

**FOR**

Easy to install and configure because it is effectively self-learning.

AGAINST

It cannot prevent the WAN link being saturated by a very severe DDoS attack.

VERDICT

Webscreen takes a radically new approach that is much more effective than traditional methods of combating DDoS attacks.

The Webscreen WS100 is designed to protect web sites from distributed denial-of-service (DDoS) attacks. Webscreen uses a totally new approach that doesn't block all traffic during a DDoS attack – it filters packets arriving during an attack based on past usage history and on current behaviour.

To attack web servers and networks, hackers have started to use massed data as an effective weapon. Denial-of-service (DoS) attacks involve sending huge amounts of data to bring web sites to a standstill. Distributed DoS (DDoS) is a development of this hacker technique in which the data is sent from thousands of sources, making attacks harder to prevent because it's more difficult to block traffic from thousands of IP addresses.

Information on how to launch a DDoS attack is easily downloadable from the Internet. The attacker uses a master computer that controls a network of unsuspecting Internet-connected computers, which have been infected with a virus or trojan horse that permits the master computer to control them remotely. These zombie computers are then used to launch an attack on a chosen web site by flooding the destination site with spurious data that blocks access to genuine site visitors. Internet worms, such as Code Red and Goner, can also be used to set up a DDoS network by insidiously installing backdoors to IRC channels. Because the attack comes from many different locations, it is difficult to detect and until recently there has been no way of defending against it.

If there are only a few attack sources or if they can be recognised as unusual data packets, they can be individually blocked by filters in routers and firewalls. However, even firewalls themselves can be the target of a DDoS attack. But, what happens if the attack is from 100,000 zombies all spoofing their source addresses using multiple attack methods, such as SYN floods, ICMP floods, UDP floods and page floods? Existing methods of defence analyse the quality of Internet data and traffic patterns to filter out data that does not conform. This detects only the most obviously bad data and lets most DDoS attacks through. A lot of good traffic may appear like bad traffic with similar peaks and troughs, and bad traffic may get through if it conforms to normal protocol.

Webscreen's new approach to the problem uses context-based algorithms not only to check data for obvious attack patterns, but it also uses a history to determine if the source is a genuine user or a zombie. Webscreen calls this 'CHARM technology'.

Each time a user (or proxy or cache) visits a web site protected by Webscreen, a note of its behaviour is made in Webscreen's real-time RAM database. When an attack is detected, this past behaviour, together with some rules Webscreen has developed that distinguish mechanistic from human usage, allows the filtering of traffic using Webscreen's CHARM algorithm. Every IP address that accesses your web site is given a CHARM value depending on its behaviour. This value changes every visit. While under attack, at the same time as mechanically rejecting bad traffic, the Webscreen WS100 only lets through IP addresses with a high enough CHARM value. Webscreen can hold the required information on 2 million users in the 512Mb model and 8 million in the 1Gb model with no loss of speed.

The higher your CHARM score, the more likely it is that you will be allowed through Webscreen during an attack. Obviously the bad guys have a poor CHARM score, and this allows Webscreen to identify the most likely attackers in a DDoS attack within five seconds of the attack beginning and display the information on a secure web interface.

Webscreen also stores the TCP state for each connection and can identify some attacks by their out-of-sequence packets. Although other security devices do this, Webscreen's advantage is its speed – it can drop up to 129,000 unsolicited ACK packets per second – and its ability to allow bona fide connections access during an attack. This means that we were able to surf our test web site normally during the 129,000 ACK/sec attack. Webscreen also deals effectively with very dispersed attacks – something other vendors have trouble with.

Of course, if an attacker can organise (or hijack) sufficient hardware to flood the wide area network (WAN) connection of the web site, it is not possible from the client end to filter out all of the attack traffic. In this extreme condition, the WS100 acts as an intelligent fuse protecting the web site from internal damage. Webscreen phase 2 – due in July 2002 – will be multi-gigabit and will be based at the ISP where it can more effectively filter the high-bandwidth traffic. WS100 will share attack information with Webscreen phase 2, making a very effective countermeasure to this kind of attack.

The Webscreen WS100 does not have an IP address visible to the outside world and is completely transparent to data passing through it, so it cannot itself be attacked. It is remotely managed using a browser-based interface from the network manager's workstation over a separate secure Ethernet port using TCP/IP. It is best positioned between the WAN router and the firewall as it can then protect the firewall also.

The WS100 is a 1U high 19-inch rack-mountable unit. It has 100Mbps/sec Ethernet interfaces. The 1Gbit/sec version called the WS1000 was not available at the time of testing, but will be available by the time you read this. It is particularly easy to install and configure. You merely need to tell it which web servers to protect and then it learns from the traffic patterns automatically. At SECURE Computing we see new security technology all the time, and therefore we are not easily impressed. However, we felt that this new product is quite exciting because it has a genuinely new approach and comes to market at just the right time to fill a badly needed security function.

Features	★ ★ ★ ★ ★
Ease of use	★ ★ ★ ★ ★
Performance	★ ★ ★ ★ ★
Documentation	★ ★ ★ ★ ☆
Support	★ ★ ★ ★ ☆
Value for money	★ ★ ★ ★ ★
Overall Rating	★ ★ ★ ★ ★



Contacts

Supplier: Webscreen Technology Ltd
Version: 1.1

Price: £15,000
Contact: +44 (0)1 344 636339
sales@webscreen-technology.com
www.webscreen-technology.com

[View On-Line Articles](#)

[Home](#) [Articles](#) [Advertising](#) [Editorial](#)