SYN Flood Mitigation - Notes

Abstract
This document contains a couple of tips and notes based on questions I have received in class.

The best and easiest setup is using separate VMs and using default routes. In task 1 for example, install a VM with a webserver, say at IP 10.0.0.2. The machine with your application that stresstests the web server could be IP 10.0.0.1. When you inject packets with spoofed addresses towards B, B would send them everywhere but host A. The easiest way to fix this is to set 10.0.0.1 as the default gateway on host B:

```
sudo ip route add default via 10.0.0.1
```

All SYN+ACKs will hence return to host A. (Make sure that host A does not forward them to the Internet though!)

To capture the traffic for your measurement, your application could either use libpcap, OR you use iptables to redirect all incoming packets to your application. The syntax is straightforward: the one liner

```
sudo iptables -t nat -I PREROUTING
   -p tcp -j REDIRECT --to-ports 1234
```

solves this and forwards them to port 1234 on your local machine.

In task 2, the goal is to do DDoS mitigation. Same principle applies. The configuration for host A you now already have. The IPS is in the example acting as a DDoS scrubber. Suppose the web server is sitting at a public IP address, for example 145.94.63.13. In order to receive the traffic, the IPS must obviously take this IP address on its public facing side, otherwise it would be able to help the web server with the DDoS. On the right side of the figure, we can use local IPs, for example 10.0.0.1 for the IPS and 10.0.0.2 for host B. Now the IPS talks to your host and everything is returned to host A because the default route points it there. If the client is validated the IPS rewrites the destination IP address to 10.0.0.2. Host B can respond because it uses the IPS as the default gateway and the IPS forwards this to your measurement host.