

INFO-0045: Introduction to Computer Security

Project 1 - Firewalls
Part 3 - iptables Rules

Maxime Goffart
180521

Olivier Joris
182113

Academic year 2021 - 2022

1 Implementation of the rules

1.1 NAT rules

We implemented rules concerning incoming traffic (SSH, SMTP, or IMAPS) using the `PREROUTING` chain and the `DNAT` target (static NAT).

We implemented rules concerning traffic staying inside the network (SSH relay and PWEB) using the `POSTROUTING` chain and the `SNAT` target (static NAT).

We implemented rules concerning outgoing traffic using the `POSTROUTING` chain and the `MASQUERADE` target (dynamic NAT).

1.2 Firewall rules

Because the firewalls are not source or destination of packets exchange in the network, we decided to adopt a policy dropping traffic related to `INPUT` and `OUTPUT` chains. Our implemented rules thus only deal with the `FORWARD` chain.

Because we wanted that our firewalls act as stateful firewalls, we needed to allow traffic related to accepted connection using this command : `iptables -A FORWARD -m conntrack -ctstate RELATED,ESTABLISHED -j ACCEPT`.

The commands implementing our firewall rules all follow a same scheme : `iptables -A FORWARD -p protocol [-d destination-ip] [-s source-ip] -dport destination-port -m conntrack -ctstate NEW -j <ACCEPT | DROP | LOG>`. These rules are implemented in their priority orders because we used the `-A` option.

2 Performed tests

We tested to the maximum the behavior of our firewalls to see if our implementation does not contain any issue. It is more difficult to see if there are no problems with what is not allowed than with what is allowed. It is why last firewall rules are there : they deny by default. The test we have done are listed below.

- We tested that `HONEYPOT` can share the `/home/sharing` directory with the NFS server.
- We tested that `U3` can synchronize files with the `RSYNC` server on the Vlad account (including through the SSH relay which implies secured `RSYNC`).
- We tested that `HONEYPOT` is reachable through the SSH relay.
- We tested that `U1` and `U2` can obtain one IP address through their respective DHCP relays.
- We tested that `U1` can access `LWEB` using the ftp and http protocol.
- We tested that `U2` can access `LWEB` using the http protocol.
- We tested that `U1` and `U2` are reachable using the SSH relay.
- We tested that `U1` and `U2` can perform http(s) requests through the http(s) proxy. We also did some http(s) request using domain name to test the requests to `LDNS` and `PDNS`.

- We tested that U1 and U2 can send mails inside and outside the network.
- We tested that U1 can connect to the SSH relay and not U2.
- We tested that DT can connect to the SSH relay and it is reachable through the SSH relay.
- We tested that DT can access PWEB using the http and https protocols and domain names (PDNS).
- We tested that PWEB is reachable from the SSH relay.