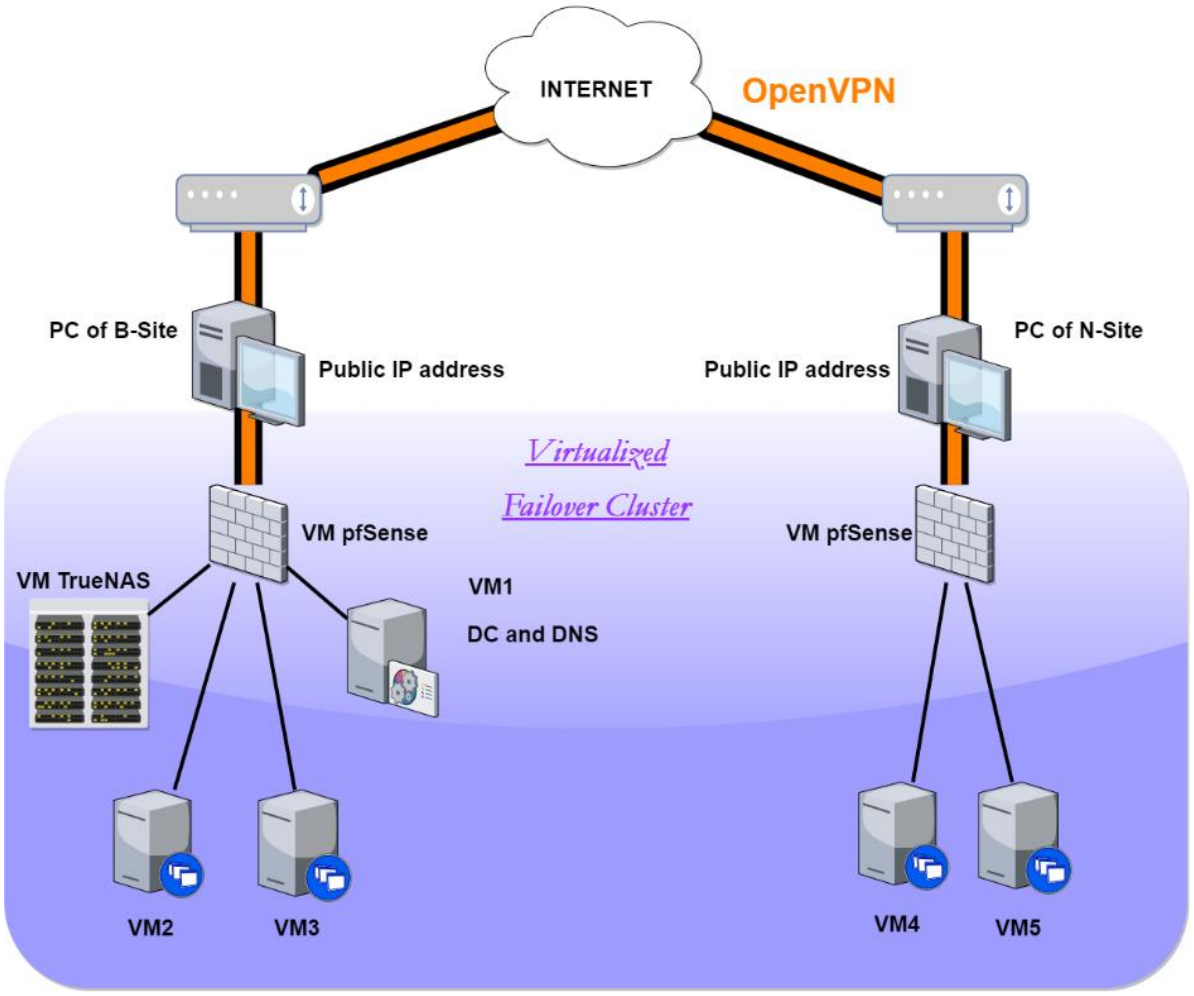
VIRTUAL FAILOVER CLUSTER PROTECTED BY OPENVPN BASED ON WMWARE WORKSTATION

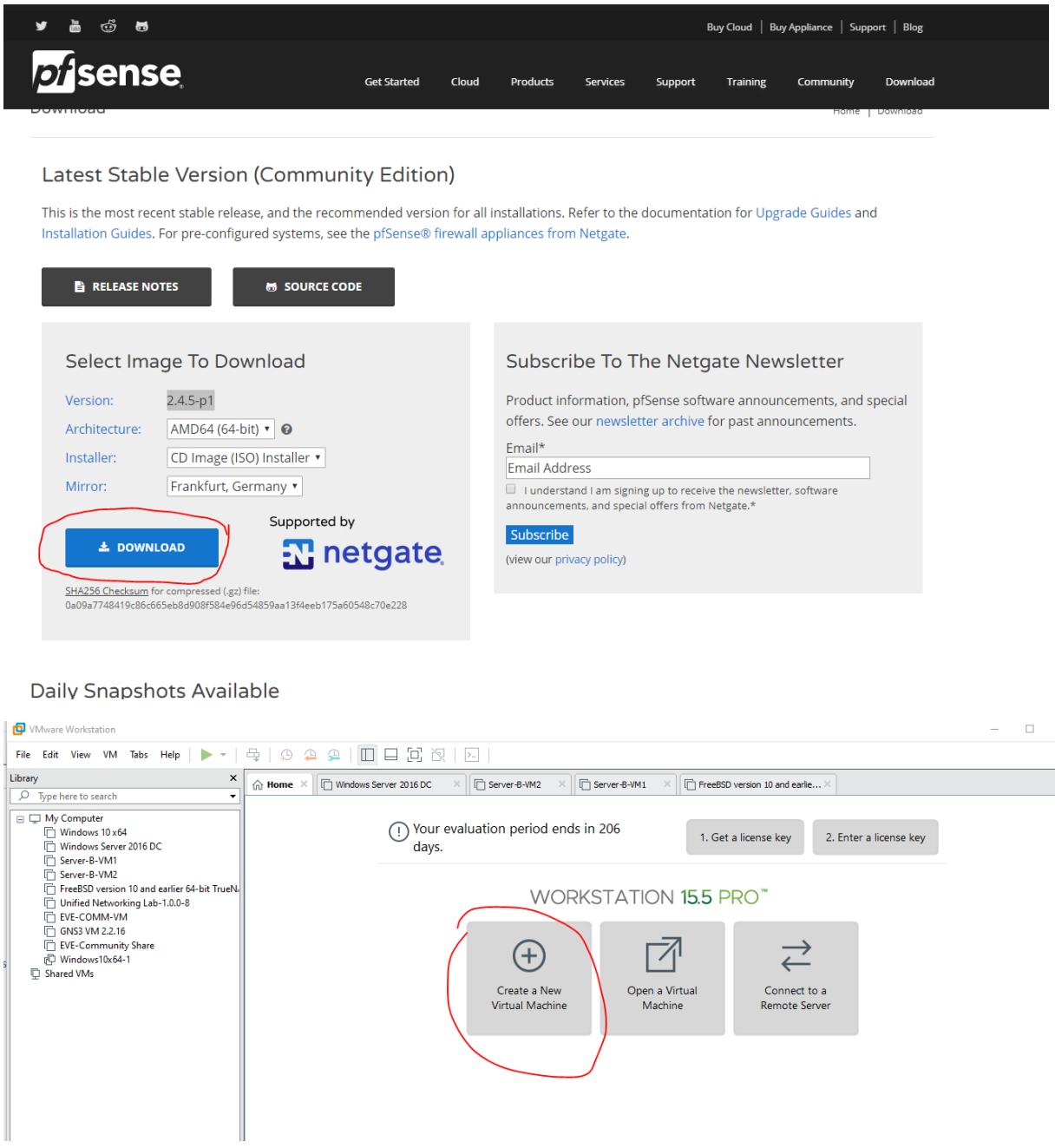


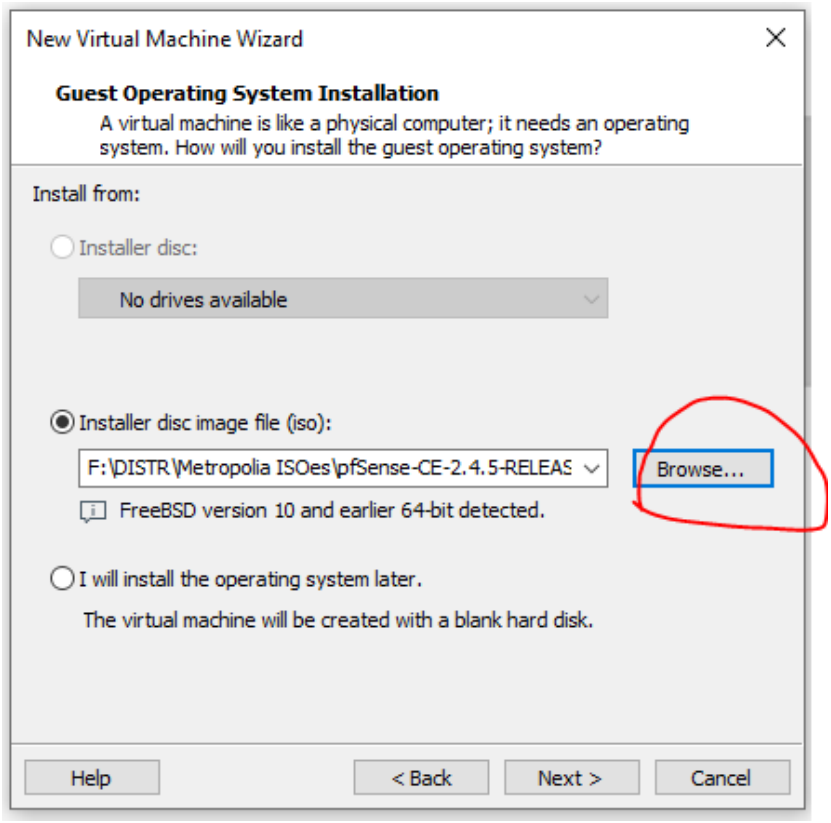
The important note. Before starting, the port forwarding must be applied on the home routers, in such a way that the public IP address from ISP will be forwarded through the home network to the PC itself. This is needed to let Pfsense VM deploy a VPN connection.

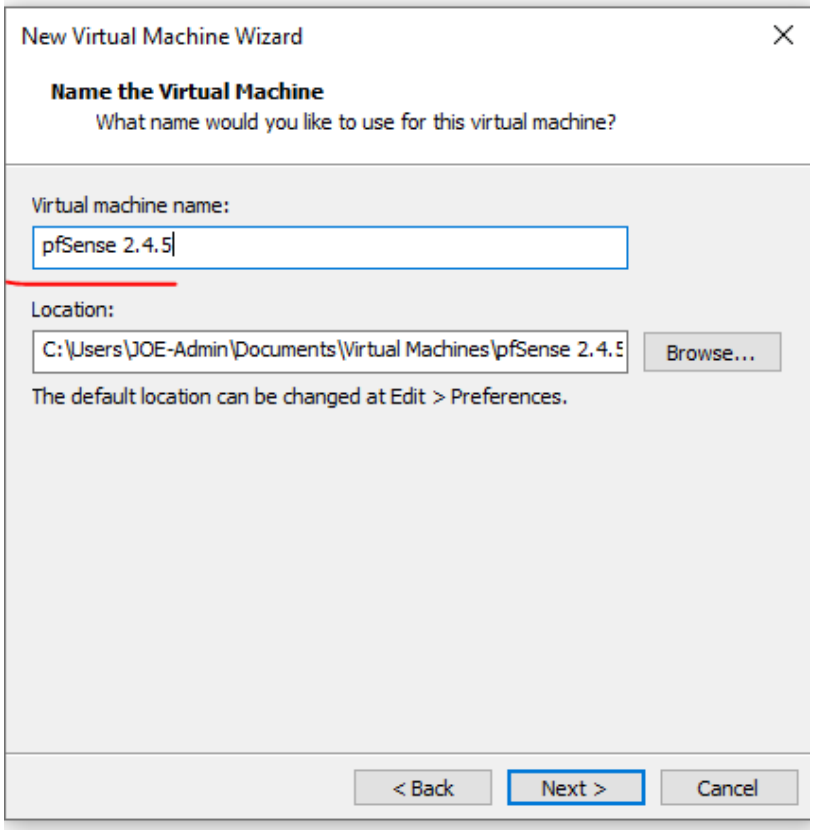
Vmware

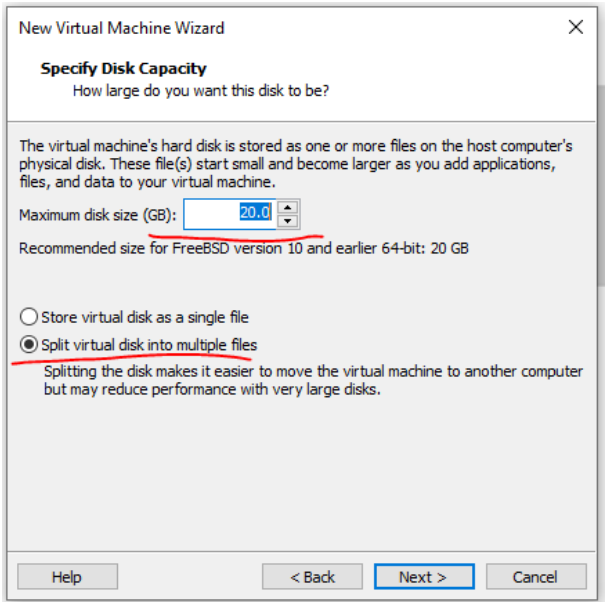
Configuration B site

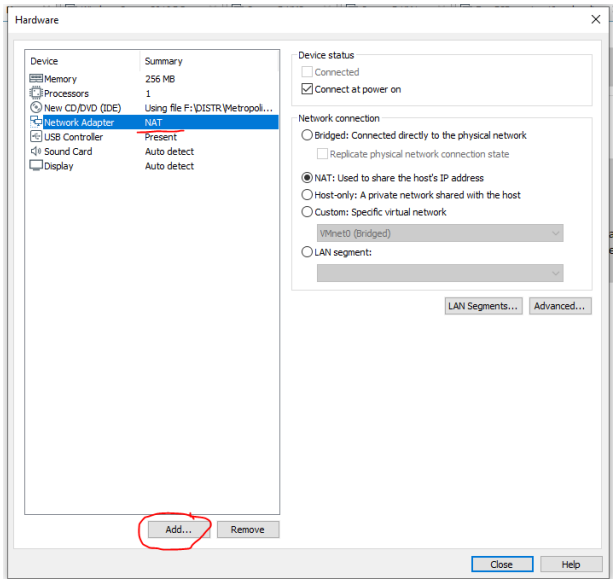
Installing pfSense as a VM

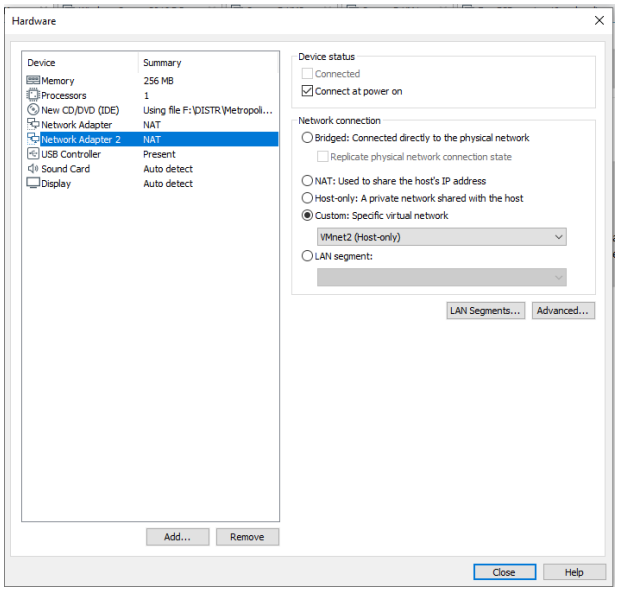


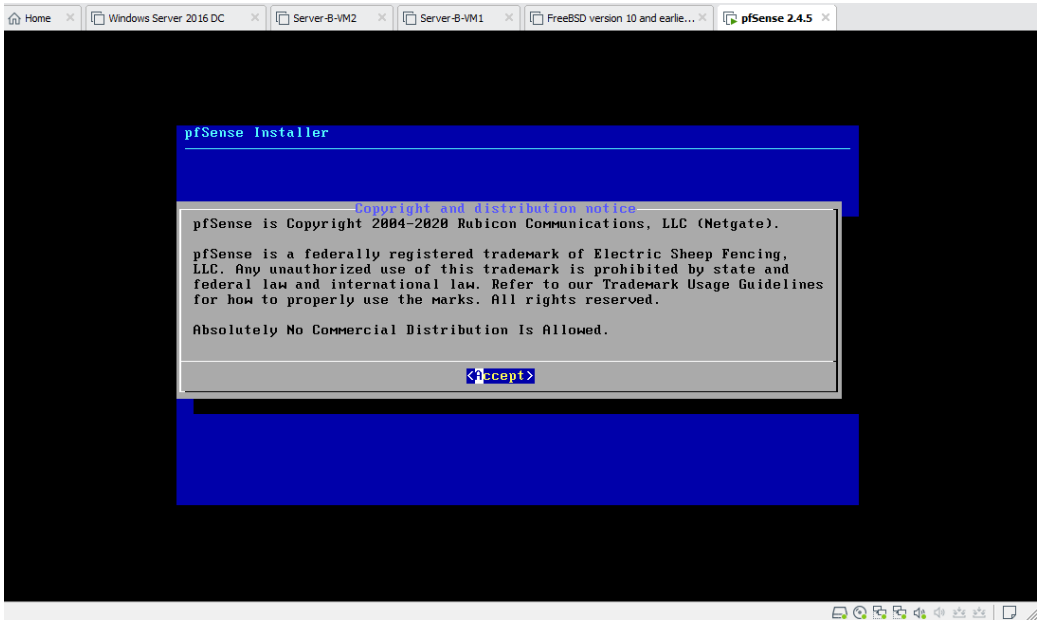

New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
No drives available
Installer disc image file (iso):
F:\DISTR\Metropolia ISOes\pfSense-CE-2.4.5-RELEAS
Browse...
FreeBSD version 10 and earlier 64-bit detected.
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel

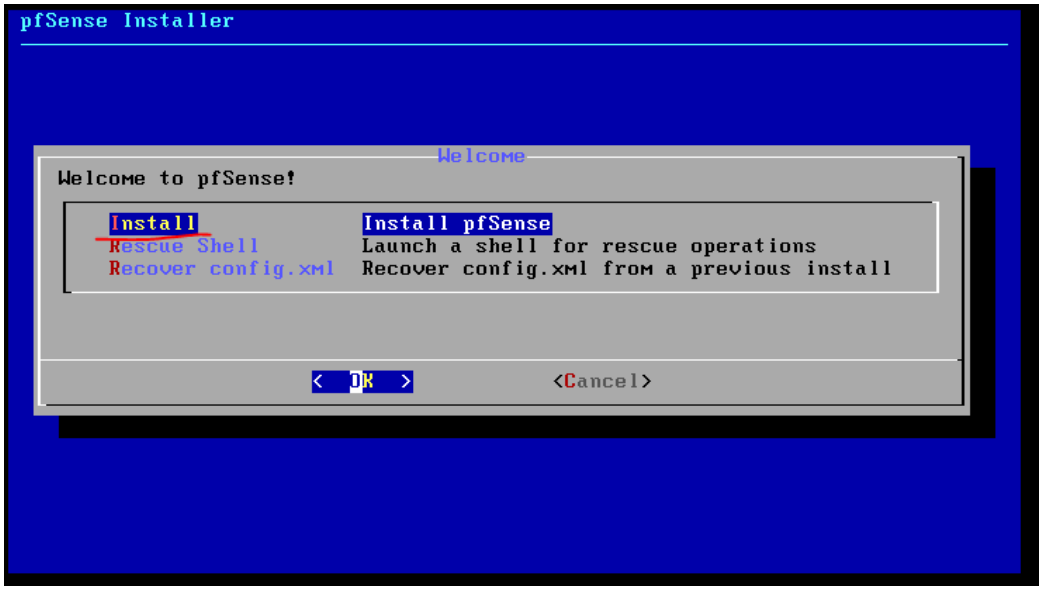

New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
pfSense 2.4.5
Location:
C:\Users\JOE-Admin\Documents\Virtual Machines\pfSense 2.4.5
Browse...
The default location can be changed at Edit > Preferences.
< Back
Next >
Cancel

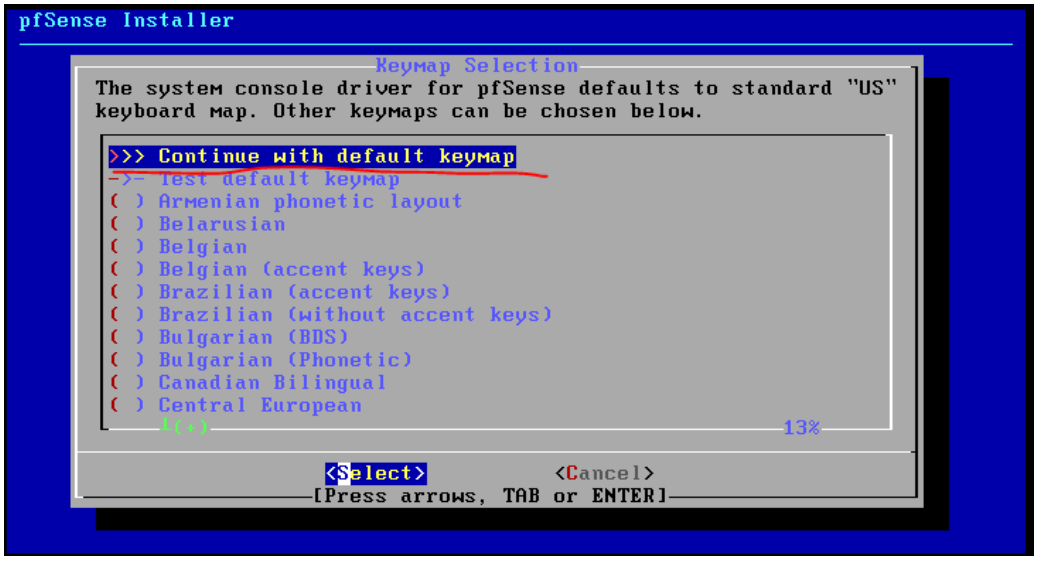

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB): 20.0
Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel

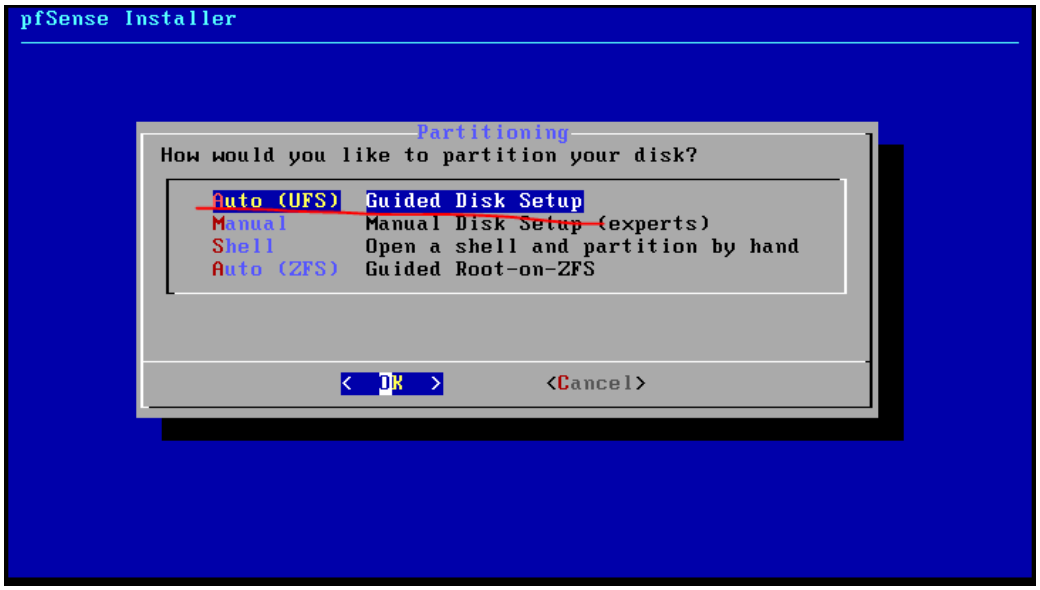

Hardware
Device
Summary
Memory
256 MB
Processors
1
New CD/DVD (IDE)
Using file F:\DISTR\Metropoli...
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0 (Bridged)
LAN segment:
LAN Segments...
Advanced...
Add...
Remove
Close
Help

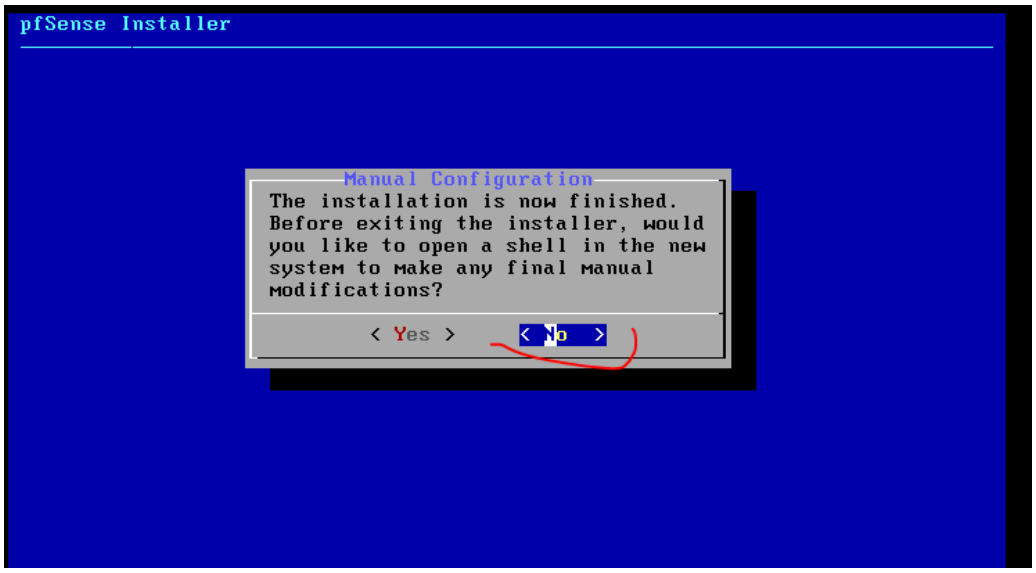

Hardware
Device
Summary
Memory
256 MB
Processors
1
New CD/DVD (IDE)
Using file F:\DISTR\Metropoli...
Network Adapter
NAT
Network Adapter 2
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet2 (Host-only)
LAN segment:
LAN Segments...
Advanced...
Add...
Remove
Close
Help

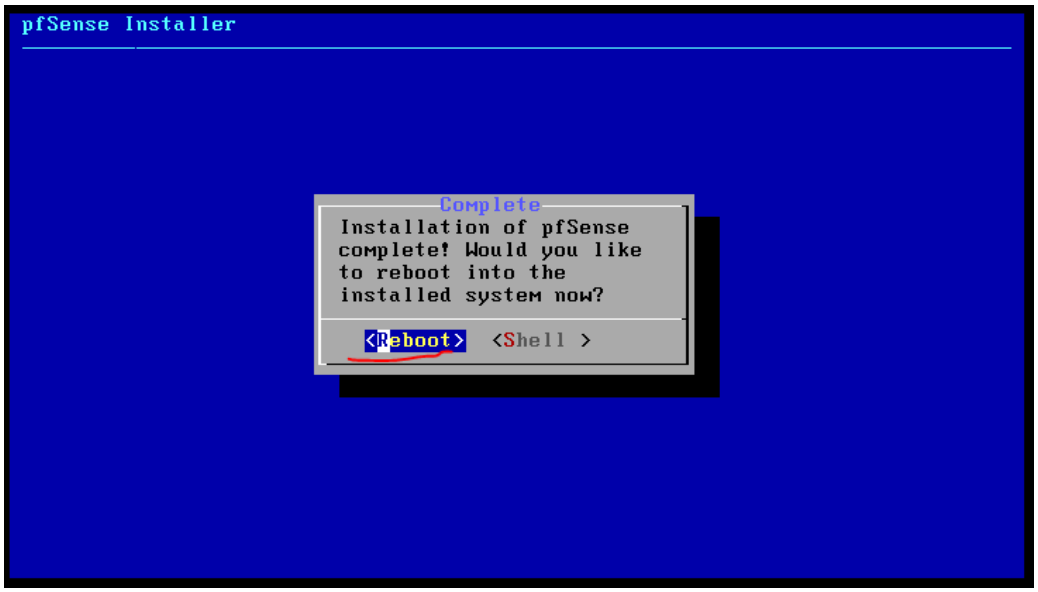

Home
Windows Server 2016 DC
Server-B-VM2
Server-B-VM1
FreeBSD version 10 and earlie...
pfSense 2.4.5
pfSense Installer
Copyright and distribution notice
pfSense is Copyright 2004-2020 Rubicon Communications, LLC (Netgate).
pfSense is a federally registered trademark of Electric Sheep Fencing, LLC. Any unauthorized use of this trademark is prohibited by state and federal law and international law. Refer to our Trademark Usage Guidelines for how to properly use the marks. All rights reserved.
Absolutely No Commercial Distribution Is Allowed.
<Accept>


pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
< OK >
<Cancel>

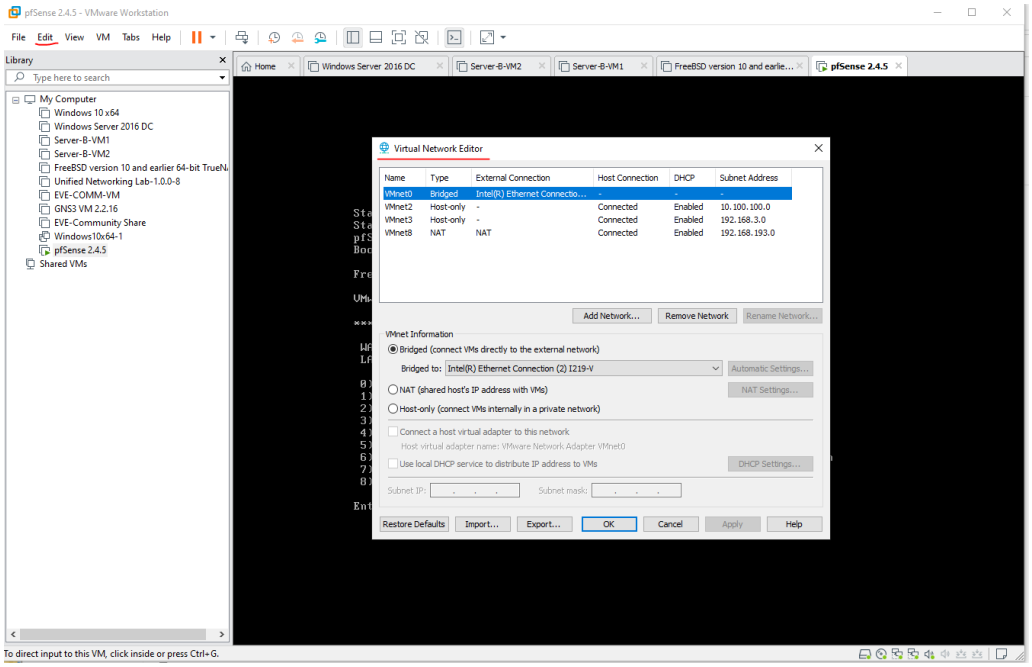

pfSense Installer
Keymap Selection
The system console driver for pfSense defaults to standard "US" keyboard map. Other keymaps can be chosen below.
>>> Continue with default keymap
-> Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
13%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]

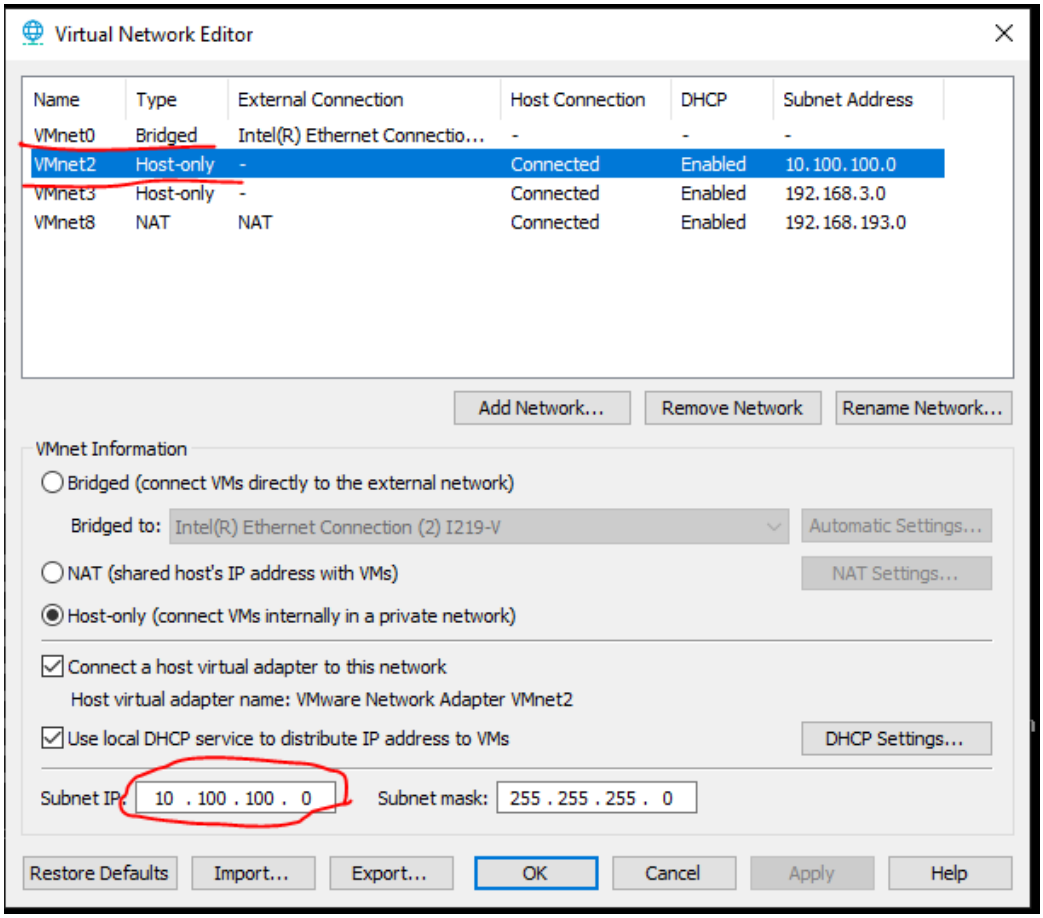

pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (UFS) Guided Disk Setup
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
Auto (ZFS) Guided Root-on-ZFS
< OK >
<Cancel>


pfSense Installer
Manual Configuration
The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?
< Yes >
< No >

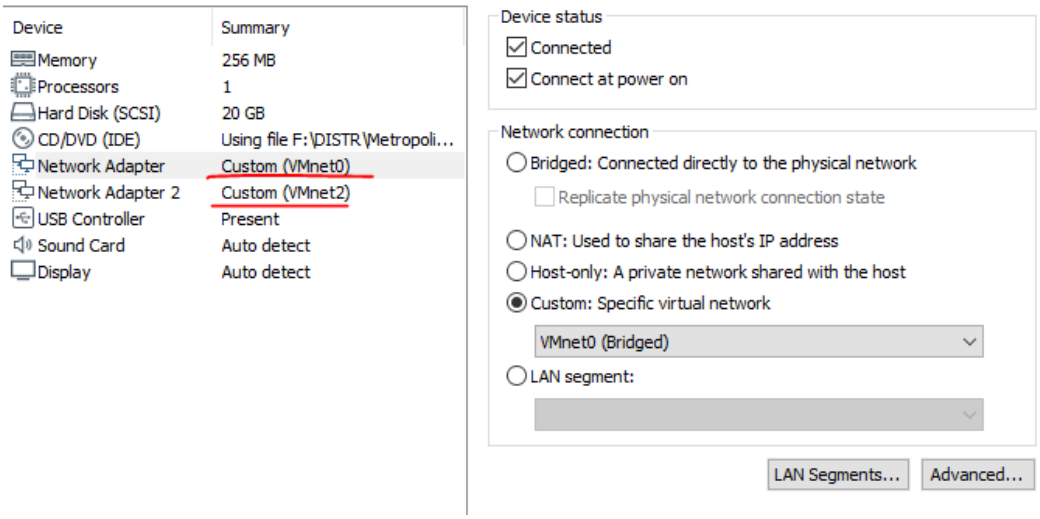

pfSense Installer
Complete
Installation of pfSense
complete! Would you like
to reboot into the
installed system now?
<Reboot> <Shell >

Editing Virtual Networks on VMware





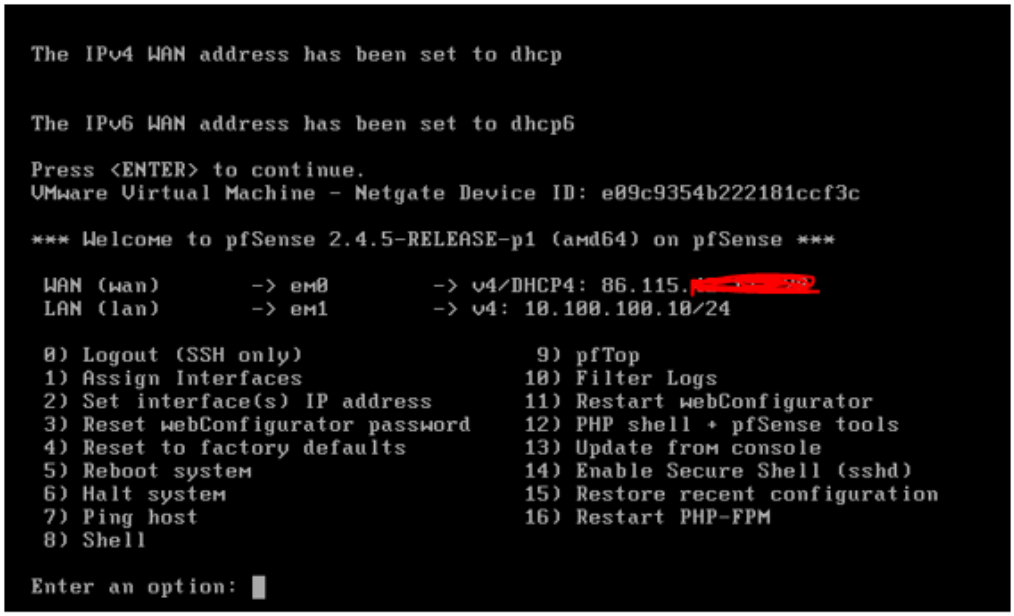
Since in pfSense we have installed two NICs we must configure the Network setting for it.



One of them will be connected to the local router via a Bridge connection, and the second one will be our virtual network, below which all VM machines are. (DC server, Server-B-VM1, Server-B-VM2, TrueNAS)

Now we must configure our NICs

Choose Assign Interfaces by selecting 1 in the Main menu



Should VLANs be set up now? **No**

Enter the WAN interface name or ‘a’ fir auto-detection (em0 em1 or a): **em0**

Enter the LAN interface name or ‘a’ for auto-detection

NOTE: this enables full Firewalling/NAT mode.

(em1 a or nothing if finished): **em1**

Do you want to proceed [y:n]? **yes**

```
em1     00:0c:29:d9:b0:7a   (up) Intel(R) PRO/1000 Legacy Network Connection 1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y:n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y:n]? y
```

The next step is configuring IP addresses for our NICs

```
The IPv4 WAN address has been set to dhcp


The IPv6 WAN address has been set to dhcp6

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: e09c9354b222181ccf3c

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 86.115.[redacted]
 LAN (lan)       -> em1        -> v4: 10.100.100.10/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2
```

For the LAN adapter, the network will be 10.100.100.0 /24

The range of IP addresses will be 10.100.100.100-254

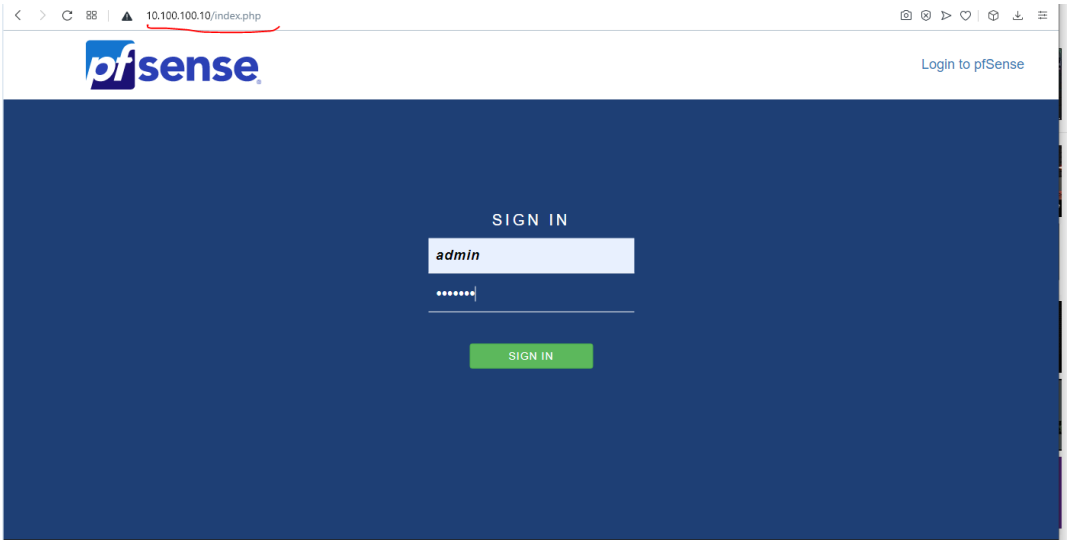
```
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.100.100.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

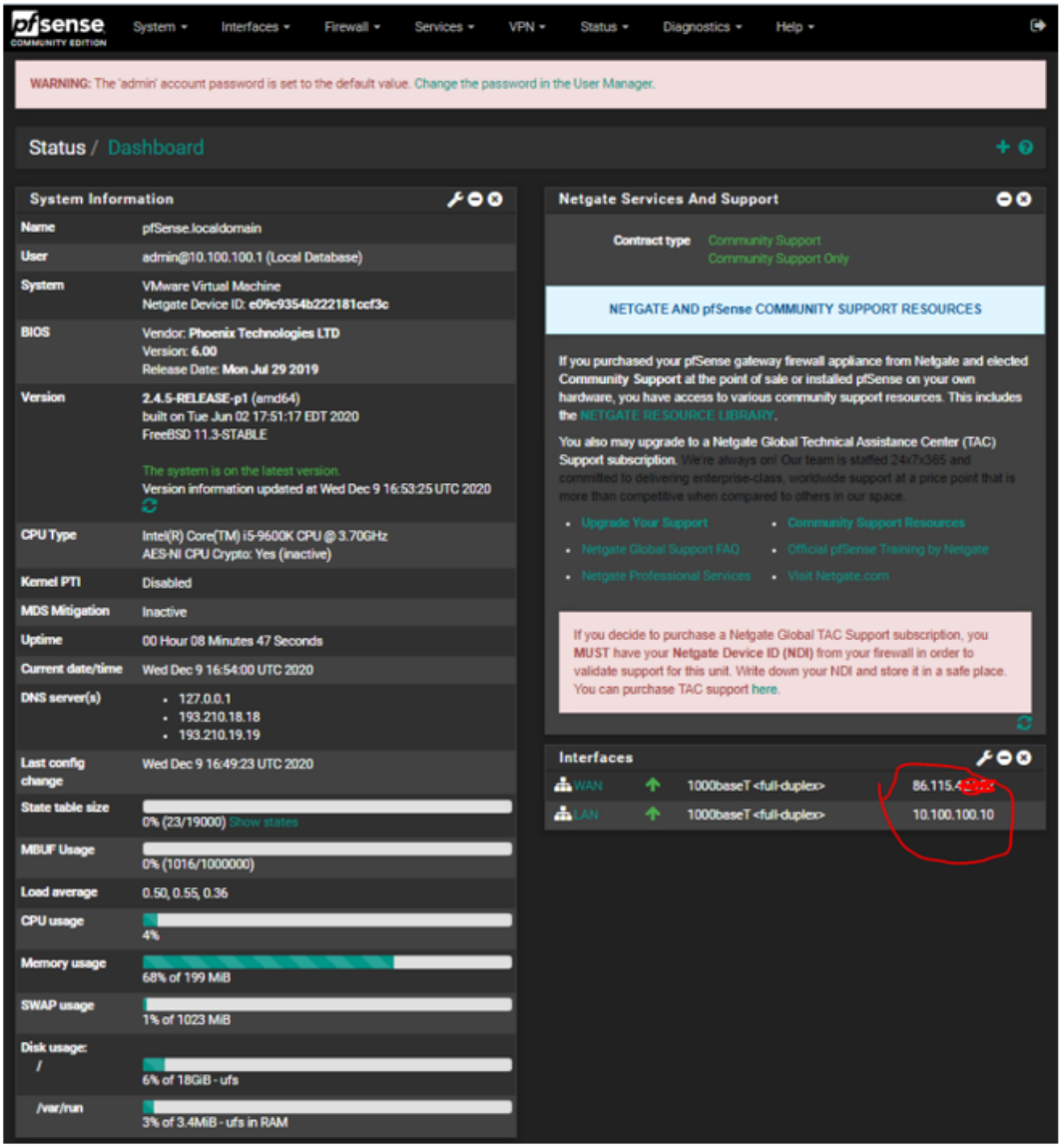
```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.100.100.100
Enter the end address of the IPv4 client address range: 10.100.100.254
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

The result must be like this. Now we can use the GUI of pfSense

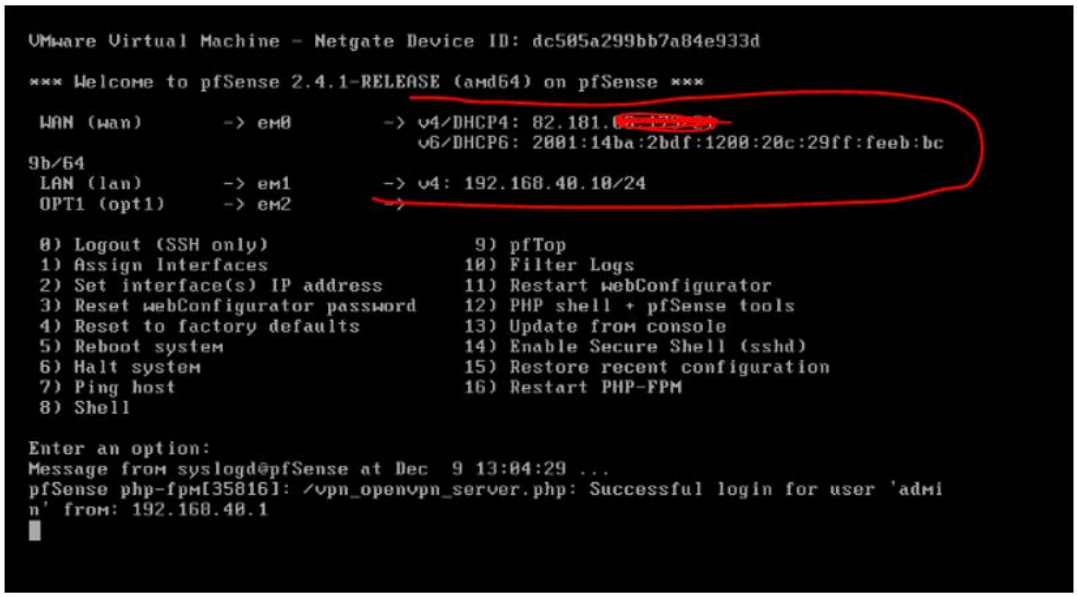
```
The IPv4 LAN address has been set to 10.100.100.10/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://10.100.100.10/

Press <ENTER> to continue.
```

By default, the login and password are *admin* and *pfsense*

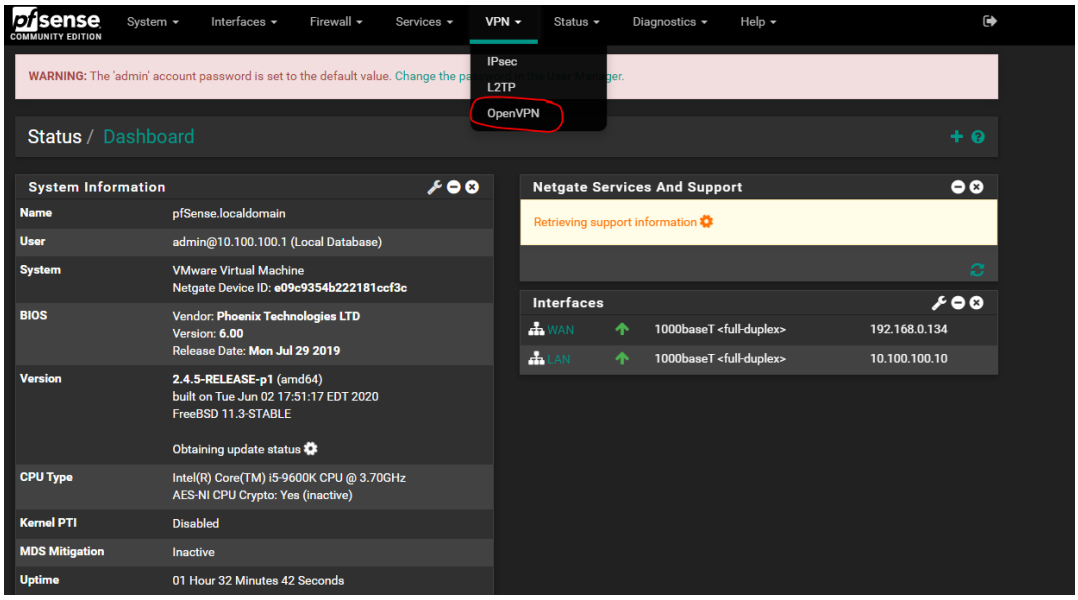


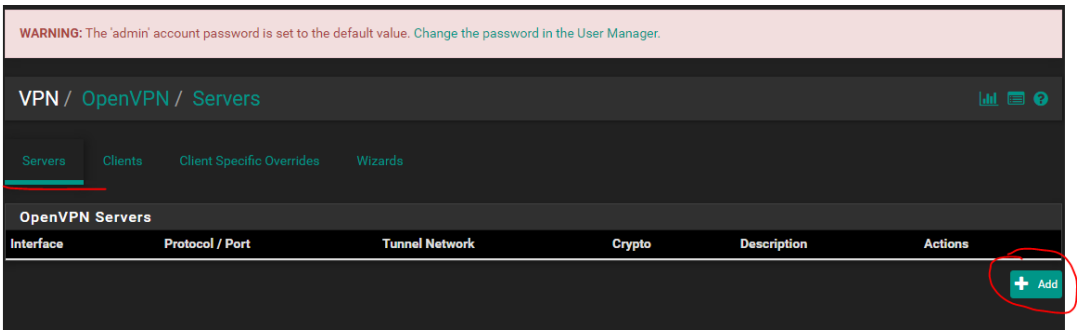


The N site has been configured with different network addresses



Configuring OpenVPN on B site





General Information

Disabled
☐ Disable this server
Set this option to disable this server without removing it from the list.

Server mode
Peer to Peer (Shared Key)

Protocol
UDP on IPv4 only

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.)

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.

Description
Server B-site
A description may be entered here for administrative reference (not parsed).

Tunnel Settings

IPv4 Tunnel Network
172.16.0.0/24
This is the IPv4 virtual network 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 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.

IPv4 Remote network(s)
192.168.40.0/24
IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

IPv6 Remote network(s)
These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

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

Compression
Disable Compression, retain compression packet framing (compres
Compress tunnel packets using the LZO algorithm.
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.

Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.

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

Cryptographic Settings

TLS keydir direction
Use default direction
The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Shared key
☑ Automatically generate a shared key

Encryption Algorithm
AES-128-CBC (128 bit key, 128 bit block)
The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.

Enable NCP
☑ Enable Negotiable Cryptographic Parameters
Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below.

NCP Algorithms

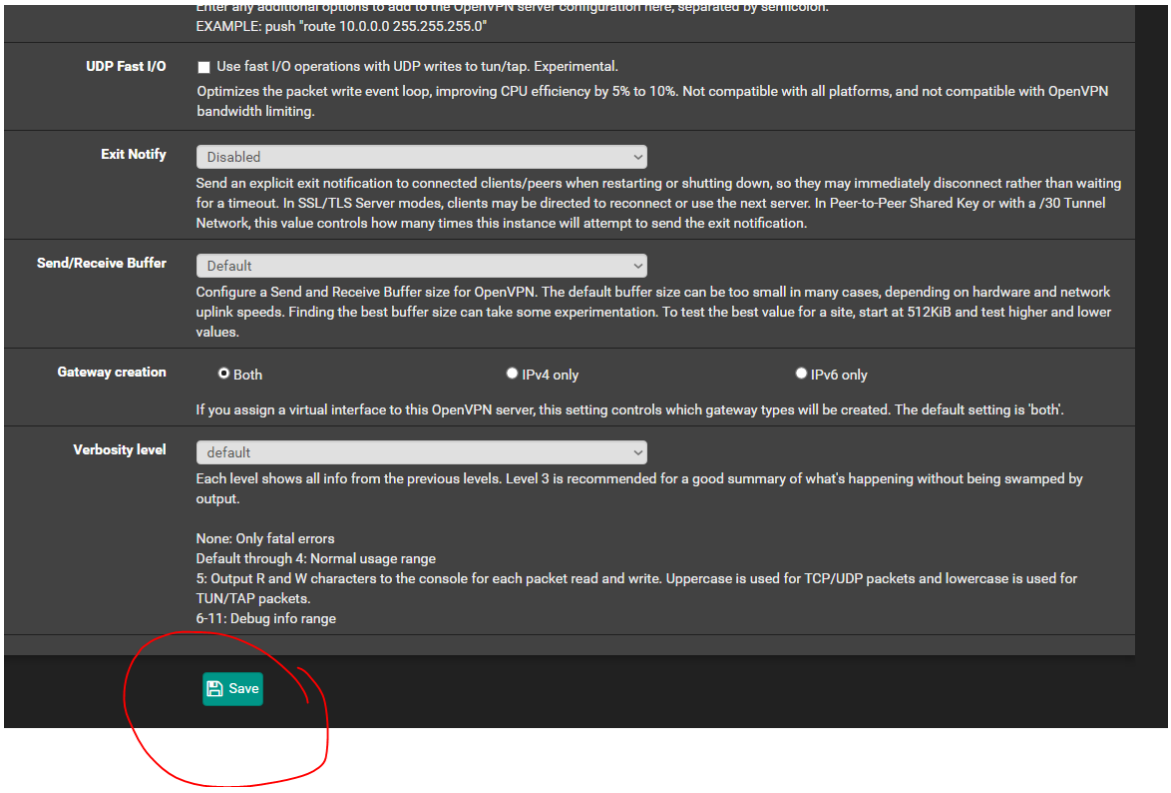
Available NCP Encryption Algorithms Click to add or remove an algorithm from the list	Allowed NCP Encryption Algorithms. Click an algorithm name to remove it from the list
AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB1 (128 bit key, 128 bit block) AES-128-CFB8 (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-128-GCM

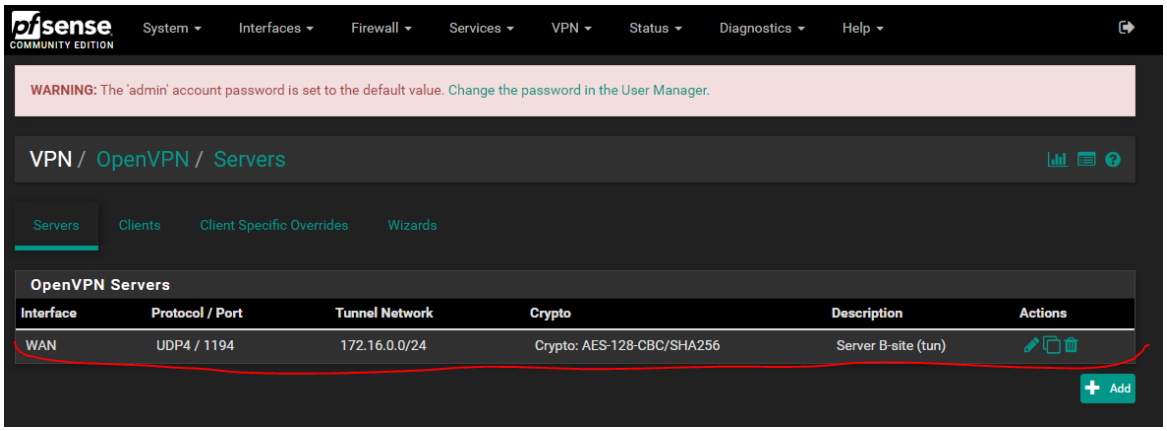
The order of the selected NCP Encryption Algorithms is respected by OpenVPN.

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.

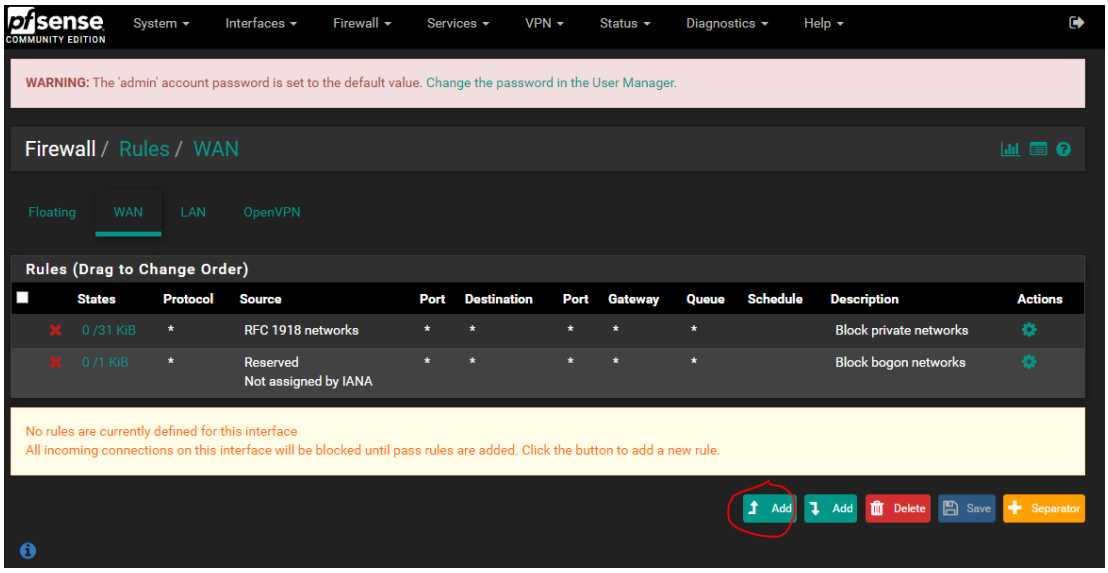
Hardware Crypto
No Hardware Crypto Acceleration

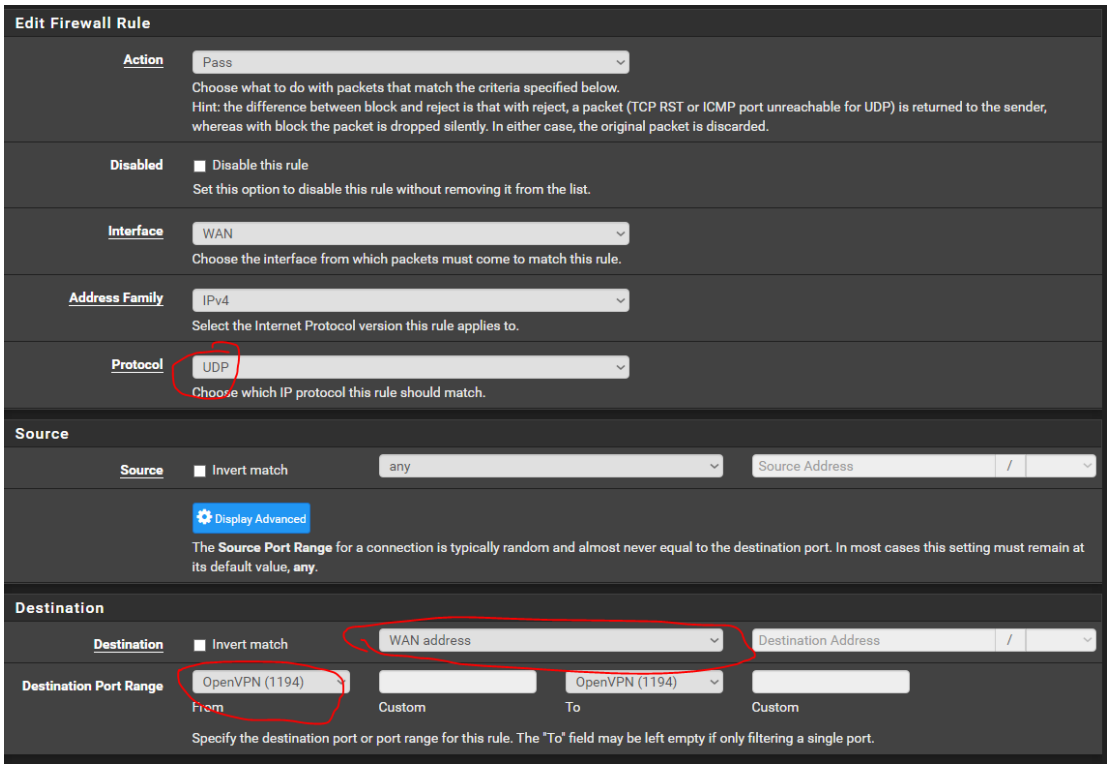
All other settings remain the same

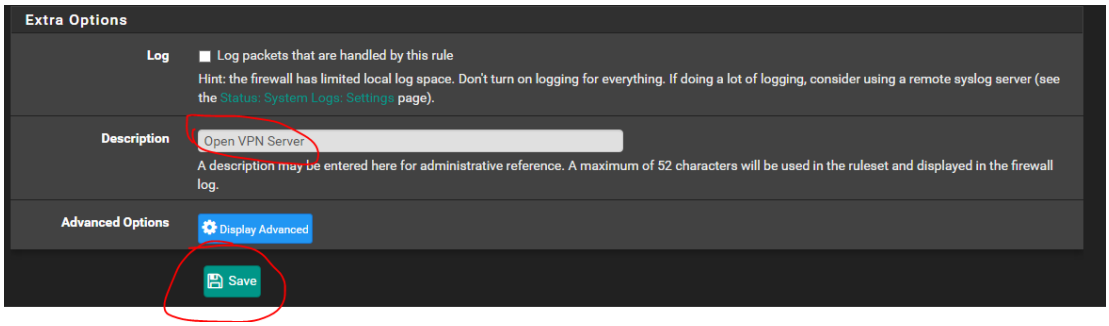




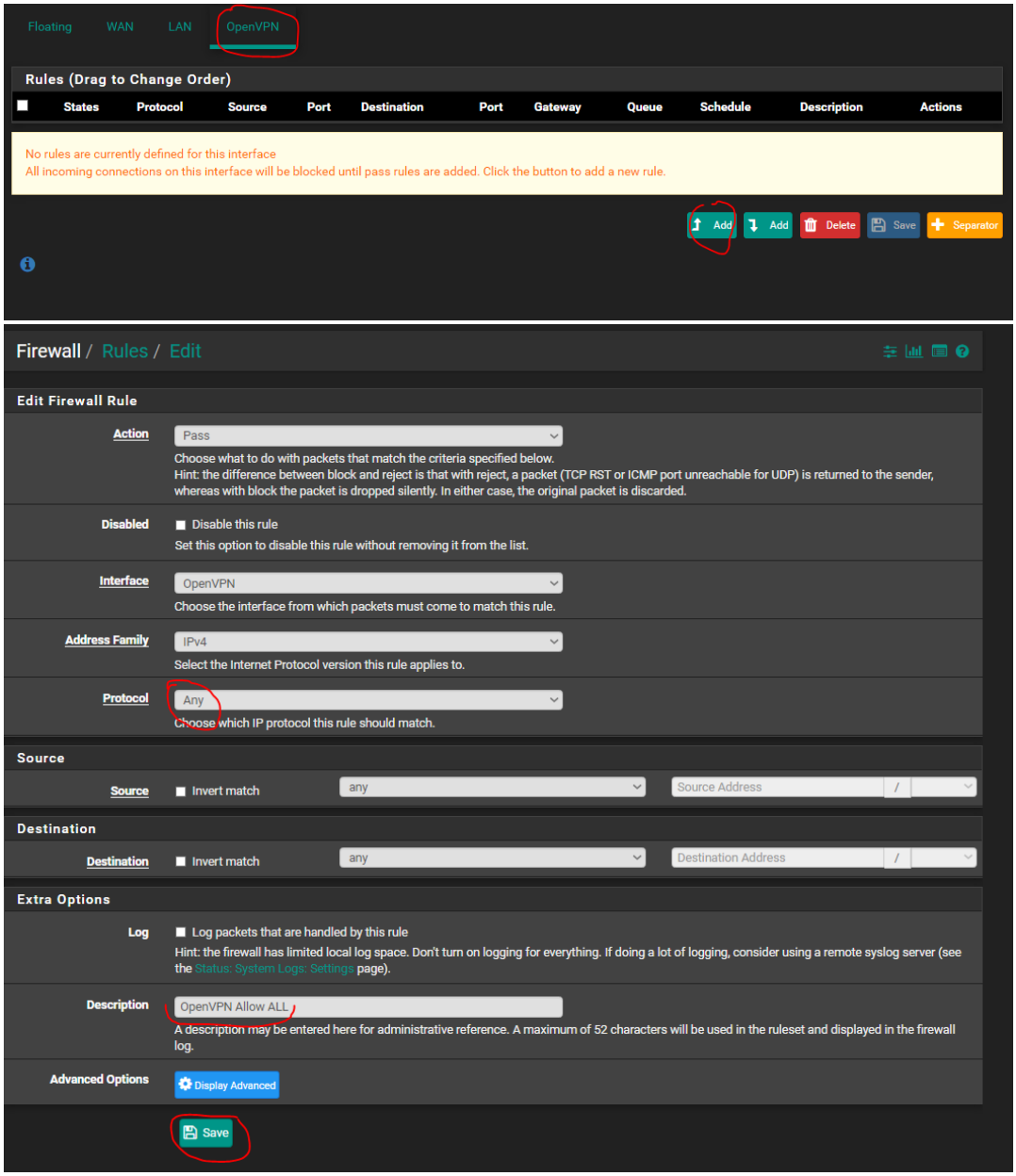
One more step is needed. Adding rules for the WAN interface



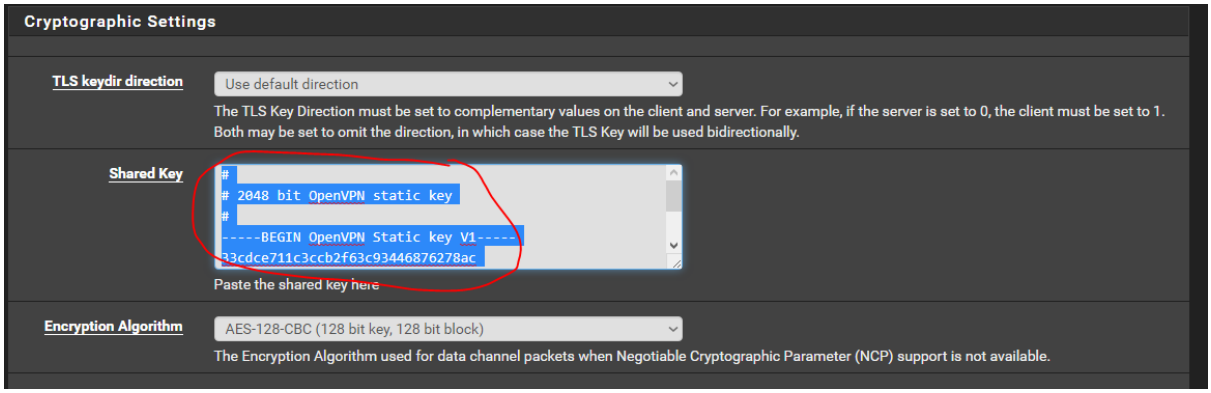




Adding rules for OpenVPN



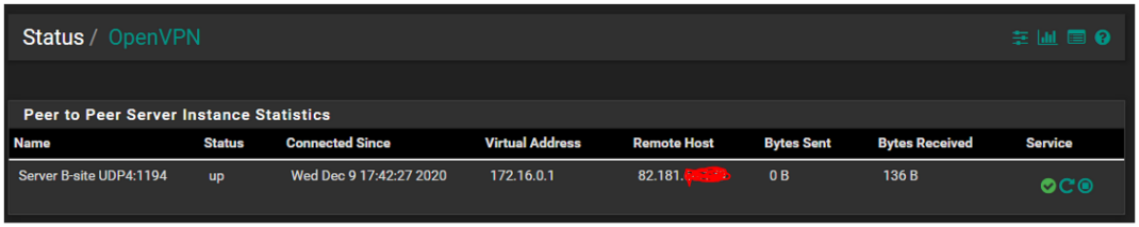
Copy the generated shared key for the client.



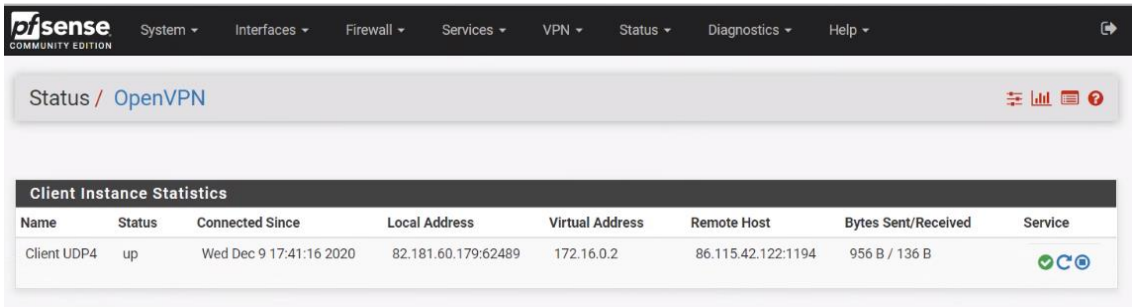
The next step is to configure the OpenVPN client

Checking the status of OpenVPN

B-site (Server)

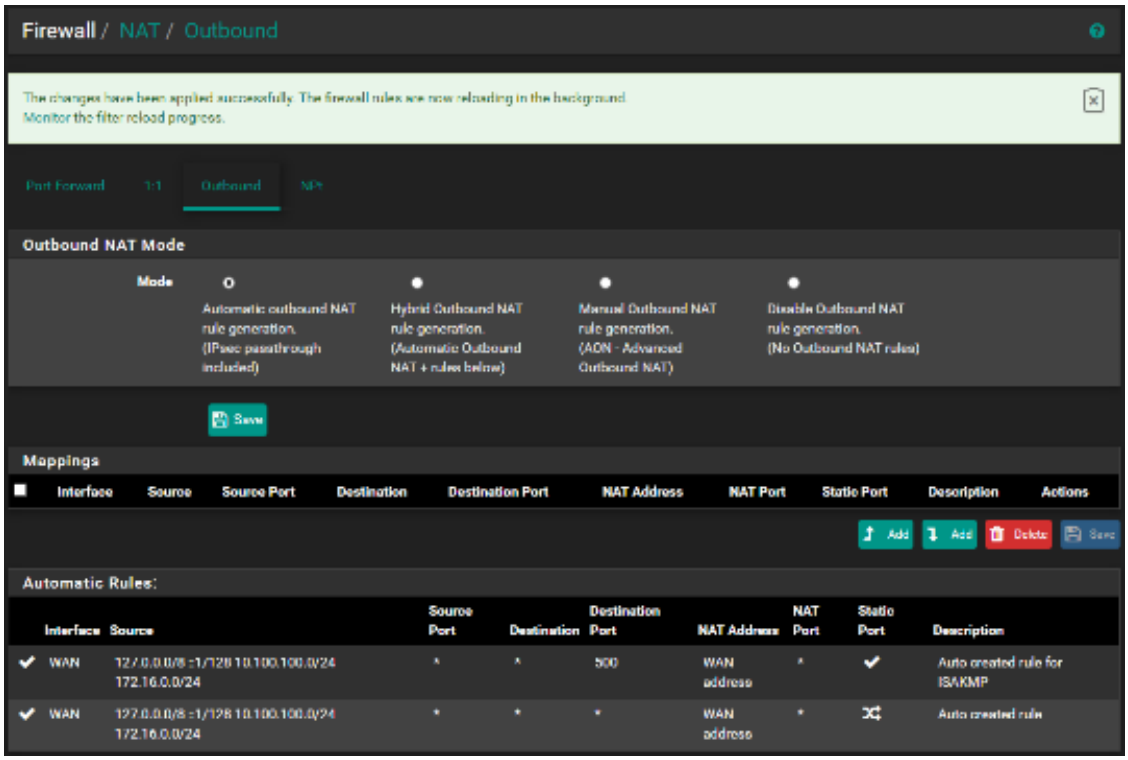


N-Site(Client)

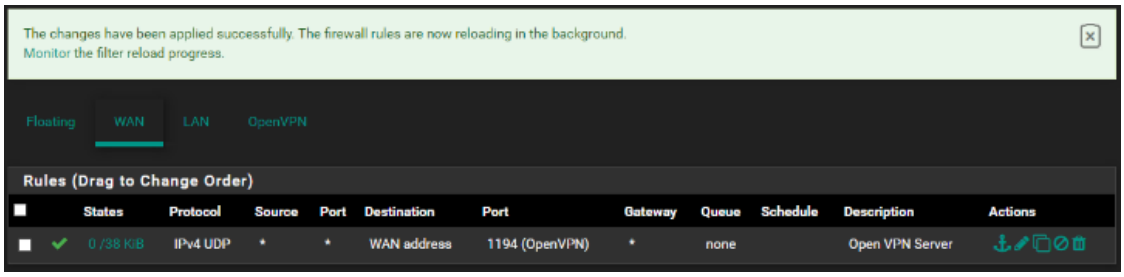


Adding rules B-site

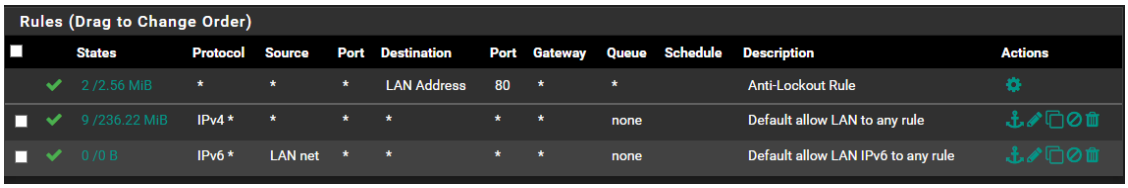
Firewall -> NAT -> Outbound



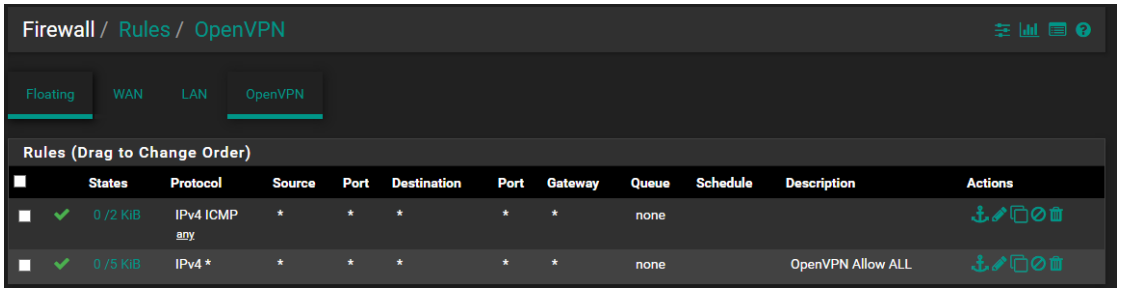
Firewall, Rules, WAN



Firewall, Rules, LAN *(for testing purposes all IPv4 and IPv6 traffic have been allowed)*. *For secure purpose, the rules shown in the picture (Default allow LAN to any rule and Default allow LAN IPv6 to any rule) must be deleted and for each kind of traffic, the new rules must be added separately.*



Firewall, Rules, OpenVPN



Checking the ping to the remote local network from B-site VM (pfSense) to the N-site VM (pfSense) and vice versa.

```
 1) Assign Interfaces              10) Filter Logs
 2) Set interface(s) IP address    11) Restart webConfigurator
 3) Reset webConfigurator password 12) PHP shell + pfSense tools
 4) Reset to factory defaults      13) Update from console
 5) Reboot system                  14) Enable Secure Shell (sshd)
 6) Halt system                    15) Restore recent configuration
 7) Ping host                      16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 192.168.40.10

PING 192.168.40.10 (192.168.40.10): 56 data bytes
64 bytes from 192.168.40.10: icmp_seq=0 ttl=64 time=32.995 ms
64 bytes from 192.168.40.10: icmp_seq=1 ttl=64 time=30.405 ms
64 bytes from 192.168.40.10: icmp_seq=2 ttl=64 time=30.250 ms

--- 192.168.40.10 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 30.250/31.217/32.995/1.259 ms

Press ENTER to continue.
```

```
 1) Assign Interfaces              10) Filter Logs
 2) Set interface(s) IP address    11) Restart webConfigurator
 3) Reset webConfigurator password 12) PHP shell + pfSense tools
 4) Reset to factory defaults      13) Update from console
 5) Reboot system                  14) Enable Secure Shell (sshd)
 6) Halt system                    15) Restore recent configuration
 7) Ping host                      16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 10.100.100.10

PING 10.100.100.10 (10.100.100.10): 56 data bytes
64 bytes from 10.100.100.10: icmp_seq=0 ttl=64 time=32.407 ms
64 bytes from 10.100.100.10: icmp_seq=1 ttl=64 time=31.064 ms
64 bytes from 10.100.100.10: icmp_seq=2 ttl=64 time=40.441 ms

--- 10.100.100.10 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 31.064/34.637/40.441/4.140 ms

Press ENTER to continue.
```

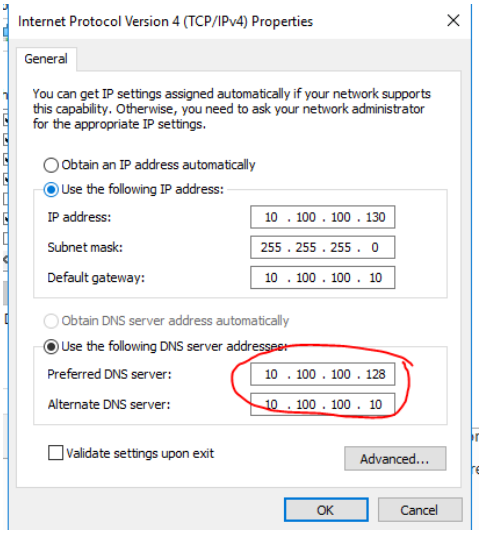
Checking ping connection from DC-Server (B-Site) to the remote LAN address server

```
C:\Users\Administrator.WIN-TO1Q4VR8991.000>ping 192.168.40.131

Pinging 192.168.40.131 with 32 bytes of data:
Reply from 192.168.40.131: bytes=32 time=33ms TTL=126
Reply from 192.168.40.131: bytes=32 time=31ms TTL=126
Reply from 192.168.40.131: bytes=32 time=31ms TTL=126
Reply from 192.168.40.131: bytes=32 time=37ms TTL=126

Ping statistics for 192.168.40.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 37ms, Average = 33ms

C:\Users\Administrator.WIN-TO1Q4VR8991.000>
```

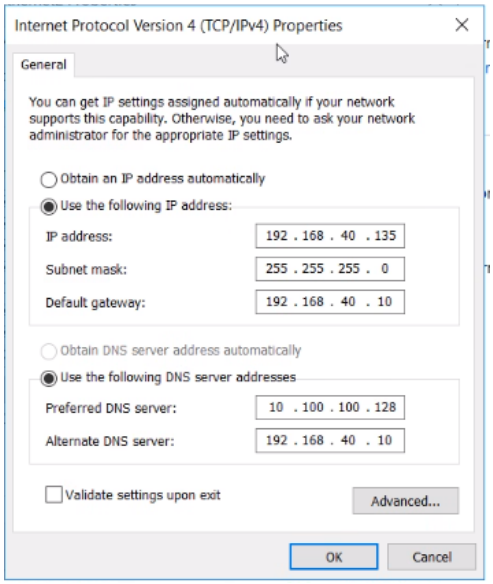
Now we are adding servers to the Domain Controller

Before that, the DNS settings must be added as well

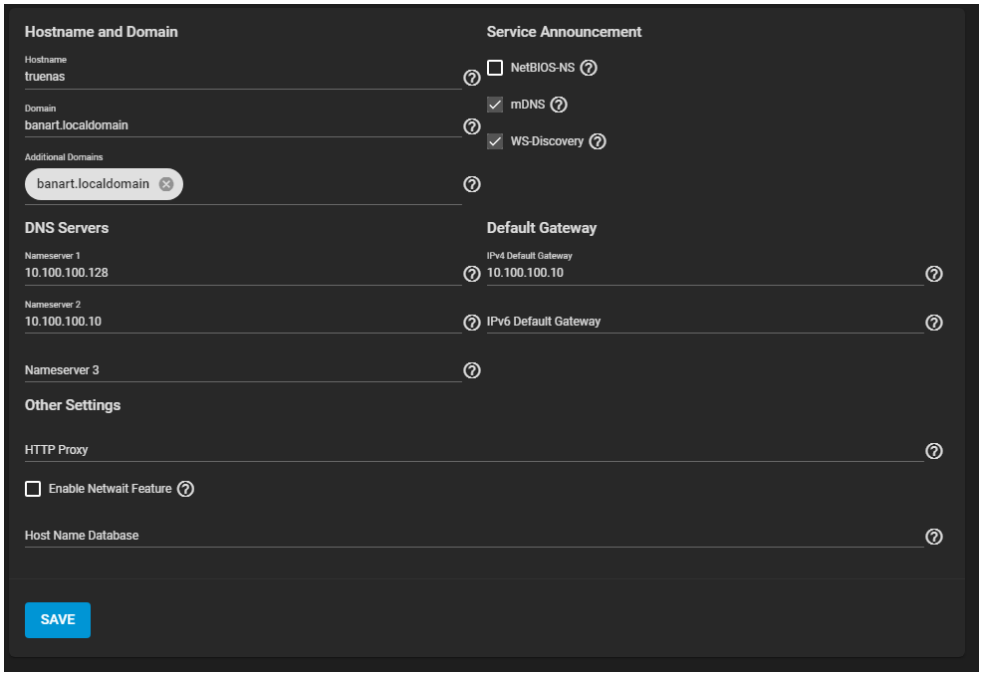
B-Site



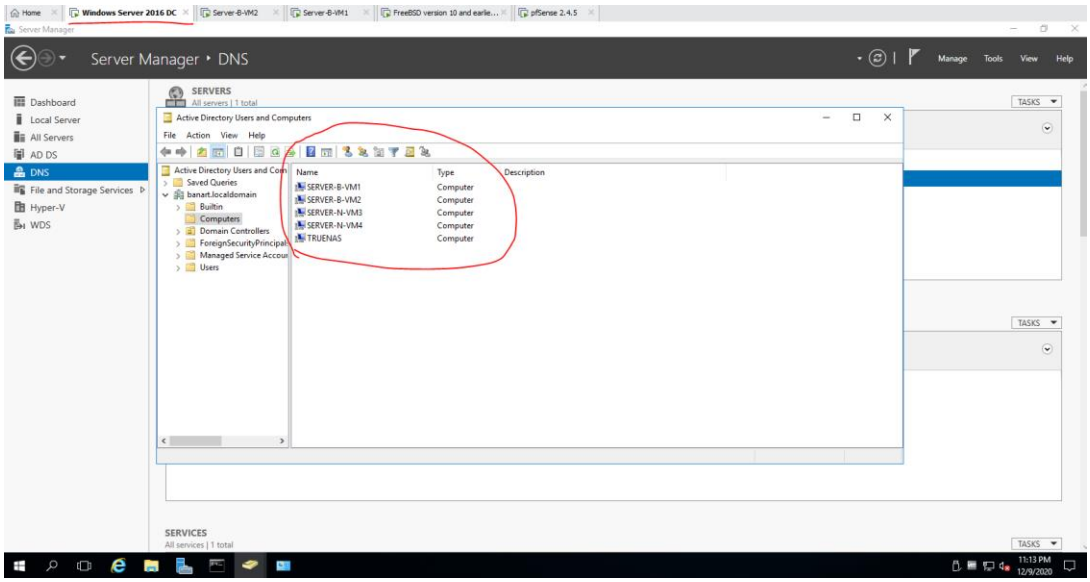
N-Site



The setting of TrueNas VM

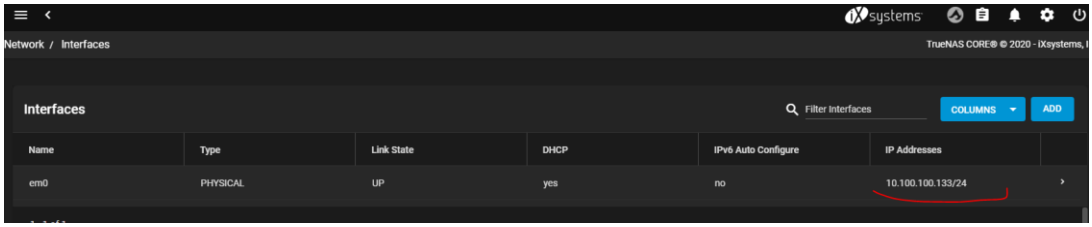


Checking the result of adding all servers from both sites to the Domain Controller

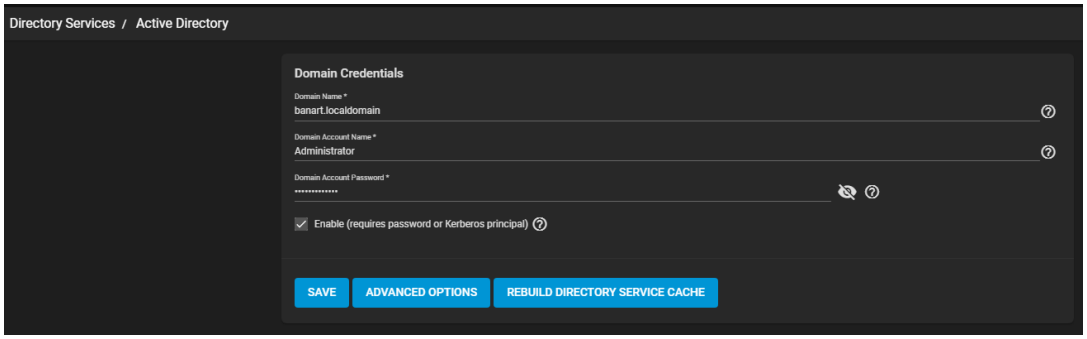


Configuring TrueNAS VM

Adding a static IP address to the TrueNAS VM

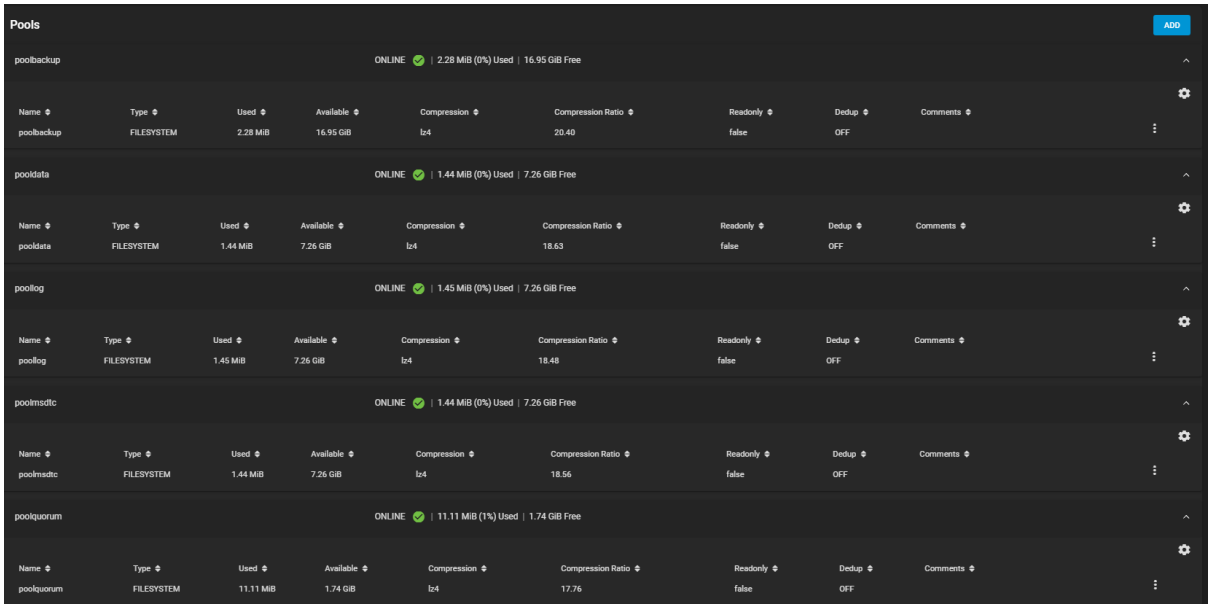


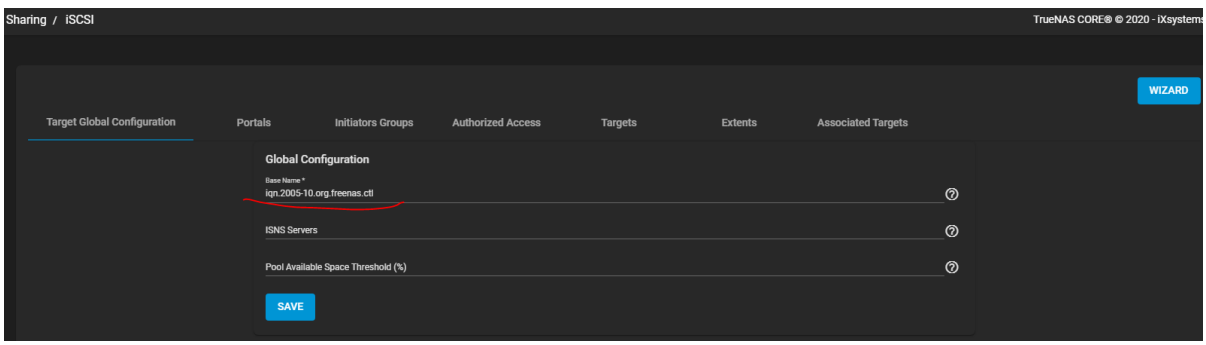
Adding TrueNAS VM to the Active Directory

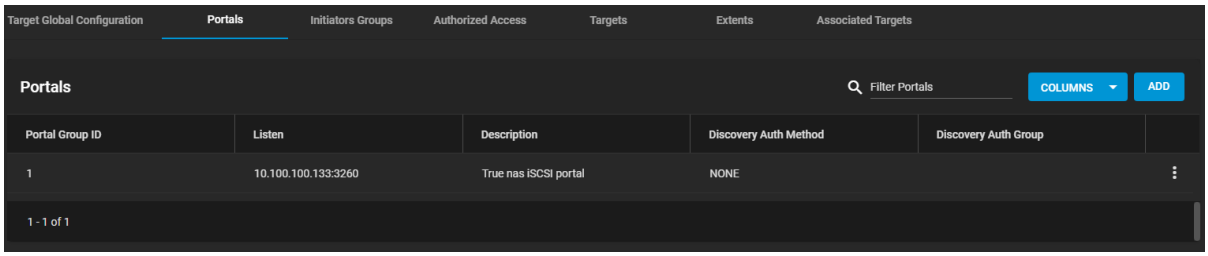


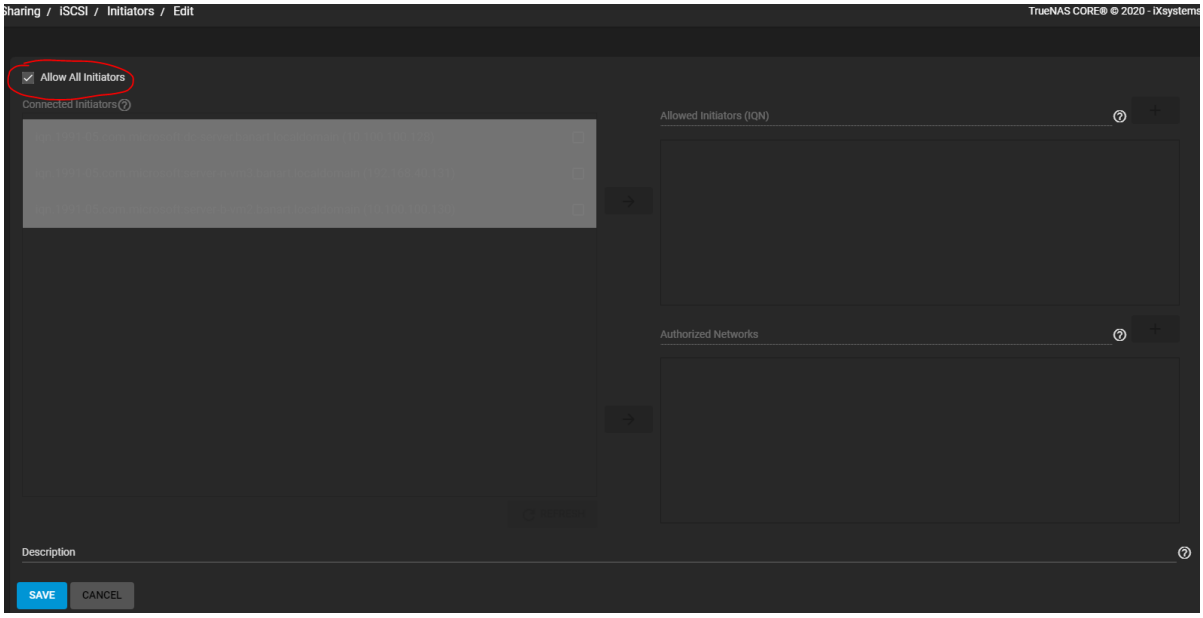
Configuring all connected Hard Drives to be available on Windows Servers

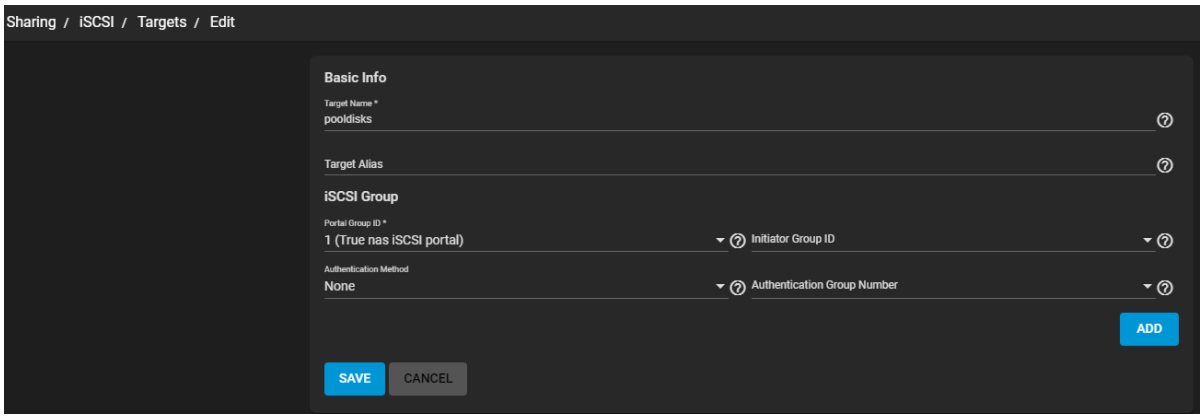
All disks triple mirrored; the result of mirroring is shown in the picture

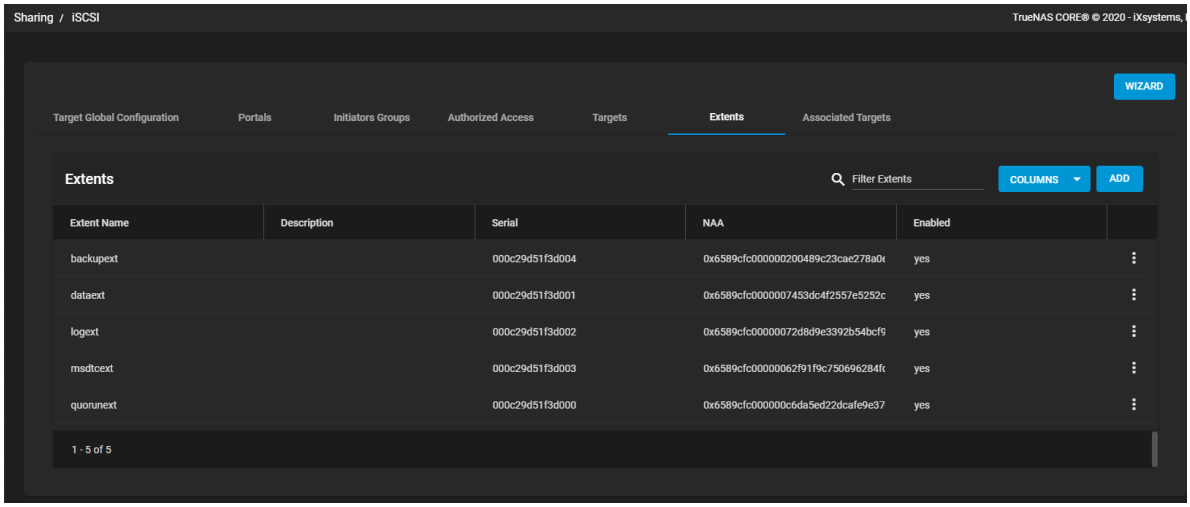


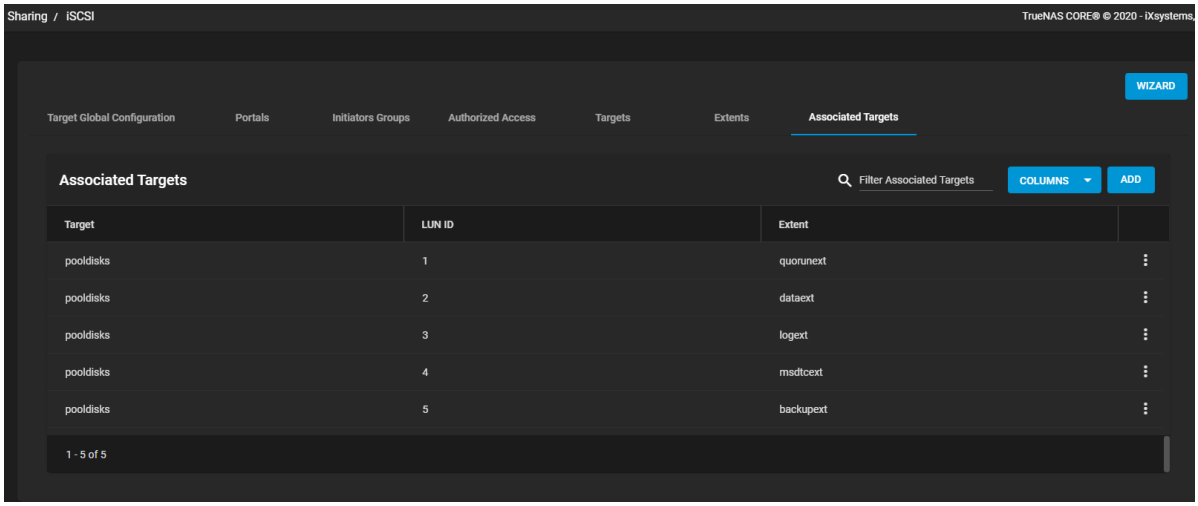


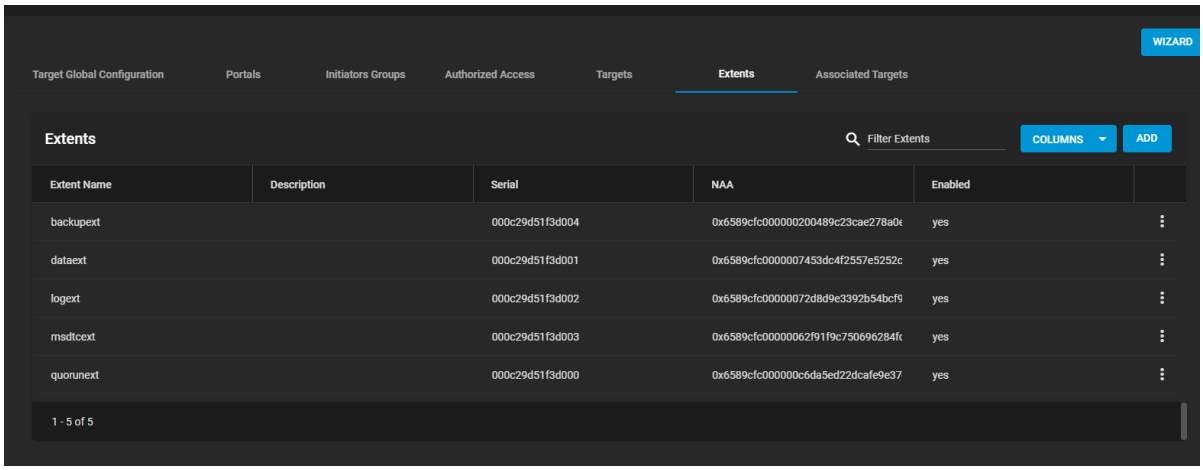

Target Global Configuration
Portals
Initiators Groups
Authorized Access
Targets
Extents
Associated Targets
Portals
Filter Portals
COLUMNS
ADD
Portal Group ID
Listen
Description
Discovery Auth Method
Discovery Auth Group
1
10.100.100.133:3260
True nas iSCSI portal
NONE
1 - 1 of 1


Sharing / iSCSI / Initiators / Edit
TrueNAS CORE® © 2020 - iXsystems
Allow All Initiators
Connected Initiators
Allowed Initiators (IQN)
Authorized Networks
Description
SAVE
CANCEL

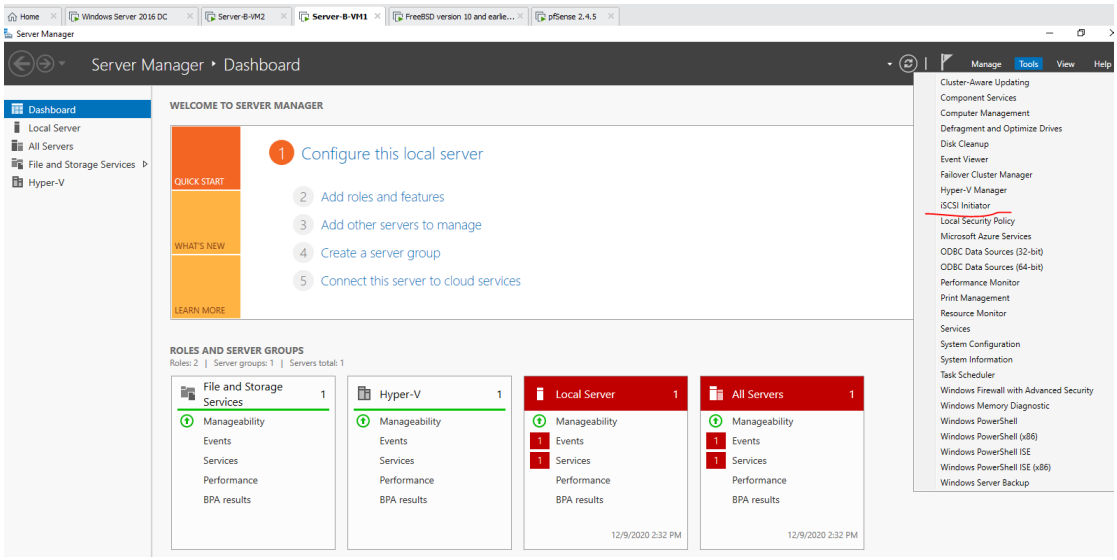

Sharing / iSCSI / Targets / Edit
Basic Info
Target Name *
pooldisks
Target Alias
iSCSI Group
Portal Group ID *
1 (True nas iSCSI portal)
Initiator Group ID
Authentication Method
None
Authentication Group Number
ADD
SAVE
CANCEL

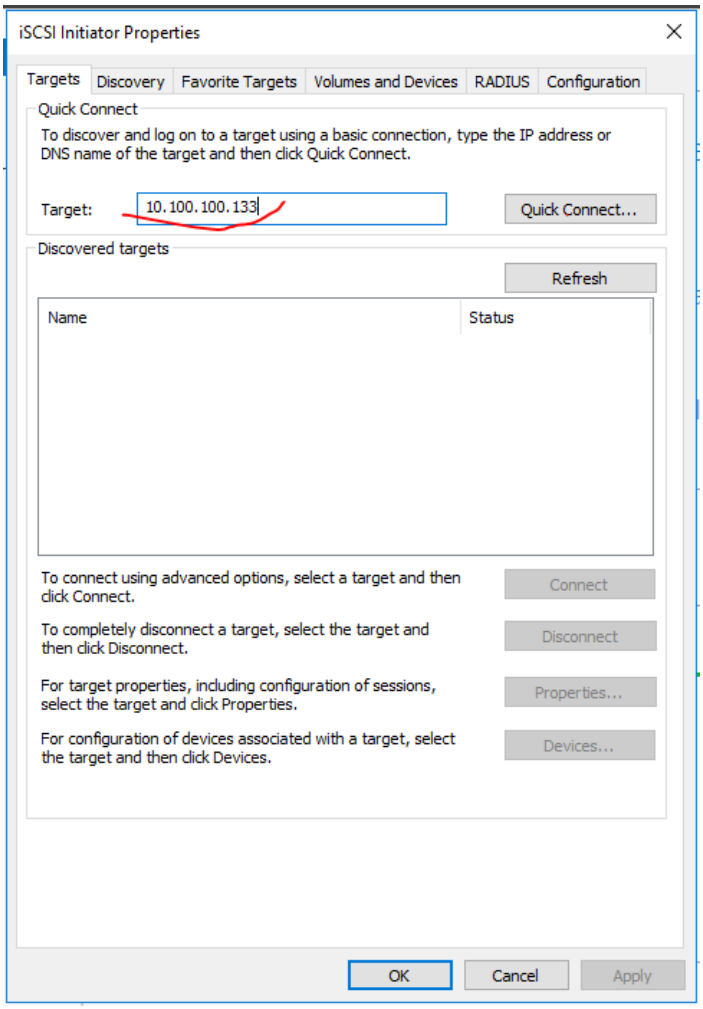

Sharing / iSCSI
TrueNAS CORE® © 2020 - iXsystems
WIZARD
Target Global Configuration
Portals
Initiators Groups
Authorized Access
Targets
Extents
Associated Targets
Extents
Filter Extents
COLUMNS
ADD
Extent Name
Description
Serial
NAA
Enabled
backupext
000c29d51f3d004
0x6589cfc000000200489c23cae278a0
yes
dataext
000c29d51f3d001
0x6589cfc0000007453dc4f2557e5252c
yes
logext
000c29d51f3d002
0x6589cfc00000072d8d9e3392b54bcf9
yes
msdtcext
000c29d51f3d003
0x6589cfc00000062f91f9c750696284f
yes
quorunext
000c29d51f3d000
0x6589cfc000000c6da5ed22dcafe9e37
yes
1 - 5 of 5

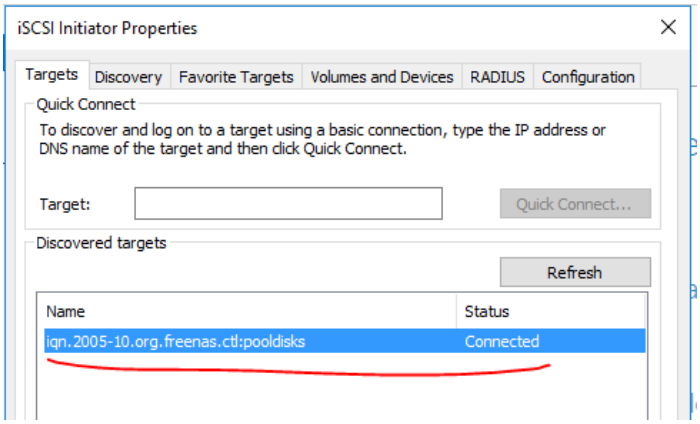


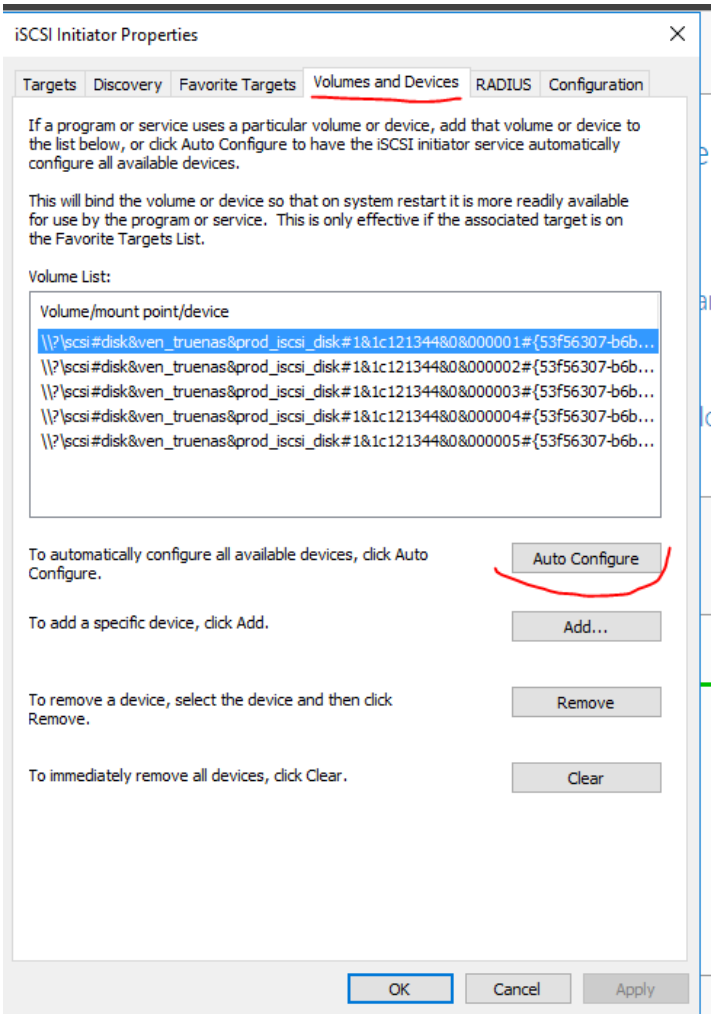


Adding Disks from TrueNAS

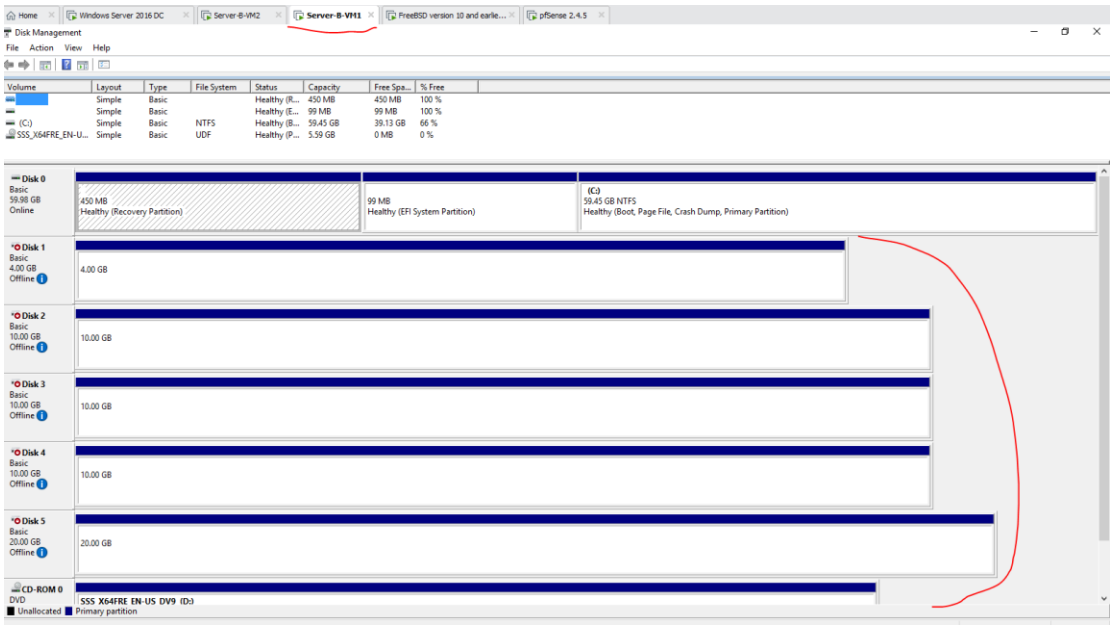

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
Hyper-V
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Hyper-V 1
Local Server 1
All Servers 1
Manageability
Events
Services
Performance
BPA results
12/9/2020 2:32 PM
Cluster-Aware Updating
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
Event Viewer
Failover Cluster Manager
Hyper-V Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup


iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.
Target:
10.100.100.133
Quick Connect...
Discovered targets
Refresh
Name
Status
To connect using advanced options, select a target and then click Connect.
Connect
To completely disconnect a target, select the target and then click Disconnect.
Disconnect
For target properties, including configuration of sessions, select the target and click Properties.
Properties...
For configuration of devices associated with a target, select the target and then click Devices.
Devices...
OK
Cancel
Apply

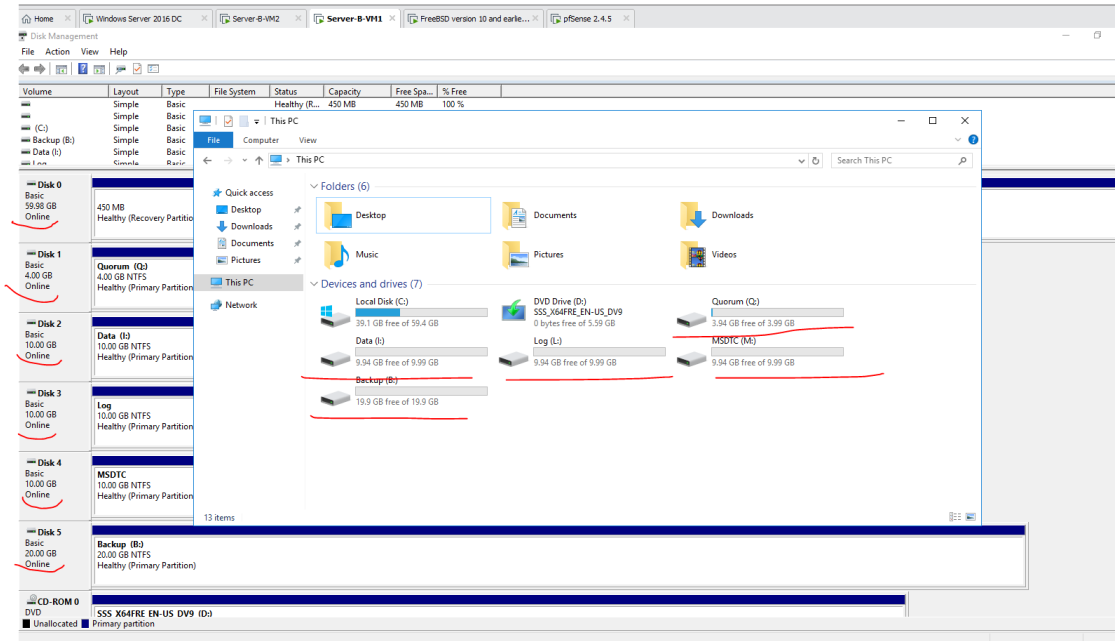

iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.
Target:
Quick Connect...
Discovered targets
Refresh
Name
Status
iqn.2005-10.org.freenas.ctl:pooldisks
Connected


iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
If a program or service uses a particular volume or device, add that volume or device to the list below, or click Auto Configure to have the iSCSI initiator service automatically configure all available devices.
This will bind the volume or device so that on system restart it is more readily available for use by the program or service. This is only effective if the associated target is on the Favorite Targets List.
Volume List:
Volume/mount point/device
\\?\scsi#disk&ven_truenas&prod_iscsi_disk#1&1c121344&0&000001#{53f56307-b6b...
\\?\scsi#disk&ven_truenas&prod_iscsi_disk#1&1c121344&0&000002#{53f56307-b6b...
\\?\scsi#disk&ven_truenas&prod_iscsi_disk#1&1c121344&0&000003#{53f56307-b6b...
\\?\scsi#disk&ven_truenas&prod_iscsi_disk#1&1c121344&0&000004#{53f56307-b6b...
\\?\scsi#disk&ven_truenas&prod_iscsi_disk#1&1c121344&0&000005#{53f56307-b6b...
To automatically configure all available devices, click Auto Configure.
Auto Configure
To add a specific device, click Add.
Add...
To remove a device, select the device and then click Remove.
Remove
To immediately remove all devices, click Clear.
Clear
OK
Cancel
Apply

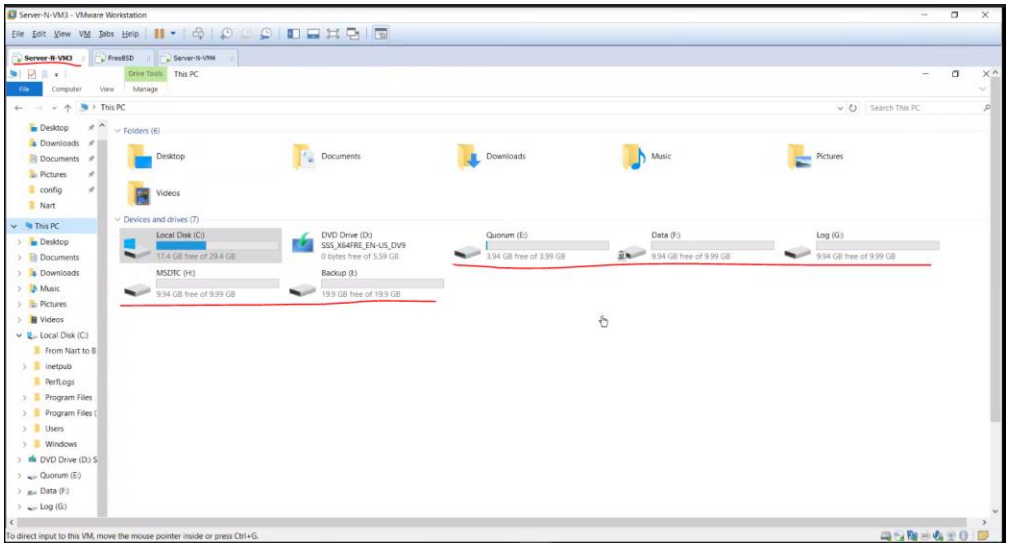
After adding all disks to the Disk Management, they must be formatted (preferred GPT format) only once. The same process must be applied to all servers (Failover Nodes) except the DC server.



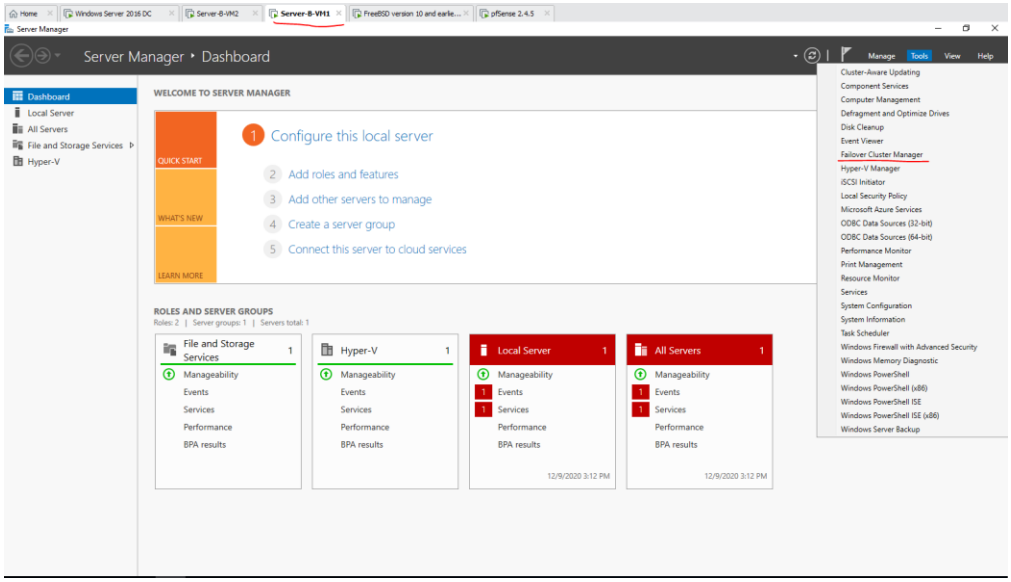
After that, the disk must be turned Online. Then they will be shown as a usual disk on the PC B-Site Server-B-VM1.

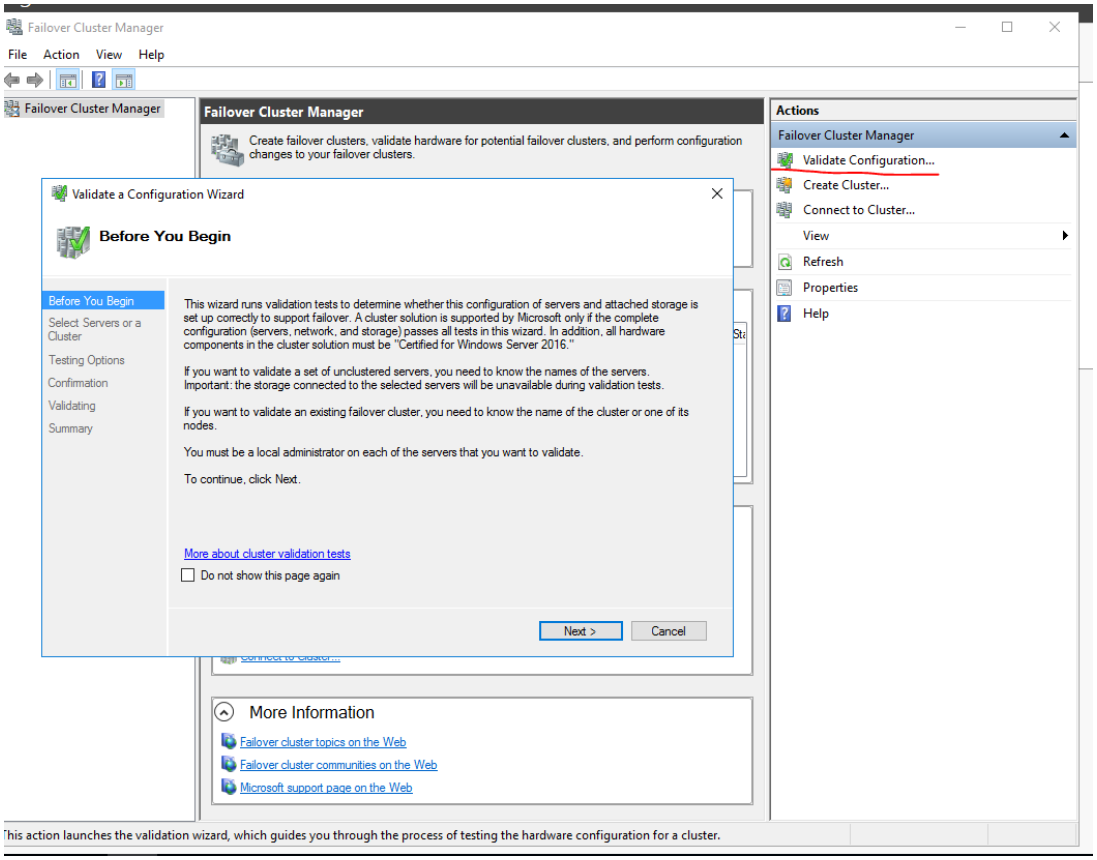


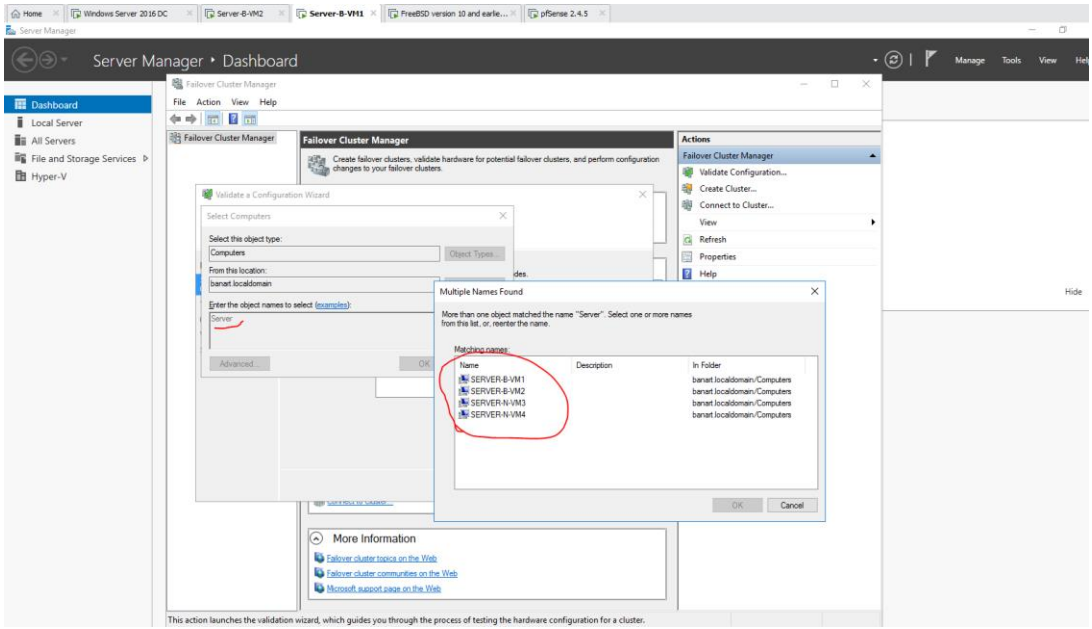
N-Site Server-N-VM3



Now the failover cluster can be installed.







The next steps are the same as we did deploy the failover cluster on Azure servers.

Check the following link:

https://github.com/gearup2000/FAILOVER-CLUSTER-PROTECTED-BY-IPSEC-BASED-ON-MICROSOFT-AZURE