

LAB: Filtering (UFW)

Lab Environment

The workshop WiFi:

- SSID: `workshop`
- PASS: `iiij/2497`

Hosts - Virtual machines (Ubuntu 18.04LTS/LXC)

- Hostname: `nsXX.workshop`
- IPv6: `fd00:2497:1::X`
- IPv4: `10.0.0.X`

Where `X` and `XX` is your group ID. For group 1, hostname is `ns01.workshop`, IPv6 address is `fd00:2497:1::1`, and IPv4 is `10.0.0.1`.

Check UFW status

UFW (Uncomplicated Firewall) is filtering management package bundled with recent Linux distributions.

Check the current status of UFW using the `ufw` command.

```
$ sudo ufw status
```

By default, UFW is inactivated.

Activate UFW

The default policy of UFW is deny all the incoming connections. Before activating UFW, we need to setup a ssh filtering rule, otherwise, we will lose ssh access from outside just after activating UFW.

```
$ sudo ufw allow ssh
```

And activate UFW.

```
$ sudo ufw enable
```

Check the status.

```
$ sudo ufw status
```

`ufw allow ssh` is equal to `ufw allow 22/tcp`. You can specify the rules in more detailed manner whenever needed.

Check the filter

Now the only ssh port is accessible. Check what happens.

- HTTP
- DNS

Check which ports are open using `nmap`.

Open ports

Now the only ssh port is available on your virtual server. You cannot access your web server anymore.

Add a new rule to allow HTTP and DNS access.

```
$ sudo ufw allow http
$ sudo ufw allow domain
```

Close ports

You have two different filter rules to close a port.

```
$ sudo ufw deny http
```

```
$ sudo ufw reject http
```

What are the difference?

Delete rules

If you don't need some rules anymore, you can delete rules. First, check the index of each rule.

```
$ sudo ufw status numbered
Status: active
```

	To	Action	From
	--	-----	----
[1]	22/tcp	ALLOW IN	Anywhere
[2]	80/tcp	ALLOW IN	Anywhere
[3]	53	ALLOW IN	Anywhere
[4]	22/tcp (v6)	ALLOW IN	Anywhere (v6)
[5]	80/tcp (v6)	ALLOW IN	Anywhere (v6)
[6]	53 (v6)	ALLOW IN	Anywhere (v6)

Remove a rule by specifying the rule index.

```
$ ufw delete 2
```

You need to check the index each time whenever you remove multiple rules, since the index number will change after deletion.

Fine grained rulesets

If you want to access to your web server from a specific client, you can specify the rule as below, for example.

```
$ sudo ufw allow proto tcp from 10.0.0.2 to any port 80
```