Overview

Our code will set up the flows in the flowtable as soon as the first packet is forwarded to the controller.

The types of rules that we initially apply are as follows.

1. Forward everything as usual (low priority).
2. Block all packets with a IPv4 destination of our 10.45.7.128/25 (medium priority)
3. Forward all DNS response packets to the controller (IP src 10.45.7.2, UDP, SRC port 53) (high priority)

This should have only the DNS response packets being forwarded to our controller.

When we get future packets (DNS responses), we “parse” the DNS packet, modify it, and then forward it. If the DNS packet is a response for a lookup for our host3. The modified DNS packet will have a new IP for the lookup.

Next, we will craft a new flow rule that allows traffic for the IP that did the DNS request to Host3. (src ip Client, dest ip Host3). This rule overrides the medium priority rule that was blocking the entire range. We set the hardTimeout of this rule to be the same of the DNS response, which we got when we parsed the DNS packet.