



CUNA CENTER FOR
RESEARCH & ADVICE

CUNA Internet Security Solutions Powered by Red Cliff Solutions

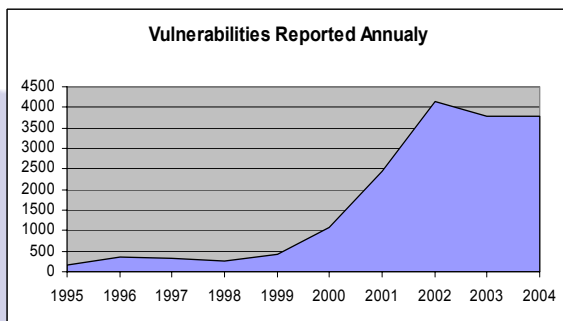
Managed & Monitored Intrusion Prevention System

FIREWALLS ARE NOT ENOUGH

Deploying firewalls throughout a network is a good thing. A correct firewall policy can minimize a network's exposure. However, many firewalls are configured to allow applications through, including email and web sites. Opening these "holes" can effectively render the firewall useless for that particular traffic. Email and web are two of the most commonly opened ports and consequently, have the greatest number of known vulnerabilities. Attackers are very good at using the ever-growing list of application vulnerabilities to compromise the few services that are being let through by a firewall. Attackers are evolving their attacks and network subversion methods. These techniques include email based Trojan horses, worms, stealth scanning techniques and actual attacks which bypass firewall policies by tunneling access over allowed protocols such as ICMP or DNS.

THE NUMBER OF VULNERABILITIES IS INCREASING

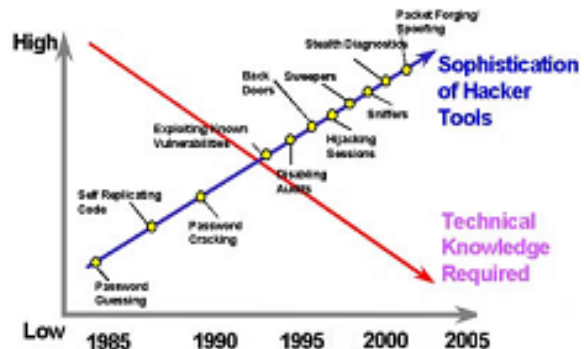
The amount of traffic posted to vulnerability mailing lists such as BUGTRAQ has exploded over the past few years. The amount of information on network vulnerabilities is so pervasive, companies such as SecurityFocus and Ernst & Young, commercially sell subscriptions to vulnerability digests, automatically tailored to a company's profile of operating systems and network hardware.



ATTACKERS ARE GETTING SMARTER

Although many network scanning and attacking techniques have been known of for several decades, it is only recently that the tools to conduct sophisticated analysis of a target network have become available to the masses. For example, the port scanners, which were publicly available in the early 90s, would simply attempt to connect to a target machine on every port to build a list of potential active ports. Modern port scanners including operating system identification, can target entire ranges of IP addresses and even send in decoy scans to make it more difficult for the target to identify who the scanner source really is.

Additionally, these scanners and other tools are available for free, on the Internet with point and click graphical user interfaces.



THE SOLUTION

The CUNA Enterprise Intrusion Prevention System (IPS), powered by Red Cliff Solutions, is strategically placed within a network topology where it can monitor and block malicious network traffic. It compares the packets of data with known "signatures" of harmful attacks as well as other methods to detect attacks. If a match is made, the IPS system can dynamically block



CUNA

Credit Union National Association



CUNA CENTER FOR RESEARCH & ADVICE

the packet in near real-time. Qualified security specialists are also available to examine other traffic that is not dynamically blocked but must be analyzed before action is taken.

The Enterprise IPS is capable of scanning the internal network and identifying those systems that are potentially at risk. The IPS is then fine tuned for that specific customer network. This results in far fewer false positives and increases reliability.

The system is designed to not require any network changes or additional hardware. It acts as a passive bridge allowing traffic to be analyzed as it passes through the in-line system. If ever the system fails, it can simply be taken out of line without causing any problems with network traffic or routing. A 3rd network card is configured as a management interface.

Enterprise Intrusion Prevention System

Intrusion Prevention System

- Acts as a network 'Surveillance Camera'
- 24x7 Monitoring of events
- Escalation procedures based on customized SLA
- Dynamic blocking of malicious traffic
- Can detect and block many known worms, viruses and Trojan horse programs
- Automatic signature (known hacker attacks) download on a daily basis giving the customer the most up-to-date protection
- High-speed traffic recording and analysis system up to 200 mbps
- Rapid detection of Distributed Denial of Service Attacks (DDOS)
- Automated and custom reports available
- Bridge mode allows prevention while not changing network topology, routing or IP addresses
- Reduced false positives with internal scanning capabilities to identify systems potentially at risk

The IPS is a powerful network surveillance system for IP networks that provides traffic recording and real-time traffic analysis and blocking. The CUNA IPS records network traffic, analyzes every packet, detects the activities of intruders and can dynamically block traffic.

Signatures that are not set to automatically block will be analyzed by a qualified Internet Security Specialist and a permit or deny decision can be made.

The IPS offers greater compliance with federally mandated security systems and monitoring.

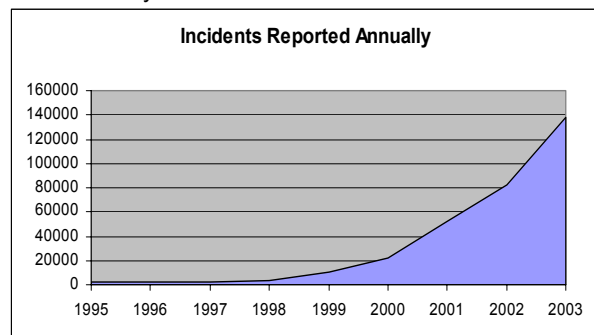
The CUNA Enterprise IPS was specifically designed for financial institutions, which have particular network environments as well as security concerns and compliance requirements.

The IPS offers full 24x7 monitoring of Internet or other network traffic that passes through the in-line system. A qualified Internet Security Specialist can help recommend the optimum placement of the IPS to get the greatest benefit for your particular network.

The IPS automatically looks for updates of the latest hacker signature database every hour. This keeps you up-to-date with the latest attack methods that a hacker will use to compromise networks.

With the CUNA IPS, you don't have to have any IT staff nor any security expertise to gain the benefits of a fully managed and monitored intrusion prevention system.

The IPS can be configured to ignore auditing systems that normally cause problems or block the intended use of the audit system.



While some IPS systems can inadvertently block many large ISP networks, the CUNA IPS will block the attack for a specific period of time, and then be released until the next attack. This prevents attackers from using the IPS as a weapon against the customer creating a denial of service.



CUNA CENTER FOR RESEARCH & ADVICE

IPS systems that use firewall signaling (sending rules to a separate firewall for blocking) or TCP Kill commands usually are ineffective for many types of attacks. The CUNA IPS is an in-line system that can stop an attack before it enters your trusted network.

Bridge mode allows the system to be in-line and not require any change in IP routing, addressing, or topology. It can be dropped into virtually any network and begin preventing attacks.

Policy based traffic such as adult material, peer-to-peer applications, chat, instant messaging, and multimedia downloads can be monitored or blocked at the customers request.

IPS - Reporting

A secure online web portal is available to review near real-time statistics. Reports available include auditor and examiner reports, board reports, technical reports, a variety of summary reports, and full custom reporting.

Policy based reports are also available to show accessed adult content, peer-to-peer applications, chat, instant messaging, multi-media downloads, and viruses.

Hardware Platform

Shelf or Rack Mount



Dimension: (1U) 19" (W) x 17" (D) x 1.75" (H)

Cooling: 2x40mm air bearing fans

Weight: 20lbs

Power: DC Power: 200W PFC: AC

Power: 4.8 amps at 115V; 2.9 amps at 230VAC (switchable)

Interfaces: 10/100 or 1000 Ethernet

CONTACT INFO

Stacey Norland | Research Analyst
CUNA Center for Research & Advice
Credit Union National Association, Inc.
5710 Mineral Point Road
Madison, WI 53705
E-mail: snorland@cuna.com
Phone: 800-356-9655 ext. 4317
Fax: 608-231-4027

To learn more, visit
securitysolutions.cuna.org