Table of Contents

Protection Against SYN Flood Attack

The service can be configured via GUI. Instruction

A SYN flood attack causes excessive resource consumption on the target system, because for every incoming SYN packet the system must allocate certain memory resources or generate a special SYN+ACK response containing a cryptographic cookie, perform session table lookups, etc. — in other words, consume significant CPU resources.

In both cases, service disruption typically occurs at a SYN flood rate of 100,000–500,000 packets per second. At the same time, even a 1 Gbps channel allows an attacker to generate traffic up to 1.5 million packets per second toward the target site.

SSG provides protection against SYN flood as follows:

1. Detects an attack when the number of unconfirmed SYN requests exceeds a configured threshold
2. Responds to SYN requests on behalf of the protected site (SYN PROXY mechanism)
3. Establishes a TCP session with the protected site only after the client confirms the request

Protection Parameter Settings:

Enable protection mode (default: 0) Allowed values: 0 — protection disabled 1 — activated automatically 2 — always enabled

```
syncf_protection=1
```

Percentage of unconfirmed client requests at which protection is automatically activated (default: 5, can be changed online):

```
syncf_unconfirmed_percent=30
```

Threshold of SYN packets per second (without confirmation) considered normal (default: 50):

```
syncf_threshold=50
```

Protection event logging (default: 0) Allowed values: 0 — no 1 — log protection on/off switching

```
syncf_trace=1
```

Interval in milliseconds for checking the number of SYN and confirmed SYN packets (default: 100):

```
syncf_check_tmout=100
```

Monitoring interval in seconds for responses to SYN+ACK generated by SKAT (default: 60):

```
syncf_tracking_packs_time=60
```

In the main configuration file `/etc/dpi/fastdpi.conf`, specify the protected port numbers (default: 80, can be changed online):

```
syncf_ports=80:443
```

This setting applies globally to all protected websites.