

NETWORK CLOAKING™
AS A
DEFENSIVE STRATEGY
FOR
INTRUSION PREVENTION SYSTEMS

By

David A. Lissberger
CEO – EcoNet.com, Inc



Network Cloaking™ (nět` 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.

Introduction

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 **

Imagine applying this way of thinking to the protection of your network. Imagine your network and its resources were “without ascertainable shape”. If your network were invisible to hackers and malicious users, then the wise would truly be unable to “pry in”, nor lay plans against you.

“You can’t hack, what you can’t see.”

The goal of this paper is to have you consider “Network Cloaking”™ and the EcoNet Sentinel IPS™ Intrusion Prevention System as a mandatory addition to your layered network security solution. Along the way, we will review several of the leading intrusion prevention strategies so we can compare and contrast them to Network Cloaking™. Whether you have a simple T-1 internet connection with a couple of servers, or a complex network with a security event management system, Sentinel IPS™ with “Network Cloaking”™ is the best way to protect your network from intrusions and malicious code at the internet gateway.

Finally, this paper will review the Sentinel IPS™ deployment strategy from the perspective of optimizing the ease of network integration. False positives have been the “Bain of existence” for many network administrators attempting to integrate in-line network devices (NIDS). Sentinel IPS™ is the market leader for effective, affordable, and ease of integration and management for IPS solutions.

The Death of the Internet Firewall.

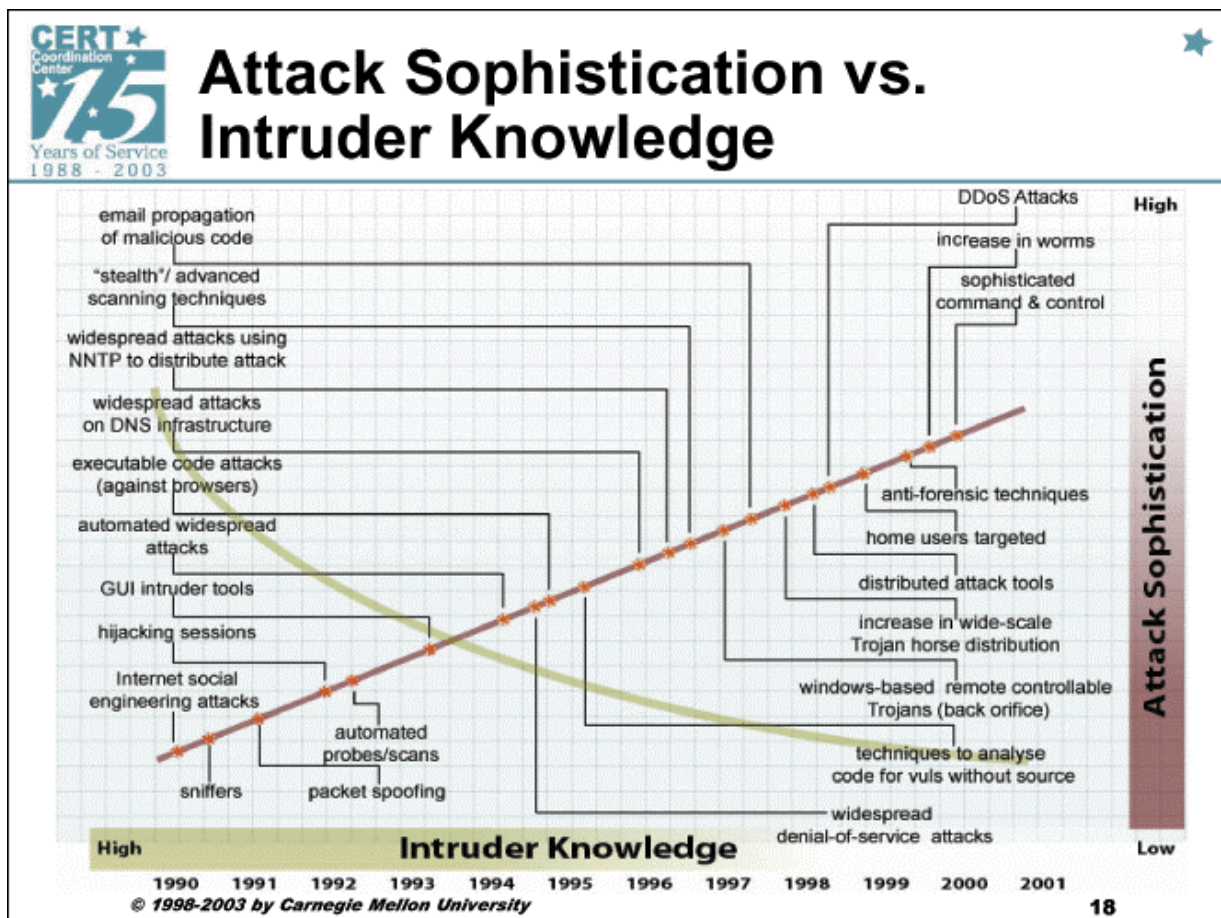
Firewalls are an excellent defense against network intrusions. With all the ports closed, the firewall may be considered "non-breachable". For all practical purposes, it is impossible to be hacked through a closed port of a quality firewall. Intrusions occur through the ports that have been opened by personnel entrusted by the organization requiring protection. By definition, opening a port on a firewall anonymously is the same as "turning off" the firewall on that port. Companies routinely turn off several ports on their firewalls for a number of reasons. Since intrusions occur through the open ports on a firewall, in reality, most companies no longer have a firewall. We would not consider letting a passenger on a commercial flight without a complete inspection, including the contents of their bags. I would suggest that we NOT let a user into our trusted private network without such an inspection as well, including the contents (payload) of their packets.

CSI's annual survey, released in the first half of 2001, found that fully 85% of companies had experienced a security breach. The total combined losses for the 186 companies that were willing to state how much money they lost to these breaches was a staggering \$378 million. (Keep in mind that only about 35% of companies surveyed agreed to divulge their financial losses.)

According to [Computer Economics](#), an independent research firm, enterprises worldwide spent \$1.2 billion in 2001 fixing vulnerabilities related to the Code Red worm alone.¹

A Firewall is not enough.

There has been an enormous increase in the range, frequency, sophistication, and success of intrusion attempts propagated on the internet. This table helps explain why.



Available at <http://www.cert.org/present/cert-overview-trends/module-2.pdf>

¹What You Need to Know About Network Security, New opportunities in Internet business bring with them new security challenges. By Kim Austin Peterson and Fred Sandsmark

It is fair to say that for most firms a firewall is not an appropriate intrusion prevention solution and the firms included in the foregoing statistics would most certainly agree. In the slide above from a CERT presentation it became clear why intruders are becoming more successful over time. Notice that the technical knowledge an intruder must possess is declining, yet the attacks are becoming more sophisticated.

In an effort to remediate the vulnerabilities around open ports in firewalls, firms have turned to a variety of solutions. Many are expensive and quite complex. Intrusion detection systems or IDS was quickly adopted as a mechanism for identifying attacks and malicious source IP's. An onslaught of signature definitions, detection methods, and deployment methodologies ensued. Good IDS's proved effective at detection but remediation became an issue that in the end has proven unsolvable for most companies. This situation has led some industry leaders to the mindset described below.

STAMFORD, CONN., June 11, 2003 — Protecting enterprises from hackers, viruses and other security vulnerabilities is a primary concern for all IS departments, and many have relied on intrusion detection systems (IDSs) as a solution. However, according to the Gartner, Inc. (NYSE: IT and ITB) Information Security Hype Cycle, IDSs have failed to provide value relative to its costs and will be obsolete by 2005.

The Gartner Information Security Hype Cycle shows that IDS technology does not add an additional layer of security as promised by vendors. In many cases IDS implementation has proven to be costly and an ineffective investment.

Gartner recommends that enterprises redirect the money they would have spent on IDS toward defense applications such as those offered by thought-leading firewall vendors that offer both network-level and application-level firewall capabilities in an integrated product. "Intrusion detection systems are a market failure, and vendors are now hyping intrusion prevention systems, which have also stalled," said Richard Stiennon, research vice president for Gartner.

Regardless of your views on IDS, good network protection still requires detection as a component to the solution. Once a source IP is detected and determined to be malicious, then remediation must be accomplished as quickly as possible. Either someone writes a new rule to the firewall or it is done automatically. Automated remediation, when combined with detection, falls into a new category of security products called intrusion prevention systems or IPS. These systems are, generally, either host based or in-line.

Host-based Intrusion Prevention System - Host based Intrusion Prevention System is software that is installed on your individual servers to protect the servers from attack and compromise. While host based Intrusion Prevention can also be effective it can be costly to deploy and cumbersome to manage. . . .²

While this might provide an important additional layer of security, it is not a viable gateway intrusion prevention strategy because it does not prevent intrusions, rather this strategy attempts to control any damage that might result. The firewall represents the primary boundary of the private network and by definition a successful host based solution means that this boundary has been breached. Intrusion management at the application server perhaps, but intrusion prevention of the network, certainly not. Better that intruders are prevented from entering the private network versus the host, making this an appropriate layer of defense versus the only means of protection.

² CIO Magazine What's the best way to prevent an infection? by Joseph Magee

There are downsides to host-based intrusion prevention, however. It's useless against intrusions aimed at your network in general—such as denial-of-service attacks. You also need to install it on every system you want to protect, which can create a deployment headache.³

The other type of IPS just emerging is the inline IPS. This type of approach has great promise. Critical factors are the ability to inspect, detect malicious content, and drop packets before they can enter the network. False positives, creating service interruptions for users, are also a fear for early adopters of this type approach. A recent flood of IPS products, vaporware, and outright misrepresentation of product capabilities has created a very noisy IPS marketplace. In the rush to be included in the IPS market, many suppliers are calling their products intrusion prevention systems, but they are, in fact, only one of the required components of an IPS strategy. Many products are only capable of monitoring specific ports and others are unable to remediate attacks that occur in the initial packet entering the network. Separating fact from fiction takes time and most network administrators lack the time or expertise to determine which IPS vendor (of which there are only a very few) should protect their network gateways.

If it's a NIDS, you better be able to deal with false positives, or the IPS will not stay on the network for very long. Blocking legitimate traffic creates extreme frustration for those that rely on unimpeded communications across the Internet. Any active in-line (NIDS) IPS product must provide some mechanism for the management of false positives. It is interesting to watch the innovative approaches firms utilize to deal with this issue. Before reviewing the EcoNet strategy utilizing Network Cloaking™, here are two recent approaches that will serve to highlight and contrast issues related to false positives.

Honey Pots

A few systems utilize either a “honey pot” or a “baiting” strategy to engage the hacker. The idea is that the hacker will interact with some false or fake data in such a way as to reveal that their intentions are indeed malicious. Once this determination is made, the source IP address can be blacklisted. Note that it is the hacker interaction with the fake data that will trigger the IPS to prevent the user from engaging the network. While this strategy almost completely eliminates the false positives, it has a few serious security vulnerabilities. First it provides no protection for intrusion attempts that are not preceded by interaction with the honey pot. The network is completely available to any exploit from a new IP address. Nothing prevents the network from being the subject of many methods of finger printing and subsequent intrusion attempts.

Group the signatures and disable those that cause trouble

A recently introduced IPS product, sold as a firewall add-on, inspects incoming packets for malicious content and will drop the offending packet. The device has no capacity to dynamically create a blacklist, so malicious source IP's are never denied access to the protected network. Their packets containing malicious payloads may be dropped, but the hacker is free to attempt entry into the network without interruption. This approach will generate frequent false positives, so the signature database used to identify malicious packet content is divided into three tiers, based on the likelihood that the signature might cause a false positive. The maker suggests that the sensitive groups of signatures be disabled from blocking packets as a methodology for dealing with false positives. While this method may effectively reduce the effects of false positives, it opens a large vulnerability for the network administrator. Namely, no remediation for a large number of attacks and since there is no

³ Defensive Postures Intrusion prevention systems offer the latest countermeasures in the war against hackers, worms and viruses BY DYLAN TWENEY CIO MAGAZINE

blacklist, an attacker can continuously try new ideas until one matches a disabled signature or an attack for which there is no signature present.

While these approaches may lack the desired level of protection, that is not to say they lack utility for the protection of private networks. As part of an overall “layered” security strategy, each component and its interplay with other network elements must be given due consideration. For many network administrators, the help of a trusted advisor is money well spent. Our experience has shown that most network administrators are still unaware they have open ports on their firewalls. They, along with those charged with a fiduciary responsibility to protect the assets of the firm, understand little about this type of vulnerability or that such a condition exists. In the face of new legal requirements and standards of liability, most organizations are ill equipped to deal with the threat of network intrusions.

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. The nature of such a threat calls directors, officers, and others responsible for network security to be diligent in securing the organization’s Internet connections. What is being offered to the market are products, specifications, testing services, service offerings, certifications, and seminars. What companies need is an effective intrusion prevention strategy for their Internet gateways.

The 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, just to list a few. There are simply too many stories to spend time reviewing them here.

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. Let them spend their time elsewhere. It may not be very “macho”, but it is extremely effective.

For almost three years, EcoNet.com, Inc. has used "Network Cloaking"[™] as a successful intrusion prevention strategy. Network Cloaking[™] is EcoNet’s proprietary technology that results in the Sentinel IPS(tm) Protected Network being invisible to a malicious user while maintaining the utility of the network for other users. Hackers and other malicious users are unable to communicate with the Sentinel IPS(tm) protected network, while legitimate network traffic remains unaffected.

The Wounded Goat

A federal law enforcement group conducted an experiment to test the effectiveness of this strategy. First they connected a PC with a public IP address to the Internet. It was loaded with a default installation of Windows XP Service Pack 1 (they called the sacrificial machine, the wounded goat). The machine was compromised within the first day and within the week it had several administrators logged on to the machine and using it to attack other machines on the Internet.

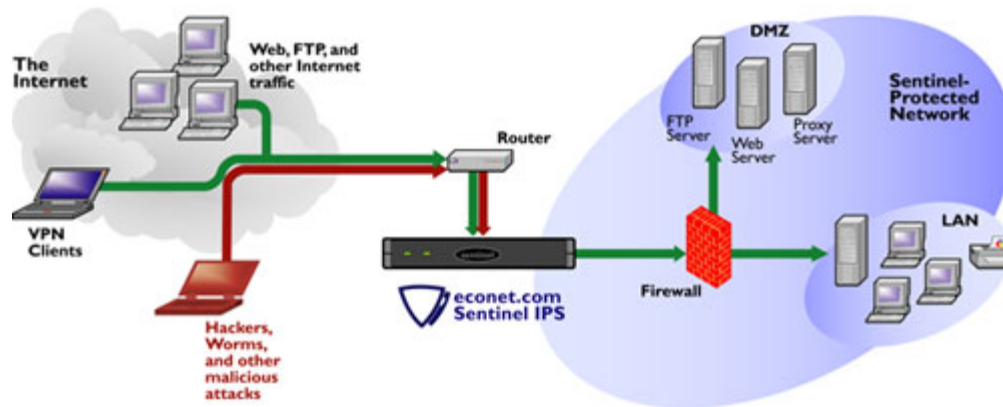
After a week or so, this federal bureau replaced the hard drive with an identical fresh install, but this time the PC was protected by a Sentinel IPS(tm) with Network Cloaking[™] activated.

The machine has been on the web since the fall of 2003 and has never been compromised. The PC is still perfectly available on the web, but it is completely invisible to malicious users.

This demonstration shows "Network Cloaking"™ is one of the most powerful tools available in preventing intrusions into private networks. Hackers cannot determine if the Sentinel IPS™ 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 IPS™ Protected Network", then Sentinel IPS(tm) will automatically engage Network Cloaking™ as a defense against that user. It is this feature that makes it impossible to portscan, stealth portscan, or Penetration Test a Sentinel IPS™ Protected Network.

What does a typical installation look like?

Generally, The Sentinel IPS(tm) IPS is installed as a Layer 2 Bridge, behind your network's router, and in front of your current firewall. Most Sentinel IPS(tm)s are installed on networks with access to the Internet through a T1 connection.



EcoNet first started deploying the commercial version of its Sentinel IPS™ product almost three years ago. The first significant technical accomplishment was active remediation of malicious IP addresses using AP-Core™ Technology (Active Packet Correlation). 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 Clients Network before the packet can leave the Sentinel IPS™ Appliance. This is accomplished so quickly as to be imperceptible to the users of the network.

How invisible is Network Cloaking™?

We wanted to see how a Sentinel IPS™ Protected Network might respond to a hacking tool or strong scan vulnerability assessment tool. What information would such a tool yield from a Sentinel Protected Network. Billy Austin, CSO for Saint Corporation, has been working with high-level government agencies, top colleges, and universities, and major financial institutions for many years in this area. SAINT security consultants provide security assessments including penetration testing, as well as other services including security planning, implementation, management, and support.

Mr. Austin provided the opportunity for EcoNet to find out what a Sentinel Protected Network using Network Cloaking™ looks like to the hacker. The Sentinel IPS™ performed flawlessly in vulnerability testing conducted by the security firm. IP addresses on either side of the Sentinel IPS(tm) protected networks were easily exploited, however those IP addresses

protected by Sentinel IPS(tm) were completely invisible. Our cyber neighbors were easy to spot, but there was no evidence the Sentinel IPS(tm) Protected Network existed.

@stake, another well known security firm was hired by one of EcoNet's clients to perform intrusion testing on the Sentinel IPS(tm) protected internet gateway. The testing showed no evidence that the client's protected network existed, however there was an interesting consequence of the test for the security consulting firm. Since Sentinel IPS™ disables all communication between the malicious source IP and the protected network, @stake was unable to send email to their client explaining that they were not able to perform the penetration test on the protected network. @stakes' IP's had to be released by the Sentinel IPS™ so they could resume communications with their client.

Disruptive channel strategy provides ease of integration

In the traditional channel for IT products manufacturers sell through distributors to Resellers or VARs. Competitive market pressures usually create gray market product channels and eventually erosion of product margins for the VAR. VAR's tend to be less interested in products they do not sell and they generally are unable and unwilling to be price competitive with the large online resellers.

Manufacturers rely on these same VARs for integration and configuration of network equipment, usually through some type of certified training program. A NIDS requires a high level of support. Such an IPS is the opposite of "set it and forget it". In fact, the more you work on it and "tweak it" the more effective it will be in protecting the network.

It takes a considerable amount of training and experience, perhaps a few years, before a technician can be totally proficient in the tuning, administration, and care, of a sophisticated IPS solution. The technicians performing this work are NOT generally the employees of the IPS manufacturers and distributors, so there are many cross company barriers that effect quality and reduce performance of the deployed IPS product. Some of these barriers include variability in the skills of the installation technicians, margin pressures reducing the amount of time a VAR can devote to specific product mastery, reduced speed of disseminating new procedures, longer times for knowledge transfer to integrators and end users.

Sentinel IPS™ is deployed through a unique and cooperative Team Approach, whereby a Sentinel IPS™ Certified Reseller (VAR) does the physical needs assessment, installation, and overall security policy management for the end user and EcoNet delivers the network integration, tuning, updating, maintenance, and technical support from a centralized Sentinel IPS™ management facility in Dallas, TX. This process is optimal for matching those skill sets needed, with the best possible resources, to service the end user customer. Who else better to manage the IPS device than the engineers that write the IPS security application. And, who else better to manage the requisition, installation, and on-premise security policies than a trusted service firm (VAR).

Capitalizing the R&D investments of your vendors

There are not many true IPS products in the Sentinel IPS™ category at this time. Network World did an IPS round up at the beginning of this year and found less than ten entries, of which Sentinel was the only product sold with management, monitoring, and support.

Although cost was not a factor in the review, most of the appliances cost between \$25,000.00 and \$75,000.00 with Sentinel being the most affordable.

When you buy a \$50,000.00 appliance, what you really bought was a box worth a thousand or two, some margin for the VAR, and \$40,000.00 for the future use of their Intellectual Property (IP). The manufacturer must recover the R&D cost (and other costs as well) incurred in development of the product.

EcoNet sells the Sentinel IPS one month at a time. This approach dramatically reduces the cost of an IPS solution, because the customer is not forced to pay for the use of the IP until they are ready to actually consume it. Using the same philosophy, costs are further reduced by bundling the support, management, and monitoring into one low monthly payment, starting at only \$299.00/month. With Sentinel IPS™, the customer never pays in advance for value they have not actually received.

This is a radically new approach, but it does reduce IT cost. It eliminates the large upfront capital cost associated with sophisticated technology products. It also moves the expenditure from an asset on the balance sheet to an expense on the income statement, which for most companies is financially very attractive. Product life cycles are now so short for most of these types of products, that the items are still being depreciated after they are no longer in service.

Advanced security functionality, expert management and support, and reduced cost of ownership make the Sentinel IPS™ the best product for protecting open ports on your network firewall. If any of the ideas expressed in this paper hold interest for you, I would invite you to contact our firm. You will find a dedicated team ready to answer questions and help you learn how Sentinel IPS™ can make a difference for your network. Companies large and small have utilized our "Free 14 day Network Gateway Security Assessment" to discover what is actually happening on their networks.

For more information about deploying Network Cloaking™ and Sentinel IPS™, call a Sentinel IPS™ Certified Reseller or contact us directly by phone or via the website:

www.networkcloaking.com
info@econet.com

EcoNet.com, Inc.
13237 Montfort Suite 850
Dallas, Texas 75240
Office: 972.991.5005
Fax: 972.991.4242