



Vishak Raman of Fortinet India

Cyberoam | Digvijay Singh

Shubhomoy Biswas of SonicWALL

Mohammed Hayath of Cisco Systems

Prasad Babu of Juniper Networks

Ajay Pillai of WatchGuard

Rakesh Singh of ZyXEL

Unified Threat Management (UTM) captivates the Indian security market

Call it a 'scientific conceit' or a 'sincere' security appliance: UTM (The Unified Threat Management) has come to stay. Almost all the players in the security space are offering UTM solutions tagged with various performance and capacities. Firms like Fortinet, Cisco Systems, Juniper Networks, WatchGuard Technologies, Cyberoam (Elitecore Technologies), SonicWALL, and ZyXEL have come out with broad security solutions. The Indian market for UTM is truly hot.

As a market intelligence and consulting organization, IDC (International Data Corporation) felt the need for the global IT industry to create a kind of 'security confederacy' consisting of key technologies for combating the growing, and increasingly targeted blended threats gripping the cyber landscape. With further insights and intensive consultations with major security and networking firms, the whole concept of Unified Threat Management (UTM) became a reality. "Industry analysts note that the rapid rise in 'blended threats' and internet viruses that attack at the application layer, have greatly contributed to a need for the flexible, highly integrated functionality that UTM delivers," says Shubhomoy Biswas, Country Manager, SonicWALL India.

"IDC has played a critical role by coining the concept of 'Unified Threat Management' (UTM)

appliances, as well as through its wide-spread publicity. In doing so, it has brought the UTM concept into the frontline. Enterprises are more familiar with the term 'integrated security appliances' which is an extension of the terminology they currently use and find it easier to relate to rather than the phrase UTM," says Digvijay Singh Chudasama, VP-Sales, Cyberoam India (The UTM division of Ahmedabad based Elitecore Technologies Ltd).

In its original definition by IDC, a typical UTM (Unified Threat Management) includes Gateway AV (Anti Virus); Firewall; IPS (The Intrusion Prevention System); and VPN (The Virtual Private Network). "The development of UTM is a major firewall inflection trend based on the need for stronger perimeter security solutions because attacks have become much more sophisticated. Application-level defenses, and the ability to prevent

known and unknown attacks for a unified threat management approach, become more critical daily," says Prasad Babu, Director Systems Engineering and Operations, Juniper Networks India Pvt Ltd.

However, the definition of classical UTM is rapidly changing from the 'four features' set defined by IDC. This would change with additional features set like 'Content Filtering; Multi-ISP Load Sharing; Anti-Spam; Traffic Management; VLAN Support; and SSL VPN. According to IDC,

the UTM segment is the 'fastest-growing' in the security appliance market globally.

IDC believes that by 2008, UTM security systems will be the biggest chunk of the \$3.45 billion combined firewall/VPN and UTM market-outpacing traditional standalone firewall/VPNs with a 58 per cent share. Moreover, India continues to be a dominant player in the APAC market registering the highest growth rates (CAGR-24 per cent). "We see India as an emerging market (\$44 million security appliance market in the year 2005) with huge infrastructure being spent on green field projects along with the huge tier 2 & tier 3 cities awaiting to take off along with the broad band internet-boom. They (UTM's) appeal the most to the green field markets, as they're the best first line of defense. This is very different from Europe & US market where infrastructure is already built with more layered approach being carried out for specific security functions," says Vishak Raman, Country Manager, Fortinet, India.

Vendors' prerogative

The security community as a whole appreciates the leading efforts of IDC towards setting a kind of 'institutionalized recognition' for UTM. Security and networking firms did come out with incipient UTM's based on the chaste definition postulated by IDC.

But as usual, the concerned vendors have tried to redefine the classical UTM's into more innovative security appliances. Thereby, individual firms infuse more innovations into their respective UTM offerings.

"To provide protection against 'inbound' and 'outbound attacks' at all levels, Juniper Networks integrates a complete set of best in-class content security features, (the UTM features) into their line of branch office firewall platforms. By leveraging the development, support and market expertise of many of the leading content security partners, Juniper Networks is able to deliver a set of best-in-class UTM features," says Prasad Babu, Juniper Networks India.

The networking and security major Cisco Systems has developed a comprehensive grammar

around UTM's. "Cisco adopts a Self Defending Network (SDN) approach to security that helps customers manage and mitigate risks more effectively. As part of the SDN Framework, Cisco offers Adaptive Threat Defense (ATD) solution that helps to further minimize network security risks by dynamically addressing threats at multiple layers, enabling tighter control of network traffic, endpoints, users, and applications. The Adaptive Threat Defense (ATD) also simplifies architectural designs and lowers operational costs. This innovative approach combines security features; multi-layer intelligence; application protection; network-wide control; and threat containment within high-performance solutions," says Mohammed Hayath, National Business Development Manager, India, (Network Security), Cisco Systems India Pvt Ltd.

However, behind all the innovative measures, a great focus is shed on enhancing the performance of UTM's making them further viable. For this all the security vendors invest heavily in designing faster 'ASIC accelerators' so that the performance of UTM's, placed on the networks, doesn't slowdown. The issue of managing the UTM assets deployed on the networks is again a challenging one. "As a market trend is moving towards the unified security devices, we, as an industry, needs to be much agile on 'reporting' and 'remotely managing' UTM devices interwoven into hybrid networking models," says Rakesh Singh, National Sales Manager, ZyXEL India Ltd.

UTM offerings

Among most active UTM players, Fortinet offers a comprehensive set of products for small, medium, and enterprise level of customers. "In a shorter period of time, we've established Fortinet as a highly specialized UTM company providing a wide range of products for the entire 'business continuum'," says Vishak Raman of Fortinet.

In the product categories of Fortinet includes FortiGate; FortiManager; FortiAnalyzer; FortiReporter; FortiMail; and FortiClient. Fortinet's FortiManager product is a centralized management system that provides coordinated policy-based provisioning, device configuration and update management, as well as, end-to-end network monitoring and device control for FortiGate systems. While FortiAnalyzer family of real-time network logging, analyzing, and

reporting systems are a series of dedicated network hardware appliances that securely aggregate log data from Fortinet devices and third party devices. FortiReporter is a Security Information Event Lifecycle Management (SIEM) and Compliance Audit Lifecycle Management (CALM) solution that provides essential real-time security intelligence to help decipher hacker/virus behavior, combat security threats, and meet compliance requirements. On the other hand, FortiMail is a specialized email security system that provides multi-layered protection against blended threats comprised of spam, viruses, worms and spyware. The company has security solutions for

anti-spam, intrusion detection and prevention, content filtering, bandwidth management and multiple link management," says Chudasama of Cyberoam.

At the same time, Cisco Adaptive Security Appliance (ASA) 5500 Series, is an innovative family of multi-function security appliances that help stop attacks before they spread through the network. "The Cisco ASA 5500 Series Adaptive Security Appliance is a modular platform that provides the next generation of security and VPN services. The Enterprise

UTM's are being delivered via security blades which delivers 10 Gigabit switching UTM performance using Advanced Telecom Computing Architecture (ATCA) on a chassis architecture is currently being adopted by enterprise customers, service providers, Carriers, Manage security service providers to offer security services "IN THE CLOUD" services.

Patrice Perche, Regional Vice President, Fortinet



the mobile devices as well (as these products are increasingly being used getting access to enterprise networks). FortiClient, with its products 'FortiClient PC', and 'FortiClient Mobile' provide unified security features for personal computers and smartphones including Personal Firewall, IPSec VPN, antivirus, anti-spyware, antispyware and web content filtering.

Ahmedabad based Elitecore Technologies with its 'Cyberoam' brand of UTM product lines, is one of the fastest growing companies in India as well. Cyberoam range of Identity-based UTM appliances come in various sizes, ranging from CR50i, CR100i, CR250i, CR500i, CR1000i to CR1500i, serving the threat management requirements of enterprises with up to 50 to over 1500 users. "Cyberoam appliances offer the entire range of security features - identity-based firewall, VPN, anti-virus,

Editions include four location-specific options: Firewall Edition, IPS Edition, Anti-X Edition, VPN Edition," says Hayath of Cisco Systems. A key component of the Adaptive Threat Defense phase of the Cisco Self-Defending Network (SDN) security strategy, the Cisco ASA 5500 Series includes the Cisco ASA 5505, Cisco ASA 5510, Cisco ASA 5520, Cisco ASA 5540 and the ASA 5550 products. This appliance family is designed to span from small and medium sized businesses to large enterprises and Service Providers.

The Juniper Networks Secure Services Gateway 5 (SSG 5) and Secure Services

Though UTM poses a growing threat to point products, it'll not completely eat into this segment. Both UTM and Point products will coexist. They'll together give customers a robust first line of defense