Блокирование попыток эксплуатации heartbeat-уязвимости в OpenSSL средствами iptables

Пример блокирования критической уязвимости CVE-2014-0160 в OpenSSL 1.0.1, позволяющей получить содержимое памяти удалённых серверных и клиентских приложений.

Отражаем в логе все heartbeat-запросы при помощи iptables и модуля u32:

```
iptables -t filter -A INPUT -p tcp --dport 443 -m u32 --u32 "52=0x18030000:0x1803FFFF"
```

Блокируем heartbeat-запросы:

```
iptables -t filter -A INPUT -p tcp --dport 443 -m u32 --u32 "52=0x18030000:0x1803FFFF"
```

Отслеживаем возможные атаки при помощи Wireshark:

```
tshark -i interface port 443 -R 'frame[68:1] == 18'
tshark -i interface port 443 -R 'ssl.record.content_type == 24'
```