Содержание

General Description

In a DoS attack, the attacker aims to mask the return (source) address so that it cannot be blocked by IP. Therefore, a DoS attack typically consists of bombarding the victim’s servers with individual packets that contain spoofed source addresses.

Service disruption in this case occurs either due to bandwidth saturation (flooding the client’s leased channel) or as a result of sending packets that trigger excessive resource consumption on the target system.

In the first case, the only effective protection is the temporary lease of a higher-capacity channel and redirecting all incoming traffic to it via BGP announcement or DNS. This type of protection is usually provided by specialized companies, but on a limited scale it can also be implemented independently by the operator or the client.

In the second case, the operator or client can organize protection independently by filtering malicious packets from incoming traffic before they reach the target system.

Typical attacks of this type include:

1. SYN flood — attack using SYN packets
2. RST flood — attack using RST packets [1)]
3. Fragmented UDP flood — attack using fragmented UDP packets

Modern operating systems can resist these types of attacks to a certain extent. However, if built-in protection mechanisms are insufficient, the solution is to deploy a filtering system in front of the attacked system.

1)
our tests have shown that this attack is ineffective against modern operating systems; however, if operational practice shows that protection against this attack type is still required, it will be added in upcoming updates