Содержание

Защита от SYN flood атаки 3

Защита от SYN flood атаки

Атака SYN flood вызывает повышенный расход ресурсов атакуемой системы, так как на каждый входящий SYN пакет система должна зарезервировать определенные ресурсы в памяти, либо сгенерировать специальный SYN+ACK ответ, содержащий криптографическую cookie, осуществлять поиск в таблицах сессий и т.п., т.е. затратить существенные процессорные ресурсы. В обоих случаях отказ в обслуживании наступает при потоке SYN-flood 100000-500000 пакетов в секунду. В то же время даже гигабитный канал позволит злоумышленнику направить на атакуемый сайт поток до 1,5 миллиона пакетов в секунду.

СКАТ осуществляет защиту от SYN flood следующим образом:

1. обнаруживает атаку по превышению заданного порога неподтвержденных клиентом SYN запросов
2. самостоятельно, вместо защищаемого сайта отвечает на SYN запросы (механизм SYN PROXY)
3. организует TCP сессию с защищаемым сайтом после подтверждения запроса клиентом

Настройки параметров защиты:

Активировать режим защиты (по умолчанию 0)
Допустимые значения:
0 - защита выключена
1 - активируется автоматически
2 - включена всегда

```
syncf_protection=1
```

Процент неподтвержденных запросов со стороны клиента, при котором защита автоматически активируется (по умолчанию 5, можно менять online)

```
syncf_unconfirmed_percent=30
```

Порог количества syn в секунду (без подтверждения), когда считаем, что все нормально (по умолчанию 50):

```
syncf_threshold=50
```

Логирование срабатывания защиты (по умолчанию 0)
Допустимые значения:
0 - нет
1 - переключения срабатывания защиты on/off

```
syncf_trace=1
```

Интервал в миллисекундах проверки количества syn и подтвержденных syn (по умолчанию 100)

```
syncf_check_tmout=100
```

Интервал времени в секундах мониторинга ответа на syn+ack, сформированного скат (по умолчанию 60)

```
syncf_tracking_packs_time=60
```

В основном конфигурационном файле */etc/dpi/fastdpi.conf* указываются защищаемые номера портов (по умолчанию 80, можно менять online)

```
syncf_ports=80:443
```

Эта настройка является общей для всех защищаемых сайтов.