

One Box Big Bite

Integrated devices ease security management and reduce network complexity
BY JEEVAN M. THANKAPPAN

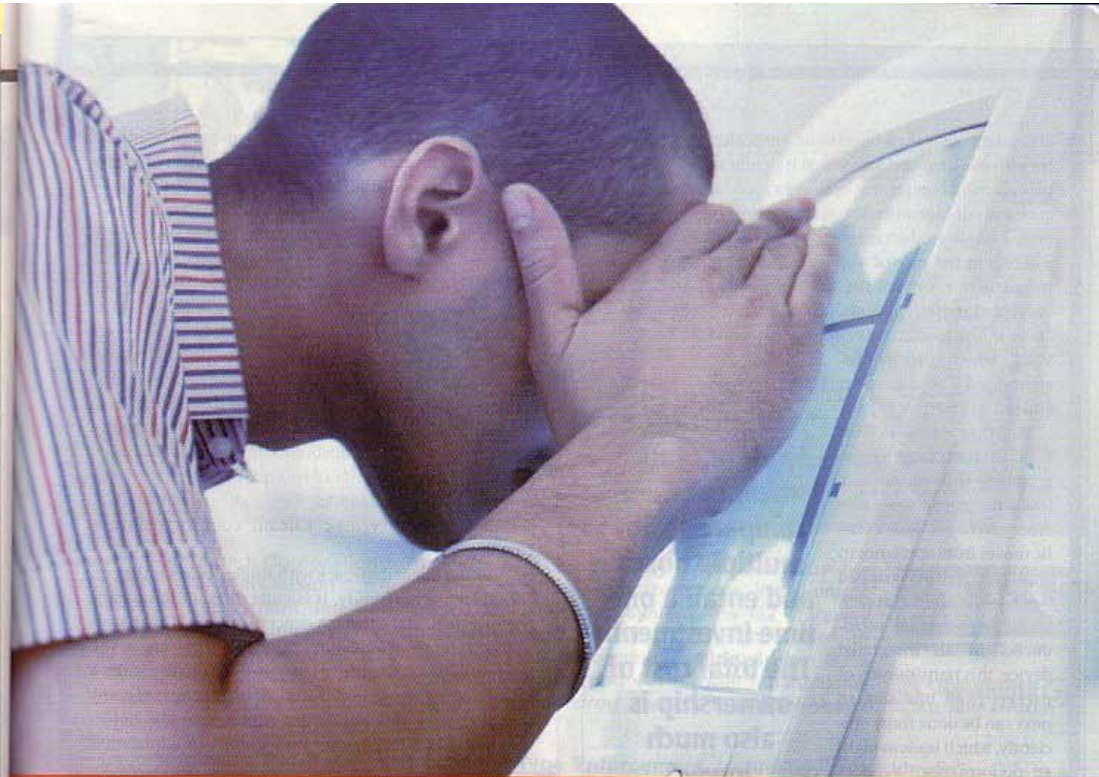
It is being touted as manna from heaven for IT managers grappling with a wide variety of complex, sophisticated threats that loom over today's business networks. It promises to drastically ease security management and network complexity. We are talking about integrated security appliances that combine a myriad of security functions into a single box.

Traditionally, organizations have tried to implement security systems by mixing disparate point solutions from various vendors. These products must all be purchased, installed, managed, and updated separately. This approach often results in difficulties with interoperability, incomplete protection, and lost time in testing and verifying patches across multiples technologies. This can slow a network's response to attacks. Also, the costs involved in implementing enough of these products to provide com-

prehensive protection can become prohibitive for most enterprises.

A number of vendors, including the big boys, are rushing to the market to help administrators overcome these problems with Swiss Army Knife-like appliances. And there are many factors driving this. Says Ajit Pillai, country manager, Watchguard, "Customers are fed up with multiple vendors and piecemeal solutions. Most enterprises don't have dedicated security administrators and the resources to manage multiple boxes." A point validated by Joy Ghosh, director-enterprise sales, Asia, Symantec: "Managing security is as big a pain as security itself. When security devices work in isolation, it results in huge gaps that attackers can take advantage of."

Ease of management is probably the number one factor in favour of such appliances. According to Rakesh Singh,



Does your firewall see it?

Ours does.

Conventional firewalls are blind to the most potentially damaging threats from the internet. Now, Fortinet can help you see - and stop - what the others miss. Our award-winning FortiGate™ Antivirus Firewalls - the First 'Quadruple-Certified' security system by ICSA Labs for Antivirus, Firewall, VPN and Intrusion Detection. Fortigate uses ASIC - powered content processing technology to scan your web, email and other network applications in real time.

The global FortiProtect™ Network and our Threat Response Team keeps FortiGate systems updated automatically against new threats, 24x7x365. So you can stop viruses, worms, trojans, intrusions and harmful content before they can enter your network - and lower your total cost in the process.

- FIREWALL • VPN • ANTIVIRUS • INTRUSION DETECTION • INTRUSION PREVENTION • ANTI SPAM • CONTENT FILTERING • TRAFFIC SHAPING



40, Ulsoor Road, New Bridge Center, Bangalore - 560 042.
Tel: 80-25325800.
Fax: 80-25325900.
Email: vraman@fortinet.com
www.fortinet.com



Bangalore: Mr. Deenu Mathew, Tel: 3865 0120. Email: deenu.mathew@techpacindia.com
Chennai: Mr. Venkateshwara Rao, Tel: 38650113. Email: venkateshwara.rao@techpacindia.com
Delhi: Mr. Tarun Khurana, Tel: 38050128. Email: tarun.khurana@techpacindia.com
Mumbai: Mr. Abbas Noorani, Tel: 9821699786. Email: abbas.noorani@techpacindia.com

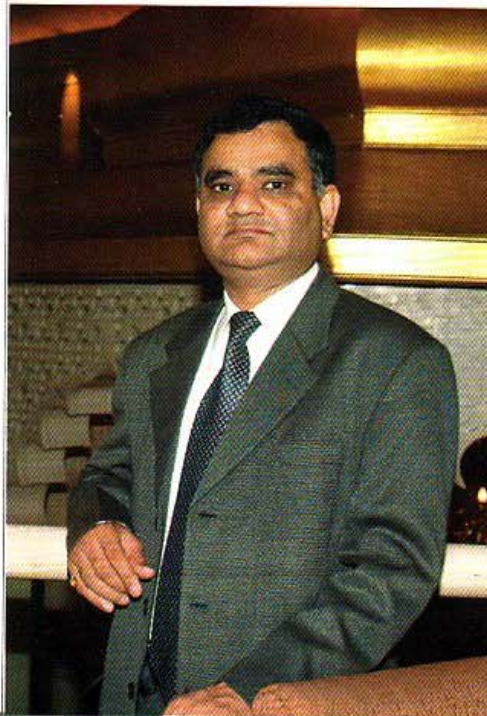
Authorised Distributor
Tech Pacific
Leaders in Technology Distribution

general manager, Asia operations, NetScaler, the inherent benefits of a single device are that it significantly simplifies management complexity, optimizes application performance and cuts operational costs to a great extent. "In addition, a single product is able to ensure complete security, whereas in the case of a series of point products, other infrastructure capabilities are nullified in the face of encrypted traffic," he adds. Moreover, most of the appliances in the market today come with management consoles, which provide for centralized management and policy creation.

Another reason for which Indian customers are gradually shifting towards integrated appliances is efficiency. When network traffic moves from appliance to appliance, getting stripped down and examined at each stage, latencies are introduced. In an integrated device, this transitioning of packets from one step to next can be done more efficiently, which leads to higher performance. Vendors point out that cost is also contributing to the exponential growth in this market, despite high import duties on hardware. The Indian market is currently fragmented, with traditional software-based point products such as firewall, VPN, IDS and anti virus, all of which come with separate licences for individual applications, or user-based licensing for each component. Needless to say, a single device can save users some serious money on the licensing front as well. Says P K Jain, managing director, Lanner Electronics, "Integrated appliances work out much cheaper when compared with multiple boxes and entail a one time investment. The total cost of ownership is also much lower."

"Integrated appliances work out much cheaper when compared with multiple boxes and entail a one time investment. The total cost of ownership is also much lower."

P K JAIN
MANAGING DIRECTOR,
LANNER ELECTRONICS



Plug and play

"Deploying integrated appliances eliminates the hassle of network design and implementation of appliances or modules from various vendors with different capabilities," says Gurdip Sethi, managing director, NetContinuum India. This is because most of the appliances are plug-and-play devices that do away with complex system configuration. Multi-dimensionality also figures in the list of benefits. Security has multiple dimensions, and is affected at all layers. Therefore, to do provide comprehensive pro-

tection, a security solution needs to operate at all those layers. It is a lot easier to address multiple layers of security in an integrated appliance, as opposed to splitting the task up into multiple appliances or software modules.

While there are benefits galore, there are also some serious shortcomings to multifunctional devices. Though an integrated appliance might drastically ease security management and reduce network complexity, it also poses the risk of a single point of failure in the network. As more functionality is added to a single device, there is an increased worry that if that device fails, the network will be left vulnerable. Vendors refute this aspect. "This is a wrong notion. If a customer's network is mission critical, he can always opt for a high-availability configuration, in which appliances can be placed in a redundant fashion, so that if one device fails, the secondary device takes over operations seamlessly," says Vishak Raman, country manager, Fortinet.

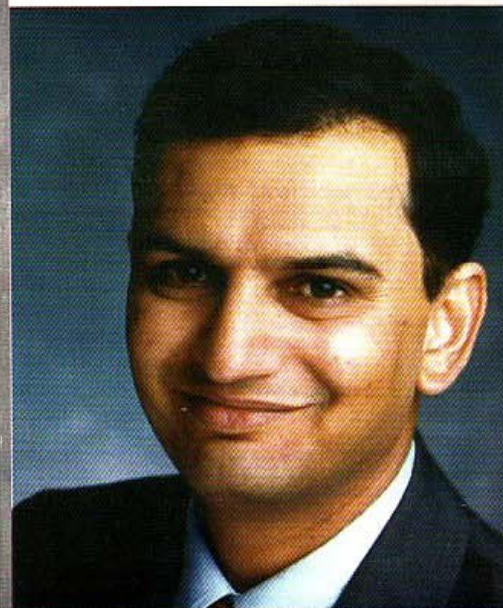
Another major drawback with single devices is the perceived lack of scalability. It is quite difficult to upgrade these devices, and there is a concern among IT managers that costs for these appliances can escalate quickly, as you layer on additional security services. Performance is also a major worry. The biggest hit on performance rates of many so-called integrated appliances comes from the implementation of "deep packet inspection", or application

"Customers are fed up with multiple vendors and piecemeal solutions. Most enterprises don't have dedicated security administrators and the resources to manage multiple boxes."


AJIT PILLAI
COUNTRY MANAGER, WATCHGUARD

layer (content) filtering, which requires significantly more processing power than packet-level (header) filtering.

Kartik Shahani, sales director-India, Network Associates offers an analogy: "It is like the copier-scanner-printer product that hit the market sometime back. It never worked out because these are purpose-built devices for specific applications. It is the same with security. When you roll all modules into one single box, it will adversely impact performance." But appliance vendors beg to differ, and argue that these devices do provide the performance, reliability and manageability levels required by enterprise customers. Says Sethi, "It is true that some security solution vendors offered hardware products with simple architecture, minimal features, and off-the-shelf hardware components, to address the needs of a cost-conscious market. There is no inherent roadblock for an appliance not to be able to deliver the performance or features required by large scale enterprises." He reckons that an appliance with



its own specifically designed hardware, like an ASIC, can deliver better performance than software solutions on general-purpose machines.

Whatever the debate, it is true that integrated appliances have already found acceptance in the cost conscious SME market. This is partly because of the fact that a small-to-medium enterprise is vulnerable to the same kind of security threats as large enterprises, but typically doesn't have the same budget or expertise in preparing defenses. Also, SMEs rarely have the IT infrastructure to maintain and manage a disparate mix of products, each with their own management stations. Now, the question is: will large-scale enterprises turn to integrated devices? Though there are devices available in the market which can cater to 1500-2000 users, it seems that large organizations are not biting the bait yet. 

Send your comments on this article to

Jeevan M Thankappan at jeevan_mt@jasubhai.com

"A single product is able to ensure complete security, whereas in the case of a series of point products, other infrastructure capabilities are nullified in the face of encrypted traffic"

RAKESH SINGH
GENERAL MANAGER, ASIA OPERATIONS,
NETSCALER