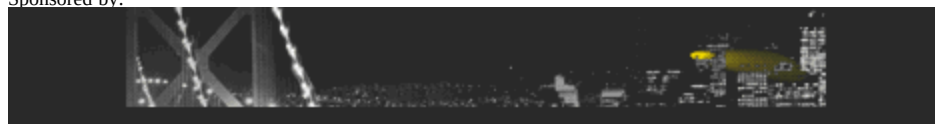


Sponsored by:



NetworkWorldFusion

This story appeared on Network World Fusion at
<http://www.nwfusion.com/reviews/2002/0902rev.html>

Review:

Denial of service: Fighting back

Test shows there are several varied, viable options that help defend your network against attacks.

By Mandy Address, Network World Global Test Alliance
Network World, 09/02/02

There's more than one way to skin a denial-of-service attack, but first you've got to catch it. Two years after the well publicized attacks on Yahoo, eBay and CNN, DoS attacks are still very prevalent - they just aren't discussed. The advent of new attack technologies, such as Naptha and Reflective DoS attacks, are making the process of protecting networks even more difficult.

In a perfect world, your ISP would detect and deal with the growing number of these attacks on its end. But because many ISPs do not want to take on the added burden and legal responsibility to provide, or claim to provide DoS protection, you'll most likely have to deal with DoS attacks - whether they are randomized DoS, general distributed DoS or reflective distributed DoS - on your own.

On the market today is a range of vendors providing DoS attack-detection and mitigation products. How each product approaches the problem runs the gamut. Signature vs. anomaly detection. Inline vs. network tap. Active vs. passive. Who does what and how does it all work?

We invited a group of vendors into our lab to help discern the advantages and disadvantages of each approach. Asta Networks, Captus Networks, CS3, Lancop, Mazu Networks, Radware and Webscreen agreed to participate in our review. AppSafe, Arbor Networks, CacheFlow, Check Point Software, Extreme Networks, FloodGuard, Internet Security Systems, IntruVert, NetScreen, Reactive Network Solutions, Recourse Technologies, Riverhead and TopLayer Networks declined.

Our tests determined that these products all work about the same in detecting attacks, with most of the products detecting 95% of the attacks we launched ([see online chart](#)). The deciding factor lies in the mitigation techniques available to you. How concerned are you that valid traffic still needs to pass? How much control do you want over the process? What type of reports and how much data do you want to have available to you? Once you have answered those questions, you quickly will be able to narrow down the top choices for your environment.

[How we did it](#)[How the devices compare in tests](#)[Detecting DoS attacks before they disable your network](#)[A glossary of DoS terms](#)[Archive of Network World reviews](#)[Subscribe to the Product Review newsletter](#)

In-line products

Captus CaptIO and CaptCC



Captus provides the most granular product we evaluated, but it could be more cohesive and easier to administer. Captus provides two devices: CaptIO is the inline DoS device, and CaptCC is the centralized management appliance that can control multiple CaptIO devices.

You can configure and manage CaptIO through a built-in Web graphical user interface, but CaptCC provides for multiple devices and some advanced GUI functionality. Overall, only basic management functionality is available through either GUI - most management is performed via the command line.

Captus representatives installed their product in our test lab. The first installation was a disaster, with the CaptIO and CaptCC devices having problems that rendered them useless. A second installation attempt with brand new boxes went smoothly. As recommended by Captus, CaptIO and the CaptCC resided on a completely different subnet than the monitored networks.

Captus products use a technology called Traffic Limiting Intrusion Detection System (TLIDS), which are defined as rules, similar to firewall rules. TLIDS rules can be defined on any of the device's interfaces. In reality, CaptIO functions much like another firewall on your network. You can define what protocols can be allowed through the device, what traffic levels you should expect and what SYN buckets to manage SYN floods. As with any baseline-based product, its effectiveness depends on how accurately your thresholds are set. Captus does not provide a threshold analyzer, but it does provide rate throttling, slowing the connection rate, opening bandwidth to let legitimate connections pass.

Captus administration is a bit frustrating and can seem a bit redundant when working with your firewall. If you configure CaptIO as recommended, blocking all ports except those that are allowed, you will configure any changes in at least two places - your gateway firewall and CaptIO/CC. While it provides an excellent defense-in-depth architecture, TLIDS rules could be a bit easier to configure.

CaptIO was very effective at identifying and handling our DoS attacks when the TLIDS rules were defined correctly. Once you understand the TLIDS syntax and options, you can have very granular control over your network traffic. When an attack is detected, CaptIO takes action as defined in the appropriate TLIDS rule and reports information to a syslog server.

Captus reports are based on syslog data and use a Crystal Reports viewer to help analyze the syslog data and render it into a user-friendly report. In addition to an improved GUI, we would like to see an improved reporting infrastructure.

Like most of these DoS devices, Captus runs on Linux and upgrades are as easy to install as any traditional Red Hat RPM application. A vulnerability assessment scan of the system showed OpenSSH vulnerabilities, meaning that an attacker potentially could compromise it.

Bottom line

Captus Networks CaptIO and CaptCC

<http://www.captusnetworks.com>

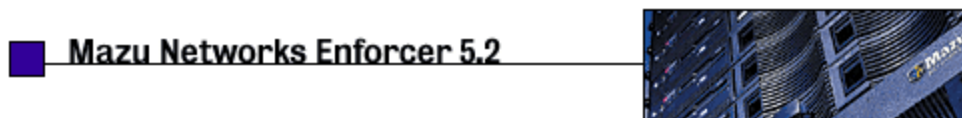
Category: Inline

Cost: CaptIO, \$15,000; CaptCC, \$8,500

Advantage: Most flexible and granular configuration options.

Disadvantages: First install attempt failed; poor reporting; poor GUI.

Best suited for: Organization that wants complete control over all configuration aspects of the device.



Mazu's Enforcer is an adaptive distributed DoS product, watching and evaluating network traffic to determine what is valid and what is malicious. The Enforcer sits inline on your network and basically has three network interfaces. Two are used for traffic monitoring (one sits on the "Internet" side and one sits on the "internal network" side). These interfaces operate in promiscuous mode to pick up and analyze all network traffic. It then has a third interface specifically for management access to the device.

Enforcer determines its baseline of "normal" traffic by analyzing network traffic for a period of time as set by the user, specifically looking at packet characteristics, such as time to live, payload and hashes. The longer the amount of time the network is analyzed, the more accurate your baseline will be. Enforcer analyzes traffic and alerts administrators when traffic that exceeds the baseline thresholds set by the user. Enforcer will recommend filters to be installed on the device (with the administrator's approval) to remove or mitigate the identified attack. These filters take an all-or-nothing approach, though, and easily can filter out valid user traffic. However, you can define trusted traffic, and these packets never will get dropped. Additionally, when running in passive mode, Enforcer will just recommend access control lists that should be installed on your routers.

Mazu usually installs Enforcer, installing the product in our test lab. Installation is straightforward, configuring the inline promiscuous interfaces and management connection. Once Enforcer is up and running, it needs to monitor network traffic to configure a baseline that best fits your network. An excellent feature in the Enforcer is the Threshold Advisor, a wizard that helps you determine what your baseline thresholds should be set at based on a period of traffic analysis you define. The Enforcer then automatically can configure its thresholds. Enforcer administrators also can change any of these values manually.

For SYN flood attacks, you define separately your SYN queue parameters, which determines how many SYN requests can come in and sit there without receiving responses. As the queue fills, older open connections are dropped.

The main page on Enforcer's administration interface contains an overview of what is happening on the network through a combination of interface packet statistics and a graph of traffic types, which is completely configurable. We had trouble getting the graph to display attacks as they occurred and discovered timing is an issue in the graphing portion of the product. Traffic analysis and counts occur as the packet enters the interface. The graph is created based on the timestamp of the packet. If timestamps

are off, the packets will not be displayed properly, which is what we encountered.

During our testing, Enforcer notified us of any activity that exceeded our defined thresholds. On a completely random TCP flood, we enabled the recommended filter and couldn't access our test Web site until we removed the filter. Like many of the distributed DoS products, Enforcer runs on Linux and a vulnerability assessment scan of its interfaces showed Secure Shell vulnerabilities on the management interface. Enforcer is good at identifying high-level traffic flows that exceed defined thresholds, but it will not solve all your problems. Enforcer picked up a sync4 attack against a system, but by then it was too late - the target system was already unresponsive, and the Web server needed to be restarted to function properly.

Bottom line

Mazu Networks Enforcer 5.2

<http://www.mazunetworks.com>

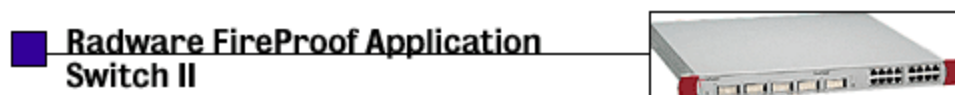
Category: Inline device

Cost: Starts at \$32,000

Advantage: Threshold Analyzer Wizard guides users well.

Disadvantages: All-or-nothing filters that can block valid traffic; reliance on Network Time Protocol timing synchronization can lead to reporting glitches.

Best suited for: Organization looking for inline device that does not require accurate attack blocking on spoofed source IP attacks to let legitimate traffic pass.



The Radware Application Switch can perform a variety of functions, including firewall load balancing, network switching, providing application security protection and protecting networks from DoS attacks. For our testing, we configured the Application Switch to run its DoS Shield and Application Security applications independently - it was not acting as any other type of device.

The Application Switch is a signature-based product, comparing a sample of network traffic (based on administrator-defined parameters) with a list of preconfigured attacks. This device is better than the other devices tested at catching those one-packet attacks that can take down a system and will not necessarily be picked up by an anomaly- or baseline-based product. When an attack is detected, the Application Switch takes action, as defined by the administrator, which includes reporting or blocking the offending packets. Our testing found this option to be successful. Malicious traffic was blocked, but valid traffic was allowed to pass. This device did not generate any alerts on our outbound DoS attack because it only appears to analyze inbound connections from the external network. It also did not identify the sudden, rapid increase in Web traffic as anomalous.

Installation was very simple. We configured an administrative port in addition to the network interfaces monitoring network traffic. Management occurs through a local Web server or a Java management console. After enabling the Application Switch and DoS Shield, we set application aging protocols, which are useful for dropping "old" connections. We also set the tracking time and threshold limit for SYN attacks, TCP port scan, User Datagram Protocol floods, ping floods and UDP port scans.

A vulnerability assessment scan of the management port showed a Web server chunked encoding vulnerability - a new type of Web server vulnerability released a few weeks ago. With this vulnerability, an attacker could disable, compromise or change configuration of the device.

Because Radware is not installed on a base Linux server, you must wait for the vendor to release a new firmware update to fix security issues. Additionally, new attack signatures are updated only through new firmware releases. Firmware updates are released every few months and they are very easy to install.

Bottom line

Radware FireProof Application Switch II

<http://www.radware.com>

Category: Inline

Cost: \$28,000

Advantage: Catches single packet attacks and other known attack types.

Disadvantage: Updates available only via new firmware.

Best suited for: Organization looking for a signature-based product or looking to combine DoS protection with load balancing.



The WS100 is an inline, passive device with a separate management interface. The device acts as a bridge between networks, with the passive interfaces not even having IP stacks bound to them. This helps protect the DoS device from being attacked itself.

Webscreen uses heuristics to identify anomalous or malicious traffic and drops traffic as necessary. Webscreen's Charm technology analyzes network traffic for behavioral characteristics and decides which traffic is malicious and which traffic is valid.

Installation and setup was simple. We configured it through its Web-based management program, defining inbound TCP ports, inbound UDP ports, inbound Internet Control Message Protocol types and IP protocols. We also defined server parameters, such as TCP backlog per port, maximum connections and total TCP backlog. Webscreen's products are optimized to protect Web servers, so much of the configuration information focuses on the specific characteristics of your Web server farm.

In our testing, the WS100 was the most accurate at identifying attacks and mitigating attack traffic to let valid traffic pass. Its reporting infrastructure could be improved to provide more detailed information and graphs. Currently, it only provides text-based statistical displays. One interesting piece of information the WS100 does provide is a list of the top-20 offending IP addresses that attack your network.

Bottom line

Webscreen WS100

<http://www.webscreen-technology.com>

Category: Inline

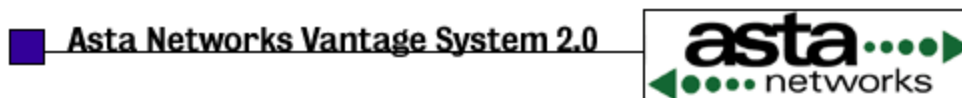
Cost: Starts at \$23,000

Advantages: Almost invisible on the network; best overall performance; Charm technology helps identify malicious traffic.

Disadvantage: No graphs in reporting.

Best suited for: Optimized to protect Web server farms.

Network tap products



The Vantage System is a network-monitoring appliance that hangs off a switch or network tap on the network and pulls traffic statistics from Cisco, Foundry Networks or Juniper Networks gear on your network. You also can place the device on a spanning port on a switch to gather traffic data. It collects data in real time, but there is a slight delay as it is sent to the device and analyzed. The system continuously analyzes network traffic to determine characteristics and will alert administrators when traffic occurs outside of a defined threshold. Administrators define network policies to help the product determine valid traffic levels.

When an attack is identified, the Vantage System will start classifying the data, recording and reporting details of the attack to administrators. The Vantage System also will provide access control lists and recommendations on how to mitigate the effects of the attack. The system does not provide any automatic filter or attack mitigation options.

Installation and configuration are easy with this device. We connected the appliance to a spanning port we configured on our Cisco Catalyst 3500 switch and were up and running in no time. System management occurs through a Web-based console.

Of all the products we evaluated, the reporting capabilities in the Vantage System were the best. The level of detail and granularity about the packets and statistics analyzing the system were unmatched. We could see every detail of the malicious traffic, down to the individual packets involved.

On the downside, the Vantage System was slower to alert us to attacks, taking a good minute or two to categorize the traffic.

The Vantage System also runs on a Linux-based server appliance, so you need to be conscious of attacks that could be launched directly against the system. A vulnerability assessment scan shows OpenSSH vulnerabilities.

Bottom line

Asta Networks Vantage System 2.0

<http://www.astanetworks.com>

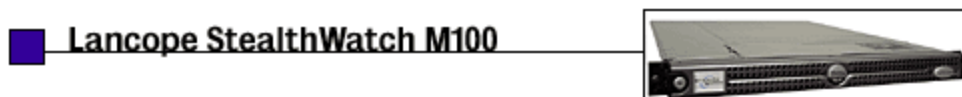
Category: Network tap

Cost: Starts at \$8,000.

Advantage: Very detailed reporting information.

Disadvantage: No autofilter option; slow identifying attacks.

Best suited for: Organization looking for an alert-only device.



The StealthWatch M100 is another passive monitoring product, marketed as an intrusion-detection system (IDS), that detects attacks based on defined thresholds and baselines. StealthWatch uses a Concern Index and Services Profiler, algorithms and security logic Lancope developed to determine attack traffic. It builds a profile of a suspected attack and alerts administrators only when the Concern

Index of the suspicious activity reaches the administrator-defined threshold. When an attack is identified, the device can take numerous actions, including sending e-mails and pages, and blocking the offending connections.

StealthWatch also watches traffic at a more granular level than some of the other products. The Services Profile is mapped down to an IP address, whereas other products just analyze the big-picture network traffic.

Setup and installation of StealthWatch went very well. After calling Lancope to obtain the administrator password (its standard practice), we logged on to the system console and configured the IP address of the management connection. We then connected to the system through the Web-based GUI to complete the configuration process. We also configured the device to run in build and report mode, which means that any new services identified on the network are added to the profile and reported to the administrator.

One feature we liked was its ability to automatically e-mail daily reports to defined administrators. With this feature, administrators can have the previous day's reports waiting in their inboxes the next morning instead of having to remember to log on to the system and check status or rely on alerts when attacks occurs. Administrators also can set specific inbound IP addresses for a watch list. Any time traffic is detected from an address on the watch list, a special report is generated. You can configure the reverse, defining addresses that cannot trigger an alarm, regardless of what traffic it is sending or receiving.

One problem with StealthWatch is that its Service Profiles are defined by IP address. If your network uses Dynamic Host Configuration Protocol (DHCP), your Service Profiles will not be accurate. In this scenario, Lancope recommends defining Service Profiles by IP address ranges equivalent to your DHCP scope.

We first defined our Concern Index levels for inside and outside hosts. We set these levels at the midrange level. Setting them too high potentially will cause the device to miss attacks, while setting it too low creates a large number of false positives. In our testing, StealthWatch performed very well, identifying and mitigating all attacks we launched during our test.

As with the majority of the rest of these products, StealthWatch runs on Linux. A vulnerability-assessment scan showed OpenSSH vulnerabilities.

Bottom line

Lancope StealthWatch M100

<http://www.lancope.com>

Category: Network tap

Cost: \$20,000

Advantages: Anomaly-based, but catches nonflood attacks; Concern Index and Services Profile to identify malicious traffic.

Disadvantage: Has problems working in DHCP networks.

Best suited for: Organizations looking for a combined IDS and DoS product.

Internal DoS product

 **CS3 MANANet Reverse Firewall**
Version 1.10



The MANANet Reverse Firewall takes a different approach, focusing on preventing DoS attacks from leaving your network.

To achieve this, the Reverse Firewall implements two critical functions: fair service to visible sources and rate limiting of unexpected packets. In terms of fair service to visible resources, the reverse firewall focuses on additional path information that has been added to the packet, such as the packet's source data. Rate limiting of unexpected packets focuses on restricting the amount of bandwidth available to traffic floods - those packets that are sent to the target but will never send responses.

CS3 also pushes router "cooperability" - network routers working together to identify distributed DoS traffic and prevent it from causing damage. MANANet is designed to identify other routers working in this cooperative, accepting all traffic from them as trusted packets. CS3 refers to this as the Path Enhanced IP Configuration.

As with most of the other devices, MANANet Reverse Firewall runs on Linux, but it also uses iptables/netfilter firewall functionality. CS3 suggests users replace their existing firewalls with MANANet by just using the iptables functionality. The Reverse Firewall also can be used to protect internal network segments, not just your Internet connection.

Installation and setup was difficult and complex. Initial setup required a floppy disk from CS3 with data specific to the appliance you buy. The data on this floppy disk must be adequately backed up and protected because your device will not work without it. Once you have completed the setup process, you can manage the device through a Web-based GUI.

Using the GUI, we set traffic rate limits and established how we wanted to be notified of attacks, via e-mail in our case. We also set how often we wanted the system to check to see if an attack was occurring, as these are not automatic. You must configure the notification engine to check every X minutes and advise it what threshold of dropped packets you need to see before an alert is sent.

The MANANet Reverse Firewall performed well in our tests, catching all of our attacks. Being the lowest priced product of the group, its price/performance ratio is high, but the device lacked detailed, in-depth reporting and alerting functionality.

Bottom line

CS3 MANANet Reverse Firewall Version 1.10

<http://www.cs3-inc.com>

Category: Works inline or tap

Cost: \$4,000

Advantages: Takes a different approach with cooperative routing.

Disadvantage: Most difficult installation.

Best suited for: Internal network subnets.

Andress is principal of ArcSec, a security consulting firm in the Bay Area. She has written several books, including *Surviving Security*, and is active on the conference circuit, speaking at Black Hat, NetWorld+Interop and numerous other conferences. She can be reached at mandy@arcsec.com.



[Global Test Alliance](#)

Andress is also a member of the Network World Global Test Alliance, a

cooperative of the premier reviewers in the network industry, each bringing to bear years of practical experience on every review. For more Test Alliance information, including what it takes to become a member, go to www.nwfusion.com/alliance.

Related Links

All contents copyright 1995-2002 Network World, Inc. <http://www.nwfusion.com>