**********DAY_07_STM**********

Firewall Assignment:

Add 2 n/w cards to VM. One in NAT mode, one in host only.

1.List all active zones.

firewall-cmd --get-active-zones

public

interfaces: ens33 ens36

2.List current configuration of public zones and internal zone.

firewall-cmd --list-all --zone=public

public (active)

target: default

icmp-block-inversion: no

interfaces: ens33 ens36

sources:

services: dhcpv6-client ssh

ports:

protocols:

masquerade: no

forward-ports:

source-ports:

icmp-blocks:

rich rules:

3.Add port 80 TCP in public zone.

firewall-cmd --add-port=80/tcp

ports: 80/tcp

4.Add ports- 25,110,20,21 (TCP) and 5666 (UDP) in internal zone.

firewall-cmd --add-port={25/tcp,110/tcp,20/tcp,21/tcp,5666/udp} --zone=internal

5.Shift the second interface to the internal zone.

firewall-cmd --remove-interface=ens36 --zone=public

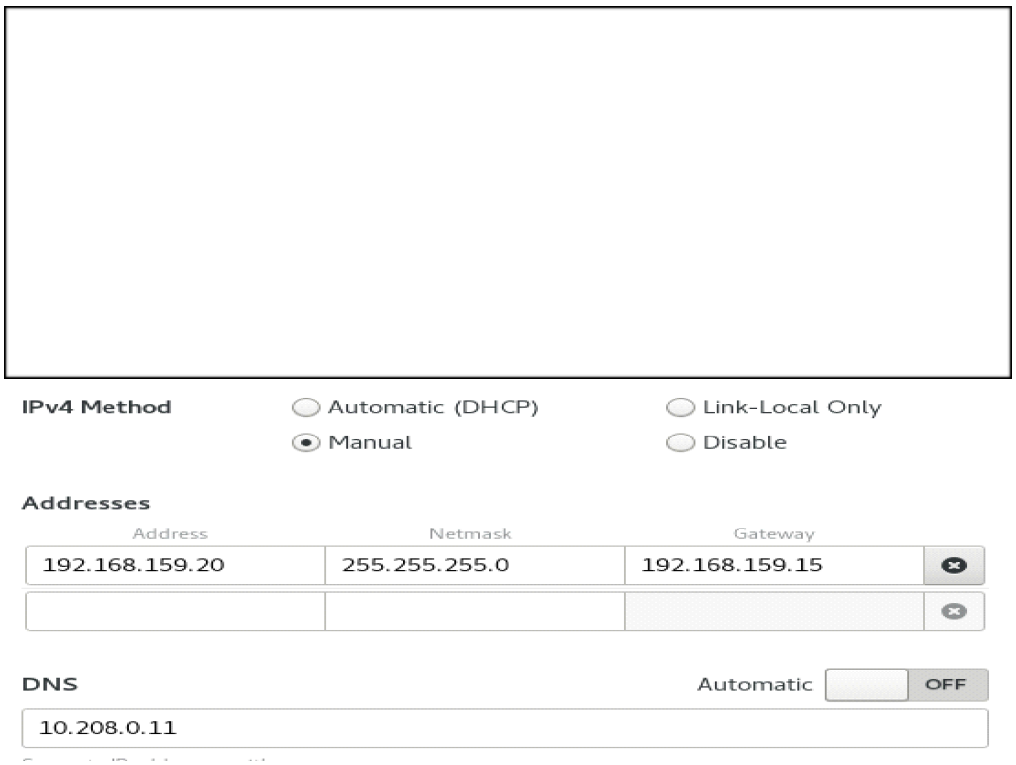
firewall-cmd --add-interface=ens36 --zone=internal

6.Add 192.168.10.15 IP address to the sources in the internal sources.

firewall-cmd --add-source=192.168.10.15 --zone=internal

7.List services pre-defined in firewalld.

firewall-cmd --get-services



Services-->Snort-->Edit

WAN rules--->Delete all rules--->save

Intrusion prevention System:

WAN settings -->Block offender –legacy

Which Ip to block --->Both -->SAVE--> restart interface

Rules--->Custom rules

alert tcp any any -> any any (content:"facebook.com"; message:"facebook accessed"; sid: 200000045,)

alert tcp any any -> any any (content:"twitter.com"; message:"twitter accessed"; sid: 200000065)

********************IP Security (IPSec)*************************

VPN: Sending encrypted data over internet. VPN stands for the Virtual Private Network. It creates a secure network connection over a public network like the internet.

Types-

n/w to n/w

dial-up vpn (mostly for individual users)

One of the protocols is **IPSec (Network layer protocol)**-

- Encrypt the data coming from upper layer.
- Decides the path for the data.
- Supports peer-authentication, data origin authentication, data integrity, replay attack protection (All he or she has to do is **capture and resend the entire thing — message and key — together**. To counter this possibility, both sender and receiver should establish a completely random session key, which is a type of code that is only valid for one transaction and can't be used again.).
- https://www.privateinternetaccess.com/blog/prevent-replay-attacks/
- IPSec is an open standard (that acts at the network level. It can be used to securely transfer data from host-to-host, network-to-network, or between a network and a host. IPsec is most commonly used to secure traffic that passes over IPv4)
- **IPsec can be implemented in two modes-**

1.Transport Mode

Destination iP	Source iP	Source Packet	Destination Packet	DATA

IPSec communication is b/w host to host.

Only the data portion of packet is encrypted. (Here blue is encrypted)

2.Tunnel Mode

Destination iP (pseudo)	Source iP (pseudo)	Dest Ip	Source Ip	Source Packet	Destination Packet	DATA

Preferred in n/w to n/w, host to host, host to n/w

- **Security Association:** Data structure containing keys. https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/topic-map/ipsec-security-associations-overview.html

SAD (Security Association Database)

- **IPSec uses two protocols to provide security**

Authentication Header (AH)- Provide two services Authentication and Integrity

AH is defined in RFC 2402 and uses **IP Protocol 51**. AH can be deployed in either transport or tunnel mode.

Provide by computing cryptographic Hash-based Authentication Code (HMAC) over the IP packet.

Encapsulation Security Payload (ESP)-

- **Diffie-Hellman**

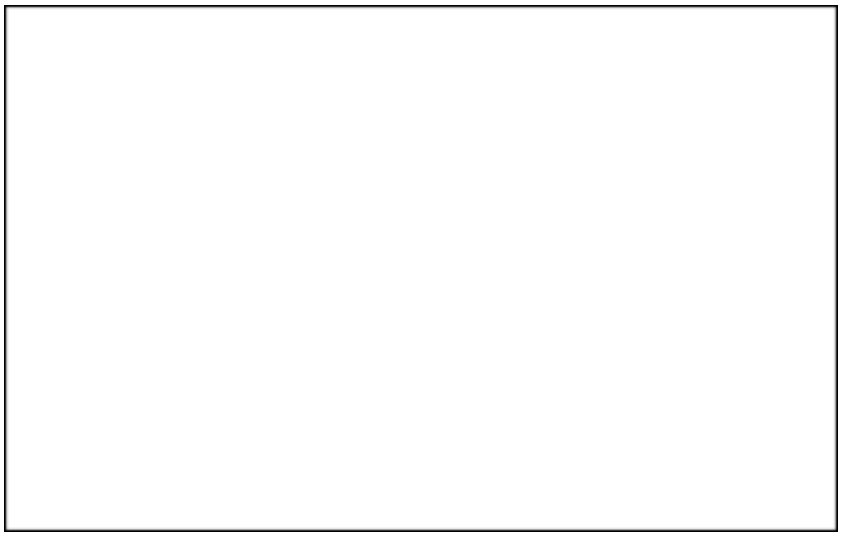
----------LAB----------

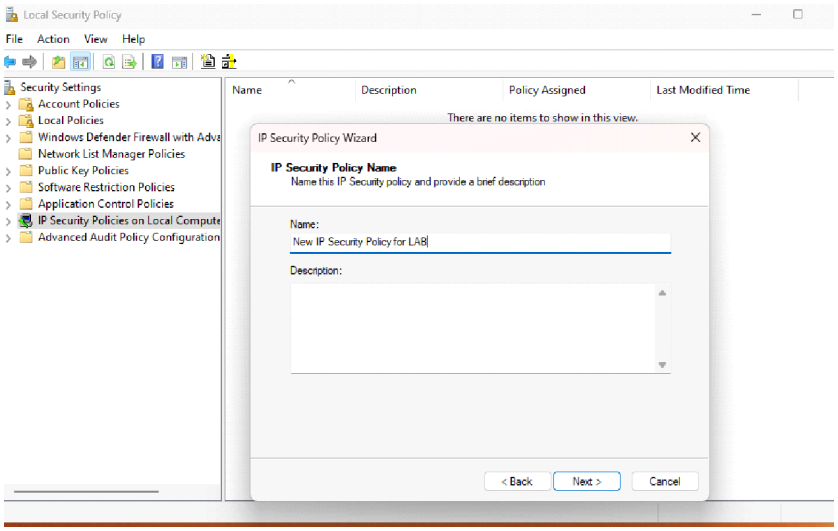
secpol.msc in windows search

IP sec policy

IP Filter List:

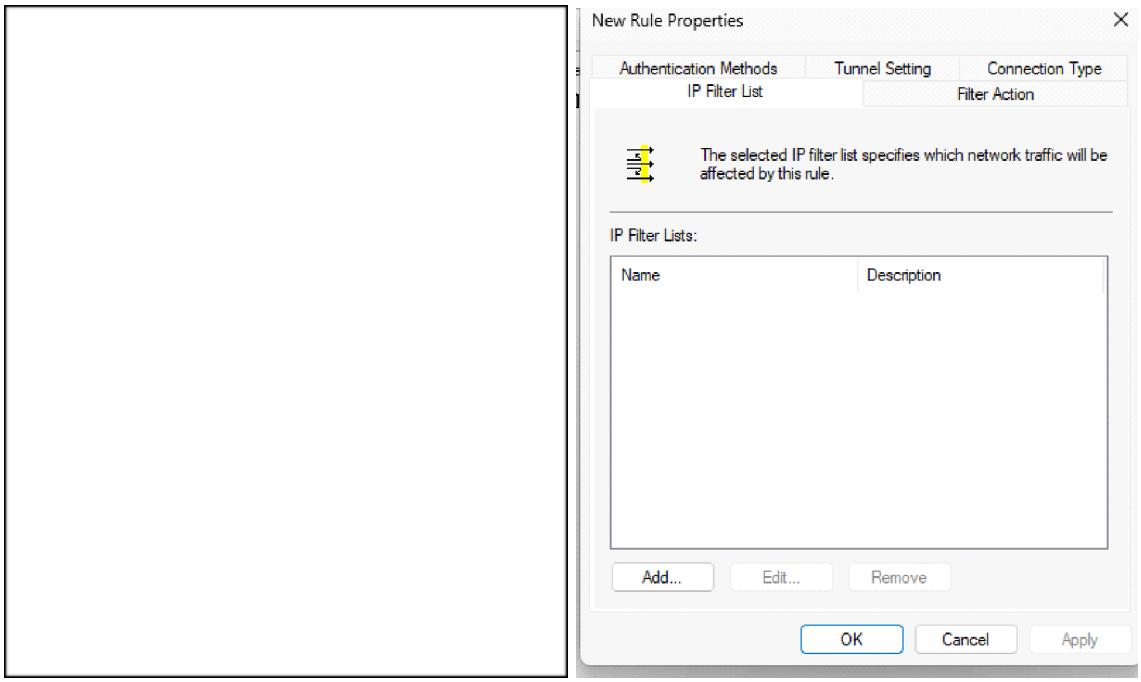
IP security Policies on Local Computer --> Right click -->Create IPsec policy





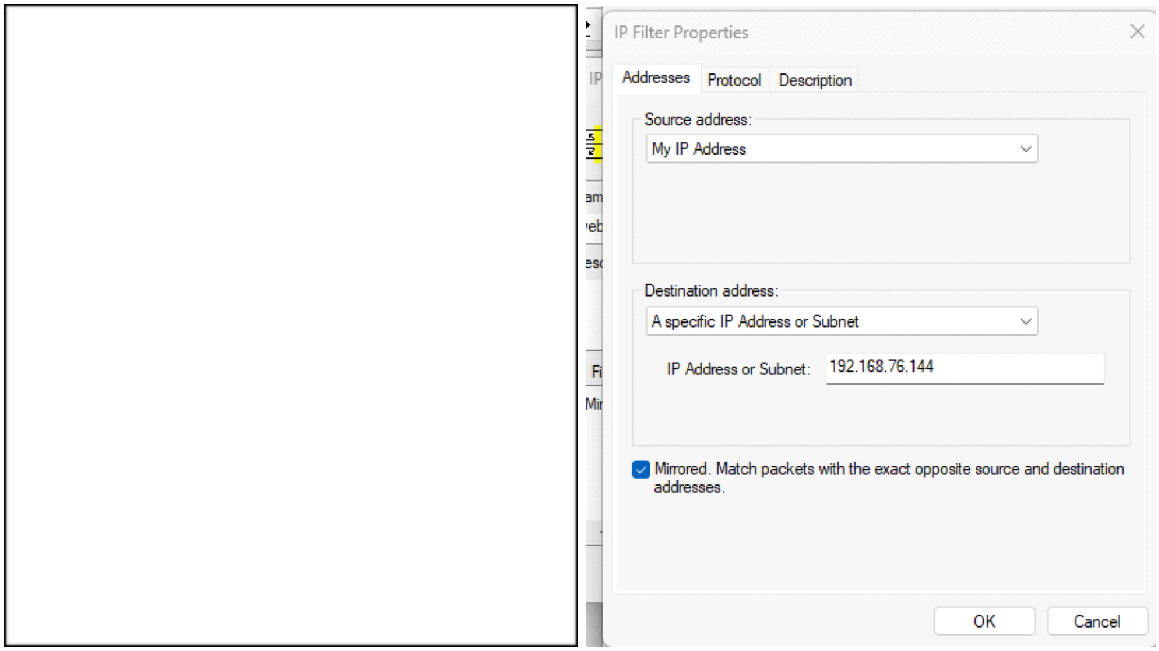
Uncheck -Use add wizard every time.

ADD—New Rule Properties--->Uncheck use add wizard-->Add—ip filter list -->Add

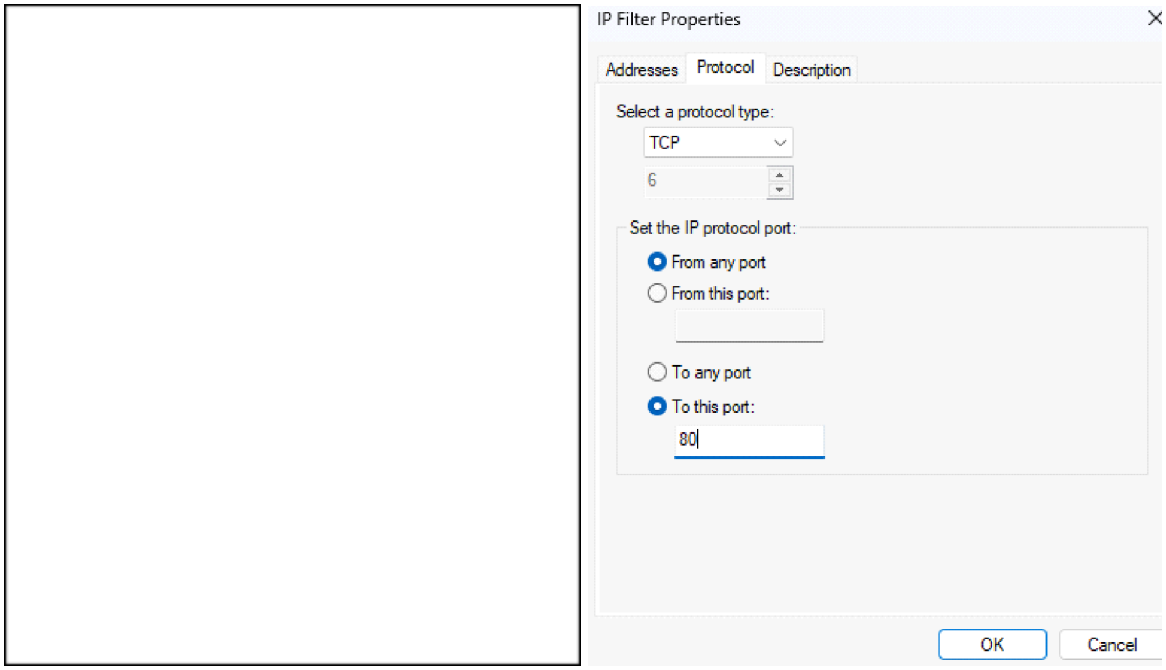


Name-- <> -->uncheck use add wizard --->Add

Address—> Source add -->Destination add



Protocol--> TCP-->From this port 80 -->to any

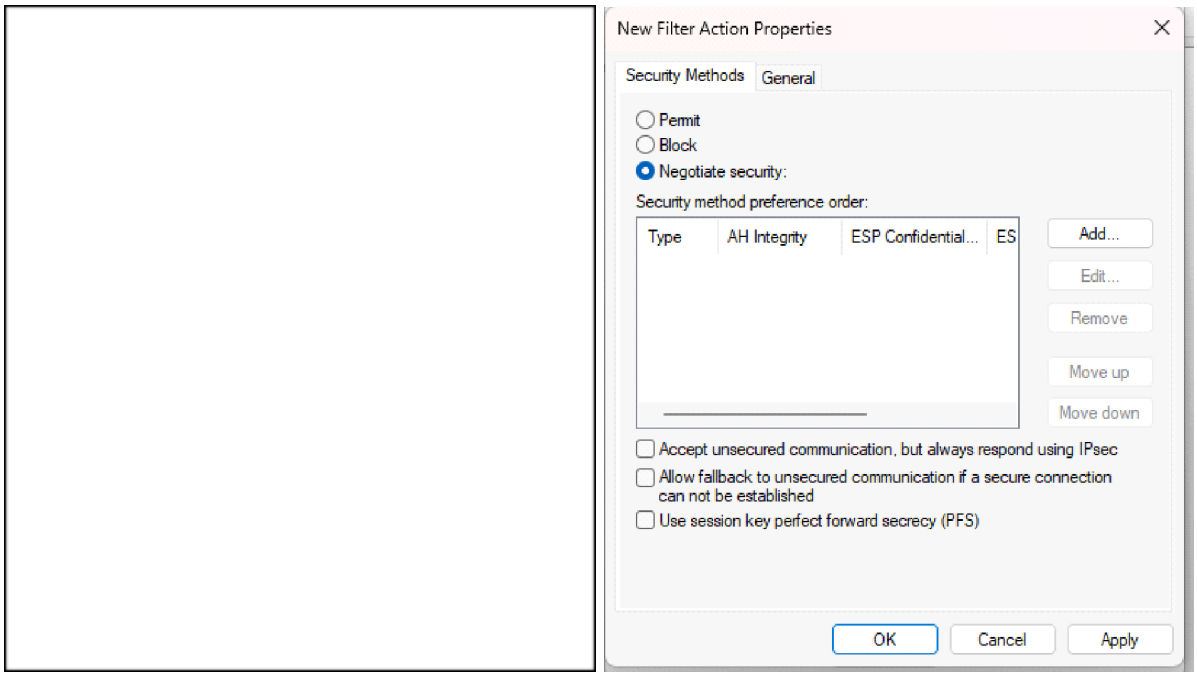


Okay

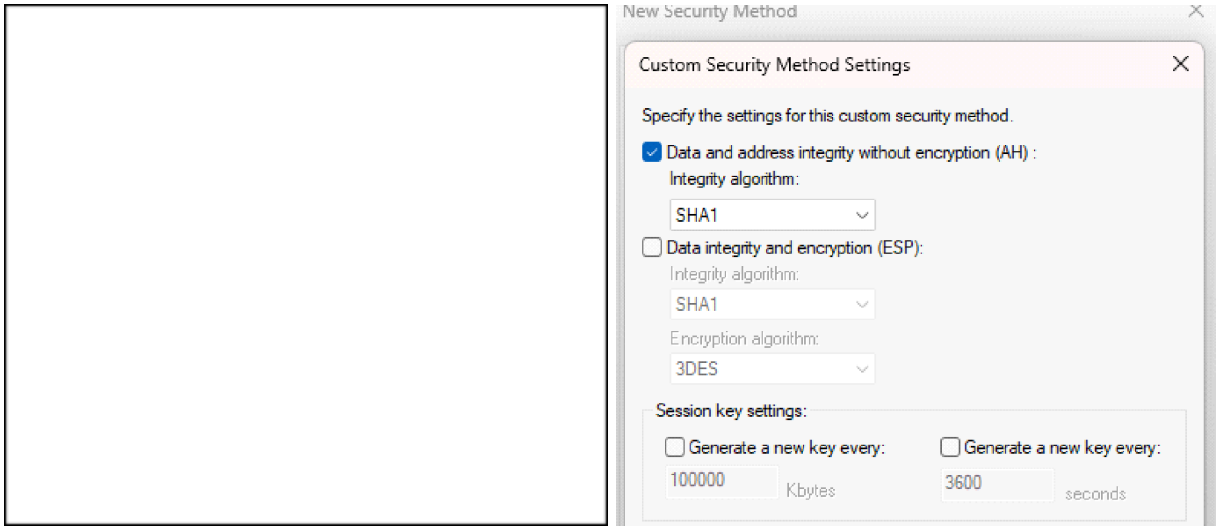
New Rules properties must be selected.

Filter Action: ipsec policies are here.

Negotiate Security--> Add



Security method -->custom -->AH -->SHA1-->ok-->ok



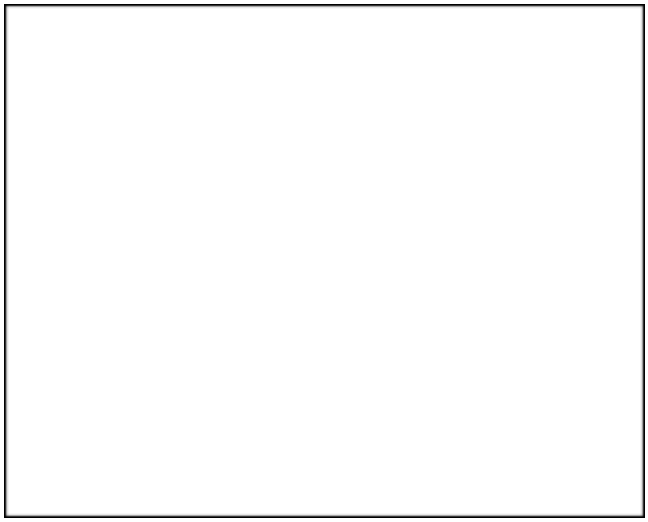
General -->name<>-->apply

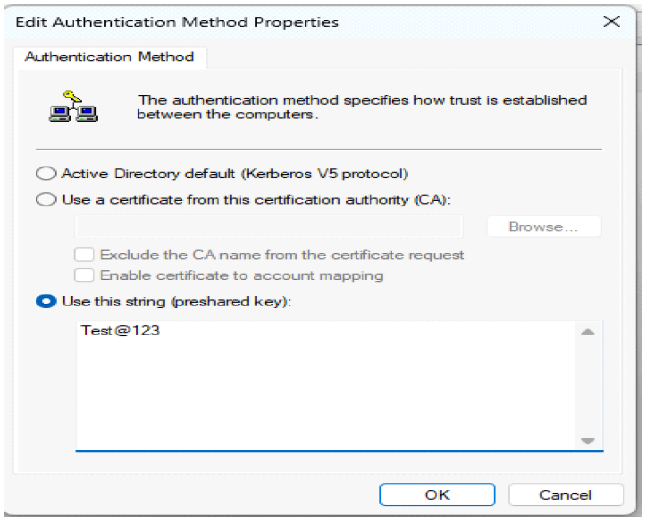
Selected action –ok

Authentication method:

Default -->click-->add

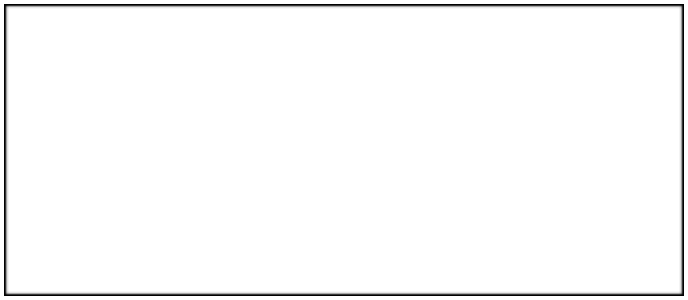
Preshared key---Test@1234-->ok

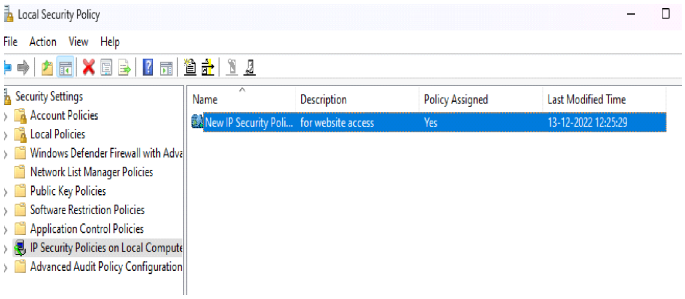




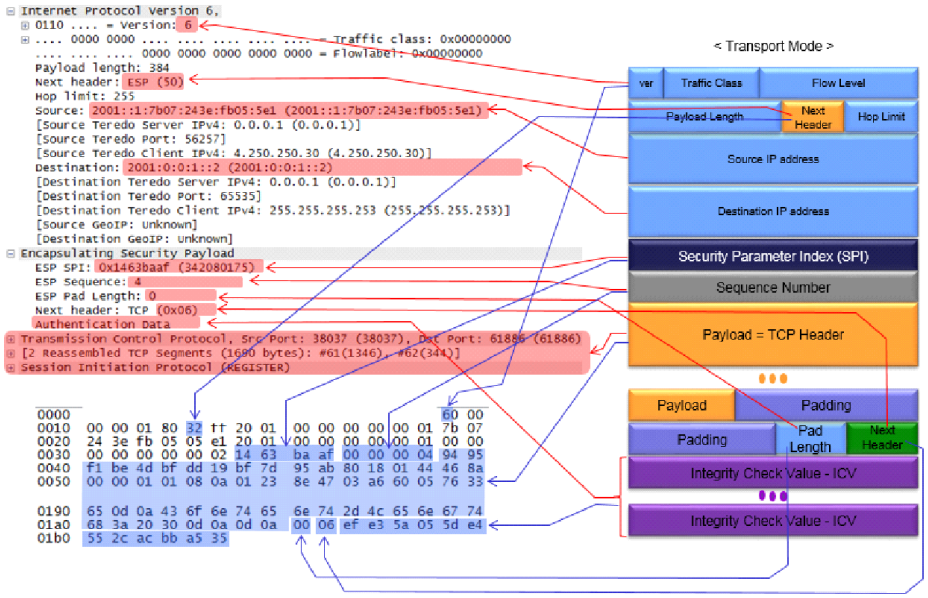
Apply—ok

Right Click-->Assign.

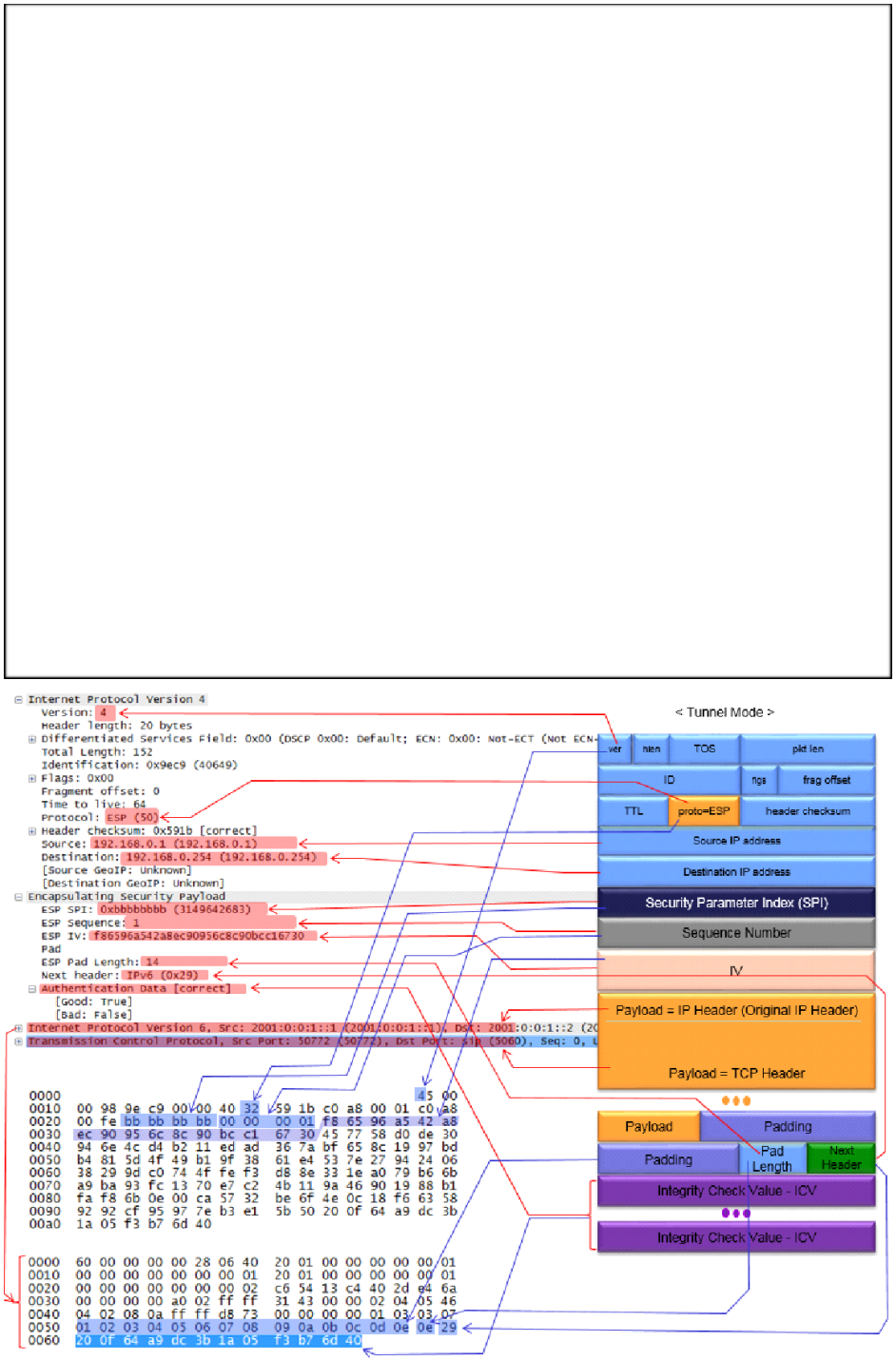




< Transport Mode Example >



< Tunnel Mode Example >


Internet Protocol Version 4
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-
Total Length: 152
Identification: 0x9ec9 (40649)
Flags: 0x00
Fragment offset: 0
Time to live: 64
Protocol: ESP (50)
Header checksum: 0x591b [correct]
Source: 192.168.0.1 (192.168.0.1)
Destination: 192.168.0.254 (192.168.0.254)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Encapsulating Security Payload
ESP SPI: 0xbbbbbbbb (3149642683)
ESP Sequence: 1
ESP IV: f86596a542a8ec90956c8c90bcc16730
Pad
ESP Pad Length: 14
Next header: IPv6 (0x29)
Authentication Data [correct]
[Good: True]
[Bad: False]
Internet Protocol Version 6, Src: 2001:0:0:1::1 (2001:0:0:1::1), Dst: 2001:0:0:1::2 (20
Transmission Control Protocol, Src Port: 50772 (50772), Dst Port: 6118 (5060), Seq: 0, L
0000
0010 00 98 9e c9 00 00 40 32 59 1b c0 a8 00 01 c0 a8
0020 00 fe bb bb bb bb 00 00 00 01 f8 65 96 a5 42 a8
0030 ec 90 95 6c 8c 90 bc c1 67 30 45 77 58 d0 de 30
0040 94 6e 4c d4 b2 11 ed ad 36 7a bf 65 8c 19 97 bd
0050 b4 81 5d 4f 49 b1 9f 38 61 e4 53 7e 27 94 24 06
0060 38 29 9d c0 74 4f fe f3 d8 8e 33 1e a0 79 b6 6b
0070 a9 ba 93 fc 13 70 e7 c2 4b 11 9a 46 90 19 88 b1
0080 fa f8 6b 0e 00 ca 57 32 be 6f 4e 0c 18 f6 63 58
0090 92 92 cf 95 97 7e b3 e1 5b 50 20 0f 64 a9 dc 3b
00a0 1a 05 f3 b7 6d 40
0000 60 00 00 00 00 00 28 06 40 20 01 00 00 00 00 00 01
0010 00 00 00 00 00 00 00 01 20 01 00 00 00 00 00 00 01
0020 00 00 00 00 00 00 00 02 c6 54 13 c4 40 2d e4 6a
0030 00 00 00 00 a0 02 ff ff 31 43 00 00 02 04 05 46
0040 04 02 08 0a ff ff d8 73 00 00 00 00 01 03 03 07
0050 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0e 29
0060 20 0f 64 a9 dc 3b 1a 05 f3 b7 6d 40
< Tunnel Mode >
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=ESP
header checksum
Source IP address
Destination IP address
Security Parameter Index (SPI)
Sequence Number
IV
Payload = IP Header (Original IP Header)
Payload = TCP Header
Payload
Padding
Padding
Pad Length
Next Header
Integrity Check Value - ICV
Integrity Check Value - ICV

==========

Turn Windows features on or off-->

Internet Information Service-->

How the IPSEC do protocols, ESP and AH provides replay protection.

ESP and AH include the sequence number fields in the respective headers. The values are used by the IPSEC peers to track duplicate packets. If a packet with an already received sequence number arrives, it would be rejected, thus providing replay protection.

https://tcpipguru.com/ipsec-interview-questions/

Pfsense--->

VPN--->IPsec-->Tunnels-->ADD

IKE Endpoint Configuration--> Remote Gateway (Public ip of other office)

Encryption Algorithm -->

Etc.

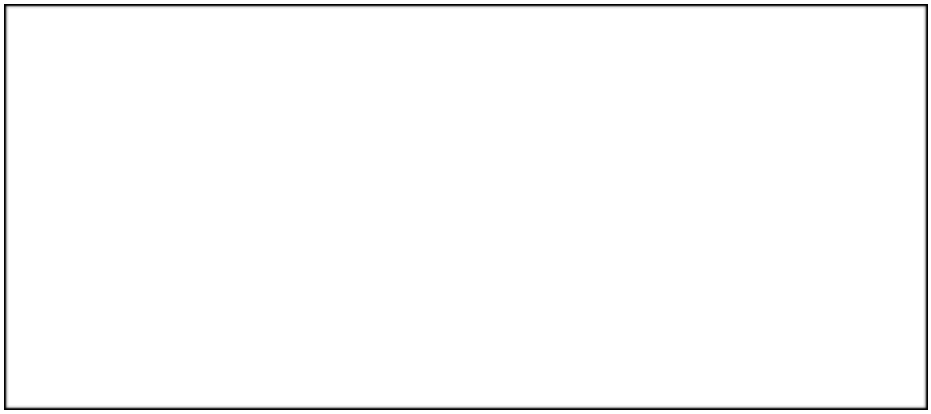
Kind a same of **secpol.msc**

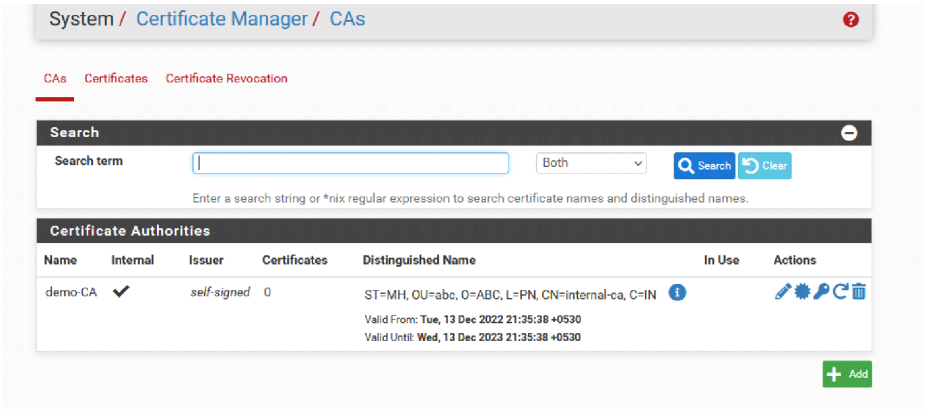
Dial-up vpn-- openVPN

SSL/TLS works in transport layer.

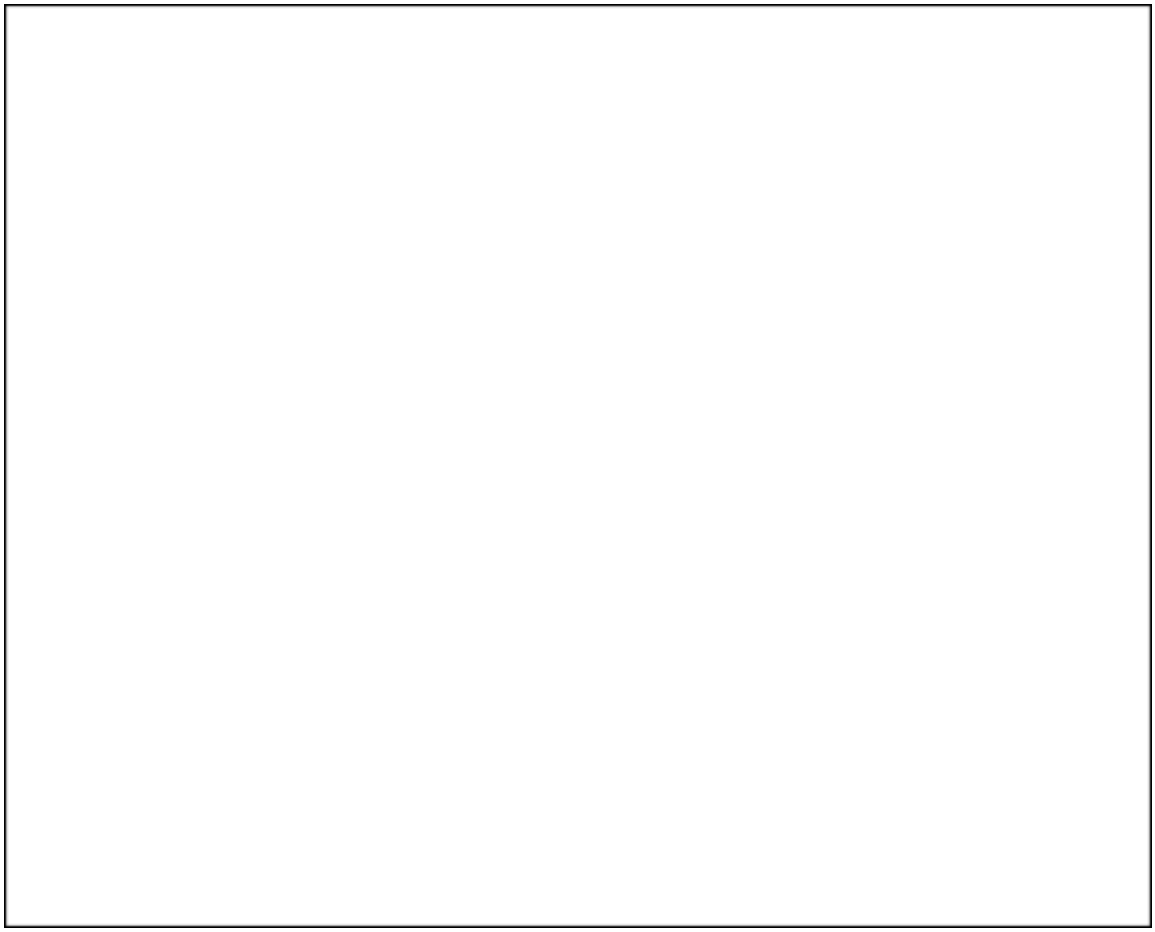
Need certificate servers

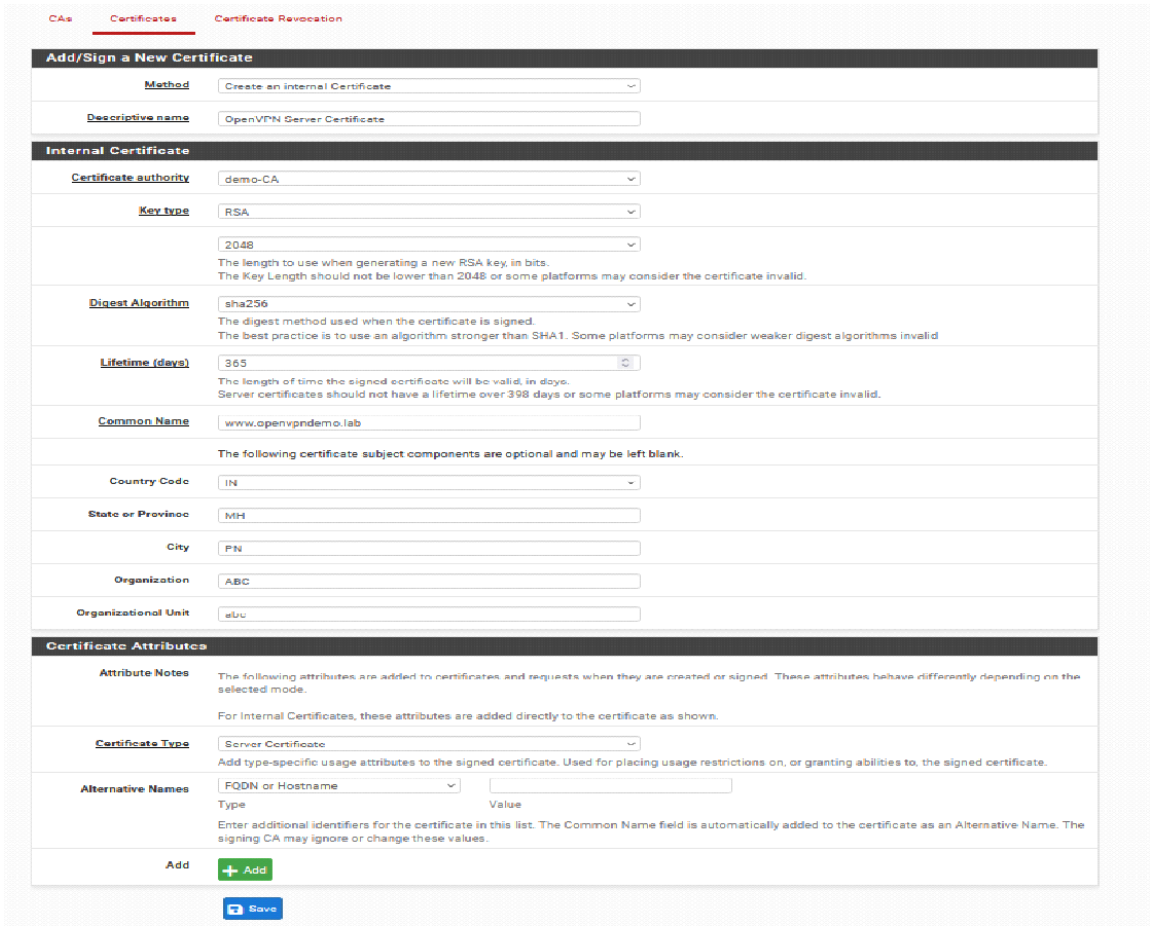
- System-->Certificate Manager-->CAs

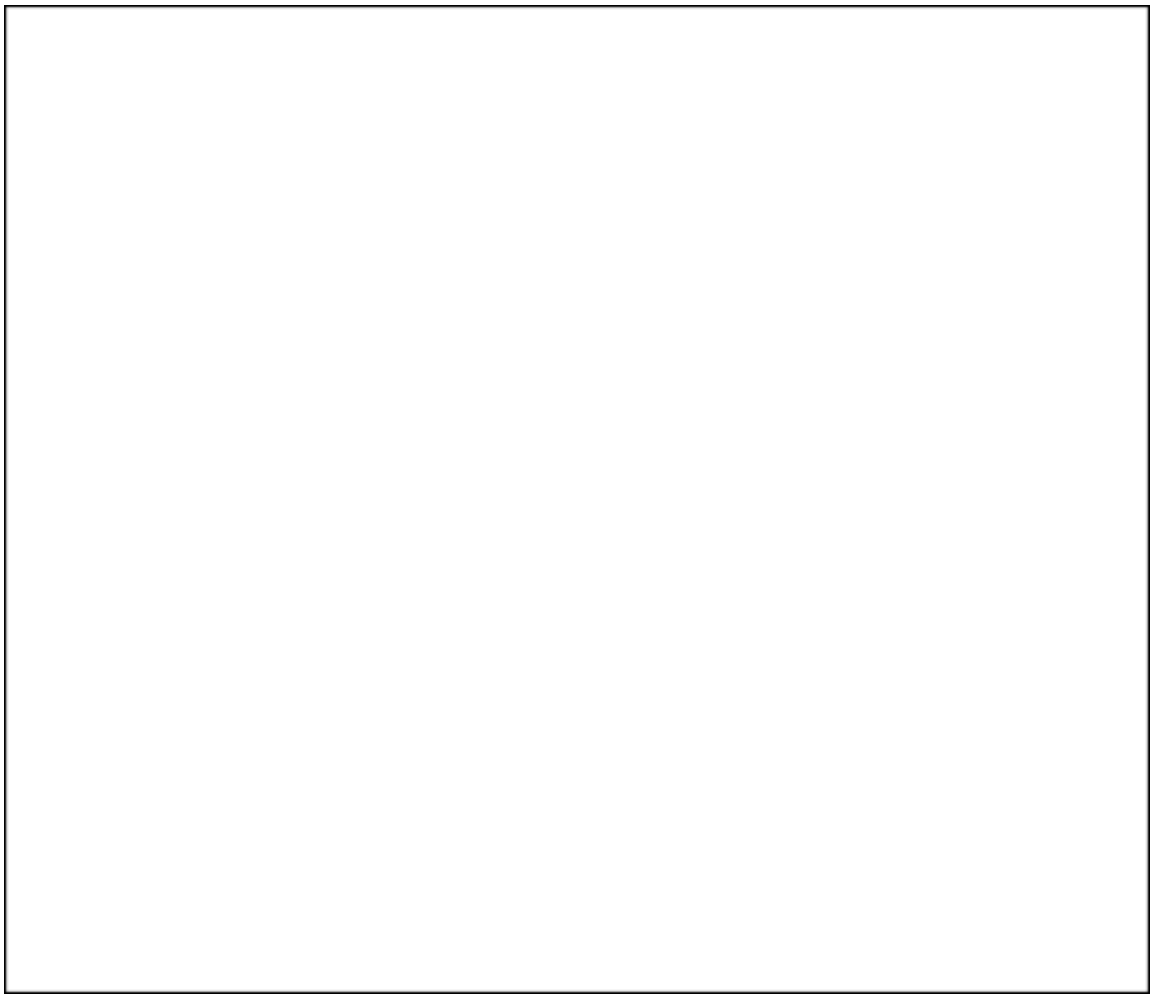


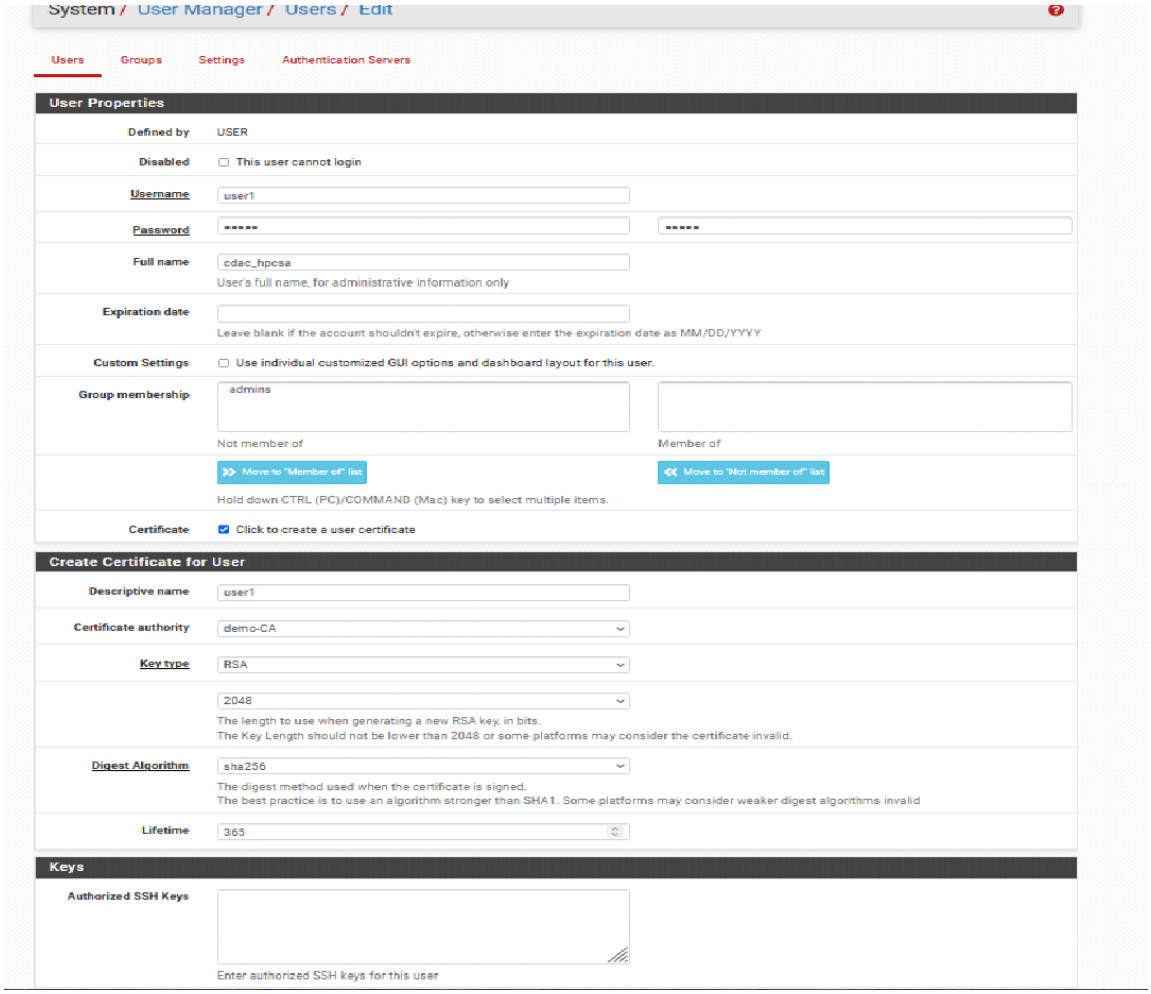


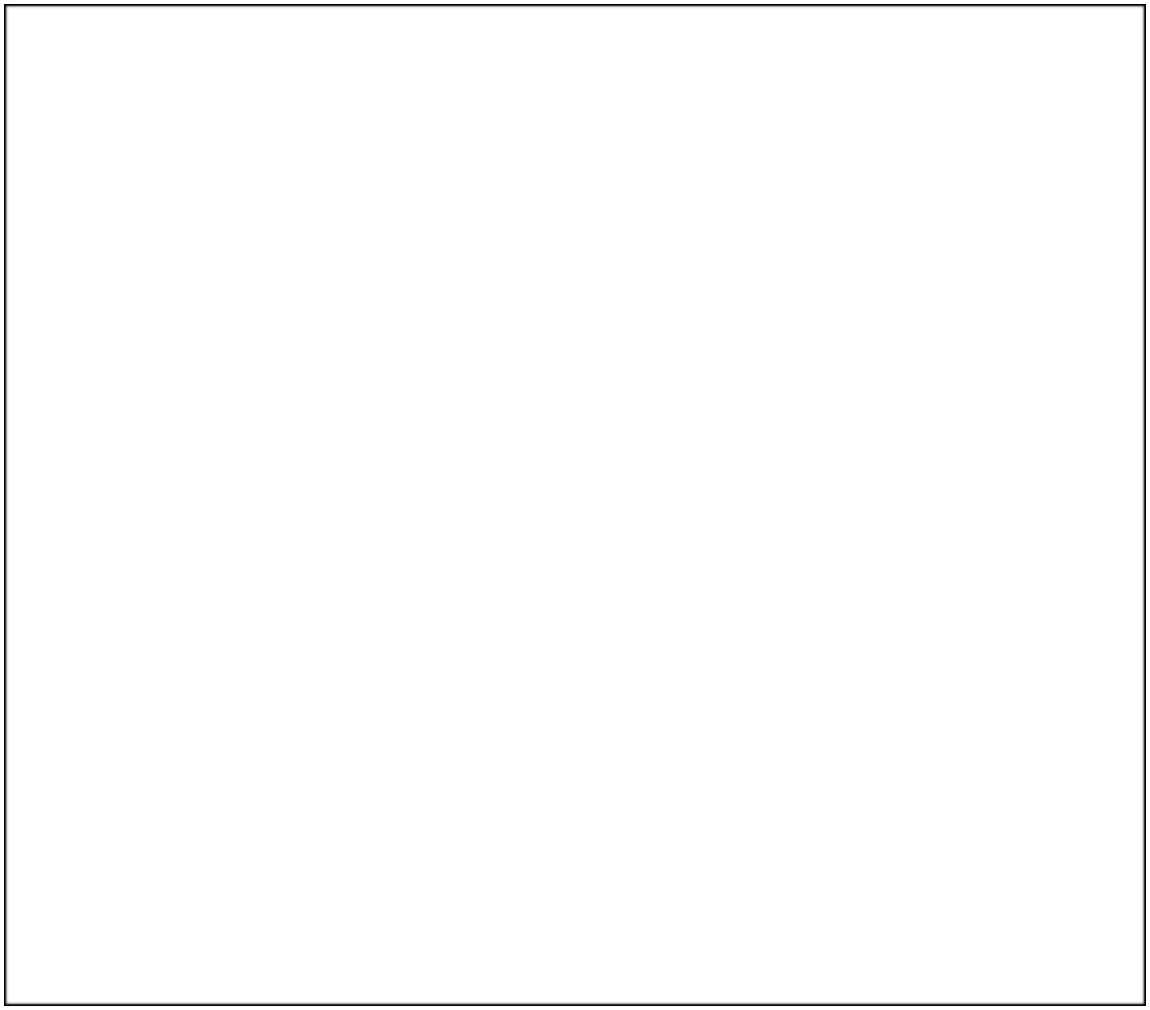
1.System-->Certificate Manager-->Certificates-->Edit

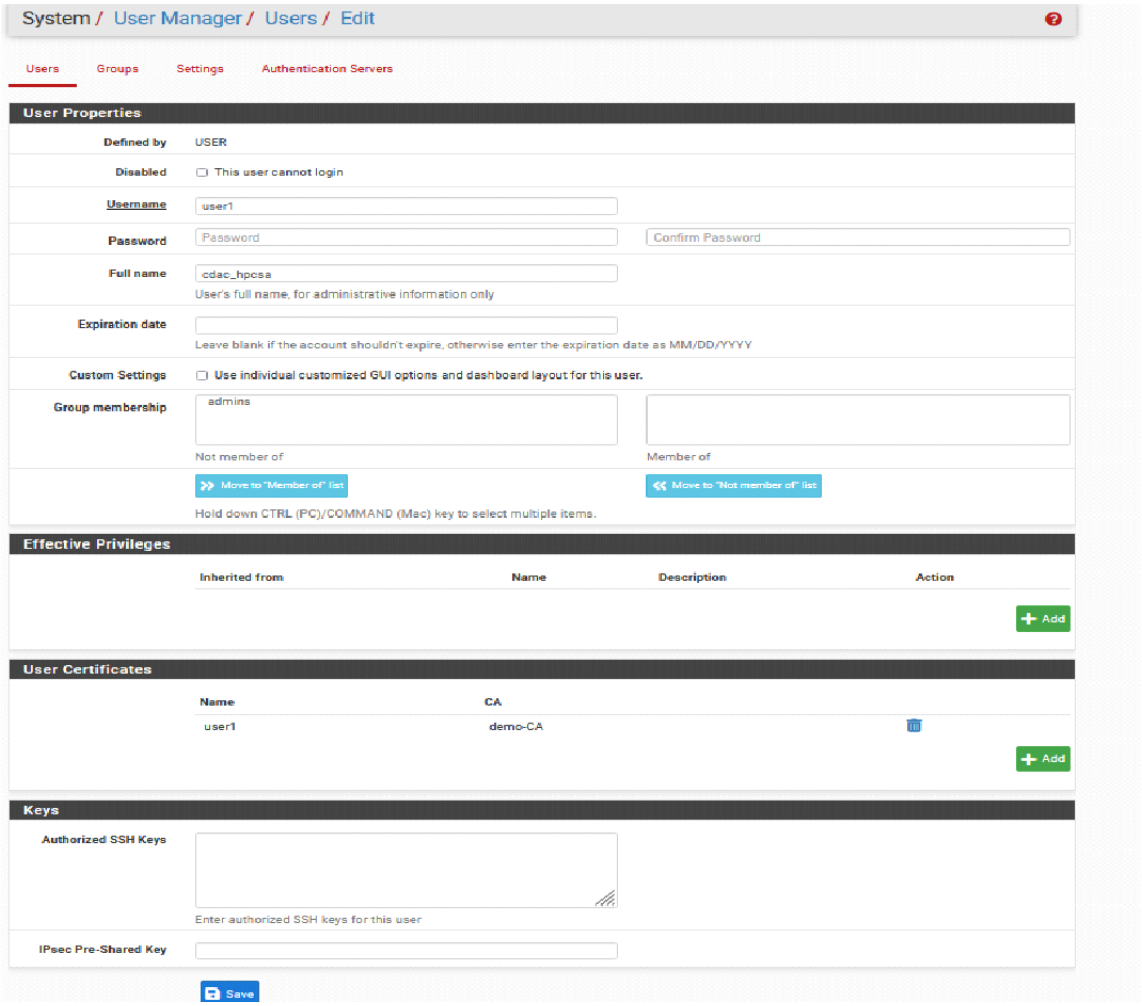



CAs
Certificates
Certificate Revocation
Add/Sign a New Certificate
Method
Create an internal Certificate
Descriptive name
OpenVPN Server Certificate
Internal Certificate
Certificate authority
demo-CA
Key type
RSA
2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm
sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime (days)
365
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Common Name
www.openvpndemo.lab
The following certificate subject components are optional and may be left blank.
Country Code
IN
State or Province
MH
City
PN
Organization
ABC
Organizational Unit
eDu
Certificate Attributes
Attribute Notes
The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.
Certificate Type
Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.
Alternative Names
FQDN or Hostname
Type
Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.
Add
Add
Save



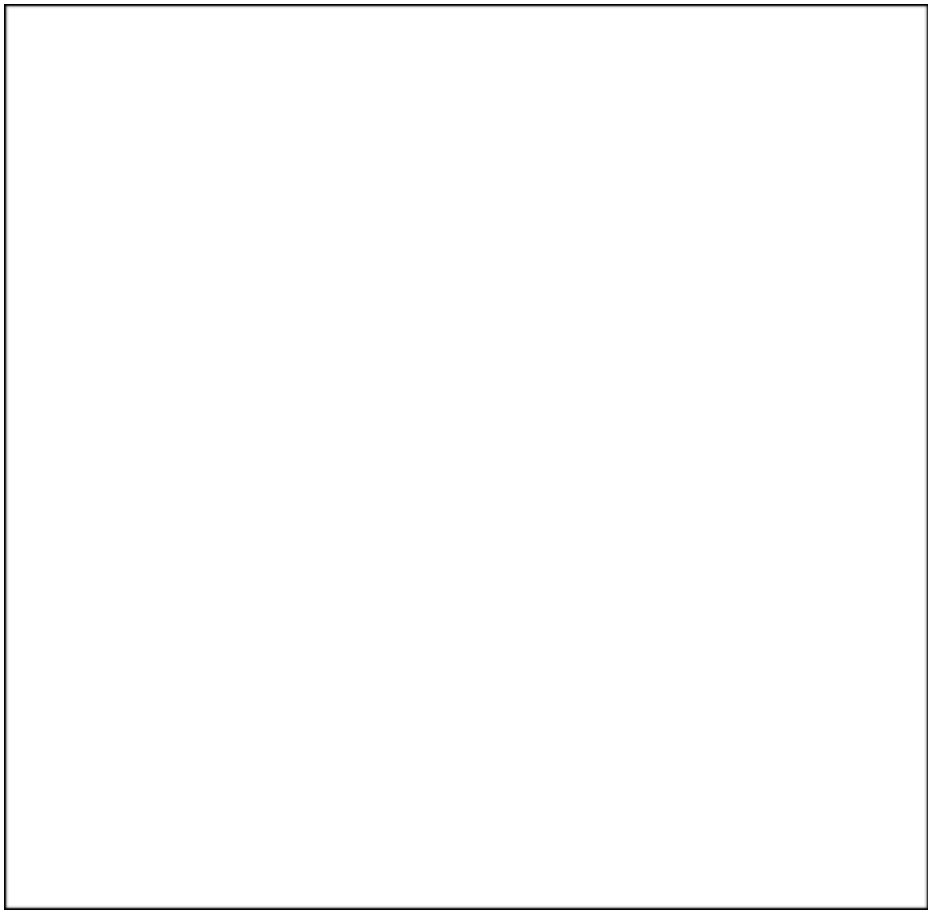

System / User Manager / Users / Edit
Users
Groups
Settings
Authentication Servers
User Properties
Defined by
USER
Disabled
This user cannot login
Username
user1
Password
Full name
cdac_hpcsa
User's full name, for administrative information only
Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings
Use individual customized GUI options and dashboard layout for this user.
Group membership
admins
Not member of
Member of
Move to "Member of" list
Move to "Not member of" list
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Certificate
Click to create a user certificate
Create Certificate for User
Descriptive name
user1
Certificate authority
demo-CA
Key type
RSA
2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm
sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime
365
Keys
Authorized SSH Keys
Enter authorized SSH keys for this user

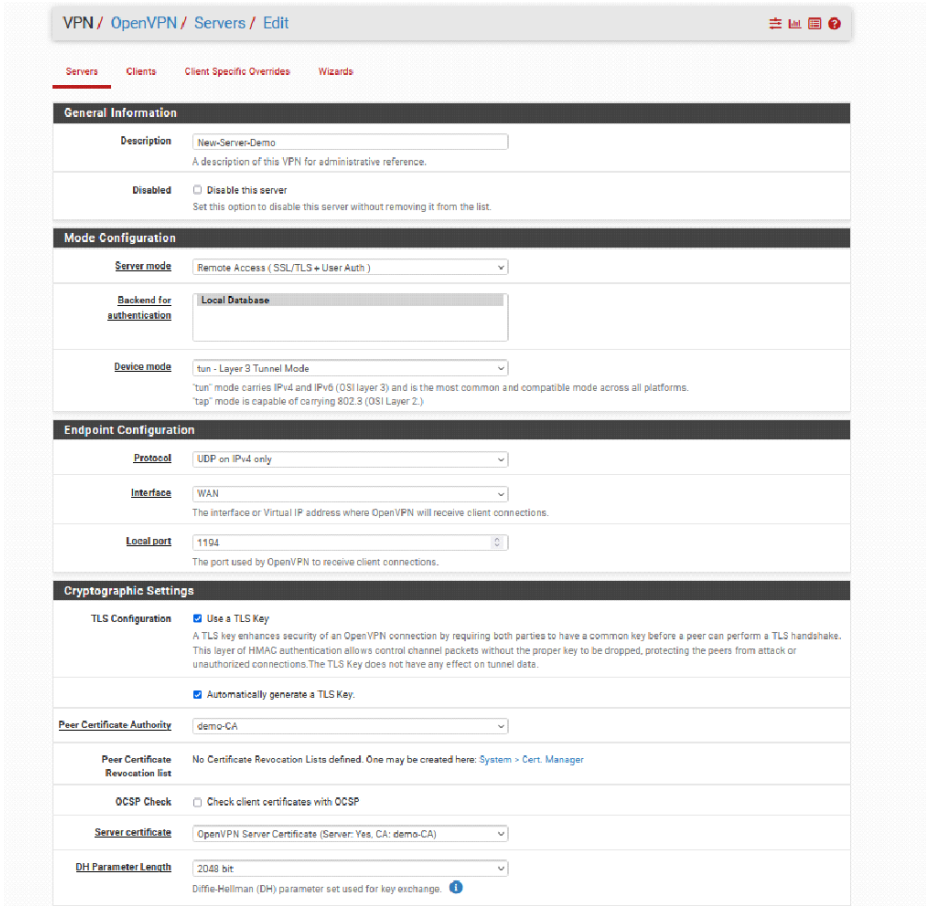


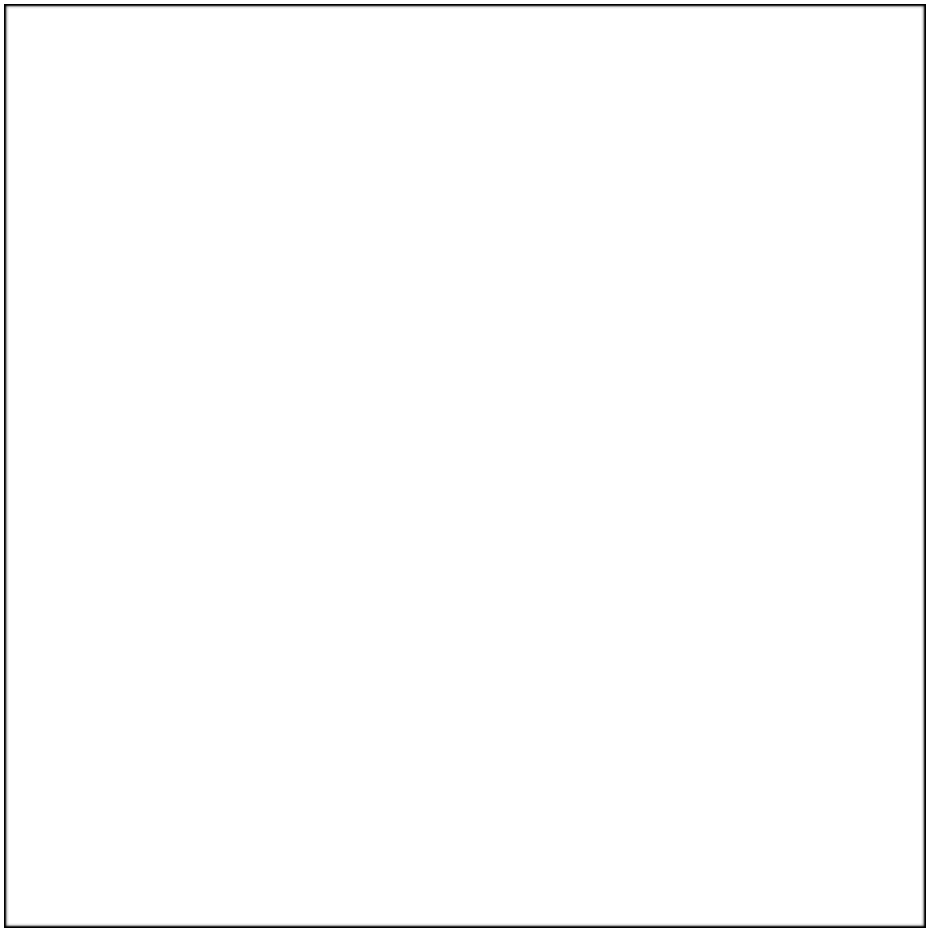


Now you can configure OpenVPN for SERVER

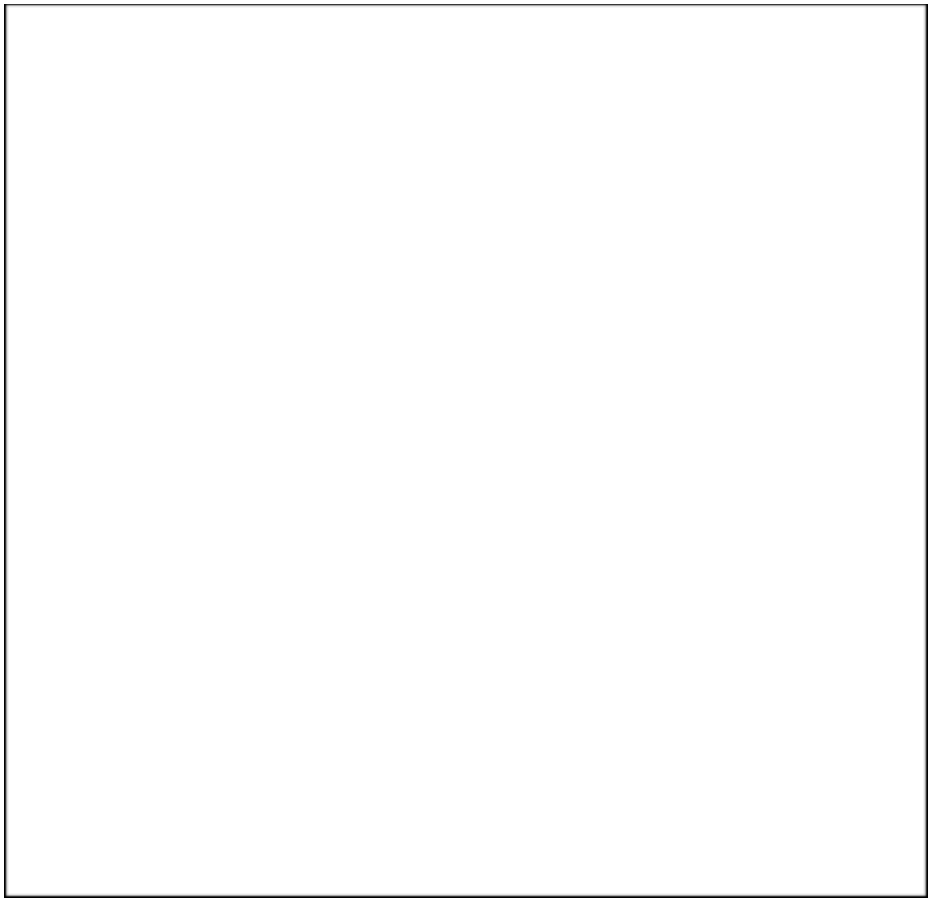
Redirect IPv4 Gateway—used in corporate network




VPN / OpenVPN / Servers / Edit
Servers
Clients
Client Specific Overrides
Wizards
General Information
Description
New-Server-Demo
A description of this VPN for administrative reference.
Disabled
Disable this server
Set this option to disable this server without removing it from the list.
Mode Configuration
Server mode
Remote Access (SSL/TLS + User Auth)
Backend for authentication
Local Database
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration
Protocol
UDP on IPv4 only
Interface
WAN
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port
1194
The port used by OpenVPN to receive client connections.
Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.
Automatically generate a TLS Key.
Peer Certificate Authority
demo-CA
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check
Check client certificates with OCSP
Server certificate
OpenVPN Server Certificate (Server: Yes, CA: demo-CA)
DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.




Server certificate
OpenVPN Server Certificate (Server: Yes, CA: demo-CA)
DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.
ECDH Curve
Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Negotiation
Enable Data Encryption Negotiation
This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.
Data Encryption Algorithms
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
Available Data Encryption Algorithms
Click to add or remove an algorithm from the list
Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.
Fallback Data Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
Auth digest algorithm
SHA256 (256-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
Hardware Crypto
No Hardware Crypto Acceleration
Certificate Depth
One (Client+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
Strict User-CN Matching
Enforce match
When authenticating users, enforce a match between the common name of the client certificate and the username given at login.
Client Certificate Key Usage Validation
Enforce key usage
Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").
Tunnel Settings
IPv4 Tunnel Network
192.168.10.0/24
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway
Force all client-generated IPv6 traffic through the tunnel.



IPv4 Local network(s)

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections

10

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression

Refuse any non-stub compression (Most secure)

Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Push Compression

☐ Push the selected Compression setting to connecting clients.

Type-of-Service

☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication

☐ Allow communication between clients connected to this server

Duplicate Connection

☐ Allow multiple concurrent connections from the same user

When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Client Settings

Dynamic IP

☐ Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet -- One IP address per client in a common subnet

Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Ping settings

Inactive

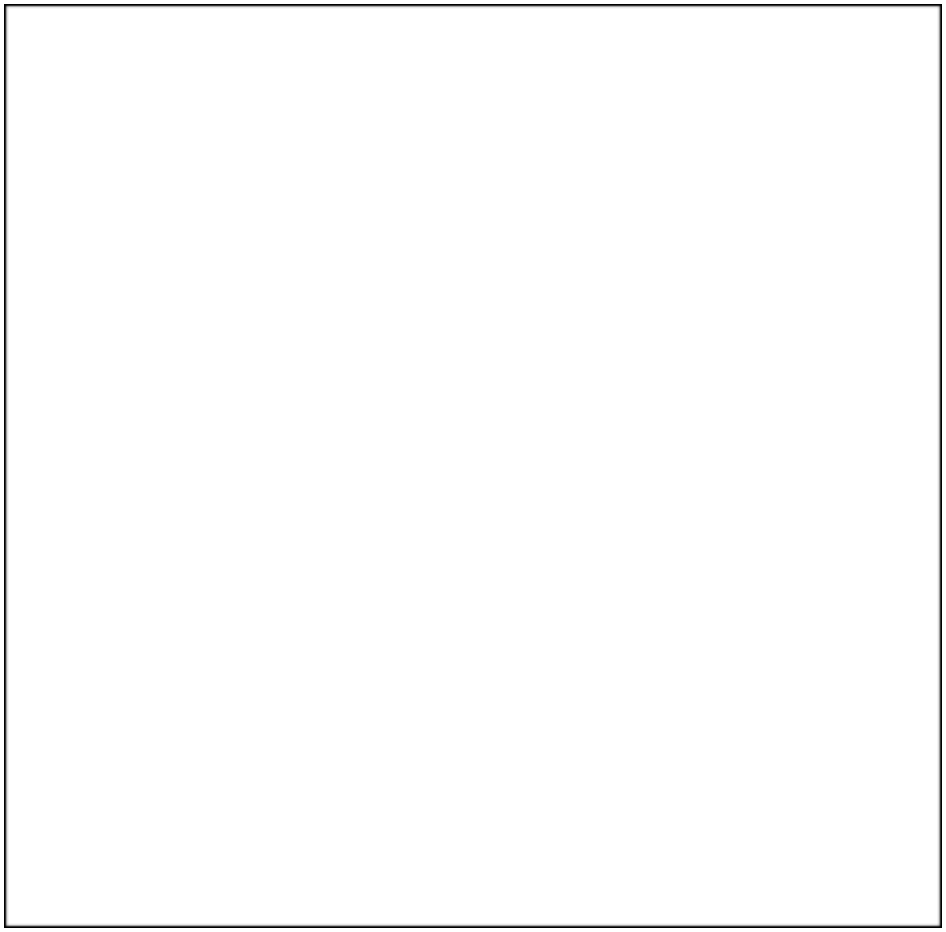
300

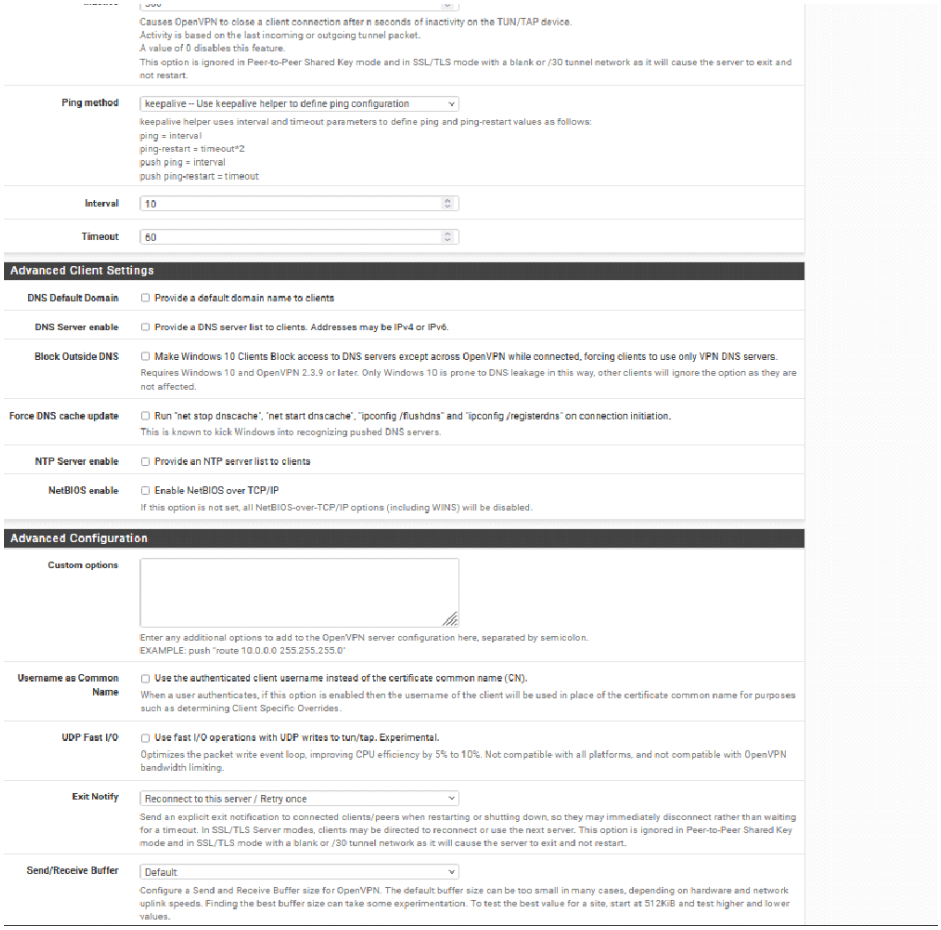
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet.
A value of 0 disables this feature.
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Ping method

keepalive -- Use keepalive helper to define ping configuration

keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
ping = interval
ping-restart = timeout*2
push ping = interval
push ping-restart = timeout

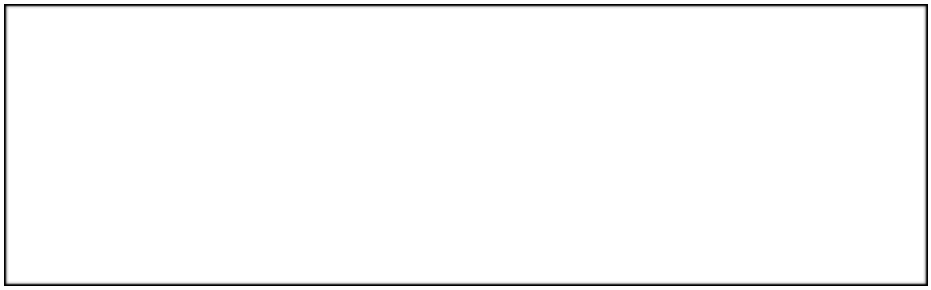


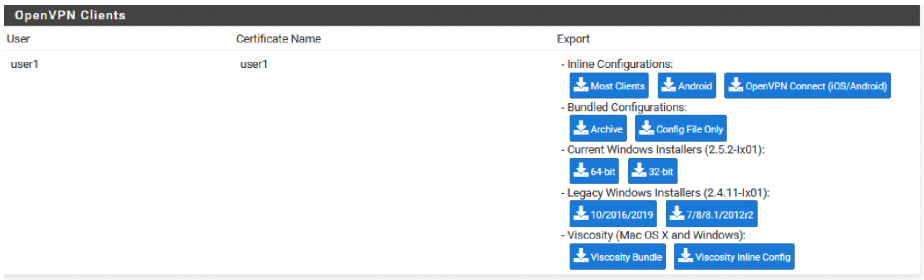


Now you can configure OpenVPN for user

System-->Package Manager-->Package Installer---> openvpn-client-export

VPN-->OpenVPN--->Client Export-->Save as Default



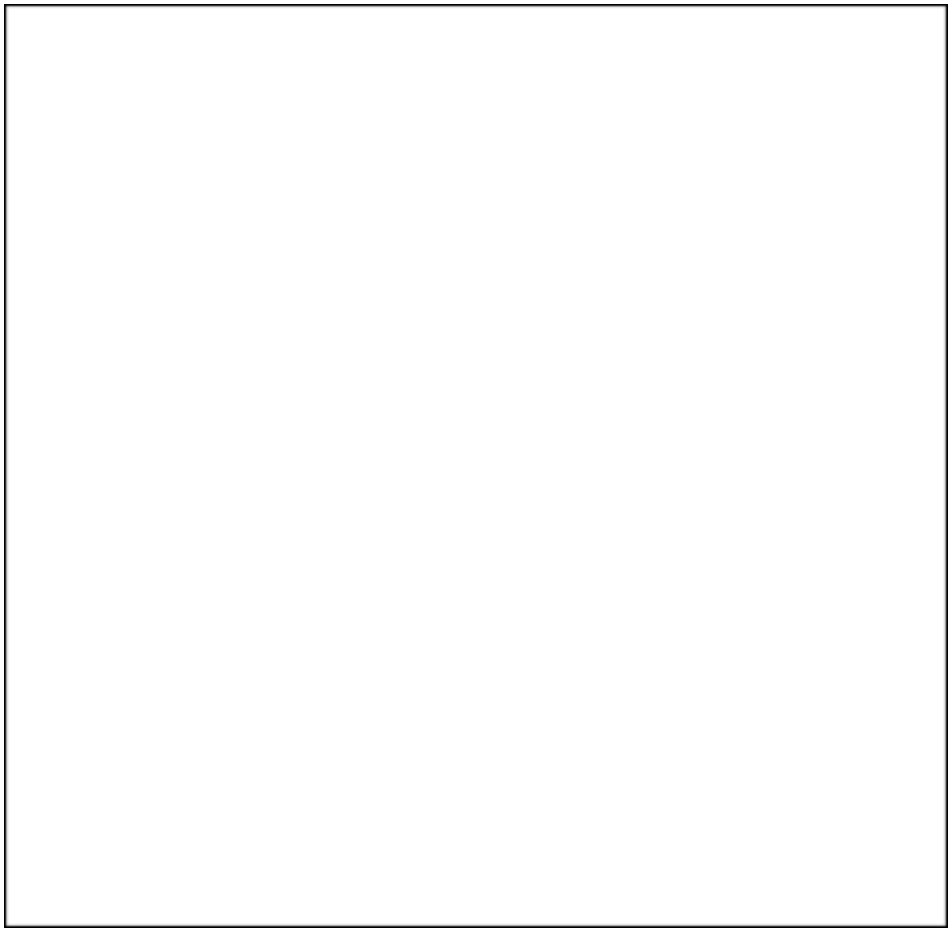


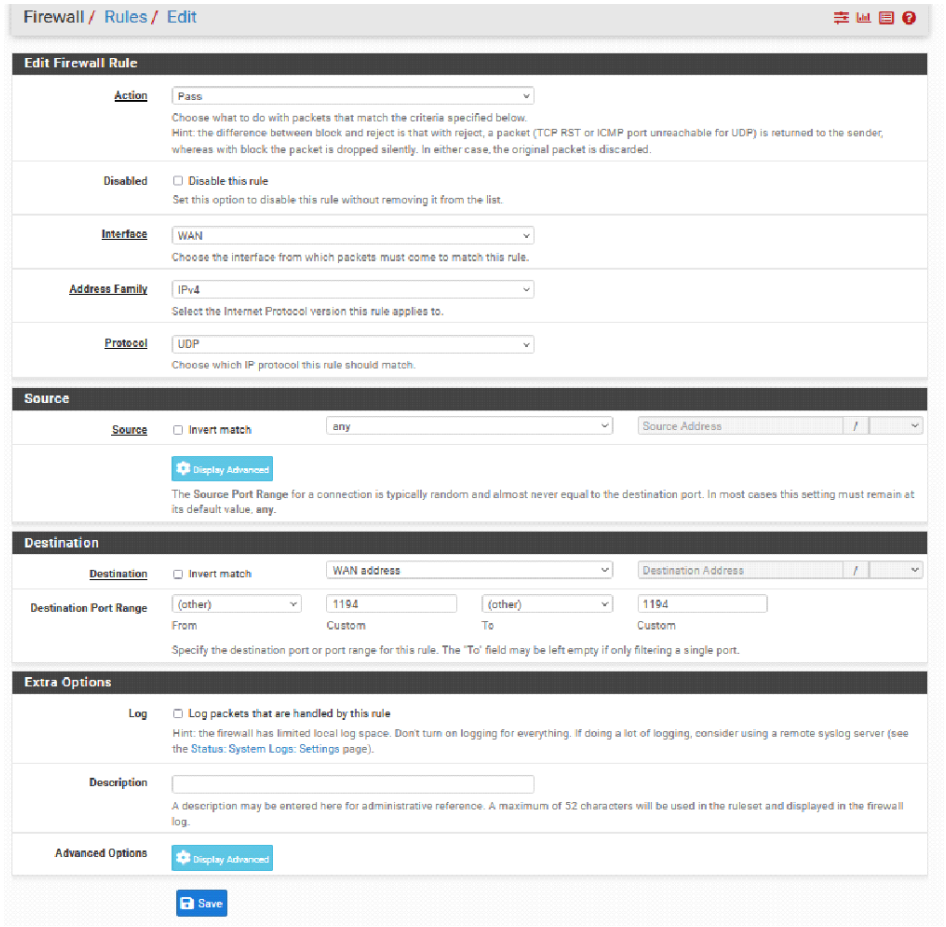
Install Current Windows 64 bit

Install the .exe file

Make rule:

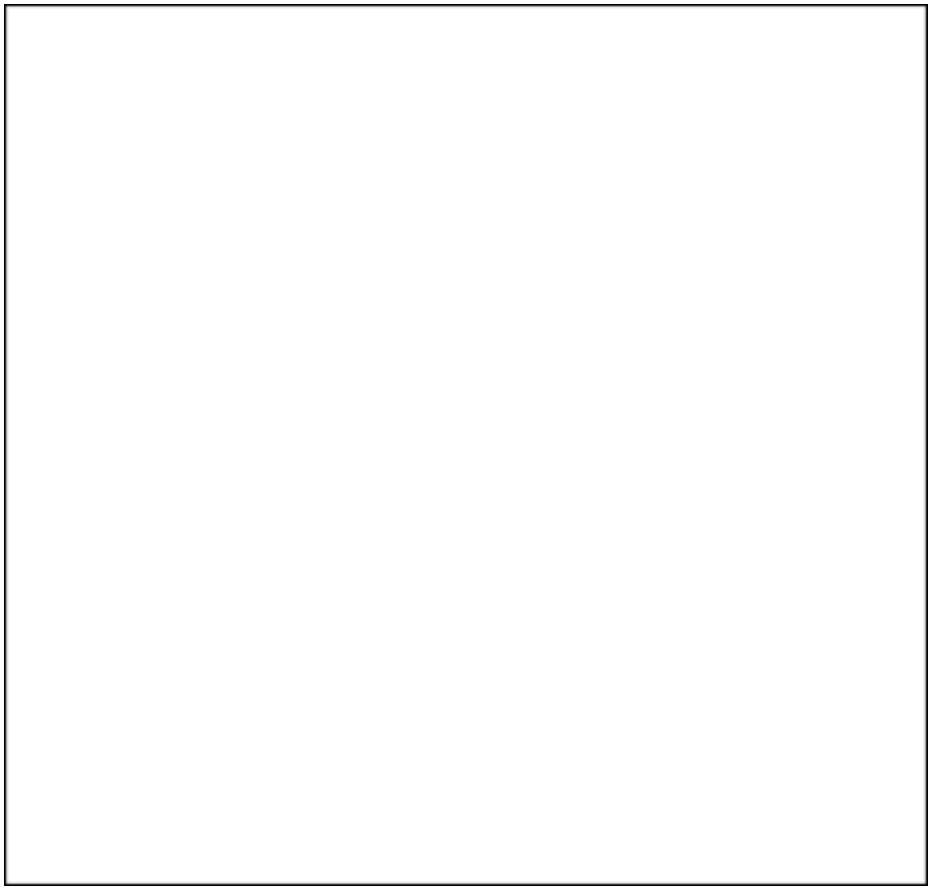
Pfsense-->Rules-->add

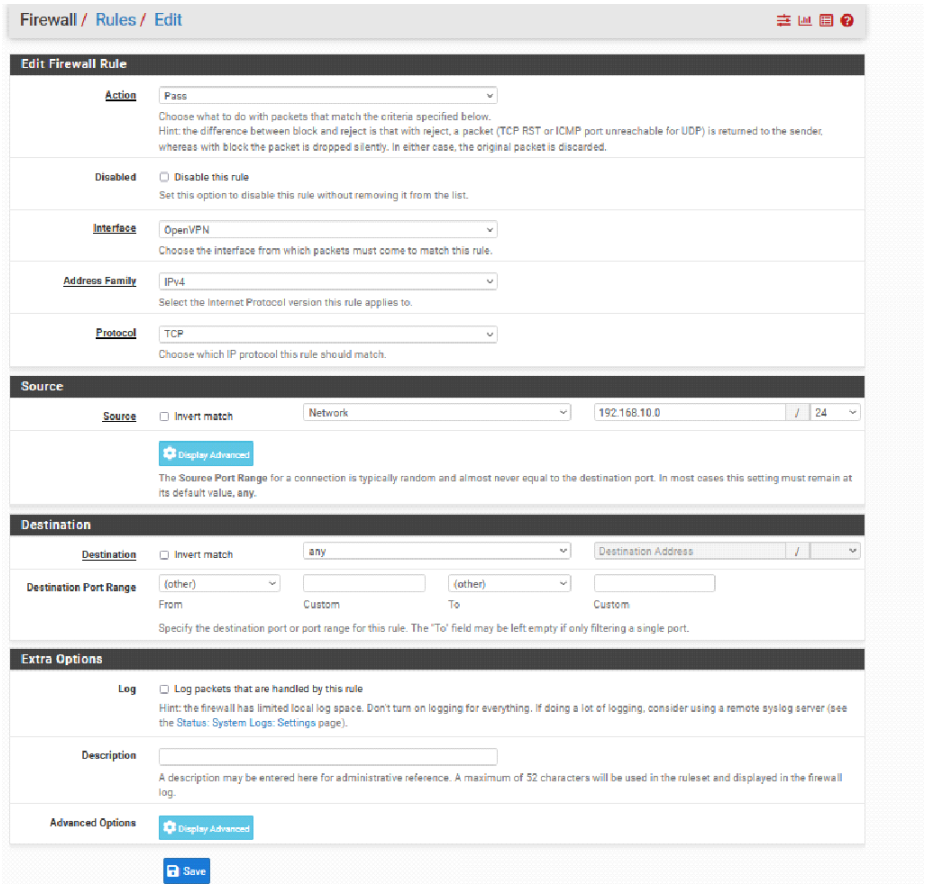




SAVE--->Apply Changes

Now OpenVPN---->Add





SAVE--->Apply Changes

Sum-up: Redirect Gateway used in VPN to make a secure network.