Introduction

The boundaries of enterprise networks are disappearing. There is no longer just a single path into the enterprise; instead branch offices and remote users access internal networks via VPNs, they embrace new applications like instant messaging that open additional communication paths, and as wireless LANs proliferate, the air itself allows entry into the network. It is no longer enough to simply harden the perimeter to provide security, because the perimeter has become so porous and dynamic, it is in effect disappearing. At the same time, network threats are increasing, both in number and in sophistication.

The traditional host-based approach to internal security, while still required, is not sufficient. There are too many hosts and too many vulnerabilities for IT administrators to keep up. What is needed is a focus on network-based security and making the network the first line of defense.

In the absence of a clear border that can be policed, all traffic, including internal traffic, must be inspected and subject to stated security policies. There have been few attempts implementing network-based internal security because the available solutions have been either too expensive or unacceptable because of performance degradation. New developments in security technology strive to overcome the cost and performance challenge.

**This paper discusses iPolicy Networks’ next generation Single-Pass Architecture, a new architectural approach that is enabling a new generation of network security platforms that are cost-effective in protecting all network communications while supporting multi gigabits per second throughput. Third-party lab tests show the remarkable performance advantage of iPolicy Networks’ architecture compared to current generation security solutions.**

The Disappearing Perimeter

As enterprise networks become increasingly distributed and global, relying only on perimeter security puts your organization at risk. Virtually all the Fortune 2000 companies have deployed firewalls to secure their networks, yet they are constantly plagued by worms, viruses, and mobile malicious code. Many security threats, such as worms, either pass through traditional firewalls, or find their way in undetected. Worms on infected internal hosts then spread to other susceptible systems, and may initiate coordinated attacks on internal or external information resources.

Paths into and out of the network are as diverse as the enterprise itself. The perimeter defining the edge of the enterprise network is vanishing, as connectivity is extended to partner extranets, distributed global offices, and to remote workers entering the network via VPNs. The physical walls of the enterprise can no longer be identified with a network access perimeter either. Workers, guests, contractors bring in laptops and mobile devices that are then connected and become part of the internal network. New applications like instant messaging create new application-layer entryways, while the proliferation of wireless LANs means that even within the physical walls of the enterprise itself, you can no longer be certain that the internal “trusted” network is walled off from the external world.
The traditional approach to defending an enterprise’s computing resources and information assets that hinges on strengthening perimeter defenses, is quickly becoming ineffective. Indeed, some estimates now show internal threats accounting for as much as 70% of all network security incidents and self-propagating worms and malware are the primary cause of the increase. The urgency to bolster internal security has risen sharply.

**Host-Based Solutions Alone Cannot Secure Internal Networks**

When it comes to internal security, most organizations focus on defending the end points. Hardening the host, patching vulnerabilities and installing up-to-date software revisions are important steps. Deploying host-based security tools—such as access control mechanisms, anti-virus programs, and personal firewalls—further protect individual servers and clients.

Keeping all the hosts protected all the time, however, has proven to be a huge IT challenge. The sheer number of hosts to protect, the multitude of applications and operating systems each with their own vulnerabilities, and an increasingly mobile and distributed work force create a security management nightmare. New security patches and new antivirus signatures are released constantly. How can the network administrator be sure that all end users have updated their devices, or that all known system vulnerabilities on corporate servers have been patched? It’s a nearly impossible task. And, indeed, according to the CERT Coordination Center, up to 99 percent of all network intrusions exploit known vulnerabilities or configuration errors, for which countermeasures were readily available.

Host-based security is very important and will remain a critical element in a layered defense strategy. But since attacks and harm can only spread to other information resources using the network infrastructure, the internal network itself should be made the first line of defense. By stopping attacks and malware while carried over the network in real time, all users and all information assets in the enterprise will be protected.

**More Threats, More Complex Threats**

It is a fact that network security threats keep increasing, both in number and in sophistication. Hackers exploit vulnerabilities in networking protocols, operating systems and applications, many of which were not designed with security foremost in mind. Fast-propagating worms, application-layer attacks, and blended multi-headed threats are increasingly common. The time between when a vulnerability is communicated and an exploit is unleashed has shrunk from months to weeks. Every new application deployed carries the potential of opening a new set of vulnerabilities. Experts anticipate the continued emergence of new types of threats for the foreseeable future.

To protect their networks, network administrators have been forced to deploy a range of specialized security solutions – DoS/DDoS mitigation devices, virus scanners, intrusion detection and prevention systems, content filters, to name a few. Separate point solutions are ill-suited to combat blended attack. Since the various protection tools come from different vendors and there are no interoperability standards, there is little opportunity for a coordinated response. Stopping the spread of the Nimda worm, for example, requires anti-virus, intrusion prevention, and dynamically hardening the firewall.

The security challenge is compounded because protection can no longer be ensured by a perimeter defense strategy alone. Devastating worms such as Code Red, Nimda or Sasser can spread from internal as well as external networks. The Blaster worm has infected countless systems on internal networks that were believed well protected. Unsuspecting users with infected laptops had physically carried the worm into the enterprise, or made a VPN connection to the internal LAN.
Network-based Internal Security Has Been Elusive

In theory, the same technologies used to inspect traffic and enforce security at the perimeter should be applicable to internal network paths. The reality is quite different. Performance, breadth of security, manageability and cost issues have been critical impediments. Until now, the vision of network-based internal security could not be realized.

The performance challenge is not trivial. Security devices designed for perimeter service perform well at WAN speeds. Compared to LANs, WANs are slow. Even expensive T3 trunks do not exceed 45Mbps. By contrast, most internal LANs run at 100Mbps and backbone networks carry multi-Gbps traffic. While security is paramount, a network-based solution cannot degrade business performance. An internal security device deployed in line must perform at multi-Gbps in order to secure internal trunk connections and be transparent to users.

The breadth and depth of security requirements is another challenge. Protecting the network means stopping all forms of attacks and security breaches. Many threat-specific security devices have been developed, each designed to overcome a particular security risk. Traditional layer 3 and 4 firewalls are giving way to deep-inspection firewalls that enable application parameter-level control. There are proxy servers, DoS mitigation devices, passive IDS and in-line IPS devices, anti-virus scanners, SPAM blockers, URL filters, etc. Individually, each device may do a fine job doing what it was designed for. However, deploying the necessary suite of specialized point products to meet all security needs adds much complexity. Furthermore, each in-line device impairs network performance and the cumulative negative impact quickly becomes unacceptable. An imperfect solution when used for perimeter security, the specialized device strategy is unfit for internal network security.

A series of standalone security point products can quickly generate management overload. Each device relies on its own management platform that must be learned and mastered by the network administrator. Each device must be configured and monitored through its own management interface. Furthermore modern blended threats that combine aspects of worms, Trojans, viruses, etc. cannot be dealt with in a holistic way and with a coordinated response, since the various defense mechanisms are unaware of each other.

Last but not least, the cost of providing security needs to be justified against the potential losses that a successful attack might inflict. These costs include the acquisition and deployment costs of multiple devices and of their respective management platforms, personnel training costs, maintenance costs, and ongoing cost operating so many systems. Performance concerns notwithstanding, the cumulative cost of deploying all the necessary discrete point solutions has made network-based internal security unfeasible.

Performance and Scalability Challenges of the All-in-One Appliance

In response to the diversity of threats and to users’ objections to the proliferation and associated costs of point solutions, security vendors have begun concentrating security functions into single physical appliances. Fortinet was an early proponent, but many established security vendors are heeding the call and have announced multi-function security products.
All-in-one security appliances have brought down the acquisition and the management cost of security. By and large, however, they remain perimeter solutions because they do not achieve the order of magnitude performance gain needed to be viable for internal network security service.

At first glance, some all-in-one security appliances tout impressive performance, some claiming gigabit/second throughput. However, the high performance number is typically a best case number, achieved with only one security application such as the firewall active. More relevant is performance when used as intended with all security functions enabled. **As more security functions are activated, the throughput of most current generation all-in-one appliances falls off sharply, some by a factor of 10 or more as illustrated by actual performance measurements reported later in this paper.**

Fundamentally, current generation all-in-one security appliances have not broken new technical ground. They may have collapsed the physical boxes into a single box; they have not integrated the logical security functions. In essence, each security function -firewall, IDS/IPS, VPN, URL filtering, Anti-virus, etc.- still runs as a distinct application. Each program inspects the packet based on its need, then applies its security rules, then passes it on to the next program and the cycle is repeated. The sequential nature of this process and the repeat packet inspection and processing it entails contribute to the severe performance drop. Measured results provided in a later section of this white paper support this assertion. Increasing the CPU power provides only limited performance relief.

Scalability is another rightful cause for concern. The number of threats, and hence the size of the knowledge base for a particular class of attacks –worm and virus signatures for example- keep expanding. Current architecture products cannot cope with expanding data bases. Most multi-function security devices available today can only handle a limited set of IPS/IDS signatures or URLs for example.

Another critical aspect of scalability is the performance impact of adding new security applications. History to date suggests that new types of threats requiring new defense mechanisms will keep emerging. For the conventional architecture, that means yet more applications need to inspect and process the traffic, resulting in further performance erosion.

It is no wonder then that despite the advent of all-in-one security boxes, most attention is still placed on perimeter security. Network-based internal security remains a goal, but is it an unattainable goal?

**The Emerging Any-to-Any Security Architecture**

Security analysts concur with the pressing need for internal security, and have acknowledged the technical challenges that need to be overcome.

“The evolution of various computing technologies has added dramatically to both the actual and potential paths into an organization’s network making internal security a necessity,” said Mark Bouchard, senior program director at META Group, a leading provider of IT research, advisory services and strategic consulting. “Fortifying internal networks involves overcoming challenges of scale, the wide variety of applications and protocols to support, management of multiple types of users and the need for greater speeds, and high volumes of traffic. Many of today’s conventional security products are not well tuned to meeting these challenges. **Organizations need enhanced security solutions that go beyond perimeter security and deliver the high-performance, breadth and depth of defense mechanisms, and flexible management to address the requirements for internal security.**”

Because the perimeter is vanishing, there is a growing need for a new kind of security platform. A twenty first-century security architecture has to protect a network with no boundaries, that provides employees, business partners and customers access to the specific computing resources they need to do their job, whether
they are based in the same building, at a remote site or on the road. **There is no alternative but to inspect and enforce security policies and to provide safeguard against attacks on any-to-any network traffic.**

Most companies have implemented a physical star internal network topology. Physical network connectivity is from the device to the wiring closet. Internal traffic, including peer-to-peer traffic travels to core switches or routers that redirect the packets to the intended destination. These points of traffic accumulation are where network-based internal security needs to be enforced. Every packet and each connection, whether destined to or coming from an internal user, the data center, the DMZ or the Internet, must be inspected for safety and subjected to the applicable security policy. By inspecting traffic on the trunks of core switches and routers, attacks originating from a compromised system or from a potential intruder can be identified and stopped and traffic from infected systems can be quarantined to prevent worms from spreading to the rest of the organization. Figure 1 illustrates the concept of an any-to-any network-based security solution.

![Network-based Security Model](image)

**Figure 1. Network-based Security Model**

But, as stated previously, security cannot be allowed to impede business processes. Modern enterprises rely on high-speed efficient network communications, and users will not accept a network-based security solution that is not transparent to them. **With today’s networks multi gigabit per second throughput is required with all security functions enabled.** So is the ability to maintain very large number of connections while still being able to service many new connection requests per second. The latter is important to enable legitimate traffic connections to be established while mitigating a DoS attack, for example.

**First generation of all-in-one security appliances do not meet the critical performance constraint, and thus are not suitable for internal security.** Fundamentally, this is because they have not taken a new approach to addressing the multi-function security problem.

Breaking with conventional thinking, iPolicy Networks aimed for a new approach, one that addresses the multi-faceted security challenge in a holistic way. The quest led to a new software architecture, one that does not compartmentalize security into discrete sequential applications. **The new thinking is embodied in the Single Pass Architecture.** As a result, iPolicy Networks’ solution does not suffer from the shortcomings of the first generation all-in-one security boxes and opens the way to network-based boundary-less security.
The Single Pass Architecture

The conventional comprehensive security model performs each security function sequentially and independently, with no knowledge of any prior or subsequent step. This is true whether security is implemented using a set of discrete point products or within the confines of a single physical box as is the case for the first generation of all-in-one appliances. Each security application enabled must inspect the packet, compare the results to its rule tree, reach its decision and activate its response. All these processes consume CPU cycles and add latency.

iPolicy Networks has taken a unified approach to comprehensive security. It has conceived of the Intrusion Prevention Firewall as a single integrated application designed from the ground up to incorporate all the security functions and to be extensible for additional security requirements in the future. The security functions are no longer distinct applications. All defense mechanisms, once selected, are performed as part of an integrated highly efficient process.

This new generation of Intrusion Prevention Firewalls combines a layer 3-7 firewall, performs IPS/IDS, mitigates DDoS attacks, protects against worms, filters content, screens URLs, enables surveillance, etc. It has been designed to be extensible, to add protection against new emerging types of attacks, such as phishing attacks.

The core technology is the Single Pass Architecture and is illustrated in Fig 2.

![Diagram](image)

**Figure 2. Single Pass Architecture**

The Single Pass Architecture model starts with a Single Pass Inspection Engine. Each packet is inspected once, and only once, and the content analysis from this deep inspection supports all enabled security functions.
In the next step, the results of the inspection are matched against a single pass, integrated and highly optimized rule tree. The integrated rule tree embodies the power of the Single Pass architectural approach.

In this architecture, the rule compiler distills a single highly-optimized rule tree using all the security policies that have been defined and all their supporting knowledge bases: access control policies, worm and attack signatures, protocol and traffic anomalies, URL lists, etc. All policy and rule matches are performed against the unified rule tree in parallel, at very high speed in a highly efficient process. With a Single Pass Architecture execution time for multiple security applications is virtually the same as for a single application. Single Pass implementations are thus virtually immune to increases in defense mechanisms. More types of rules get compiled, but the end result is still a single optimized rule tree.

Following a rule or pattern match, the enforcement engine uses enforcement rules to take appropriate action in real time. For example, it determines if the packet should be allowed to pass or dropped, if it should be logged, if an event or alarm should be generated. It determines if the source IP address should be quarantined, or a session reset.

A blended attack typically results in multiple concurrent rule matches: a firewall rule, an IPS rule, a behavioral rule. Each match will trigger an appropriate response. Thus, inherent to the Single Pass architecture is the correlation of threats and the resulting coordinated multi-faceted response that will thwart blended attacks in real time. This is a powerful and distinct advantage for the Single Pass architecture. Indeed, the inability to support coordinated responses in real time has been identified as a major shortcoming of the conventional approach that uses a series of point products.

When security is defined and enforced through a unified platform, security management is greatly simplified. All the security functions, firewall, IPS, IDS, URL filtering, etc. can be enabled, configured, monitored, logged using a consistent interface and using only one management platform. The result is enhanced security with greatly reduced management and operating costs.

The Single Pass architecture represents a new unified approach to network security, one that overcomes the low performance, long latency, interoperability problems and management shortcomings of the first generation all-in-one security devices and of otherwise disparate point solutions.

The following section provides evidence on the relative performance of a multi-function security platform representing the conventional architecture and the iPolicy Networks platform based on the next generation Single Pass architecture.
Comparing the Performance of a Security Platform based on the new Single Pass Architecture versus the current Architecture

iPolicy Networks has commissioned the Tolly Group to compare the performance of a multi-function security platform based on current generation architecture with the iPolicy Networks security platform based on Single Pass architecture. The measurements were to help assess the suitability of either solution for internal network security, when all security functions are enabled.

Fortinet’s FortiGate product line is the best representative of the current generation all-in-one security platforms: the FortiGate product series includes firewall, IPS/IDS, URL filtering and antivirus scanning functionality. Our focus on meeting the demand of internal security, which requires multi gigabit throughput led to the selection of the FortiGate-3600, which is rated at 4Gbps throughput and supports one million concurrent sessions.

For the Single Pass architecture-based model, the iPolicy-6400 series Intrusion Prevention Firewall was selected. The iPolicy-6400 Intrusion Prevention Firewall is rated at 4 Gigabit /second throughput, supports one million concurrent sessions and delivers firewall, IPS/IDS, URL filtering and antivirus scanning functionality.

The ability to sustain high throughput is one of the most important requirements for internal security. Figure 4 shows that with all security functions are enabled the FortiGate-3600 drops a large number of frames when subjected to 4Gbps traffic. This means the throughput has fallen to only a fraction of the rated throughput value of 4Gbps.

Figure 4. Tolly Comparison, UDP frame loss, iPolicy-6400 versus FortiGate-3600
The iPolicy-6400 shows near-zero frame loss under the same conditions including for traffic that simulates the Internet packet size mix (IMIX), meaning that it maintains its rated 4Gbps performance with all defense mechanisms active.

To meet internal enterprise connectivity requirements, an internal security solution must also be able to support both a large number of sessions and a high new connection rate.

![930,000 Active Connections and 15,000+ New Connections per Second](chart)

Figure 5 shows that FortiGate-3600’s ability to complete new connections or transactions in the presence of 930,000 active sessions falls of sharply when all security functions are enabled.

The iPolicy-6400 solution completed all transactions when subjected to 15,000 new connections attempts per second. The performance was maintained with all security functions enabled.

The full report is available at [www.ipolicynetworks.com/docs/tolly-report](http://www.ipolicynetworks.com/docs/tolly-report)
Realizing the Boundary-less Network Security Vision

Enterprises can now avail themselves of a security solution that delivers internal and external security at multi gigabit performance, with flexible yet powerful management and at an affordable cost. These requirements could not be met running discrete security applications on a multi-function appliance that is based on today’s architecture.

Performance degradation occurs as additional security functions are enabled, a limitation inherent to the conventional architecture. The Single Pass architecture invented by iPolicy Networks overcomes this limitation. In particular, the iPolicy-6400 intrusion prevention firewall meets the requisite performance, breadth and depth of security, manageability, and cost requirements for internal security. Figure 6 illustrates a network-based security solution that leverages the new generation security platform.

The iPolicy Networks Advantage

iPolicy Networks offers a complete line of network security products that protect corporate enterprises, managed security service providers and government agencies from emerging forms of security threats and network attacks while maintaining the best possible network performance and at a substantial reduction in total cost of ownership.

The iPolicy Intrusion Prevention Firewall incorporates multiple firewall defense mechanisms built into a single, high-performance security platform. This platform is one that analysts have been anticipating. In June 2003, Gartner predicted that traditional perimeter firewalls would be replaced by deep-inspection firewalls with multiple security features integrated into one platform.
The iPolicy Intrusion Prevention Firewall provides multiple correlated security services including layer 3-7 stateful firewall, intrusion detection, intrusion prevention, DDoS and attack mitigation, URL screening, surveillance and anti-virus. It is readily extensible to protect against new threats.

Additional distinctive features of the iPolicy Networks solution are the support for Security Domains and for hierarchical, policy-based management through the iPolicy Security Manager (ISM). Security Domains allow to manage enterprise security as virtual security platforms that can span multiple physical devices and geographies, each associated with its own policies and security rules. ISM provides flexible, scalable management options, including the implementation of a centralized, hierarchical or shared management model.

Key benefits of the iPolicy Networks solution are high performance, virtually unaffected by the number of rules or the number of defense mechanisms enabled, low latency, scalability, and real-time protection against attacks, all in a cost-effective package.

For additional information, please visit www.ipolicynetworks.com

**Conclusion**

As the enterprise boundaries disappear, traditional perimeter solutions can no longer be relied upon for security. In order to secure an organization’s internal assets, what is needed is any-to-any network-based security. Strong security implies inspecting all traffic, be it external or internal and applying many defenses to thwart, in real time, attacks from an increasingly diverse and growing number of threats.

Any-to-any traffic inspection and comprehensive security policy enforcement requires a high-performance, integrated solution that is cost-effective. The Single Pass Security architecture is the breakthrough that enterprises have been waiting for. Lab results show that it overcomes the limitations of solutions which are based on current generation architecture such as Fortinet’s. The Single Pass security architecture allows the synergistic combination of many security functions into a single platform, with no noticeable performance impact when additional security functions are enabled.

iPolicy Networks is proud to have been first in delivering a new generation of Intrusion Prevention Firewalls that meet the boundary-less security challenge.