INTERNSHIP PROJECT ON ISP SETUP WITH MIKROTIK, CISCO AND SECURING WITH FORTIGATE FIREWALL

INTERNSHIP REPORT BY

FAHIM ABDUL AZIZ
ID: 183-16-360

SUPERVISED BY

DR. MOHAMMED NADIR BIN ALI
REGISTRAR

Department of Computing and Information System
Faculty of Science and Technology
Daffodil International University

This Report Presented in Sectional Gratification of the Requirements of the Degree of Bachelor of Science in Computing and Information System

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH
SUMMER 2022

APPROVAL

This internship report titled **"INTERNSHIP PROJECT ON ISP SETUP WITH MIKROTIK, CISCO AND SECURING WITH FORTIGATE FIREWALL"**, submitted by **Fahim Abdul Aziz**, ID: **183-16-360** to the Department of Computing and Information System, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computing and Information System and approved as to its style and contents. The presentation has been held on 21-11-2022.

BOARD OF EXAMINERS

Mr. Md Sarwar Hossain Mollah
Associate Professor and Head
Department of Computing & Information Systems
Faculty of Science & Information Technology
Daffodil International University

Chairman

Mr. Abdullah Bin Kasem Bhuiyan
Lecturer
Department of Computing & Information Systems
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Mr. Md. Mehedi Hasan
Lecturer
Department of Computing & Information Systems
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Dr. Saifuddin Md. Tareeq
Professor & Chairman
Department of Computer Science and Engineering
University of Dhaka, Dhaka

External Examiner

DECLARATION

I hereby declare that; this internship has been done by me under supervision of **Dr. Mohammed Nadir Bin Ali, Registrar (In-Charge)** of Daffodil International University. I am also declaring that this project or any part of there has never been submitted anywhere else for the award of any educational degree like, B.Sc., M.Sc., Diploma or other qualifications.

Supervised By

16/10/22

Dr. Mohammed Nadir Bin Ali
Registrar (In-Charge)
Daffodil International University

Submitted By

Fahim

Fahim Abdul Aziz
ID: 183-16-360
Department of CIS
Daffodil International University

ACKNOWLEDGEMENT

Alhamdulillah, with the help of the almighty Allah, I am able to successfully complete the project despite experiencing multiple challenges. In order to complete this variously challenging project, many credible people would need to be acknowledged.

I want to express my gratitude to my parents for providing me with such a great opportunity to pursue my favorite subject, computer science. My self-esteem, confidence, skills, and passion for learning all significantly enhanced as a result of this opportunity.

I would like to express my gratitude to **Dr. Md. Nadir Bin Ali, Registrar, Head of IT at Daffodil International University**, for inspiring my interest in computer networks. His supervision, advice, and lessons enhanced my interest in network-based projects. Made it easy to complete the project.

I want to thank **Md. Sarwar Hossain Mollah from the Daffodil International University's Department of Computing and Information System (CIS)**. I was able to successfully complete a wonderful networking project-based internship. Thanks to sir's acceptance of the internship at ISP.

Without the help and guidance of **Daffodil Online Ltd. (DOL)** employees, my project-based internship won't be any better. For allowing me to finish this project, I'm grateful to the team.

DEDICATION

This project-based internship is intended for students majoring in computer science, cybersecurity, network engineering, and networking who are hesitant to choose an internship in the field or are struggling to choose a career path.

Dedicated to those looking to change the world and advance technology, such as IoT, AI, and command scripting in the field of computer networks.

Dedicated to those who value cyber security and can reduce network vulnerabilities and weaknesses. can protect against cyber-attacks.

This internship report is intended for all future computer science students.

ABSTRACT

Configuring the ISP is very common and simple with routers and switches. Every student of computer science develops an interest in networking and chooses to complete this topic. But throughout my undergraduate studies, I became interested in computer networks and network security. I subsequently added the security topic to the ISP setup topic in order to complete my undergraduate degree. Device security is challenging, despite how easy it is to configure a device. Therefore, I set up firewalls to secure this ISP configuration. The way this firewall was set up was really cool. Firewall definitely captured my attention. While I was an intern, I made the decision to take on this challenging project.

As a challenge, I decide to add additional routers, switches, and firewalls where everyone uses a single network device. I'm hoping that the interest in network sector projects will grow as a result of this project and additional interested individuals.

TABLE OF CONTENTS

CONTENTS **PAGES**

CHAPTER **PAGE NO**

LIST OF FIGURES

FIGURES **PAGE NO**

LIST OF ABBREVIATIONS

ISP	INTERNET SERVICE PROVIDER
DOL	DAFFODIL ONLINE LIMITED
IIG	INTERNATIONAL INTERNET GATEWAY
CISCO	COMPUTER INFORMATION SYSTEM COMPANY
COM	COMMUNICATION PORT
OS	OPERATING SYSTEM
ISO	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
GUI	GRAPHICAL USER INTERFACE
DDOS	DISTRIBUTED DENIAL OF SERVICE
IP	INTERNET PROTOCOL
NAT	NETWORK ADDRESS TRANSLATION
CLOUD	COMMUNITIES AND LIBRARIES ONLINE UNION DATABASE
WEB	WORLD WIDE WEB
VLAN	VIRTUAL LOCAL AREA NETWORK
WAN	WIDE AREA NETWORK
LAN	LOCAL AREA NETWORK
FTP	FILE TRANSFER PROTOCOL
PPPOE	POINT TO POINT PROTOCOL OVER ETHERNET
VPN	VIRTUAL PRIVATE NETWORK
IPSEC	INTERNET PROTOCOL SECURITY
PPTP	POINT-TO-POINT TUNNELING PROTOCOL
NOC	NETWORK OPERATIONS CENTER
AWS	AMAZON WEB SERVICES
VMWARE	VIRTUAL MACHINE WARE
EVE-NG	EMULATED VIRTUAL ENVIRONMENT NEXT GENERATION
DMZ	DEMILITARIZED ZONE
ESXI	ELASTIC SKY X INTEGRATED
GGC	GOOGLE GLOBAL CACHE
FNA	FACEBOOK NETWORK APPLIANCE
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
BGP	BORDER GATEWAY PROTOCOL
RIP	ROUTING INFORMATION PROTOCOL
OSPF	OPEN SHORTEST PATH FIRST
L2TP	LAYER 2 TUNNELING PROTOCOL

GRE	GENERIC ROUTING ENCAPSULATION
DNS	DOMAIN NAME SERVER
SSL	SECURE SOCKETS LAYER
QOS	QUALITY OF SERVICE
MAC	MEDIA ACCESS CONTROL ADDRESS
RJ45	REGISTERED JACK-45
USB	UNIVERSAL SERIAL BUS
PING	PACKET INTERNET/INTER NETWORK GROPPER
SSH	SECURE SHELL
TELNET	TELETYPE NETWORK PROTOCOL
HTTPS	HYPERTEXT TRANSFER PROTOCOL SECURE
SD-WAN	SOFTWARE-DEFINED WIDE AREA NETWORK
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
ARP	ADDRESS RESOLUTION PROTOCOL
PAP	PASSWORD AUTHENTICATION PROTOCOL
MITM	MAN IN THE MIDDLE
URL	UNIFORM RESOURCE LOCATOR
MBPS	MEGABITS PER SECOND

CHAPTER 1
INTRODUCTION

1.1 Introduction

Inter connected electronic devices are called internet. Internet service provider serve the global internet connection to a wide area network from a router to user end computer. There are several routers, among them Mikrotik is a very popular, user-friendly router and OS to operate in Bangladesh most. Most of the ISP, enterprise network management operate with Mikrotik.

It is just as easy for hackers to hack, get illegal access, and process large network traffic overflow to bring down an ISP. Device vulnerability, port security, device log history, packet filtering, and other factors must be considered in order to keep it safe.

1.2 Objectives

Information communication technology is currently one of the most important requirements for establishing a career, and security is also a matter to consider. The goal of this hands-on learning about internet connectivity, usages, network securities by Mikrotik, Cisco devices and Fortigate Firewalls:

- To serve the internet service to clients via proper bandwidth management, client account, passwords, dynamic host IP addresses etc. by Mikrotik device and OS. Also securing the Mikrotik device from getting unauthorized access.
- Configuring switches to distribute network connections at ISP.
- Configuring firewalls to protect my ISP devices and servers from DDoS attack, unauthorized network traffics and access.

1.3 Motivation

Studying computer networks, network security, cloud computing, and enterprise network management courses during my undergraduate degree brought me encouragement. During my studies, I learned about security, backup solutions, configuration, and other related topics. I discovered a way to apply these skills to this internship. Additionally, this project-based implementation is expandable to additional computer network areas.

1.4 Report Layout

- **Chapter 1:** Objectives of my project-based internship, motivation.
- **Chapter 2:** Occurred internship company’s introduction, their roles, services, strengths and previously done projects.
- **Chapter 3:** My project-based internship planning, goals, features, challenges, devices.
- **Chapter 4:** Configuration terms and figures of my project.
- **Chapter 5:** Results, outputs of my configured project.
- **Chapter 6:** Conclusion, future scalability of this project.

CHAPTER 2
COMPANY’S PROFILE

2.1 About Daffodil Online Ltd.

Daffodil Online Ltd. is an internet service provider which is also a datacenter for various businesses and organizations. It is located in Dhanmondi, Dhaka, at the Islam Tower. They started their journey in 2002. Apart from several other ISPs, it is presently one of Bangladesh's leading ISPs. DOL provides internet access to local clients in a variety of packages. Serves organizations both inside and outside of Dhaka, companies' internet, datacenter facilities such as bandwidth, server, cloud storage, and etc. DOL's employees, like those who supply internet services, are very skilled at troubleshooting for their clients and offer a variety of customer services. Internship, training, and lab facilities are also available for students and employees. They train basic to expert networking skills using networking devices.

2.2 Products and Services

- Datacenter
- ISP support
- Web, domain hosting
- FTP server
- Remote troubleshooting
- Internship, Training vendor academy with Mikrotik, Cambium
- Lab room with Mikrotik, Cisco, Juniper etc. devices
- Cache Servers of Google, Facebook, Internet etc.

2.3 Company’s Strengths

- 24/7 Customer support
- Strong relationship management with clients
- Expert employees for services like datacenter servers, routing, hosting, cloud, firewall etc.
- High integrates
- Expert trainer
- Server room with cooling system, backup electricity generators.

2.4 Company’s Projects

- Wide area PPPoE client internet connections at Mohammadpur, Lalmatia, Dhanmondi, Kolabagan etc.
- Company, enterprise internet connections to Chandpur, Rajshahi
- VPN, PPTP connections to banks.
- AWS clouds services to Daffodil family.
- Mikrotik lab training to international students.
- Mikrotik lab training for 3 years by online and offline.

2.5 Schedule of ISP

- The schedule for employee’s employment includes both day and night shifts.
- The day shift office is open from 8 AM to 8 PM.
- NOC supports for the night shift as requested by clients.
- Fewer people are at work on Friday.
- The cable management team sets up PPPoE connections from 10 am to 2 pm every day.

CHAPTER 3

INTERNSHIP PROJECT ACTIVITIES

This chapter explains how I started to understand, how a network diagram for an ISP should be designed. How internet access is provided by IIGs, connected by a variety of cable methods, and then delivered to internal offices and locations outside of the ISP. Discovered how an ISP provides its clients with an internet connection. Datacenter servers, different server varieties, operating systems, policies, routing, and firewall, router, switch, and other networking devices and their models. ISP protection for my setup includes Fortinet Fortigate firewall and Mikrotik devices.

3.1 Internship Activities

Month 1

- Studied and reviewed the fundamentals of computer networks
- Cable configuration, management, and connections
- Learned about networking devices including routers and switches
- Tasks and office work flows
- Troubleshooting for clients
- Get to know client services

Month 2

- Configured Mikrotik router
- Configured Cisco switch
- Configuration by web GUI and GUI tool “WinBox”
- Configuration by console command
- Device troubleshooting

Month 3

- Firewall concepts
- Introduced to Fortigate firewall
- Firewall configuration
- Secured Mikrotik, Cisco devices
- Configured IPSec VPN

Month 4

- Introduced to VMWare
- VMWare, EVE-NG setup, configuration
- Practiced configuration via VMWare

Month 5

- Configured my complete project at DOL

Month 6

- Configured my complete project on VMWare, EVE-NG

3.2 Planning for My ISP Setup and Firewalls

- Four Mikrotik Routers for core router, backup router, distribution router, PPPoE router for clients to serve
- Two Cisco switches for VLAN, VLANs into office, lab connections
- Three Fortigate Firewalls for VPN connection, WAN, DMZ protections
- Laptop, office, lab PCs to implement, test connections
- Outside office Mikrotik router for IPSec VPN connection

3.3 Challenges

- Internships on the topic of ISP setup with Mikrotik projects were completed multiple times. Now I want to make this project-based internship exciting and challenging by including firewalls. I covered all essential networking topics in my undergraduate studies, and now it's time to put those theoretical learnings into practice in this internship.
- ISPs do not depend only on a single router. It is suitable for a variety of distribution-based routers and switches. By thinking in this manner, I will be able to work with routers as they should be. This network diagram will include zones such as OUTSIDE, DMZ, and INSIDE. For these zones, several firewall policies must be defined.
- Two WAN connections will connect to the Fortigate firewall first, just as professional ISP configurations do.
- I must first create VLANs on the firewall before creating Cisco switches for distributing VLANs.
- IPSec VPN tunnel from a firewall to the outside of a Mikrotik router for testing purposes.

3.4 OS

3.4.1 Mikrotik OS

Mikrotik and Fortigate devices operating systems are easy to understand and easy to use. Instead of using a command line interface like Cisco or Juniper, the Mikrotik OS's graphical user interface (GUI) makes configuration incredibly simple. Officially, Mikrotik offers WinBox, an open-source program, for configuring their products. Simply launch WinBox after LAN cable connection to the device.

3.4.2 Fortigate OS

FortiOS offers standard security policy deployment and enforcement, entirely expands graphical user interfaces and control panels, and enables centralized management throughout the entire distributed network. The security mode, routings, connected devices traffic shapper, and CPU usages are all described on this OS's dashboard.

To keep their devices updated, this OS offers a number of firmware and OS upgrades. FortiOS7 is now Fortigates current operating system.

3.4.3 Cisco OS

A very well OS is Cisco IOS, which Cisco provides for its routers and switches. Executed using commands from the command line. For most Linux users, a configuration mechanism that is friendly to the command line is available. Cisco IOS is preferred by users for quick, dependable configurations.

3.4.4 VMWare OS

VMware is a virtualization and cloud computing program. The business's main office is in Palo Alto, California. The ESX/ESXi x86 bare-metal hypervisor is the foundation for VMware's virtualization products.

VMware Server sets up a hypervisor on the virtualization server so that multiple virtual machines (VMs) can run on the same physical server. Because each VM can run its own operating system, a physical server can support many OSes. All virtual machines on a single physical server share resources like networking and RAM.

3.5 Features

3.5.1 ISPs Mainly Use Mikrotik Routers for its Incredible Features

- Bandwidth management
- Client connection services: PPPoE, PPTP
- Queue for extra bandwidth services to each client from GGC, FNA, INT cache servers
- Firewalls NAT, application blocking by rules
- Device log management, backups
- Ethernet port naming, addressing
- DHCP pool by addressing
- Routing
- Multiple connections load balance and failover
- It affords most popular routing BGP, RIP, OSPF easily
- Devices ports can be used as bridge mode
- Device can be used as switch by all ports as bridge mode
- VLANs like tagged vlan, untagged vlan
- IPv6 addressing, DHCP pool
- WLAN, hotspot server
- LT2P, GRE, IPSec VPNs
- Port forwarding
- Schedule backups via email/to syslog server

3.5.2 Fortinet Fortigate Firewall Features

- Profile-based, Policy-based policies
- Interface naming, zone selection
- Dashboard
- Notification panel, alert
- Multiple connections load balancing, failover
- Application, services, DNS filtering
- Custom address range including
- Dynamic IP Pool for NAT
- Virtual IP Pool
- Source static NAT
- Device detection
- Log monitoring, reporting
- Routing

- VLAN
- DDoS Policy
- Site to Site IPSec VLAN
- Port forwarding
- SSL certifications
- Antivirus scan
- Bandwidth traffic shaper
- DHCP Pool

3.5.3 Cisco Switch Features

- OSI Layer 2, Layer 3 mode
- Rack-mountable
- Multiple ether ports, giga ports
- VLAN
- Remote Management Protocol Supported
- IPV6 support, IPV6 rely agent
- QoS
- Port security
- MAC binding

3.6 Device Details

3.6.1 Mikrotik Router Device Details

The Mikrotik RB2011 is a low-cost router device with 10 ethernet ports that display lights according on their usage. This router device is powered by RouterOS, is designed for indoor use, and comes in a variety of casings with a multitude of configurations.

This router has four roles in my ISP configuration: main router, backup router, distributed router, and PPPoE router.

Figure 3.6.1: Mikrotik RB2011 router device

3.6.2 Fortigate Firewall Device Details

The next-generation firewall from Fortinet, the Fortigate FG-30E, has 5 ports. Working with FortiOS7. Extremely light weight while not a router, it does support routings. Port definitions are possible for protect zone responsibilities such OUTSIDE, DMZ, and INSIDE. With its graphical user interface, dashboard, policies, application control, filtering, etc., this modern firewall is easy to operate. It is set up on the WAN and DMZ sides for my ISP setup. My ISP will be protected in this manner both inside and out.

Figure 3.6.2: Fortigate FG-30E firewall device

3.6.3 Cisco Switch Device Details

The Cisco switch SG350X-24PD is a medium, weight device that is primarily designed to use at home, offices, and other small spaces. This compact device functions as a router or switch. This device comes with 24 Ethernet ports. Operates in both as a layer 2 or layer 3 switch.

In my ISP arrangement, this device serves VLANs from firewall to lab and office computer devices.

Figure 3.6.3: Cisco SG350X-24PD switch device

CHAPTER 4

DESIGN AND CONFIGURATION OF MY ISP PROJECT

4.1 Diagram of This ISP Setup Project

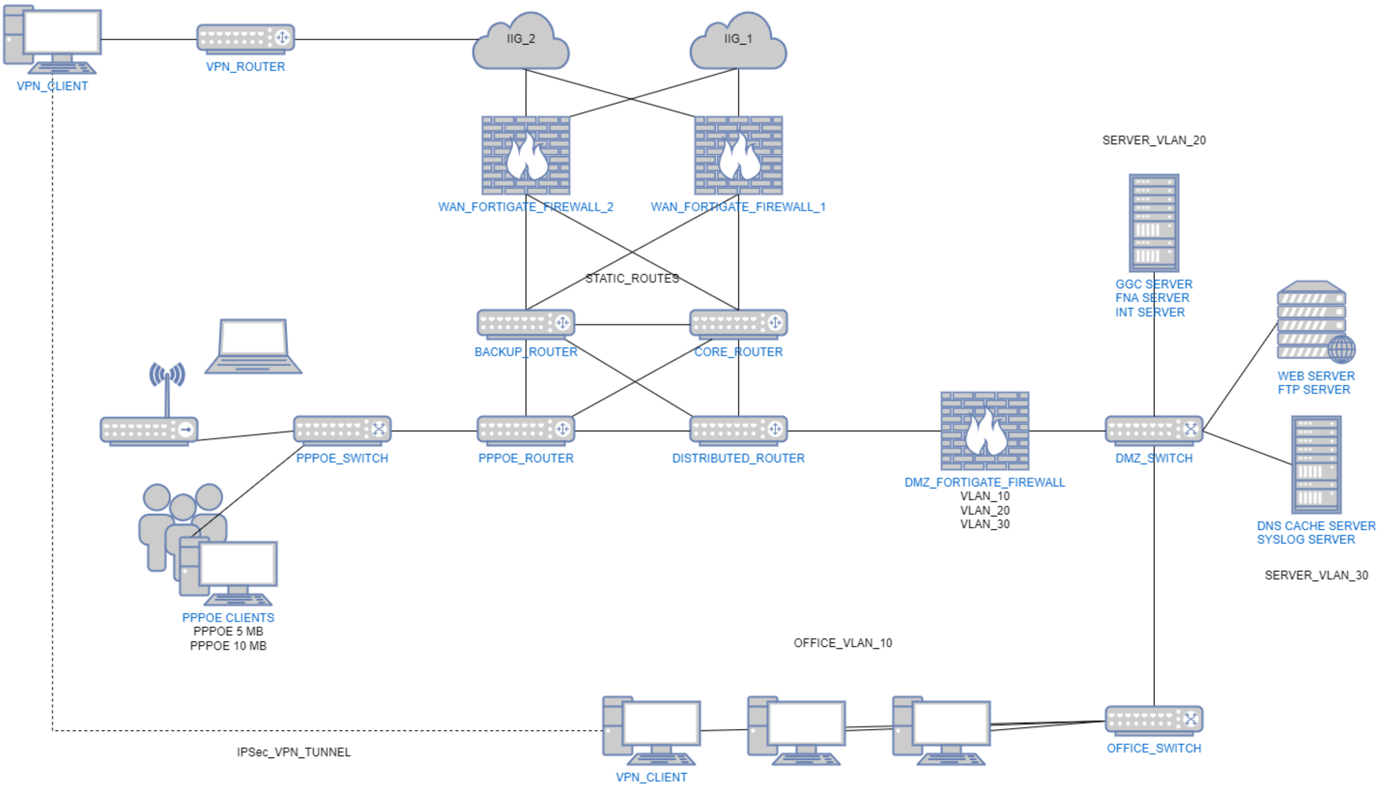


Figure 4.1: Diagram of ISP setup and securing with Mikrotik, Cisco and Fortigate devices

4.2 First WAN Connections for Two Fortigate Firewalls

- At first download putty open-source software for console connection.
- Device connects using RJ45 cable from computer USB to device console port.

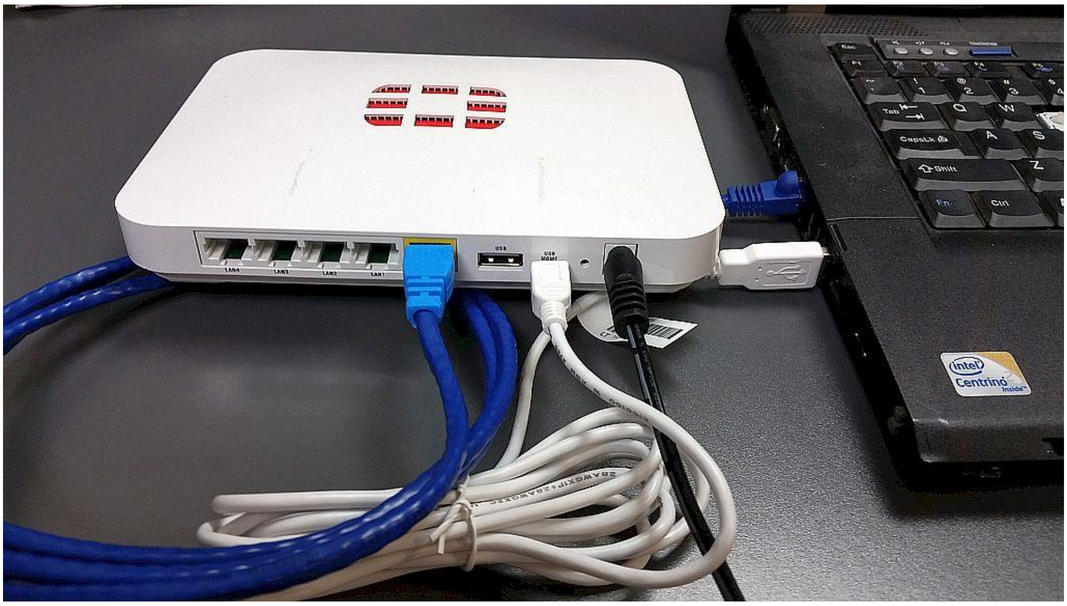


Figure 4.2: Firewall device connection to computer for configuration

4.2.1 Putty Console Setup

- Open ‘Device Manager’ of windows
- Expand ‘Ports’, identify COM serial number
- Open ‘Putty’
- ‘Putty’ connects to COM serial port

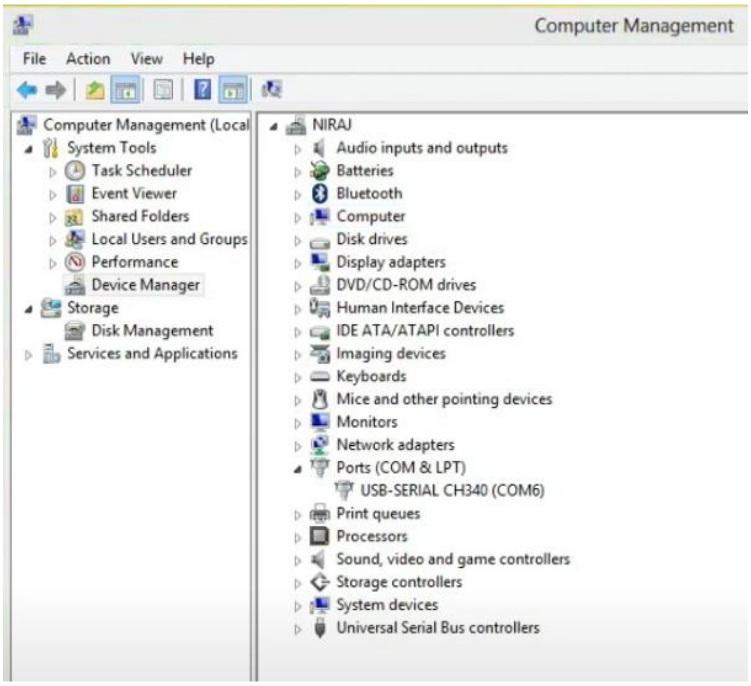
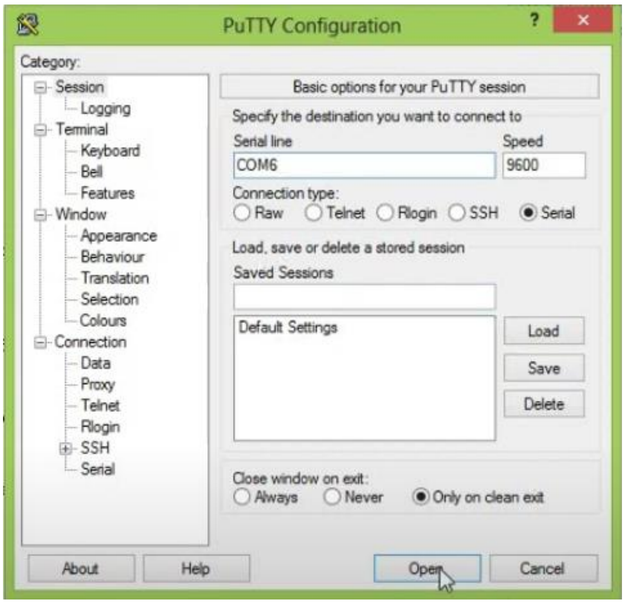


Figure 4.2.1.1: Firewall device COM port identification by ‘Device Manager’



Specify the destination you want to connect to

Serial line: COM6

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

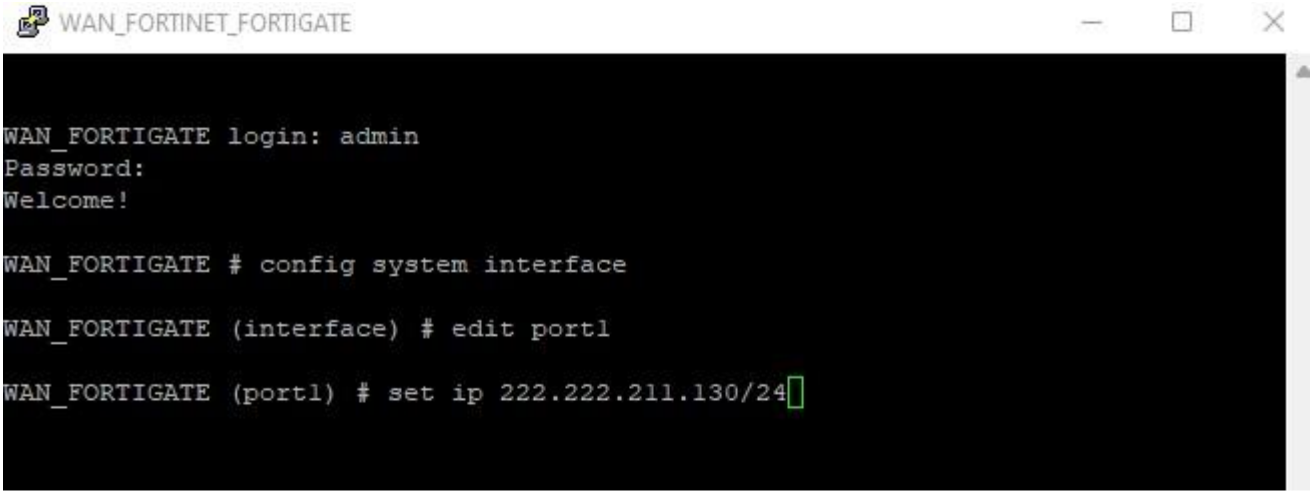
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 4.2.1.2: COM port connection by ‘Putty’

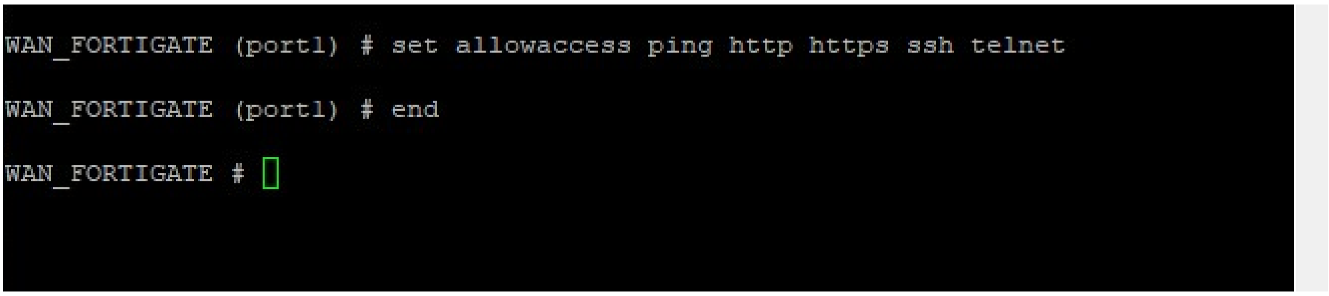
- Command prompt terminal opens, needs to login as admin. No password required for first login. Needs to set new password, confirm password
- Configure system interface of connected wan port with assigning ip address



```
WAN_FORTIGATE login: admin
Password:
Welcome!

WAN_FORTIGATE # config system interface

WAN_FORTIGATE (interface) # edit port1

WAN_FORTIGATE (port1) # set ip 222.222.211.130/24
```

Figure 4.2.1.3: Firewall port configuration by console mode

- Set allow access to ping, ssh, telnet, http, https



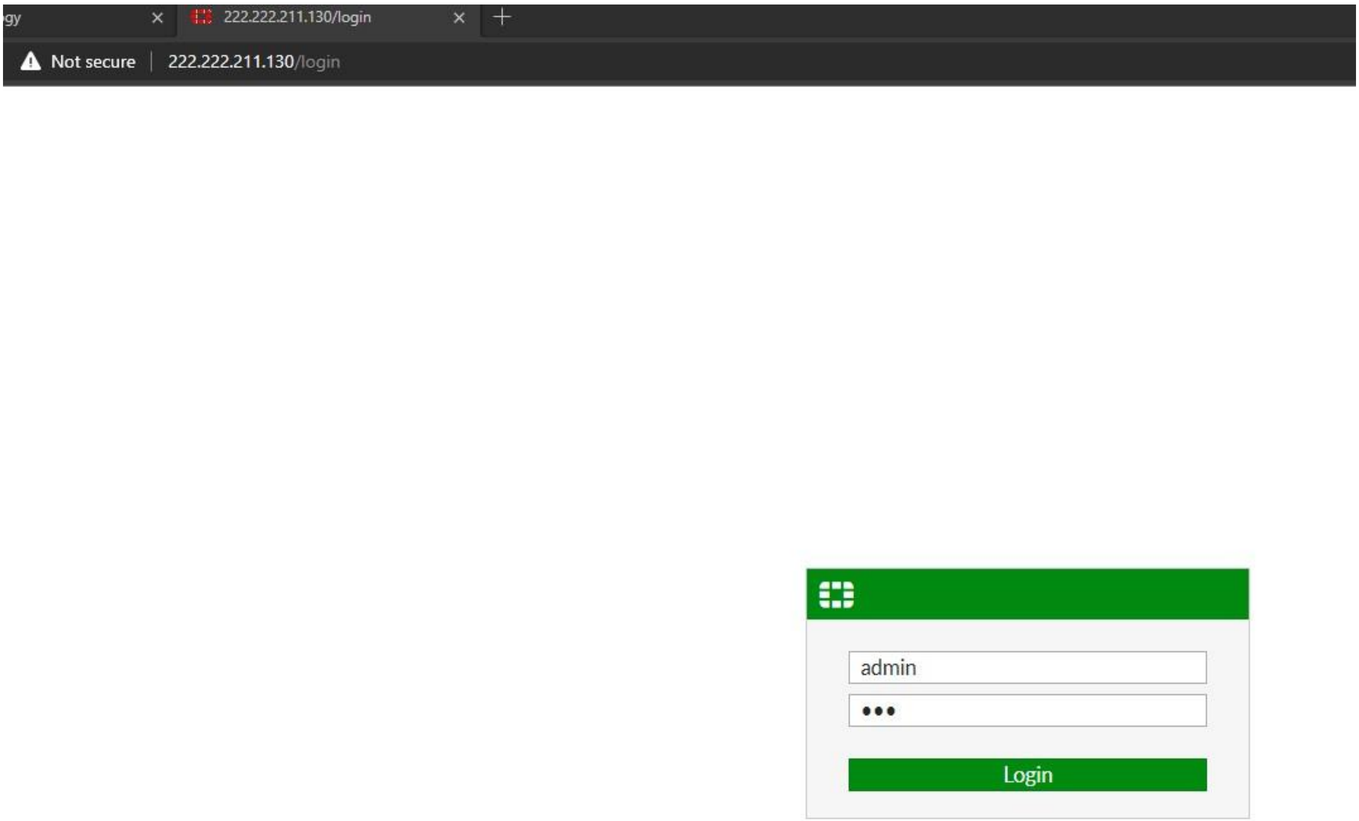
```
WAN_FORTIGATE (port1) # set allowaccess ping http https ssh telnet

WAN_FORTIGATE (port1) # end

WAN_FORTIGATE #
```

Figure 4.2.1.4: Browser accessible configuration

- Now firewall can be accessed from browser using assigned ip address

4.2.2 Browser Access to Firewall

- Open browser
- Type assigned firewall ip address on http address bar
- Login to firewall dashboard by assigned username and password



gy ×   222.222.211.130/login ×

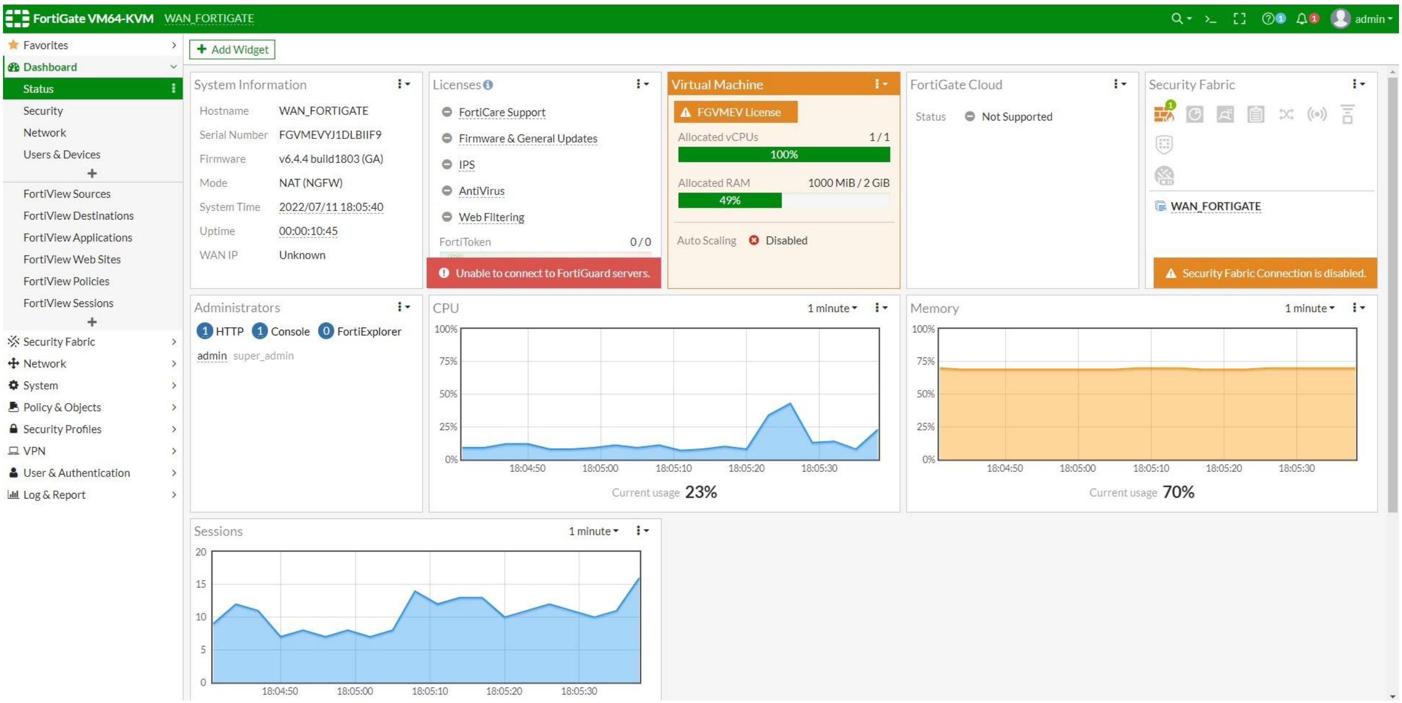
Not secure | 222.222.211.130/login

admin

•••

Figure 4.2.2.1: Accessing firewall via browser

- Rename firewall after login.
- Dashboard of Fortigate firewall



System Information

Hostname WAN_FORTIGATE
Serial Number FGVMEVYJ1DLBIIF9
Firmware v6.4.4 build1803 (GA)
Mode NAT (NGFW)
System Time 2022/07/11 18:05:40
Uptime 00:00:10:45
WAN IP Unknown

FortiToken 0 / 0

Unable to connect to FortiGuard servers.

Virtual Machine

FGVMEV License
Allocated vCPUs 1 / 1 100%
Allocated RAM 1000 MiB / 2 GiB 49%
Auto Scaling Disabled

FortiGate Cloud

Status Not Supported

WAN_FORTIGATE

Security Fabric Connection is disabled.

1 HTTP 1 Console 0 FortiExplorer
admin super_admin

Current usage 23%

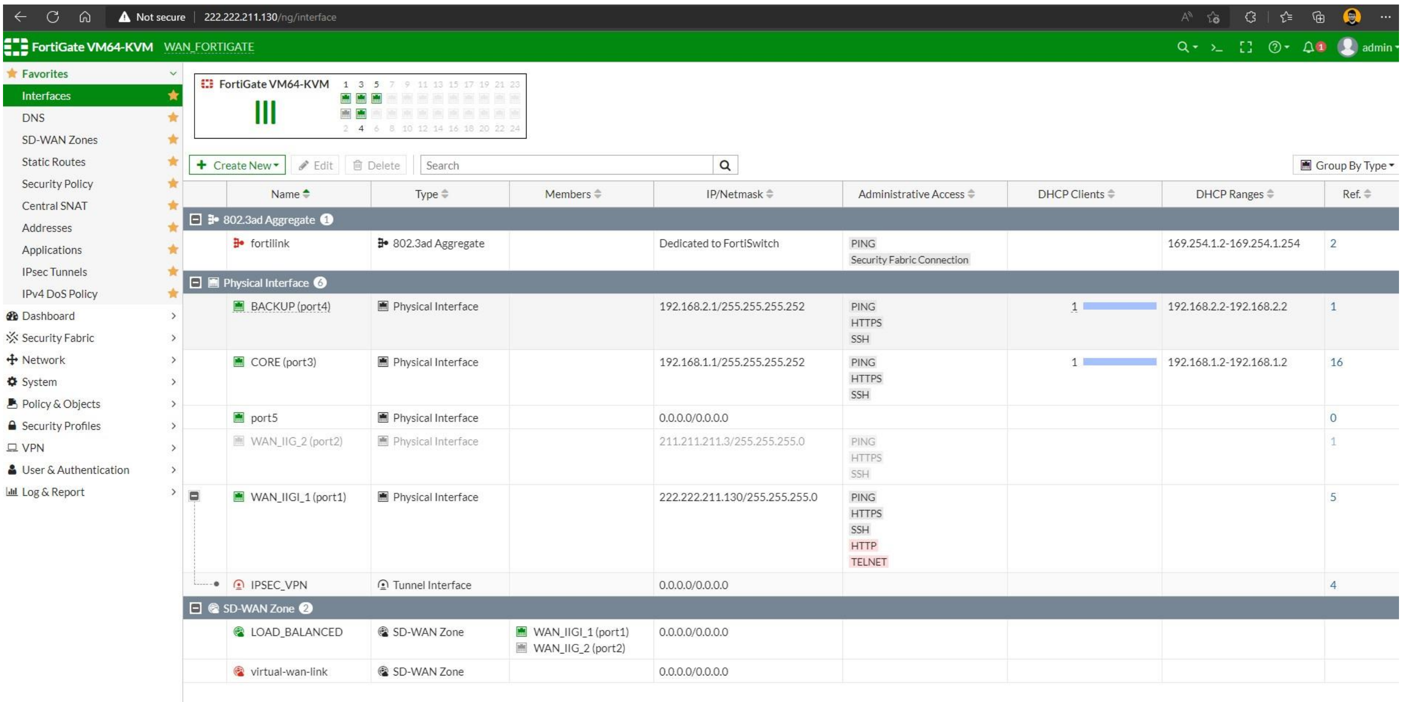
Current usage 70%

Figure 4.2.2.2: WAN firewall dashboard

4.2.3 Network Configuration

4.2.3.1 Interface Renames, IP Address Assigning, DNS Assigning

- Open ‘Network’ > ‘Interfaces’ > click on port by connected to configure
- Assign ip address, rename interface port name, set DNS
- Interfaces of port renamed to ‘CORE’, ‘BACKUP’, ‘WAN_IIG_1’, ‘WAN_IIG_2’

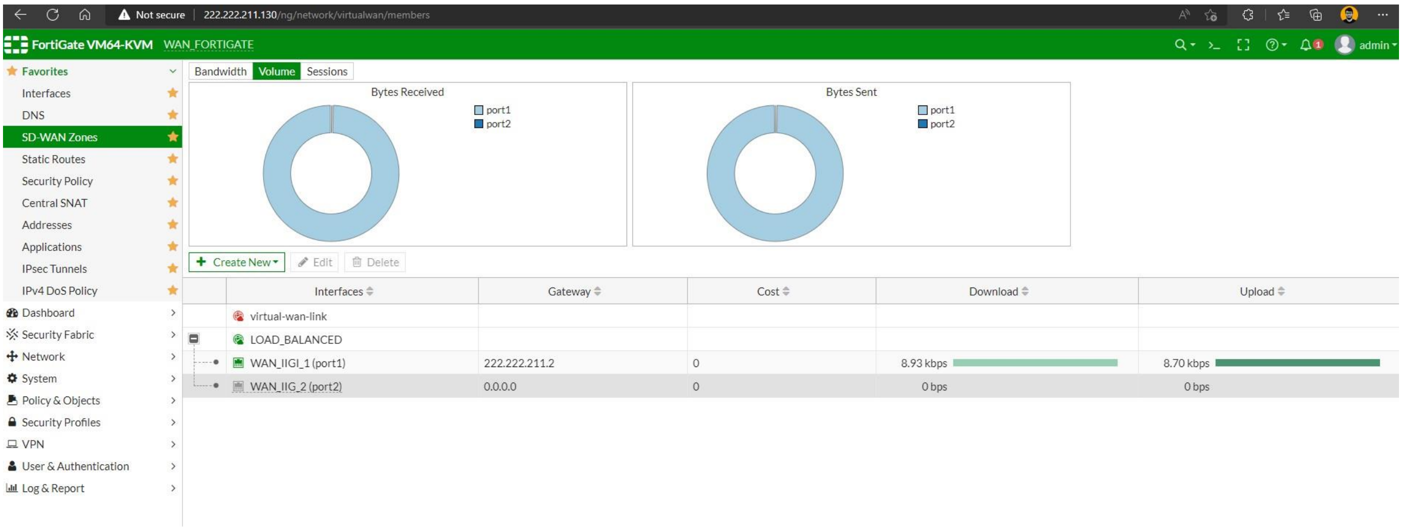


Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Physical Interface 6							
BACKUP (port4)	Physical Interface		192.168.2.1/255.255.255.252	PING HTTPS SSH	1	192.168.2.2-192.168.2.2	1
CORE (port3)	Physical Interface		192.168.1.1/255.255.255.252	PING HTTPS SSH	1	192.168.1.2-192.168.1.2	16
port5	Physical Interface		0.0.0.0/0.0.0.0				0
WAN_IIG_2 (port2)	Physical Interface		211.211.211.3/255.255.255.0	PING HTTPS SSH			1
WAN_IIGI_1 (port1)	Physical Interface		222.222.211.130/255.255.255.0	PING HTTPS SSH HTTP TELNET			5
IPSEC_VPN	Tunnel Interface		0.0.0.0/0.0.0.0				4
SD-WAN Zone 2							
LOAD_BALANCED	SD-WAN Zone	WAN_IIGI_1 (port1) WAN_IIG_2 (port2)	0.0.0.0/0.0.0.0				
virtual-wan-link	SD-WAN Zone		0.0.0.0/0.0.0.0				

Figure 4.2.3.1: WAN firewall interface port names, ip addresses

4.2.3.2 Load Balance Configuration by SD WANS

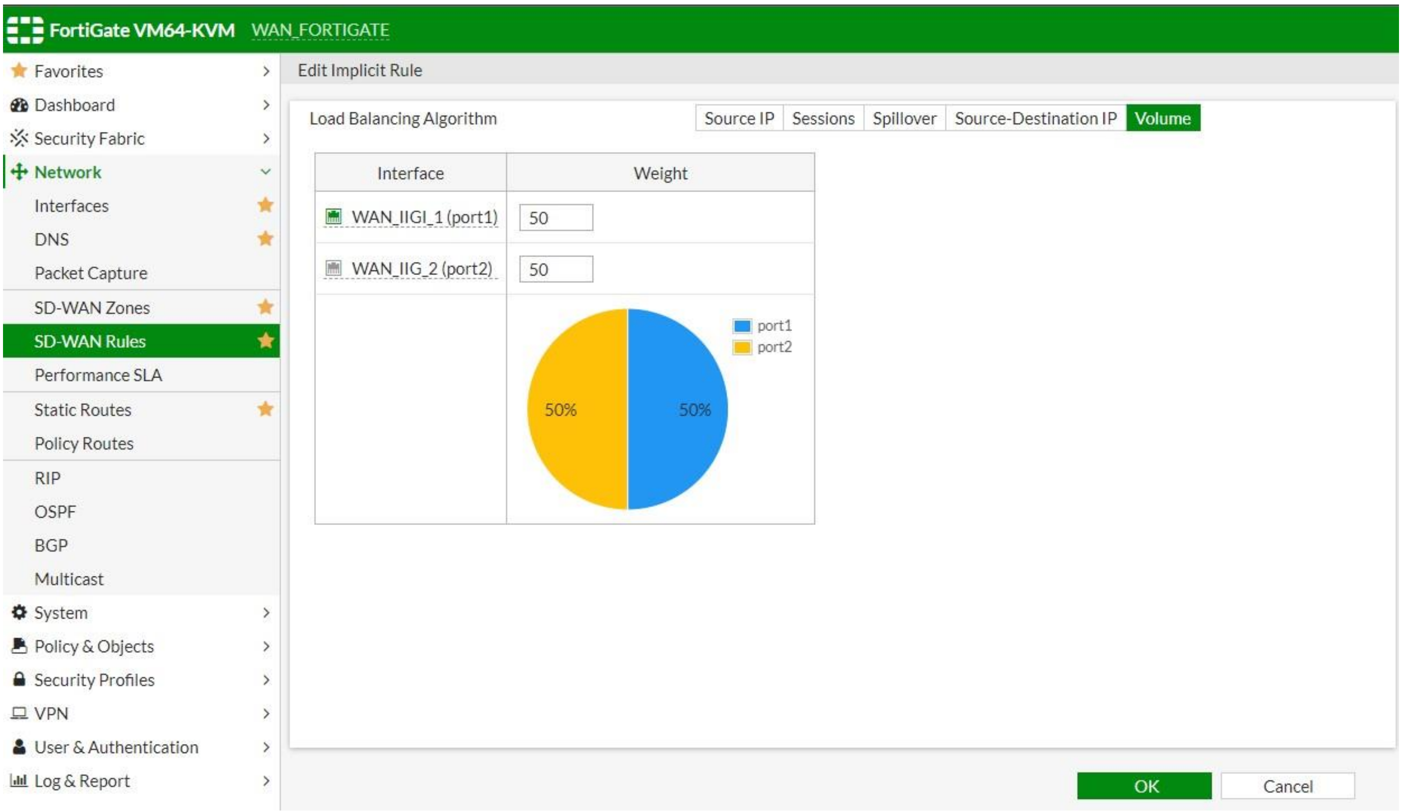
- Open ‘Network’ > ‘SD WAN Zones’ > click on ‘Create Zone’ to configure
- Type name, add ‘Interface’ of connected WAN ports
- Configuration named to ‘LOAD BALANCE’



Interfaces	Gateway	Cost	Download	Upload
virtual-wan-link				
LOAD_BALANCED				
WAN_IIGI_1 (port1)	222.222.211.2	0	8.93 kbps	8.70 kbps
WAN_IIG_2 (port2)	0.0.0.0	0	0 bps	0 bps

Figure 4.2.3.2.1: Load balance dashboard

- Open ‘Network’ > ‘SD WAN Rules’ > click on created zone to configure
- Set ‘Volume’ of two wan ports to ‘50%’



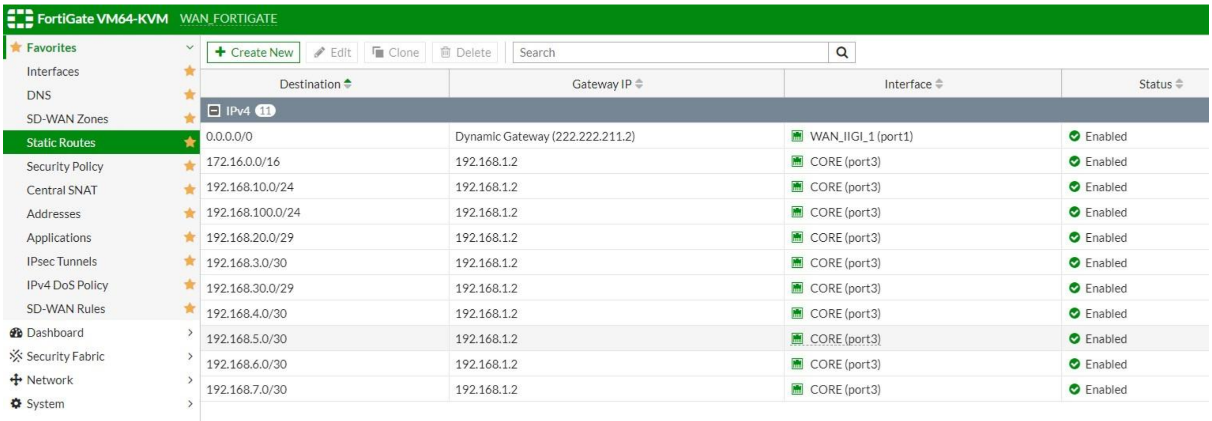
Load Balancing Algorithm: Source IP | Sessions | Spillover | Source-Destination IP | **Volume**

Interface	Weight
WAN_IIGI_1 (port1)	50
WAN_IIG_2 (port2)	50

Figure 4.2.3.2.2: Load balance configuration

4.2.3.3 Static Routes

- Open ‘Network’ > ‘Static Routes’ > click on ‘Create New’ to configure
- Add ‘Ip address’ > ‘Gateway’ > ‘Interface’ and save



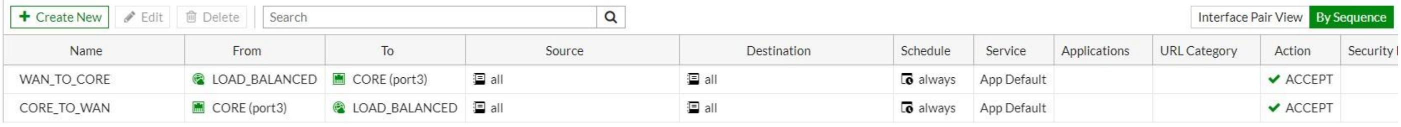
Destination	Gateway IP	Interface	Status
IPv4 11			
0.0.0.0/0	Dynamic Gateway (222.222.211.2)	WAN_IIGI_1 (port1)	Enabled
172.16.0.0/16	192.168.1.2	CORE (port3)	Enabled
192.168.10.0/24	192.168.1.2	CORE (port3)	Enabled
192.168.100.0/24	192.168.1.2	CORE (port3)	Enabled
192.168.20.0/29	192.168.1.2	CORE (port3)	Enabled
192.168.3.0/30	192.168.1.2	CORE (port3)	Enabled
192.168.30.0/29	192.168.1.2	CORE (port3)	Enabled
192.168.4.0/30	192.168.1.2	CORE (port3)	Enabled
192.168.5.0/30	192.168.1.2	CORE (port3)	Enabled
192.168.6.0/30	192.168.1.2	CORE (port3)	Enabled
192.168.7.0/30	192.168.1.2	CORE (port3)	Enabled

Figure 4.2.3.3: Static routes

4.2.4 Policy and Objects Configuration

4.2.4.1 Defining Security Policies for Incoming and Outgoing Interfaces

- Open ‘Policy and Objects’ > ‘Security Policy’ > click on ‘Create New’ to configure
- Rename policy > select ‘From interface’ and ‘To interface’ > select ‘Source’ ip addresses to ‘all’ > select ‘Destination’ ip addresses to ‘all’ > Action ‘ACCEPT’
- Policy objects named to ‘WAN_TO_CORE’, ‘CORE_TO_WAN’, ‘BACKUP_TO_WAN’ and ‘WAN_TO_BACKUP’

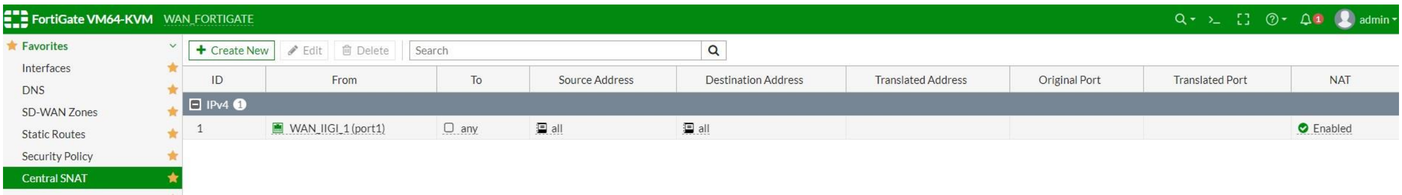


Name	From	To	Source	Destination	Schedule	Service	Applications	URL Category	Action	Security I
WAN_TO_CORE	LOAD_BALANCED	CORE (port3)	all	all	always	App Default			✓ ACCEPT	
CORE_TO_WAN	CORE (port3)	LOAD_BALANCED	all	all	always	App Default			✓ ACCEPT	

Figure 4.2.4.1: Firewall policies for source, destinations

4.2.4.2 Central Static Nat for Outgoing Interface from Incoming Interface

- Open ‘Policy and Objects’ > ‘Central SNAT’ > click on ‘Create New’ to configure
- Name > add interface to ‘To’ > source address to ‘all’ > destination address to ‘all’

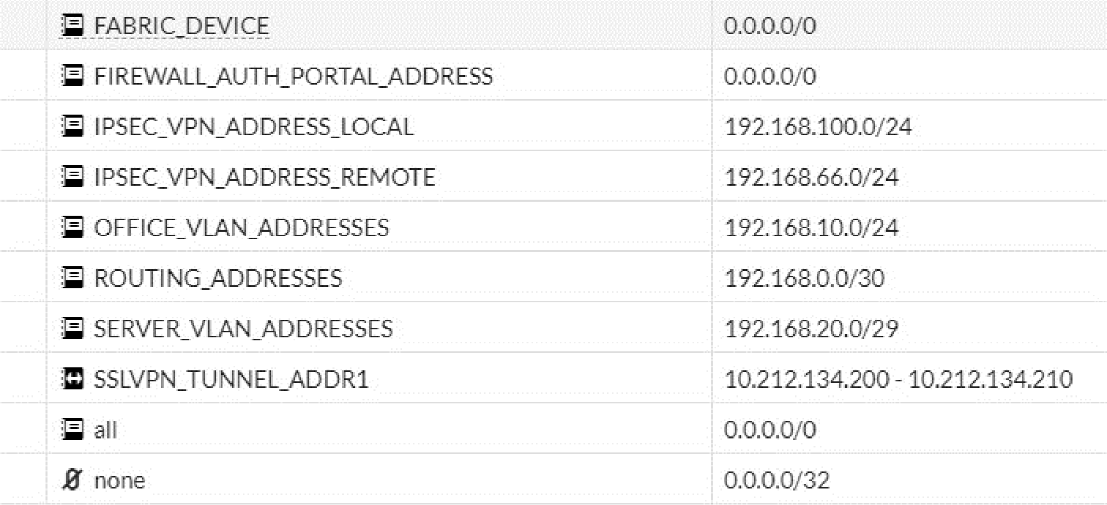


ID	From	To	Source Address	Destination Address	Translated Address	Original Port	Translated Port	NAT
IPv4 1								
1	WAN_IIGI_1 (port1)	any	all	all				Enabled

Figure 4.2.4.2: Static Nat configured

4.2.4.3 Custom IP Address Ranges for Security

- Open ‘Policy and Objects’ > ‘Addresses’ > click on ‘Create New’ to configure
- Name address > add ‘ip address’ with subnet > save

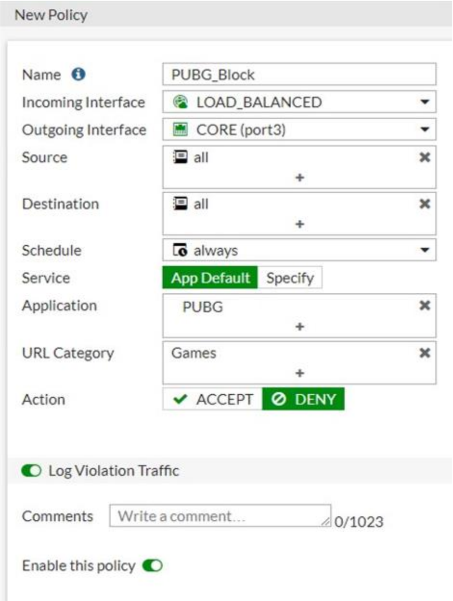


FABRIC_DEVICE	0.0.0.0/0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0
IPSEC_VPN_ADDRESS_LOCAL	192.168.100.0/24
IPSEC_VPN_ADDRESS_REMOTE	192.168.66.0/24
OFFICE_VLAN_ADDRESSES	192.168.10.0/24
ROUTING_ADDRESSES	192.168.0.0/30
SERVER_VLAN_ADDRESSES	192.168.20.0/29
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210
all	0.0.0.0/0
none	0.0.0.0/32

Figure 4.2.4.3: Custom ranged ip addresses for firewall

4.2.4.4 Blocking Application on Firewall

- Open ‘Policy and Objects’ > ‘Application’ > click on ‘Create New’ to configure
- Name application > select ‘Incoming interface’ > select ‘Outgoing interface’ > select source address to ‘all’ > select destination to ‘all’ > select ‘Schedule’ to ‘always’ > select service ‘App Default’ > select ‘Application’ > select ‘URL Category’ > select ‘Action’ to ‘Deny’ > select ‘Log Violation Traffic’ > select ‘enable this policy’ > save
- Created Application block configuration for “PUBG”



New Policy

Name	PUBG_Block
Incoming Interface	LOAD_BALANCED
Outgoing Interface	CORE (port3)
Source	all
Destination	all
Schedule	always
Service	App Default ● Specify
Application	PUBG
URL Category	Games
Action	✓ ACCEPT ● DENY

● Log Violation Traffic

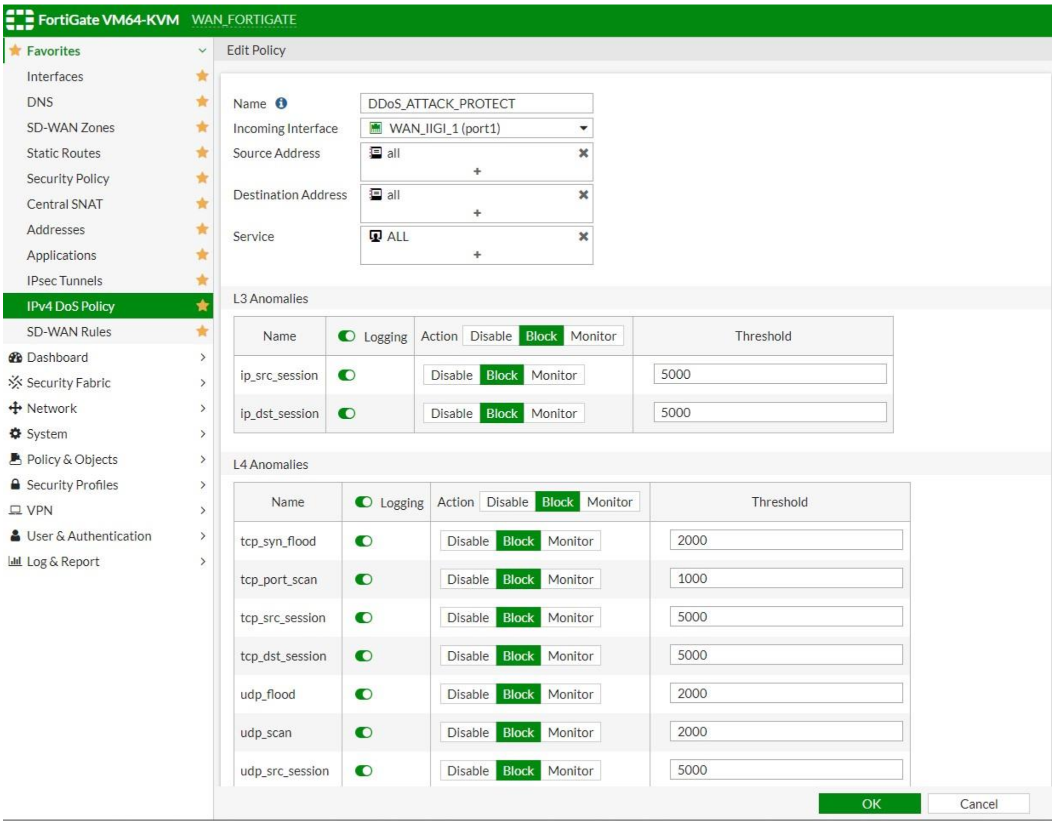
Comments: Write a comment... 0/1023

Enable this policy ●

Figure 4.2.4.4: Blocking PUBG on firewall applications

4.2.4.5 DDoS Attack Prevention Policy

- Open ‘Policy and Objects’ > ‘IPV4 DDoS Policy’ > click on ‘Create New’ to configure
- Name > select ‘Incoming Interface’ > select ‘Source Address’ to ‘all’ > select ‘Destination Address’ to ‘all’ > select ‘Source’ to ‘ALL’ > enable all ‘logging’ and select to ‘Block’ > set ‘icmp_sys_flood’ Threshold to ‘1000’ > save



Edit Policy

Name: DDoS_ATTACK_PROTECT
Incoming Interface: WAN_IIGI_1 (port1)
Source Address: all
Destination Address: all
Service: ALL

L3 Anomalies

Name	Logging	Action: Disable [✓ Block] Monitor	Threshold
ip_src_session	●	Disable [✓ Block] Monitor	5000
ip_dst_session	●	Disable [✓ Block] Monitor	5000

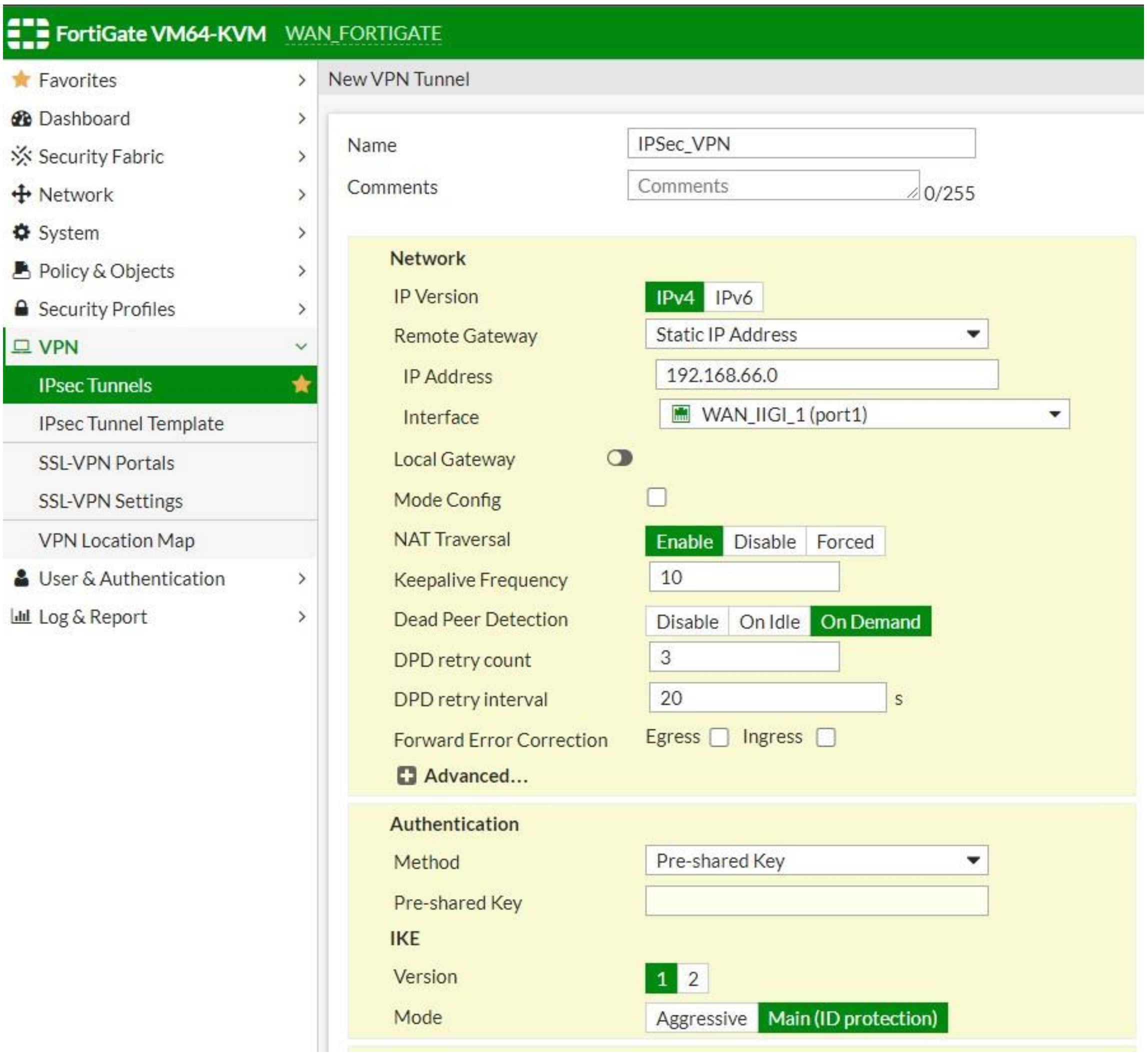
L4 Anomalies

Name	Logging	Action: Disable [✓ Block] Monitor	Threshold
tcp_syn_flood	●	Disable [✓ Block] Monitor	2000
tcp_port_scan	●	Disable [✓ Block] Monitor	1000
tcp_src_session	●	Disable [✓ Block] Monitor	5000
tcp_dst_session	●	Disable [✓ Block] Monitor	5000
udp_flood	●	Disable [✓ Block] Monitor	2000
udp_scan	●	Disable [✓ Block] Monitor	2000
udp_src_session	●	Disable [✓ Block] Monitor	5000

Figure 4.2.4.5: DDoS attack prevention policy

4.2.4.6 IPSec VPN Configuration

- Open ‘VPN’ > ‘IPsec Tunnels’ > click on ‘Create New’ to configure
- Name vpn > select ‘IP Version’ to ‘IPv4’ > Remote Gateway to ‘Static IP Address’ > Assign IP Address > select ‘Interface’ > select ‘NAT Traversal’ to ‘Enable’ > select ‘Authentication’ ‘Method’ to ‘Pre-shared Key’ > add ‘Pre-shared Key’ > save
- Remote address of a Mikrotik router, outside from DOL added
- VPN configuration named to ‘IPSec_VPN’



New VPN Tunnel

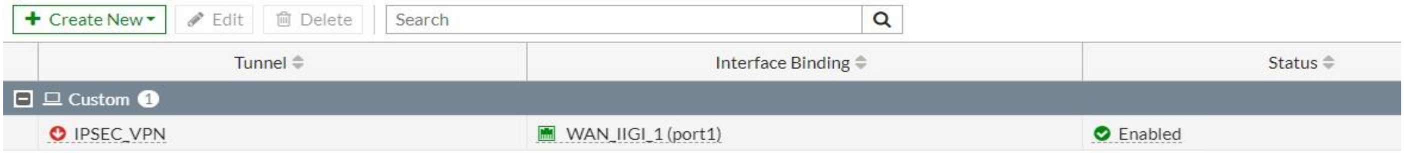
Name: IPSec_VPN
Comments: Comments 0/255

Network
IP Version: IPv4 | IPv6
Remote Gateway: Static IP Address
IP Address: 192.168.66.0
Interface: WAN_IIGI_1 (port1)
Local Gateway
Mode Config ☐
NAT Traversal: Enable | Disable | Forced
Keepalive Frequency: 10
Dead Peer Detection: Disable | On Idle | On Demand
DPD retry count: 3
DPD retry interval: 20 s
Forward Error Correction: Egress ☐ Ingress ☐

Authentication
Method: Pre-shared Key
Pre-shared Key:
IKE
Version: 1 | 2
Mode: Aggressive | Main (ID protection)

Figure 4.2.4.6.1: IPSec VPN configuration

- VPN establishment status



Tunnel	Interface Binding	Status
Custom 1		
IPSEC_VPN	WAN_IIGI_1 (port1)	Enabled

Figure 4.2.4.6.2: IPSec VPN status

4.3 All Mikrotik Router Configurations

- Ethernet connection from firewall to Mikrotik RB2011UAS router port.
- Router port to LAN computer connection for configuration.
- Other three router connection from core router ports.

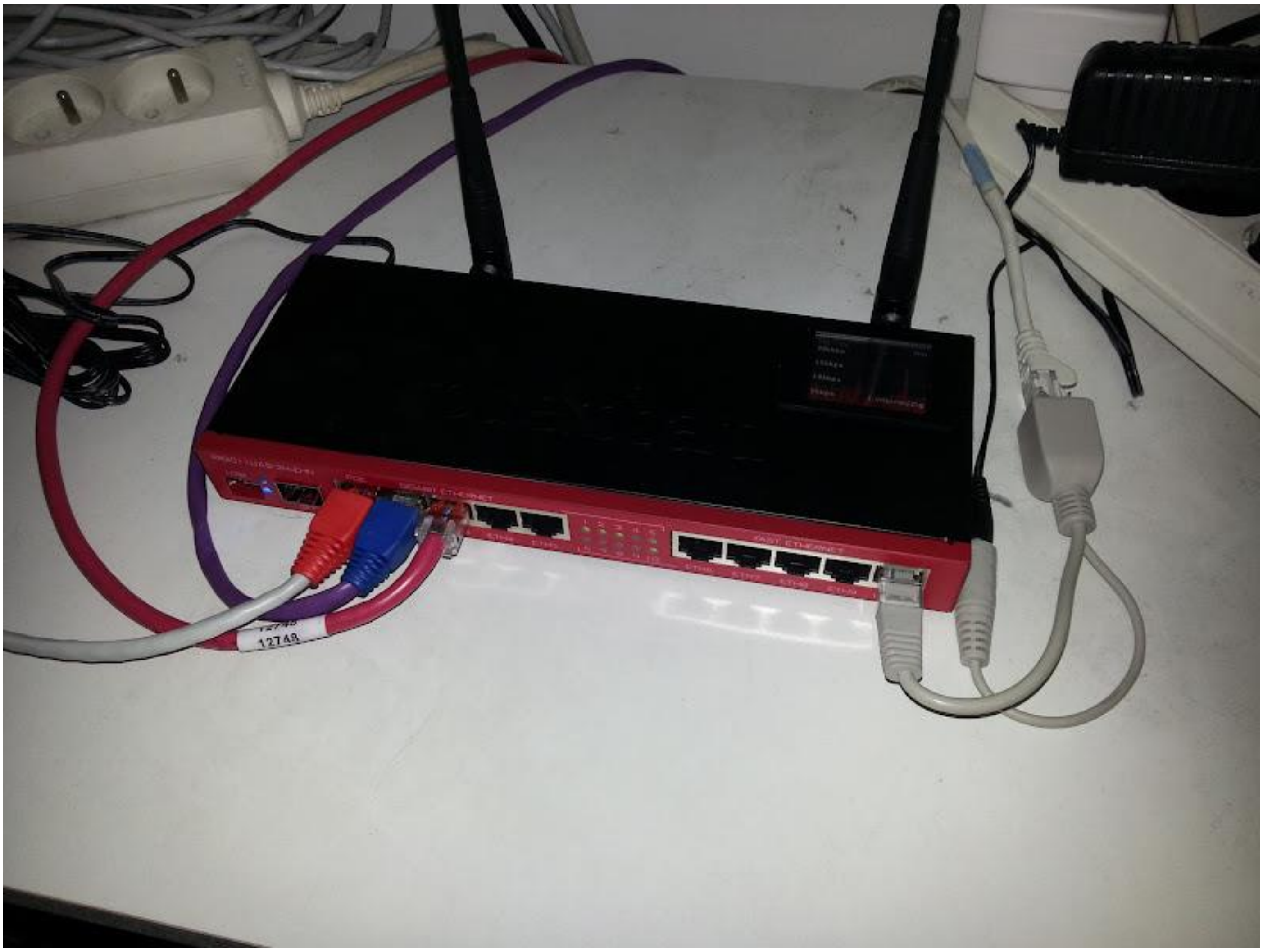
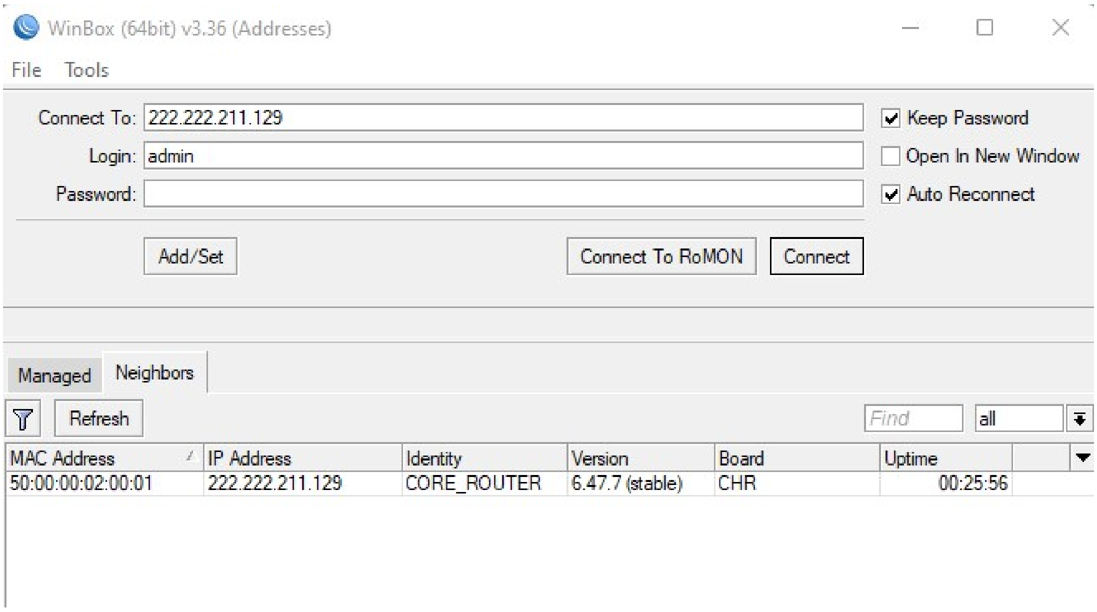


Figure 4.3.1: Mikortik RB2011UAS device

- Download, open open-source software ‘WinBox’
- Select ‘Connect’ to Mikrotik device by confirming ‘Uptime’ from ‘Neighbors’



Connect To: 222.222.211.129

Login: admin

Password:

☑ Keep Password
☐ Open In New Window
☑ Auto Reconnect

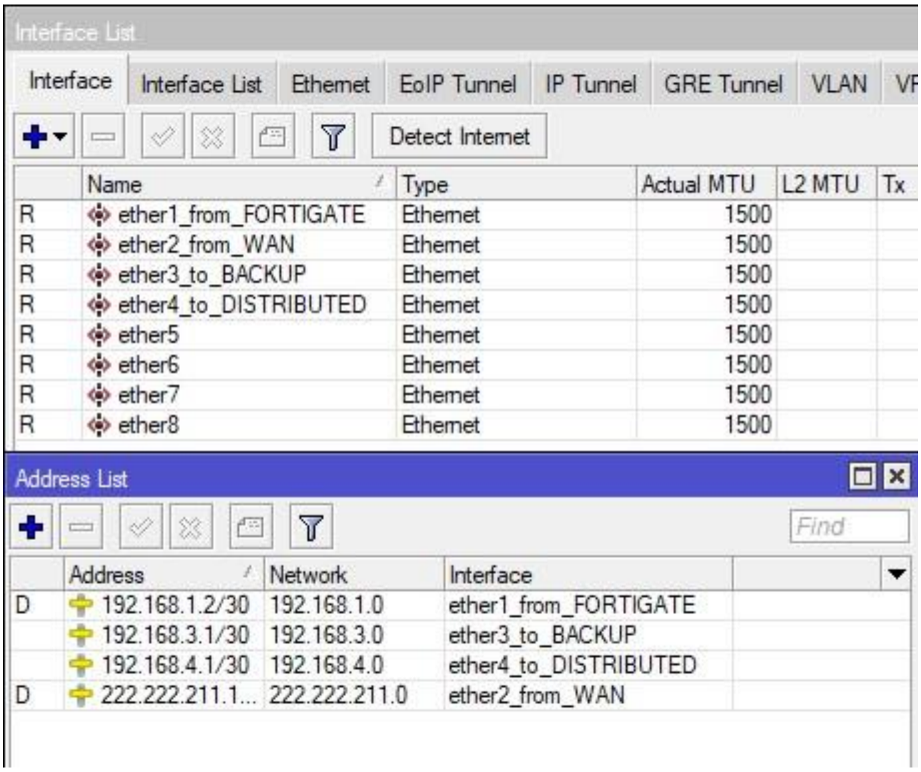
all

MAC Address	IP Address	Identity	Version	Board	Uptime
50:00:00:02:00:01	222.222.211.129	CORE_ROUTER	6.47.7 (stable)	CHR	00:25:56

Figure 4.3.2: ‘WinBox’ tool to connect Mikrotik routers

4.3.1 Primary Configurations for Core, Backup, Distributed and PPPoE Routers

- Open ‘IP’ > ‘Interface’ > Double click on ‘ether’ interface > rename interface > select ‘OK’
- Interfaces renamed by connected devices
- Open ‘IP’ > ‘Address’ > Click on ‘+’ to configure
- Add ‘Name’ > set ip address, subnet > select ‘Interface’ > save

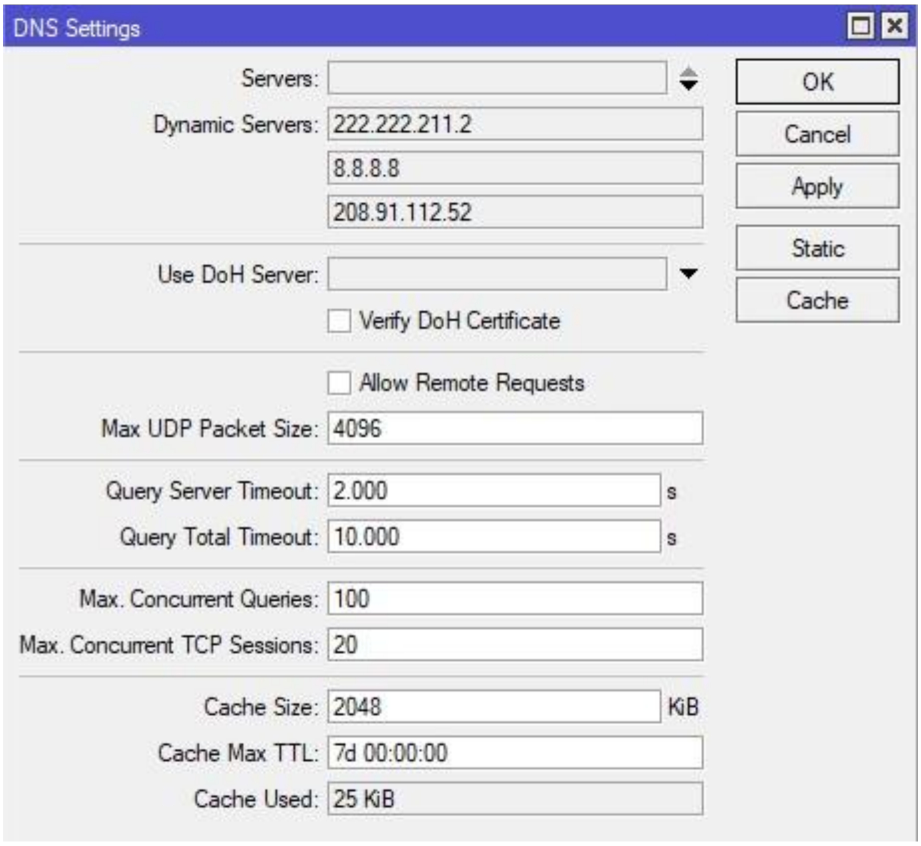


	Name	Type	Actual MTU	L2 MTU	Tx
R	ether1_from_FORTIGATE	Ethernet	1500		
R	ether2_from_WAN	Ethernet	1500		
R	ether3_to_BACKUP	Ethernet	1500		
R	ether4_to_DISTRIBUTED	Ethernet	1500		
R	ether5	Ethernet	1500		
R	ether6	Ethernet	1500		
R	ether7	Ethernet	1500		
R	ether8	Ethernet	1500		

	Address	Network	Interface
D	192.168.1.2/30	192.168.1.0	ether1_from_FORTIGATE
	192.168.3.1/30	192.168.3.0	ether3_to_BACKUP
	192.168.4.1/30	192.168.4.0	ether4_to_DISTRIBUTED
D	222.222.211.1...	222.222.211.0	ether2_from_WAN

Figure 4.3.1.1: Mikortik router’s interface names, ip addresses

- Open ‘IP’ > ‘DNS’ > add ‘Servers’ address to Google DNS > select OK



DNS Settings

Servers:

Dynamic Servers: 222.222.211.2
8.8.8.8
208.91.112.52

Use DoH Server:

□ Verify DoH Certificate

□ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

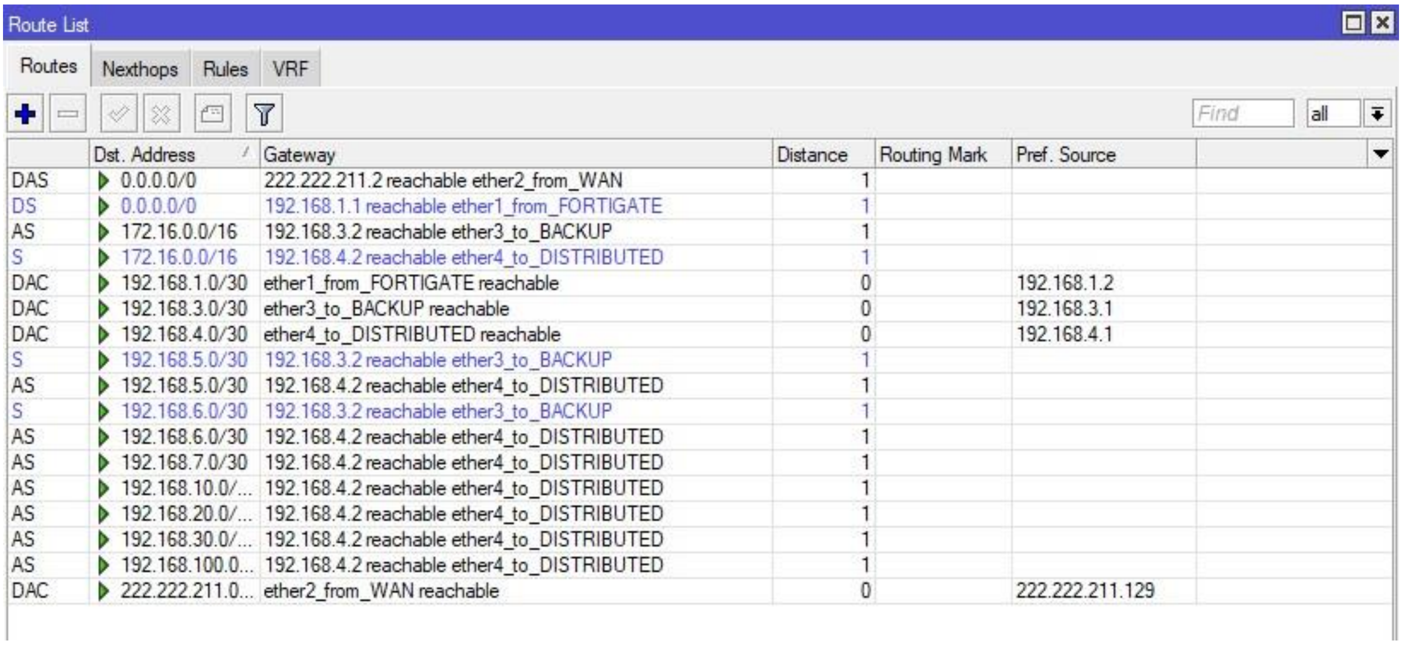
Cache Size: 2048 KiB

Cache Max TTL: 7d 00:00:00

Cache Used: 25 KiB

Figure 4.3.1.2: DNS configuration

- Open ‘IP’ > ‘Routes’ > Click on ‘+’ to configure
- Add ‘Destination Address’ by ip address range > select ‘Gateway’ > select OK



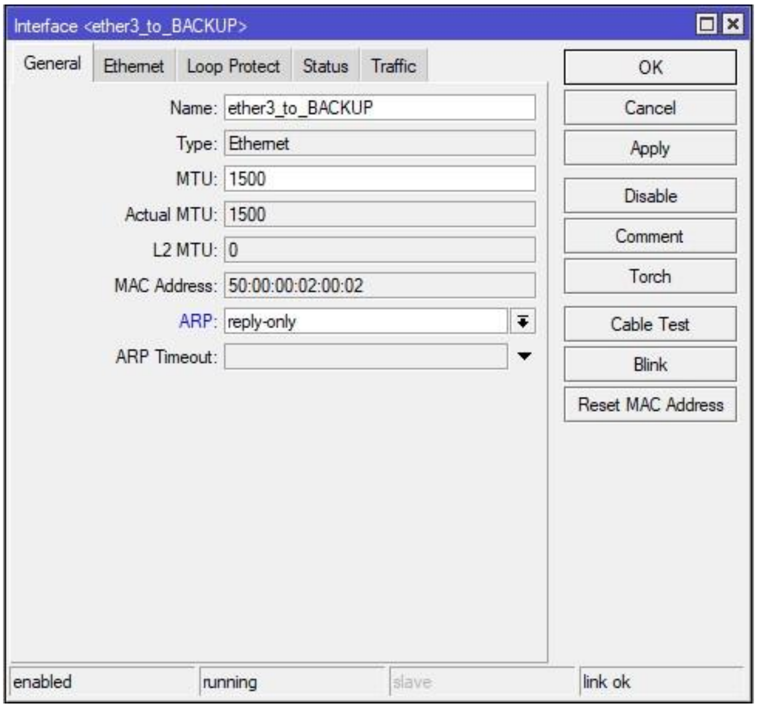
Route List

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	222.222.211.2 reachable ether2_from_WAN	1		
DS	0.0.0.0/0	192.168.1.1 reachable ether1_from_FORTIGATE	1		
AS	172.16.0.0/16	192.168.3.2 reachable ether3_to_BACKUP	1		
S	172.16.0.0/16	192.168.4.2 reachable ether4_to_DISTRIBUTED	1		
DAC	192.168.1.0/30	ether1_from_FORTIGATE reachable	0		192.168.1.2
DAC	192.168.3.0/30	ether3_to_BACKUP reachable	0		192.168.3.1
DAC	192.168.4.0/30	ether4_to_DISTRIBUTED reachable	0		192.168.4.1
S	192.168.5.0/30	192.168.3.2 reachable ether3_to_BACKUP	1		
AS	192.168.5.0/30	192.168.4.2 reachable ether4_to_DISTRIBUTED	1		
S	192.168.6.0/30	192.168.3.2 reachable ether3_to_BACKUP	1		
AS	192.168.6.0/30	192.168.4.2 reachable ether4_to_DISTRIBUTED	1		
AS	192.168.7.0/30	192.168.4.2 reachable ether4_to_DISTRIBUTED	1		
AS	192.168.10.0/...	192.168.4.2 reachable ether4_to_DISTRIBUTED	1		
AS	192.168.20.0/...	192.168.4.2 reachable ether4_to_DISTRIBUTED	1		
AS	192.168.30.0/...	192.168.4.2 reachable ether4_to_DISTRIBUTED	1		
AS	192.168.100.0...	192.168.4.2 reachable ether4_to_DISTRIBUTED	1		
DAC	222.222.211.0...	ether2_from_WAN reachable	0		222.222.211.129

Figure 4.3.1.3: Static routes of all devices

4.3.2 Secure configuration for all router ether ports

- Open ‘IP’ > ‘Interface’ > Double click on interface
- Select ‘ARP’ to ‘reply-only’ > select OK



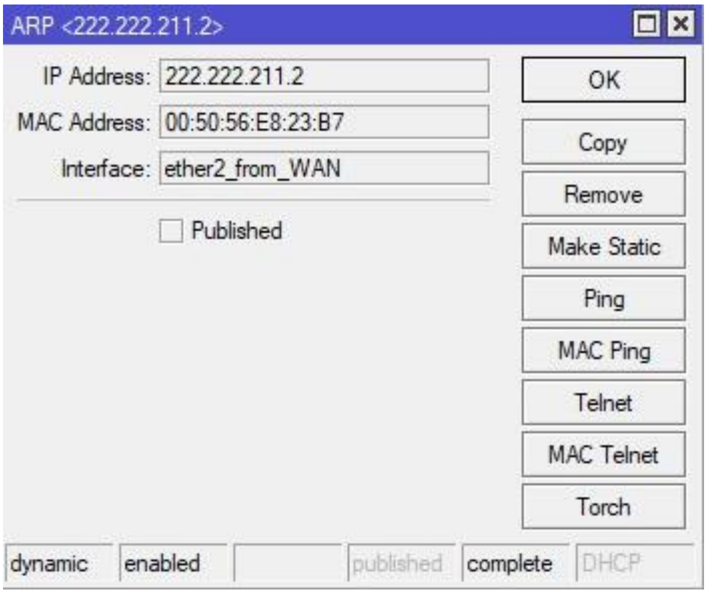
Interface <ether3_to_BACKUP>

Name: ether3_to_BACKUP
Type: Ethernet
MTU: 1500
Actual MTU: 1500
L2 MTU: 0
MAC Address: 50:00:00:02:00:02
ARP: reply-only
ARP Timeout:

enabled | running | slave | link ok

Figure 4.3.2.1: ARP configuration

- Open ‘IP’ > ‘ARP’ > Double click to arp > assign ‘MAC Address’ > select OK



ARP <222.222.211.2>

IP Address: 222.222.211.2
MAC Address: 00:50:56:E8:23:B7
Interface: ether2_from_WAN

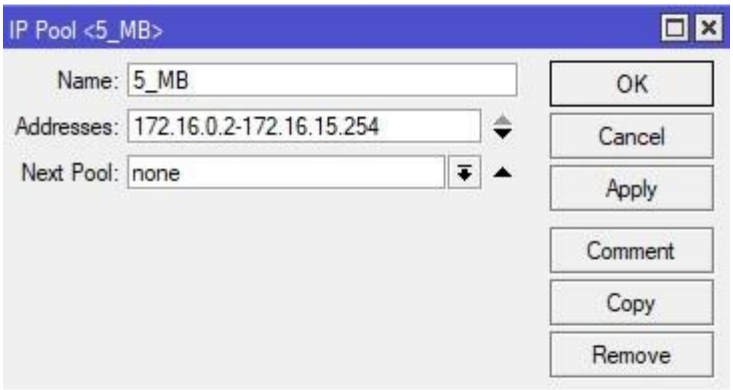
☐ Published

dynamic | enabled | | published | complete | DHCP

Figure 4.3.2.2: MAC address of firewall

4.3.3 PPPoE Router Server Configuration

- Open ‘IP’ > ‘Pool’ > click ‘+’ to create new configure
- Add ‘Name’ > add ip ranges to ‘Addresses’ > select ‘Next Pool’ to ‘none’ > select OK



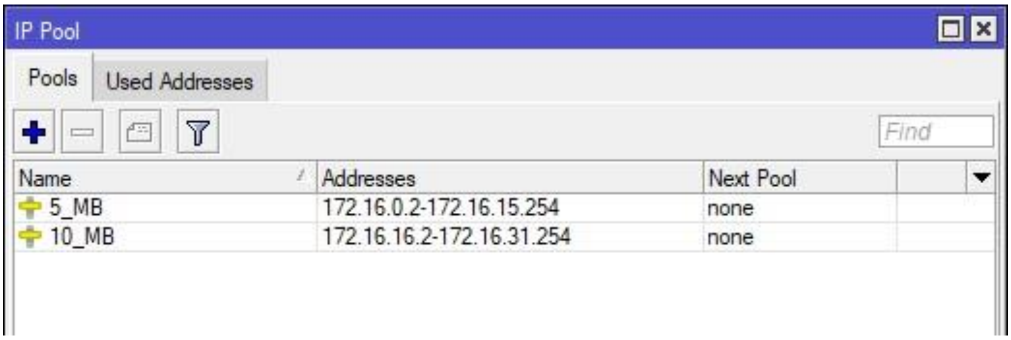
IP Pool <5_MB>

Name: 5_MB

Addresses: 172.16.0.2-172.16.15.254

Next Pool: none

Figure 4.3.3.1: Ip pool addresses of packages

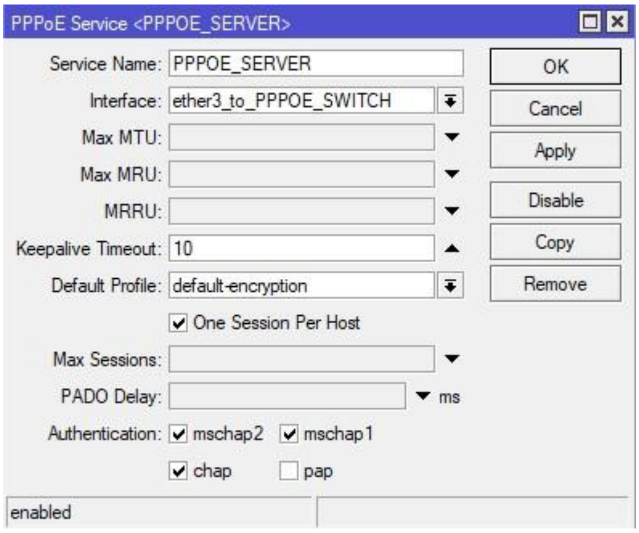


IP Pool

Name	Addresses	Next Pool
5_MB	172.16.0.2-172.16.15.254	none
10_MB	172.16.16.2-172.16.31.254	none

Figure 4.3.3.2: DHCP ip pool addresses

- Open ‘PPPoE’ > click ‘+’ > select ‘PPPoE Service’ to create new configure
- Add ‘Service Name’ > select ‘Interface’ > select ‘One Session Per Host’ > deselect ‘pap’ > select OK



PPPoE Service <PPPOE_SERVER>

Service Name: PPPOE_SERVER

Interface: ether3_to_PPPOE_SWITCH

Max MTU:

Max MRU:

MRRU:

Keepalive Timeout: 10

Default Profile: default-encryption

☑ One Session Per Host

Max Sessions:

PADO Delay: ms

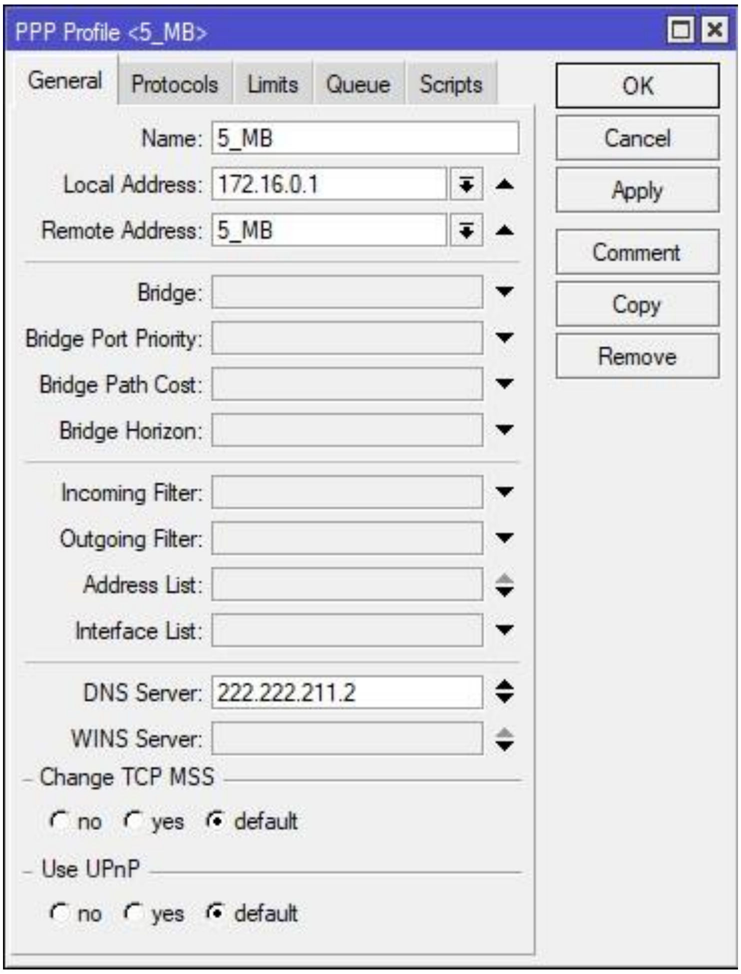
Authentication: ☑ mschap2 ☑ mschap1

☑ chap ☐ pap

enabled

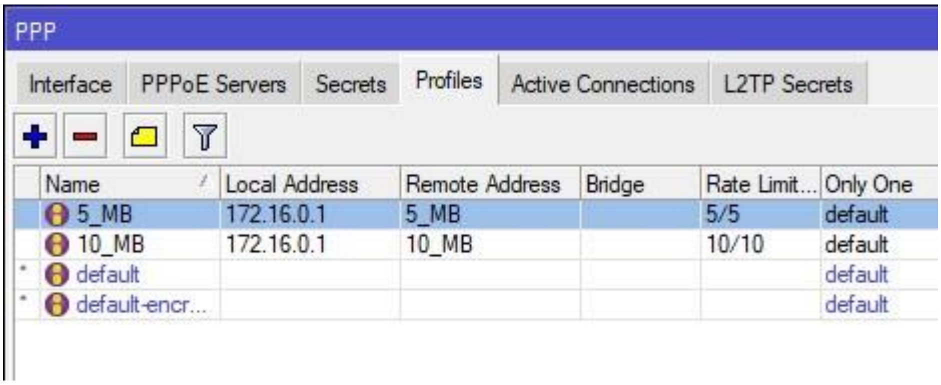
Figure 4.3.3.3: PPPoE server configuration

- Select ‘PPPoE Profile’ > click ‘+’ > to create new configure
- ‘General’ > Add ‘Name’ > add ‘Local Address’ > Select ‘Remote Address’ > Add ‘DNS Server’ to Google or IIG provided DNS > select ‘rate limit’ > select OK
- PPPoE Profile created of ‘5_MB’ and ‘10_MB’



Name: 5_MB
Local Address: 172.16.0.1
Remote Address: 5_MB
Bridge:
Bridge Port Priority:
Bridge Path Cost:
Bridge Horizon:
Incoming Filter:
Outgoing Filter:
Address List:
Interface List:
DNS Server: 222.222.211.2
WINS Server:
Change TCP MSS
○ no ○ yes ● default
Use UPnP
○ no ○ yes ● default

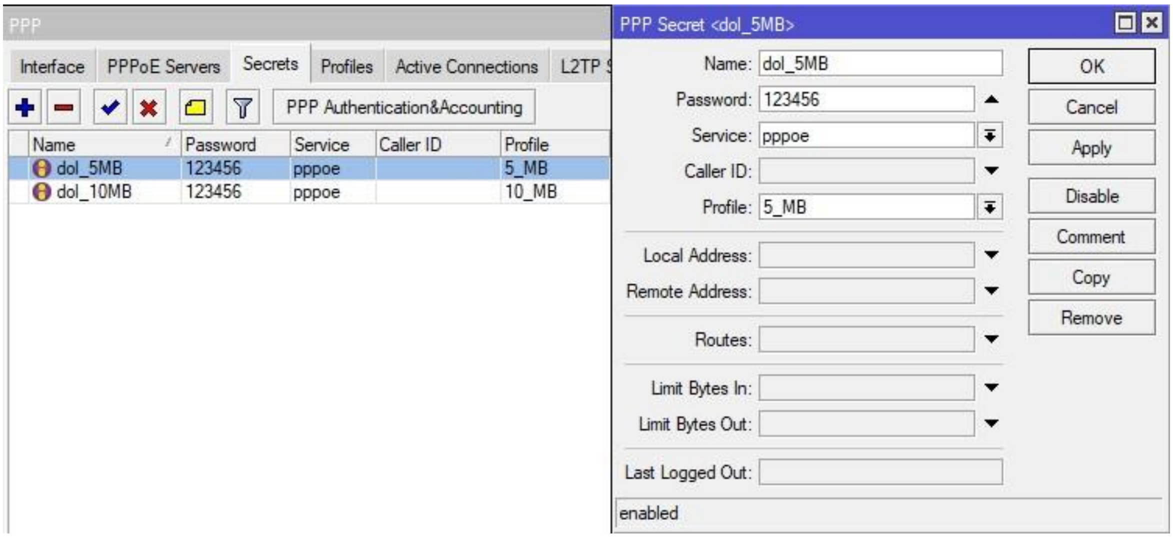
Figure 4.3.3.4: PPPoE server of package



Name	Local Address	Remote Address	Bridge	Rate Limit...	Only One
5_MB	172.16.0.1	5_MB		5/5	default
10_MB	172.16.0.1	10_MB		10/10	default
* default					default
* default-encr...					default

Figure 4.3.3.5: PPPoE server of package profiles

- Select ‘Secretes’ > click ‘+’ > to create new configure
- Add ‘Name’ > add ‘Password’ > select ‘Service’ to PPPoE > select ‘Profile ‘5_MB’ > select OK
- PPPoE Secret created for ‘5_MB’ and ‘10_MB’ users



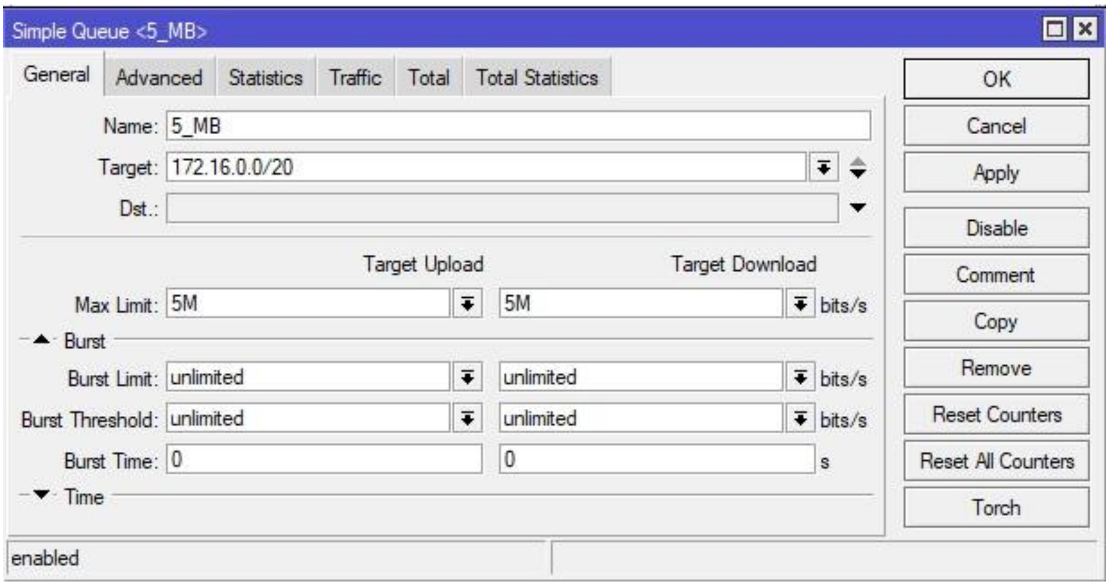
Name	Password	Service	Caller ID	Profile
dol_5MB	123456	pppoe		5_MB
dol_10MB	123456	pppoe		10_MB

Name: dol_5MB
Password: 123456
Service: pppoe
Caller ID:
Profile: 5_MB
Local Address:
Remote Address:
Routes:
Limit Bytes In:
Limit Bytes Out:
Last Logged Out:
enabled

Figure 4.3.3.6: PPPoE users profile, secretes

4.3.4 Bandwidth Queues on PPPoE Router

- Open ‘Queues’ > click ‘+’ to create new configure
- Add ‘Name’ > add ‘Target’ > add ‘Max Limit’ of ‘Target Upload’ and ‘Target Download’ > select OK



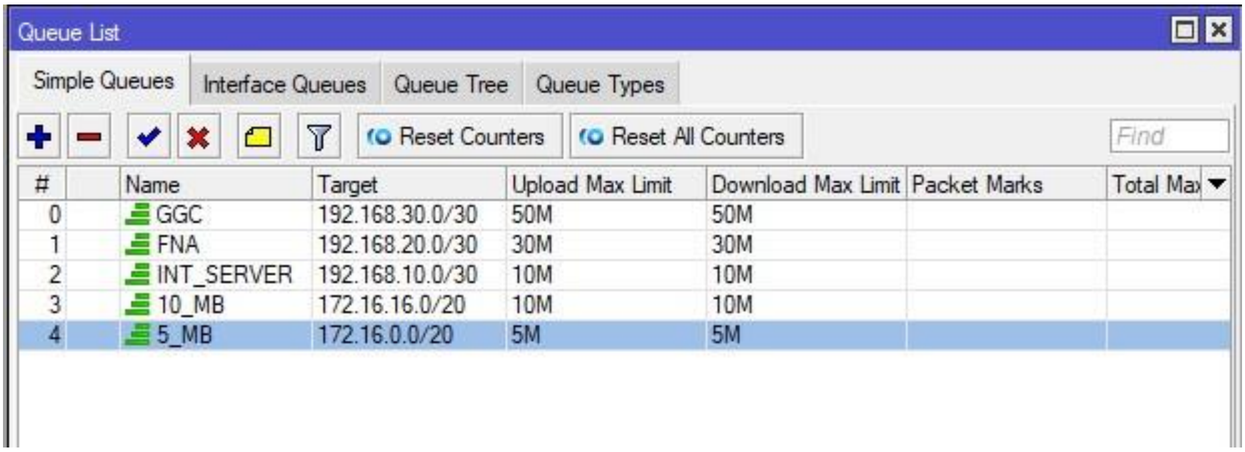
Name: 5_MB
Target: 172.16.0.0/20
Dst.:

	Target Upload	Target Download	
Max Limit:	5M	5M	bits/s
Burst Limit:	unlimited	unlimited	bits/s
Burst Threshold:	unlimited	unlimited	bits/s
Burst Time:	0	0	s

enabled

Figure 4.3.4.1: Queue configuration for package

- Created Queue list of GGC, FNA, INT server from DOL according to bandwidth limit for PPPoE clients



#		Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max
0		GGC	192.168.30.0/30	50M	50M		
1		FNA	192.168.20.0/30	30M	30M		
2		INT_SERVER	192.168.10.0/30	10M	10M		
3		10_MB	172.16.16.0/20	10M	10M		
4		5_MB	172.16.0.0/20	5M	5M		

Figure 4.3.4.2: Queue list

4.4 Third Fortigate Firewall for DMZ

- LAN connection from Distributed Mikrotik router to Fortigate firewall connects
- Open ‘Device Manager’ of windows
- Expand ‘Ports’, identify ‘COM serial number’
- Open ‘Putty’
- ‘Putty’ connects to ‘COM serial port’
- Command prompt terminal opens, needs to login as admin. No password required for first login. Needs to set new password, confirm password
- Configure system interface of connected wan port with assigning ip address
- Set allow access to ping, ssh, telnet, http, https
- Firewall can be accessed from browser

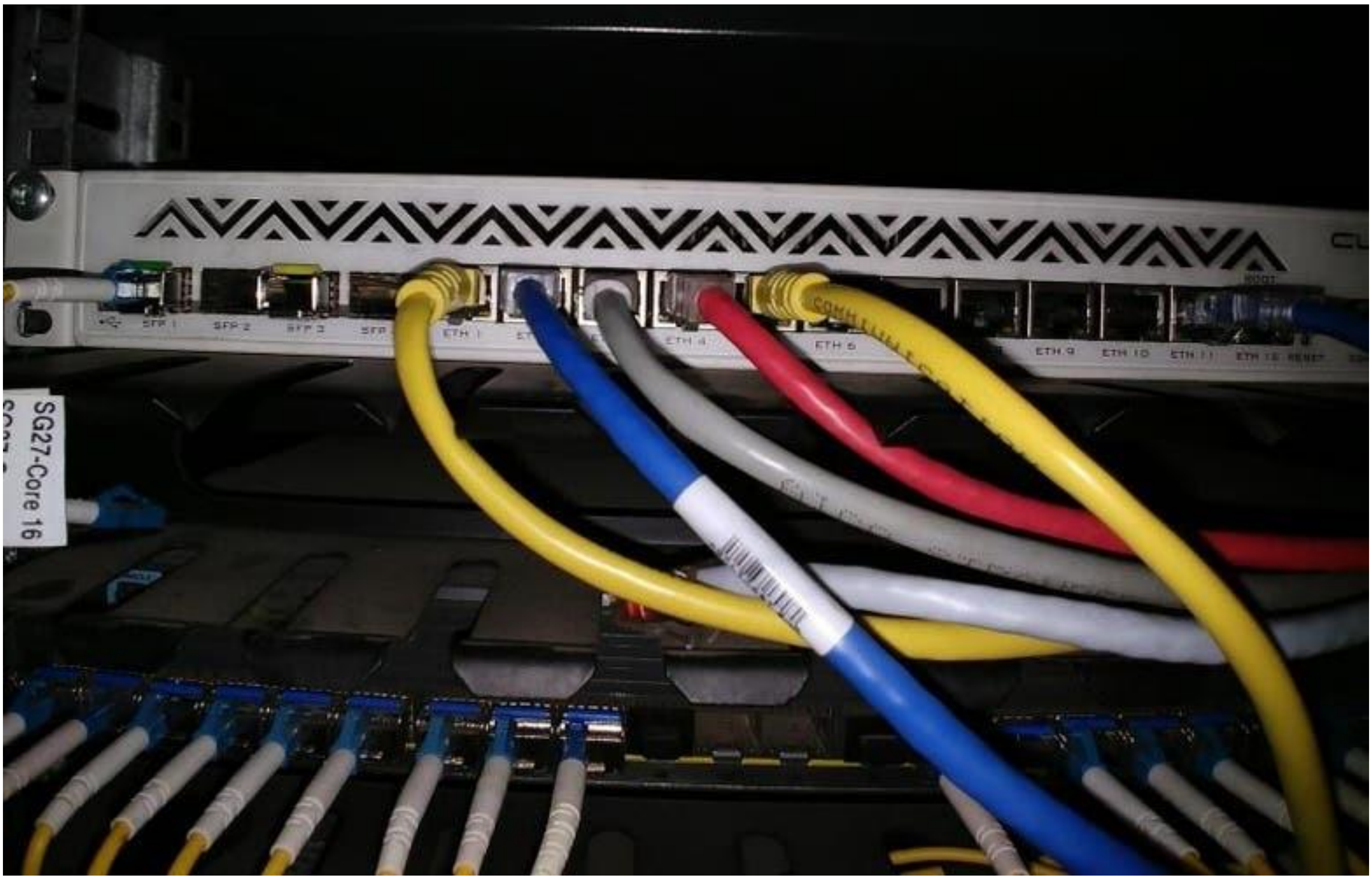
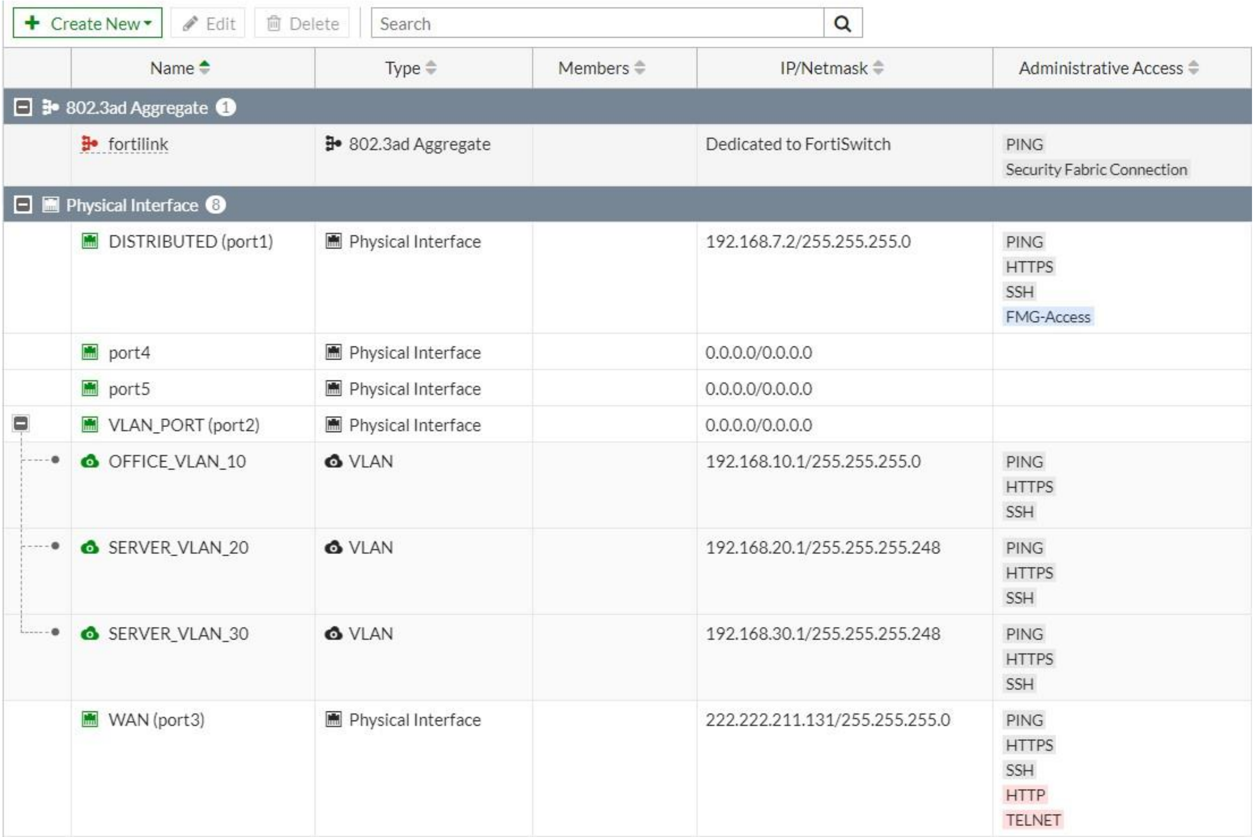


Figure 4.4: Fortigate firewall on server rack

4.4.1 Network Configuration

4.4.1.1 Interface Naming, Addressing, VLAN, DNS Configuration

- Open ‘Network’ > ‘Interfaces’ > click on port by connected to configure
- Assign ‘ip address’, rename ‘interface port name’, set ‘DNS’
- Interfaces of port renamed to ‘DISTRIBUTED’, ‘OFFICE_VLAN_10’, ‘SERVER_VLAN_20’, ‘SERVER_VLAN_30’

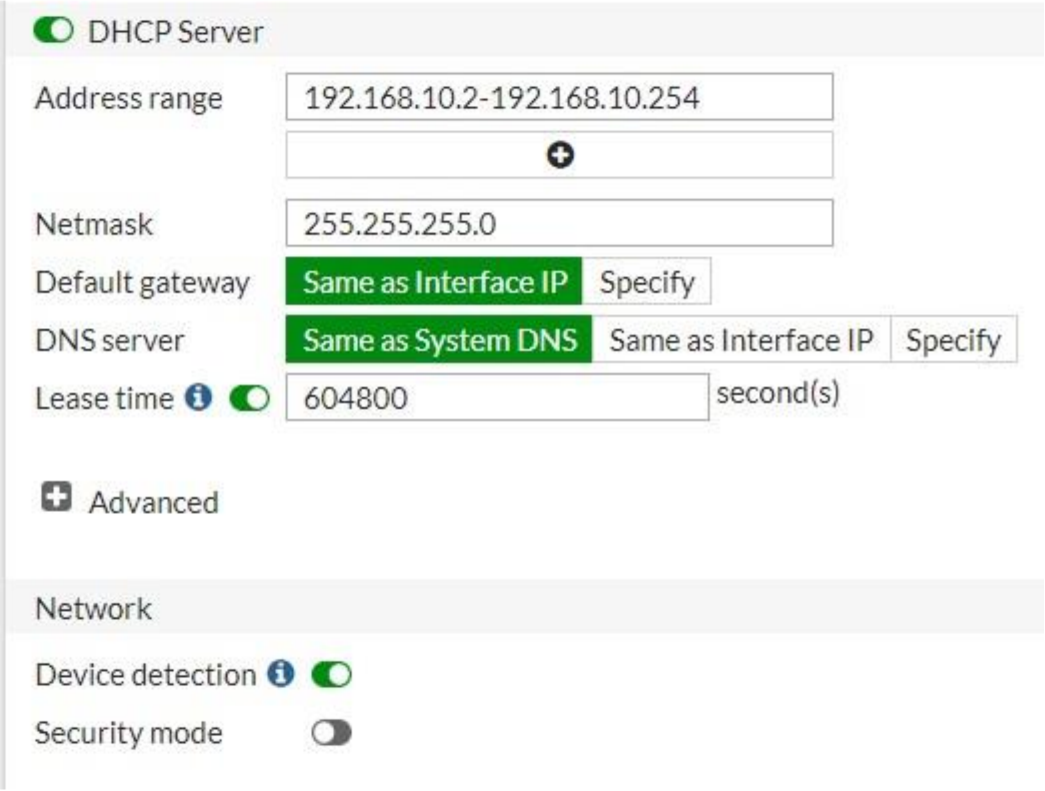


Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 8				
DISTRIBUTED (port1)	Physical Interface		192.168.7.2/255.255.255.0	PING HTTPS SSH FMG-Access
port4	Physical Interface		0.0.0.0/0.0.0.0	
port5	Physical Interface		0.0.0.0/0.0.0.0	
VLAN_PORT (port2)	Physical Interface		0.0.0.0/0.0.0.0	
OFFICE_VLAN_10	VLAN		192.168.10.1/255.255.255.0	PING HTTPS SSH
SERVER_VLAN_20	VLAN		192.168.20.1/255.255.255.248	PING HTTPS SSH
SERVER_VLAN_30	VLAN		192.168.30.1/255.255.255.248	PING HTTPS SSH
WAN (port3)	Physical Interface		222.222.211.131/255.255.255.0	PING HTTPS SSH HTTP TELNET

Figure 4.4.1.1: Configured interface names, ip addresses

4.4.1.2 VLAN Configuration

- Open ‘Network’ > ‘Interfaces’ > click on port by connected to configure
- Select interface type as VLAN, assign ‘ip address’ , ‘vlan id’ , enable ‘DHCP Server’, add ip of ‘Address range’ , ‘Netmask’ , add ‘Lease time’ , enable ‘Device detection’ > save



● DHCP Server

Address range: 192.168.10.2-192.168.10.254

Netmask: 255.255.255.0

Default gateway: [✓ Same as Interface IP] Specify

DNS server: [✓ Same as System DNS] Same as Interface IP Specify

Lease time ● 604800 second(s)

Advanced

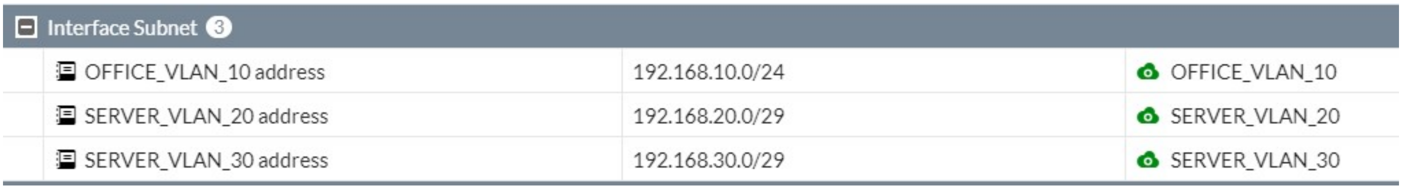
Network

Device detection ●

Security mode ○

Figure 4.4.1.2.1: DHCP server configuration for VLAN

- Custom ip address ranges for all routing and VLANs configured

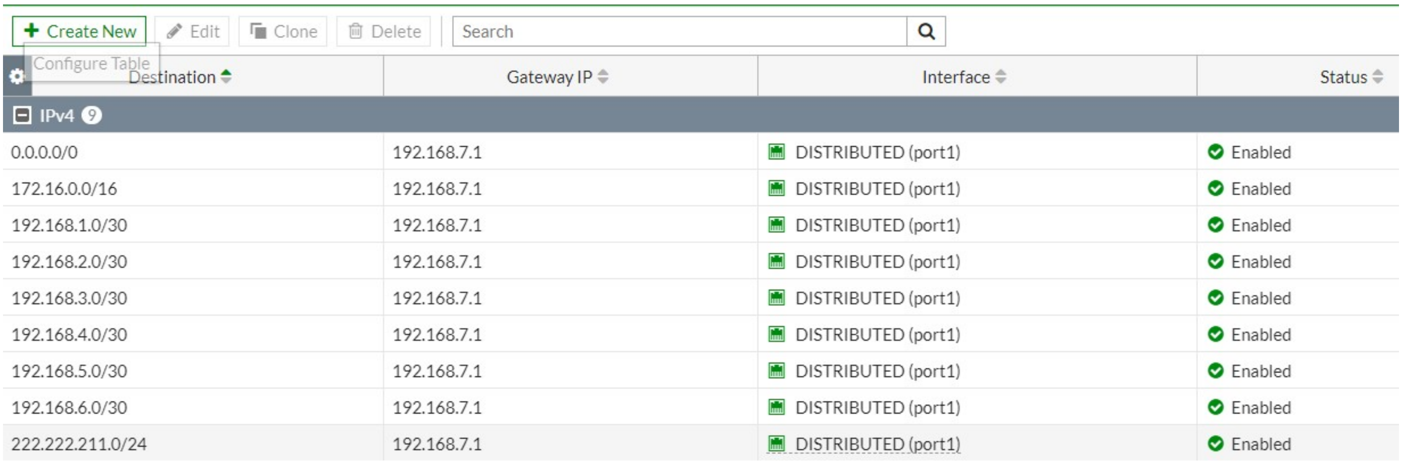


Interface Subnet 3		
OFFICE_VLAN_10 address	192.168.10.0/24	OFFICE_VLAN_10
SERVER_VLAN_20 address	192.168.20.0/29	SERVER_VLAN_20
SERVER_VLAN_30 address	192.168.30.0/29	SERVER_VLAN_30

Figure 4.4.1.2.2: Custom ip addresses for VLANs

4.4.1.3 Static Routes

- Open ‘Network’ > ‘Static Routes’ > click on ‘Create New’ to configure
- Add ‘Ip address’ > ‘Gateway’ > ‘Interface’ and save



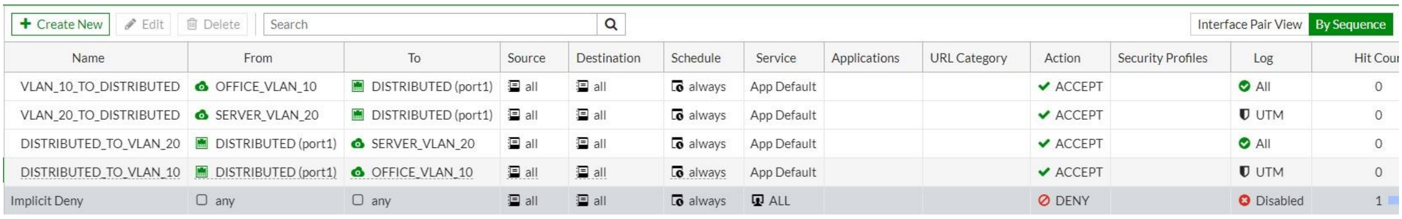
Destination	Gateway IP	Interface	Status
0.0.0.0/0	192.168.7.1	DISTRIBUTED (port1)	Enabled
172.16.0.0/16	192.168.7.1	DISTRIBUTED (port1)	Enabled
192.168.1.0/30	192.168.7.1	DISTRIBUTED (port1)	Enabled
192.168.2.0/30	192.168.7.1	DISTRIBUTED (port1)	Enabled
192.168.3.0/30	192.168.7.1	DISTRIBUTED (port1)	Enabled
192.168.4.0/30	192.168.7.1	DISTRIBUTED (port1)	Enabled
192.168.5.0/30	192.168.7.1	DISTRIBUTED (port1)	Enabled
192.168.6.0/30	192.168.7.1	DISTRIBUTED (port1)	Enabled
222.222.211.0/24	192.168.7.1	DISTRIBUTED (port1)	Enabled

Figure 4.4.1.3: Static routes

4.4.2 Policy and Objects

4.4.2.1 Defining Security Policies for Incoming and Outgoing Interfaces

- Open ‘Policy and Objects’ > ‘Security Policy’ > click on ‘Create New’ to configure
- Rename policy > select ‘From interface’ and ‘To interface’ > select ‘Source’ ip addresses to ‘all’ > select ‘Destination’ ip addresses to ‘all’ > Action ‘ACCEPT’
- Policy objects named to ‘VLAN_10_TO_DISTRIBUTED’, ‘VLAN_20_TO_DISTRIBUTED’, ‘VLAN_30_TO_DISTRIBUTED’ , ‘DISTRIBUTED_TO_VLAN_10’ , ‘DISTRIBUTED_TO_VLAN_20’ and ‘DISTRIBUTED_TO_VLAN_30’

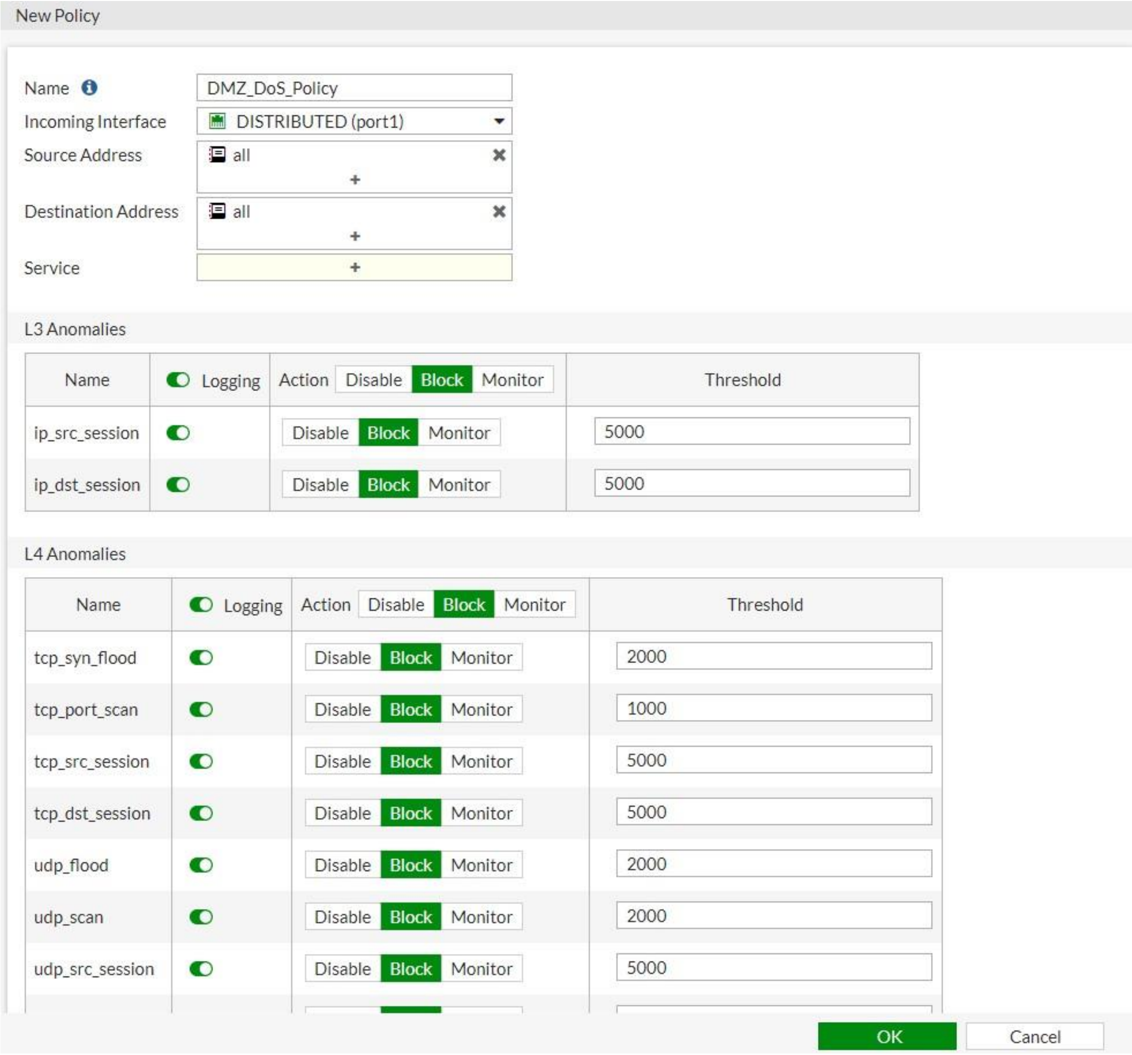


Name	From	To	Source	Destination	Schedule	Service	Applications	URL Category	Action	Security Profiles	Log	Hit Cou
VLAN_10_TO_DISTRIBUTED	OFFICE_VLAN_10	DISTRIBUTED (port1)	all	all	always	App Default			✓ ACCEPT		All	0
VLAN_20_TO_DISTRIBUTED	SERVER_VLAN_20	DISTRIBUTED (port1)	all	all	always	App Default			✓ ACCEPT		UTM	0
DISTRIBUTED_TO_VLAN_20	DISTRIBUTED (port1)	SERVER_VLAN_20	all	all	always	App Default			✓ ACCEPT		All	0
DISTRIBUTED_TO_VLAN_10	DISTRIBUTED (port1)	OFFICE_VLAN_10	all	all	always	App Default			✓ ACCEPT		UTM	0
Implicit Deny	□ any	□ any	all	all	always	ALL			⊘ DENY		Disabled	1

Figure 4.4.2.1: Configured policies for routes

4.4.2.2 DDoS Attack Prevention Policy

- Open ‘Policy and Objects’ > ‘IPV4 DDoS Policy’ > click on ‘Create New’ to configure
- Name > select ‘Incoming Interface’ > select ‘Source Address’ to ‘all’ > select ‘Destination Address’ to ‘all’ > select ‘Source’ to ‘ALL’ > enable all ‘logging’ and select to ‘Block’ > set ‘icmp_sys_flood’ Threshold to ‘1000’ > save



New Policy

Name	DMZ_DoS_Policy
Incoming Interface	DISTRIBUTED (port1)
Source Address	all
Destination Address	all
Service	+

L3 Anomalies

Name	Logging	Action: Disable [✓ Block] Monitor	Threshold
ip_src_session	●	Disable [✓ Block] Monitor	5000
ip_dst_session	●	Disable [✓ Block] Monitor	5000

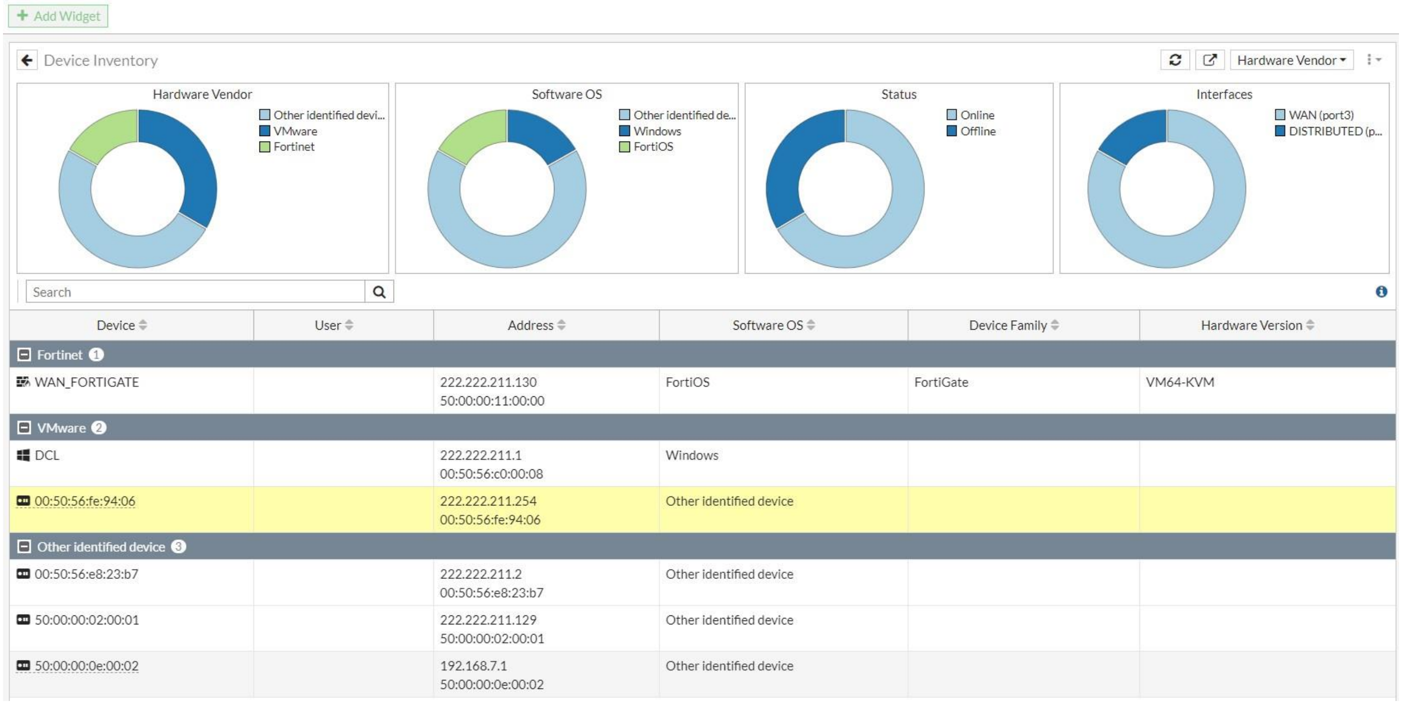
L4 Anomalies

Name	Logging	Action: Disable [✓ Block] Monitor	Threshold
tcp_syn_flood	●	Disable [✓ Block] Monitor	2000
tcp_port_scan	●	Disable [✓ Block] Monitor	1000
tcp_src_session	●	Disable [✓ Block] Monitor	5000
tcp_dst_session	●	Disable [✓ Block] Monitor	5000
udp_flood	●	Disable [✓ Block] Monitor	2000
udp_scan	●	Disable [✓ Block] Monitor	2000
udp_src_session	●	Disable [✓ Block] Monitor	5000

Figure 4.4.2.2: DDoS attack prevention policy

4.4.2.3 Device Detection, MAC Address Panel

- Open ‘Policy and Objects’ > ‘Detected devices’



Device	User	Address	Software OS	Device Family	Hardware Version
⊟ Fortinet 1					
WAN_FORTIGATE		222.222.211.130 50:00:00:11:00:00	FortiOS	FortiGate	VM64-KVM
⊟ VMware 2					
DCL		222.222.211.1 00:50:56:c0:00:08	Windows		
00:50:56:fe:94:06		222.222.211.254 00:50:56:fe:94:06	Other identified device		
⊟ Other identified device 3					
00:50:56:e8:23:b7		222.222.211.2 00:50:56:e8:23:b7	Other identified device		
50:00:00:02:00:01		222.222.211.129 50:00:00:02:00:01	Other identified device		
50:00:00:0e:00:02		192.168.7.1 50:00:00:0e:00:02	Other identified device		

Figure 4.4.2.3: Dashboard of detected devices, mac addresses

4.5 Cisco Switch SG350X-24PD Configuration for VLANs

- Connection from DMZ Fortigate firewall port to ethernet port.

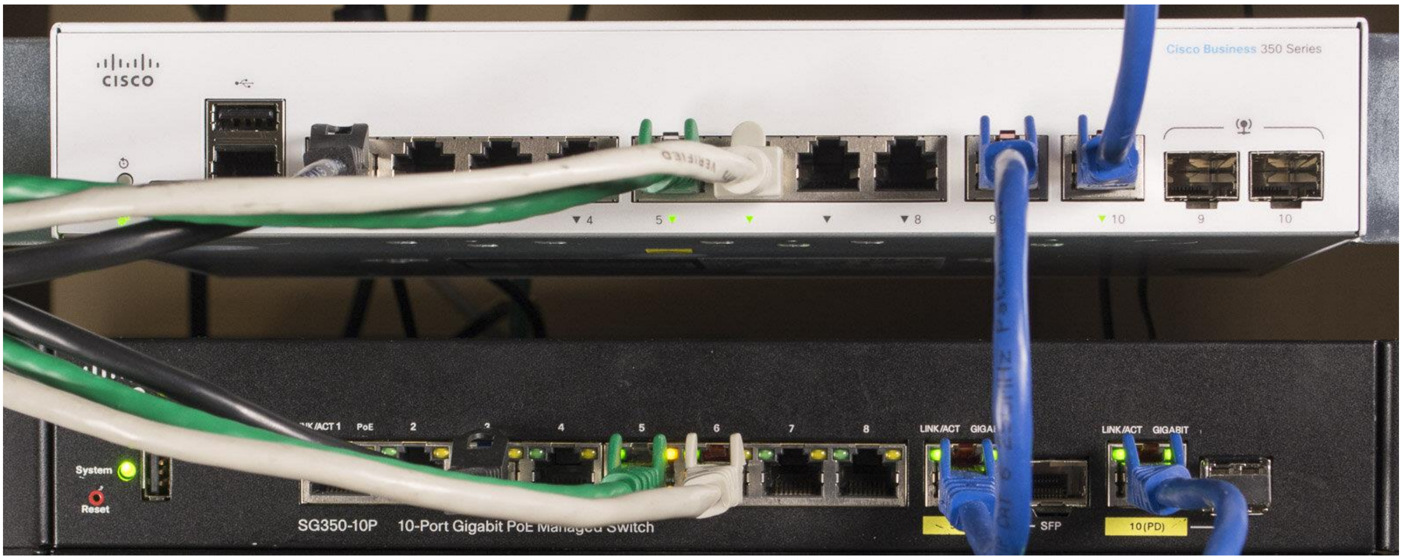
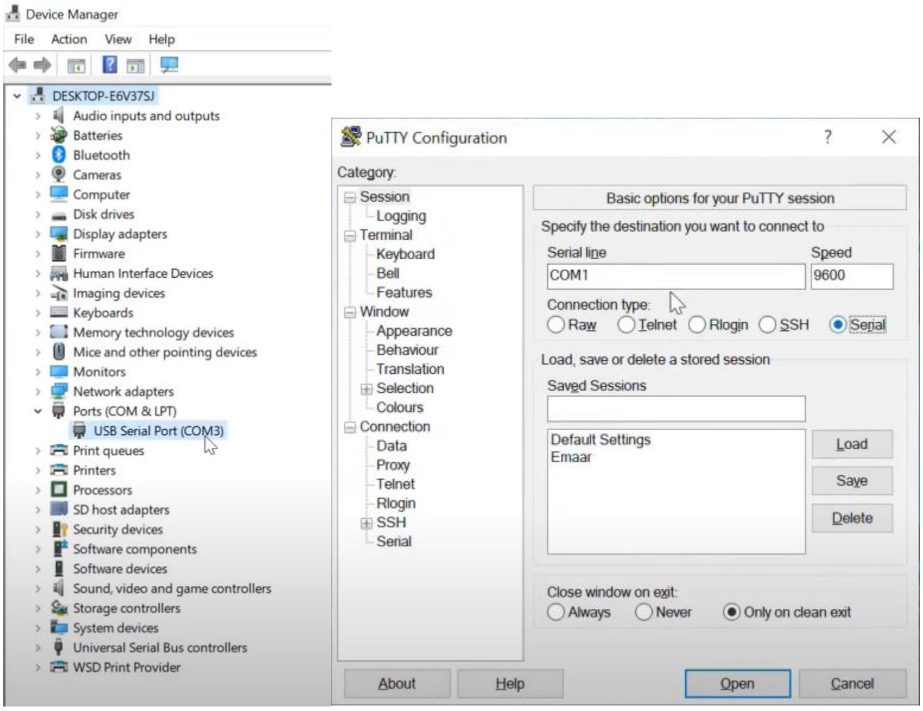


Figure 4.5: Cisco switch SG350X-24PD on server rack

4.5.1 DMZ Cisco Switch Configuration

- Open ‘Device Manager’ of windows
- Expand ‘Ports’, identify COM serial number


Device Manager

DESKTOP-E6V37SJ
- Audio inputs and outputs
- Batteries
- Bluetooth
- Cameras
- Computer
- Disk drives
- Display adapters
- Firmware
- Human Interface Devices
- Imaging devices
- Keyboards
- Memory technology devices
- Mice and other pointing devices
- Monitors
- Network adapters
- Ports (COM & LPT)
  - USB Serial Port (COM3)
- Print queues
- Printers
- Processors
- SD host adapters
- Security devices
- Software components
- Software devices
- Sound, video and game controllers
- Storage controllers
- System devices
- Universal Serial Bus controllers
- WSD Print Provider

PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1
Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

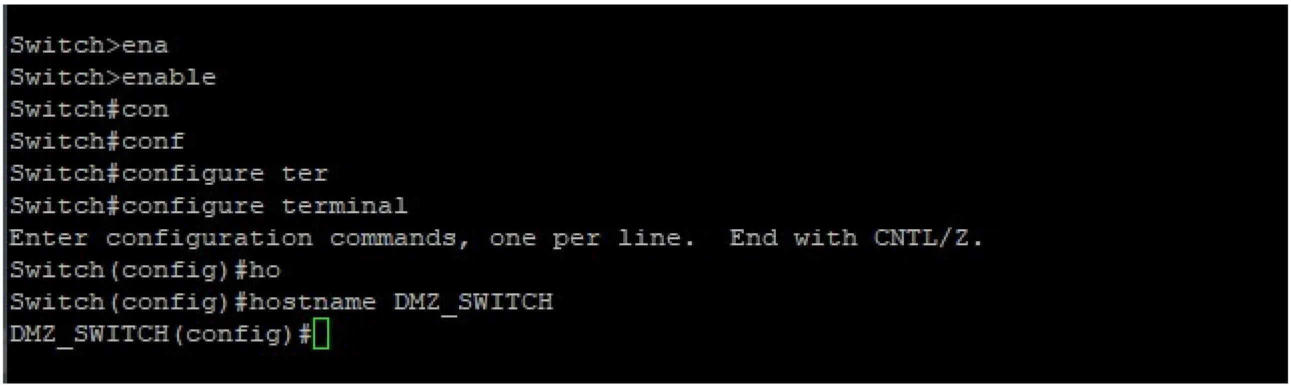
Default Settings
Emaar

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 4.5.1: Putty connection to Cisco switch for configuration

- Open ‘Putty’
- ‘Putty’ connects to COM serial port
- Command prompt terminal opens, needs to login as admin. No password required for first login. Needs to set new password, confirm password
- Configure system interface of connected wan port with assigning ip address

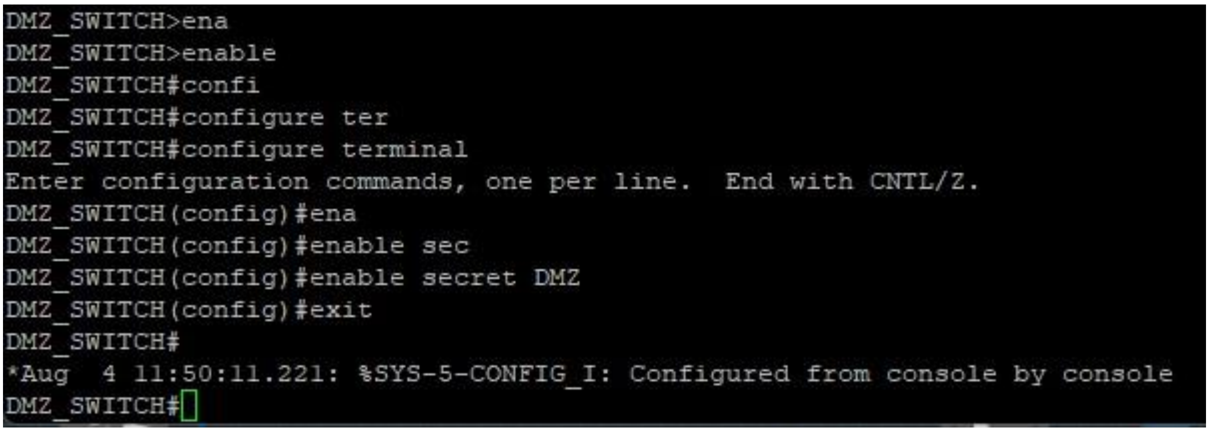
4.5.2 DMZ Cisco Switch Hostname Configuration



```
Switch>ena
Switch>enable
Switch#con
Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ho
Switch(config)#hostname DMZ_SWITCH
DMZ_SWITCH(config)#
```

Figure 4.5.2: console configuration for switch hostname

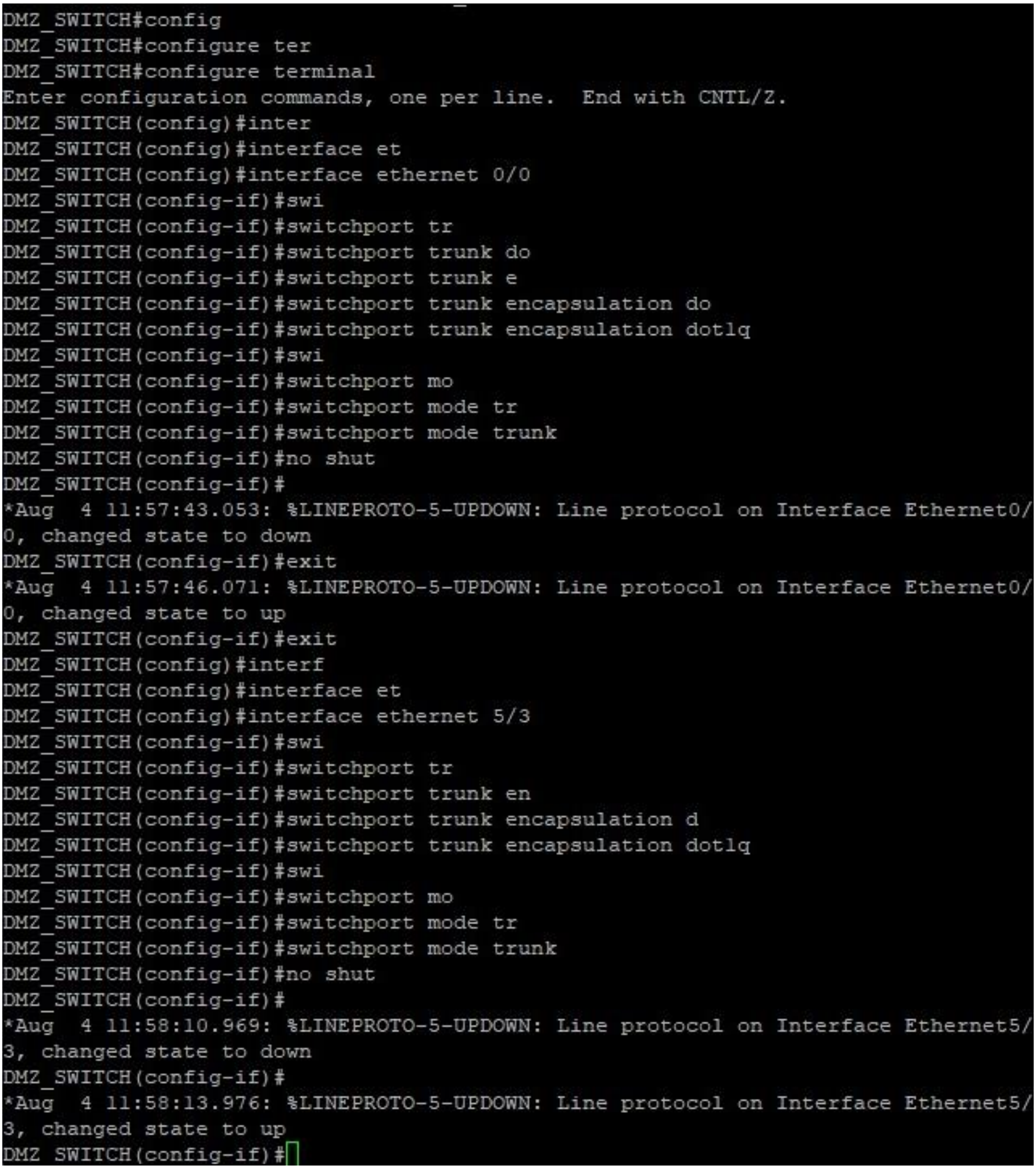
4.5.3 DMZ Cisco Switch Privilege Mode Security Configuration



```
DMZ_SWITCH>ena
DMZ_SWITCH>enable
DMZ_SWITCH#confi
DMZ_SWITCH#configure ter
DMZ_SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DMZ_SWITCH(config)#ena
DMZ_SWITCH(config)#enable sec
DMZ_SWITCH(config)#enable secret DMZ
DMZ_SWITCH(config)#exit
DMZ_SWITCH#
*Aug  4 11:50:11.221: %SYS-5-CONFIG_I: Configured from console by console
DMZ_SWITCH#
```

Figure 4.5.3: secret configured for privilege mode

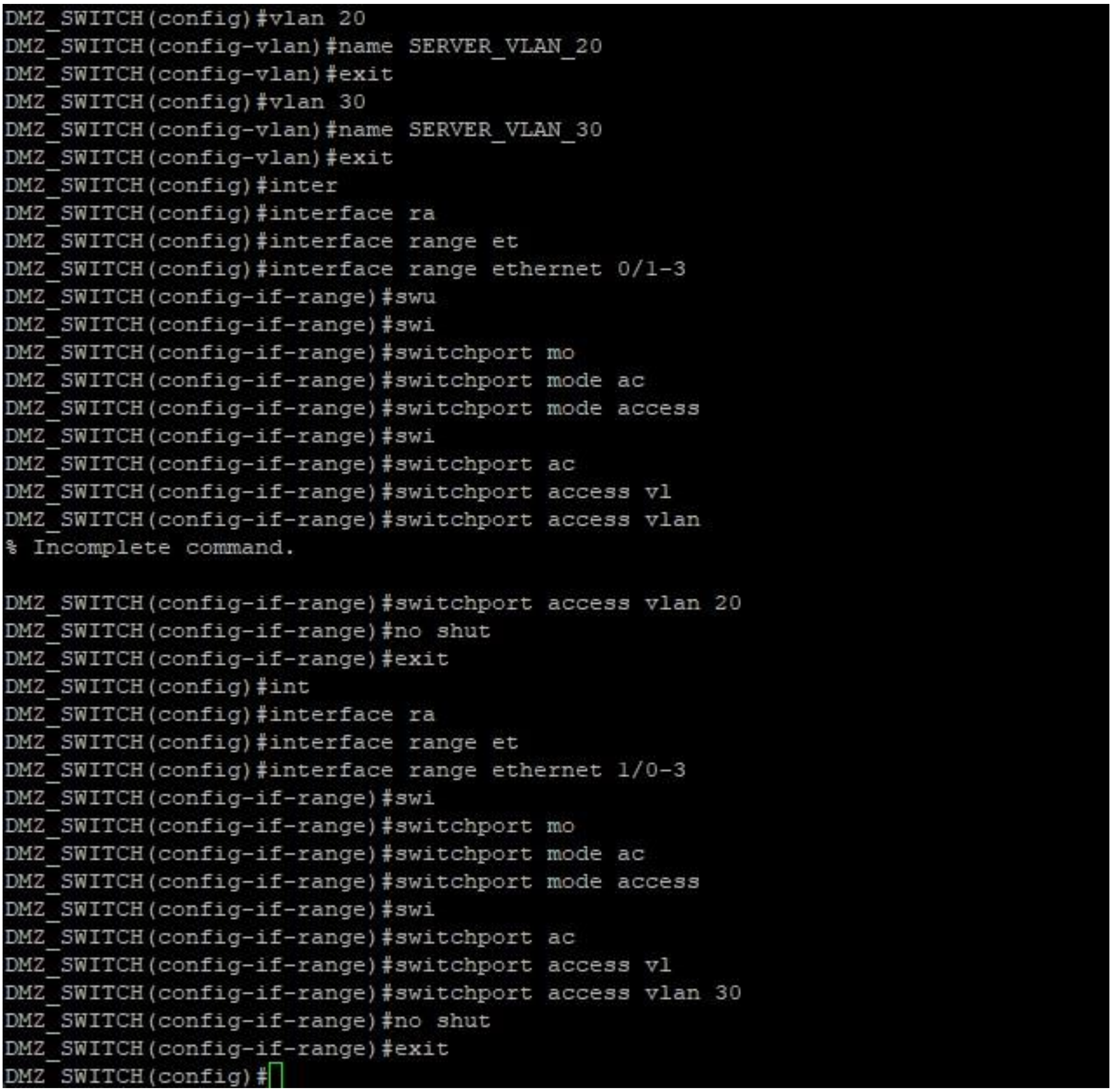
4.5.4 DMZ Cisco Switch Trunk Configuration for VLANs



```
DMZ_SWITCH#config
DMZ_SWITCH#configure ter
DMZ_SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DMZ_SWITCH(config)#inter
DMZ_SWITCH(config)#interface et
DMZ_SWITCH(config)#interface ethernet 0/0
DMZ_SWITCH(config-if)#swi
DMZ_SWITCH(config-if)#switchport tr
DMZ_SWITCH(config-if)#switchport trunk do
DMZ_SWITCH(config-if)#switchport trunk e
DMZ_SWITCH(config-if)#switchport trunk encapsulation do
DMZ_SWITCH(config-if)#switchport trunk encapsulation dot1q
DMZ_SWITCH(config-if)#swi
DMZ_SWITCH(config-if)#switchport mo
DMZ_SWITCH(config-if)#switchport mode tr
DMZ_SWITCH(config-if)#switchport mode trunk
DMZ_SWITCH(config-if)#no shut
DMZ_SWITCH(config-if)#
*Aug  4 11:57:43.053: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
DMZ_SWITCH(config-if)#exit
*Aug  4 11:57:46.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to up
DMZ_SWITCH(config-if)#exit
DMZ_SWITCH(config)#interf
DMZ_SWITCH(config)#interface et
DMZ_SWITCH(config)#interface ethernet 5/3
DMZ_SWITCH(config-if)#swi
DMZ_SWITCH(config-if)#switchport tr
DMZ_SWITCH(config-if)#switchport trunk en
DMZ_SWITCH(config-if)#switchport trunk encapsulation d
DMZ_SWITCH(config-if)#switchport trunk encapsulation dot1q
DMZ_SWITCH(config-if)#swi
DMZ_SWITCH(config-if)#switchport mo
DMZ_SWITCH(config-if)#switchport mode tr
DMZ_SWITCH(config-if)#switchport mode trunk
DMZ_SWITCH(config-if)#no shut
DMZ_SWITCH(config-if)#
*Aug  4 11:58:10.969: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet5/
3, changed state to down
DMZ_SWITCH(config-if)#
*Aug  4 11:58:13.976: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet5/
3, changed state to up
DMZ_SWITCH(config-if)#
```

Figure 4.5.4: Trunk configured for VLANs

4.5.5 DMZ Cisco Switch VLAN Configuration for VLANs from DMZ Fortigate Firewall

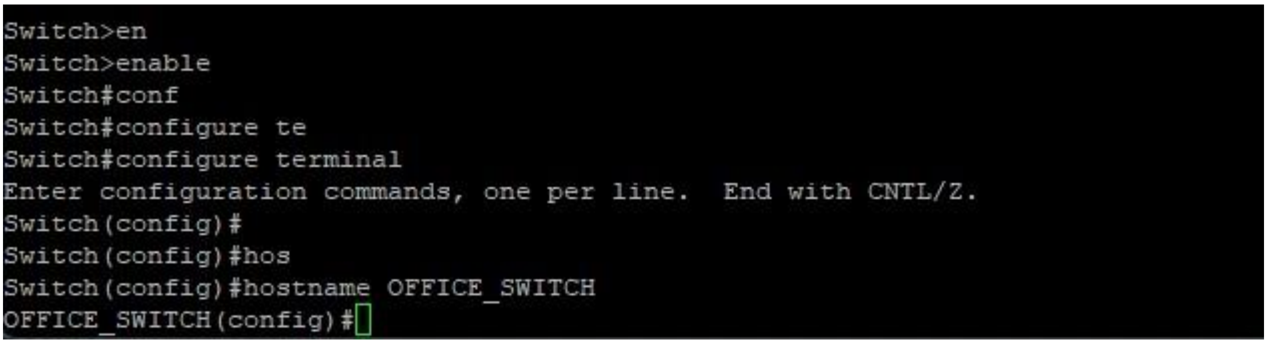


```
DMZ_SWITCH(config)#vlan 20
DMZ_SWITCH(config-vlan)#name SERVER_VLAN_20
DMZ_SWITCH(config-vlan)#exit
DMZ_SWITCH(config)#vlan 30
DMZ_SWITCH(config-vlan)#name SERVER_VLAN_30
DMZ_SWITCH(config-vlan)#exit
DMZ_SWITCH(config)#inter
DMZ_SWITCH(config)#interface ra
DMZ_SWITCH(config)#interface range et
DMZ_SWITCH(config)#interface range ethernet 0/1-3
DMZ_SWITCH(config-if-range)#swu
DMZ_SWITCH(config-if-range)#swi
DMZ_SWITCH(config-if-range)#switchport mo
DMZ_SWITCH(config-if-range)#switchport mode ac
DMZ_SWITCH(config-if-range)#switchport mode access
DMZ_SWITCH(config-if-range)#swi
DMZ_SWITCH(config-if-range)#switchport ac
DMZ_SWITCH(config-if-range)#switchport access vl
DMZ_SWITCH(config-if-range)#switchport access vlan
% Incomplete command.

DMZ_SWITCH(config-if-range)#switchport access vlan 20
DMZ_SWITCH(config-if-range)#no shut
DMZ_SWITCH(config-if-range)#exit
DMZ_SWITCH(config)#int
DMZ_SWITCH(config)#interface ra
DMZ_SWITCH(config)#interface range et
DMZ_SWITCH(config)#interface range ethernet 1/0-3
DMZ_SWITCH(config-if-range)#swi
DMZ_SWITCH(config-if-range)#switchport mo
DMZ_SWITCH(config-if-range)#switchport mode ac
DMZ_SWITCH(config-if-range)#switchport mode access
DMZ_SWITCH(config-if-range)#swi
DMZ_SWITCH(config-if-range)#switchport ac
DMZ_SWITCH(config-if-range)#switchport access vl
DMZ_SWITCH(config-if-range)#switchport access vlan 30
DMZ_SWITCH(config-if-range)#no shut
DMZ_SWITCH(config-if-range)#exit
DMZ_SWITCH(config)#
```

Figure 4.5.5: VLANs configured

4.6 Office Cisco Switch Configuration for VLANs from DMZ Fortigate Firewall

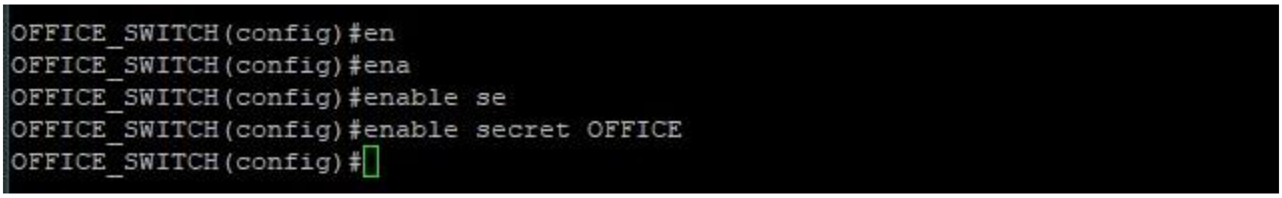
4.6.1 Office Cisco Switch Hostname Configuration



```
Switch>en
Switch>enable
Switch#conf
Switch#configure te
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#hos
Switch(config)#hostname OFFICE_SWITCH
OFFICE_SWITCH(config)#
```

Figure 4.6.1: hostname configured

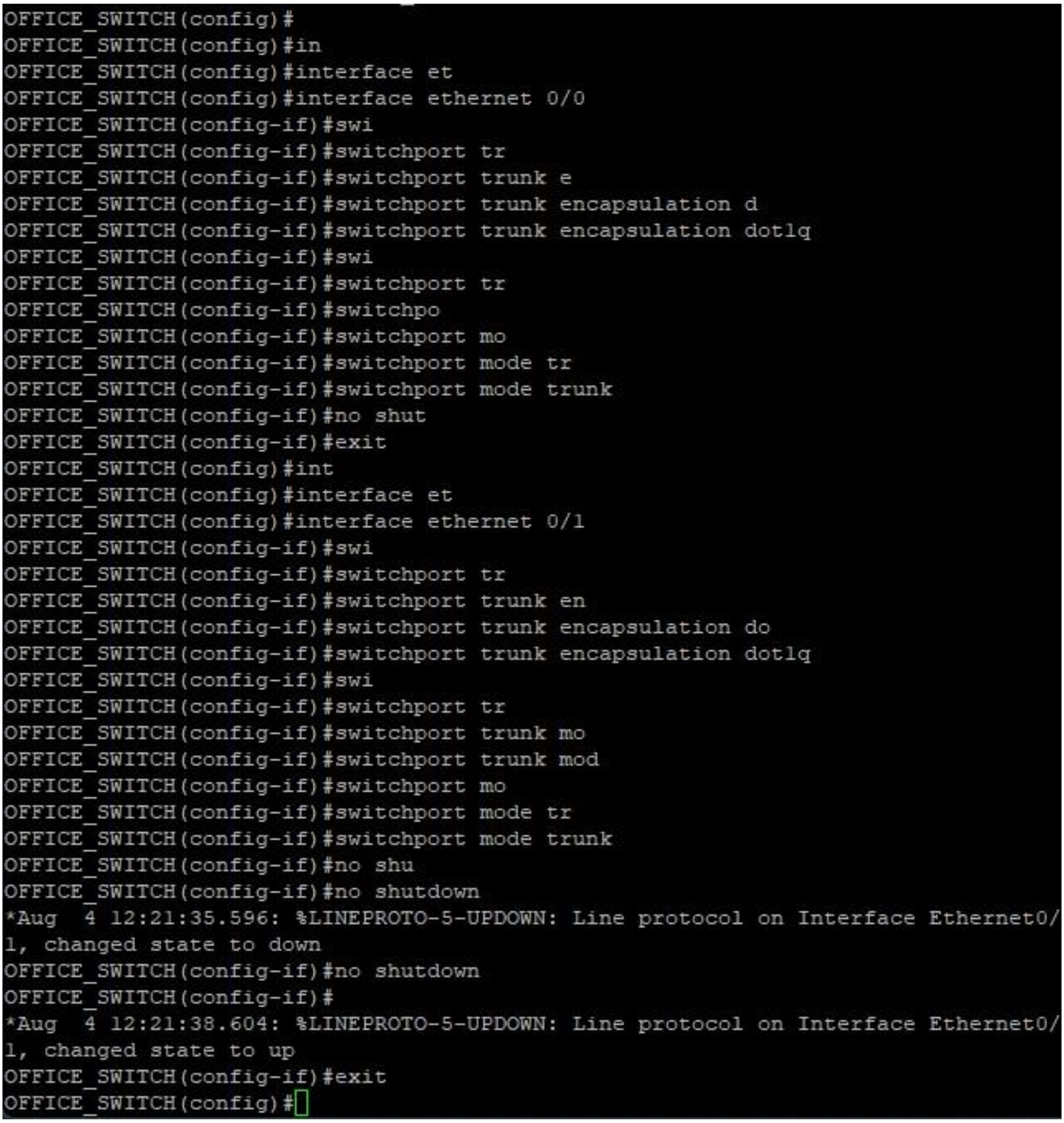
4.6.2 Office Cisco Switch Privilege Security Configuration



```
OFFICE_SWITCH(config)#en
OFFICE_SWITCH(config)#ena
OFFICE_SWITCH(config)#enable se
OFFICE_SWITCH(config)#enable secret OFFICE
OFFICE_SWITCH(config)#
```

Figure 4.6.2: secret configured

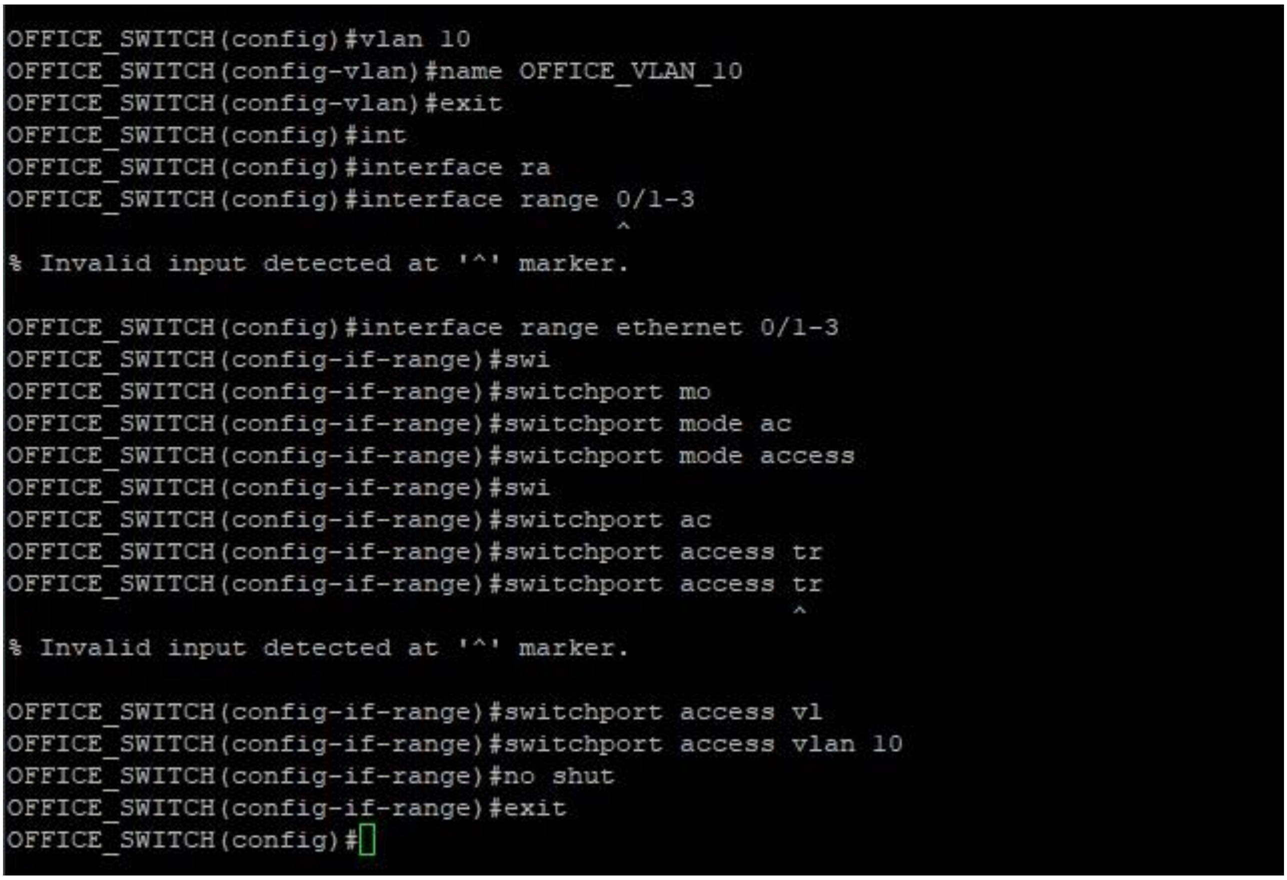
4.6.3 Office Cisco Switch Trunk Mode Configuration



```
OFFICE_SWITCH(config)#
OFFICE_SWITCH(config)#in
OFFICE_SWITCH(config)#interface et
OFFICE_SWITCH(config)#interface ethernet 0/0
OFFICE_SWITCH(config-if)#swi
OFFICE_SWITCH(config-if)#switchport tr
OFFICE_SWITCH(config-if)#switchport trunk e
OFFICE_SWITCH(config-if)#switchport trunk encapsulation d
OFFICE_SWITCH(config-if)#switchport trunk encapsulation dotlq
OFFICE_SWITCH(config-if)#swi
OFFICE_SWITCH(config-if)#switchport tr
OFFICE_SWITCH(config-if)#switchpo
OFFICE_SWITCH(config-if)#switchport mo
OFFICE_SWITCH(config-if)#switchport mode tr
OFFICE_SWITCH(config-if)#switchport mode trunk
OFFICE_SWITCH(config-if)#no shut
OFFICE_SWITCH(config-if)#exit
OFFICE_SWITCH(config)#int
OFFICE_SWITCH(config)#interface et
OFFICE_SWITCH(config)#interface ethernet 0/1
OFFICE_SWITCH(config-if)#swi
OFFICE_SWITCH(config-if)#switchport tr
OFFICE_SWITCH(config-if)#switchport trunk en
OFFICE_SWITCH(config-if)#switchport trunk encapsulation do
OFFICE_SWITCH(config-if)#switchport trunk encapsulation dotlq
OFFICE_SWITCH(config-if)#swi
OFFICE_SWITCH(config-if)#switchport tr
OFFICE_SWITCH(config-if)#switchport trunk mo
OFFICE_SWITCH(config-if)#switchport trunk mod
OFFICE_SWITCH(config-if)#switchport mo
OFFICE_SWITCH(config-if)#switchport mode tr
OFFICE_SWITCH(config-if)#switchport mode trunk
OFFICE_SWITCH(config-if)#no shu
OFFICE_SWITCH(config-if)#no shutdown
*Aug  4 12:21:35.596: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to down
OFFICE_SWITCH(config-if)#no shutdown
OFFICE_SWITCH(config-if)#
*Aug  4 12:21:38.604: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to up
OFFICE_SWITCH(config-if)#exit
OFFICE_SWITCH(config)#
```

Figure 4.6.3: Trunk configured for VLANs

4.6.4 Office Cisco Switch VLAN Configuration



```
OFFICE_SWITCH(config)#vlan 10
OFFICE_SWITCH(config-vlan)#name OFFICE_VLAN_10
OFFICE_SWITCH(config-vlan)#exit
OFFICE_SWITCH(config)#int
OFFICE_SWITCH(config)#interface ra
OFFICE_SWITCH(config)#interface range 0/1-3
                                      ^
% Invalid input detected at '^' marker.

OFFICE_SWITCH(config)#interface range ethernet 0/1-3
OFFICE_SWITCH(config-if-range)#swi
OFFICE_SWITCH(config-if-range)#switchport mo
OFFICE_SWITCH(config-if-range)#switchport mode ac
OFFICE_SWITCH(config-if-range)#switchport mode access
OFFICE_SWITCH(config-if-range)#swi
OFFICE_SWITCH(config-if-range)#switchport ac
OFFICE_SWITCH(config-if-range)#switchport access tr
OFFICE_SWITCH(config-if-range)#switchport access tr
                                                 ^
% Invalid input detected at '^' marker.

OFFICE_SWITCH(config-if-range)#switchport access vl
OFFICE_SWITCH(config-if-range)#switchport access vlan 10
OFFICE_SWITCH(config-if-range)#no shut
OFFICE_SWITCH(config-if-range)#exit
OFFICE_SWITCH(config)#
```

Figure 4.6.4: VLAN configured

4.7 Mikrotik IPSec VPN Connection for Firewall

- VPN testing at outside of DOL

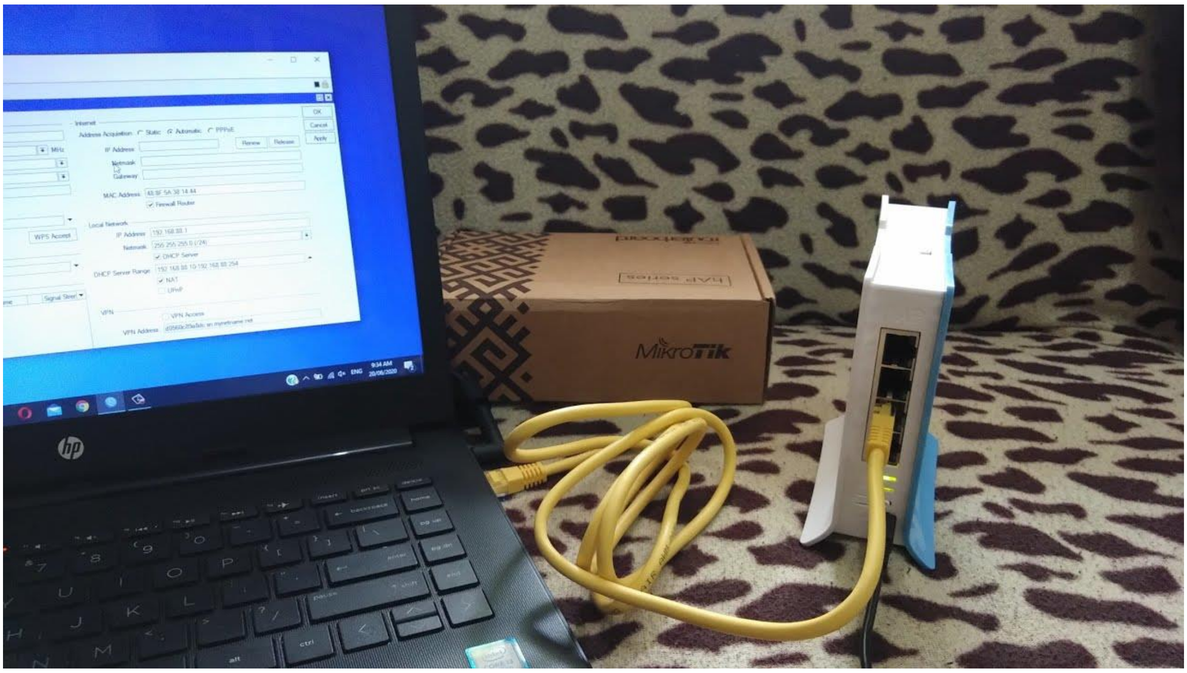
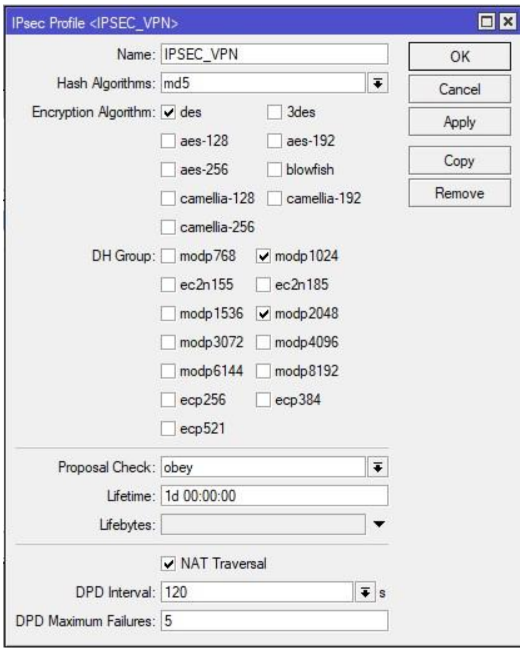


Figure 4.7: Mikrotik hAP lite TC device connected by laptop, accessing via WinBox

4.7.1 IPSec Configuration

- Open ‘IP’ > ‘IPsec’ > select ‘Profile’ > click ‘+’ to configure
- Add ‘Name’ > add ‘md5’ to ‘Hash Algorithms’ > enable ‘des’ to ‘Encryption Algorithm’ > enable ‘NAT Traversal’ > click OK



IPsec Profile <IPSEC_VPN>

Name: IPSEC_VPN

Hash Algorithms: md5

Encryption Algorithm: ☑ des ☐ 3des ☐ aes-128 ☐ aes-192 ☐ aes-256 ☐ blowfish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256

DH Group: ☐ modp768 ☑ modp1024 ☐ ec2n155 ☐ ec2n185 ☐ modp1536 ☑ modp2048 ☐ modp3072 ☐ modp4096 ☐ modp6144 ☐ modp8192 ☐ ecp256 ☐ ecp384 ☐ ecp521

Proposal Check: obey

Lifetime: 1d 00:00:00

Lifebytes:

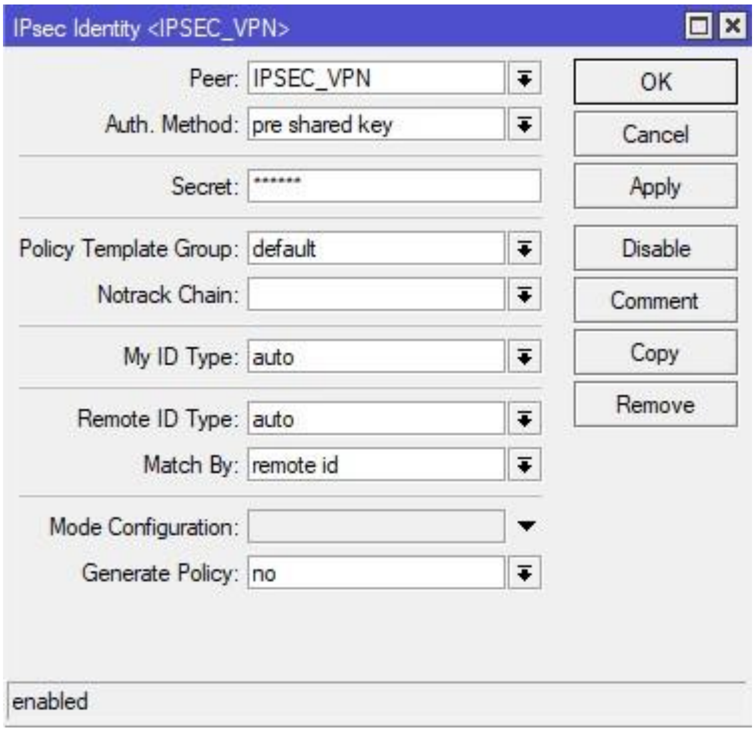
☑ NAT Traversal

DPD Interval: 120 s

DPD Maximum Failures: 5

Figure 4.7.1.1: IPSec VPN configuration

- Select ‘Identity’ > click ‘+’ to configure new > select ‘Peer’ from created profile > select Auth. Method ‘pre shared key’ > add ‘Secret’ > click OK



IPsec Identity <IPSEC_VPN>

Peer: IPSEC_VPN

Auth. Method: pre shared key

Secret: ******

Policy Template Group: default

Notrack Chain:

My ID Type: auto

Remote ID Type: auto

Match By: remote id

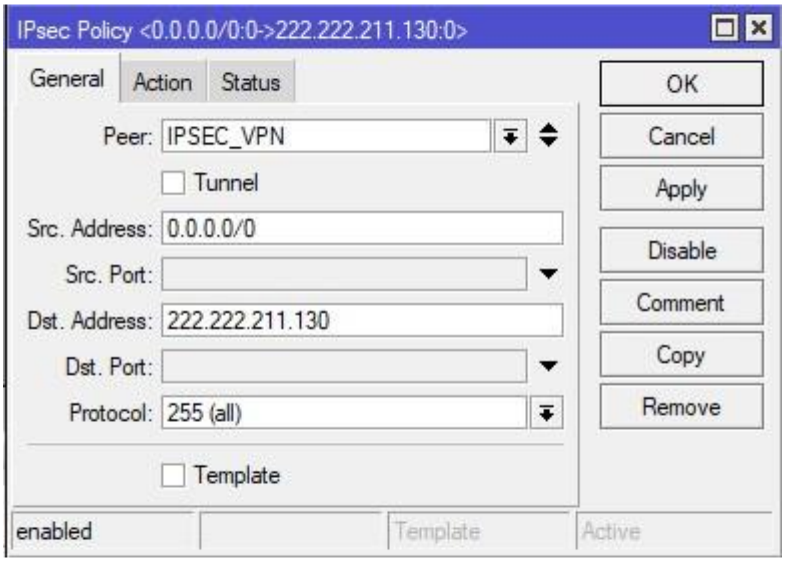
Mode Configuration:

Generate Policy: no

enabled

Figure 4.7.1.2: IPSecVPN pre-sared key assigned

- Select ‘Policy’ > click ‘+’ to configure new > select ‘Peer’ from created profile > add ‘Dst. Address’ > click OK
- Firewalls ip address assigned on Dst. Address for IPSec VPN



IPsec Policy <0.0.0.0/0:0->222.222.211.130:0>

General | Action | Status

Peer: IPSEC_VPN

□ Tunnel

Src. Address: 0.0.0.0/0

Src. Port:

Dst. Address: 222.222.211.130

Dst. Port:

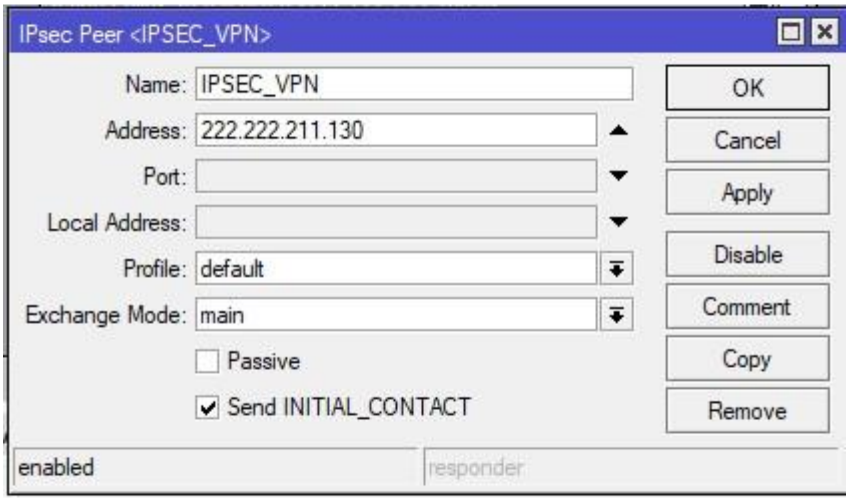
Protocol: 255 (all)

□ Template

enabled | | Template | Active

Figure 4.7.1.3: IPSecVPN policy

- Select ‘Peer’ > click ‘+’ to configure new > add ‘Name’ > add ‘Address’ > select ‘Profile’ as ‘default’ > click OK
- Peer address of Firewall added



IPsec Peer <IPSEC_VPN>

Name: IPSEC_VPN

Address: 222.222.211.130

Port:

Local Address:

Profile: default

Exchange Mode: main

□ Passive

☑ Send INITIAL_CONTACT

enabled

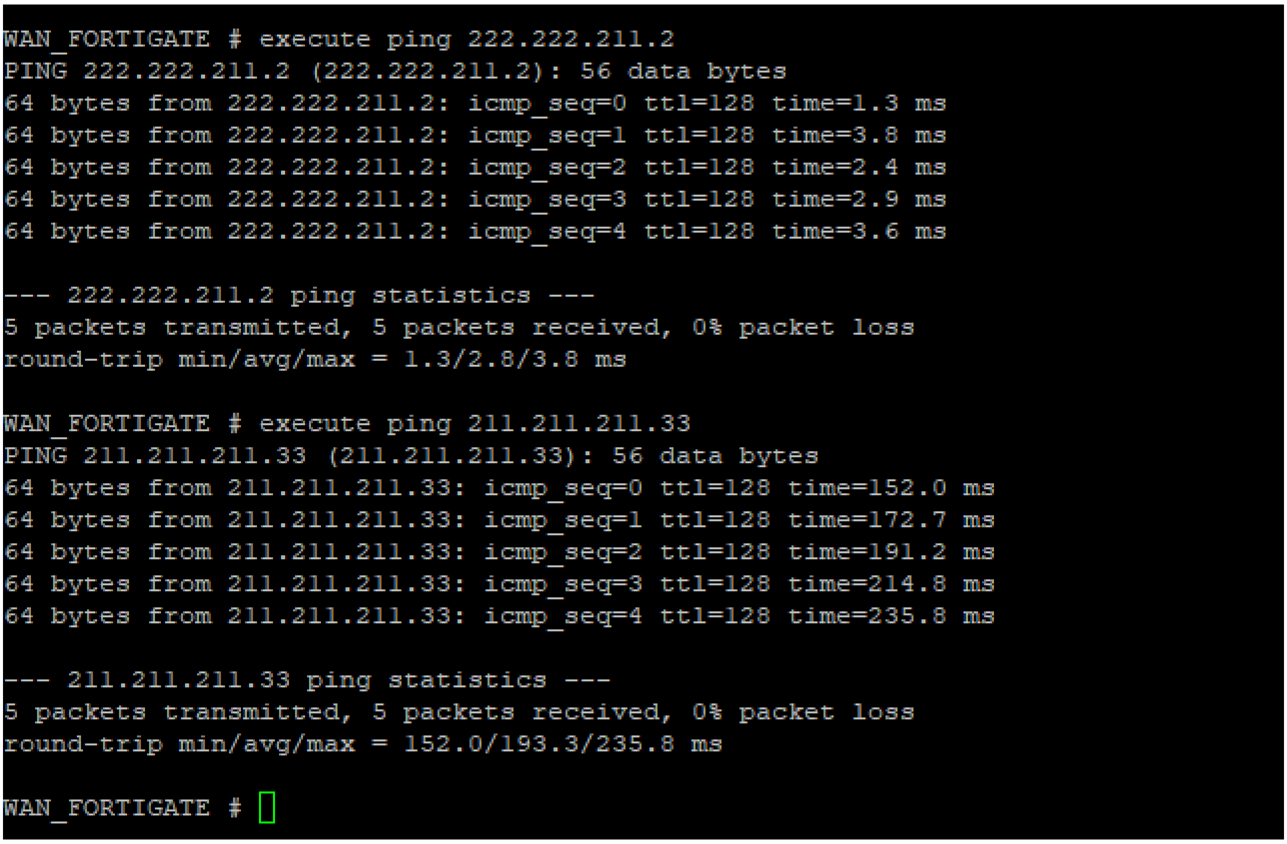
responder

Figure 4.7.1.4: Ip address connection for peer

CHAPTER 5

OUTPUTS OF MY PROJECT

5.1 Output of WAN Firewall Load Balance

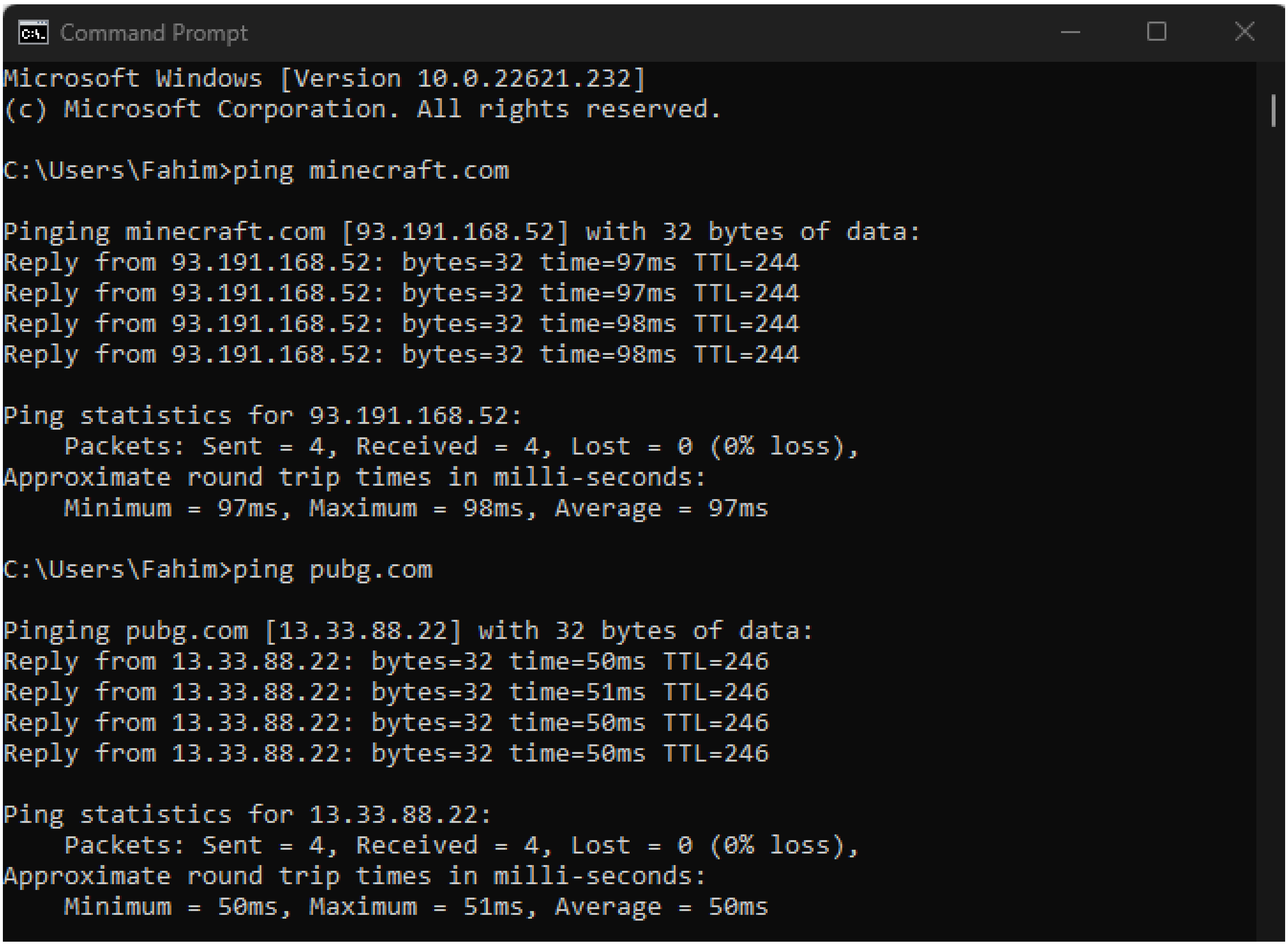


```
WAN_FORTIGATE # execute ping 222.222.211.2
PING 222.222.211.2 (222.222.211.2): 56 data bytes
64 bytes from 222.222.211.2: icmp_seq=0 ttl=128 time=1.3 ms
64 bytes from 222.222.211.2: icmp_seq=1 ttl=128 time=3.8 ms
64 bytes from 222.222.211.2: icmp_seq=2 ttl=128 time=2.4 ms
64 bytes from 222.222.211.2: icmp_seq=3 ttl=128 time=2.9 ms
64 bytes from 222.222.211.2: icmp_seq=4 ttl=128 time=3.6 ms

--- 222.222.211.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.3/2.8/3.8 ms

WAN_FORTIGATE # execute ping 211.211.211.33
PING 211.211.211.33 (211.211.211.33): 56 data bytes
64 bytes from 211.211.211.33: icmp_seq=0 ttl=128 time=152.0 ms
64 bytes from 211.211.211.33: icmp_seq=1 ttl=128 time=172.7 ms
64 bytes from 211.211.211.33: icmp_seq=2 ttl=128 time=191.2 ms
64 bytes from 211.211.211.33: icmp_seq=3 ttl=128 time=214.8 ms
64 bytes from 211.211.211.33: icmp_seq=4 ttl=128 time=235.8 ms

--- 211.211.211.33 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 152.0/193.3/235.8 ms

WAN_FORTIGATE # 
```

Figure 5.1: Ping check for load balance connectivity

5.2 Output of PUBG and Mine Craft from Firewall Rules

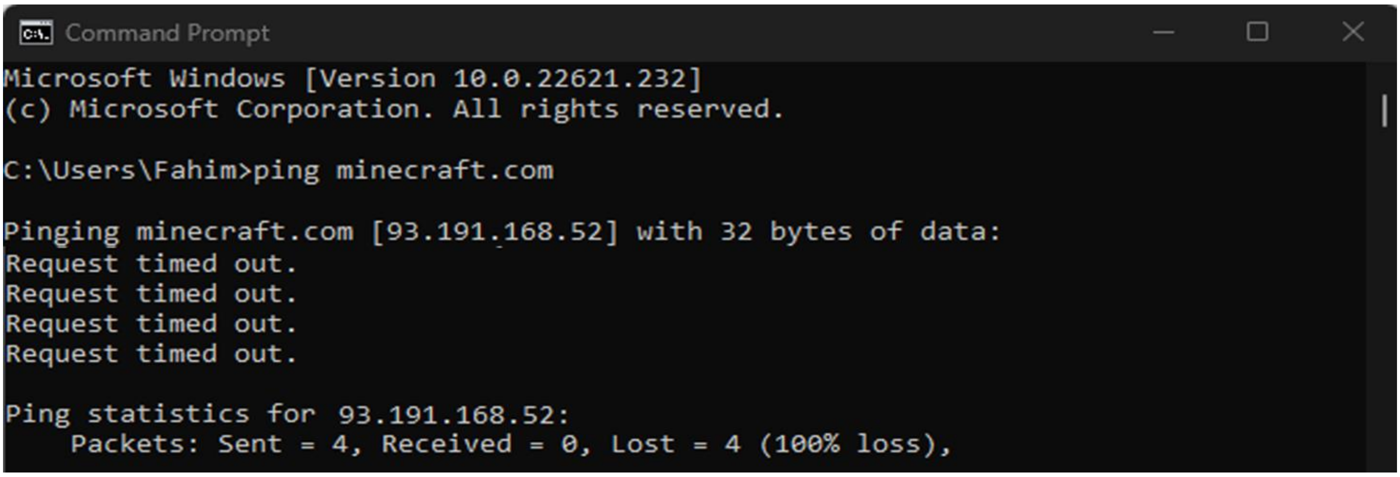
- Before



```
Microsoft Windows [Version 10.0.22621.232]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Fahim>ping minecraft.com

Pinging minecraft.com [93.191.168.52] with 32 bytes of data:
Reply from 93.191.168.52: bytes=32 time=97ms TTL=244
Reply from 93.191.168.52: bytes=32 time=97ms TTL=244
Reply from 93.191.168.52: bytes=32 time=98ms TTL=244
Reply from 93.191.168.52: bytes=32 time=98ms TTL=244

Ping statistics for 93.191.168.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 97ms, Maximum = 98ms, Average = 97ms

C:\Users\Fahim>ping pubg.com

Pinging pubg.com [13.33.88.22] with 32 bytes of data:
Reply from 13.33.88.22: bytes=32 time=50ms TTL=246
Reply from 13.33.88.22: bytes=32 time=51ms TTL=246
Reply from 13.33.88.22: bytes=32 time=50ms TTL=246
Reply from 13.33.88.22: bytes=32 time=50ms TTL=246

Ping statistics for 13.33.88.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 51ms, Average = 50ms
```

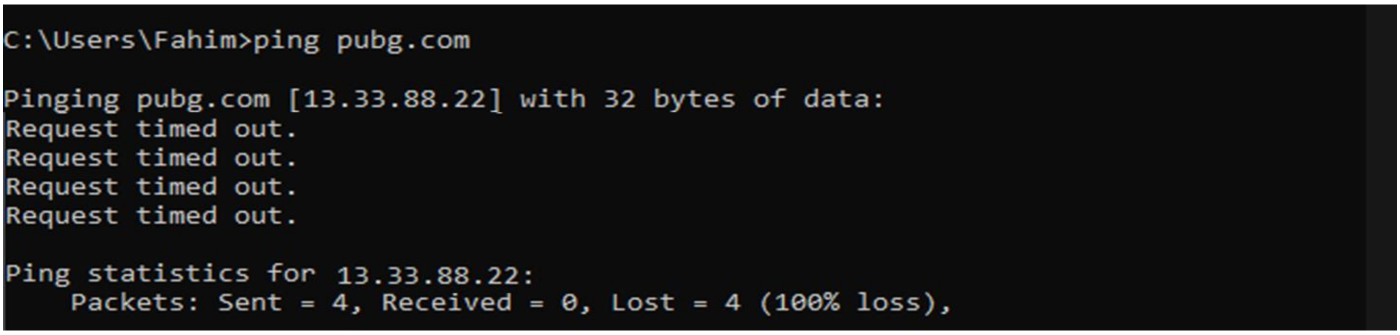
Figure 5.2.1: Ping check to PUBG and Minecraft host addresses

- After



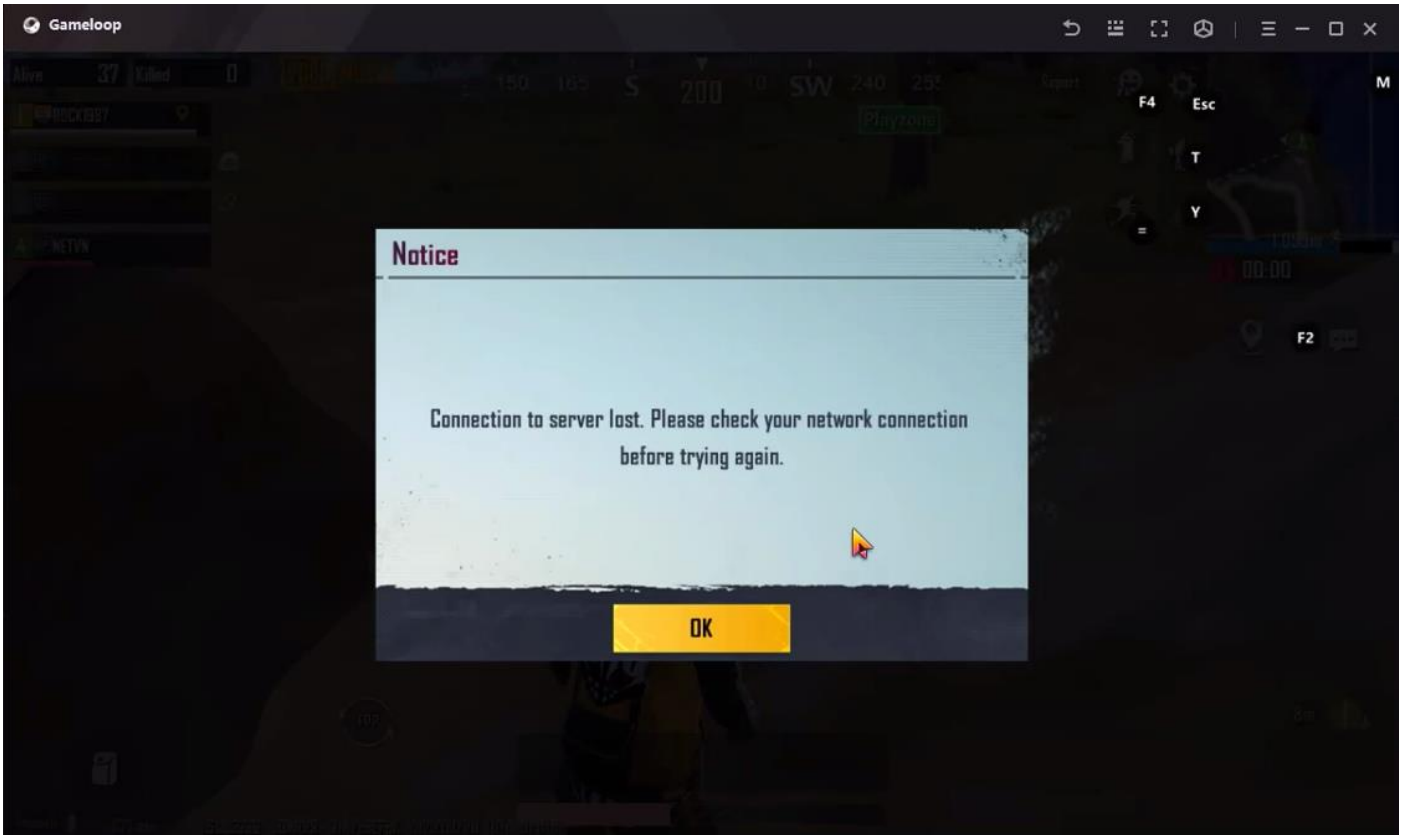
```
Microsoft Windows [Version 10.0.22621.232]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Fahim>ping minecraft.com

Pinging minecraft.com [93.191.168.52] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 93.191.168.52:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 5.2.2: Ping result of Minecraft host address



```
C:\Users\Fahim>ping pubg.com

Pinging pubg.com [13.33.88.22] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.33.88.22:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

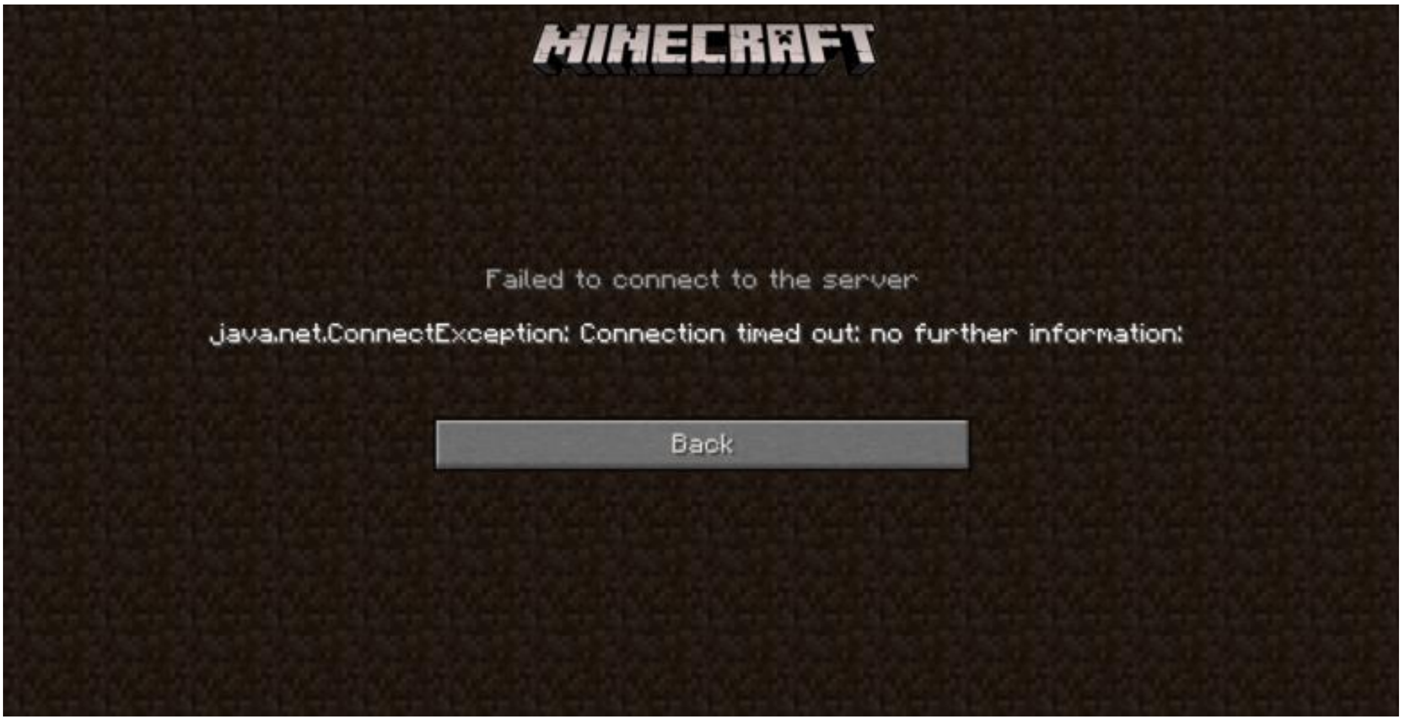
Figure 5.2.3: Ping result of PUBG host address



Notice

Connection to server lost. Please check your network connection before trying again.

Figure 5.2.4: Output of PUBG connection lost

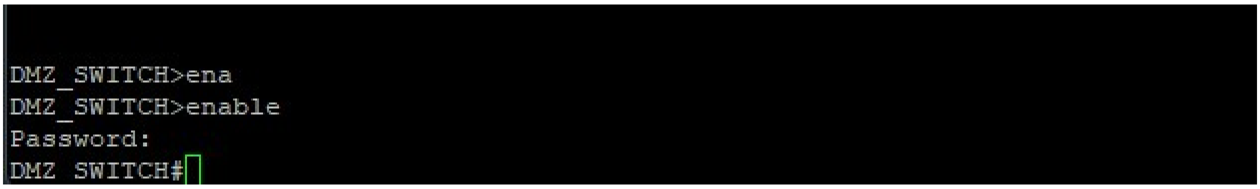


Failed to connect to the server

java.net.ConnectException: Connection timed out: no further information:

Figure 5.2.5: Output of Minecraft connection lost

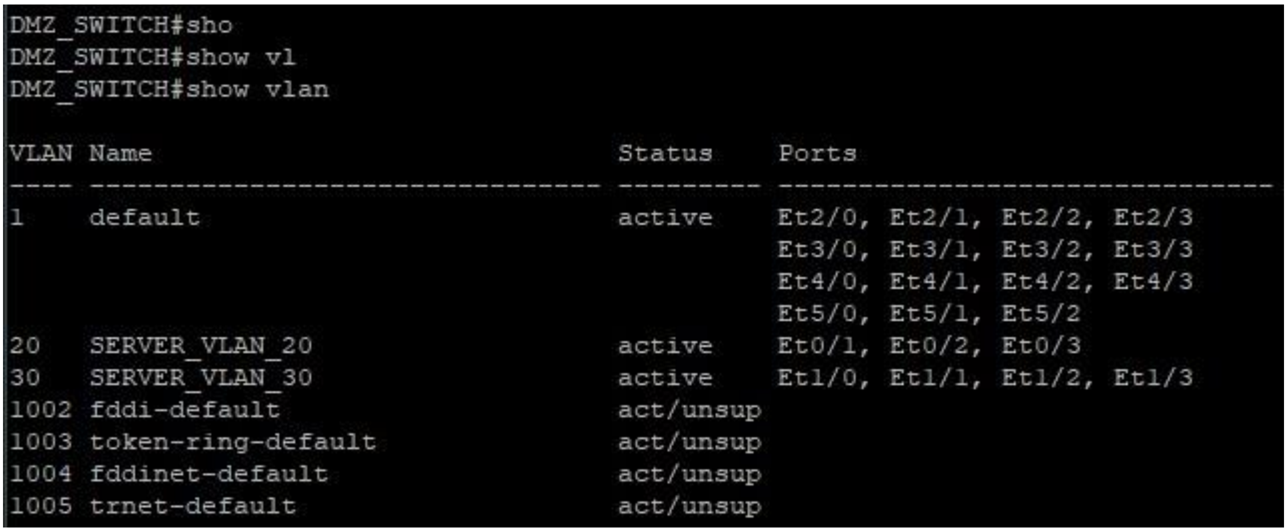
5.3 DMZ Cisco Switch Enable Secret



```
DMZ_SWITCH>ena
DMZ_SWITCH>enable
Password:
DMZ_SWITCH#
```

Figure 5.3: Output of switch enable secret

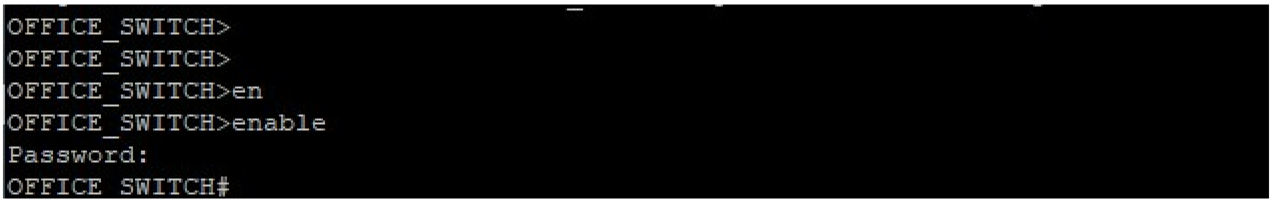
5.4 DMZ Cisco Switch VLANs



```
DMZ_SWITCH#sho
DMZ_SWITCH#show vl
DMZ_SWITCH#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
                                                Et4/0, Et4/1, Et4/2, Et4/3
                                                Et5/0, Et5/1, Et5/2
20   SERVER_VLAN_20                   active    Et0/1, Et0/2, Et0/3
30   SERVER_VLAN_30                   active    Et1/0, Et1/1, Et1/2, Et1/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figure 5.4: Output of switch configured VLANs

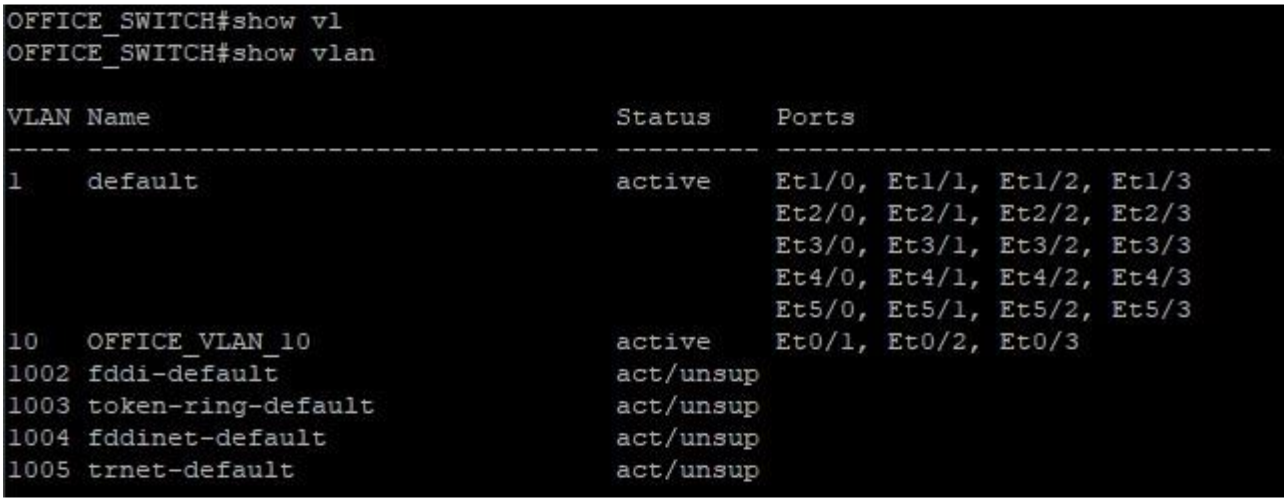
5.5 Office Cisco Switch Enable Secret Output



```
OFFICE_SWITCH>
OFFICE_SWITCH>
OFFICE_SWITCH>en
OFFICE_SWITCH>enable
Password:
OFFICE_SWITCH#
```

Figure 5.5: Output of switch enable secret

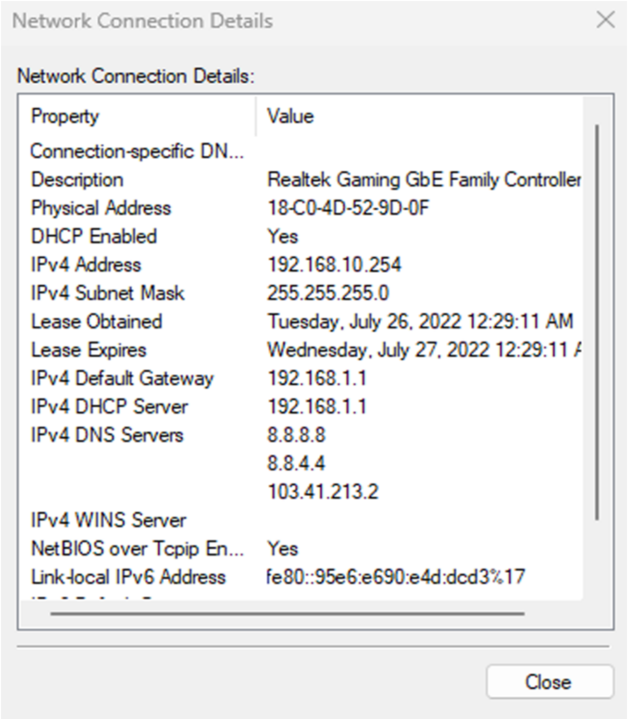
5.6 Office Cisco Switch VLANs



```
OFFICE_SWITCH#show vl
OFFICE_SWITCH#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
                                                Et4/0, Et4/1, Et4/2, Et4/3
                                                Et5/0, Et5/1, Et5/2, Et5/3
10   OFFICE_VLAN_10                   active    Et0/1, Et0/2, Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figure 5.6: Output of switch configured VLANs

5.7 VLAN DHCP Leases from DMZ Firewall

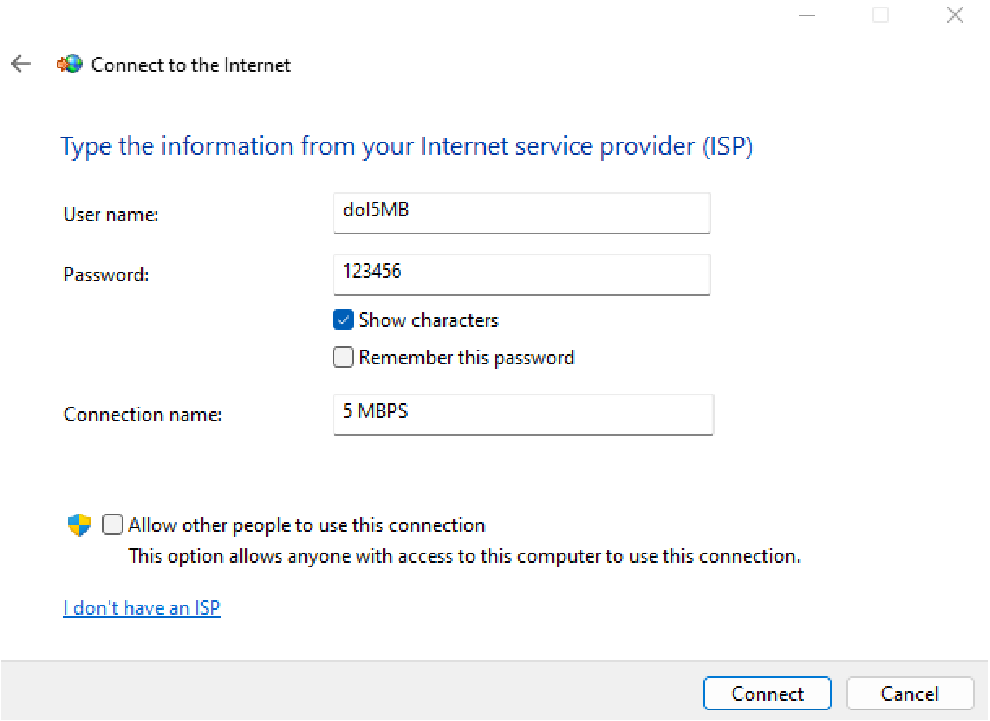


Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek Gaming GbE Family Controller
Physical Address	18-C0-4D-52-9D-0F
DHCP Enabled	Yes
IPv4 Address	192.168.10.254
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Tuesday, July 26, 2022 12:29:11 AM
Lease Expires	Wednesday, July 27, 2022 12:29:11 A
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Servers	8.8.8.8 8.8.4.4 103.41.213.2
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::95e6:e690:e4d:dcd3%17

Figure 5.7: Output of DHCP leased ip address

5.8 PPPoE User Connection from PPPoE Mikrotik Router



Type the information from your Internet service provider (ISP)

User name: dol5MB

Password: 123456

☑ Show characters

☐ Remember this password

Connection name: 5 MBPS

☐ Allow other people to use this connection

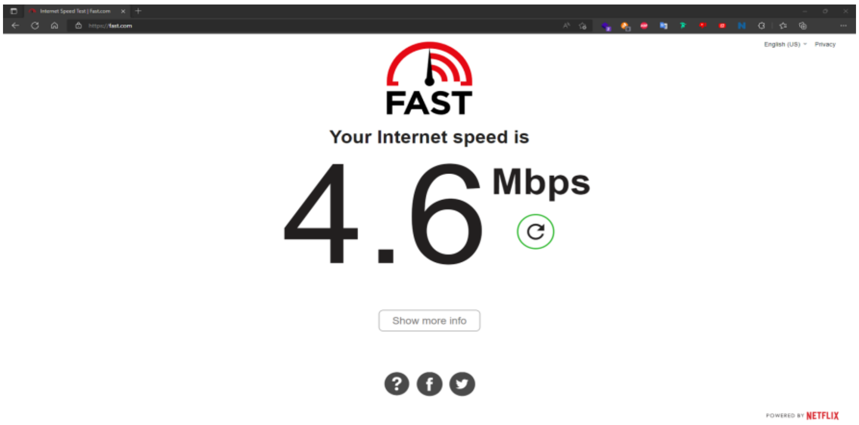
This option allows anyone with access to this computer to use this connection.

I don't have an ISP

Figure 5.8: PPPoE client configuration

5.9 PPPoE Bandwidth Queue Performance

- 5 MBPS Bandwidth Queue Performance

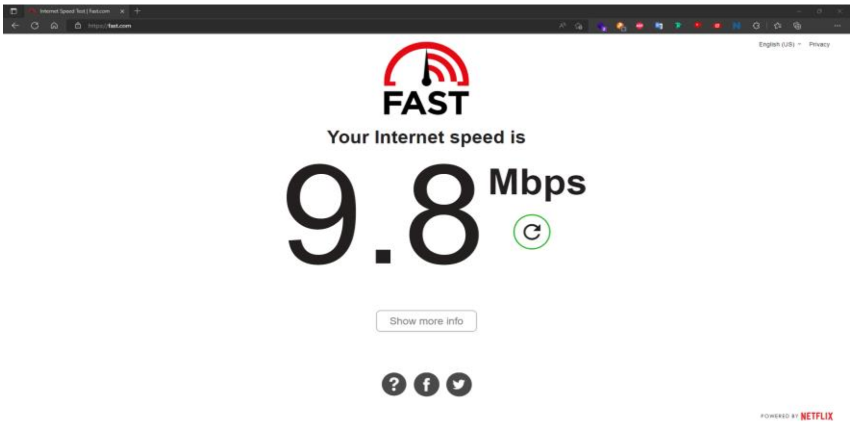


Your Internet speed is

4.6 Mbps

Figure 5.9.1: Screenshot output of 5 MBPS bandwidth

- 10MBPS Bandwidth Queue Test

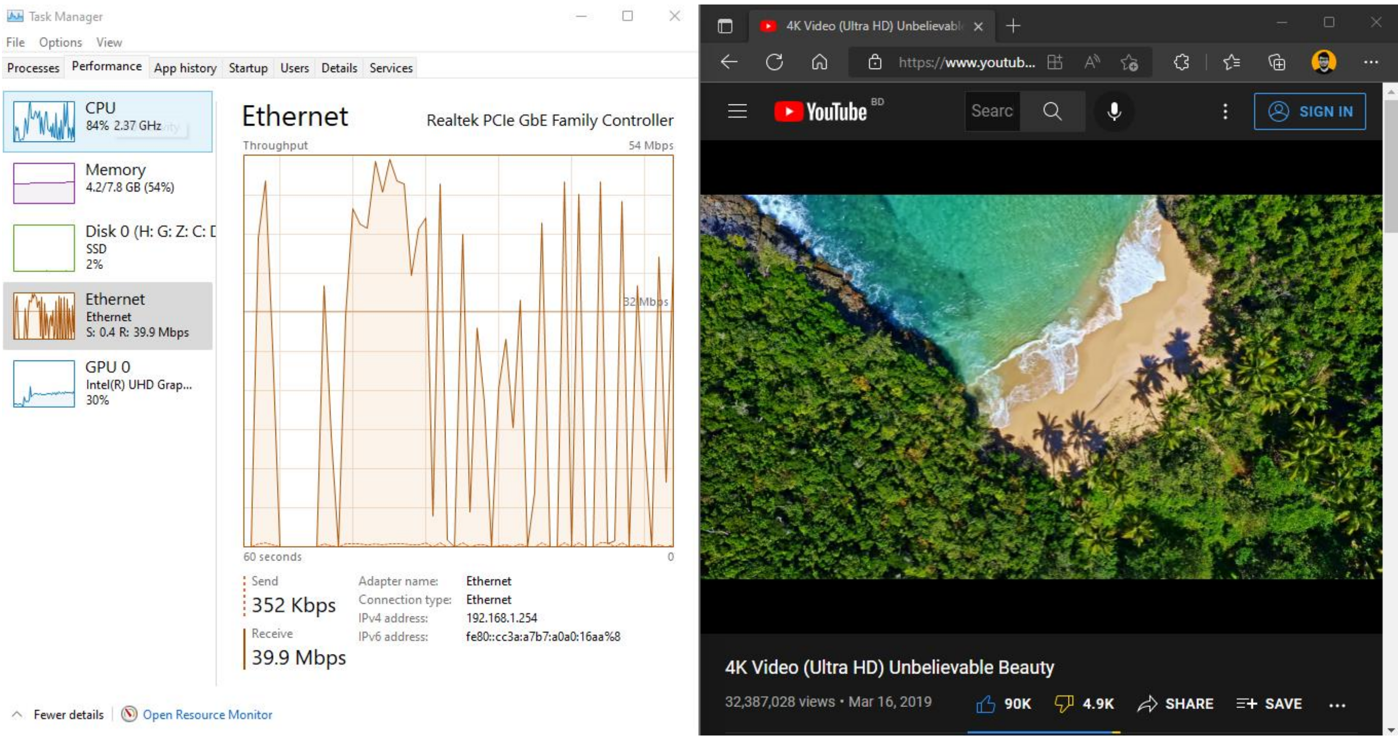


Your Internet speed is

9.8 Mbps

Figure 5.9.2: Screenshot output of 10 MBPS bandwidth

- GGC Cache Server bandwidth



Send
352 Kbps

Receive
39.9 Mbps

Adapter name: Ethernet
Connection type: Ethernet
IPv4 address: 192.168.1.254
IPv6 address: fe80::cc3a:a7b7:a0a0:16aa%8

4K Video (Ultra HD) Unbelievable Beauty

32,387,028 views • Mar 16, 2019

Figure 5.9.3: Screenshot output of GGC bandwidth

CHAPTER 6

CONCLUSION AND SCOPE

6.1 Conclusion

My theoretical networking knowledge was much enhanced by regularly attending DOL, organizing projects, studying practically every day, configuring, resolving, troubleshooting issues, and so on. I can now operate and configure several devices. If necessary, I will be able to configure a better routing protocol in place of static routing. I did not configure any Windows or Linux-based servers during this internship, but by doing so, my self-learning improved, and I will learn these configurations on my own if necessary.

The next-generation firewalls are a fantastic network security technology to understand. It's a brilliant technology because it filters all incoming and outgoing packets. I will be able to contribute my all to future company fields by participating in this project-based internship.

6.2 Future Scope and Scalability of This Project

Penetration Testing:

- To detect and to secure open ports of ISP devices can be done by penetration testing.
- Vulnerabilities can be minimized.
- MITM, DNS spoofing, IP spoofing, DDoS, Rootkits, Botnets etc. network attacks can be minimized by penetration testing.

Linux Server Installation:

- FTP, Web, DNS cache, Syslog etc. servers can be configured to establish this project.

Windows Server Installation:

- Lab, office computers can be controlled along IP addresses under a domain from a Windows server.

Different Device Installation:

- Fortigate firewalls can be substituted with pfSense firewalls.
- Cisco switches can be substituted with a Juniper switch device.

REFERENCES

Daffodil Online Ltd. | About (2020). Retrieved July 16, 2022 from Daffodil Online Ltd.'s Website: https://www.daffodilnet.com/about-us.php

Google Scholar Contributors. *Get help from a project report.* Retrieved June 13, 2022 from Google Scholar, Website: https://scholar.google.com/

Mikrotik, Cisco and Fortigate OS. Retrieved July 18, 2022 from Mikrotik's Website: http://www.mikrotik-routeros.net/routeros.aspx/

Wikipedia Contributors. (2019, August 15). *Cisco IOS*. Retrieved from Wikipedia, The Free Encyclopedia: https://en.wikipedia.org/wiki/Cisco_IOS/

Mikrotik, Cisco and Fortigate OS. Retrieved July 18, 2022 from Fortigate's Website: https://www.fortinet.com/products/next-generation-firewall/

Fortigate Firewall Features. Retrieved July 18, 2022 from Router Switch Information Website: https://www.router-switch.com/fg-30e.html/

Cisco Switch Features. Retrieved July 18, 2022 from Website: https://www.batna24.com/en/p/cisco-sg350x24pd-poe-swtich-rmmmm/

Mikrotik, Fortigate, Cisco Device Details. Retrieved July 19, 2022 from Mikrotik's Website: https://mikrotik.com/product/RB2011UiAS-RM/

Diagram of This ISP Setup Project. Retrieved July 21, 2022 from Draw io's Website: http://draw.io/

Putty | About. Retrieved June 14, 2022 from Putty's Website: https://www.putty.org/

WinBox | About. Retrieved June 14, 2022 from WinBox's Website: https://mikrotik.com/download/

Penetration Testing. Retrieved August 8, 2022 from Security Zine's Website: https://securityzines.com/flyers/networkattacks.html

Firewall Working Method. (28 Jun, 2022) Retrieved October 26, 2022 from Geek for Geek's Website: *https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/*

Internet Speed Tester. Retrieved June 12, 2022 from Website: https://fast.com/

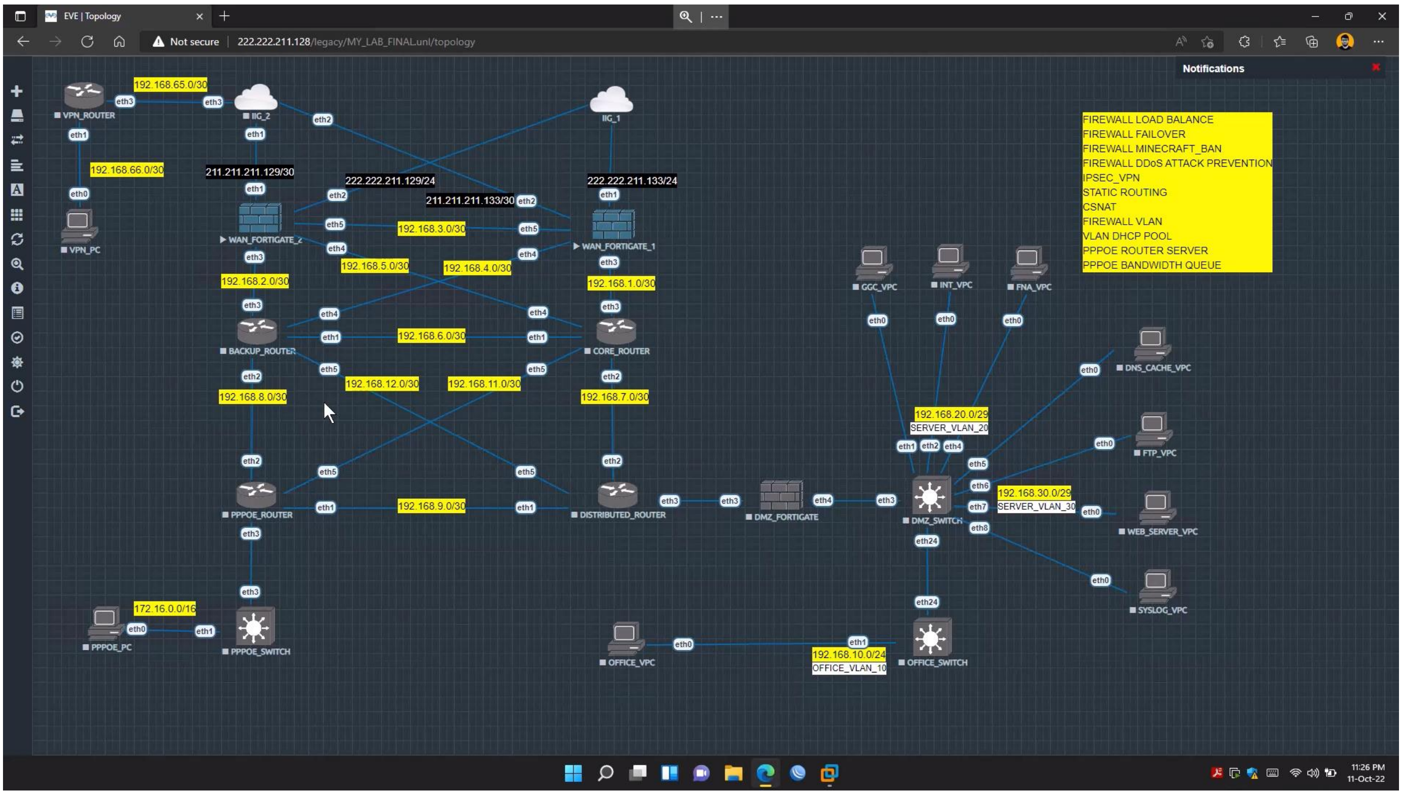
APPENDICES

Appendix A: Screenshot of VMWare EVE-NG Projects Done

Demo virtual environment lab of my project from DOL. Describing OUTSIDE, INSIDE, DMZ protected by firewalls. Core router along with backup router, network distribution to internal office, DMZ from distributed router. Client service from PPPoE router. An exceptional VPN router to establish IPSec VPN from outside of ISP to internal office.

Virtual environment images of:

- Three Fortigate firewalls images
- Five Mikrotik routers images
- Three Cisco switches images
- Few VPCs to test connectivity, VPN



FIREWALL LOAD BALANCE
FIREWALL FAILOVER
FIREWALL MINECRAFT_BAN
FIREWALL DDoS ATTACK PREVENTION
IPSEC_VPN
STATIC ROUTING
CSNAT
FIREWALL VLAN
VLAN DHCP POOL
PPPOE ROUTER SERVER
PPPOE BANDWIDTH QUEUE

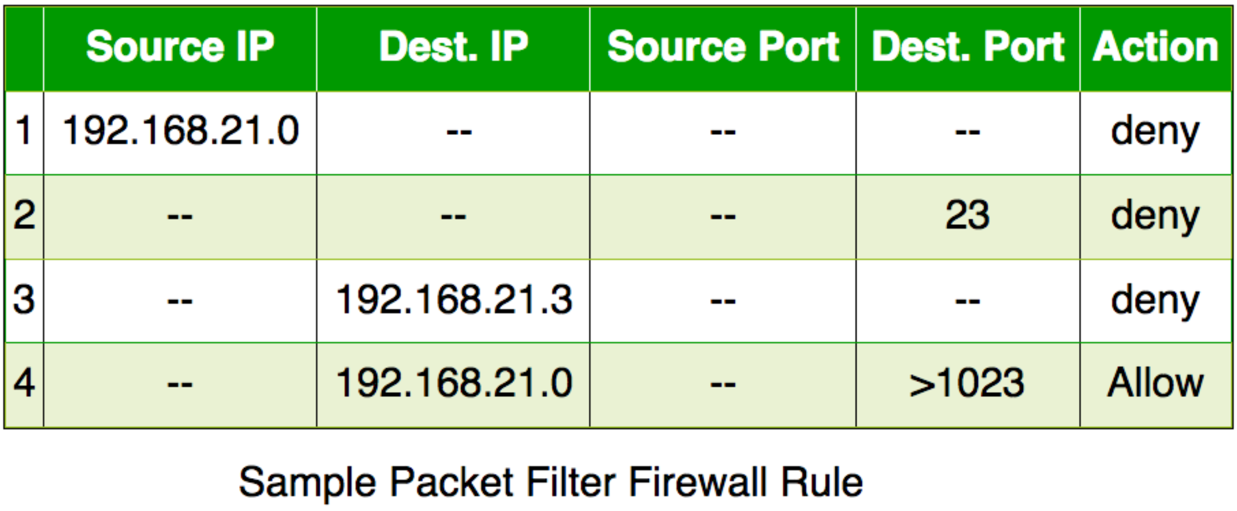
Demo VMWare EVE-NG project lab

Appendix B: Firewall Working Method

During the third month of my internship at DOL, the trainer taught me how to operate a firewall.

Methods:

- Accept: permits traffic
- Reject: blocks traffic but responds with "unreachable error"
- Drop: prevents traffic but makes no response



	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

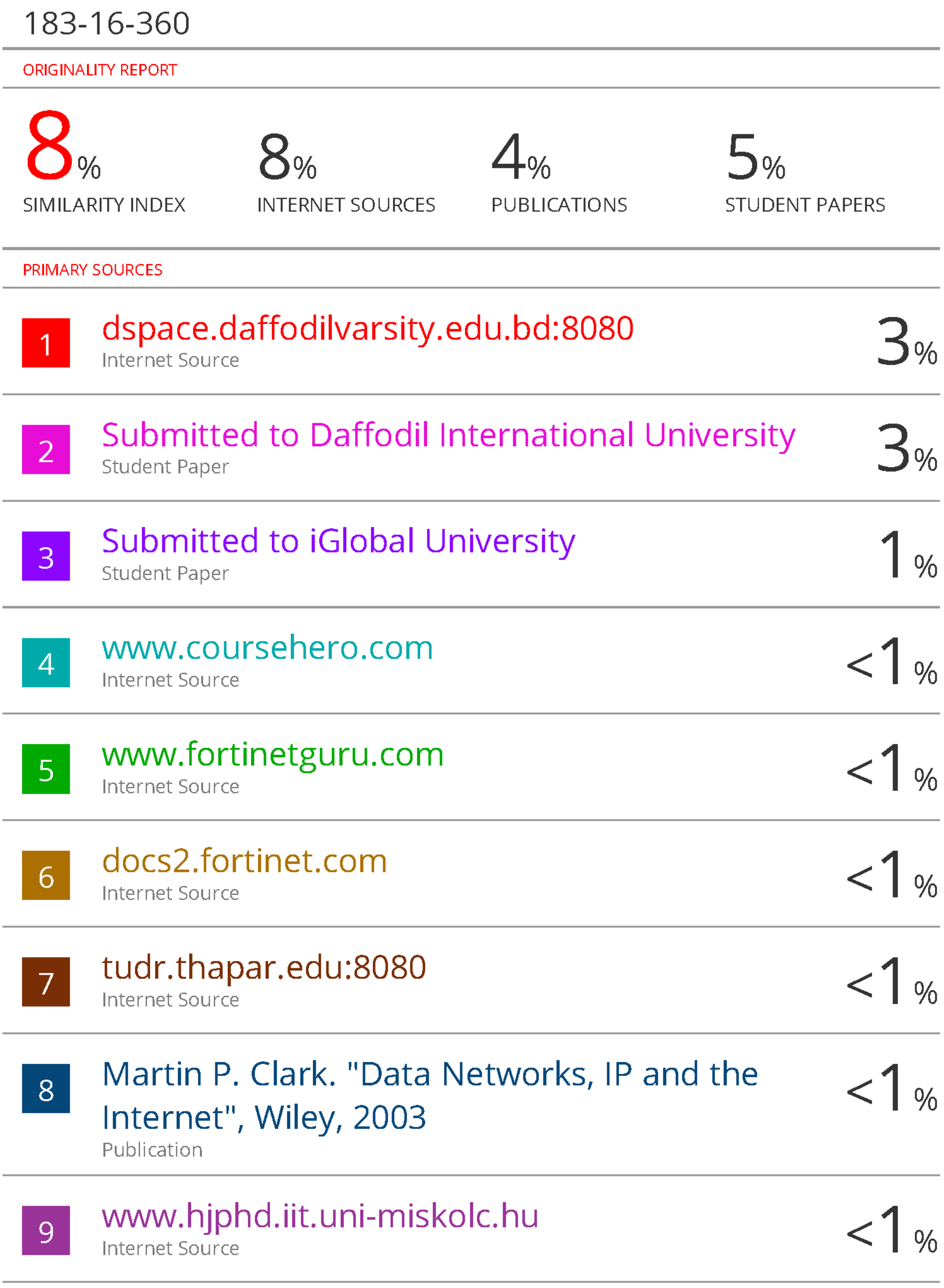
Firewall working methods/rules

A separate set of rules is maintained by the firewall for each scenario. The majority of the traffic that came from the server itself was permitted to pass. Nevertheless, enforcing a restriction on outbound traffic is always preferable in order to increase security and stop undesired communication.

Different rules are applied to oncoming traffic. One of these three main Transport Layer protocols “TCP, UDP, or ICMP” makes up the majority of traffic that enters the firewall. These types are all addressed at both their source and destination. TCP and UDP both have port numbers. To identify the purpose of a packet, ICMP utilizes a type code rather than a port number.

Default policy: It is quite challenging to explicitly cover every firewall rule that could possibly exist. This necessitates that the firewall always has a default policy. Action is the only component of default policy (accept, reject or drop).

Let's say the firewall has no rules about SSH connections to the server. It will therefore adhere to the default policy. Any computer outside of your office can connect to the server using SSH if the firewall's default policy is configured to accept. Therefore, it is always a good practice to set the default policy to drop (or reject).



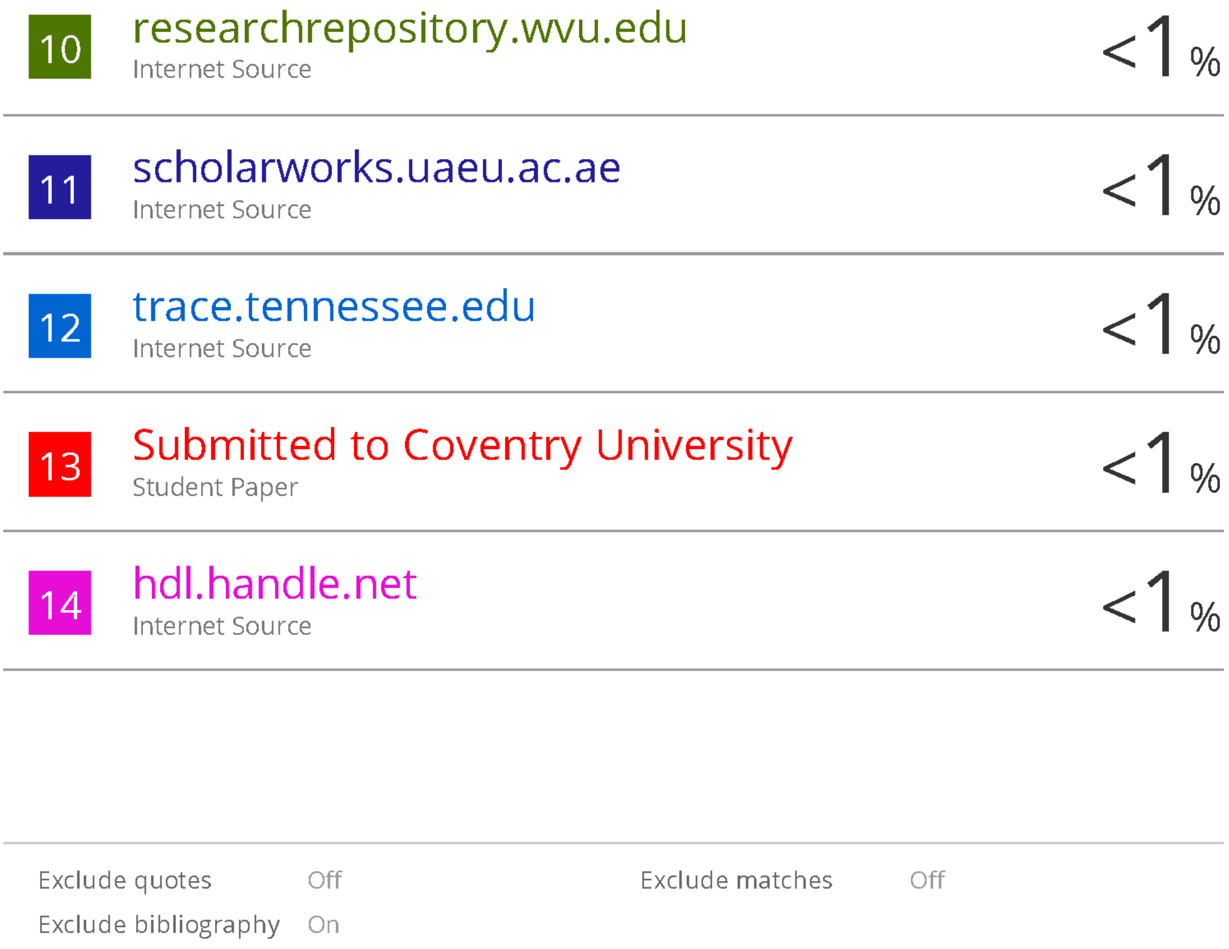
183-16-360

ORIGINALITY REPORT

8%	8%	4%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	3%
2	Submitted to Daffodil International University Student Paper	3%
3	Submitted to iGlobal University Student Paper	1%
4	www.coursehero.com Internet Source	<1%
5	www.fortinetguru.com Internet Source	<1%
6	docs2.fortinet.com Internet Source	<1%
7	tudr.thapar.edu:8080 Internet Source	<1%
8	Martin P. Clark. "Data Networks, IP and the Internet", Wiley, 2003 Publication	<1%
9	www.hjphd.iit.uni-miskolc.hu Internet Source	<1%



10	researchrepository.wvu.edu Internet Source	<1%
11	scholarworks.uaeu.ac.ae Internet Source	<1%
12	trace.tennessee.edu Internet Source	<1%
13	Submitted to Coventry University Student Paper	<1%
14	hdl.handle.net Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		