## Window 10 client installation

## Documentation with photos

PC Name:

Password:

* OS: Windows 10 (64-Bit)
* iso:en\_windows\_10\_eval\_22h2\_release\_svc\_refresh\_CLIENTENTERPRISEEVAL\_OEMRET\_x64FRE\_en-us.iso
* Specs: 4GB RAM, 1 CPU Threads, 50GB Storage
* Network Adapter: Bridged Adapter

Name: Realtek PCIe GBE Family Controller

Assigned task status completion:

IP Address: 192.168.108.23

Week 1 date: 06/06/2024

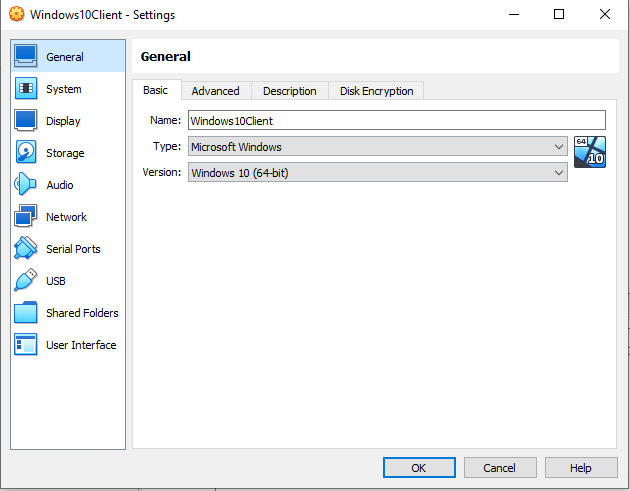
Install Window Client 10

Description: Setting up windows 10 so it can be connected to Window server 22

Issues: no issue

Other comments

Windows 10 set up screenshots



Setting it up in Virtual box

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a network

Description automatically generated

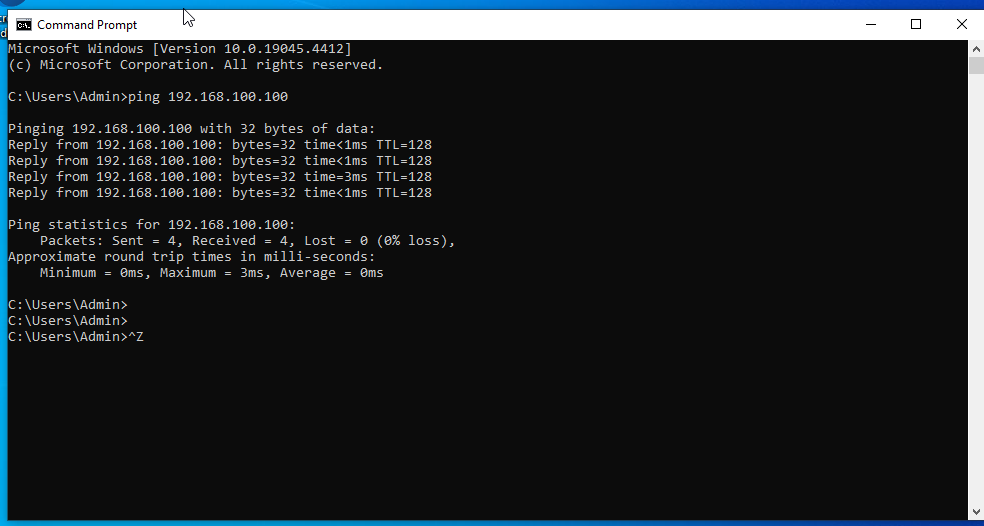
Windows 10 IP config /all

A screenshot of a computer

Description automatically generated

A computer screen shot of a program

Description automatically generated



## Windows Server 22 (Server-PT)

PC Name:

Password:

* OS: Windows 10 (64-Bit)
* iso:en\_windows\_10\_eval\_22h2\_release\_svc\_refresh\_CLIENTENTERPRISEEVAL\_OEMRET\_x64FRE\_en-us.iso
* Specs: 4GB RAM, 1 CPU Threads, 50GB Storage
* Network Adapter: Bridged Adapter

Name: Realtek PCIe GBE Family Controller

* Assigned task status completion:

Tasks to be done on Windows server 22

1. Change IP Address, GW and DNS

IP :192.168.100.100

Gateway:

DNS=8.8.8.8

1. Promote Server to Domain controller
2. Create user accounts and Security groups
3. Join Window clients to Domain: LP.local
4. Configure DNS settings

Forward lookup

Description: Setting up Window server 22 is very important because it gave internet to the win 10 and other computers

Issues: we had one issue where we couldn’t get the window server to give internet to window clients

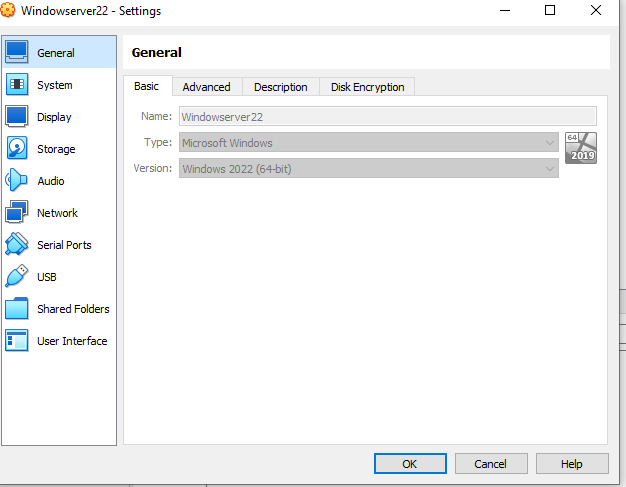
Other comments

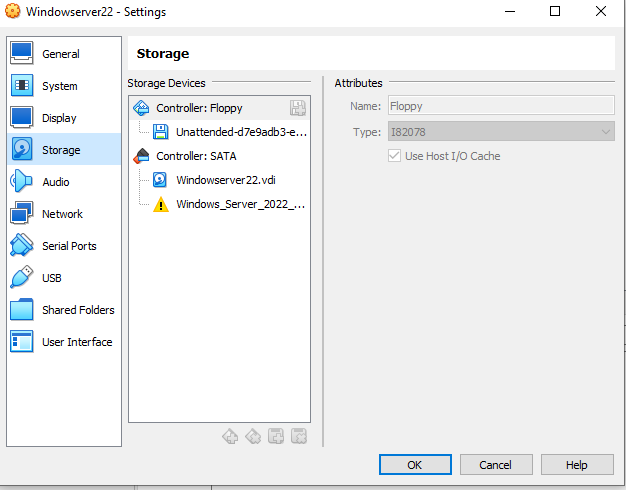
**Windows 22 server screenshots**

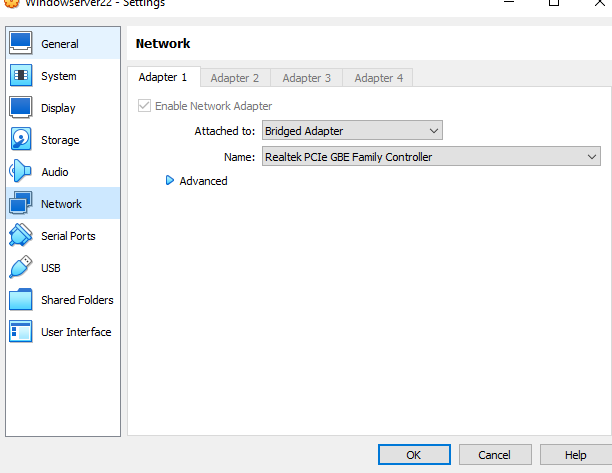
A screenshot of a computer

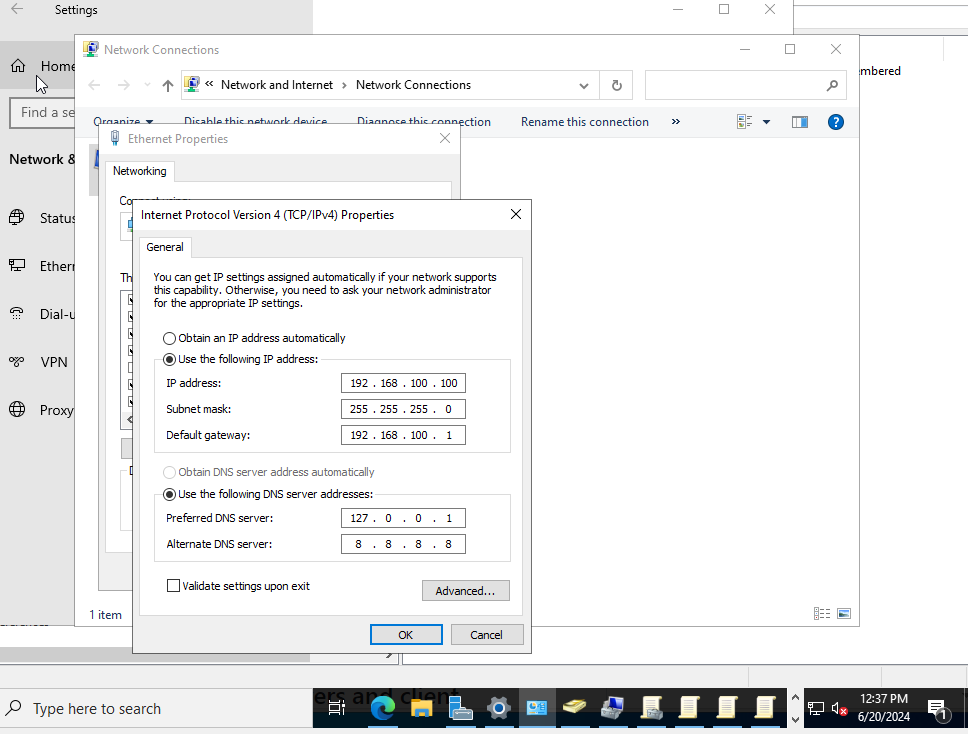
Description automatically generated

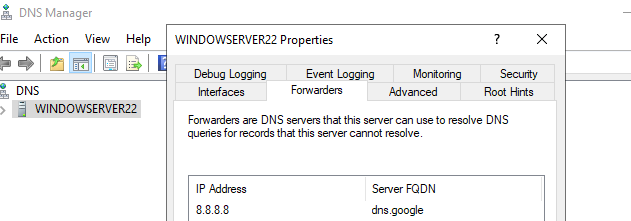
**Allowing internet to window server above pic**

****

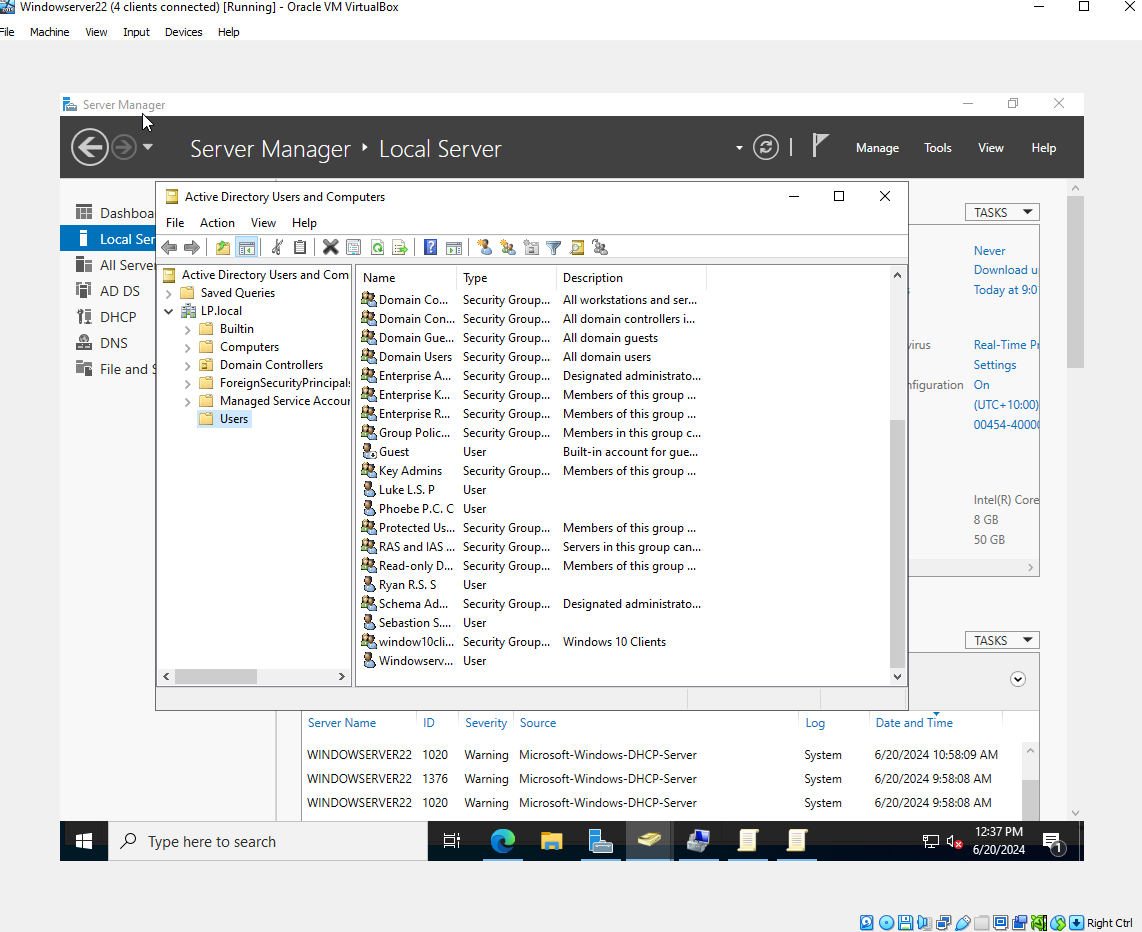
****

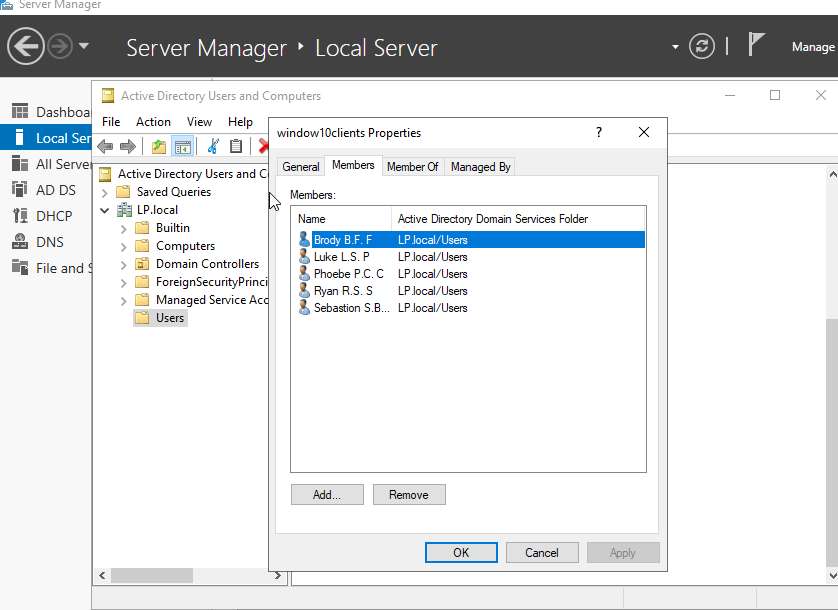
****

****



**Adding forwarder**

****

****

## Set up DMZ Server (Notes: 8.5 might fix log to kibana for production)

PC Name: DMZ server

Password:

VirtualBox Machine > new

Name: DMZ Web Server Folder: (D: Drive)

ISO Image: Not selected

Type: Linux

Version: Ubuntu 22.04 LTS (64-bit)

Memory: 4096 MB

Use an existing Virtual hard disk : xx.vmdk (D:Drive)

Settings > network

Adapter 1

Attached to: NAT Network

Name: DMZ Network

IP address: 192.168.50.100

GW: 192.168.50.1

Tasks to be done on DMZ

1. Do Update (Sudo apt update && sudo apt upgrade -y
2. Install elastic defend

Commands:

$sudo apt install curl

$nano elasticAgentScript.sh

chmod +x elasticAgentScript.sh

./elasticAgentScript.sh

1. Add security policy for DMZ

Policies > security - Add

General

Name: inside-to-DMZ

Source

SOURCE ZONE - add inside

Destination

DESTINATION ZONE - add DMZ

Application - any

Service / URL Category - application-default

Actions

Action Setting - Action : Allow

Log setting - log at session end

Log Forwarding: KaliPurpleSIEMProfile

Policies > security - Add

General

Name: DMZ-to-outside

Source

SOURCE ZONE - add DMZ

Destination

DESTINATION ZONE - add outside

Application - any

Service / URL Category - application-default

Actions

Action Setting - Action : Allow

Log setting - log at session end

Log Forwarding: KaliPurpleSIEMProfile

ping 8.8.8.8

sudo apt update

8.6.3.1 PAFW Security policy - outside to DMZ WEB Server

This policy allows web browsing application traffic from outside to DMZ server with the outside address of 192.168.108.1XX

Policies > security - Add

General

Name: outside-to-DMZ

Source

SOURCE ZONE - add outside

Destination

DESTINATION ZONE - add DMZ

DESTINATION ADDRESS - 192.168.108.1XX

Application - web-browsing

Service / URL Category - application-default

Actions

Action Setting - Action : Allow

Log setting - log at session end

Log Forwarding: KaliPurpleSIEMProfile

Profile Setting - Profile Type: None

Policies > NAT - Add

General

Name: dstNat-outside-dmz

NAT Type: ipv4

Original Packet

SOURCE ZONE: outside

Destination zone: outside

Destination Interface: any

Service : Service-http

SOURCE ADDRESS : any

DESTINATION ADDRESS: 192.168.108.1XX

Translated packet

Source Address translation: None

Destination Address translation:

Translation Type: Static IP

Translated Address: 192.168.50.100

Translated Port:

OK

1. Install ssh and xrdp

$sudo apt install xrdp -y

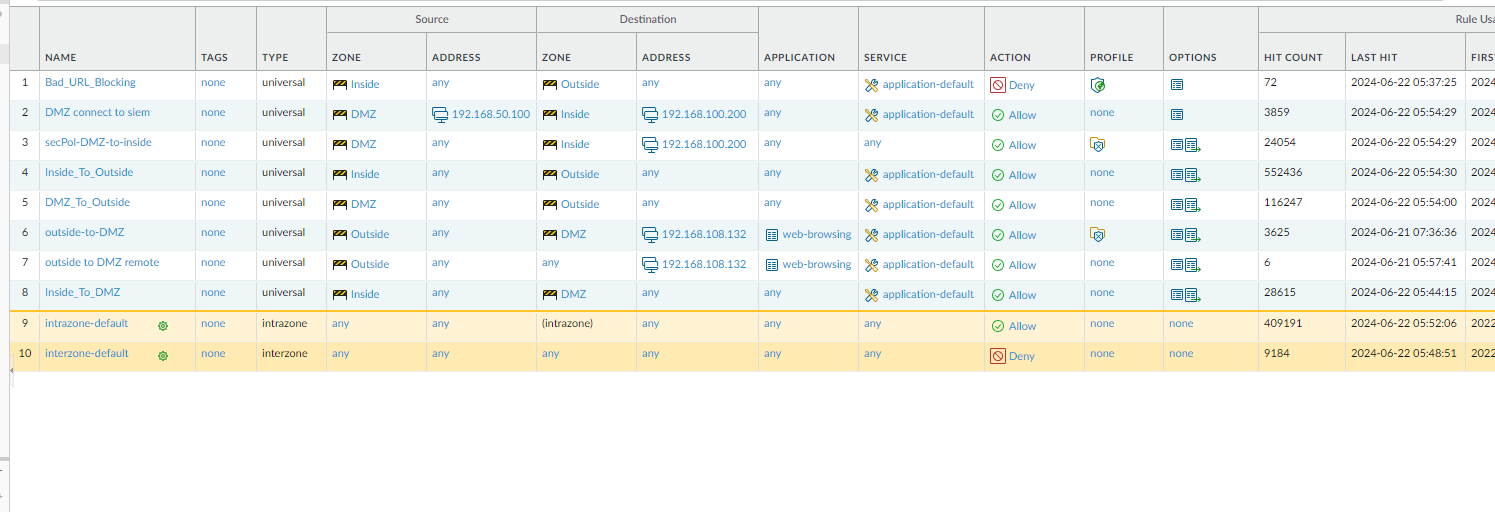
$sudo systemctl status xrdp

$sudo systemctl start xrdp

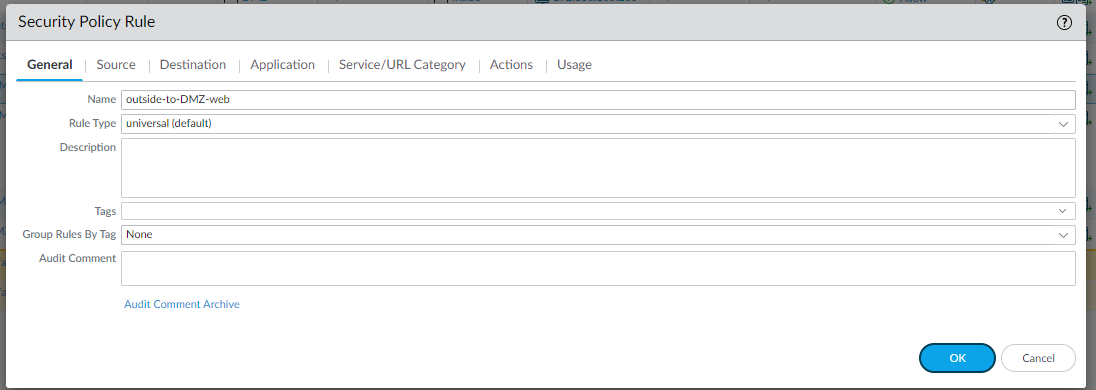
$sudo apt-get install openssh-server

$sudo systemctl enable ssh

**Palo alto configuration**



**Outside to dmz**



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated