

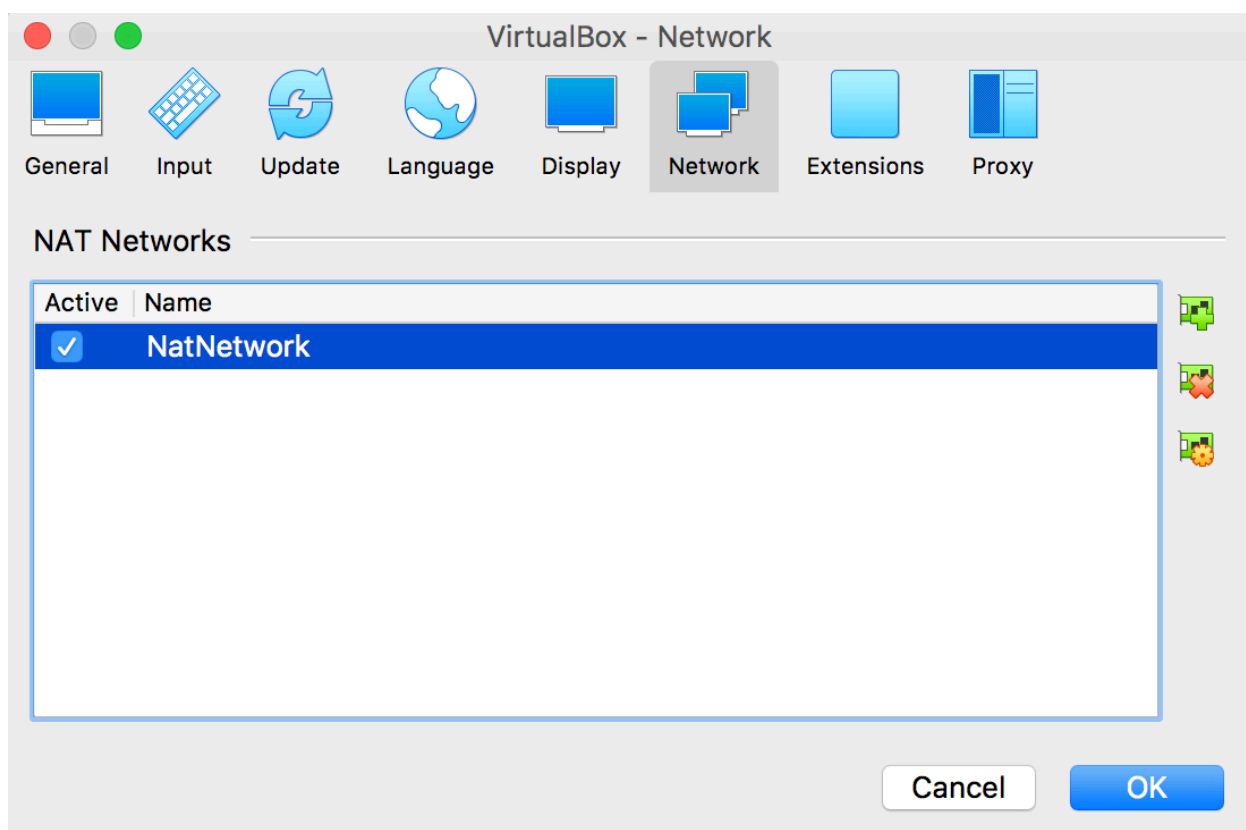
Remote Access Services

This document is divided in the following three main sections.

- A) Pre-Installation Configuration and Overview (**Read first**)
- B) Installations Section
- C) Configuration Section

It is important to follow the instructions as describe in this document to ensure the virtual infrastructure is properly set up for this lab and future used. This lab will serve as the cornerstone for our labs virtual environment. Part I (this document) will consists of setting the environment and Part II (future document) will focus on both offensive and defensive security.

We recommend reading information in this document entirely before proceeding with the installation and configuration for this lab. It is better to have an overall view and understanding of all steps that will required for successfully setting this virtual environments. Futures



labs will be develop utilizing this environment and will demonstrate some aspects about cyber forensic and cyber security.

The table of contents is empty because you aren't using the paragraph styles set to appear in it.

Table of Contents

Pre-Installation Configuration.....3

Installation Section.....7

Configuration Section.....17

External Resources

<https://blogs.technet.microsoft.com/rasblog/>

<https://blogs.technet.microsoft.com/rasblog/2009/03/17/remote-access-design-guidelines-part-1-overview/>

<https://social.technet.microsoft.com/wiki/contents/articles/37890.windows-server-2016-installation.aspx>

<https://www.wikihow.com/Install-Windows-10-in-VirtualBox>

<https://blogs.technet.microsoft.com/canitpro/2015/04/01/step-by-step-installing-windows-10-on-oracle-virtualbox/>

<https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/>

<https://youtu.be/1xAXqmN9tiU>

PRE-INSTALLATION CONFIGURATION

Oracle VirtualBox Configuration

- 1) One VirtualBox Network - Select the following Menu Options to create and NatNetwork and assign the following IP network (10.0.2.0/24)

VirtualBox / Preferences / Network - Virtual Box Menu Options

VirtualBox File Machine Window Help

- a) NatNetwork
10.0.2.0/24

Create or modify your existing Nat Networks based on the information provided above.

This NatNetwork will be assign to the following VMs

- 1) Endian Firewall/Router (bridged)
- 2) Windows 10 Remote Client (**only when testing RAS server**) - This windows 10 remote client will be configure in two different networks during the lab depending on the functions it will performed. (Administrator Client virtual machine when working on the internal network, and when accessing the network remotely using the windows VPN services.

- b) Three Host Networks

- 1) vboxnet0 - this network is the internal network for our secure server infrastructure. (PDC)
192.168.56.0/24
dhcp option enabled

2) vboxnet1 - this network is the internal network for our DMZ perimeter. (RAS)

192.168.57.0/24

dhcp option disable

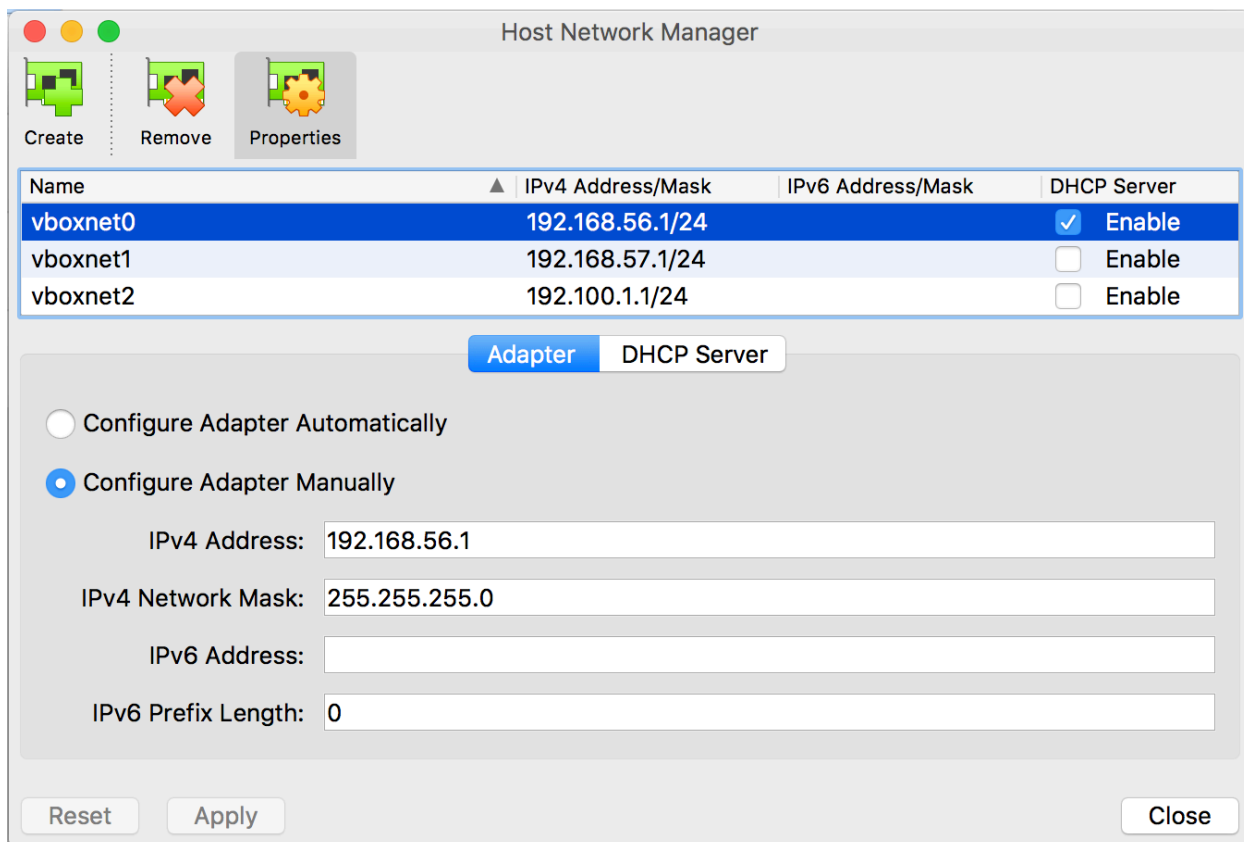
3) vboxnet2 - this network is the WAN network for our DMZ perimeter. (RAS)

192.100.1.0/24

dhcp option disable

VirtualBox File Machine Window Help

File / Host Network Manager / create - Virtual Box Manu Options



Host Network Manager

Create Remove Properties

Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
vboxnet0	192.168.56.1/24		<input checked="" type="checkbox"/> Enable
vboxnet1	192.168.57.1/24		<input type="checkbox"/> Enable
vboxnet2	192.100.1.1/24		<input type="checkbox"/> Enable

Adapter DHCP Server

☐ Configure Adapter Automatically

☒ Configure Adapter Manually

IPv4 Address: 192.168.56.1

IPv4 Network Mask: 255.255.255.0

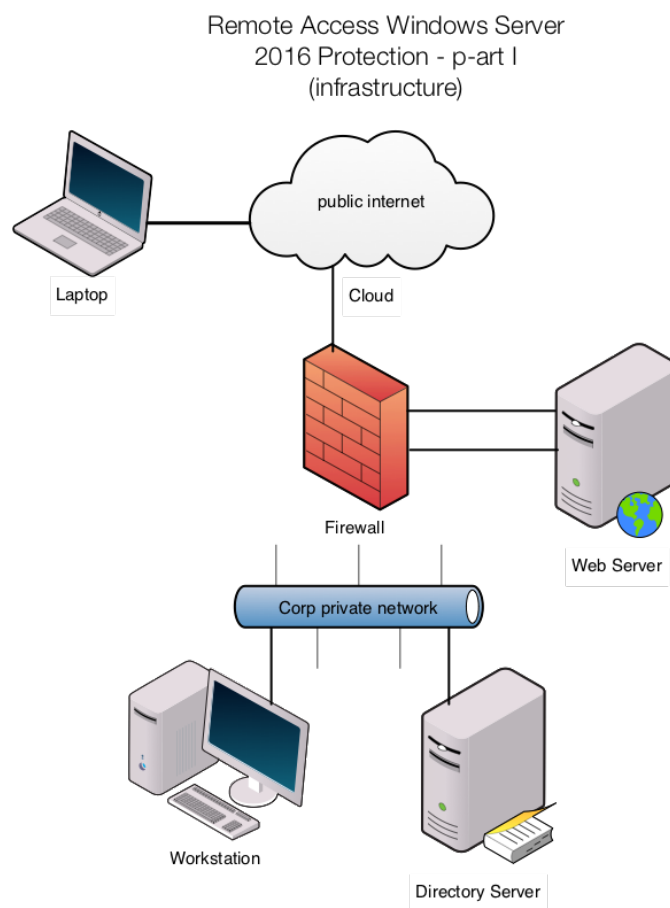
IPv6 Address:

IPv6 Prefix Length: 0

Reset Apply Close

Note: The following information is provided as an overview of the assignment and attachment of virtual networks during the installation. Not action is required below this point the pre-configuration. You might need to make reference later to this information.

The ip networks and vboxnet0 and vboxnet1 adapters are default configuration for virtualbox, Please, note that vboxnet2 is not a default IP addresses and must be a public ip address for VPN configuration on RAS server to work.



FW/Router (endian fw)

Four Network Adapters will be assigned to Endian FW/Router VM. It's recommended to assign two adapters when installation the firewall and configured them during the installation configuration steps. We will identify the adapters and networks as RED, GREEN, ORANGE and BLUE on Endian. The following four adapters will be configured for Endian FW/Router Virtual Machine. (the following screenshots are only available after creating FWR VM for Endian)

The windows 10 vm will be assign to vboxnet0 and dhcp configuration will be required (default on windows 10 vm)

Two Windows 2016 Standard servers will be install and configure with one or two network adapters as follow.

 pdc server
 vboxnet0 (only one interface attach and configure on primary domain controller)

 ras server
 vboxnet1 (internal)
 vboxnet2 (WAN)

End of section: Pre-Configuration and Overview.

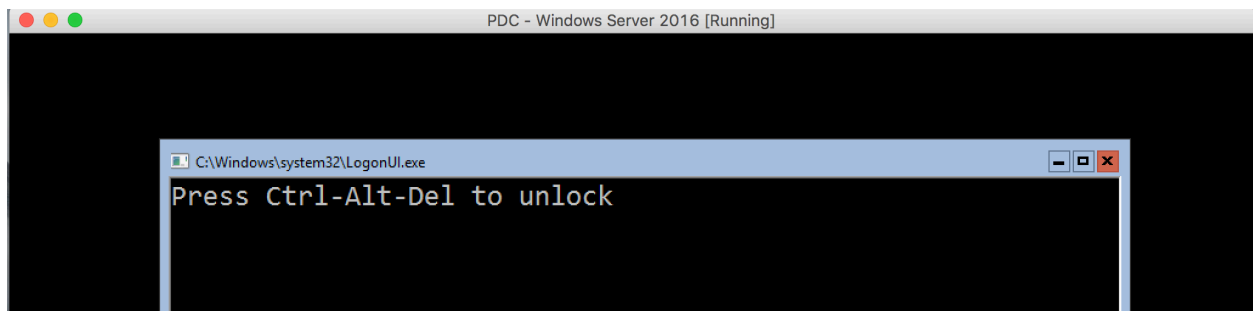
INSTALLATIONS SECTION

Instructions for Windows Servers (PDC1, RAS Server)

- 1) Create two NEW VM on VirtualBox for Windows Server 2016
- 2) Add ISO to New Windows Server 2016 Storage (download ISO file)
- 3) follow the steps listed on the following document (**select Installation desktop experience**)
- 4) the same steps must be follow for two VMs (PDC1, RAS)

<https://social.technet.microsoft.com/wiki/contents/articles/37890.windows-server-2016-installation.aspx>

In our example, we selected Windows Server 2016 Evaluation (desktop experienced)



Once the installation is completed the screen above will display when the VM from VirtualBox is started and **core server without desktop experience was selected during the installation**. You will be able to login with the administrator password to perform network configuration, adding windows services, troubleshoot and validate configuration. You could opt to continue with the configuration of the first server or continue

preparing the virtual infrastructure by adding the other vm machines required for the lab.

Note: follow the exact instructions for **two windows server installations**. Below we will provide configuration instructions under Configuration Section for both windows servers (primary domain controller and the remote access server). The installation instructions are identical for both servers.

HOW TO LOGIN? (instructions)

VirtualBox (Menu Bar Options)

VirtualBox VM	Machine	View	Input	Devices	Window	Help
----------------------	---------	------	-------	---------	--------	------

Input —> Keyboard —> Insert Ctrl-Alt-Del to login to Windows Servers.

Note: this menu bar options are available only if you have an active running virtual machine.

Instructions for Windows 10 Client Installation

A Windows 10 Client VM is required for this lab. The Windows 10 Client VM will have twofold purpose. First, the Client will be utilized for accessing the Firewall (Endian FW/Router) web application and make configuration changes to it. In addition, the Windows 10 Client VM will be configured to access the internal network from a remote network (in a virtual environment). We will be providing configuration instructions for Windows 10 Client RAS/VPN access.

Follow the steps by steps Windows Client Installation on VirtualBox by using either one of the following links.

<https://www.wikihow.com/Install-Windows-10-in-VirtualBox>

<https://blogs.technet.microsoft.com/canitpro/2015/04/01/step-by-step-installing-windows-10-on-oracle-virtualbox/>

Once the installation is completed the virtual machine for windows 10 client is ready for installation. The installation steps are listed under the configuration section on page 24.

Instructions for Endian Community Firewall/ Router Installation

The installation of Endian Community Firewall is very simple installation. Once the software is downloaded and stored in your local hard drive, use VirtualBox to create a VM for Linux.

Create New Virtual Machine

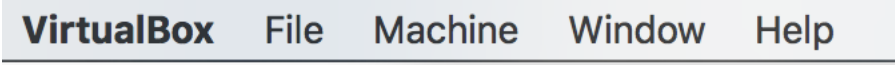
Once you have the Endian Firewall ISO downloaded, launch VirtualBox and create a new virtual machine. In this guide, we are going to setup EFW with the following minimum requirements;

- 8GB storage disk
- 2GB RAM
- 1 CPU cores
- At least two network interface cards. This guide uses 4 interfaces (LAN, WAN, DMZ, DMZ-WAN) for complete configuration.
 - First Interface: GREEN Zone (LAN) – Internal network
 - Second Interface: RED Zone (WAN) – **NAT**
 - Third Interface: ORANGE Zone (DMZ) – Internal network
 - Four Interface: BLUE Zone (DMZ-WAN) - Internal network

VirtualBox (Manu Bar options)

Select Machines from VirtualBox Menu Bar then click on New

VirtualBox Menu Bar —> Machines —> New



VirtualBox File Machine Window Help

The Endian Firewall will require four VirtualBox Network Interfaces. Ensure that Endian VM setting is property configured as described in the above section under FW/Router (Endian/FW) pre-configuration.

Select your New VM (Endian/FW), right click and select Setting then select the Network Options.

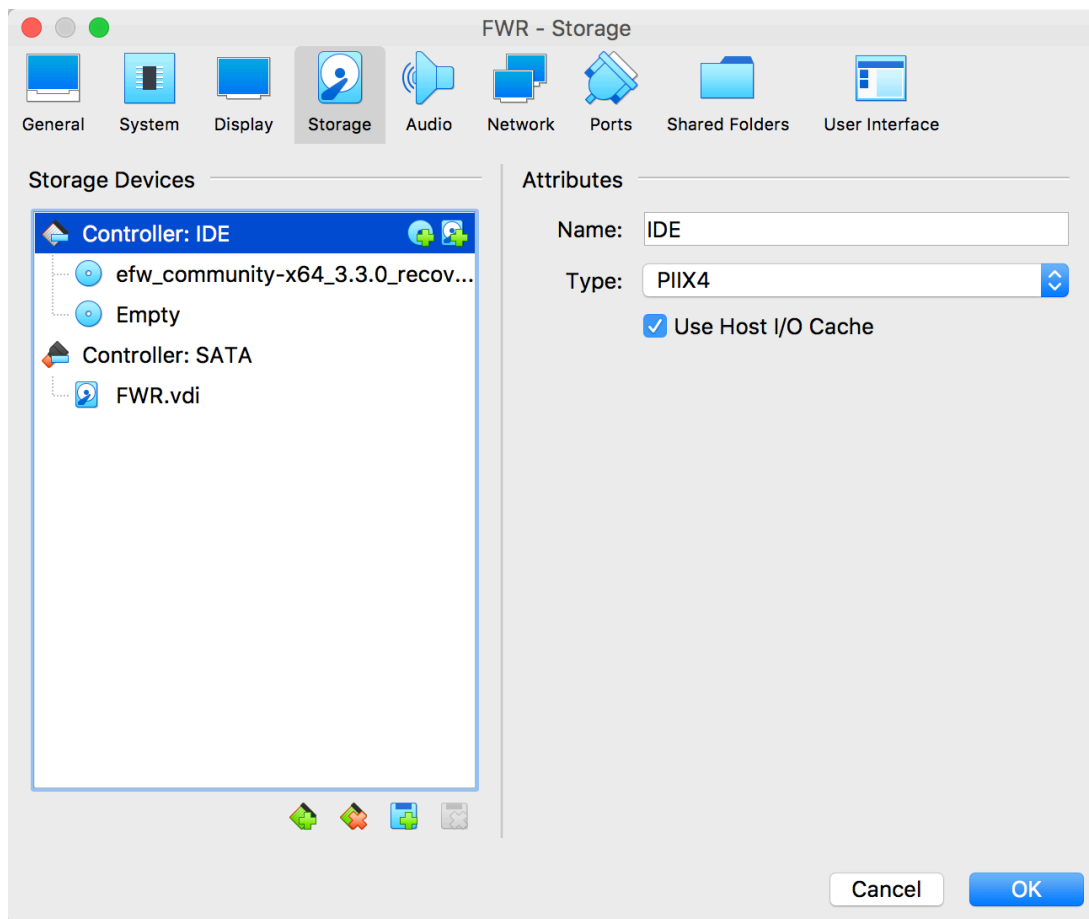
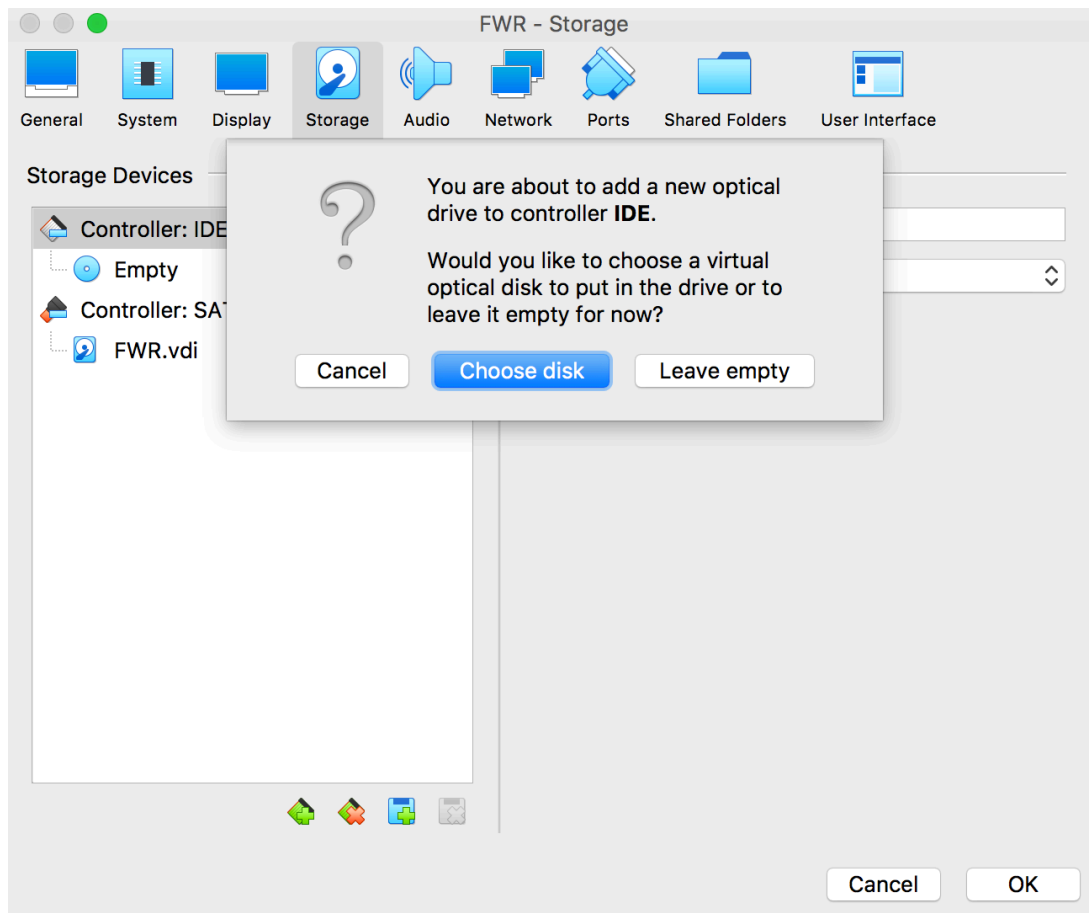
You must ensure that each of the Network Adapters are assigned and attached to the correct VM Hosts Networks as listed under VirtualBox Pre-Installation Configuration.

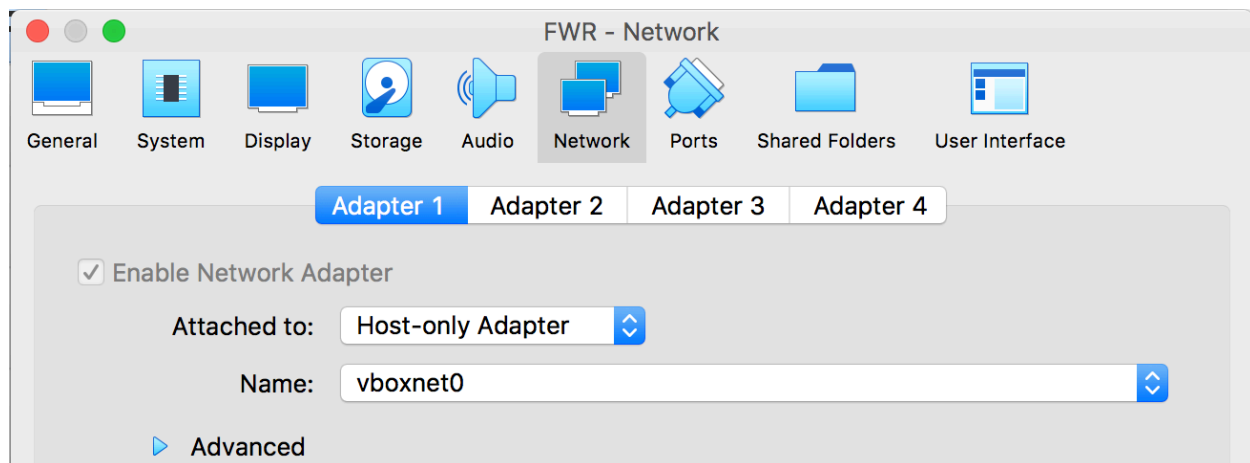
Once you have created a new virtual machine, mount the Endian Firewall ISO and boot the new virtual machine with it.

VirtualBox Menu Bar —> Machines —> Setting

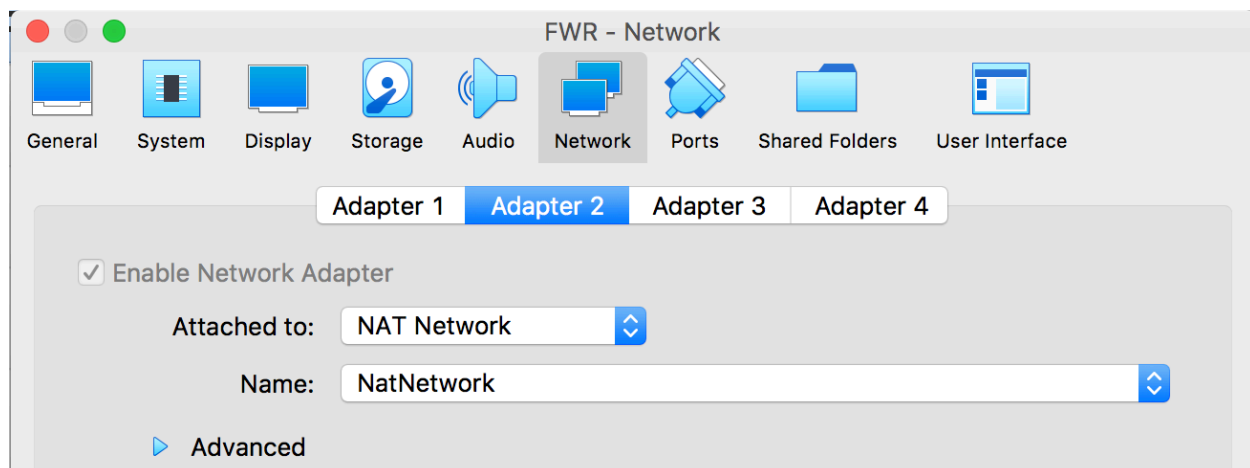
Select Storage and highlight Controller IDE to add a new Disk

Select Choose Disk to attach the ISO file download from Endian FW website.

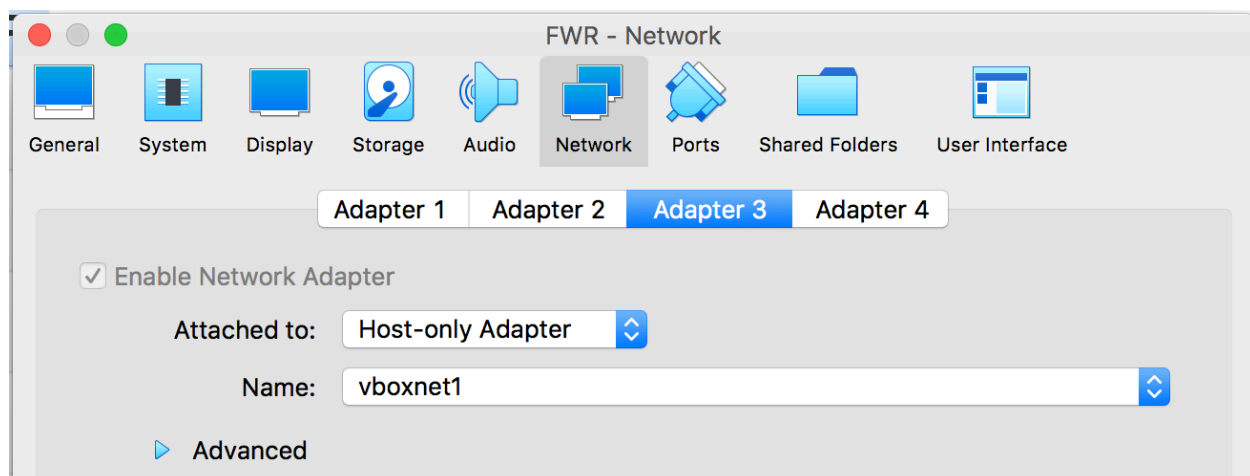




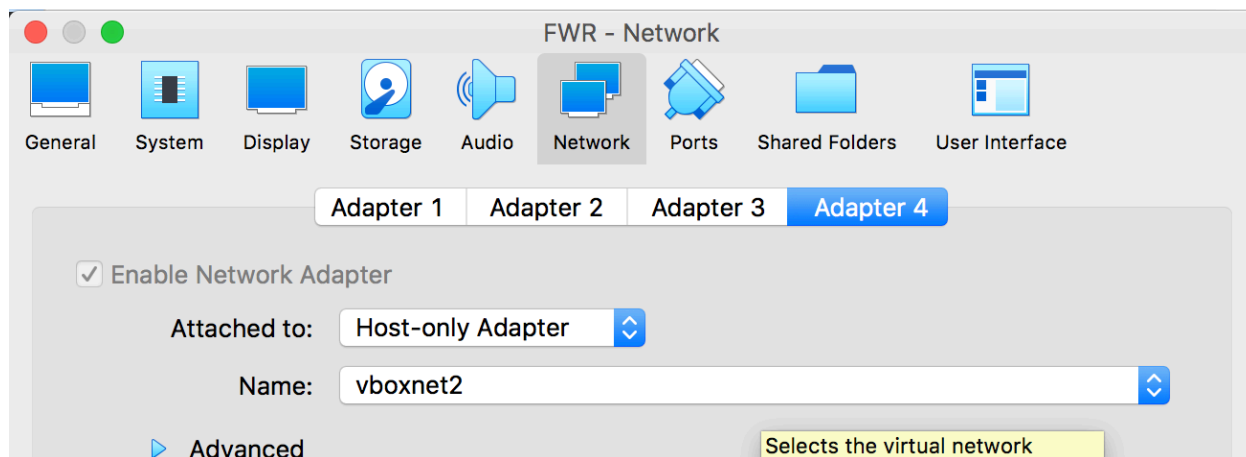
Adapter 1 is the internal interface for private network.



Adapter 2 is the outside interface that connect the FW to the internet.



Adapter 3 is the interface that communicate with the internal network and is more secure than the interface that allow Client VPN users to connect to the internal Network.



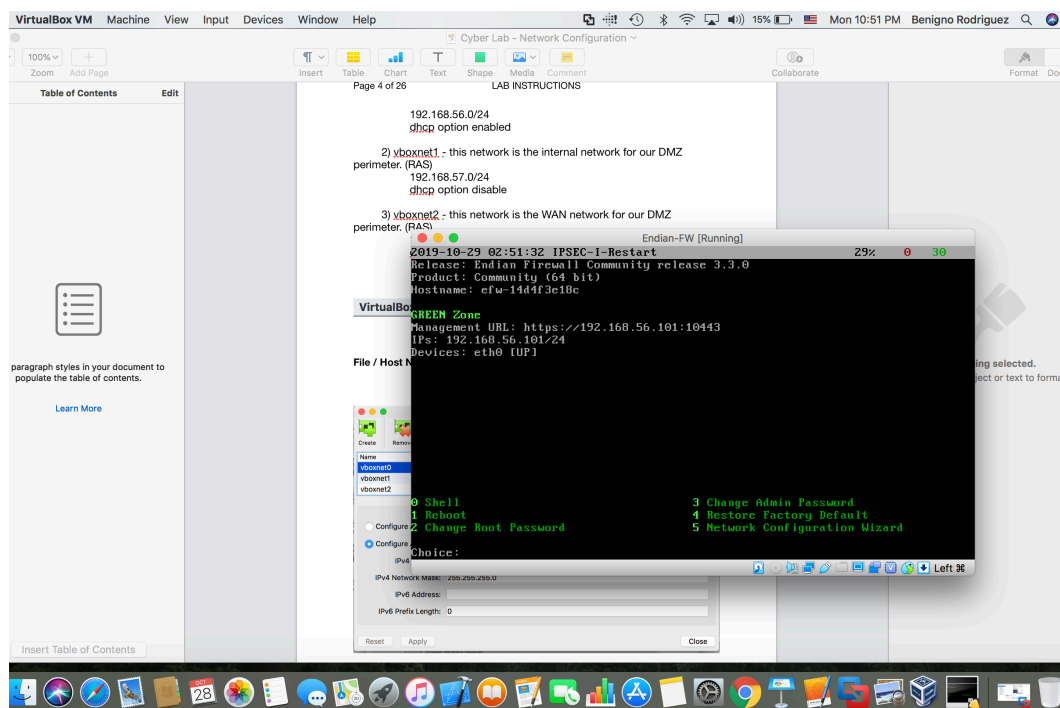
Adapter 4 is the interface that allow outside devices to connect via VPN to internal resources.

Install and Configure Endian Firewall on VirtualBox

Once you are done setting up the virtual machine networks and storage, you are ready to begin the installation. Start the VM, the first installation prompt will be selecting the installation language.

Note: Reference Document... The following link provide information about Endian Firewall Installation on VirtualBox.

<https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/>



SCREENSHOTS - ENDIAN-FW

This images gallery shows some of the screen capture from our installation. There are few minimum installation setting for the FW.

- 1) Language Selection
- 2) Hard Drive Partitioning
- 3) Network Interface for GREEN Interface (The green interface is the local secure interface for internal resources. In our lab, it includes a primary domain controller and a windows 10 client virtual machine.)

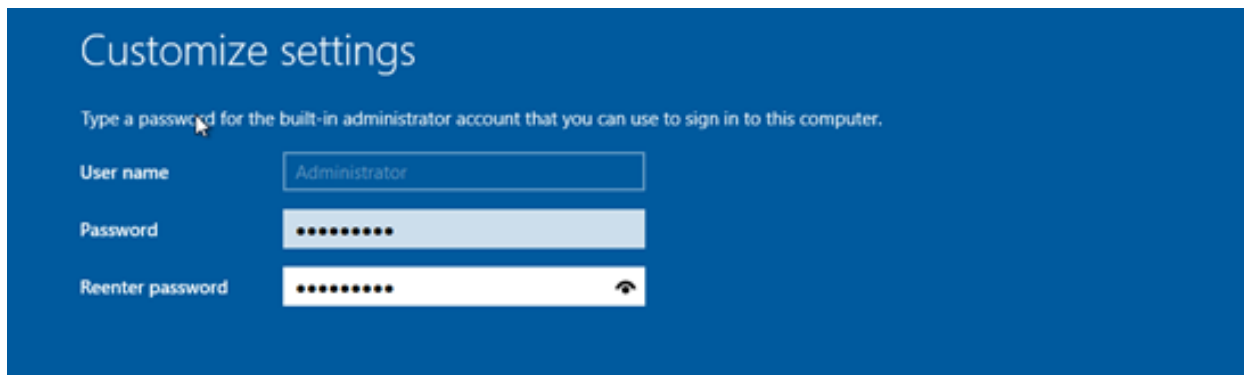
CONFIGURATION SECTION

Network configuration for windows servers VM

VirtualBox VM Machine View Input Devices Window Help

VirtualBox (Menu Bar)

Select Input / Keyboard / Insert Ctrl-Alt-Del to login with your password credential provided for administrator during installation. This is the password provided during the installation step shown below.



Customize settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name Administrator

Password

Reenter password

Windows PDC Server (2016)

```
powershell  
rename-computer PDC
```

```
New-NetIPAddress -IPAddress 192.168.56.150 -InterfaceAlias  
"Ethernet" -DefaultGateway 192.168.56.101 -AddressFamily IPv4 -  
PrefixLength 24
```

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -  
ServerAddresses 127.0.0.1  
restart-computer
```

Windows Domain Configuration

```
Install-WindowsFeature AD-Domain-Services -  
IncludeManagementTools  
Install-ADDSForest -DomainName "corp.localdomain"  
Add-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools  
Install-AdcsCertificationAuthority -CAType EnterpriseRootCA
```

The Windows Server will restart and the configuration can be verified with the following powershell commands to ensure AD domain services has been installed.

```
Powershell  
Get-WindowsFeature
```

Alternative you might want to create few powershell scripts with the commands listed above and execute then. We will provide troubleshoot instructions later to confirm that the configuration is complete and correct.

Now, continue with the network configuration for the RAS server by following steps below. Select RAS Server VM from VirtualBox Manager (start the VM if not started before)

VirtualBox (Menu Bar)

Input / Keyboard / Insert Ctrl-Alt-Del - login with password credential provided for administrator while installation.

VirtualBox VM	Machine	View	Input	Devices	Window	Help
----------------------	---------	------	-------	---------	--------	------

Windows RAS Server (2016)

```
powershell  
rename-computer ras
```

```
New-NetIPAddress -IPAddress 192.168.57.150 -InterfaceAlias "Ethernet" -  
DefaultGateway 192.168.57.101 -AddressFamily IPv4 -  
PrefixLength 24
```

Note: Ensure the following interface does not have a default gateway!

```
New-NetIPAddress -IPAddress 192.100.1.150 -InterfaceAlias "Ethernet  
2" -AddressFamily IPv4 -PrefixLength 24
```

route -P add 192.168.56.0 mask 255.255.255.0 192.168.57.101

```
restart-computer
```

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses  
192.168.56.150
```

```
add-computer -DomainName corp.localhost -DomainCredential  
corp\administrator
```

Install-WindowsFeature RemoteAccess -IncludeManagementTools

Install-WindowsFeature RSAT-RemoteAccess-PowerShell

Install-WindowsFeature DirectAccess-VPN

Install-WindowsFeature Routing

shutdown /r

Note: Windows Powershell commands listed above will install all services requires for completing the LAB. However, the following services required further configuration.

Remote Access

Routing

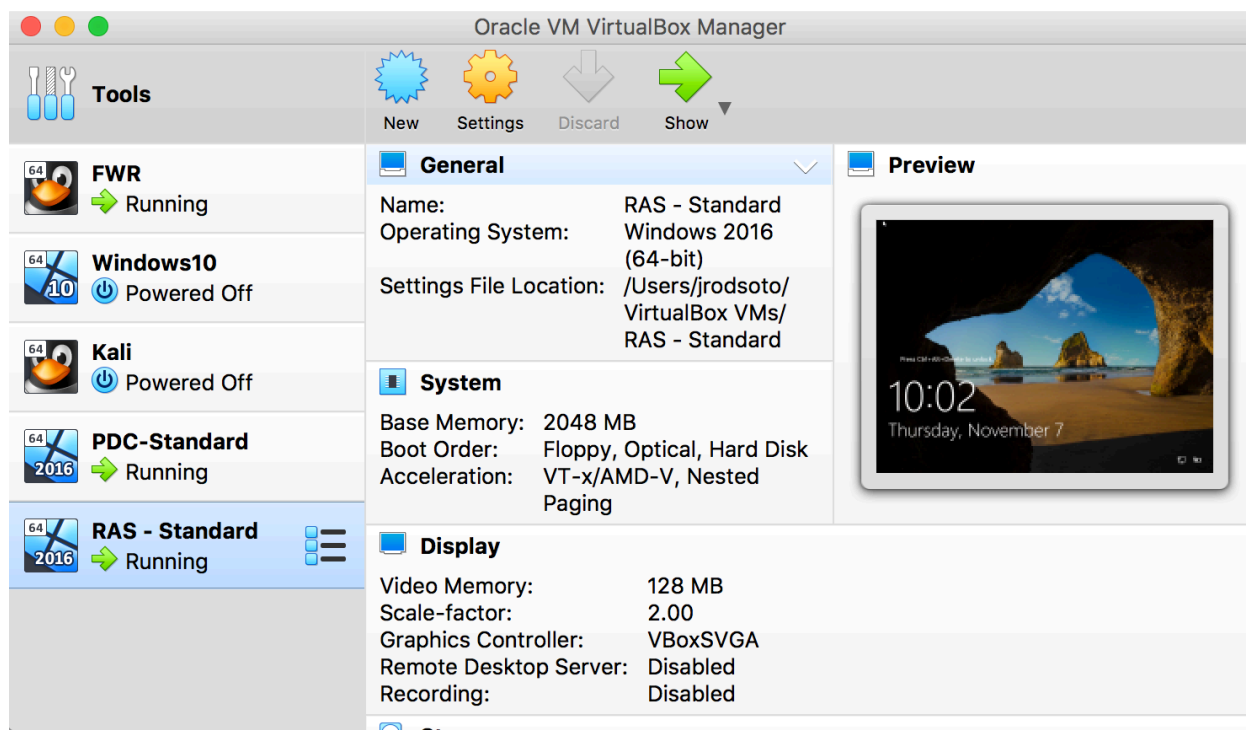
Microsoft CA

Installing Server Certificate (RAS Server) and Binding the Certificate to IIS and Remote Access VPN.

Endian Firewall Configuration

The Endian Firewall requires four VirtualBox Network Interfaces or adapters. Ensure that the VM for endian setting is properly configured before continue with the following steps.

Select Endian FW from your VirtualBox Man



VirtualBox Menu Bar —> Machines —> Start —> Normal Start

```
FWR [Running]
Release: Endian Firewall Community release 3.3.0
Product: Community (64 bit)
Hostname: fw-router

GREEN Zone [DHCP SERVER ENABLED]
Management URL: https://192.168.56.101:10443
IPs: 192.168.56.101/24
Devices: eth0 [UP]

Uplink - main [ACTIVE]
IPs: 10.0.2.5/24 10.0.2.100/24 10.0.2.150/24 10.0.2.200/24 10.0.2.250/24 [STATIC]
Device: eth1 [UP]

0 Shell
1 Reboot
2 Change Root Password
3 Change Admin Password
4 Restore Factory Default
5 Network Configuration Wizard

Choice:
```

```
FWR [Running]

Choice: 5
Enter Root Password:
Network Configuration Wizard
-----
Hostname: fw-router
Domain: localdomain
RED interface type: STATIC
RED device: eth1
RED IPs (IP/CIDR): 10.0.2.5/24 10.0.2.100/24 10.0.2.150/24 10.0.2.200/24 10.0.2.250/24
RED gateway: 10.0.2.1
Primary DNS: 10.0.0.1
Secondary DNS: 8.8.8.8
GREEN devices: eth0
GREEN IPs (IP/CIDR): 192.168.56.101/24
Enable DHCP server on GREEN: on
ORANGE devices: eth2
ORANGE IPs (IP/CIDR): 192.168.57.101/24
BLUE devices:
BLUE IPs (IP/CIDR): 192.100.1.101/24
Enable SSH access: on
Allow access to ports 22, 80 and 10443 from any interface: off

Hostname? fw-router_
```

Console Network Configuration (this is option 5 from the console of the FW)

Select Option 5 from Console Menu and provide Endian Root Password.

The current configuration will be display.

Note: current configuration should display information configured during initial VM installation. (see Endian FW Installation)

The configuration wizard will prompt for information, ensure that the following information is enter. The goal is to configure network setting for all interfaces and firewall access, including new password for endian-fw. (the default password is : endian)

Confirm Configuration and write configuration as shown below.

Important firewall configuration: the primary DNS for the nat interface (red interface) should be your hosts dns primary DNS. (used ifconfig,

```
Domain: localdomain
RED interface type: STATIC
RED device: eth1
RED IPs (IP/CIDR): 10.0.2.5/24 10.0.2.100/24 10.0.2.150/24 10.0.2.200/24 10.0.2.
50/24
RED gateway: 10.0.2.1
Primary DNS: 10.0.0.1
Secondary DNS: 8.8.8.8
GREEN devices: eth0
GREEN IPs (IP/CIDR): 192.168.56.101/24
Enable DHCP server on GREEN: on
RANGE devices: eth2
RANGE IPs (IP/CIDR): 192.168.57.101/24
BLUE devices:
BLUE IPs (IP/CIDR): 192.100.1.101/24
Enable SSH access: on
Allow access to ports 22, 80 and 10443 from any interface: off

Is the above correct <yes/no>? yes
Write configuration <yes/no>? yes_
```

and/or ipconfig commands on the host machine to find your DNS server IP addresses)

Note: Option 5 (network configuration wizard) can be run anytime, if you have mis-configured the firewall, you can go back and re-configure it again with appropriate information. NAT and Firewall Rules are required after initial configuration.

Endian Firewall Configuration - Graphical User Interface
Login to Windows Server 2016 - PDC
Find Microsoft Edge and connect to the following link.

<https://192.168.56.101:10443>

The screenshot shows the Endian Firewall GUI with the 'Firewall' tab selected. The left sidebar contains a menu with 'Port forwarding / NAT' highlighted. The main content area is titled 'Port forwarding / Destination NAT'. It has two sub-tabs: 'Port forwarding / Destination NAT' (selected) and 'Source NAT Incoming routed traffic'. Below the sub-tabs is a section for 'Current rules' with a link to 'Add a new Port forwarding / Destination NAT rule'. A table lists the current rules:

#	Incoming IP	Service	Policy	Translate to	Remark	Actions
1	10.0.2.250 (Uplink Main uplink)	<ANY>	→	192.168.57.150		✓ + ✎ 🗑

Legend: ☒ Enabled (click to disable) ☐ Disabled (click to enable) ✎ Edit 🗑 Remove

Show system rules >>>

Status: Connected: main (1d 5h 25m 52s) Uptime: 23:58:33 up 2:51, 0 users, load average: 0.00, 0.00, 0.00

Endian Firewall Community release 3.3.0 (c) Endian

Port forwarding / Source Network Address Translation

The screenshot shows the Endian Firewall GUI with the 'Firewall' tab selected. The left sidebar contains a menu with 'Port forwarding / NAT' highlighted. The main content area is titled 'Source Network Address Translation'. It has two sub-tabs: 'Port forwarding / Destination NAT' and 'Source NAT Incoming routed traffic' (selected). Below the sub-tabs is a section for 'Current rules' with a link to 'Add a new source NAT rule'. A table lists the current rules:

#	Source	Destination	Service	NAT to	Remark	Actions
1	192.168.57.150	Uplink ANY	<ANY>	10.0.2.250		✓ ✎ 🗑

Legend: ☒ Enabled (click to disable) ☐ Disabled (click to enable) ✎ Edit 🗑 Remove

Show system rules >>>

Status: Connected: main (1d 5h 28m 34s) Uptime: 23:59:15 up 2:51, 0 users, load average: 0.00, 0.00, 0.00

Endian Firewall Community release 3.3.0 (c) Endian

SystemStatusNetworkServices**Firewall**ProxyVPNLogs and Reports




Port forwarding / NAT
Outgoing traffic
Inter-Zone traffic
VPN traffic
System access
Firewall Diagrams



Incoming firewall configuration

>> Port forwarding / Destination NATSource NATIncoming routed traffic

>> Current rules

[Add a new firewall rule](#)

#	Source	Destination	Service	Policy	Remark	Actions
1	<ANY>	192.168.57.150	<ANY>	→		  

Legend ☒ Enabled (click to disable) ☐ Disabled (click to enable)  Edit  Remove

Show system rules >>>

Status: Connected: main (1d 5h 26m 50s) Uptime: 23:59:31 up 2:52, 0 users, load average: 0.00, 0.00, 0.00
Endian Firewall Community release 3.3.0 (c) Endian

Incoming and Inter-Zone Rules





































SystemStatusNetworkServices**Firewall**ProxyVPNLogs and Reports



Port forwarding / NAT
Outgoing traffic
Inter-Zone traffic
VPN traffic
System access
Firewall Diagrams

Inter-Zone firewall configuration

>> Current rules

[Add a new inter-zone firewall rule](#)

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN	GREEN	<ANY>	→		↑↓   
2	GREEN	BLUE	<ANY>	→		↑↓   
3	GREEN	ORANGE	<ANY>	→		↑↓   
4	BLUE	BLUE	<ANY>	→		↑↓   
5	ORANGE	ORANGE	<ANY>	→		↑↓   
6	ORANGE	GREEN	<ANY>	→		↑↓   
7	192.168.57.150	192.168.56.150	<ANY>	→	ras server to pdc server	↑↓   
8	192.168.56.150	192.158.57.150	<ANY>	→	pdc to ras server	↑↓   
9	192.168.58.150	<ANY>	<ANY>	→		↑↓   
10	Interface 3	<ANY>	<ANY>	→		↑↓   
11	BLUE	<ANY>	<ANY>	→		↑↓   
12	<ANY>	ORANGE	<ANY>	→		↑   

Legend: ☒ Enabled (click to disable) ☐ Disabled (click to enable)  Edit  Remove

Show rules of system services >>>

>> Inter-Zone Firewall Settings

Enable Inter-Zone firewall ☒

☒ Log accepted Inter-Zone connections

Outgoing firewall rules

Port forwarding / NAT

Outgoing traffic

Inter-Zone traffic

VPN traffic

System access

Firewall Diagrams

Outgoing firewall configuration

>> Current rules

[Add a new firewall rule](#)

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN BLUE	RED	TCP/80		allow HTTP	
2	GREEN BLUE	RED	TCP/443		allow HTTPS	
3	GREEN	RED	TCP/21		allow FTP	
4	GREEN	RED	TCP/25		allow SMTP	
5	GREEN	RED	TCP/110		allow POP	
6	GREEN	RED	TCP/143		allow IMAP	
7	GREEN	RED	TCP/995		allow POP3s	
8	GREEN	RED	TCP/993		allow IMAPs	
9	ORANGE	RED	<ANY>			
10	GREEN ORANGE BLUE	RED	TCP+UDP/53		allow DNS	
11	GREEN ORANGE BLUE	RED	ICMP/8 ICMP/30		allow PING	
12	192.168.57.150	192.168.56.150	<ANY>			
13	192.168.56.150	192.168.57.150	<ANY>			
14	192.168.57.150	RED	<ANY>			

Legend Enabled (click to disable) ☐ Disabled (click to enable) Edit Remove

Show system rules >>

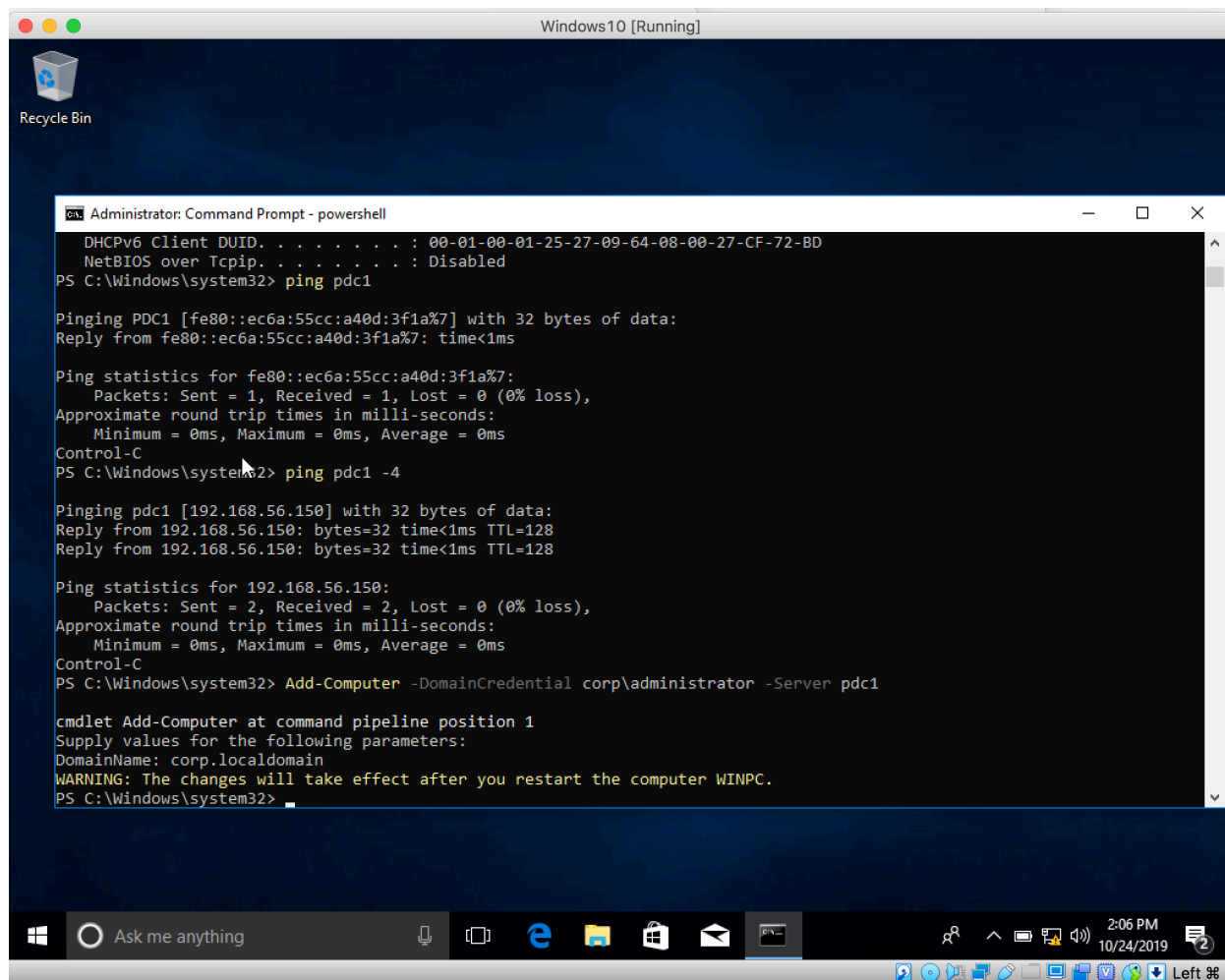
Network configuration for windows 10 client VM

CONFIGURATION OF WINDOWS 10 CLIENT will required the following steps

1. login to windows 10 VM (username and password provided while installation)
2. runs as administrator CMD
3. powershell
4. rename-computer WINPC
5. restart-computer
6. set dns server ip address
 - a. Set-DnsClientServerAddress (see below)
7. add-computer -DomainName corp.localhost -DomainCredential corp\administrator (see screenshot for powershell with -server option)

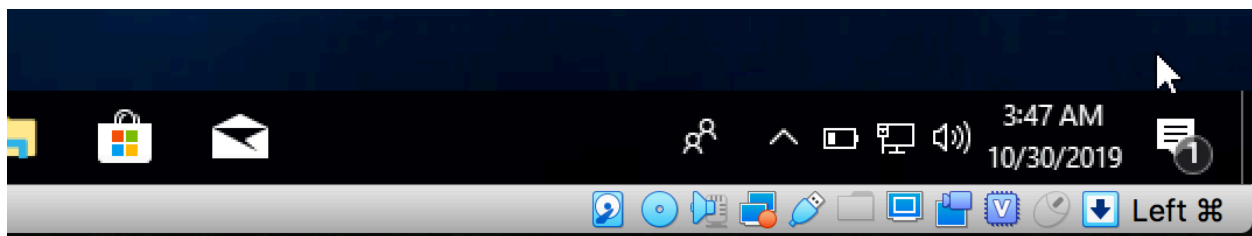
Set-DnsClientServerAddress -inetrerfaceAlias "ethernet" -serverAddress "192.168.56.150" -validate

Remember that this VM will use a vboxnet0 with DHCP enable, therefore not ipaddress configuration is require, you must confirm ip address with ipconfig /all command line.



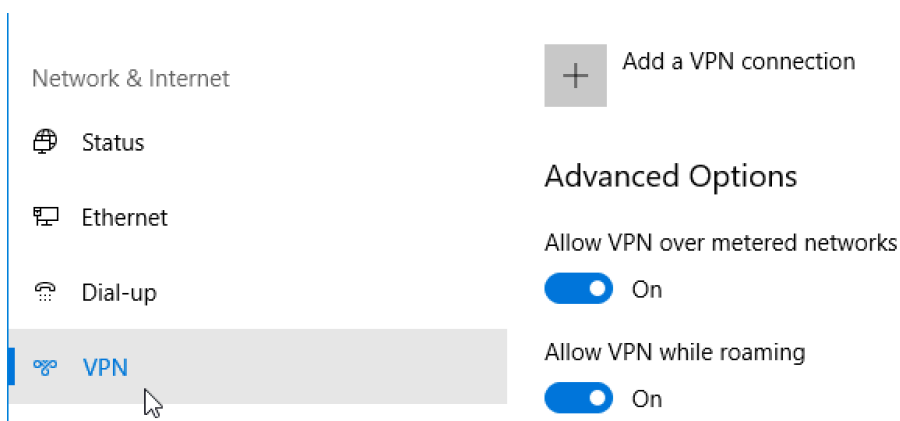
VPN Configuration for windows 10 client VM

VPN Configuration can be found under setting for windows network setting and internet connections. In the bottom right side of your windows 10 client VM open network setting by right-click on the PC icon. Network & internet windows will pop up.



Network & Internet Setting Windows

Select VPN on the left side panel then click Add a VPN Connection.



Fill out the all information as shown below and save the configuration.

Settings

Edit VPN connection

These changes will take effect the next time you connect.

Connection name

myVPN2

Server name or address

vpn.corp.localdomain

VPN type

Automatic

Type of sign-in info

User name and password

User name (optional)

corp\administrator

Save Cancel

Apply Cancel

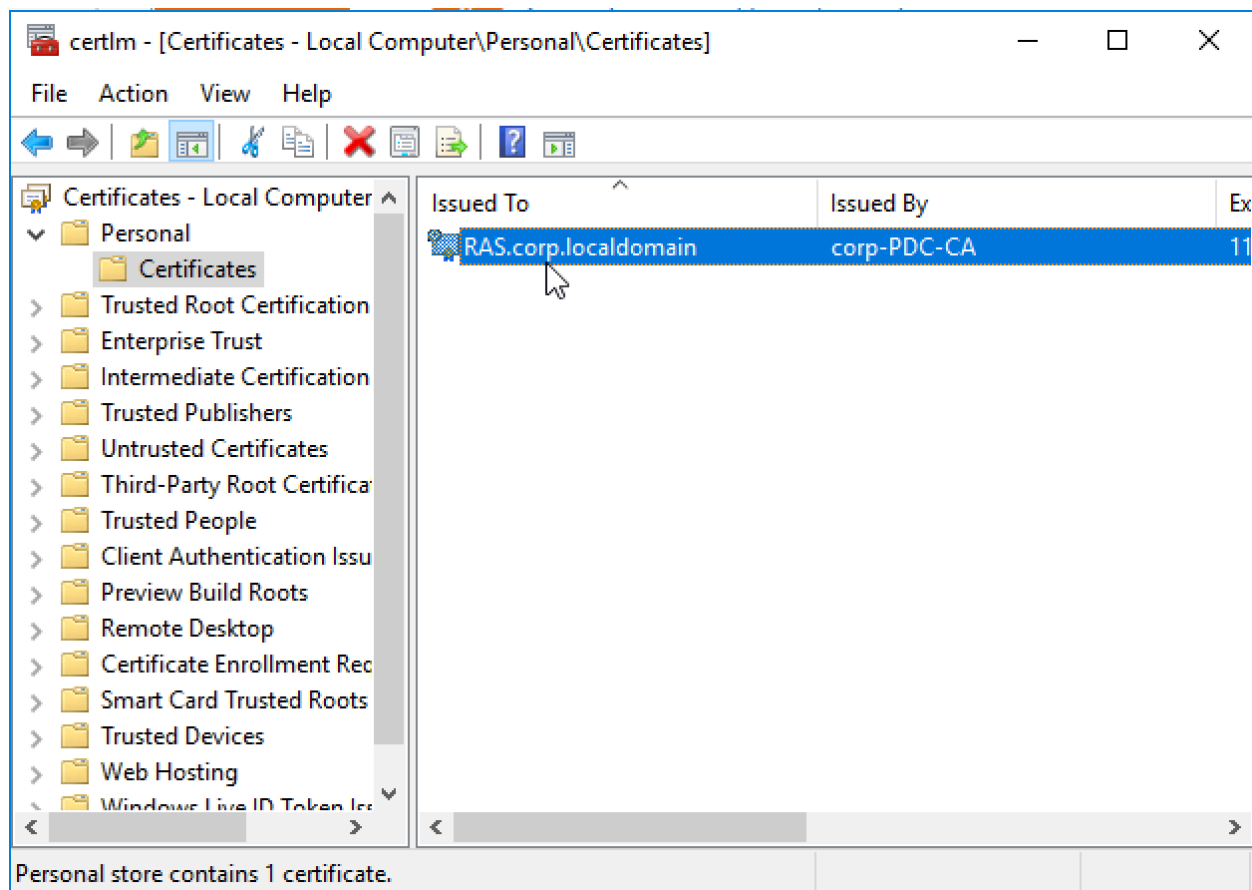
Note: The server name or address is the outside interface of the Endian Firewall. IP forwarding is require to forward VPN traffic to RAS server. (vpn.corp.localdomain is a CN for RAS.corp.localhost certificate)

Remote Access Configuration

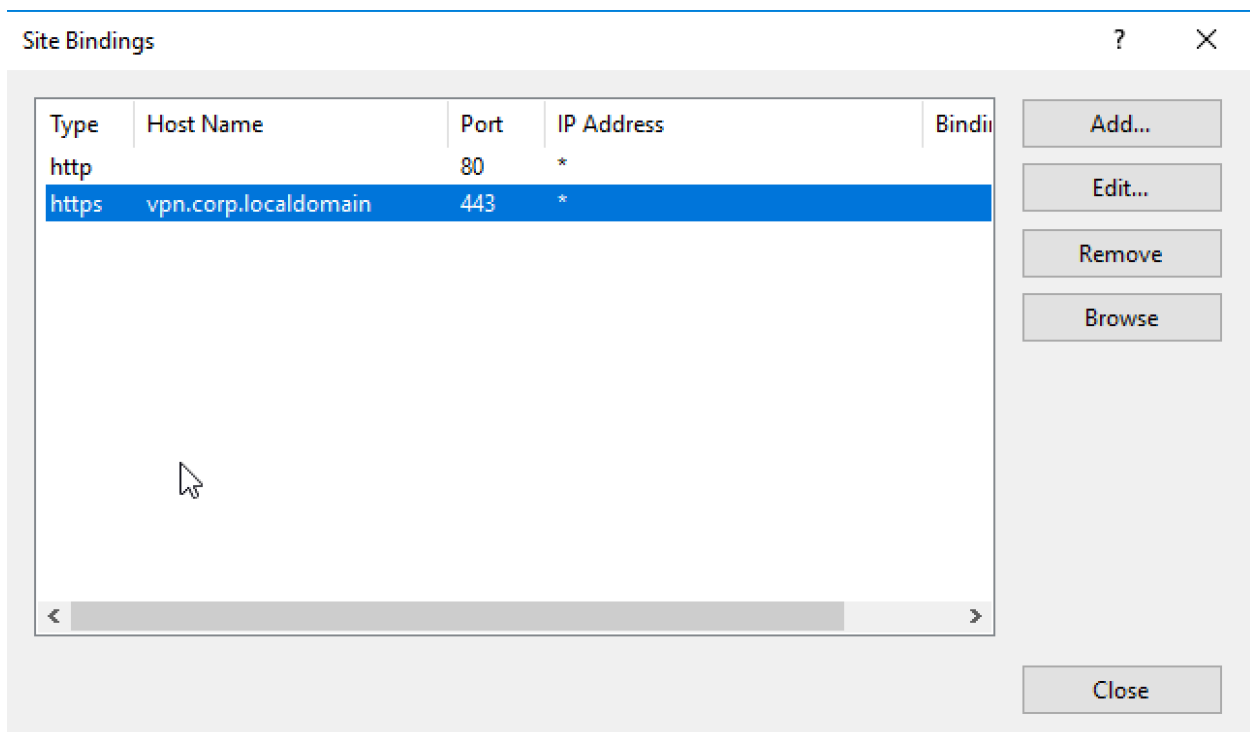
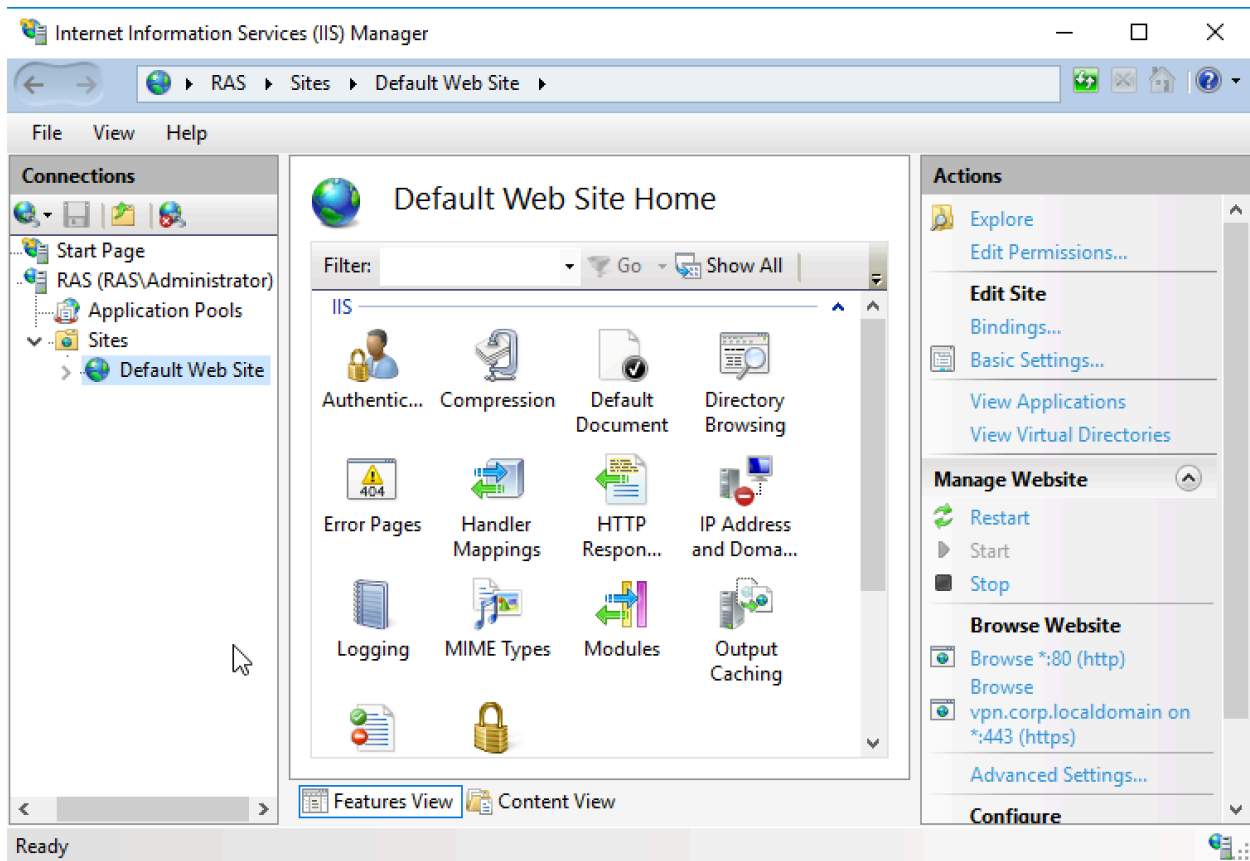
Remote Access Services required a client authentication certificate on the RAS server for user authentication. The PDC Server is already configured for AD CA services. We will illustrate the steps to configured the RAS server, request a certificate from the CA server (internally) and show how to bind the certificate to Remote Access Server.

We will utilized desktop experience interfaces to configured RAS server, request a server certificate for authentication and biding it to both Web Server and RAS services. I will suggest to watch the video explaining the configuration steps for requesting a certificate for the server and binding, a contribution from NLB Solutions.

Certificate Request



Binding Certificate to Web Server Default Site



Binding Certificate to RAS Services (Routing and Remote Access)

The screenshot shows the 'RAS Properties' dialog box with the 'Security' tab selected. The 'Authentication provider' is set to 'Windows Authentication'. The 'Accounting provider' is set to 'Windows Accounting'. The 'Allow custom IPsec policy for L2TP/IKEv2 connection' checkbox is unchecked. The 'Preshared Key' field is empty. The 'SSL Certificate Binding' section is expanded, showing the 'Use HTTP' checkbox is unchecked and the 'Certificate' dropdown is set to 'RAS.corp.localdomain'.

RAS Properties ? X

General Security IPv4 IPv6 IKEv2 PPP Logging

The Authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider:
Windows Authentication [v] Configure...

Authentication Methods...

The accounting provider maintains a log of connection requests and sessions.

Accounting provider:
Windows Accounting [v] Configure...

The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.

☐ Allow custom IPsec policy for L2TP/IKEv2 connection

Preshared Key:
[]

SSL Certificate Binding:

☐ Use HTTP

Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)

Certificate: RAS.corp.localdomain [v] View

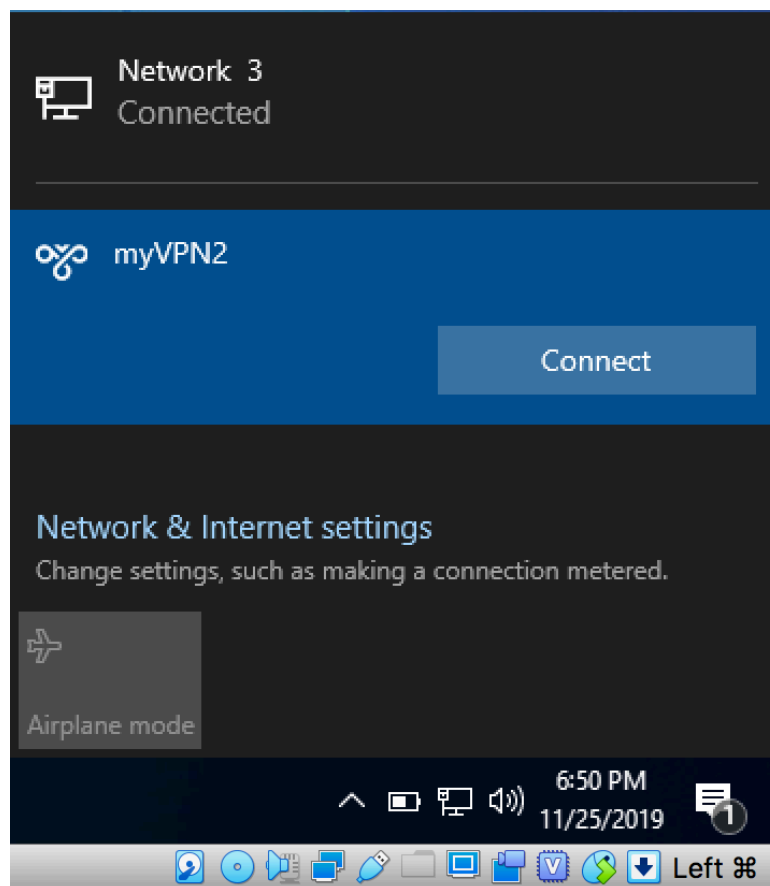
OK Cancel Apply

The following video was also used for reference. Contribution by NLB Solutions

<https://youtu.be/1xAXqmN9tiU>

VPN Configuration Test

VPN Configuration can be found under setting for windows network setting and internet connections. In the bottom right side of your windows 10 client VM open network setting by click on the PC icon. Both the local and VPN networks should display as shown below.



Select myVPN2 Connection and click Connect. This should allow the users to be authenticated internally by the Remote Access Server (RAS). Following shown the two network ip addresses assigned to the client from the CMD prompt (ipconfig).

```
Command Prompt
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\jrodsoto>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::681b:27:8886:bf2b%7
    IPv4 Address. . . . . : 10.0.2.8
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

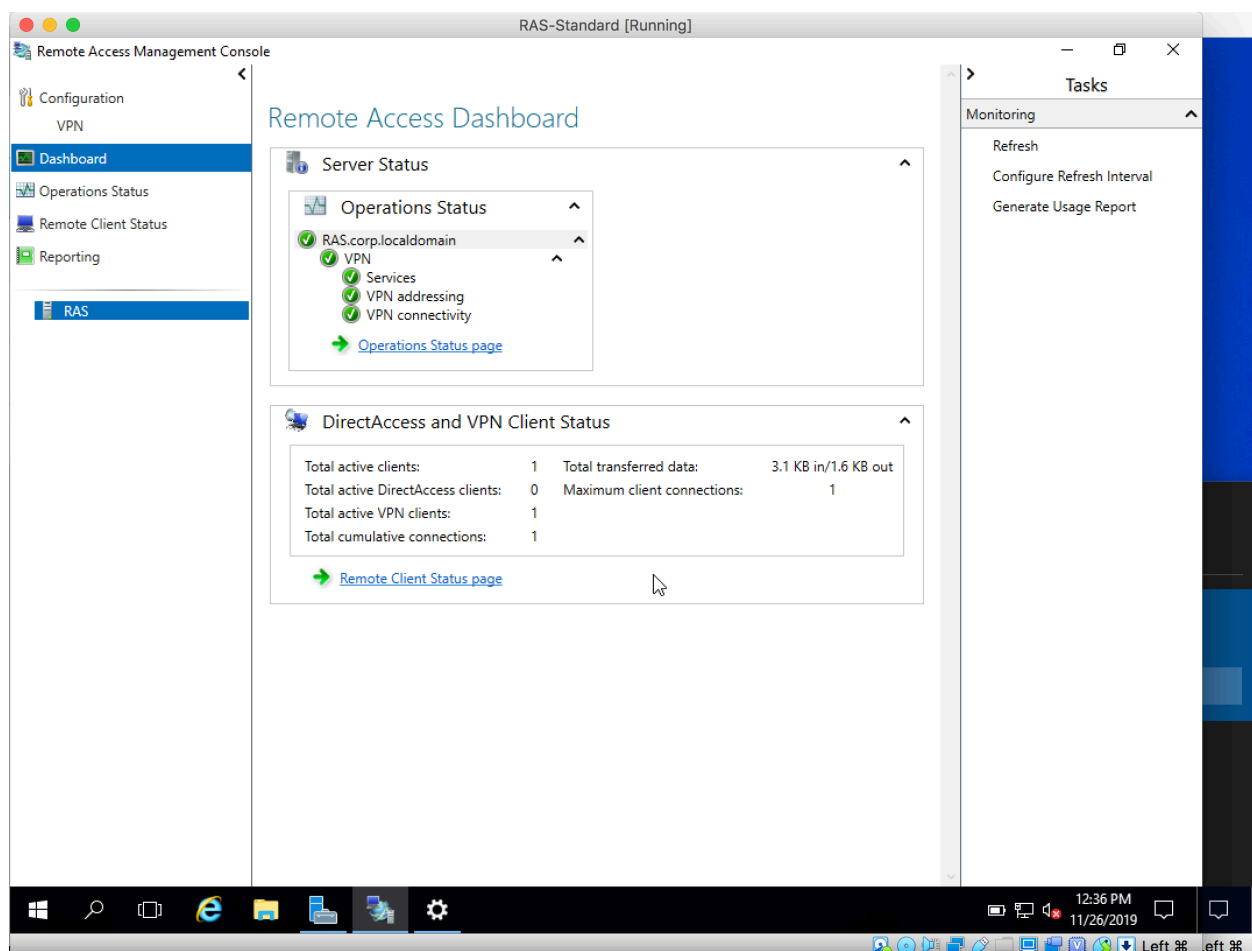
PPP adapter myVPN2:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.57.202
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 

C:\Users\jrodsoto>
```

Remote Access Management Console

The total clients shown 1 user after successfully connecting to RAS service on the RAS server.



THE FOLLOWING INSTRUCTIONS SHOULD NOT BE NEEDED - Instructions were used for troubleshooting configuration issues.

change default route - Original the default IP address for the two vm might be assign to VM switch IP address, therefore we must change the default gateway to the interfaces of the Endian FW/Router. Perform the following powershell commands on both Windows Standard Servers.

PDC1 Server

powershell

```
remove-netroute 0.0.0.0/0
```

when prompted to remove the route enter: yes

```
new-netroute 0.0.0.0/0 -nextHop 192.168.56.101
```

RAS Server

powershell

```
remove-netroute 0.0.0.0/0
```

when prompted to remove the route enter: yes

```
new-netroute 0.0.0.0/0 -nextHop 192.168.57.101
```

```
get-NetAdapter
```

```
remove-netIPAddress
```