Содержание

Protection against UDP flood attack 3

Protection against UDP flood attack

This attack is handled by fragmented UDP packets. The target system has to spend a lot of resources to assemble and analyse them.

The protection is carried out by disabling of unnecessary protocols on the site under protection. You can learn how to configure the protocol's filter here: configuring priorities.

For a typical WEB site under protection, the required protocols are HTTP and HTTPS. Therefore the proper configuration looks like this:

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

To convert the ready configuration file into the internal format and to send it to DPI:

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

The protection against DDos attack of DNS/NTP amplification type can be arranged similarly. This attack overloads the incoming channel by the traffic that exceeds the channel's capabilities. The operation of this protection is limited by operator's ability to provide additional channel capacity. If the inbound traffic exceeds this capacity, one has to rent additional channels or redirect the traffic to dedicated services that provide a protection against such attacks. They rent very wide channels to exceed the capabilities of DDoS attacks.