Lab8 – Snort

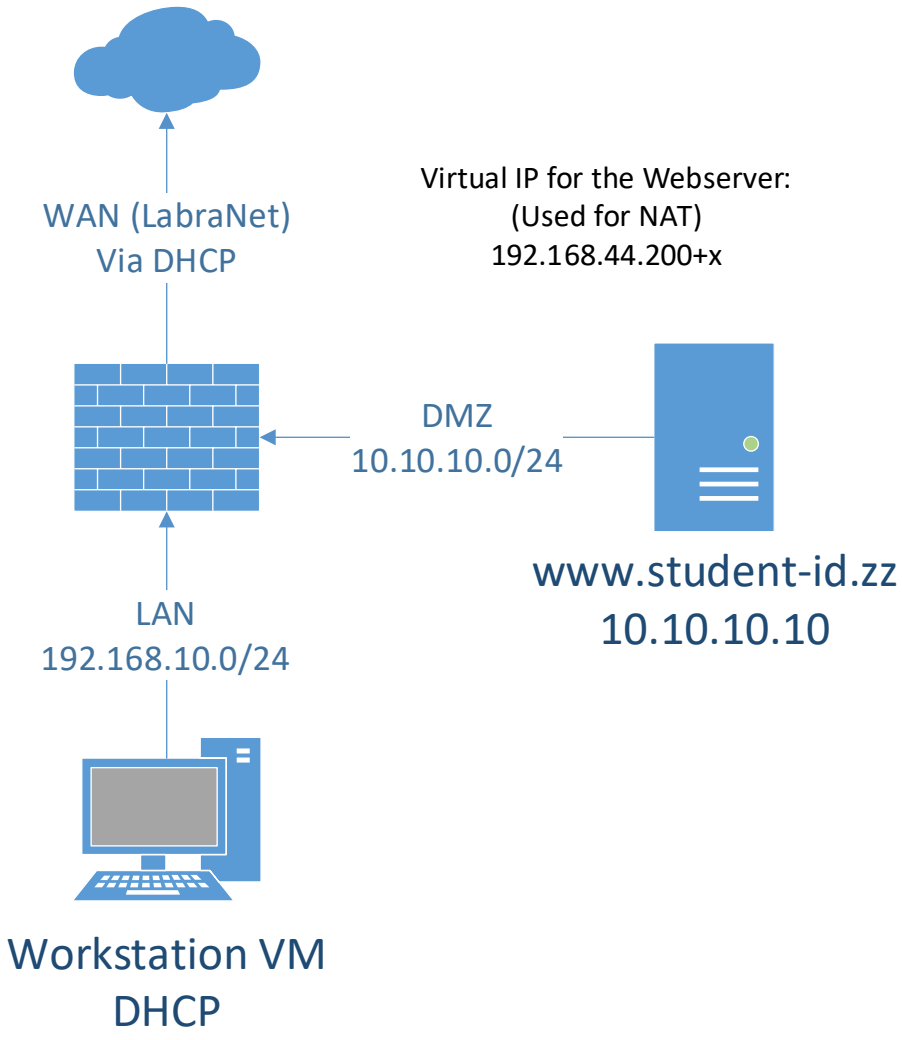
You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ at the end of the line is used to mark that the command needs to be on one line. Replace **student-id** with your own student-id and **x** or **y** as your VMs correct IP in the labs.

NOTE! The subsequent labs will have more complex topology. The Firewall will have two internal networks (intnet) with names LAN and DMZ, the third network is bridged.

This lab uses the topology from basic firewalling lab, so make sure that is already set up. Snort will be installed on the PfSense firewall as a package.

You will also need a Kali VM for testing to generate attacks against the webserver. You can use on in the templates-folder or provide your own.



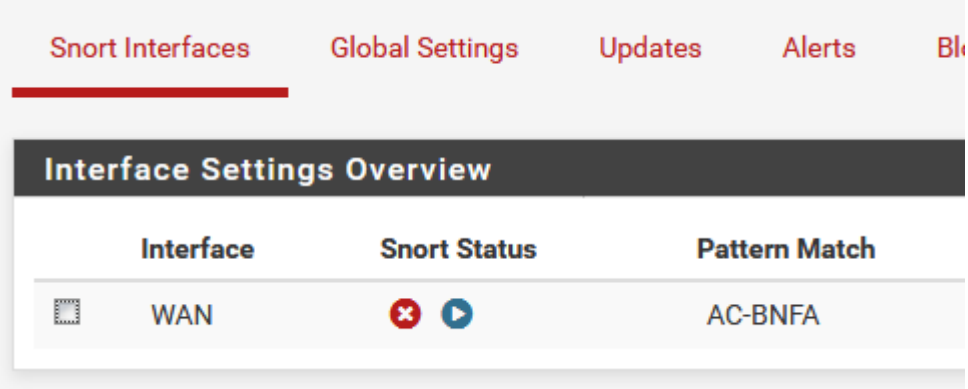
- **Install Snort**

In the PfSense, install Snort (System - Packages - Available Packages).

NOTE, it might be required to upgrade the PfSense installation before package installation (System - Update). This might take few minutes, let the firewall finish the update before doing any more work.

After installation, Snort can be found under Services - Snort. Configure few basic settings first:

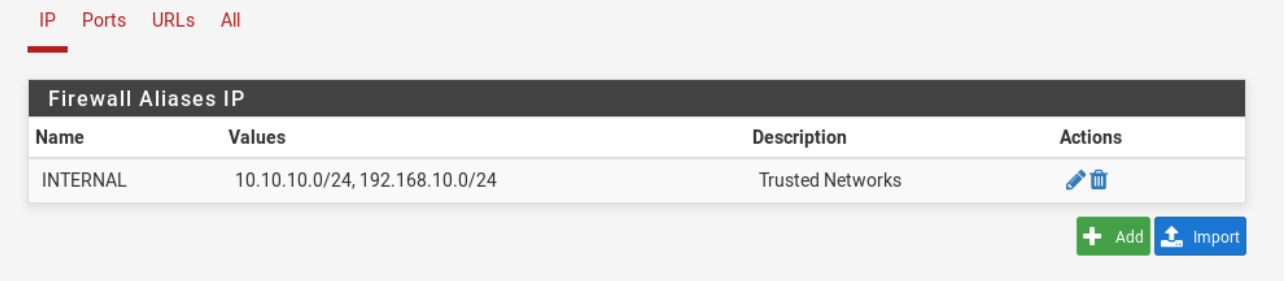
- Global Settings: Enable Snort GPLv2 rules
- Updates: fetch the newest list of rules.
- Snort Interfaces: enable Snort on WAN-interface.
- Snort Interfaces: WAN - WAN Categories: Enable the community ruleset
- Snort Interfaces: Start Snort by pressing the small play-button:



- **Snort Networks**

For Snort to work correctly, you have to create an Alias that tells Snort which networks are local (Home Net). Steps to do this are:

- Create a firewall alias (Firewall - Aliases) with the name INTERNAL. Add your internal networks only to this alias (192.168.10.0/24 and 10.10.10.0/24)

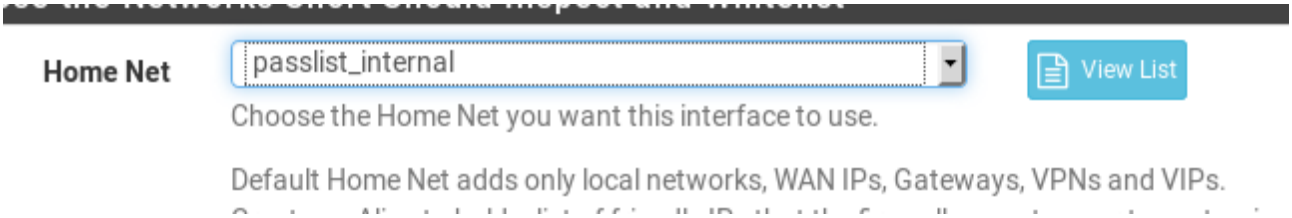


  - luotetut verkot

- Create a snort Pass List with the name passlist_internal and set Assigned Alias to INTERNAL

  - kerrotaan, snortille, että minkä aliaksen ipt ovat luotettuja

- Under WAN Interface settings, set Home Net to passlist_internal



Restart WAN interface processing under Snort Interfaces.

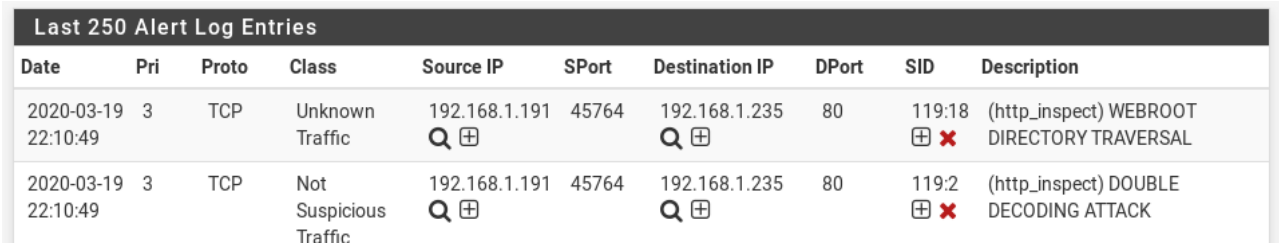
- **Testing**

Now you can test the webserver. Launch a Kali VM and first check that you can access the webserver using the NAT IP of the firewall. You are doing the attacking from OUTSIDE the LAN/DMZ network, so make sure the Kali VM is Bridged to the classroom IP pool. Do some basic nikto scanning against the NAT IP (for example ***nikto -h***). This should generate alerts.

Find where the alerts are located in the PfSense and what rules are triggered.

/services/snort/alerts

-

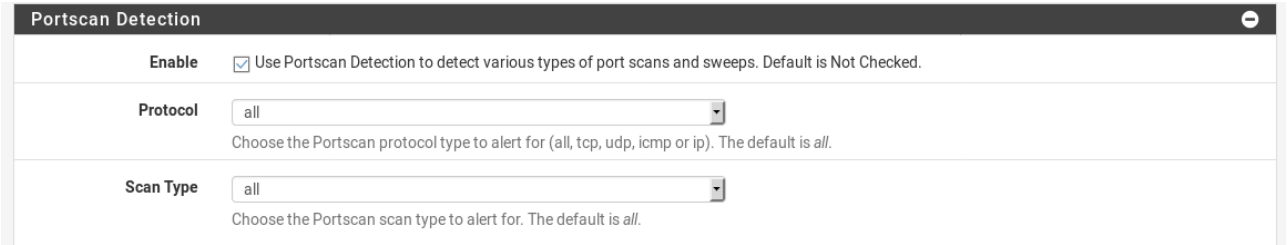


- **Port scans**

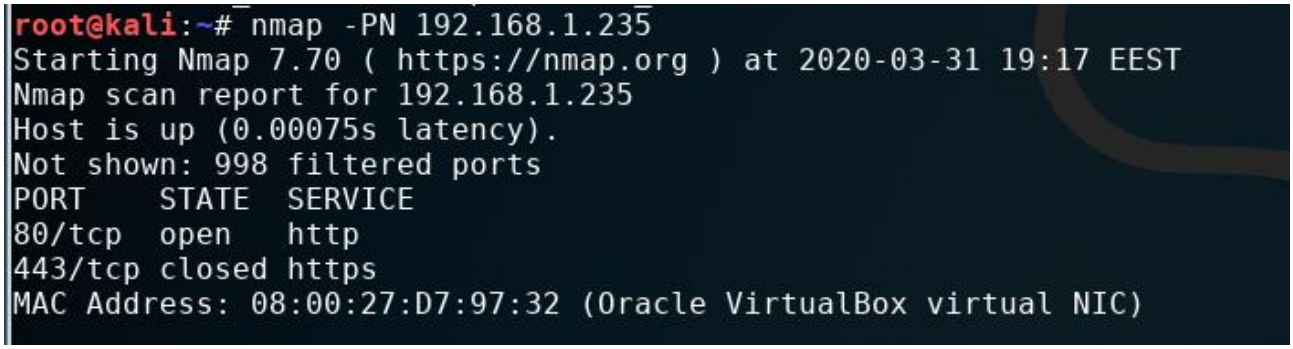
Try to do a port scan against the NAT IP with nmap (for example **nmap -PN**). This should succeed by default.

Find where in the Snort WAN Interface settings you can enable port scan detection. Enable port scan detection for all types of scans and test that scanning now generates alerts.

  - Services/Snort/Edit interface / Wan / Wan Preprocs



NOTE! If your Home Net is not set correctly under the WAN Interface settings, Snort may think that port scan is coming from a trusted source. Make sure you have the correct networks under INTERNAL alias. Also check the Virtual IP netmask from previous lab, if it is /24, the whole classroom network will be regarded as home network.

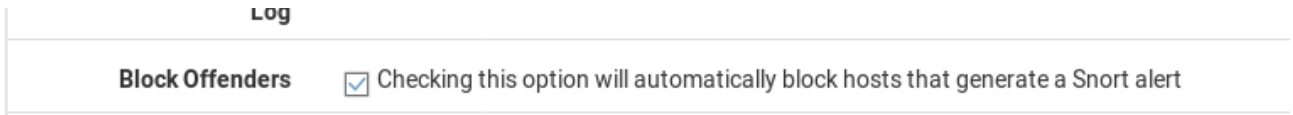


- **Blocking**

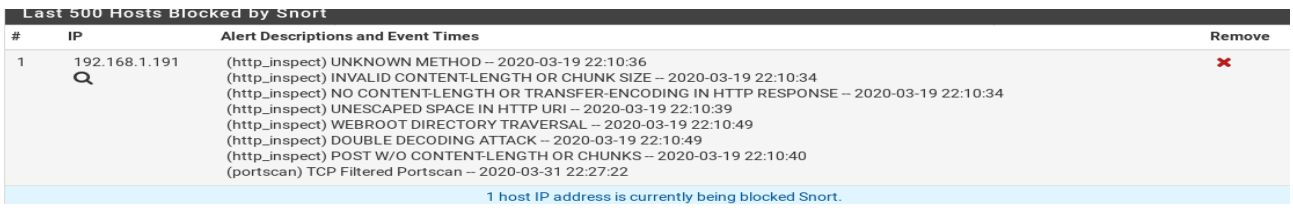
By default Snort is set to Alert on attacks. Set it to block offenders as well. Test by using any attack.

Find where you can remove a blocked entry from the lists. Find also how you can suppress a single rule.

If you are done, generate some more advanced attacks using Kali and see what rules they trigger.



- Kyseisen täpän valittua, snort blokkaa ne osoitteett, joista tulee hälytyksen generoivaa liikennettä.



- snortin alert description listassa näkyy hyökkäyksen tiedt, ja ip osoite.