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

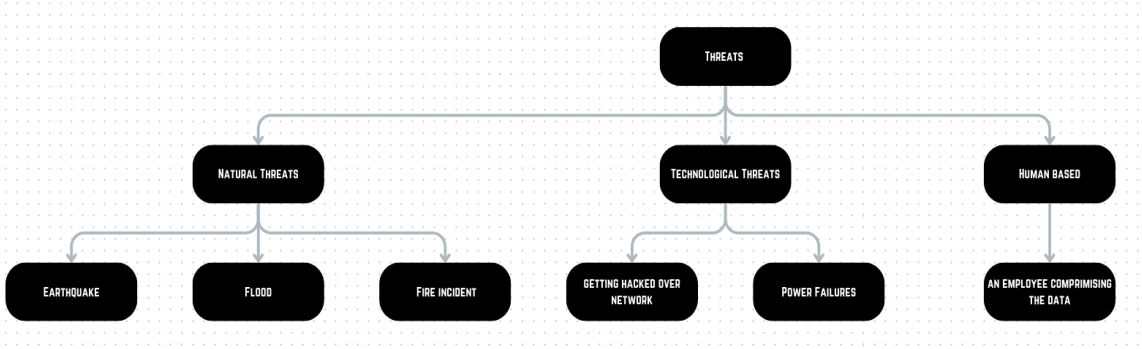
2) Asset Identification : identify all assets that store,use or transmit the critical information of the organisation

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
```

```
       l settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward=1
```

```
# 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
```

```
[root@master ~]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
RETURN     all  --  192.168.122.0/24     base-address.mcast.net/24
RETURN     all  --  192.168.122.0/24     255.255.255.255
MASQUERADE  tcp  --  192.168.122.0/24    !192.168.122.0/24     masq ports: 1024-65535
MASQUERADE  udp  --  192.168.122.0/24    !192.168.122.0/24     masq ports: 1024-65535
MASQUERADE  all  --  192.168.122.0/24    !192.168.122.0/24
MASQUERADE  all  --  192.168.171.0/24     anywhere
```

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

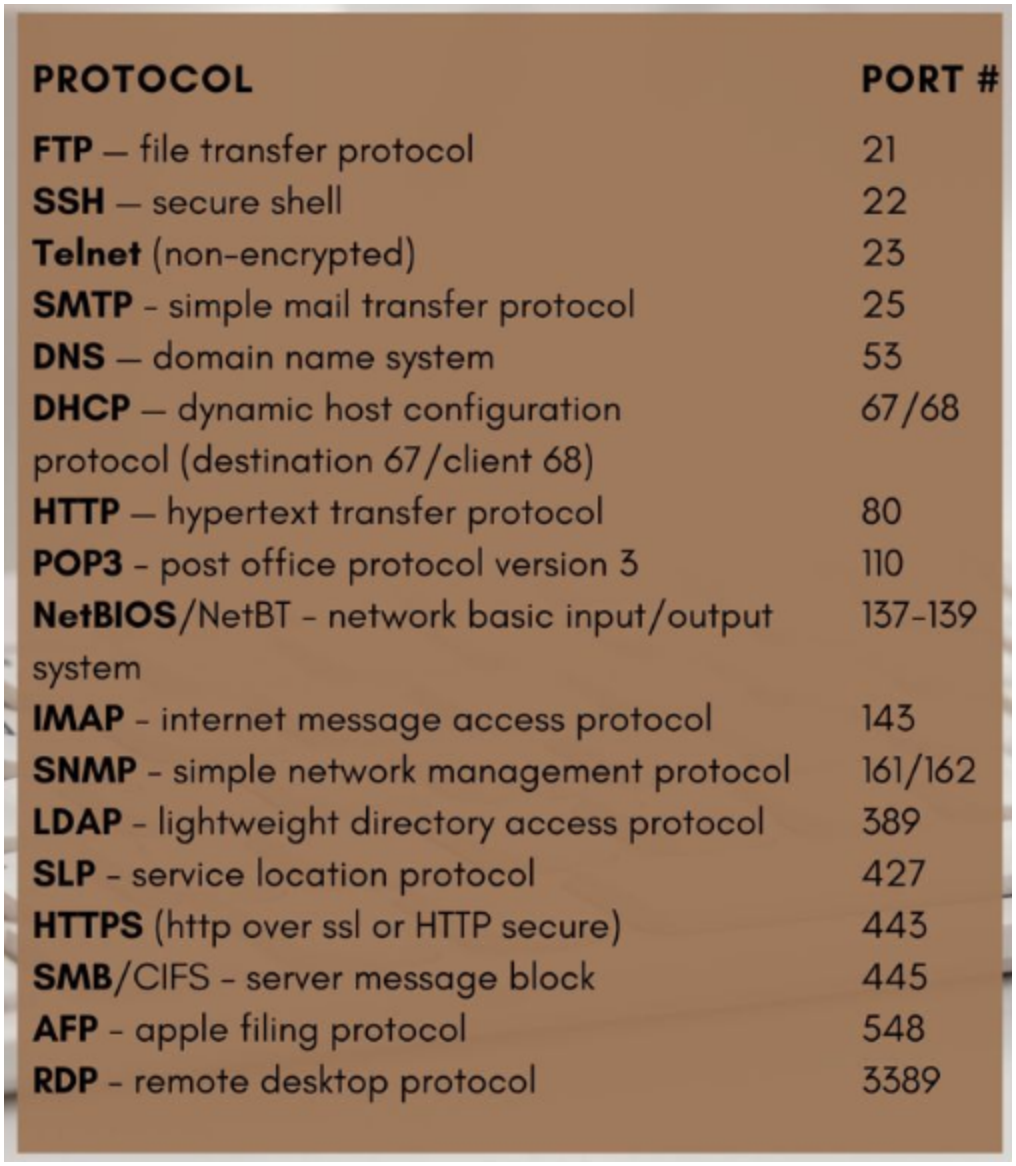
```
   48  clear
   49  init 6
   50  systemctl restart network
   51  hostnamectl set-hostname master.cdac.in
   52  exec bash
   53  whoami
   54  hostname
   55  clear
   56  vim /etc/hosts
   57  cat /etc/sysctl.conf
   58  clear
   59  ip a | grep ens33
   60  init 0
   61  clear
   62  ip a |grep ens
   63  echo 1 > /proc/sys/net/ipv4/ip_forward
   64  cat /proc/sys/net/ipv4/ip_forward
   65  echo 0 > /proc/sys/net/ipv4/ip_forward
   66  cat /proc/sys/net/ipv4/ip_forward
   67  echo 1 > /proc/sys/net/ipv4/ip_forward
   68  cat /proc/sys/net/ipv4/ip_forward
   69  vi /etc/sysctl.conf
   70  systemctl status iptables
   71  iptables -F
   72  ip a | grep ens
   73  iptables -t nat -A POSTROUTING -s 192.168.171.0/24 -o ens33 -j MASQUERADE
   74  iptables -t nat
   75  iptables -t nat -L
   76  iptables -L
   77  iptables -P FORWARD ACCEPT
   78  history
[root@master ~]# iptables -P FORWARD DROP
[root@master ~]# iptables -A FORWARD -s 192.168.171.0/24 -d 192.168.171.129 -p udp --dport=53 -j ACCEPT
[root@master ~]# iptables -A FORWARD -d 192.168.171.0/24 -s 192.168.171.129 -p udp --sport=53 -j ACCEPT
[root@master ~]#
[root@master ~]# iptables -A FORWARD -s 192.168.171.0/24 -d 192.168.171.129 -p udp --dport 53 -j ACCEPT
[root@master ~]# iptables -A FORWARD -d 192.168.171.0/24 -s 192.168.171.129 -p udp --sport 53 -j ACCEPT
[root@master ~]# iptables -A FORWARD -s 192.168.171.0/24 -d www.google.com -p tcp --dport 443 -j ACCEPT
[root@master ~]# iptables -A FORWARD -d 192.168.171.0/24 -s www.google.com -p tcp --sport 443 -j ACCEPT
[root@master ~]#
```

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 -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
A ipt
# 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
```

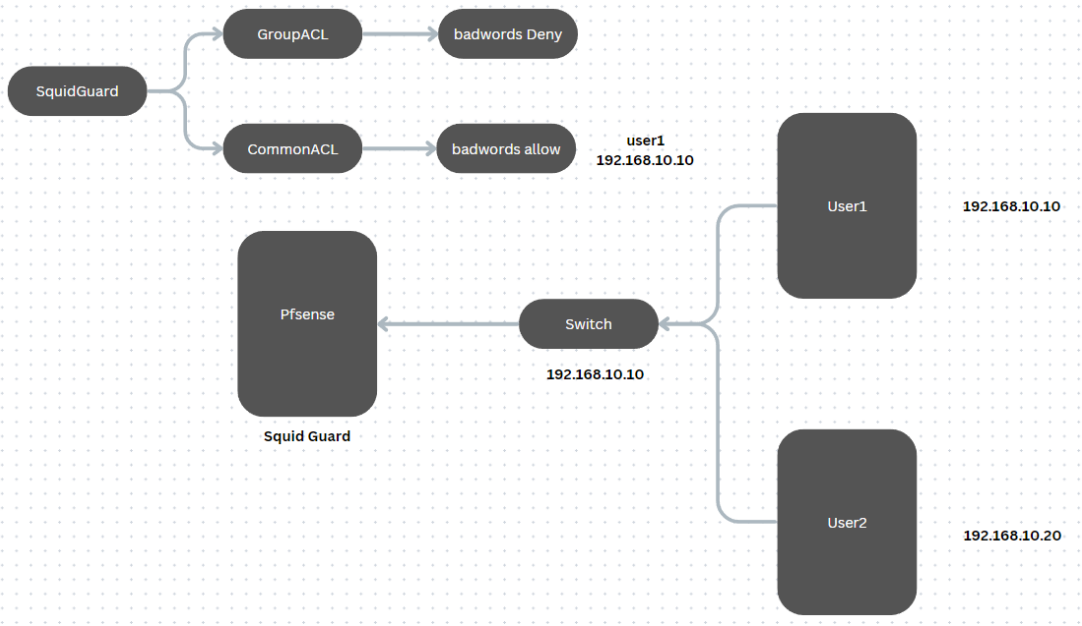


PROTOCOL	PORT #
FTP – file transfer protocol	21
SSH – secure shell	22
Telnet (non-encrypted)	23
SMTP - simple mail transfer protocol	25
DNS – domain name system	53
DHCP – dynamic host configuration protocol (destination 67/client 68)	67/68
HTTP – hypertext transfer protocol	80
POP3 - post office protocol version 3	110
NetBIOS/NetBT - network basic input/output system	137-139
IMAP - internet message access protocol	143
SNMP - simple network management protocol	161/162
LDAP - lightweight directory access protocol	389
SLP - service location protocol	427
HTTPS (http over ssl or HTTP secure)	443
SMB/CIFS - server message block	445
AFP - apple filing protocol	548
RDP - remote desktop protocol	3389

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

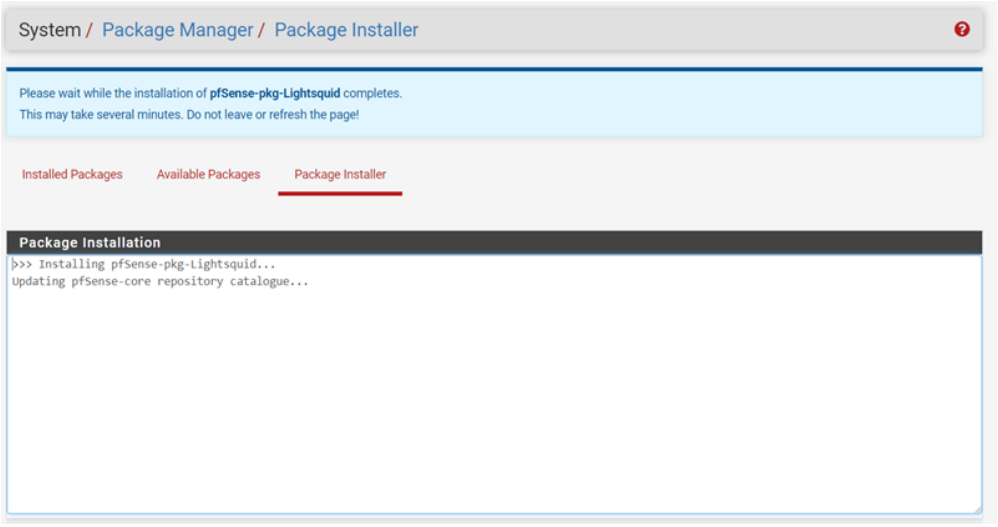
############
Pfsense
############

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

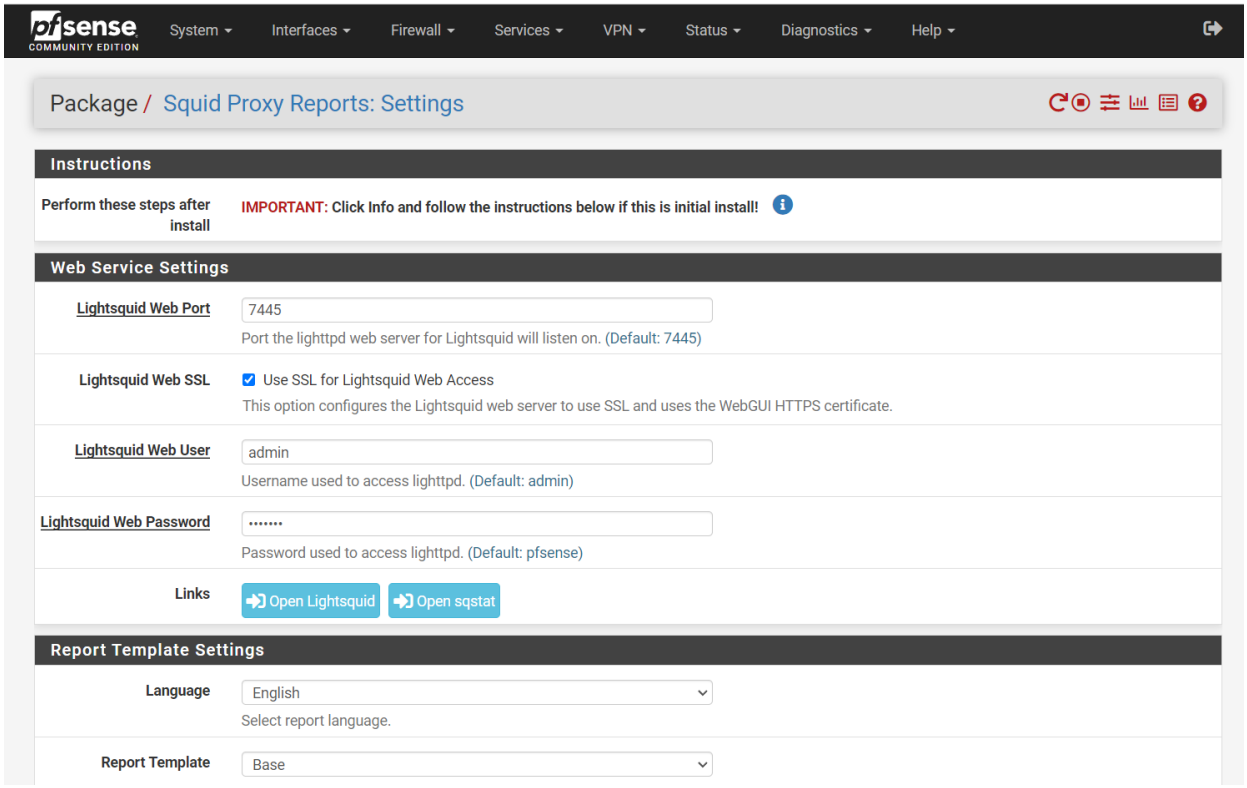


Reporting in pfSense
==========

-> 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
```

LigthSquid diagnostic.
Error : report folder '/var/lightsquid/report' not contain any valid data! Please run lightparser.pl (and check 'report' folder content)
Please check config file !

Variable	value
$tplpatph	/usr/local/www/lightsquid/tpl
$templatename	base
$langpatph	/usr/local/share/lightsquid/lang
$langname	eng
$reportpath	/var/lightsquid/report
Access to '/var/lightsquid/report' folder	yes
$graphreport	1

folder content:

```
# after opening
```

Squid user access report
Work Period: Jun 2023

Calendar											
2023											
01	02	03	04	05	06	07	08	09	10	11	12

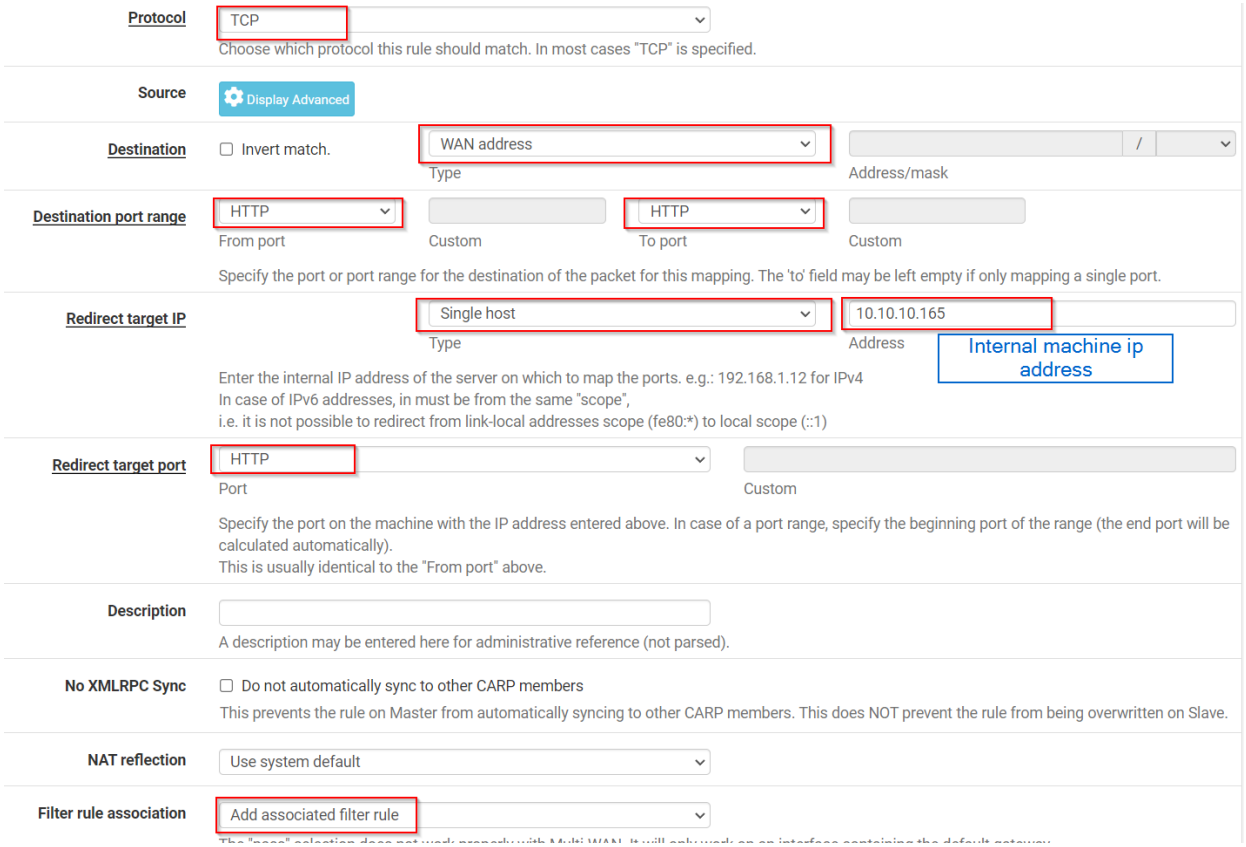
Top Sites	Total	Group
YEAR	YEAR	YEAR
MONTH	MONTH	MONTH

Date	Group	Users	Oversize	Bytes	Average	Hit %
28 Jun 2023	grp	2	1	70.3 M	35.1 M	0.02%
Total/Average:		2	1	70.3 M	35.1 M	0.02%

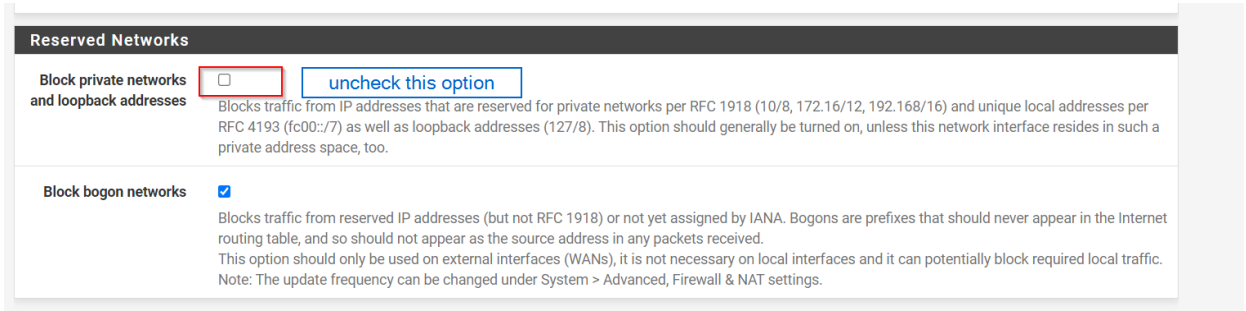
LightSquid v1.8 (c) Sergey Erokhin AKA ESL

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

```
[root@localhost ~]# nmtui
[root@localhost ~]# nmcli n off;nmcli n on; systemctl restart network;
```

```
[root@localhost ~]# nslookup google.com
Server:         192.168.112.2
Address:        192.168.112.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.110
Name:   google.com
Address: 2404:6800:4009:80d::200e

[root@localhost ~]# ip a | grep ens
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    inet 192.168.112.143/24 brd 192.168.112.255 scope global noprefixroute dynamic ens33
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    inet 10.10.10.52/24 brd 10.10.10.255 scope global noprefixroute ens34
[root@localhost ~]#
```

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

Step 2: disable the firewalld.service

```
[root@localhost ~]# systemctl status firewalld;
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-06-28 13:11:59 EDT; 4min 0s ago
     Docs: man:firewalld(1)
 Main PID: 727 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─727 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid

Jun 28 13:11:59 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Jun 28 13:11:59 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
Jun 28 13:11:59 localhost.localdomain firewalld[727]: WARNING: AllowZoneDrifting is enabled. This is considered an insecure configuration option.... it now.
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost ~]# systemctl stop firewalld;systemctl disable firewalld;
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
[root@localhost ~]# _
```

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

```
[root@localhost ~]# hostnamectl set-hostname firewall;exec bash
[root@firewall ~]# _
```

Step 4: install iptables

```
[root@firewall ~]# yum install iptables*
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.mirror.net.in
 * extras: centos.mirror.net.in
 * updates: centos.mirror.net.in
Package iptables-1.4.21-35.el7.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
---> Package iptables-devel.x86_64 0:1.4.21-35.el7 will be installed
---> Package iptables-services.x86_64 0:1.4.21-35.el7 will be installed
---> Package iptables-utils.x86_64 0:1.4.21-35.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package              Arch          Version              Repository        Size
================================================================================
Installing:
 iptables-devel       x86_64        1.4.21-35.el7        base              57 k
 iptables-services    x86_64        1.4.21-35.el7        base              52 k
 iptables-utils       x86_64        1.4.21-35.el7        base              62 k

Transaction Summary
================================================================================
```

```
[root@firewall ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@firewall ~]# _
```

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

```
[root@firewall ~]# iptables -t nat -A POSTROUTING -s 10.10.10.55 -o ens33 -j MASQUERADE
[root@firewall ~]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  10.10.10.55          anywhere
[root@firewall ~]#
```

Step 7: enable the ip forwarding on the firewall

```
[root@firewall ~]# cat /proc/sys/net/ipv4/ip_forward
0
[root@firewall ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@firewall ~]# cat /proc/sys/net/ipv4/ip_forward
1
[root@firewall ~]# _
```

permanent ip_forwarding

```
[root@firewall ~]# echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf
[root@firewall ~]# cat /etc/sysctl.conf
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward=1
[root@firewall ~]# _
```

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

```
[root@user1 ~]# nslookup www.google.com
Server:         192.168.112.2
Address:        192.168.112.2#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.183.196
Name:   www.google.com
Address: 2404:6800:4009:82d::2004
```

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

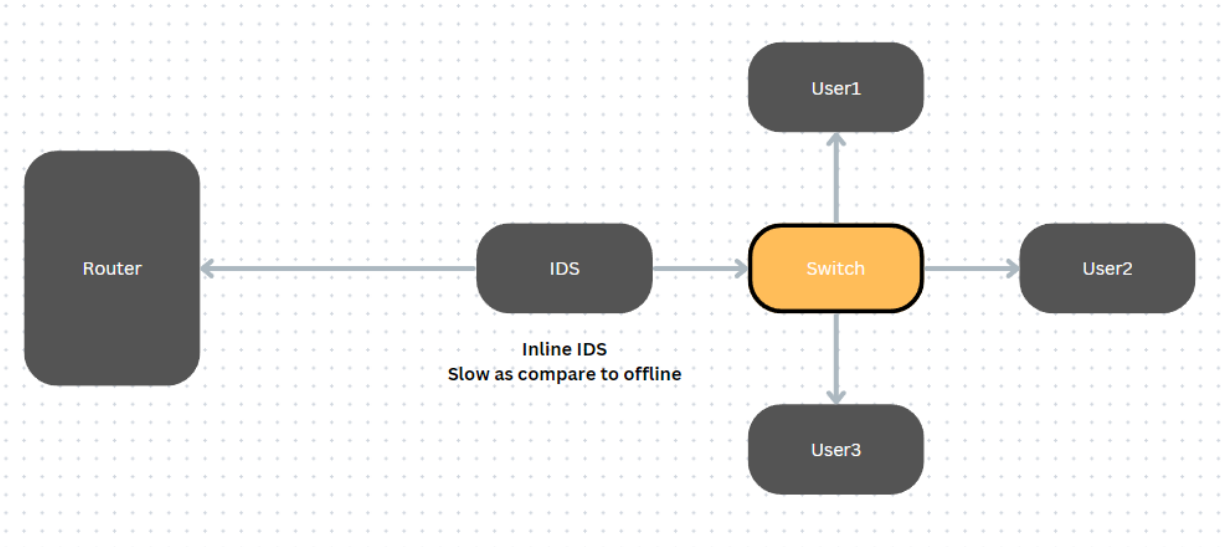
new anomalies can't be detected using signature based method..

False Positive: Normal traffic detected as malicious
False Negative: Malicious traffic detected as Positive

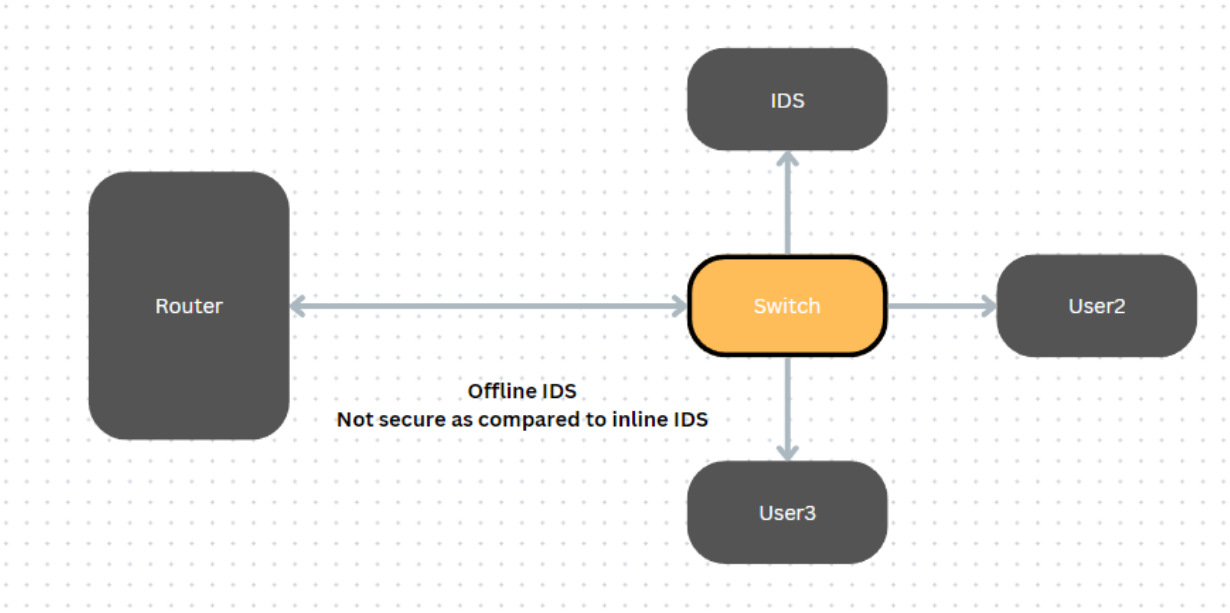
IDS and IPS tuning : we change configuration of IDS and IPS for False Positive or False Negative.

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:

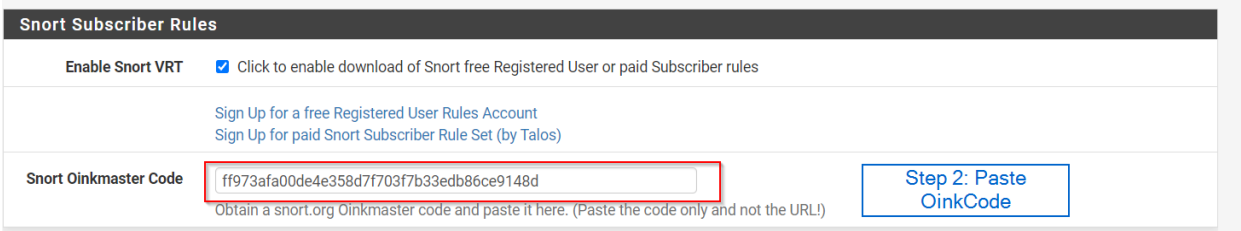


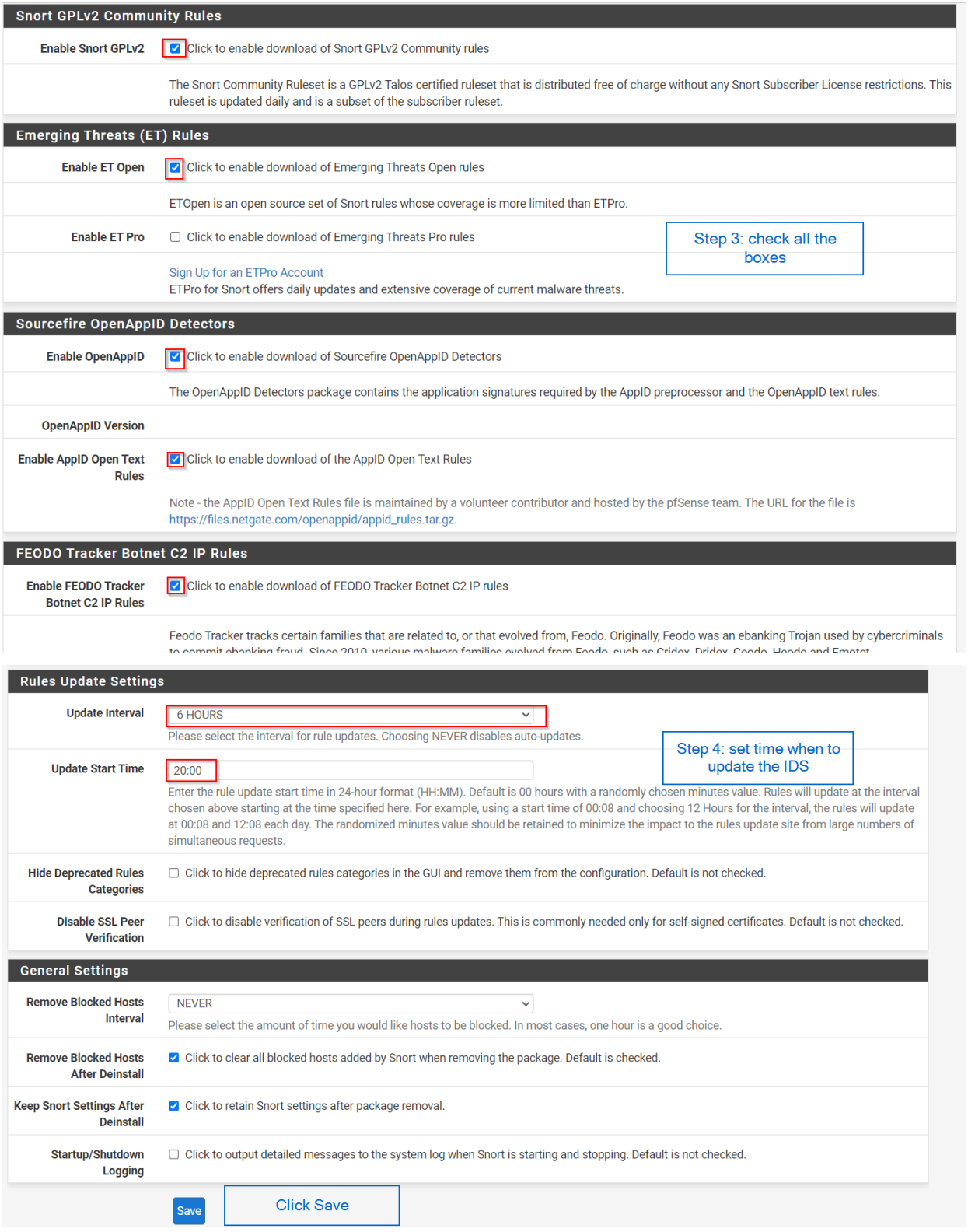
2. offline mode:

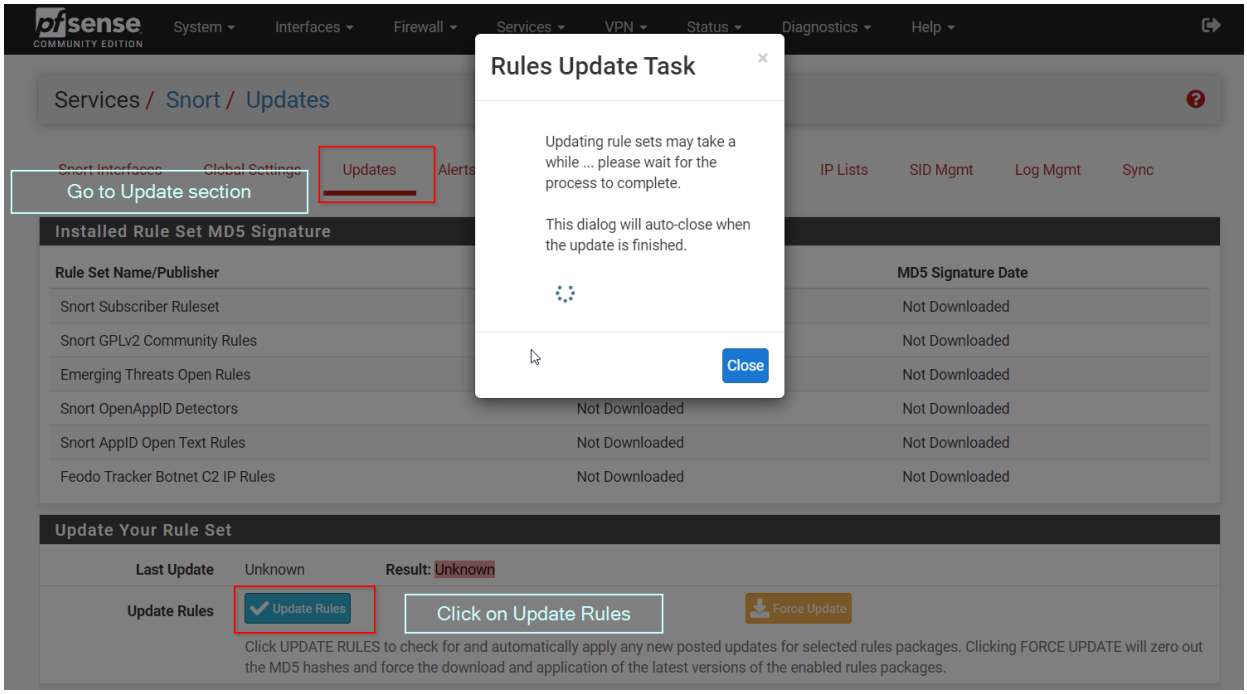


Snort Module: first go to snort website and register for the website and get the oinkcode from there for future use.

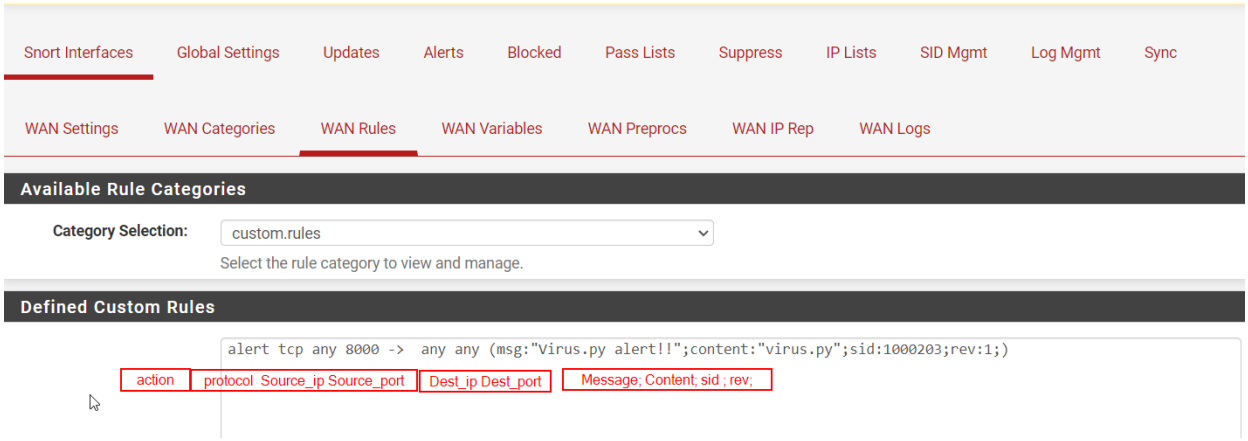
then install snort package in pfsense.. and proceed with the instruction shown below..




Snort GPLv2 Community Rules
Enable Snort GPLv2
Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.
Emerging Threats (ET) Rules
Enable ET Open
Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
Enable ET Pro
Click to enable download of Emerging Threats Pro rules
Step 3: check all the boxes
Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.
Sourcefire OpenAppID Detectors
Enable OpenAppID
Click to enable download of Sourcefire OpenAppID Detectors
The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.
OpenAppID Version
Enable AppID Open Text Rules
Click to enable download of the AppID Open Text Rules
Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz.
FEODO Tracker Botnet C2 IP Rules
Enable FEODO Tracker Botnet C2 IP Rules
Click to enable download of FEODO Tracker Botnet C2 IP rules
Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals
Rules Update Settings
Update Interval
6 HOURS
Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Step 4: set time when to update the IDS
Update Start Time
20:00
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.
Hide Deprecated Rules Categories
Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification
Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.
General Settings
Remove Blocked Hosts Interval
NEVER
Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.
Remove Blocked Hosts After Deinstall
Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall
Click to retain Snort settings after package removal.
Startup/Shutdown Logging
Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.
Save
Click Save



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:"";
```

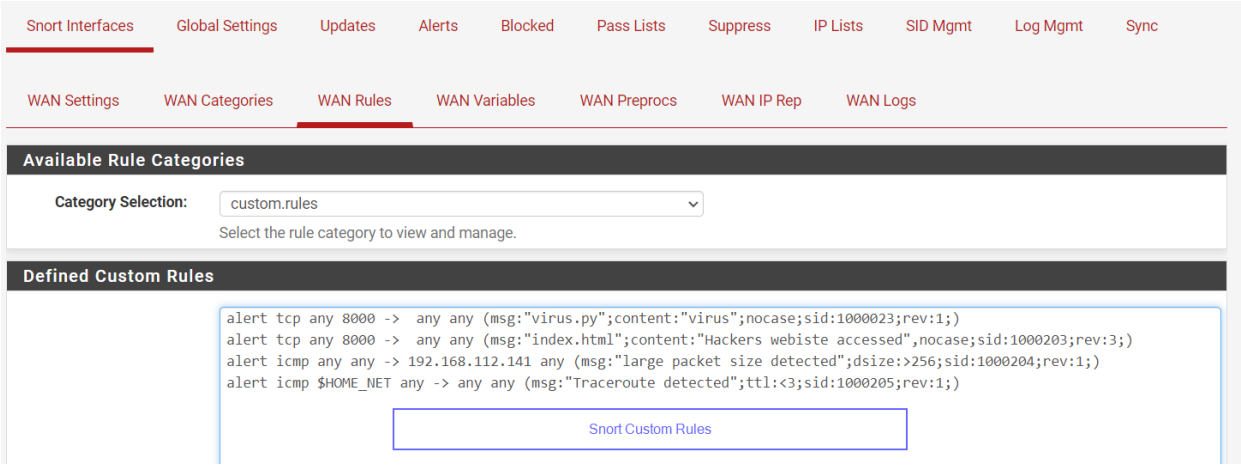
itype: used to define icmp message type

icode:

ICMP Type	Code	Description
0	0	eco reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	7	destination host unknown
8	0	eco request
10	0	router discovery
11	0	TTL expired

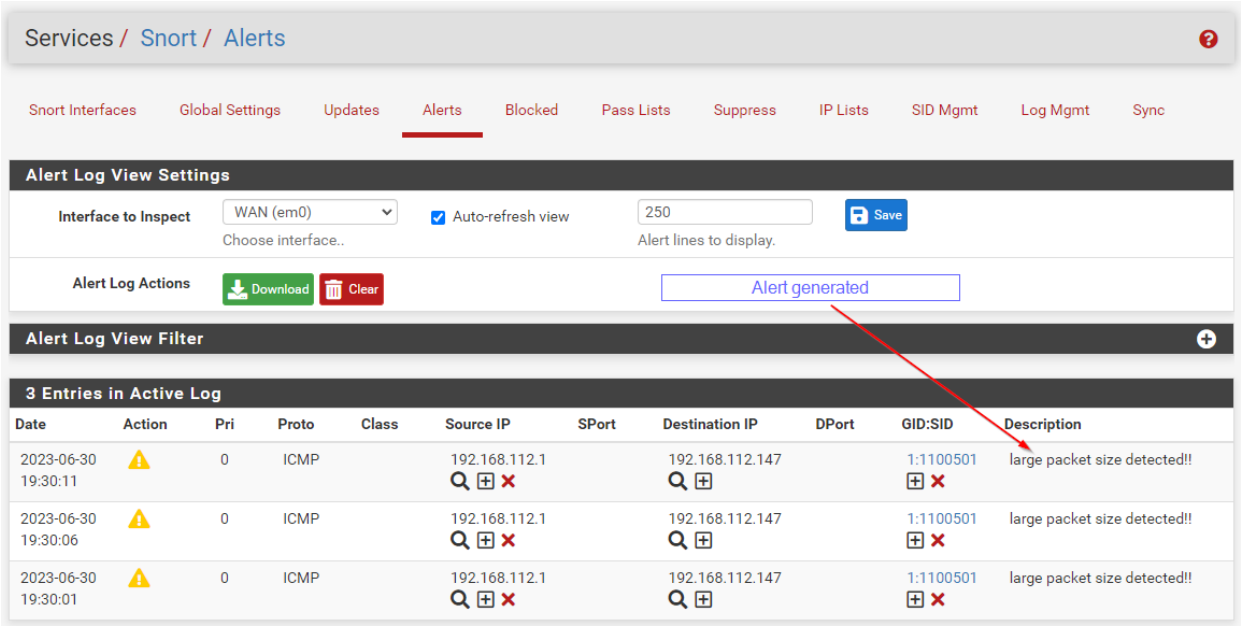
Table 1-3 ICMP Message Types

#Snort Rules

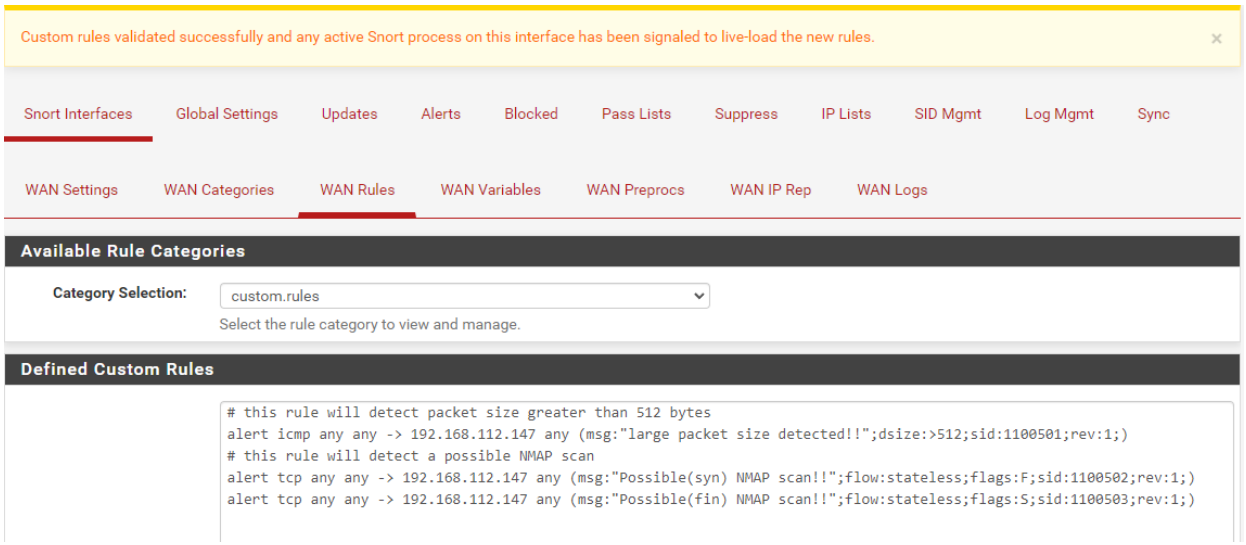


Assignment 4:

-> detect ping for packet greater than 512 bytes



-> detect nmap scan -sF -sS




```
└─# nmap -sS 192.168.112.147;nmap -sF 192.168.112.147;
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-30 08:26 MDT
Nmap scan report for 192.168.112.147
Host is up (0.00041s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8000/tcp open  http-alt
MAC Address: 00:0C:29:50:3C:92 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-30 08:26 MDT
Nmap scan report for 192.168.112.147
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.112.147 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:50:3C:92 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
```

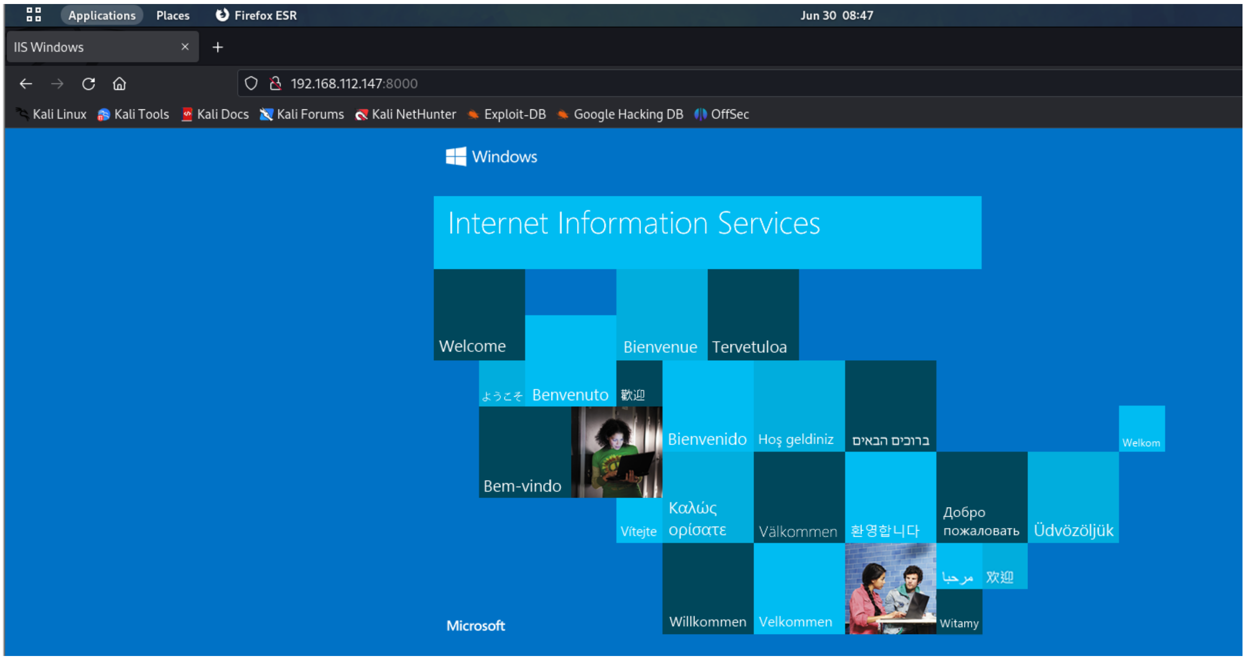
Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-06-30 19:57:09	⚠	0	TCP		192.168.112.1	57002	192.168.112.147	443	1:1100503	Possible(fin) NMAP scan!!
2023-06-30 19:57:08	⚠	0	TCP		192.168.112.1	56999	192.168.112.147	443	1:1100503	Possible(fin) NMAP scan!!
2023-06-30 19:57:08	⚠	0	TCP		192.168.112.1	57000	192.168.112.147	443	1:1100503	Possible(fin) NMAP scan!!
2023-06-30 19:57:01	⚠	0	TCP		192.168.112.1	57002	192.168.112.147	443	1:1100503	Possible(fin) NMAP scan!!
2023-06-30 19:57:00	⚠	0	TCP		192.168.112.1	57000	192.168.112.147	443	1:1100503	Possible(fin) NMAP scan!!
2023-06-30 19:57:00	⚠	0	TCP		192.168.112.1	56999	192.168.112.147	443	1:1100503	Possible(fin) NMAP scan!!
2023-06-30 19:57:00	⚠	0	TCP		192.168.112.142	40615	192.168.112.147	3268	1:1100502	Possible(syn) NMAP scan!!
2023-06-30 19:57:00	⚠	0	TCP		192.168.112.142	40615	192.168.112.147	646	1:1100502	Possible(syn) NMAP scan!!
2023-06-30 19:57:00	⚠	0	TCP		192.168.112.142	40615	192.168.112.147	1914	1:1100502	Possible(syn) NMAP scan!!
2023-06-30 19:57:00	⚠	0	TCP		192.168.112.142	40615	192.168.112.147	2191	1:1100502	Possible(syn) NMAP scan!!

-> detect if windows website is accessed from kali linux generate alert
& if it is accessed from base machine no alert

Defined Custom Rules

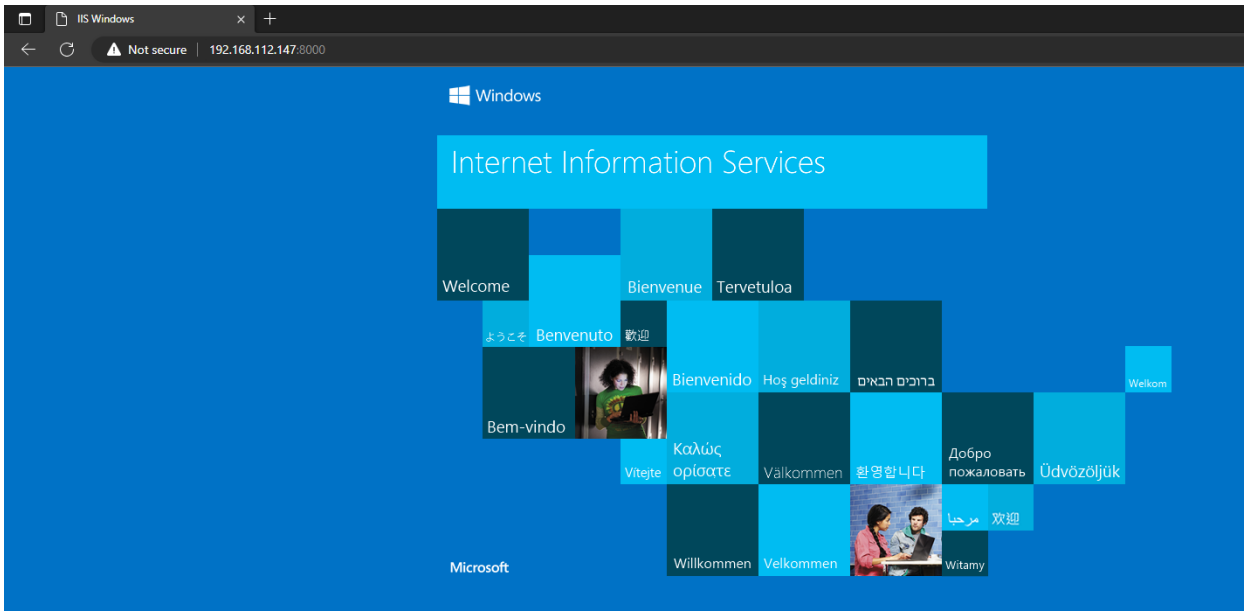
```
# this rule will detect packet size greater than 512 bytes
alert icmp any any -> 192.168.112.147 any (msg:"large packet size detected!!";dsize:>512;sid:1100501;rev:1;)
# this rule will detect a possible NMAP scan
alert tcp any any -> 192.168.112.147 any (msg:"Possible(syn) NMAP scan!!";flow:stateless;flags:F;sid:1100502;rev:1;)
alert tcp any any -> 192.168.112.147 any (msg:"Possible(fin) NMAP scan!!";flow:stateless;flags:S;sid:1100503;rev:1;)
# generate ip if windows website  is accessed from kali machine
alert tcp 192.168.112.142 any -> 192.168.112.147 8000 (msg:"hacker detected!!!";sid:1100504;rev:1;)
```



34 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-06-30 20:17:42	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:17:32	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:17:22	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:17:11	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:17:01	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:16:51	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:16:41	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:16:41	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:16:41	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:16:41	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:16:41	⚠	0	TCP		192.168.112.142	44260	192.168.112.147	8000	1:1100504	hacker detected!!!

```
# accessed from base windows machine
```



5 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-06-30 20:22:13	⚠	0	TCP		192.168.112.142	46796	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:22:03	⚠	0	TCP		192.168.112.142	46796	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:21:53	⚠	0	TCP		192.168.112.142	46796	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:21:42	⚠	0	TCP		192.168.112.142	46796	192.168.112.147	8000	1:1100504	hacker detected!!!
2023-06-30 20:21:32	⚠	0	TCP		192.168.112.142	46796	192.168.112.147	8000	1:1100504	hacker detected!!!

```
Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fb6f:5d87:50c6:4b91%16
   IPv4 Address. . . . . . . . . . . : 192.168.82.124
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.82.254
```

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

Available Rule Categories

Category Selection: custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```
# this rule will detect packet size greater than 512 bytes
alert icmp any any -> 192.168.112.147 any (msg:"large packet size detected!!";dsize:>512;sid:1100501;rev:1;)
# this rule will detect a possible NMAP scan
alert tcp any any -> 192.168.112.147 any (msg:"Possible(syn) NMAP scan!!";flow:stateless;flags:F;sid:1100502;rev:1;)
alert tcp any any -> 192.168.112.147 any (msg:"Possible(fin) NMAP scan!!";flow:stateless;flags:S;sid:1100503;rev:1;)
# generate ip if windows website  is accessed from kali machine
alert tcp 192.168.112.142 any -> 192.168.112.147 8000 (msg:"hacker detected!!!";sid:1100504;rev:1;)

# RULE to detect if there is any ssh to the NAT ip of the pfsense.. (ssh uses tcp)
alert tcp any any -> 192.168.112.147 22 (msg:"ssh login detected";sid:1100505;rev:1;)
```

```
C:\Users\rajesh>ssh root@192.168.112.147
The authenticity of host '192.168.112.147 (192.168.112.147)' can't be established.
ECDSA key fingerprint is SHA256:P3GwlK7NDrWZP/2NVG23E6Li4IGld/nORSHa31CYCoE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.112.147' (ECDSA) to the list of known hosts.
root@192.168.112.147's password:
Last login: Fri Jun 30 12:12:43 2023
[root@master ~]#
```

18 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-06-30 20:29:41	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:40	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:40	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:40	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:40	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:40	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:39	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:38	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:38	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected
2023-06-30 20:29:38	⚠	0	TCP		192.168.112.1	57338	192.168.112.147	22	1:1100505	ssh login detected

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

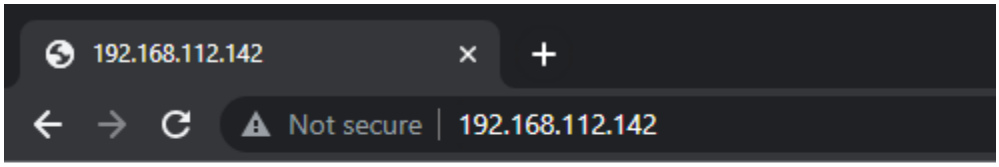
Available Rule Categories

Category Selection: custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```
# this rule will detect packet size greater than 512 bytes
alert icmp any any -> 192.168.112.147 any (msg:"large packet size detected!!";dsize:>512;sid:1100501;rev:1;)

# this rule will detect a possible NMAP scan
alert tcp any any -> 192.168.112.147 any (msg:"Possible(syn) NMAP scan!!";flow:stateless;flags:F;sid:1100502;rev:1;)
alert tcp any any -> 192.168.112.147 any (msg:"Possible(fin) NMAP scan!!";flow:stateless;flags:S;sid:1100503;rev:1;)

# generate ip if windows website  is accessed from kali machine
alert tcp 192.168.112.142 any -> 192.168.112.147 8000 (msg:"hacker detected!!!";sid:1100504;rev:1;)

# RULE to detect if there is any ssh to the NAT ip of the pfsense.. (ssh uses tcp)
alert tcp any any -> 192.168.112.147 22 (msg:"ssh login detected";sid:1100505;rev:1;)

# RULE to check if kali website is accessed or not .
alert tcp any any -> 192.168.112.142 any (msg:"restricted webiste is accessed";sid:1100506;rev:3;)

# RULE to block if kali website is accessed or not .
block tcp any any -> 192.168.112.142 any (msg:"restricted webiste is blocked";sid:1100506;rev:3;)
```



welcome to the ghost's website

Alert Log View Filter

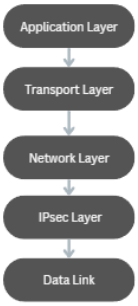
36 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-06-30 21:07:30	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked
2023-06-30 21:07:30	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked
2023-06-30 21:07:04	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked
2023-06-30 21:07:04	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked
2023-06-30 21:06:38	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked
2023-06-30 21:06:38	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked
2023-06-30 21:06:30	⚠	0	TCP		192.168.112.1	57588	192.168.112.142	80	1:1100506	restricted webiste is blocked
2023-06-30 21:06:12	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked
2023-06-30 21:06:12	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked
2023-06-30 21:05:46	⚠	0	TCP		35.201.124.9	443	192.168.112.142	54158	1:1100506	restricted webiste is blocked

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

VPN

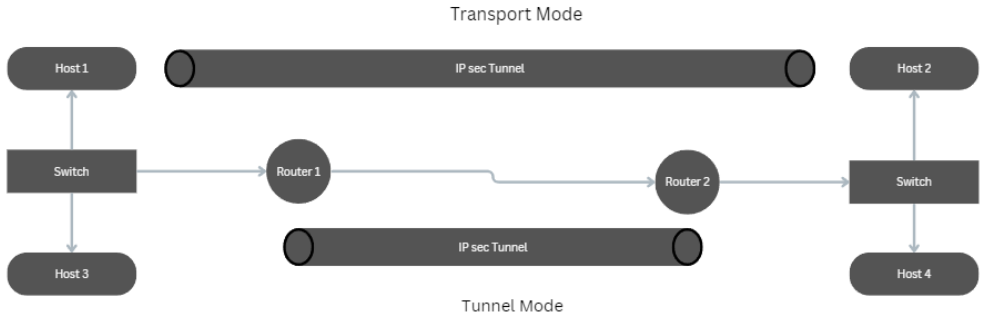
############



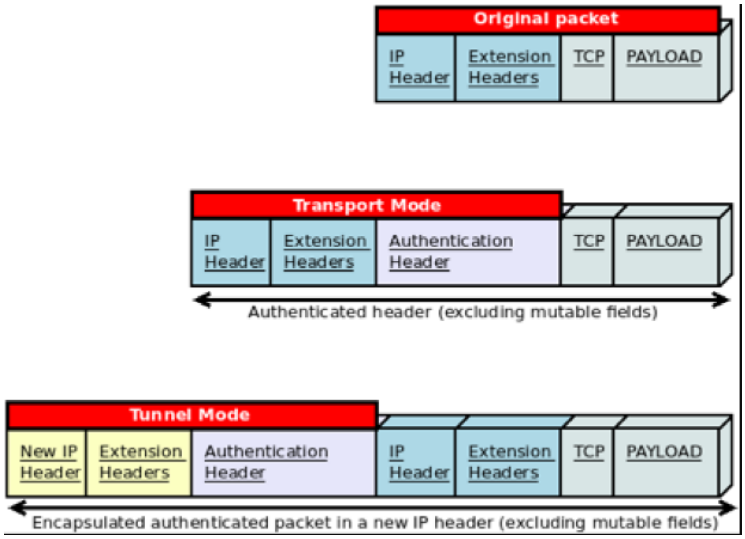
VPN encrypts the data from the network layer to data link layer with the help of data Ipsec layer.

vpn modes:

1. Transport Mode : encryption between host to host
2. Tunnel Mode : encryption between router to router



IPsec headers:

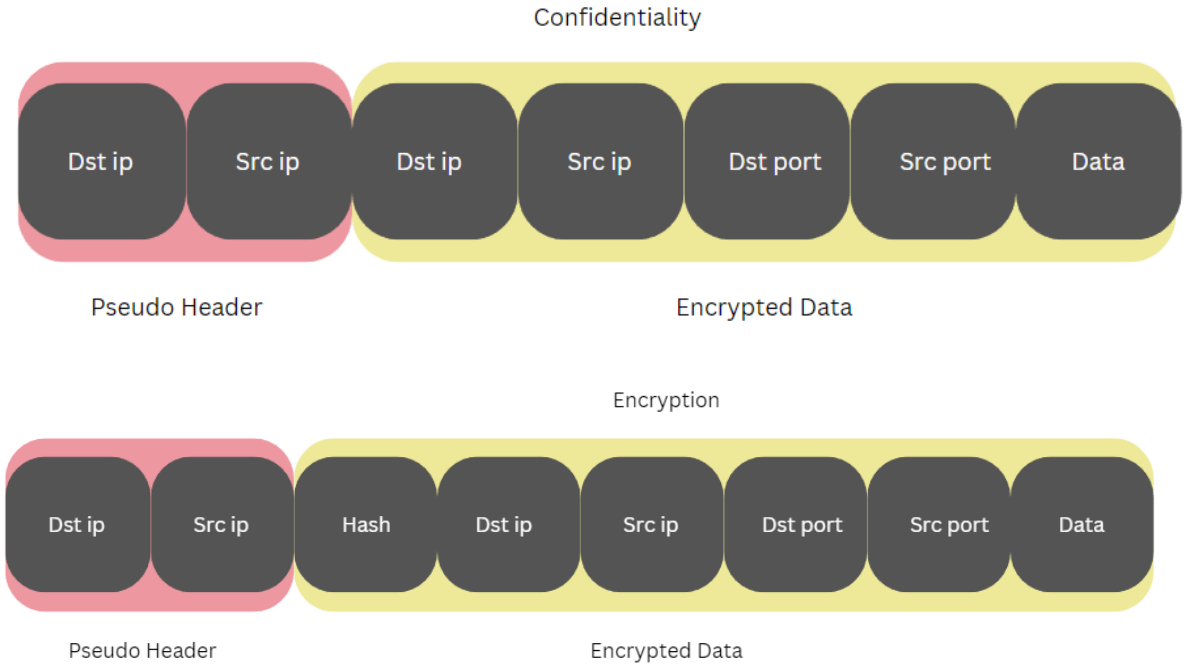


Authentication Header(AH)
Used to check integrity of the data Does not provide confidentiality data is not encrypted.

-> when a hash is also encrypted before sending we call it.
HMAC(Hashboard Message Authentication Code)

-> during HMAC calculation the mutable field actual values are not used rather the value is replaced by 0

When to use encryption: to maintain confidentiality
when to use Hashing: to maintain confidentiality + integrity

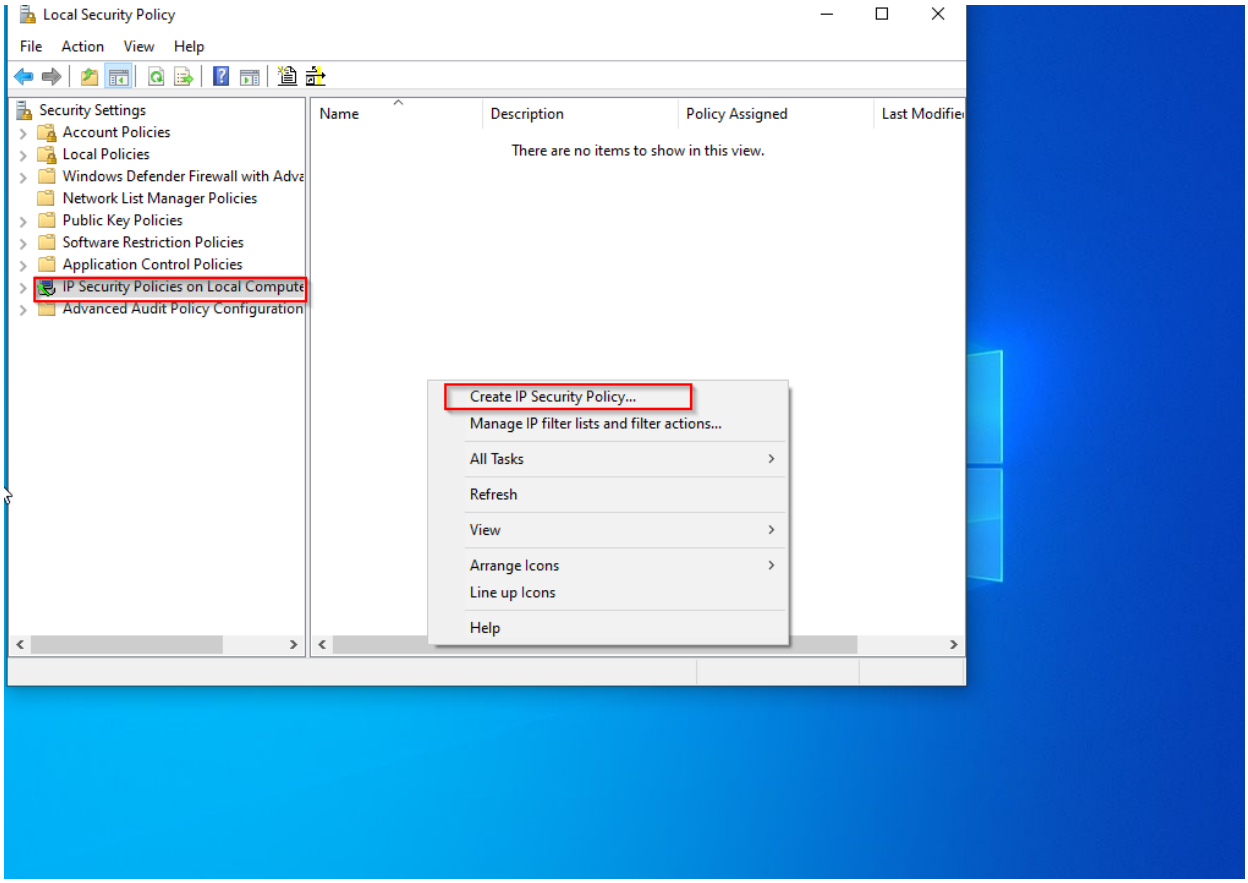


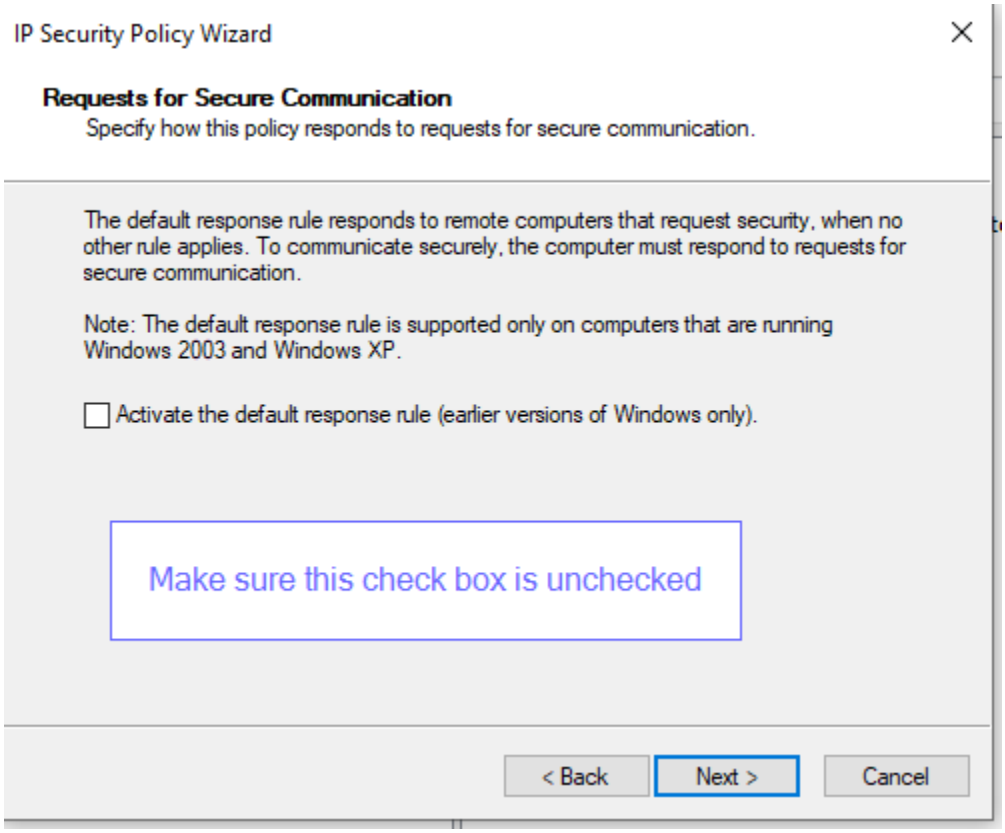
IPSEc implementation:

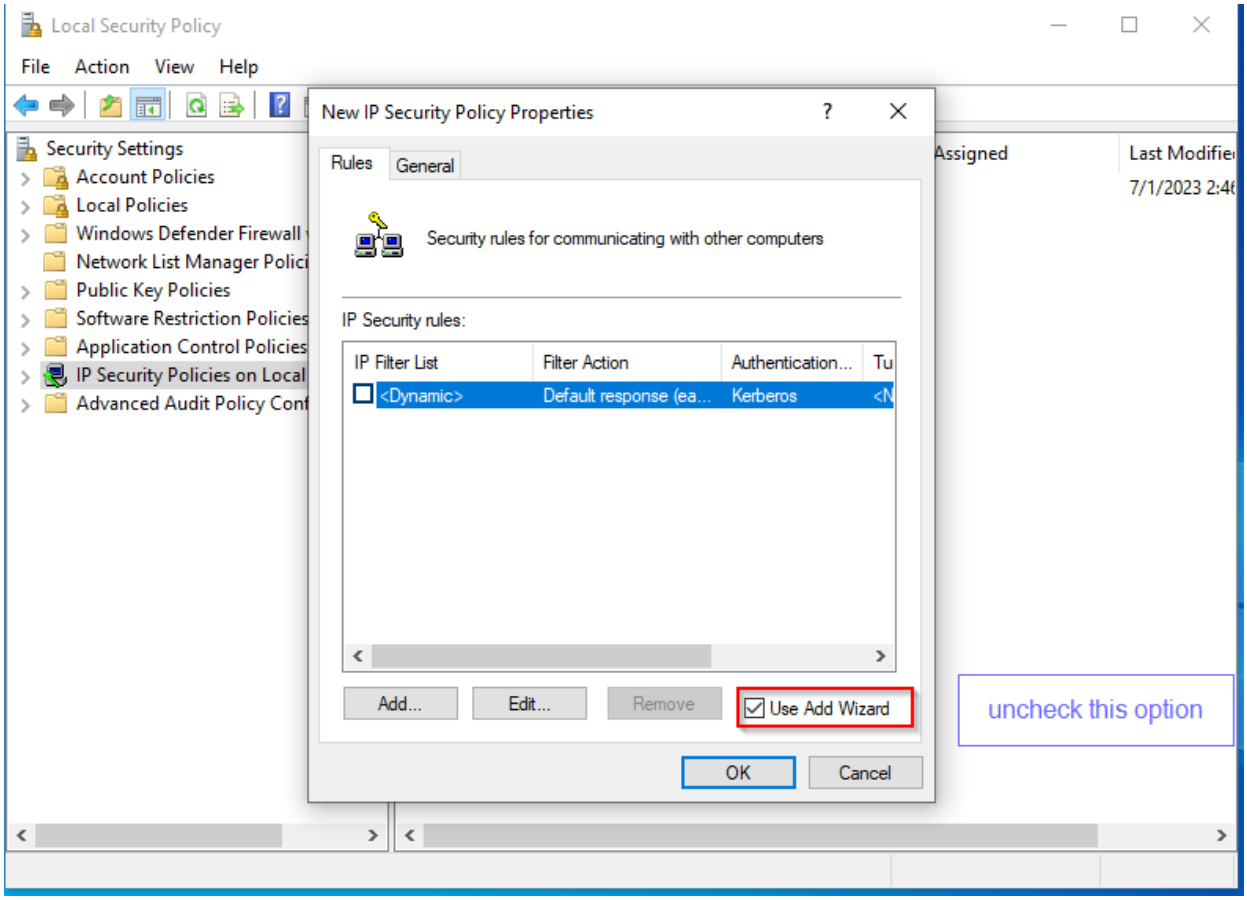
window machine1 : FTP server with login

window machine2 : FTP server with login

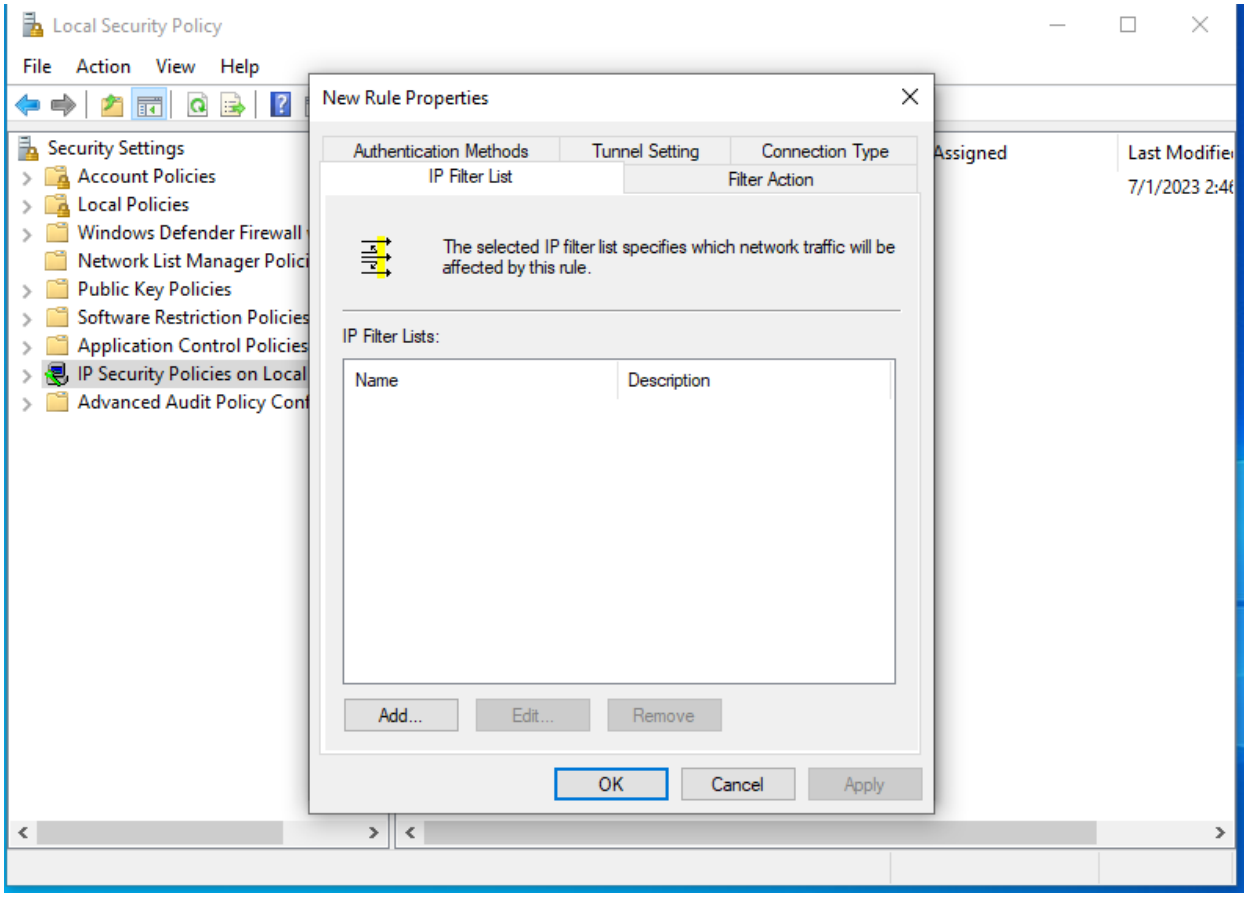
-> search for
secpol.msc
-> right click in the blank space and choose


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Name
Description
Policy Assigned
Last Modifie
There are no items to show in this view.
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
Refresh
View
Arrange Icons
Line up Icons
Help

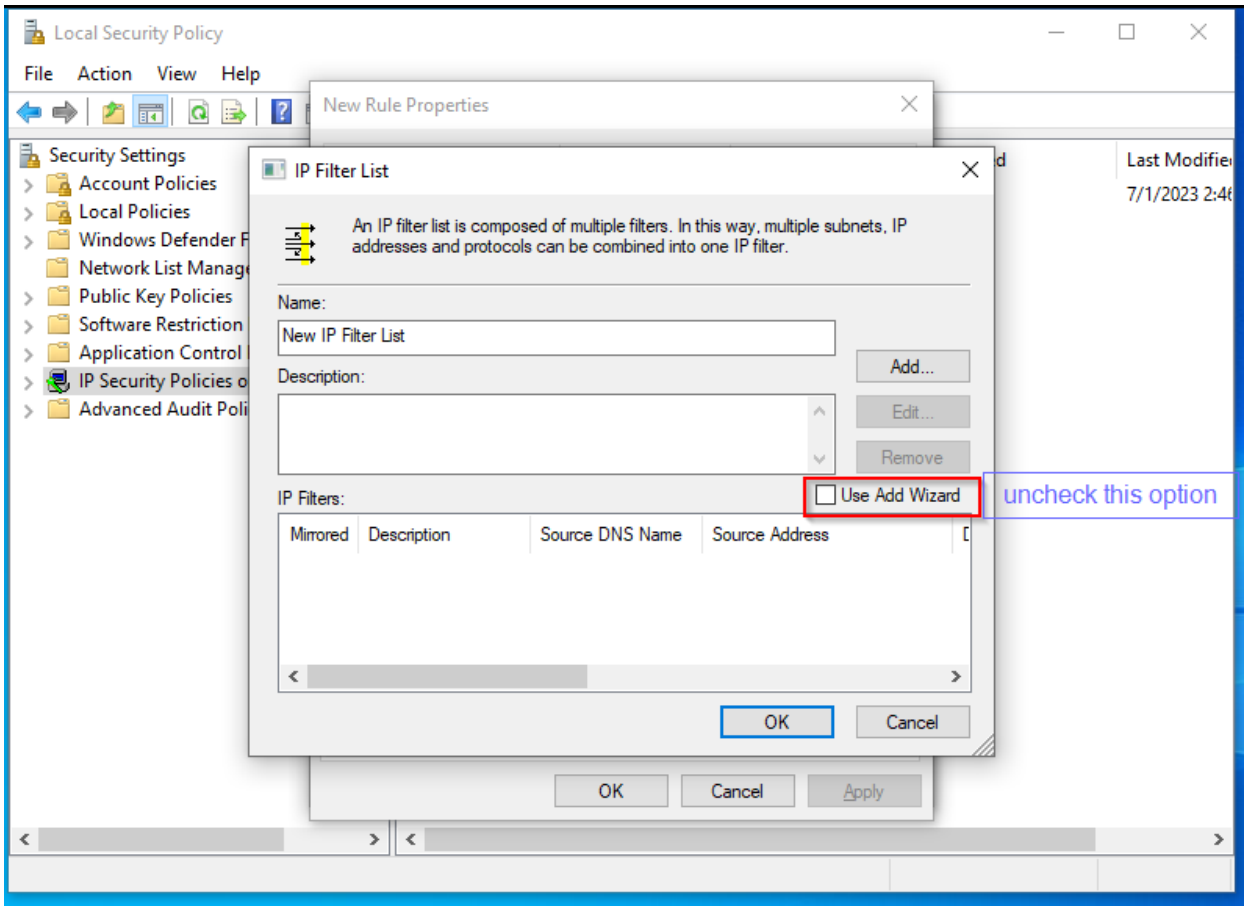

IP Security Policy Wizard
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
Note: The default response rule is supported only on computers that are running Windows 2003 and Windows XP.
Activate the default response rule (earlier versions of Windows only).
Make sure this check box is unchecked
< Back
Next >
Cancel



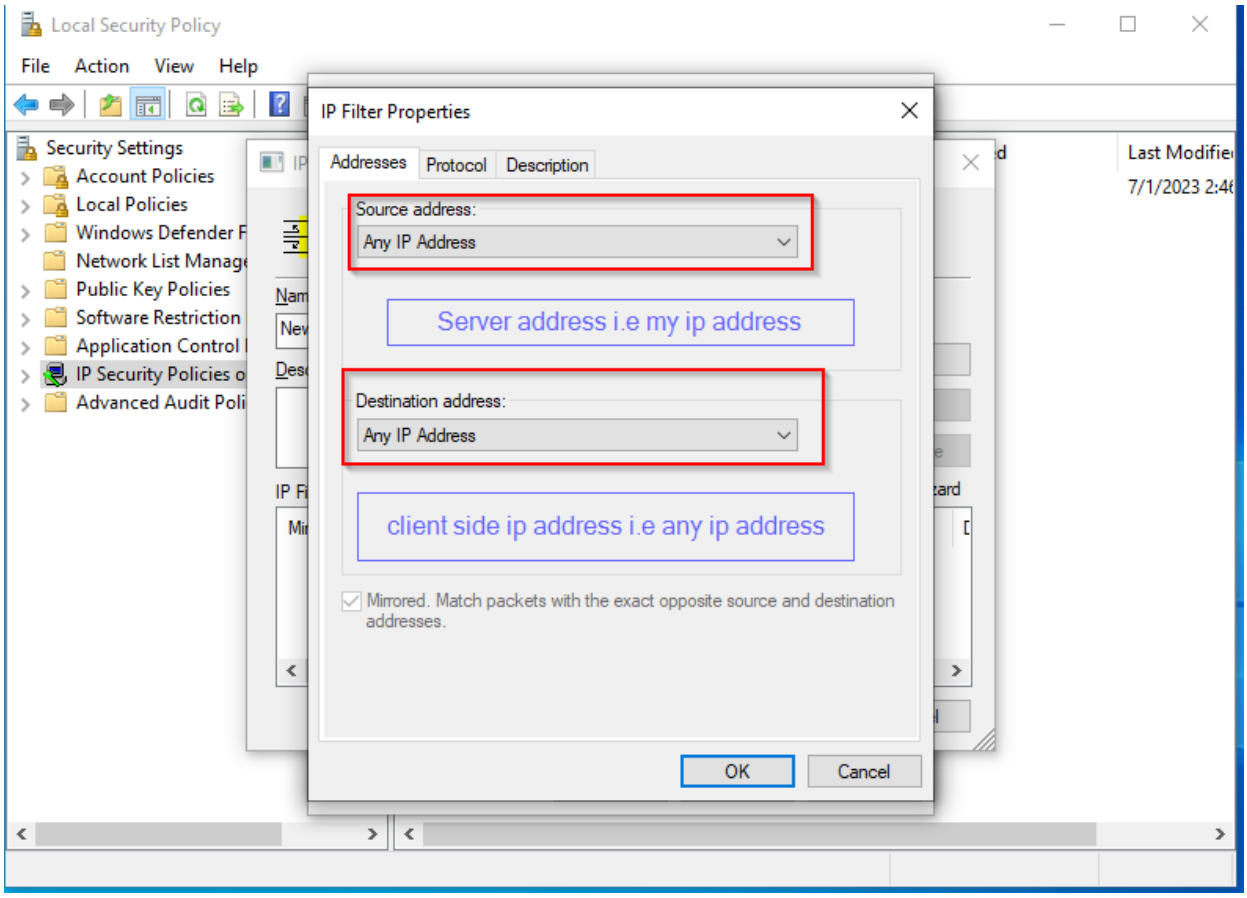
after clicking on the add button

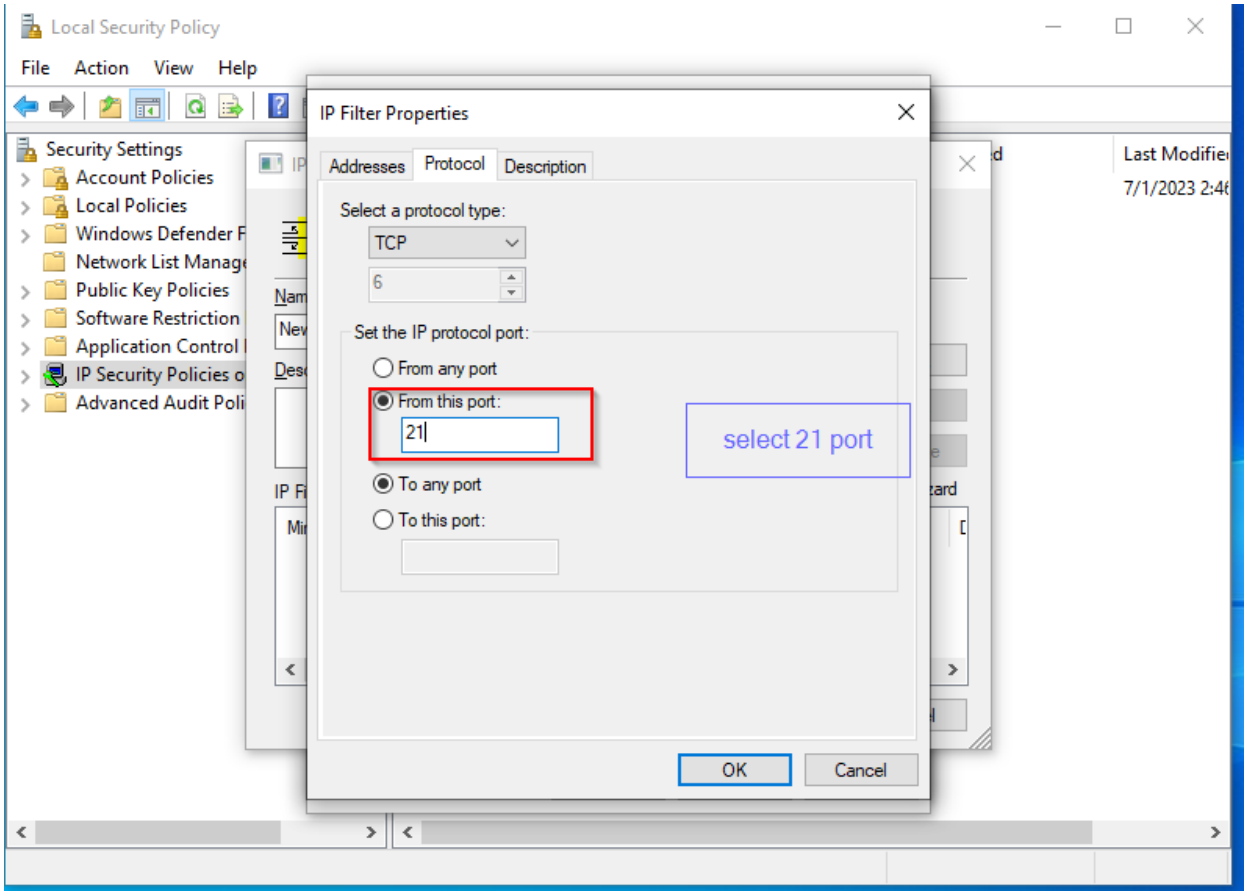


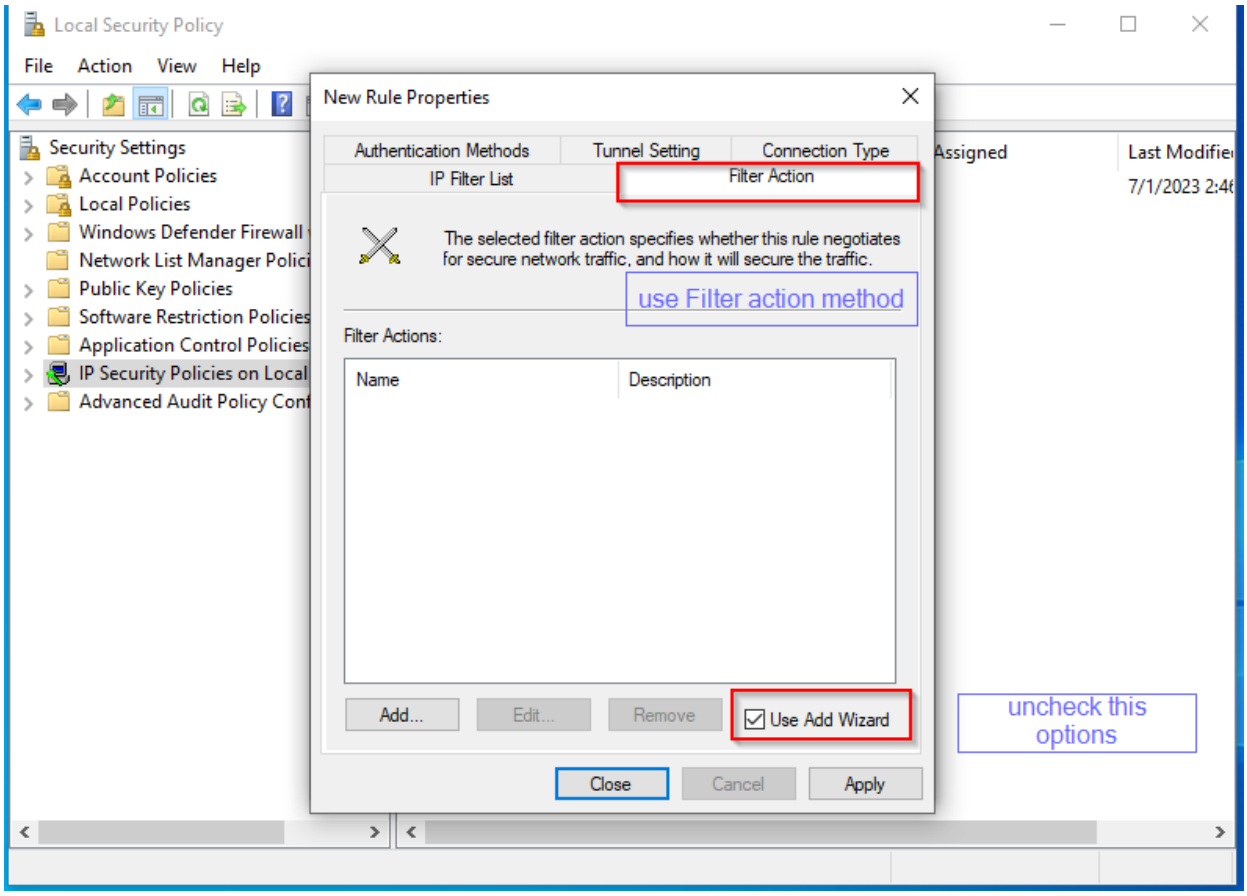
click add in IP filter list

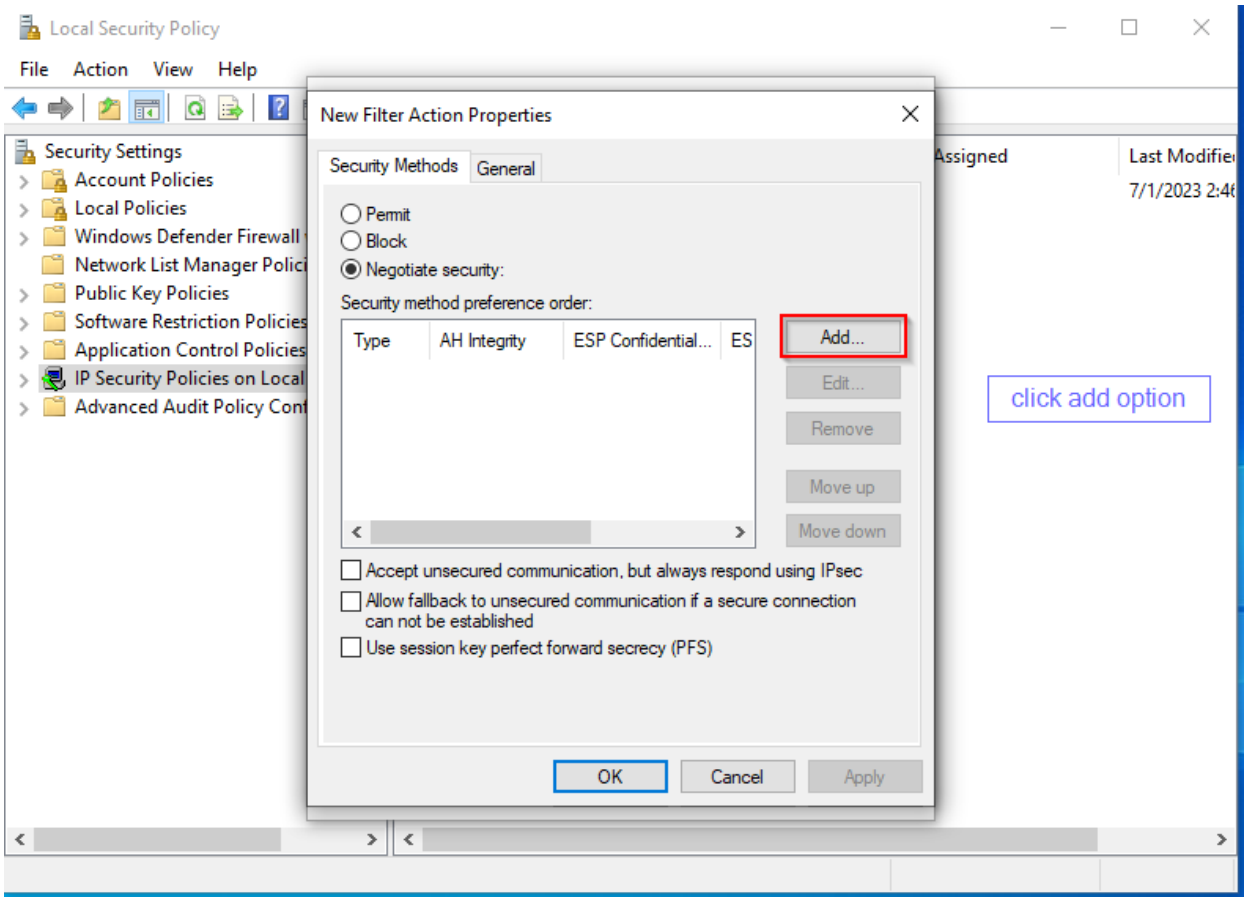


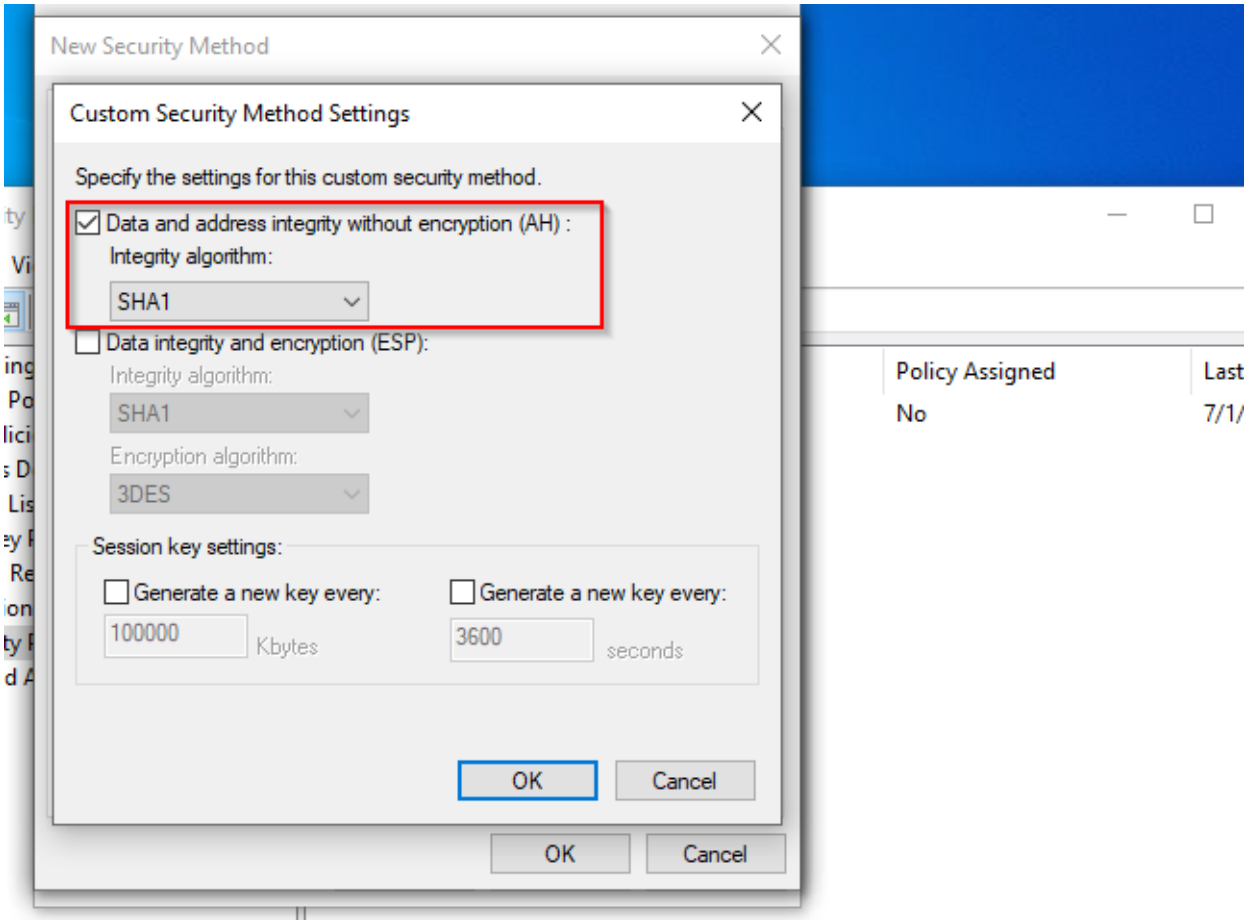
click add in IP filter list


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Defender F
Network List Manage
Public Key Policies
Software Restriction
Application Control
IP Security Policies o
Advanced Audit Poli
Last Modifie
7/1/2023 2:46
IP Filter Properties
Addresses
Protocol
Description
Source address:
Any IP Address
Server address i.e my ip address
Destination address:
Any IP Address
client side ip address i.e any ip address
Mirrored. Match packets with the exact opposite source and destination addresses.
OK
Cancel

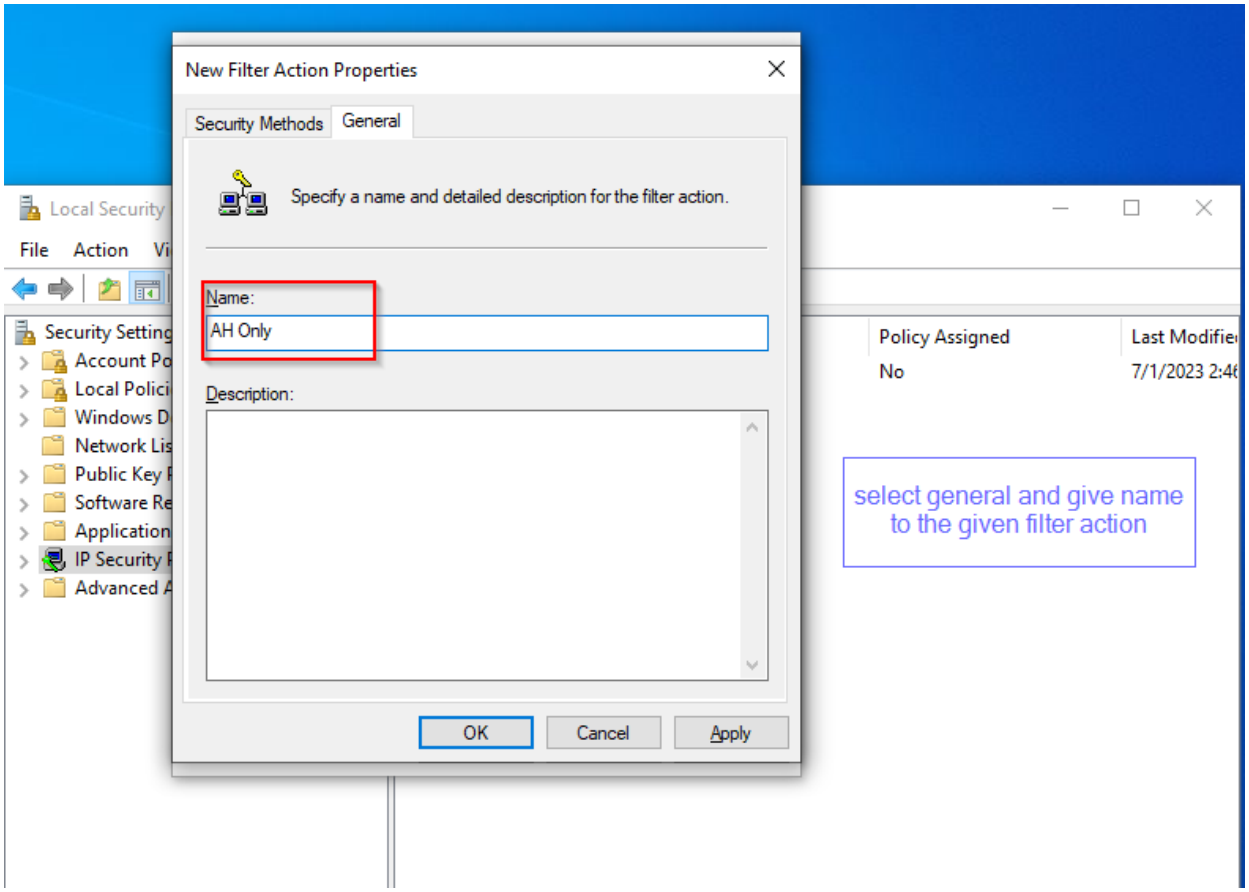

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Defender F
Network List Manage
Public Key Policies
Software Restriction
Application Control
IP Security Policies o
Advanced Audit Poli
Last Modifie
7/1/2023 2:46
IP Filter Properties
Addresses
Protocol
Description
Select a protocol type:
TCP
6
Set the IP protocol port:
From any port
From this port:
21
To any port
To this port:
select 21 port
OK
Cancel


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall
Network List Manager Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local
Advanced Audit Policy Cont
Assigned
Last Modifie
7/1/2023 2:46
New Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.
use Filter action method
Filter Actions:
Name
Description
Add...
Edit...
Remove
Use Add Wizard
uncheck this options
Close
Cancel
Apply

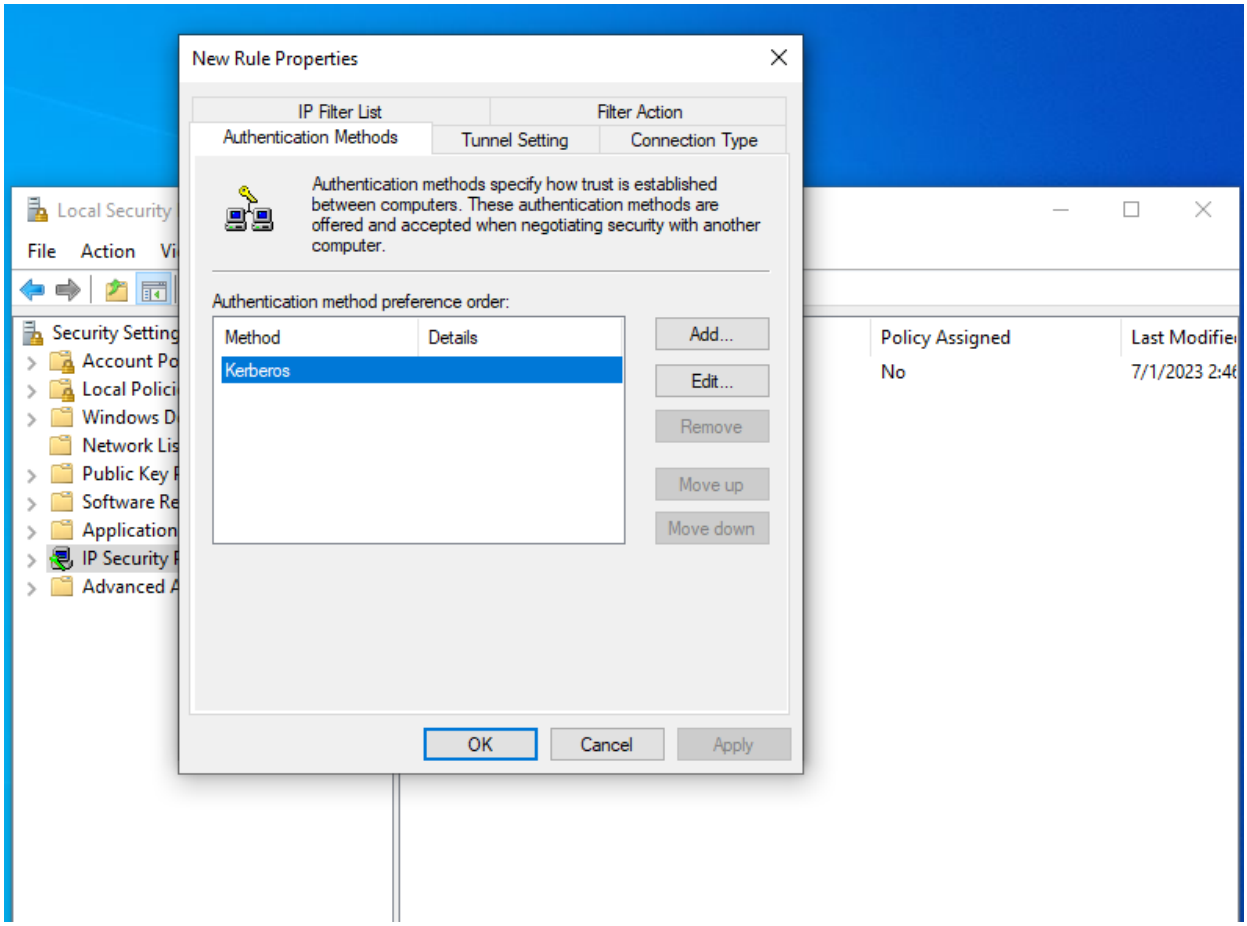

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall
Network List Manager Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local
Advanced Audit Policy Conf
Assigned
Last Modifie
7/1/2023 2:4
New Filter Action Properties
Security Methods
General
Permit
Block
Negotiate security:
Security method preference order:
Type
AH Integrity
ESP Confidential...
ES
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPsec
Allow fallback to unsecured communication if a secure connection can not be established
Use session key perfect forward secrecy (PFS)
OK
Cancel
Apply
click add option


New Security Method
Custom Security Method Settings
Specify the settings for this custom security method.
Data and address integrity without encryption (AH) :
Integrity algorithm:
SHA1
Data integrity and encryption (ESP):
Integrity algorithm:
SHA1
Encryption algorithm:
3DES
Session key settings:
Generate a new key every:
100000
Kbytes
Generate a new key every:
3600
seconds
OK
Cancel
OK
Cancel
Policy Assigned
Last
No
7/1/

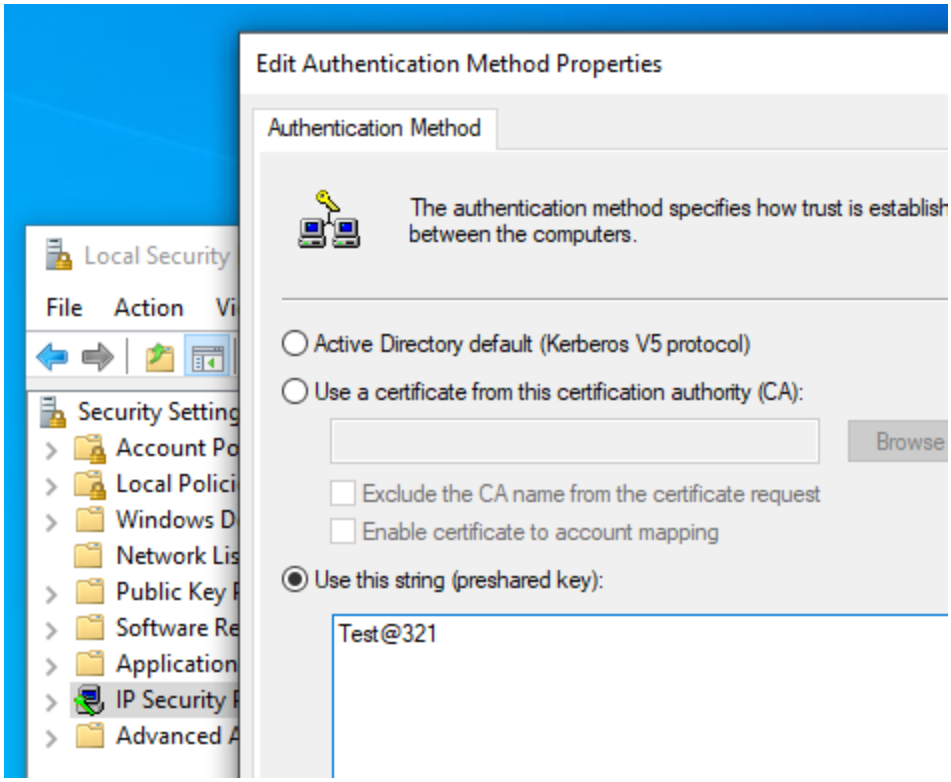
click ok



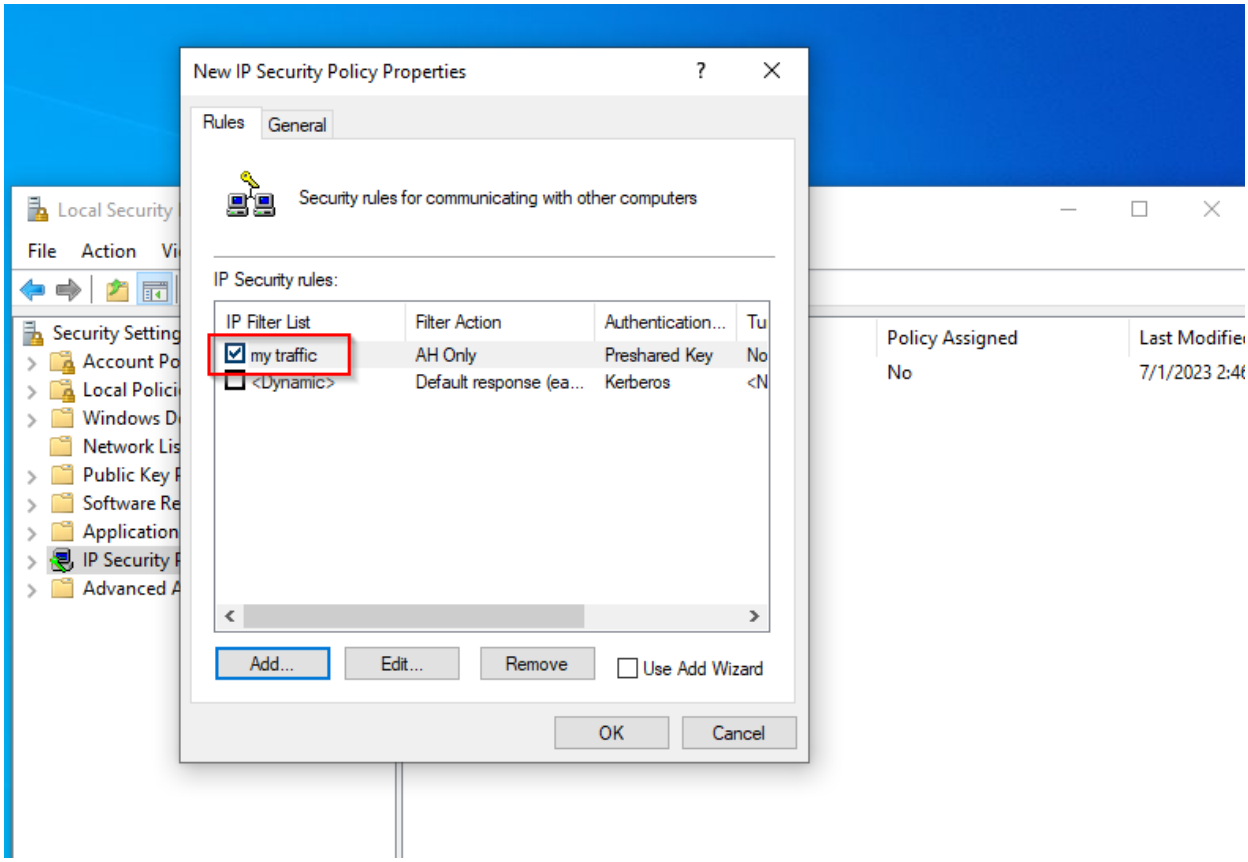
click apply and ok



click edit in authentication method



click apply and ok



==========

-> go to c drive

-> go inside inetpub

-> create a folder web2

-> create a index.html inside web2