Содержание

Protection Against UDP Flood

This type of attack is carried out using fragmented UDP packets. The target platform is forced to spend significant resources reassembling and analyzing these packets.

Protection is implemented by dropping protocol types that are not relevant to the protected site. Protocol filter configuration is described in the option Traffic Prioritization.

For a typical protected web site, the relevant protocols are HTTP and HTTPS. In this case, the configuration looks as follows:

```
http        cs0
https       cs0
default     drop
```

Convert the prepared configuration file into the internal format and load it into DPI:

```
cat my_dscp.txt | lst2dscp protocols.dscp
mv protocols.dscp /etc/dpi/protocols.dscp
service fastdpi reload
```

Similarly, protection can be implemented against DNS/NTP amplification DDoS attacks, where the incoming channel is saturated with traffic exceeding its capacity.

The effectiveness of this protection is limited by the operator’s ability to provide additional bandwidth. If the attack traffic exceeds available capacity, it becomes necessary to lease additional channels or redirect traffic to specialized mitigation services that maintain bandwidth capacity exceeding the scale of such DDoS attacks.