Table of Contents

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.

SCAT 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
```

Port numbers to cover (it is 80 by default, can be modified online):

```
syncf_ports=80:443
```

The percent of unconfirmed client's requests to activate the protection (it is 5 by default, can be modified online):

```
syncf_unconfirmed_percent=30
```