# why we need security

->

# how to secure:

->

# information security management

1) information classification : how crucial is the data

# How to find the data is crucial or not?

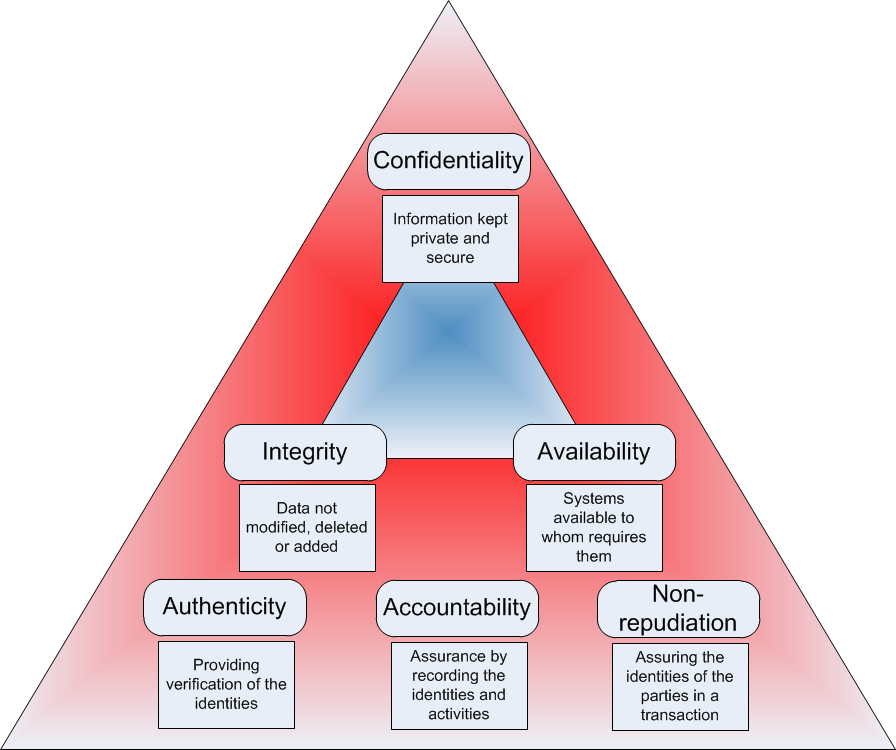
# CIA Triad

-> Confidentiality : disclosure of information to unauthorised users

-> Integrity : unauthorised modification of the information

-> Availability : information is not available to authorised users

-> Privacy : Problem with an individual's information



# birthdate is very important date

2) Asset Identification : identify all assets that store,use or transmit the critical information of the organisation

Tangible Assets:

1. Computers, routers, switches,storages, backups devices, pen drives,CDS

Intangible Assets:

-> employee storing information in their memory

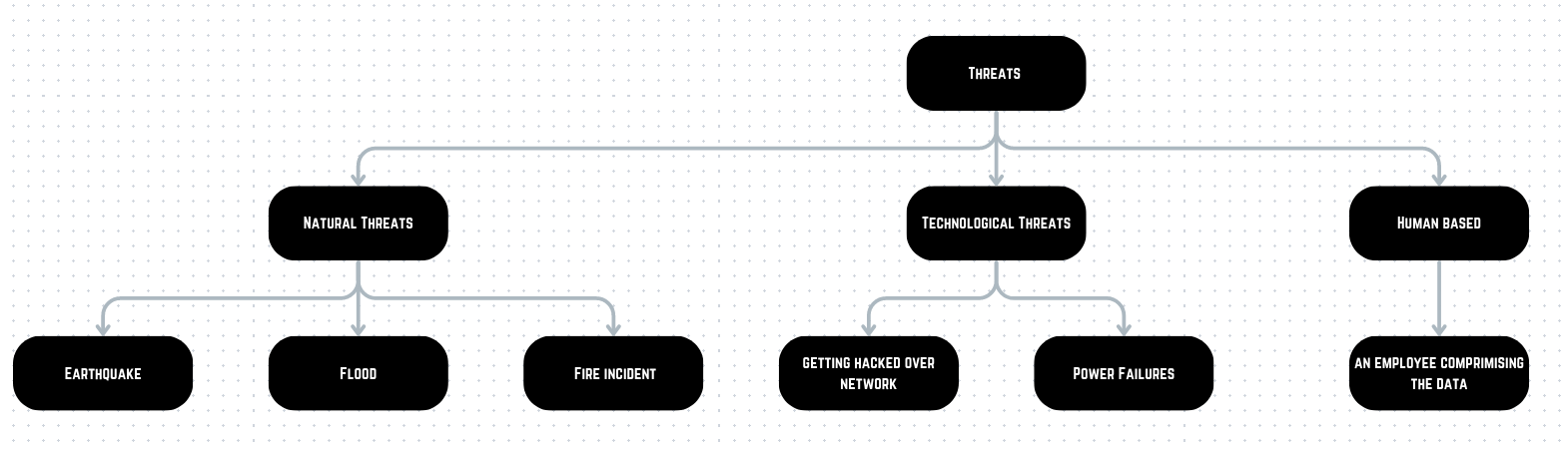
3) Threat Identification :

-> vulnerability: weaknesses in a system/software/human

-> threat : possible event which can have negative impact

-> exploit : it is a method by which we can take advantage of a vulnerability to gain unauthorised access

-> Risk : financial or other loss due to a threat



Threat agent: entity that performs the threat

Motive: Purpose of performing threat

4) Risk assessment:

-> assign risk rating for each critical threat identified

5) Risk mitigation:

-> Risk avoidance

-> avoid activities that poses high risk

-> risk reduction:- the high risk activities are performed with some controls that reduce the probability of threats.

->For controlling risk reduction

1.install antivirus

2.backup

3.install firewall

6) Risk transfer

transfer risk to third party insurance outsourcing.

Types of Networks:

1. Trusted network
2. Untrusted network

Types of attacks

1. DOS and DDOS attacks
2. malware attacks
3. employees may install third party pirated application
4. hacking-API's
5. IOT based threats
6. web apps attacks
7. man in the middle attacks
8. spoofing attacks
9. password attacks
10. vulnerability in existing software/hardwares
11. social engineering attacks
12. physical attacks

Firewall architecture

-> screening Router

-> DMZ Firewall

-> Firewall sandwich

-> layered Firewall

-> packet Filtering : works upto transport layer or network layer only

-> iptables was the first firewall used in linux

-> net Filter is the kernel level firewall used in linux

-> firewalld is used in linux

chain based filtering

-> chain contains rules for packet filtering

-> specific chains are used to perform actions on the packets based on stage in which the packet is.

what type of different chains are present

network card -> network buffer ->

===============================

installing IPtables

===============================

pre-requisits:

-> disable firewalld

# install iptables

-> yum install iptables-services iptables-utils

or

-> yum install iptables\*

# create two new machines

1. linux
2. windows

# enable the ip forwarding

# proc folder contains kernel level parameters

-> echo 1 > /proc/sys/net/ipv4/ip\_forward

# edit the file /etc/sysctl.conf

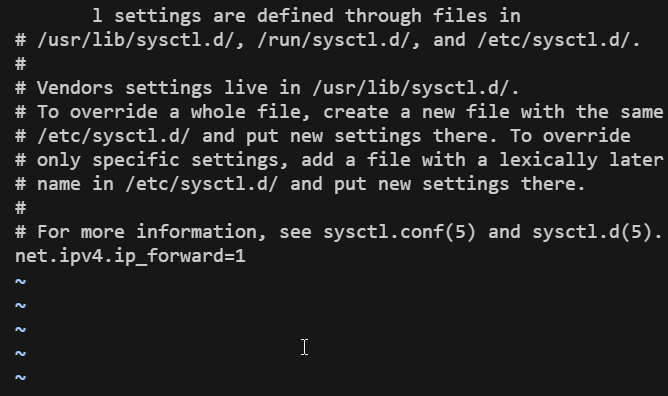
-> vi /etc/sysctl.conf

# now add the line

-> net.ipv4.ip\_foward=1

or

-> echo net.ipv4.ip\_forward=1 >> /etc/sysctl.conf



# check if iptables are running or not

-> systemctl status iptables

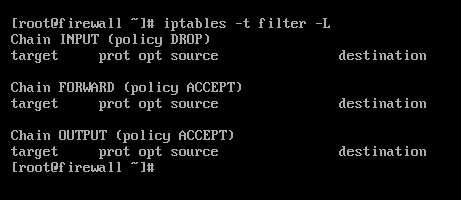
# flush the iptables

-> iptables -F

# how to change the policy of the table

-> iptables -t [table\_name] [chain\_name]

-> iptables -t filter --policy INPUT ACCEPT

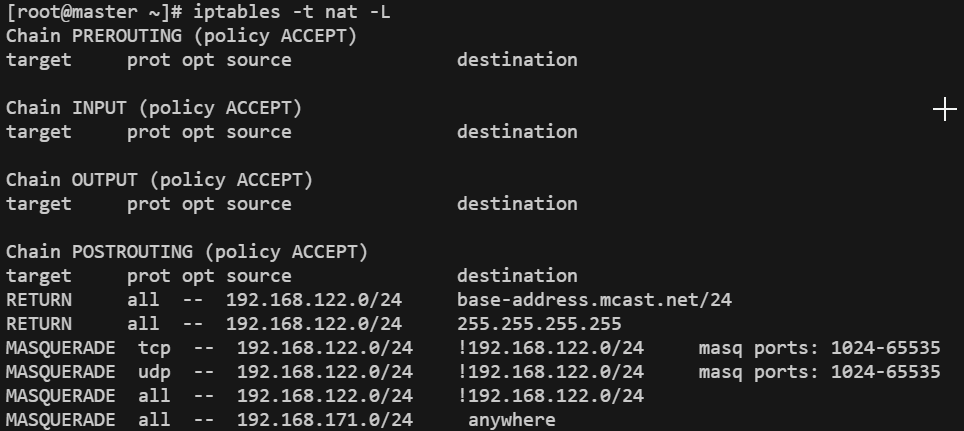


# to add POSTrouting to nat

-> iptables -t nat -A POSTROUTING -s [client\_machine\_ip] -o ens33 -j MASQUERADE

# to check if given entry has been made to the table or not

-> iptables -t nat -L



# go on client machine

# how to allow packets to move

-> iptables -P FORWARD ACCEPT

# how to drop packets from clients machines

-> iptables -P FORWARD DROP

# what traffics to allow from firewall

# therefore we need to add two rules for a network ,these rules are known as

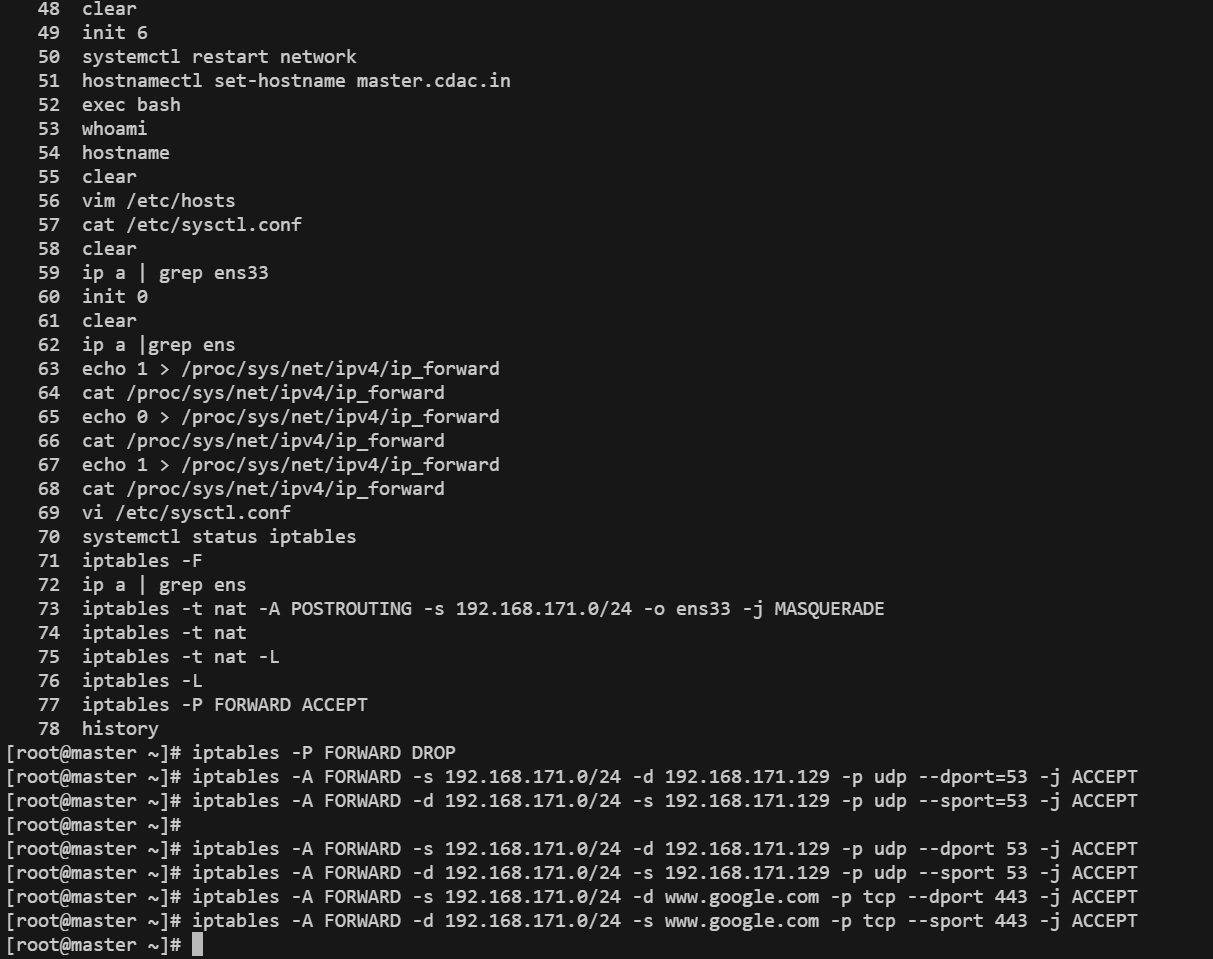
inbound and outbound rules

-> iptables -A FORWARD -s [host\_network/24] -d [dns\_ip] -p udp --dport=53 -j ACCEPT

# iptables -A FORWARD -s 192.168.171.0/24 -d 192.168.171.129 -p udp --sport=53 -j ACCEPT

-> iptables -A FORWARD -d [dns\_ip] -s [host\_network/24] -p udp --dport=53 -j ACCEPT

# iptables -A FORWARD -d 192.168.171.0/24 -s 192.168.171.129 -p udp --sport=53 -j ACCEPT



# how to save iptables permanently

-> service iptables save

==============================================================================

23rd June 2023

==============================================================================

#

-> vim

# check ip tables status

-> systemctl status iptables

-> iptables -F

-> iptables -t nat -A POSTROUTING -s [network\_ip] -o [adapter\_name] -j MASQUERADE

# allowed domains on client 1

-> youtube

-> microsoft

-> cisco

-> AWS

# allow youtube on client 1

-> iptable -A FORWARD -s [machine\_ip\_client1] -d [www.youtube.com](http://www.youtube.com) -p tcp --dport=443 -j ACCEPT

-> iptable -A FORWARD -s [machine\_ip\_client1] -p udp --dport=53

-> iptables -t nat -A POSTROUTING -s [machine\_ip\_client1] -o [adapter\_name] -j MASQUERADE

-> iptables -t nat -A POSTROUTING -s 11.11.10.150/24 -o ens33 -j MASQUERADE

# how to delete specific rule from iptables

-> iptables -D FORWARD [rule\_no]

#for adding new state

-m state --state NEW,ESTABLISHED

-j ACCEPT

# add new client to new state

-> iptables -A FORWARD -s [client\_machine\_ip] -d [website] -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT

-> iptables -A FORWARD -d [client\_machine\_ip] -s [website] -p tcp --sport 443 -m state --state NEW,ESTABLISHED -j ACCEPT

========================================================

ICMP Ping (DDoS Attack)

========================================================

# how to block ping request

# to block ping on internal network

-> iptables -A FORWARD -d [network\_ip/24] -p icmp --icmp-type echo-request -j DROP

# to block ping from external network

-> iptables -A INPUT -i [adapter\_name] -p icmp --icmp-type echo-request -j DROP

# to limit the ICMP requests

-> iptables -A INPUT -i ens33 -p icmp -m limit --limit 5/s -j ACCEPT

# to limit size of the ICMP request

-> iptables -A INPUT -i [interface\_name] -p icmp -m length --length 128:65500 -j ACCEPT

# maximum ping load

-> ping -l [0-65500] [ip]

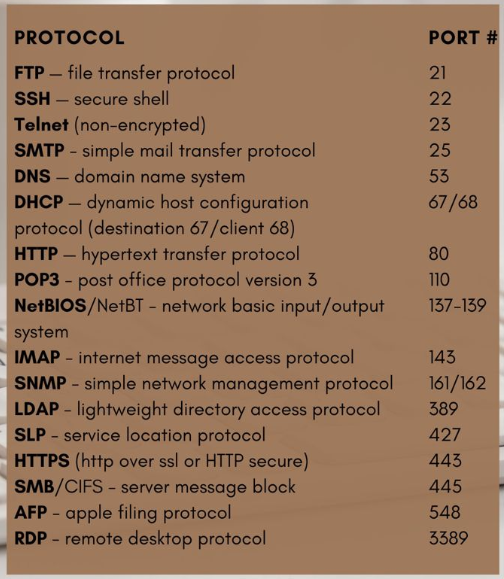
============================================================================

# how to map client machine packets to nat interface

-> iptables -t nat -A POSTROUTING -s 11.11.10.150/24 -o ens33 -j MASQUERADE

============================================================================

# PORTs



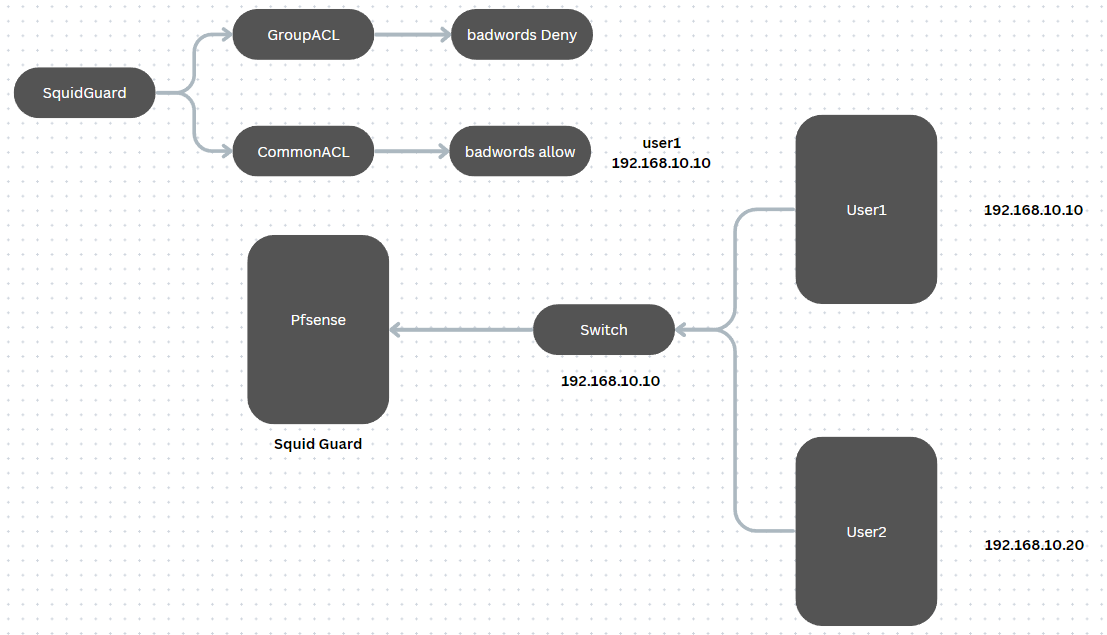
<https://in.pinterest.com/pin/3377768464889552/>

############

Pfsense

############

-> first GROUP ACL is checked for any user if, there is no entry is found in GROUPACL then CommonACL is applied.

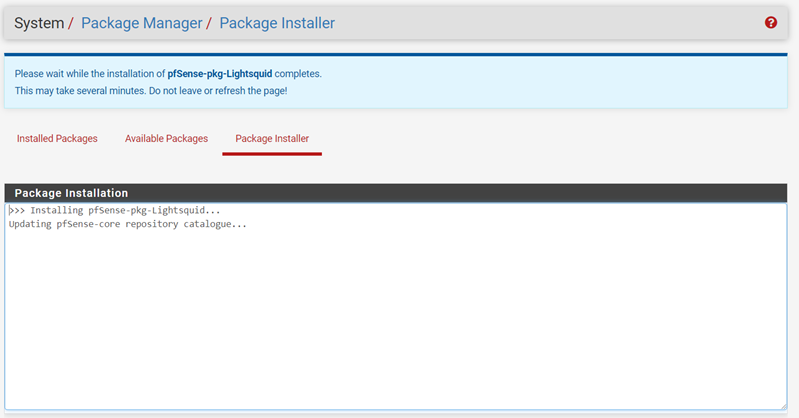


# Reporting in pfSense

==========================

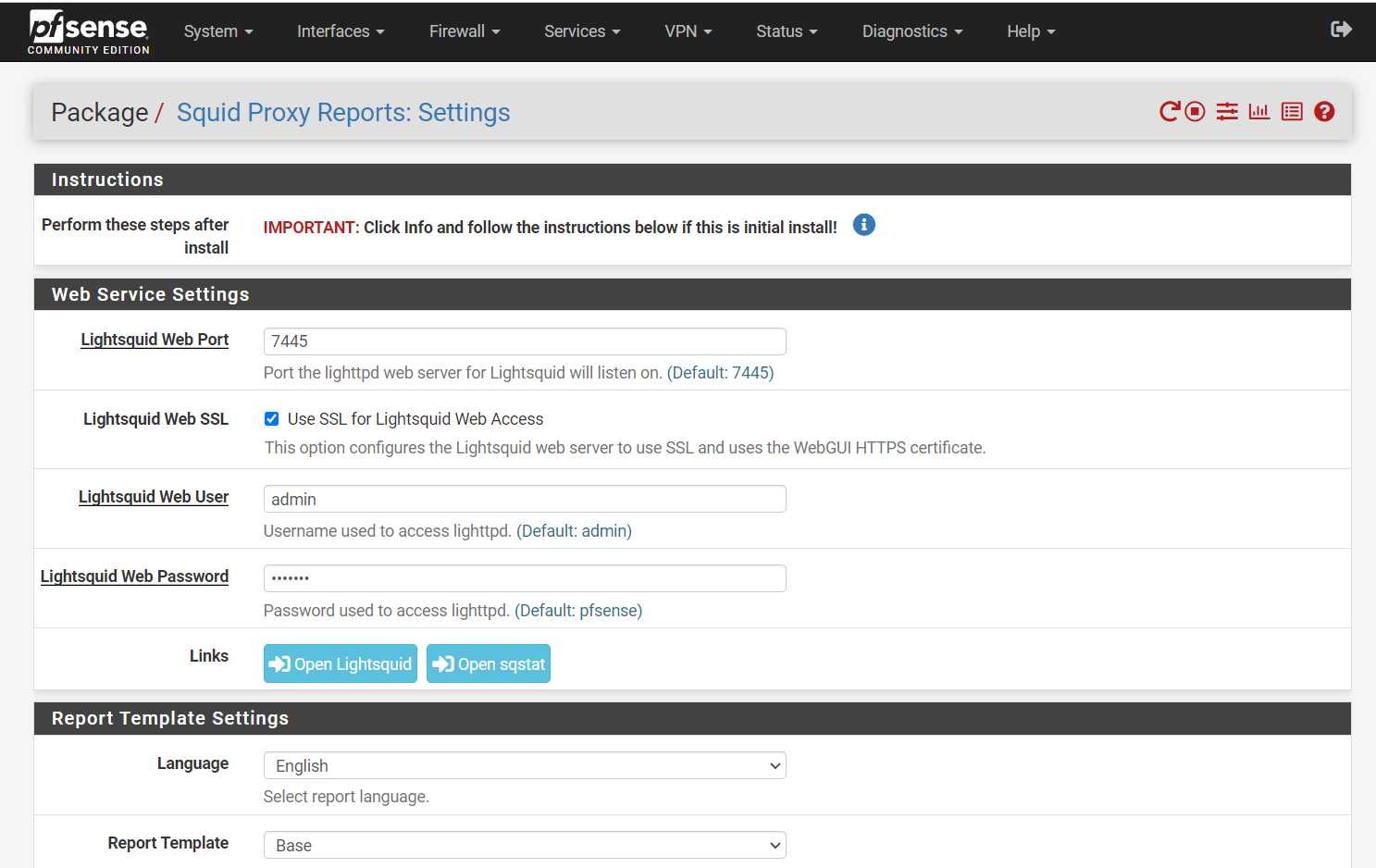
-> install lightsquid

-> system -> package manager -> search lightsquid -> click install



-> go to status -> squid proxy reports ->

#default port: 7445

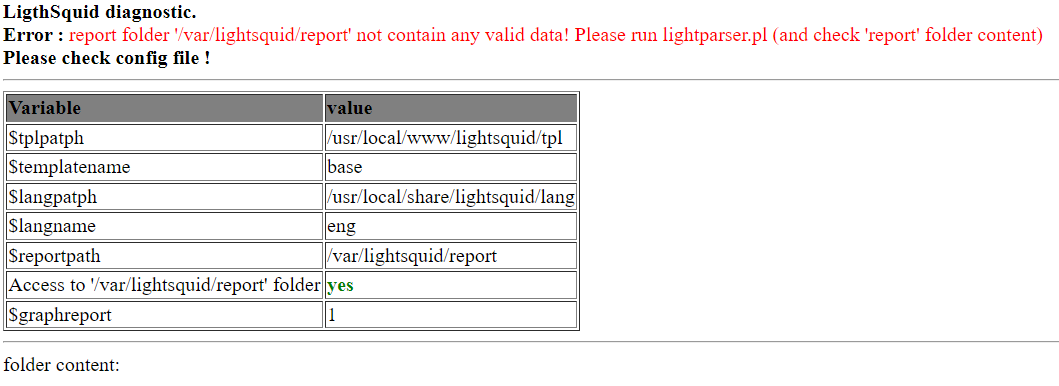


# set refresh scheduler : 10!

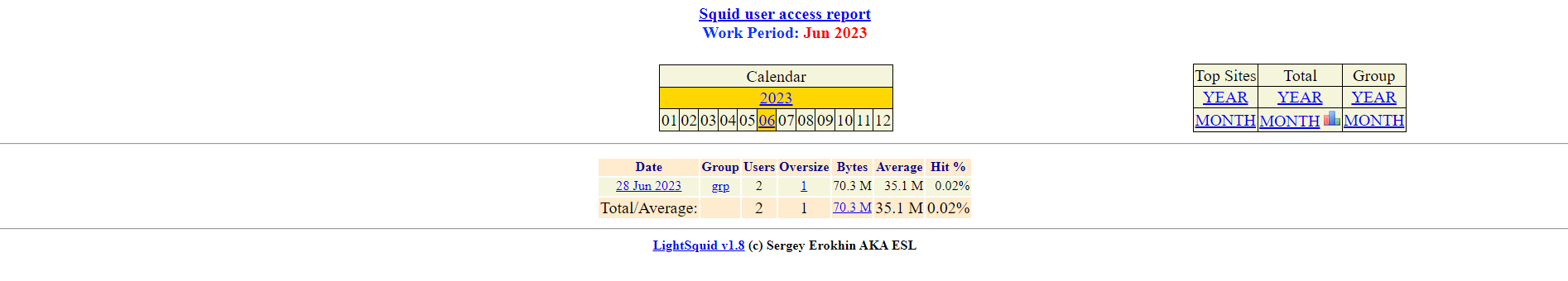
# click save -> refresh full

# click Open Lightsquid

# before opening



# after opening



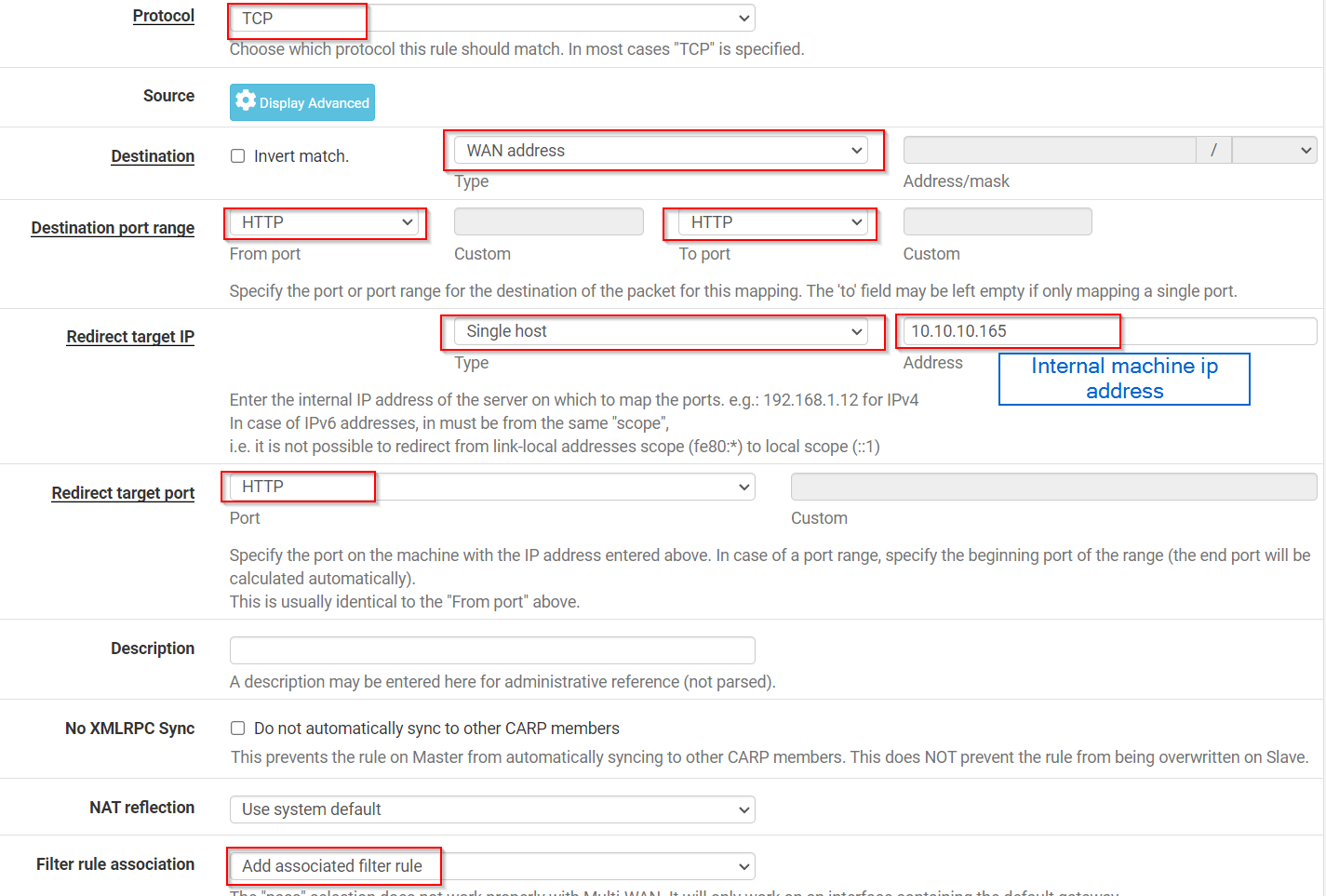
# access internal webpage from pfsense external ip address

-> install httpd

# adding port forwarding rule

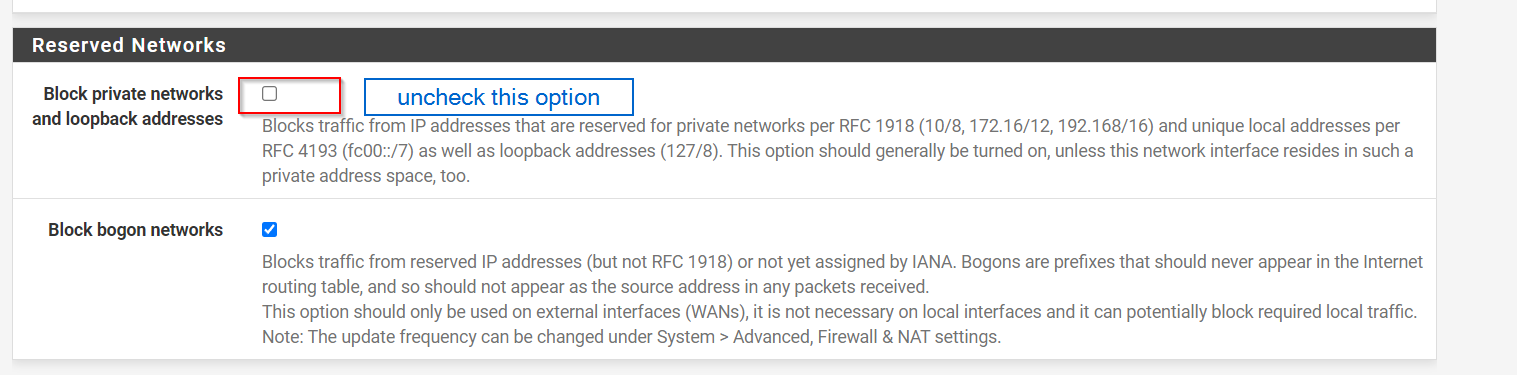
-> pfsense -> firewall rules -> nat -> Port Forwarding -> add

# make the following changes



# go to firewalls -> Rules -> WAN -> select the first option and click on settings

and then uncheck the option shown below



=============================================================================

assignment 1:

1> enable ip-forwarding and NAT(Masquerade)

2> for client 1 allow [bookmyshow,cisco,microsoft,google] with stateful packet inspection

3> for client 2 allow [redhat, awsamazon.com,azure.com,google.com] with stateful packet inspection

4> add rules to block ping with packet size 64 and above

5> add rules to accept ping packet 10/s

# how to assign static ip to give vm

#######################################################################

# solution

Question1:

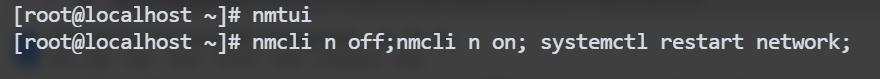
step 1: attach 2 network adapters

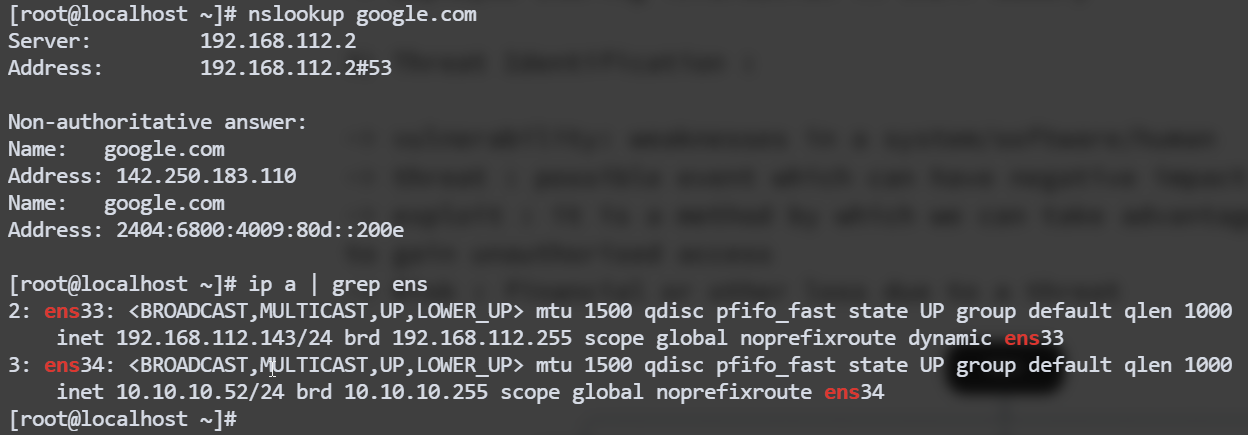
-> NAT

-> Host only

-> assign static ip to host only network

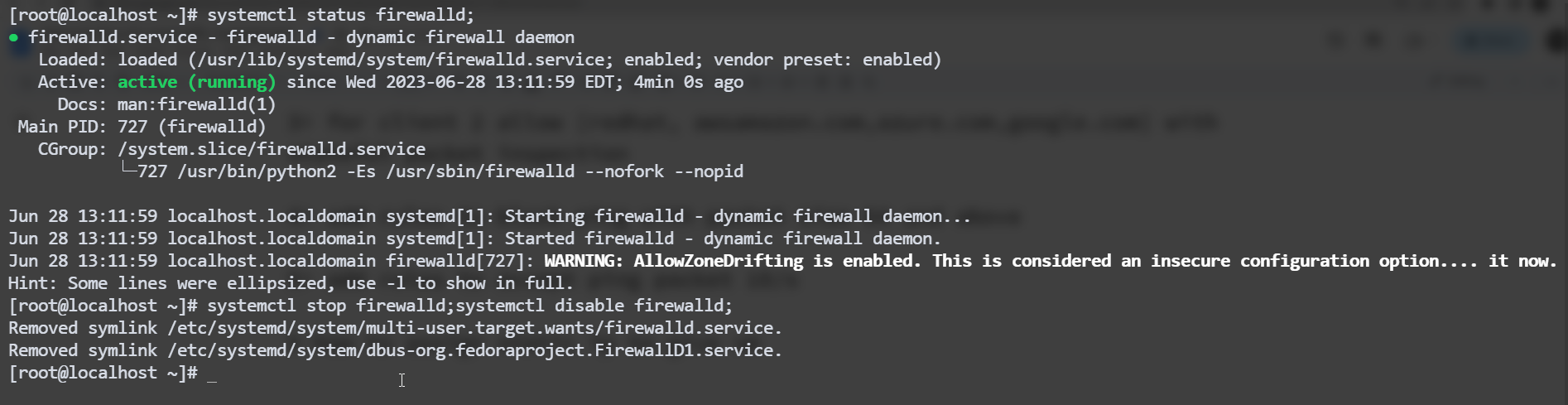
-> IP address of the given host only network



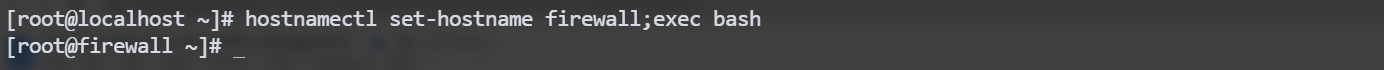


# we don't give gateway to host only interface on firewall

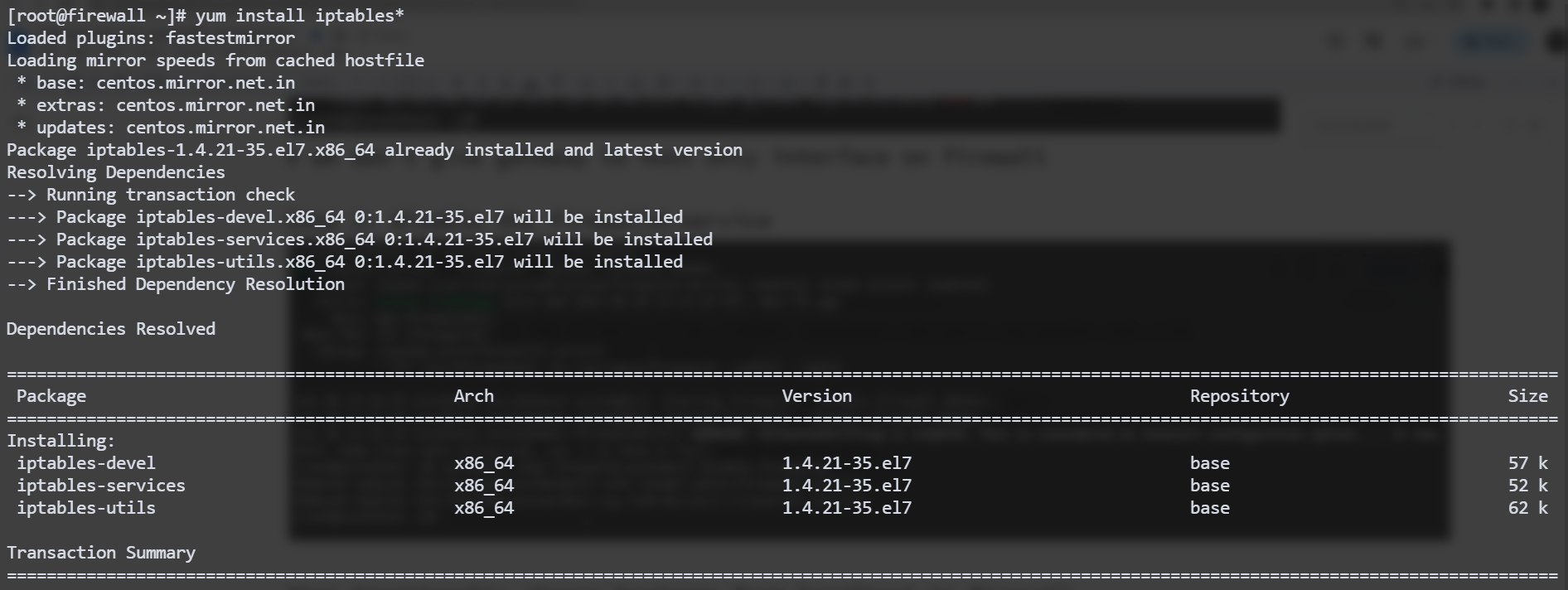
Step 2: disable the firewalld.service

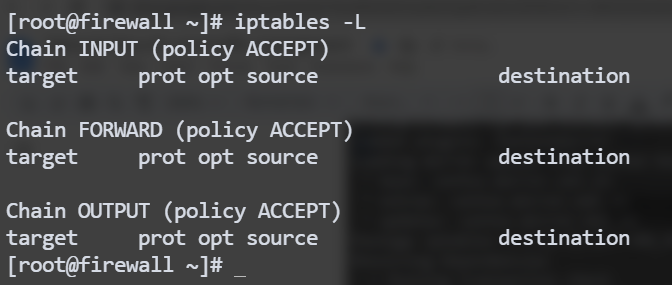


Step 3(optional): change hostname from localhost to firewall



Step 4: install iptables





Step 5: setup the client machine

-> ip address : 10.10.10.55/24

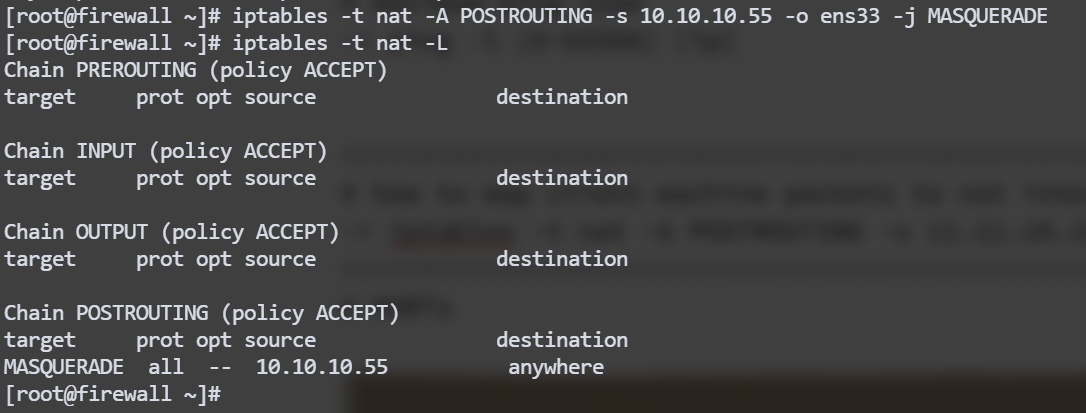
-> Gateway : 10.10.10.52

-> DNS : 192.168.112.254 (Vmware DNS)

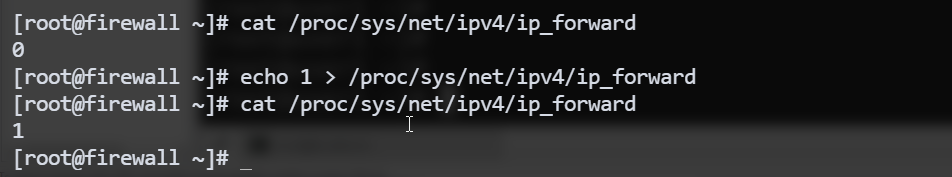
-> #DNS : 192.168.72.20 (CDAC DNS)

-> change hostname from localhost -> user1

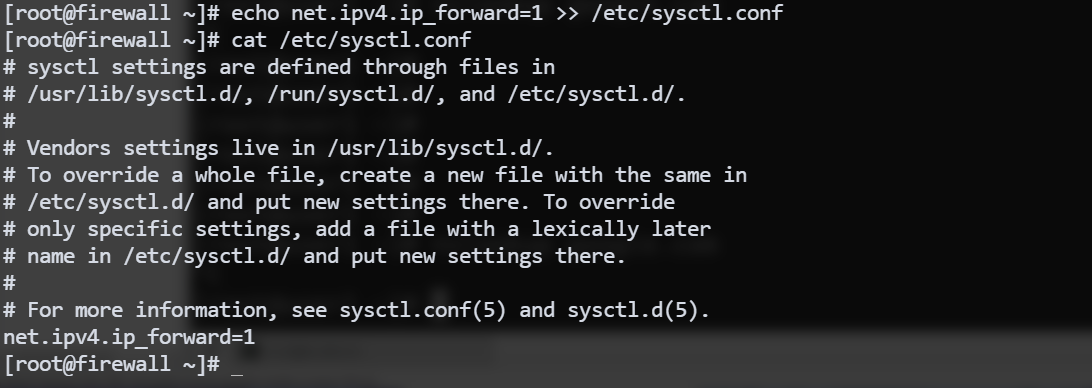
Step 6: make entry in firewall for ip forwarding



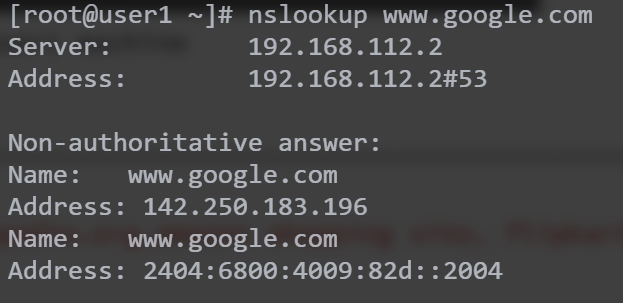
Step 7: enable the ip forwarding on the firewall



# permanent ip\_forwarding



Step 8: try to find google.com from user1 machine



# notes:

1. default policy for FORWARD in filter table must be ACCEPT mode
2. next we add entry in the nat table with -j=masquerade

Question2:

Solution:

Step 1:

==============================================================================

assignment 2:

1> allow these 2 users websites: wikipedia.org,amazon shopping site, flipkart, myntra, block all other websites.

# create R1 & R2 users

2> allow these users websites: redhat.com, cisco.com, microsoft.com,google.com

block all other websites.

block words - pirated,torrent,code,software,crack

3> for all other user: allow google.com, gmail.com, yahoo.com

block all other sites..

==============================================================================

(29th June 2023)

#################

IDS

#################

# Firewall can't check the payloads they only check for input\_ip:input\_ports and output\_ip:output\_ports

# to fulfil this objective we use IDS(Intrusion Detection System) to check

payloads inside the packets

# Question is how IDS finds out what's inside the packet

there are two ways

1. behaviour based
2. signatour based

types of IDS

-> NIDS : Network IDS

-> HIDS : Host Based IDS

-> in HIDS, packets are encrypted from host to client therefore it can't be detected by host or client.

proxy -> forward proxy: squid proxy server : control access of internet

\-> reverse proxy:

Intrusion:

os can be divided into 2 levels

1. kernel space
2. userspace

most of the services start in user space hence can't affect the operating system, to affect systems we have threat from rootkits.

what rootkit do, they replace the system level service and get the root access.. after getting the root access. they can harm the infrastructure.

Definition of IDS:

1. Intrusion detection: the process of monitoring the event occurring in a computer system or network and analysing them for signs of possible intrusion(incident)
2. Intrusion detection system: is a software that automates the intrusion detection process. The primary responsibility of an IDS is to detect unwanted and malicious activities.
3. Intrusion Prevention system(IPS) : software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents

SIEM : Security information and event management

new anomalies can't be detected using signature based method..

False Positive: Normal traffic detected as malicious

False Negative: Malicious traffic detected as Positive

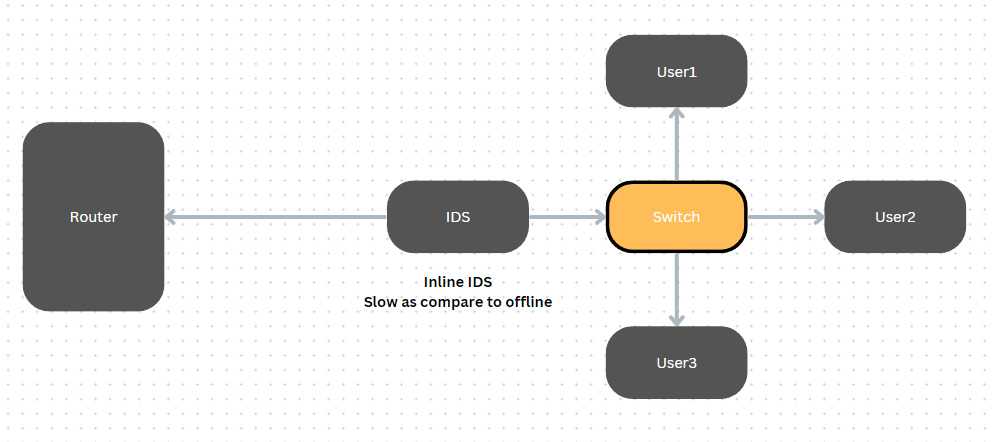
IDS and IPS tuning : we change configuration of IDS and IPS for False Positive or False Negative.

How to monitor network:

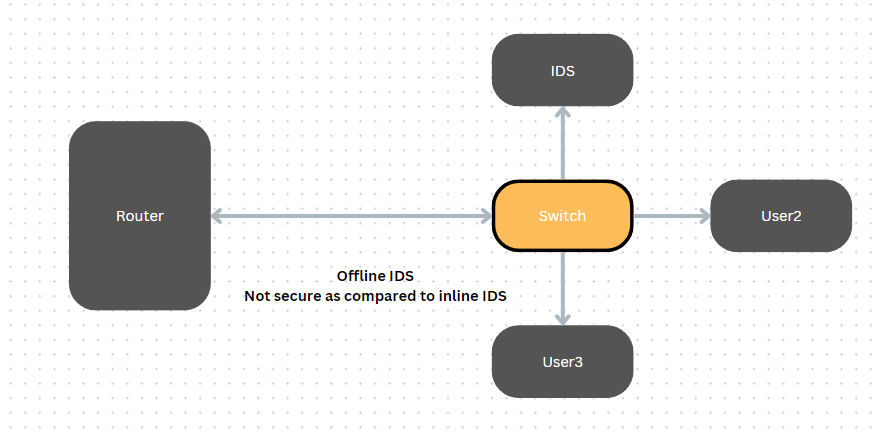
1. promiscuous mode: in this method each and every copy of frame is sent to the IDS for packet sniffing.
2. Port mirroring: if promiscuous mode is not available on the system then we use Port mirroring method to sent packet to IDS.

IDS can be implement in two modes.

1. Inline mode:

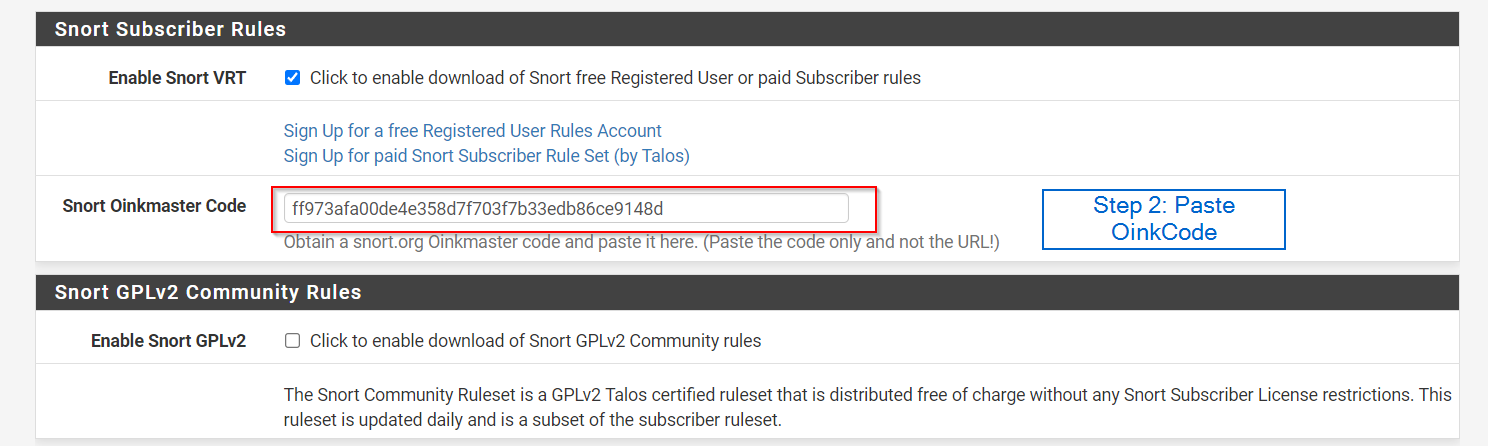


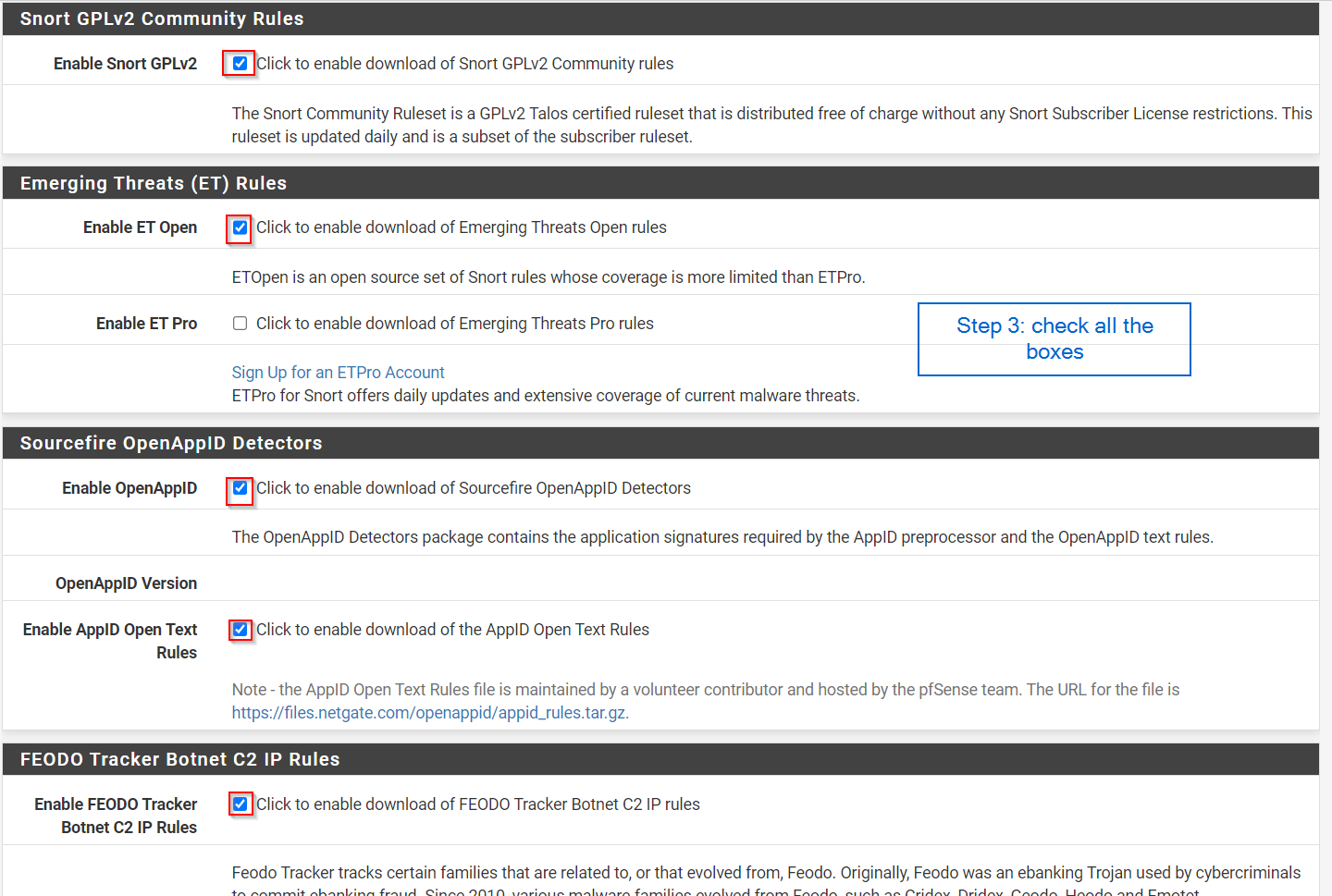
1. offline mode:

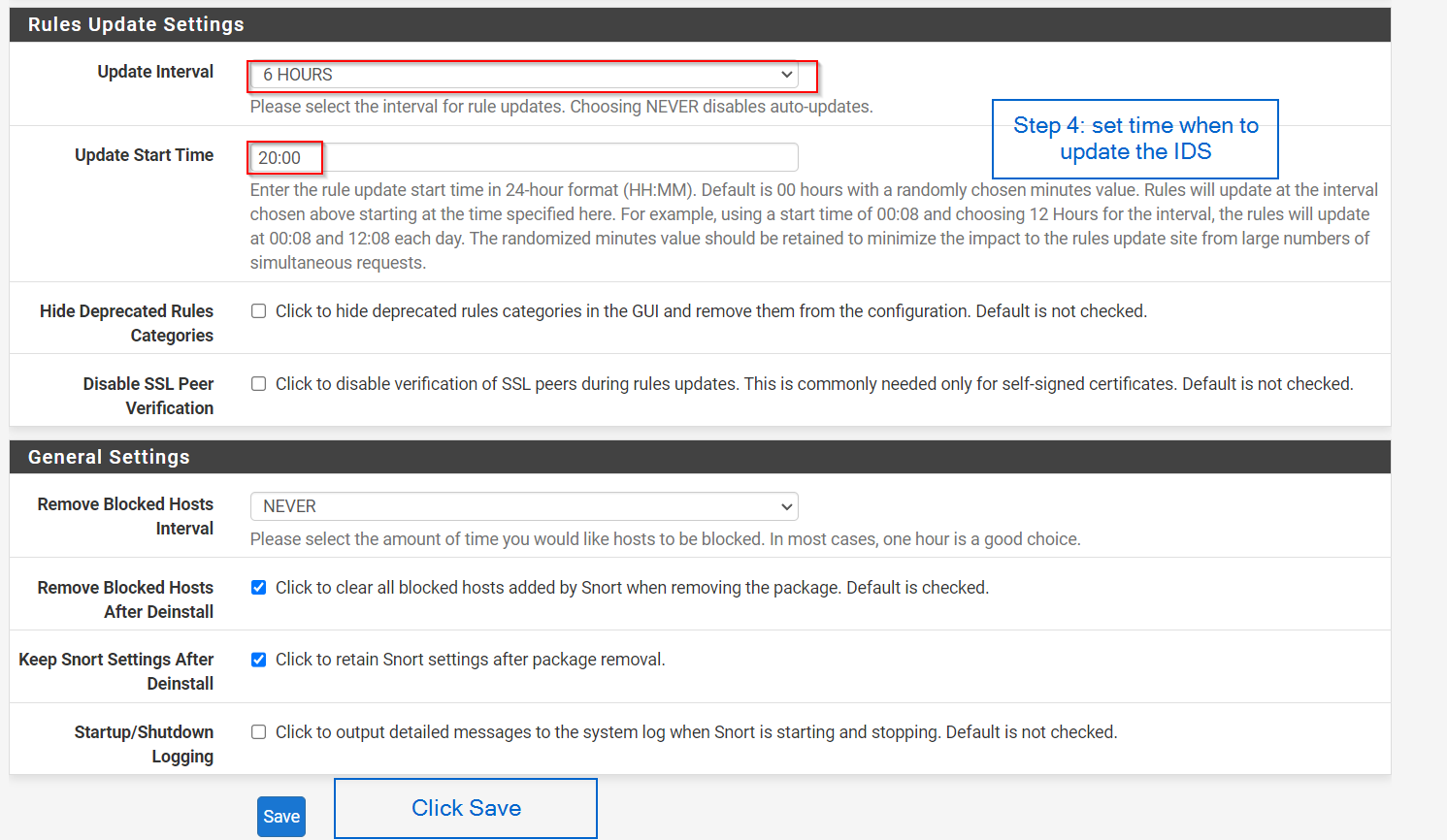


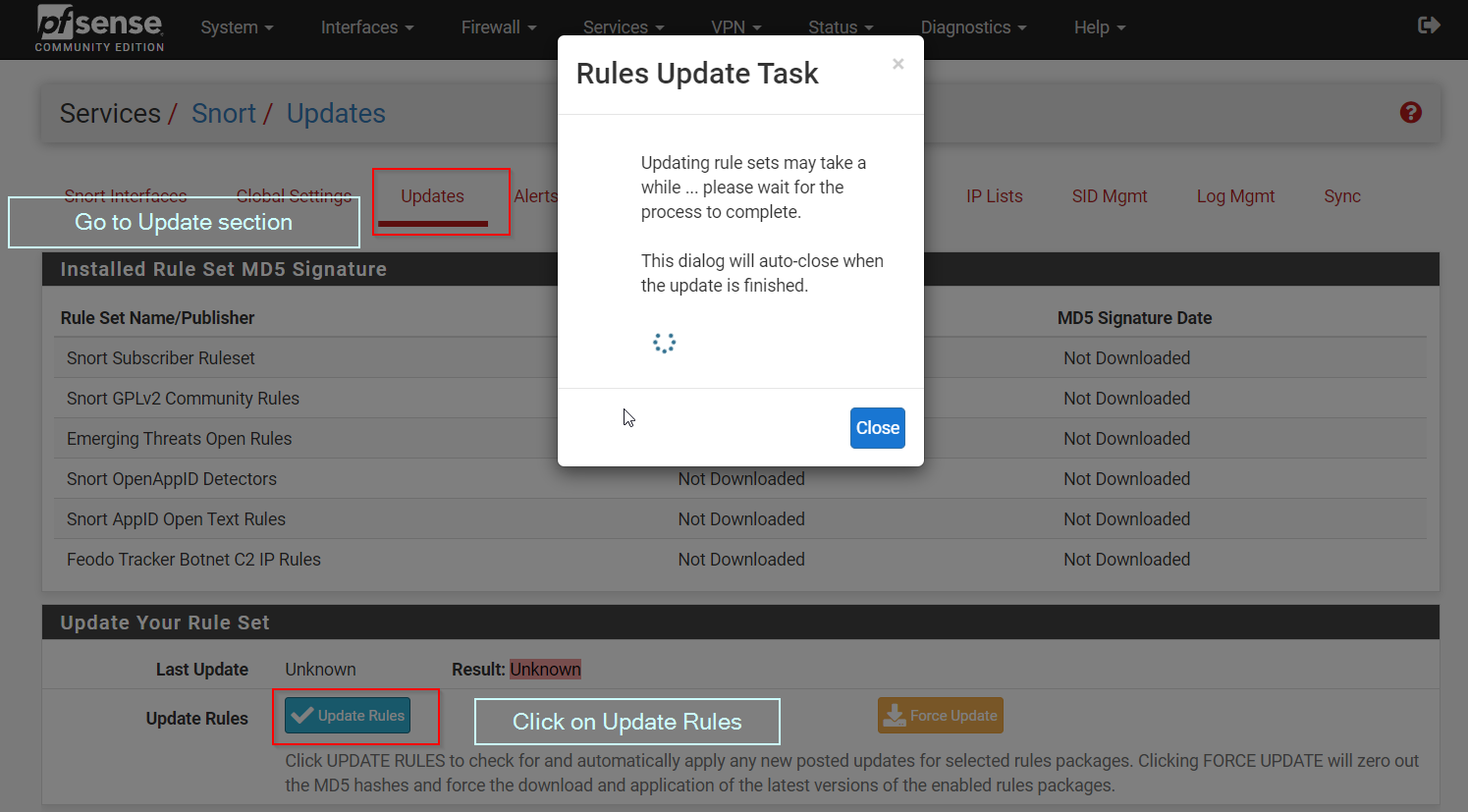
Snort Module: first go to snort website and register for the website and get the oinkcode from there for future use.

then install snort package in pfsense.. and proceed with the instruction shown below..

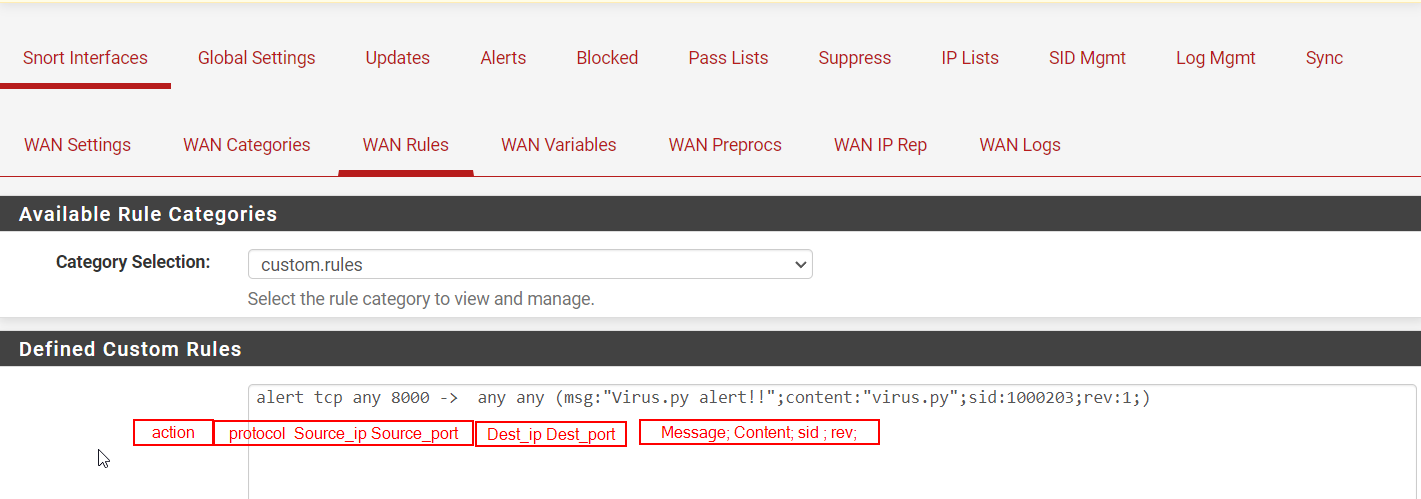








How to add custom rule to snort.



Assignment 3:

-> find size of the packet (ping packet > 256)

# to mention size of the packet in snort rules we have option dsize to define size of the packet

ex. alert udp any any -> any any (msg:""; content:""; dsize:<512;sid:)

# for further study follow the link

https://docs.snort.org/rules/headers/actions

-> how to specify file's hash in the rule

# to check for the file hash we use protected\_content:"hashed value";hash:md5|sha1|sha512

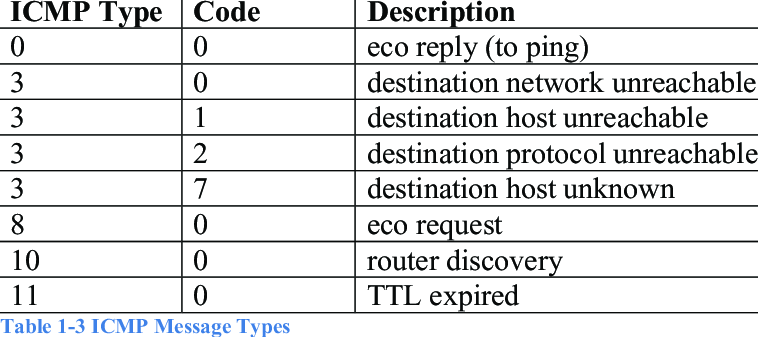
ex. alert tcp any any -> any any (

msg:"";

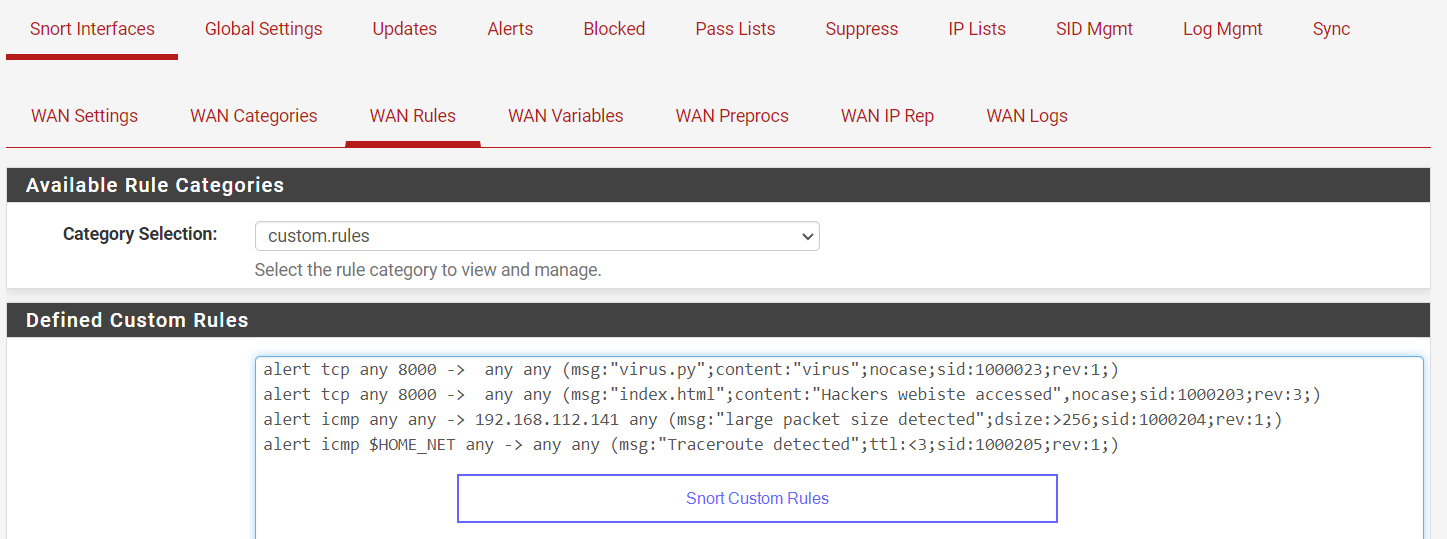
content:"";

itype: used to define icmp message type

icode:



#Snort Rules

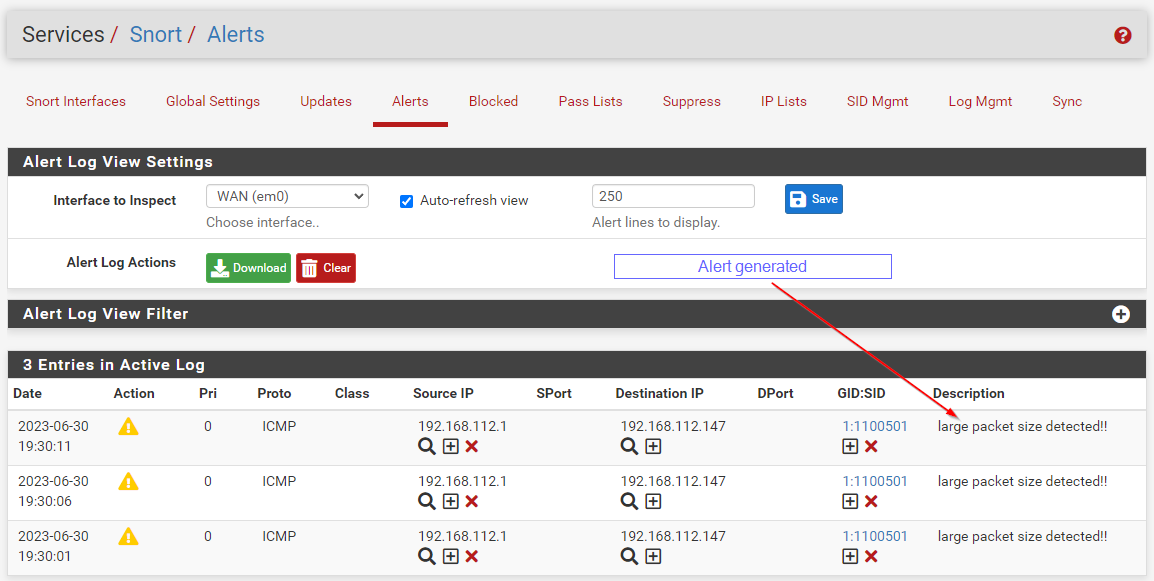


Assignment 4:

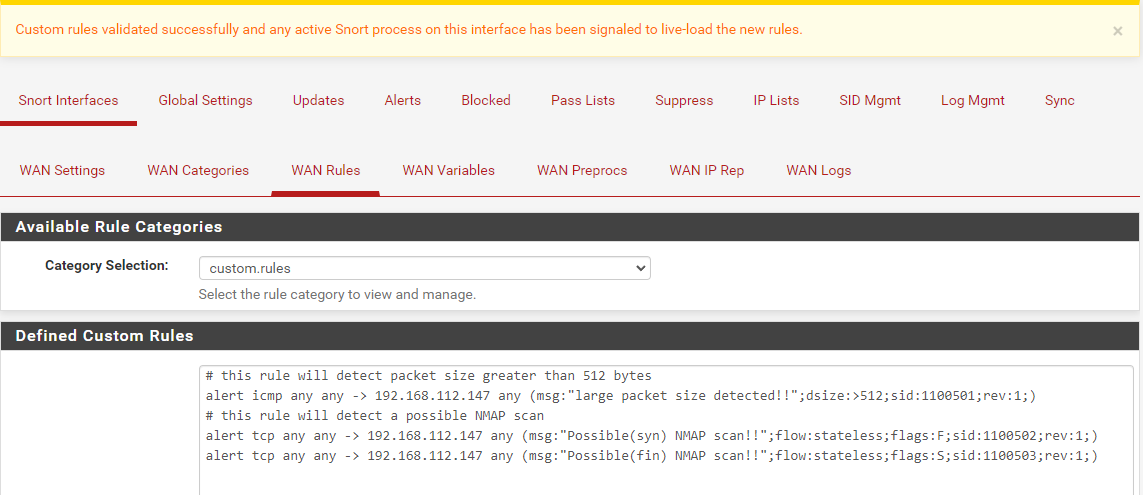
-> detect ping for packet greater than 512 bytes

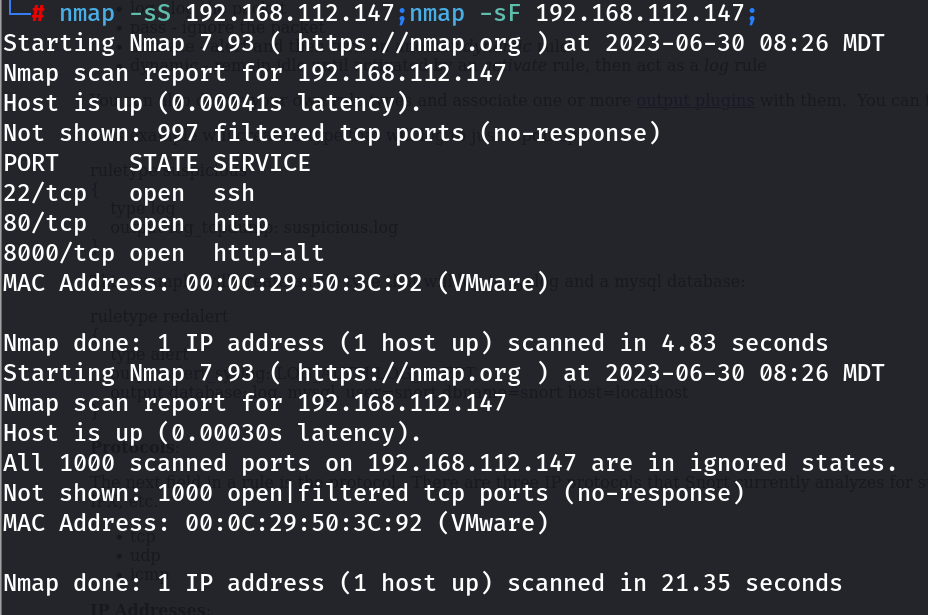


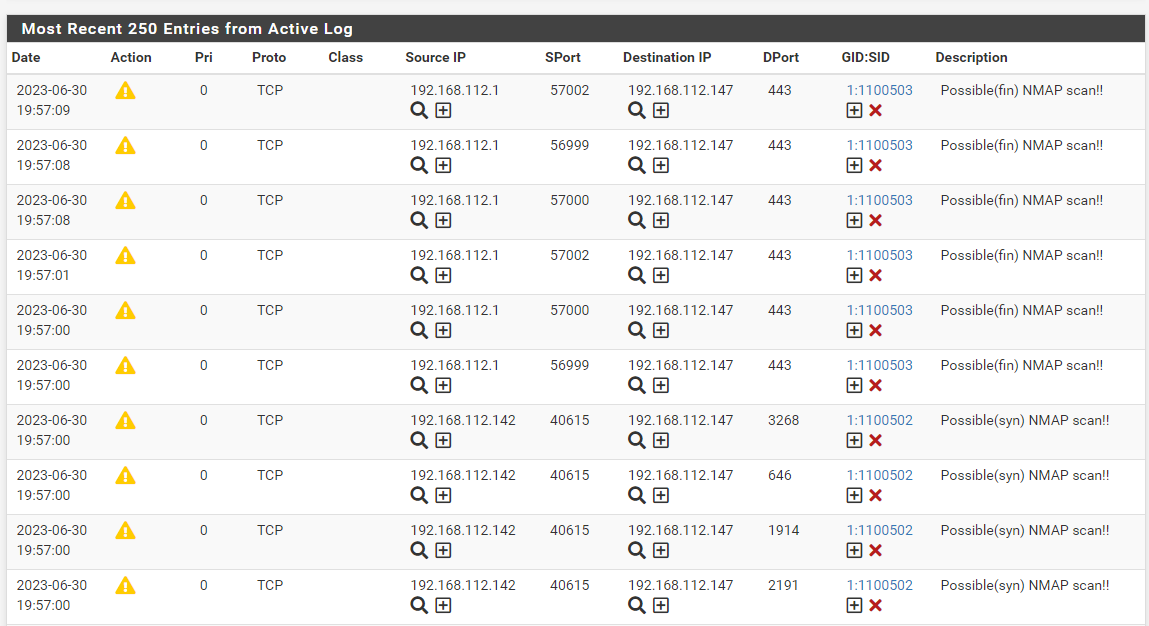




-> detect nmap scan -sF -sS

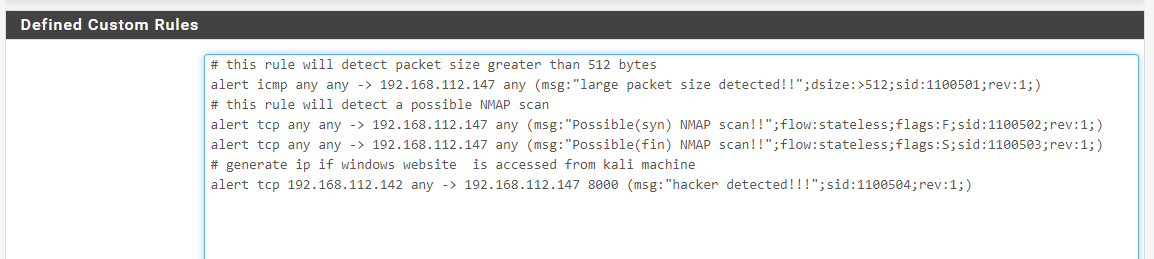


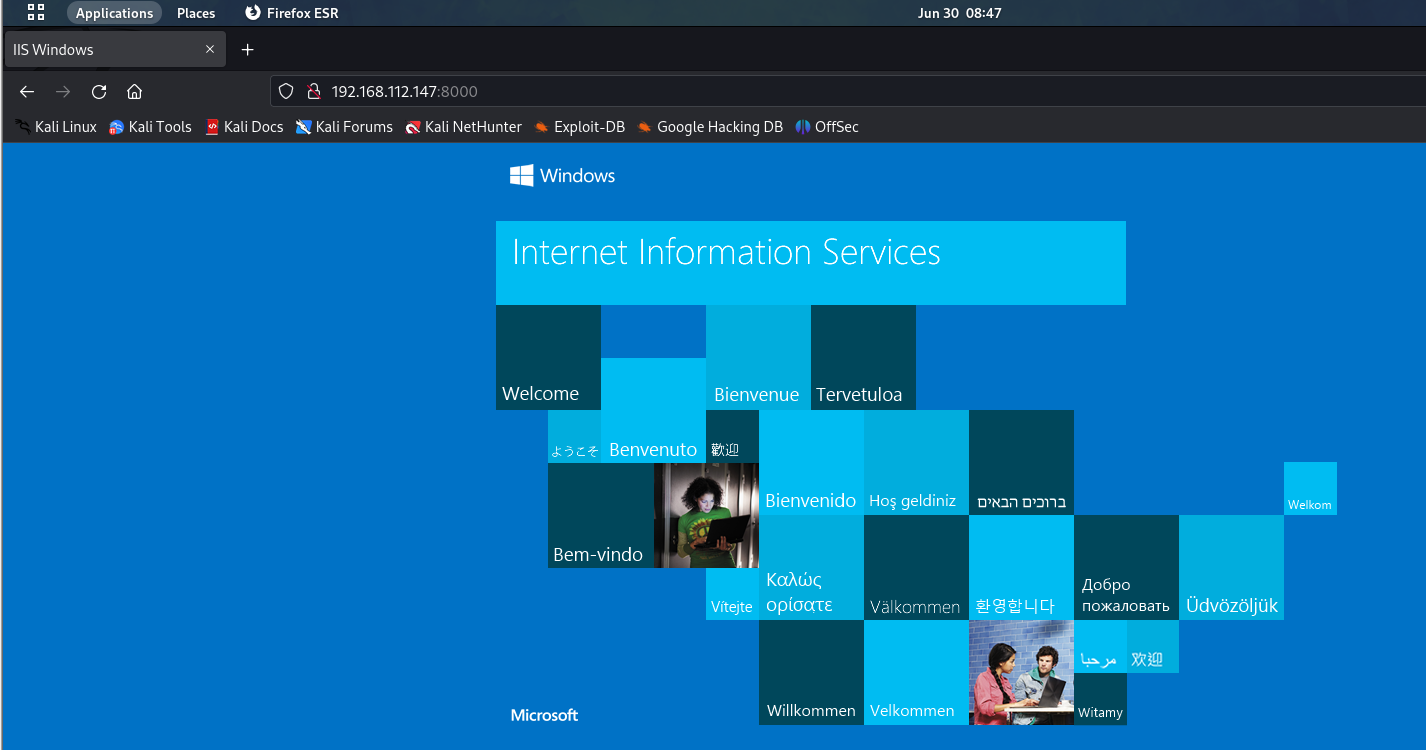


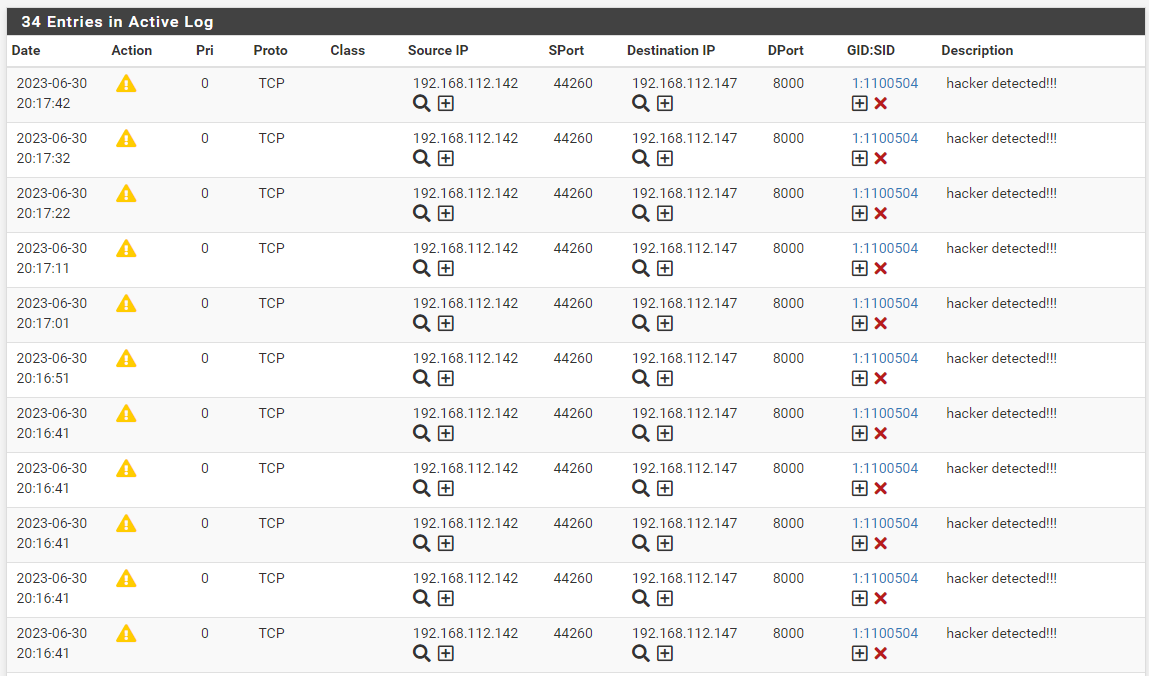


-> detect if windows website is accessed from kali linux generate alert

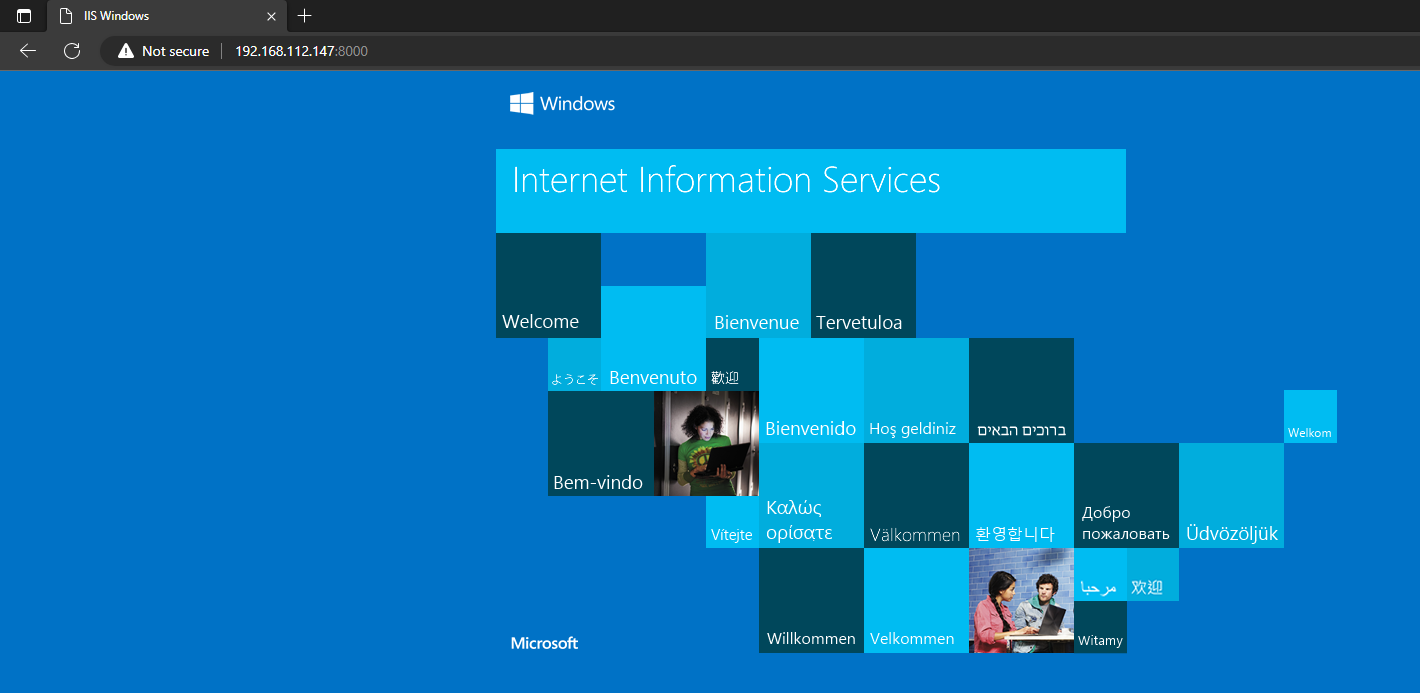
& if it is accessed from base machine no alert

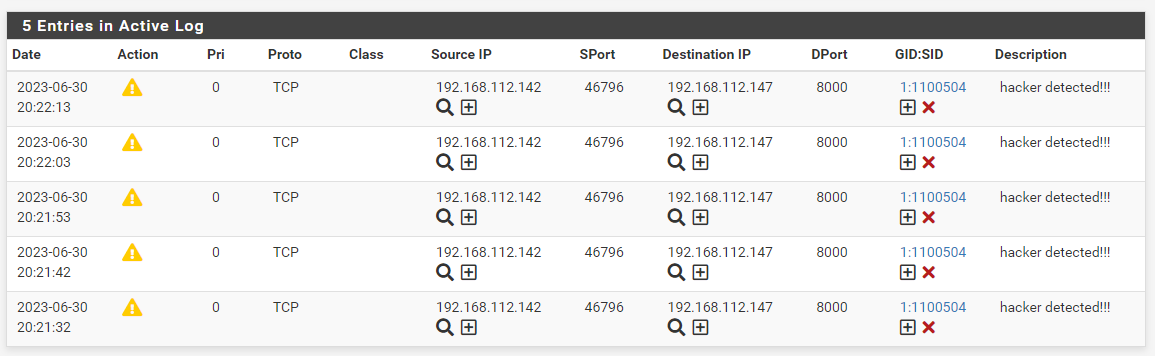


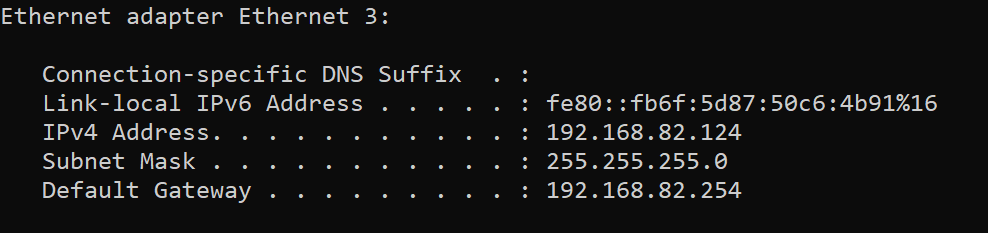




# accessed from base windows machine

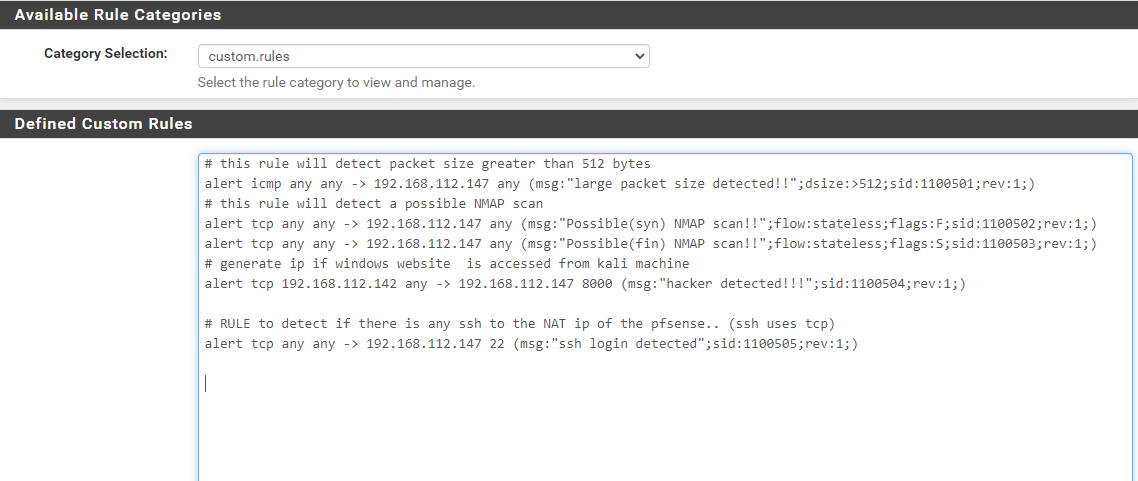


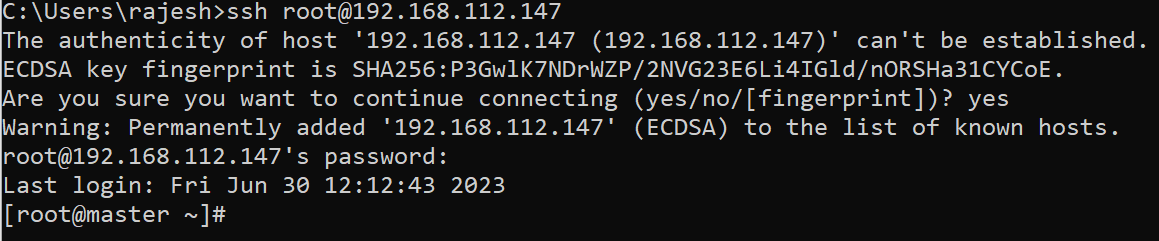


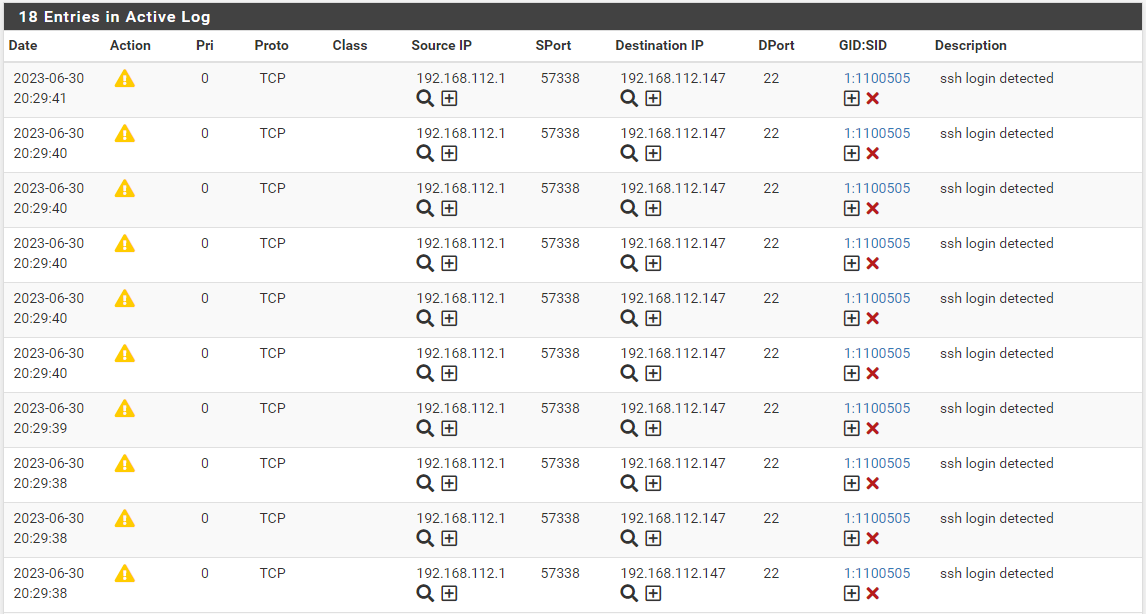


no base machine ip(192.168.82.124) found in logs, which means no log is generated for base machine access for windows website

-> detect if ssh to nat ip is done







-> create a website on kali linux write a rule to detect if website is accessed (try drop action to check if access is blocked)

