RFI SUBMISSION

First Line of Defense® to Protect Critical Infrastructure

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Response to NIST
Docket # 130208119-3119-01
Document # 2013-044B

corero
FIRST LINE OF DEFENSE

Introduction

Cyber attackers are increasingly focusing their attention on critical infrastructure of an enterprise network, a data center, a disaster recovery site, or even Industrial Control Systems (ICS). The impact of taking down one of these systems can include:

- Lost revenues due to negative impact on intended transactions that can't go through
- Dissatisfied "good users" who get tired of waiting on a service that is slow or unresponsive
- Loss of trust and reputation when the public learns that the business is unable to protect its critical infrastructure

If the systems being attacked are Industrial Control Systems, the impacts can be devastating because they are used to monitor and control a variety of operations in industrial facilities, including military institutions, power grids, water distribution systems and public and private buildings.

Many organizations rely on firewalls to protect against such attacks. But when the firewall is the first line of defense against such attacks, a number of things can happen to the network infrastructure at a technical level:

- Firewalls often times get overworked when processing large numbers of connections for both good and bad traffic. Even a large capacity next generation firewall can become flooded with activity and become so degraded that it begins adding significant latency and even worse, often starts dropping good traffic.
- IT infrastructure gets stressed processing not only the good traffic but the bad traffic as well.
- Servers are often overwhelmed with unnecessary traffic, resulting in unresponsive applications. For example, a server CPU may go to 100% usage and degrade performance for every application dependent on that server. This may include applications totally unrelated to the Web process under attack, causing a ripple effect of downtime for many of the organization's applications.

This submission summarizes best practices for a new First Line of Defense against today's ever-changing threat landscape and outlines five key steps of protection. These steps move successively deeper into the protocol stack to inspect the packets more closely in order to address far more issues than any firewall alone can mitigate. These steps are necessary to stop DDoS and other advanced attacks before they reach the network. When such unwanted traffic is blocked, an organization is better able to ensure that critical infrastructure such as firewalls, load balancers, servers and databases are working on genuinely desired traffic, thus protecting the critical IT infrastructure, eliminating downtime, and improving the robustness of all web-facing services.

Please contact Nirav Shah at nirav.shah@corero.com for any questions regarding this submission.

Key Steps of Protection for a First Line of Defense

In order to eliminate the broadest spectrum of unwanted traffic and cyber attacks in the industry today, a systematic approach must be taken at the perimeter of the network. The approach can be summarized into "**Five Key Steps of Protection:**"

Step	Protection	Function
1	**Restrict Access**	Allow only the EXPECTED traffic
2	**Limit Rates**	Evaluate the AMOUNT of traffic
3	**Enforce Protocol**	Enforce the CORRECTNESS of traffic
4	**Prevent Intrusions**	Analyze the INTEGRITY of traffic
5	**Increase Visibillty**	Provide VISIBILITY into unwanted traffic and attacks

- The first step (Restrict Access) allows only expected traffic and restricts access of known attackers, via IP Reputation, Geolocation and other intelligence gained from internal and/or external logging systems and regulatory agencies.

- The second step (Limit Rates) prevents attacks based upon clients' individual traffic behaviors and controls the amount of traffic from suspicious sources. For example, blocking is performed against sources that transmit volumes of traffic toward the critical infrastructure, as well as those that open excessive number of connections, keeping vital resources tied up and potentially forcing systems offline.

- The third step (Enforce Protocol) ensures all allowed traffic conforms to RFC (Request for Comments) specifications and de facto standards, thereby enforcing the correctness of traffic. Any traffic not conforming to standards or expected behavior is discarded.

- The fourth step (Prevent Intrusions) analyzes integrity of traffic and detects known, and possibly unknown, buffer overflows, code injections, malware and other targeted attacks. Through extremely high-speed (multi-gigabit) deep packet inspection (DPI) capabilities, unwanted traffic is quickly and easily eliminated.

- The fifth step (Increase Visibility) provides operators and security personnel insight into what is happening on their networks. It includes the ability to collate data from SYSLOG events, SNMP polls and traps, and proprietary APIs, enabling meaningful visibility and a stream of potentially critical information.

Each of these steps has a series of questions that help guide a better defensive solution.

Step 1. How can an organization restrict access to its network?

a. Does the traffic come from a known attacker?
b. Is the traffic coming from a geolocation in a part of the world that the organization doesn't do business with?
c. Is the traffic originator on a list of malicious or unwanted IP addresses, either provided by internal log intelligence or intelligence gathered elsewhere?

Inspection of traffic at this level involves primarily looking at source IP addresses and comparing them to known bad IP addresses via reputation, geolocation and other customized lists of unwanted source IP addresses provided by the customer or elsewhere. In this step, case by case whitelisting can be used to allow known good sources. Once traffic passes through the first gate of "restricted access," more inspection must be performed concerning the rate of the traffic to head off volumetric attacks.

Step 2. At what rate can traffic enter the network?

a. Does the traffic look like attack traffic? For example, half open connections, unable to complete a transmission control protocol (TCP) three-way handshake, etc.
b. Why does this user have thousands of connections open to a target (victim) server?
c. How can application abusers be controlled?

Inspection of traffic at this level involves dynamic threat assessment as a way of determining the threat level of unknown attackers. Limiting concurrent client and client group TCP connections plus analyzing request and response behaviors are techniques used to detect too many requests, too many connections and other network and application layer usage. Assuming that traffic is not flagged for entering the network at an abnormal rate, the next step is to look at its behavior.

Step 3. Is the traffic conforming to desired behavior?

a. Is the traffic conforming to established protocols?
b. Are there questionable protocols or protocol violations within the allowed traffic?
c. Can the traffic be inspected bi-directionally?

Inspection of traffic at this level involves primarily looking at clients, servers, ports, protocols, allows, blocks, intrusion prevention (IPS) rule sets and security policy enforcement. Stateful protocol analysis as a way of protocol enforcement resides at this level, as well as bi-directional traffic inspection. If the traffic has appropriate behavior, the next step is to inspect the actual payloads.

Step 4. Does the traffic contain known security issues?

a. What are the traffic's payloads actually carrying?
b. Are there any server-side exploits or malware in the headers or payloads?
c. Is advanced evasion being used in blended attacks?

Inspection of traffic at this level involves deep packet inspection, attack and vulnerability signatures, overflows, injections and brute-force password protection and advanced evasion detection. Once traffic gets to this point in the inspection process and it has passed all the "tests," most likely it is good customer traffic that can be allowed past this first line of defense.

However, given that attacks are continuously changing and growing more sophisticated, there is one more step of protection to consider in a new first line of defense solution: increased visibility.

Step 5. How can added visibility secure my network better against future threats?

a. How can the network be better protected against future threats?

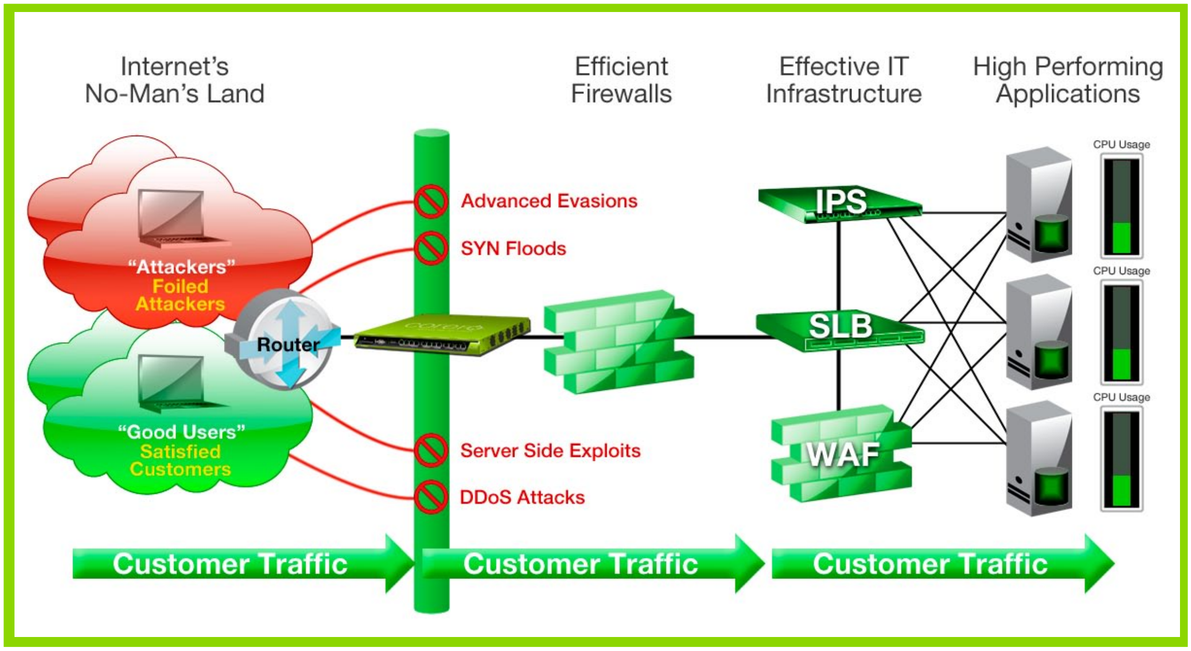
b. Will increased visibility allow a better understanding of what's going on at the perimeter?

c. Will this visibility increase the ability to better control traffic?

The fifth step is more of a comprehensive step that gives IT administrators an insight into what is happening on their network. It includes the ability to collate data from SYSLOG events, SNMP gets & traps, and proprietary APIs into a meaningful stream of information and enables integration with Security Information and Event Management (SIEM) software. With that, organizations can reassess the threat landscape to see if their security policies are effective.

Conclusion

A solution that can take the key five steps of protection and go deeper and deeper into analyzing and approving or rejecting all network traffic before it reaches the firewall will eliminate the problem of an IT infrastructure that is overwhelmed by volumetric and other modern-day attack methods. As seen in the figure below, a First Line of Defense solution placed at the outermost position of the network perimeter – even before the firewall, weeds out cyber attacks and other unwanted traffic while allowing good customer traffic to proceed. By filtering out the bad traffic before it encroaches the critical infrastructure, First Line of Defense allows critical infrastructure components to do their intended jobs more efficiently and effectively.



Though firewalls are still a critical and necessary component of any network, they are no longer the best type of device to deploy as the network's first line of defense. Firewalls, even modern Next Generation firewalls, have limitations in what they are designed to do. Attackers know these limitations and have devised attacks that can evade or overwhelm a firewall, as well as the secondary security devices behind the firewall, such as an IPS. Once an attacker gets past the firewall, he can put a choke hold on the critical infrastructure in no time and harm the critical IT infrastructure rendering it unavailable to legitimate users. A modern security solution must deflect unwanted traffic and even go deeper into the traffic's packets to inspect payloads, understand behavior and dynamically assess and mitigate threats in real-time.

Such a modern solution, the new First Line of Defense, defines the network perimeter to be in front of the firewall, protects the critical infrastructure and enables maximum uptime of business applications.

About Corero Network Security

Corero Network Security (CNS:LN), an organization's First Line of Defense, is an international network security company and a leading provider of Distributed Denial of Service (DDoS) defense and next generation security solutions. As the First Line of Defense, Corero's products and services stop attacks at the perimeter including DDoS, server targeted, and zero-day attacks, protecting IT infrastructure and eliminating downtime. Customers include enterprises across industries from banking, to financial services, gaming, education, retail and critical infrastructure as well as service providers and government organizations worldwide. Corero's solutions are dynamic and automatically respond to evolving cyber attacks, known and unknown, allowing existing IT infrastructure – such as firewalls which are ineffective at stopping much of today's unwanted traffic at the perimeter – to perform their intended purposes. Corero's products are transparent, highly scalable and feature the lowest latency and highest reliability in the industry. Corero is headquartered in Hudson, Massachusetts with offices around the world. www.corero.com.

Corporate Headquarters
1 Cabot Road
Hudson, MA 01749
Phone: +1.978.212.1500
www.corero.com

EMEA Headquarters
68 King William Street
London, England
EC4N 7DZ
Phone: +44 (0) 207.959.2496