Making a Case for IPS

The Strategic Catalyst
TeleChoice
for the Telecom Industry

Introduction

The concern over network security long ago moved out of the exclusive realm of IT and became something that every corporate manager and executive is focused on. While the IT organization retains the primary responsibility for warding off network intrusions, the impact of any attack is felt throughout an organization today – both in the direct costs of repairing the damage, and in the indirect costs which are incurred when corporate resources are "down" and core business goals simply can't be forwarded.

The problem for all of us is that these security incidents are getting worse, and fast. Attacks are getting more sophisticated and networks are becoming more complex. As more of business moves on-line and internal processes are tied together, the cost of an intrusion is jumping dramatically. More operations, employees, and profits are affected.

To make matters worse, network threats have moved from predictable front door attacks to all sorts of internal and external, wired and wireless, direct and indirect assaults. Whether these are virus or worm infestations, denial of service floods, spyware, or active hacking by individuals, it almost does not matter. "Downtime" means "Out of Action" – your business will lose money, the only question is, "How much?"

Lest you think this is some sort of attempt to sow fear, uncertainty and doubt in a baseless fashion, we've verified attacks in our own TeleChoice networks, protected by standard firewall and anti-virus software. Our results? Unprotected machines were compromised within one *minute*! Indeed, when our own servers at TeleChoice were hacked into despite leading edge gear protecting them, this very quickly moved from being an IT issue to a CEO issue.

Growing network complexity exposes your organization

In an effort to solve company problems and meet corporate objectives, the network has become more complex. The devices attached to the network have themselves become both more numerous and more complex. And the inroads to the network have increased greatly as well – with Internet-exposed Web and application servers, branch office connections and remote connections into the network all commonplace for today's enterprise.

Unfortunately, businesses cannot go back to an easy-to-secure limited application environment. The pathways into a corporate network have increased – and will continue to increase – as more users of an enterprise's workforce require access to networked applications.

You think you are already protected

So we know what you are thinking – "I've heard all of this before, this is nothing new." Well to some degree, you are right. The issues we discuss above aren't news to anyone who's been paying attention to the state of network security or even just reading the daily newspaper. These high profile incidents are really just the tip of the iceberg. Beneath the public's and media's radar, thousands and thousands of

network attacks take place every day. IT professionals have, of course, taken many steps to try to head off these attacks, and have had some level of success. For example, many enterprises have implemented the following solutions:

- Installing a *firewall system* to regulate traffic flowing onto and off of the network.
- Installing *antivirus software* on all PCs to reduce the chances that viruses will attack the network from within.
- Implementing an IDS (*Intrusion Detection System*) to alert IT staff when a potential attack is taking place.

These steps provide a degree of safety and are an improvement over leaving a network fully exposed and unprotected. But these solutions, alone or in concert with one another, simply aren't enough – and believing that they will provide true security is a dangerous assumption for any enterprise.

The Three Myths of Network Security

Many firms are laboring under the IT equivalent of "Old Wives' Tales" when it comes to security, and we think these myths need to be dispelled.

Myth #1: The firewall can do the job

A firewall is, of course, the most basic building block of any network security strategy. The problem with a firewall is that it's really just a dumb box. Firewalls only know how to block this port or that protocol – based upon rules that the manufacturer and your IT staff implement.

But as you provide access to your network, your firewall must be configured to allow ports or protocols to be open (for example, port 80, used for most HTTP traffic). These open ports and protocols provide an entry to hackers or worms. A firewall *can* provide some inspection of incoming traffic on open ports, but typically this inspection does not rise above the Layer 2 or 3 level (looking at things like IP addresses and ports) – and does not have the intelligence to look for anomalies in the traffic within the actual application data itself.

Myth #2: Anti-virus software will do the trick

Anti-virus software – when installed on *all* clients and servers in the network and maintained religiously – theoretically provides some protection against many attacks. But while anti-virus software *is* an essential tool, there are three big failings here.

First, anti-virus software only protects your individual systems from *known* viruses. It is based primarily on pattern recognition techniques which rely upon *definitions* of known viruses – and despite the best efforts of vendors, there is often a time lag between the identification of a new (or mutated) virus and the implementation of a fix. New worms that are being produced today don't give the anti-virus firms or you that luxury of time. These worms can mutate hours after an initial infection, making detection by pattern matching almost impossible.

Second, anti-virus solutions are limited. They cannot protect against all forms of threats, like Denial of Service attacks or Trojans.

Third, anti-virus solutions require more administration and management than a network-based solution because each individual desktop must have the software installed and updated regularly. In some situations, it is difficult to enforce the update of every anti-virus software on every desktop.

Myth #3: IDS systems protect you

An IDS performs packet analysis on traffic flowing onto and off of your network, and marries this analysis with a report generation system. When the IDS determines that an attack is taking place, it uses this report generation system to provide console warnings, emails, and even SMS or paged alert messages to system administrators.

The problem with this approach is primarily one of time – by the time even the most alert on-call network administrator gets these warnings, it is too late to do anything but shut the infected system or network down. This leaves the enterprise with two big issues: first they must spend the time to examine the system, clean it up if necessary, and then bring it back online; second, while this happens, legitimate users of the network are left without access to their mission critical applications and data.

You need a *comprehensive* and *proactive* solution

What's needed is a system that can take a much more *proactive* approach to network security. Cataloging and recognizing known attacks is essential, but the only way to truly stay ahead of the security game is to become more predictive and intelligent about blocking attacks. The best business practice in this area today is to leverage a security system that incorporates vulnerability-based protection to block exploits on vulnerabilities and worms. By securing the underlying vulnerability when it is disclosed, intelligent security solutions deploy security "patches" to protect against any future exploits, including those unknown and undeveloped.

In order to gain this kind of protection, companies require an intelligent solution that sits in-line and inspects all traffic for threats, through Layer 7. Additionally, the update service and security coverage of the security solution is critical. Companies need protection against more than just viruses. They need protection against a barrage of threats: worms, viruses, Trojans, Denial of Service attacks, Phishing, Spyware, and VoIP threats.

Going with the State-Of-The-Art, IPS

When our organization needed to take the next step, we stepped up to an *Intrusion Prevention System* (IPS). An IPS differs from firewalls, anti-virus software and IDS by proactively inspecting all traffic through Layer 7 and blocking malicious traffic.

A prime example of an IPS is found in the TippingPoint IPS products. TippingPoint's Threat Suppression Engine (TSE), the architecture of the company's line of IPS products, examines each individual incoming packet. Individual application data

flows are examined on a packet-by-packet basis (at "wire speed", so data traffic is not slowed down), using its own security filters and algorithms. The instant the TSE discovers a malicious data flow, the system blocks that traffic and stops the attack before it can damage your network.

The IPS is updated regularly with the latest vulnerability and threat protection through the TippingPoint Digital Vaccine service. The IPS offers comprehensive protection against worms, viruses, Trojans, Denial of Service attacks, VoIP threats, Spyware and Phishing attacks. It also performs bandwidth management.

An IPS is a complement — a necessary complement in our opinion — to your existing security systems, and provides the next level of protection available to companies today.

Making the Business Case for IPS

To us, there's no question every firm should have an IPS front-ending its network.
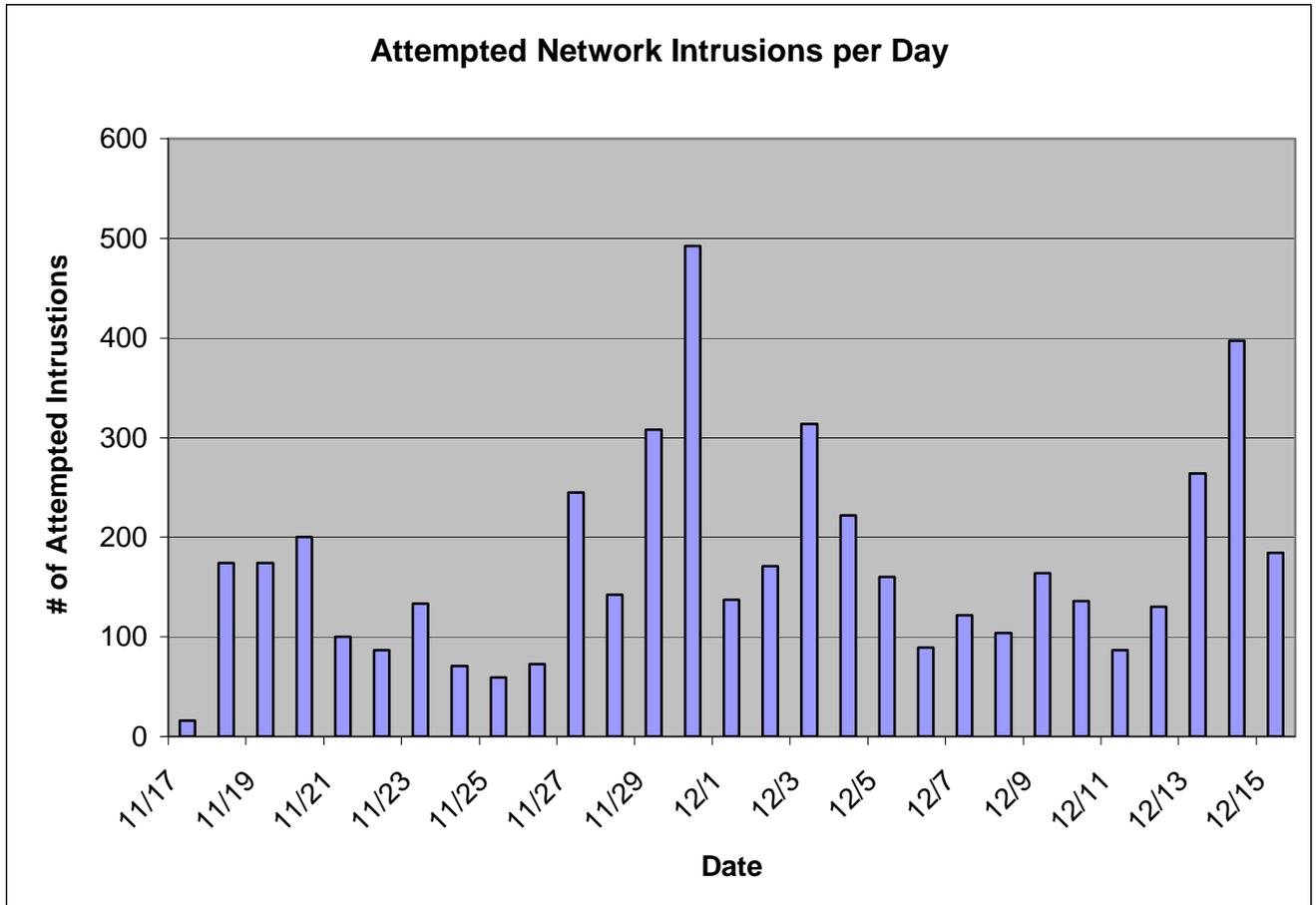
Our own experiences have taught us this lesson many times over. Prior to the installation of an intrusion prevention system within our corporate network, we – like many companies – were subject to a number of debilitating network attacks which decreased performance, subjected our corporate data to compromise and on several occasions brought our entire network offline.

Even with a diligent IT staff, up-to-date server and anti-virus patches, and a top-of-the-line firewall system in place, we were simply unable to keep our relatively small network (2 main internet connections, less than a dozen servers publicly exposed to the Internet) protected.

The installation of a TippingPoint IPS system provided us the solution we needed to stem this tide – our network has had zero outages related to intrusions since the installation over a year ago. And this record has been maintained in the face of a growing number of intrusion attempts.

In fact, in a one month period in late 2005, our IPS blocked nearly 4,900 unique attempts to compromise our network. This is an average of over 170 attacks a day, and on some days the number of attacks spiked to nearly 500.

Any one of these attacks, if successful, could have cost us thousands of dollars in lost productivity, IT staff time and network downtime. The chart below demonstrates these attacks on a day-by-day basis for this not atypical month.

Attempted Network Intrusions per Day

# of Attempted Intrustions (y-axis): 0, 100, 200, 300, 400, 500, 600

Date (x-axis): 11/17, 11/19, 11/21, 11/23, 11/25, 11/27, 11/29, 12/1, 12/3, 12/5, 12/7, 12/9, 12/11, 12/13, 12/15

At its heart, installing an IPS in a corporate network is, like any capital investment in IT, a business, and not a technical, decision. And like any business decision, an investment must provide some payback in order to be worth considering.

The business case for IPS can be made clearly based upon two factors:

- The costs associated with the repair and "clean-up" of compromised systems
- The loss of core business productivity and production caused by an attack on the network

Cleaning a compromised system can take a very smart server tech between a day and week in time/labor depending on the type of infection. That can add up quickly when you are faced with an average cost of 40 or more dollars per hour for a system admin to perform major repairs (like rebuilding an affected server).

Take, as an example, the case of a large enterprise with 1000 workstations and 50 servers (providing email, messaging, file storage and application services). In a typical instance, a single worm attack which spreads throughout this enterprise could infect a quarter of these servers and 30 percent of these workstations.

A conservative estimate for repairing such damage – based upon 8 hours of system admin time to rebuild an infected server, and 2 hours to rebuild a workstation – would put the cost of a single incident in this sample enterprise over $4,000 for the server, and the cost of repairing workstations could be as high as $24,000. This figure does not include the costs of patching unaffected systems, nor does it account for overtime or other expenses incurred when the infection occurs after hours or on a weekend/holiday. It also does not include the lost time of the IT staff doing other business strategic tasks for the firm. And this figure, remember, is for a single incident – many enterprises face such incidents multiple times per year.

The Table below demonstrates this situation:

	Number	% Infected	Number Infected	Hours to Repair	Repair Costs
Servers	50	25%	13	104	$4,160
Workstations	1000	30%	300	600	$24,000
				Total	$28,160

The costs of IT staff time aren't the only expenses incurred during such a security breach. The lost time and productivity of the corporation's staff during such an outage must also be accounted for. If the average employee affected by the outage is paid $45,000 a year, and has a fifty percent reduction in productivity during the 8 hour outage, our example enterprise could lose over $21,000 in worker productivity due to the server outage, as shown below.

Number of Employees Reliant Upon	Percentage of Employees Affected by Outage	Length of Outage (hours)	Productivity Loss during outage	Average Hourly Rate per affected employee	Productivity Losses
1000	25%	8	50%	$21.63	$21,630

Then there are all the hard-to-estimate costs of an outage – employee disdain for IT, the time involved in each employee resetting all of their cookies and other program settings, that lost file that each was working on when the shutdown occurred, etc. We won't include those in this analysis, but sometimes these are the most expensive aspects of any outage!

This leaves a good, per-incident estimate in losses at nearly $50,000 — losses that could, in most cases, be eliminated by the introduction of an IPS defense in the corporate network.

Total Expenses of a Single Attack

Server Repairs	$4,160
Workstation Repairs	$24,000
Productivity Losses Due to Server Outage	$21,630
Total	$49,790

The cost of an IPS deployment to protect upon such attacks varies from network to network – we typically recommend that an enterprise deploy an IPS system at each outbound network connection point, and some networks may segment internally and apply additional IPS resources at those segmentation points.

The cost of an IPS could easily be paid back if it prevented only 1 or 2 of the incidents we have described above. And you won't be facing only one or two such incidents – as our experience above shows, even a smaller enterprise will be facing thousands of such potential intrusions every month.

The Bottom Line

For us, it took only the experience of one hacking attack and our CEO was sold on not wanting it to happen again. So while it's good to quantify these savings, we'd hate it if the only way to prove them out was to go through an attack.

IPS is an essential part of a comprehensive security strategy for any networked business. The difference that IPS brings to the table is its proactive approach to security. IPS isn't simply a static system that fights "yesterday's wars" by attempting to filter out known threats. Nor is it a passive system that warns your network admins after an attack is already underway.

Instead, IPS actively examines your incoming and outgoing traffic and uses a variety of filters, patterns, and algorithms to examine every packet and to make intelligent decisions about the threat level of those packets. IPS then automatically takes timely actions to block those threats without requiring a complete takedown of your network.

If your business is exposed to the Internet, and you value your security, IPS should be the next cornerstone in your security strategy.