CAi NETWORKS

MONTHLY NEWSLETTER

Volume #1,
Issue #1
September, 2007

In this issue

Distributed Denial of Service (DDoS) attacks: the big threat in the war on downtime

The army has been equipped for battle as the commander scopes out his target. Primed for attack, the troops include ... your mom? The green grocer across town?? A playwright in London??? A veterinarian from Chicago????

The commander is a 15-year-old student from Baltimore with a wallet fatter than most of his high school classmates. With the push of a button, he launches an attack that within seconds will start to cause thousands of casualties.

What's going on here?

Read the entire article starting on page 3

Better than an upgrade: a server load balancer

Is your web server running out of steam? Can't keep up with the traffic? SSL putting on an additional strain? Will it drop to its knees if traffic surges? Will it crash under the weight of an attack?

Instead of upgrading your web server or replacing it wth a bigger one, why not take a more sensible approach and grow horizontally rather than vertically? Adding an additional server and using a server load balancer to automatically have them share the work not only gives you unlimited scalability (since you can add more servers whenever you want) but also provides fault tolerance: in case any server fails, the other(s) can take up the work.

WebMux info at www.cainetworks.com/products/webmux/webmux.htm

News

WebMux adds DDoS attack protection

WebMux validated by Oracle as compatible with Oracle 10g

WebMux supports IEEE 802.3ad, doubles capacity on OOP mode

IPV6 support for WebMux now available as standard feature

Articles start on page 3

Current Releases

DnsMux	3.1.0
WebMux	8.3.00
WebSpray	3.35

Newsletter

To subscribe to our monthly newsletter or to modify your subscription, please visit our website at www.cainetworks.com or email us at newsletter@cainetworks.com

CAI Networks Contacts

CAI Networks, Inc.
1715 E. Wilshire Ave.,
Suite 719
Santa Ana, CA 92705
www.cainetworks.com

SALES
sales@cainetworks.com
PARTNERS
partners@cainetworks.com
MARKETING
marketing@cainetworks.com
TECHNICAL SUPPORT
support@cainetworks.com

Oracle validates WebMux as Oracle AS 10g compatible

ORACLE

WebMux has survived the rigors of Oracle validation testing for Oracle Application Server 10g and came through with flying colors. Oracle has recently validated WebMux (rev. 8.2) for compatibility with Oracle AS.

Oracle's vertified testing found WebMux to work acceptably with Oracle AS 10g (9.0.4, 10.1.2) Products, OracleAS Protal, OracleAS Forms, OracleAS Reports, OracleAS Portal, Oracle AS Forms, Oracle AS Reports, OracleAS Wireless, OracleAS Web Cache, Oracle HTTP server, OracleAS Discoverer, and OracleAS Single Sign-On with and without SSL, as well as supporting the Oracle 10g R3 and Oracle AS 10g SOA topologies.

Read more about this in the news article on the right sidebar

The car is free ... but has costs $100 per gallon

In contemplating the purchase of a server load balancer -- or just about any product -- more than the sticker price needs to be considered. More important than the price is the cost of ownership.

Some of our competitors offer a low-priced entry level product that is stripped of features that an average user would need, and then charges to add those in. Or add user license fees with annual renewal fees to the product cost.

At CAI Networks, we bundle not only all features into our products but we bundle in the industry’s best warranty and support: every CAI Networks appliance carries our unmatched “3+3 Guarantee”, which provides a three-year warranty, three years of upgrades, and three years of technical support -- all at no additional cost.

So as with most products, with server load balancers it pays to look beyond the price to see the true cost.

Get all the details at www.cainetworks.com/sales/3+3.htm

Happy Birthday to us: CAI Networks turns 10

CAI Networks is proud to announce our ten year anniversary. Since 1997, we have been developing networking products for the commercial marketplace, always with mission of quality and functionality at an affordable price.

We'd like to thank all our customers and partners for helping us make it ten great years as we look forward to the next ten years and beyond.

Learn more about CAI Networks at www.cainetworks.com/company

About CAI Networks

Founded in 1997, CAI Networks specializes in Internet appliances and Internet server reliability solutions and is a leading provider of IP load balancers and traffic managers. CAI Networks products are installed world-wide by businesses, government agencies, ISPs, ASPs, SaaS providers, and others to maintain the reliability and availability and enhance the performance of web sites, portals, and web-based applications.

CAI Networks customers include The U.S. Navy, U.S. Dept. of Commerce, Electronic Clearing House, CNN.com, Microsoft, General Dynamics, Sony, Siemens, Sprint, Verizon, Georgia Tech Research Institute, and the State of Texas.

CAI Networks' WebMux server load balancer product is certified and used by Microsoft and has been validated by Oracle for compatibility with Oracle AS.

At CAI Networks, we believe our success is based on our customers’ success. We design and manufacture our products based on these simple principles: easy to use and deploy, long lasting reliability, and reasonably priced.

Distributed Denial of Service (DDoS) Attacks: The Big Threat in the War on Downtime

The army has been equipped for battle as the commander scopes out his target. Primed for attack, the troops include ... your mom? The green grocer across town?? A playwright in London??? A veterinarian from Chicago????

The commander is a 15-year-old student from Baltimore with a wallet fatter than most of his high school classmates. With the push of a button, he launches an attack that within seconds will start to cause thousands of casualties.

What's going on here?

Some of today's most feared and hard to defend against threats are "botnet" armies: hundreds of thousands of PCs that have been infected with specially-designed malware – all under the control of evil puppet masters, and generally without the knowledge of their unsuspecting owners. These armies of infected "zombie" computers are capable of wreaking havoc, and they are multiplying at a rate so staggering that would make any recruiter's head spin.

The MyDoom virus affected more than 1 million computers in 2004 and attacked SCO and Microsoft, while a variant targeted Google, AltaVista, and Lycos.

The platoons of these zombie armies are comprised of users with Internet-connected PCs with exposed vulnerabilities. You probably know some of them: friends and relatives who call us "IT professionals" when their PC is "acting strange", starts rebooting itself, or the occasional nuisance pop-up turns into a chronic flurry. But unlike malware designed to display ads or crash PCs, well-behaved botnet malware lives quietly in the background – waiting for the attack signal from its commander.

You run a decent company: it cares about quality and service, looks after its customers, supports the community – but you're preventing an unscrupulous competitor from gaining the market share he wants. He wants: your customers. And one way to try to get them is to make their online experience with your website a frustrating experience – so frustrating that they will abandon your company and do business with his.

Welcome to the age of the contract electronic "hit", where for a fee you have a website crippled.

Too bad to be true?

If this all sounds like a bad fantasy, we need to look back no further than the year 2000, when several large websites – including Amazon.com, CNN.com, eBay and E-Trade – were victims of some of the earliest DDoS attacks. These companies were unprepared, and the resulting disruption of operations made headlines and cost millions.

Most will remember the MyDoom virus, which in 2004 spread via email and infected an estimated one million computers that launched a DDoS attack against the software company SCO. SCO moved to a new domain

CAI Networks' WebMux Load Balancer Adds DDoS Attack Protection

Santa Ana, CA, August 8, 2007 – CAI Networks™ has announced a firmware upgrade for its WebMux™ server load balancer appliance which provides DDoS attack protection for all web and Internet servers being load-balanced and traffic-managed by WebMux.

WebMux's DDOS protection both detects and blocks attackers involved in coordinated DDoS attacks, thereby preventing web servers from being bombarded with malicious traffic. This feature enhances WebMux's comprehensive security features, which include DoS and SYN protection and a built-in firewall.

Unlike DoS attacks, which generally originate from a single IP address and are therefore easy to detect and counter, DDoS attacks can come from many IP addresses and largely appear as normal traffic patterns. DDoS attacks are typically carried out by botnets – ordinary user PCs that have been compromised by malware to form a "zombie army" – usually without the knowledge of their users. WebMux's attack protection capabilities are able to accept traffic from any IP address when it is non-malicious and block it when it is malicious, so as not to inadvertently block hijacked PCs when they are not in attack mode.

WebMux's DDoS protection is currently shipping in new units and is available as a free enhancement via a firmware upgrade to version 8.3.00 for customers under CAI Networks' inclusive 3-year warranty and extended service plans.

WebMux SLB Validated by Oracle as Compatible with Oracle 10g

and removed its old one from the DNS and managed to avoid major damage. A variant of MyDoom targeted Microsoft, but did not spread widely and so Microsoft's pre-emptive alternate domain shift was not required and its website remained up. A later MyDoom variant attacked Google, AltaVista, and Lycos, completely disabling Google for more than half a day and slowing the others down for hours.

At the time of the writing of this article, a worm named Storm had infected an estimated 1.7 million computers over a three month period, creating a massive zombie army capable of not only taking down the websites and flooding the bandwidth of any company but many countries. Unlike MyDoom, which had its target IP addresses hard-coded, giving its intended victims time to prepare, Storm is capable of receiving its attack coordinates dynamically, so any site can be a put into its crosshairs at any time.

The Denial of Service attack

So-called "denial of service", or "DoS attacks" are electronic assaults intended to make a company or organizations outward-facing computing resources unavailable to users. They generally strive to prevent a website from functioning efficiently or at all, effectively disabling its owner's web presence. DoS attacks may try to deprive service temporarily or even indefinitely.

DoS attacks typically do harm by causing a target system to reset or saturating it with external communication requests so fast and so furious that it cannot respond to legitimate traffic, or that it responds so slowly that users time out or give up in frustration. DDoS attacks can gobble up all available bandwidth so that networks are unable to carry any traffic other than that imposed by the attack, or cause network devices to lock up or crash.

The Storm trojan has infected almost two million computers, creating a massive zombie army capable of not only taking down the websites and flooding the bandwidth of any company but many countries.

The user experience during a denial of service attack is familiar to anyone who has tried to access a very popular website at a very popular moment: you either cannot get through or it's infuriatingly slow ... and then maybe it times out. In fact, it is not unusual for website operators to create their own inadvertent denial-of-service events by failing to provide sufficient capacity to handle peak user activity. (The forward-thinking companies and organizations that anticipate and plan for such situations is the reason we're in business.)

To be clear, a DoS attack is not intended to compromise security, steal data or money, or cause the kinds of problems that other kinds of assaults can – but the consequences are often the same: loss of business, revenue, customers, market confidence, etc. And like other types of assaults, there is the potential of the attacker holding a gun to your head asking to be compensated to not do it or make it stop, and positing that the cost of calling off an attack is small compared with the potential damage it could cause.

The Distributed Denial of Service attack

Denial-of-service attacks are nothing new: they have been around for years, and effective methods have been developed to deal with them. What's new is the increased effectiveness of such attacks, brought about by the ease of coordinating multiple attackers in a simultaneous assault. Such "distributed denial of service" or "DDoS" attacks can be vastly more effective not only because the volume of the attack can be so much greater but because the mechanisms generally used to detect and stop such attacks is quite a bit more complicated.

Oracle testing validates CAI Networks' WebMux server load balancer compatible with with Oracle Application Server 10g

Santa Ana, CA, June 29 2007 – CAI Networks™ announces Oracle's successful testing and compatibility validation of its WebMux™ server load balancer with Oracle's Application Server 10g.

Based on successful compatibility testing, Oracle found WebMux to "work acceptably for the Oracle Application Server 10g (9.0.4, 10.1.2) Products OracleAS Portal, OracleAS Forms, OracleAS Reports, OracleAS Wireless, OracleAS Web Cache, Oracle HTTP Server, OracleAS Discoverer and OracleAS Single Sign-On with and without SSL" and also is supported by "OracleAS 10g R3 and OracleAS 10g SOA topologies".

Oracle does not certify Load Balancer products, rather it only confirms that testing against its requirements has been successful achieved.

Testing was done using two pairs of WebMuxes deployed and configured in a rigid framework specified by Oracle in order to ensure the product's successful operation in a representative Oracle AS 10g environment.

WebMux provides users of Oracle AS and related products with an easy-to-implement, high performance, and lower-priced alternative to other network appliances in the same product category. WebMux's functionality includes load balancing and failover of multiple servers, thereby ensuring high performance and high availability of Oracle AS environments. WebMux further enhances performance and security with FIPS-compliant and hardware-based SSL acceleration.

A distributed-denial-of-service attack is rather the same as a lot of users trying to access a website at the same time: like trying to get onto CNN.com or bbcnews.com after a huge news event, like 9-11. This was not an intentional attack, but the conditions and the consequences were the same: too much traffic for the website to handle, resulting in poor performance or a crash.

Detecting and stopping denial-of-service attacks

In this article, we will not go into detail about how DoS and DDoS attacks actually perpetrate their evils. It is not important for this discussion, and we do not want to give clues to hackers (although such information can easily be readily found on the Internet). It is sufficient to know the following:

- DoS attacks are normally characterized by a single automated attacker sending transactions much faster than any human user could, and often trying to exploit a host-side vulnerability that would cause the impact of the bombardment to be heightened.

- Detecting and stopping a DoS attack involves determining the IP address that is sending all the traffic and blocking it (and reporting it to authorities: DoS attacks are illegal).

- DDoS attacks are similar to DoS attacks except because there are multiple attackers they do not necessarily need to exploit vulnerabilities: the sheer volume of normal transactional traffic that can be generated could be sufficient to bring down a website or flood a network that lacks the capacity to handle it.

- DDoS attacks do not need to generate very substantial transaction volumes from any client, since the same – and much more – volume of traffic can be generated by all the attacking computers in concert.

- Detecting and stopping DDoS attacks cannot simply pinpoint and block a single IP address since there are a multitude of IP addresses involved in the attack, and few if any of them may be generating an inordinate amount of traffic.

Time is of the essence in determining that an attack is underway and stopping it. If too late, it could be difficult if not impossible to get sufficient system control to slow down or stop the attack without a

- Since DDoS attacks are done from a multitude of computers, it is very difficult if not impossible to identify the Commander in Chief of the attack. (The MyDoom author, believed to be a Russian programmer, is today still at large despite rewards in the hundreds of thousands offered for his unmasking.)

For both DoS and DDoS attacks, time is of the essence in determining that an attack is underway and stopping it. If too late, depending on the nature of the attack, it could be difficult if not impossible to get sufficient system control to slow down or stop the attack without a system shutdown.

Preventing denial-of-service attacks

The best protection against denial-of-service attacks of any flavor is a strong defense. This first of all means closing any holes an attacker could exploit. This, of course, cannot include closing off the channel to the Internet, since without that there is no service to be denied; rather, it means following best practices in setup and configuration and correcting any known vulnerabilities. But even with no vulnerabilities available for an attacker to exploit, there still remains the fact that a large enough volume of traffic– as would be the norm for a very busy website – could bring a website to its knees, or worse.

WebMux is a IPV6 compliant rack-mounted network appliance that operates at OSI layers 2, 3, 4, 5, and 7, thereby providing content-aware switching and intelligent traffic management at wire speed. Its unique MAP capability ensures successful handling of streaming media and other advanced traffic across multiple ports and servers.

Details of WebMux's deployment in an Oracle AS environment can be found at http://cainetworks.com/support/Oracle-WebMux.pdf and http://www.oracle.com/technology/products/ias/hi_av/Tested_LBR_FW_SSLAccel.html.

WebMux doubles its capacity in OOP mode with new firmware

Supports both IPV4 and IPV6 network load balancing

Santa Ana, CA, June 5, 2007 – CAI Networks™ announces new firmware release 8.2.07 for models 481S, 591SG, and 680P models of its WebMux™ load balancer/traffic management appliance.

WIth this new firmware, WebMux supports IEEE 802.3ad protocol to gain higher bandwidth handling capabilities. IEEE 802.3ad protocol is also called network teaming protocol, which allowing more than one interface to be “ganged” together to handle larger capacities. Originally designed for 680P model WebMux, WebMux firmware with teaming support has already been deployed to provide UUNET picture downloading services for tens of thousands of concurrent users.

With this new firmware rleease, in Out-of-Path (OOP) mode, WebMu is able to use both WAN and LAN interfaces together to handle larger amounts of traffic. With IEEE 802.3ad capable

A DDoS attack in particular poses the greatest threat, since via a substantial botnet with each zombie sending traffic to the website, the multiplying effect will be much more pronounced than a DoS attack. This means that a rapid response is often not enough – the response must be immediate.

It was when one of our customers fell victim to a DDoS attack that we implemented DDoS protection in its installed WebMux device, to augment WebMux's existing DoS and other types of protection and

As stated, early detection and corrective action when an attack hits are imperative. This means that detection needs to be done by an intelligent mechanism and, ideally, the same mechanism immediately takes corrective action – or is in close communication with the correcting agent.

Without detailing the nature of the mechanisms that detect and correct for DoS and DDoS attacks, it is obvious that all traffic to a website needs to be monitored to identify attack traffic, since legitimate and malicious traffic may look the same. This means that a mechanism able to monitor all incoming traffic to a website is required, and that it operates at high speed. This mechanism should also be capable of blocking malicious traffic while allowing legitimate traffic to pass through, ideally unimpeded.

WebMux's DoS and DDoS protection

It was when one of our customers fell victim to a DDoS attack that we implemented DDoS protection in its installed WebMux device, to augment WebMux's existing DoS and other types of protection and security capabilities. This company was already mindful of the need for sufficient capacity to handle spikes in user traffic, which is why it deployed multiple web servers with a WebMux load balancer in front of them to distribute the traffic.

We were all a bit skeptical – us, the customer, their ISP, and their security consultants– that they were actually being attacked: after all, they were not the type of organization that one would think would warrant such an assault. But the data did not lie, and the WebMux DDoS protection solution was successful in defending against the attack. (The attack did not stop, but its negative impact on the company's website was stopped.)

WebMux is a standalone network appliance that connects to the network, in between the external and internal firewalls, or using its own firewalling capability. All incoming traffic passes through the WebMux, where it is automatically routed to the appropriate web server, either agnostically or intelligently based on content (URL, MIME header, cookie, etc.). So WebMux is a natural place to put DoS and DDoS protection since it is the gatekeeper for all inbound traffic.

With a built-in detection and correction mechanism to handle DDoS attacks in addition to its existing DoS attack protection, WebMux is the only server load balancer in its class to offer this critical functionality.

WebMux users with DDoS protection (available as a free firmware upgrade for incumbent customers under support) can add this need-to-have safeguard to the long list of high availability and high performance capabilities WebMux provides.

The Storm is on the horizon, the armies are massing, and the clock is ticking.

The checkbooks are open, and so are the wallets.

WebMux is guarding the border.

Are you protected?

network switches, another network cable can simply be connected to increase bandwidth without any software change.

This firmware release also incorporates the latest OpenSSL security fix, as well as SSH enhancements for the disagnostic port.

This firmware is being incorporated into all shipping WebMuxes. Customers under warranty support can obtain this firmware update free of charge.

CAI Networks announces IPV6 support for its WebMux load balancer/traffic manager appliance

Santa Ana, CA, Feb. 5, 2007 – CAI Networks™ announces the support of IPV6 by its WebMux™ load balancer/traffic management appliance. IPV6 is the successor Internet protocol to IPV4 which, most significantly, increases in the number of IP addresses available for networked devices.

WebMux is one of the first network devices to support IPV6, which is gaining increasing popularity and acceptance as many businesses and government agencies are mandating IPV6 support for all networking components primarily due to concerns about limited address space under IPV4. In 2006, White House informed CAI Networks for the needs of IPV6 supports in the WebMux family of products. CAI Networks responded immediately to that request.

IPV6 support is available in WebMux version 8.2.01, which is currently shipping and which is installable by existing WebMux customers as a firmware upgrade. WebMux 8.2.01 supports concurrent inbound and outbound IPV4 and IPV6 traffic.