Lab8 – Snort

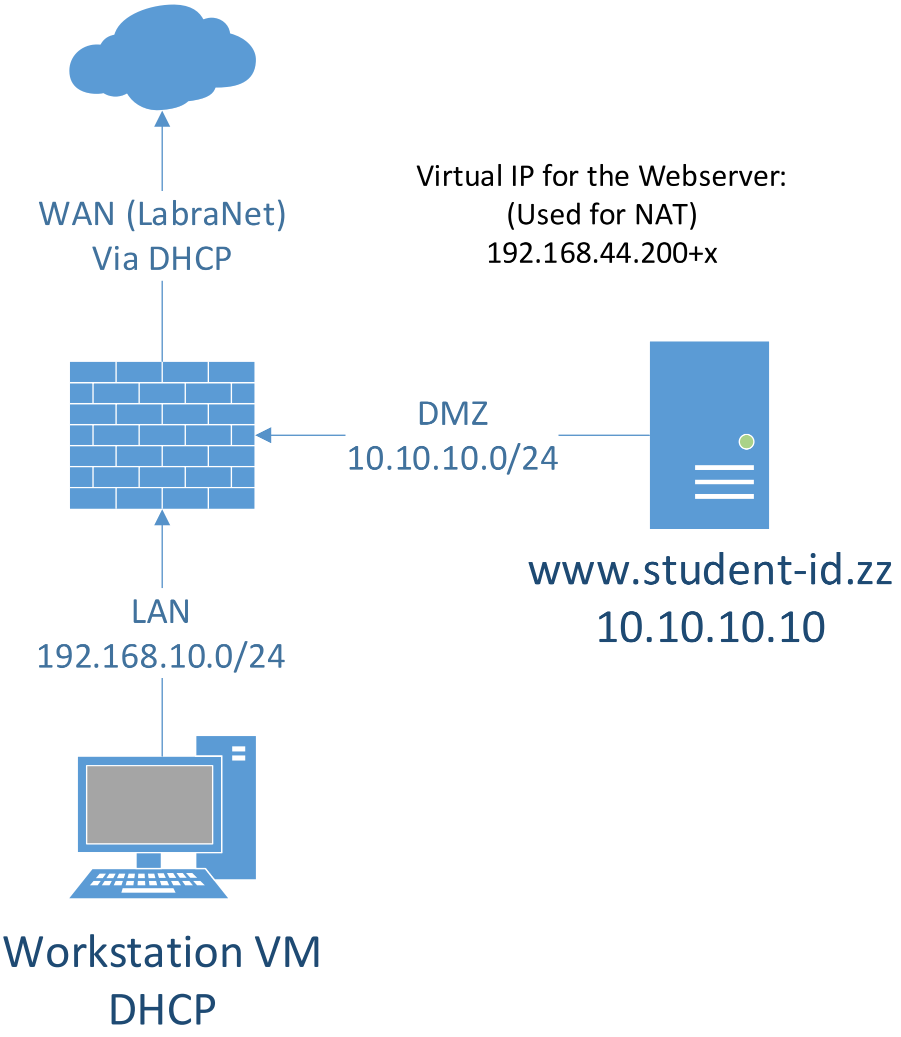
You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ 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.

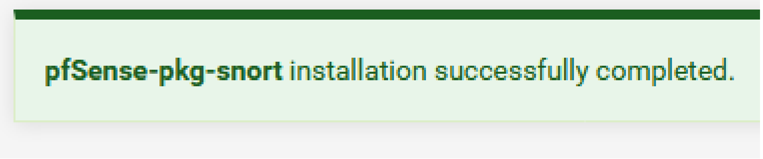
This lab uses the topology from basic firewalling lab, so make sure that is already set up. Snort will be installed on the PfSense firewall as a package.

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.

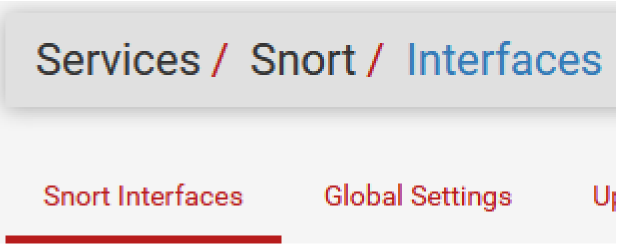


- **Install Snort**

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



pfSense-pkg-snort installation successfully completed.



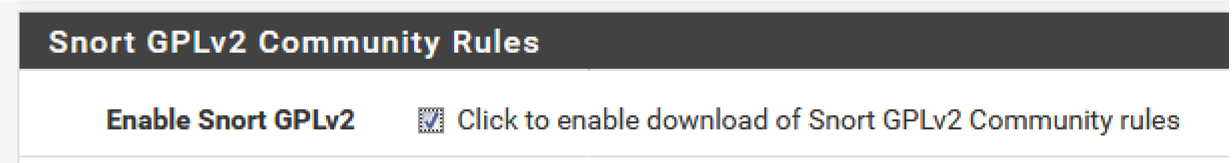
Services / Snort / Interfaces

asensin snortin

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:

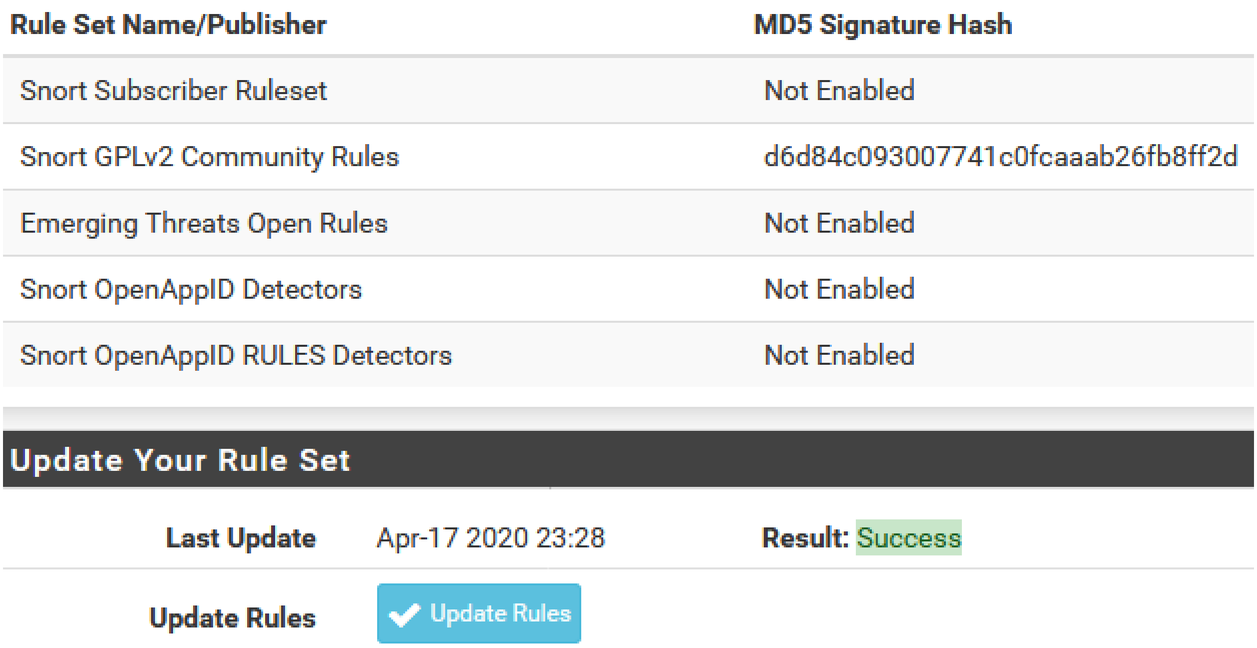
- Global Settings: Enable Snort GPLv2 rules



Snort GPLv2 Community Rules

Enable Snort GPLv2 ☑ Click to enable download of Snort GPLv2 Community rules

- Updates: fetch the newest list of rules.



Rule Set Name/Publisher	MD5 Signature Hash
Snort Subscriber Ruleset	Not Enabled
Snort GPLv2 Community Rules	d6d84c093007741c0fcaaab26fb8ff2d
Emerging Threats Open Rules	Not Enabled
Snort OpenAppID Detectors	Not Enabled
Snort OpenAppID RULES Detectors	Not Enabled

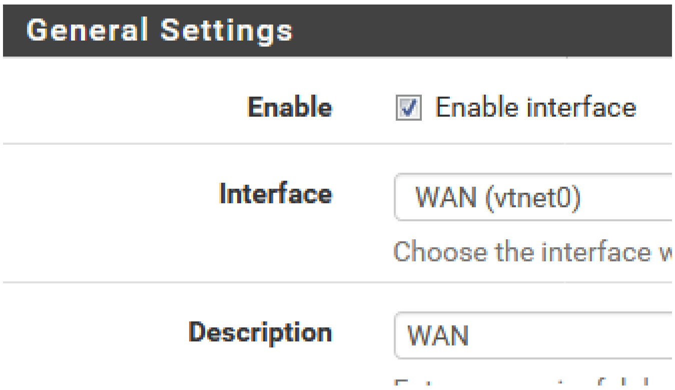
Update Your Rule Set

Last Update Apr-17 2020 23:28 **Result:** Success

Update Rules ✓ Update Rules

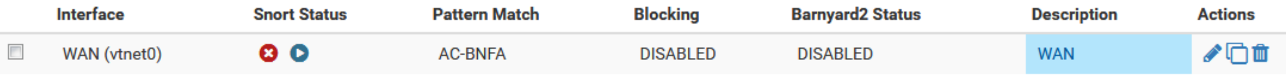
Päivitin säännöt

- Snort Interfaces: enable Snort on WAN-interface.



General Settings

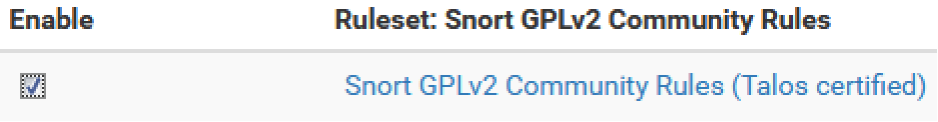
Enable	☑ Enable interface
Interface	WAN (vtnet0) Choose the interface w
Description	WAN



	Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
□	WAN (vtnet0)	☒ ▶	AC-BNFA	DISABLED	DISABLED	WAN	

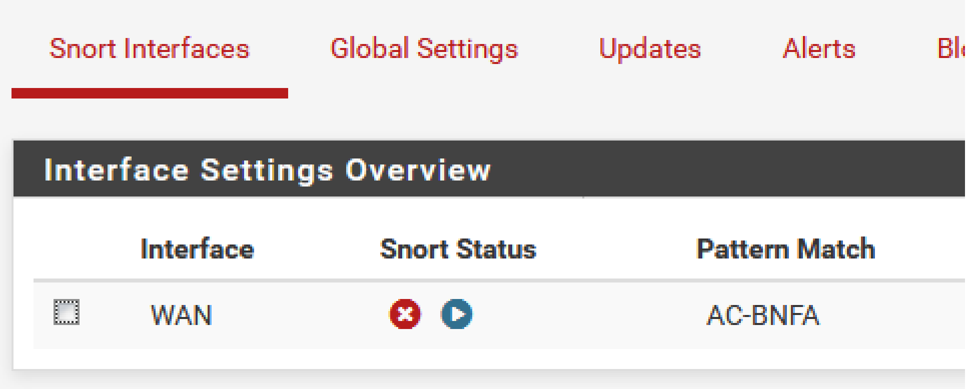
enabloin WAN-interfacen

- Snort Interfaces: WAN - WAN Categories: Enable the community ruleset



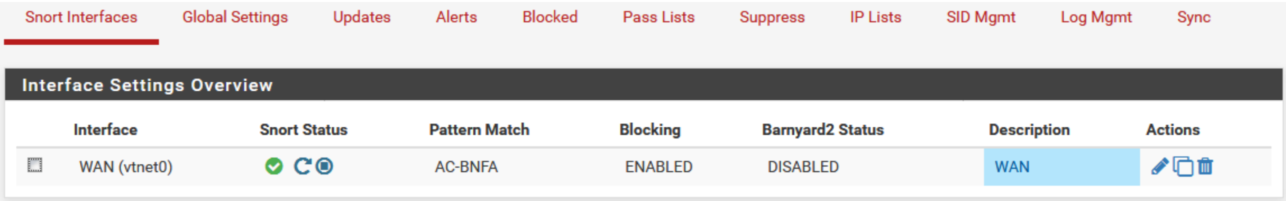
Enable	Ruleset: Snort GPLv2 Community Rules
☑	Snort GPLv2 Community Rules (Talos certified)

- Snort Interfaces: Start Snort by pressing the small play-button:



Interface Settings Overview

	Interface	Snort Status	Pattern Match
□	WAN	☒ ▶	AC-BNFA



Interface Settings Overview

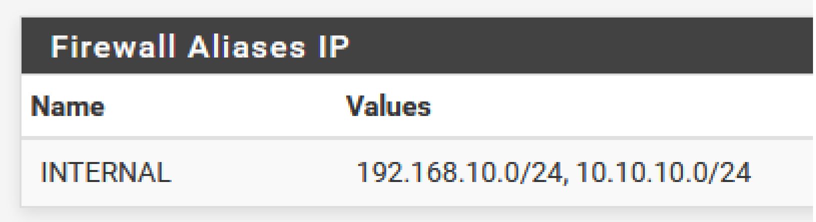
	Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
□	WAN (vtnet0)	✓ ↻ ●	AC-BNFA	ENABLED	DISABLED	WAN	

käynnistin snortin

- ### 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)

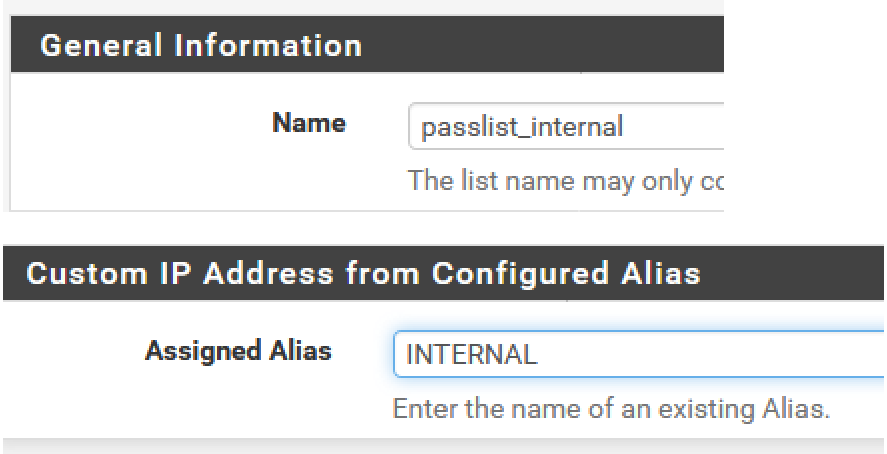


Firewall Aliases IP

Name	Values
INTERNAL	192.168.10.0/24, 10.10.10.0/24

alias ipt

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



General Information

Name: passlist_internal

The list name may only cc

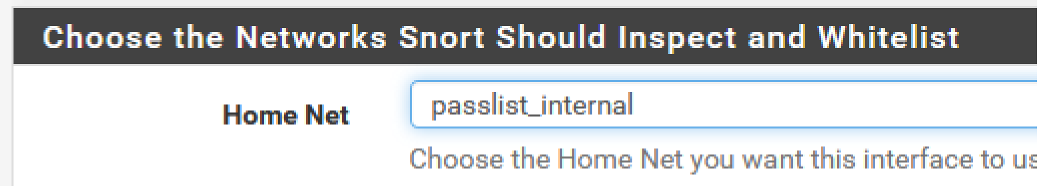
Custom IP Address from Configured Alias

Assigned Alias: INTERNAL

Enter the name of an existing Alias.

muutoksen snort pass listiin

- Under WAN Interface settings, set Home Net to passlist_internal



Choose the Networks Snort Should Inspect and Whitelist

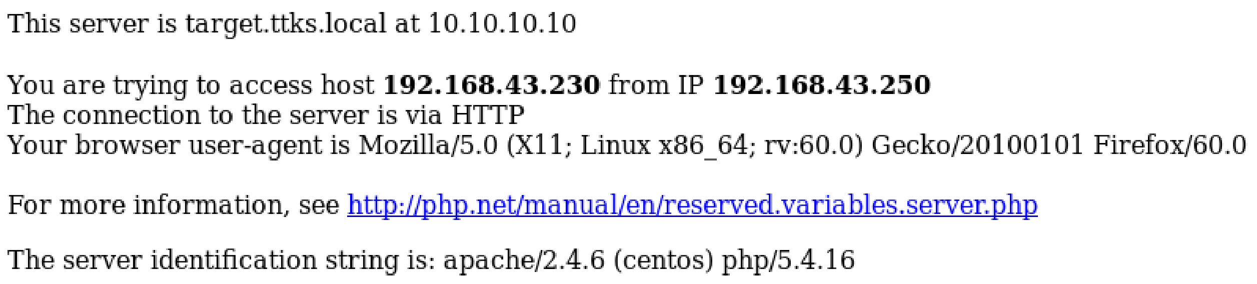
Home Net: passlist_internal

Choose the Home Net you want this interface to us

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.



This server is target.ttks.local at 10.10.10.10

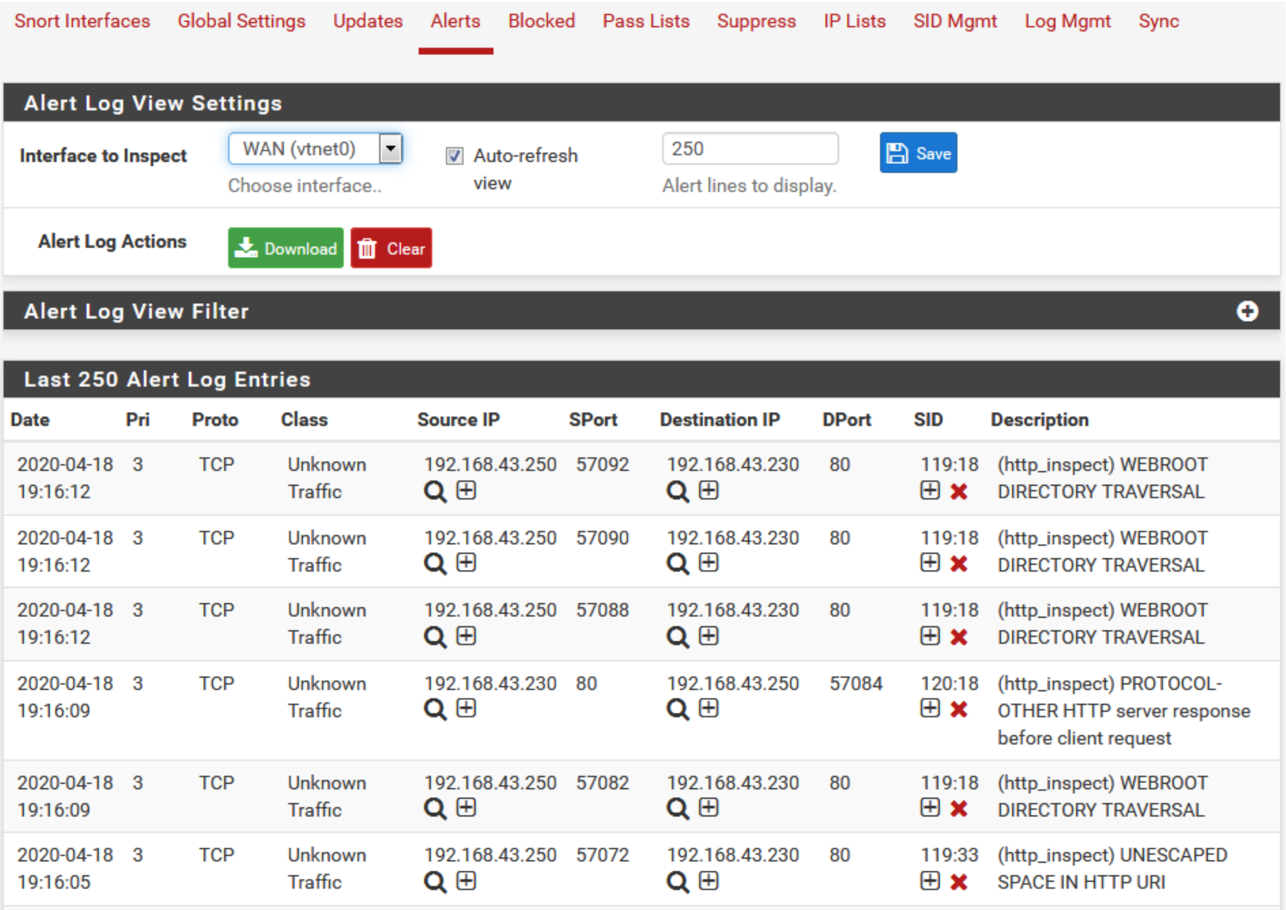
You are trying to access host **192.168.43.230** from IP **192.168.43.250**
The connection to the server is via HTTP
Your browser user-agent is Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

For more information, see http://php.net/manual/en/reserved.variables.server.php

The server identification string is: apache/2.4.6 (centos) php/5.4.16

servu löytyy

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



Alert Log View Settings

Interface to Inspect: WAN (vtnet0) — Choose interface..

☑ Auto-refresh view

250 — Alert lines to display.

Alert Log Actions

Alert Log View Filter

Last 250 Alert Log Entries

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2020-04-18 19:16:12	3	TCP	Unknown Traffic	192.168.43.250	57092	192.168.43.230	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2020-04-18 19:16:12	3	TCP	Unknown Traffic	192.168.43.250	57090	192.168.43.230	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2020-04-18 19:16:12	3	TCP	Unknown Traffic	192.168.43.250	57088	192.168.43.230	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2020-04-18 19:16:09	3	TCP	Unknown Traffic	192.168.43.230	80	192.168.43.250	57084	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2020-04-18 19:16:09	3	TCP	Unknown Traffic	192.168.43.250	57082	192.168.43.230	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2020-04-18 19:16:05	3	TCP	Unknown Traffic	192.168.43.250	57072	192.168.43.230	80	119:33	(http_inspect) UNESCAPED SPACE IN HTTP URI

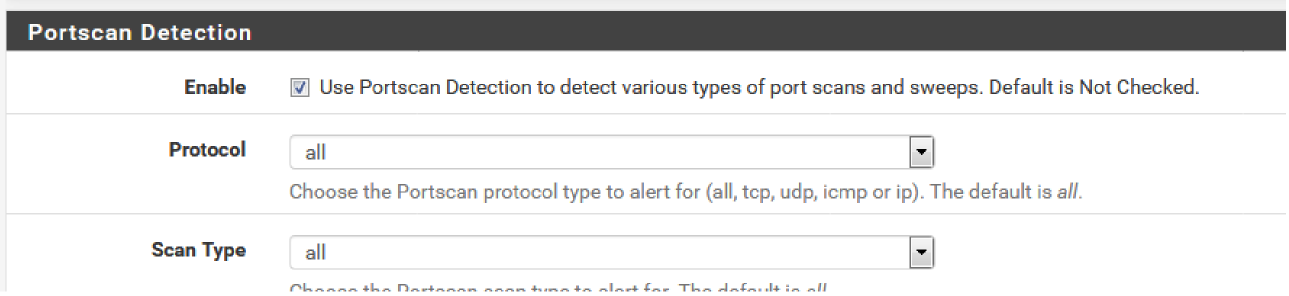
alertit löytyy snortin alert välilehden alta

triggerit: webrot directory traverse, protocol other http, double decoding attack, unescaped space in http uri, no content length or transfer encoding in http response, invalid content-length or chunk

- ## 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.

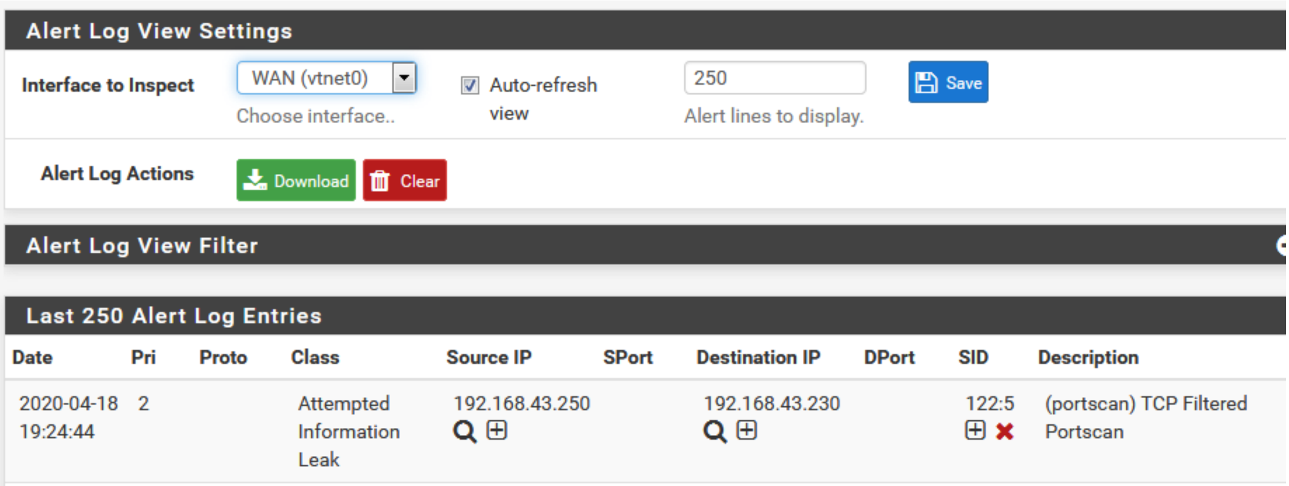


Portscan Detection

Enable ☑ Use Portscan Detection to detect various types of port scans and sweeps. Default is Not Checked.

Protocol all
Choose the Portscan protocol type to alert for (all, tcp, udp, icmp or ip). The default is *all*.

Scan Type all
Choose the Portscan scan type to alert for. The default is all.



Alert Log View Settings

Interface to Inspect WAN (vtnet0)
Choose interface..

☑ Auto-refresh view

250
Alert lines to display.

Alert Log Actions

Alert Log View Filter

Last 250 Alert Log Entries

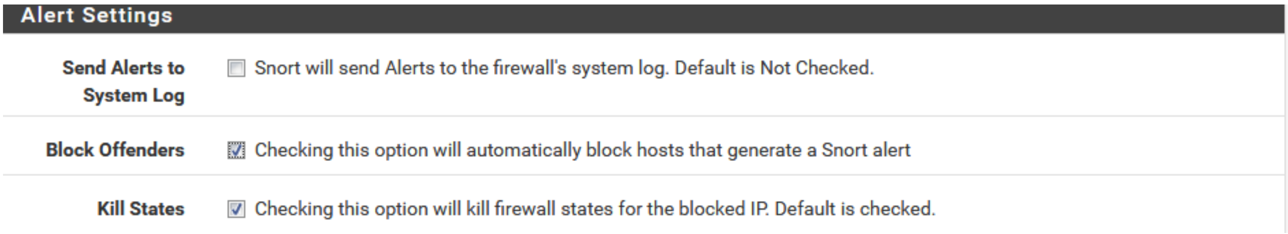
Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2020-04-18 19:24:44	2		Attempted Information Leak	192.168.43.250 🔍 ⊞		192.168.43.230 🔍 ⊞		122:5 ⊞ ✖	(portscan) TCP Filtered Portscan

alertteja syntyy

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.



Alert Settings

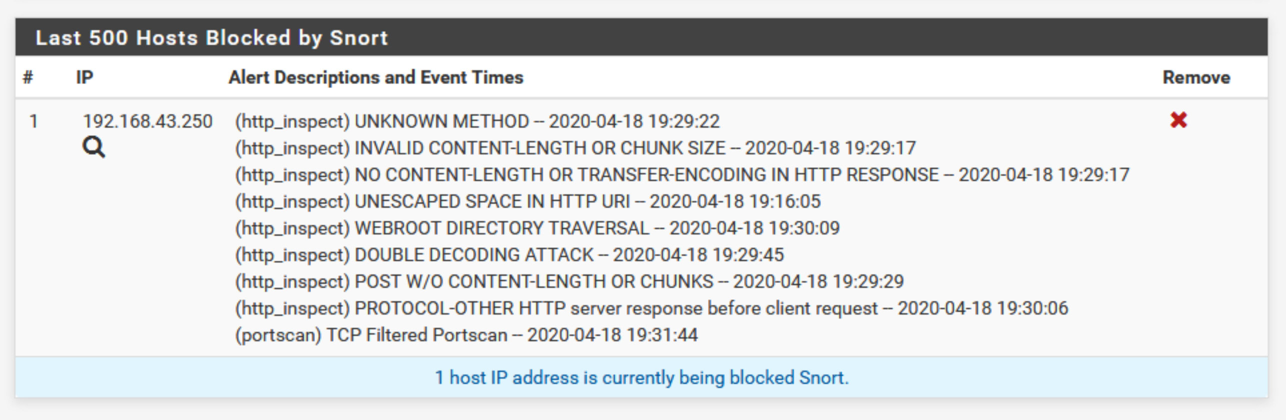
Send Alerts to System Log □ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Block Offenders ☑ Checking this option will automatically block hosts that generate a Snort alert

Kill States ☑ Checking this option will kill firewall states for the blocked IP. Default is checked.

löytyy snort -> wan settings-> alert settings

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

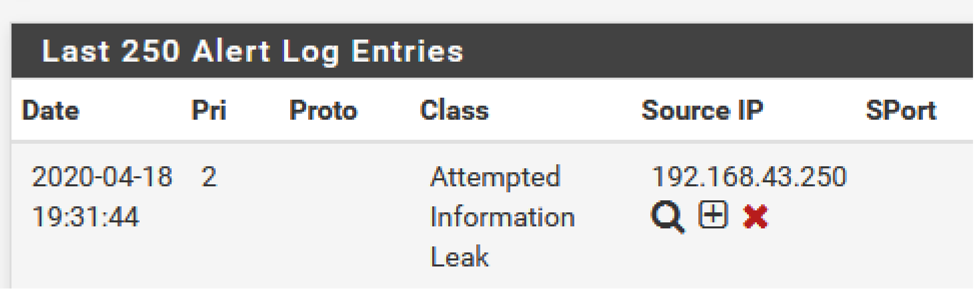


Last 500 Hosts Blocked by Snort

#	IP	Alert Descriptions and Event Times	Remove
1	192.168.43.250 🔍	(http_inspect) UNKNOWN METHOD – 2020-04-18 19:29:22 (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE – 2020-04-18 19:29:17 (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE – 2020-04-18 19:29:17 (http_inspect) UNESCAPED SPACE IN HTTP URI – 2020-04-18 19:16:05 (http_inspect) WEBROOT DIRECTORY TRAVERSAL – 2020-04-18 19:30:09 (http_inspect) DOUBLE DECODING ATTACK – 2020-04-18 19:29:45 (http_inspect) POST W/O CONTENT-LENGTH OR CHUNKS – 2020-04-18 19:29:29 (http_inspect) PROTOCOL-OTHER HTTP server response before client request – 2020-04-18 19:30:06 (portscan) TCP Filtered Portscan – 2020-04-18 19:31:44	✖

1 host IP address is currently being blocked Snort.

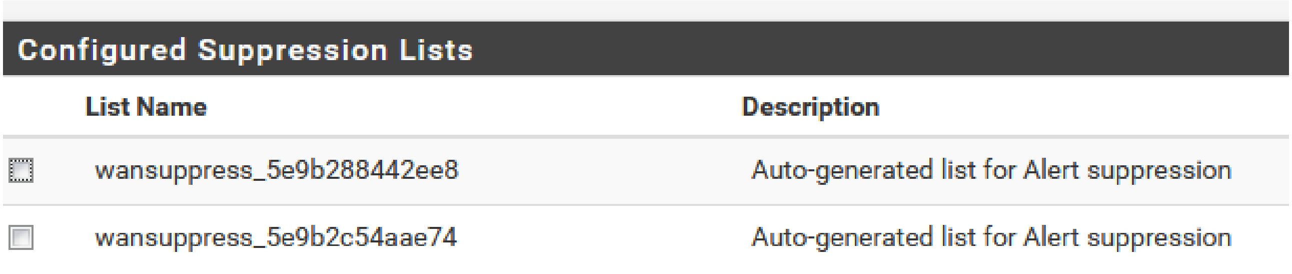
löytyy snort->blocked



Last 250 Alert Log Entries

Date	Pri	Proto	Class	Source IP	SPort
2020-04-18 19:31:44	2		Attempted Information Leak	192.168.43.250 🔍 ⊞ ✖	

tuosta plussasta kuin painaa niin toimii

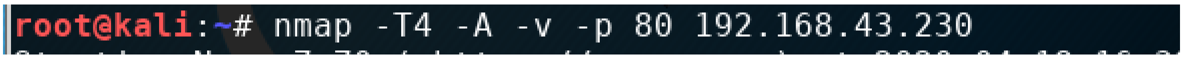


Configured Suppression Lists

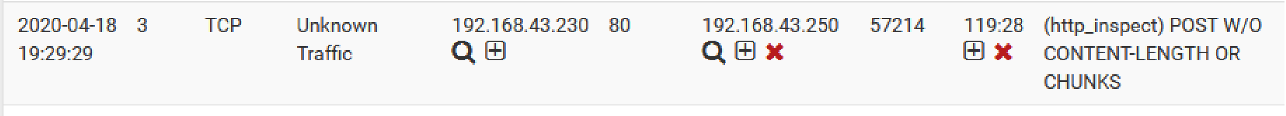
	List Name	Description
☐	wansuppress_5e9b288442ee8	Auto-generated list for Alert suppression
☐	wansuppress_5e9b2c54aae74	Auto-generated list for Alert suppression

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

kokeilin nmap -T4 -A -v -p 80 192.168.43.230 ja sain tuollaisen alertin, muuten tuli paljon samoja kuin aikaisemmin.



```
root@kali:~# nmap -T4 -A -v -p 80 192.168.43.230
```



2020-04-18 19:29:29	3	TCP	Unknown Traffic	192.168.43.230 🔍 ⊞	80	192.168.43.250 🔍 ⊞ ✖	57214	119:28 ⊞ ✖	(http_inspect) POST W/O CONTENT-LENGTH OR CHUNKS