Network Security Challenge 03 - Hard

The firewall is still in place and now has a new ruleset seen in Table 1. The ruleset is applied in the order given in the table and the server stores the state `(src, dst, src_port, dst_port)` for each connection. All packages from you to the network arrive at the firewall at eth0 and all packages from the network to you arrive at eth1.
On the server 131.159.15.68 there is a flag distribution service running on port 1337. Flags are only distributed to IPs from the trusted block 161.40.0.0/16. To avoid that somebody steals a flag, the firewall blocks all new traffic to this address.

No.	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
1	eth0	*	131.159.15.68	TCP	*	*	NEW	DROP
2	eth0	10.0.0.0/8	*	UDP	*	53	EST	ACCEPT
3	eth0	*	*	ICMP	*	*	*	ACCEPT
4	eth0	*	*	TCP	*	*	EST	ACCEPT
5	eth0	161.40.0.0/16	*	*	*	*	*	DROP
6	eth0	*	*	*	*	*	*	DROP
7	eth1	*	10.0.0.0/8	TCP	*	80	NEW	ACCEPT
8	eth1	131.159.15.68	*	TCP	*	7331	EST	ACCEPT
9	eth1	*	8.8.8.8	UDP	*	53	NEW	ACCEPT
10	eth1	10.0.0.0/8	*	UDP	53	*	EST	ACCEPT
11	eth1	131.159.15.68	*	TCP	*	*	EST	DROP
12	eth1	*	*	TCP	*	*	EST	ACCEPT
13	eth1	*	*	ICMP	*	*	*	ACCEPT
14	eth1	*	*	*	*	*	*	DROP

Table 1: Firewall ruleset.

You can “send packets” through the firewall by sending a line in the following format: `{src_ip},{dst_ip},{protocol},{src_port},{dst_port}`. If you send the correct packet through the firewall, you will get the flag.

Exercise 3–2 is hosted at `netsec.net.in.tum.de` at port 20203.
We recommend connecting to the server using `netcat (man nc)` first. It is advisable to have a Linux system at hand for the challenges. Our servers and clients are written in python.