PUBLISHED SINCE 1997
siliconindia
BUSINESS & TECHNOLOGY IN THE U.S. & INDIA APRIL 2008 SILICONINDIA.COM

The Hybrid Approach to Security

BY Jayakishore Bayadi

CEO Dr. Parag Pruthi and his team of engineers at NIKSUN are keenly watching the shift in the enterprise world from 1 GB Ethernet to 10 GB Ethernet. Though the transformation to the new paradigm has been relatively slow, they are confident that the pace will catch up in a year or two.

In the 10 GB Ethernet world there will be multitude of services and application available to users. At the same time the rate of information flow will be much higher. Dr. Pruthi firmly believes that software-based network security solutions that are designed for today's networks will not be able to scale up and address the challenges of a 10 GB Ethernet world. "Software-based solutions will not be able to cope up with the high volume and large variety of information flowing on the network," he argues.

Despite the fact that organizations have deployed devices such as firewalls and intrusion detection systems (IDSs) to secure their networks, they continue to experience security violations and network attacks. Chief Security Officers have started to believe that there is no such thing as 100 percent security. Firewalls can be bypassed or tunneled through. Authentication can be foiled, guessed, or attacked. IDS systems can be evaded. Signatures and anti-virus systems can only flag known attacks. IPS systems can be compromised or made to cause denial-of-service (DoS) situations themselves. Due to the complexity of network attacks and the extent of the damage they cause, organizations are spending considerably more time and resources recovering from security incidents than in the past.

Network security is typically performed by detection mechanisms that identify anomalies or potentially harmful data. In particular, the IDS scans for known attack patterns and generates alarms when those patterns are detected in the network traffic or in host logs. Essentially this is based on signatures or trying to match patterns of packets or strings that flow in

Dr. Parag Pruthi

a network. However, scanning the network traffic in a 10 GB Ethernet world is not that simple using this approach.

"IDSs are not the network security panacea they were originally thought to be, but rather are prone to suffering from a host of shortcomings," says Pruthi. Chief among these shortcomings is the proliferation of false positives, the cases where the IDS raises an alarm when no real breach has occurred thereby greatly reducing the effectiveness, usability, and manageability of such systems. Indeed, industry estimates generally place the average occurrence of false positives above 90 percent. The increasing need to monitor faster and faster networks threatens to make matters worse.

> "IDSs are not the network security panacea they were originally thought to be, but rather are prone to suffering from a host of shortcomings"

Another trend that one has to be aware of is that the nature of information embedded in data streams is getting quite complicated. The types of things that your data is protected against are deep inside packets and message elements that are encoded. They are not simply detectable based on just pattern recognition.

It's a no brainer that the detection provided by IDSs, although crucial, is only one part of the process. Policies, procedures, personnel, and products must be in place for managing incidents beyond the detection phase. Ideally, a quick decision needs to be made on the legitimacy, severity, and on-going risk posed by an event. From here, an appropriate response can be enacted. How quickly such a decision and response can be made ultimately depends on the skill of the team and the power of their tools.

We have to do online real-time decoding at the application layer, go deep into application semantics and decode deep within to understand what actually is being transferred and determine who is authorized to transfer certain data," explains Pruthi. "And that's not easy." Software-based solutions that must go very deep into the reconstruction of application protocols and across a number of different flows simply fail at very high rates of network traffic.

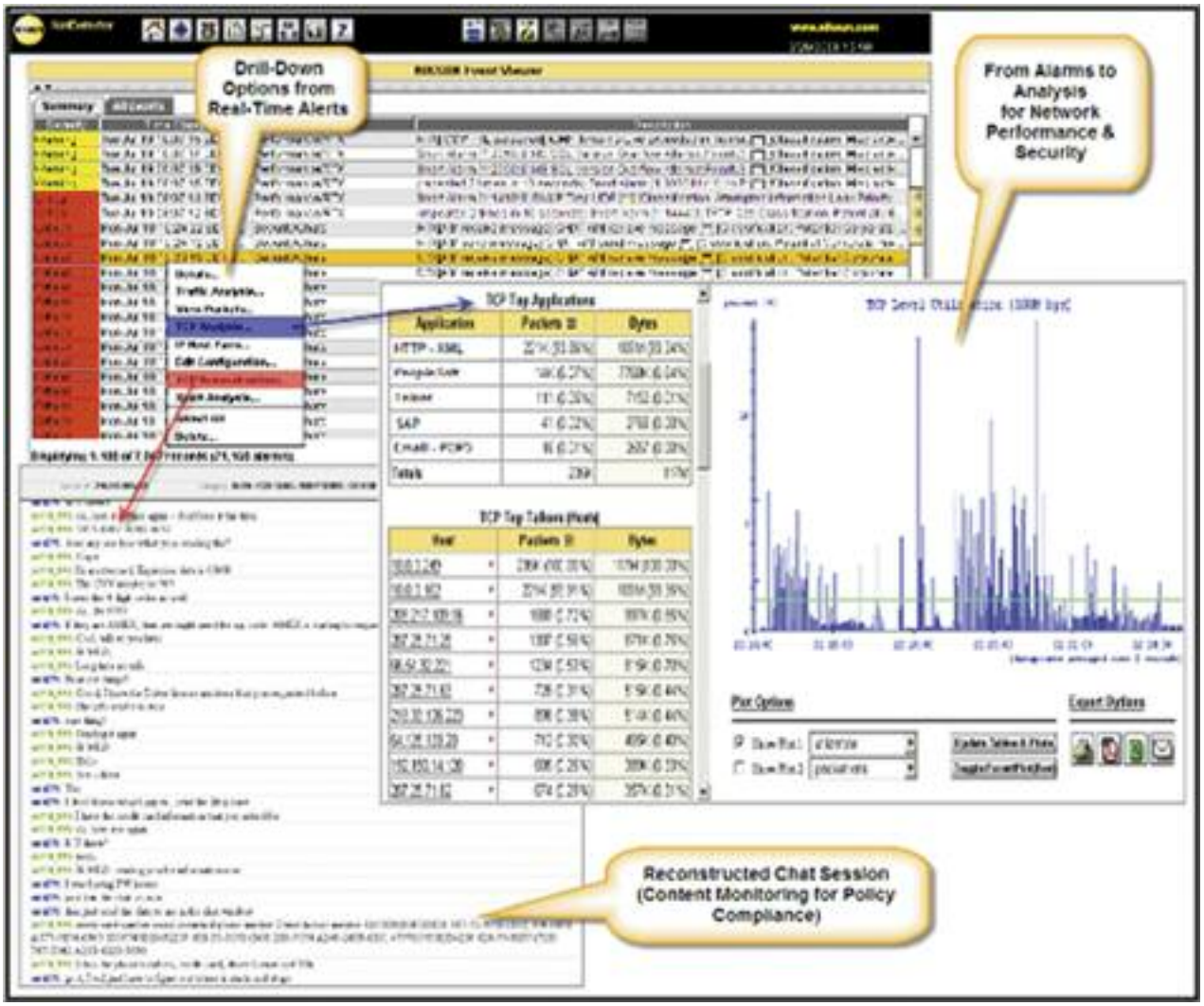
This is where New Jersey-based NIKSUN comes to play. Its robust security solutions, spearheaded by the flagship NetDetector suite, provide the additional necessary depth to fill these gaps. So whether an attack is an

NetDetector is a full-featured appliance for network security surveillance, detection, analytics, and forensics. It complements an organization's existing network security infrastructure, including firewalls/IPS, IDS, and switches/routers, to help provide defense at unprecedented depths. "When appliances are distributed throughout the enterprise and then centrally managed along with aggregated reporting and analysis, a new unprecedented level of security monitoring unfolds," states Pruthi.

NetDetectorLive builds on the award winning foundation of NIKSUN's patented real-time analytics engine by continuously capturing and warehousing network traffic, and alerting on specific signatures and traffic patterns enabling fast and accurate monitoring of content. Built-in modules provide complementary signature and statistical anomaly detection, thus locating the "needles" of actionable information in the "haystack" of raw data. NetDetectorLive allows users to not only rewind to and playback violations but also search all data flowing on a network for forensic reconstruction of surreptitious activity.

NetDetectorLive monitors network communication channels such as email, web-mail, instant messaging, chat, ftp, and others, for document and content leaks. In addition to custom alert and scanning capability, NetDetectorLive provides users with templates of regulatory and corporate policy profiles making it immediately useful right out of the box. All this and more is rounded out by a highly intuitive web-based GUI.

NetDetectorLive stores all captured network and application data in an internal repository. This stored data is then used to recreate documents and incident contexts, used to perform audits, security and compliance forensics, or troubleshoot problems.



> "We need a hardware-software expertise and a systems-based approach to solve many of the network monitoring, security, surveillance and forensics needs of tomorrow"

external break-in, an internal theft and disclosure of sensitive data, or the latest worm, the continuous surveillance and powerful analysis of NIKSUN's solutions ensure that the incident can be captured, traced, and remediated.

NIKSUN does this is by way of hybrid approach. Since there are new applications being deployed on the network and the nature of the applications change frequently, we need a hardware-software expertise and a systems-based approach to solve many of the network monitoring, security, surveillance and forensics needs of tomorrow," says Pruthi.

NetDetector is a combination of hardware and software that work together to combat threats. It provides the users a capability to customize the hardware. One can load different patterns, different actions, program the algorithm for a new environment, and write new exceptions and rules. The hardware is flexible enough to run the software at a very high rate. "This is indeed a cost effective solution and can be deployed at different locations within the network," notes Pruthi.

With over 600 customers having signed up since the company's start in 1997, NIKSUN is already seeing success. High level thinking coupled with its fundamental architecture and design is what makes NIKSUN's solution truly a revolutionary one in the industry. si

siliconindia

■ PUBLISHING ■ ONLINE MEDIA ■ EVENTS

U.S.: California
44790, S Grimmer Blvd, # 202 Fremont, CA - 94538
T: 510-440-8249 F: 510-440-8276

India
No. 124, 2nd floor, South Block, Surya Chambers
Airport Main Road, Murugeshpalya, Bangalore-560017.
T: + 91.80.41510601 F: + 91.80.41321359

Printed in the U.S.A

siliconindia, Inc

www.siliconindia.com