MANAnet SHIELD

A Real DDoS Solution with Comprehensive Protection

Cs3 breakthrough MANAnet Shield contains the building blocks to defend against packet flooding Distributed Denial of Service (DDoS) attacks on the Internet. The MANAnet Shield includes the MANAnet Router (an enhanced router), the MANAnet Firewall (an enhanced firewall), and the MANAnet Reverse Firewall, which can be deployed alongside conventional firewalls. Together, the MANAnet Router, the MANAnet Firewall, and the MANAnet Reverse Firewall comprise Cs3's systemic DDoS solution. However, the MANAnet Reverse Firewall also has considerable value deployed on its own.

Protect Sites from Incoming DDoS Attacks

It is impossible to provide DDoS protection at an individual site with today's Internet. By the time a packet flood hits a victim, it is too late – many of the packets of legitimate customers would have already been discarded upstream thanks to the congestion caused by the attack. Cs3 advocates specific infrastructure changes to address these problems:

- ❑ Routers are required to add path information to packets (called Path Enhanced IP or PEIP) so that one can have accurate data about the source of a data packet, and

- ❑ Routers provide Places-based Fair Queuing (PLFQ) to schedule packets based on more accurate information about paths

A MANAnet Router is a router enhanced with PEIP/PLFQ. Cooperative neighborhoods of MANAnet Routers work together to share packet path information, making it easier to locate the origins of packet flooding attacks, and defend against them effectively.

The MANAnet Firewall plays an important role in fighting incoming DDoS attacks at the individual site. In addition to being a traditional firewall, the MANAnet Firewall implements both PEIP and PLFQ, enabling the device to use path data and fair service to schedule incoming packets. In addition, the Firewall also permits administrators to set thresholds for "unexpected" packets that could be site-specific, and to limit the rates of such packets. The Firewall also requests upstream MANAnet Routers to slow down packets with specific paths if it senses an attack (i.e., when it is dropping too many packets). The two devices work in unison to provide a working DDoS defense.

THE ULTIMATE IN DDoS PROTECTION • CS3 MANAnet

Protect Sites from Outgoing DDoS Attacks

The MANAnet Reverse Firewall can fight DDoS attacks by stopping packet floods before they exit the local networks where they originate. The Reverse Firewall essentially provides fair service to *outgoing* packets by using variants of PEIP/PLFQ as described above. It can also greatly reduce the rate of "unexpected" outgoing packets. In effect, DDoS attacks are squelched at the point where they hit the Reverse Firewall. This not only benefits the Internet at large, it affords DDoS protection to the legitimate users of the local infrastructure, protecting their ability to communicate with each other and the outside, if an attack is launched by hackers or their proxies within that network.