Combating DoS/DDoS Attacks Using Cyberoam

Eliminating the DDoS Threat by Discouraging the Spread of Botnets
Introduction

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have increased in number. Take note: saying THAT would be a gross understatement.

Back in the comfortable past, only people with specialized knowledge and a good amount of resources were able to launch such high-end attacks. Today, anyone with access to the Internet and minimal technical know-how can very well execute and succeed in launching such attacks. In fact, these attacks have become a favourite tool not only among criminal enterprises and political operatives, but also disgruntled customers, ex-employees and social protesters.

Findings from a recent study titled “European Distributed Denial of Service (DDoS) Attacks & Impact Report” by Neustar, a provider of real-time information and analysis, reveal a substantial increase in the complexity, length and cost of DDoS attacks on businesses. 40 percent of companies estimate hourly losses near $150,000 - a 470 percent increase from last year; 26 percent of companies said brand/consumer trust is the biggest loss as a result of a DDoS attack; more than one-third of DDoS attacks affected businesses from one to two days.

Know-How of DDoS Attacks

A Denial of Service (DoS) attack is an attempt to make a system unavailable to its intended users. One common method of attack involves saturating the target system with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered unavailable. Another method is to exploit an open vulnerability of the target system in such a way that it becomes useless for any further service.

A Distributed Denial of Service (DDoS) attack is the attack where a collection of compromised systems perform a DoS Attack on a single target. Nowadays, such attacks are essentially launched using Botnets.

What are Botnets?

A Botnet is a network of compromised systems whose scope typically extends across the globe. Hackers take control of many vulnerable computers at a time by infecting them with malware (called "bots"). These computers then become “zombies”, which operate as part of a powerful "botnet" controlled by a master called “bot-herd”. After a computer is taken over by a bot, it can be used to carry out a variety of automated tasks like spreading viruses and spyware, stealing personal information, click fraud, and the primary one among them being DDoS attacks. DDoS attacks are fuelled by the increasing popularity and ease of acquisition of such Botnets. Ready access botnets are available for hire for a minimal amount in the digital black market. Using forums and dedicated web sites botmasters advertise botnet-availability and allow attackers to easily utilize a bot network and execute attacks.

DDoS Attack Mechanisms

Early DDoS attacks strictly exploited low-level protocols in Layers 3 and 4. Today, the attacks have spread their leg onto the Layer 7 (Application Layer) too. In fact, many attacks use a combination of vectors, for instance, mixing network floods with Application Layer strikes (HTTP Attacks).

For detailed article, click here.
Attacks over TCP, UDP, IP and ICMP (Layer 3 and 4)

Simple Network Attacks (Layers 3 and 4) mainly involve flooding target systems with traffic over the lower layers of the network stack. These attacks typically include:

<table>
<thead>
<tr>
<th>Attack</th>
<th>Effect on Target System</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN flood</td>
<td>Fake TCP connection setup overflows tables in stateful devices.</td>
</tr>
<tr>
<td>Conn flood</td>
<td>Real, but empty, connection setup overflows tables in stateful devices.</td>
</tr>
<tr>
<td>UDP flood</td>
<td>Floods server with UDP packets. Consumes bandwidth and CPU.</td>
</tr>
<tr>
<td>Ping flood</td>
<td>Floods of these control messages overwhelm stateful devices.</td>
</tr>
<tr>
<td>ICMP fragments</td>
<td>Hosts allocate memory for fragment reassembly, then run out of memory</td>
</tr>
<tr>
<td>Smurf attack</td>
<td>Exploits misconfigured routers to amplify an ICMP flood by getting every device in the network to respond with an ICMP broadcast</td>
</tr>
<tr>
<td>Christmas tree</td>
<td>Packets with all flags set except SYN consume more CPU than normal packets</td>
</tr>
<tr>
<td>SYN/ACK, ACK, ACK/PUSH floods</td>
<td>SYN-ACK, ACK, or ACK/PUSH without first SYN cause host CPUs to spin, checking the flow tables for connections that aren’t there</td>
</tr>
<tr>
<td>LAND</td>
<td>Identical source and target address IPs consume host CPU as they process these invalid addresses</td>
</tr>
<tr>
<td>Fake TCP</td>
<td>TCP sessions that look real, but are only recordings of previous TCP sessions; enough can consume flow tables and avoid SYN flood detection</td>
</tr>
<tr>
<td>Teardrop</td>
<td>Sends a stream of IP fragments; meant to exploit an overlapping fragment problem present in some systems</td>
</tr>
</tbody>
</table>

DNS Attacks (Layer 7)

Nearly all systems on the Internet rely on DNS queries to reach their intended destination, which makes DNS the most critical of all services, and also a potential single point of failure. When DNS is disrupted, all external services (not just a single application) are affected. The relatively simple, UDP-based DNS protocol enables DNS attacks to be easy to generate and difficult to defend against. This virtue of the DNS service makes it quite a tempting target for attackers who are looking to brew trouble on a large scale. Typically DNS attacks include UDP Floods and overwhelming of DNS servers using Legitimate Queries for non-existent hosts.

HTTP Attacks (Layer 7)

Over 80 percent of modern DDoS attacks are HTTP floods that intend to take down web servers. To conventional firewall technology, these requests are indistinguishable from normal traffic, so they are simply passed through to the web servers inside the data center. The thousands or millions of attacking clients overwhelm the web servers with a massive number of requests.
Cyberoam: Hitting the DDoS Problem at its Root

Usually, we tend to consider ourselves as the damsels in distress. Ever thought that we might, knowingly or unknowingly, be the wicked witch?

Confused?

Well, it is a common practice for us to fret about how we could be possible victims of DoS or DDoS attacks. We usually concentrate on strengthening our defences against possible attacks, tighten each knot, fill up holes, and check all nooks and cronies. But, have you ever thought that we could be the perpetrators? Our resources may be exploited, our very defences used against us to cause havoc elsewhere?

Previously, we discussed about botnets where vulnerable machines are infected and made into "zombies", and then remotely controlled by botmasters to carry out their malicious activities. Well, what if resources within your network or your entire network itself have been looped into a botnet?

Cyberoam Discourages the Spreading of Botnets

Cyberoam hits the problem at its root by preventing your network from being part of any attacker's weaponry. It refuses access to bots (malicious codes that infect vulnerable machines) at the network gateway itself. It does so with the help of its varied features like the Layer 8 Human Identity-based Firewall, Web Application Firewall, Intrusion Prevention System, Anti Virus, Anti Spam, etc.

Repelling Bots at the Network Gateway

Cyberoam's Intrusion Prevention System is loaded with anti-Spyware and anti-DDoS signatures (as shown in figure 1) which prevent bots from entering your network. Any malicious attempt of lasso-ing your network, or any vulnerable resource in your network, into a botnet is stubbed at the Gateway itself.

Over and above that, Cyberoam allows you to create Threshold-based Custom IPS signatures based on both Source and Destination. These allow you to design your defences specific to the kind of traffic that your network encounters.

Cyberoam hits the problem at its root by preventing your network from being part of any attacker's weaponry.
DDoS signatures

![DDoS signatures](image)

**Figure 1**
Safeguarding Network Resources
Mostly bots approach machines in the form of malware or links in Spam mails that lead to malicious websites or download of malicious apps that load the bots onto machines. Hence, Cyberoam's Gateway Anti Virus, Gateway Anti Spam and Web and Application Filtering modules provide an added layer of protection against malware, Spam and malicious websites/apps respectively, discouraging proliferation of any kind of bots into the network at the Gateway itself.

Hardening Web Server against Manipulation
While Cyberoam's Anti Virus and Anti Spam protect against entry of bots into network resources, Cyberoam's Web Application Firewall holds the fort at the Application Layer (Layer 7) front, thus safeguarding your Web Server. Based on the Intuitive Website Flow Detector, WAF ensures the sanctity of Web Applications in response to server requests, protecting them against any kind of manipulation by malicious entities.

Cyberoam: Protecting Against DoS/DDoS Attacks
The DoS and DDoS threat has spread its influence all over the globe. All and sundry are likely to come under its radar sooner or later. Legacy systems have proved to be inadequate against their onslaught. Seeing that the attacks are taking newer and more evolved forms, Network Security Solutions have to pull up their socks and get prepared to combat them at multiple levels.

Cyberoam, with its Patent-Pending, Layer 8 Human Identity-based Firewall offers stateful and deep packet inspection for network, application and user identity-based security. The Firewall remains in a constant state of alertness against entry of any kind of suspicious traffic, thus preventing organizations from falling prey to DoS, DDoS and IP Spoofing attacks.

Cyberoam allows Administrators to configure DoS settings through which they can control the incoming packets to their network. This enables Cyberoam to prevent against most of the known Layer 3 and Layer 4 attacks such as SYN, UDP, TCP, ARP or ICMP flood, ICMP Redirect Packets, etc.

![Figure 2](image-url)
Conclusion

Attacks on networks are on the rise, ever changing and advancing in sophistication. Botnets are being used to send spam, distribute malware and above all – participate in DDoS attacks which inflict huge damage on companies. Cyberoam attempts to remove the root cause of the problem by eliminating the possibility of Cyberoam-protected networks from being part of botnets. On the other hand, Cyberoam provides enterprises with the protection techniques that are required to stop these attacks. Hence, Cyberoam not only protects your network from being a victim, but, more importantly, also prevents it from being exploited to victimize others.