proactively defends systems before operating system patches or virus signatures



technology. The solution should utilize proven technologies, even if they are from other vendors. There should be no compromise on quality of your security in order to have an integrated solution.

Components are really integrated:

Does the solution integrate the management and updateability of each of the components? For instance, even if the product uses a third-party antivirus or anti-spyware engine, it should be easily updatable from the main interface.

Ease of integrating into, and manage within, organizational environment:

Here's where many solutions really fall short. Some vendors assume that as a company requires an integrated appliance, they are dealing with a simple, single-site environment. This is rarely the case. Examine how easy (or not so easy) it is to manage and update the multiple UTM gateways across your network. Even three or four appliances can turn into both a management headache and a security risk if the UTM appliances are not capable of being managed and updated in a timely and streamlined fashion.

Though companies like Fortinet, Symantec, Check Point believes that

integration of different security components in single package raises compatibility and co-ordination issues but company like Gajshield does not believe in this and feels it is better for the customer as there is a single vendor who takes care of their perimeter security and it would be easier to build redundancies this way.

Market Facts

According to IDC, the Unified Threat Management (UTM) security system will outgrow the traditional firewall/ VPN appliances sector - garnering 58% of the overall share, since it integrates multiple security features like anti-virus, firewall, intrusion detection and prevention systems into a single appliance. Symantec believes that like most other IT products, the UTM market is gaining ground in SME and SOHO segments and is no longer just another corporate acquisition. India is an emerging market as far as security beyond antivirus goes. But with increased awareness and booming Internet penetration, it is experiencing tremendous growth. The need for securing enterprise assets and awareness has created a huge potential and an accelerated growth. Check Point also points out that similar to rest of the

world Indian market, specifically in the Small and Medium enterprise is edging towards an UTM appliance market.

According to Fortinet, India continues to be a fertile market for UTM products in APAC, registering the highest growth rates (CAGR - 24 %). The UTM market last year was around 30 crores and Gajshield calculates that it is expected to grow 100% this year.

Ending Note

The principal advantages of UTM are simplicity, streamlined installation and use, and the ability to update all the security functions or programs concurrently. As the nature and diversity of Internet threats evolves and grows more complex, UTM products can be tailored to keep up with them all. This eliminates the need for systems administrators to maintain multiple security programs over time. Even though of late several vendors have embraced the UTM by bringing out customized solutions and products, the applications and various functionalities of UTM has been deployed and utilized effectively by the end users. *

By: 'InfoSecurity' Bureau.

are available. Simplified management of the product provides real-time information of network client status and fast distribution of software updates and definitions.

Juniper SSG 500 series

The Juniper Networks Secure Services Gateway 500 Series (SSG) represents a new class of purpose-built security appliance that delivers a perfect mix of performance, security and LAN/WAN connectivity for regional and branch office deployments. Traffic flowing in and out of the branch office is protected from worms, Spyware, Trojans, and malware by a complete set of Unified Threat Management (UTM) security features including Stateful firewall, IPSec VPN, IPS, Antivirus (includes Anti-Spyware, Anti-Adware, Anti-Phishing), Anti-Spam, and Web Filtering.

Complementing the powerful UTM security features is a robust routing engine that allows the SSG 500 Series to be deployed as a traditional branch office router or as a combination

firewall and routing device to reduce capital and operational expenses.

The SSG 500 Series are ideally suited for regional/branch offices, medium businesses and service providers that want a security platform to protect their WAN and high speed internal networks while extending the platform return on investment through high levels of system and interface modularity.

DefenderMX from Fort Systems

DefenderMX is an e-mail firewall product, works at the Gateway level, ensuring that only legitimate and virus free emails reach your mail server. DefenderMX is the commercial version MailScanner, with much more advanced features and administrate via feature-rich browser based control panel. It can easily integrate with any mail server and network and even can work in clusters.

DefenderMX captures Viruses, Trojans, possible malicious code and Spam as soon as it enters your network, before it gets to your servers and users. Having multiple layers of Security is the best way to protect your network. It automatically detects and removes phishing emails, preventing your users from accidentally give out confidential or private information.

