
PRODUCT WHITEPAPER:

DoS PREVENTION TECHNOLOGIES

A discussion on prevention technologies deployed to break down the most lethal DoS attacks and their Distributed counterparts.

The Internet is now the largest known business platform known to markets worldwide. This business platform enables business round the clock and across borders. The most expensive problem known to businesses on the Internet is uptime. Organisations spend heavily to add a few notches to their uptime.

The Internet is plagued with attacks which in most cases compromise the integrity of valuable data and in some cases result in downtime. The attacks that cause down time are called *Denial of Service* (DoS) attacks. There are two types of DoS attacks, attacks that cause downtime by attacking system vulnerability and attacks that consume connectivity resources paralysing network activity.

A large number of attacking hosts are required to consume bandwidth to the extent of choking the target network. These hosts are usually networked and controlled by the central attacker and this form is the most lethal form of attack called *Distributed Denial of Service* (DDoS) attacks.

In this paper we would discuss all the aspects of DoS and DDoS attacks. Aspects that discuss the damage a family of resource breakdown attack can cause and prevention technologies that can prevent such attacks. NetMonastery has employed self researched technologies in the DoS prevention space, this document discusses the details required to prevent DoS attacks. The following sections talk about the different kinds of DoS attacks and as to how they could be prevented.

Vulnerability DoS

The tradition denial of service attacks have been targeted on vulnerable system software. System software that may have an unchecked vulnerability which when exploited may lead to a memory space overflow. Exploitable vulnerabilities when improperly exploited almost certainly lead to the system software crashing and in effect resulting in a denial of service attack. A vulnerable web server that performs inaccurate or insufficient bounds checking is a good example of vulnerable software based DoS.

On invalid user input the server injects the user input data into the pre-allocated memory space. There may be a state in which the pre-allocated memory space is overflowed with excess data. This will almost certainly crash the web server application. The application crash creates a denial of service situation as legitimate users of the web applications are denied access. The tiny fragment attack and the mangled fragment attack are examples of this vulnerability DoS family in these attacks the packet is broken into extremely tiny fragments, which either overwhelms the target or confuses the target host.

Such system application vulnerabilities are not categorised as true denial of service attacks as the cause of attack is in secure system applications. These attacks on the application server are blocked by the application protocol anomaly based detection system that filters user input according to the protocol requirements. Alternatively these attacks can also be detected by the signature based attack that may have attack vectors for the specific system vulnerability. Fragmented attacks are blocked by the data traffic normalizer that allows only a pre-defined set of data protocols.

Targeted Flooding

Flooding network devices with specific network anomalies, may lead to an unstable situation where the network device may momentarily or permanently stop responding to service requests. On an average targeted flooding perform attacks on core protocols, in other words targeted flooding DoS attack protocol stacks. A SYN Flood attack is a good example of a targeted flooding attack.

To initiate a tcp (transmission control protocol) connection a host needs to negotiate a connection with the opposite host. This negotiation is a series of data packets exchanged with specific flags on. A typical tcp handshake is accomplished with a series of flags in the tcp header; a tcp handshake will have the following flag pattern.

Client - SYN → Server
Client ← SYN + ACK - Server
Client - ACK → Server

Once a host receives a SYN packet it responds to the client with a SYN + ACK packet. The host then waits for a preset time interval for the ACK response. Till the final ACK arrives the session is stored in a buffer. If there could be a flood of SYN packets sent to the destination host in a limited time frame, there could be an overflow situation at the target host where the session buffer is full and the host isn't able to respond to legitimate requests. This causes a denial of service situation as the target host isn't able to respond to service requests.

Attacks on the base protocol stack is the hardest to detect, specially when the attack is a legitimate protocol packet. There are several ways this could be tackled.

A threshold limit could be set for one system to send simultaneous requests to the target. Assuming the threshold limit is set to e.g. 300 then one single host may not be able to send more than 300 similar packets to the destination in a pre defined time frame.

This may have its own drawback as the limiting factor may be high or low and may generate false positives, or there could be a situation where the attacker uses two hosts to attack and overflow the session buffer. Or the attacker may send such packets to varying destination ports to defeat this system

Another option would be to prevent 3, 5, 10 or 20 simultaneous packets from one single host. One might face huge amount of false positives adopting such an approach, wherein legitimate traffic trying to reconnect to a target host may be denied access, hence creating a denial of service situation. Such attacks are possible all major protocols such as tcp, udp and icmp.

NetMonastery employs several techniques of preventing such attacks, the SiteVaxinPro series have special algorithms that are able to collect packets based on the type and the destination of the packet. By looking for similar packets for a specified destination the device is able to throttle similar packets to a single destination. It also works on a threshold packet prevention mechanism that is connected to the destination packet inspection system. This allows the thresholds to be set dynamically and helps in preventing attacks from two or more hosts as well and reduces false positives.

Distributed DoS

DDoS is the distributed version of denial of service attacks. They are the most lethal category of known attacks prevailing on the Internet. DDoS is simply DoS attacks launched from not one or two but a larger group of host. Sometimes the larger group may mean several hundred hosts on the Internet. DDoS attacks are usually controlled centrally by a single attacker, however in this tree like architecture it becomes virtually impossible to detect the actual attacker. The basic difference between a traditional DoS and an advanced DDoS attack is that unlike DoS

attacks DDoS attacks target infrastructure such as bandwidth rather than attacking systems.

A typical DDoS attack would generate millions of packets per second and will be targeted towards the network virtually choking it. Traditionally packets are seen to have large amounts of data in them so that the data chokes the total bandwidth capacity of the connecting network. Some attacks also use a reverse feedback technique such as a large ping packet that is sent to a network that partially chokes the upstream network but when the destination receives the packet it responds to the ping also choking the downstream network too.

DDoS attacks are the only attacks that cannot be prevented at the end point as the objective of such an attack is to choke the upstream bandwidth and disable the network. Hence, these attacks have to be stopped at the ISP end or a wider approach should be adopted and large DDoS generating networks need to be plugged to prevent global DDoS attacks. Traditionally large enterprise and university networks have been used as attack nodes to attack third part.

NetMonastery uses similar destination based algorithms to detect DDoS attacks, except that it has a few features that can sometimes reduce the impact of DDoS attacks to an extent. Features like dropping packets rather than rejecting them, reduces reverse feedback attacks and requires a double effort to create a DDoS situation. All SiteVaxinPro devices perform egress DDoS filtering too in order to prevent local networks being used as slaves in a larger attack. SiteVaxinPro has a versatile and an extremely configurable traffic anomaly detection system that is deployed only towards detecting denial of service attacks and hence increases the overall effectiveness of the network attack prevention system.

For more product information visit www.netmonastery.com/products NetMonastery bridges the gap between traditional intrusion detection systems and the cutting edge prevention technologies. The difference is in the detection technologies used and the extended attack recognition systems that are built only for the intrusion prevention space and may not be relevant in the intrusion detection space.

Global Headquarters

F - 109, Kailash Industrial Complex, Park Site,
Vikhroli (west), Mumbai 400079, INDIA

Tel: +91 22 30965080

Email: sales@netmonastery.com



NetMonasteryTM
Monitoring Internet Security

Copyrights 2004 NetMonastery Network Security Private Limited. All rights reserved worldwide

SiteVaxinPro is trademark of NetMonastery Network Security Pvt. Ltd. logo are registered trademark, of NetMonastery Network Security Pvt. Ltd. All other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.