Содержание

Protection against SYN flood attack

SYN flood attack leads to lack of resources on its target system. Indeed, for each SYN packet the system has to allocate some memory resources, or to look up sessions lists, or to generate the specific SYN+ACK reply. The latest contains cryptographic cookie. This requires significant CPU resources. In all cases denial of service happens at incoming rate of SYN packets from 100,000 to 500,000 per second. Note that even 1Gb/s channel allows a hacker to send up to 1.5 million packets per second to the target site.

VAS Experts DPI implements the SYN flood protection as follows:

1. Detects the attack by exceeding of SYN requests by unconfirmed clients
2. Independently replies to SYN requests: instead of the protected site
3. Arranges TCP session to the protected site after the confirmation of request by a client

Configuration parameters of this protection:

To switch the protection mode on and off (it is 0 by default, allows online modification)
Acceptable values:
0 - protection is off
1 - protection is activated automatically
2 - protection is always on

```
syncf_protection=1
```

The percentage of unconfirmed requests from the client beyond which the protection is automatically activated (the defaul value is 5 , it can be modified online)

```
syncf_unconfirmed_percent=30
```

The threshold number of syn per second (without acknowledgement), judge to be normal (defaul value is 50):

```
syncf_threshold=50
```

Alert logging (default value is 0)
Valid values:
0 - alert logging is off
1 - alert logging triggering on/off

```
syncf_trace=1
```

The interval in milliseconds of checking the syn count and the acknowledged syn count (default value is 100)

```
syncf_check_tmout=100
```

The time interval in seconds for monitoring the response to syn+ack being formed by the VAS Experts DPI (default value is 60)

```
syncf_tracking_packs_time=60
```

In the main configuration file /etc/dpi/fastdpi.conf the covered port numbers are specified (default value is 80 , can be modified online)

```
syncf_ports=80:443
```

This setting is common to all the protected sites.