



WALTER HUNTER MONTGOMERY FLAGG

I WANT YOU FOR C.I. ARMY

NEAREST RECRUITING STATION



WWW.NETWORKCLOAKING.COM



“The era of the stand alone defense is giving way to the collective.”

Marc Seybold CIO SUNY-Old Westbury

The story behind
Sentinel IPS™ with Collective Intelligence

Using Sentinel IPS and Sentinel EPS to Prevent Intrusions, Remediate Antivirus Software Failures and Stop Malware Uploads/Downloads from Your Internal Network

by

David A. Lissberger
President and CEO
Sentinel Intrusion Prevention Systems

ABSTRACT

This paper explores the use of collective intelligence with sophisticated intrusion prevention technologies, but is accomplished in a way that both technical and non-technical readers can appreciate. Although Sentinel IPS products are discussed openly, it is the security concepts themselves that have great value for the reader in understanding the defense of any network.

Sentinel IPS^(ci)™ is the most affordable Intrusion Prevention System available, and the only one that has Network Cloaking™. Sentinel IPS™ utilizes Network Cloaking, a technology that makes your protected network invisible to malicious external traffic, while allowing complete and uninterrupted access for legitimate users. Sentinel IPS is everything you need for state-of-the-art Intrusion Prevention in one affordable, fixed monthly fee, including the appliance, our security management service, 24/7 monitoring, unlimited support, update services, upgrades, and enhancements, starting at only \$299/month.

You have the right to be secure. We believe this right includes your network and that you have the right to operate your network free from the threat of intruders. The single focus of our company is protecting your right to be secure. It is why we are here. It is rooted in an understanding that if the bad guys harm you, they have also harmed me. Who we are, is that they not prevail. We will win this challenge, by working together and sharing our knowledge. Make a difference for others by sharing this information, and enroll them in the movement to be secure.

Collective Intelligence (CI) is not new. Similar ideas have been illuminated as far back as a concept of a 'group mind' derived from Plato's concept of panpsychism (that mind or consciousness is omnipresent and exists in all matter). In the discussion that follows Wikipedia is utilized as a source of reference information regarding the definition and attributes of CI. Wikipedia material is identified by the emphasized text and is cited as follows:

Wikipedia contributors. "Collective intelligence." *Wikipedia, The Free Encyclopedia*. Wikipedia, The Free Encyclopedia, 6 Feb. 2010. Web. 4 Mar. 2010.

It seems appropriate that Wikipedia be a reference for CI, as most will agree that it is in and of itself, a medium that fully displays the concepts encompassing collective intelligence.

Collective intelligence is a shared or group intelligence that emerges from the collaboration and competition of many individuals. Collective intelligence appears in a wide variety of forms of consensus decision making in bacteria, animals, humans, and computer networks. The study of collective intelligence may properly be considered a subfield of sociology, of business, of computer science, of mass communications and of mass behavior—a field that studies collective behavior from the level of quarks to the level of bacterial, plant, animal, and human societies. The concept also frequently appears in science fiction as telepathically linked species and cyborgs.

Linked cyborgs? What about linked computers or linked networks of computers, aka. the internet?

Collective intelligence (CI) can also be defined as a form of networking enabled by the rise of communications technology, namely the Internet. Web 2.0 has enabled interactivity and thus, users are able to generate their own content. . . . Collective intelligence is not merely a quantitative contribution of information from all cultures, it is also qualitative.

We will later discuss the integration of CI into our intrusion prevention systems, but for now let's make a distinction between quantitative and qualitative intelligence. CI can be used quantitatively to collect attack information, which is quite valuable in defending networks, but imagine utilizing CI to provide meaningful context to that data. Utilizing heuristics, identifying anomalies, and mitigating false positives are qualitative activities, not quantitative. Utilizing the power of CI with regard to internet security is quite a compelling idea for our company, because it gives us a window into how the bad guys think and the remediation strategies which are most effective, not just the history of their attacks.

One CI pioneer, George Pór, defined the collective intelligence phenomenon as "the capacity of human communities to evolve towards higher order complexity and harmony, through such innovation mechanisms as differentiation and integration, competition and collaboration." [2] Tom Atlee and George Pór state that "collective intelligence also involves achieving a single focus of attention and standard of metrics which provide an appropriate threshold of action". Their approach is rooted in Scientific Community Metaphor.

The single focus of our company is protecting your right to be secure. It is why we are here. It is rooted in an understanding that if the bad guys harm you, they have also harmed me. That they not prevail is at the core of our being. The internet is the epitome of interconnectedness. We are in fact, one global community of users and

producers. In Ubuntu culture, safeguarding the collective provides protection of the individual.

Ubuntu speaks particularly about the fact that you can't exist as a human being in isolation. It speaks about our interconnectedness. You can't be human all by yourself, and when you have this quality - Ubuntu - you are known for your generosity. We think of ourselves far too frequently as just individuals, separated from one another, whereas you are connected and what you do affects the whole world. When you do well, it spreads out; it is for the whole of humanity.

Early in 2002, Econet.com, Inc. began construction of a network of Intrusion Prevention Systems (IPS) of our own design. This was at a time when intrusion detection was “state of the art”, and IPS was limited to labs and a few commercial attempts, but generally IPS devices were criticized for their non-workability. Sentinel IPS units were much differently designed and well liked by our customers because they were fast, highly effective, and we did all the management, maintenance, and monitoring for them. We originally thought we were networking the IPS units so we could manage them more efficiently. What we quickly realized was that this very unique and special network had the capacity to provide qualitative information, harness the wisdom in collective behavior, and learn what the bad guys are doing.

Levy and de Kerckhove consider CI from a mass communications perspective, focusing on the ability of networked ICT's to enhance the community knowledge pool. They suggest that these communications tools enable humans to interact and to share and collaborate with both ease and speed (Flew 2008). With the development of the Internet and its widespread use, the opportunity to contribute to community-based knowledge forums, such as Wikipedia, is greater than ever before. These computer networks give participating users the opportunity to store and to retrieve knowledge through the collective access to these databases and allow them to “harness the hive” (Raymond 1998; Herz 2005 in Flew 2008). Researchers[3] at the MIT Center for Collective Intelligence research and explore collective intelligence of groups of people and computers.

“Harnessing the hive”, is a great metaphor for utilizing the quantitative and qualitative intelligence of the Sentinel IPS user network for the benefit of all the participants. Members of the Sentinel IPS community of users, help protect one another through their enrollment, participation, and diligence in securing their own networks. Tens of thousands of individual security decisions are executed by network managers using the latest intrusion prevention technologies, then harnessed and directed at defending those networks and continuously updated every 30 minutes around the clock. Imagine the power of working in unison with IT managers around the world protecting your right to be secure.

We define CI as it relates to intrusion prevention as a human network composed of Sentinel IPS end users combined with an infrastructure described as follows.

Sentinel IPS^(ci)™ is a networked IPS device, managed and monitored by Econet.com, Inc. The function of the device is based upon a group of technologies, methodologies, and strategies integrated into a holistic approach for protecting private networks from intrusions and failures in antivirus and malware protection. Each Sentinel IPS^(ci) device is a node on the Sentinel IPS Management System (SMS) private secure wide area network (WAN). The SMS

WAN and its users function as a collective intelligence network that supports the security efforts of each individual, and utilized by all. When a bad guy attempts to harm an individual Sentinel IPS user, the attack is defeated, and the intelligence is shared by the collective. In many cases, this allows networks that are protected by Sentinel IPS^(ci) to be immune to an attack, because it has been defended preemptively.

Network Cloaking™, DPAM, and EPS are three important technologies that support our CI efforts. We will discuss them briefly, but more detail is available via our corporate website. CI and its integrated technologies provide a superior security posture against intrusions for sure, but it also solves a critical processing problem that has been raised by security evangelists. That being a point in time whereby improvements in IPS technology will no longer keep pace the amount of data that must be analyzed for networks to remain protected. More on this later, but let's take a brief look at three important intrusion prevention ideas at the heart of our CI efforts.

1. Network Cloaking™ (nĕt` wûrk` klōk`-ing)

n. 1. A combined technology and methodology that prevents network intrusions by making protected networks invisible to malicious external users.

v. 2. The act of utilizing the Sentinel IPS™ to protect a network.

Etymology: Created in 2002 by **econet.com, Inc.** to describe the functionality of their Sentinel IPS™ product.

Or said another way, Network Cloaking is a technology that makes your protected network invisible to malicious external traffic, while allowing complete and uninterrupted access for legitimate users.

External vulnerabilities pose a special type of threat for private networks, because this type of vulnerability is ubiquitously available and exploitable. Quite literally, a world of exploitable possibilities exists and "Network Cloaking" is one of the most powerful tools available in preventing intrusions into private networks. Hackers cannot determine if the Sentinel Protected network is "cloaked" and if they attempt to determine if such may be the case, their attempt becomes the cause of their inability to make the determination. If a non-malicious user initiates a malicious act against a "Sentinel Protected Network", then Sentinel will automatically engage Network Cloaking as a defense against that user. It is this feature that makes it highly unlikely anyone can port scan, or stealth port scan, a Sentinel Protected Network. They can't hack what they can't see.

Sentinel IPS is able to inspect and drop packets so fast that the destination IP address appears unused to the offender. This means that the packet is inspected, correlated, the event logged, a copy of the packet recorded for administrative use, the network admin is alerted, the packet is dropped, and a new rule is written preventing the source IP from communicating with the Sentinel Protected Network before the packet can leave the Sentinel Appliance. This is accomplished so quickly as to be imperceptible to the users of the network.

Sentinel IPS protected networks are regularly penetration and vulnerability tested by certified Authorized Scanning Vendors, known as ASV's. The diagram that follows shows the result of such a scan.

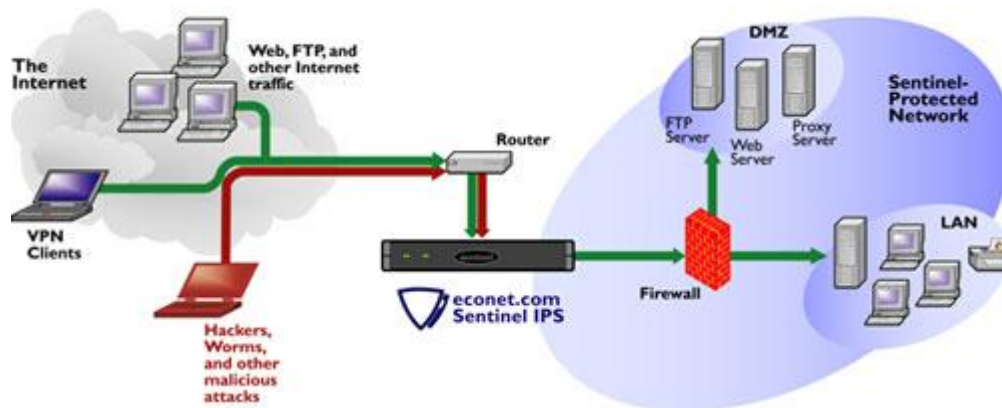
COMPLIANCE DASHBOARD

Network Scan Vulnerabilities		
	0 High Vulnerabilities	You do not have any high-severity security vulnerabilities in the systems included in your scan.
	0 Medium Vulnerabilities	You do not have any medium-severity security vulnerabilities in the systems included in your scan.
	0 Low Vulnerabilities	You do not have any low-severity security vulnerabilities in the systems included in your scan.
	0 Informational Vulnerabilities	You do not have any informational notices for the systems included in your scan.

2. DPAM™ (Distributed Pre-emptive Attack Mitigation)

DPAM is our methodology by which all the Sentinel IPS units act as detectors for malicious traffic and teach one another what IP's to block proactively. Built into each Sentinel IPS unit is an ability to gather information that may NOT be correlated to a specific attack profile, but might be malicious none the less. This is not a honey pot function, but rather like listening to the background noise that a noise-cancelling headset eliminates. As it turns out there is great value in looking at what goes unlooked at. We monitor this background traffic and utilize the intelligence contained within to assist in developing groups of IP addresses that should not be authorized to connect to Sentinel IPS protected networks.

Sentinel IPS units are in-line devices installed on premise, in front of the firewall, and not detectable themselves because they exist on the network as a layer 2 bridge, sometimes referred to as a promiscuous bridge. (See diagram below) Although the device has an IP address, the bridge function itself is independent of any IP address, so that no IP address can appear in a trace route and only the protected network can access the device directly. The combination of an undetectable defensive device providing Network Cloaking, firewall functions, and utilizing CI, allows an attack to be mitigated before it ever occurs. Many of the attacks a Sentinel IPS unit defends are from a bad guy that we learned about from another Sentinel IPS unit on the SMSWAN. Essentially, we gang up on them and everyone contributes.



3. Sentinel EPS: Extrusion Protection Sensor

It's not just the infrastructure that forms the CI Network, but also the Sentinel IPS user community. Users are also producers and together we defend our collective and individual right to be secure. As you might suspect there is a robust feedback mechanism at play, and Sentinel IPS customers are enormously creative. They also tend to have a sense of duty and are compelled to contribute to a noble cause. They lend their intellect and just as importantly, their "production networks" for the development of new methods to improve security. Sentinel EPS™ is the result of our collaboration with a university in New York and a city in Texas to affect a solution to one of the most difficult security issues now facing the security community.

Up To 9 Percent Of Machines In An Enterprise Are Bot-Infected

"In a three-month study of more than 600 different botnets found having infiltrated enterprise networks, researchers from Damballa discovered nearly 60 percent are botnets that contain only a handful to a few hundred bots built to target a particular organization. Only 5 percent of the bot infections were from big-name botnets, such as Zeus/ZDbot and Koobface."


Sep 24, 2009 | 03:59 PM By Kelly Jackson Higgins, DarkReading

With browser based attacks on the rise, the "bad guys" are now using a strategy that has an internal machine on the target network initiate a session with a machine they "own", allowing for a download of all sorts of malware. Since it is an internal request from the protected network, their firewall simply passes the traffic as valid, enabling the subsequent download containing key loggers, cracking utilities, spam servers, etc. These cleverly crafted exploits are designed to evade anti-virus programs and quickly spread across the LAN, propagated by "dirty" machines and infected USB drives.

Our customers' idea was simple, but elegant. As a gateway device, all internet traffic passes through the Sentinel IPS. If the Sentinel IPS could inspect the outbound traffic, we would be in a position to watch for this type of botnet activity. All alerts and blocks performed by the IPS are synced to NTP (network time protocol). By comparing these time stamps to other logging that the customer is doing, it should be possible to determine which machines are infected on the LAN side. Because NAT (network address translation) strips away the internal IP address of the botted host machine on

the protected network, it makes sense to utilize correlation of time stamps to identify which machine(s) are infected.

Early in 2009, we began development of the new outbound inspection engine and created new customized attack profiles for the attempts of a potentially compromised internal machines trying to contact botnet controllers. We refined the process so as not to degrade network performance, while continuing to improve the granularity with which we could inspect the outbound traffic. We began to see a payoff for our hard work and as fate would have it, the first few months of 2009 were very active for worm and Trojan propagation. New malware and variants of older malware were popping up everywhere so quickly the Antivirus vendors could not keep up. We decided to modify our code so that “phone home” attempts by infect hosts on the protected network would be blocked. This would prevent communication with botware controllers and other external malicious host machine on the internet. Now for the first time we had the capability to detect the AV failures and stop internal machines from “talking” to malware servers dead in their tracks. The following diagram is an example of how this shows up in real time reporting.



Tuesday, 6 October 2009 16:32:35 CDT

Sentinel IPS 3.0.0.0

home
sentinel management
statistics & reporting
support center
logout

Sentinel Management

Home > Sentinel Management > Current Blocked Networks

Current Blocked Networks

4289 blocked nets - 7 Filtered networks showing

Filter by :

page 1 of 1 [first](#) | [previous](#) | [next](#) | [last](#) per page

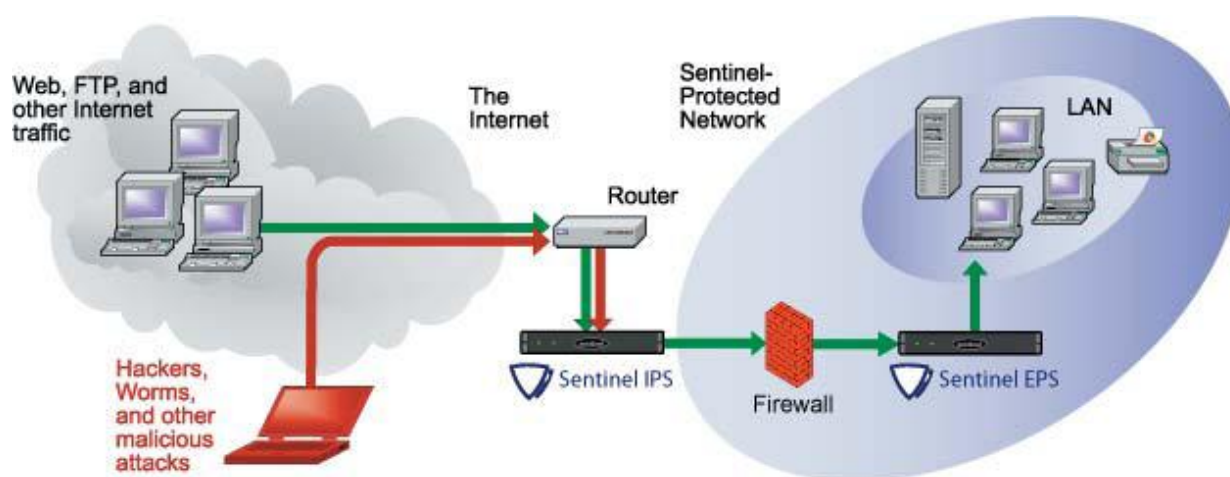
Network	Date Added	Last Packet Blocked	Priority	Attack Type
<input type="checkbox"/> release checked <input type="checkbox"/> release all <input type="checkbox"/> release filtered				
<input type="checkbox"/> 69.20.234.2/32	10/06/2009 08:18:03	10/06/2009 08:18:04		EPS: suspicious destination ip (group 17) whois references
<input type="checkbox"/> 69.72.236.188/32	10/06/2009 07:34:09	10/06/2009 07:35:43		EPS: suspicious destination ip (group 17) whois references
<input type="checkbox"/> 78.157.104.207/32	10/02/2009 22:15:53	10/02/2009 22:15:53		EPS: suspicious destination ip (group 22) whois references
<input type="checkbox"/> 208.87.149.251/32	10/01/2009 14:53:04	10/01/2009 14:53:22		EPS: trojan blink.com related backdoor checkin whois references
<input type="checkbox"/> 200.207.8.87/32	09/30/2009 15:04:11	09/30/2009 18:12:40		EPS: suspicious destination ip (group 3) whois references
<input type="checkbox"/> 64.208.176.19/32	09/30/2009 01:08:56	09/30/2009 01:17:17		EPS: trojan general dns changer checkin whois references
<input type="checkbox"/> 74.41.18.106/32	09/05/2009 17:48:17	10/02/2009 22:27:12		EPS: suspicious destination ip (group 20) whois references

page 1 of 1 [first](#) | [previous](#) | [next](#) | [last](#) [back to top](#)

All times are displayed in Central Standard Time (CDT).

[home](#) | [sentinel management](#) | [statistics & reporting](#) | [support center](#) | [logout](#)
 Sentinel IPS v3.0.0.0. Copyright © 2005-2008 Econet.com, Inc. All Rights Reserved.

For some network administrators the task of correlating EPS attacks to internal logging is enormously time consuming. Imagine trying to find the one machine on an internal network that is “owned” by a botnet out of 3500 devices in 16 buildings spread across a city of 300 square miles. Working with a city in Texas, we tested the idea of modifying our Sentinel IPS device to operate on the inside of a network. The result is Sentinel EPS, our Extrusion Protection Sensor. It runs on your LAN, and analyzes traffic originating from your network. If it identifies malicious traffic, it records the offending internal IP address and the type of attack. It is designed to supplement our Intrusion Prevention Systems (Sentinel IPS), so Sentinel EPS keeps an eye on your network’s internal infrastructure. The Sentinel EPS records malicious traffic originating from your network, giving you the power to identify potentially compromised machines on your LAN, while the IPS unit performs the remediation.



Let us now take a look at a couple of secondary contributions that are available through the integration and use of CI. In this discussion of CI, we need to make the distinction between improving versus transforming our approach to intrusion prevention technology. Improving security is important and worthwhile but recognize there is a limit to what is possible and that limit is systemic. It is imposed by an inherited past, past practices, past assumptions, and past ways of thinking. In transformation it is possible to disappear a problem, by transforming the context in which it occurs. Whether or not this is attainable in the world on intrusion prevention is open for debate, but the value of such a goal is not.

Hack attempts are not a problem in the context that they are completely ineffective and improving our existing approach to intrusion prevention security will NOT “get us there”. The transformative effects of applying CI to intrusion prevention are profound. We will look at two areas where upon the effects of the application of CI are transformational. The first is the methodology we use to prevent intrusions and the second is the constraints imposed upon the resources we use to prevent them.

A truth for network administrators is that they are simply “out gunned”. There are more resources deployed attempting to penetrate their network than they have time or money

to employ for its protection. Organized crime syndicates, identity thieves, industrial espionage agents, those attempting ransom, political spies, vandals, disgruntled employees, script kiddies, and cyber-terrorist, are just some of the types of bad guys that target private networks.

Chinese General, Circa 500 B.C.

“The ultimate in disposing one's troops is to be without ascertainable shape. Then the most penetrating spies cannot pry in nor can the wise lay plans against you.”

** Sun Tzu **

Over many years of successfully defending networks, this has proven to be an excellent security strategy. Without Network Cloaking, we are locked into a contest to defend our networks, whereby the bad guys invent new ways of penetrating the network, forcing us to respond with new countermeasures. Attack, countermeasure, the contest continuously escalates. The point being, it always ends the same way, we lose. It's time to change the rules. Instead of going “toe to toe” and working to counter each new threat with a new method of remediation, why not simply avoid the fight. Never engage the hacker in the first place. We believe CI, integrated with Network Cloaking, DPAM, and EPS transforms intrusion prevention so that the bad guy's time and energy yields no return on investment. That is how network intrusions will end, because the result of that activity is no longer worth the effort.

SANS is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center. The following excerpt is from the a SANS blog article.

Detection, Bandwidth, and Moore's Law

Posted by [mikecloppert](#) on January 5, 2010 – 1:15 pm

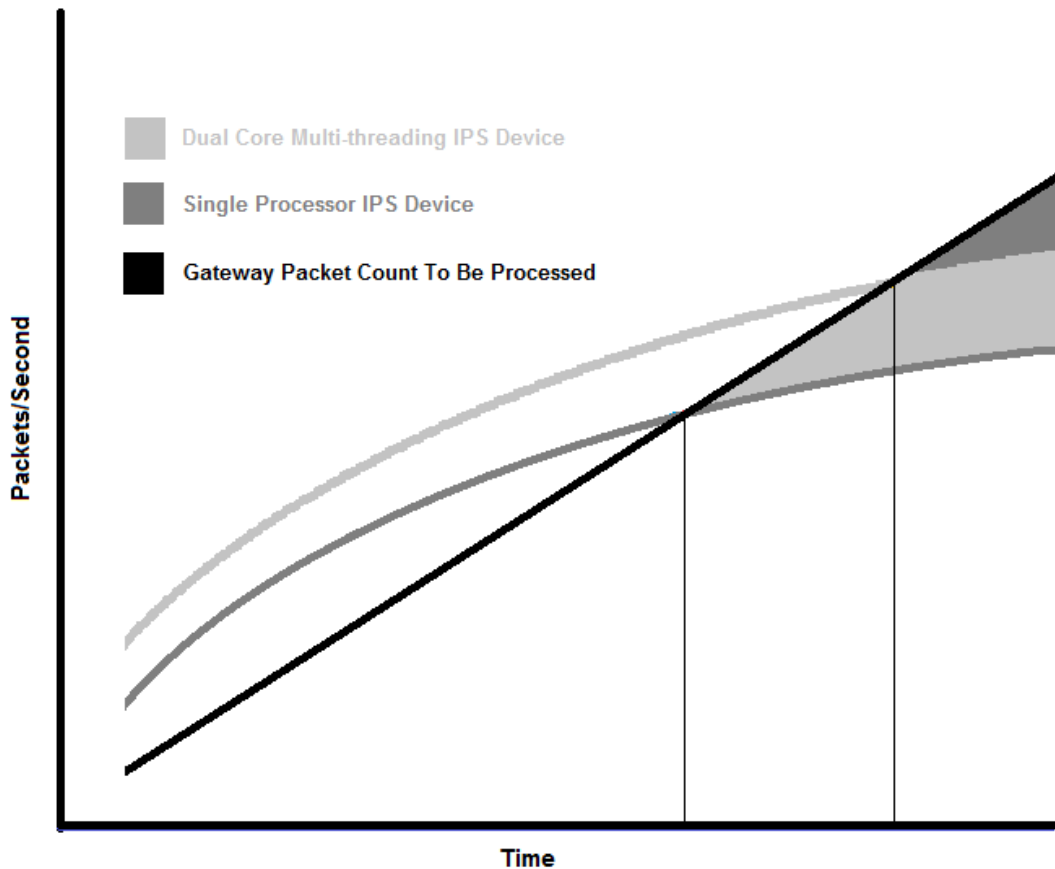
Filed under [Incident Response](#), [Network Forensics](#)

A Call to Arms for Intrusion Detection Software Innovation

For over a generation of professionals, Moore's Law has guided strategic planning related to computer hardware and software development. The security industry is no exception. However, there is a looming cataclysmic shift in the manifestation of this reality; one that requires the focus and attention of our vendors, lest our network analysis be left in the digital dust.

Network analysis is hard. Be it the real-time analysis expected of IPS devices, or the cached analysis which is badly needed but never provided by our vendors, our ability to detect hostility is constrained by four fundamental factors: what we look for, how we look for it, the amount of data we need to sift through to find it, and the computational power available to execute said detections. It is the interdependence of these last components that stands to most immediately and severely impacts our ability to analyze network traffic.

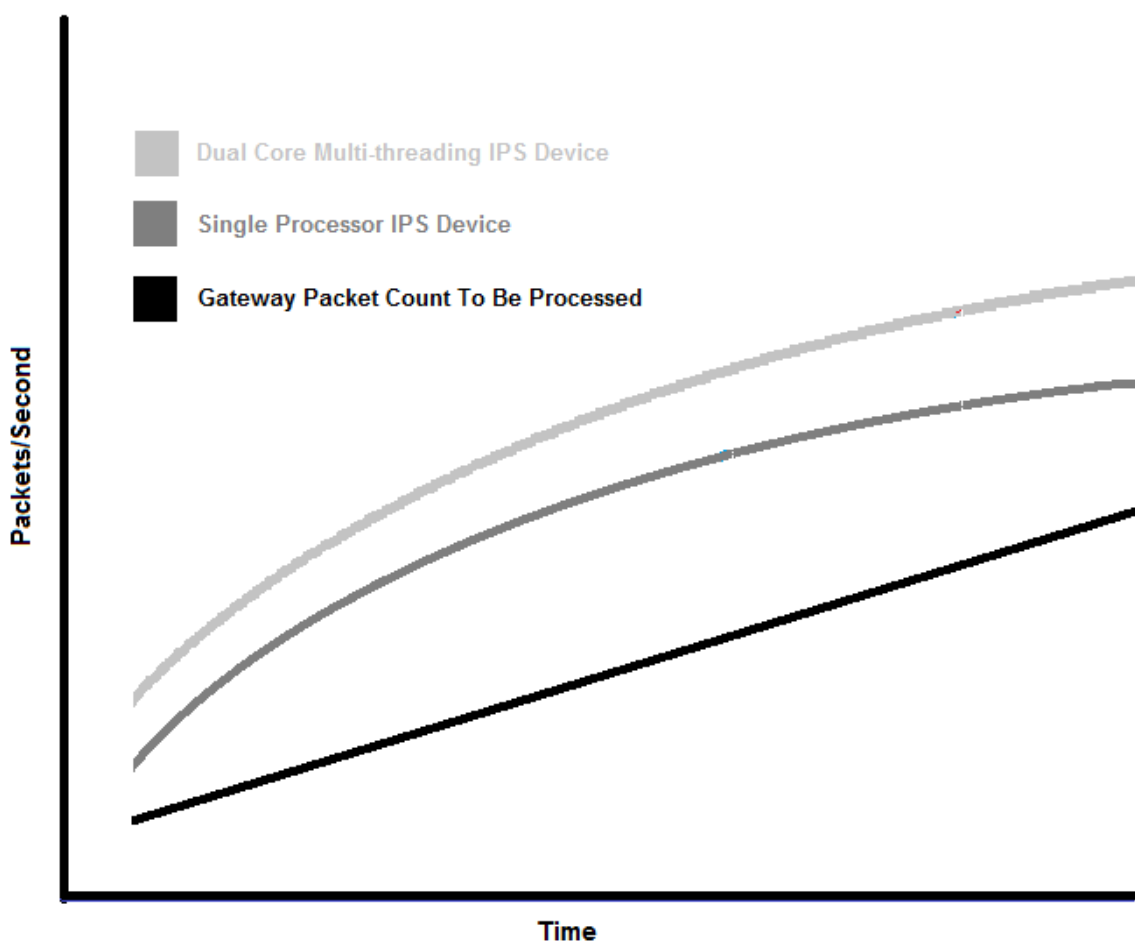
What is being illuminated here is essentially some type of speed limit, or maximum realized capacity to perform the functions required for intrusion prevention. We can try to improve the functions related to IPS and we can improve the hardware it runs upon, even adding parallel processors. This only extends the date of non-workability. We can represent this graphically, in the diagram that follows.



Note that the grey area represents the point at which the integrity of our IPS systems fail. If this is an accurate depiction of reality, the question becomes NOT if, but when?

Past ways of thinking, impose constraints that may not exist in reality. To merely improve IPS technology has us do extraordinary work focusing on technical tradeoffs, making minimal improvements, as we reach the limit of what is possible. One approach to transforming this problem might be to consider a way to no longer have it be a problem. Is such an outcome even possible? We believe CI, integrated with Network Cloaking, DPAM, EPS, and changes to network architecture can significantly alter the number of packets to be processed.

Suppose we dedicate our efforts to transforming the gateway packet count to be processed. Network Cloaking and DPAM have proven to dramatically reduce the resources required for packet analysis. Why spend CPU cycles analyzing packets sent by a “bad guy”? Instead use a relatively non-resource intensive firewall contained inside the Sentinel IPS device to prevent the communication in the first place. CI, fully developed and properly implemented will likely conform to the 80/20 rule. With 20% of the work, we will, remediate 80% of the threats. The remaining 20% will require innovative ways of dealing with the bad guys. But it is well within the capabilities of the security community to develop these solutions going forward. We can represent this graphically, in the diagram that follows.



In closing I want to impress upon the reader to make sure you get a Network Gateway Assessment for your network. We provide NGA's for qualifying networks at no charge. We also conduct a mapping/scan of your network by a certified ASV to see how your network advertises itself to the outside world. You learn a great deal about who is attacking your network and what they are doing to exploit your vulnerabilities.

Additionally, the EPS module will look for any botnet machines active inside your organization and you can use that information to track them down and clean it up.

Our support team is always up for a new mission, if it impacts your network security or makes us better. Sentinel IPS with Collective Intelligence™ is the biggest breakthrough in network security since the firewall. Find out what CI can do for your network security. Join the movement, and we will work together, because it is your right to be secure.

FREE 14 Day Network Gateway Assessment (NGA) plus a certified ASV mapping scan, and use of the EPS module to look for any “botnet” machines active inside your organization.



Learn who is attacking your network.
Learn how your network advertises itself to the “bad guys”.
Learn what the “bad guys” are doing to exploit your network.
Learn about security compliance for your internet gateway.

OK, here's the fine print:

First, we install our Sentinel IPS on your network's gateway. This process is usually completed in under two minutes, an install kit is provided (cables, cross-over adapter, and power cord are included), and no changes to your network are required. Once it is installed, the Sentinel IPS begins logging information about attacks, hacks, and other malicious traffic. You have complete access and can view reports and attack summaries in real-time, configure the unit to send you email alerts, and compliance reports. We also conduct a mapping/scan of your network by a certified ASV to see how your network advertises itself to the outside world. Then, after a period of 14 days, we take the time to review the data gathered by the Sentinel IPS with you. There is no obligation to buy anything; just clear, concise data showing you exactly who is trying to exploit your network and how you can use Collective Intelligence to protect your network.