Table of Contents

1 General description

It is important to hide a hacker's IP address in case of DoS attack: otherwise it is easy to block him by IP. Therefore DoS attack is in bombing of victim's servers by separate packets with fake return address. Denial of service is a result of either overflow of the rented client's bandwidth or by lack of resources on a system under attack. The latest happens due to bombing by packets that cause heavy waste of resources.

The only effective protection in the first case is in temporary renting of a wide channel and redirecting of the whole incoming traffic into that channel by BGP announcement or DNS. This kind of protection is typically offered by dedicated companies. However, an operator or a client can use it in a limited scale by themselves.

The operator or the client can arrange protection by there own means in the second case: by filtering dangerous packets from the inbound traffic before they reach the system under attack.

The typical attacks of this second kind are:

1. SYN flood: an attack by SYN packets
2. RST flood: an attack by RST packets[1]
3. fragmented UDP flood - an attack by fragmented UDP packets

Modern operating systems are capable to sustain such attacks to some degree. If it is not enough, one has to use the filtering system inserted before the system under attack.

[1] Our tests show that this kind of attack is not effective against modern OS. However, if in practice the protection against them is still required, we shall add it in the coming upgrades.