NETWORK CLOAKING ™
AS A
DEFENSIVE STRATEGY
FOR
INTRUSION PREVENTION SYSTEMS

By
David A. Lissberger
CEO – EcoNet.com, Inc

The goal of this paper is to have you consider "Network Cloaking"™ and the EcoNet Sentinel Intrusion Prevention System as a mandatory addition to your layered network security solution. 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.

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.

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]

It is fair to say that for most firms a firewall is not an appropriate intrusion prevention solution. Most of the firms included in the foregoing statistics would agree,

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

[1] What 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

end has proven unsolvable for most companies. This situation has lead 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 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 perhaps, but intrusion prevention, certainly not. Better that intruders are prevented from entering the private network versus the host.

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 and ability to inspect, detect malicious content, and drop packets before they can enter the network. False positives, creating

---

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

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

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.

Our experience has shown that most network administrators are still unaware that they have open ports on their firewalls and that they along with the fiduciary responsibility holders of the firm understand little about this type vulnerability and that such a condition even 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 organizations 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. For the last year and a half, EcoNet.com, Inc. has used "Network Cloaking"™ as a successful intrusion prevention strategy. Cloaking the network makes it invisible to malicious IP's. Hackers and other malicious users are unable to communicate with the cloaked network, while normal network traffic remains unaffected.

Network Cloaking™ is EcoNet's proprietary technology that results in the Sentinel Protected Network being invisible to a malicious user while maintaining the utility of the network for other users. EcoNet.com, Inc. created the technology and incorporated it into the Sentinel IPS. "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 impossible to portscan, or stealth portscan, a Sentinel Protected Network

EcoNet first started deploying the commercial version of its Sentinel IPS product in the first half of 2002. The first significant accomplishment was active

remediation of malicious IP addresses using AP-Core™ Technology (Active Packet Correlation). Sentinel 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.

It is interesting to see how a Sentinel Protected Network might look to a hacking tool or strong scan vulnerability assessment tool. 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. Sentinel performed flawlessly in vulnerability testing conducted by the security firm. IP addresses on either side of the Sentinel protected networks were easily exploited, however those IP addresses protected by Sentinel were completely invisible.

@stake, another well known security firm was hired by one of EcoNet's clients to perform intrusion testing on the Sentinel 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 consulting firm. Sentinel disallows communication between the malicious source IP and the protected network, so @stakes' IP's had to be released so they could resume communications with their client.

For more information about deploying Network Cloaking™ and Sentinel IPS, contact,

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

Press Contact:
David A. Lissberger
davidl@econet.com