Maximizing the Benefits of Intrusion Prevention Systems: *Effective Deployments Strategies*

Charles Iheagwara, Farrukh Awan, Yusuf Acar, Calvin Miller
Office of the Chief Technology, District of Columbia Government
Washington DC

18th Annual FIRST Conference
Baltimore Maryland

June 25 – 30, 2006

Introduction

Six basic drawbacks of current IDS products that limit its effectiveness as a security solution [1]:

- Performance Barriers
- Detection Accuracy
- Product Complexity
- Growing IDS Evasion
- Passive Device
- Enterprise Scalability

- The drawbacks were put squally in front of the burner when research firm Gartner Inc. provided another nudge when it declared IDS will be obsolete by 2005 [2]. The report accelerated the call by some industry analysts to kiss a final goodbye to the IDS as an essential security technology. And since then, the death knell for intrusion detection has been getting louder.

Introduction Cont.

Gartner provides three reasons for this:

- “99 out of 100” alerts mean nothing
- Plethora of false positives
- Voluminous amounts of data

"The underlying problem with IDS is that enterprises are investing in technology to detect intrusions on a network. This implies they are doing something wrong and letting those attacks in," said Gartner vice president of research Richard Stiennon [3].

Industry Reaction

- In the aftermath of Gartner's assertions, many industry analysts have risen to the defense of IDSes; and calls for improvement of existing technologies. For example, Andre Yee, NFR Security [4] writes:

- *"The Silver Bullet Syndrome… In view of these perceived limitations, some industry pundits are writing off IDSs altogether in favor of newer network intrusion prevention systems (NIPS). However well intended, casting NIPS technology as a remedy to all that ails the IDS is an unfortunate oversimplification. There are three reasons for this. First, as noted in the prior section, many of the issues regarding current generation IDS products are unrelated to the issue of "prevention versus detection". For example, the distinct challenge of scaling IDS from a point product to an enterprise solution have more to do with good design than with the benefits of prevention over detection. A poorly designed NIPS product will undoubtedly encounter similar scalability problems as a poorly designed IDS product…"*

Industry Reaction Cont.

- Thus, the prevailing concerns about IDS provides the need and is an impetus for a new kind of network intrusion management product that comprehensively addresses the limitations of current products while delivering better detection, enterprise manageability, and prevention.

- In the last two years, there has been some noticeable progress in the development of intrusion prevention systems (IPS). Some of the developments are in the beta testing stage and others have made their debut in the IPS in the market place.

- Against this background, this paper presents the business and technical imperatives of the IPS and reviews IPS concepts and implementation, analyzes performance factors and proposes effective deployment strategies.

Industry Reaction Cont.

- Thus, the prevailing concerns about IDS provided the need and impetus for a new kind of network intrusion management product that comprehensively addresses the limitations of current products while delivering better detection, enterprise manageability, and prevention.

- There were other techno-economic imperatives

Techno-Economic Imperatives of Introducing IPS to the Market Place

- Three basic premises define the needs:

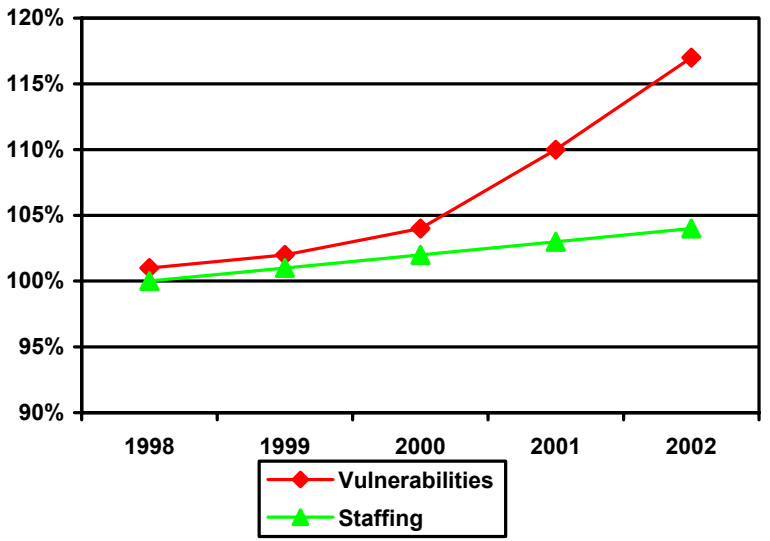
- Mission critical applications and systems must be available
  - What are my mission critical applications and systems?
  - Which critical assets are at risk? Under attack?

- Regulatory compliance and risk mitigation are a modern business reality
  - Are we compliant with rules and regulations?
  - We've invested all this money – how secure are we?

- Resources are constrained
  - Turn-key, real-time, 24*7 security infrastructure.
  - Cost-effectiveness is paramount.

Techno-Economic Imperatives of Introducing IPS to the Market Place:

Figure 1: Resource Gap



Gartner's Recommendations: A Precursor to IPS Introduction

- Gartner recommended “Real-time Network Defense.”
- … intrusion prevention systems to support rapid shielding
- ABC’s of Defense – Alert, Block, or Correct
- In the last few years, several commercial intrusion prevention systems (IPS) made their debut in the IPS in the market place.

Definition

- Intrusion Prevention is the act of dropping detected bad traffic in real-time by not allowing the traffic to continue to its destination, and is useful against denial of services floods, brute force attacks, vulnerability detection, protocols anomaly detection and prevention against ‘Zero day” (unknown) exploits.

- A basic **distinction** is that the IDS is an out of band technology whereas the IPS sits in-line on the network. In this case, the IPS monitors the network much like the IDS but when an event occurs, it takes action based on prescribed rules. Security administrators can tweak such rules so the systems respond in the way they would.

Intrusion Prevention Approaches

- "Intrusion prevention" can be achieved through three main approaches: Secure engineering - building systems with no vulnerability, Taking perfect remediation steps to uncover vulnerabilities and patch them, and detecting the exploit attempts and blocking them before serious damage is done.

In-line Mode Vs. Out of Band Concepts

- As stated before, the IPS operates on the In-line mode i.e. the sensor is placed directly in the network traffic path, inspecting all traffic at wire speed as it passes through the assigned port pair. In-line mode enables the sensor to run in a protection/prevention mode, where packet inspection is performed in real time, and intrusive packets are dealt with immediately – the sensor can drop malicious packets (defined though policy) because it is physically in the path of all network traffic. This enables it to actually prevent an attack reaching its target.

- Thus, given the mission defined for it and in contrast to the IDS, the IPS mode of operation enables it to provide preemptive protection.

IPS Performance Metrics

- Given the functional requirement for the IPS, the performance metrics should be measured in terms of:

- The IPS's dynamic alerting capability,
- The IPS's dynamic blocking capability, or
- The IPS's ability to correctly identify attacks.
- The IPS's ability to identify if a system's patch level makes it susceptible to impending attacks,
- The IPS's Accuracy of dropping packets
- The number of false positives
- The IPS's Fail open and fail safe capability
- The IPS's High availability and redundancy architecture

Effectiveness Measures

- The decision to invest on the IPS hinges on the ability to demonstrate a positive ROI. In essence, this entails quantifying the IPS's value prior to deploying it.

- Therefore, the effectiveness of the IPS will be tied to a positive ROI value.

IPS Deployment Strategies

- Generally, there are several product configurable and network/system parametric variables that affect the performance effectiveness of the IPS:

- High Bandwidth Throughput
- Minimum Packet Latency
- Accuracy of Detection
- Accuracy of Dropping Packets
- Ability to detect unknown attacks (Protocol Anomaly)
- Few false Positives
- Policy based Controls
- Fail Open and Fail Safe Capability
- High Availability and Redundancy Architecture

Area of coverage

- To maximize the benefits of the IPS, it must be deployed in a way that positions the traffic streams to transverse through it for a wider scope of visibility such that it can perform a deep inspection of the packets and based on the pre-defined rules take appropriate actions i.e. allowing passage of the packets, sending an RST, dropping packets, etc.

- Based on previous studies [10] and data from our field practice [AWAN], we propose the following deployment location to maximize the IPS effectiveness:
- Deployment where high security and protection is required

- Deployment at the defense perimeter

- Deployment where there is a high probability of an internal outbreak and attack; and

- Deployment through strategic segmentation of the network into smaller areas for better distributed architecture

Deployment Scenarios

- ***Deployment at Ingress/Egress***
- In considering the choice of a particular scenario over the other, it is important to consider the benefits associated with each scenario and the suitability for each environment.

- The advantages of deploying the IPS at Ingress/Egress point within the network like traditional Firewalls and NIDS are few but much defined. This style of deployment allows stopping malicious traffic from entering or leaving the network perimeter and internal outbound traffic. This type of deployment is most useful in preventing attacks against Perimeter infrastructure e.g. if some is trying to compromise Border router, Firewalls and VPN devices. This approach can also be useful in protecting Secure Zones such as DMZ.

- At the same time, there is a high amount of generated alerts as the perimeter s often the starting point for attackers who are probing for vulnerable systems. Also, devices deployed at Ingress/Egress Points within the network offer little value in preventing internal outbreaks from spreading to other internal areas within the network. For instance, a single infected internal host could potentially infect every other vulnerable internal host without traversing through the IPS thereby generating a negative ROI value.

Deployment Scenarios Cont.

- ***Deployments at Core switches and Access layer Trunks***
- IPS Deployments at Core switches and Access layer Trunks VLANS provides the most coverage area and protection against internal attacks. With this strategy it defines very small containment areas where in the event of an internal outbreak the infection will be able to propagate only within a single area.

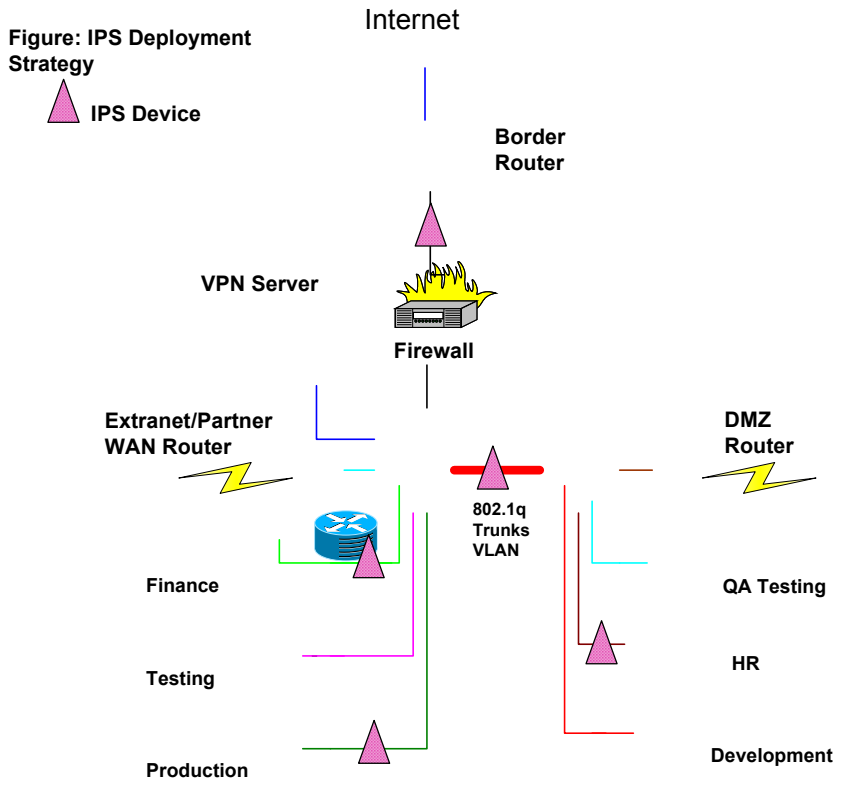
- In cases where the majority of the hosts on any given access layer switch device are in dissimilar VLANs, the containment are may be reduced even further due to the necessity of traffic traveling from one VLAN to another to traverse the core switch/router device. This deployment strategy is the most effective as it is closest to the end user but not cost effective since in order to cover 100%, IPS needs to be deployed at each Access layer Switch. The Real World deployment is to deploy IPS on Core Switch Truck VLANS to provide high degree of protection against internal and external threats.

Deployment Scenarios Cont.

- The best approach is to optimize the deployment using a combination of all the above approaches with deployment at Perimeter; Core switches on Trunk VLANS and critical access layer switches.

- In the Figure 2 below, the IPS deployment is distributed to protect Internet Firewall, DMZ and Intranet against external attacks from Internet. The advantage of placing IPS on the Trunk VLAN between core switch give access to all VLANS as the traffic passes through Truck via trucking protocols (802.1q).

Deployment Scenarios Cont.



Specifications for Bandwidth, Availability and Interface Type.

- **Two important issues to consider with respect to the IPS performance are:**

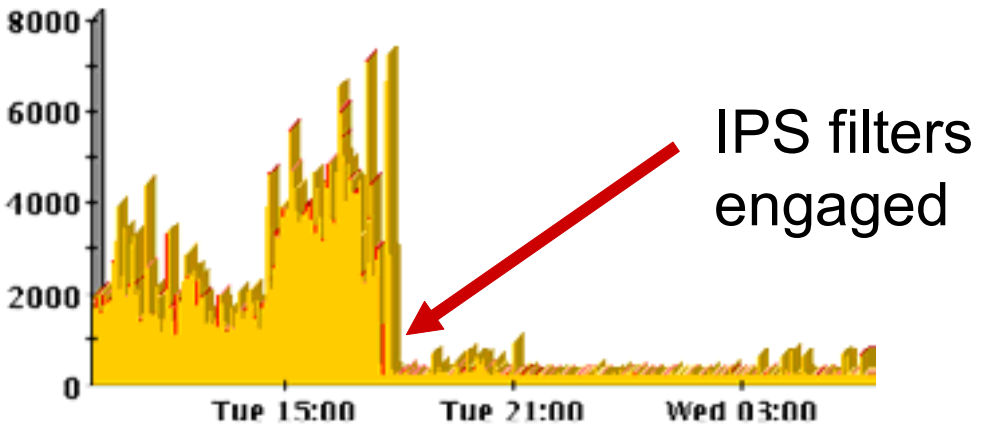
- **Varying bandwidth levels for different interfaces**
- With respect to the bandwidth level, one key criterion to determine in the deployment is the bandwidth requirements on the Trunk link and the type of interface i.e. the use of fiber or copper interfaces based on the core switch topology. In this regard, it is worthy to note that 802.1q Trunks often carries extremely heavy load of traffic and this may result in the saturation of the inline IPS devise causing it to drop packets it cannot handle.

- **Failover/Failopen mechanism**
- As for failover mechanism, considerations should be given to configuring the IPS with fail open arrangement such that when the IPS malfunctions, it acts like a wire or the IPS needs to be configured in array so it fails secure. Thus, at a minimum the IPS should fail open, regardless of the network media to provide high availability along with low latency, which is often the most critical performance factor for Network Intrusion Prevention Systems.

Empirical Performance Data and IPS Value Proposition

- For now, it is known that immediate benefits have begun to accrue from current deployments. One implementation using T-1 outbound connection on a network system [13] asserts the following:
- Prior to implementation, infected internal machines were choking bandwidth to a point of uselessness
- IPS implementation prevented T-1 upgrade resulting to a saving of approximately $600 per month
- The IPS identified infected machines and kept Blaster Virus traffic off the network.
- When an IPS was implemented on outbound T-1 connection, substantial bandwidth was reclaimed (wasted bandwidth average from 3Mbps to <1Mbps) and prevented T-1 upgrade (saved ~$600 per month). The actual traffic data is presented in Figure 3.

Empirical Performance Data and IPS Value Proposition



Conclusion

- When an IPS device is deployed in a complex environment, there are several factors/variables that influence the performance.
- And, hence to effectively deploy the IPS, there is the need to have a sound understanding of the environment where the IPS is deployed including, at a minimum, the impact of deployment location, area of coverage, bandwidth levels and interface type. In line with this, we have presented the factors/variables and analyzed how they affect the IPS performance.
- For this, we have proposed strategies to optimize the effectiveness of the IPS using proven deployment techniques.

Empirical Performance Data and IPS Value Proposition Cont.

- In Figure 3 above, bandwidth consumption is represented on the “X” (vertical) axis while the “Y” horizontal axis represents time in minutes. Also, data obtained from implementation of the IPS on network [13] shows:
- That the IPS is blocking over 100,000 attacks per month.

- That estimates for prevention of Viruses, Worms, Spyware is roughly 5000 infections

- For the 5000 infections prevented, we can express the economic benefit (EB) of the damages prevented in the form of:
- EB= (Repair Time X Wages X Attacks Blocked) =2hrs X $40 X 5000 = $400,000
- Where the time to repair an infected workstation = 2 hour; and
- The Sys Admin hourly wage = $40.
- The EB while not exactly an exact computation of return on investment, nevertheless, is a pointer to a positive ROI in the above case given.

References

- [1] C. Iheagwara, “The effectiveness of intrusion detection systems.” Ph.D. Thesis, University of Glamorgan, Pontypridd, Wales, 2004
- [2] http://www.esecurityplanet.com/views/article.php/2228631
- [3] http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci905961,00.html
- [4] A. Yee, “The intelligent IDS: next generation network intrusion management revealed.” NFR security white paper. Available at: http://www.eubfn.com/arts/887_nfr.htm
- [5] C. Iheagwara, “The Effect Of Intrusion Detection Management Methods On The Return On Investment” *Computers & Security Journal,* Vol 23, issue 3, pp 213-228, May 2004
- [6] The Computer Economics Journal “Cost estimates for viruses and worms.” 2004
- [7] SourceFire, Inc. “Real-time Network Defense - The Most Effective Way to Secure the Enterprise.” White Paper, Columbia, Maryland, 2004
- [8] E. Hurley, “Intrusion prevention: IDS' 800-pound gorilla.” News Article, April 8, 2003 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci892744,00.html

References Cont.

- [9] C. Iheagwara and A. Blyth, “Evaluation of the performance of IDS systems in a switched and distributed environment,” Computer Networks, 39 (2002) 93-112
- [10] C. Iheagwara, A. Blyth and M. Singhal, **“**A Comparative Experimental Evaluation Study of Intrusion Detection System Performance in a Gigabit Environment,” Journal of Computer Security, Vol 11(1), January, 2003
- [11] K. Richards, "Network Based Intrusion Detection: a review of technologies,” Computers & Security, 18 (1999) 671-682.
- [12] C. Iheagwara, A. Blyth, K. David, T. Kevin, “Cost – Effective Management Frameworks: The Impact of IDS Deployment on Threat Mitigation.” Information and Software Technology Journal, Vol 46, Issue: 10, pp.651-664, May 2004
- [13] TippingPoint, Inc. Case Study. Available at: http://www.tippingpoint.com/pdf/resources/casestudies/505323-001_UnivofDaytonCaseStudy.pdf