

What's inside ...

INTEGRATED SECURITY

A look at the future of network security.

STRONG ON THE INSIDE

According to the Gartner Group, more than half of enterprise security breaches are internal. A look at how you can build a network that is strong on the inside.

CASE STUDY

Pacific & Orient Insurance Co. Berhad

PARTNERSHIP

Network integrators are a crucial link between product vendors and end user organisations. Certification programs like Cisco's Certified Partner Program make it easy for end users to recognise expertise when they see it.



INTEGRATED SECURITY

A LOOK AT THE FUTURE OF NETWORK SECURITY.

THIS IS THE POWER OF THE NETWORK. **now.**



INTEGRATED SECURITY

A LOOK AT THE FUTURE OF NETWORK SECURITY.

What is wrong with most firewalls, network intrusion detection systems (NIDS), virtual private networks (VPNs) and the range of modern security measures today? Not much, except that they could be doing a great deal more than they do today—if only they could “talk” with one another.

In the last two decades, integration has been the natural progression of most computing models. But not so, it seems, when it comes to network security. Most firewalls today have no idea what their VPN brethren are doing at the other end of the network; nor can an NIDS tell a firewall in the same network to kick out a suspicious connection that the former has detected.

The good news is that this kind of co-operation between devices is emerging. With this, we see the spawning of a new network security paradigm—one where different security devices are integrated as a collective, and where security devices are distributed across the network to provide multi-layer defences.

INTEGRATE

So how does an integrated security model look like in practice? Imagine, for a start, an NIDS that can talk to a network switch or router to proactively tweak network access, like reconfiguring access control lists (ACL) or even terminating network connections, when it detects untoward traffic. Or picture an NIDS which can get a firewall to reset a suspicious TCP session to frustrate any hacker who might be probing the network in ways that don't constitute a full-blown attack.

Through collaboration between different security devices, an integrated security model creates synergies between various security components so that the sum of the defence system becomes greater than its parts. Another

benefit is that there is now a common way to manage security devices and administer security policies.

Integrated security also creates more transparency in the network, through the sharing of information between devices so that various security components are constantly abreast with the general traffic behaviour in the network.

Though it is still at an early stage, integrated security is no longer considered a novelty. With escalating threat levels, increased sophistication of hackers and the blurring of boundaries in corporate networks, this type of network protection has become a necessity. A recent Business Times article reported that Asia Pacific endured 76 million hacking incidents in the first six months this year. This nearly doubled the 43 million incidents in the year-ago period. Quite simply, if network threats continue to escalate at such an alarming rate, an integrated security model will be needed by organisations just to cope with the routine of screening network traffic.

EMPOWER

Besides cobbling together multitudes of security devices, another effective way to integrate security is to build different security functions into a single, “do-it-all” device. Today, network vendors like Cisco Systems are doing this with a modular approach. For instance, Cisco's access routers support VPN and NIDS plug-in modules in the same chassis, effectively making the router a security device.

This approach offers two key benefits: It creates a high level of cohesiveness among the different modules, since they share the same hardware platform; and it is also more cost-effective, due to the possibility of hardware reuse and ease of scalability.

With such multi-function security devices, a



whole gamut of network defence mechanisms can be activated at a single network node, thus strengthening that node and anything that is connected to it. This notion also begs the question: Why not build these features into a network switch or router?

This is a logical progression of network security, and it makes sense from several angles. Firstly, switches and routers are natural security hot spots, due to their strategic nature and location in a network. Not only are they natural aggregation points of network traffic, they are usually the first points of contact for data centres. Secondly, if a router combines security components like firewall, dynamic VPN and in-line NIDS, network traffic can now be inspected at the point of entry instead of waiting for it to cross network boundaries, as is the case with typical NIDS deployment today.

Thirdly, embedding security into switches enable hitherto impossible-to-achieve defence strategies which can incorporate network traffic considerations. Again, this is about creating synergies—and here, it is between the security and network components.

Take the example of securing of Web-based applications. These applications typically use Secure Sockets Layer (SSL) encryption to secure data transmission. The problem with SSL is that it is resource-intensive, typically demanding a high CPU utilisation on the server. Besides the server, the network is also taxed as it needs to inspect potentially harmful SSL payload.

Again, if we were to take a Cisco example, the Cisco CSS 11500 Content Services Switch or the Content Switching Module (CSM) for the Cisco Catalyst 6500 Series can be used, in this case, to alleviate these performance bottlenecks by off-loading SSL decryption. Decrypted traffic can then leverage on the NIDS to protect back-end servers. To mitigate network performance loss, Layer 4 to 7 load

balancing can be done through global server load balancing (GSLB) solutions like the Cisco GSS 4480.

PERVASIVE SECURITY

From a higher-up perspective, embedding security in network switches and integrating various security components will lead to a network where security is pervasive. This is where security becomes not only persistent, but also omnipresent.

With pervasive security, the entire network becomes much harder to crack, not because there are now no weak spots, but because different security components can rise up together to tackle a network threat, wherever it occurs. Such a network will also tackle threats faster, because of its heightened awareness to threats in general.

In addition, pervasive security is probably the only effective defence against internal threats, which according to the FBI, afflict nine out of 10 organisations it recently surveyed. These threats may be posed by either disgruntled or fired staff. However, it is the more prosaic but less visible internal threats that are likely to wreck havoc in a network. These are threats that arise when untrained staff fail to follow standard security protocols, like changing network access passwords regularly, or patching their antivirus application when prompted, or indiscriminately forwarding email attachments that they have received. There can be many other scenarios.

Internal threats cannot be tackled by a perimeter-only defence, which looks outwards instead of inwards. The answer is therefore a security regime that remains strong throughout the whole network.

And that, in essence, is the goal of having a network where firewalls can talk to a switch or router, which is also on good terms with that NIDS device two network nodes away.



SECURITY THREATS ON THE RISE

In a recent published report, security vendor e-Cop.net said that USA and Japan were top hacking sources in June, accounting for half of all originating IP addresses that spawned attacks and intrusion attempts. This was primarily due to a resurgence of web server probes and attacks from a variety of networks, said e-Cop.net.

Third is Korea, which is responsible for 16% of attacks. The Netherlands is fourth on this dubious honour roll with 9%. e-Cop.net also observed an increase in web server probes and attacks, which contributed to 51% of the total recorded activity types. Common targeted web servers were Apaches and Microsoft IIS. In addition, variants of new and old web exploits techniques were recorded on a daily basis.

E-Cop.net also issued high alerts of Microsoft machine probes and attacks involving the exploitation of Internet Explorer. Opportunistic random port scanning of HTTPS TCP 443, DNS TCP 53, SNMP UDP 162 and ever rising TCP Microsoft 445 server port probe plagued the month of June, reported e-Cop.net, contributing to a collective 11% of activity types recorded.

Ominously, the SQL Slammer worm continued its run for the sixth consecutive month, recording an overall 3% using automated script attacks targeting mainly on udp 1434 port. Bottomline? While the Slammer may seem like old news now, don't put it out of your radar just yet.

The need to have a network that is strong behind its perimeter defences has never been more apparent. One reason is the rise of internal network threats in enterprises. According to the Gartner Group, more than half of all enterprise security breaches today are spawned internally.

The other reasons are less specific, and has to do with the way networks have evolved

STRONG ON THE INSIDE

ACCORDING TO THE GARTNER GROUP, MORE THAN HALF OF ENTERPRISE SECURITY BREACHES ARE INTERNAL. A LOOK AT HOW YOU CAN BUILD A NETWORK THAT IS STRONG ON THE INSIDE.

today. Put simply, networks are getting more exposed—some by necessity—and threats have become more numerous and sophisticated. Equally alarming are readily-available hacking tools that can attack just about any device that resides in the network.

To be strong on the inside, three key areas are important. These are: A sophisticated identity mechanism; switch-based security; and end-point protection.

CREATING IDENTITY

Many organisations assume inherent trust if someone accesses the network from behind its firewalls. This is a dangerous assumption, because internal network access by outsiders are always likely to happen, unless an organisation totally refuses guests and visitors into their premises. Furthermore, as more companies embrace wireless networking, it has become easier—and stealthier—to sneak into corporate networks.

An unauthorised network guest could easily spoof the email account of a senior company staff and send out rogue email messages that create panic. Or, he could hack into sensitive databases to steal or destroy information. Or, he could use your company network as a springboard to launch a denial-of-service (DOS) attack on other networks.

To protect against these threats, enterprises can start by instilling a security regime that requires users to identify themselves regardless of where the user is sited. This security scheme must also be so transparent and easy-to-use that users will not be tempted to sidestep it.

This is what a switch-based authentication standard called the IEEE 802.1x is about. It enables what is known as “port-level authentication”, where any network port is equipped with the ability to act on an unsuccessful—or successful—user or device login. If the login is unsuccessful, network access will be denied by the switch-port. Another key benefit of 802.1x is that both user

and device identities must be concurrently ratified before user access is allowed. This makes the network much harder to crack.

SECURING THE SWITCH

Network switches are where most network traffic are aggregated. This makes them natural abode for security measures. Toughening up switches can also be vital in safeguarding data centres, which typically contain multiple servers connected to switches and routers, before they are exposed to the LAN and WAN.

The notion of a secured switch is still new today. Among major network vendors, Cisco is one that has built their switches with the ability to accept security modules, like VPN, NIDS and firewall devices. Besides fortifying the switches and resources connected to them, having an army of secured switches working in tandem creates a secured network fabric that can defend from deep within the network.

SECURING END-POINTS

Mobility is a wonderful productivity notion, but it is also one that presents a security headache. The problem is that laptops, PDAs and other end-point devices are used mostly in the field, where trust levels are uncertain. They also create security headaches when stolen or misplaced. What this means is that organisations should take enforcing security on end-point devices very seriously.

But how does one enforce such security measures in practice? The difficulties stem from the fact that it is not easy synchronising security policies in end-points that won't stay still, are geographically dispersed and aren't always connected.

This is where software security agents can help. These small and intelligent applets, like the Cisco Security Agent (CSA), can reside in end-point devices to update them whenever they are connected to the network. This makes enforcing and updating security in end-point devices a maintenance-free exercise.



SECURED SWITCHING: MORE IN SYNC

By integrating security with network services, there will no longer be a mismatch between network demands and security coverage. This makes network security scalable.



INSURING NETWORK ACCESS

AN INSURANCE PROVIDER USES VPN TO RECHARGE ITS BUSINESS OPERATIONS

By nature, the insurance industry has a higher requirement for network security than most, because it deals with sensitive client documents that include medical, personal and financial records.

But insurance companies also need to have an open network. Most insurance companies are reliant on a workforce that is highly mobile, one which needs to constantly access the office network to download—and upload—contracts, files, policies and other vital documents. Not surprisingly, this industry is one of the biggest consumers of virtual private network (VPN) solutions.

VPN makes it safe for the mobile worker to send and receive data over a public network. Using encryption to scramble data, VPN is also flexible since safe connections can be made from wherever there is a network port—as long as the VPN client sits in the connecting device.

So when Pacific & Orient Insurance Co. Berhad decided to revamp both its computing and networking infrastructures in 2002, choosing the right VPN solution was critical. Specifically, the leading motor insurer in Malaysia, needed to connect its seven branches nationwide—in Johor Bahru, Kuantan, Kuching, Penang, Ipoh, Malacca and Klang Valley—with its mobile workforce of about 1,000 agents.

THE CHALLENGE

The company previously used leased connections, in the form of 9.6Kbps analog leased lines, to link up branch offices and agents. While this offered robust security, it was also expensive. And with the company's mobile workforce growing rapidly, leased lines were proving too inflexible. For the company,

dial-up connections secured by VPN was the answer. But could a solution cater for the company's ambitious connectivity goals?

"We wanted a solution that can secure our entire IP infrastructure, which we use to perform customer information transactions. We also needed a solution that can provide a tangible return on investment," says Mr. Douglas Ong, Executive Director of Pacific and Orient Insurance.

After evaluating several offerings on the market, the company chose Cisco's VPN 3000 Series Concentrators. Explaining why he was attracted to the product, Mr. Ong says: "The

field-swappable and customer-upgradeable components let us easily add capacity, and in a mobile office environment, that is an important consideration," he says. These components are called Scalable Encryption Processing (SEP) modules.

Secondly, he is also enticed by the fact that the Cisco VPN Client can be had at no additional costs, and that the solution offers unlimited distribution licensing. These two factors, plus the fact that the company can now do away with its previous service contract for 50 leased lines, meant that the return on VPN investment was nearly immediate.

But cost-savings from hardware was only one part of the company's goal, says Mr. Ong. More important was increased agent productivity. No longer do agents need to rely on slow connections or hurry back to their offices to clear contracts or extract information. With the new VPN solution, key business processes like claims processing and settlement time were significantly improved, leading to priceless a payback: A better repute.

Cisco's VPN solution has also provided an effective platform for the company to move into new work processes. With more bandwidth and extended secured connectivity options, the company was able to implement new workflow automation processes to improve sales processing, quotation and document management. It also rolled out Web-based self-service solutions that let agents update policy, perform online checking and initiate insurance applications.

As Pacific & Orient Insurance clearly shows, enterprise security doesn't have to be a passive necessity. Instead, it can be the underpinning for new cost equations and better productivity.

about P&O Insurance

Pacific & Orient Insurance Co. Berhad, a subsidiary of Pacific & Orient Berhad, was established as a licensed insurer in 1972. The company has since grown to become one of Malaysia's largest and most reputable insurer in the motor segment. Today, it operates a network of about 1,000 agents throughout the Malaysian Peninsula, with over 400 personnel from various branch offices. To prepare for future growth, the company recently migrated to a state-of-the-art computing environment and networking architecture, and is working to add more applications to further ramp up the efficiency of its front offices.

Love the product, love the integrator? While that may be true in monopolistic markets, most customers don't have to grin and bear unresponsive or ineffectual network integrators, especially in the current austere economic climate.

So what makes a good network integrator? Three factors come to mind. For starters, it has to be a product expert. In an ideal world, the network integrator would be as knowledgeable as the vendors it is representing. Secondly, it must be robustly supported by principal vendors. This ensures that help, and a larger pool of resource, is always at hand for end users. This is especially crucial when dealing

CERTIFIABLY GOOD

NETWORK INTEGRATORS ARE A CRUCIAL LINK BETWEEN PRODUCT VENDORS AND END USER ORGANISATIONS. CERTIFICATION PROGRAMS LIKE CISCO'S CERTIFIED PARTNER PROGRAM MAKES IT EASY FOR END USERS TO RECOGNISE EXPERTISE WHEN THEY SEE IT.

with difficult projects. Third, and perhaps the most crucial factor is network integrator experience. Given the turnkey nature of IT deployment these days, experience can make or break new deployment and complex projects.

But how can end users tell if their network integrator fulfils these criteria at face value? The answer is a partner certification program. A good example is the Cisco Channel Partner program, which addresses precisely the three aspects above.

To ensure a high level of integrator expertise, the program mandates that Cisco partners undergo rigorous training and stringent qualification tests before they can attain certification. And this leads to more, because once they are certified as registered partners, network integrators will be given access to a wealth of Cisco resources and collateral materials available only internally to Cisco.

Further, to sharpen network integrator focus, technology-specialisation is a requirement, in areas like VPN/Security, IP Telephony, WLAN and others. This is crucial in enterprise networking deployment, which have become too complex an operation these days to allow for generic value-adding from network integrators. Specialisation means that deployment can be tackled quickly and expertly.

There are three tiers of Cisco partnership certification: Gold, Silver and Premier. Each

reflect the different levels of operational competency and expertise of network integrators. At the helm is the Gold Certified Partner. To appreciate its stringency, consider some of the requirements needed: Round-the-clock call centre and technical support, one-hour call-back support requirement, and four-hour on-site response time. Furthermore, both Gold and Silver Certified partners are required to maintain a specified number of staff with recognised industry certifications like CSE, CCNA, CCDA and CCIE, to tackle customer deployment. CCIE, in particular, are widely considered by many to be "guru" consultants, who are trained to handle the most complex network deployment issues.

What about network integrator experience? This one is easy. Cisco partners are tested not just rigorously, but repeatedly. Across all partner tiers, certification status is reviewed and renewed yearly, so no Cisco partner can rest on its laurels. In other words, an integrator which has long-term certification status demonstrates not just excellent experience, but longevity.

But all the certification in the world would be useless if customer-satisfaction levels are not worked into the mix. The Cisco Certified program does so by tying certification renewal and employee incentives to a yearly customer satisfaction survey—a sure-fire way to keep network integrators on their toes, and on top of their technology.



CISCO SYSTEMS SECURITY SPECIALISED PARTNERS

Gold Certified Partners
Datacraft (Malaysia) Sdn Bhd
Tel : 03 21666363 | Fax : 03 21667728
www.datacraft-asia.com

Getronics Solutions (Malaysia) Sdn Bhd
Tel : 03 22676888 | Fax : 03 22723231
www.getronics.com

Hewlett-Packard Sales (Malaysia) Sdn Bhd
Tel : 03 26986555 | Fax : 03 26952033
www.hp.com

IBM Malaysia Sdn Bhd
Fax : 03 77272188
www.ibm.com

Silver Certified Partners
Computer Systems Advisers (M) Bhd
Tel : 03 79587878 | Fax : 03 79586888
www.csam.com.my

Mesiniaga Berhad
Tel : 03 56358828 | Fax : 03 56363838
www.mesiniaga.com.my

Premier Partners
Business Information Technology (M) Sdn Bhd
Tel : 03 80241461 | Fax : 03 80241464
www.bit.com.my

SCS Computer Systems Sdn Bhd
Tel : 03 79565800 | Fax : 03 79577900
www.scs.com.my