

With hackers moving faster than patching and other reactive security tools, Intrusion Prevention Systems is the next logical step. But why are so few organisations using it to defend their networks?

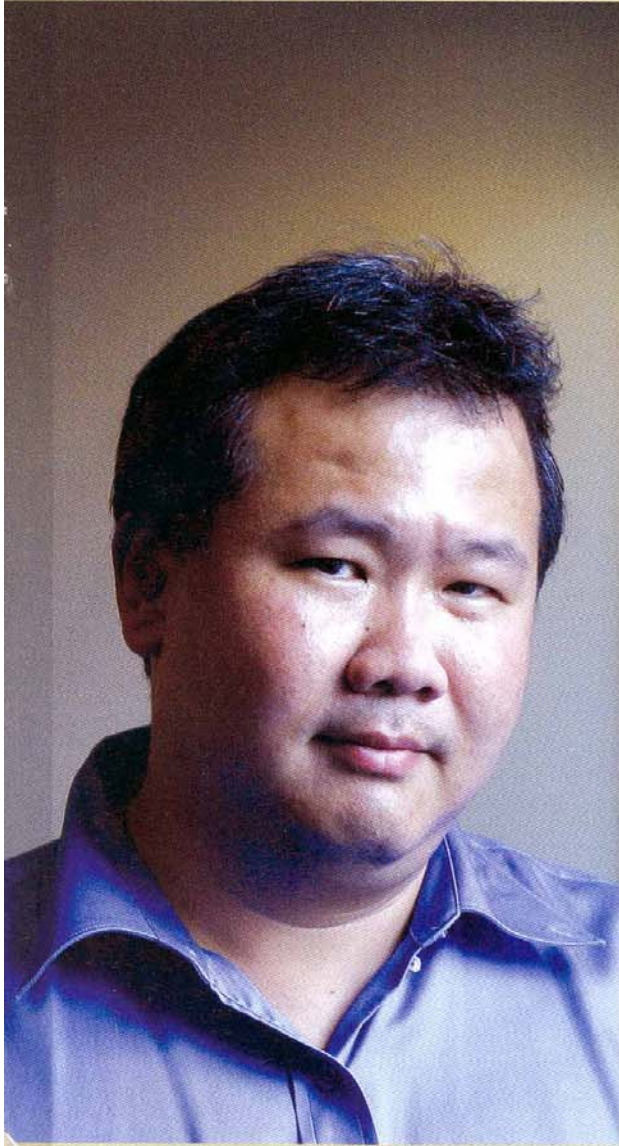
BY OO GIN LEE

# IPS: Only a good idea?

**Executive summary:** Intrusion Prevention Systems may be a relatively new technology, but the National University of Singapore (NUS) has implemented it. IPS goes one step further than IDS solutions by not only detecting attacks but also stopping them. However, NUS realised that it is challenging to make IPS user-friendly for the end-users, and it does not prevent an infected desktop from spreading the contagion within the network.

Intrusion prevention systems (IPS) may be a relatively new technology, but the National University of Singapore (NUS) has already implemented it campus-wide. Roland Yeo, the network manager for NUS says that the tertiary institution has deployed host-based IPS that protects against network-based attacks for all its users.

"This agent is loaded onto our desktops automatically whenever our users login to our network, and runs in the background to protect the desktop against any



PHOTOGRAPHY BY SAMUEL ISAAC CHUA

IPS is something the industry should have spent more time focusing on instead of IDS. It is certainly a **MORE EFFECTIVE** technology, and will ultimately **REPLACE IDS** altogether.

**Roland Yeo**  
Network Manager for National University of Singapore

but how does the end-user decide whether the application is malicious in the first place?" asks Yeo.

Another difficulty is the lack of tools which prevent a compromised desktop within the network from spreading the contagion internally, Yeo adds.

"It's not good enough for the IPS or security agent to just prevent network attacks from compromising a desktop. It's also important for the agent to prevent a desktop which has been compromised, or a rogue desktop, from sending out its malicious or anomalous traffic into the rest of the network," he says.

Besides, the IPS must work in a highly scalable manner, says Yeo. "Network and systems performance must be preserved. Otherwise the IPS itself becomes a conduit for denial of service," he says.

#### Security moves from passive to active

IPS is fast becoming a hot topic of discussion. According to a Gartner report in August 2002, IDS technology was built on the belief that security attacks could not be blocked, and could only be monitored, due to the number of security vulnerabilities and clever hackers targeting them.

But Gartner believes that "intrusion prevention relegates this theory to the same dustbin that contains client/servers, banner ads and pet rocks."

In April this year, Gartner issued a report that went one step further—it is ending its half-yearly Magic Quadrant reports on IDS, and will only rank vendors who have IPS solutions. Gartner added in that report: "IDS vendors that have not introduced blocking capabilities by the end of 2004 will not be viable providers beyond the end of 2005."

compromise," says Yeo.

However, he says it is difficult to make the IPS user friendly for the end-users, and at the same time be effective against network attacks.

"There are many tools today which will prompt the end-user to decide whether to allow certain actions, and often the end-user is left with the choice of clicking 'Yes' to give full-access to the application, or clicking 'No' to prevent the application from further action.

"The choice is obvious when it's a malicious application,

Wong Loke Yeow, security evangelist with TruSecure, says that "eventually IDS will adopt features of IPS".

In essence, all IPS products are IDS products, but not all IDS products are IPS. The difference is the response mechanism that changes the role of IDS from passive to active.

IDS monitors network traffic and alarms users to malicious activity. IPS takes IDS one step further by not only detecting the attacks, but actually stopping them.

The recent blended attacks from worms and viruses like Slammer, Blaster and Nachi illustrated the limitations of standalone IDS products.

"Organisations and vendors have come to realise the ineffectiveness of IDS and the real need for IPS. IPS is something that the industry should have spent more time focusing on instead of IDS. It is certainly a more effective technology, and will ultimately replace IDS altogether," says NUS's Yeo.

Ashley Wearne, area vice-president for Southeast Asia, India, Australia and New Zealand, McAfee, says that normal firewalls and IDS cannot block distributed denial of service (DDoS) attacks, which appear as "normal packets".

Besides, IT managers are months behind their patches because "you can't just take your networks down to patch them, you have to test if the patches work well with the rest of your system first," says Wearne.

The biggest problem is dealing with the unknown attacks. "The entire approach to security needs to be changed. It used to be [about] stopping the abnormalities, now it's about understanding what is normal, and stopping everything else," Wearne added.

Cisco Systems is another leading IPS solutions vendor in Gartner's Magic Quadrant.

In 2003, Cisco purchased Okena, a desktop and server intrusion prevention vendor. Okena's IPS product enabled the University of California

## Insights from IEA Award Winner

**B**AX Global is a logistics provider that has evaluated a host-based IPS solution, and decided against it. Ramon Baclay Jr, Regional IT director, Technology & Infrastructure, CTO Office, BAX Global, says that his company has put in place a good firewall and a very strong Internet policy, which has worked well for the company.

It also has an existing network IDS solution which helps it to monitor the intrusion attempts. Baclay says that the IDS solution complements its already-effective firewall and strict Internet policy implementations.

"There are 12 pages of configuration in our firewall and we are close to closing every single possible port number in our system," says Baclay.

"BAX Global's strategy has always been to deploy perimeter defence technology in-house rather than outsource. IDS has been in place for the last 3 years and has effectively mitigated our risk exposure. The cost of IPS would be a major factor in deploying this technology, considering the marginal benefit it would give in return (with IDS already working effectively)," says Baclay.

"In addition, we would have to re-look the entire set-up and applications group. The existing IDS solution may also have to be replaced."

He adds that his counterparts at the BAX Global HQ also found that the IPS they were evaluating turned up many false positives. And a lot of continuous fine-tuning needed to be done on the IPS.

On top of that, Baclay adds that the current IDS solution was affordable because it was bought at a small additional cost from Cisco Systems, since BAX Global is already using Cisco's routers and the IDS was an add-on function. A new IPS solution, on the other hand, would cost a lot more.

In light of these circumstances, his company decided against migrating to an IPS solution.

at Berkeley to emerge unscathed when it was attacked by the Slammer worm—even though it was running unpatched servers.

## Two IPS flavours

According to Damien Wong, vice-president and general manager, Meta Group Singapore, there are two different types of IPS—network-based and host-based.

For networked-based IPS there are two main flavours—packet-sniffing and protocol anomaly.

Packet sniffing looks at patterns in the network packet stream that match suspicious activity, forbidden actions or known attacks. Some also call this deep-packet scanning. Protocol anomaly looks for traffic that breaks standard protocol.

"The first is effective but requires a lot of processing power and is tedious to maintain. The second provides high performance but is only 80% effective," says Meta's Wong.

As for host-based IPS, the latest method is the operating shield

**Ramon Baclay Jr, Regional IT director, Technology & Infrastructure, CTO Office, BAX Global, says that IPS is not value for money, only has "marginal" benefits and leads to many false positives.**



method, which wraps itself around the core kernel of the OS and stops the OS from executing "things that are not normal." While this is effective, Wong warns that this method could interfere with the running of valid applications.

TruSecure's Wong cautions that current IPS technologies are still mainly signature-based.

Signature-based IPS is more accurate, he adds, but it does not protect against the unknown.

"There are some with deep packet scanning, but I haven't seen one that

works very well," he says.

Deep-packet scanning is generally effective but may lead to a lot of false negatives, says Matthew Young, vice-president of Fortinet Asia-Pacific. This is because deep packet scanning often fails to detect attacks that are sent across multiple packets.

Network Associates' Wearne acknowledges the limitations of deep packet scanning, which Network Associates uses, and says companies must combine a deep packet network IPS with a host-based IPS that can

offer a second layer of defense.

Alex Ho, regional product marketing manager, Asia Pacific and Greater China, Nokia Enterprise Solutions, cautions that IPS is more of a good idea than an actual mainstream technology at this point.

"The challenges include difficulty of deployment, amount of false positives, performance issue and the ability to fail-over. False positives are the primary reason why users are moving slowly to the intrusion prevention concept," he says.

### You need to layer security

While experts and vendors disagree on the effectiveness and viability of IPS, most agree that an in-depth approach to security is needed.


Kang Meng Chow, chief security and privacy adviser, Asia Pacific and Greater China, Microsoft, says while IPS is still evolving and is a useful addition to the security tools, layers of protection, and a security management infrastructure, including people and processes, must be in place.

"Without the support of a security management infrastructure, it would be rather futile to have an IPS," he says.

Meta's Wong agrees.

"End-user organisations interested in IPS/IDS should focus on process first, staffing and sourcing second and technology third."

Jukka Sieppi, director, product management, Stonesoft, says an organisation needs both width (different complementary technologies like firewall and IDS/IPS) as well as depth (segmentation of internal network with firewalls in addition to perimeter defense).

"If you lack depth in your defense, detection becomes very difficult. End-users who benefit most from IDS/IPS are the ones who know where in their network they have valuable assets and for which they are able to define what they want to use it for," he says. 

more on security:  
[www.intelligentasia.com/security](http://www.intelligentasia.com/security)