Intrusion Prevention: A White Paper

How to evaluate competing Internet Security Gateways and Firewalls

ABSTRACT:

Internet based access is fundamental for doing business today. As such, traditional tools such as perimeter firewalls, desktop anti-virus, and passive forensic monitoring using intrusion detection are in need of augmentation via additional, more sophisticated protection. Such protection is provided by an emerging class of security solution entitled *intrusion prevention systems* (IPS). This white paper will examine the positioning of intrusion prevention as part of an overall layered security strategy and a review of evaluation criteria for identifying and selecting an IPS.

This paper is brought to you by Cressida Technology, a Software To Be Sure Security Solutions provider and NitroSecurity exclusive European Distributors. To contact Cressida please email us on info@cressida.info or please visit our site at http://www.cressida.info/ContactUs.htm for a listing of our pan-European sales and support contact information.

Background

Consider the Internet. It is a pervasive global communications medium that allows even the most remote home based business to attract and obtain clientele worldwide. Yet with that global reach comes a stark reality. While thousands of legitimate businesses and individuals utilize this powerful medium, there exists a growing threat of individuals and/or groups that unleash malicious activities into cyberspace. These activities range from simple user abuse and harassment to the destruction of a corporation's business data, intellectual property, and brand identity. In 2003 alone, billions of dollars in damages to organizations occurred through the security breaches caused by Internet based worms such as Sobig, MS Blaster, SQL Slammer, and others.

In response, organizations are developing and implementing security practices that protect critical on-line assets from both external and internal exploits. The most popular security solutions installed today include firewalls, intrusion detection systems (IDS), anti-virus software, and content inspection to name a few. While each one has its own role in a layered or *defense-in-depth* security strategy, these products are not designed to provide the rapid, proactive in-line blocking required today to protect against today's new generation of hackers and hybrid or "blended" attacks.

For example, firewalls were originally intended to be deployed at the network perimeter to deny unwanted access by *external* users and applications to internal resources. Equally, to permit data exchanges and business transactions, firewalls must leave "holes" open to the internal network thus allowing bi-directional traffic to flow. This legitimate "hole" now becomes a portal for malicious users to enter into the internal network. Another security technology is the intrusion detection system (IDS). IDS is designed to recognize and detect *intrusions* that somehow bypassed the firewall. IDS provide good traffic classification and forensic information but cannot, by its passive design and nature, effectively block an attack. In the extreme case, if an IDS identifies a single packet attacks, by the time it is identified and logged, the attacker has compromised the target. An IDS also requires human intervention and specialized training to implement the proper remediation behavior. These shortcomings limit the effectiveness of IDS solutions as the first line of security defense.

In response, a new class of security mechanism designed for active, network-wide protection is required. Such protection is provided by a solution entitled *intrusion prevention system* (IPS). IPS is designed to augment the existing security infrastructure and tools while providing a proactive, in-line protection *solution* for current and future cyber exploits. Industry analysts such as the Gartner Group tend to support this distinction between security tools and *solutions* to secure networks:

"By implementing a network-based intrusion prevention system, organizations can immediately solve some of their key security issues by stopping network attacks and blocking unauthorized access to important data and information," said Rich Stiennon, research director at Gartner.

Given ever-increasing Internet usage coupled with corresponding complex cyber threats, the question that IT and security staff should answer is not *"should I deploy intrusion prevention"* but rather *"which one?"*

To be viable, IPS must meet both *business goals* as well as *technological justification*. Consider the following due diligence reviews:

Intrusion Prevention: The Business Case

Today, companies are re-establishing business practices based on measurable goals, known practices that can adapt to rapid changes, and accountability. Attributes of today's successful business goals for corporate expenditures today include:

- The technology should be consistent with the company's business practices and policies, including security policies.
- The investment must be predictable resulting in an effective IT infrastructure that is available and reliable.

- Best practices involving corporate spending should ensure there are "no surprises" (risk management) to daily operation or how the company reacts to changing conditions where these changes are targeted, e.g., competitive action, or broad in scope, e.g. market shifts.
- Targeted operating expenditures that augment what's already in place to protect existing investments
- Technology deployments must be able to respond via quick, immediate response to significant events, changes, or disasters to maintain business continuity with customers and partners.
- Investments must produce timely & measurable ROI.
- Technology deployments, like the corporate operating policies they support, must be flexible to adapt to ever changing conditions and markets.
- Reliable in their accounting and reporting due to best practices.
- Technology must support regulatory compliance.

Without specific, quantifiable business goals, a company cannot succeed in today's ever-changing economy and markets. As such, strategic assets, including the IT security architecture and support infrastructure, must support these corporate goals as well.

Just as a company's *commercial environment* is affected by dynamics such as economics, politics, and competition, the underlying network operating environment in support of the business has its own set of challenges. IT and network operations must have *their own goal sets* that align with corporate objectives if they are to succeed in supporting the overall business. More specifically, IT expenditures must be held to the same scrutiny and metrics as any other corporate asset used in running the business. This is especially true when companies are considering investments in emerging technologies such as next-generation security solutions like an intrusion prevention system (IPS).

Businesses must choose between host-based IPS (HIPS) and network-based IPS (NIPS) solutions. NIPS are typically deployed at the perimeter of your network, perform deep packet inspection using several methodologies, operate at wireline speeds, and prevent malicious traffic from ever entering your network. As a stand alone solution, NIPS are designed to meet your business and IT goals because it does not consume network bandwidth or leave your network vulnerable between the moment of intrusion detection and the moment of consequential response.

NIPS, such as NitroSecurity provided by NitroSecurity, Inc, must be developed not only as a premier solution to secure IT networks but must align with corporate best practices and goals. Below is a chart that maps such goals with IPS advantages and associated customer benefits:

Corporate Goals	**NitroSecurity IPS Advantage**	**Customer Benefit**
Investments must be predictable resulting in an effective IT infrastructure that is available and reliable.	NitroSecurity intrusion prevention solutions that are based on *field proven rule sets a*nd *deterministic technologies* can provide *predictable* and measurable protection. Savings occur due to this protection being quantifiable in hard $$$ savings (see below).	**Known results** using known techniques give end users assurance that their protection **solution is working** "as advertised" Reduced operational issues due to predictable behavior of IPS

"No surprises" (risk management) to daily operation or how the company reacts to changing conditions	Ease of configuration is a strong attribute of any IPS solution. Furthermore, the IPS must utilize a combination of multiple, advanced mechanisms.	Ability to deal with **"what we don't know about"** attack scenarios **Reduction in downtime** due to "surprise" exploits entering corporate network. Low operational expenses due to fewer devices to manage
Protect existing investments	The NitroSecurity IPS augments and re-fortifies existing network security investments such as legacy firewalls and IDS, allowing them to perform targeted functions such as NAT, VPN termination, and attack classification and forensic analysis.	**Future cost savings** via IPS investment now. **Extended investment amortization** of security $$ already spent.
Quick, immediate response to significant events, changes, or disasters to maintain business continuity	Signature development and deployment must be swift and rule sets verified by a large user community, and made available to users on a widespread basis. The NitroSecurity IPS solution support auto-updates of signatures and rule sets.	Operational **peace of mind** knowing that they (customer) have a "rapid response" protection scheme in place. **Measurably higher performance** of security organization (including reduced staffing and lower operational expenditures)
Investments must produce timely & measurable ROI	Intrusion prevention solutions mean less operating expenses and less lost revenues due to network or resource outages. The IPS' functional success in protecting can be measured and quantified.	**Verifiable payback** when compared with potential remediation costs & business losses **Cost effective** protection of critical resources
Must be flexible to adapt to ever changing conditions, markets	Network attackers are mutating their exploits, becoming more sophisticated, and constantly changing their targets and penetration techniques. The IPS must be able to block exploits "as is", can be quickly reconfigured, or key signatures and updates downloaded that respond to very diverse exploit methodology.	Offering a **flexible** deployment approach makes it easier for security staff to prioritize their defense in depth deployment plans using a single architecture suitable for many uses. Increase the **adaptability** of the security infrastructure to respond and protect against new and existing threats.

Reliable in their accounting and reporting	The IPS must provide comprehensive event logging and correlation event reporting and logging which **produces verifiable evidence** for attacks blocked as part of meeting service level agreements for both internal and external network users down to the "box" level.	Companies can provide ample proof/ evidence/documentation of **conformance to internal (policy control systems) and external (government, industry related) security regulations and procedures** e.g. HIPPA, Sarbanes-Oxley, GBLA. Corporate executives can get the **assurance** they need on the security of their organization while performing on-going risk assessments.
Regulatory Compliance	The NitroSecurity IPS provides protection as to meet various regulatory requirements. Applicable legislation includes: - Gramm-Leach-Bliley Act - Sarbanes Oxley - Patriot Act - California SB 1386	

Below please find a simple return on investment (ROI) example on the cost savings incurred by investing in a NitroSecurity IPS solution by protecting against a single cyber attack.

ROI of IPS Example: Small/ Medium Business ($20M in sales)

Revenue loss due to an individual security breach - $2300 sales/hour x 12 hours server downtime	$27,600
Restoration Costs - 12 servers; 2.5 hours to rebuild per server; consultant's fee: $250/hour	$ 7,500
Total cost due to individual security breach & failure	**$35,100**
Hypothetical NitroSecurity multi-IPS capital investment ▪ Includes one NitroSecurity 200 IPS appliance, 3 workgroup appliances, and services	$36,000
Annual savings due to improved IT staff productivity 1/3 of fully loaded IT resource for patching, virus removal, incident response	($19,800)
Single incident OPEX savings due to NitroSecurity IPS protection	**$18,900**
Predicted ROI in first 6 months	

Intrusion Prevention: The Technology Case

For an IPS to be credible, the solution must: be comprehensive in its attack blocking mechanisms; be field-proven verifying that it works "as advertised"; be easy to install and deploy; and should scale for expanded deployments.

For example, the NitroSecurity next-generation intrusion prevention product line is based on Open Source technology developed by information security professionals over the past three years as part of the Honeynet project (**www.honeynet.org**). The resulting product is the NitroSecurity intrusion prevention system (IPS). The NitroSecurity solution includes the integration of a complete active firewall with field-proven intrusion detection (e.g. SNORT), a fast and smart-logic proprietary database to enable deep-packet inspection of all traffic at wireline speeds, and prevention logic underneath the control of a single management console.

This approach provides a fully supported, open-signature-based solution that is designed and optimized for in-line protection. Many times, proprietary approaches and architectures require significant validation that in fact they do work which takes time and effort. Validation of blocking mechanisms and associated rules sets via the extensive testing and production use by the Open Source community provides the "tried and true" assurance that the NitroSecurity IPS solution "works as advertised".

Lastly, any IPS must be flexible in its network placement options and meet certain functional criteria to be effective. The next section will review typical deployment scenarios along with examples of common test criteria that evaluators must review and verify before investing into a specific IPS offering.

Intrusion Prevention: Selecting a solution

The following is a suggested set of deployment options and evaluation criteria recommendations for intrusion prevention systems (IPS). NitroSecurity provides these recommendations based on its experience at deploying in-line IPS in a wide range of customer networks.

Although NitroSecurity believes that in-line intrusion prevention is the most comprehensive way to protect against network wide cyber threats, it does recommend as part of "best practices" that both client systems and servers be up to patch level.

NitroSecurity IPS Deployment Location Options

Depending upon its specific security policies, an organization may deploy a NitroSecurity IPS in various locations within the network. This layered approach provides comprehensive protection against both internal as well as external cyber threats.

Illustration 1 shows key IPS placement options as indicated by the numerals 1, 2, 3, and 4.

1. Behind the network perimeter firewall and any VPN terminations.
2. Between the network perimeter firewall and DMZ-based servers such as Web and email servers
3. In front of critical internal assets such as application servers
4. In front of key departmental workgroups

IPS *Defense in Depth* Deployment Options

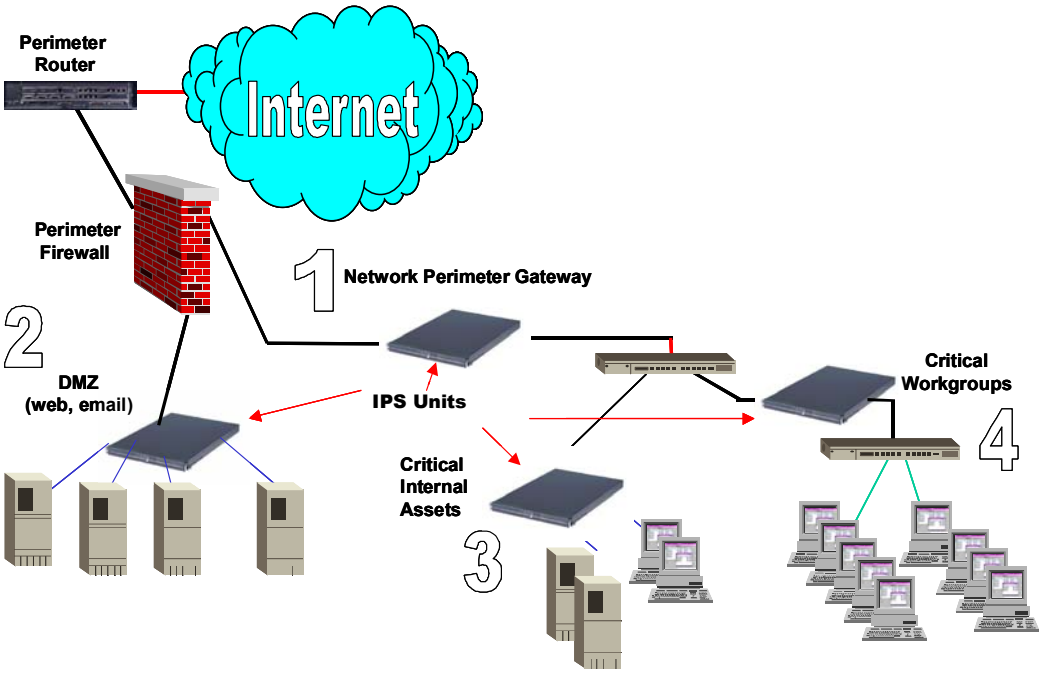

Illustration 1– Potential IPS Deployment Options

Evaluation Criteria

This section suggests the top five high-level feature categories that users should test and evaluate when verifying a vendor's product for its ability to perform as an effective intrusion prevention system. An IPS should be able to perform the following functions:

- Offer flexibility in deployment options
- Have a comprehensive suite of field proven attack blocking mechanisms
- Perform at "wire speed" when under attack and heavy user traffic load
- What redundancy options for high system availability
- Be easily manageable locally or remotely

Below are examples of features and functions for consideration during IPS evaluation

Deployment Options

- In-Line deployment with all rule sets disabled.
- In-Line deployment with all rule sets turned to passively detect only
- In-Line deployment with rule sets features set to block attacks
- Dedicated internal and external network ports for traffic isolation
- Ability to be deployed in a wide range of topologies
- VLAN support: standards based (IEEE 802.1q) or vendor specific (Cisco ISL)

Attack Blocking Mechanisms

- Layer 2 bridge filtering functions
- Layer 3 address blocking
- Blocking based on TCP/UDP Port numbers or a combination IP address and TCP/UDP Port Numbers
- Blocking single packet attacks
- Blocking ICMP Flood Denial of Service attacks
- Blocking SYN Flood Denial of Service (DoS), Distributed Denial of Service (DDoS) attacks
- Blocking unsolicited ICMP echo response communication
- Blocking TCP packets with bad packet formats, flag usage
- Blocking Illegal IP Fragments
- Ability to handle/ re-order TCP segments; IP fragments
- Ability to safeguard internal operations against intentional misuse
- Blocking IP packets that use illegal Options settings
- Blocking HTTP requests with malformed METHOD
- Blocking HTTP requests with buffer overflow exploit
- Blocking HTTP requests with buffer overflow exploit when:
  Exploit is distributed across multiple packets
  Exploit is created with modified encoding techniques
- Blocking unwanted peer to peer (P2P) traffic
- Ability to perform outbound content filtering as to protect against illegal distribution of intellectual property or worm/ virus propagation.
- Ability to define custom signatures for use with IP, TCP, or UDP packets

Performance

- Minimal throughput impact at high connection setup/ teardown rates
- Connection setup/teardown rates
- Low latency across a range of packet sizes and transmission rates

- Blocking Denial of Service (e.g. SYN Flood) attacks while maintaining acceptable end user application response times

Redundancy

- Ability to operate with single cooling fan failure
- Redundant, hot swappable fan units; power supplies

Management

- Central management console for local and remote IPS systems
- Data base engine for high performance query and report generation
- Centralized event logging and correlation for remotely dispersed IPS systems
- Ability to perform software updates for multiple systems from a central location
- Ability to select manual or automatic signature updates for deployed systems

Summary

The need for pervasive access to the Internet to perform business is greater than ever. With this access come the risks of threats from both within and outside of an organization. Despite an increasing volume and complexity of such cyber attacks, protection solutions such as NitroSecurity are available on the market today. NitroSecurity IPS products proactively prevent undesired/unauthorized access and stopping network attacks such as denial of service, application overloads, as well as exploitation of other critical vulnerabilities by hackers, worms, viruses, and other malicious traffic.

Securing networks is NitroSecurity' core competence. As such, the NitroSecurity IPS solutions deliver comprehensive *in-line protection*, which is a critical part of a defense in depth strategy. Furthermore, they are designed to be *cost effective,* utilize *field proven blocking mechanisms*, and provide *demonstrable* ROI. This ROI is a direct result of blocking attacks before they occur while maintaining business operations, continuity, and IT operations staff productivity while providing a safer, more secure network environment.

This paper has been brought to you by Cressida Technology, NitroSecurity exclusive European Distributors. To contact Cressida please email us on info@cressida.info or please visit our site for a http://www.cressida.info/ContactUs.htm listing of our pan-European sales and support contact information.