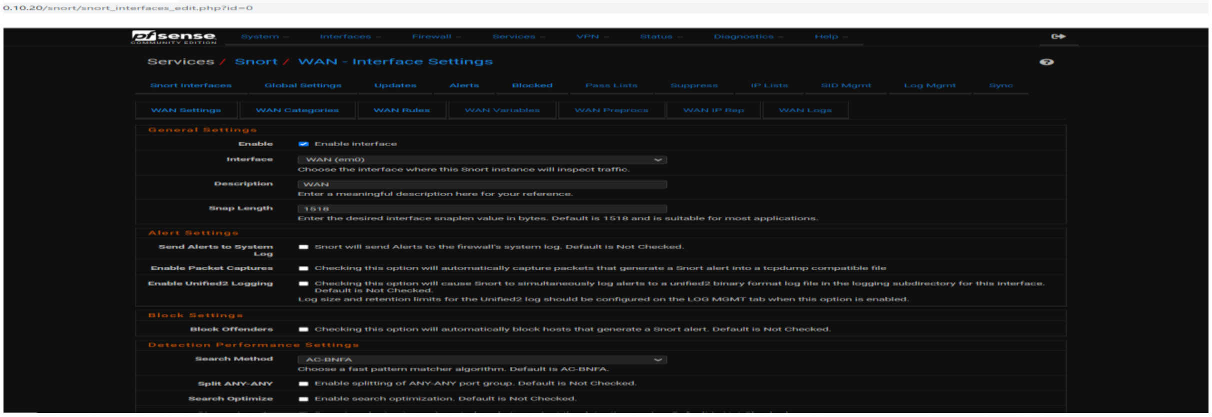
Q3).. Step1→configure the snort



Services / Snort / WAN - Interface Settings

General Settings

Enable ☑ Enable interface

Interface: WAN (em0)
Choose the interface where this Snort instance will inspect traffic.

Description: WAN
Enter a meaningful description here for your reference.

Snap Length: 1518
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

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

Enable Packet Captures □ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Enable Unified2 Logging □ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings

Block Offenders □ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

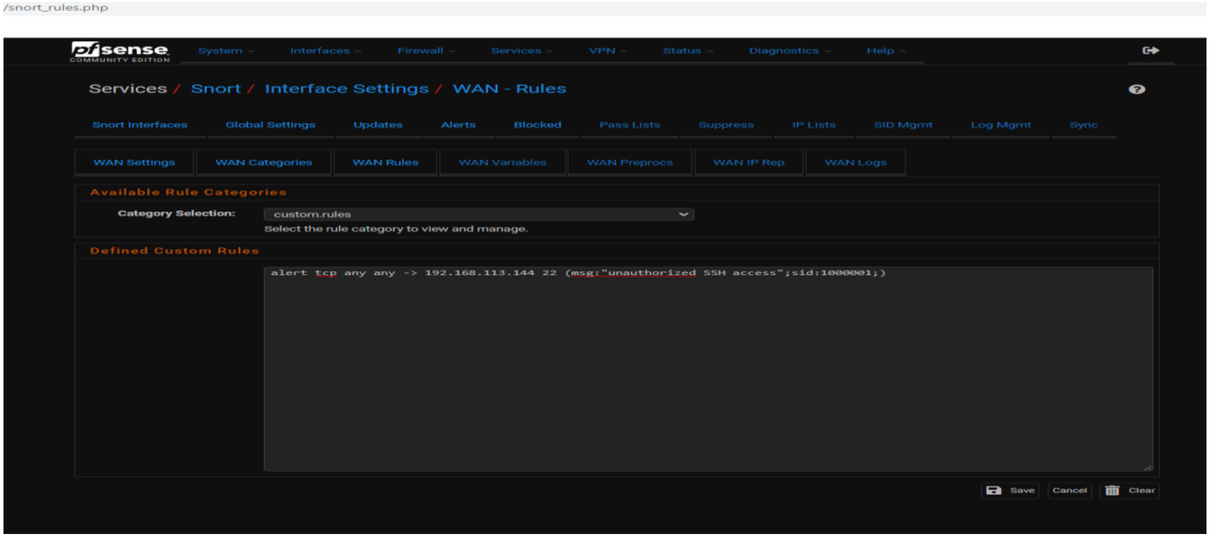
Detection Performance Settings

Search Method: AC-BNFA
Choose a fast pattern matcher algorithm. Default is AC-BNFA.

Split ANY-ANY □ Enable splitting of ANY-ANY port group. Default is Not Checked.

Search Optimize □ Enable search optimization. Default is Not Checked.

Step2→goto WAN rules and select category custum rules..and save it



Services / Snort / Interface Settings / WAN - Rules

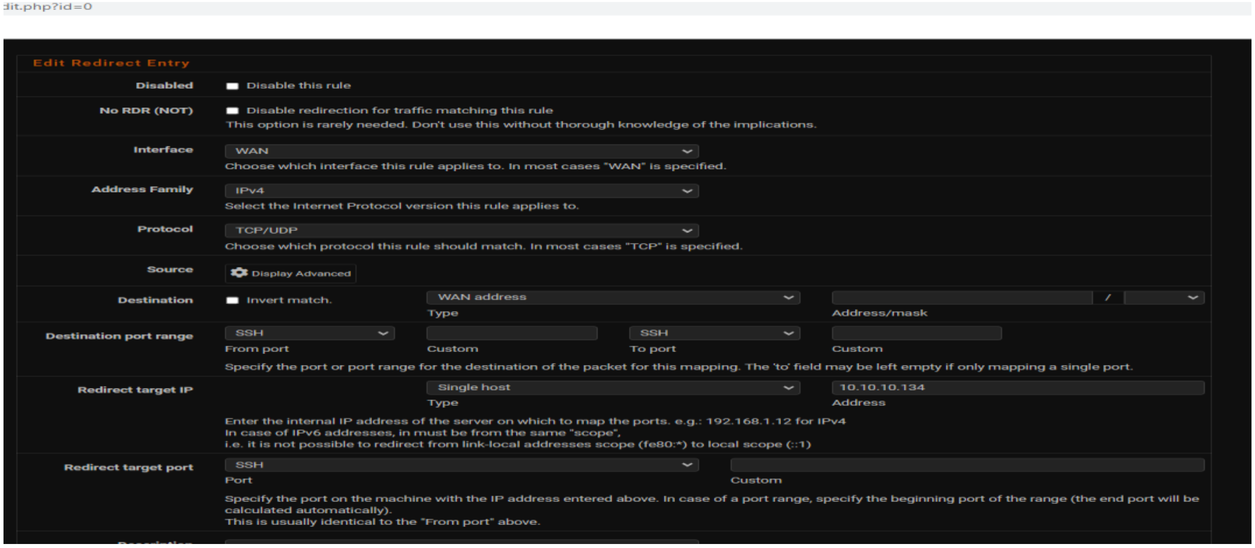
Available Rule Categories

Category Selection: custom.rules
Select the rule category to view and manage.

Defined Custom Rules

```
alert tcp any any -> 192.168.113.144 22 (msg:"unauthorized SSH access";sid:1000001;)
```

Step3→goto firewall NAT configuration and set the client ip to alerts msg



Edit Redirect Entry

Disabled □ Disable this rule

No RDR (NOT) □ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface: WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP/UDP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

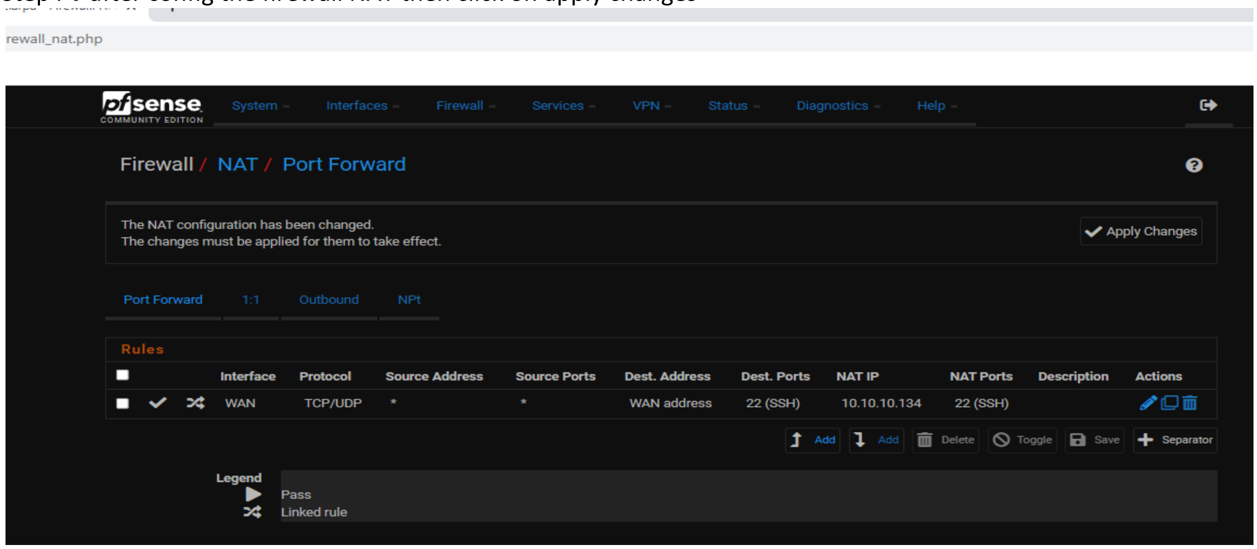
Destination □ Invert match. Type: WAN address Address/mask: /

Destination port range: From port: SSH Custom: To port: SSH Custom:
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP: Type: Single host Address: 10.10.10.134
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port: Port: SSH Custom:
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Step4→after config the firewall NAT then click on apply changes



Firewall / NAT / Port Forward

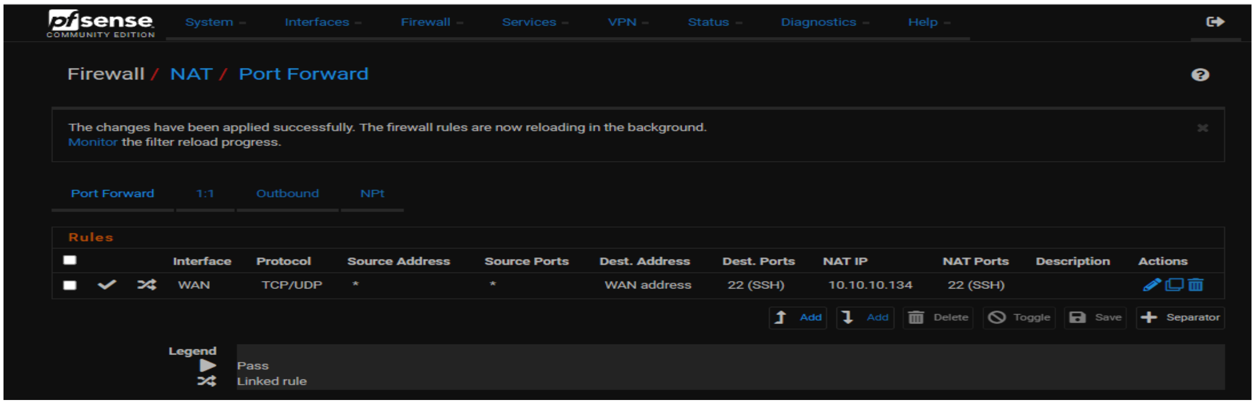
The NAT configuration has been changed.
The changes must be applied for them to take effect.

Rules

□			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤮	WAN	TCP/UDP	*	*	WAN address	22 (SSH)	10.10.10.134	22 (SSH)		

Legend
▶ Pass
⤮ Linked rule

Step5→ the change s have been applied successfully



Firewall / NAT / Port Forward

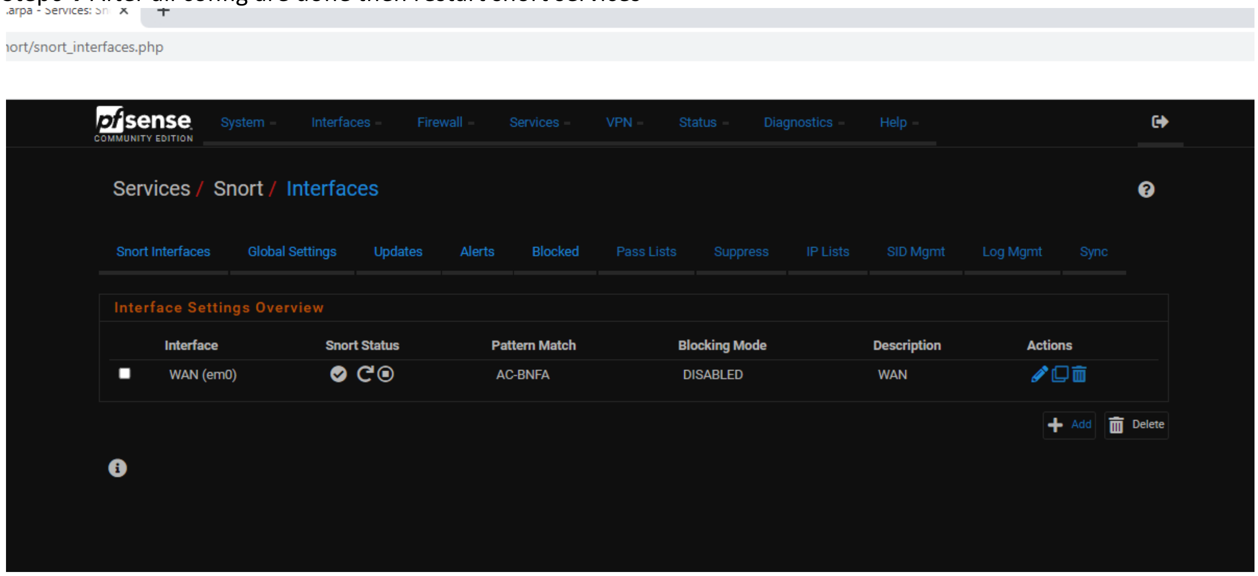
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules

□			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤮	WAN	TCP/UDP	*	*	WAN address	22 (SSH)	10.10.10.134	22 (SSH)		

Legend
▶ Pass
⤮ Linked rule

Step6→After all config are done then restart snort services

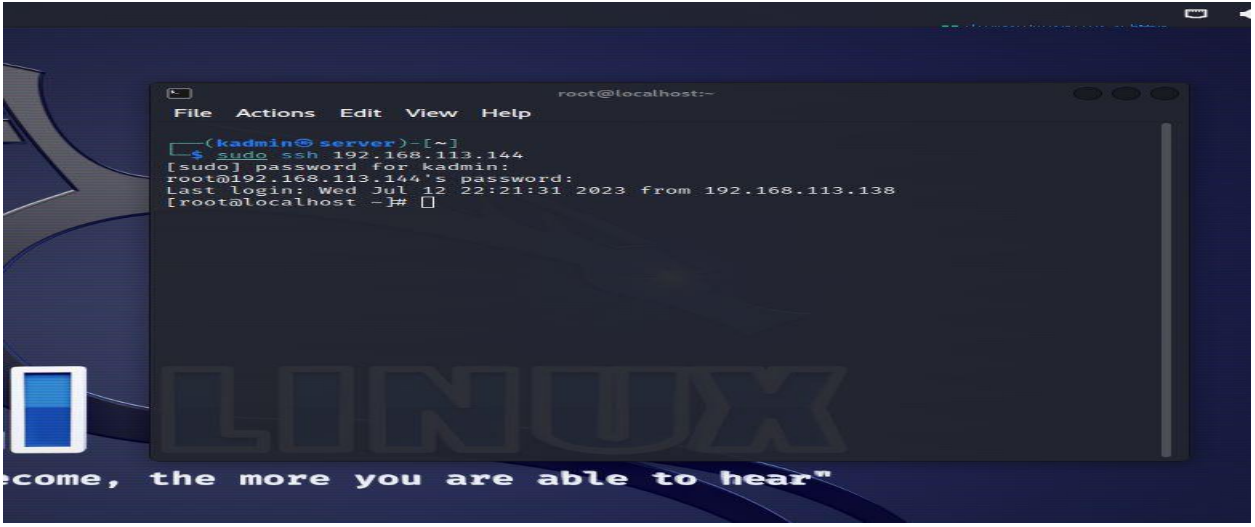


Services / Snort / Interfaces

Interface Settings Overview

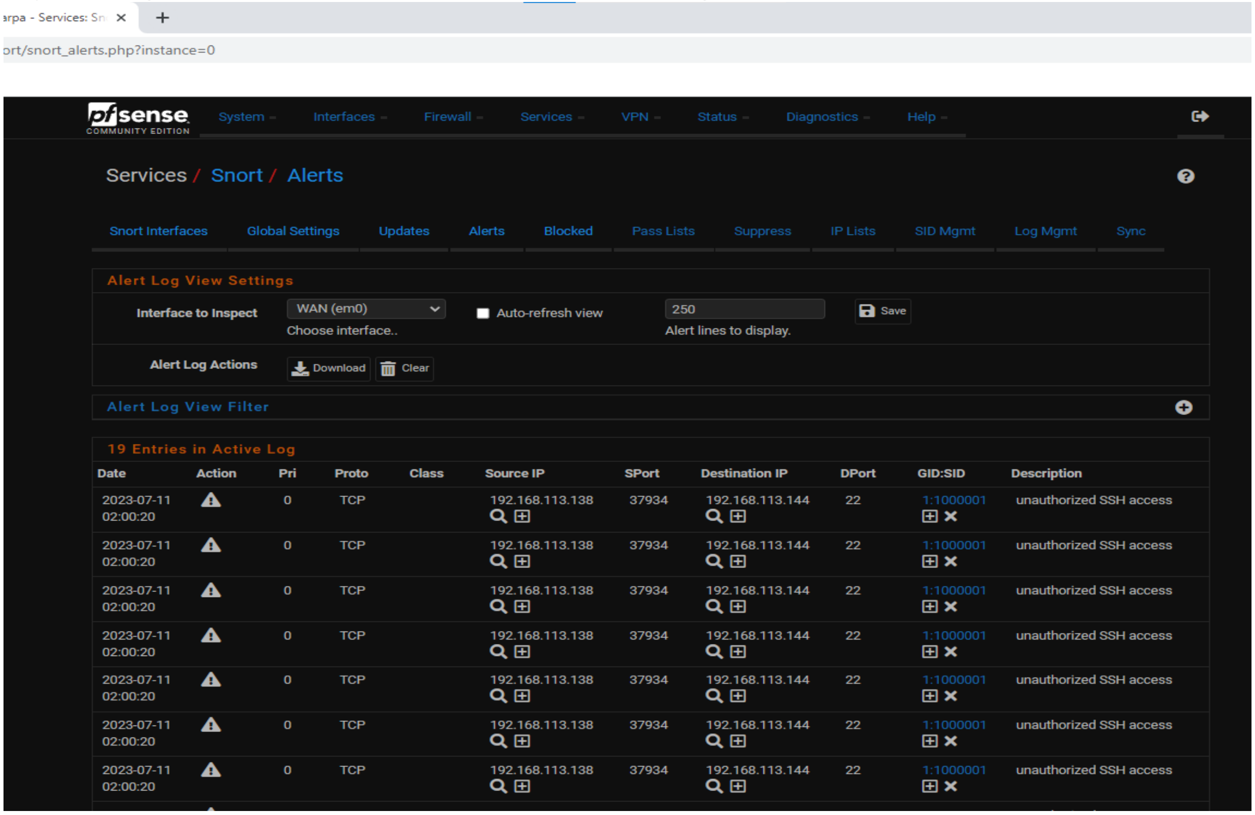
	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	WAN (em0)		AC-BNFA	DISABLED	WAN	

Step7→then goto another machine and ssh to pfsense NAT ip(192.168.113.144)



```
┌──(kadmin㉿ server)-[~]
└─$ sudo ssh 192.168.113.144
[sudo] password for kadmin:
root@192.168.113.144's password:
Last login: Wed Jul 12 22:21:31 2023 from 192.168.113.138
[root@localhost ~]# □
```

Step8→then goto alert tab in snort services and see the alert msgs "unauthorized SSH access"



Services / Snort / Alerts

Alert Log View Settings

Interface to Inspect: WAN (em0)
Choose interface..

□ Auto-refresh view

250
Alert lines to display.

Alert Log Actions

Alert Log View Filter

19 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-07-11 02:00:20	⚠	0	TCP		192.168.113.138	37934	192.168.113.144	22	1:1000001	unauthorized SSH access
2023-07-11 02:00:20	⚠	0	TCP		192.168.113.138	37934	192.168.113.144	22	1:1000001	unauthorized SSH access
2023-07-11 02:00:20	⚠	0	TCP		192.168.113.138	37934	192.168.113.144	22	1:1000001	unauthorized SSH access
2023-07-11 02:00:20	⚠	0	TCP		192.168.113.138	37934	192.168.113.144	22	1:1000001	unauthorized SSH access
2023-07-11 02:00:20	⚠	0	TCP		192.168.113.138	37934	192.168.113.144	22	1:1000001	unauthorized SSH access
2023-07-11 02:00:20	⚠	0	TCP		192.168.113.138	37934	192.168.113.144	22	1:1000001	unauthorized SSH access
2023-07-11 02:00:20	⚠	0	TCP		192.168.113.138	37934	192.168.113.144	22	1:1000001	unauthorized SSH access