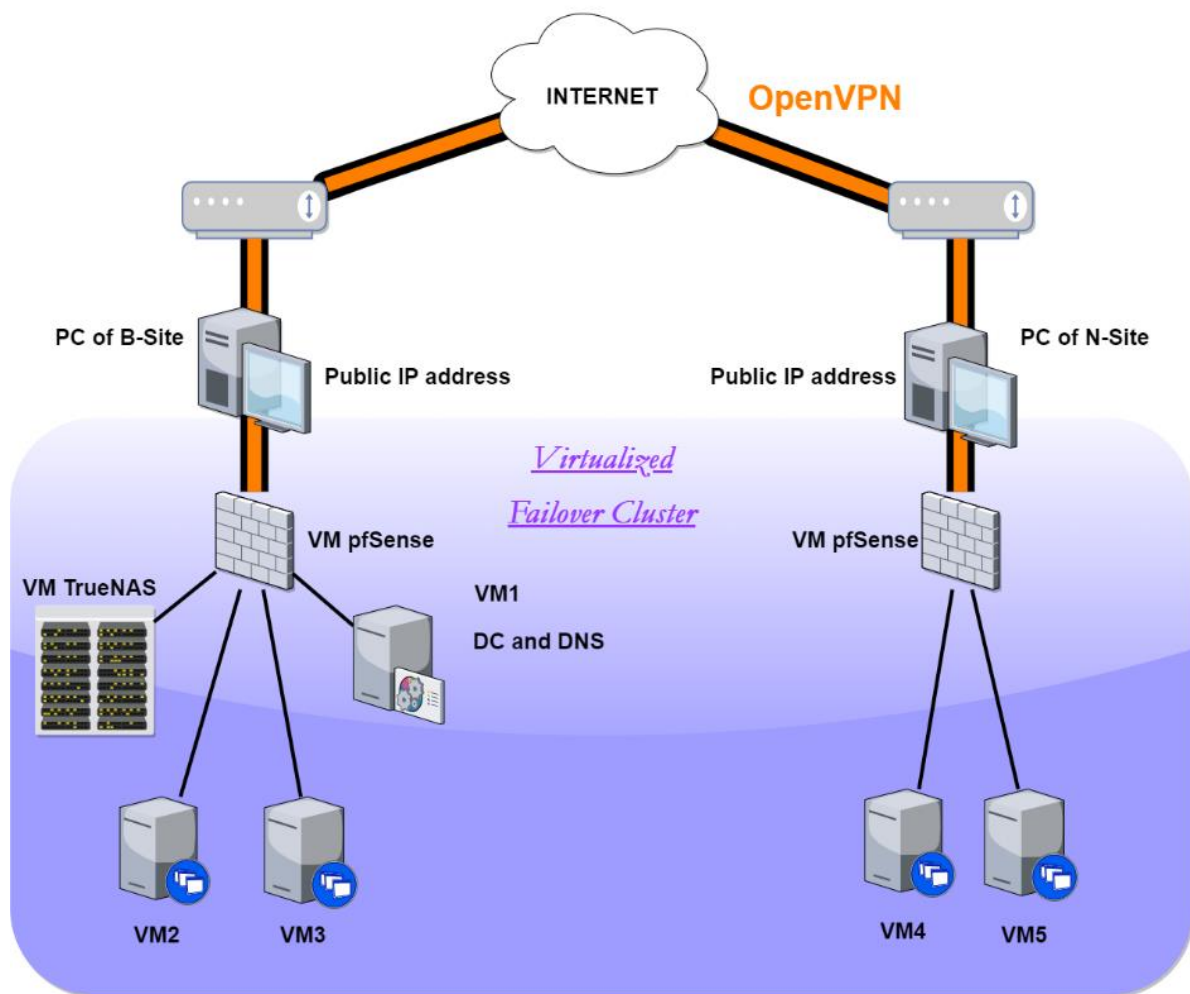


VIRTUAL FAILOVER CLUSTER PROTECTED BY OPENVPN BASED ON WMWARE WORKSTATION

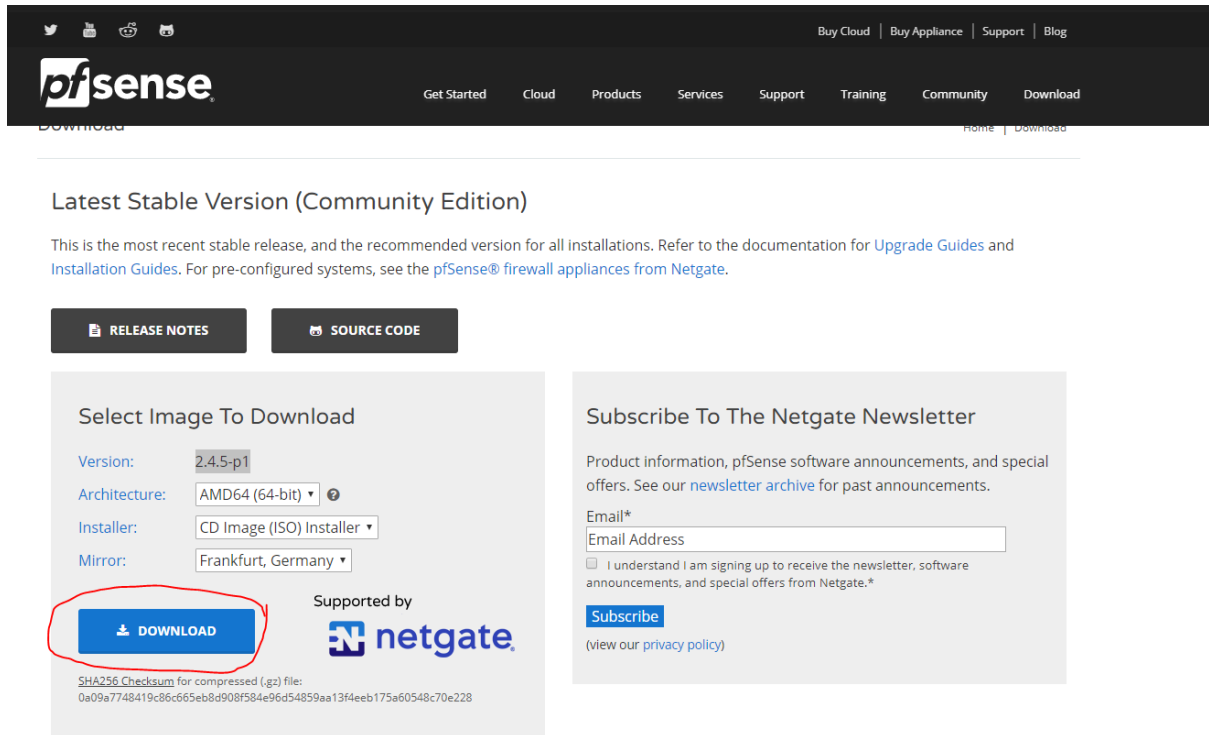


The important note. Before starting, the port forwarding must be applied on the home routers, in such a way that the public IP address from ISP will be forwarded through the home network to the PC itself. This is needed to let Pfsense VM deploy a VPN connection.

Vmware

Configuration B site

Installing pfSense as a VM



The screenshot shows the pfSense website's download page. At the top, there's a navigation bar with links like 'Buy Cloud', 'Buy Appliance', 'Support', and 'Blog'. Below the navigation bar, the pfSense logo is on the left, and a list of links (Get Started, Cloud, Products, Services, Support, Training, Community, Download) is on the right. The main heading is 'Latest Stable Version (Community Edition)'. Below this, a paragraph explains that this is the most recent stable release and refers to documentation for 'Upgrade Guides' and 'Installation Guides'. There are two buttons: 'RELEASE NOTES' and 'SOURCE CODE'. The 'Select Image To Download' section has dropdown menus for 'Version' (2.4.5-p1), 'Architecture' (AMD64 (64-bit)), 'Installer' (CD Image (ISO) Installer), and 'Mirror' (Frankfurt, Germany). A red circle highlights the 'DOWNLOAD' button. To the right of the download section is a 'Subscribe To The Netgate Newsletter' form with an email input field and a 'Subscribe' button. At the bottom of the download section, there's a SHA256 checksum for the compressed file.

pfSense

Get Started Cloud Products Services Support Training Community Download

Latest Stable Version (Community Edition)

This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#).

[RELEASE NOTES](#) [SOURCE CODE](#)

Select Image To Download


Version: 2.4.5-p1

Architecture: AMD64 (64-bit)

Installer: CD Image (ISO) Installer

Mirror: Frankfurt, Germany

[DOWNLOAD](#)

Supported by 

SHA256 Checksum for compressed (.gz) file:
0a09a7748419c86c65eb8d908f584e96d54859aa13f4eeb175a60548c70e228

Subscribe To The Netgate Newsletter

Product information, pfSense software announcements, and special offers. See our [newsletter archive](#) for past announcements.

Email*

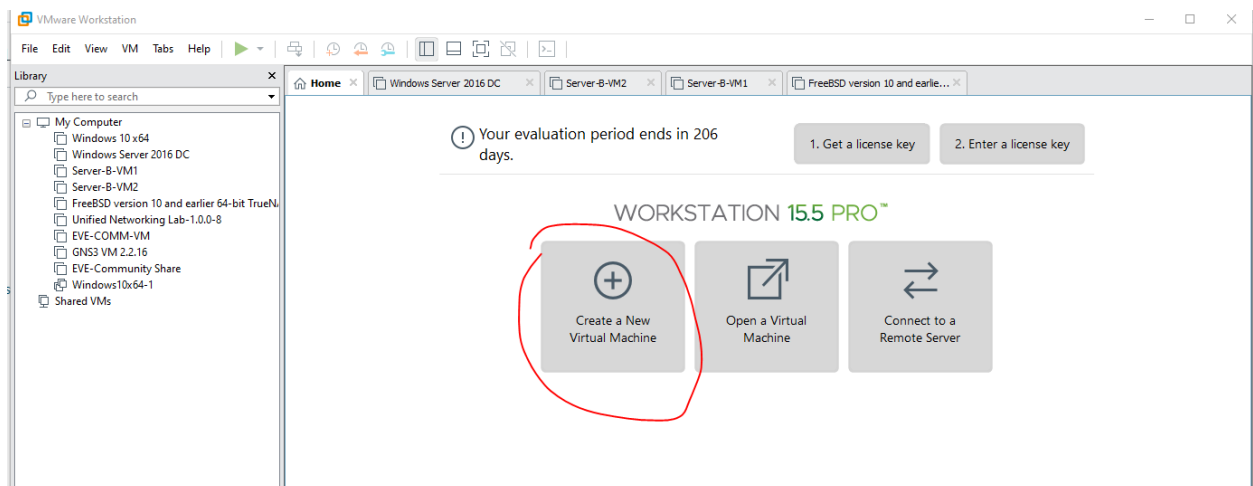
Email Address

☐ I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate.*

[Subscribe](#)

(view our [privacy policy](#))

Daily Snapshots Available



The screenshot shows the VMware Workstation 15.5 Pro interface. The top menu bar includes 'File', 'Edit', 'View', 'VM', 'Tabs', and 'Help'. Below the menu bar is a toolbar with various icons. The left sidebar shows a 'Library' with a search bar and a list of VMs under 'My Computer' and 'Shared VMs'. The main window displays a 'Home' tab with a message: 'Your evaluation period ends in 206 days.' Below this message are two buttons: '1. Get a license key' and '2. Enter a license key'. The main area features three large buttons: 'Create a New Virtual Machine' (highlighted with a red circle), 'Open a Virtual Machine', and 'Connect to a Remote Server'. The text 'WORKSTATION 15.5 PRO™' is displayed above the buttons.

VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer

- Windows 10 x64
- Windows Server 2016 DC
- Server-B-VM1
- Server-B-VM2
- FreeBSD version 10 and earlier 64-bit TrueN
- Unified Networking Lab-1.0.0-8
- EVE-COMM-VM
- GNS3 VM 2.2.16
- EVE-Community Share
- Windows10x64-1

Shared VMs

Home

Windows Server 2016 DC

Server-B-VM2

Server-B-VM1

FreeBSD version 10 and earlie...

! Your evaluation period ends in 206 days.

1. Get a license key 2. Enter a license key

WORKSTATION 15.5 PRO™

Create a New Virtual Machine

Open a Virtual Machine

Connect to a Remote Server

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-RELEASES ▾

☐ 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

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):

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\Metropol...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Add...

Remove

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...

Hardware

Device	Summary
Memory	256 MB
Processors	1
New CD/DVD (IDE)	Using file F:\DISTR\Metropol...
Network Adapter	NAT
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Add...

Remove

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

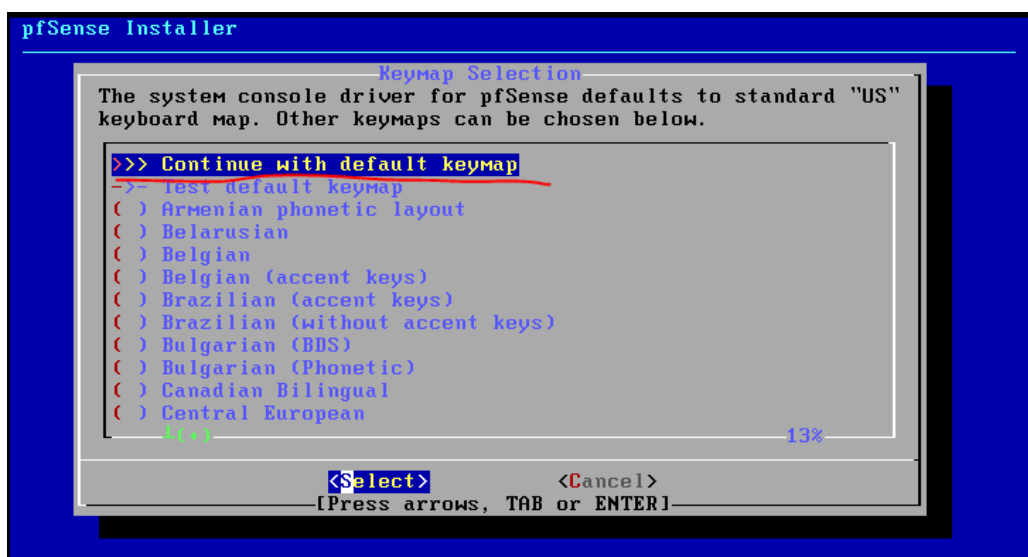
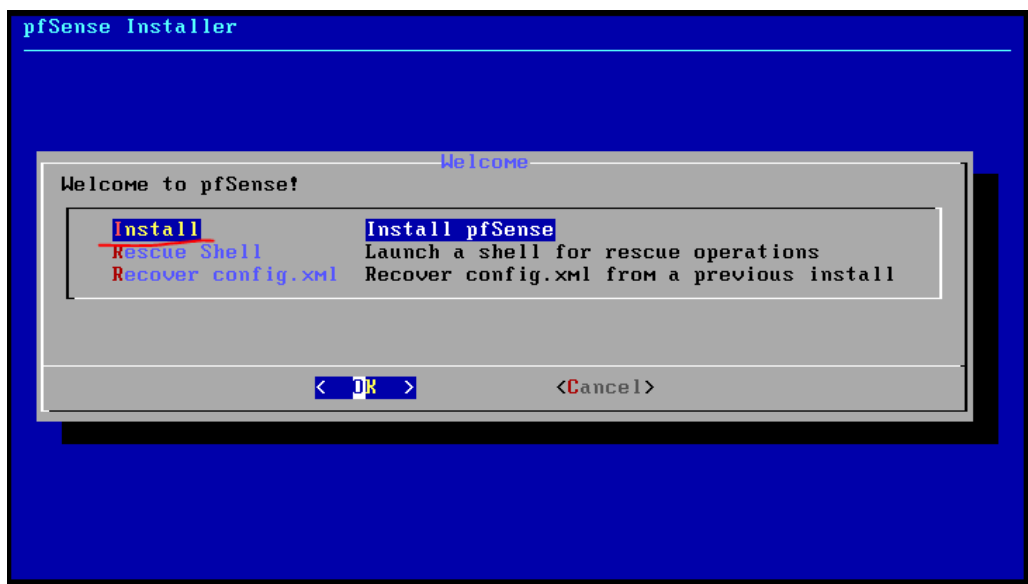
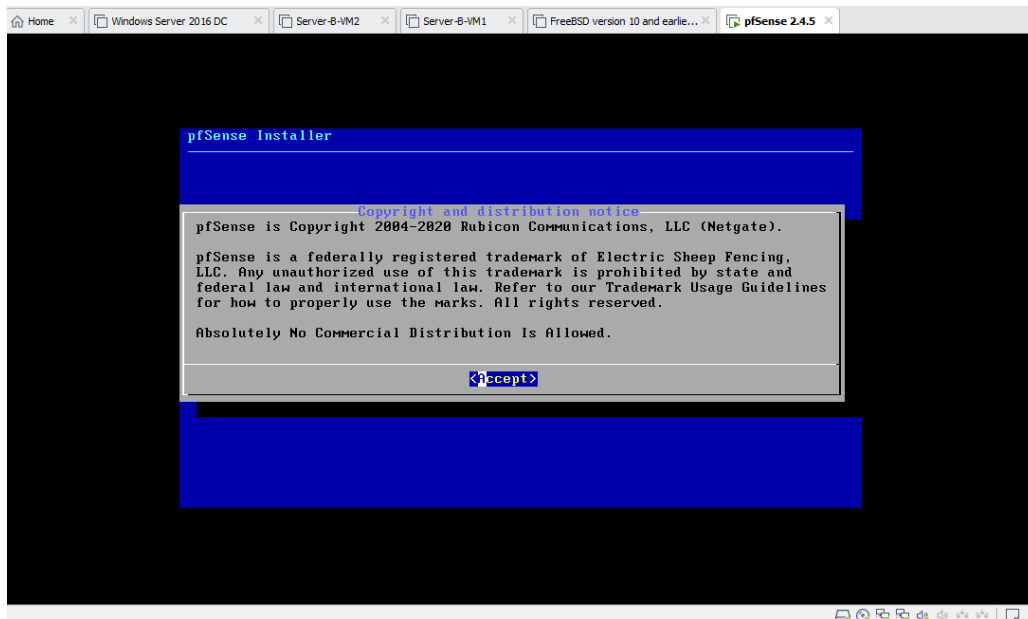
☒ Custom: Specific virtual network

VMnet2 (Host-only)

☐ LAN segment:

LAN Segments...

Advanced...



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 >

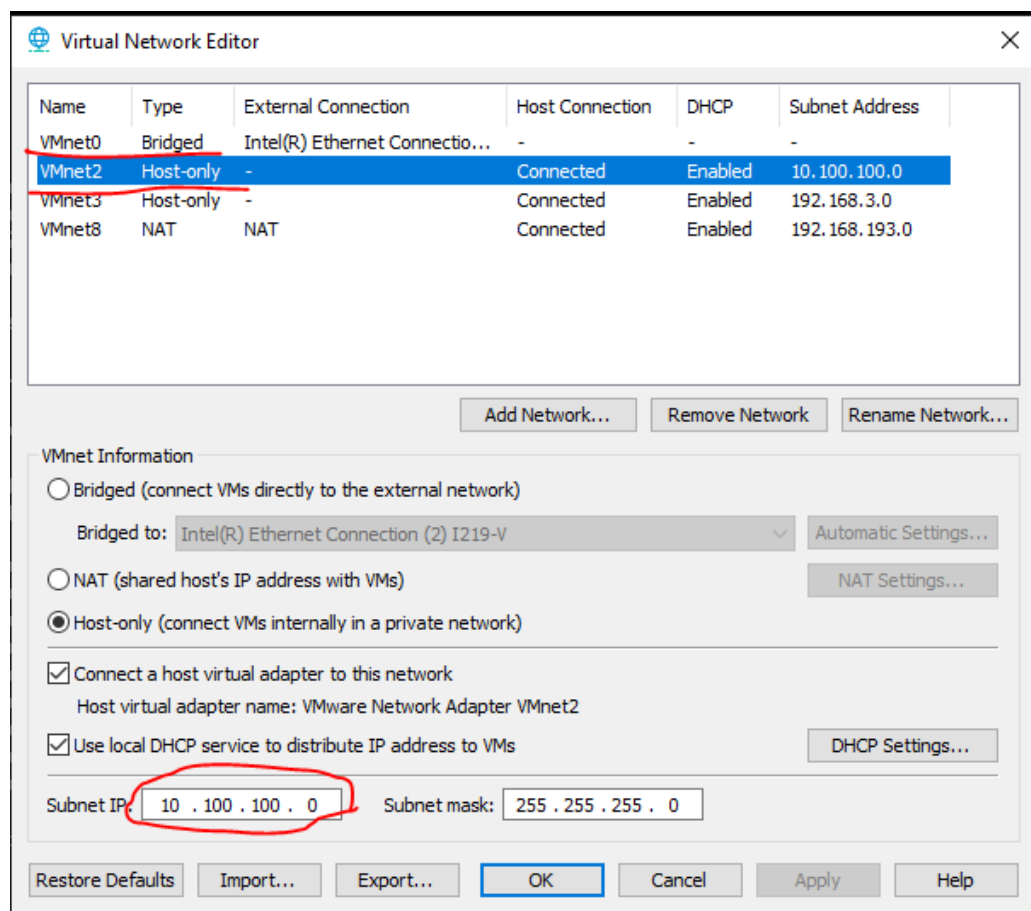
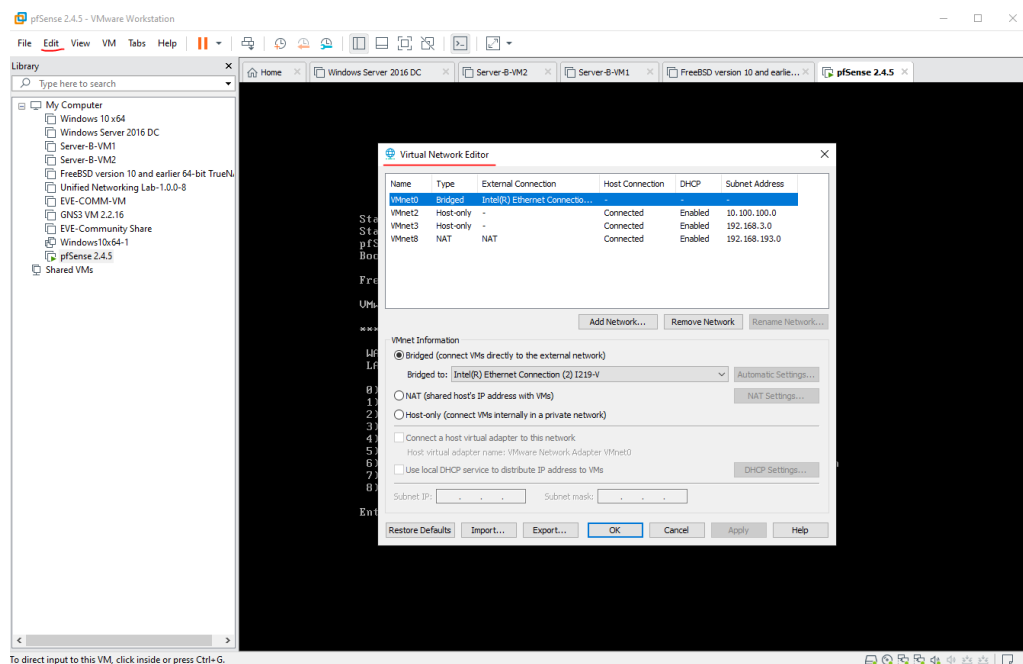
pfSense Installer

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.

Device	Summary
Memory	256 MB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file F:\DISTR\Metropoli...
Network Adapter	<u>Custom (VMnet0)</u>
Network Adapter 2	<u>Custom (VMnet2)</u>
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:

▼

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

```

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: e09c9354b222101ccf3c

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

WAN (wan)      -> em0      -> v4/DHCP4: 86.115.100.100
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: █

```

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

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**

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: 86.115.12.250
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

```

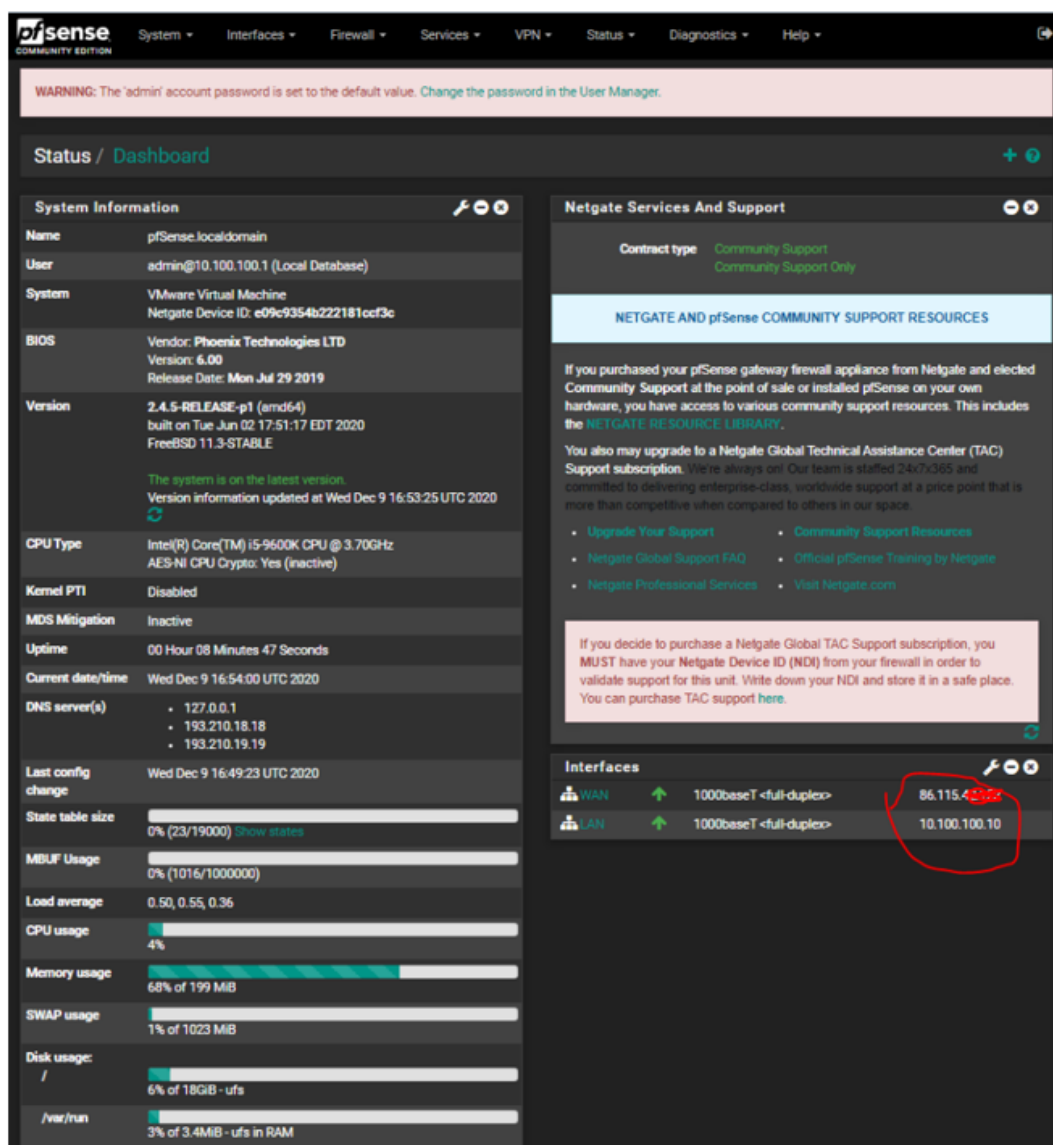
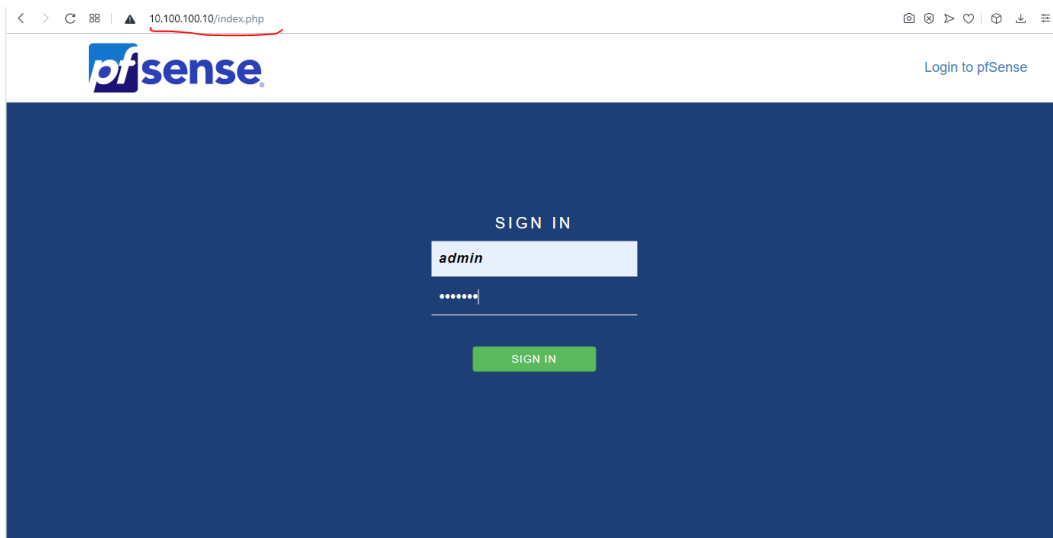
Reverting webConfigurator...

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

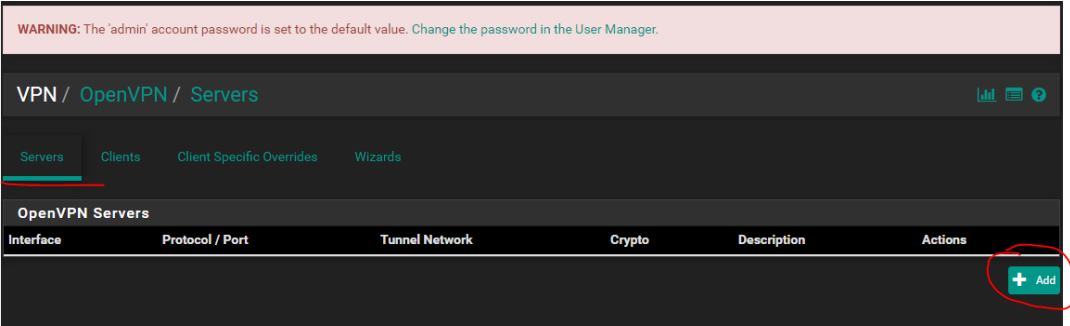
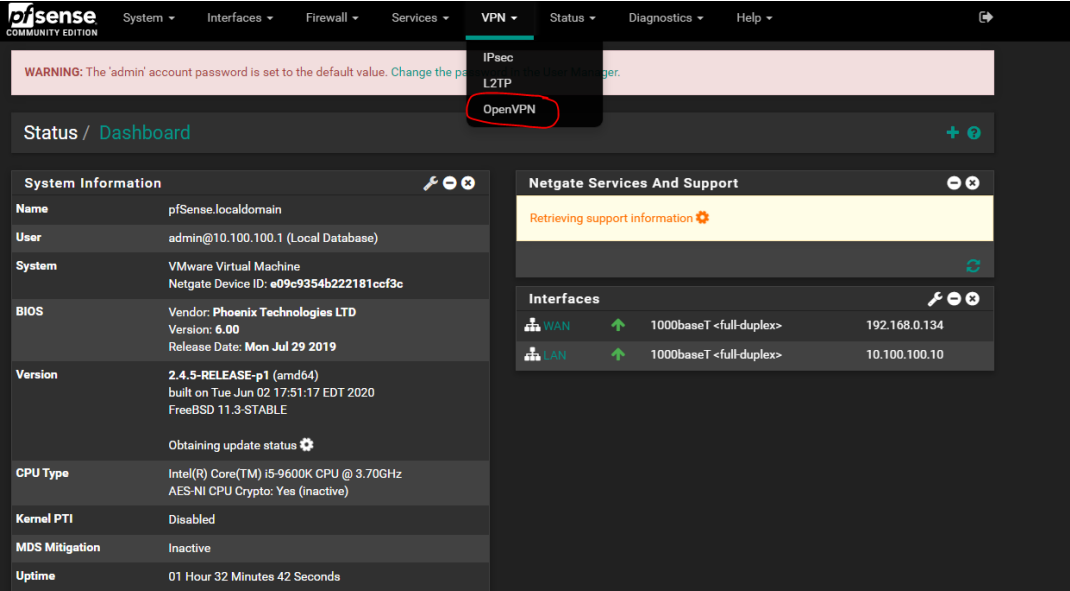
```
VMware Virtual Machine - Netgate Device ID: dc505a299bb7a84e933d
*** Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 82.181.66.135
                v6/DHCP6: 2001:14ba:2bdf:1200:20c:29ff:feeb:bc
9b/64
LAN (lan)      -> em1      -> v4: 192.168.40.10/24
OPT1 (opt1)    -> em2      ->

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:
Message from syslogd@pfSense at Dec  9 13:04:29 ...
pfSense php-fpm[35816]: /vpn_openvpn_server.php: Successful login for user 'admin' from: 192.168.40.1
```

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 [compress:]

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

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)

Available NCP Encryption Algorithms
Click to add or remove an algorithm from the list

AES-128-GCM

Allowed NCP Encryption Algorithms. Click an algorithm name to remove it from the list

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

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

UDP Fast I/O ☐ Use fast I/O operations with UDP writes to tun/tap. Experimental.
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.


Exit Notify Disabled
Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. In Peer-to-Peer Shared Key or with a /30 Tunnel Network, this value controls how many times this instance will attempt to send the exit notification.

Send/Receive Buffer Default
Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

Gateway creation ☐ Both ☒ IPv4 only ☐ IPv6 only
If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level default
Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range






pfsense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾


WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

VPN / OpenVPN / Servers 📊 📄 ⓘ

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	172.16.0.0/24	Crypto: AES-128-CBC/SHA256	Server B-site (tun)	  



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

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / WAN

Floating **WAN** LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/31 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
✗ 0/1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogus networks	⚙

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

↑ Add **↓ Add** **🗑 Delete** **💾 Save** **+ Separator**

Edit Firewall Rule

Action Pass ▾
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface WAN ▾
Choose the interface from which packets must come to match this rule.

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

Protocol UDP ▾
Choose which IP protocol this rule should match.

Source
Source ☐ Invert match any ▾ Source Address ▾ / ▾ ▾

Display Advanced
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination
Destination ☐ Invert match WAN address ▾ Destination Address ▾ / ▾ ▾

Destination Port Range OpenVPN (1194) ▾ From ▾ Custom OpenVPN (1194) ▾ To ▾ Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description Open VPN Server ▾
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options **Display Advanced**

Save

Adding rules for OpenVPN

The screenshot shows the Mikrotik WinBox interface for adding a new firewall rule. The 'OpenVPN' tab is selected in the top navigation bar. Below the tabs, a message states: 'No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.' A red circle highlights the 'Add' button (upward arrow icon) in the bottom right corner of this section.

The 'Edit Firewall Rule' form is displayed below. The 'Action' is set to 'Pass'. The 'Interface' is 'OpenVPN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'Any', which is circled in red. The 'Source' and 'Destination' are both set to 'any'. The 'Description' is 'OpenVPN Allow ALL'. The 'Save' button at the bottom is also circled in red.

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
--------	----------	--------	------	-------------	------	---------	-------	----------	-------------	---------

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface: OpenVPN
Choose the interface from which packets must come to match this rule.

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

Protocol: Any
Choose which IP protocol this rule should match.

Source: ☐ Invert match | any | Source Address

Destination: ☐ Invert match | any | Destination Address

Extra Options

Log: ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: OpenVPN Allow ALL
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: [Display Advanced](#)

Save

Copy the generated shared key for the client.

The screenshot shows the 'Cryptographic Settings' window in Mikrotik WinBox. The 'TLS keydir direction' is set to 'Use default direction'. The 'Shared Key' field contains a 2048-bit static key, which is circled in red. The key is displayed as a hexadecimal string: '2048 bit OpenVPN static key' followed by a long string of characters. The 'Encryption Algorithm' is set to 'AES-128-CBC (128 bit key, 128 bit block)'.

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:
2048 bit OpenVPN static key

-----BEGIN OpenVPN Static key V1-----
93cdce711c3ccb2f63c93446876278ac
Paste the shared key here

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.

The next step is to configure the OpenVPN client

Checking the status of OpenVPN

B-site (Server)

Status / OpenVPN							
Peer to Peer Server Instance Statistics							
Name	Status	Connected Since	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
Server B-site UDP4:1194	up	Wed Dec 9 17:42:27 2020	172.16.0.1	82.181.40.22	0 B	136 B	

N-Site(Client)

Status / OpenVPN							
Client Instance Statistics							
Name	Status	Connected Since	Local Address	Virtual Address	Remote Host	Bytes Sent/Received	Service
Client UDP4	up	Wed Dec 9 17:41:16 2020	82.181.60.179:62489	172.16.0.2	86.115.42.122:1194	956 B / 136 B	

Adding rules B-site

Firewall -> NAT -> Outbound

Firewall / NAT / Outbound

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

Port Forward1:1OutboundNAT

Outbound NAT Mode

Mode

☒

☐

☐

☐

Automatic outbound NAT rule generation.
(IPsec passthrough included)

Hybrid Outbound NAT rule generation.
(Automatic Outbound NAT + rules below)

Manual Outbound NAT rule generation.
(ADON - Advanced Outbound NAT)

Disable Outbound NAT rule generation.
(No Outbound NAT rules)

Save

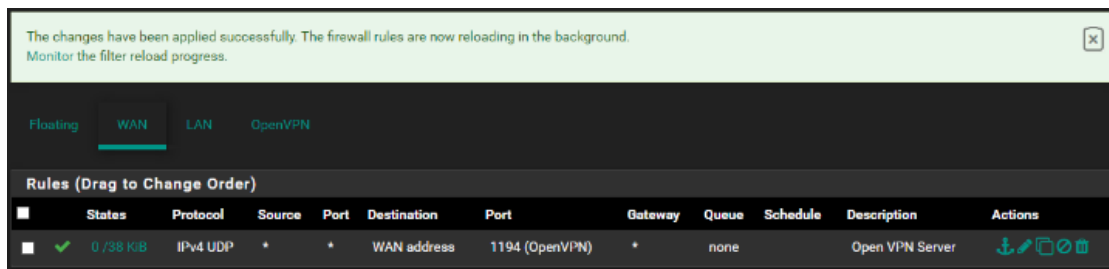
Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
									<div> Add Add Delete Save</div>

Automatic Rules:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓ WAN	172.16.0.0/24 - 172.16.0.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓ WAN	172.16.0.0/24 - 172.16.0.0/24	*	*	*	WAN address	*		Auto created rule

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.

Rules (Drag to Change Order)											
■	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
■	✓ 2 / 2.56 MiB	*	*	*	LAN Address	80	*	*		Anti-Logout Rule	⚙️
■	✓ 9 / 236.22 MiB	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule	📌 ⚙️ 🗑️
■	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 ⚙️ 🗑️

Firewall, Rules, OpenVPN

Rules (Drag to Change Order)											
■	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
■	✓ 0 / 2 KiB	IPv4 ICMP any	*	*	*	*	*	none			📌 ⚙️ 🗑️
■	✓ 0 / 5 KiB	IPv4 *	*	*	*	*	*	none		OpenVPN Allow ALL	📌 ⚙️ 🗑️

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-T01Q4VR8991.000>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

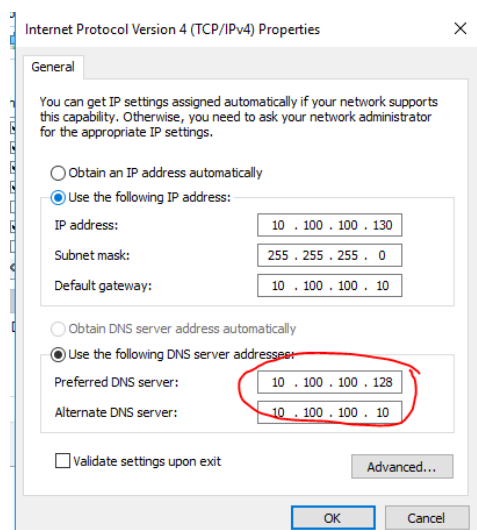
Ping statistics for 192.168.40.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 37ms, Average = 33ms

C:\Users\Administrator.WIN-T01Q4VR8991.000>
```

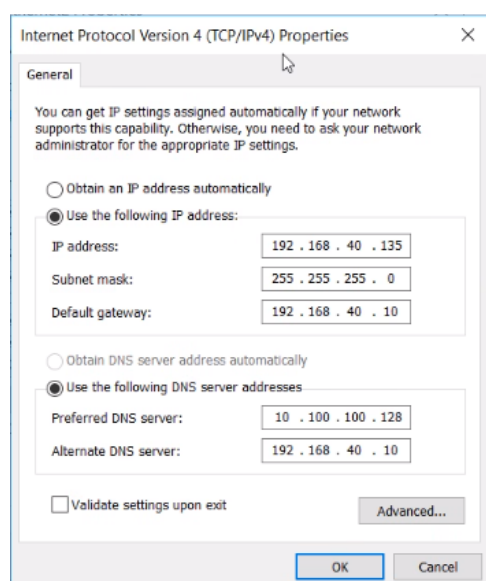
Now we are adding servers to the Domain Controller

Before that, the DNS settings must be added as well

B-Site



N-Site



The setting of TrueNas VM

Hostname and Domain

Hostname
truenas

Domain
banart.localdomain

Additional Domains
banart.localdomain

Service Announcement

☐ NetBIOS-NS

☒ mDNS

☒ WS-Discovery

DNS Servers

Nameserver 1
10.100.100.128

Nameserver 2
10.100.100.10

Nameserver 3

Default Gateway

IPv4 Default Gateway
10.100.100.10

IPv6 Default Gateway

Other Settings

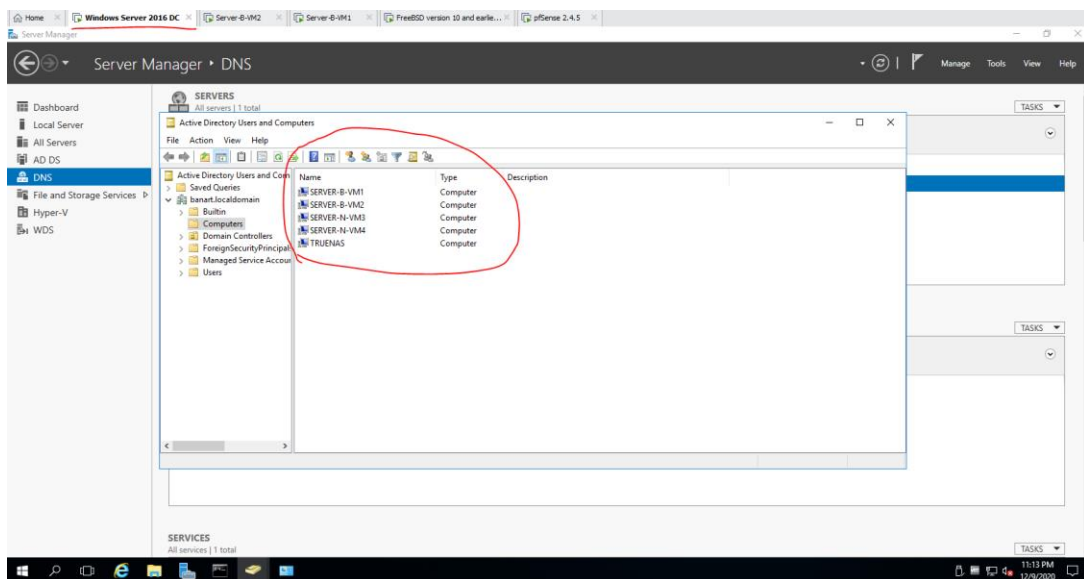
HTTP Proxy

☐ Enable Netwait Feature

Host Name Database

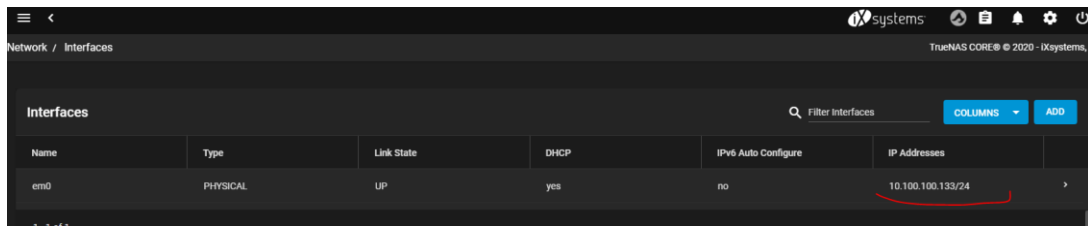
SAVE

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

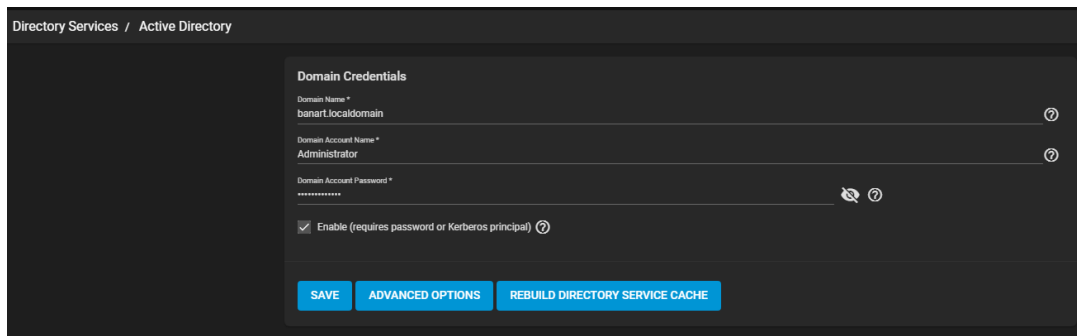


Configuring TrueNAS VM

Adding a static IP address to the TrueNAS VM

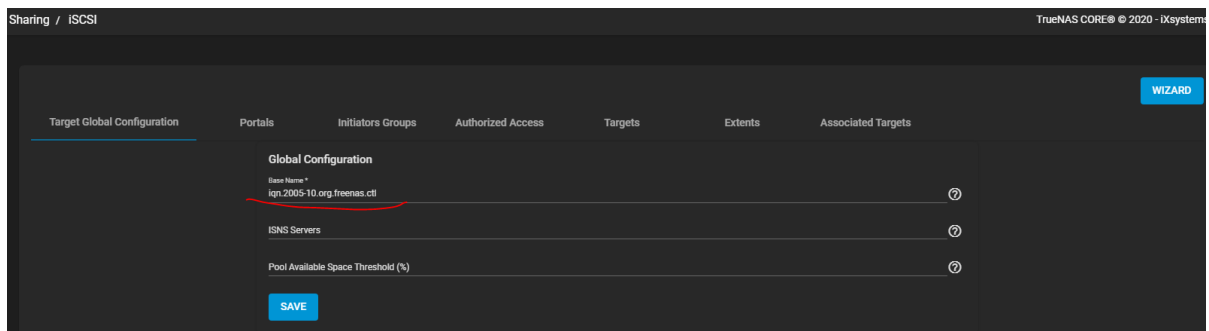
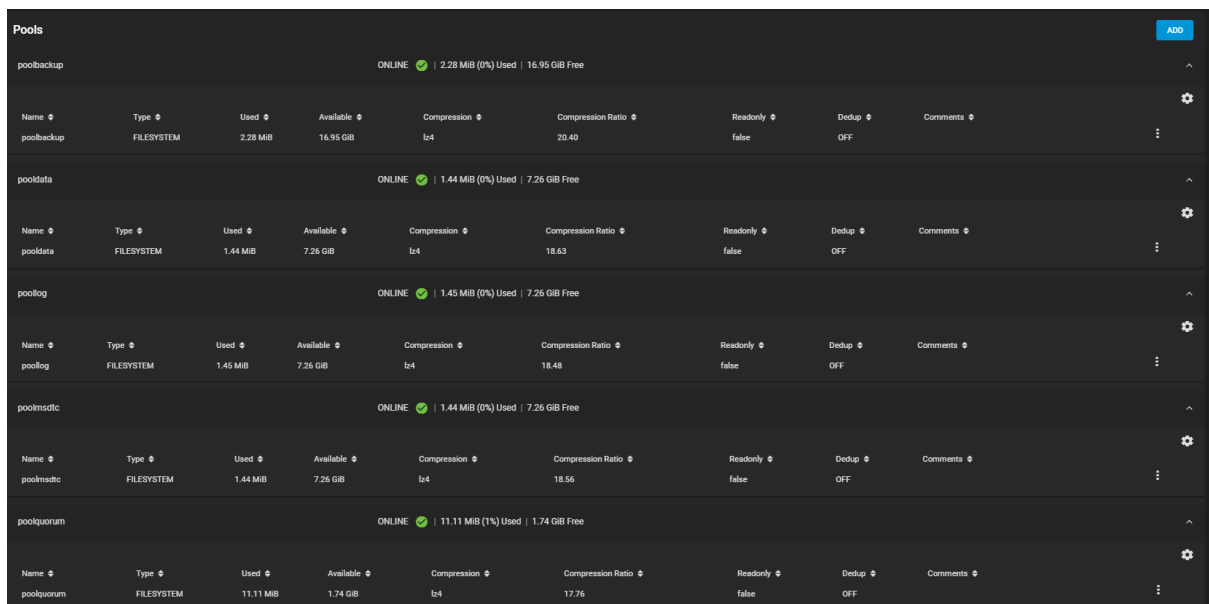


Adding TrueNAS VM to the Active Directory



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 ConfigurationPortalsInitiators GroupsAuthorized AccessTargetsExtentsAssociated Targets

Portals

Filter Portals

COLUMNSADD

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 / EditTrueNAS CORE © 2020 - iXsystems

☒ Allow All Initiators

Connected Initiators

Allowed Initiators (IQN)

Authorized Networks

Description

SAVECANCEL

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

SAVECANCEL

ADD

Sharing / iSCSITrueNAS CORE © 2020 - iXsystems

Target Global ConfigurationPortalsInitiators GroupsAuthorized AccessTargetsExtentsAssociated TargetsWIZARD

Extents

Filter Extents

COLUMNSADD

Extent Name	Description	Serial	NAA	Enabled	
backupext		000c29d51f3d004	0x6589cfc000000200489c23cae278a0t	yes	
dataext		000c29d51f3d001	0x6589cfc0000007453dc4f2557e5252c	yes	
logext		000c29d51f3d002	0x6589cfc00000072d8d9e3392b54bcf6	yes	
msdtcext		000c29d51f3d003	0x6589cfc00000062f91f9c75069e284ft	yes	
quorumext		000c29d51f3d000	0x6589cfc000000c6da5ed22dcafe9e37	yes	

1 - 5 of 5

Sharing / iSCSI

TrueNAS CORE © 2020 - iXsystems

Target Global Configuration

Portals

Initiators Groups

Authorized Access

Targets

Extents

Associated Targets

WIZARD

Associated Targets

Filter Associated Targets

COLUMNS

ADD

Target	LUN ID	Extent	
pooldisks	1	quorunext	⋮
pooldisks	2	dataext	⋮
pooldisks	3	logext	⋮
pooldisks	4	msdtcext	⋮
pooldisks	5	backupext	⋮

1 - 5 of 5

Target Global Configuration

Portals

Initiators Groups

Authorized Access

Targets

Extents

Associated Targets

WIZARD

Extents

Filter Extents

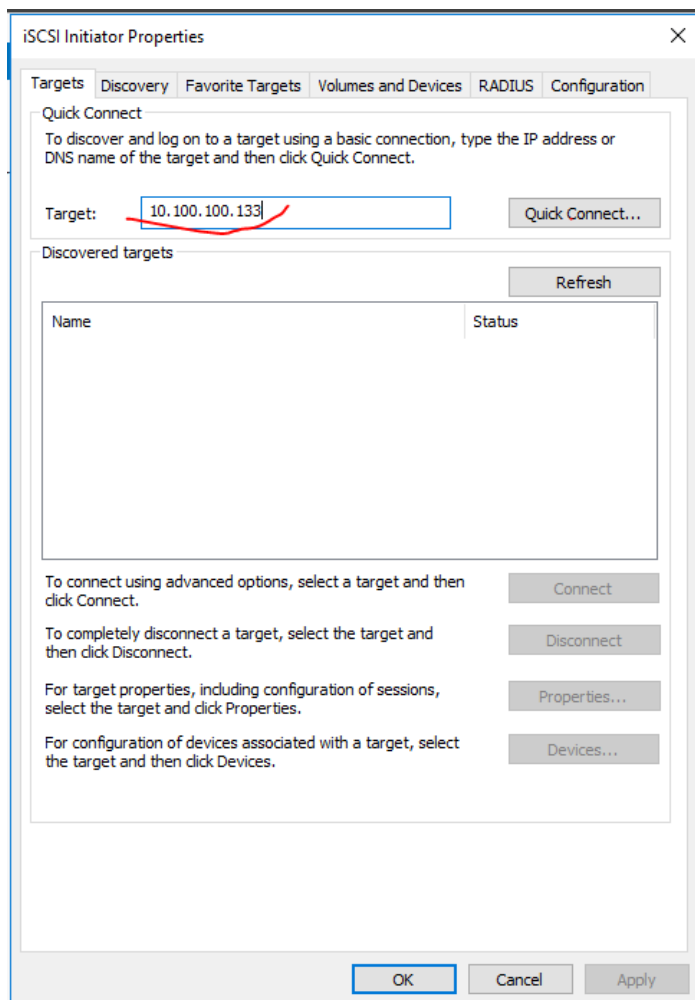
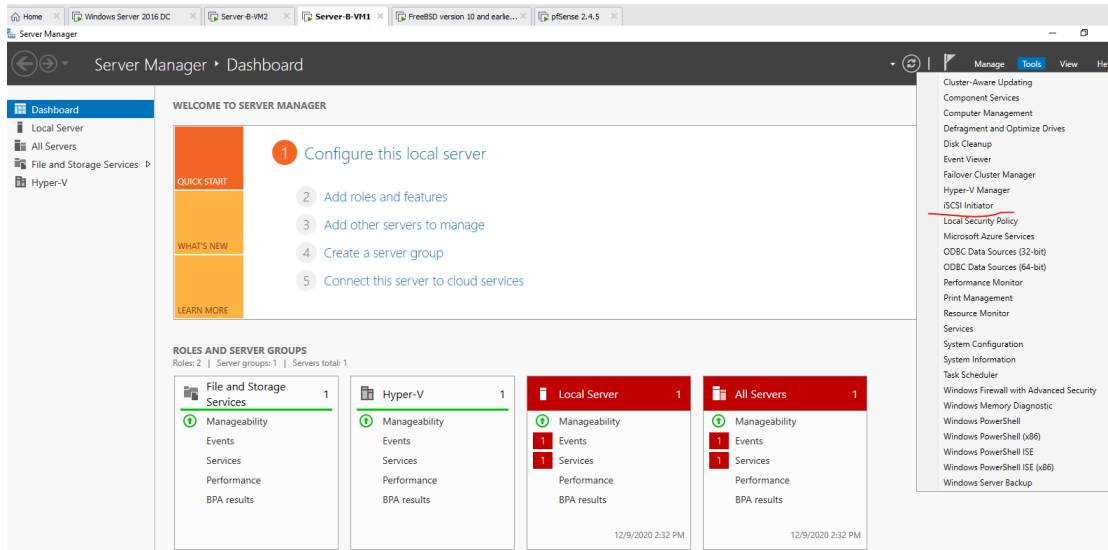
COLUMNS

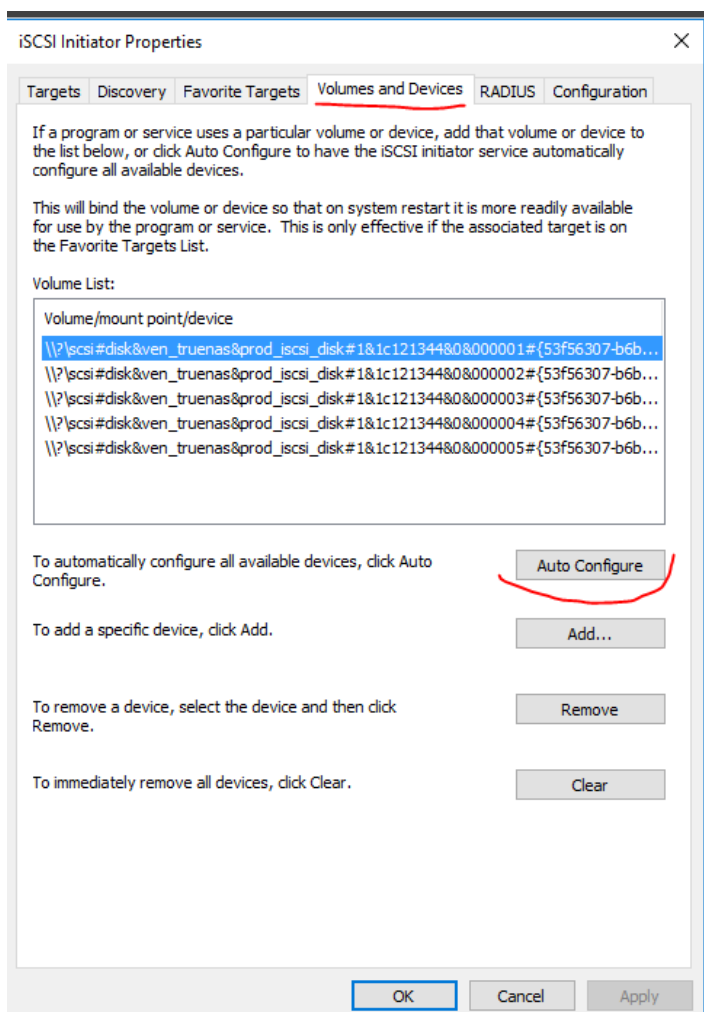
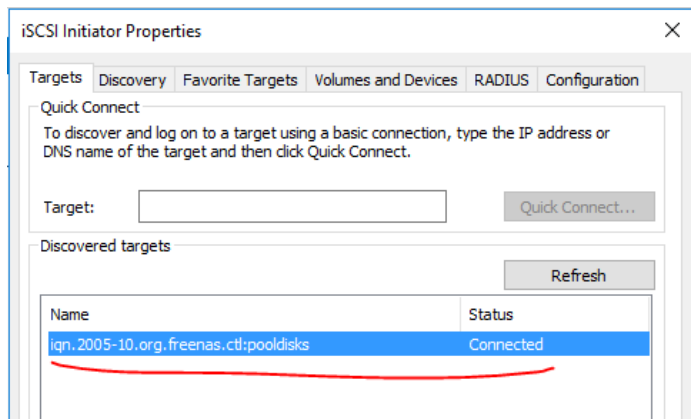
ADD

Extent Name	Description	Serial	NAA	Enabled	
backupext		000c29d51f3d004	0x6589cfc000000200489c23cae278a0t	yes	⋮
dataext		000c29d51f3d001	0x6589cfc0000007453dc4f2557e5252c	yes	⋮
logext		000c29d51f3d002	0x6589cfc00000072d8d9c3392b54bcfs	yes	⋮
msdtcext		000c29d51f3d003	0x6589cfc00000062f91f9c750696284fc	yes	⋮
quorunext		000c29d51f3d000	0x6589cfc000000c6da5ed22dcafe9e37	yes	⋮

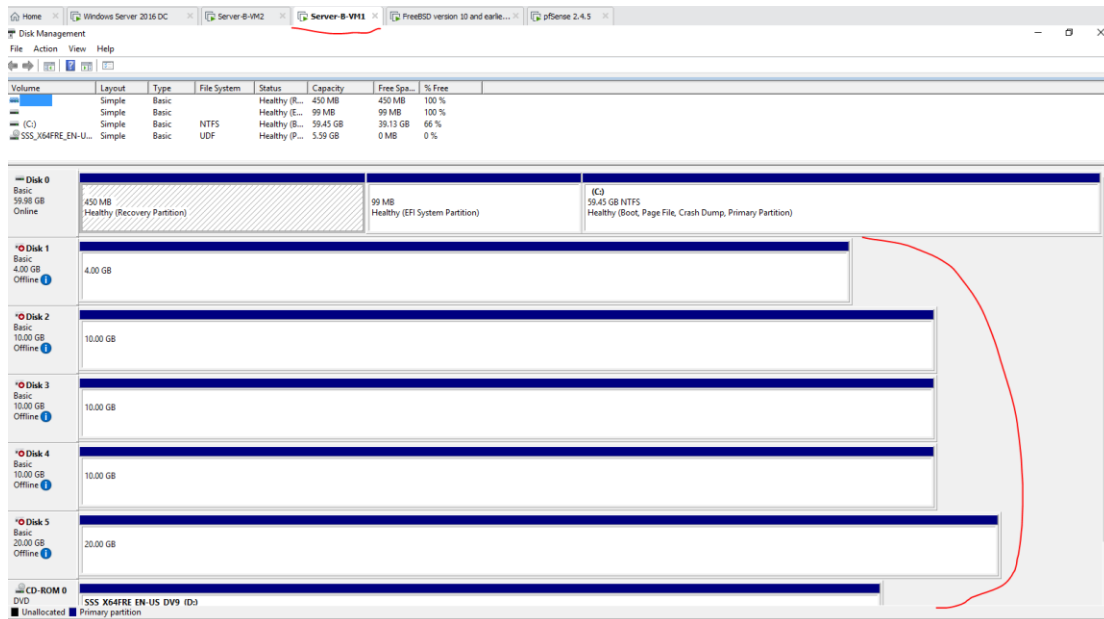
1 - 5 of 5

Adding Disks from TrueNAS

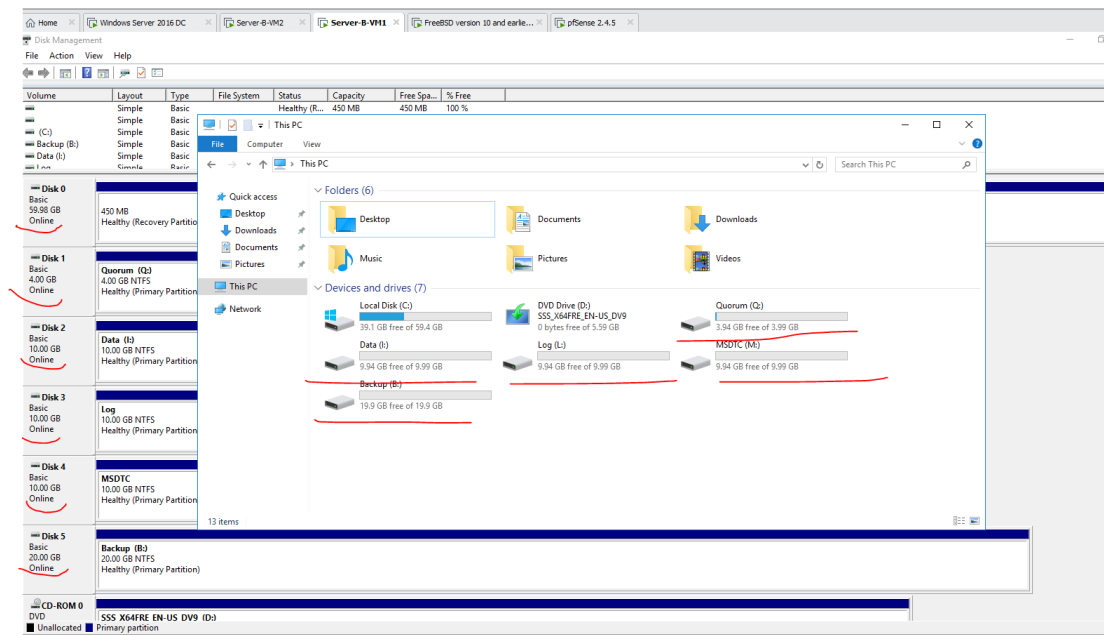




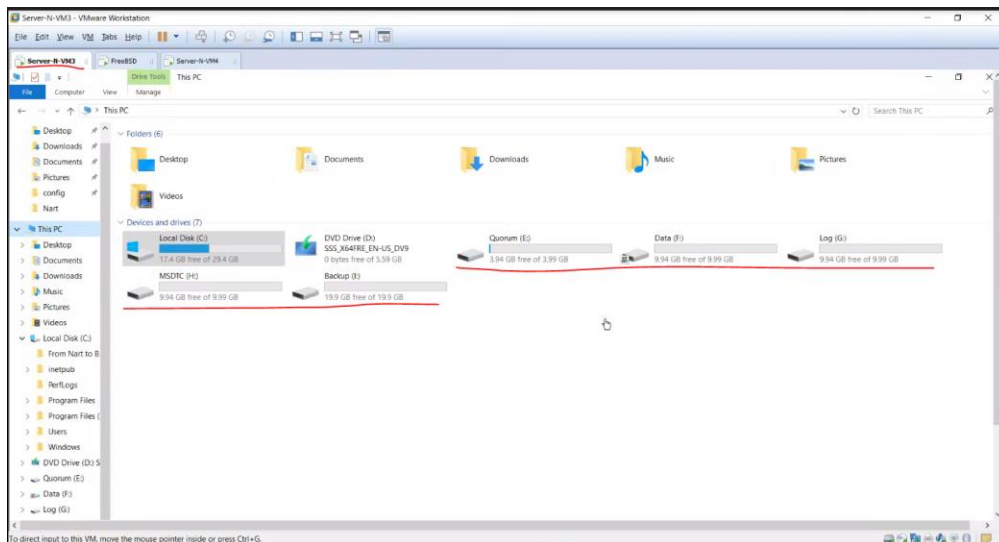
After adding all disks to the Disk Management, they must be formatted (preferred GPT format) only once. The same process must be applied to all servers (Failover Nodes) except the DC server.



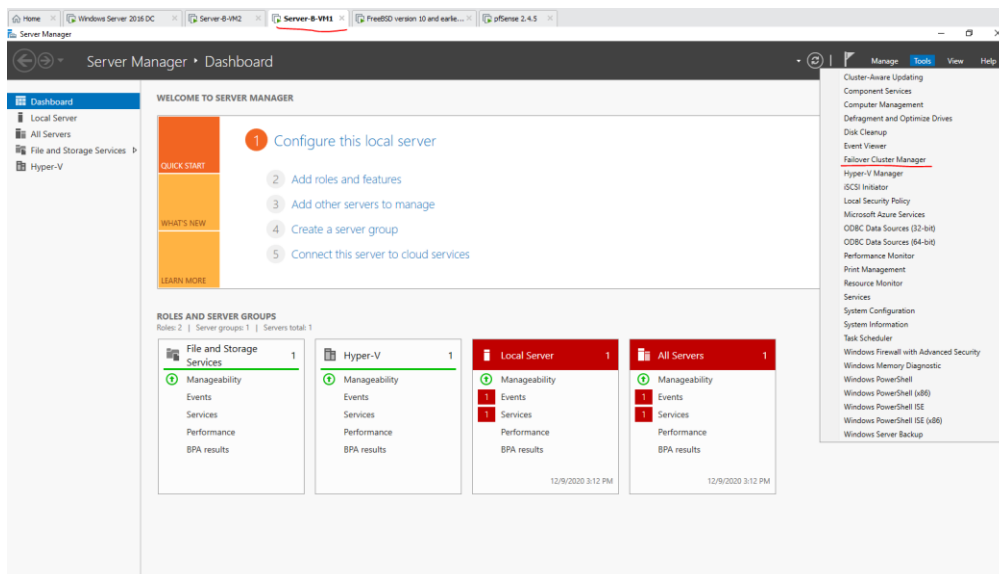
After that, the disk must be turned Online. Then they will be shown as a usual disk on the PC B-Site Server-B-VM1.

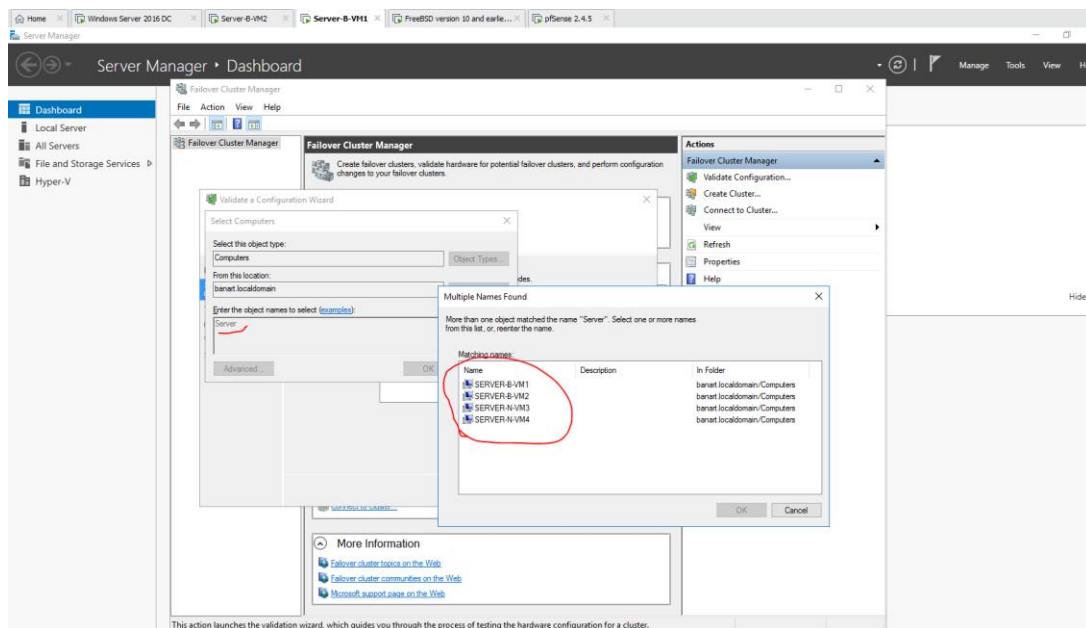
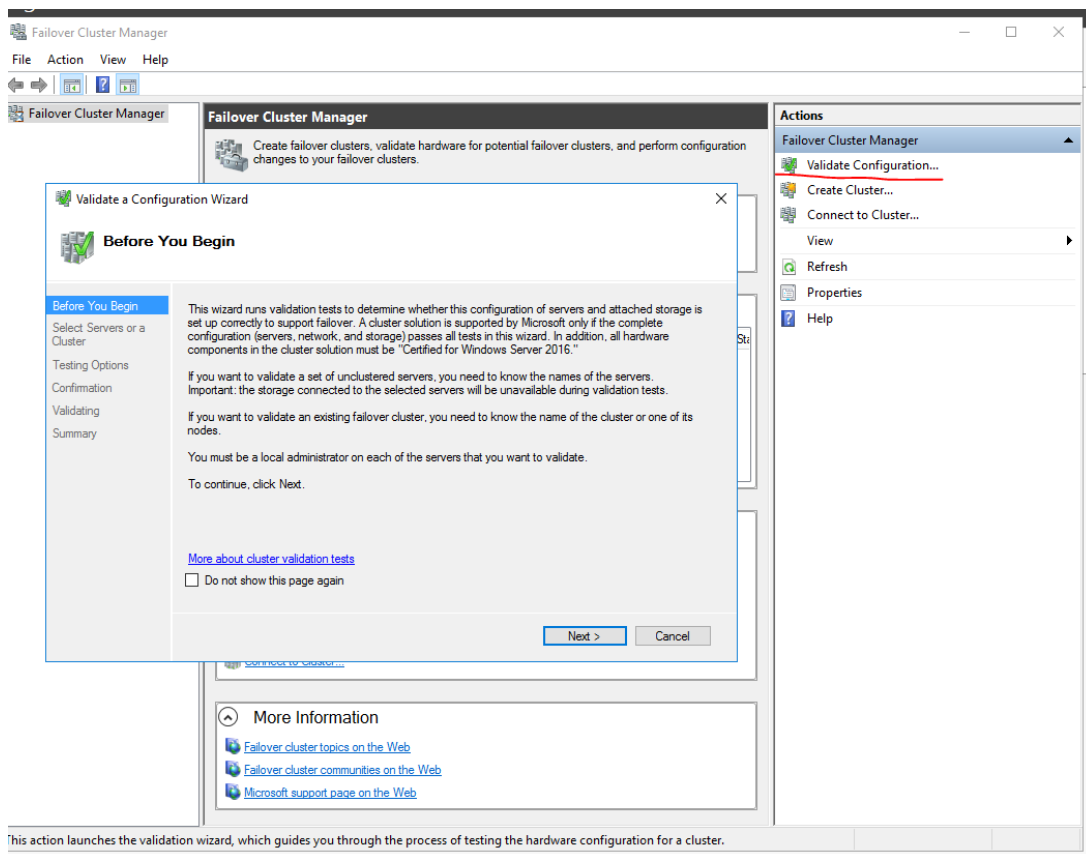


N-Site Server-N-VM3



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>