

The year 2004 saw the debut of Intrusion Prevention Systems (IPS) that aim at taking a proactive approach to network security by attacking the root cause of the problem rather than detecting a problem and then fixing it

THE NEED FOR INTEGRATION

Integrated security appliances are more than just the sum of their parts. Enterprises today are adopting proactive, integrated models that provide:

- Early warning against emerging attacks. A cyber alert system should provide actionable information on how to protect the environment against an impending attack. This information must be customized so that it is relevant to the environment and prioritized so it can be acted upon immediately.
- Protection of key assets. Although no single technology can adequately protect against today's complex threats, an integrated approach to security can help eliminate the challenges of point products and deliver a more comprehensive solution. Such an approach focuses less on the individual protection technologies and more on the tiers of the systems architecture. This means the focus shifts to the gateway, application server, and client levels versus picking a firewall or an intrusion sensor. Doing so creates "defense-in-depth."
- Management: The ability to test, monitor, and measure. This means quickly correlating information, simplifying it, and prioritizing any necessary action. Management can become particularly challenging in environments hosting disparate products from multiple vendors, where each device generates its own overflow of data. Security processes must measure metrics such as Mean Time Between Failure (MTBF), Mean Time To Repair (MTTR), and Time To Respond (TTR).
- Response when the inevitable attack occurs. Organizations must be prepared to respond when an attack penetrates their defenses. An effective response plan starts with intelligence about the attack as well as countermeasures to address it and details on how to clean up any damage. Also essential is 24x7 support on mission-critical security products, which includes automatic updates to firewall rules, virus definitions, and intrusion signatures.

add-on component. The salient feature of such signature-based Intrusion Prevention is in-line protection from attacks that comply with protocol standards but carry malicious content.

To shift or not to shift

So are we seeing a radical shift in consumer preferences from traditional multi-point applications to integrated suites? "The scenario is different for large enterprises and medium scale ones", says Pillai as he further sketches out the trends, "many of the large enterprises which have very

complex networks show a resistance to change".

"However, the medium and small enterprise sector is very receptive to the idea of installing integrated suites. There is a lot of demand there," says Pillai.

Vishak Raman, Country Manager, Fortinet, also testifies to this: "Where traditional security solutions already exist, large enterprises are seeking to adopt a layered approach wherein they are deploying specialized products to address their specialized needs." **NC**

aditya_kelekar@jasubhai.com

Ideal for
Medium
to Large
Enterprise
Deployments

Juniper
NETWORKS

Juniper Networks NetScreen-SA 6000

Remote access that's
strong, secure and scalable.

To find out more, call 91-22-3068-0011.

Juniper
NETWORKS

ager – Enterprise Security, Symantec India corroborates this point, “When an outbreak occurs, the ‘fixes’ that each vendor provides must be tested and verified across the various technologies. This can slow response to attacks, potentially augmenting the costs that are incurred. And, since they were not designed to work together, independent point products can also degrade network performance.”

As such, the implications of traditional security solutions (multiple point solutions) vis-à-vis integrated suites include inefficiencies, inadequate protection against blended threats, and a higher cost of ownership. Deshmukh

“The log traffic that is generated is co-related and analyzed automatically by the integrated packages to identify whether the alarm has to be sounded. It would be a nightmare to physically find out,” says Deshmukh.

In addition, integrated applications also address the issues of integration and scalability. Integration is particularly of concern when the products that go into the integrated package are not all from the same brand. For instance, Cisco—which has an alliance with Trend Micro for the antivirus component of its security packages—claims that the different components integrate very well. Also, as enterprises grow, they inevitably feel the need to



“Where traditional security solutions already exist, large enterprises are seeking to adopt a layered approach wherein they are deploying specialized products to address their specialized needs”

VISHAK RAMAN, Country Manager - Fortinet

mukh sums it up, “It all adds up to an under-performing security posture that is difficult to understand and provides little insight into enterprise security planning. Reliance on information security point products and informal processes leaves too many security holes open.”

More than the sum of its parts

But integrated appliances are not simply individual appliances put together; the current breed also includes several other features that help ensure that system performance and security are not compromised—these include features that cover all the four security quadrants of alerting, protection, management, and response (see box). The management aspect of the package is probably what lends to the package its special sheen.

upgrade their security solutions—this may be in the form of enhanced spam protection, more network ports or some other aspect of security. The integrated applications generally are easily upgradable to add new features. As Ajit Pillai, Country Manager – Watchguard, puts it, “the beauty of the packages lies in the fact that they can be upgraded by just tapping in software keys.”

The Intrusion Prevention Component

The year 2004 saw the debut of Intrusion Prevention Systems (IPS) that aim at taking a proactive approach to network security by attacking the root cause of the problem rather than detecting a problem and then fixing it. Today, most integrated packages have Intrusion Prevention bundled along with it, either as an essential feature or as an



Ideal for
**Securing
VoIP**

Juniper Networks NetScreen-ISG 2000

**Secure VoIP? Nothing beats
the new Juniper Networks
NetScreen-ISG 2000.**

To find out more, call 91-22-3068-0011.



Integration is the key

The day seems to have finally dawned for integrated security appliances, which today are seen to be the most favored protection solution on the Information Security scene. **BY ADITYA KELEKAR**

Integrated security appliances include firewalls, VPN, intelligent layered security, gateway antivirus, intrusion prevention, spam blocking, and Web content filtering. But what is driving the need for bundling all these solutions into one packet?

Better protection, lower cost, wider reach

Primarily, the need for integrated packages, (the development of unified threat management) has arisen due to several challenges that one faces while implementing enterprise security solutions. Security solutions typically consist of multiple point products, each working inde-

pendently. Because they are not integrated, multiple point products are difficult to manage, which increases IT administration and support costs. Protection is usually not comprehensive. Next, integrated security appliances make it possible to provide proactive, multilayered threat and intrusion protection for every point on the network. This addresses one of the biggest issues IT teams deal with: keeping their organizations secure over time, especially in the face of continually evolving threats and changing security requirements. Unmesh Deshmukh, Country Sales Manager, Symantec India



"Reliance on information security point products and informal processes leaves too many security holes open"

UNMESH DESHMUKH, Country Sales Manager - Enterprise Security, Symantec India

pendently. Because they are not integrated, multiple point products are difficult to manage, which increases IT administration and support costs. Protection is usually not comprehensive.

On the cost front, integrated security appliances offer

tection for every point on the network. This addresses one of the biggest issues IT teams deal with: keeping their organizations secure over time, especially in the face of continually evolving threats and changing security requirements. Unmesh Deshmukh, Country Sales Manager, Symantec India

Ideal for Large Enterprise Deployments

Juniper Networks NetScreen-IDP 1100

Stop network threats in their tracks.

To find out more, call 91-22-3068-0011.