

FortiGate Firewall

FortiGate Firewall

Practical Guidance and Hands-On Labs

Hamid Talebi

BCCAMPUS
VICTORIA, B.C.



FortiGate Firewall by Hamid Talebi is licensed under a Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>), except where otherwise noted.

© 2023 Hamid Talebi

The CC licence permits you to retain, reuse, copy, redistribute, and revise this book—in whole or in part—for free providing the author is attributed as follows:

FortiGate Firewall: Practical Guidance and Hands-On Labs by Hamid Talebi is licensed under a CC BY 4.0 licence (<http://creativecommons.org/licenses/by/4.0/>).

If you redistribute all or part of this book, it is recommended the following statement be added to the copyright page so readers can access the original book at no cost:

Download for free from the B.C. Open Collection (<https://collection.bccampus.ca/>).

Sample APA-style citation (7th Edition):

Talebi, H. (2023). *FortiGate firewall: Practical guidance and hands-on labs*. BCcampus. <https://opentextbc.ca/fortigatefirewall/>

Cover image attribution:

“Firewall” (https://www.flaticon.com/free-icon/firewall_886917) by Chanut-is-Industries (<https://www.flaticon.com/authors/chanut-is-industries>) is licensed under a Flaticon licence (<https://www.freepikcompany.com/legal#nav-flaticon-agreement>).

Ebook ISBN: 978-1-77420-225-8

Print ISBN: 978-1-77420-224-1

Visit BCcampus Open Education (<http://open.bccampus.ca/>) to learn about open education in British Columbia.

This book was produced with Pressbooks (<https://pressbooks.com>) and rendered with Prince.

Contents

Accessibility Statement	vii
For Students: How to Access and Use this Textbook	xi
About BCcampus Open Education	xiii
Preface	1
Dedication	3
Chapter 1. Basic Settings	
1.1 Basic Settings	7
Chapter 2. Policy	
2.1 Security Policy	23
2.2 Application Profile	35
Chapter 3. NAT	
3.1 Source NAT	51
3.2 Destination NAT	57
Chapter 4. VPN	
4.1 IPsec VPN	65
4.2 SSL VPN	85
Chapter 5. Authentication	
5.1 Captive Portal	103
5.2 FSSO	111
Chapter 6. High Availability	
6.1 High Availability	121

Chapter 7. Security	
7.1 DDoS Prevention	131
7.2 Security Profile	137
7.3 VLAN and Security Profile	147
Chapter 8. VDOM	
8.1 VDOM	157
8.2 Inter-VDOM Routing	169
Chapter 9. SD-WAN	
9.1 SD-WAN	181
Chapter 10. Cloud Technologies	
10.1 IPsec VPN from FortiGate (on Premise) to Azure	199
10.2 Deploy FortiGate in Azure	219
10.3 Site to Site VPN between FortiGate on Premise and FortiGate in the Azure	225
10.4 IPsec VPN from FortiGate (on Premise) to AWS	229
10.5 Deploy FortiGate in AWS	253
10.6 Site-to-Site VPN between FortiGate on Premise and FortiGate in the AWS	275
Appendix: GNS3 Basics	283
Acknowledgements	317
About the Author	319
Versioning History	321

Accessibility Statement

BCcampus Open Education believes that education must be available to everyone. This means supporting the creation of free, open, and accessible educational resources. We are actively committed to increasing the accessibility and usability of the resources we produce.

Accessibility of this Textbook

The web version of this resource (<https://opentextbc.ca/fortigatefirewall/>) has been designed to meet Web Content Accessibility Guidelines 2.0 (<https://www.w3.org/TR/WCAG20/>), level AA. In addition, it follows all guidelines in Appendix A: Checklist for Accessibility (<https://opentextbc.ca/accessibilitytoolkit/back-matter/appendix-checklist-for-accessibility-toolkit/>) of the *Accessibility Toolkit – 2nd Edition* (<https://opentextbc.ca/accessibilitytoolkit/>). It includes:

- **Easy navigation.** This resource has a linked table of contents and uses headings in each chapter to make navigation easy.
- **Accessible images.** All images in this resource that convey information have alternative text. Images that are decorative have empty alternative text.
- **Accessible links.** All links use descriptive link text.

Accessibility Checklist

Element	Requirements	Pass?
Headings	Content is organized under headings and subheadings that are used sequentially.	Yes
Images	Images that convey information include alternative text descriptions. These descriptions are provided in the alt text field, in the surrounding text, or linked to as a long description.	Yes
Images	Images and text do not rely on colour to convey information.	Yes
Images	Images that are purely decorative or are already described in the surrounding text contain empty alternative text descriptions. (Descriptive text is unnecessary if the image doesn't convey contextual content information.)	Yes
Tables	Tables include row and/or column headers that have the correct scope assigned.	Yes
Tables	Tables include a title or caption.	Yes
Tables	Tables do not have merged or split cells.	Yes
Tables	Tables have adequate cell padding.	Yes
Links	The link text describes the destination of the link.	Yes
Links	Links do not open new windows or tabs. If they do, a textual reference is included in the link text.	Yes
Links	Links to files include the file type in the link text.	Yes
Font	Font size is 12 point or higher for body text.	Yes
Font	Font size is 9 point for footnotes or endnotes.	Yes
Font	Font size can be zoomed to 200% in the webbook or eBook formats.	Yes

Known Accessibility Issues and Areas for Improvement

- The book relies heavily on screenshots from FortiGate Firewall. These screenshots do not have alt text. While many of the screenshots are described in the surrounding text, the book has not been reviewed to ensure that the surrounding text is an adequate alternative for all images in the book.

Let Us Know if You are Having Problems Accessing This Book

We are always looking for ways to make our resources more accessible. If you have problems accessing this textbook, please contact us to let us know so we can fix the issue.

Please include the following information:

- The name of the textbook

- The location of the problem by providing a web address or page description.
- A description of the problem
- The computer, software, browser, and any assistive technology you are using that can help us diagnose and solve your issue (e.g., Windows 10, Google Chrome (Version 65.0.3325.181), NVDA screen reader)

You can contact us one of the following ways:

- Web form: BCcampus IT Support (<https://open.bccampus.ca/contact-us/>)
- Web form: Report an Error (<https://collection.bccampus.ca/report-error/>)

This statement was last updated on August 31, 2023.

The Accessibility Checklist table was adapted from one originally created by the Rebus Community (<https://press.rebus.community/the-rebus-guide-to-publishing-open-textbooks/back-matter/accessibility-assessment/>) and shared under a CC BY 4.0 License (<https://creativecommons.org/licenses/by/4.0/>).

For Students: How to Access and Use this Textbook

This textbook is available in the following formats:

- **Online webbook.** You can read this textbook online on a computer or mobile device in one of the following browsers: Chrome, Firefox, Edge, and Safari.
- **PDF.** You can download this book as a PDF to read on a computer (Digital PDF) or print it out (Print PDF).
- **Mobile.** If you want to read this textbook on your phone or tablet, you can use the EPUB (eReader) file.
- **HTML.** An HTML file can be opened in a browser. It has very little style so it doesn't look very nice, but some people might find it useful.

For more information about the accessibility of this textbook, see the Accessibility Statement.

You can access the online webbook and download any of the formats for free here: *FortiGate Firewall: Practical Guidance and Hands-On Labs* (<https://opentextbc.ca/fortigatefirewall>). To download the book in a different format, look for the “Download this book” drop-down menu and select the file type you want.

How can I use the different formats?

Format	Internet required?	Device	Required apps	Accessibility Features	Screen reader compatible
Online webbook	Yes	Computer, tablet, phone	An Internet browser (Chrome, Firefox, Edge, or Safari)	WCAG 2.0 AA compliant, option to enlarge text, and compatible with browser text-to-speech tools	Yes
PDF	No	Computer, print copy	Adobe Reader (for reading on a computer) or a printer	Ability to highlight and annotate the text. If reading on the computer, you can zoom in.	Unsure
EPUB	No	Computer, tablet, phone	An eReader app	Option to enlarge text, change font style, size, and colour.	Unsure
HTML	No	Computer, tablet, phone	An Internet browser (Chrome, Firefox, Edge, or Safari)	WCAG 2.0 AA compliant and compatible with browser text-to-speech tools.	Yes

Tips for Using This Textbook

- **Search the textbook.**
 - If using the online webbook, you can use the search bar in the top right corner to search the entire book for a key word or phrase. To search a specific chapter, open that chapter and use your browser’s search feature by hitting **[Cntr] + [f]** on your keyboard if using a Windows computer or **[Command] + [f]** if using a Mac computer.
 - The **[Cntr] + [f]** and **[Command] + [f]** keys will also allow you to search a PDF, HTML, and EPUB files if you are reading them on a computer.
 - If using an eBook app to read this textbook, the app should have a built-in search tool.
- **Navigate the textbook.**
 - This textbook has a table of contents to help you navigate through the book easier. If using the online webbook, you can find the full table of contents on the book’s homepage or by selecting “Contents” from the top menu when you are in a chapter.
- **Annotate the textbook.**
 - If you like to highlight or write on your textbooks, you can do that by getting a print copy, using the Digital PDF in Adobe Reader, or using the highlighting tools in eReader apps.

About BCcampus Open Education

FortiGate Firewall: Practical Guidance and Hands-On Labs by Hamid Talebi was funded by BCcampus Open Education.

BCcampus Open Education (<https://open.bccampus.ca/>) began in 2012 as the B.C. Open Textbook Project with the goal of making post-secondary education in British Columbia more accessible by reducing students' costs through the use of open textbooks and other OER. BCcampus (<https://bccampus.ca/about-us/>) supports the post-secondary institutions of British Columbia as they adapt and evolve their teaching and learning practices to enable powerful learning opportunities for the students of B.C. BCcampus Open Education is funded by the British Columbia Ministry of Post-Secondary Education and Future Skills (<https://www2.gov.bc.ca/gov/content/governments/organizational-structure/ministries-organizations/ministries/post-secondary-education-and-future-skills>) and the Hewlett Foundation (<http://www.hewlett.org/>).

Open educational resources (OER) are teaching, learning, and research resources that, through permissions granted by the copyright holder, allow others to use, distribute, keep, or make changes to them. Our open textbooks are openly licensed using a Creative Commons licence (<https://creativecommons.org/licenses/>) and are offered in various eBook formats free of charge, or as printed books that are available at cost.

For more information about open education in British Columbia, please visit the BCcampus Open Education (<https://open.bccampus.ca/>) website. If you are an instructor who is using this book for a course, please fill out our Adoption of an Open Textbook (<https://open.bccampus.ca/use-open-textbooks/tell-us-youre-using-an-open-textbook/>) form.

This book was produced using the following styles: FortiGate Firewall: Practical Guidance and Hands-On Labs Style Sheet (<https://opentextbc.ca/fortigatefirewall/wp-content/uploads/sites/438/2022/05/FortiGate-Firewall-Style-Sheet.docx>)

Preface

Firewall technologies are growing very fast and knowing how to protect the network is vital for network administrators. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been the first line of defense in network security for over 25 years.¹ The lack of materials available for students to learn is part of our issue.

Since I have been teaching Enterprise Security at BCIT, I have received a lot of feedback from my students. Then, I have decided to collect all labs and make them as a book for students. This book is part of the Enterprise Security Course and is based on the practical labs in the class. Each chapter begins with a learning objective and step-by-step explanations in GNS3 to beginners on how to build different security scenarios from scratch.

The book is divided into ten chapters as following:

- **Chapter 1. Basic Settings** of FortiGate firewall and how to work with CLI or GUI to configure the firewall.
- **Chapter 2. Policy:** We will focus on firewall policy and how firewall pass the traffic from one port to another port.
- **Chapter 3. NAT:** We will use Source NAT and Destination NAT. You will learn how to use port forwarding when you are using DNAT.
- **Chapter 4. VPN:** This is very important chapter focus on SSL VPN and IPsec VPN. You will learn how to set site-to-site VPN.
- **Chapter 5. Authentication:** This chapter will focus on Captive Portal and FSSO. You will learn how to install FSSO Agent in the server and monitor Active Directory.
- **Chapter 6. High Availability:** This chapter will focus on High Availability (Active-Passive) in FortiGate firewalls.
- **Chapter 7. Security:** This chapter will focus on security profile, DDoS prevention and VLANs configuration.
- **Chapter 8. VDOM** or Virtual Domain is a feature in FortiGate firewalls to manage resources and access. You will learn how to enable VDOM and how to use it.
- **Chapter 9. SD-WAN:** This chapter will focus on SD-WAN and how to use this feature.
- **Chapter 10. Cloud Technologies:** This chapter will focus on how to deploy FortiGate in the cloud.
- **Appendix:** We will cover basic GNS3 settings you need during this book.

As we know “a picture is worth 1000 words” and that is why this book is based on snapshots and

1. What is a Firewall? (https://www.cisco.com/c/en_ca/products/security/firewalls/what-is-a-firewall.html)

2 Hamid Talebi

screen-capture all the steps and configurations. This will be useful for fast-tracking. This book will be a practical resource/guide that can be used by BCIT students, and students at other institutions as well as IT professionals.

Hamid Talebi

Dedication

This book is dedicated to those looking to further their knowledge of next-generation firewalls.

Chapter 1. Basic Settings

1.1 Basic Settings

Learning Objectives

- Create a basic configuration in FortiGate
- Identify CLI commands in FortiGate
- Create an IP access in FortiGate
- Create a DHCP server in FortiGate
- Restore previous configurations in FortiGate using backups

Scenario: This exercise will access a FortiGate device using the command-line interface (CLI). Setup your GNS3 and try to connect to FortiGate through WebTerm.

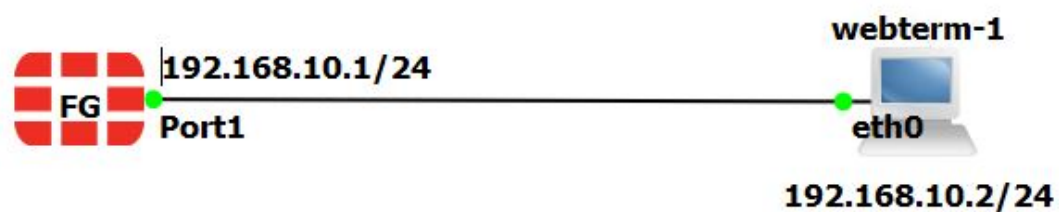


Figure 1.1: Main scenario

Explore the CLI

To explore the CLI, from the GNS3 double click on FortiGate to open the console. In the Password field, type **<the default password is blank>**, and then press enter.

Enter the following command:

```
get system status
```

```
FortiGate-VM64-KVM # get system status
Version: FortiGate-VM64-KVM v7.0.1,build0157,210714 (GA)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
Serial-Number: FGVMEVYCVRJ7IIE1
License Status: Valid
Evaluation License Expires: Wed Mar 23 20:32:13 2022
VM Resources: 1 CPU/1 allowed, 997 MB RAM/2048 MB allowed
Log hard disk: Available
Hostname: FortiGate-VM64-KVM
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 1
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0157
Release Version Information: GA
FortiOS x86-64: Yes
System time: Tue Mar 8 20:35:58 2022
Last reboot reason: warm reboot
```

Figure 1.2: Get system status output

This command displays basic status information about FortiGate. The output includes FortiGate's serial number, operation mode, and a lot of useful information. When the More prompt appears on the CLI, do one of the following:

- To continue scrolling, Space bar.

- To scroll one line at a time, Enter.
- Enter the following command: get ?

The ? character is not displayed on the screen.

This command shows all of the options that the CLI will accept after the # get command. Depending on the command, you may need to enter additional words to completely specify a configuration option.

- Enter the following command: **execute ?**
- This command lists all options that the CLI will accept after the execute command.
- Type exe, and then press the Tab key. Notice that the CLI completes the current word.
- Press the space bar and then press the Tab key three times.
- Each time you press the Tab key, the CLI replaces the second word with the next possible option for the execute command, in alphabetical order.

You can abbreviate most commands. In this book, many of the commands that you see will be in abbreviated form. For example, instead of typing execute, you can type exe.

Use this technique to reduce the number of keystrokes that are required to enter a command. Often, experts can configure FortiGate faster using the CLI than the GUI.

Configuration

Table 1.1: Check configuration CLI

Action	Command
Check configuration	<pre># show # show grep xxxx # show full-configuration # show full-configuration grep XXXX # show full-configuration grep -f XXXX ← display with tree view</pre>

Network**Table 1.2: Routing and firewall policy CLI**

Action	Command
Check Routing	# get router info routing-table detail # show router static# config router static (static) # show (static) # end
Check Firewall Policy	# show firewall policy # show firewall policy XXXX# config firewall policy (policy) # show

Hardware**Table 1.3: Hardware CLI**

Action	Command
Check Hardware Information	# get hardware status
Check Version, BIOS, Firmware, etc.	# get system status
Check version	# get system status
Display CPU / memory / line usage	# get system performance status
Display of NTP server	# get system ntp
Display the current time and the time of synchronization with the NTP server	# execute time
Check interfaces status, Up or Down	# get system interface physical
Check interfaces	# config system interface (interface) # show (interface) # end
Display of ARP table	# get system arp

High Availability (HA)**Table 1.4: High Availability CLI**

Action	Command
Check HA Status	# get system ha status
Check HA Configuration	# get system ha # show system ha

Network Time Protocol (NTP)

Table 1.5: NTP CLI

Action	Command
Check NTP	# execute time # get system ntp # diagnose sys ntp status

On a fresh line, enter the following command to view the port3 interface configuration:

```
show system interface port3
```

```
FGVM01TM19008000 # show system interface port3
config system interface
  edit "port3"
    set vdom "root"
    set type physical
    set snmp-index 3
  next
end
```

Figure 1.3: Configuration of port3

Enter the following command:

```
show full-configuration system interface port3
```

```
FGVM01TM19008000 # show full-configuration system interface port3
config system interface
  edit "port3"
    set vdom "root"
    set vrf 0
    set fortilink disable
    set mode static
    set dhcp-relay-interface-select-method auto
    set dhcp-relay-service disable
    set ip 0.0.0.0 0.0.0.0
    unset allowaccess
    set fail-detect disable
    set pptp-client disable
    set arpforward enable
    set broadcast-forward disable
    set bfd global
    set l2forward disable
    set icmp-send-redirect enable
    set icmp-accept-redirect enable
    set vlanforward disable
    set stpforward disable
    set ips-sniffer-mode disable
    set ident-accept disable
    set ipmac disable
    set subst disable
```

Figure 1.4: Show full-configuration of port3

Enter the following command:

```
show system interface
```

For setting an IP address on the port1:

```
config system interface
edit port1
set mode static
set ip 192.168.10.1 255.255.255.0
set allowaccess ping ssh http https
end
```

Now you should be able to reach the firewall from port1. In browser, type `http://192.168.10.1` and enter username and password.

In the licensed devices, you should type `https://192.168.10.1` and then enter username and password.

Configuring Administrator Accounts

FortiGate offers many options for configuring administrator privileges. For example, you can specify the IP addresses that administrators are allowed to connect from. In this exercise, you will work with administrator profiles and administrator user accounts. An administrator profile is a role that is assigned to an administrator user that defines what the user is permitted to do on the FortiGate GUI and CLI.

Configure a User Administrator Profile

1. Click **System > Admin Profiles**.
2. Click **Create New**.
3. In the Name field, type **Security_Admin_Profile**.
4. In the permissions table, set Security Profile to **Read-Write**, but set all other permissions to Read.
5. Click **OK** to save the changes.

Name

Comments 0/255

Access Permissions

Access Control	Permissions	Set All
Security Fabric	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
FortiView	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
User & Device	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
Firewall	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Log & Report	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Network	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
System	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Security Profile	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
VPN	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
WAN Opt & Cache	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
WiFi & Switch	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	

Permit usage of CLI diagnostic commands

Override Idle Timeout

Figure 1.5: Create a custom profile

Create an Administrator Account

Now, you will create a new administrator account. You will assign the account to the administrator profile you created previously. The administrator will have read-only access to most of the configuration settings. To create an administrator account Continuing on the Local-FortiGate GUI, click **System > Administrators**. Click Create New and then click Administrator to add a new administrator account and assign the previous profile you have created to the administrator.

Figure 1.6: Create a local user

Test the New Administrator Account

In this procedure, you will confirm that the new administrator account has read-write access to only the security profiles configuration.

To test the new administrator account Continuing on the Local-FortiGate GUI, click username (in my case, it's admin2) and then Logout to log out of the admin account's GUI session.

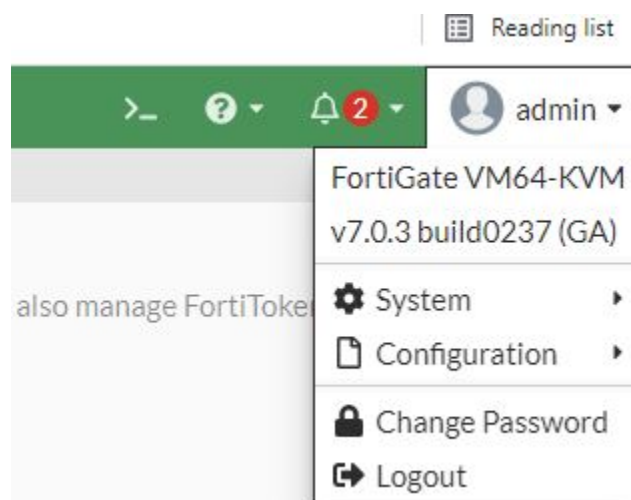


Figure 1.7: Logout option

Explore the permissions that you have in the GUI. You should see that this account can configure only security profiles. Log out of the GUI once done.

Restrict Administrator Access

Now, you will restrict access for FortiGate administrators. Only administrators connecting from a trusted subnet will be allowed access. This is useful if you need to restrict the access points from which administrators connect to FortiGate. To restrict administrator access.

1. Click **System > Administrators**. Edit the admin account.
2. Enable Restrict login to trusted hosts, and set **Trusted Host 1** to the address **192.168.10.100/32**.
3. Click **OK** to save the changes.

The screenshot shows the 'Edit Administrator' configuration page in the FortiGate GUI. The 'Username' field is set to 'admin2'. The 'Type' dropdown menu is open, showing options: 'Local User' (selected), 'Match a user on a remote server group', 'Match all users in a remote server group', and 'Use public key infrastructure (PKI) group'. The 'Comments' field contains 'Write a comment...' and the 'Administrator profile' is set to 'Security_Admin_Profile'. Below the main form, there are three toggle switches: 'Two-factor Authentication' is disabled, 'Restrict login to trusted hosts' is enabled, and 'Restrict admin to guest account provisioning only' is disabled. Under the 'Restrict login to trusted hosts' toggle, the 'Trusted Host 1' field is populated with '192.168.10.100/32' and a plus icon button is visible below it.

Figure 1.8: Create a trusted host for the user

To test the restricted access

1. Continuing on Local-Windows, log out of the Local-FortiGate GUI session as the admin user.
2. Try to log in to the admin2 account again with password < Your password>. Because you are trying to connect from the 192.168.10.101 address, you shouldn't be able to connect.
3. Log in as admin with password <Your password>. Enter the following CLI commands to add

192.168.10.101/32 as the second trusted IP subnet (Trusted Host 2) to the admin account:

```
config system admin
edit admin
set trusthost2 192.168.10.101/32
end
```

4. Try to log in to the Local-FortiGate GUI at <IP address> with the username admin and password <Your password>. You should be able to log in. (**Hint:** add the IP address 192.168.10.101 to WebTerm and try to reach to the firewall.)

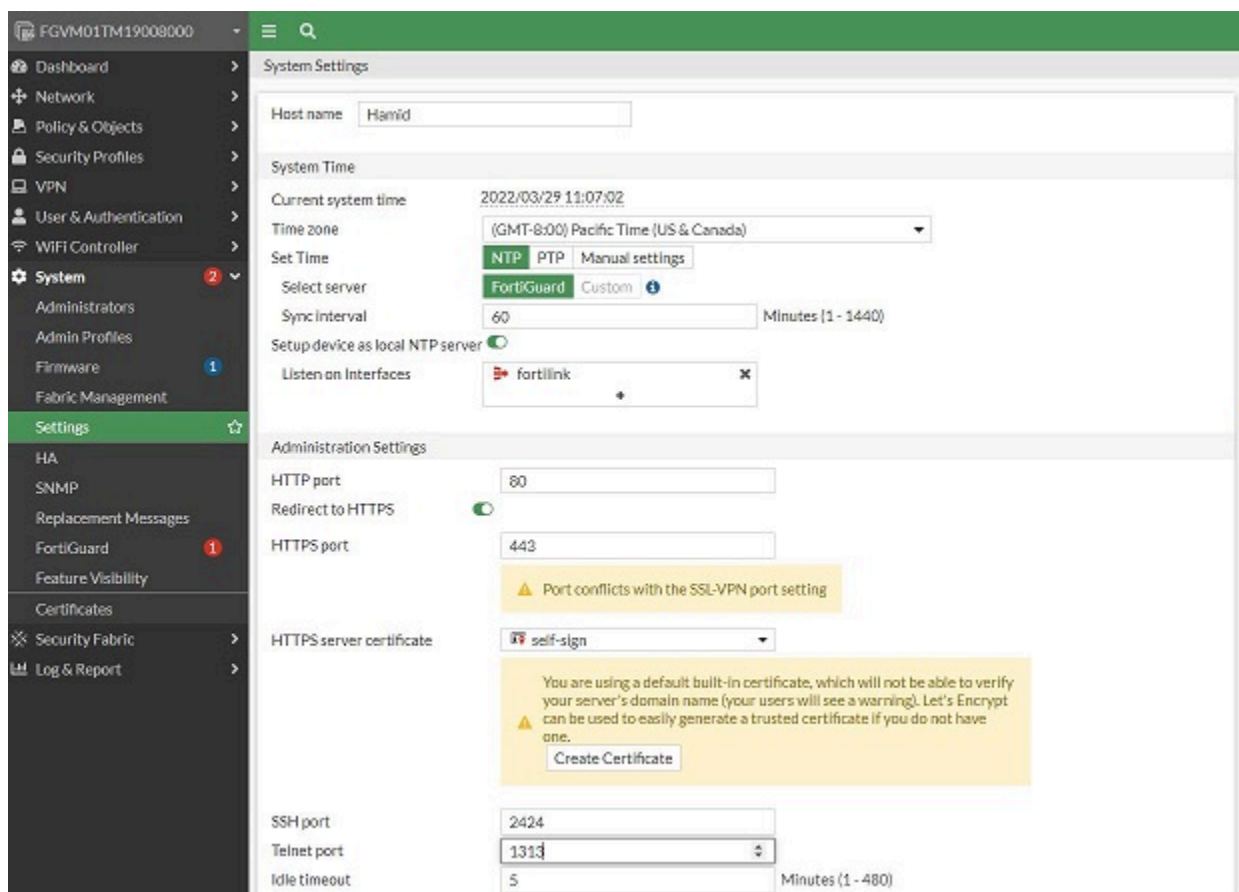


Figure 1.9: System settings

Configuration Backups

The configuration files produced by backups allow you to restore to an earlier FortiGate configuration.

Backup & Restore

Always back up the configuration file before making changes to FortiGate (even if the change seems

minor or unimportant). There is no undo. You should carefully consider the pros and cons of an encrypted backup before you begin encrypting backups. While your configuration, including things like private keys, remains private, an encrypted file hampers troubleshooting because Fortinet support cannot read the file. Consider saving backups in plain-text and storing them in a secure place instead. Now, you will create an encrypted file with the backup of the FortiGate's current configuration.

To save an encrypted configuration backup

Continuing on the Local-FortiGate GUI, in the upper-right corner, click **admin**, and then click **Configuration > Backup**. On the Backup System Configuration page, enable Encryption. In the Password field, enter **fortigate** and repeat in the Confirm password field.

Figure 1.10: Backup System Configuration

Click **OK**.

Select **Save File** and click **OK**.

To restore an encrypted configuration backup

Continuing on the Local-FortiGate GUI, in the upper-right corner, click **admin**, and then click **Configuration > Restore**. On the Restore System Configuration page, click **Upload**. Browse to your **Downloads** folder and select the configuration file that you created in the previous procedure. In the Password field, type **fortigate**, and then click **OK**.


DHCP (Dynamic Host Configuration Protocol)

You can configure one or more DHCP servers on any FortiGate interface. A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP.


Configure DHCP on the FortiGate


To add a DHCP server on the GUI:


1. Go to **Network > Interfaces**.
2. Edit an interface.
3. Enable the DHCP Server option and configure the settings.

Name  port3

Alias

Type  Physical Interface

VRF ID 

Role 


Address

Addressing mode Manual DHCP Auto-managed by IPAM One-Arm Sniffer


IP/Netmask

Secondary IP address


Administrative Access


IPv4 HTTPS HTTP  PING

FMG-Access SSH SNMP

FTM RADIUS Accounting Security Fabric Connection 

Speed Test

Receive LLDP  Use VDOM Setting Enable Disable

Transmit LLDP  Use VDOM Setting Enable Disable

DHCP Server

DHCP status Enabled Disabled

Address range

Netmask

Default gateway Same as Interface IP Specify

DNS server Same as System DNS Same as Interface IP Specify


Lease time  second(s)

Figure 1.11: Enable DHCP Server

To do it through command line, use following commands:

```
FGVM01TM19008000 # config system dhcp server
FGVM01TM19008000 (server) # edit 1
FGVM01TM19008000 (1) # set dns-service default
FGVM01TM19008000 (1) # set netmask 255.255.255.0
FGVM01TM19008000 (1) # config ip-range
FGVM01TM19008000 (ip-range) # edit 1
FGVM01TM19008000 (1) # set start-ip 192.168.1.1
FGVM01TM19008000 (1) # set end-ip 192.168.1.1
FGVM01TM19008000 (1) # next
FGVM01TM19008000 (ip-range) # edit 2
new entry '2' added
FGVM01TM19008000 (2) # set start-ip 192.168.1.20
FGVM01TM19008000 (2) # set end-ip 192.168.1.30
FGVM01TM19008000 (2) # next
FGVM01TM19008000 (ip-range) # end
FGVM01TM19008000 (1) # next
FGVM01TM19008000 (server) # end
```

If you are looking for a specific configuration or CLI, the FortiGate document library (<https://docs.fortinet.com/product/fortigate>) has full resources.

Resources

- Fortinet Fortigate CLI Commands (<https://cmdref.net/hardware/fortigate/index.html>)
- FortiGate document library (<https://docs.fortinet.com/product/fortigate/7.2>)

Chapter 2. Policy

2.1 Security Policy

Learning Objectives

- Create a Security Policy in FortiGate
- Reorder Firewall Policies and Firewall Policy Actions

Scenario: We are going to allow traffic from the local network to the Internet. We will set Security Policy that allows the traffic from Port 2 to Port 3. Then, WebTerm1 will be able to reach the Internet.

Security Policy

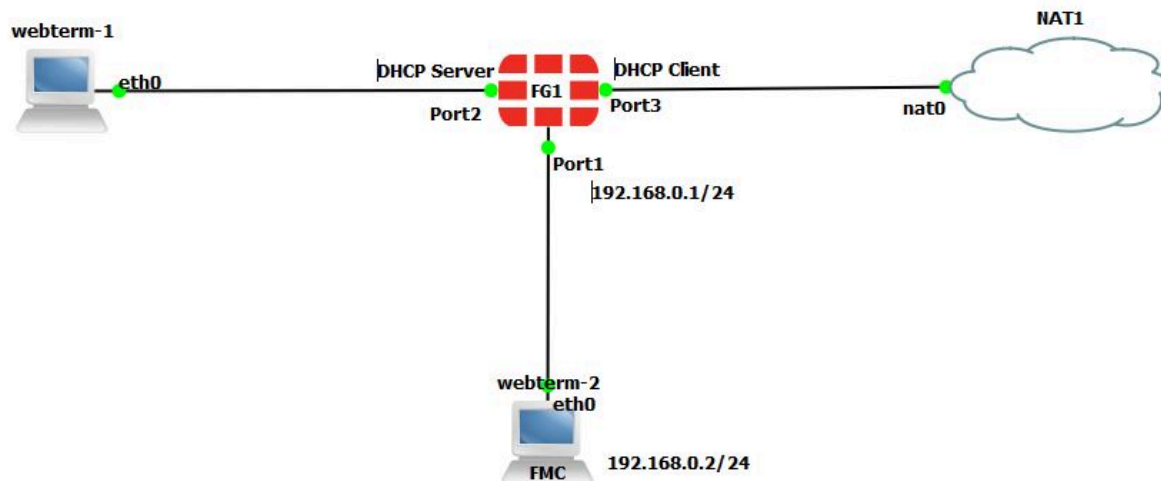


Figure 2.1: Main scenario

Table 2.1: Devices configuration

Device	Configuration
FortiGate	Port 2: DHCP Server Port 3: DHCP Client
WebTerm	DHCP Client

Configuration of port1 of the firewall in CLI is as follows:

```
FGVM01TM19008000 # config system interface
FGVM01TM19008000 (interface) # edit port1
FGVM01TM19008000 (port1) # set mode static
FGVM01TM19008000 (port1) # set ip 192.168.0.1/24
FGVM01TM19008000 (port1) # set allowaccess http https
FGVM01TM19008000 (port1) # end
```

Figure 2.2: Configuration of port1

1. Open the browser in WebTerm2 and type `https://192.168.0.1`. You should be able to access the firewall.

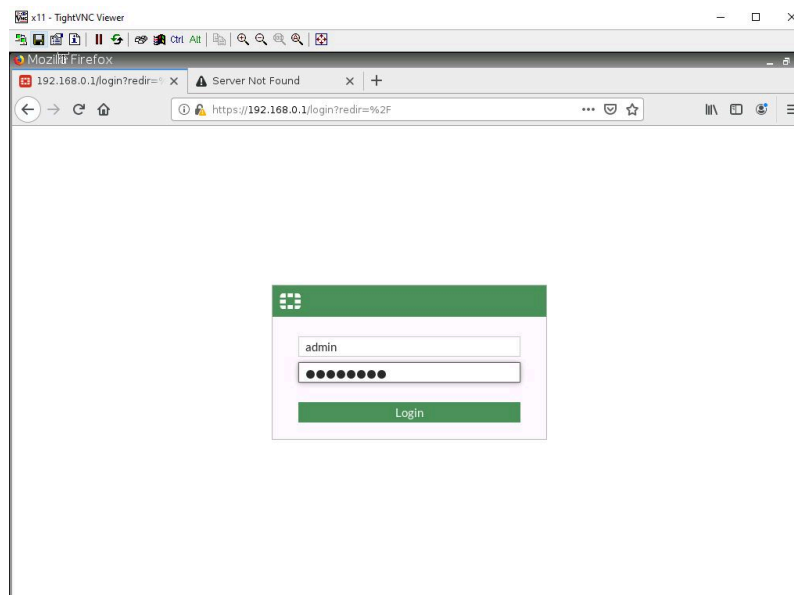


Figure 2.3: Log in to the FortiGate

2. Go to **Network > Interfaces > Port2**, set the interface IP address as **192.168.1.1/24** and configure DHCP server on interface port2 (Range of IP addresses should be: 192.168.1.20 to

192.168.1.30, DNS: 4.2.2.4) and **Enable Device Detection** under Port2.

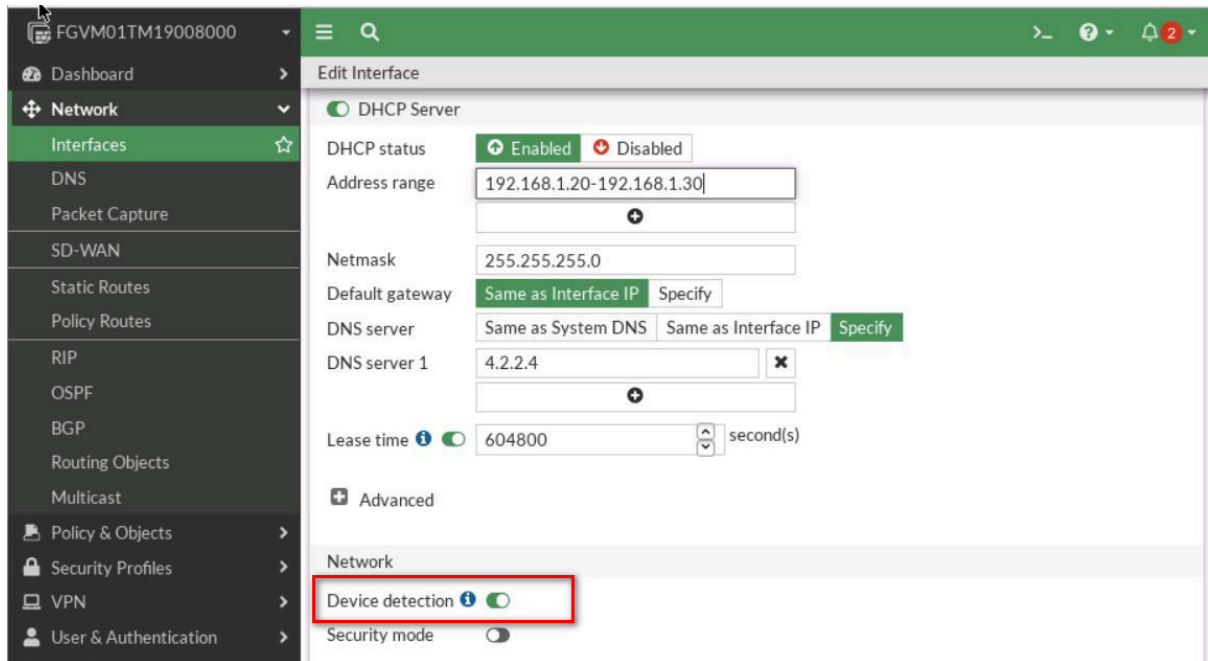


Figure 2.4: Enable DHCP Server

- Set a port3 as a DHCP client and enable **Device Detection** under Port3.



Figure 2.5: Enable DHCP Client

- Set a Static route in the firewall to reach the NAT object. Go to **Network > Static Route > Create a new**.

The image shows a 'New Static Route' configuration window. It includes the following fields and options:

- Automatic gateway retrieval:** A toggle switch that is currently turned off.
- Destination:** A dropdown menu set to 'Subnet' and 'Internet Service', with a text input field containing '0.0.0.0/0.0.0.0'.
- Gateway Address:** A dropdown menu set to 'Dynamic' and 'Specify', with a text input field containing '192.168.122.1'.
- Interface:** A dropdown menu showing 'port3' with a plus sign below it and an 'x' icon to the right.
- Administrative Distance:** A text input field containing '10'.
- Comments:** A text input field containing 'Write a comment...' and a character count '0/255'.
- Status:** Two radio buttons, 'Enabled' (selected) and 'Disabled'.
- Advanced Options:** A section with a plus sign icon and the text 'Advanced Options'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Figure 2.6: Configure a static route

5. Go to **Policy & Objects > Firewall Policy** section, click **Create New** to add a new firewall policy, and configure the following settings:
 - Name: **LocalToInternet**
 - From **inside** to **outside (port2 to port3)**
 - Source: **Create an address for local network (Subnet: 192.168.1.0/24)**
 - Destination: **all**
 - Schedule: **Always**
 - Service: Only **HTTP, HTTPS, DNS, Ping**
 - Action: **Accept**

Figure 2.7: Set local subnet

Figure 2.8: Set firewall policy

6. Go to **WebTerm1**, Set interface as DHCP and then open the browser, you should be able to access the internet.

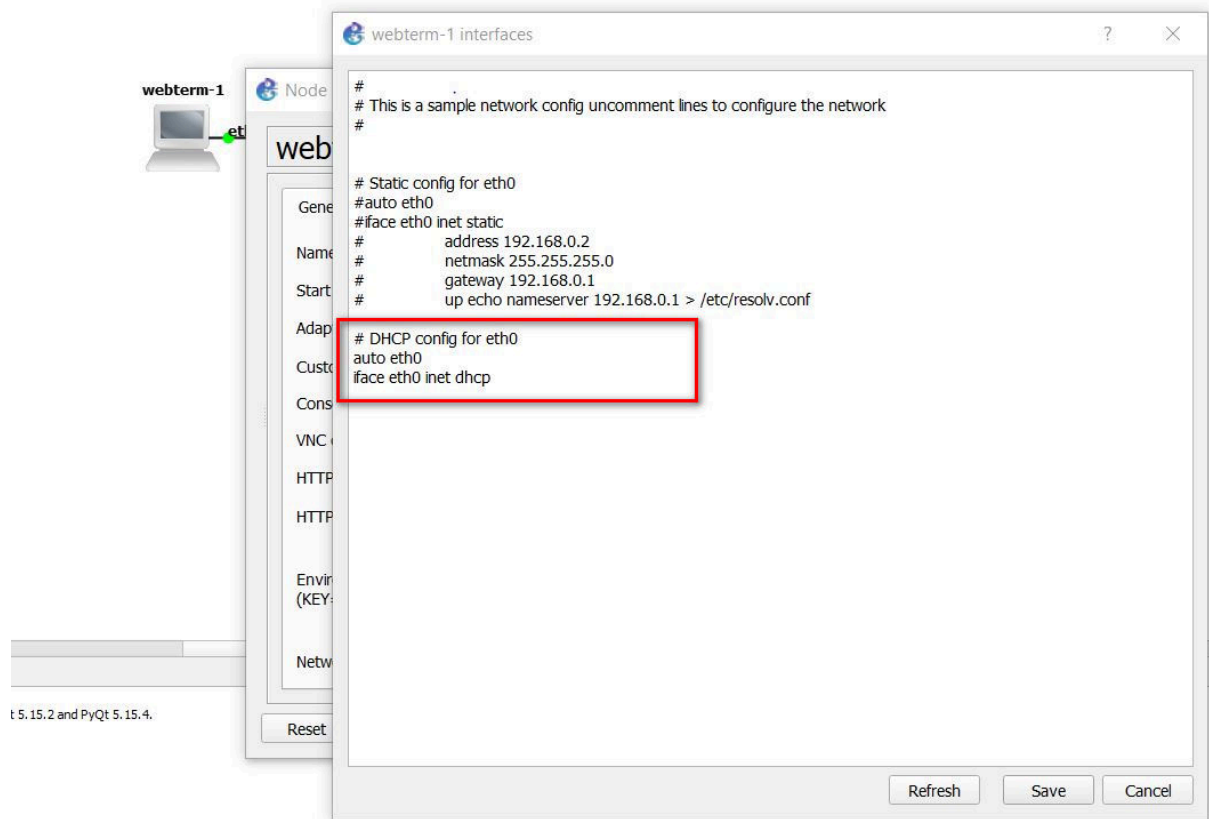


Figure 2.9: Enable DHCP Client on WebTerm1

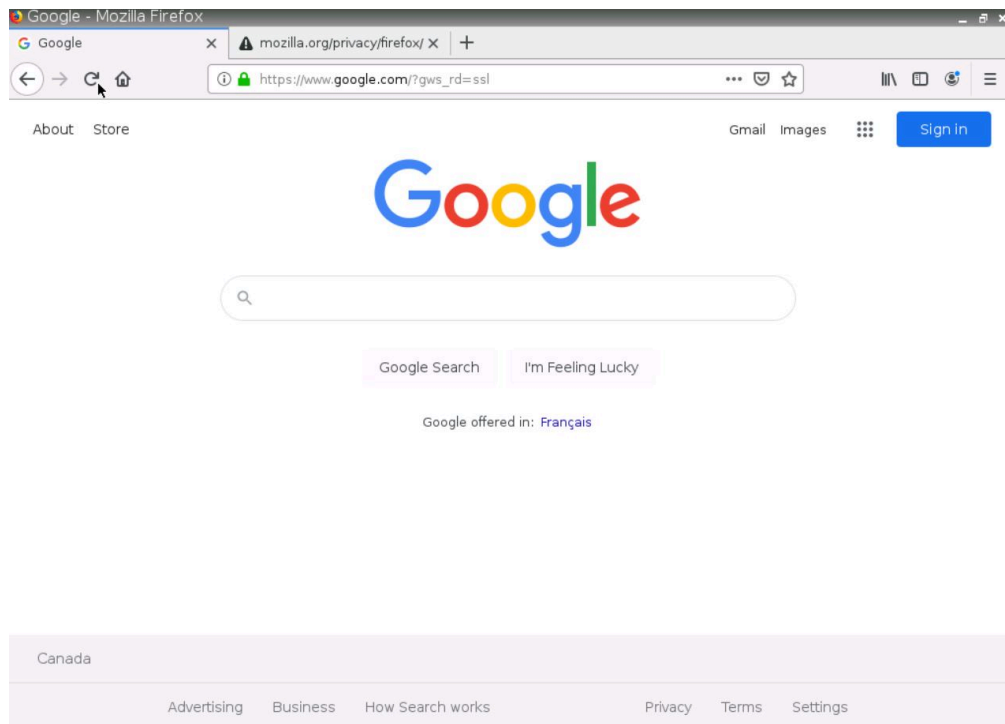


Figure 2.10: Verify your configuration by testing Google.com

Verify Your Configuration

- Go to **Dashboard > FortiView Sessions**. You should be able to see the traffic.

Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes
192.168.1.2		4.2.2.4	UDP/53	UDP	49284	53	266 B
192.168.1.2		4.2.2.4	UDP/53	UDP	50948	53	266 B
192.168.1.2		4.2.2.4	UDP/53	UDP	51594	53	171 B
192.168.1.2		4.2.2.4	UDP/53	UDP	52754	53	251 B
192.168.1.2		4.2.2.4	UDP/53	UDP	53934	53	251 B
192.168.1.2		4.2.2.4	UDP/53	UDP	52974	53	278 B
192.168.1.2		4.2.2.4	UDP/53	UDP	54356	53	162 B
192.168.1.2		4.2.2.4	UDP/53	UDP	57184	53	266 B
192.168.1.2		34.120.237.76	TCP/443	TCP	60838	443	135.04 kB
192.168.1.2		4.2.2.4	UDP/53	UDP	37632	53	266 B
192.168.1.2		4.2.2.4	UDP/53	UDP	40966	53	266 B
192.168.1.2		4.2.2.4	UDP/53	UDP	41720	53	162 B
192.168.1.2		4.2.2.4	UDP/53	UDP	43104	53	159 B
192.168.1.2		4.2.2.4	UDP/53	UDP	43286	53	266 B
192.168.1.2		4.2.2.4	UDP/53	UDP	44476	53	245 B
192.168.1.2		4.2.2.4	UDP/53	UDP	46612	53	169 B
192.168.1.2		34.120.5.221	TCP/443	TCP	48182	443	74.91 kB
192.168.1.2		4.2.2.4	UDP/53	UDP	47746	53	266 B

Figure 2.11: FortiView Sessions

- Go to Firewall Policy and on the right side of the screen, you should be able to see **Hit count**.

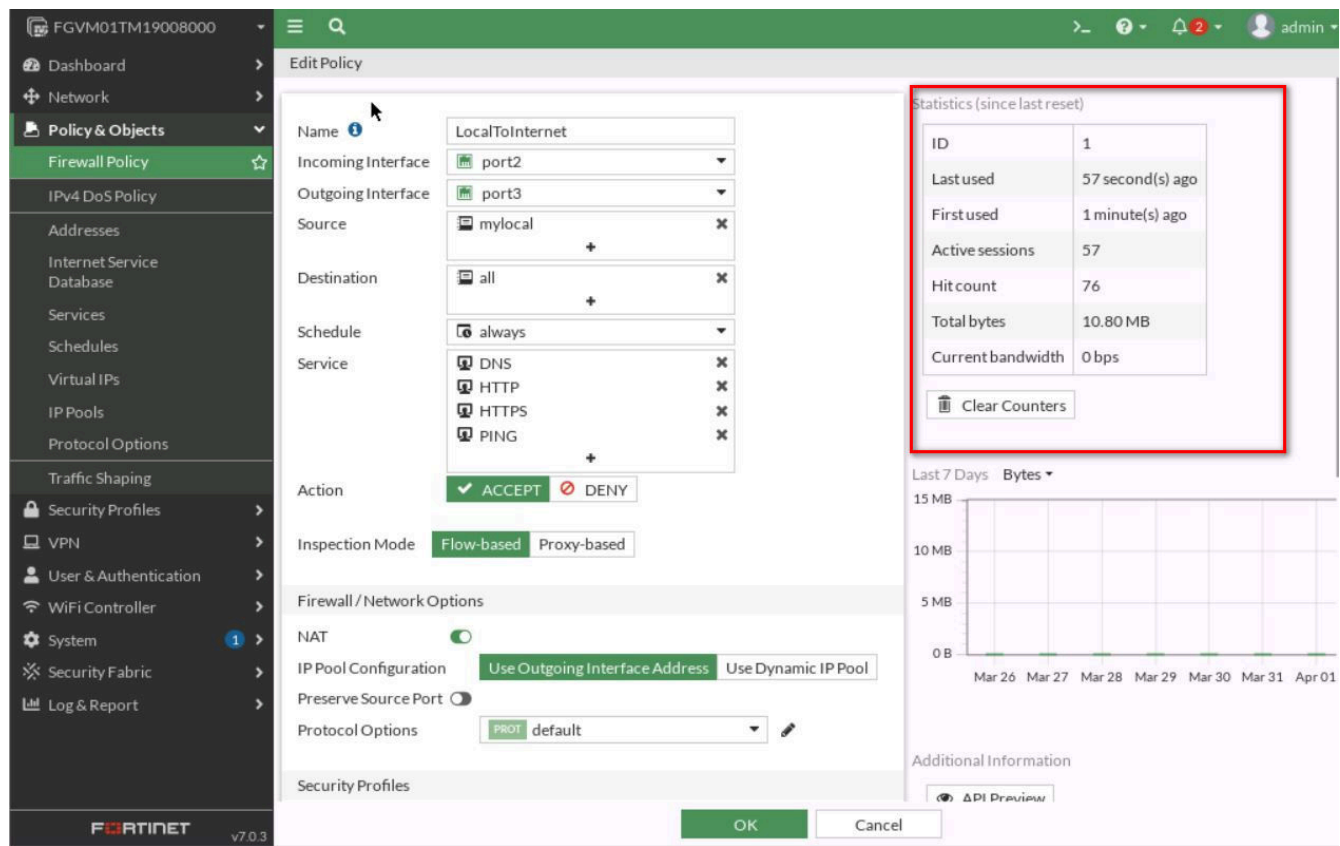


Figure 2.12: Hit count in the Firewall Policy

- Go to **Dashboard** > **Users & Devices** > **Device Inventory** and verify the IP and Mac address of the device.

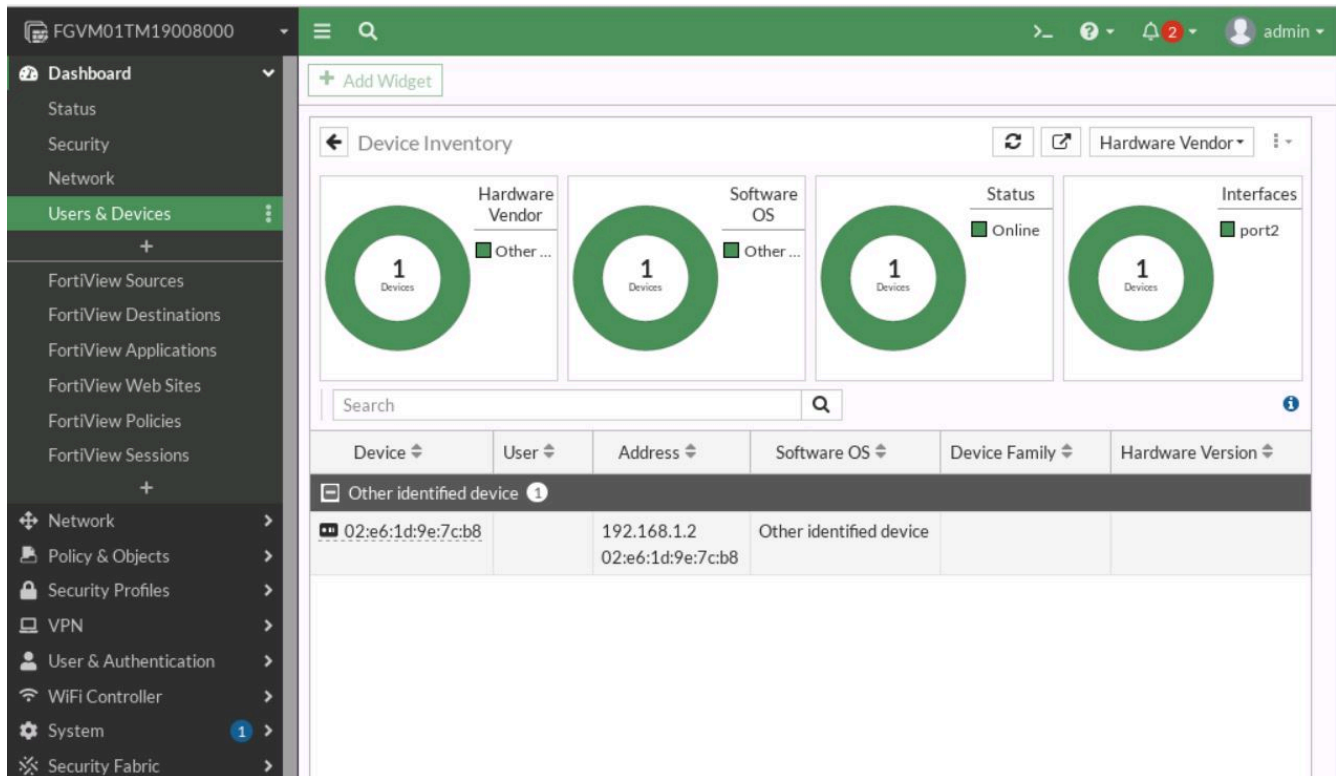


Figure 2.13: Device Inventory

Reordering Firewall Policies and Firewall Policy Actions

FortiGate will look for a matching policy, beginning at the top. Usually, you should put more specific policies at the top; otherwise, more general policies will match the traffic first, and your more granular policies will never be applied.

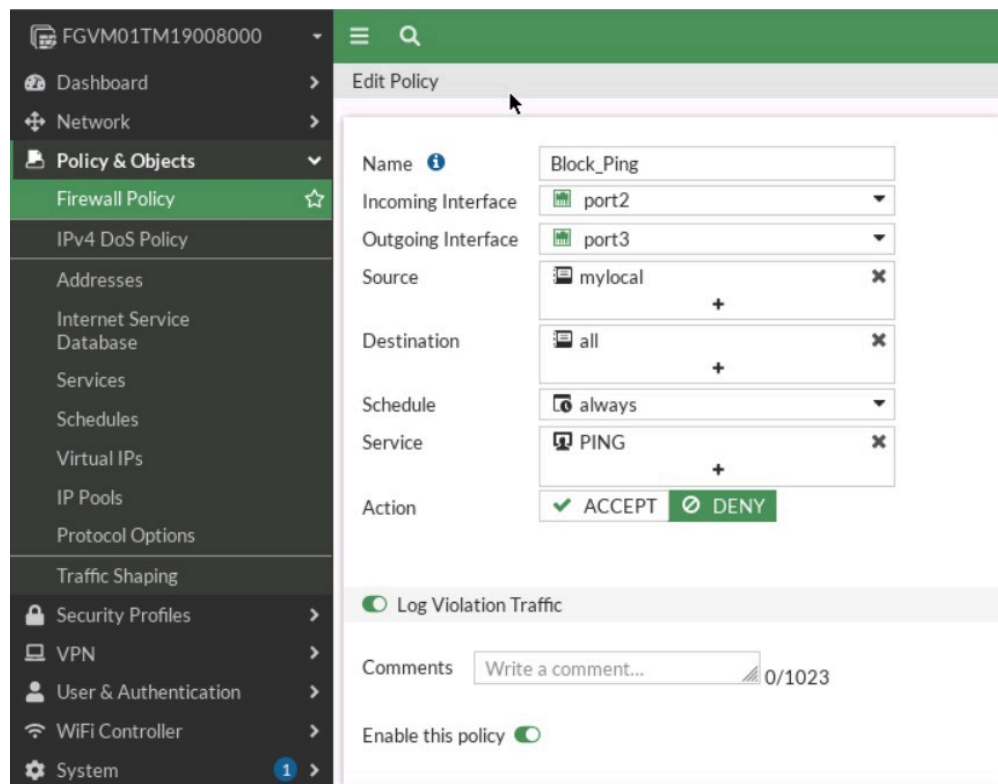
You will create a new firewall policy with more specific settings such as source, destination, service, and action set to **DENY**. Then, you will move this firewall policy above the existing firewall policies and observe the behaviour of firewall policy reordering.

Create a firewall policy

You will create a new firewall policy to match a specific source, destination, service, and action set to **DENY**.

Table 2.2: Firewall policy configuration

Field	Value
Name	Block_Ping
Incoming Interface	Port2
Outgoing Interface	Port3
Source	LOCAL_SUBNET
Destination	All
Schedule	Always
Service	PING
Action	DENY
Log Violation Traffic	<enable>
Enable this policy	<enable>

*Figure 2.14: Set firewall policy to block ping*

Click **OK** to save the changes. Add this policy on top of the previous policy.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Block_Ping	mylocal	all	always	PING	DENY			✓ AI
LocalToInternet	mylocal	all	always	DNS HTTP HTTPS PING	ACCEPT	Enabled	SSL no-inspection	U

Figure 2.15: Priority of *Block_Ping* should be higher than *LocalToInternet*

Go to **Webterm1** and ping **4.2.2.4**. You shouldn't be able to ping!

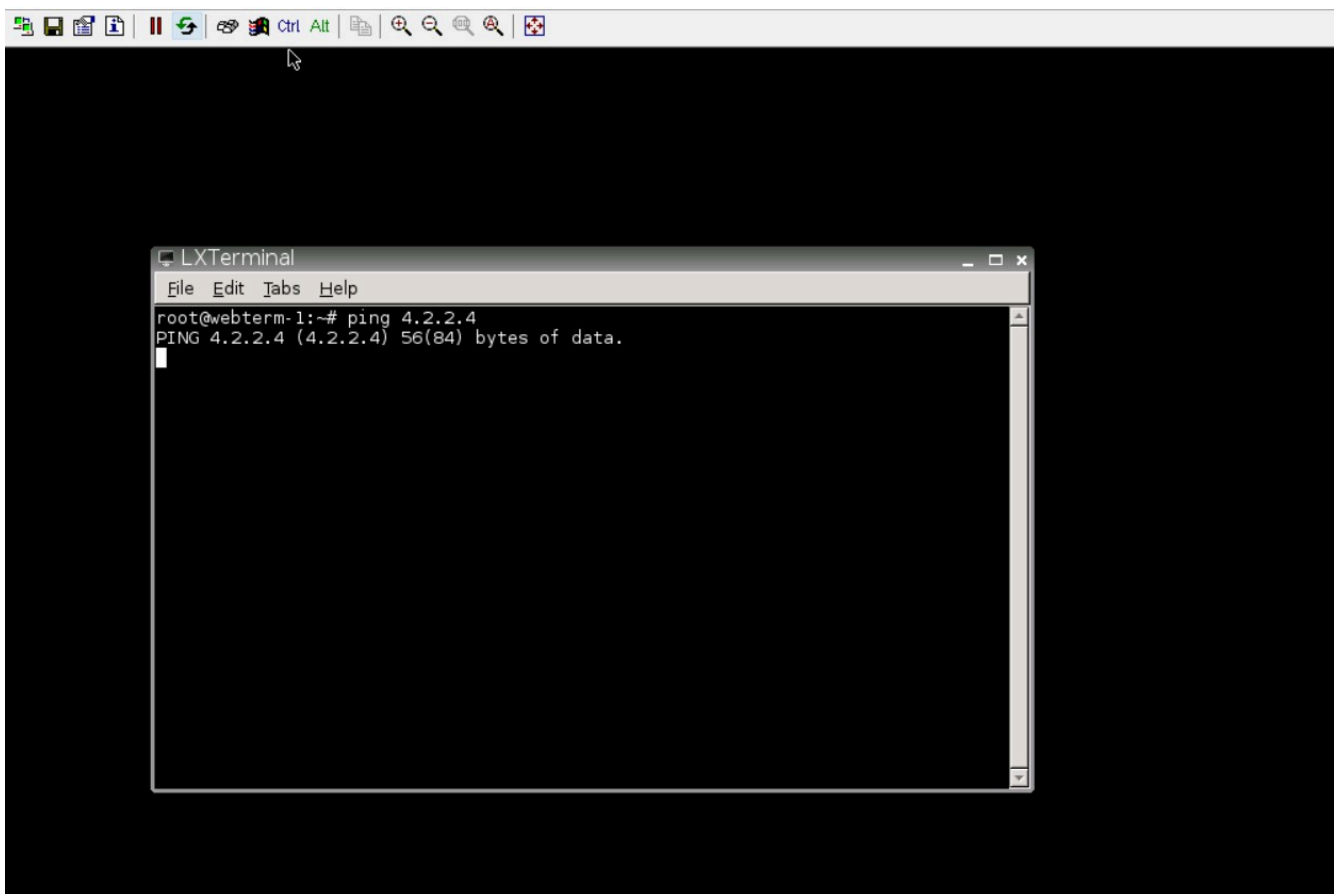


Figure 2.16: Verify ping in the *WebTerm1*

2.2 Application Profile

Learning Objectives

- Work with application profile in FortiGate
- Create a Traffic Shaper
- Apply Traffic Shaping to the traffic

Scenario: Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols. We are going to block social networks in the first example and then we are going to set Traffic Shaper for the local PCs in the second example. Finally, we will try to verify the connection speed in both PCs in the local network and compare them together.

Working with Application Profile

1. Go to **Policy & Objects > Firewall Policy** section, select **LocalToInternet** policy you have created in the previous section. Click on Edit.
2. Go to **Security Profile section > Application Control**.
 - Create a new Application Control
 - Name: **Ban-SocialNetwork**
 - In Categories **Block** Social Media, Video/Audio

New Application Sensor

i 93 Cloud Applications require deep inspection.
0 policies are using this profile.

Name

Comments 0/255

Categories

<input type="button" value="Business (179, ☁ 6)"/>	<input type="button" value="Cloud.IT (31)"/>
<input type="button" value="Collaboration (293, ☁ 6)"/>	<input type="button" value="Email (87, ☁ 12)"/>
<input type="button" value="Game (124)"/>	<input type="button" value="General.Interest (241, ☁ 9)"/>
<input type="button" value="Mobile (3)"/>	<input type="button" value="Network.Service (332)"/>
<input type="button" value="P2P (85)"/>	<input type="button" value="Proxy (106)"/>
<input type="button" value="Remote.Access (91)"/>	<input type="button" value="Social.Media (150, ☁ 31)"/>
<input type="button" value="Storage.Backup (296, ☁ 16)"/>	<input type="button" value="Update (48)"/>
<input type="button" value="Video/Audio (206, ☁ 13)"/>	<input type="button" value="VoIP (31)"/>
<input type="button" value="Web.Client (18)"/>	<input type="button" value="Unknown Applications"/>

Figure 2.17: Block Social.Media and Video/Audio

For Application and Filter Overrides. Because a filter override is configured to block applications that use excessive bandwidth, it will block all applications using excessive bandwidth, regardless of categories that allow these applications.

3. In **Application and Filter overrides > Create a new.**

1. Select **Application**
2. Action: **Block**
3. Application: **YouTube**

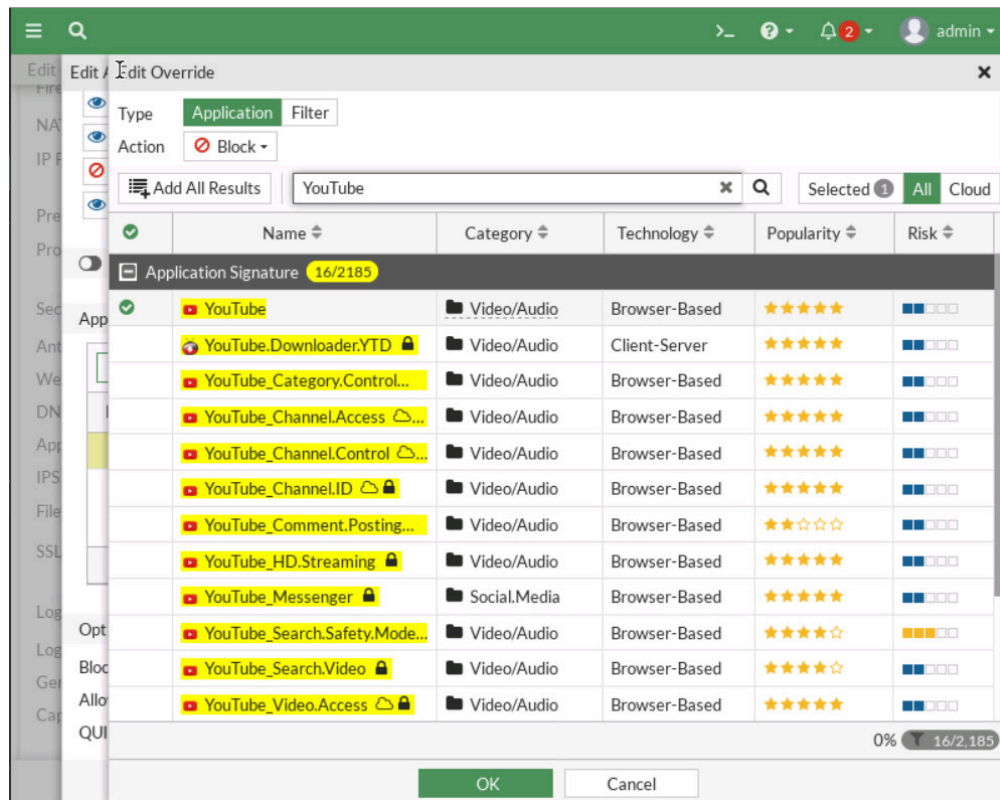


Figure 2.18: Block YouTube

4. In **Application and Filter overrides** > **Create a new**.

1. Select **Application**
2. Action: **Block**
3. Application: **Facebook_Chat**

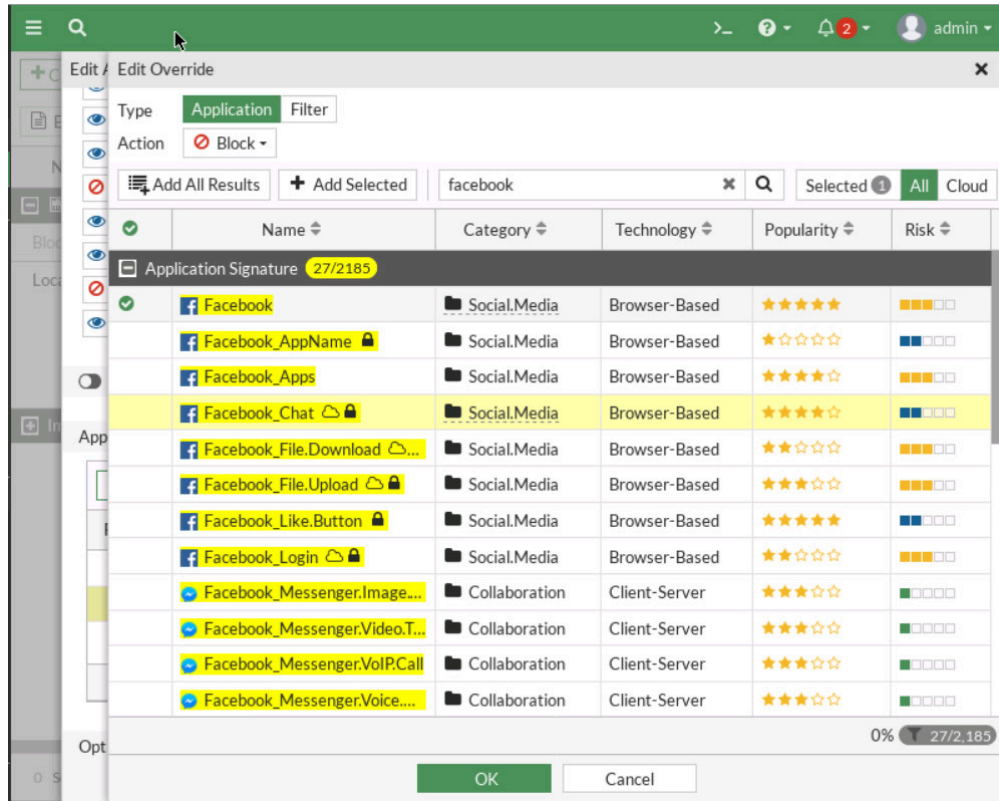


Figure 2.19: Block Facebook

5. **OK** all and now open the browser and go to **Twitter.com** or **YouTube.com** and try to search for a video and you should receive an application block page.

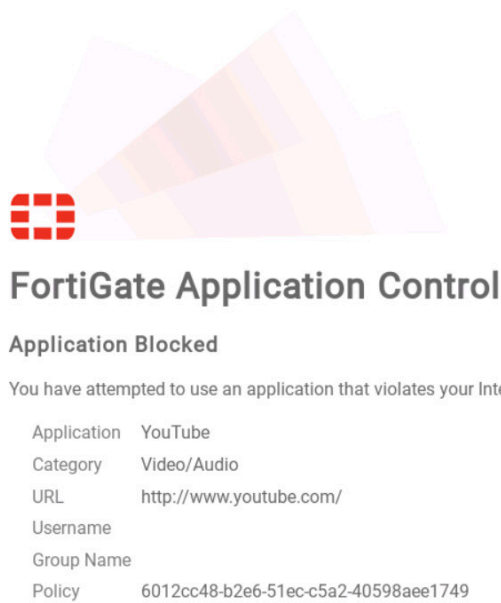
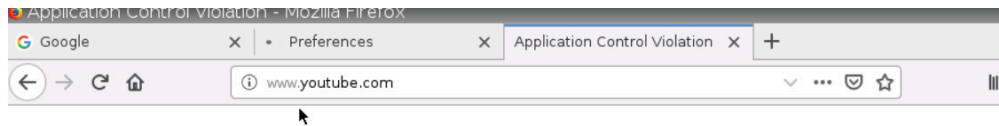


Figure 2.20: Application Control Blocked page

6. Go to **Log & Report > Application Control** and try to find the logs related to the previous step.

Source	Destination	Application Name	Action	Application User	App
192.168.1.2	142.251.46.195 (fonts.gstatic.com)	Google.Services	pass		
192.168.1.2	142.251.46.195 (fonts.gstatic.com)	SSL	pass		
192.168.1.2	142.250.191.78 (apis.google.com)	YouTube	block		
192.168.1.2	142.251.46.234 (fonts.googleapis.c...)	Google.Services	pass		
192.168.1.2	142.251.46.234 (fonts.googleapis.c...)	SSL	pass		
192.168.1.2	172.217.6.78 (www.youtube.com)	YouTube	block		
192.168.1.2	34.120.237.76 (img-getpocket.cdn...)	HTTPS.BROWSER	pass		
192.168.1.2	34.120.237.76 (img-getpocket.cdn...)	SSL	pass		
192.168.1.2	34.120.237.76 (img-getpocket.cdn...)	HTTPS.BROWSER	pass		
192.168.1.2	34.120.237.76 (img-getpocket.cdn...)	SSL	pass		
192.168.1.2	157.240.22.35 (facebook.com)	Facebook	block		
192.168.1.2	157.240.22.35 (facebook.com)	SSL	pass		
192.168.1.2	157.240.22.35 (facebook.com)	Facebook	block		
192.168.1.2	157.240.22.35 (facebook.com)	SSL	pass		
192.168.1.2	157.240.22.35 (facebook.com)	Facebook	block		
192.168.1.2	157.240.22.35 (facebook.com)	SSL	pass		
192.168.1.2	157.240.22.35 (facebook.com)	Facebook	block		

Figure 2.21: Application Control logs

Working with Application Profile: Part 2

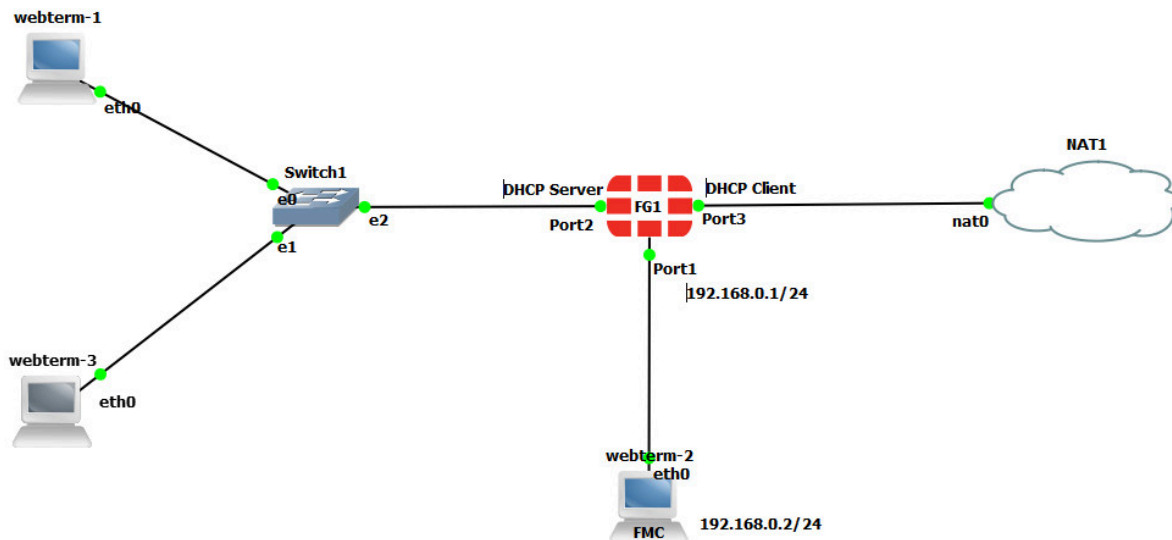


Figure 2.22: Main scenario

Table 2.3: Devices Configuration

Device	Configuration
FortiGate	Port 2: DHCP Server (192.168.1.20 – 192.168.1.30) Port 3: DHCP Client
WebTerm1	DHCP Client
WebTerm3	DHCP Client

1. Remove the application control you have set for policies in the previous step.
2. Add Ethernet Switch and **WebTerm3** to your GNS3. WebTerm3 should receive an IP address from DHCP.

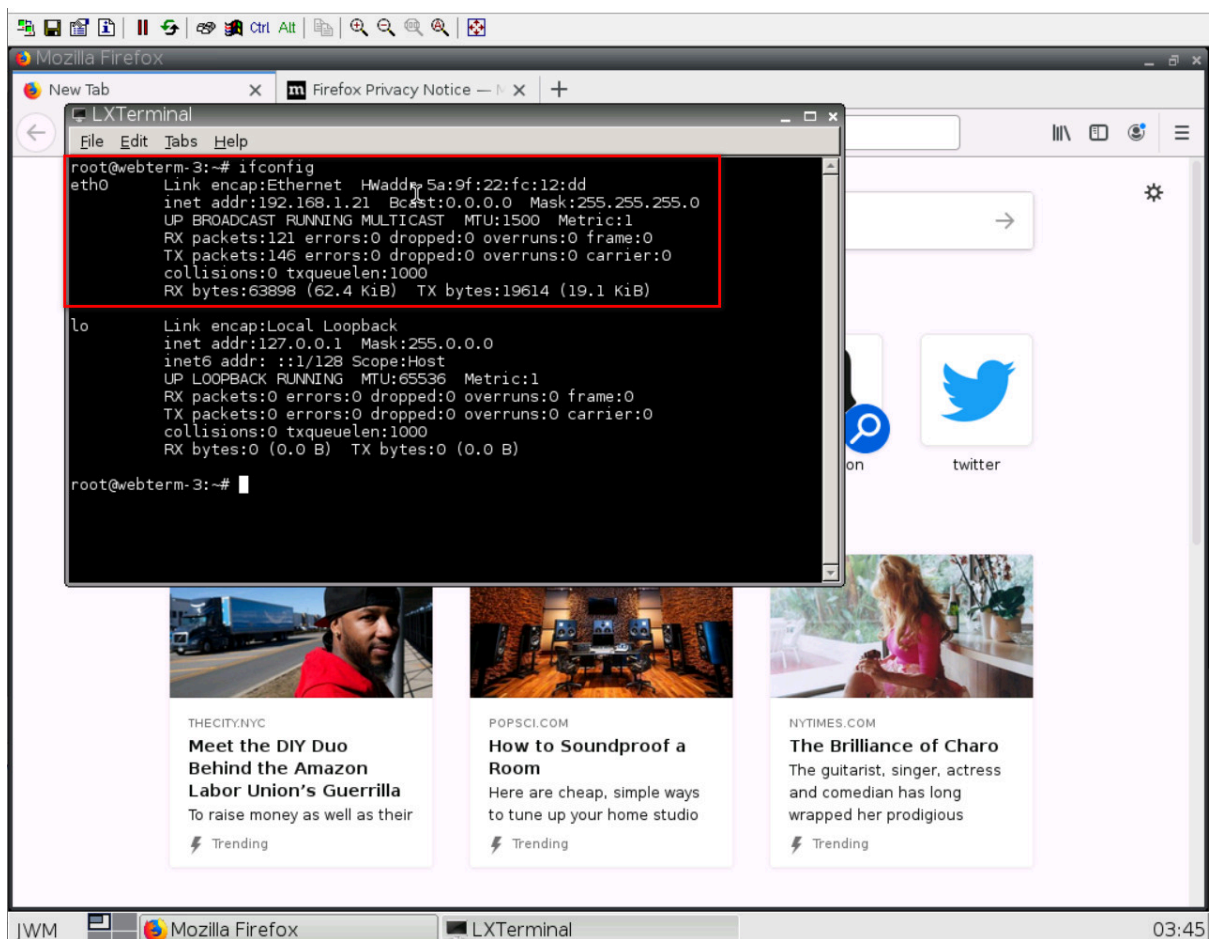


Figure 2.23: Verify DHCP address in WebTerm3

3. Set traffic shaping for WebTerm3 to save the bandwidth.
 - Create an Address object for WebTerm3. Go to **Addresses > Create a new Address** with the following information:

Table 2.4: Create a new Address for WebTerm3

Field	Value
Name	WebTerm3
Type	Subnet
Subnet/IP Range	192.168.1.21/32 (Check your IP in WebTerm3)
Interface	any

Figure 2.24: WebTerm3 IP address

4. Go to **Policy & Objects > Traffic Shapers** and create a new Per-IP traffic shaper. Shared affects upload speed while Per-IP affects download and upload speed.

Table 2.5: Traffic Shaper Configuration

Field	Value
Type	Per-IP
Name	WebTerm3
Max Bandwidth	10000
Max Concurrent Connections	5000

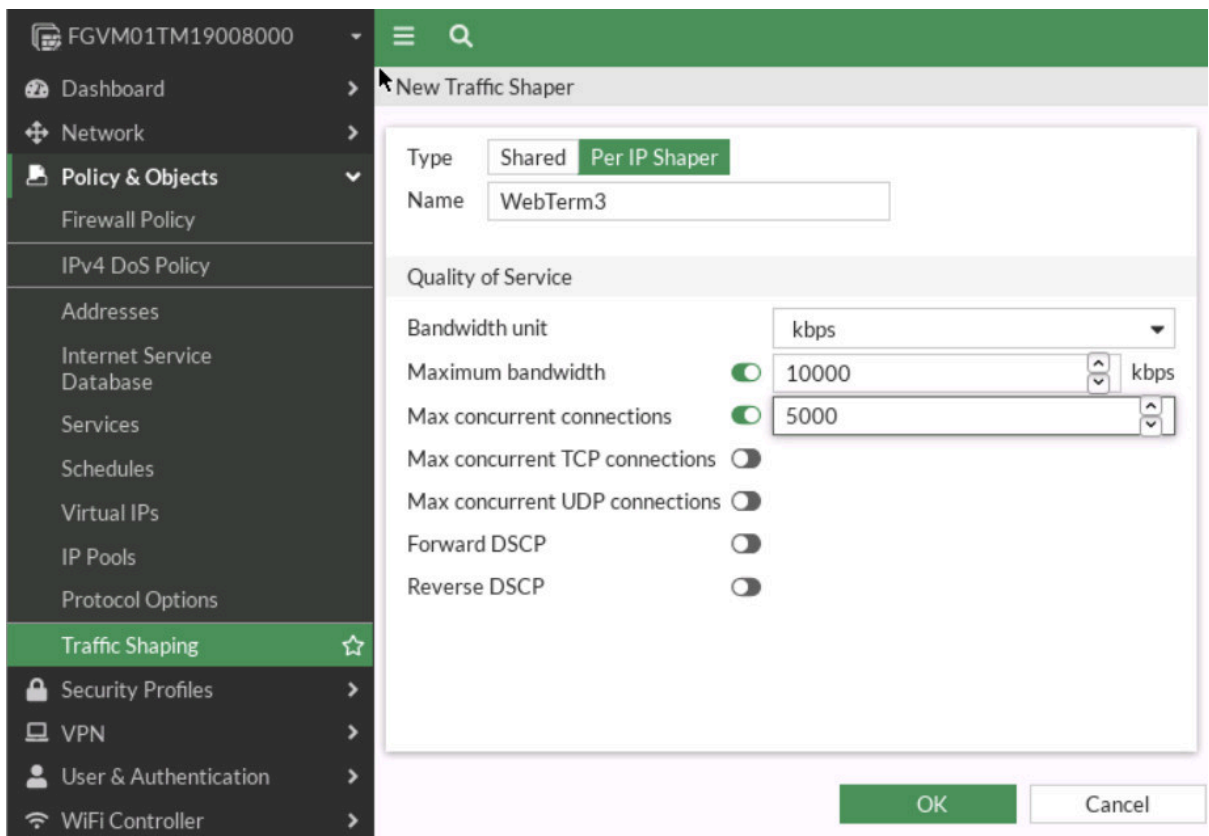


Figure 2.25: Set traffic shaping

5. Go to **Policy & Objects > Traffic Shaping Policy** and create a new Policy.

Table 2.6: Traffic Shaping Policy Configuration

Field	Value
Source	WebTerm3
Destination	ALL
Service	ALL
Outgoing interface	Port3
Per-IP Shaper	WebTerm3

New Traffic Shaping Policy

Name:

Status: Enabled Disabled

Comments: 0/255

If Traffic Matches:

Source:

Destination:

Schedule:

Service:

Application:

URL Category:

Then:

Outgoing interface:

Apply shaper:

Shared shaper:

Reverse shaper:

Per-IP shaper:

Assign shaping class ID:

Additional Information

Figure 2.26: Set traffic shaping policy

6. To verify open the browser in the WebTerm3 and go to **Fast.com**.

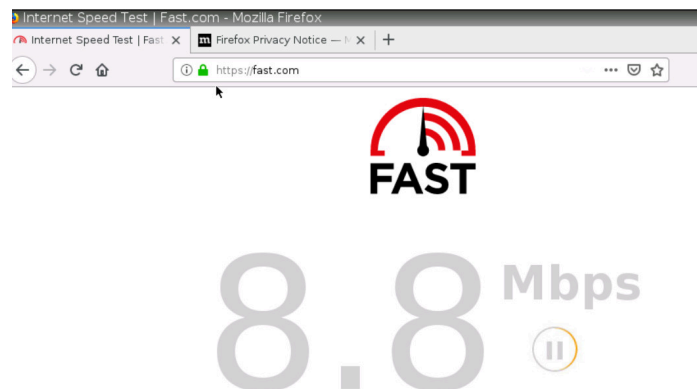


Figure 2.27: WebTerm3 speed test

7. Now, open the browser in WebTerm1 and go to **Fast.com**.

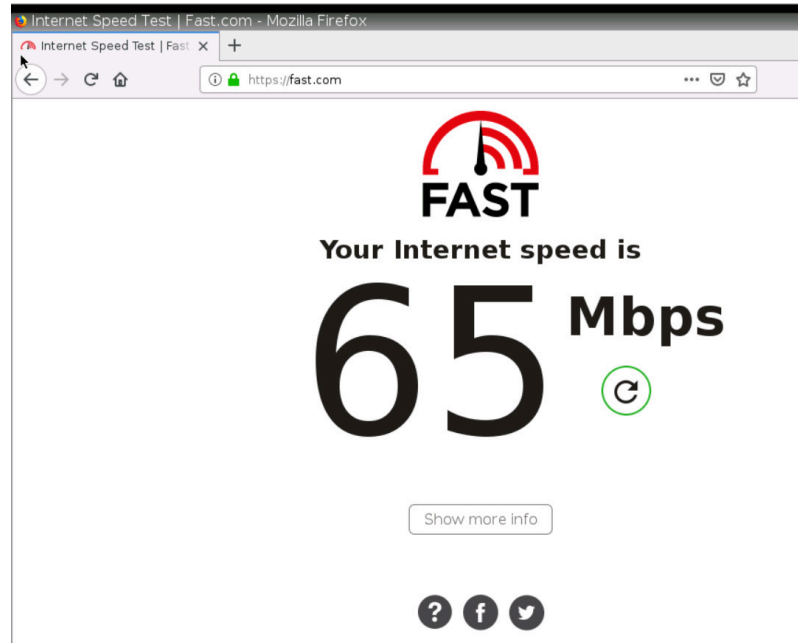


Figure 2.28: WebTerm1 speed test

8. We are going to allow only twitter Applications in WebTerm3. Other applications should be blocked. To do:

1. Add a new Policy from port2 to port3.

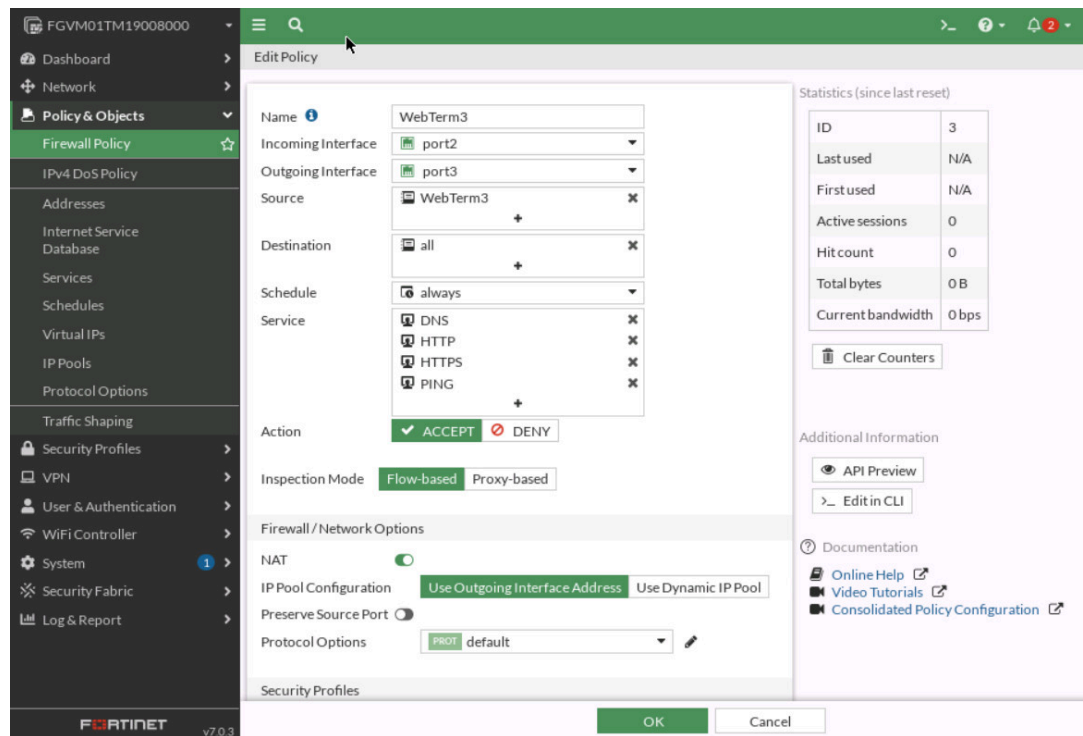


Figure 2.29: Set Firewall Policy

2. Add and Application Control and Block all applications except Twitter. Then, assign the WebTerm3 profile to Application Control.

Edit Application Sensor

Name:

Comments: 0/255

Categories

- All Categories
- Business (153, ☁ 6)
- Email (77, ☁ 12)
- Mobile (3)
- Proxy (174)
- Storage.Backup (161, ☁ 19)
- VoIP (23)
- Cloud.IT (66, ☁ 1)
- Game (86)
- Network.Service (333)
- Remote.Access (95)
- Update (49)
- Web.Client (24)
- Collaboration (268, ☁ 16)
- General.Interest (233, ☁ 8)
- P2P (56)
- Social.Media (118, ☁ 32)
- Video/Audio (155, ☁ 17)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New ✎ Edit 🗑 Delete

Priority	Details	Type	Action
1	<ul style="list-style-type: none"> Twitter Twitter.Video Twitter_Login Twitter_Message Twitter Post 	Application	Allow

Figure 2.30: WebTerm3 Application Control Settings

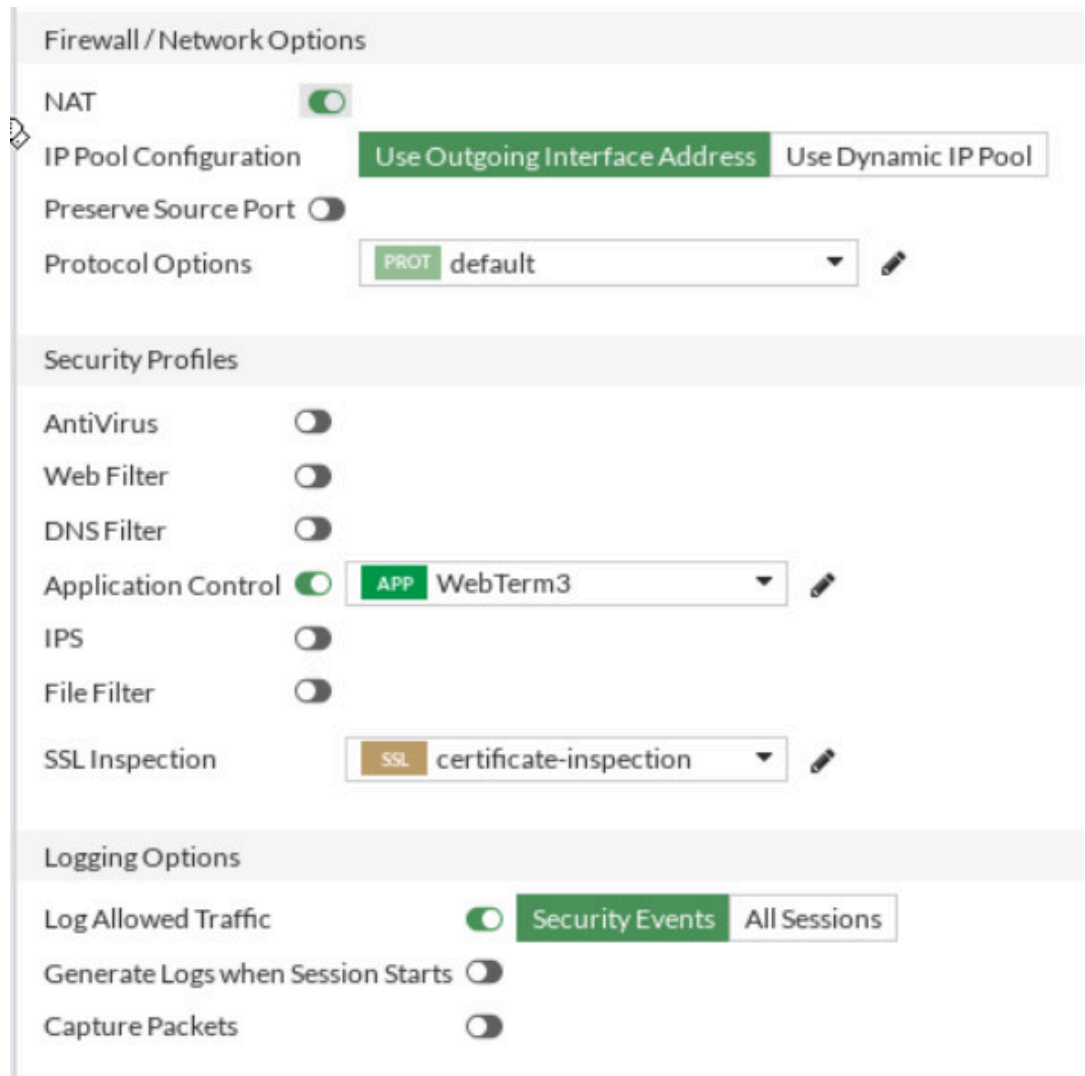


Figure 2.31: Set Application Control

- Then, put the policy you have created above LocalToInternet Policy.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Block_Ping	mylocal	all	always	PING	DENY			All
WebTerm3	WebTerm3	all	always	DNS HTTP HTTPS PING	ACCEPT	Enabled	APP WebTerm3 SSL certificate-inspection	UTM
LocalToInternet	mylocal	all	always	DNS HTTP HTTPS PING	ACCEPT	Enabled	SSL certificate-inspection	UTM
Implicit								

Figure 2.32: Priority of policies

- Verify: in WebTerm1, you should be able to reach any websites.

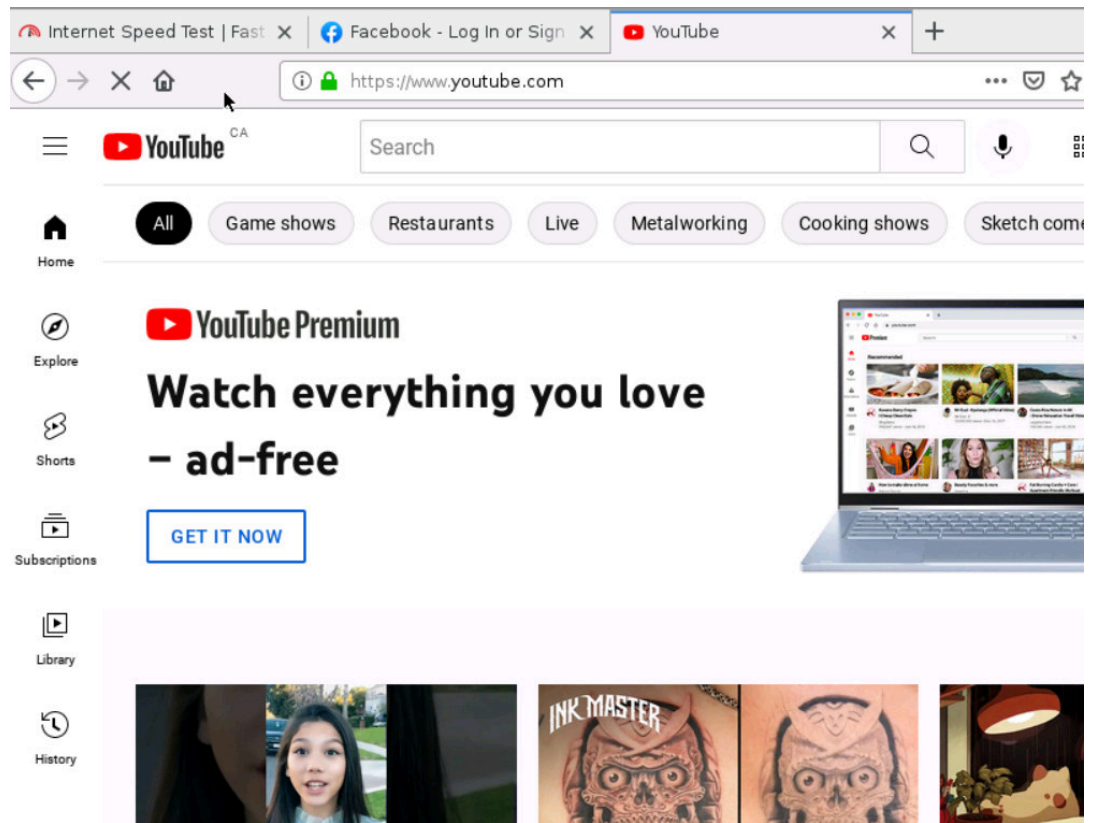


Figure 2.33: Verify the result in WebTerm1

Chapter 3. NAT

3.1 Source NAT

Learning Objectives

- Configure a NAT policy in FortiGate
- Identify source NAT

Scenario: We are going to enable Source NAT (SNAT) to reach the Internet from Kali. That means that all traffic from the local network to the Internet should be allowed.

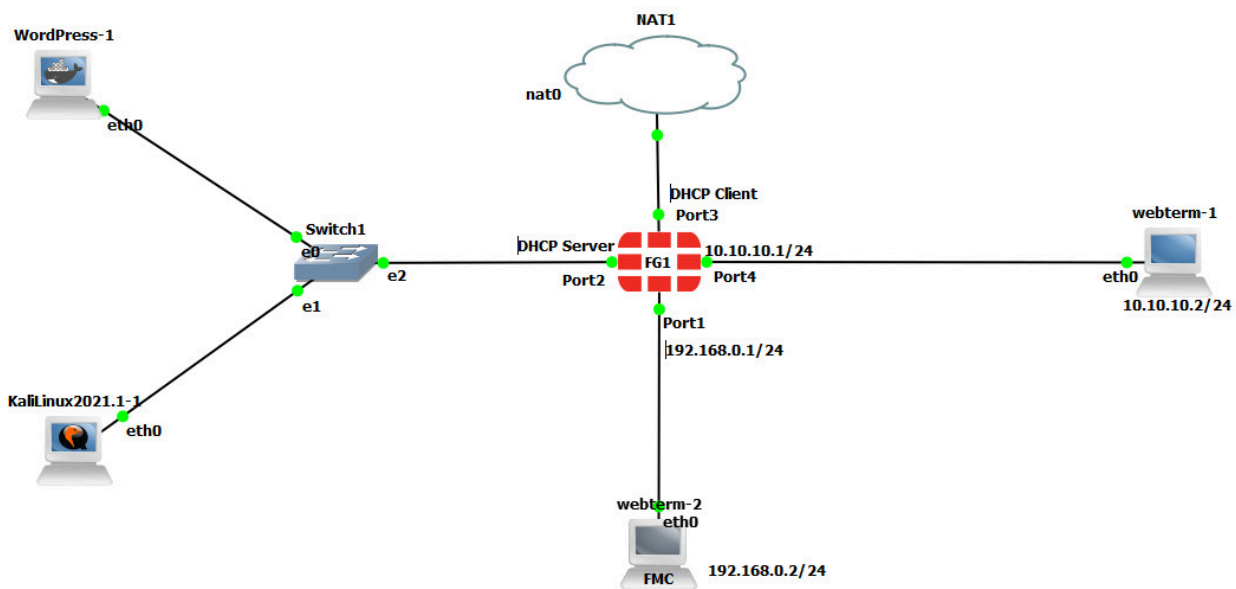


Figure 3.1: Main scenario

Source NAT

Table 3.1: Devices configuration

Device	IP address	Access
Kali	DHCP Client	–
WordPress/Kali	DHCP Client	–
Ethernet Switch	–	–
FortiGate	Port 2 – (192.168.1.1/24) – DHCP Server (192.168.1.10 to 192.168.1.20) Port 3 – DHCP Client Port 4 – 10.10.10.1/24	ICMP-HTTP-HTTPS
WebTerm	10.10.10.2/24	–

Basic Configuration

1. Port configuration in the firewall as follows:

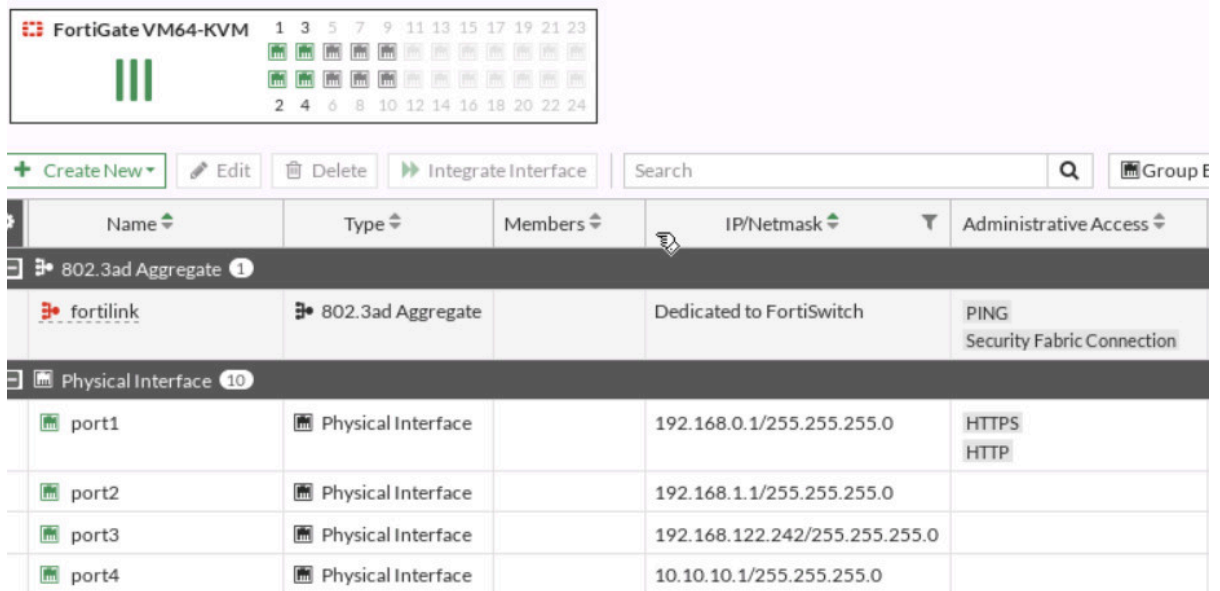


Figure 3.2: Ports configuration in the firewall

2. Set a DHCP server on interface port2 (Range of IP address should be: 192.168.1.10 to 192.168.1.20, DNS: 4.2.2.4).

DHCP Server

DHCP status Enabled Disabled

Address range

Netmask

Default gateway Same as Interface IP Specify

DNS server Same as System DNS Same as Interface IP Specify

DNS server 1

Lease time second(s)

Advanced

Network

Device detection

Security mode

Figure 3.3: DHCP Server configuration

- Set port3 as a DHCP client and connect to the NAT.

Address

Addressing mode Manual DHCP Auto-managed by IPAM

Status Connected

Obtained IP/Netmask

Expiry Date

Acquired DNS

Default gateway

Retrieve default gateway from server

Distance

Override internal DNS

Figure 3.4: DHCP client configuration

- Set a static route in the firewall to reach to NAT object.

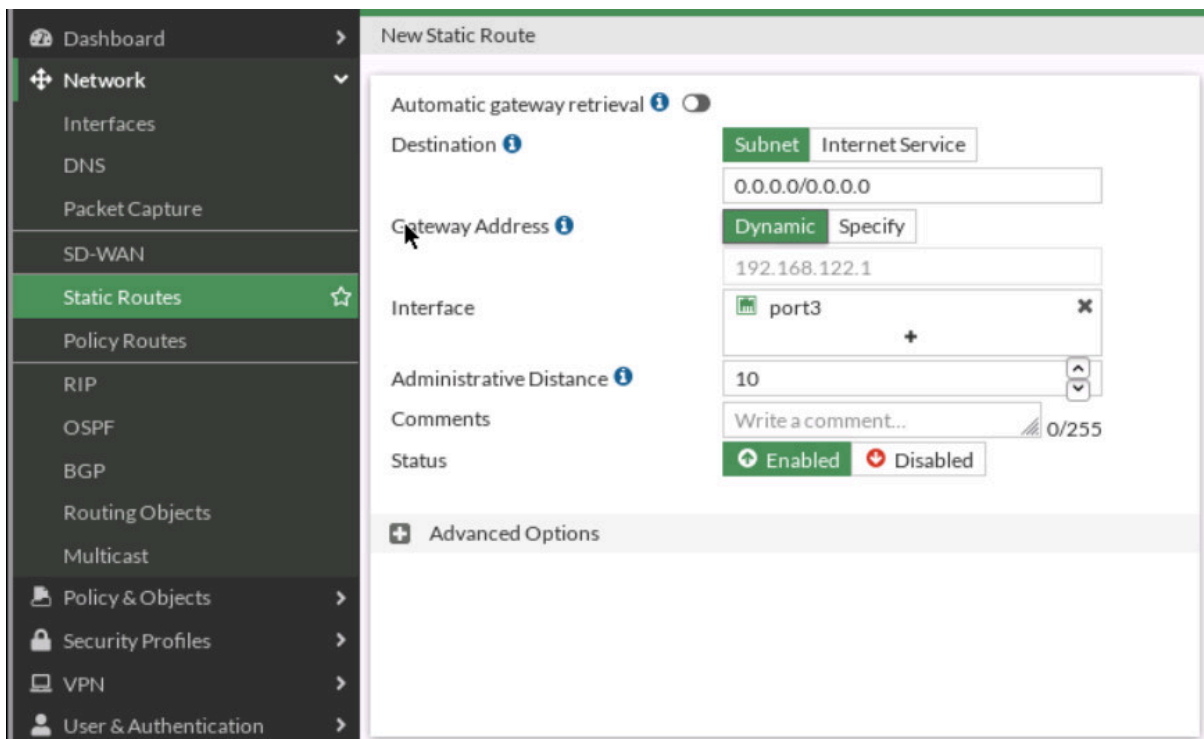


Figure 3.5: Set a static route

5. Go to **Policy & Objects** > **Firewall Policy** section, click **Create New** to add a new firewall policy, and configure the following settings:
 - Name: **LocalToInternet**
 - From **inside to outside (port2 to port3)**
 - Source: **Create an address for the local network** (Subnet: 192.168.1.0/24)
 - Destination: **all**
 - Schedule: **Always**
 - Service: **Only HTTP, HTTPS, and DNS**
 - Action: **Accept**

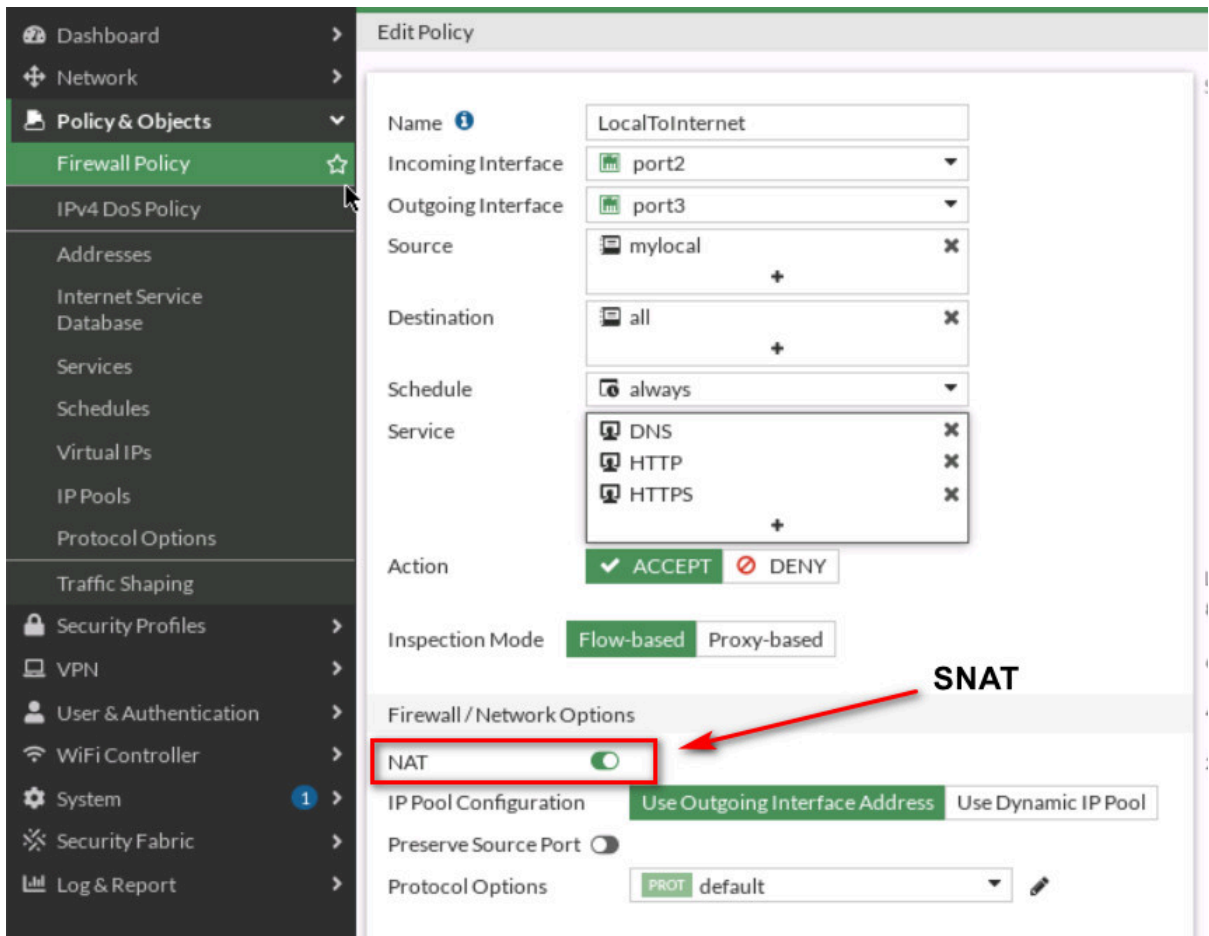


Figure 3.6: Configure Firewall Policy and enable Source NAT

- Open the browser in Kali, you should be able to access the internet.

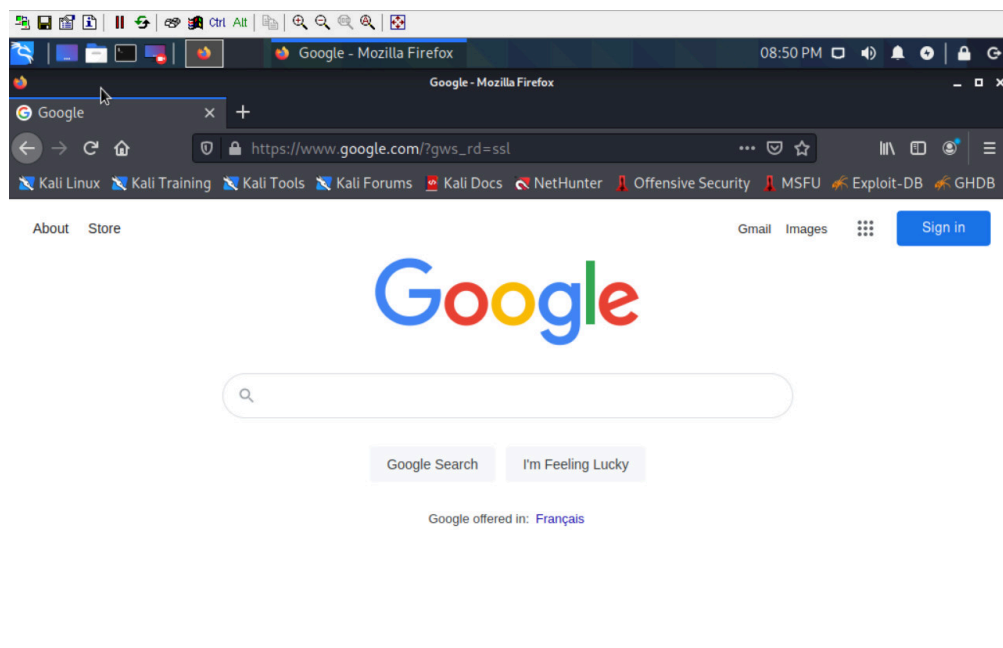


Figure 3.7: Verify your configuration

3.2 Destination NAT

Learning Objectives

- Create a virtual IP address
- Create a Destination NAT
- Create a Port Forwarding

Scenario: We are going to enable Destination NAT (DNAT) and able to reach WordPress from WebTerm1. That means if someone from WebTerm1 opens the browser and types `http://10.10.10.1` should be able to reach WordPress.

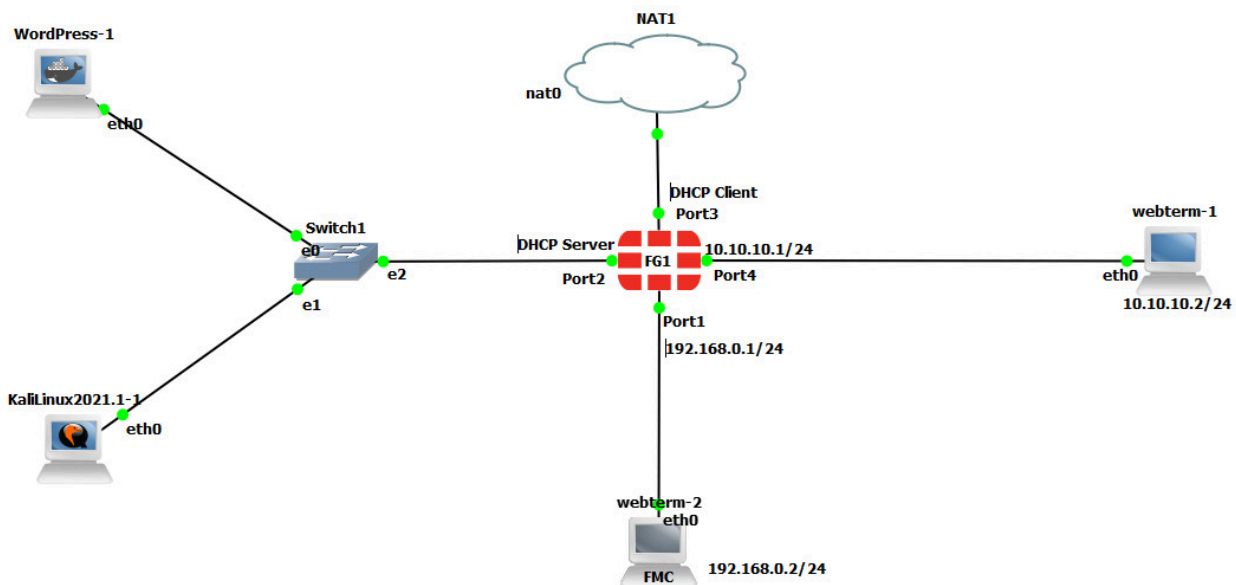


Figure 3.8: Main scenario

VIP (Virtual IP address)

Go to **Policy Objects > Virtual IPs** and Create a new Virtual IP:

- Name: **outsideToDMZ**
- Interface: **Port 4**
- External IP address: **10.10.10.1**
- Mapped IP address: **192.168.1.X** (Find the local IP address of your WordPress)
- Enable Port Forwarding:
 - External Service Port: **TCP 80**
 - Map to Port: **TCP 80**

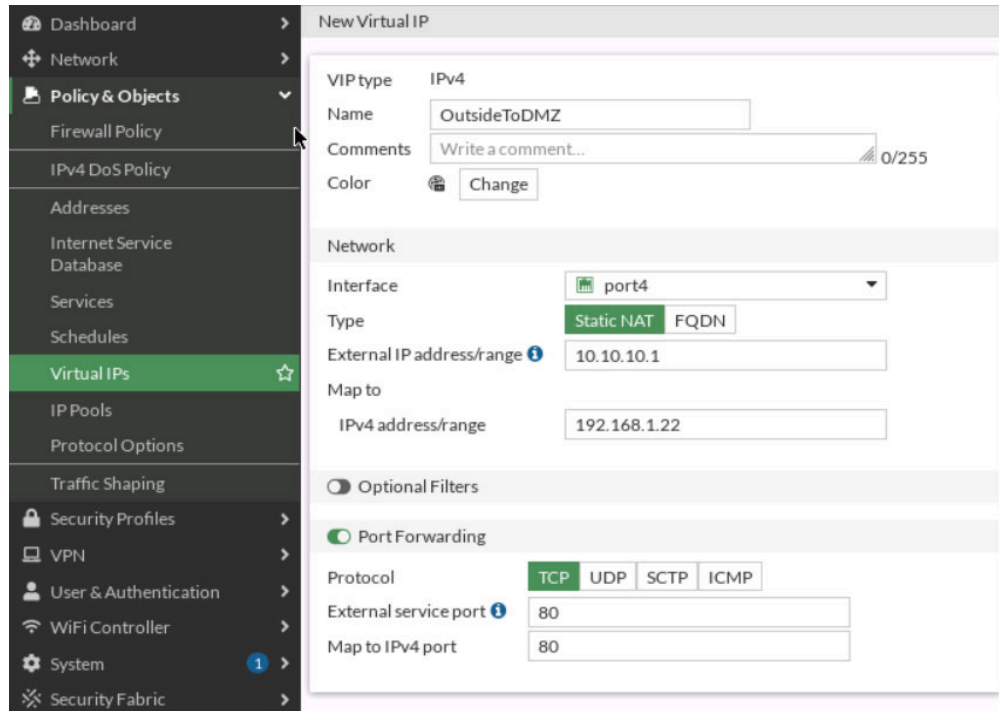


Figure 3.9: Configure Virtual IP

Create a Firewall Policy

You will create a new firewall policy to match a specific source, destination, service, and action set to Accept.

Table 3.2: Firewall policy configuration

Field	Value
Name	Outside-DMZ
Incoming Interface	Port 4
Outgoing Interface	Port 2
Source	All
Destination	Select your VIP Name (outsideToDMZ)
Schedule	Always
Service	HTTP
Action	ACCEPT
Log Violation Traffic	<enable>
Enable this policy	<enable>

Click **OK** to save the changes.

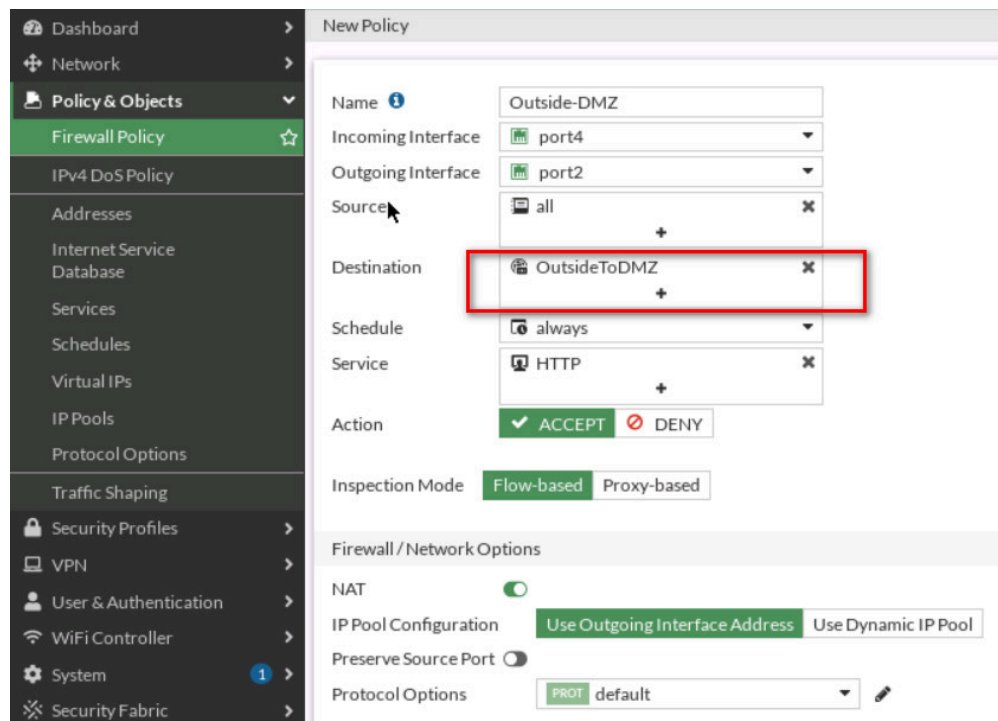


Figure 3.10: Set Firewall Policy

To confirm traffic matches, go to WebTerm1, open the browser and type `http://10.10.10.1` in the browser. You should be able to reach WordPress.

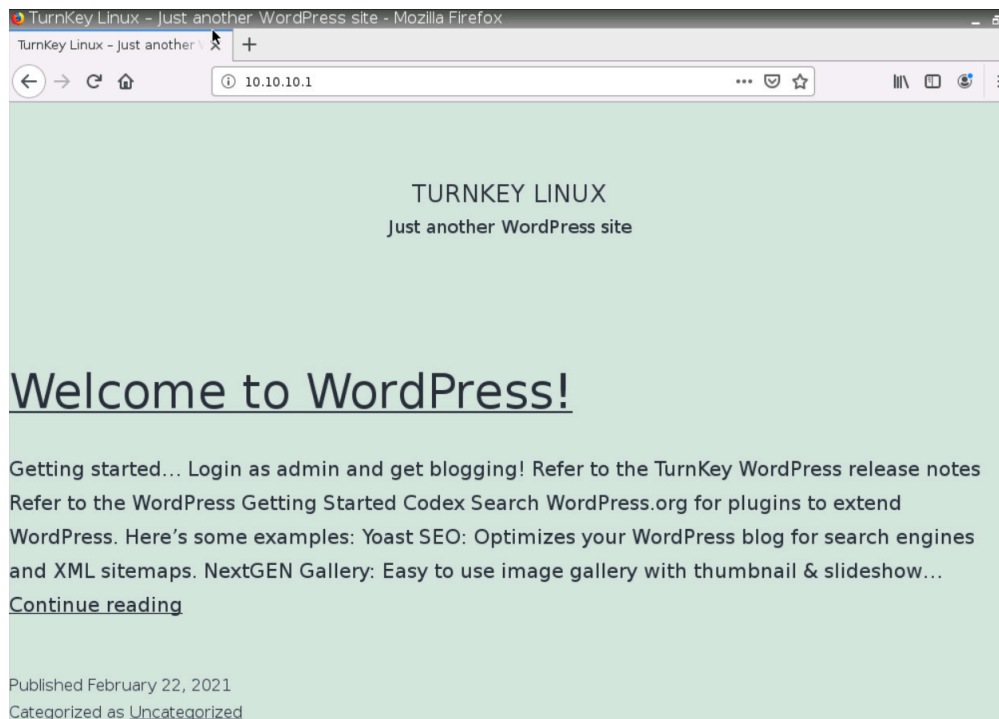


Figure 3.11: Verify configuration

Port Forwarding

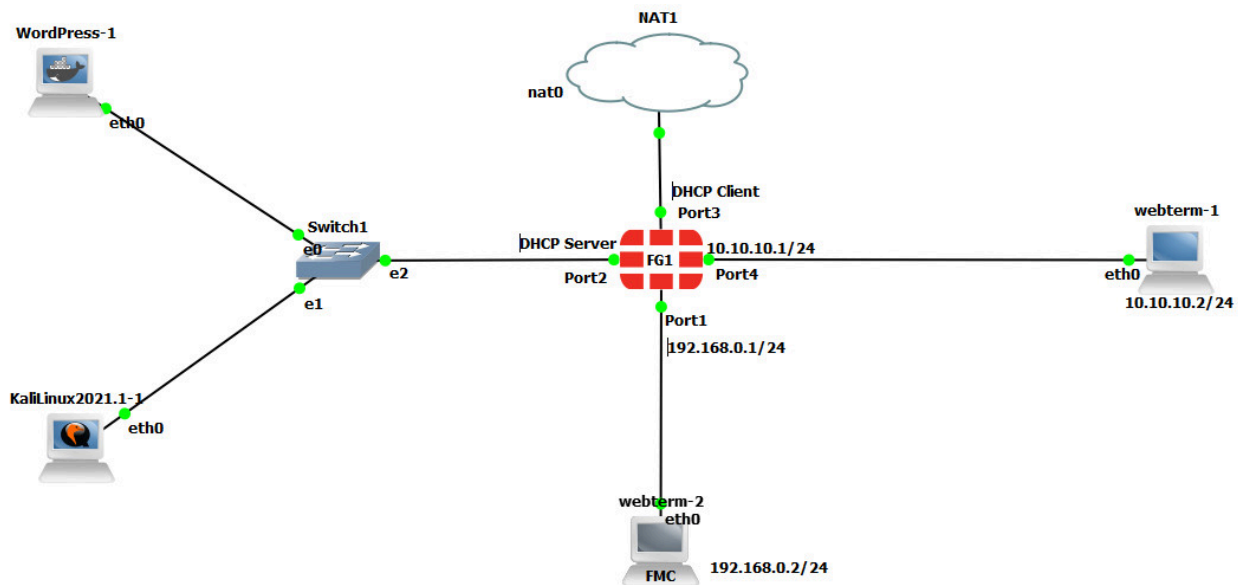


Figure 3.12: Main scenario

1. Set the interface of Kali as a DHCP client and enable SSH in Kali. To enable SSH in Kali type Figure 3.13 command:

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ service ssh start

```

Figure 3.13: Enable SSH service in Kali

```

(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.23 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::592f:fc00:6db5:f6de prefixlen 64 scopeid 0x20<link>
    ether 0c:ea:85:2f:00:00 txqueuelen 1000 (Ethernet)
    RX packets 10654 bytes 13841347 (13.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4170 bytes 481667 (470.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 3.14: Verify you've received an IP address from DHCP

- Repeat the previous steps we have done for DNAT and try to reach Kali from port 8080 (Port Forwarding: 8080 → 22)

The screenshot shows the FortiGate web interface with the 'Virtual IPs' configuration page. The configuration is as follows:

- VIP type:** IPv4
- Name:** Kali
- Comments:** Write a comment...
- Color:** Change
- Network:**
 - Interface:** port4
 - Type:** Static NAT
 - External IP address/range:** 10.10.10.1
 - Map to:**
 - IPv4 address/range:** 192.168.1.23
- Optional Filters:**
 - Port Forwarding:**
 - Protocol:** TCP (selected), UDP, SCTP, ICMP
 - External service port:** 8080
 - Map to IPv4 port:** 22

Buttons for 'OK' and 'Cancel' are visible at the bottom of the configuration window.

Figure 3.15: Map External port 8080 to local port 22

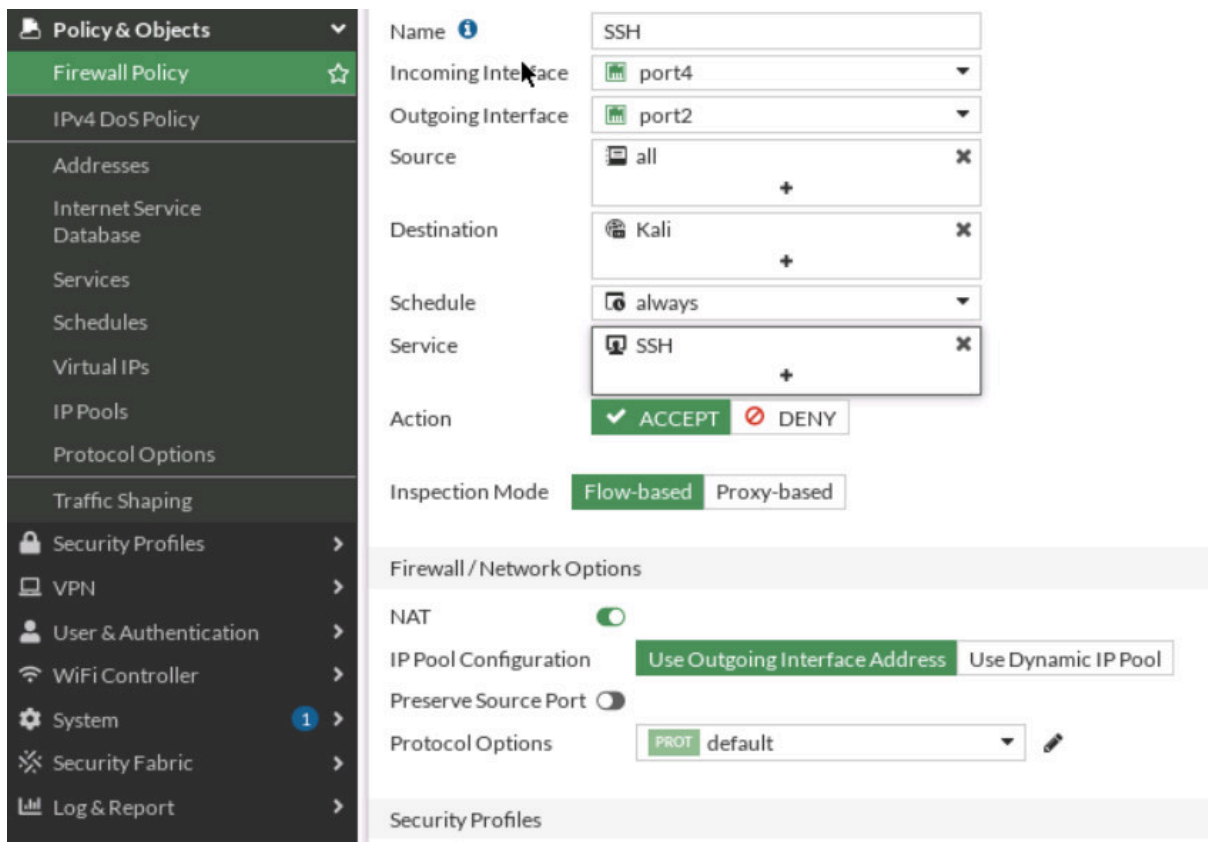


Figure 3.16: Set Firewall Policy

3. Verify your connection from WebTerm (**Hint:** `ssh user@10.10.10.1 -p 8080`).

```

kali@kali: ~
File Edit Tabs Help
root@webterm-1:~# ssh kali@10.10.10.1 -p 8080
The authenticity of host '[10.10.10.1]:8080 ([10.10.10.1]:8080)' can't be established.
ECDSA key fingerprint is a6:f2:10:5f:a9:b7:8f:45:1c:51:0d:9e:33:8d:63:64.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.10.1]:8080' (ECDSA) to the list of known hosts.
kali@10.10.10.1's password:
Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
#####(Message from Kali developers)
#####
##### We have kept /usr/bin/python pointing to Python 2 for backwards
##### compatibility. Learn how to change this and avoid this message:
##### https://www.kali.org/docs/general-use/python3-transition/
#####
#####(Run #####touch ~/.hushlogin##### to hide this message)
#####kali#####kali) - [~]

```

Figure 3.17: Verify SSH connection

Chapter 4. VPN

4.1 IPsec VPN

Learning Objectives

- Configure an IPsec VPN
- Configure a site-to-site VPN

Scenario: We are going to have IPsec VPN from Windows to FortiGate Firewall. First, we are going to install FortiClient on Windows and then we will configure the firewall for FortiClient. The goal of this scenario is to have connectivity from Windows to PC1. You should be able to ping PC1 after you have established your VPN connection.

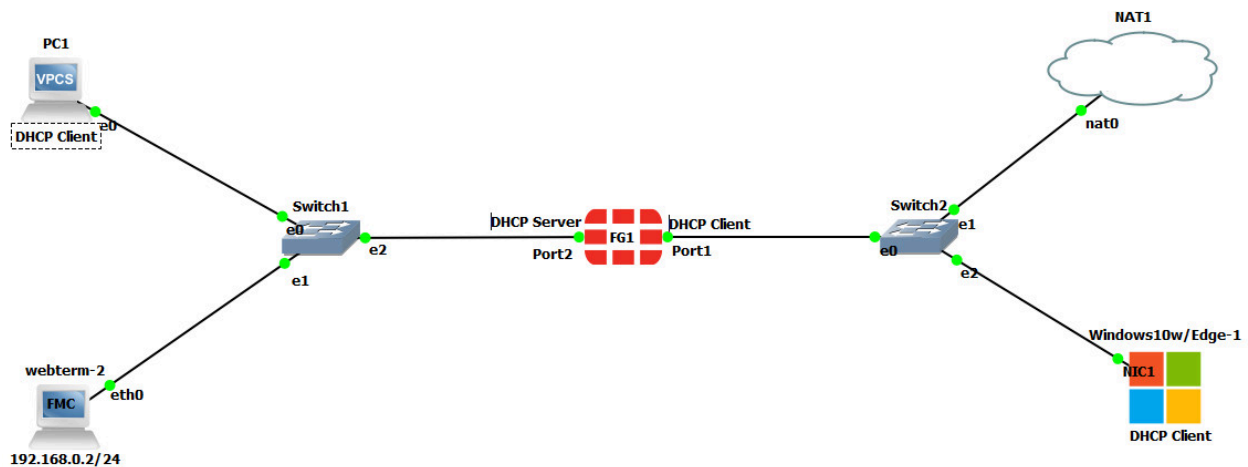


Figure 4.1: Main scenario

Configuration

Table 4.1: Devices configuration

Device	IP address	Access
WebTerm2	192.168.0.2/24	–
VPC	DHCP Client	–
Ethernet Switch1-2	–	–
FortiGate	Port 1: DHCP Client Port 2: 192.168.0.1/24 DHCP Server (192.168.0.10 to 192.168.0.20)	ICMP HTTP HTTPS
Windows	DHCP Client	–

Before you begin the configuration, please remember with VPC's and Web terms this is how we edit their IP settings for static and or DHCP Addressing:

Before dragging in your web terms or other devices remember to always choose GNS3 VM:

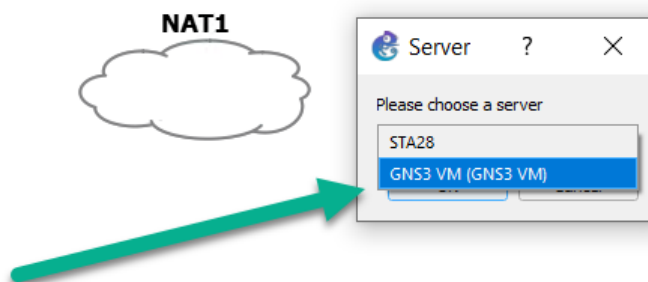


Figure 4.2: Dragging a NAT under GNS3 VM

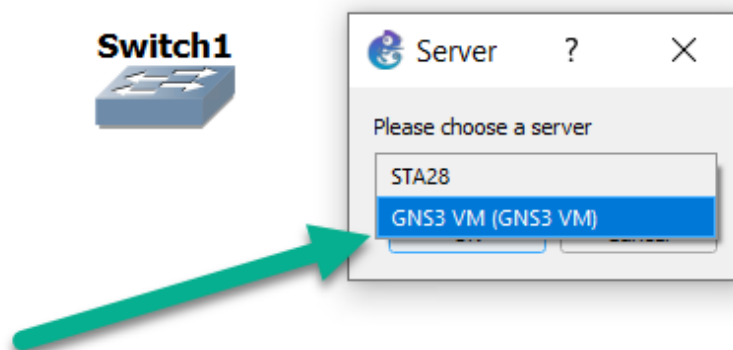


Figure 4.3: Dragging a switch under GNS3 VM

1. Set a DHCP server on interface port2 (Range of IP address should be: 192.168.0.20 to 192.168.0.30, DNS: 4.2.2.4).

The screenshot shows the FortiGate configuration interface for the DHCP Server on interface port2. The DHCP Server is enabled, and the address range is set to 192.168.0.10-192.168.0.20. The netmask is 255.255.255.0. The default gateway is set to 'Same as Interface IP', and the DNS server is set to 'Same as System DNS'. The lease time is 604800 seconds.

Figure 4.4: Set DHCP IP address

The screenshot shows a webterminal window titled 'webterm-1 interfaces'. The terminal displays the following configuration:

```
#
# This is a sample network config uncomment lines to configure the network
#
# Static config for eth0
#auto eth0
#iface eth0 inet static
#   address 192.168.0.2
#   netmask 255.255.255.0
#   gateway 192.168.0.1
#   up echo nameserver 192.168.0.1 > /etc/resolv.conf
# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
```

A green arrow points to the DHCP configuration lines. Below the terminal, the text reads: "Its the same process for DHCP we take out the '#' for the two lines underneath the heading".

Figure 4.5: Enable DHCP client

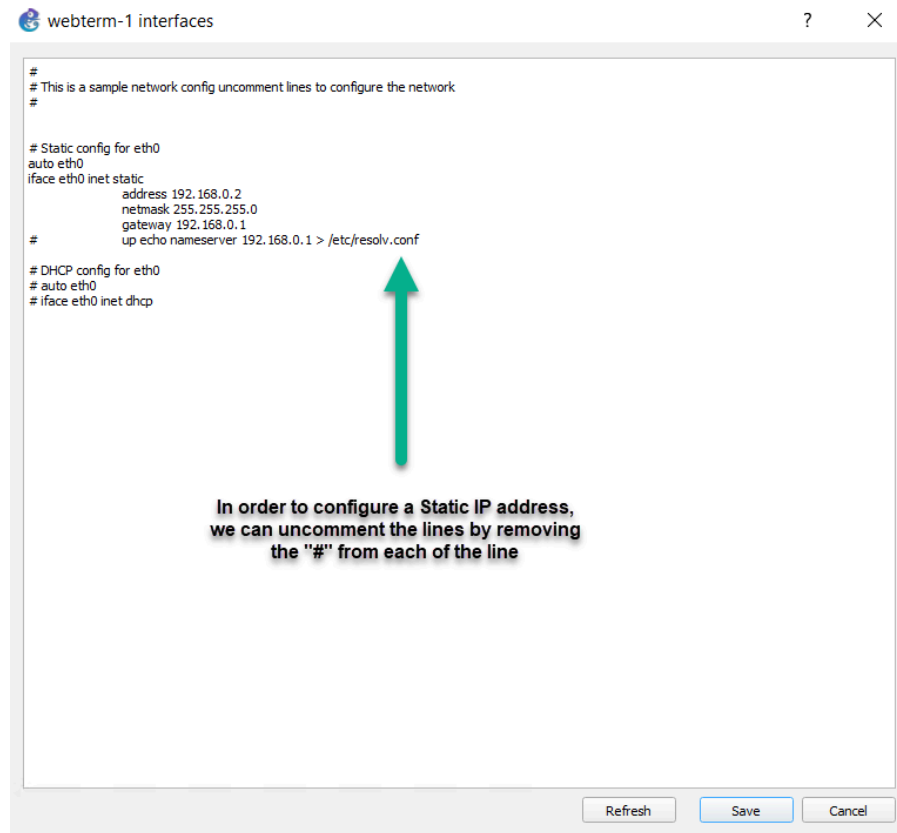


Figure 4.6: Configure a static IP address

2. Go to **User & Authentication > User Group > Create New:**

- Name: **VPN_GRP_A0ID**
- TYPE: **Firewall**

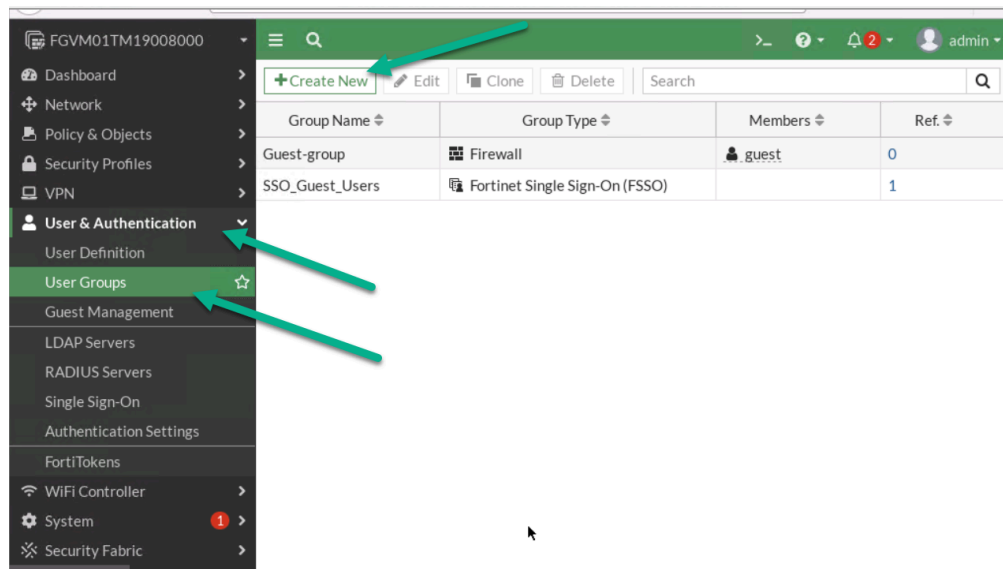


Figure 4.7: Create a user group

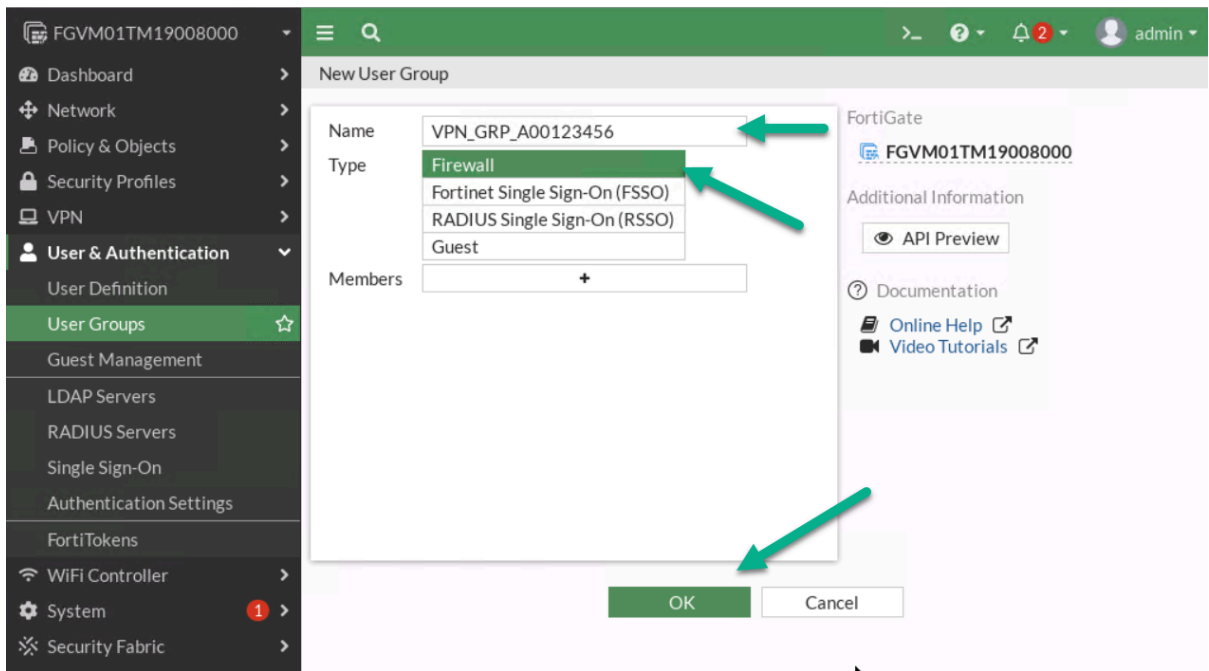


Figure 4.8: Create a group in the firewall

3. Go to **User & Authentication** > **User Definition** > **Create a User**:

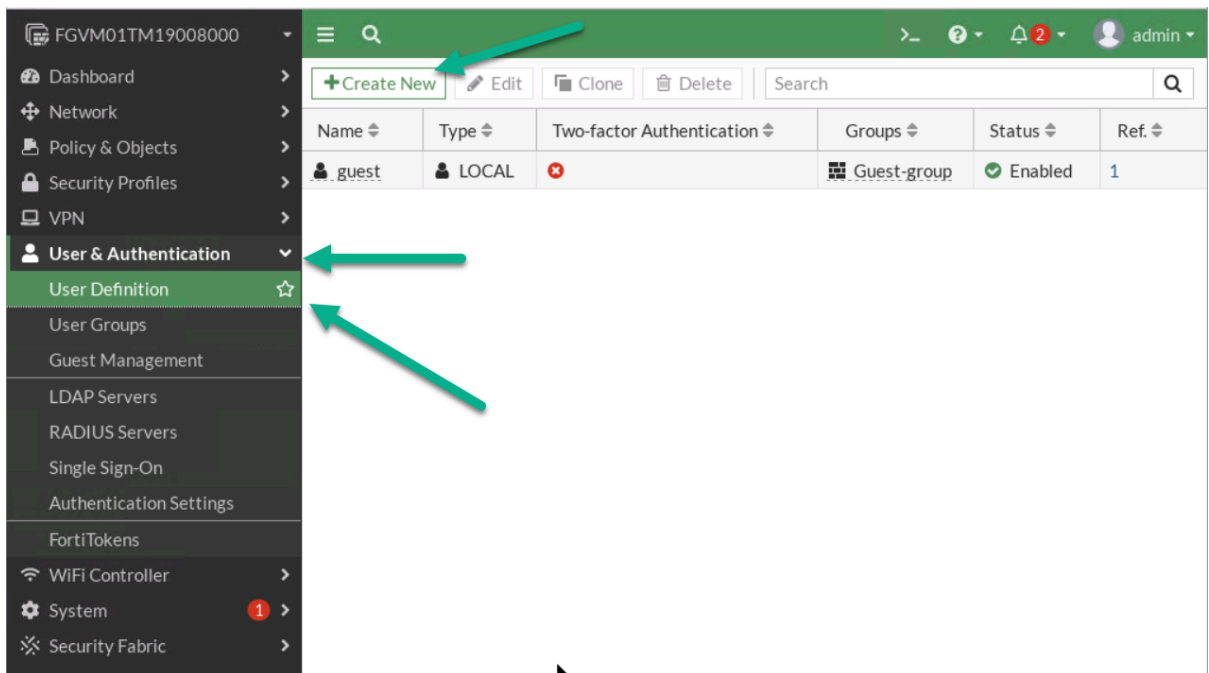


Figure 4.9: Create a new user

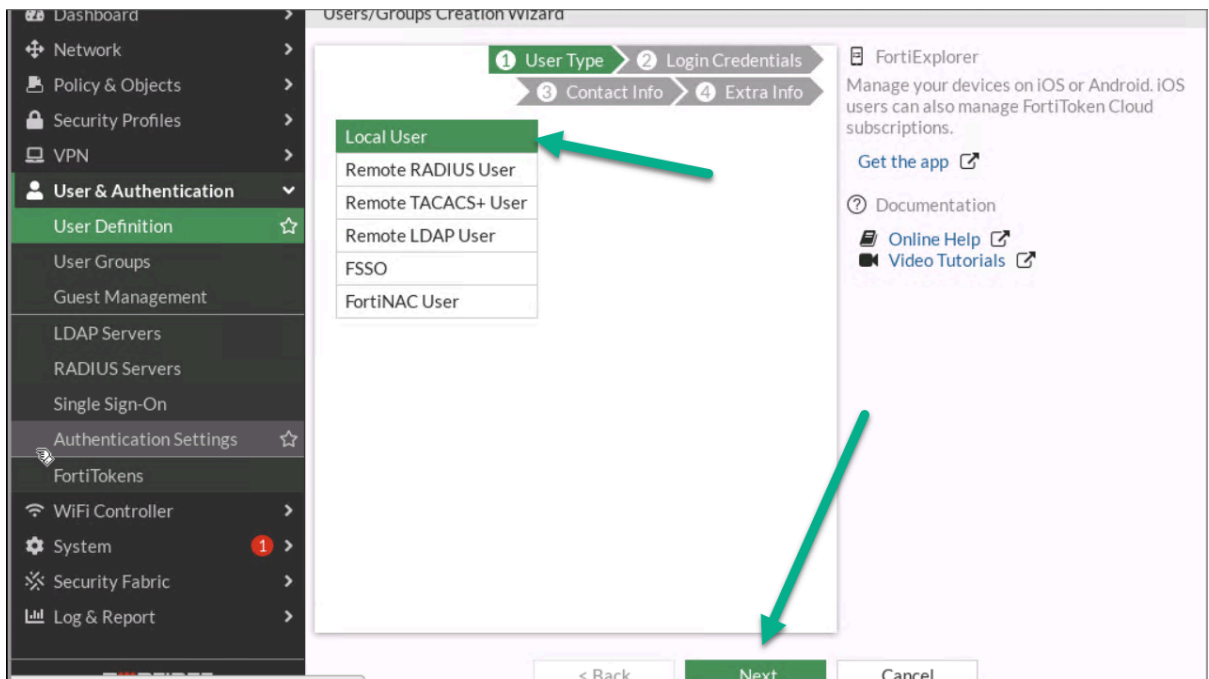


Figure 4.10: Create a local user

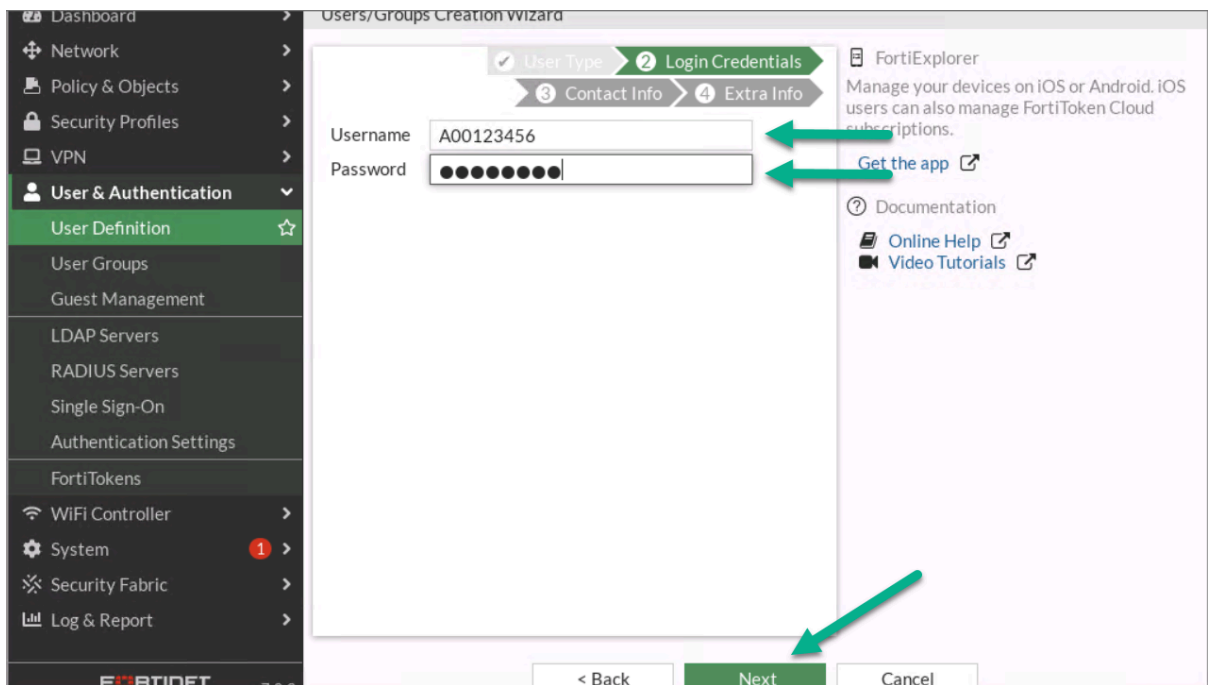


Figure 4.11: Configure login credentials for the user

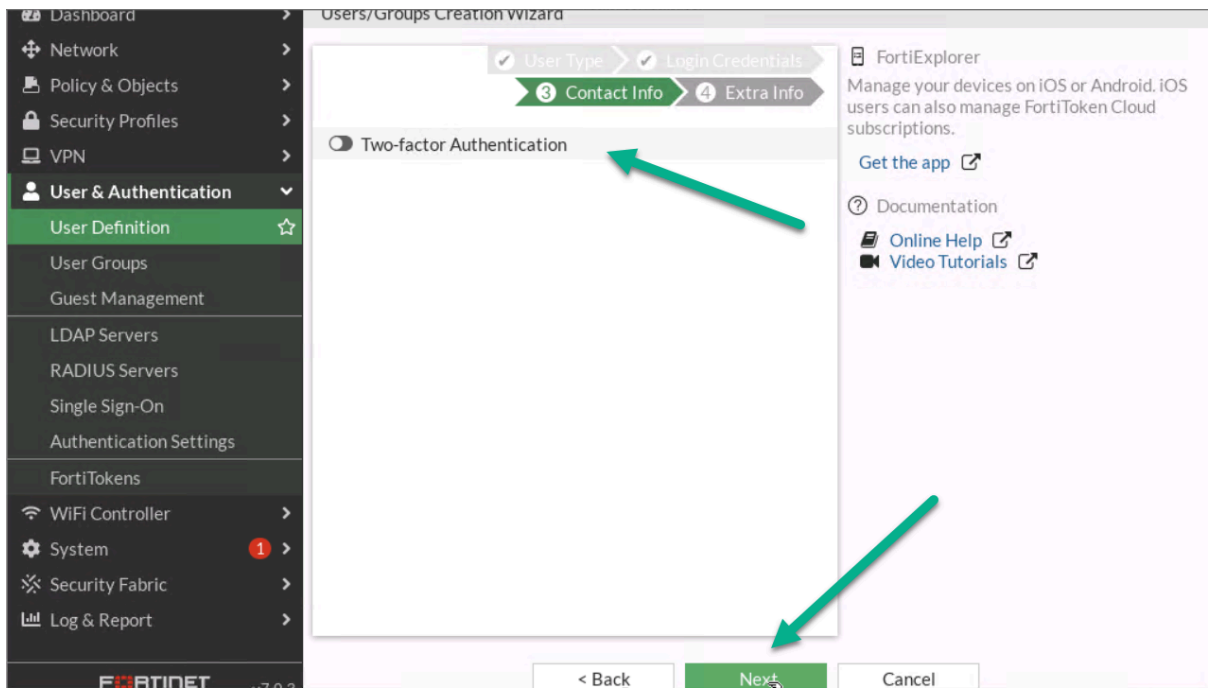


Figure 4.12: Contact info

4. Assign User Group to your profile.

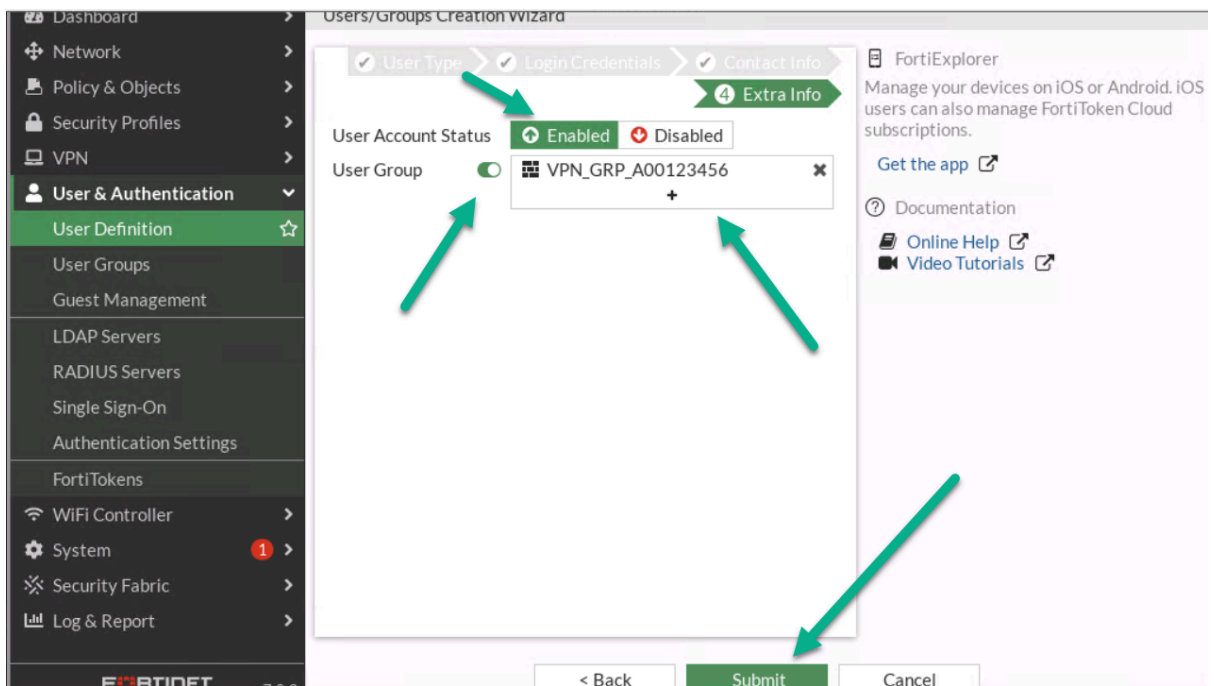


Figure 4.13: Assign a user to the group

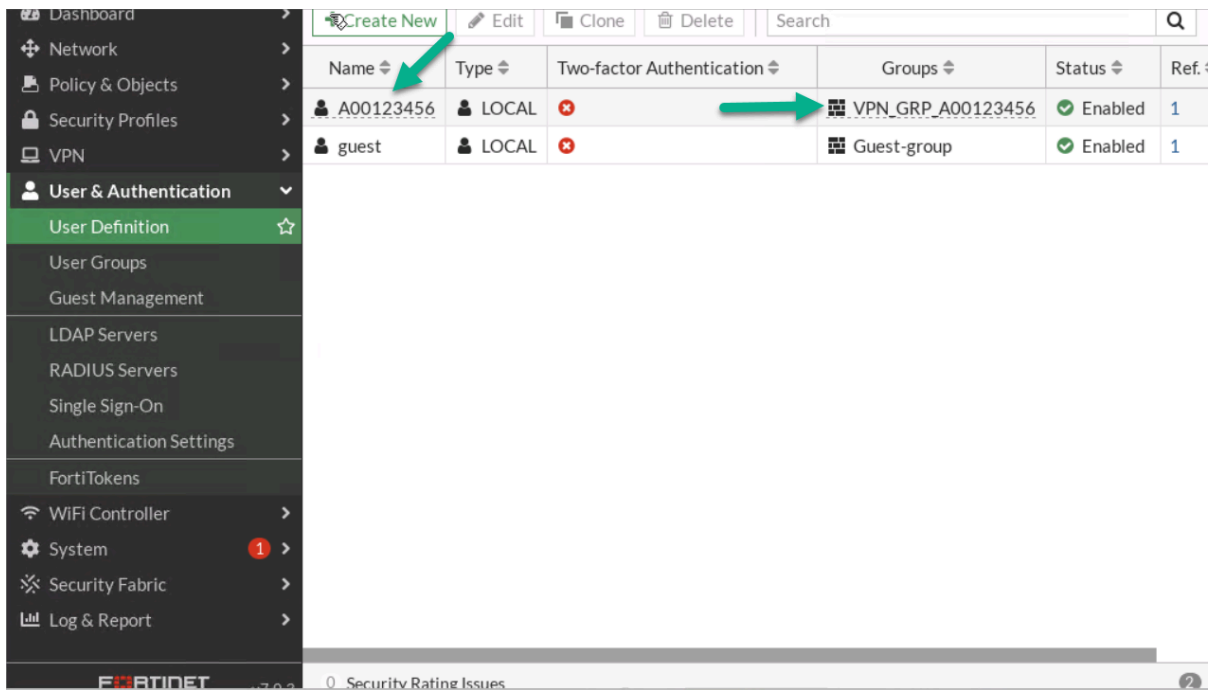


Figure 4.14: Verify configuration

5. Go to **VPN > IPsec Wizard**.

1. First:

- Select Name: **A0ID- VPN(A0ID is a student ID)**
- Template Type: **Remote Access**
- Remote Type Device: **FortiClient**

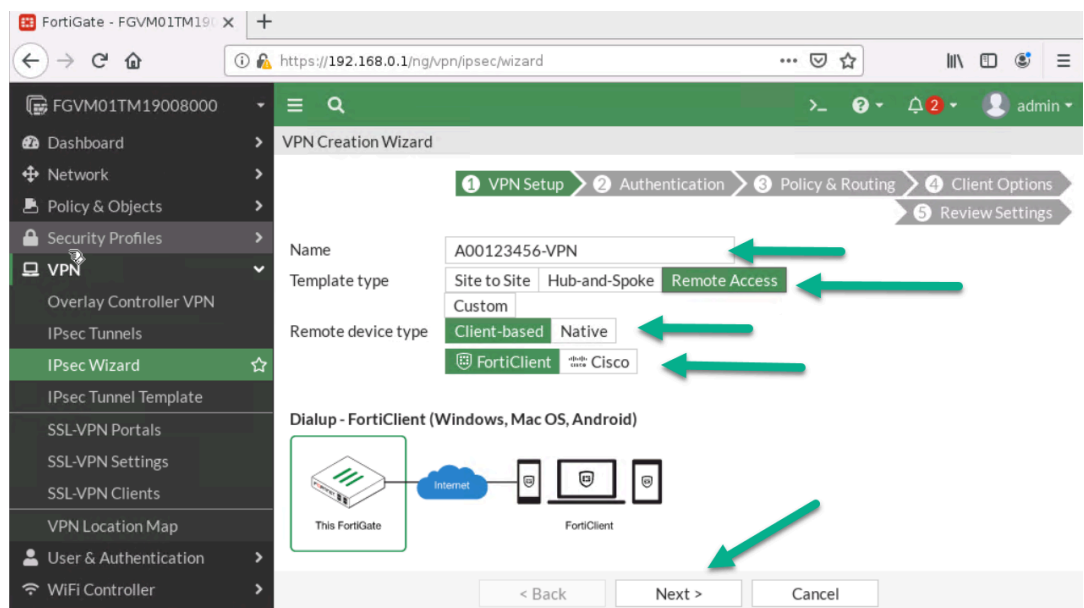


Figure 4.15: Create a VPN connection

2. Then:

- Incoming Interface: **Port1**
- Pre-shared Key: <Select a key like a password>
- User Group: **VPN_GRP_A0ID**

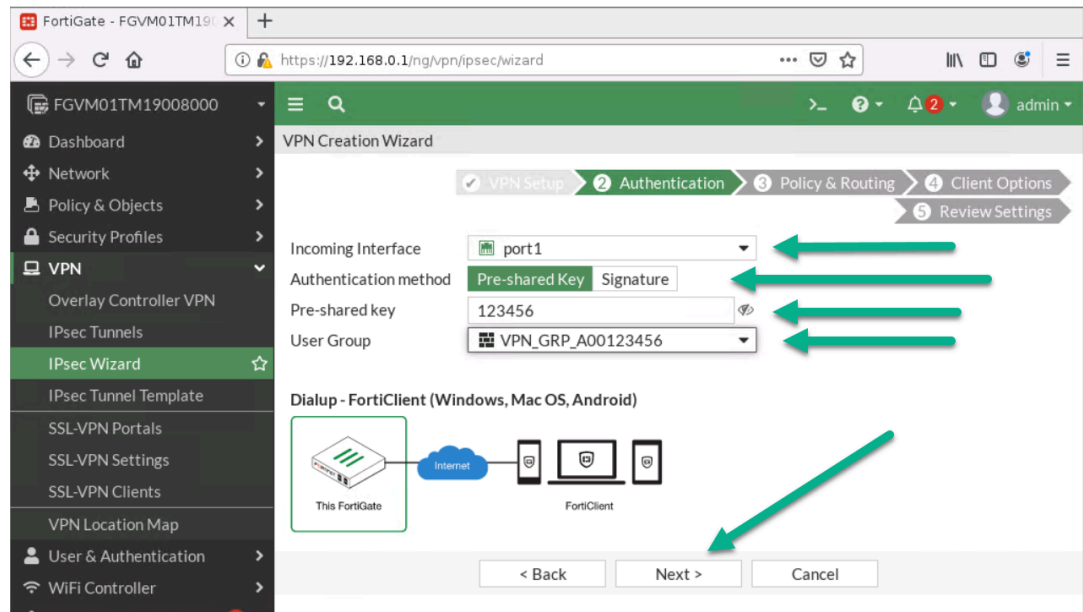


Figure 4.16: Configure authentication

3. Next:

- Local Interface: **Port 2**
- Local Address: Add your local range of IP address (192.168.0.0/24)
- Client Range: **172.16.0.1 to 172.16.0.10**
- Subnet Mask: **255.255.255.0**
- **Disable Split Tunneling**

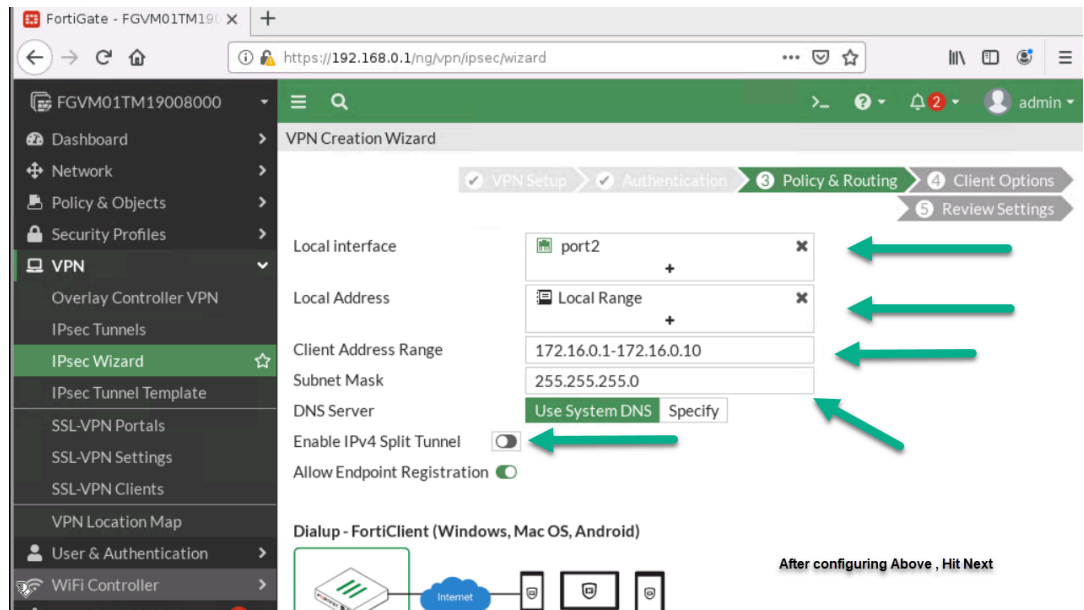


Figure 4.17: Configure Policy & Routing

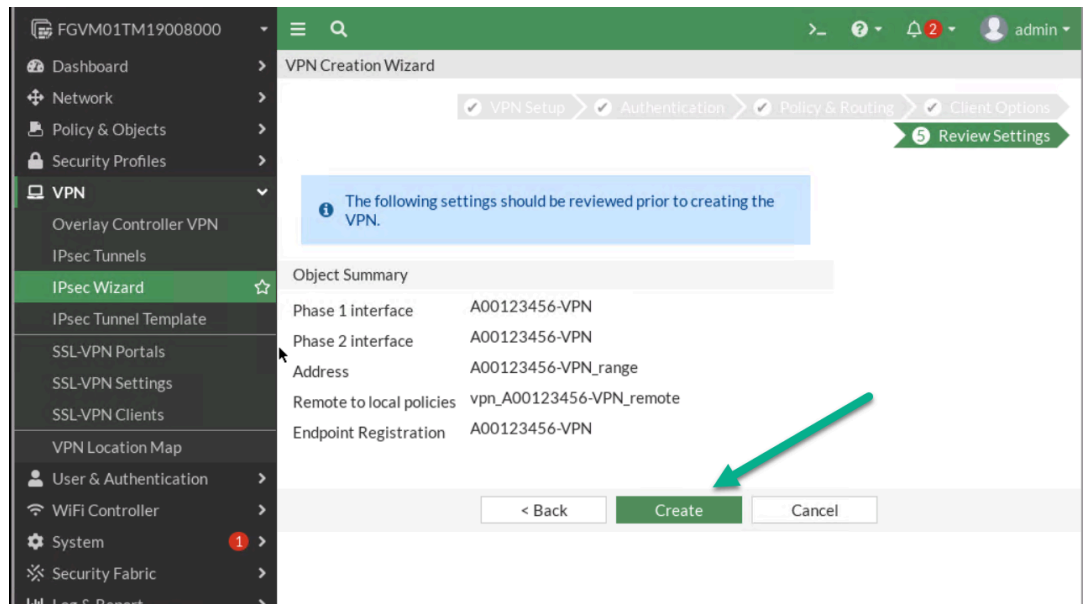


Figure 4.18: Review Settings

- On Windows machine, download FortiClient from Fortinet (<https://www.fortinet.com/products/endpoint-security/forticlient>). Install the FortiClient and configure IPsec as set in the previous steps. Your remote Gateway IP should be the Port1 IP address.

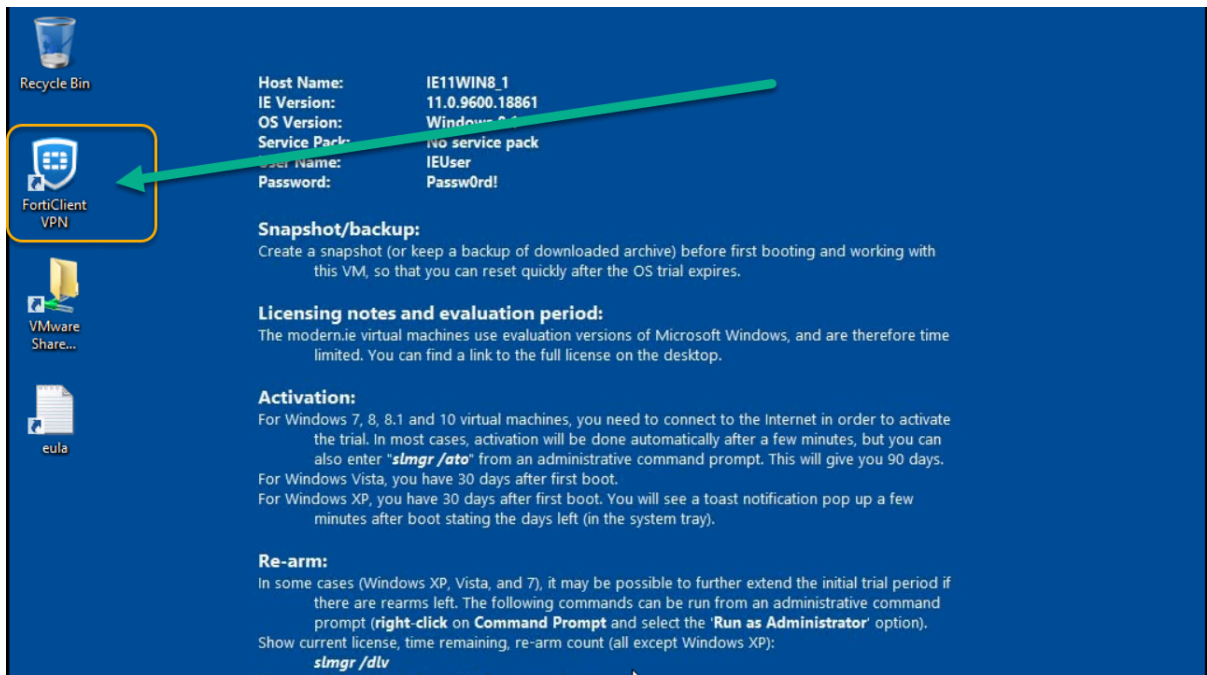
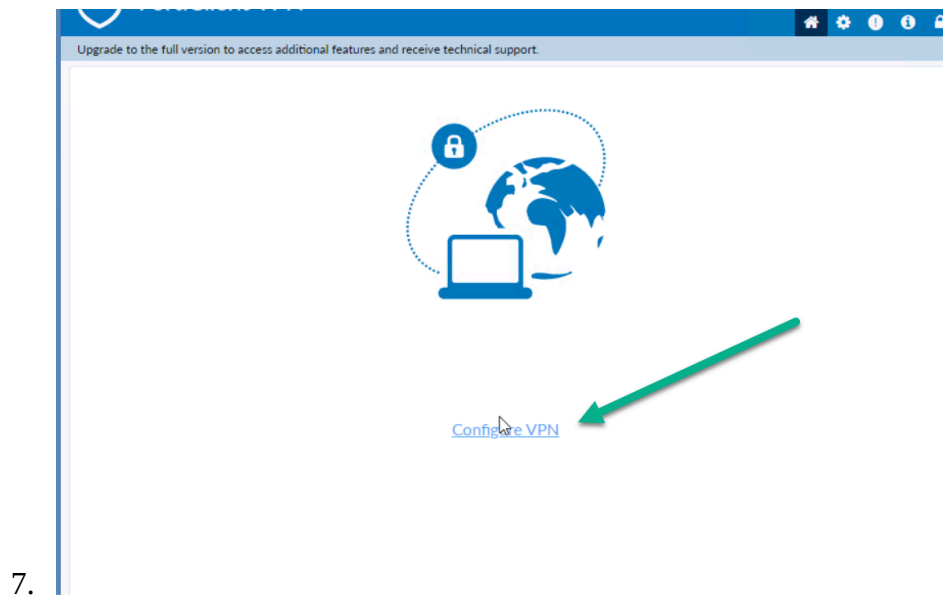


Figure 4.19: Install FortiClient on Windows



7.

Figure 4.20: Configure VPN in FortiClient

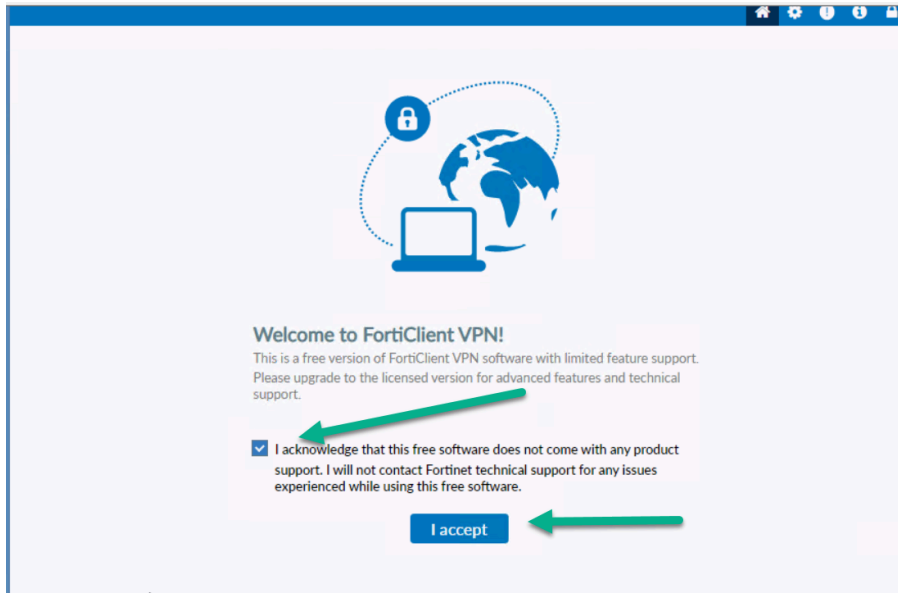


Figure 4.21: Accept FortiClient Free Licence

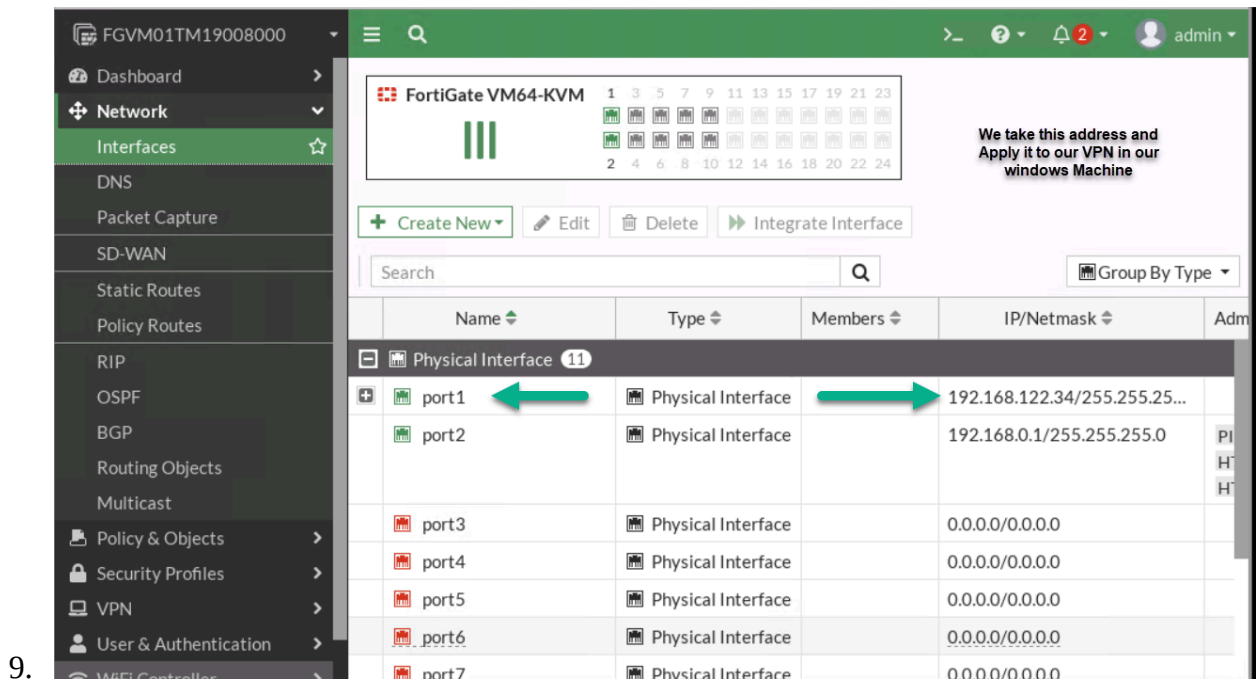
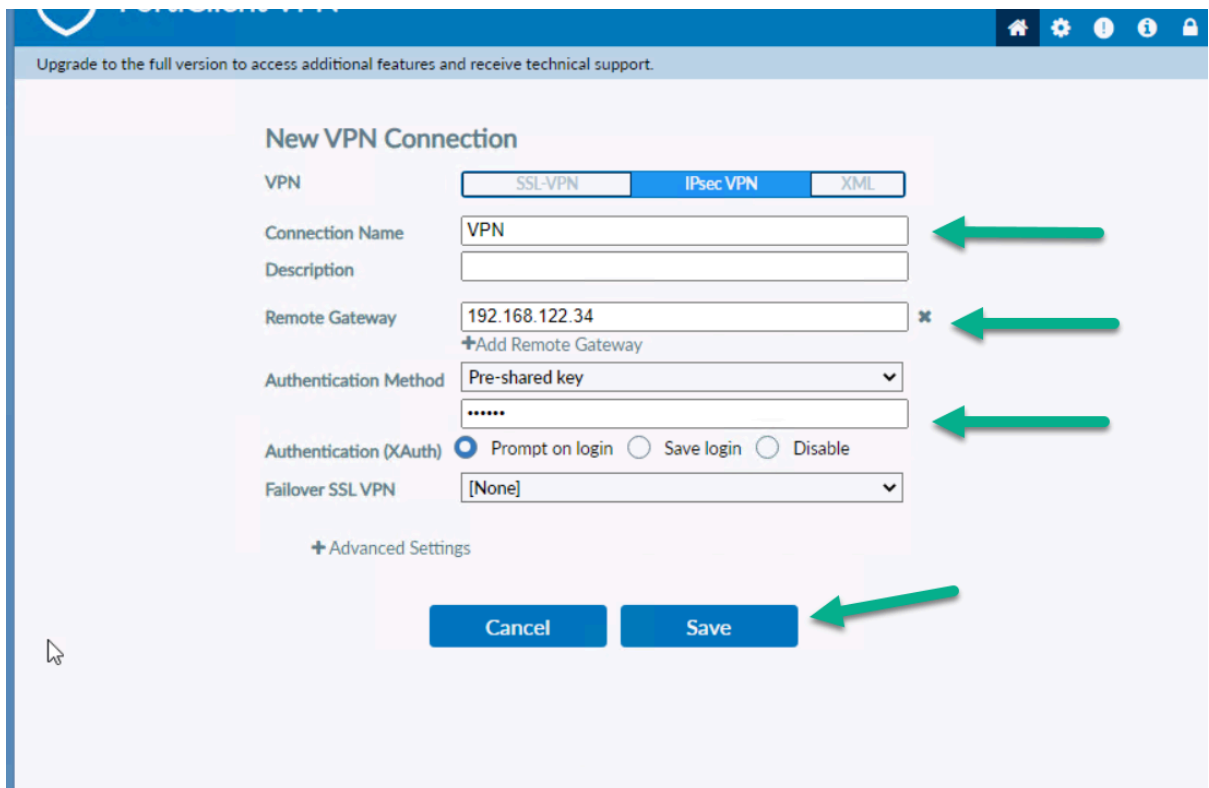


Figure 4.22: Port1 IP Address



10.

Figure 4.23: Configure FortiClient Remote Gateway and Pre-shared key

11. You should be able to ping from Windows to VPC.

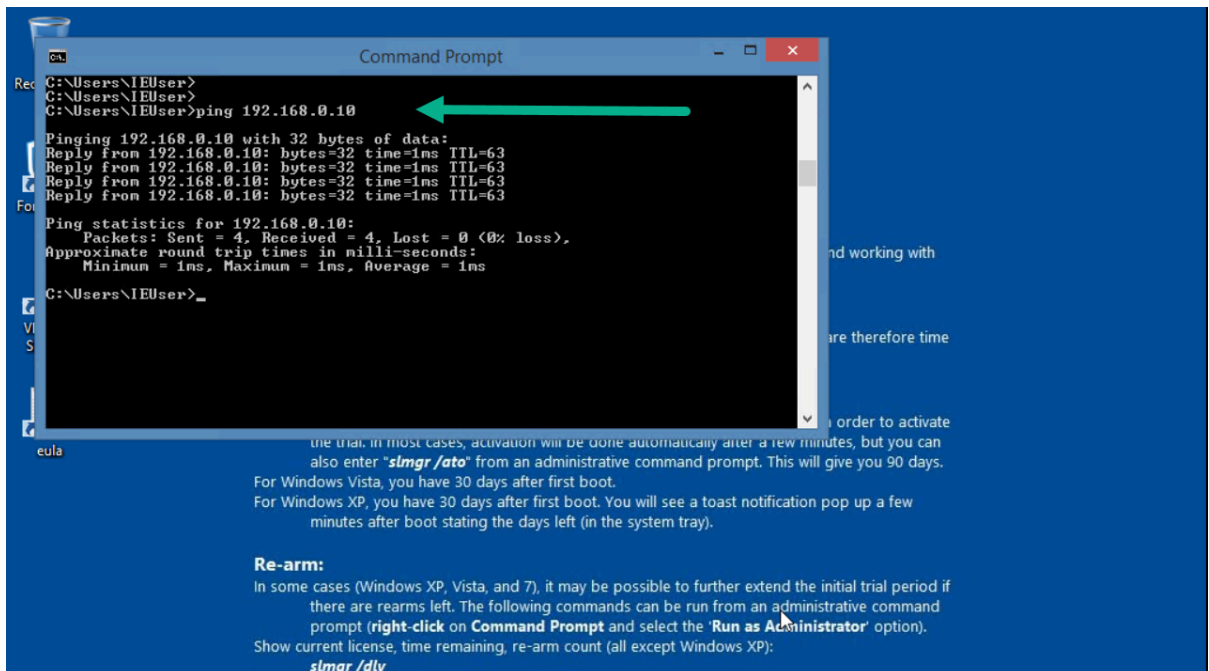


Figure 4.24: Verify configuration

Site-to-Site VPN (IPsec VPN)

Scenario: We are going to have IPsec VPN from WebTerm1 to WebTerm2. First, we are going to configure both firewalls through IPsec VPN Wizards and then we will verify connectivity from WebTerm1 to WebTerm2.

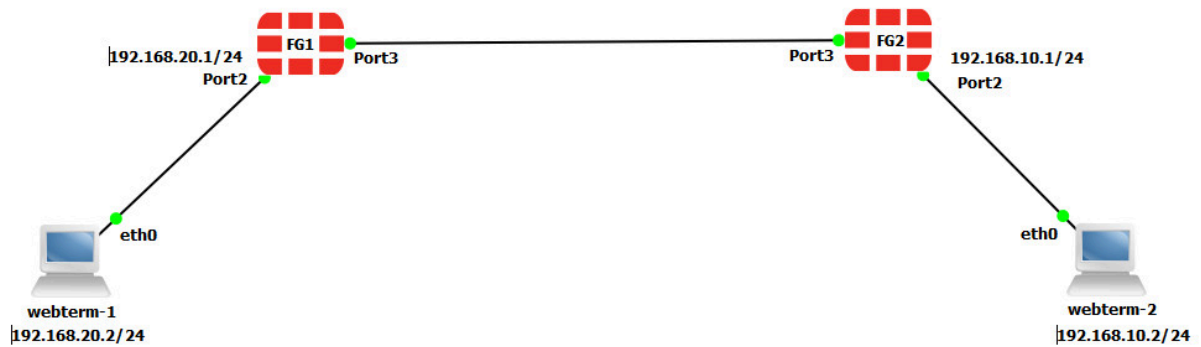


Figure 4.25: Main scenario

To validate Firewalls licences, we are going to connect them to the Internet.

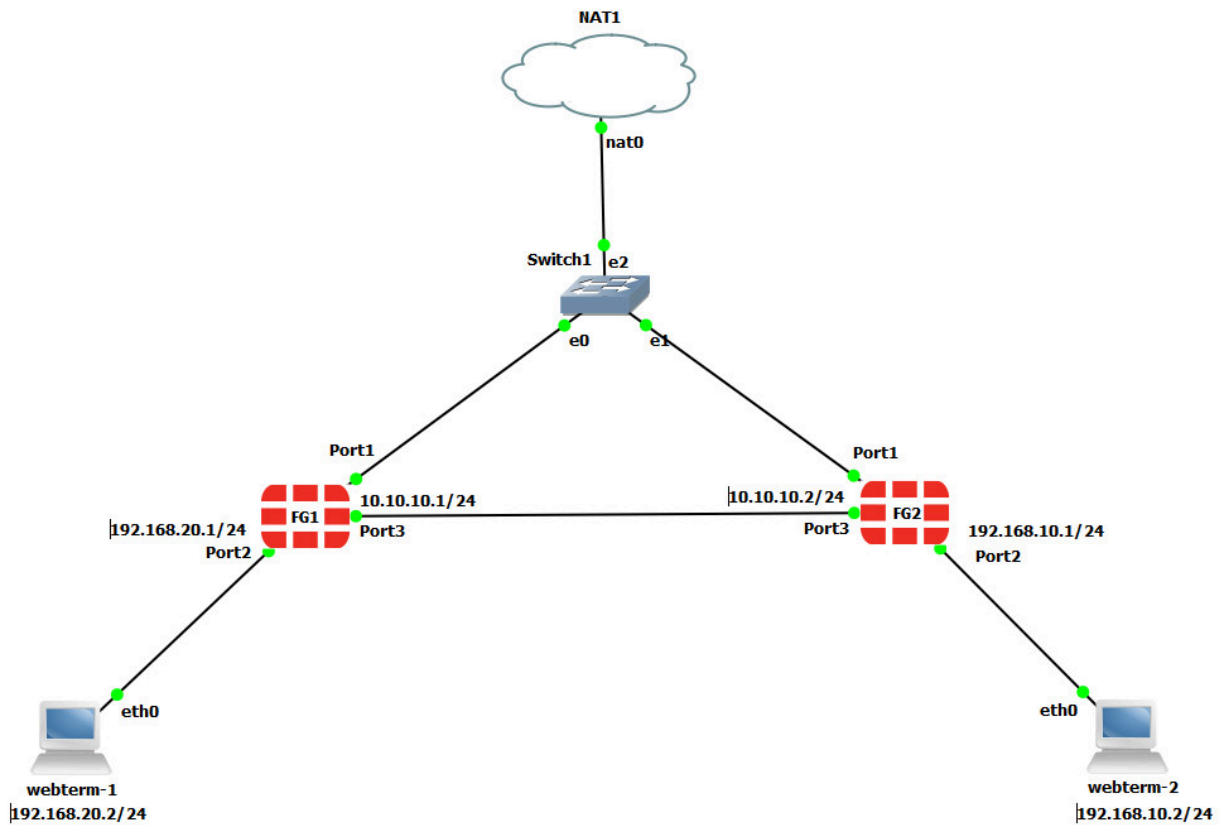


Figure 4.26: Validate firewall licences

Table 4.2: Devices configuration

Device	IP address	Access
Fortigate1	10.10.10.1/24	ICMP-HTTP-HTTPS
Fortigate2	10.10.10.2/24	ICMP-HTTP-HTTPS
WebTerm1	192.168.20.2/24	–
WebTerm2	192.168.10.2/24	–

1. On the FG1, go to **VPN > IPsec Wizard** and select Site to Site – FortiGate.

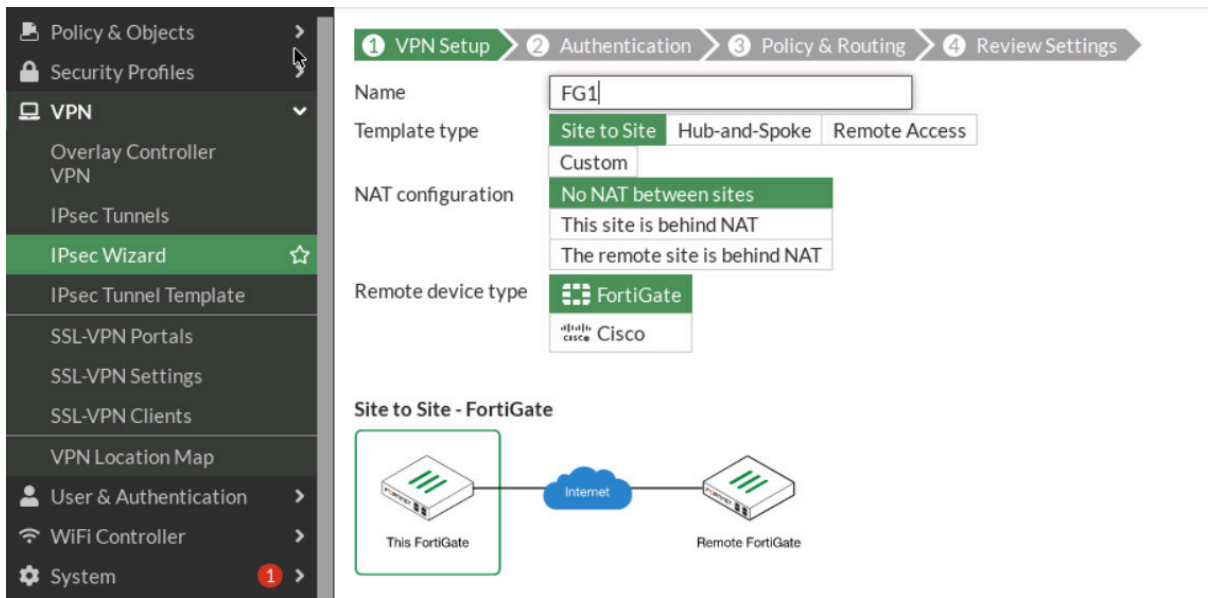


Figure 4.27: VPN Setup

2. Select **Site2Site/ FortiGate /No Nat**. Enter Remote IP: **10.10.10.2/24**, outgoing interface: **port3**.

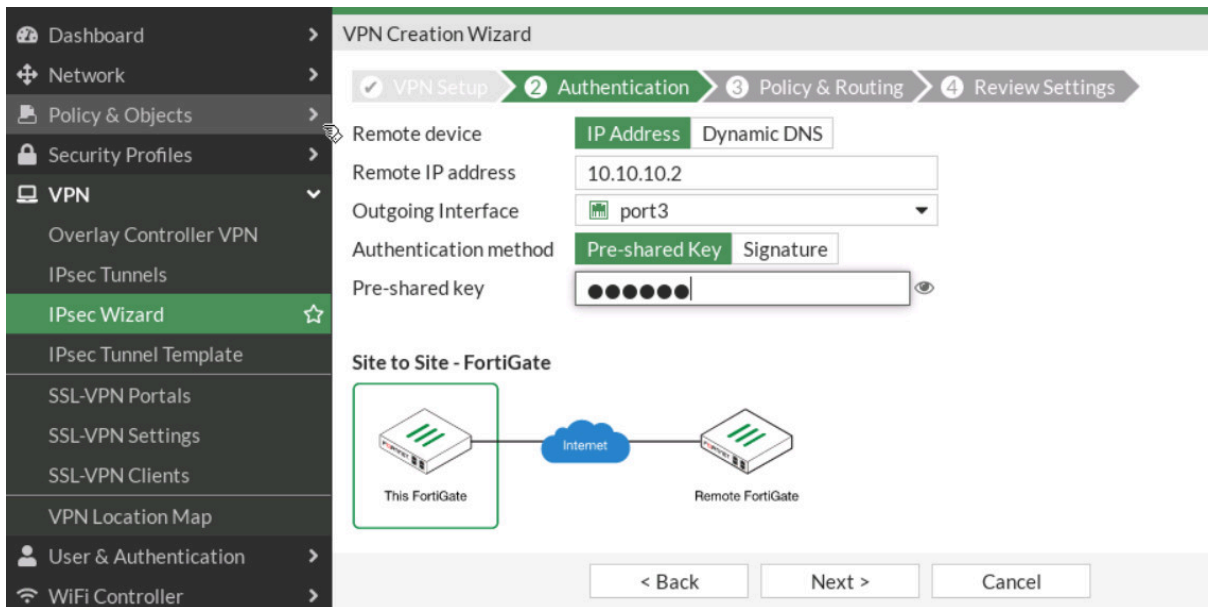


Figure 4.28: Authentication

3. Local Interface: port2, IP: **192.168.20.0/24**, Remote subnet: **192.168.10.0/24**. Through the wizard, FortiGate creates two policies and two static routes in the firewall.

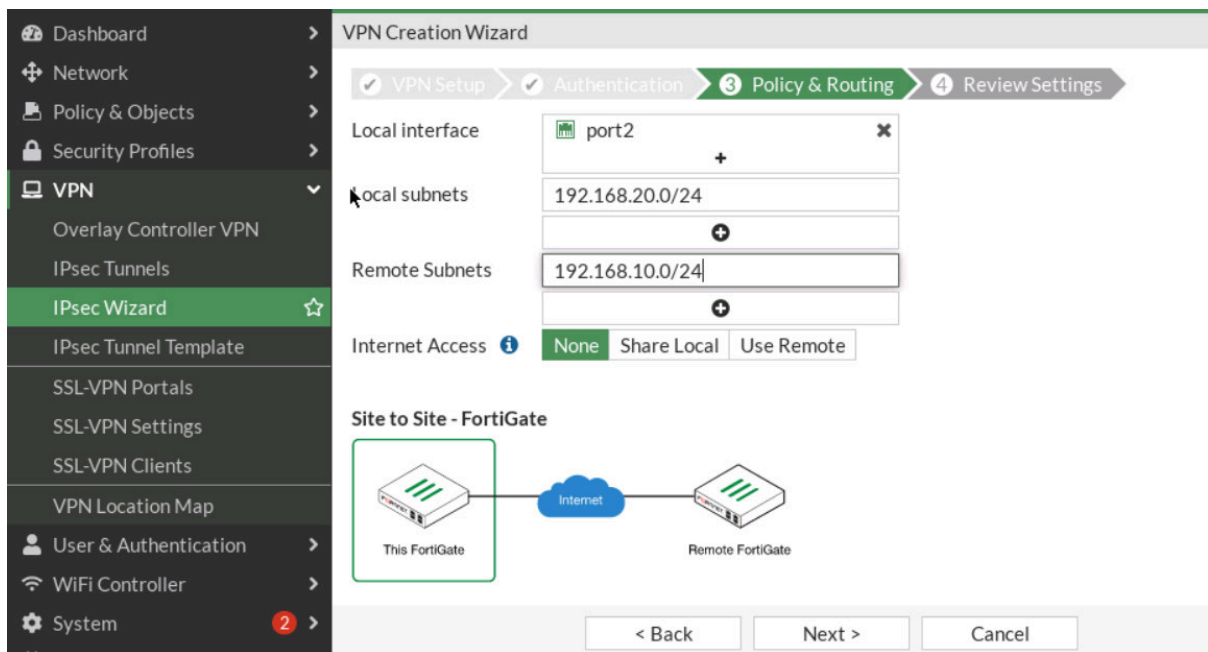


Figure 4.29: Policy & Routing

4. On the FG2, go to **VPN > IPsec Wizard** and select Site-to-Site – FortiGate.

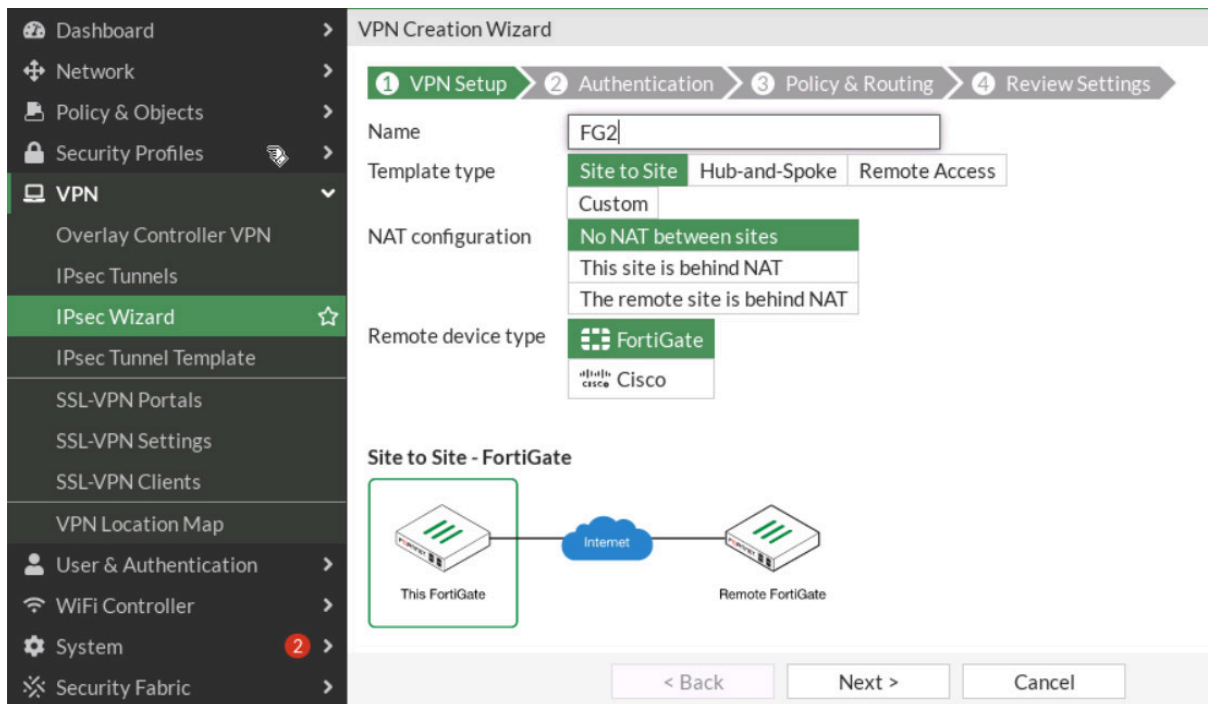


Figure 4.30: Set up FG2

5. Do the same configuration for FG2 (remote IP is 10.10.10.1/24 and local IP is 192.168.10.0/24).

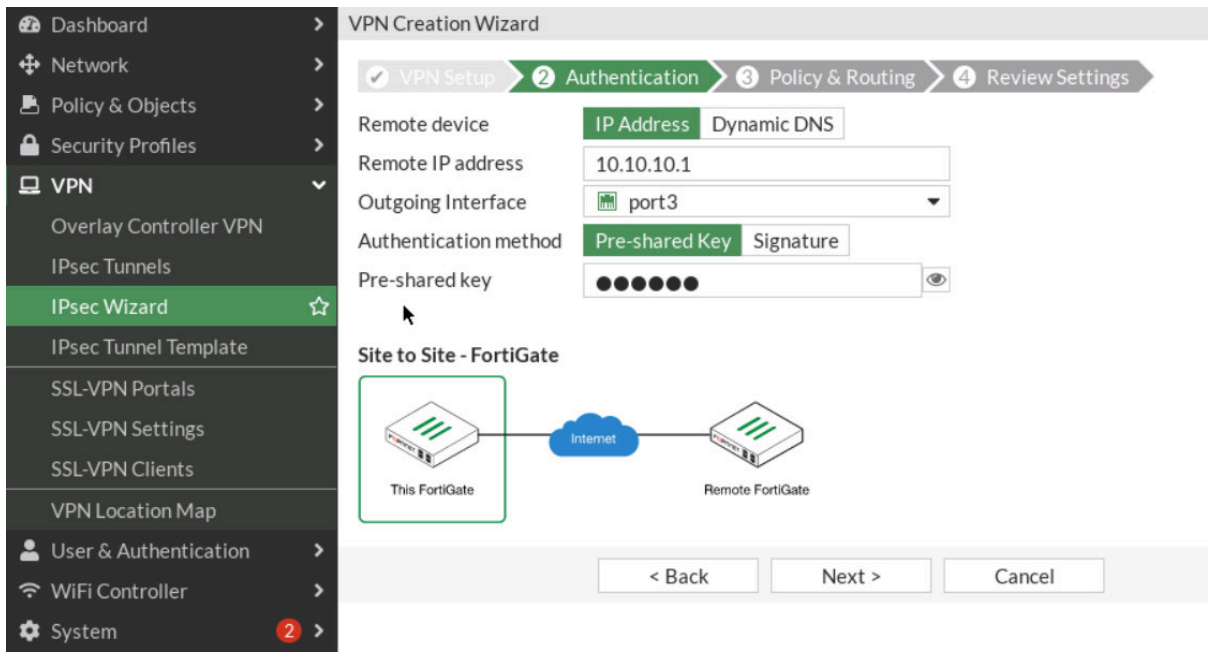
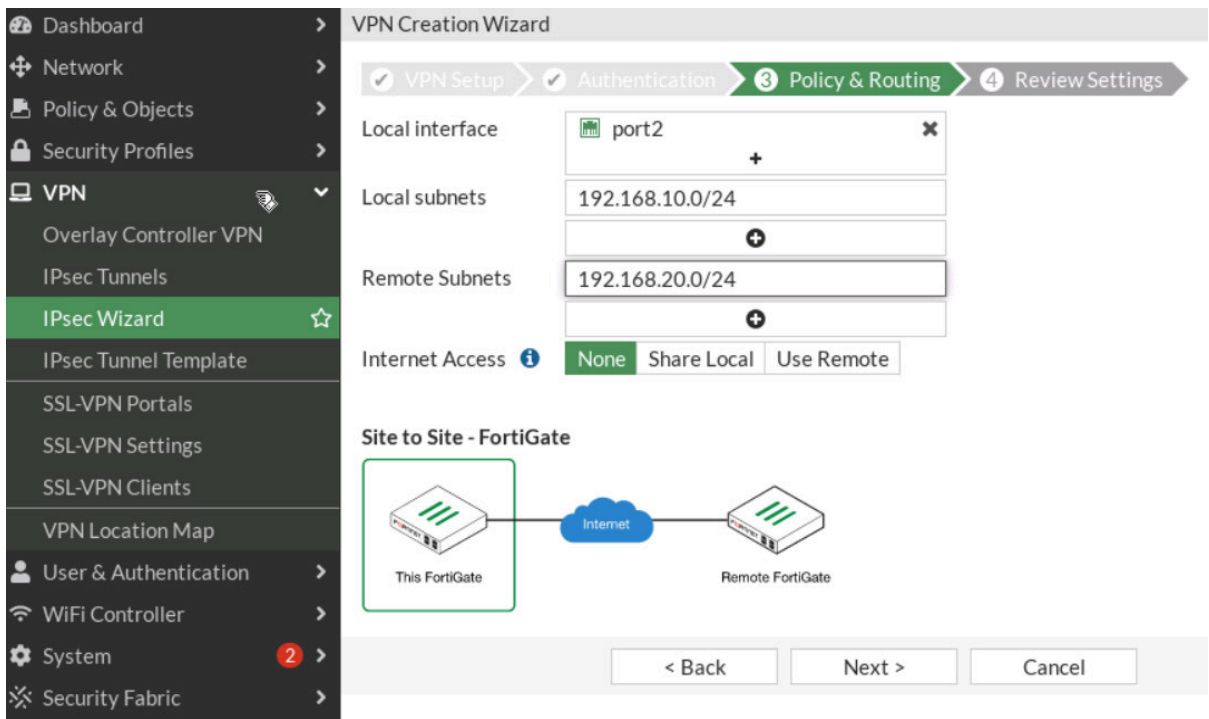


Figure 4.31: Authentication in FG2



6.

Figure 4.32: Policy & Routing in FG2

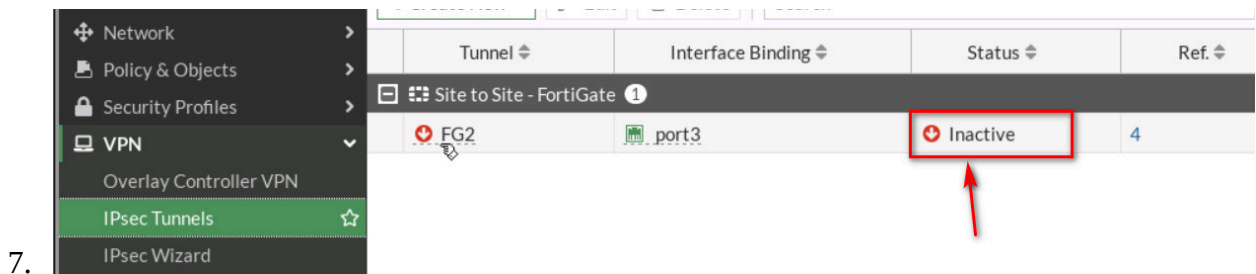


Figure 4.33: Configure IPsec Tunnels

Then, go to your IPsec Tunnels and double click on Inactive.

On the next windows, right click on the **tunnel > Bring UP > All Phase 2 selectors**. Then, your tunnel should be up!

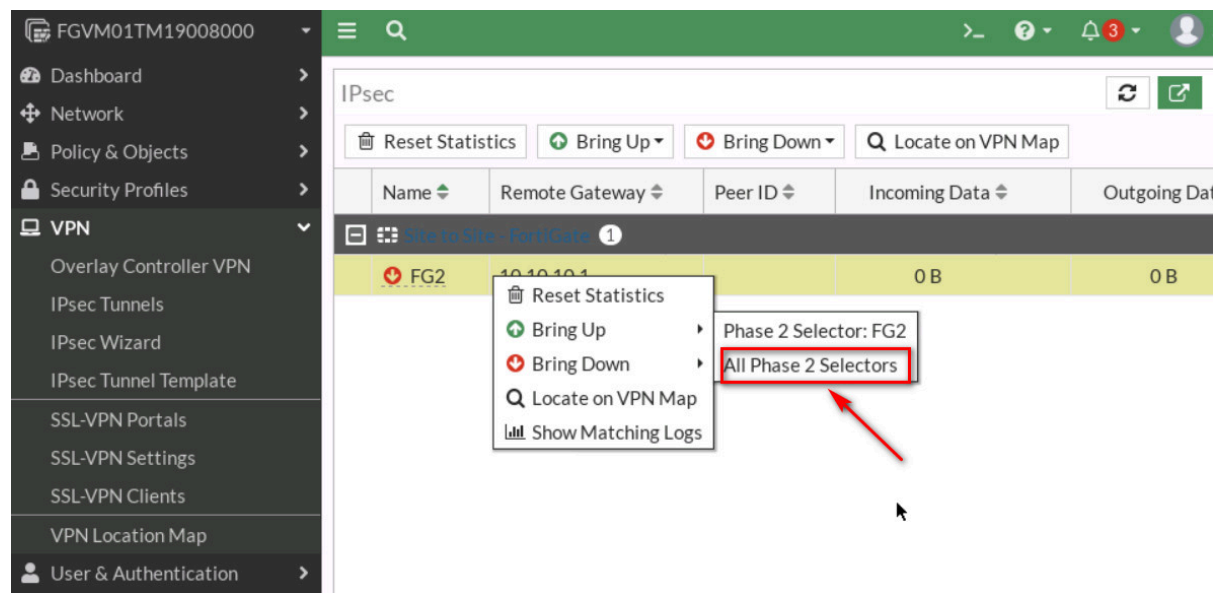


Figure 4.34: Bring up IPsec Tunnel

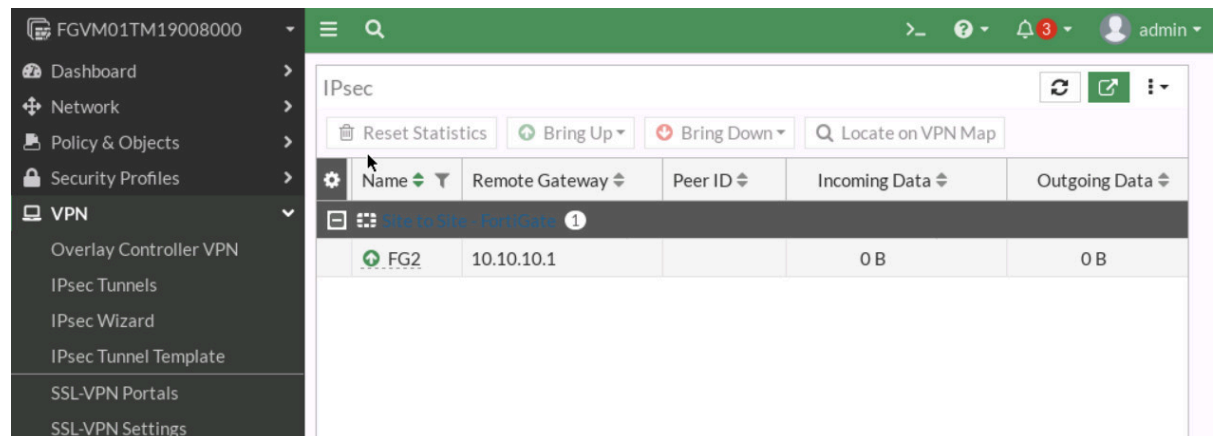


Figure 4.35: Verify the status of the tunnel

8. Go to **Logs & Reports > Event > VPN Event** and verify your configuration.

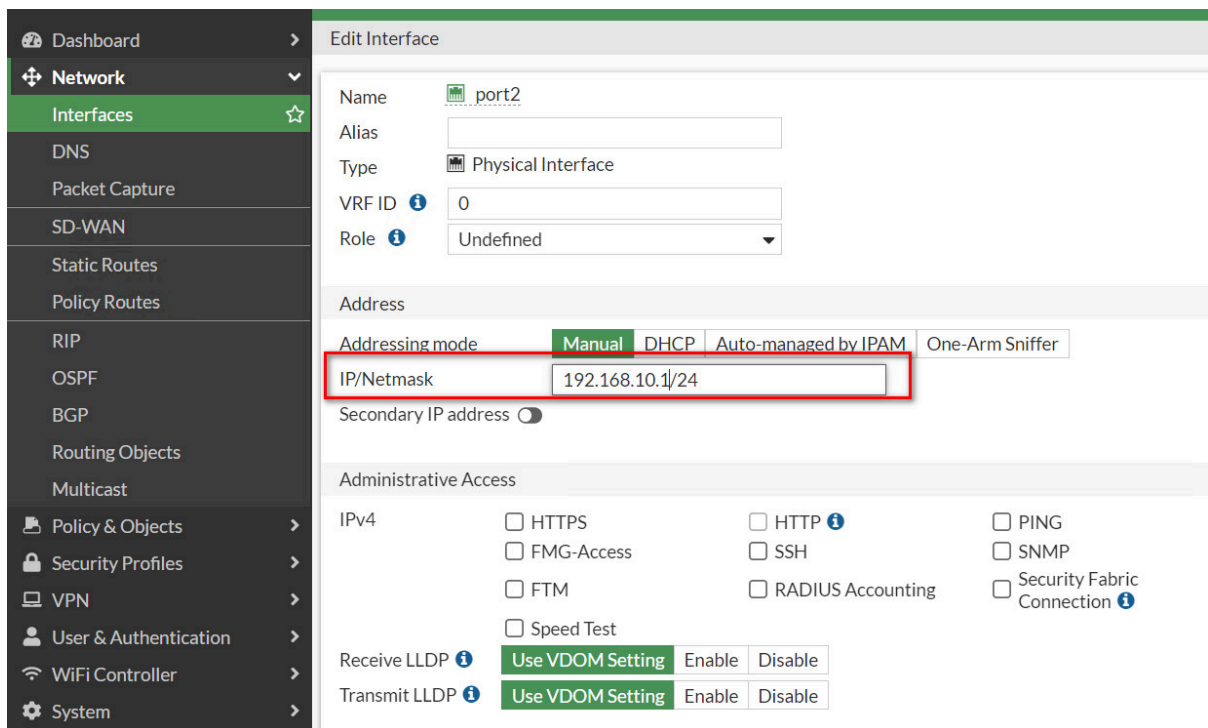


Figure 4.36: Verify configuration

You should be able to ping from WebTerm1 to WebTerm2.

```

LX Terminal
File Edit Tabs Help
root@webterm-1:~# ifconfig
eth0  Link encap:Ethernet  HWaddr 5a:3f:1e:c3:02:61
      inet addr:192.168.20.2 Bcast:0.0.0.0 Mask:255.255.255.0
      inet6 addr: fe80::583f:1eff:fec3:261/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
      RX packets:1434 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1411 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:889762 (868.9 KiB) TX bytes:167976 (164.0 KiB)

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:65536 Metric:1
      RX packets:3152 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3152 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:266304 (260.0 KiB) TX bytes:266304 (260.0 KiB)

root@webterm-1:~# ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=62 time=1.76 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=62 time=1.35 ms

```

Figure 4.37: Verify configuration

4.2 SSL VPN

Learning Objectives

- Configure a tunnel-based SSL VPN
- Configure a web-based SSL VPN (Web Portal)

Scenario: We are going to have SSL VPN from Windows to FortiGate Firewall. First, we will install FortiClient on Windows and then we will configure the firewall for FortiClient. We have two types of SSL VPN, Web based mode and Tunnel mode. Web based mode doesn't need any agents and you should be able to reach WordPress and SSH Server from Windows. Tunnel mode is through FortiClient. The goal of this scenario is to have connectivity from Windows to WordPress and SSH Server.

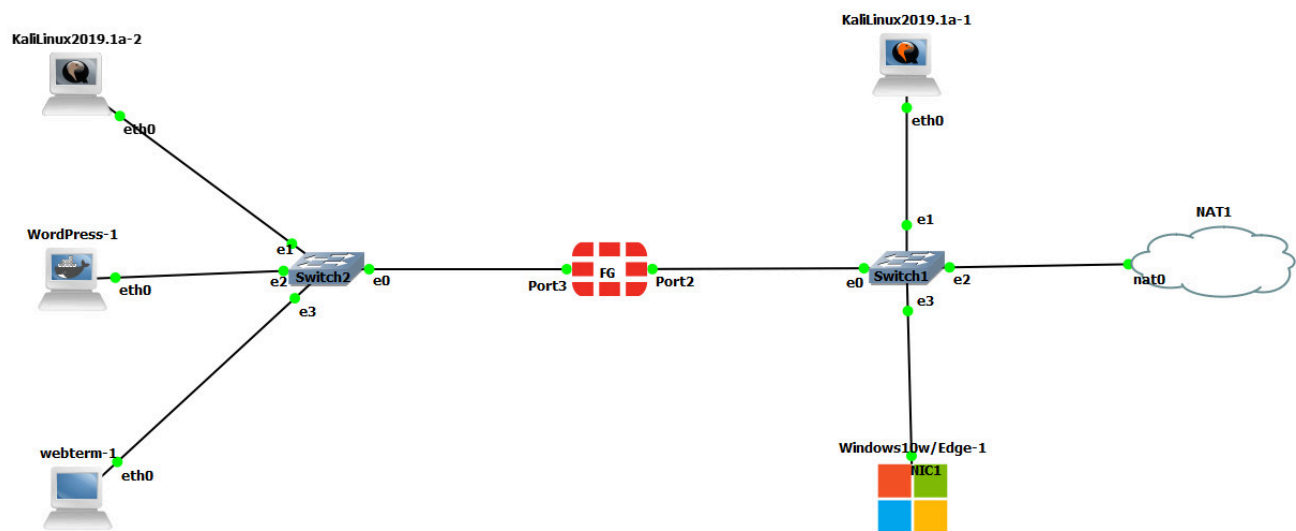


Figure 4.38: Main scenario

Table 4.3: Devices configuration

Device	IP address	Access
FortiGate	Port3: 192.168.1.1/24 – DHCP (192.168.1.20 to 192.168.1.30) Port2: DHCP Client	ICMP-HTTP-HTTPS
WebTerm (FMC)	192.168.1.2/24	–
KALI Linux (SSH Server)	192.168.1.3/24	–
WordPress	192.168.1.4/24	
KALI-outside	DHCP Client	
Windows	DHCP Client	

Configure the interfaces of the firewall. Port2 and Port3 should be configured in the terminal to access the firewall.

1. Port 3 Configuration:

```
FGVM01TM19008000 # config system interface
FGVM01TM19008000 (interface) # edit port3
FGVM01TM19008000 (port3) # set ip 192.168.1.1/24
FGVM01TM19008000 (port3) # set allowaccess http https
FGVM01TM19008000 (port3) # end
FGVM01TM19008000 #
```

Figure 4.39: Port3 settings

2. Port 2 Configuration:

```
FGVM01TM19008000 # config system interface
FGVM01TM19008000 (interface) # edit port2
FGVM01TM19008000 (port2) # set mode dhcp
FGVM01TM19008000 (port2) # end
```

Figure 4.40: Port2 settings

3. Configure DHCP Server on port3.

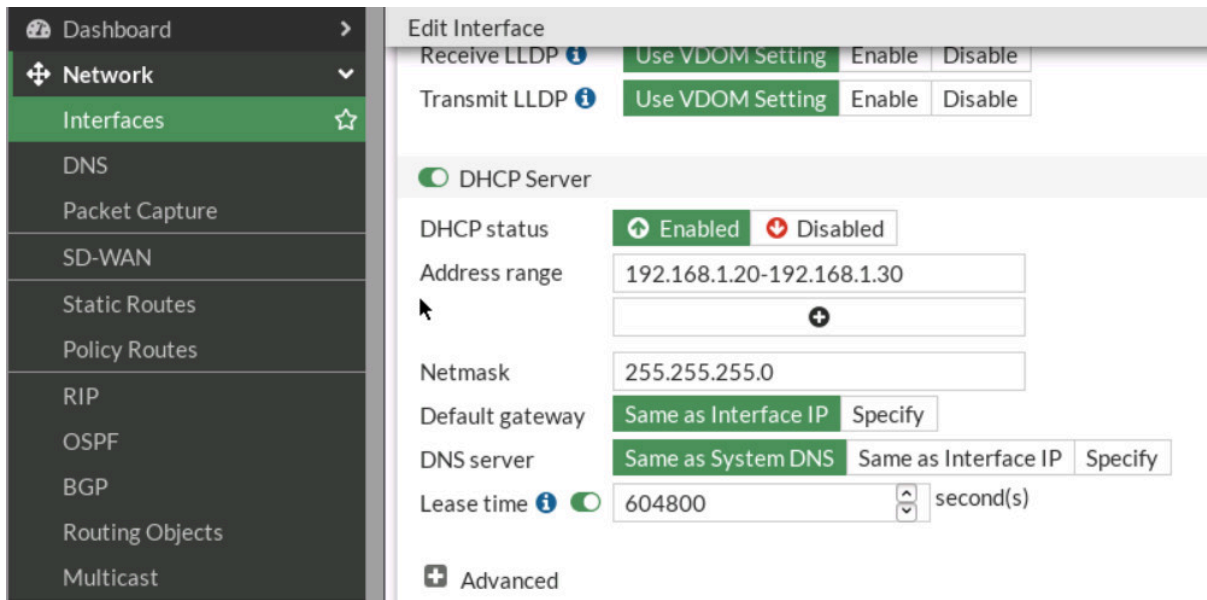


Figure 4.41: Enable DHCP Server on port3

- Configure user and user group. Go to **User & Authentication** > **User Definition** to create a local user **sslypnuser1**.

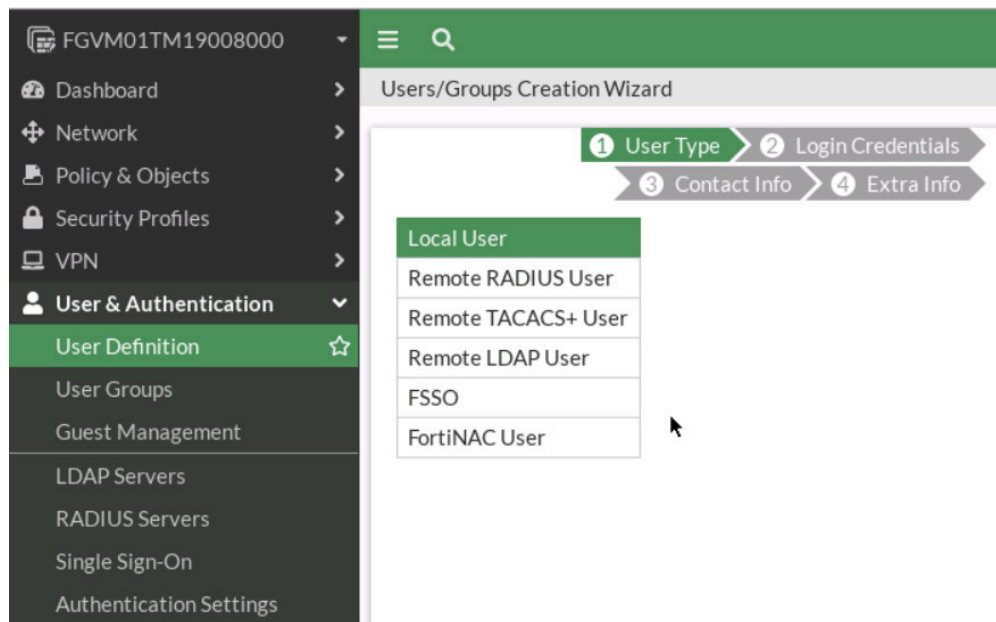


Figure 4.42: Create a local user

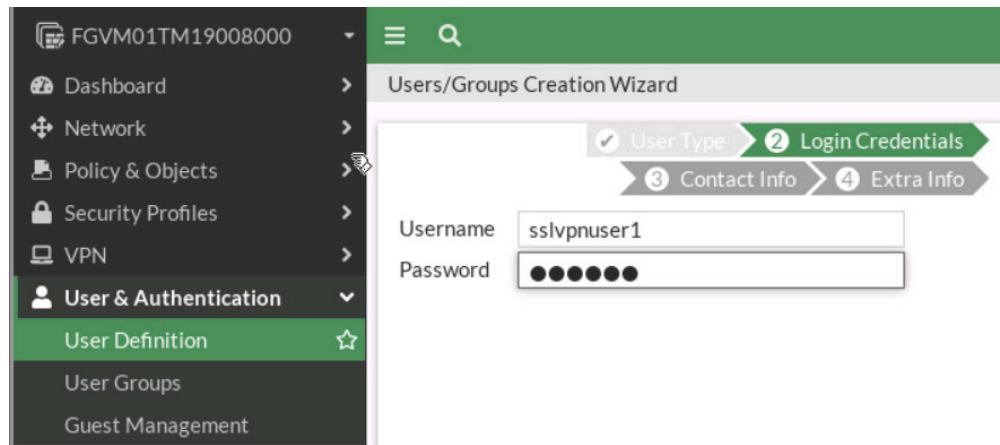


Figure 4.43: Configure login credentials

Go to **User & Authentication** > **User Groups** to create a group **sslvpngroup** with the member **sslvpnuser1**.

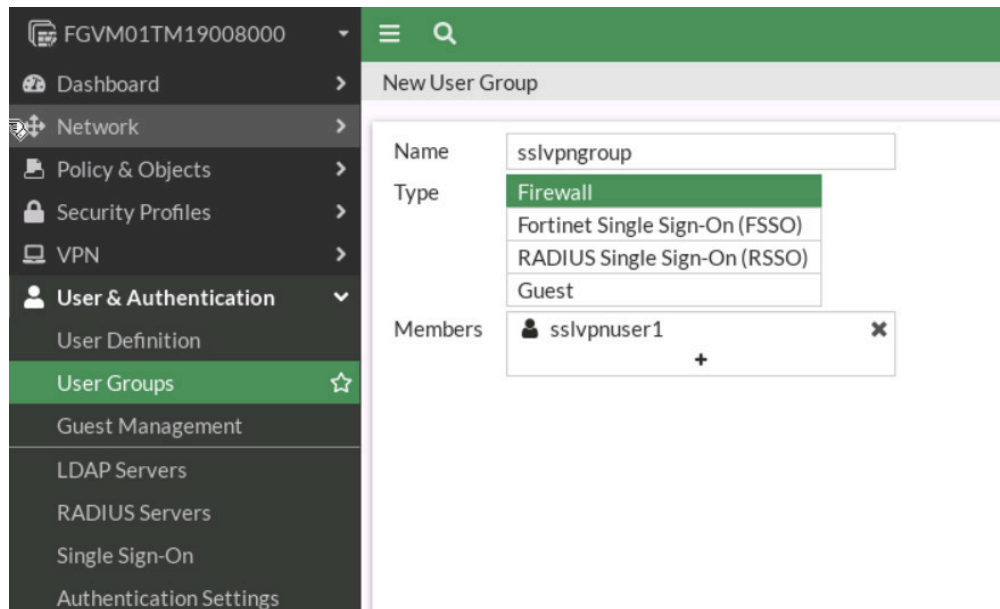


Figure 4.44: Create a group

5. Configure SSL VPN web portal and Tunnel mode. Go to **VPN** > **SSL-VPN Portals**:

- **Split-Tunneling**: Disabled
- **Source IP Pools**: SSLVPN_TUNNEL_ADDR1

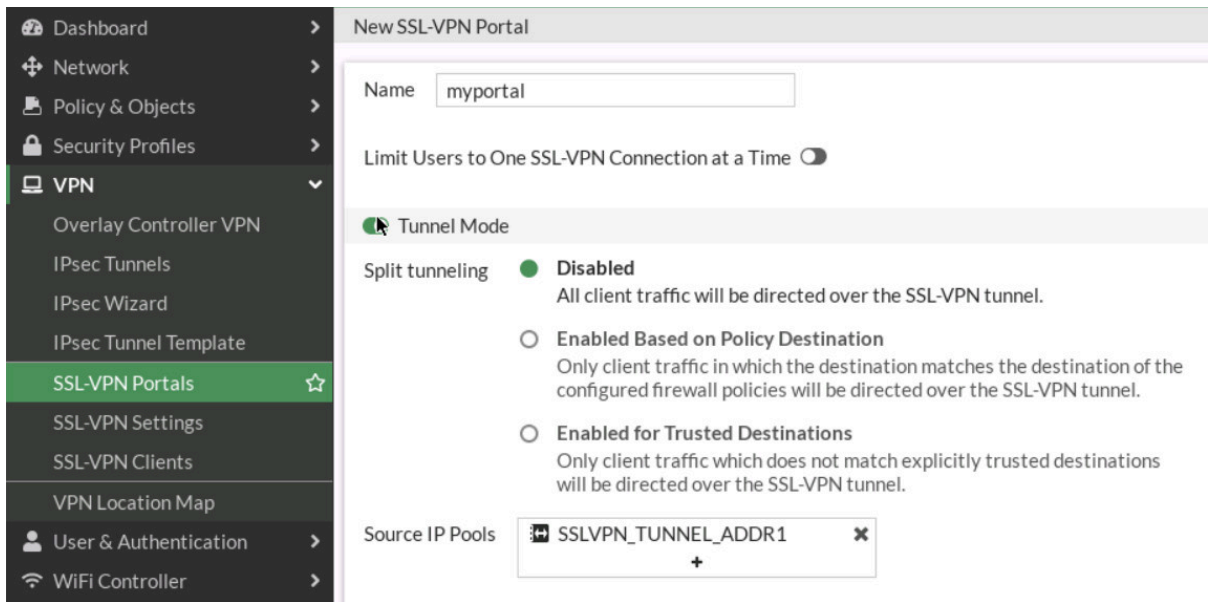


Figure 4.45: SSL-VPN Portal

Go to **VPN > SSL-VPN Portals**, add KALI IP address (SSH Server: *IP Address of Kali*) and WordPress (*IP Address of WordPress*) in the bookmark section.

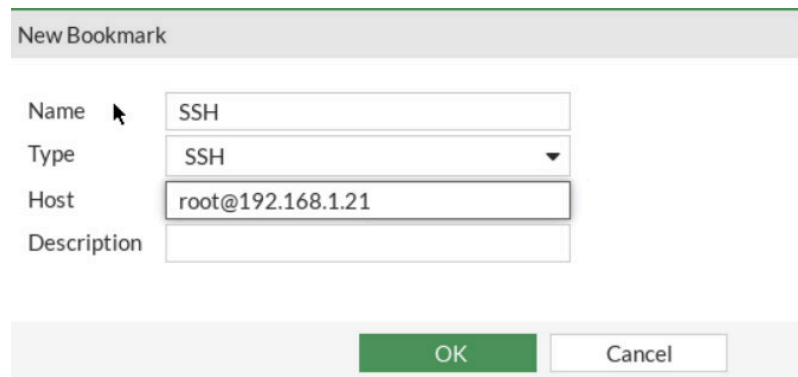


Figure 4.46: Create an SSH bookmark

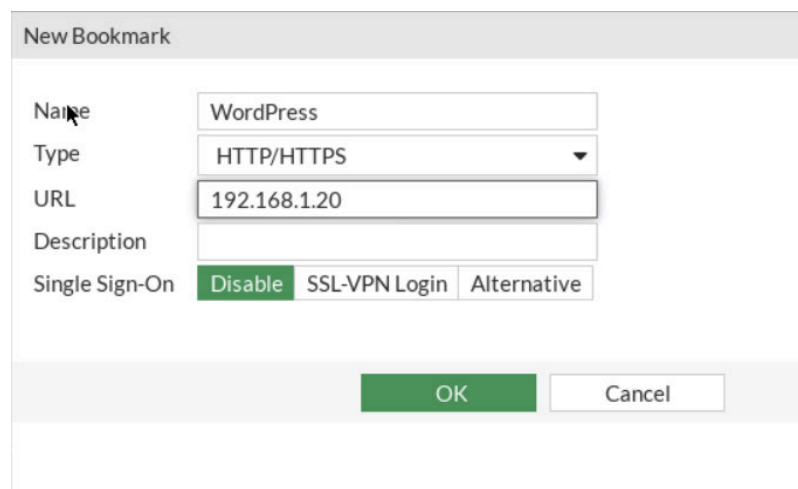


Figure 4.47: Create an HTTP/HTTPS bookmark

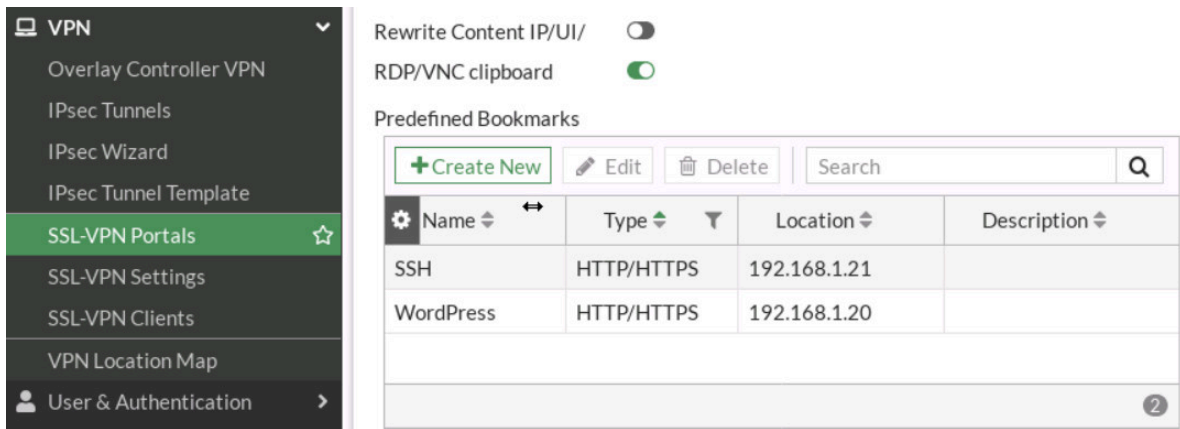


Figure 4.48: Bookmark settings

6. Configure SSL VPN settings. Go to **VPN > SSL-VPN Settings**:

- For Listen on Interface(s), select Port2.
- Set Listen on Port to 8080.
- Server Certificate: Fortinet
- In restrict Access, select “Allow access from any host”
- Address range: **Automatically assign address.**
- In Authentication/Portal Mapping All Other Users/Groups, set the Portal to **MyPortal**
- Create new Authentication/Portal Mapping for group **sslvpngroup** mapping portal MyPortal.

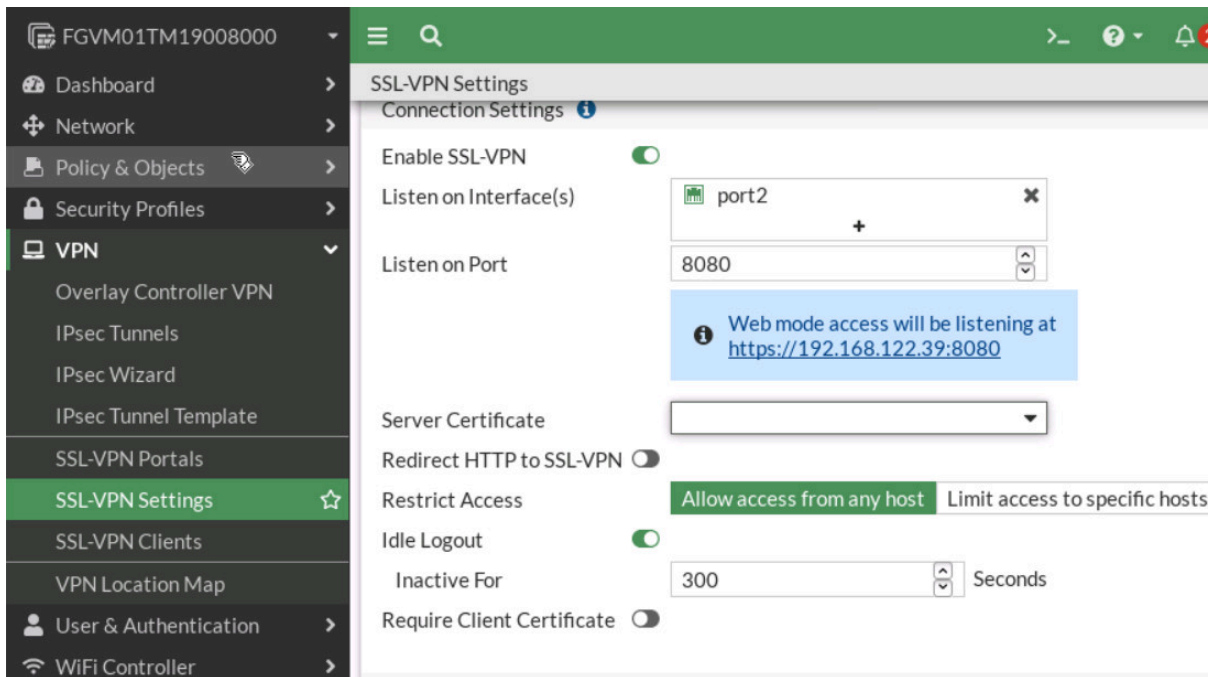


Figure 4.49: Enable SSL-VPN Settings

New Authentication/Portal Mapping

Users/Group: sslvpngroup

Portal: MyPortal

OK Cancel

Figure 4.50: Assign sslvpngroup to MyPortal

Authentication/Portal Mapping

+ Create New Edit Delete Send SSL-VPN Configuration

Users/Groups	Portal
sslvpngroup	MyPortal
All Other Users/Groups	MyPortal

Figure 4.51: Authentication/Portal Mapping

7. Configure SSL VPN firewall policy:

1. Go to **Policy & Objects > Firewall Policy**.
2. Fill in the firewall policy name. In this example, **SSLVPN** full tunnel access.
3. The incoming interface must be SSL-VPN tunnel interface(ssl.root).
4. Choose an Outgoing Interface. In this example, port3.
5. Set the Source to all and group to **sslvpngroup**.
6. Set the Destination to all.
7. Set Schedule to always, Service to ALL, and Action to Accept.

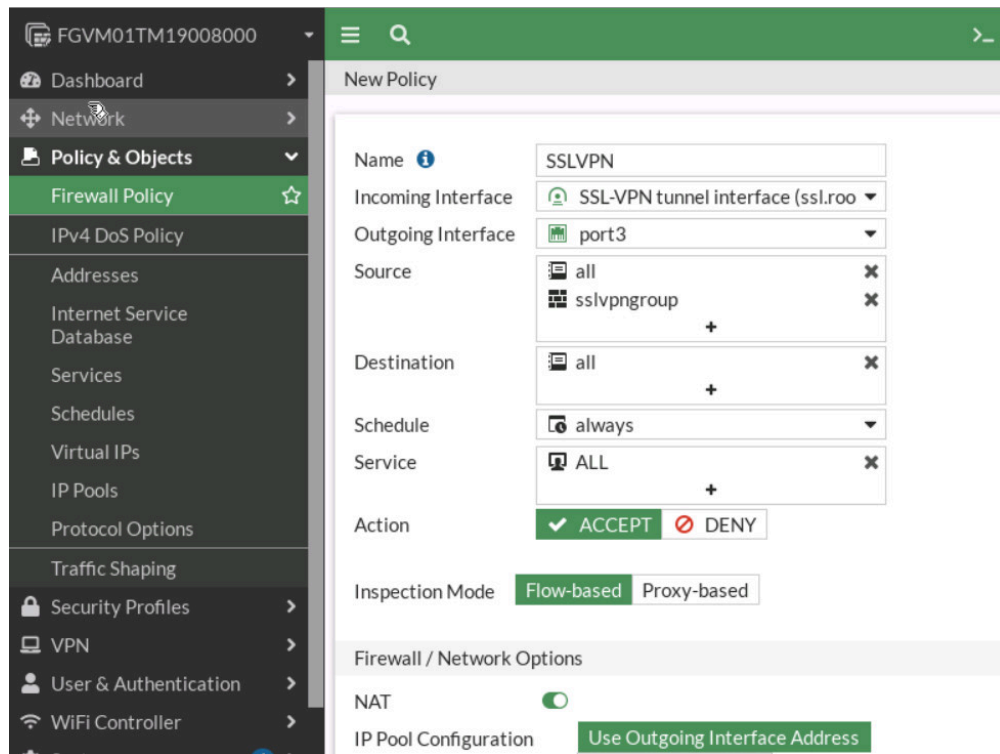


Figure 4.52: Create a Firewall Policy for SSLVPN

- Now connect to Kali outside and open the browser **https://IP-PORT 2-Firewall:8080**. Enter the username and password you created earlier. Then try to connect to the KALI SSH Server and WordPress through the browser.

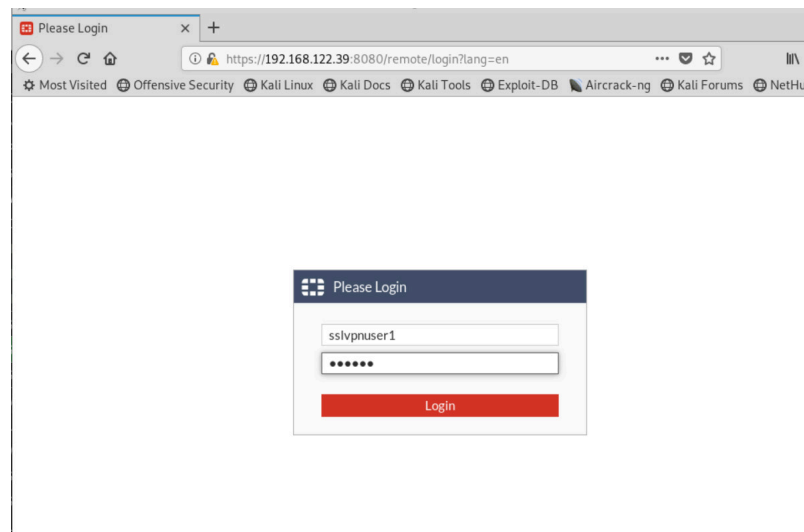


Figure 4.53: SSL-VPN Portal

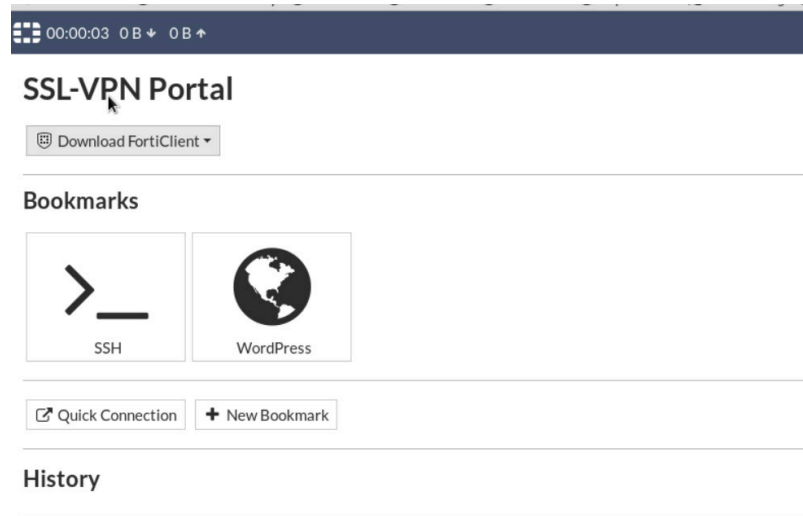


Figure 4.54: SSL-VPN Portal

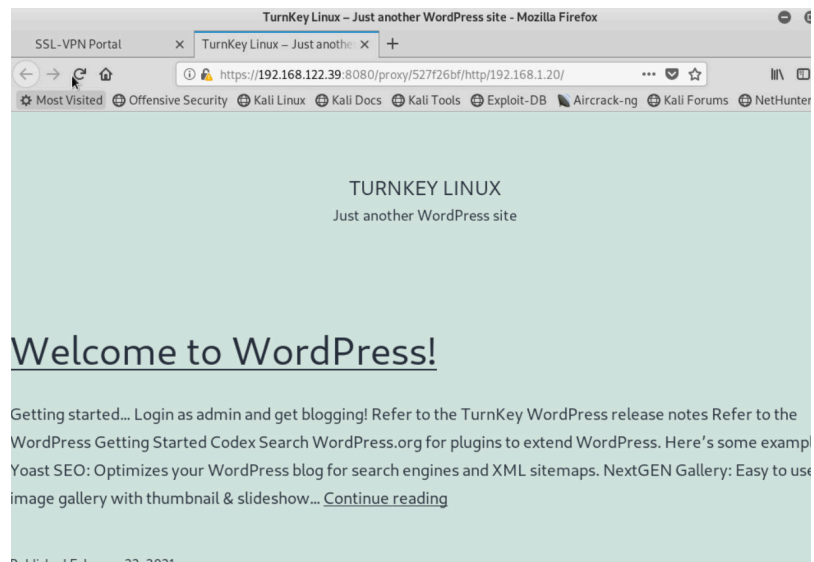


Figure 4.55: Verify WordPress

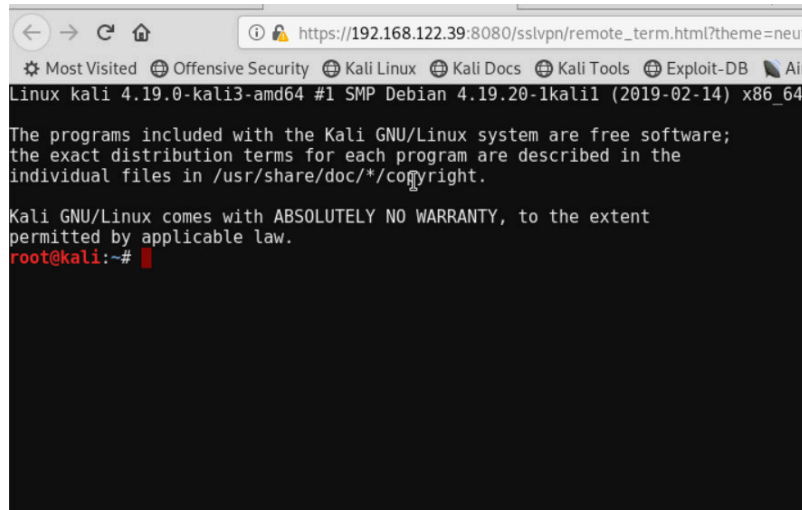


Figure 4.56: Verify SSH

9. Now, go to Windows and install FortiClient on Windows. Try to use FortiClient to connect through SSLVPN.

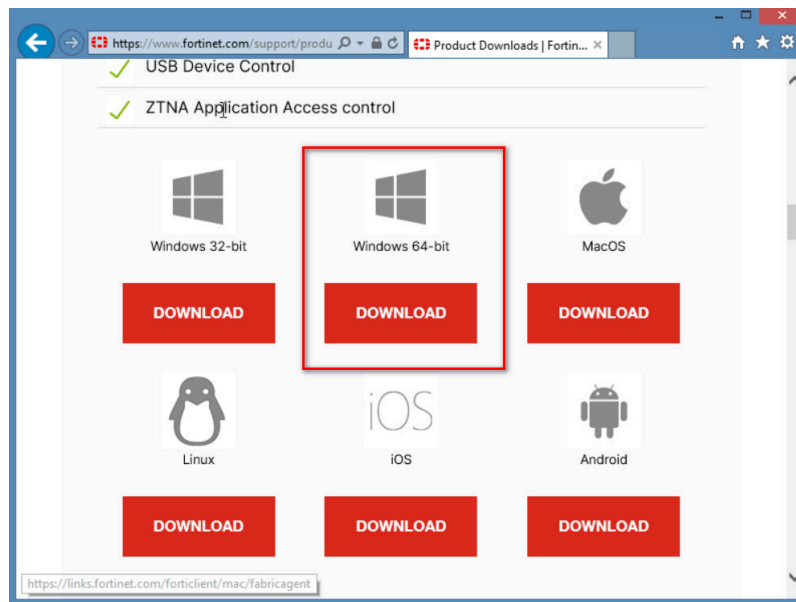


Figure 4.57: Download FortiClient

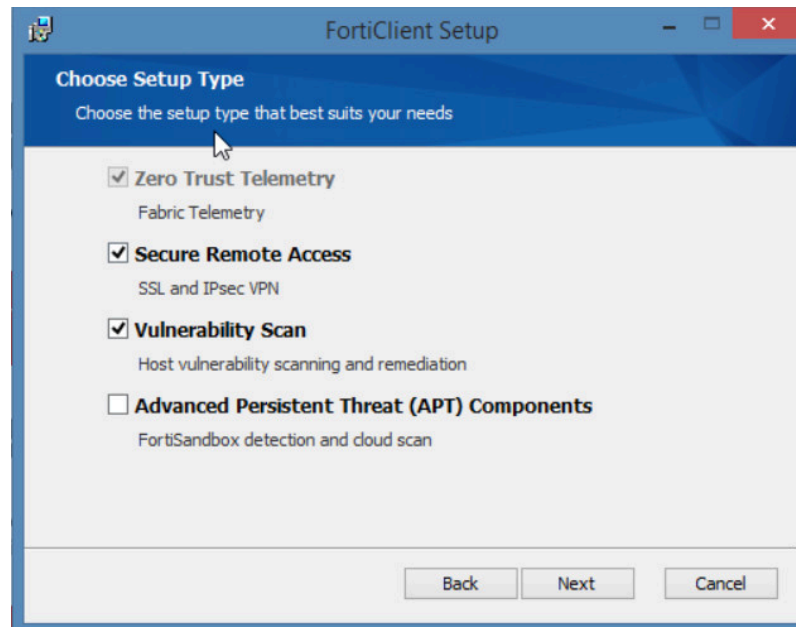


Figure 4.58: FortiClient Installation

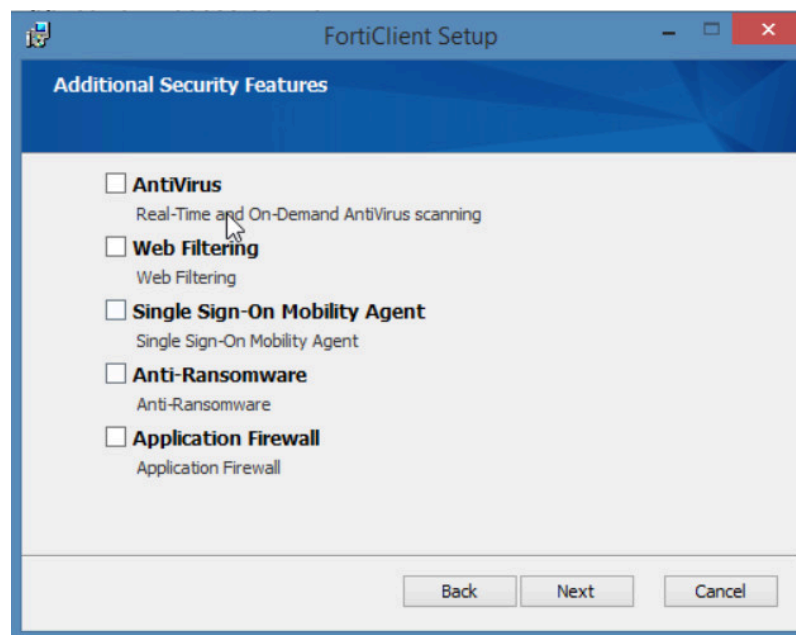


Figure 4.59: FortiClient Installation

10. Configure FortiClient.

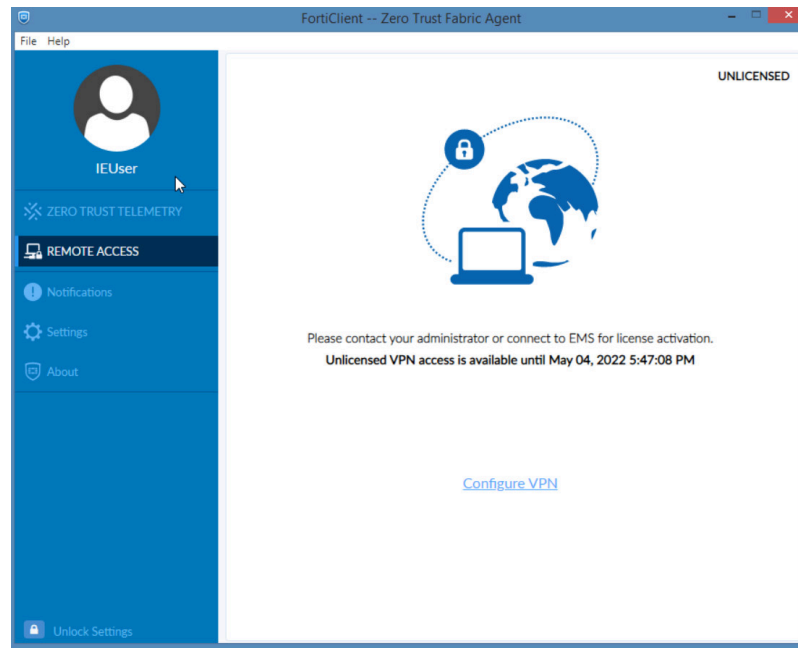


Figure 4.60: Configure FortiClient

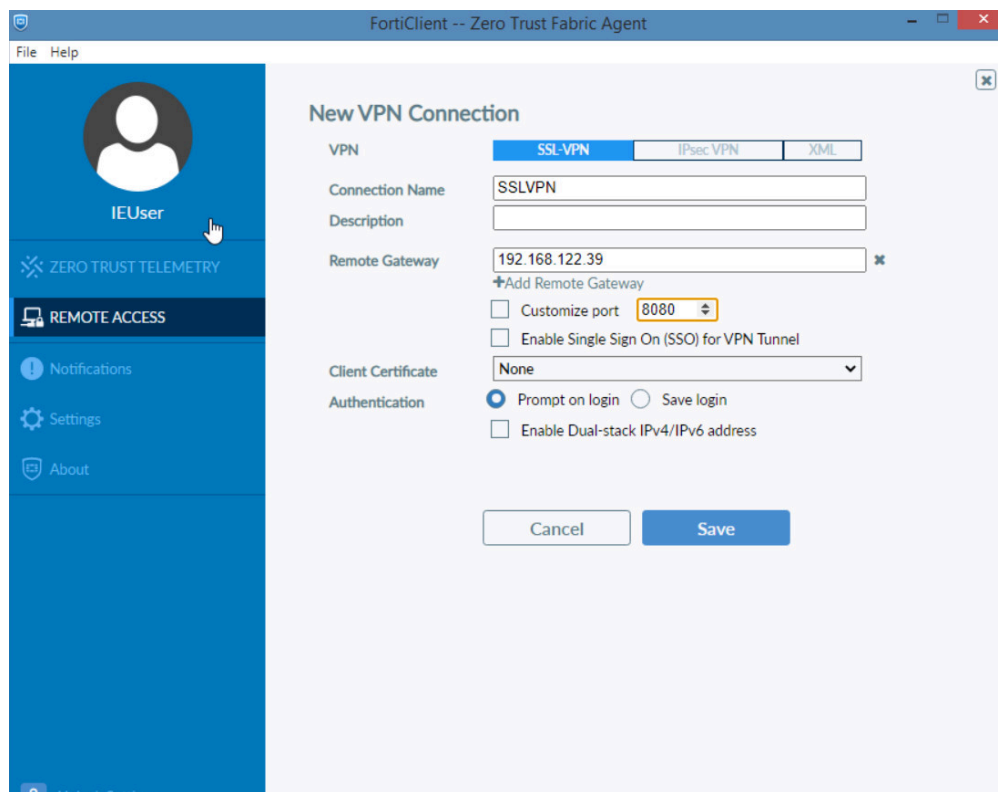


Figure 4.61: Configure SSLVPN

11. Verify configuration. Enter the Username and Password you have set for SSLVPN.

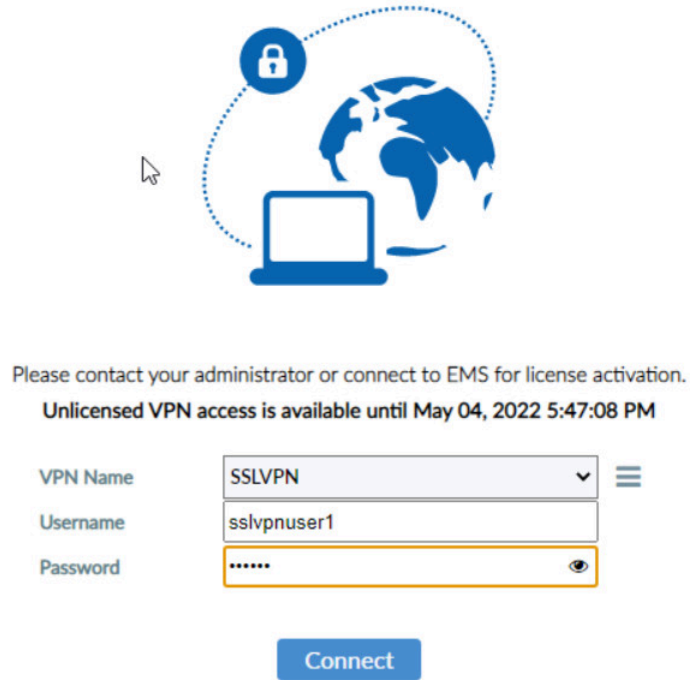


Figure 4.62: SSLVPN Credentials

Accept the Certificate Issuer to have a secure connection.

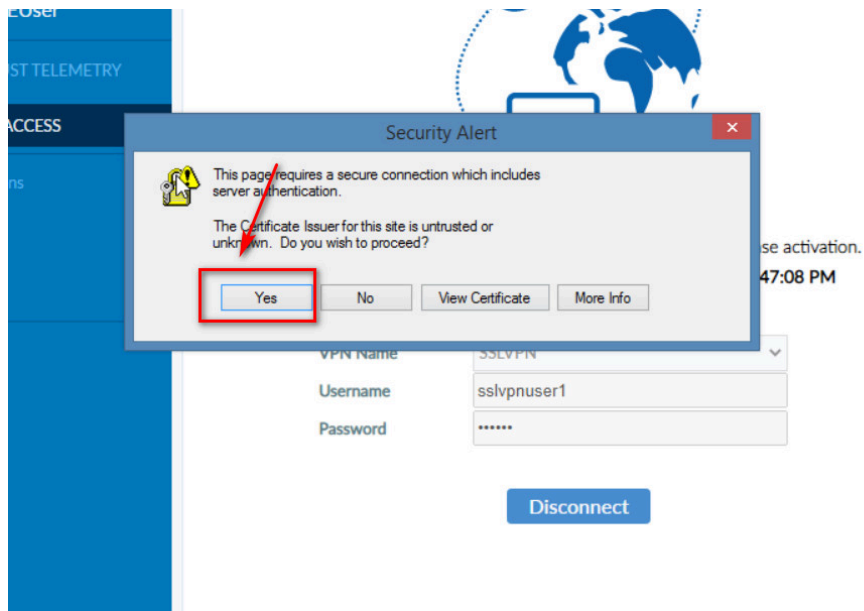


Figure 4.63: Click on Yes in Security Alert

VPN Connected



Figure 4.64: Verify SSLVPN Connection

Verify your connectivity by entering the IP address of WordPress.

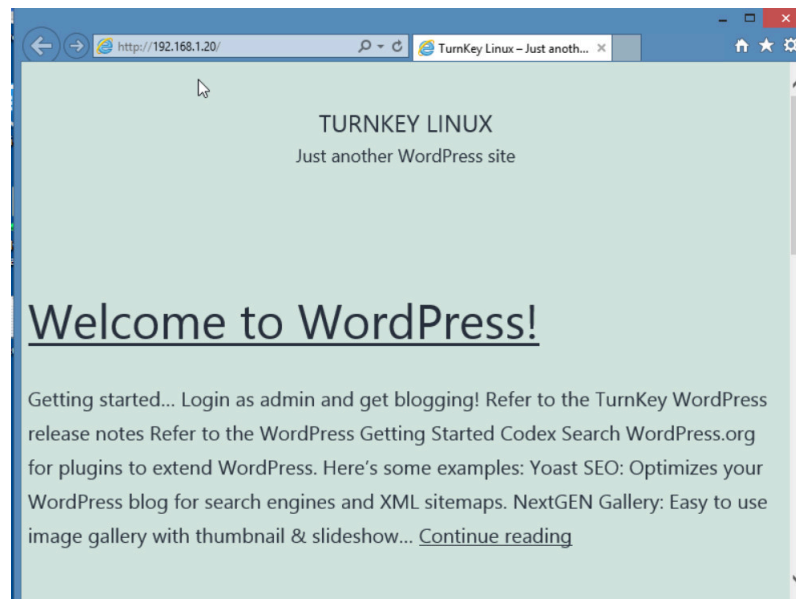
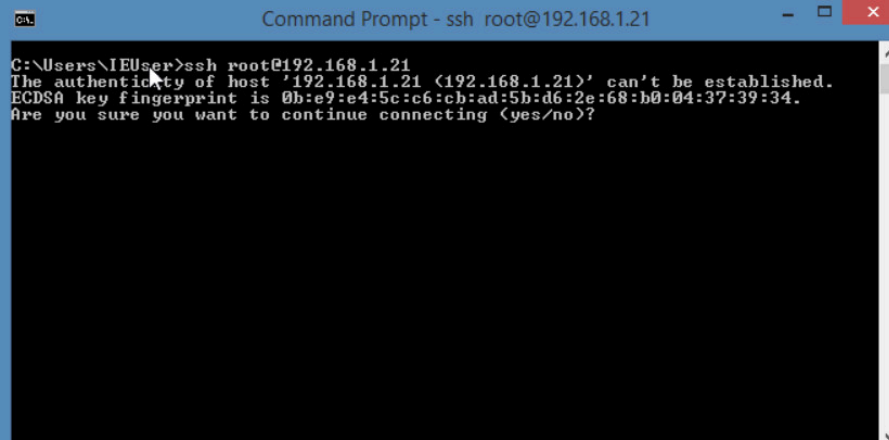


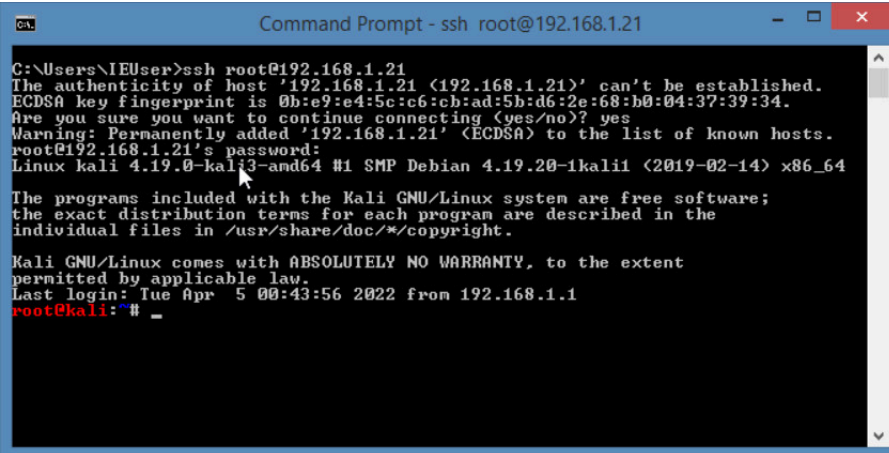
Figure 4.65: Verify WordPress

Verify your connectivity by entering the IP address of SSH Server.



```
Command Prompt - ssh root@192.168.1.21
C:\Users\IEUser>ssh root@192.168.1.21
The authenticity of host '192.168.1.21 (192.168.1.21)' can't be established.
ECDSA key fingerprint is 0b:e9:e4:5c:c6:cb:ad:5b:d6:2e:68:b0:04:37:39:34.
Are you sure you want to continue connecting (yes/no)?
```

Figure 4.66: Verify SSH



```
Command Prompt - ssh root@192.168.1.21
C:\Users\IEUser>ssh root@192.168.1.21
The authenticity of host '192.168.1.21 (192.168.1.21)' can't be established.
ECDSA key fingerprint is 0b:e9:e4:5c:c6:cb:ad:5b:d6:2e:68:b0:04:37:39:34.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.21' (ECDSA) to the list of known hosts.
root@192.168.1.21's password:
Linux kali 4.19.0-kali3-amd64 #1 SMP Debian 4.19.20-1kali1 (2019-02-14) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr 5 00:43:56 2022 from 192.168.1.1
root@kali:~#
```

Figure 4.67: Verify SSH connection

Chapter 5. Authentication

5.1 Captive Portal

Learning Objectives

- Configure a Captive Portal

Scenario: We are planning to enable Captive Portal on port2. Then, when users want to connect to the Internet, first they should enter their username and password and after that they are allowed to surf the Internet.

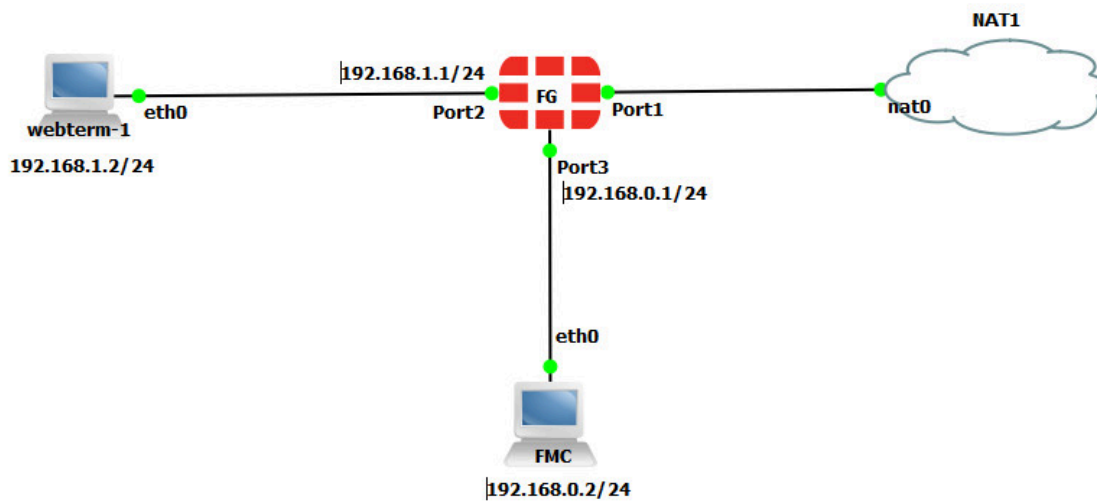


Figure 5.1: Main scenario

Table 5.1: Devices configuration

Device	IP address	Access
WebTerm1	192.168.1.2/24	–
FortiGate	Port 1: DHCP Client Port 2: 192.168.1.1/24 Port 3: 192.168.0.1/24	ICMP HTTP HTTPS
WebTerm (FMC)	192.168.0.2/24	–

1. Prerequisites:

1. Set the IP addresses in the firewall as above table. The CLI is available as following:

```

FGVM01TM19008000 # config system interface
FGVM01TM19008000 (interface) # edit port1
FGVM01TM19008000 (port1) # set mode dhcp
FGVM01TM19008000 (port1) # end

FGVM01TM19008000 # config system interface
FGVM01TM19008000 (interface) # edit port2
FGVM01TM19008000 (port2) # set ip 192.168.1.1/24
FGVM01TM19008000 (port2) # end

FGVM01TM19008000 # config system interface
FGVM01TM19008000 (interface) # edit port3
FGVM01TM19008000 (port3) # set ip 192.168.0.1/24
FGVM01TM19008000 (port3) # set allowaccess http https
FGVM01TM19008000 (port3) # end

```

2. Set a static route in the firewall. You should always set the default route in the firewall (0.0.0.0 0.0.0.0 Internet IP).

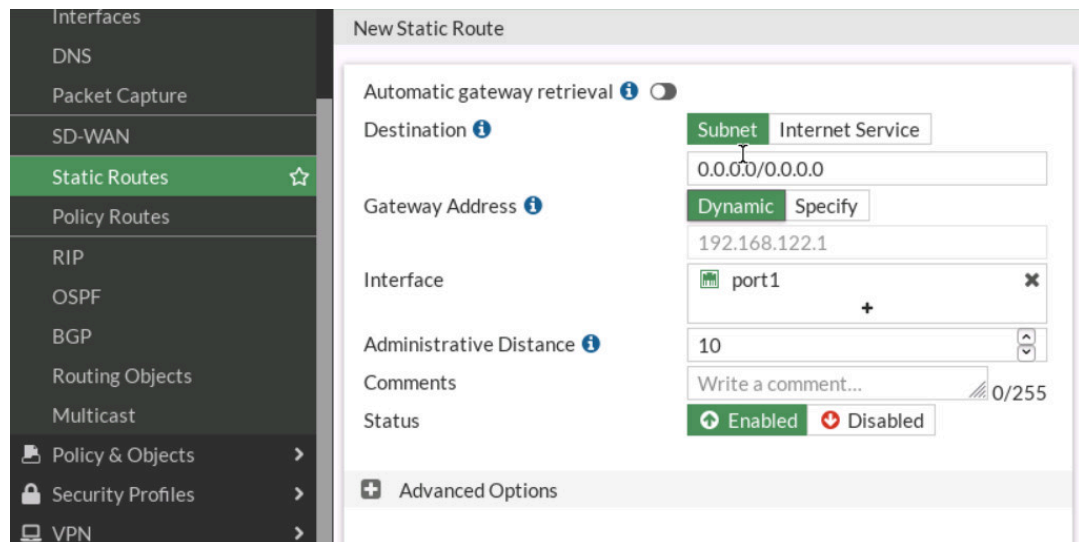


Figure 5.2: Configure a static route

3. Set a Firewall Policy from **port2** to **port1**.

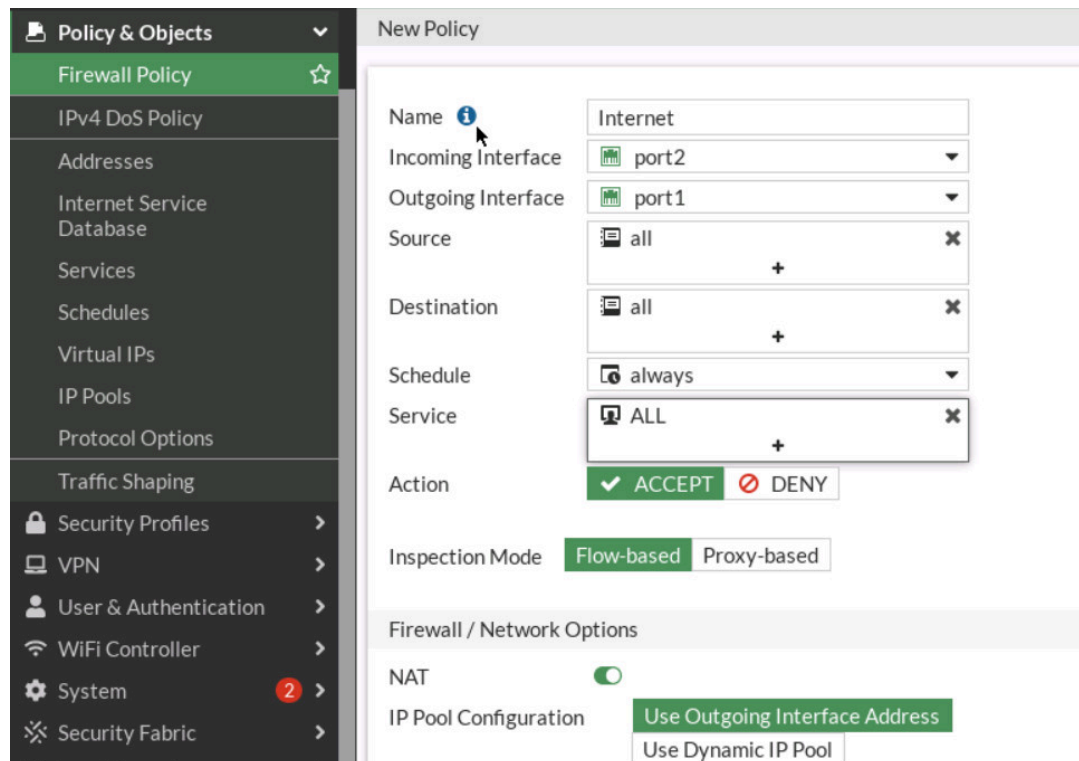


Figure 5.3: Set a Firewall Policy

4. Set the static IP address in WebTerm1 (192.168.1.2/24).

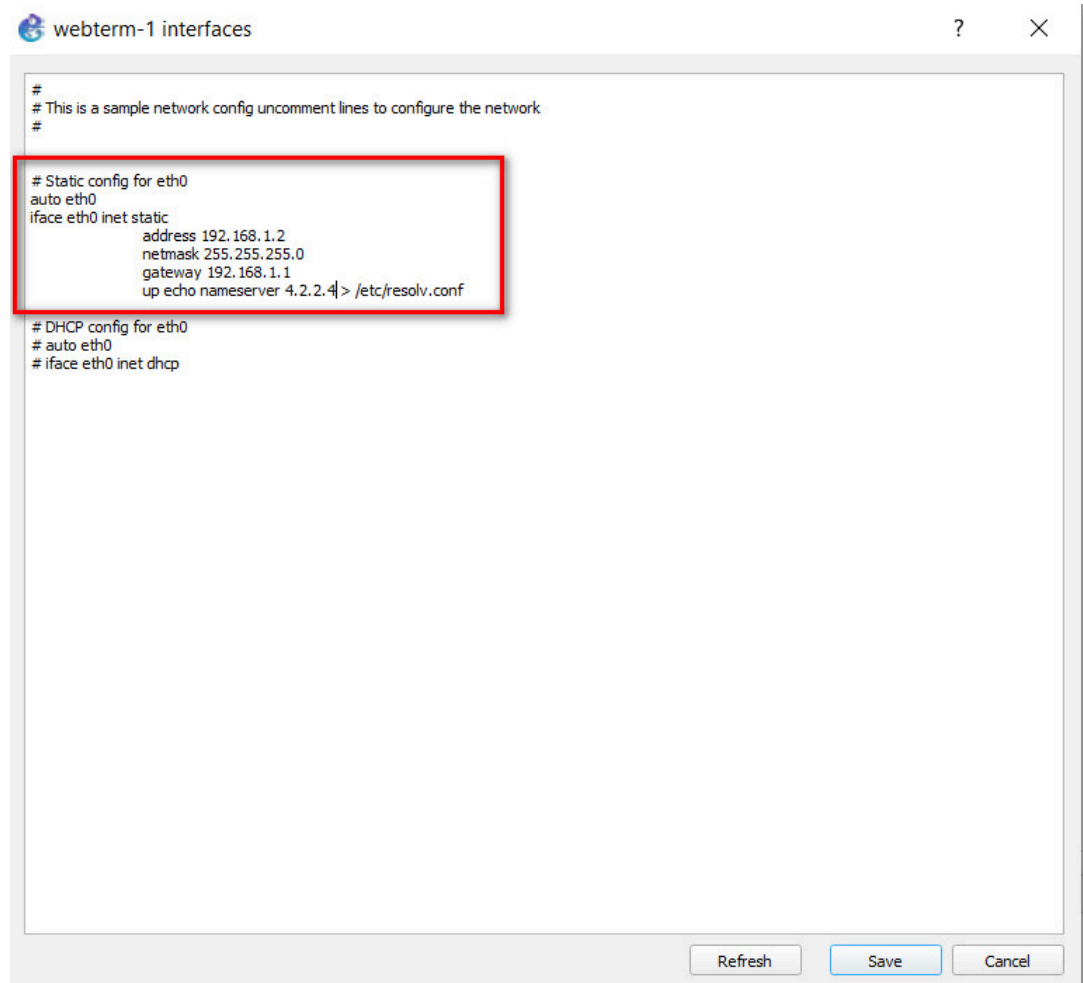


Figure 5.4: Configure a static IP address in WebTerm1

2. Create a user and group. Go to **User & Authentication > User Groups**. Create a group name: **CaptivePortal**.

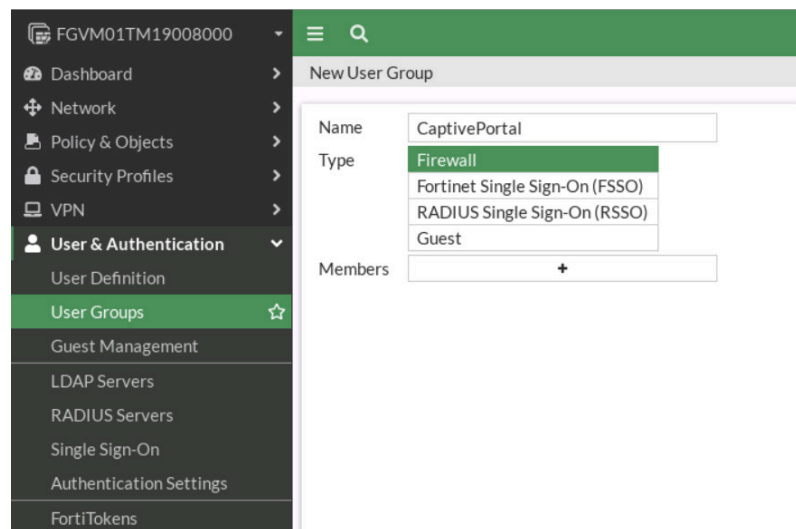


Figure 5.5: Create a group

Go to **User & Authentication > User Definition > Create a New User** and assign your user in step 4 to A0ID-CaptivePortal Group.

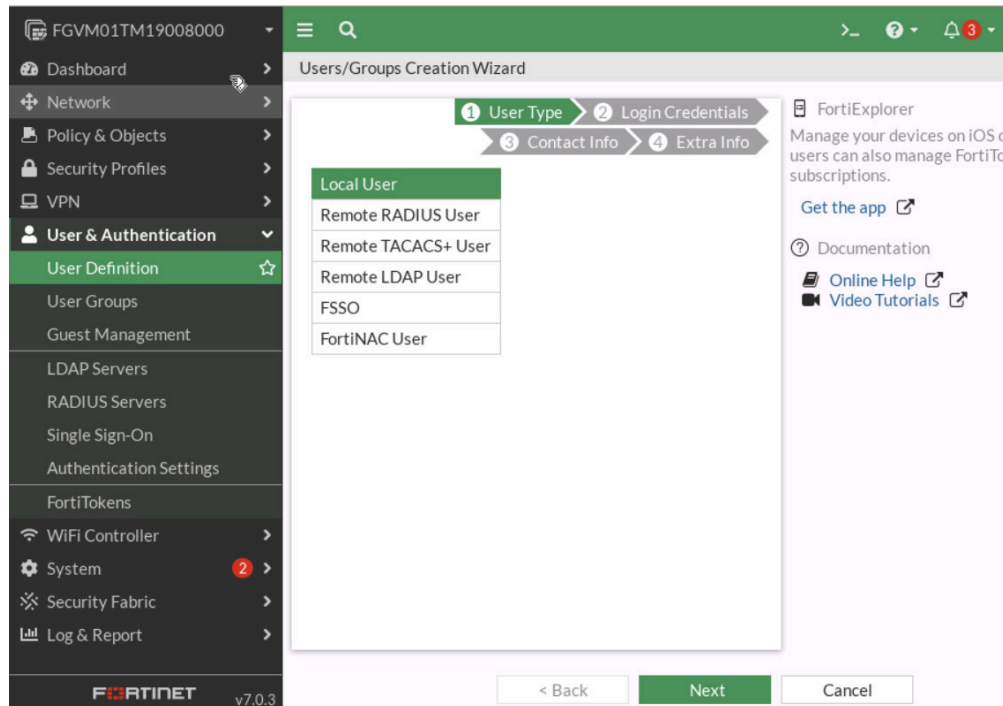


Figure 5.6: Create a user

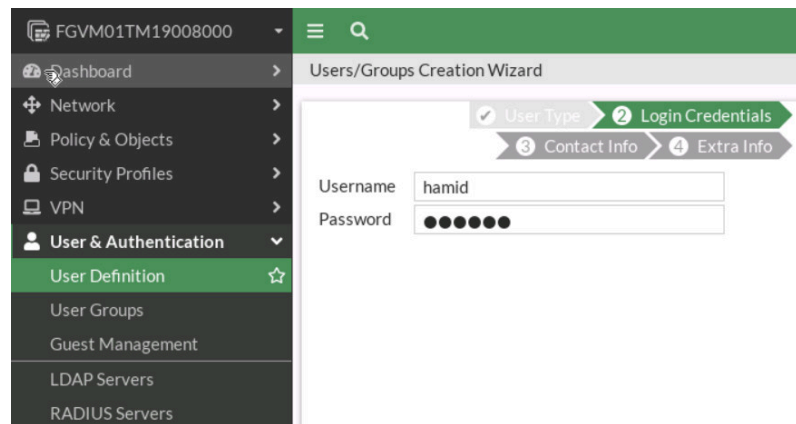


Figure 5.7: Create login credentials

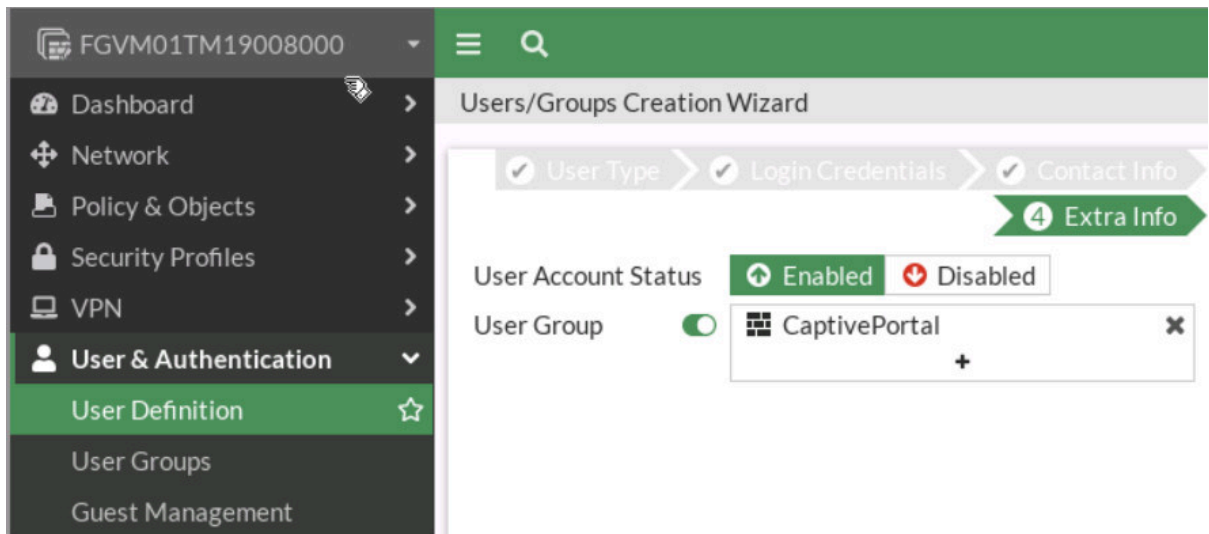


Figure 5.8: Add user to the group

3. Go to **Network > Interfaces and edit port 2**. In the Admission Control section, set:
 - **Security mode:** captive portal
 - **Authentication Portal:** Local
 - **User Access:** Restricted to Group and assign the group you have created in the previous step.

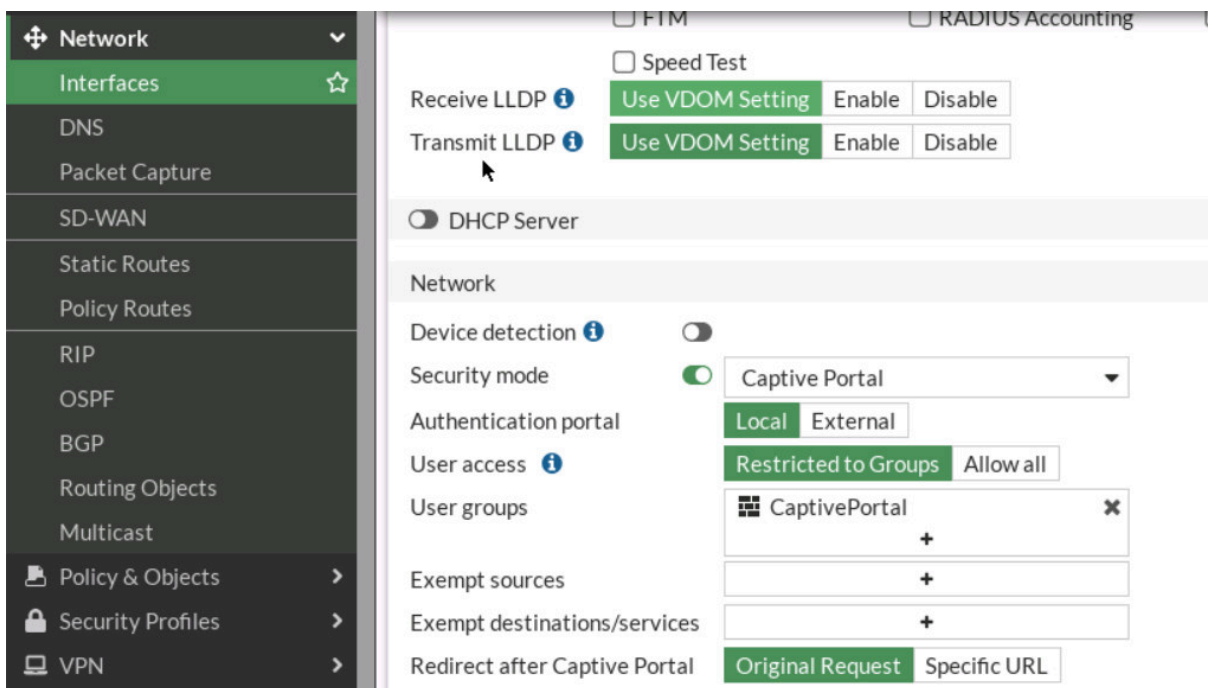


Figure 5.9: Configure Captive Portal on port2

4. Now, open the browser in WebTerm1 and type `http://talebi.ca`.

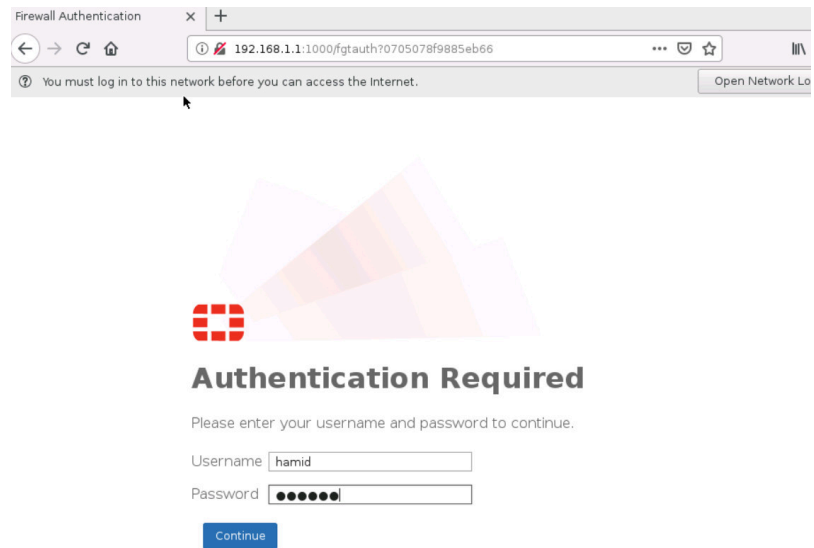


Figure 5.10: Verify Captive Portal

5.2 FSSO

Learning Objectives

- Install FSSO Agent on Windows Server
- Configure a FSSO

Scenario: FSSO stands for Fortinet Single Sign-on and it is used to allow users to login into the network with one single login credential. In this scenario, we are going to focus on agent-based FSSO and we are going to install the agent on Windows Server. Then, anyone logins through Active Directory, we can track them through FortiGate Logs and Events.

1. In this scenario, we are going to join windows 10 to Active Directory that we have set already. The domain controller name is Hamid.local. First, we will join Windows 10 to the domain controller.

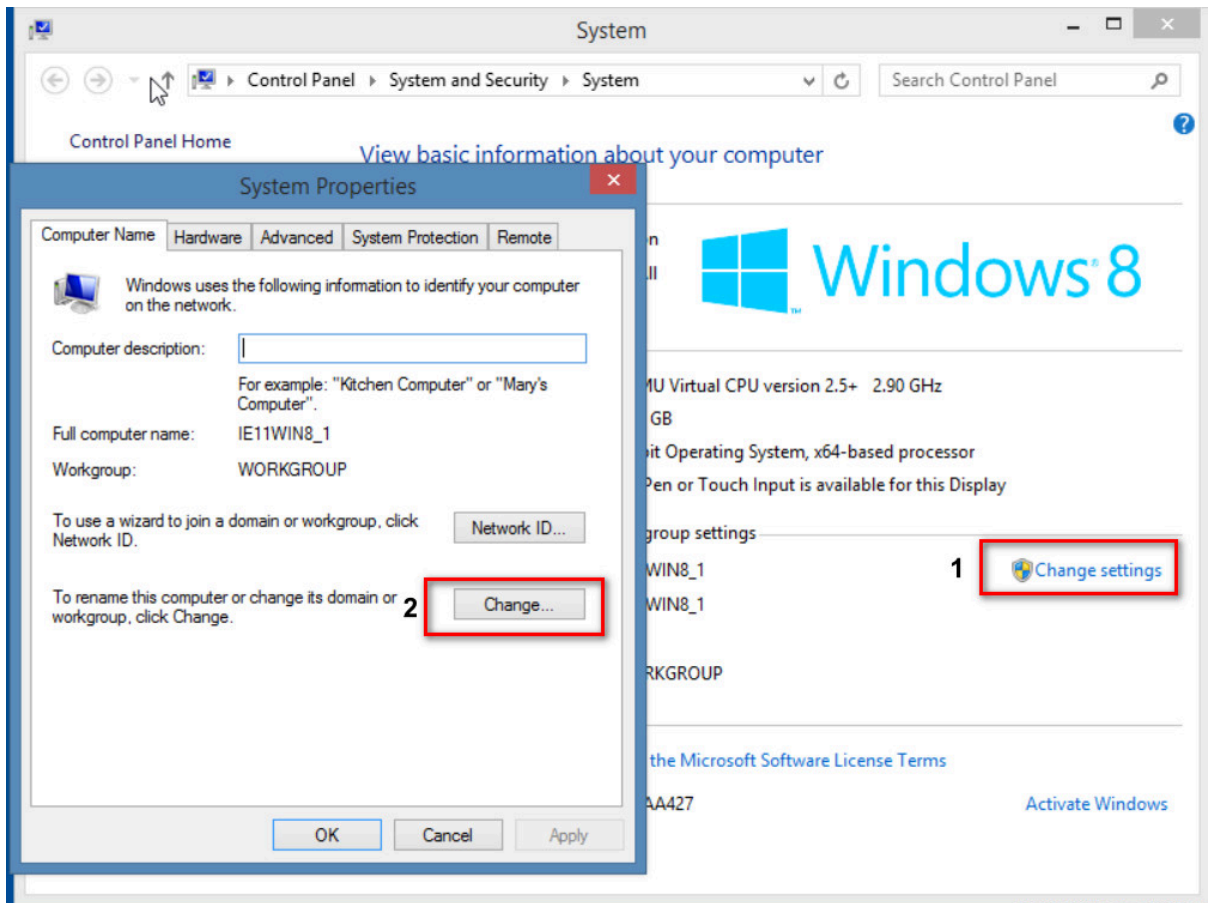


Figure 5.11: Join Windows to the Active Directory

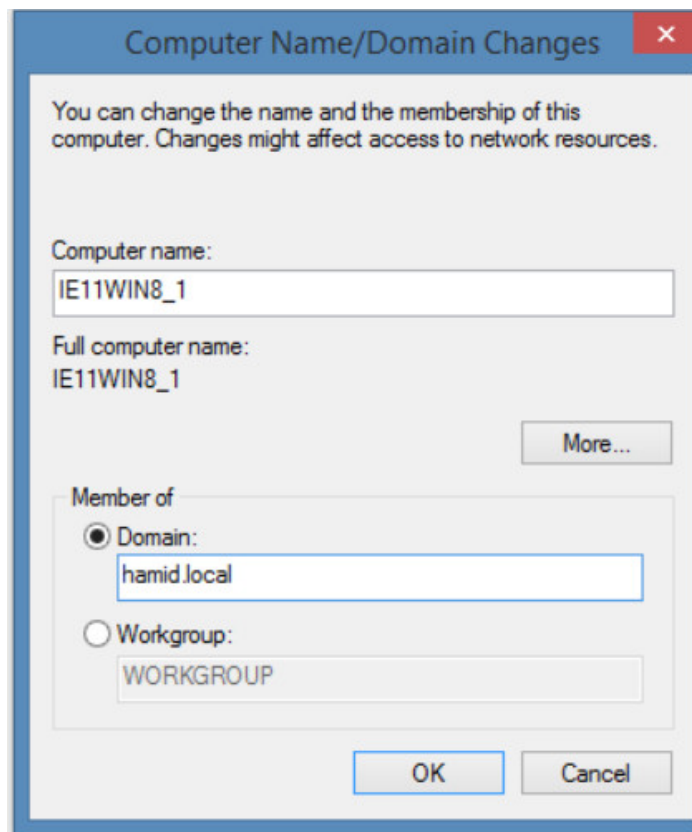


Figure 5.12: Enter Domain name

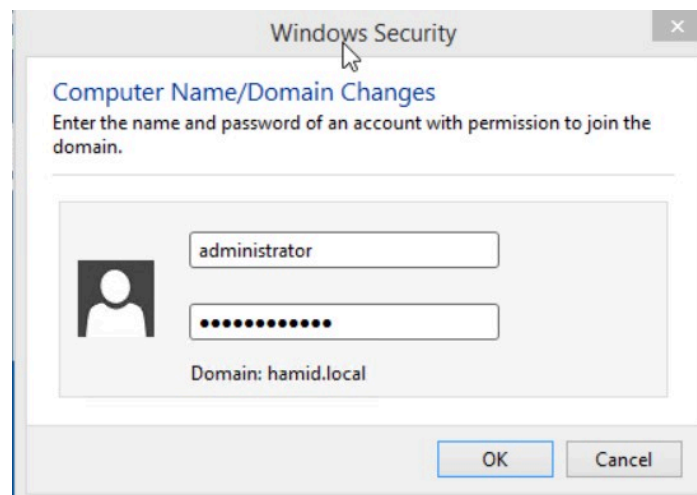


Figure 5.13: Enter username and password of AD administrator

2. Install FSSO Agent on the AD server.

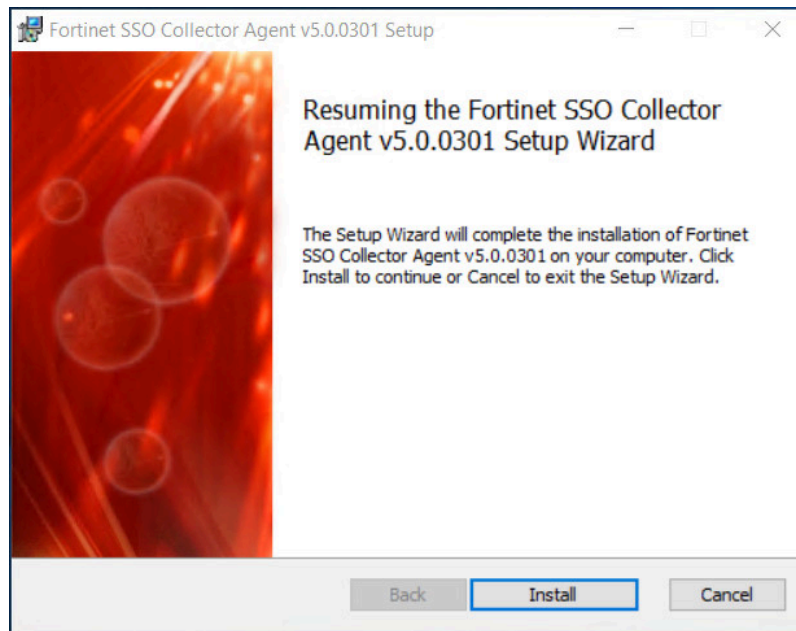


Figure 5.14: Install FSSO Agent

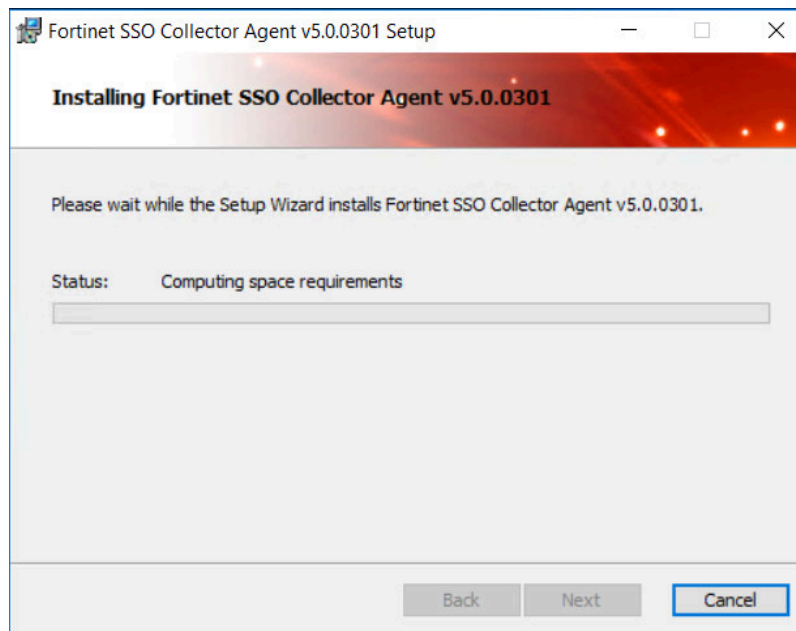


Figure 5.15: Install FSSO Agent

The password you set here for the agent is going to be used in the FortiGate firewall when you want to connect to the FSSO Agent.

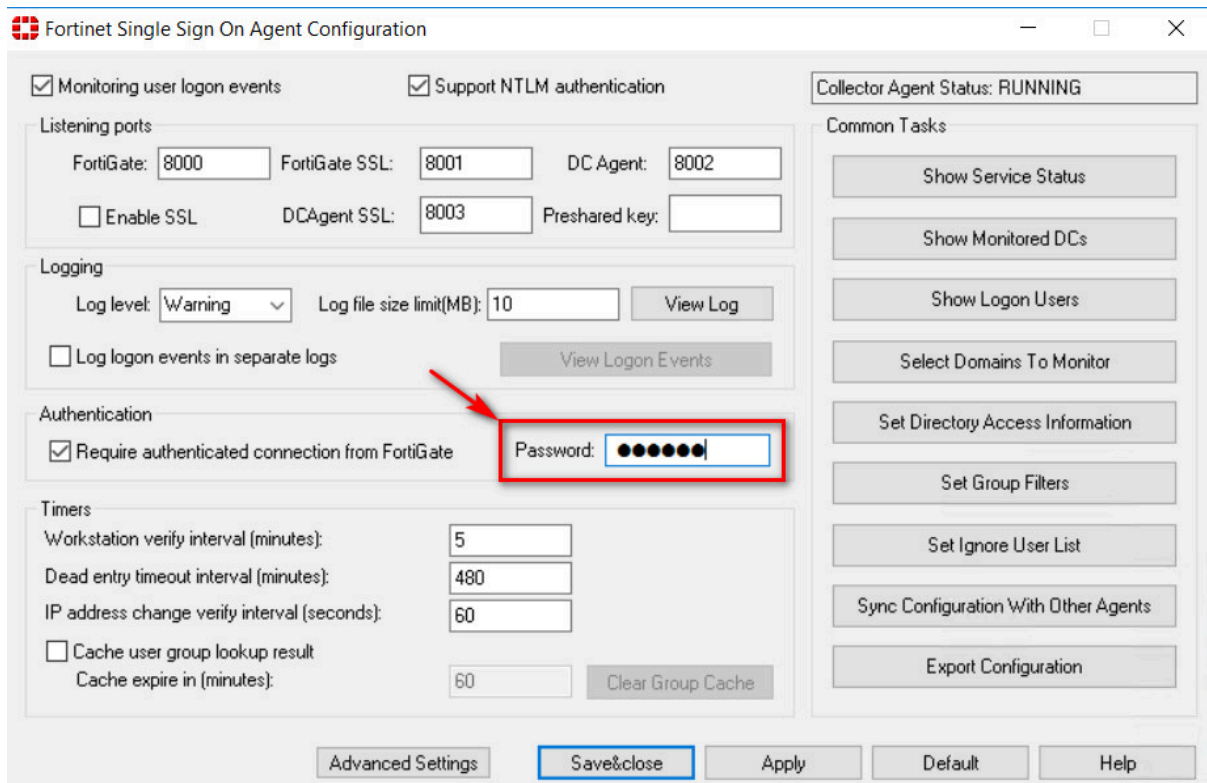


Figure 5.16: Configure FSSO Agent

3. In the FortiGate firewall, go to **Security Fabric > External Connectors > FSSO Agent on Windows AD**.

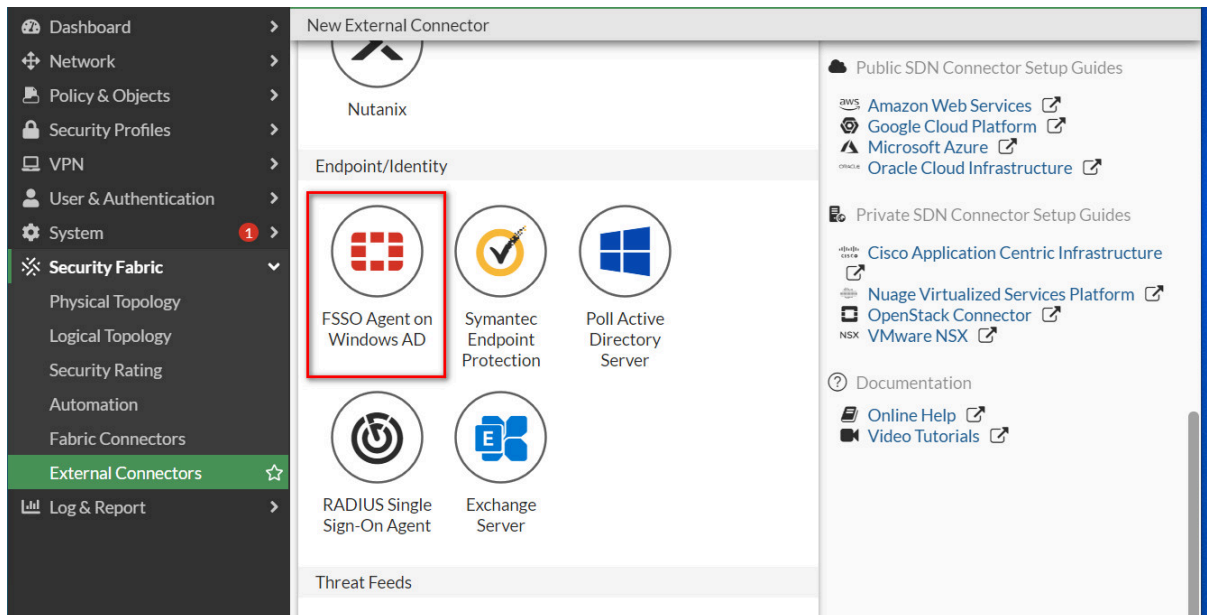


Figure 5.17: Set external connectors

Enter the same password you have set in step 2.

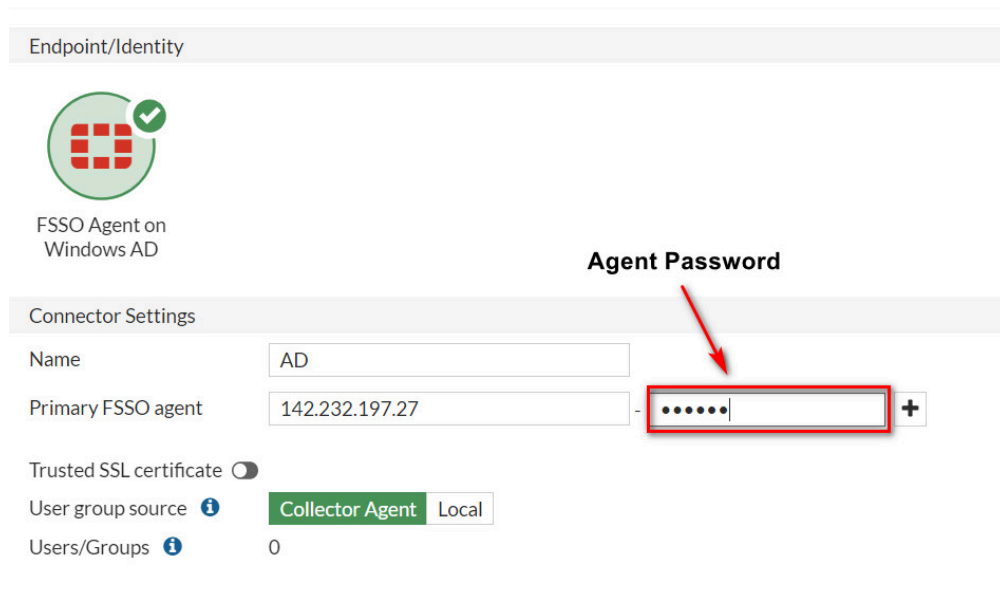


Figure 5.18: Set FSSO Agent settings

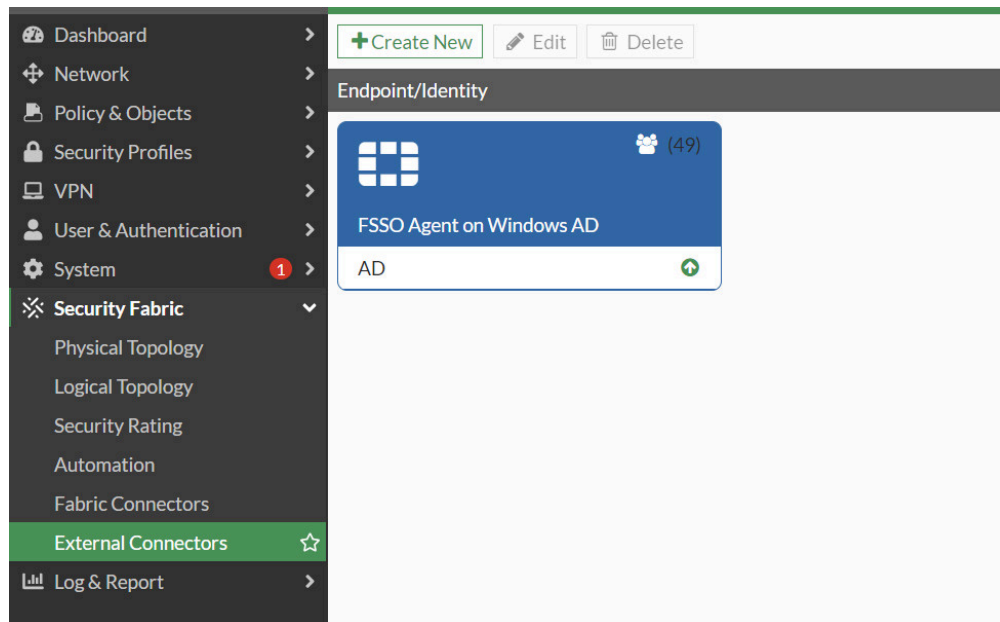


Figure 5.19: FSSO Agent status

4. You should be able to connect to FSSO Agent and you can verify the status of the external connector.
5. Verify your configuration by going to **Log & Report > Events > User Events**.

Date/Time	Level	User	Action	Message
49 seconds ago	■■■■■■	HTALEBI	auth-logon	User HTALEBI added to auth logon
54 seconds ago	■■■■■■	HTALEBI	auth-logon	User HTALEBI added to auth logon
54 seconds ago	■■■■■■	HTALEBI	FSSO-logon	FSSO-logon event from AD: user HTALEBI logged
54 seconds ago	■■■■■■		server-connect	FSSO server AD(142.232.197.27) is connected

Figure 5.20: FSSO event logs

- After connecting to the Agent, you should be able to see users and groups in AD when you are creating a new user.

Users/Groups Creation Wizard

1 User Type 2 Remote Groups 3 Local Group

FSSO Agent: AD

AD Groups: CN=DOMAIN USERS,CN=USERS

Select Entries

Search: [] + Create

AD (49)

- CN=ACCESS CONTROL ASSISTANCE
- CN=ACCOUNT OPERATORS,CN=BUI
- CN=ADMINISTRATORS,CN=BUILTI
- CN=ALLOWED RODC PASSWORD RE
- CN=BACKUP OPERATORS,CN=BUILT
- CN=CERT PUBLISHERS,CN=USERS,D
- CN=CERTIFICATE SERVICE DCOM A
- CN=CLONEABLE DOMAIN CONTROL
- CN=CRYPTOGRAPHIC OPERATORS,<
- CN=DENIED RODC PASSWORD REPI
- CN=DISTRIBUTED COM USERS,CN=
- CN=DNSADMINS,CN=USERS,DC=HA
- CN=DNSUPDATEPROXY,CN=USERS,I
- CN=DOMAIN ADMINS,CN=USERS,D
- CN=DOMAIN COMPUTERS,CN=USEI
- CN=DOMAIN CONTROLLERS,CN=US
- CN=DOMAIN GUESTS,CN=USERS,DC
- CN=DOMAIN USERS,CN=USERS,DC=
- CN=ENTERPRISE ADMINS,CN=USER

Close

Figure 5.21: Verify configuration

Chapter 6. High Availability

6.1 High Availability

Learning Objectives

- Configure HA (Active-Passive) between two firewalls

Scenario: In this lab, we are going to have two firewalls. One of them is Primary or Active and the other one is Secondary or Passive. We are going to have High Availability between these two firewalls and if we shut down one of them, the other one will be Primary.

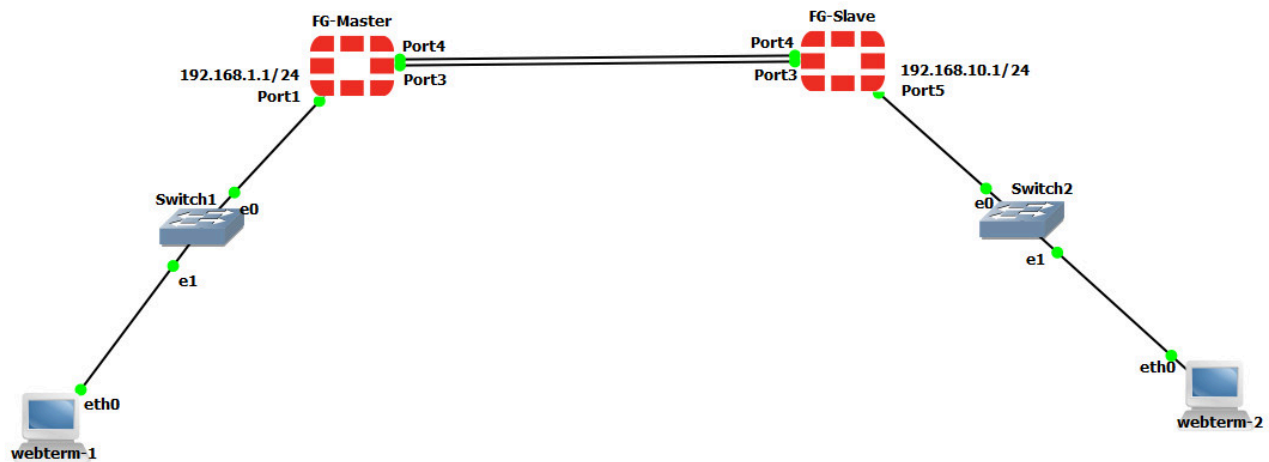


Figure 6.1: Main scenario

Table 6.1: Devices configuration

Device	IP address	Access
WebTerm1	192.168.1.2/24	–
WebTerm2	192.168.10.2/24	–
EthernetSwitch1	–	–
EthernetSwitch2	–	–
FG-Primary	Port 1: 192.168.1.1/24 Port 5: 192.168.10.1/24	ICMP-HTTP-HTTPS
FG-Secondary	Port 1: 192.168.1.1/24 Port 5: 192.168.10.1/24	ICMP-HTTP-HTTPS

1. CLI Configuration for Primary and Secondary:

FG-Primary

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FG-Primary
FortiGate-VM64-KVM (global) # end

FG-Primary # config system interface
FG-Primary (interface) # edit port1
FG-Primary (port1) # set mode static
FG-Primary (port1) # set ip 192.168.1.1/24
FG-Primary (port1) # set allowaccess http https ping
FG-Primary (port1) # end
FG-Primary # config system interface
FG-Primary (interface) # edit port5
FG-Primary (port5) # set ip 192.168.10.1/24
FG-Primary (port5) # set allowaccess http https ping
FG-Primary (port5) # end
```

FG-Secondary

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FG-Secondary
FortiGate-VM64-KVM (global) # end
```

```

FG-Secondary # config system interface
FG-Secondary(interface) # edit port1
FG-Secondary (port1) # set mode static
FG-Secondary (port1) # set ip 192.168.1.1/24
FG-Secondary (port1) # set allowaccess http https ping
FG-Secondary (port1) # end
FG-Secondary # config system interface
FG-Secondary (interface) # edit port5
FG-Secondary (port5) # set ip 192.168.10.1/24
FG-Secondary (port5) # set allowaccess http https ping
FG-Secondary (port5) # end

```

2. Go to **System > HA in the FG-Primary:**

- Select the Mode: **Active-Passive**
- Device Priority: **128** (The higher priority is primary)
- Group Name: **HRT** (The Group name between Primary and Secondary should be the same)
- Password: **Set a password** (The Password between Primary and Secondary should be the same)
- Monitor Interface: **Port 3**
- Heartbeat Interface: **Port 4**

The screenshot displays the FortiGate configuration interface for High Availability (HA) primary configuration. The left sidebar shows the navigation menu with 'System' selected and 'HA' highlighted. The main panel shows the following configuration:

- Mode:** Active-Passive
- Device priority:** 128
- Cluster Settings:**
 - Group name:** HRT
 - Password:** 123456
 - Session pickup:**
 - Monitor interfaces:** port3
 - Heartbeat interfaces:** port4
- Management Interface Reservation:**
- Unicast Heartbeat:**

Figure 6.2: HA primary configuration

Do the same configuration in the FG-Secondary but set the Device priority to 50.

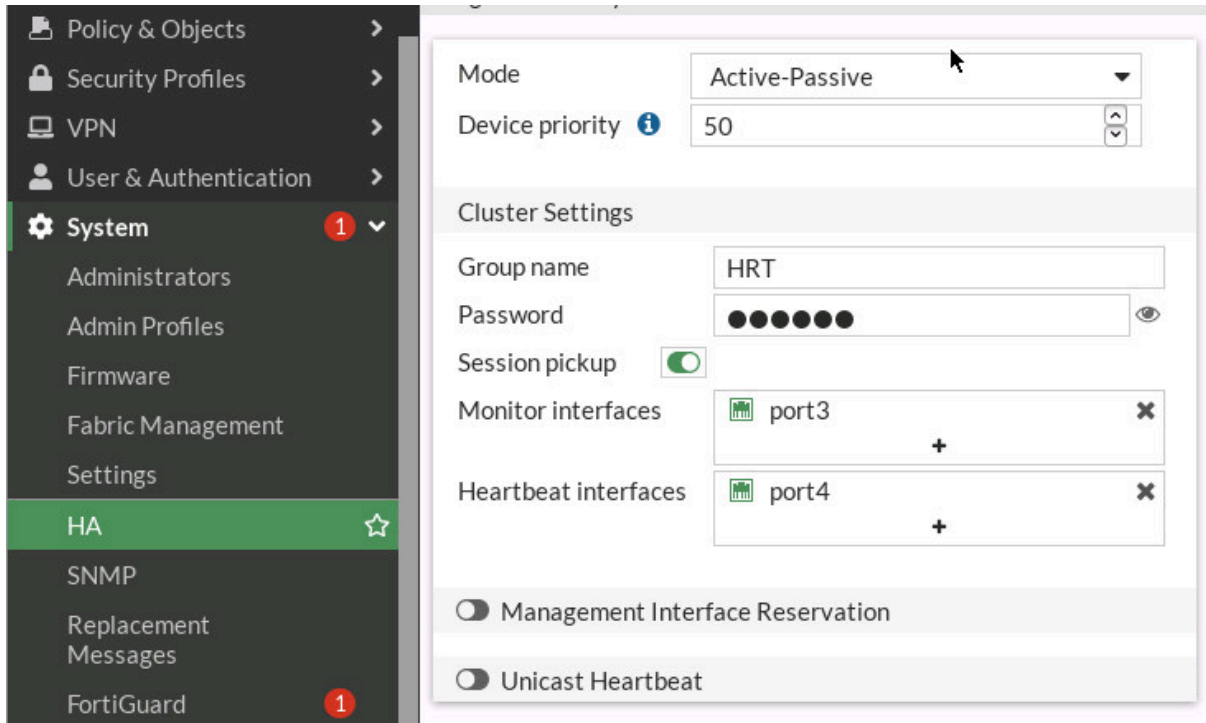


Figure 6.3: HA secondary configuration

3. After setting secondary device, no longer be able to access secondary device. Go to **FG-Primary > System > HA** and evaluate your result.

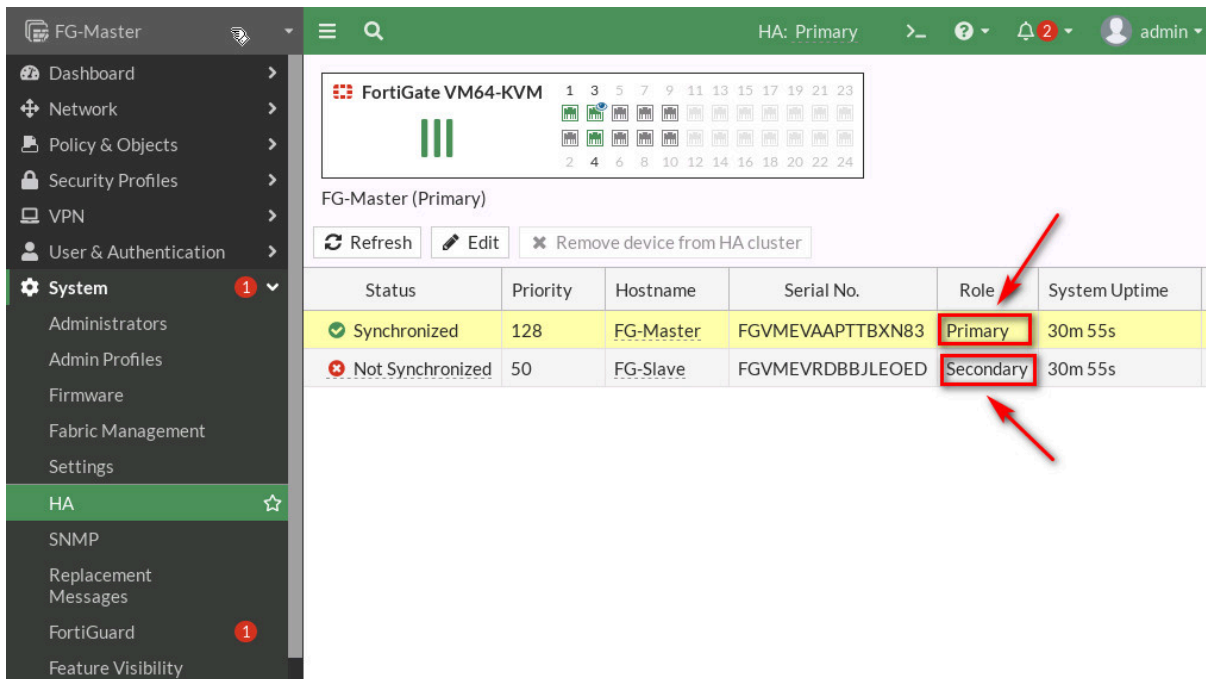


Figure 6.4: HA status

Two devices will be synchronized after a while.

The screenshot shows the FortiGate HA status page. The top navigation bar includes 'FG-Master', a search icon, and 'HA: Primary'. The main content area displays 'FortiGate VM64-KVM' with a status bar and a table of HA cluster members. Below the table are buttons for 'Refresh', 'Edit', and 'Remove device from HA cluster'. The table lists the status, priority, hostname, serial number, role, and system uptime for both the Primary and Secondary devices.

Status	Priority	Hostname	Serial No.	Role	System Uptime
✓ Synchronized	128	FG-Master	FGVMEVAAPTBTXN83	Primary	36m 7s
✓ Synchronized	50	FG-Slave	FGVMEVRDBBJLEOED	Secondary	36m 7s

Figure 6.5: HA Synchronized status

4. Now, connect other interfaces like Figure 6.6.

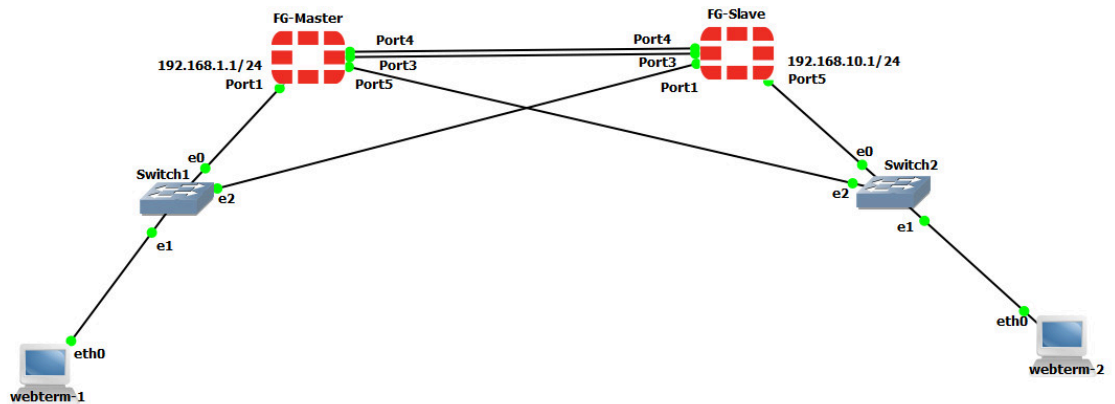


Figure 6.6: Main scenario

Try to Stop FG-Primary and go to WebTerm1. Can you reach the firewall?

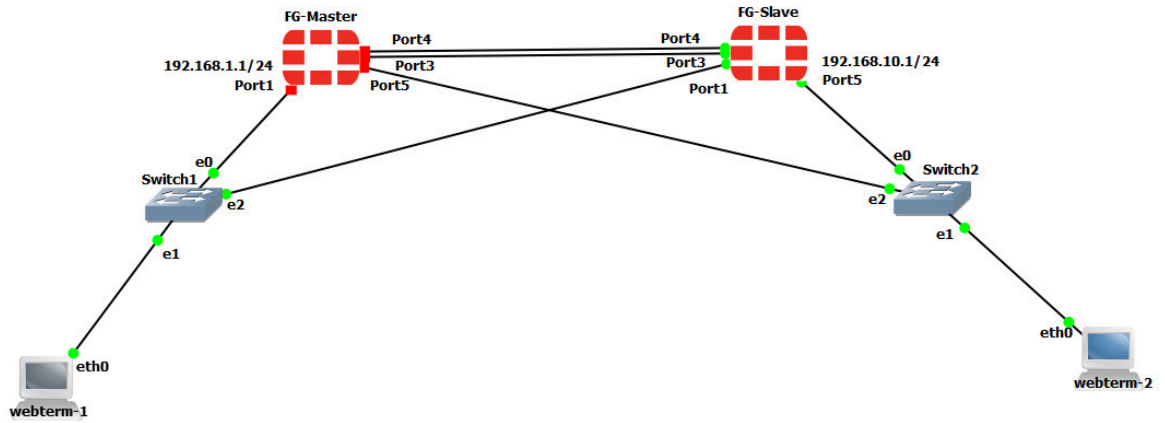


Figure 6.7: Stopping FG-Primary

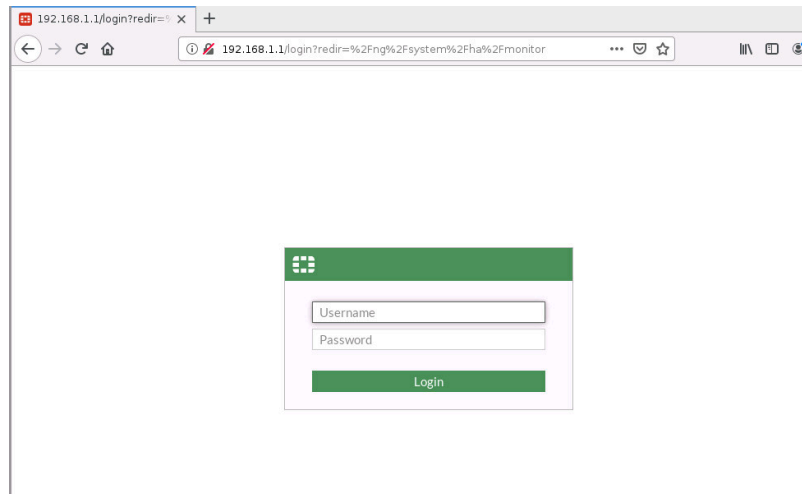


Figure 6.8: Verify connectivity to the firewall

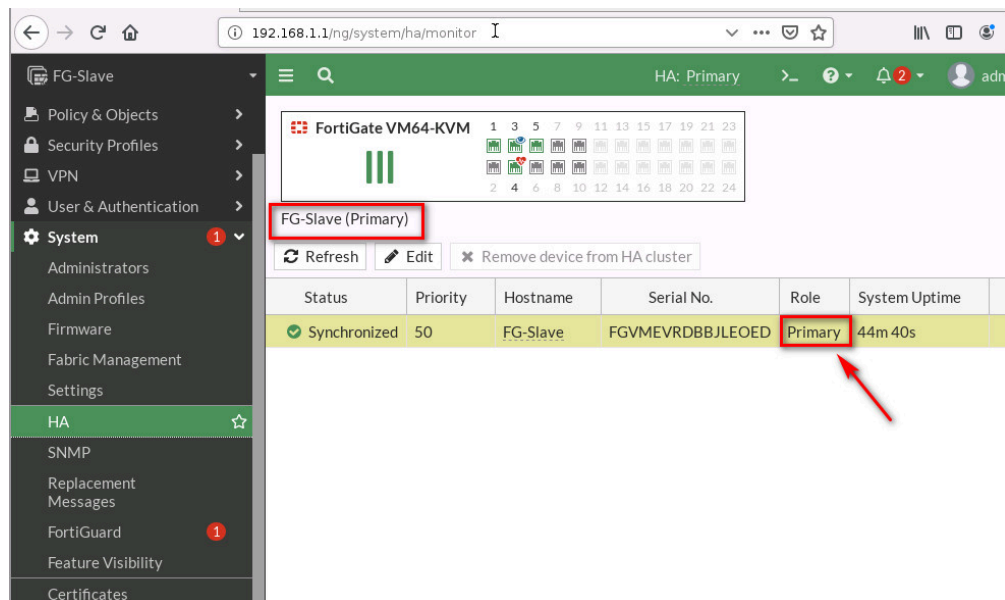


Figure 6.9: Verify firewall role after stopping FG-Primary

5. Go to **Log & Report > Events > HA Events** and download the log. Verify your result.

Date/Time	Level	Action	Message
Minute ago	■□□□□□		Virtual cluster's member state moved
Minute ago	■□□□□□		Virtual cluster detected member dead
Minute ago	■□□□□□		Heartbeat packet lost
11 minutes ago	■□□□□□		The sync status with the primary
12 minutes ago	■□□□□□		The sync status with the primary
12 minutes ago	■□□□□□		The sync status with the primary
14 minutes ago	■□□□□□		The sync status with the primary
14 minutes ago	■□□□□□		Virtual cluster's member state moved
14 minutes ago	■□□□□□		Virtual cluster detected member join
14 minutes ago	■□□□□□		HA device(interface) peerinfo
14 minutes ago	■□□□□□		HA activity report
14 minutes ago	■□□□□□		Virtual cluster add HA device
14 minutes ago	■□□□□□		HA activity report

Figure 6.10: HA Events

Chapter 7. Security

7.1 DDoS Prevention

Learning Objectives

- Configure a DDoS prevention profile

Scenario: In this lab, we are going to set a DDoS Prevention on traffic from Port1 to Port2. In Kali, we are going to install a script to do a DOS attack and in the firewall, we will set a DDoS Prevention Policy to block DOS traffic.

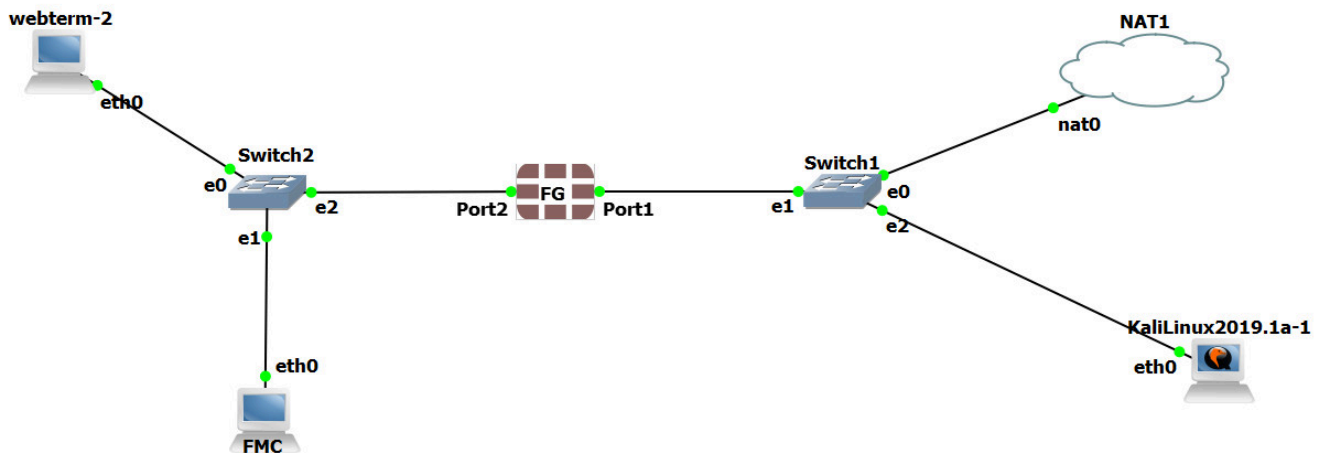


Figure 7.1: Main scenario

Table 7.1: Devices configuration

Device	IP address	Access
Kali1	DHCP Client	–
FortiGate	Port 1: DHCP Client Port 2: 192.168.0.1/24, DHCP Server (192.168.0.10-192.168.0.20)	ICMP-HTTP-HTTPS
WebTerm1 (FMC)	192.168.0.2/24	–
WebTerm2	DHCP Client	–

1. FortiGate CLI Configuration for port2.

```
FGVM01TM19008000 # config system interface
FGVM01TM19008000 (interface) # edit port2
FGVM01TM19008000 (port2) # set ip 192.168.0.1/24
FGVM01TM19008000 (port2) # set allowaccess http https ping
FGVM01TM19008000 (port2) # end
```

2. Go to Kali and Download the pentmenu repository (<https://github.com/GinjaChris/pentmenu>) and run **DOS > UDP FLOOD > Enter port1 IP address > Port 443.**

```

root@kali: ~
File Edit New Search Terminal Help
root@kali:~# wget https://raw.githubusercontent.com/GinjaChris/pentmenu/master/pentmenu
--2022-04-07 23:55:24-- https://raw.githubusercontent.com/GinjaChris/pentmenu/master/pentme
nu
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.
111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 49548 (48K) [text/plain]
Saving to: 'pentmenu'

pentmenu          100%[=====] 48.39K  --.-KB/s   in 0.007s

2022-04-07 23:55:24 (6.52 MB/s) - 'pentmenu' saved [49548/49548]

root@kali:~# ls
Desktop Documents Downloads Music pentmenu Pictures Public Templates Videos
root@kali:~# chmod 777 pentmenu
root@kali:~# ls
Desktop Documents Downloads Music pentmenu Pictures Public Templates Videos
root@kali:~# ./pentmenu

```

Figure 7.2: Download and execute pentmenu script

```

1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>2
1) ICMP Echo Flood          6) TCP XMAS Flood          11) Distraction
2) ICMP Blacknurse         7) UDP Flood               12) DNS NXDOMAIN
3) TCP SYN Flood           8) SSL DOS                 13) Go back
4) TCP ACK Flood           9) Slowloris
5) TCP RST Flood           10) IPsec DOS
Pentmenu>7
UDP Flood uses hping3...checking for hping3...
hping3 found, continuing!
Enter target:
192.168.122.127
Enter target port (defaults to 80):
443
Using Port 443
Enter random string (data to send):
asdfasdfasfda
Enter Source IP, or [r]andom or [i]nterface IP (default):
i

```

Figure 7.3: Running UDP Flood

3. Go to **Policy & Object > IPV4 DOS Policy**:

- Name: **DOS**
- Incoming Interface: **Port1**
- Source, Destination, Service: **all**
- L3 Anomalies: Status and Logging: **Enable, Action Block**
- L4 Anomalies: Status and Logging: **Enable, Action Block**

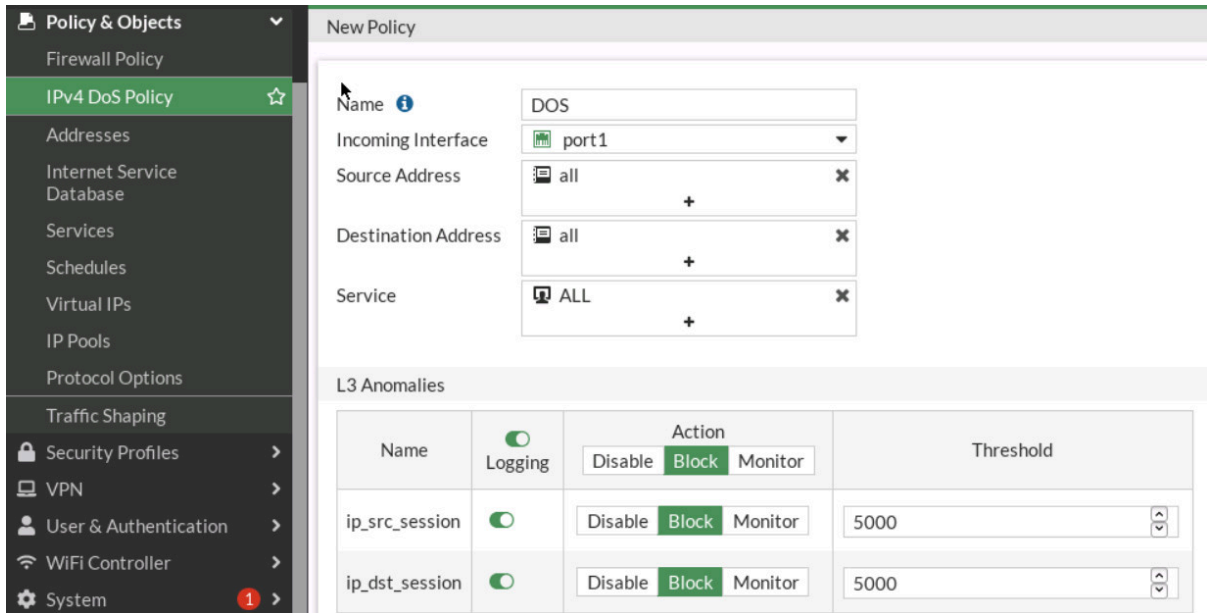


Figure 7.4: IPv4 DoS Policy

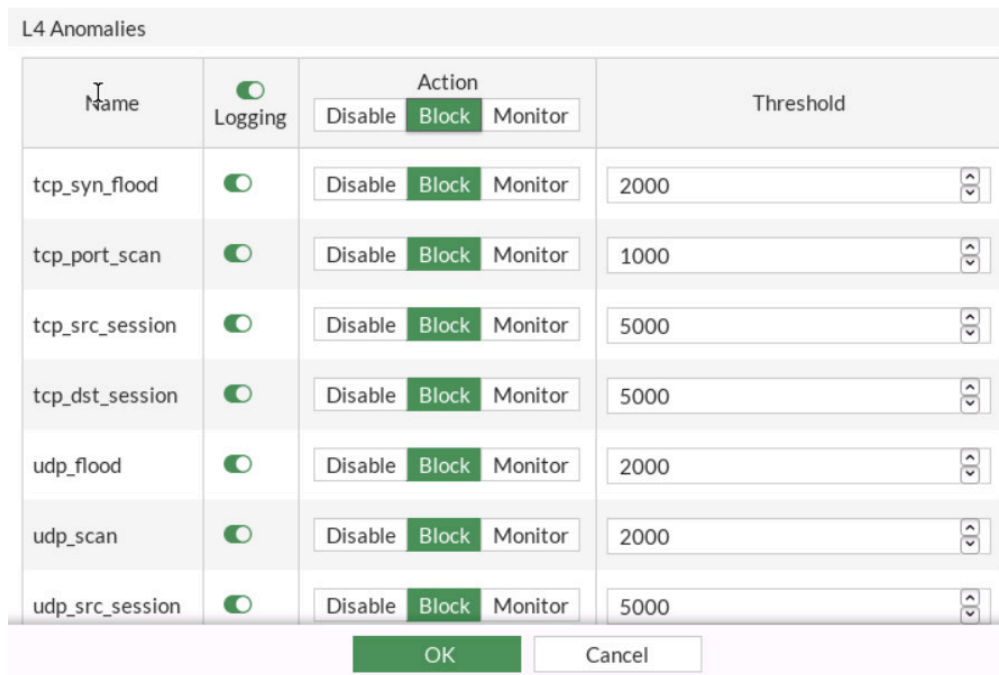


Figure 7.5: IPv4 DOS Policy Settings

4. Now, start the attack again and go to **Log & Report > Anomaly**.

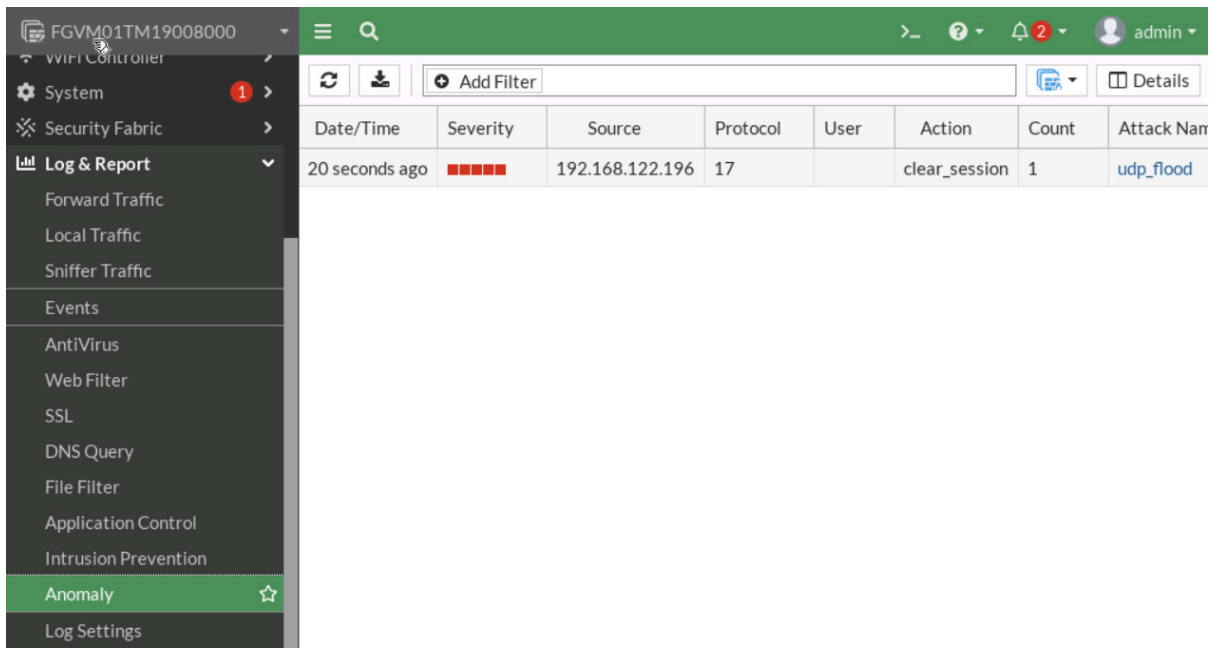


Figure 7.6: View anomaly report

Go to **Dashboard > Security > Top Threats** and verify your result.

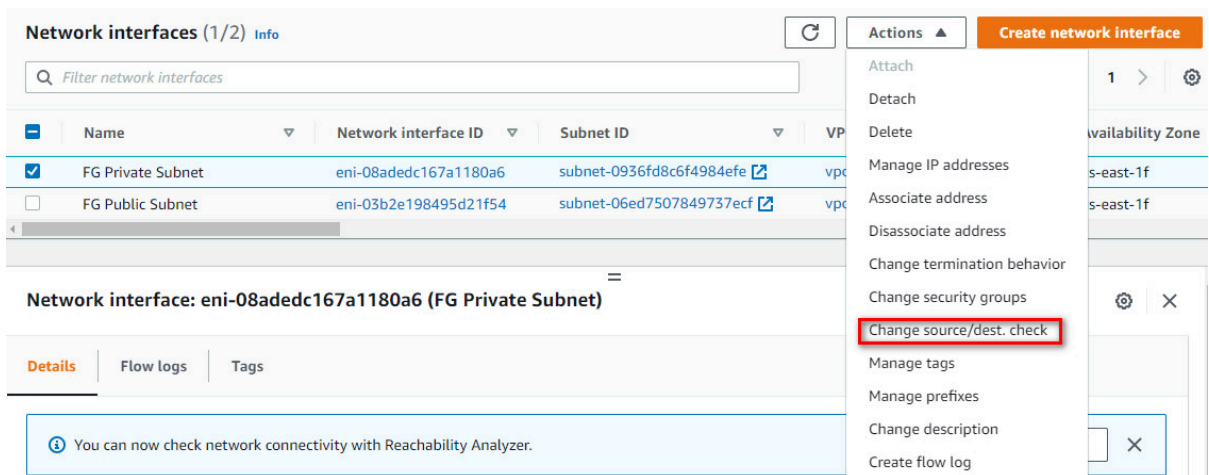


Figure 7.7: Verify result

5. Go to FortiGate CLI and configure DOS Policy for ICMP_flood as follows:

```
FGVM01TM19008000 # config firewall DoS-policy
FGVM01TM19008000 (DoS-policy) # edit 2
FGVM01TM19008000 (2) # set interface "port1"
FGVM01TM19008000 (2) # set srcaddr "all"
FGVM01TM19008000 (2) # set dstaddr "all"
FGVM01TM19008000 (2) # set service "ALL"
```

```

FGVM01TM19008000 (2) # config anomaly
FGVM01TM19008000 (anomaly) # edit "icmp_flood"
FGVM01TM19008000 (icmp_flood) # set status enable
FGVM01TM19008000 (icmp_flood) # set log enable
FGVM01TM19008000 (icmp_flood) # set quarantine attacker
FGVM01TM19008000 (icmp_flood) # set quarantine-expiry 2m
FGVM01TM19008000 (icmp_flood) # set quarantine-log disable
FGVM01TM19008000 (icmp_flood) # set threshold 10
FGVM01TM19008000 (icmp_flood) # next
FGVM01TM19008000 (anomaly) # end
FGVM01TM19008000 (2) # end

```

6. Go to Kali and run this command. First, 10 packets were allowed, and the 11th packet triggered the following block.
root@ubuntu:~# ping -c 2000 -i 0.01 *Port1-IP-Address*.

```

root@kali:~# ping -c 2000 -i 0.01 192.168.122.127
PING 192.168.122.127 (192.168.122.127) 56(84) bytes of data.
64 bytes from 192.168.122.127: icmp_seq=1 ttl=255 time=0.920 ms
64 bytes from 192.168.122.127: icmp_seq=2 ttl=255 time=0.657 ms
64 bytes from 192.168.122.127: icmp_seq=3 ttl=255 time=0.737 ms
64 bytes from 192.168.122.127: icmp_seq=4 ttl=255 time=0.664 ms
64 bytes from 192.168.122.127: icmp_seq=5 ttl=255 time=0.745 ms
64 bytes from 192.168.122.127: icmp_seq=6 ttl=255 time=0.678 ms
64 bytes from 192.168.122.127: icmp_seq=7 ttl=255 time=0.750 ms
64 bytes from 192.168.122.127: icmp_seq=8 ttl=255 time=0.632 ms
64 bytes from 192.168.122.127: icmp_seq=9 ttl=255 time=0.688 ms
64 bytes from 192.168.122.127: icmp_seq=10 ttl=255 time=0.667 ms
64 bytes from 192.168.122.127: icmp_seq=11 ttl=255 time=0.628 ms
64 bytes from 192.168.122.127: icmp_seq=12 ttl=255 time=0.674 ms

```

Figure 7.8: Verify DOS prevention

7.2 Security Profile

Learning Objectives

- Configure a Security Profile

Scenario: In this lab, we are going to become familiar with different types of Security Profile such as AntiVirus, File Filter, IPS and DNS Filter. WebTerm2 acts as a local computer and we set a Security Profile on traffic passing from Port2 to Port1.

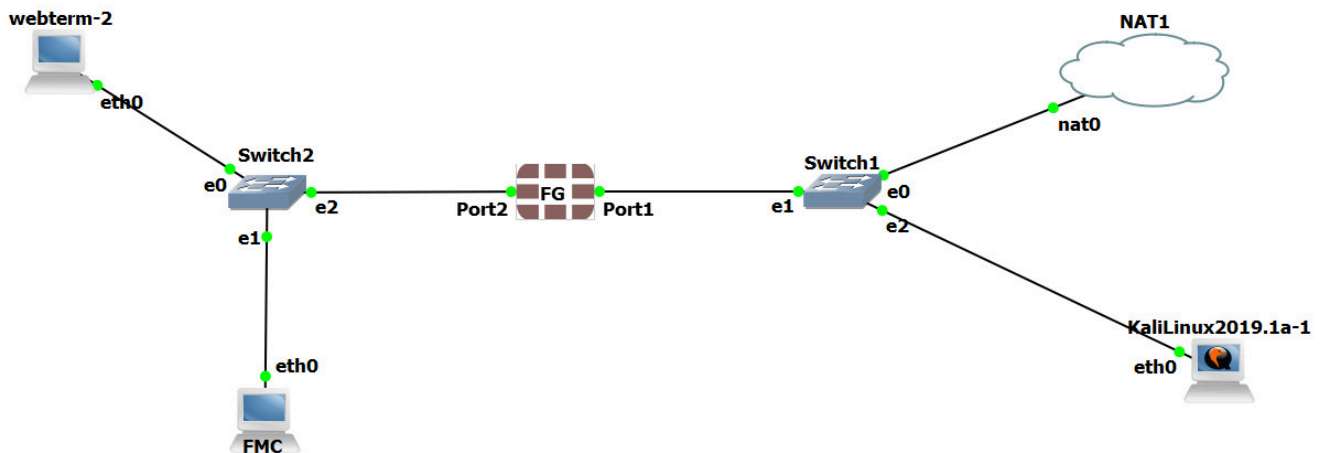


Figure 7.9: Main scenario

1. We will continue the previous scenario and set up a DHCP server on port2.

DHCP Server

DHCP status: **Enabled** Disabled

Address range: 192.168.0.10-192.168.0.20

Netmask: 255.255.255.0

Default gateway: **Same as Interface IP** Specify

DNS server: Same as System DNS Same as Interface IP **Specify**

DNS server 1: 4.2.2.4

Lease time: 604800 second(s)

Advanced

Figure 7.10: Enable DHCP Server on port2

2. Go to **security profile > Anti-Virus**, create a new profile:
 - Name: **myantivirus**
 - Scan Mode: **full**
 - Inspection Protocol: **HTTP, SMTP, IMAP, POP3, FTP**

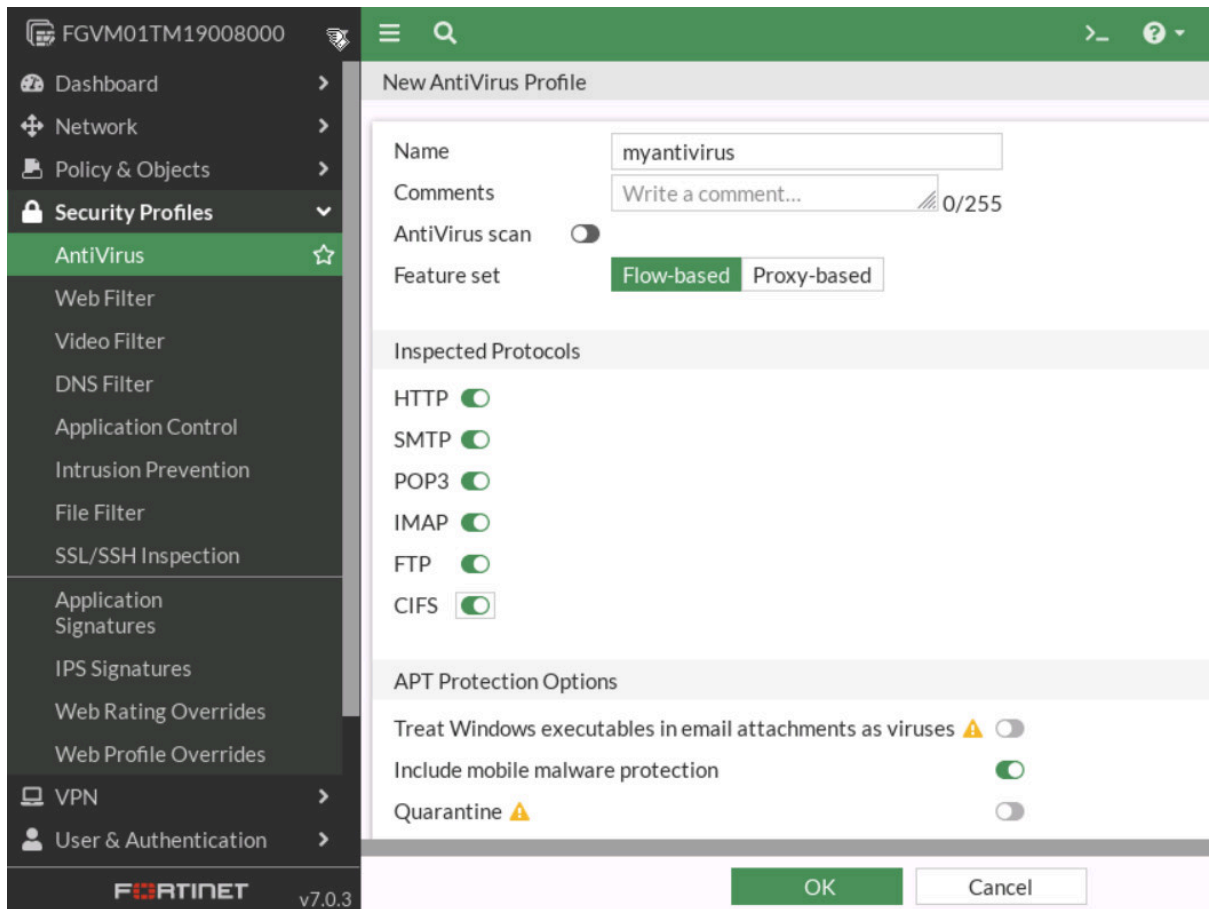


Figure 7.11: AntiVirus Profile

3. Create a Firewall policy:

- Name: **Port2-to-Port1**
- Incoming Interface: **Port2**
- Outgoing interface: **port1**
- Source, Destination, Service: **all**
- Security Profile: **myantivirus**

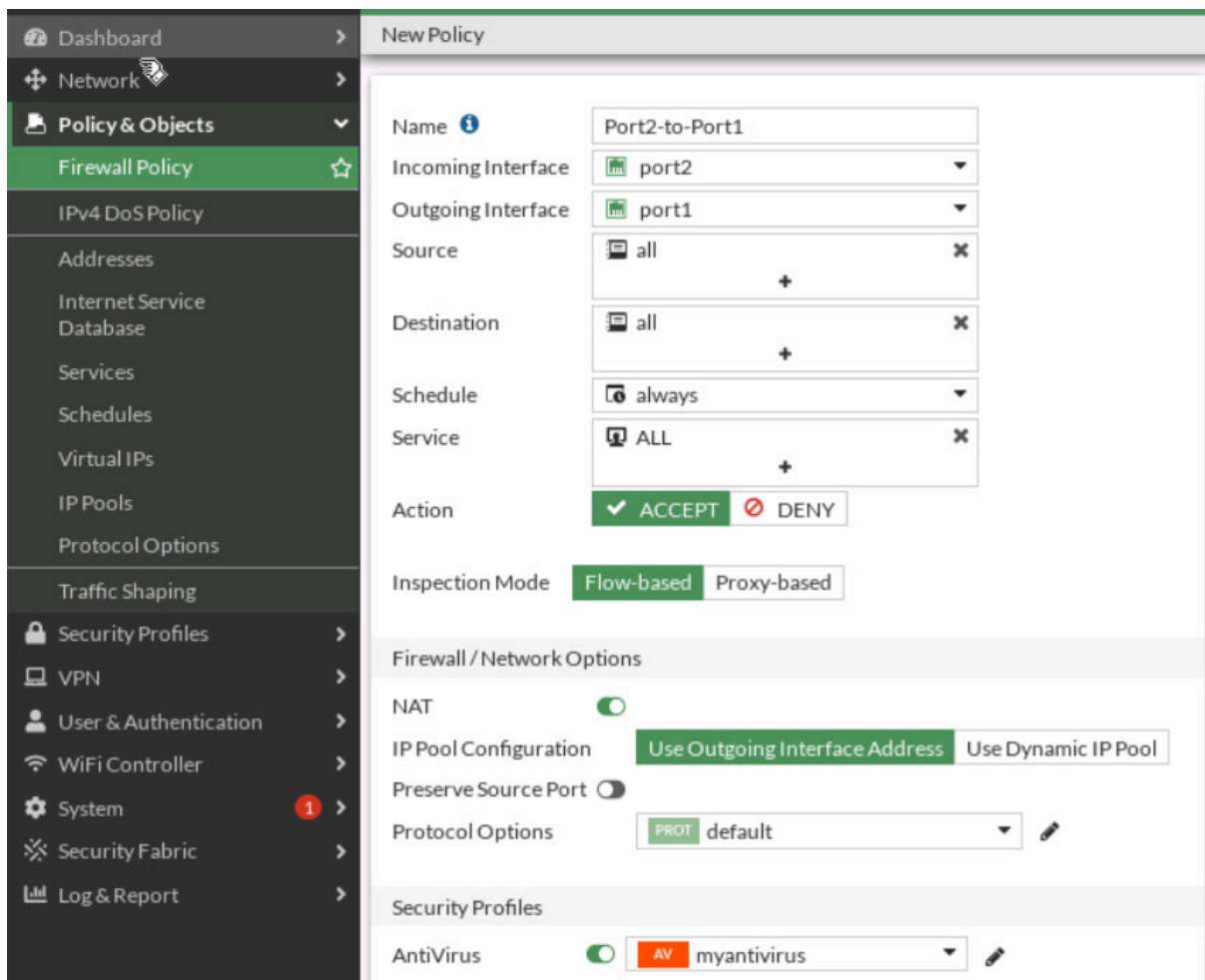


Figure 7.12: Create a Firewall Policy and assign AntiVirus Profile

4. Go to **Security Profile** > **File Filter**, Create a new profile:

- Name: **MyFileFilter**
- Create a New Filter rule
 - Name: **Block-PDF-ZIP**
 - Protocols: **HTTP-FTP**
 - File Type: **PDF-ZIP**
 - Action: **Block**
 - Direction: **any**

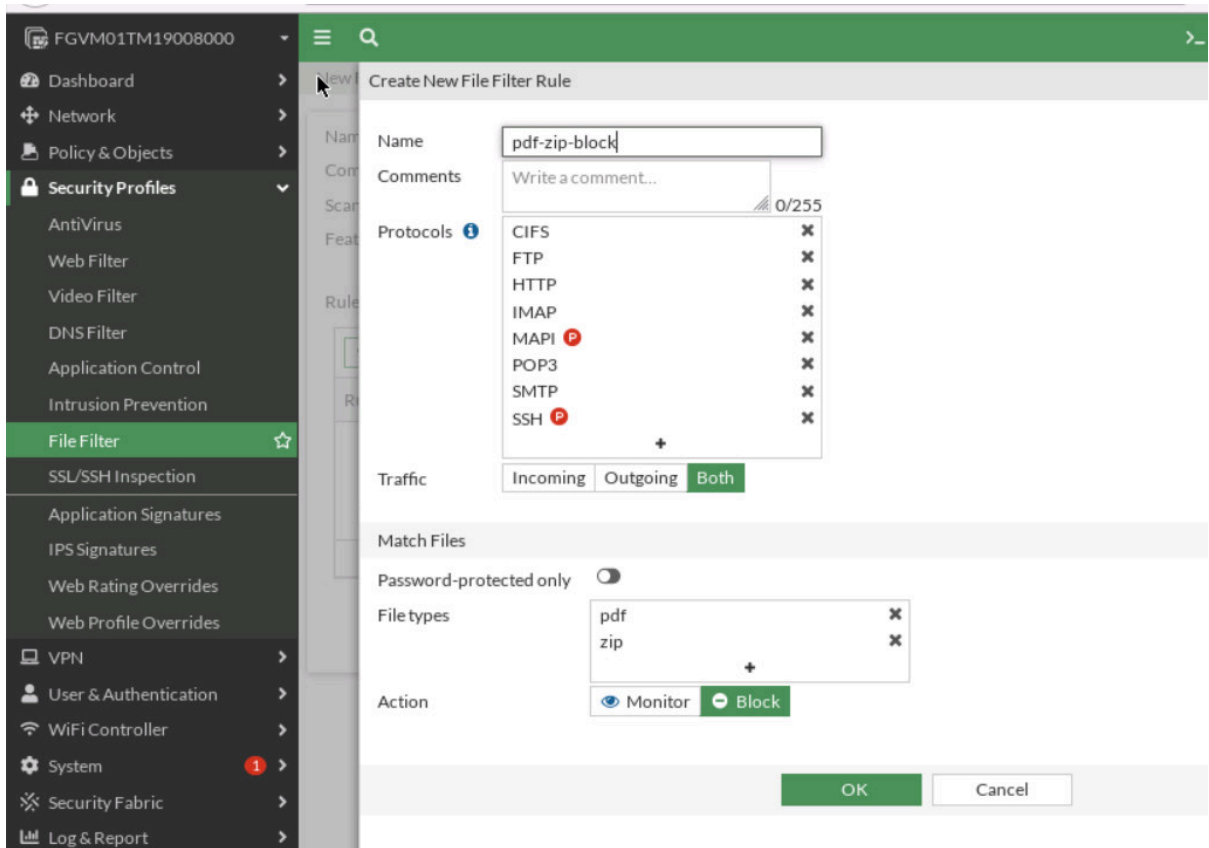


Figure 7.13: File Filter profile

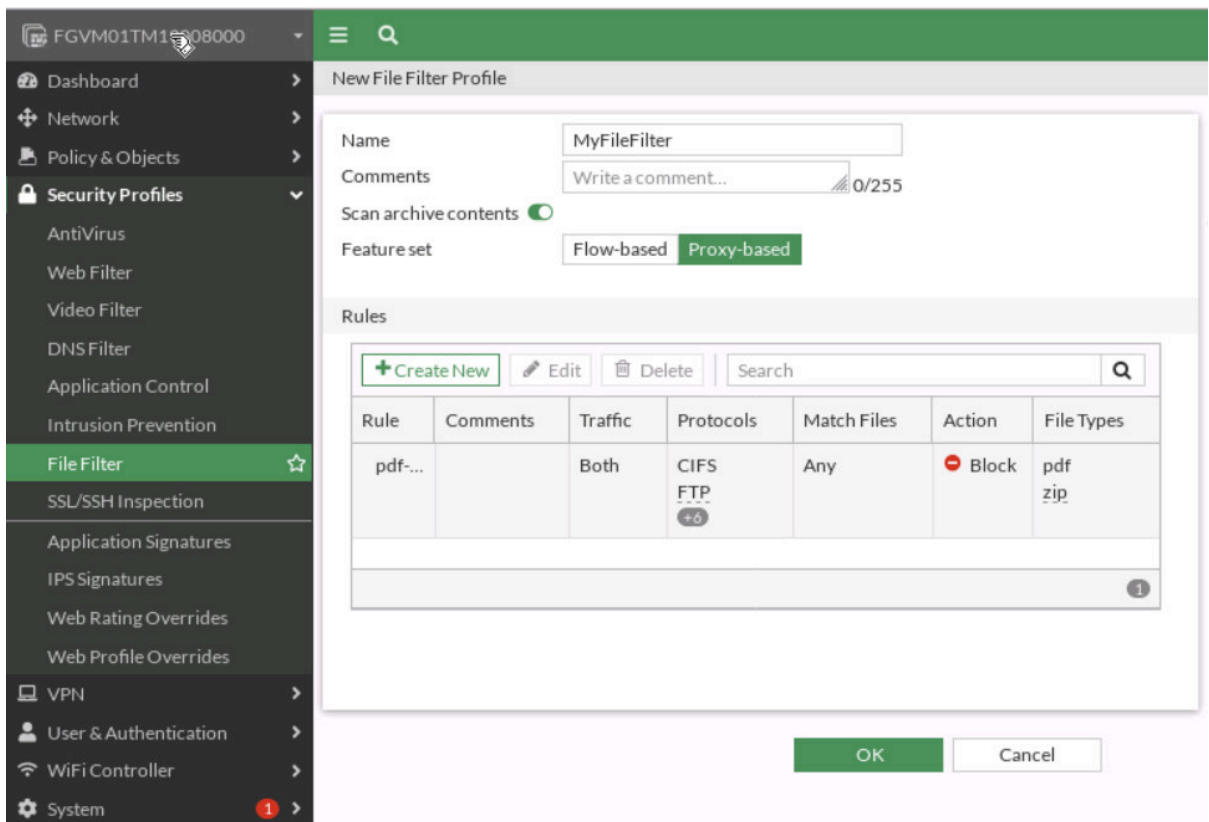


Figure 7.14: Blocking Pdf-Zip

- Set the firewall Policy to **Proxy mode**.
- Go to **Policy & Objects > Firewall Policy** and assign MyFileFilter to the “Port2-to-Port1” policy.

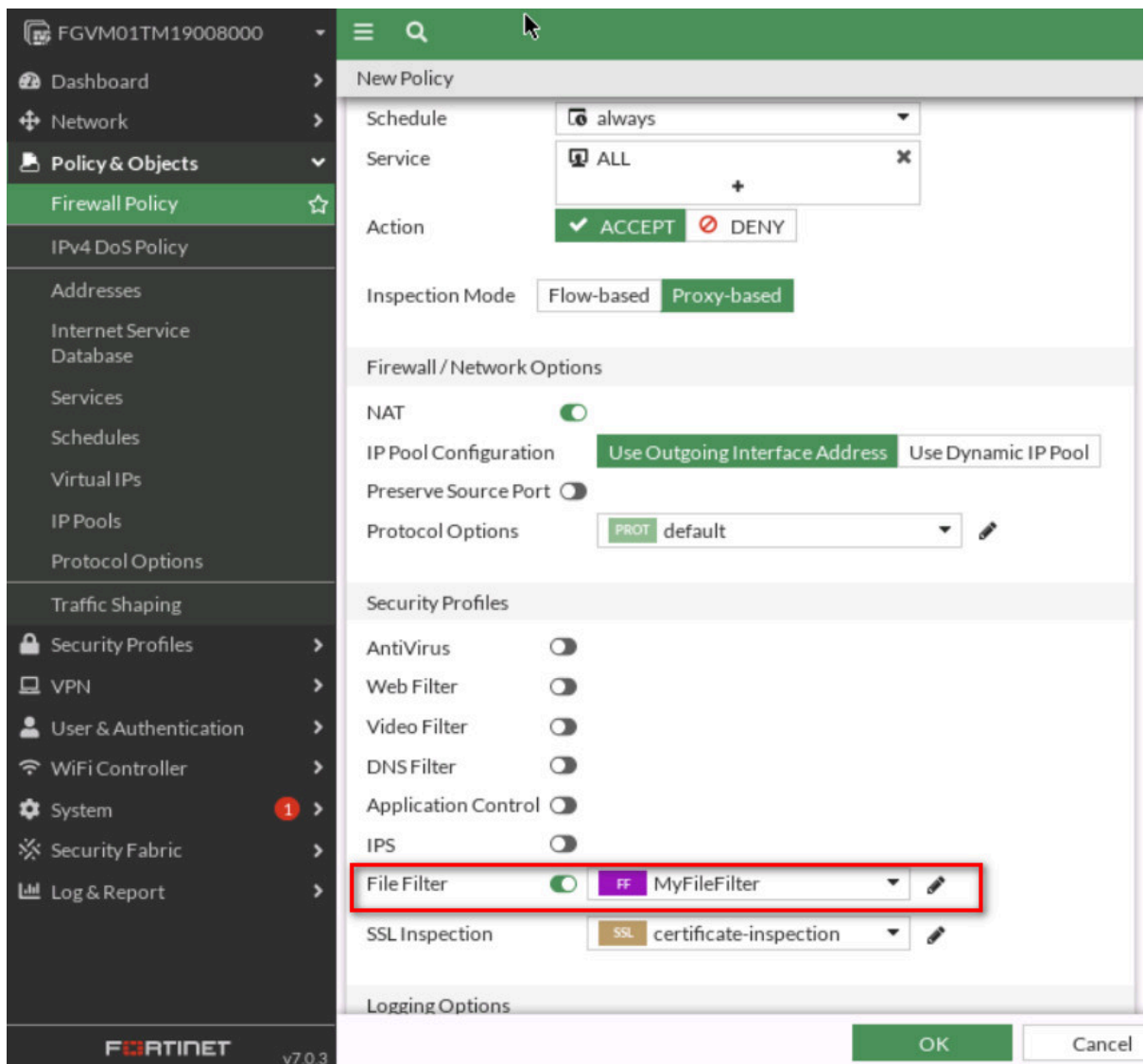


Figure 7.15: Assign File Filter profile to Firewall Policy

5. Go to <http://talebi.ca/wp-content/uploads/2021/11/prtgdesktop.pdf> and verify your result.

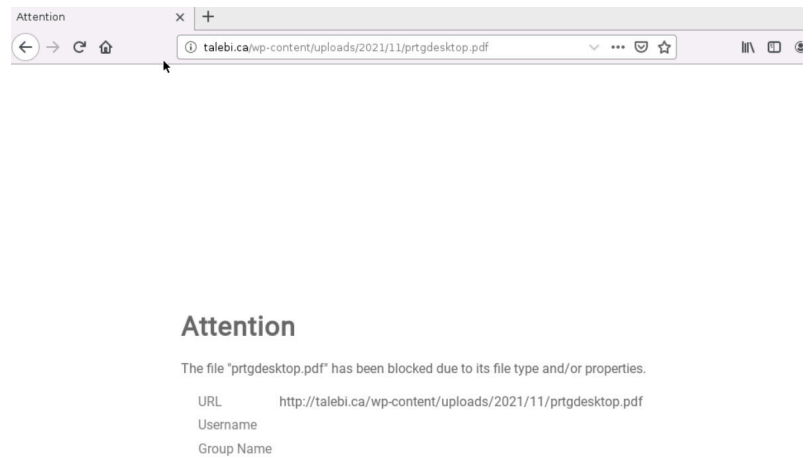


Figure 7.16: Verify configuration

6. Go to **Security Profile > Intrusion Prevention**, create a new profile:

- Name: **MyIPS**
- Add Signature: **AAEH Botnet, Acunetix Web Vulnerability Scanner, Adobe Flash Player CSRF**

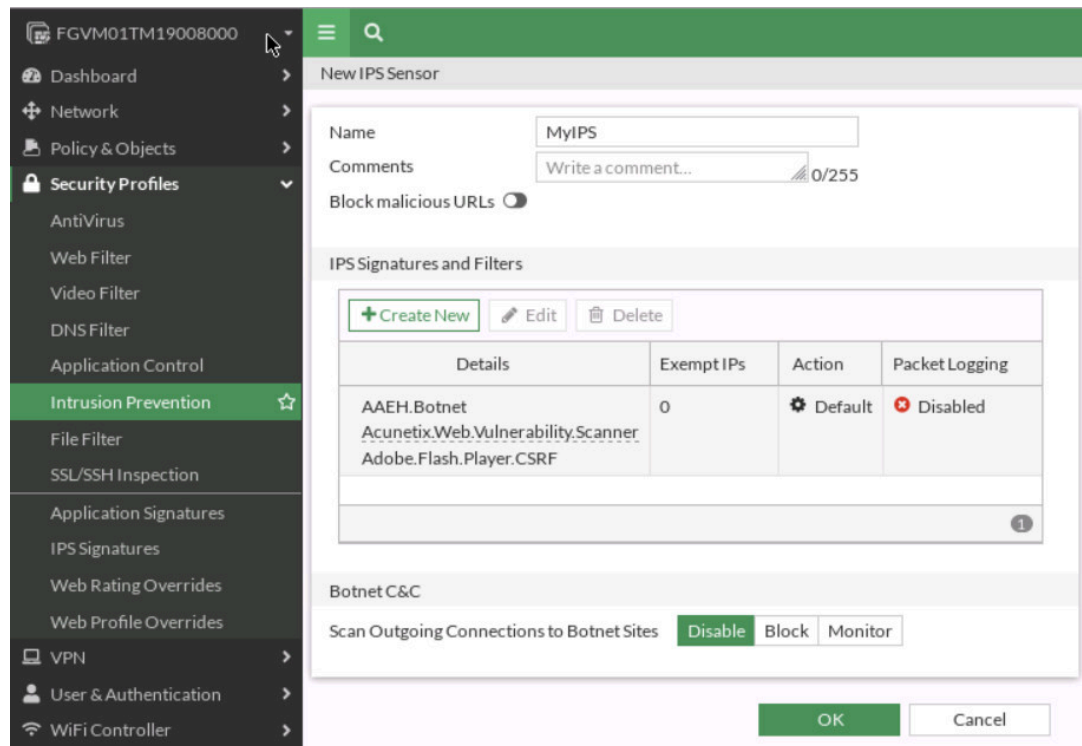


Figure 7.17: Intrusion Prevention Profile

7. Go to **Policy & Objects > Firewall Policy** and assign MyIPS to the “Port2-to-Port1” policy.

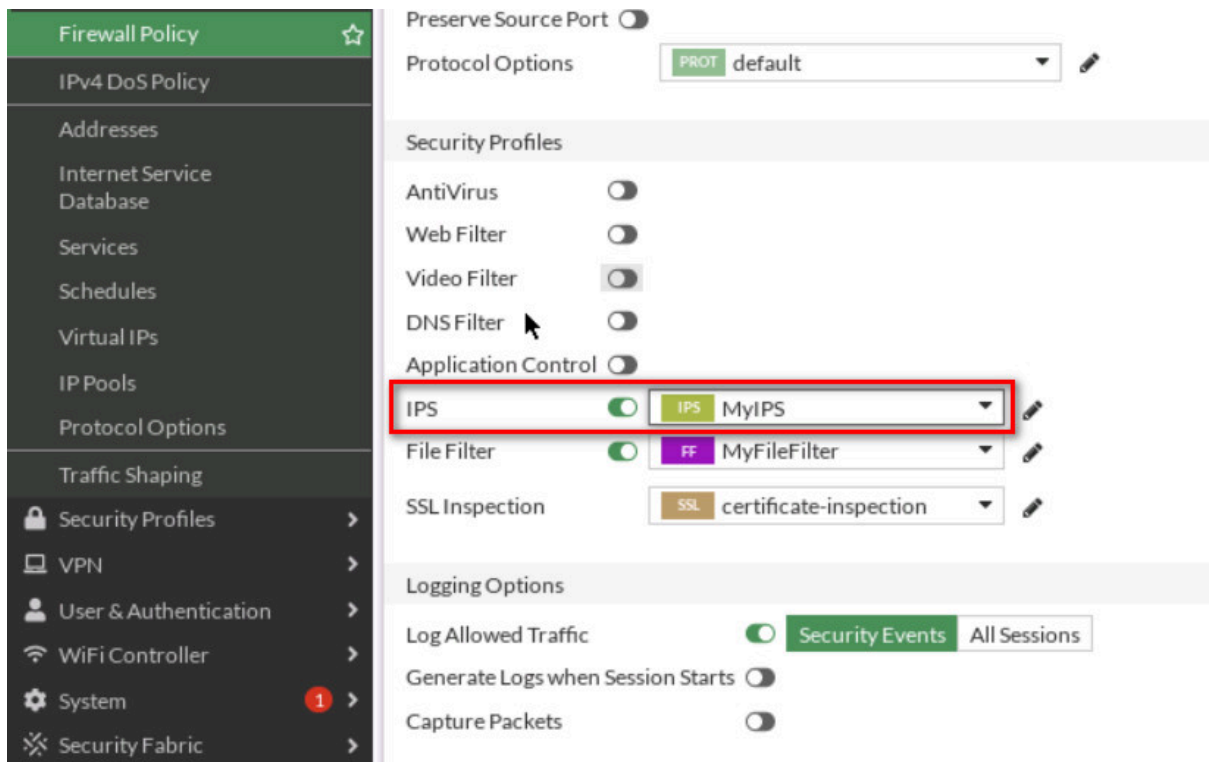


Figure 7.18: Assign IPS profile to Firewall Policy

8. Go to **Security Profile > DNS Filter**, create a new profile:
 - Name: **MyDNS**
 - FortiGate Category Based Filter:
 - Bandwidth Consuming: **Peer-to-Peer File Sharing: Block, Internet Radio and TV: Block**

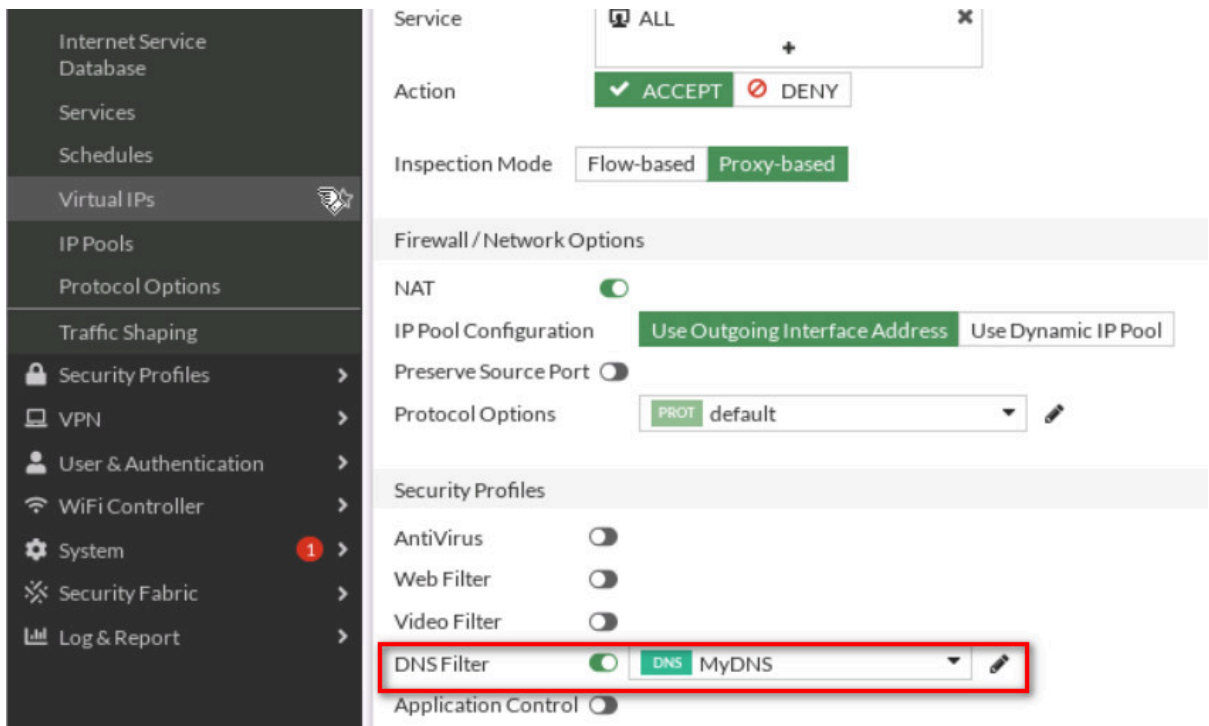


Figure 7.19: Assign DNS Filter Profile to Firewall Policy

You can verify your configuration by visiting <http://talebi.ca>.

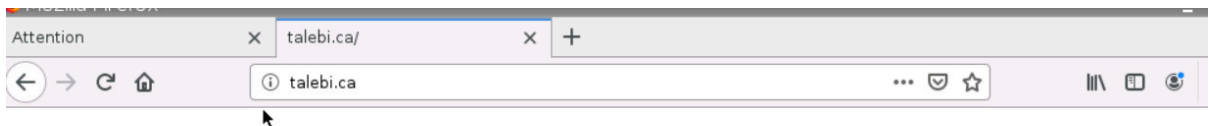


Figure 7.20: Verify configuration

Verify your **Log & Report > DNS Query**.

Date/Time	DNS Type	Source	Domain Name	Query Type	Policy ID
4 minutes ago	dns-response	192.168.0.4	talebi.ca	A	1
4 minutes ago	dns-response	192.168.0.4	talebi.ca	A	1
4 minutes ago	dns-response	192.168.0.4	talebi.ca	A	1
6 minutes ago	dns-response	192.168.0.4	talebi.ca	A	1
6 minutes ago	dns-response	192.168.0.4	fonts.gstatic.com	A	1
6 minutes ago	dns-response	192.168.0.4	globalurl.fortinet.net	A	1
6 minutes ago	dns-response	192.168.0.4	fonts.googleapis.com	A	1
6 minutes ago	dns-response	192.168.0.4	www.facebook.com	A	1
6 minutes ago	dns-response	192.168.0.4	www.youtube.com	A	1
6 minutes ago	dns-response	192.168.0.4	getpocket.com	A	1
6 minutes ago	dns-response	192.168.0.4	fonts.googleapis.com	A	1
6 minutes ago	dns-response	192.168.0.4	fonts.googleapis.com	A	1
6 minutes ago	dns-response	192.168.0.4	fonts.googleapis.com	A	1
6 minutes ago	dns-response	192.168.0.4	fonts.googleapis.com	A	1

Figure 7.21: Verify

7.3 VLAN and Security Profile

Learning Objectives

- Configure VLANs in FortiGate firewall
- Configure a Security Policy for VLANs

Scenario: In this lab, we are going to learn how to set VLAN on Port2 of the firewall. WebTerm1 is belong to Vlan10 and WebTerm2 is belong to Vlan20. We will set different policies on each VLAN and try to verify configuration.

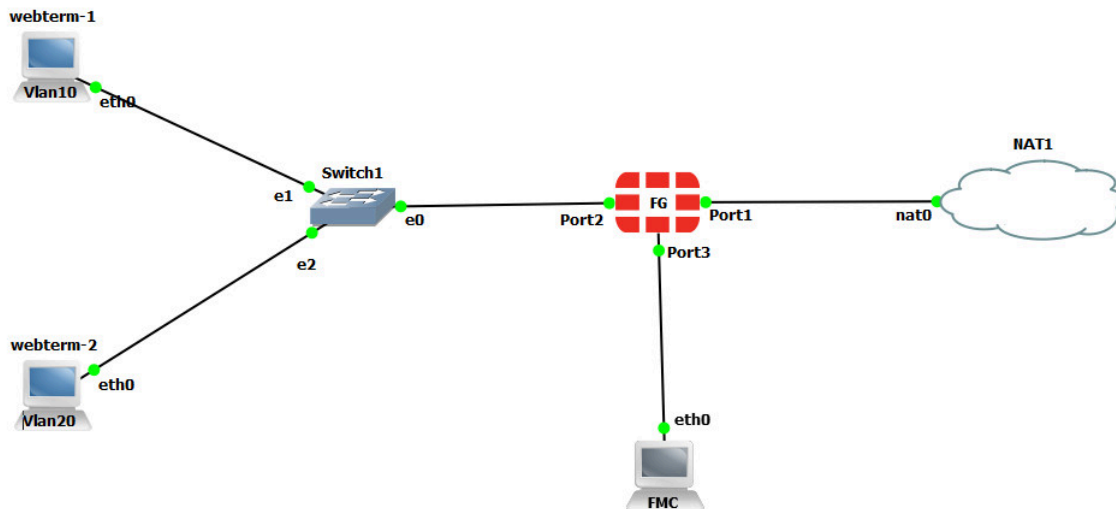


Figure 7.22: Main scenario

Table 7.2: Devices configuration

Device	IP address	Access
FortiGate	Port 1: DHCP Client Port 2: Vlan 10: 192.168.10.1/24 Vlan 20: 192.168.20.1/24	ICMP-HTTP-HTTPS
WebTerm1	DHCP Client	–
WebTerm2	DHCP Client	–

1. Configure switches. Right-click on the **Switch > Configure**, configure eth0, eth1, and eth2 as Table 7.3:

Table 7.3: Switch configuration

Port	VLAN	Type
0	1	Dot1q
1	10	Access
2	20	Access

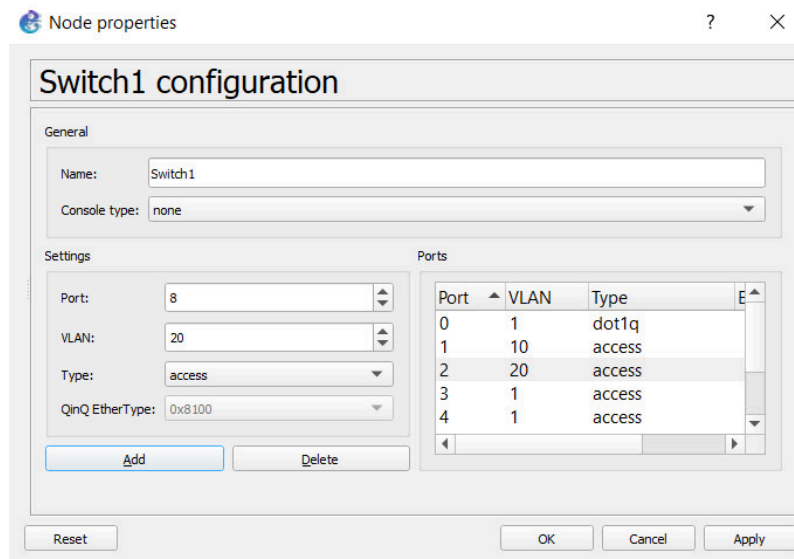


Figure 7.23: Switch configuration

2. You should create two sub-interfaces on port2 of the firewall.

The screenshot shows the 'New Interface' configuration window in the Fortinet management console. The left sidebar contains a navigation menu with 'Network' expanded and 'Interfaces' selected. The main configuration area is titled 'New Interface' and contains the following fields:

- Name: Vlan10
- Alias: (empty)
- Type: VLAN
- VLAN protocol: 802.1Q (selected), 802.1AD
- Interface: port2
- VLAN ID: 10
- VRF ID: 0
- Role: LAN

The 'Address' section is also visible:

- Addressing mode: Manual (selected), DHCP, Auto-managed by IPAM
- IP/Netmask: 192.168.10.1/24
- Create address object matching subnet:
- Name: Vlan10 address
- Destination: 192.168.10.1/24
- Secondary IP address:

At the bottom of the window are 'OK' and 'Cancel' buttons. The Fortinet logo and version 'v7.0.5' are visible in the bottom left corner of the sidebar.

Figure 7.24: Vlan10 Configuration

The screenshot shows the 'New Interface' configuration window in the Fortinet management console, similar to Figure 7.24 but for a different VLAN. The left sidebar is the same. The main configuration area is titled 'New Interface' and contains the following fields:

- Name: Vlan20
- Alias: (empty)
- Type: VLAN
- VLAN protocol: 802.1Q (selected), 802.1AD
- Interface: port2
- VLAN ID: 20
- VRF ID: 0
- Role: LAN

The 'Address' section is also visible:

- Addressing mode: Manual (selected), DHCP, Auto-managed by IPAM
- IP/Netmask: 192.168.20.1/24
- Create address object matching subnet:
- Name: Vlan20 address
- Destination: 192.168.20.1/24
- Secondary IP address:

At the bottom of the window are 'OK' and 'Cancel' buttons. The Fortinet logo and version 'v7.0.5' are visible in the bottom left corner of the sidebar.

Figure 7.25: Vlan20 Configuration

port2	Physical Interface	0.0.0.0/0.0.0.0
vlan10	VLAN	192.168.10.1/255.255.255.0
vlan20	VLAN	192.168.20.1/255.255.255.0

Figure 7.26: Vlan10 and Vlan20 IP addresses

3. Block YouTube and Social Media on Vlan 20:

1. Create an application profile as Figure 7.27.

i 93 Cloud Applications require deep inspection.
0 policies are using this profile.

Name:

Comments: 0/255

Categories

<input type="button" value="Business (179, ☁ 6)"/>	<input type="button" value="Cloud.IT (31)"/>	<input type="button" value="Collaboration (293, ☁ 6)"/>
<input type="button" value="Email (87, ☁ 12)"/>	<input type="button" value="Game (124)"/>	<input type="button" value="General.Interest (241, ☁ 9)"/>
<input type="button" value="Mobile (3)"/>	<input type="button" value="Network.Service (332)"/>	<input type="button" value="P2P (85)"/>
<input checked="" type="button" value="Proxy (106)"/>	<input type="button" value="Remote.Access (91)"/>	<input checked="" type="button" value="Social.Media (150, ☁ 31)"/>
<input type="button" value="Storage.Backup (296, ☁ 16)"/>	<input type="button" value="Update (48)"/>	<input checked="" type="button" value="Video/Audio (206, ☁ 13)"/>
<input type="button" value="VoIP (31)"/>	<input type="button" value="Web.Client (18)"/>	<input checked="" type="button" value="Unknown Applications"/>

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
No results			

Figure 7.27: Block Social.Media and Video/Audio

2. Configure Firewall Policy from Vlan 20 to Port1 and assign application control to the Firewall Policy.

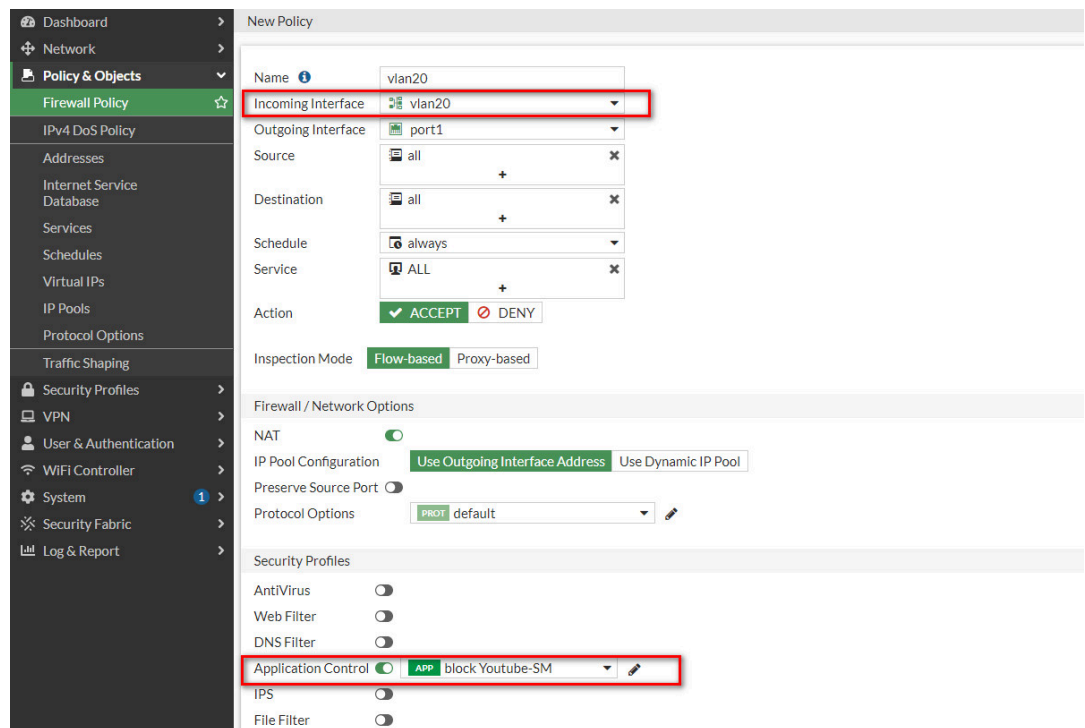


Figure 7.28: Create vlan20 Firewall Policy and assign Application Control Profile

3. Verify your configuration by visiting Twitter.com or YouTube.com.



Figure 7.29: Verify configuration

4. Filter .zip, .pdf files on Vlan 10:

1. Create a File filter profile. File filter only works on the unencrypted protocol. Set traffic for both and finally set the action to block.

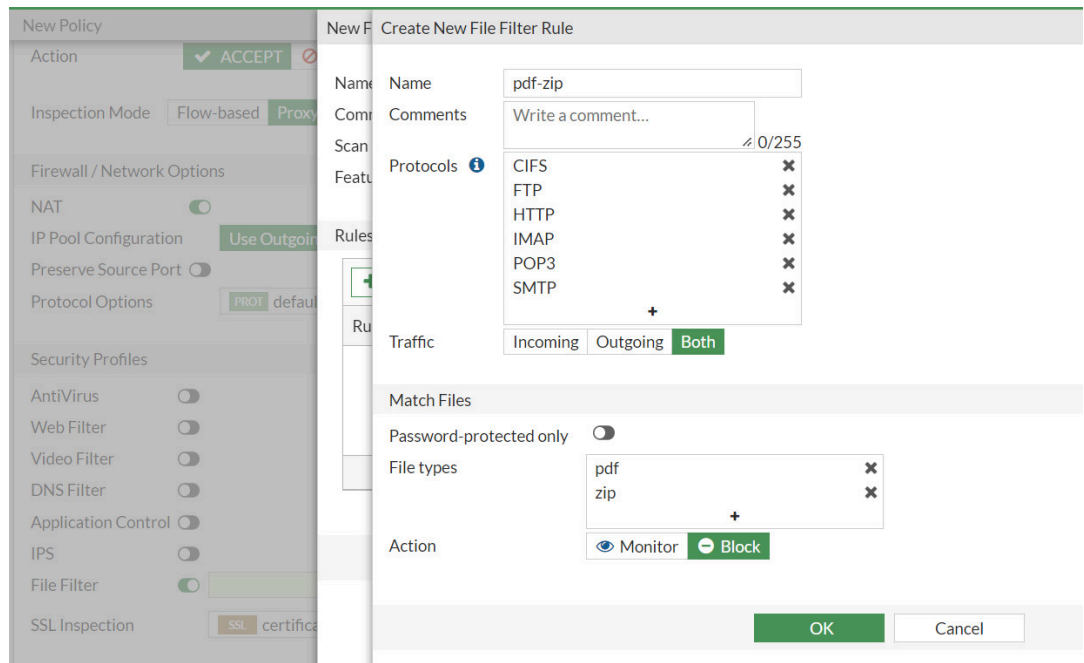


Figure 7.30: Block PDF and ZIP files

2. Make sure to set the feature set as flow-based.

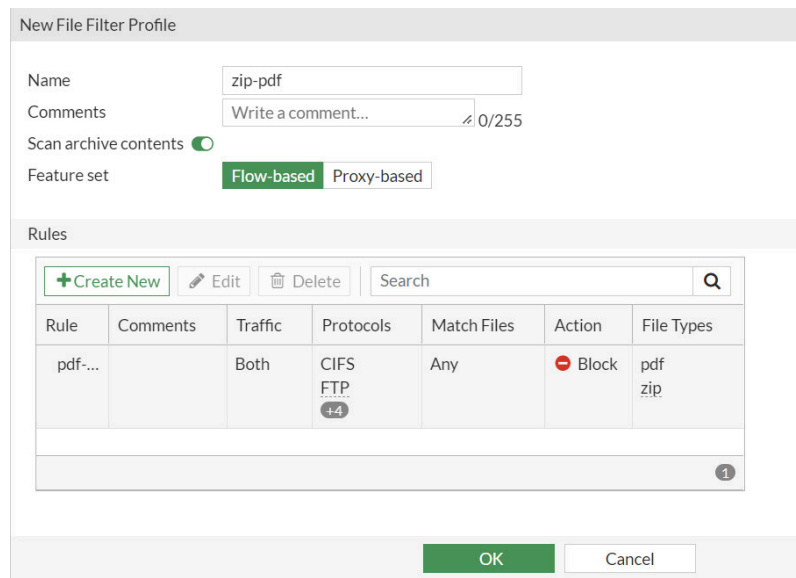


Figure 7.31: Block profile

3. Create a Firewall Policy in the firewall from vlan10 to port1, inspection mode should be Proxy-based, and assign the profile you have created to File Filter.

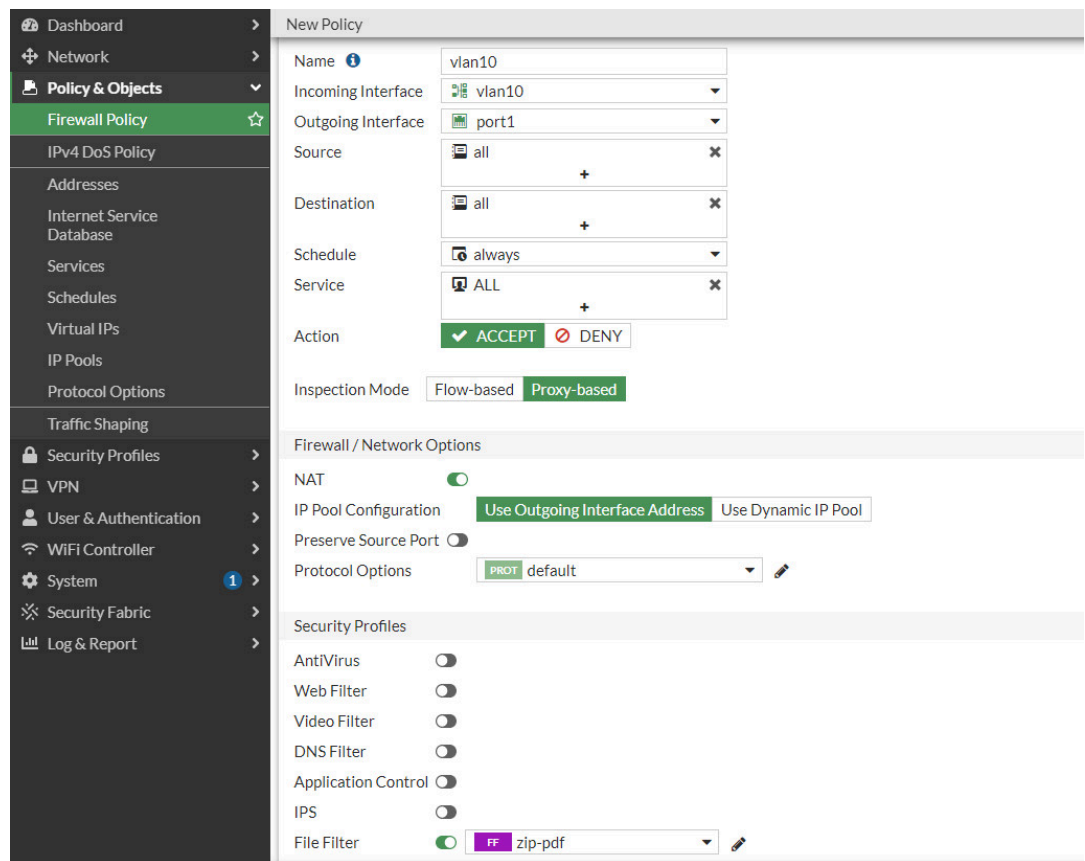


Figure 7.32: Create vlan10 Firewall Policy and assign File Filter Profile

- Verify your configuration by downloading a zip or pdf file from HTTP websites.

Attention

The file "prtgdsktop.pdf" has been blocked due to its file type and/or properties.

URL <http://talebi.ca/wp-content/uploads/2021/11/prtgdesktop.pdf>

Username

Group Name

Figure 7.33: Verify configuration

Chapter 8. VDOM

8.1 VDOM

Learning Objectives

- Create a VDOM
- Configure a security policy in VDOMs

Scenario: This example illustrates how to use VDOMs to host two FortiOS instances on a single FortiGate unit.

Virtual Domains (VDOMs) can be used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function as independent FortiGate units. This example simulates an ISP that provides Company A and Company B with distinct internet services. Each company has its own VDOM, IP address, and internal network.

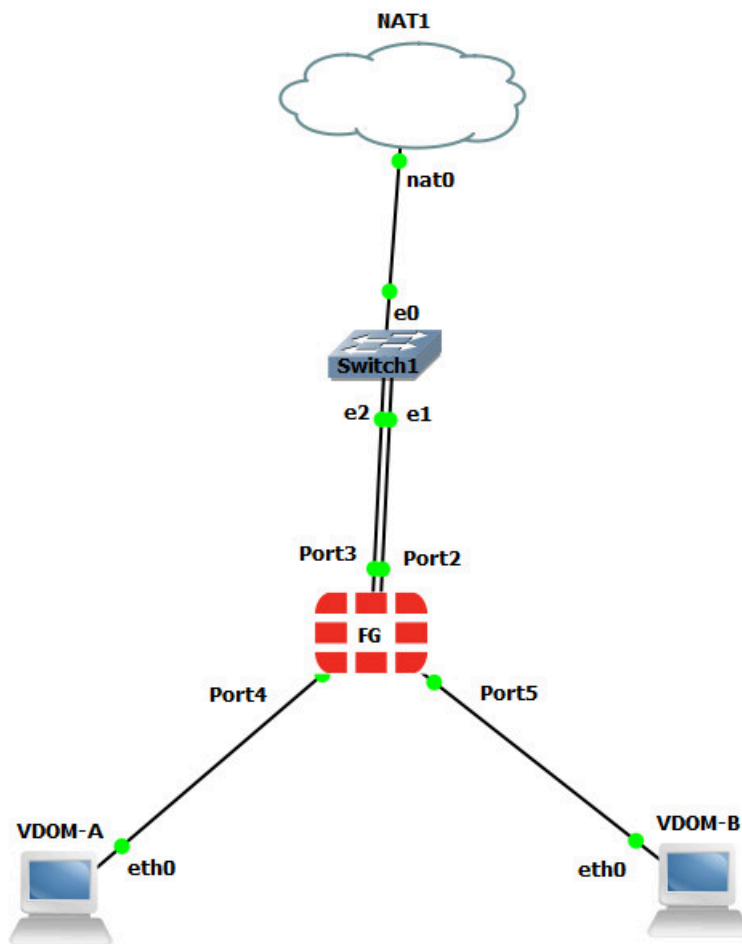


Figure 8.1: Main scenario

Enable VDOMs

Table 8.1: Devices configuration

Device	IP address	Access
WebTerm-VDOMA	DHCP Client	HTTPS
WebTerm-VDOMB	DHCP Client	HTTPS
FortiGate	Port 2: DHCP Client – VDOM B Port 3: DHCP Client – VDOM A Port 4: DHCP SERVER – VDOM A Port 5: DHCP SERVER – VDOM B	Port 2 – Management Access
Ethernet Switch	–	–
NAT	–	–

1. In order to enable Virtual Domains, the following CLI command is required:

```
config system global
set vdom-mode multi-vdom
end
```

2. Log out FortiGate and log in again. You should be able to see the Figure 8.2 result.

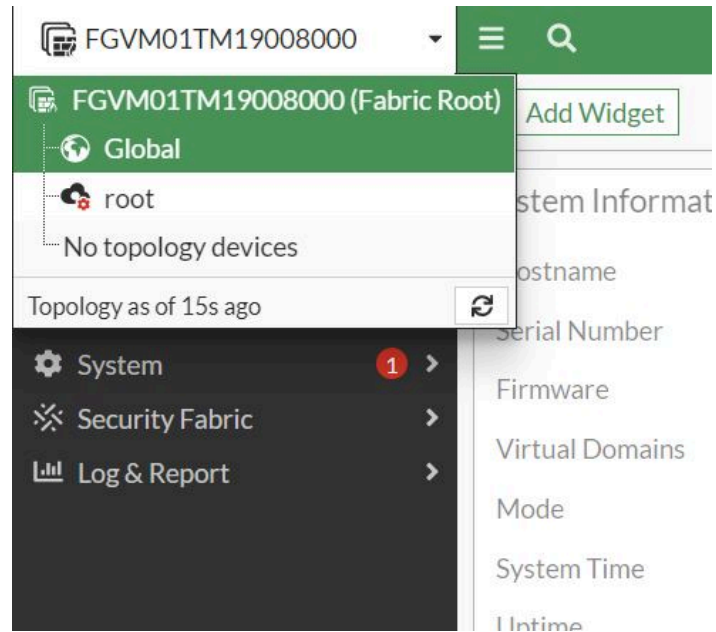


Figure 8.2: Default VDOMs

3. Go to **Global > System > VDOM**. Create two VDOMs, **VDOM-A** and **VDOM-B**. Leave both VDOMs as Enabled, with Operation Mode set to **NAT** and NGFW mode to **profile-based**.

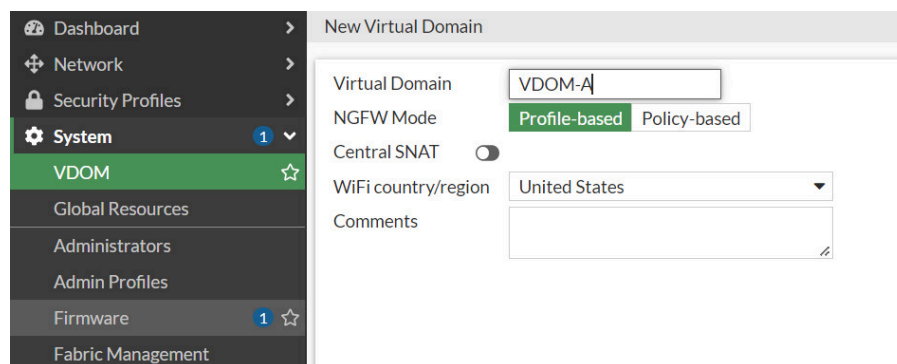


Figure 8.3: VDOM-A configuration

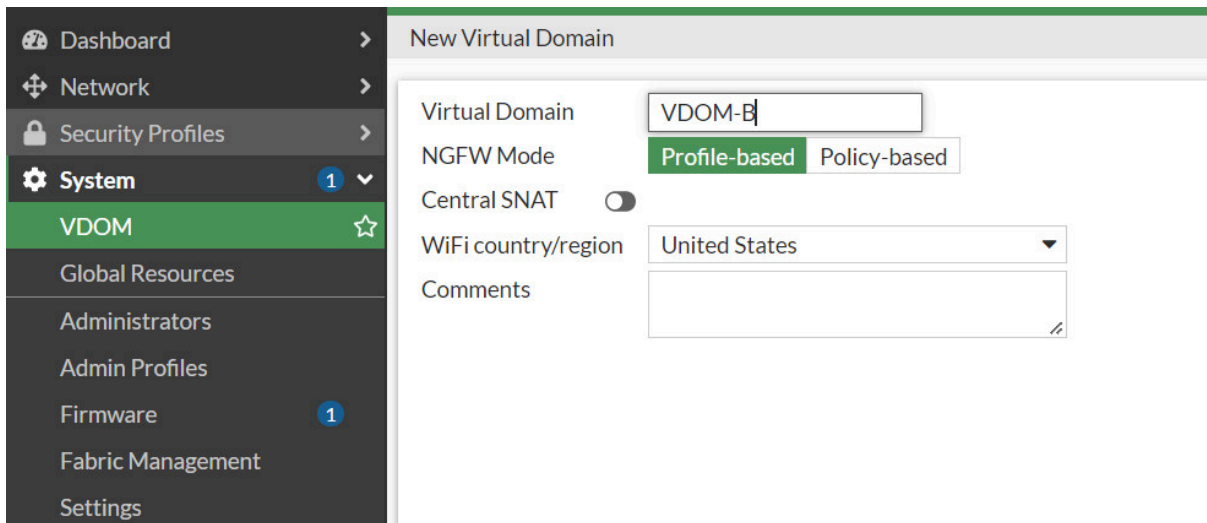


Figure 8.4: VDOM-B configuration

4. Go to **Global > Network > Interfaces**. Edit Port2 and add it to VDOM-B. Set Addressing Mode to **DHCP**.

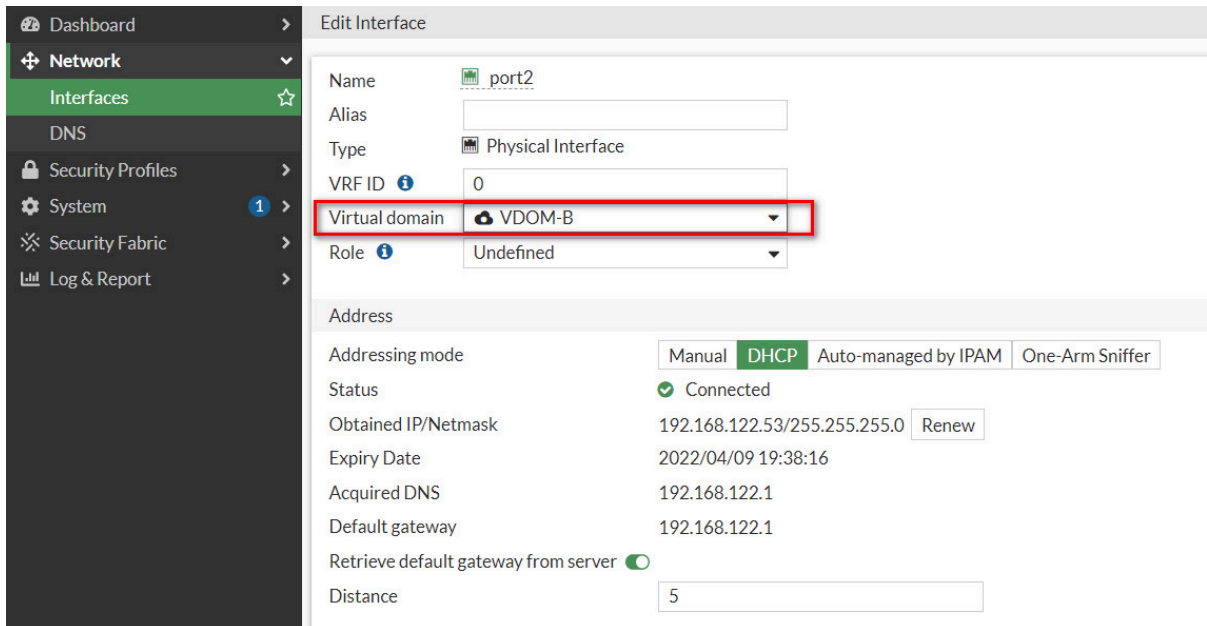


Figure 8.5: Port2 configuration

If the port is under root and you can't modify it to VDOM-B, you should first delete the references related to the port.

5. Go to **Global > Network > Interfaces**. Edit Port4 and add it to VDOM-A. Set Addressing Mode to Manual and assign an IP/Network mask to the interface (192.168.91.1/255.255.255.0) and finally Enable DHCP Server.

The screenshot shows the 'Edit Interface' configuration for 'port4'. The left sidebar contains navigation options: Dashboard, Network, Interfaces (selected), DNS, Security Profiles, System, Security Fabric, and Log & Report. The main configuration area includes:

- Name: port4
- Alias: (empty)
- Type: Physical Interface
- VRF ID: 0
- Virtual domain: VDOM-A (highlighted with a red box)
- Role: Undefined
- Addressing mode: Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask: 192.168.91.1/255.255.255.0 (highlighted with a red box)
- Secondary IP address: (disabled)
- Administrative Access:
 - IPv4:
 - HTTPS:
 - HTTP:
 - PING:
 - FMG-Access:
 - SSH:
 - SNMP:
 - FTM:
 - RADIUS Accounting:
 - Security Fabric Connection:
 - Speed Test:
 - Receive LLDP: Use VDOM Setting, Enable, Disable
 - Transmit LLDP: Use VDOM Setting, Enable, Disable
- DHCP Server:
 - Enabled (checked)
 - DHCP status: Enabled (green), Disabled (red)
 - Address range: 192.168.91.2-192.168.91.254 (highlighted with a red box)

Figure 8.6: Port4 configuration

- Go to **Global > Network > Interfaces**. Edit Port3 and add it to VDOM-A and set Addressing Mode to DHCP.

The screenshot shows the 'Edit Interface' configuration for 'port3'. The left sidebar is the same as in Figure 8.6. The main configuration area includes:

- Name: port3
- Alias: (empty)
- Type: Physical Interface
- VRF ID: 0
- Virtual domain: VDOM-A (highlighted with a red box)
- Role: Undefined
- Addressing mode: Manual, DHCP (selected), Auto-managed by IPAM, One-Arm Sniffer
- Status: Connected (checked)
- Obtained IP/Netmask: 192.168.122.54/255.255.255.0 (with a Renew button)
- Expiry Date: 2022/04/09 19:38:16
- Acquired DNS: 192.168.122.1
- Default gateway: 192.168.122.1
- Retrieve default gateway from server: (checked)
- Distance: 5

Figure 8.7: Port3 configuration

- Go to **Global > Network > Interfaces**. Edit Port5 and add it to VDOM-B. Set Addressing Mode to Manual and assign an IP/Network Mask to the interface (192.168.92.1/255.255.255.0) and set Administrative Access to **HTTPS**, **PING**, and **SSH**. Enable DHCP Server.

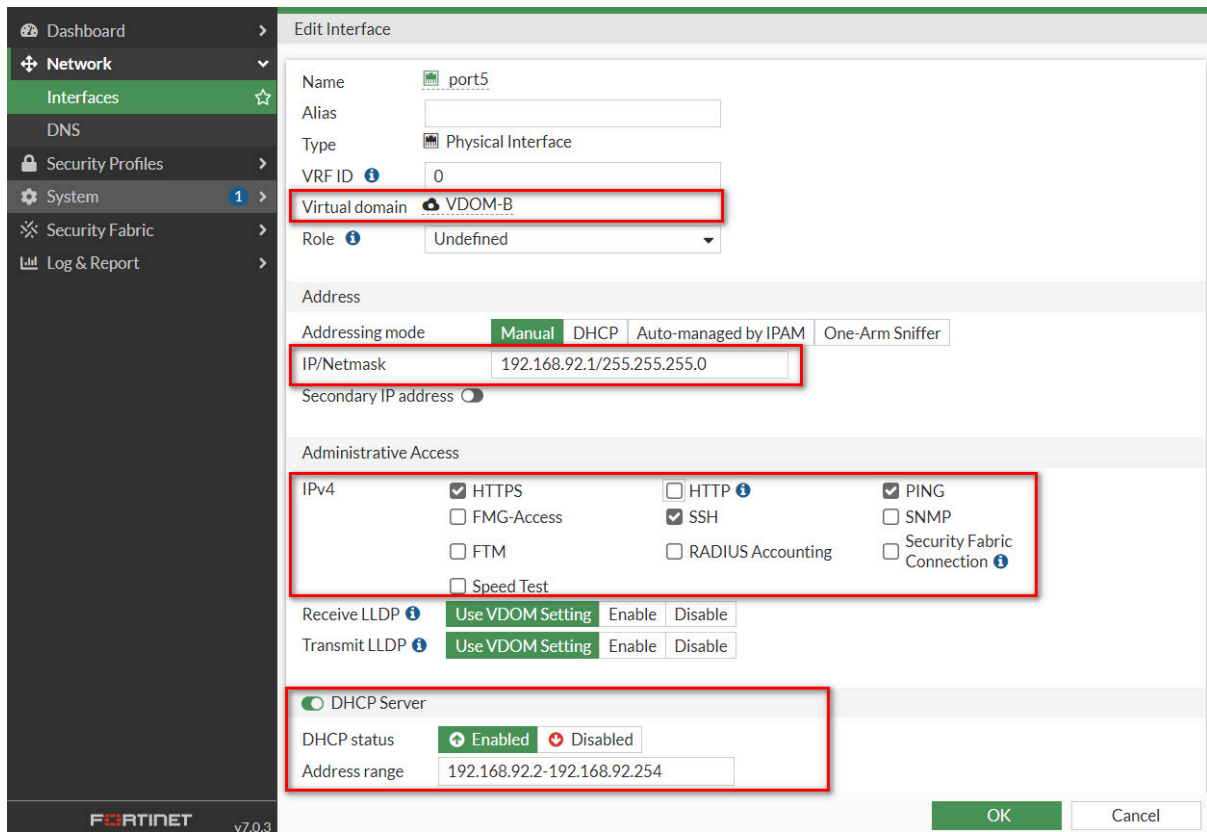


Figure 8.8: Port5 configuration

Creating Administrators for Each VDOM

1. Go to **Global > System > Administrators**. Create an administrator for VDOM-A, called vdom-a. Set Type to **Local User**, enter and confirm a password, set Administrator Profile to **prof_admin**, and set Virtual Domain to **VDOM-A**. Make sure to remove the root VDOM from the Virtual Domain list.

Figure 8.9: Administrators for VDOM-A

2. Go to **Global > System > Administrators**. Create an administrator for **VDOM-B**, called **vdom-b**. Set Type to **Local User**, enter and confirm a password, set Administrator Profile to **prof_admin**, and set Virtual Domain to **VDOM-B**. Make sure to remove the root VDOM from the Virtual Domain list.

Figure 8.10: Administrators for VDOM-B

Security Policy Setting for VDOM-A

1. **Virtual Domains > VDOM-A > Network > Static Routes**. Click Create New to create a default route for the VDOM. Set Destination IP/Mask to 0.0.0.0/0.0.0.0, set Device to port3,

and set Gateway to the IP of the gateway router.

The screenshot shows the 'Static Routes' configuration page in VDOM-A. The left sidebar is expanded to 'Network' > 'Static Routes'. The main configuration area includes the following fields:

- Automatic gateway retrieval:
- Destination: Subnet Internet Service, 0.0.0.0/0.0.0.0
- Gateway Address: Dynamic Specify, 192.168.122.1
- Interface: port3
- Administrative Distance: 10
- Comments: Write a comment... (0/255)
- Status: Enabled Disabled

Figure 8.11: Static route in VDOM-A

- Go to **Policy & Objects > Firewall Policy**. Create a policy to allow internet access. Set Incoming Interface to port4 and Outgoing Interface to port2. Ensure NAT is turned ON. Set Source Address to all, Destination Address to all, and Service to ALL.

The screenshot shows the 'New Policy' configuration page in VDOM-A. The left sidebar is expanded to 'Policy & Objects' > 'Firewall Policy'. The main configuration area includes the following fields:

- Name: VDOM-A
- Incoming Interface: port4
- Outgoing Interface: port3
- Source: all
- Destination: all
- Schedule: always
- Service: ALL
- Action: ACCEPT DENY
- Inspection Mode: Flow-based Proxy-based

Firewall / Network Options:

- NAT:
- IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool
- Preserve Source Port:
- Protocol Options: PROT default

Security Profiles:

- AntiVirus:
- Web Filter:

Figure 8.12: Firewall Policy in VDOM-A

- Now, you should be able to reach the internet from WebTerm VDOM-A.

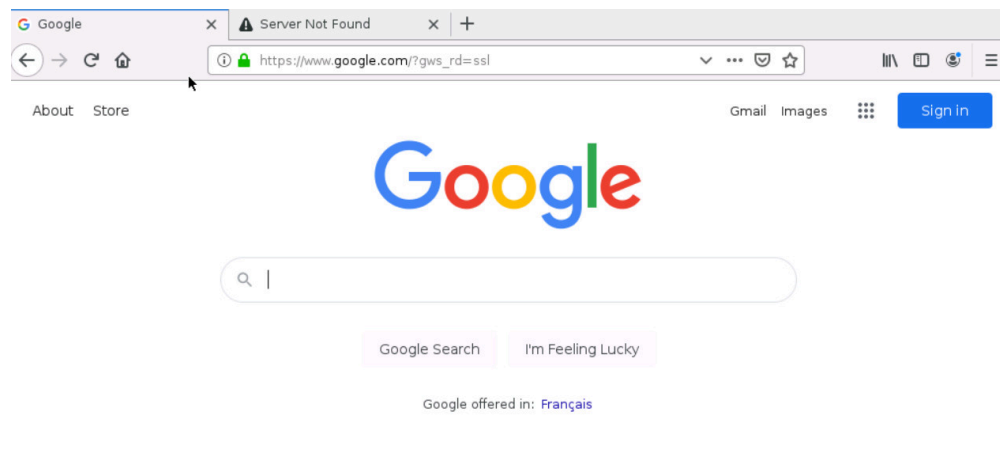


Figure 8.13: Verify configuration in VDOM-A

Security Policy Setting for VDOM-B

1. **Virtual Domains > VDOM-B > Network > Static Routes.** Click Create New to create a default route for the VDOM. Set Destination IP/Mask to 0.0.0.0/0.0.0.0, set Device to port2, and set Gateway to the IP of the gateway router.

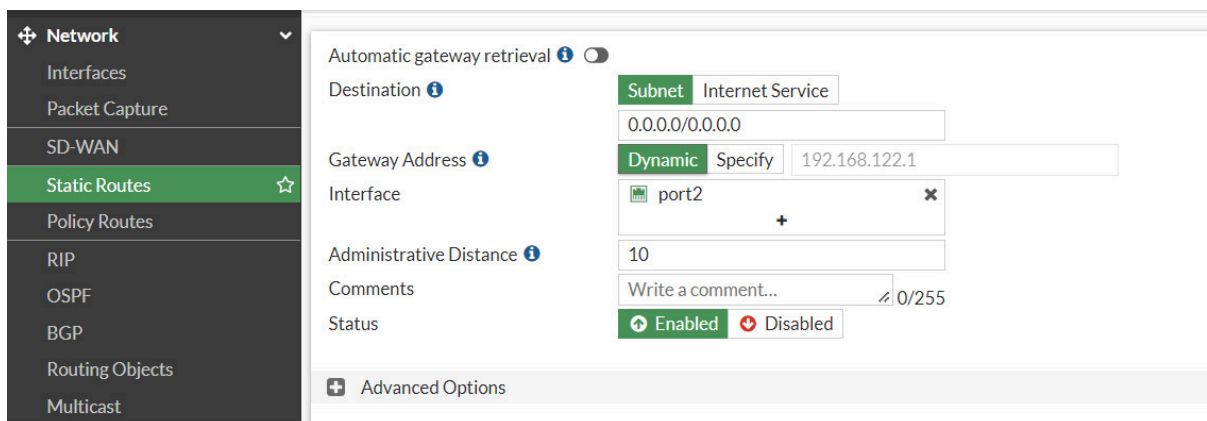


Figure 8.14: Static route in VDOM-B

2. Go to **Policy & Objects > Policy > IPv4.** Create a policy to allow internet access. Set Incoming Interface to port5 and Outgoing Interface to port2. Ensure NAT is turned ON. Set Source Address to all, Destination Address to all, and Service to ALL.

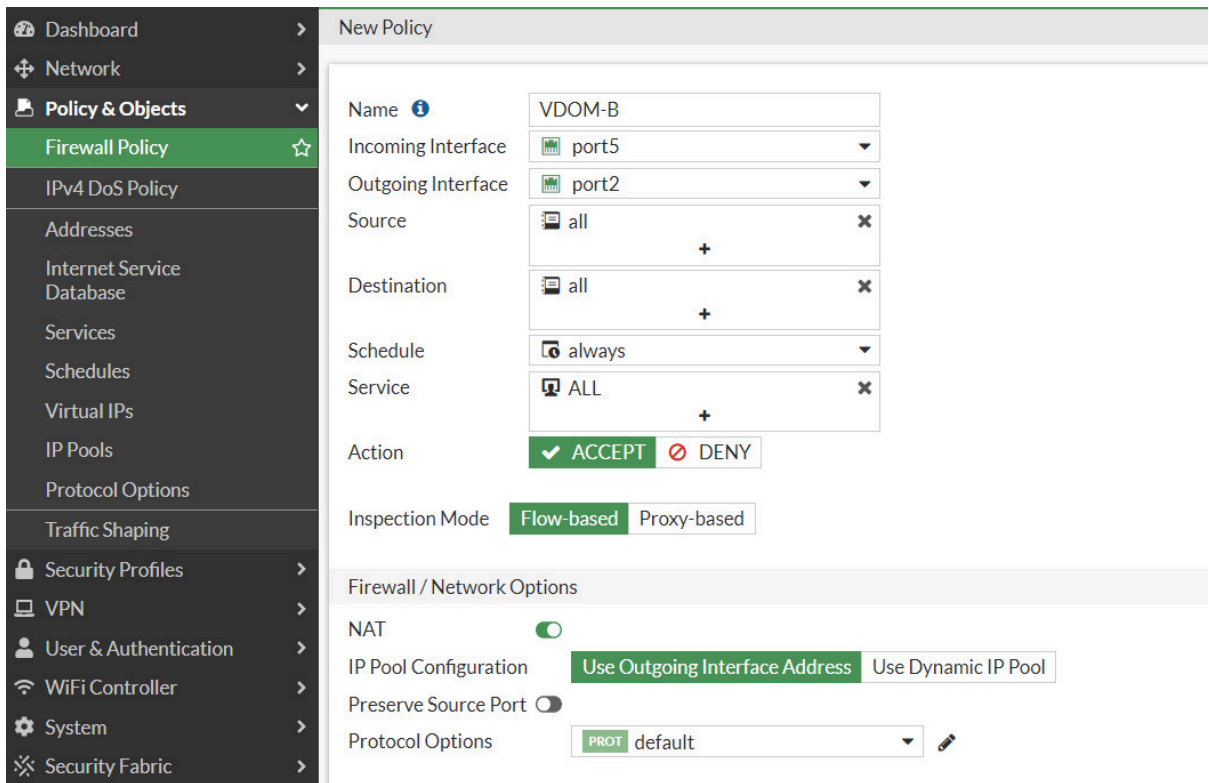


Figure 8.15: Firewall Policy in VDOM-B

3. Create a Traffic shaping under **Policy & Objects** as follows:

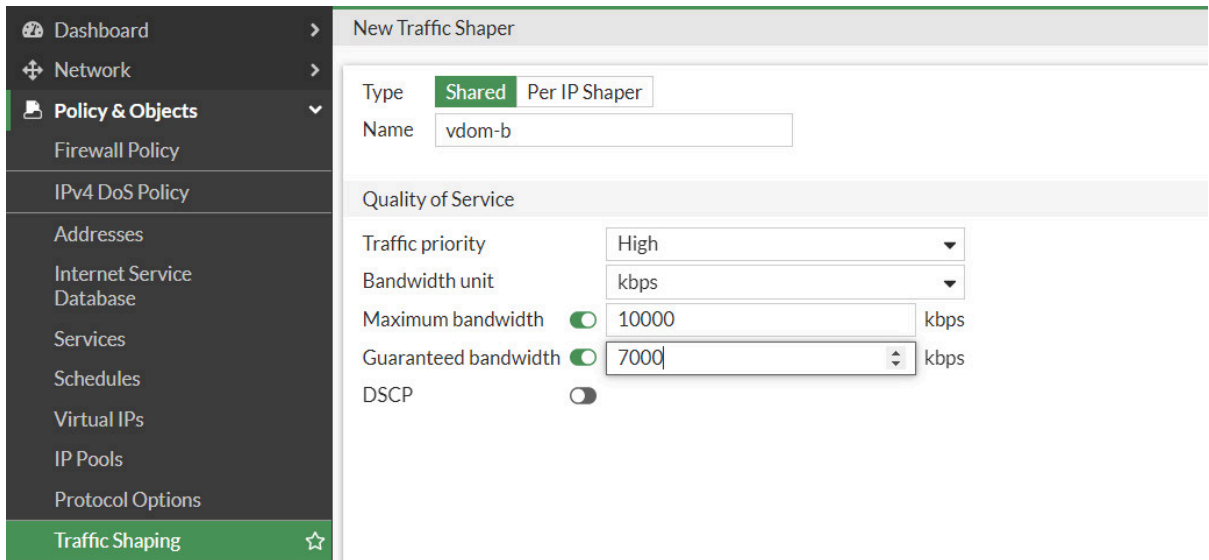


Figure 8.16: Create a traffic shaper in VDOM-B

4. Create a Traffic Shaping Policy with the following configuration:

- Name: **VDOMB**
- Source: **All**
- Destination: **All**
- Service: **All**

- Outgoing Interface: **Port2**
- Shared Shaper: **VDOMB**
- Reverse Shaper: **VDOMB**

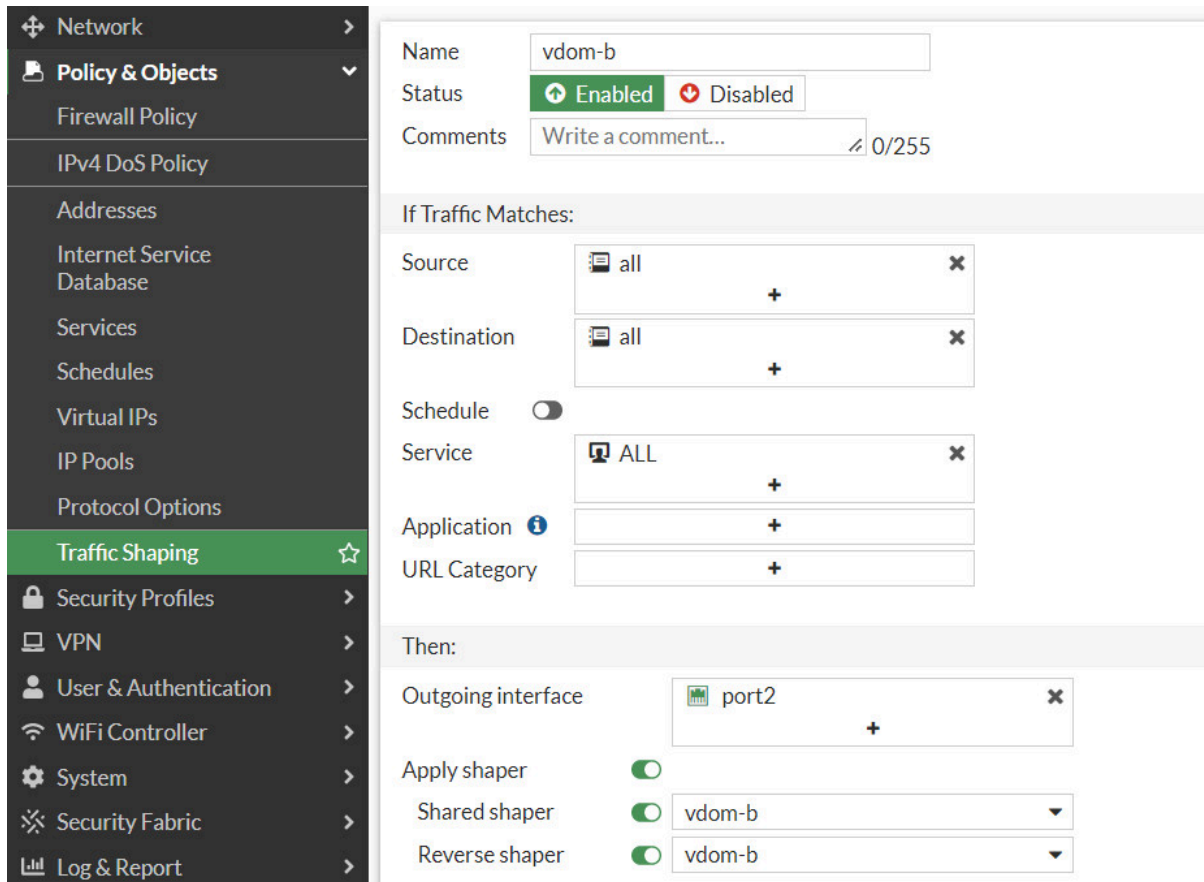


Figure 8.17: Traffic Shaping Policy in VDOM-B

5. Now open the browser in WebTerm VDOM-B and go to Fast.com (<https://fast.com>) and verify your configuration.

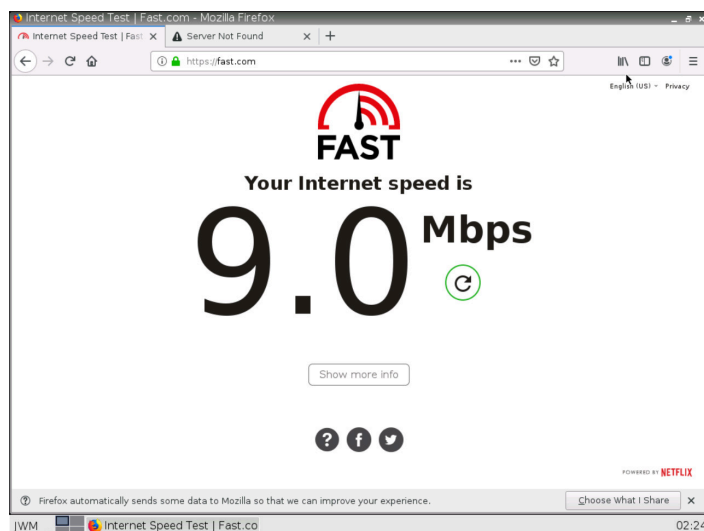


Figure 8.18: Verify configuration in VDOM-B

8.2 Inter-VDOM Routing

Learning Objectives

- Configure a VDOM to pass traffic between VDOMs
- Configure an Inter-VDOM routing

Scenario: Inter-VDOM routing is the communication between VDOMs. VDOM links are virtual interfaces that connect VDOMs. A VDOM link contains a pair of interfaces, each one connected to a VDOM and forming either end of the inter-VDOM connection. We want to create a link between VDOM Sales and Accounting, then the traffic from WebTerm1 should be reached to WebTerm2.

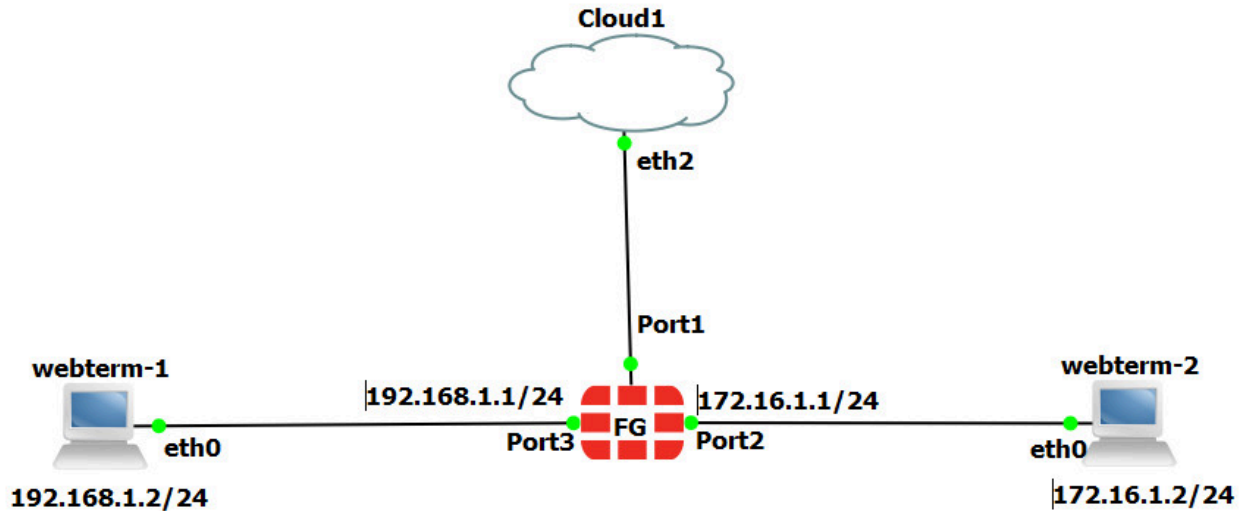


Figure 8.19: Main scenario

Table 8.2: Devices configuration

Device	IP address	Access
WebTerm1	192.168.1.2/24	–
WebTerm2	172.16.1.2/24	–
FortiGate	Port 1: DHCP Client Port 2: 172.16.1.1/24 Port 3: 192.168.1.1/24	Port 1: https, ping
Cloud1		–

1. First, enable VDOMs in the firewall.

```
FGVM01TM19008000 # config system global
FGVM01TM19008000 (global) # set vdom-mode multi-vdom
FGVM01TM19008000 (global) # end
```

2. Create two VDOMs, **Sales** and **Accounting**.

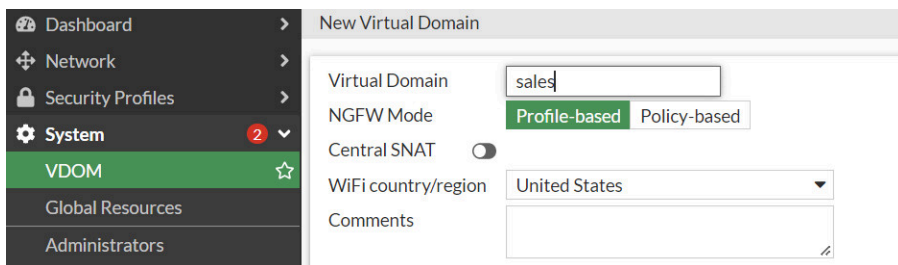


Figure 8.20: Create a VDOM Sales

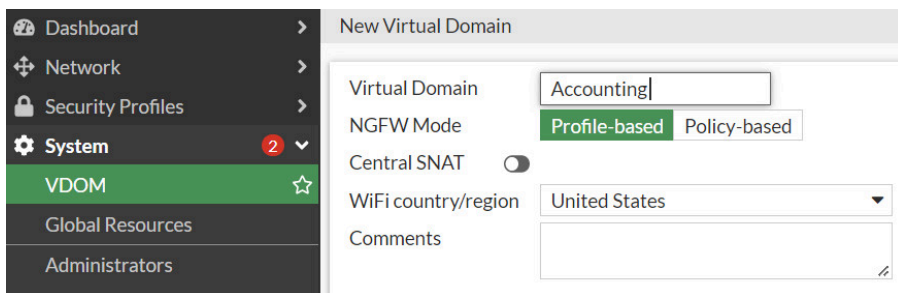


Figure 8.21: Create a VDOM Accounting

- Configure IP addresses for the Interfaces Port2 and Port3. Assign port3 to Sales Vdom and port2 to Accounting Vdom.

Physical Interface 10				
port1	Physical Interface	142.232.89.76/255.255.255.128	HTTPS	HTTP
port2	Physical Interface	172.16.1.1/255.255.255.0		
port3	Physical Interface	192.168.1.1/255.255.255.0		

Figure 8.22: Port2 and Port3 IP address configuration

Dashboard > Network > Interfaces > Edit Interface

Name: port2
 Alias:
 Type: Physical Interface
 VRF ID: 0
 Virtual domain: Accounting
 Role: Undefined

Addressing mode: Manual | DHCP | Auto-managed by IPAM | One-Arm Sniffer
 IP/Netmask: 172.16.1.1/255.255.255.0
 Secondary IP address:

Figure 8.23: Port2 configuration

Network > Interfaces > Edit Interface

Name: port3
 Alias:
 Type: Physical Interface
 VRF ID: 0
 Virtual domain: sales
 Role: Undefined

Addressing mode: Manual | DHCP | Auto-managed by IPAM | One-Arm Sniffer
 IP/Netmask: 192.168.1.1/255.255.255.0
 Secondary IP address:

Figure 8.24: Port3 configuration

- Go to **Global VDOM > Network Interfaces > Create a new VDOM Link**, and configure it as Figure 8.25:

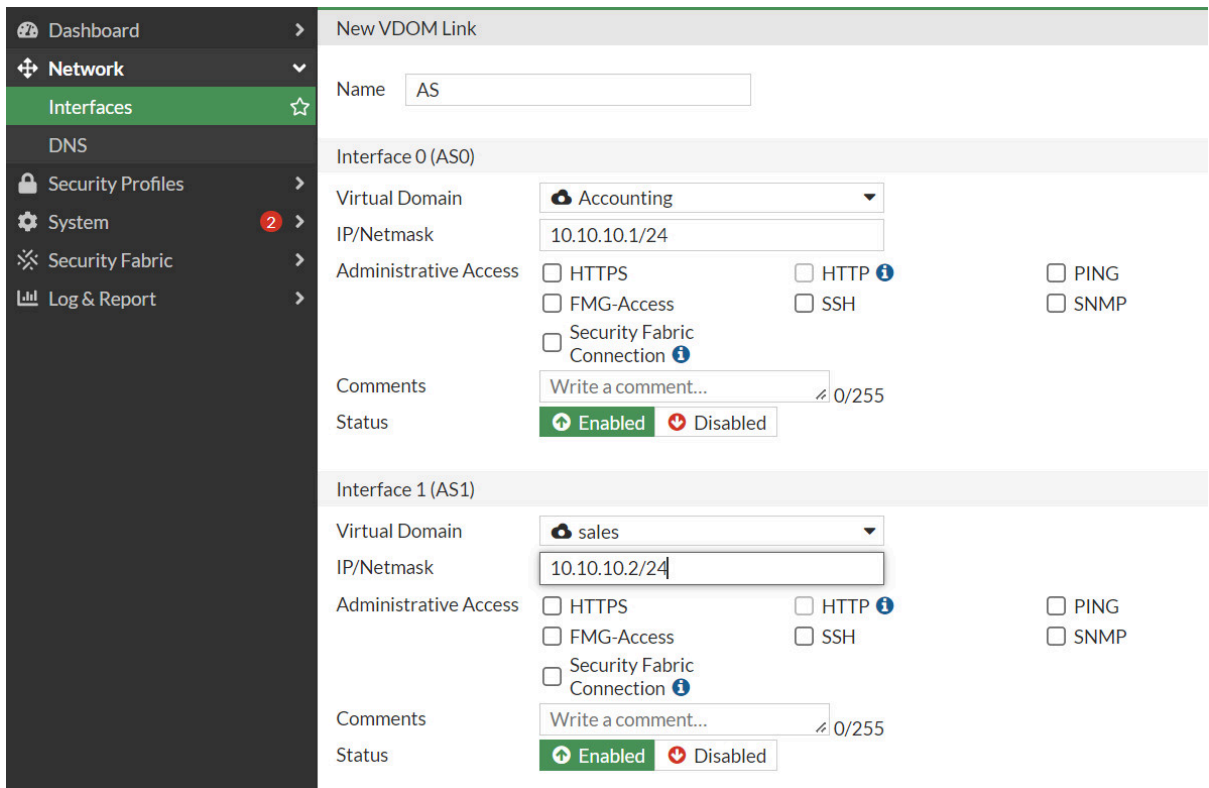


Figure 8.25: Create a VDOM link between Sales and Accounting

5. In Accounting VDOM, Create two static routes:

- **Destination:** 192.168.1.0/255.255.255.0
- **Interface:** Accounting-Sales
- **Gateway:** 10.10.10.2

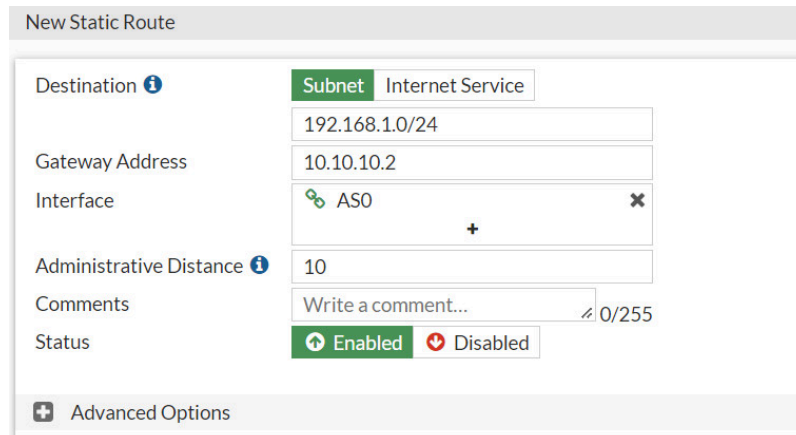


Figure 8.26: Create a static route in Accounting VDOM

- **Destination:** 172.16.1.0/255.255.255.0
- **Interface:** Accounting-Sales
- **Gateway:** 10.10.10.2

New Static Route

Destination **i** Subnet Internet Service
172.16.1.0/24

Gateway Address
10.10.10.2

Interface
AS0

Administrative Distance **i**
10

Comments
Write a comment... 0/255

Status
 Enabled Disabled

+ Advanced Options

Figure 8.27: Create a static route in Accounting VDOM

6. In Accounting VDOM, Create two Firewall Policies:

- **Incoming:** Port 2
- **Outgoing:** AS0
- NAT Disable

Name **i**
P2

Incoming Interface
port2

Outgoing Interface
AS0

Source
all

Destination
all

Schedule
always

Service
ALL

Action
 ACCEPT DENY

Inspection Mode Flow-based Proxy-based

Firewall / Network Options

NAT

Protocol Options PROT default

Figure 8.28: Create a Firewall Policy in Accounting VDOM from Port2 to AS0

Incoming:

- **Incoming:** AS0
- **Outgoing:** Port2
- NAT Disable

The screenshot shows a configuration form for a Firewall Policy. The fields are as follows:

- Name:** P1
- Incoming Interface:** AS0
- Outgoing Interface:** port2
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (selected), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based

Below the policy configuration, there is a section for "Firewall / Network Options":

- NAT:** Disabled (toggle)
- Protocol Options:** PROT default

Figure 8.29: Create a Firewall Policy in Accounting VDOM from AS0 to Port2

7. In Sales VDOM, Create two static routes:

- **Destination:** 192.168.1.0/255.255.255.0
- **Interface:** AS1
- **Gateway:** 10.10.10.1

The screenshot shows the "New Static Route" configuration form with the following details:

- Destination:** Subnet (selected), Internet Service. Address: 192.168.1.0/24
- Gateway Address:** 10.10.10.1
- Interface:** AS1
- Administrative Distance:** 10
- Comments:** Write a comment... (0/255)
- Status:** Enabled (selected), Disabled

There is an "Advanced Options" section at the bottom, which is currently collapsed.

Figure 8.30: Create a static route in Sales VDOM

- **Destination:** 172.16.1.0/255.255.255.0
- **Interface:** AS1
- **Gateway:** 10.10.10.1

New Static Route

Destination ⓘ **Subnet** Internet Service
172.16.1.0/24

Gateway Address
10.10.10.1

Interface
AS1

Administrative Distance ⓘ
10

Comments
Write a comment... 0/255

Status
 Enabled Disabled

Advanced Options

Figure 8.31: Create a static route in Sales VDOM

8. In Sales VDOM, Create two Firewall Policies:

- **Incoming:** Port3
- **Outgoing:** AS1
- **NAT Disable**

New Policy

Name ⓘ P1

Incoming Interface
port3

Outgoing Interface
AS1

Source
all

Destination
all

Schedule
always

Service
ALL

Action
 ACCEPT DENY

Inspection Mode
 Flow-based Proxy-based

Firewall / Network Options

NAT

Protocol Options
PROT default

Figure 8.32: Create a Firewall Policy in Sales VDOM from Port3 to AS1

- **Incoming:** AS1

- **Outgoing:** Port3
- NAT Disable

The screenshot shows the 'Edit Policy' configuration page. The policy name is 'P2'. The incoming interface is 'AS1' and the outgoing interface is 'port3'. The source and destination are both set to 'all'. The schedule is 'always' and the service is 'ALL'. The action is set to 'ACCEPT'. The inspection mode is 'Flow-based'. Under 'Firewall / Network Options', NAT is disabled and protocol options are set to 'default'.

Figure 8.33: Create a Firewall Policy in Sales VDOM from AS1 to Port3

9. Now, you should verify your configuration and should be able to ping from WebTerm1 to WebTerm2.

```

LXTerminal
File Edit Tabs Help
root@webterm-1:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 96:3c:81:44:e4:e5
          inet addr:192.168.1.2  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::963c:81ff:fe44:e4e5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:264 (264.0 B)  TX bytes:1076 (1.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:5808 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5808 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:492032 (480.5 KiB)  TX bytes:492032 (480.5 KiB)

root@webterm-1:~# ping 172.16.1.2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
64 bytes from 172.16.1.2: icmp_seq=1 ttl=62 time=1.85 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=62 time=3.98 ms
64 bytes from 172.16.1.2: icmp_seq=3 ttl=62 time=3.82 ms

```

Figure 8.34: Verify configuration

To delete a VDOM link in the CLI:

```

config system vdom-link
delete <VDOM-LINK-Name>
end

```


Chapter 9. SD-WAN

9.1 SD-WAN

Learning Objectives

- Create a Demo of SDWAN
- Configure SDWAN features

Scenario: Software-defined wide-area network (SD-WAN) solutions transform an organization's capabilities by leveraging the corporate wide-area network (WAN) as well as multi-cloud connectivity to deliver high-speed application performance at the WAN edge of branch sites. One of the chief benefits of SD-WAN is that it provides a dynamic path selection among connectivity options—MPLS, 4G/5G, or broadband—ensuring organizations can quickly and easily access business-critical cloud applications.¹ In this scenario, we are simulating SD-WAN by using OpenWrt and this allows you to play with the features of SD-WAN. Port 4 and Port 5 acts like your different connection and you can manage them through SD-WAN.

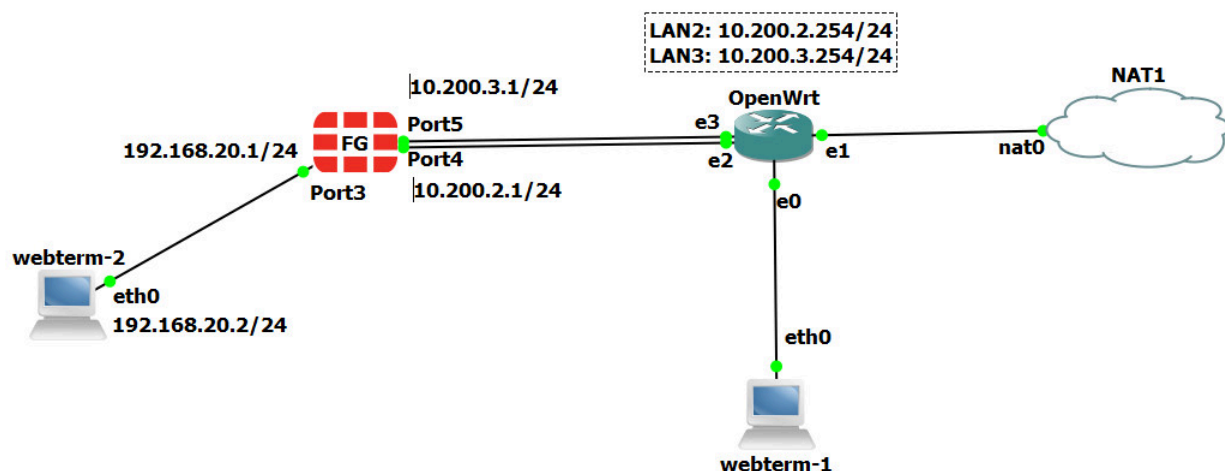


Figure 9.1: Main scenario

1. SD-WAN Document Library (<https://docs.fortinet.com/document/fortigate/6.2.10/cookbook/19246/sd-wan>)

Table 9.1: Devices configuration

Device	IP address
WebTerm1 (WRT Manager)	192.168.1.2/24
WebTerm2 (Firewall Manager)	192.168.20.2/24, GW: 192.168.20.1, DNS: 4.2.2.4
FortiGate	Port 3: 192.168.20.1/24 Port 4: 10.200.2.1/24 Port 5: 10.200.3.1/24
OpenWrt	Eth0: connected to WRT Manager Eth1: connected to NAT Eth2: 10.200.2.254/24 Eth3: 10.200.3.254/24
NAT	

Configure OpenWrt

To configure OpenWrt, you should connect through port eth0. By default, the IP address of eth0 is 192.168.1.1/24. So, you can set the WRTManager as 192.168.1.2/24 and connect to OpenWrt through the web browser. You can type in the browser: `http://192.168.1.1`, and click on “Login” without entering any password.

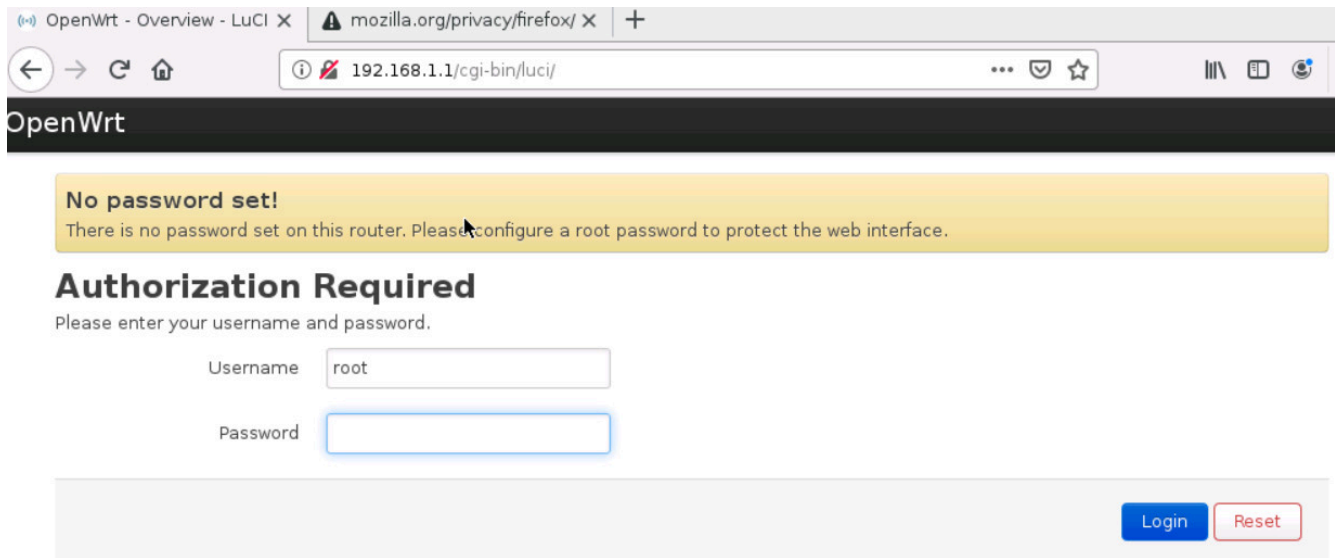


Figure 9.2: OpenWrt

Then, go to **network > interfaces > Add new interface ...**

And Enter the following information:

- Name of Interface: **LAN2**
- Cover the following interface: **eth2**
- Then, submit and add IPV4: **10.200.2.254**, netmask: **255.255.255.0**
- And finally, under Firewall Settings select **firewall-zone** as Lan

Add new interface...

Name

Protocol

Device

Figure 9.3: Add a new interface

Interfaces » LAN2

[General Settings](#) [Advanced Settings](#) [Firewall Settings](#) [DHCP Server](#)

Status

Protocol

Device

Bring up on boot

IPv4 address

IPv4 netmask

IPv4 gateway

Figure 9.4: LAN2 IPv4 configuration

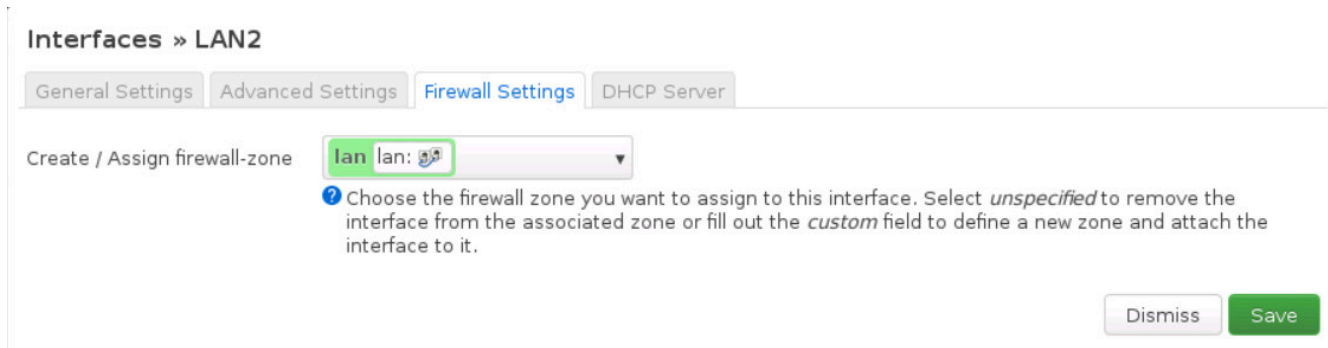


Figure 9.5: Firewall settings for LAN2

- Name of Interface: **LAN3**
- Cover the following interface: **eth3**
- Then, submit and add IPv4: **10.200.3.254** netmask: **255.255.255.0**
- And finally, under Firewall Settings select **firewall-zone** as Lan

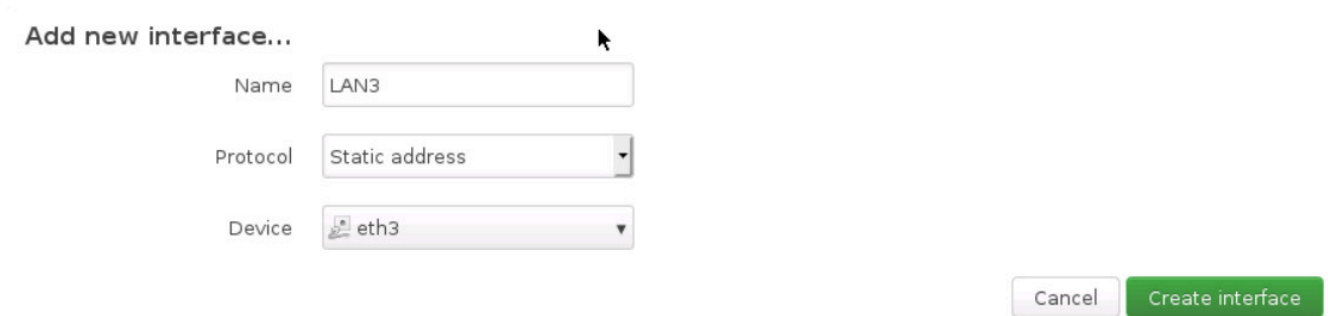


Figure 9.6: Add a new interface (LAN3)

Interfaces » LAN3

General Settings | Advanced Settings | Firewall Settings | DHCP Server

Status Device: eth3
MAC: 0C:76:09:C7:00:03
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Protocol Static address

Device eth3

Bring up on boot

IPv4 address 10.200.3.254

IPv4 netmask 255.255.255.0

IPv4 gateway 192.168.122.1 (wan)

Figure 9.7: IP configuration for LAN3

Interfaces » LAN3

General Settings | Advanced Settings | Firewall Settings | DHCP Server

Create / Assign firewall-zone lan lan: LAN2:

? Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *custom* field to define a new zone and attach the interface to it.

Dismiss Save

Figure 9.8: Firewall settings for LAN3

Your interfaces in OpenWrt should be like Figure 9.9:

Interfaces	
<div style="background-color: #e0ffe0; padding: 2px; border: 1px solid #ccc;">LAN2</div> <div style="border: 1px solid #ccc; padding: 2px; text-align: center;">eth2</div>	Protocol: Static address Interface has 5 pending changes <div style="float: right; text-align: right;"> <input type="button" value="Restart"/> <input type="button" value="Stop"/> <input style="background-color: #007bff; color: white;" type="button" value="Edit"/> <input style="border: 1px solid #dc3545; color: #dc3545;" type="button" value="Delete"/> </div>
<div style="background-color: #e0ffe0; padding: 2px; border: 1px solid #ccc;">LAN3</div> <div style="border: 1px solid #ccc; padding: 2px; text-align: center;">eth3</div>	Protocol: Static address Interface has 5 pending changes <div style="float: right; text-align: right;"> <input type="button" value="Restart"/> <input type="button" value="Stop"/> <input style="background-color: #007bff; color: white;" type="button" value="Edit"/> <input style="border: 1px solid #dc3545; color: #dc3545;" type="button" value="Delete"/> </div>
<div style="background-color: #e0ffe0; padding: 2px; border: 1px solid #ccc;">LAN</div> <div style="border: 1px solid #ccc; padding: 2px; text-align: center;">br-lan</div>	Protocol: Static address Uptime: 0h 17m 6s MAC: 0C:76:09:C7:00:00 RX: 419.87 KB (4308 Pkts.) TX: 2.18 MB (4396 Pkts.) IPv4: 192.168.1.1/24 IPv6: fd2e:66ec:7197::1/60 <div style="float: right; text-align: right;"> <input type="button" value="Restart"/> <input type="button" value="Stop"/> <input style="background-color: #007bff; color: white;" type="button" value="Edit"/> <input style="border: 1px solid #dc3545; color: #dc3545;" type="button" value="Delete"/> </div>
<div style="background-color: #ffe0e0; padding: 2px; border: 1px solid #ccc;">WAN</div> <div style="border: 1px solid #ccc; padding: 2px; text-align: center;">eth1</div>	Protocol: DHCP client Uptime: 0h 17m 3s MAC: 0C:76:09:C7:00:01 RX: 11.25 KB (133 Pkts.) TX: 13.48 KB (145 Pkts.) IPv4: 192.168.122.133/24 <div style="float: right; text-align: right;"> <input type="button" value="Restart"/> <input type="button" value="Stop"/> <input style="background-color: #007bff; color: white;" type="button" value="Edit"/> <input style="border: 1px solid #dc3545; color: #dc3545;" type="button" value="Delete"/> </div>
<div style="background-color: #ffe0e0; padding: 2px; border: 1px solid #ccc;">WAN6</div> <div style="border: 1px solid #ccc; padding: 2px; text-align: center;">eth1</div>	Protocol: DHCPv6 client MAC: 0C:76:09:C7:00:01 RX: 11.25 KB (133 Pkts.) TX: 13.48 KB (145 Pkts.) <div style="float: right; text-align: right;"> <input type="button" value="Restart"/> <input type="button" value="Stop"/> <input style="background-color: #007bff; color: white;" type="button" value="Edit"/> <input style="border: 1px solid #dc3545; color: #dc3545;" type="button" value="Delete"/> </div>

Figure 9.9: OpenWrt Interfaces

Firewall Configuration

1. Set the port3 as a management port and connect it to Firewall Manager (WebTerm2).

```

FGVM01TM19008000 # config system interface
FGVM01TM19008000 (interface) # edit port3
FGVM01TM19008000 (port3) # set ip 192.168.20.1/24
FGVM01TM19008000 (port3) # set allowaccess http https
FGVM01TM19008000 (port3) # end
  
```

2. Go to **Firewall > Network > Interfaces > port4**. Set Name as **WAN2** and IPv4 as **10.200.2.1/24**.

The screenshot shows the configuration page for a network interface named 'port4'. The left sidebar is under the 'Network' menu, with 'Interfaces' selected. The main configuration area includes the following fields:

- Name:** port4
- Alias:** WAN2
- Type:** Physical Interface
- VRF ID:** 0
- Role:** Undefined

The 'Address' section is expanded, showing:

- Addressing mode:** Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask:** 10.200.2.1/24
- Secondary IP address:** (toggle is off)

Figure 9.10: Port4 configuration

- Go to **Firewall > Network > Interfaces > port 5**. Set Name as **WAN3** and IPv4 as **10.200.3.1/24**.

The screenshot shows the configuration page for a network interface named 'port5'. The left sidebar is under the 'Network' menu, with 'Interfaces' selected. The main configuration area includes the following fields:

- Name:** port5
- Alias:** WAN3
- Type:** Physical Interface
- VRF ID:** 0
- Role:** Undefined

The 'Address' section is expanded, showing:

- Addressing mode:** Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask:** 10.200.3.1/24
- Secondary IP address:** (toggle is off)

Figure 9.11: Port5 configuration

- Go to **Network > SD-WAN > Select Interface Port4**. Gateway: **10.200.2.254**.

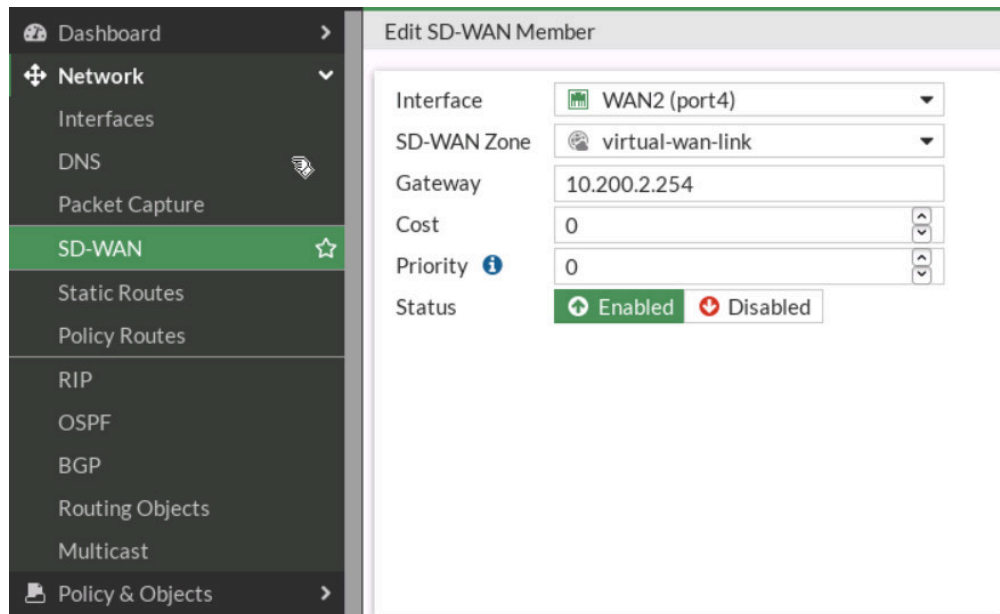


Figure 9.12: Add port4 as SD-WAN members

5. Add SD-WAN > Select Interface Port5. Gateway: 10.200.3.254.

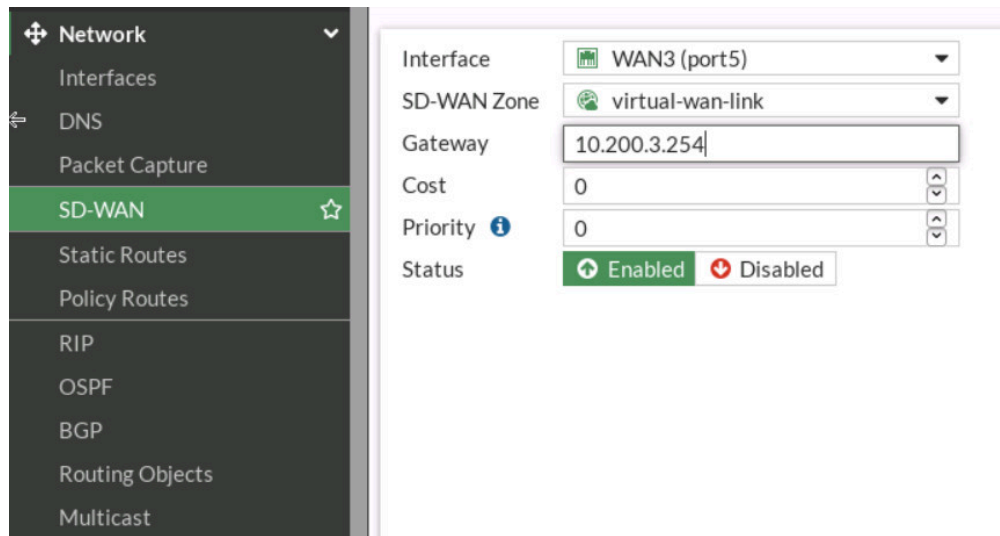


Figure 9.13: Add port5 as SD-WAN members

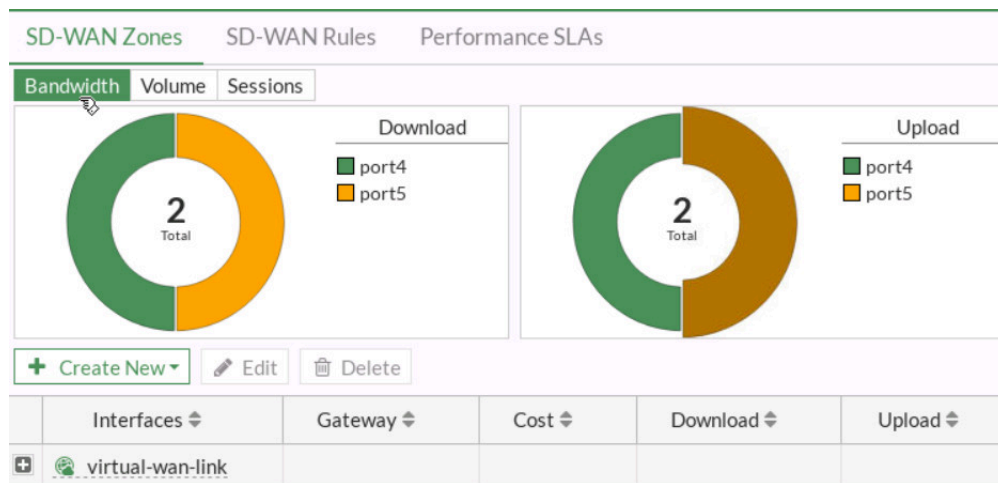


Figure 9.14: SD-WAN Zones

6. Create a static route as Figure 9.15.

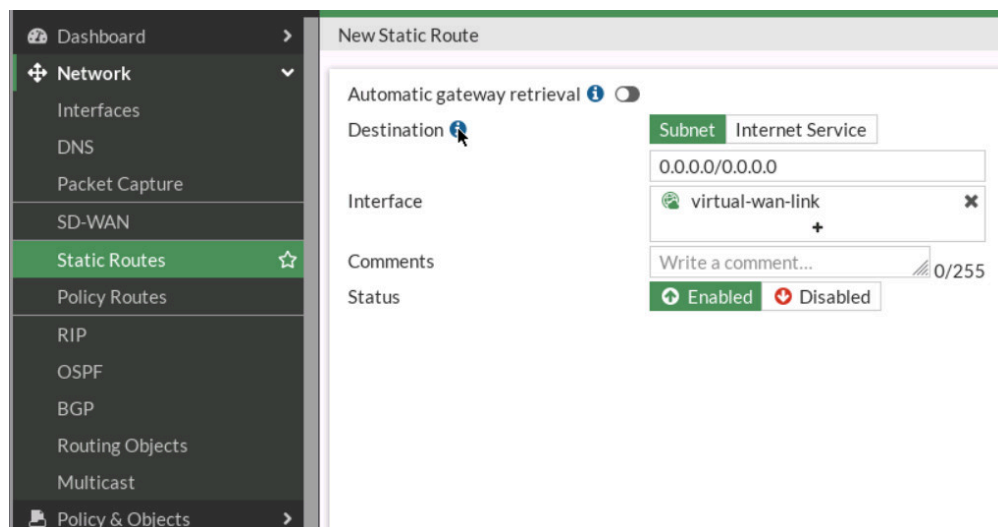


Figure 9.15: Create a static route to SD-WAN

7. Create a firewall policy as following table:

Table 9.2: Firewall Policy configuration

Field	Value
Name	SDWAN
Incoming Interface	LAN (PORT3)
Outgoing Interface	SD-WAN
Source	ALL
Destination	ALL
Schedule	Always
Service	ALL

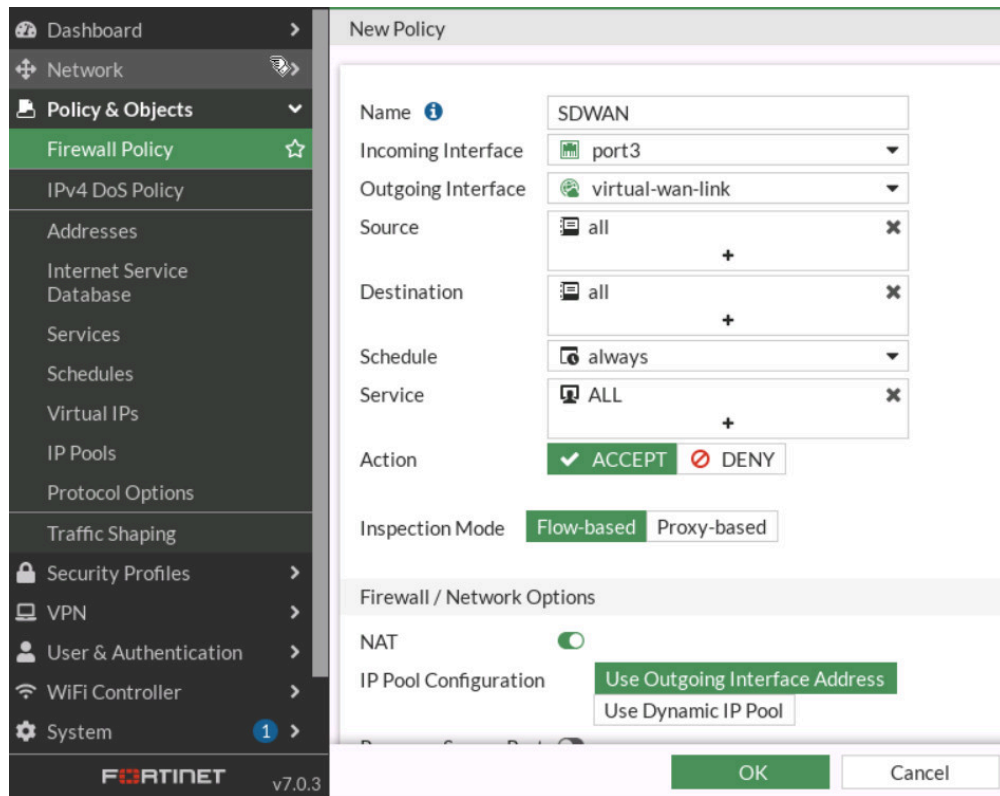


Figure 9.16: Create a Firewall Policy

8. Go to **Network > SD-WAN Rule**, create a rule as follows:

- Name: **MyRule**
- Source Address: **All**
- Destination Address: **All**
- Protocol Number: **Any**
- Strategy: **Best Quality**
- Interface Preference: **Port 4, Port 5**

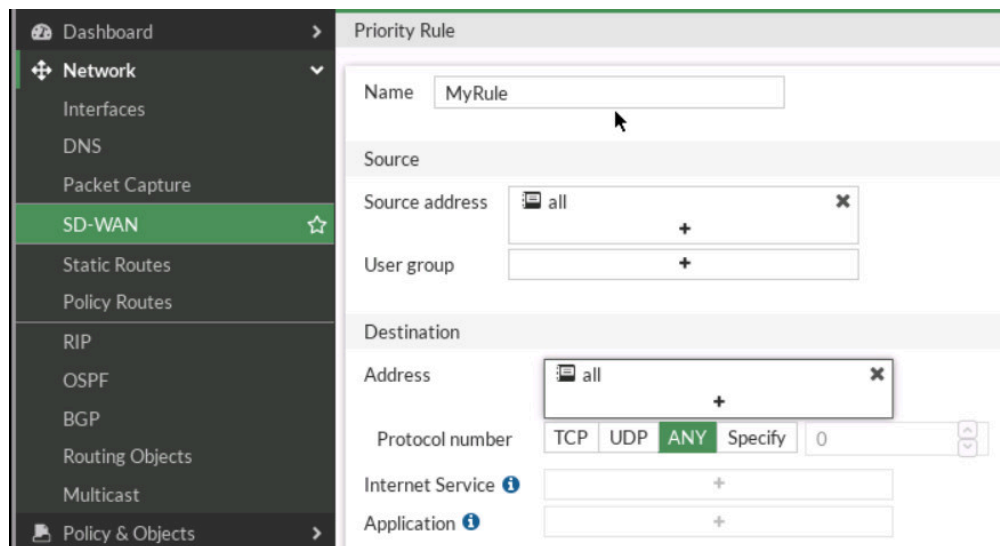


Figure 9.17: Priority Rule

9. Measured SLA. Create a SLA:

- Name: **MySLA**
- Protocol: **Ping**
- Server: **4.2.2.4**
- Add Target and leave the default parameters

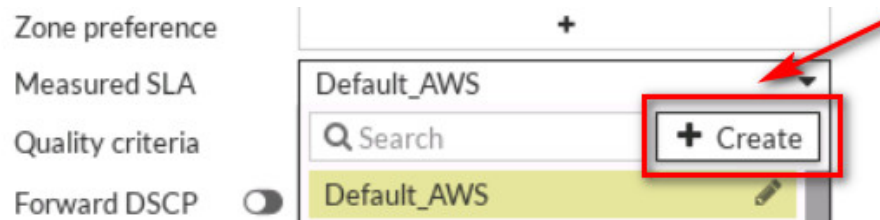


Figure 9.18: Add target

New Performance SLA

Name

Probe mode **i** Active Passive Prefer Passive

Protocol Ping HTTP DNS

Server

Participants All SD-WAN Members Specify

SLA Target

Link Status

Check interval ms

Failures before inactive **i**

Restore link after **i** check(s)

Actions when Inactive

Update static route **i**

Figure 9.19: Create a SLA

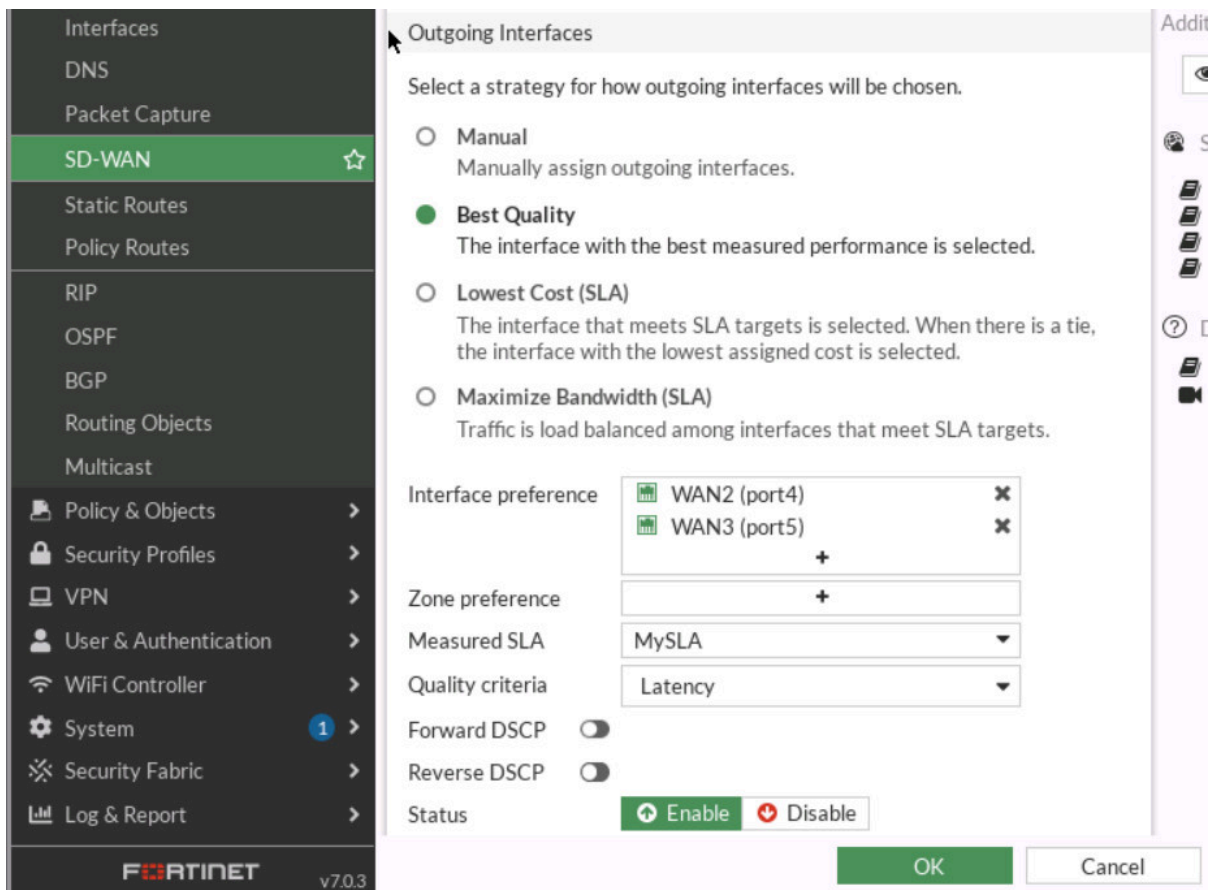


Figure 9.20: SD-WAN Configuration

10. Go to **Network > SD-WAN** and verify your **SD-WAN Usage**.

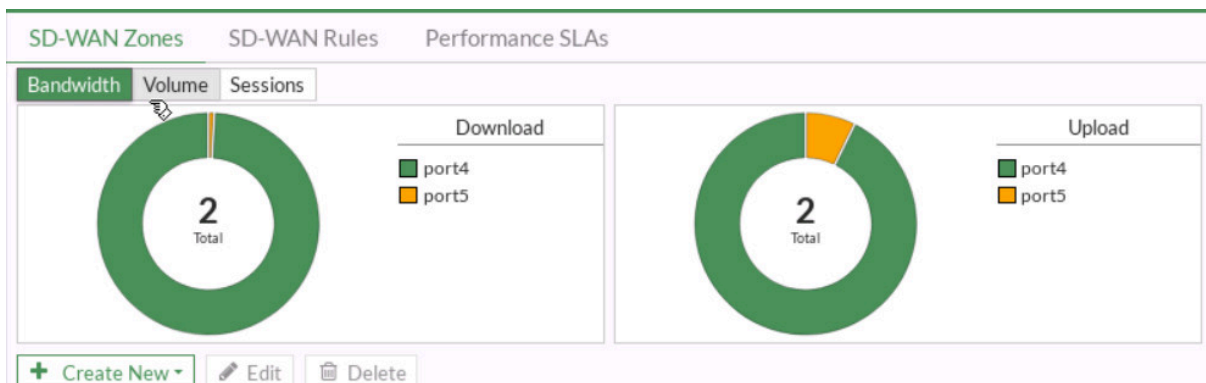


Figure 9.21: SD-WAN usage

11. Now, go to GN3 and disconnect port4. You should be able to reach the Internet from Firewall Manager.

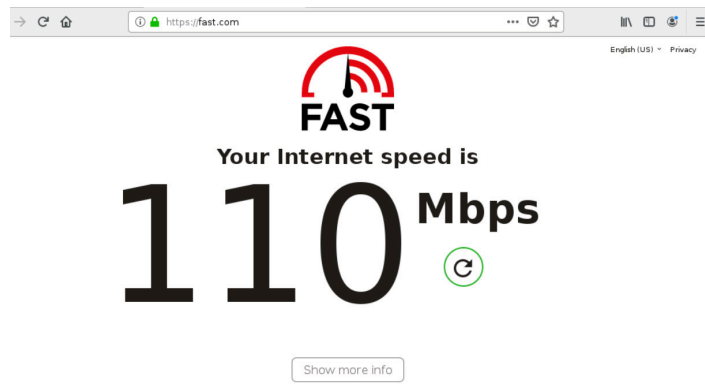


Figure 9.22: Verify configuration

- Go to **Network > SD-WAN** and verify your **SD-WAN Usage**.

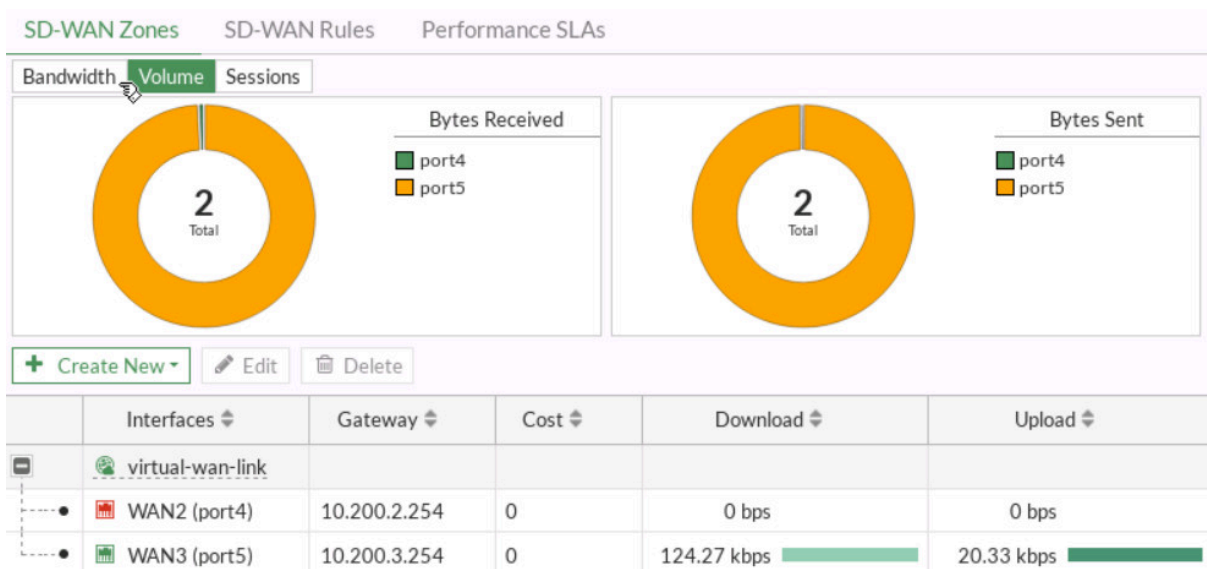


Figure 9.23: Status of interfaces

- Open the browser in the Firewall Manager and type **msn.com** and then go to the **Dashboard > FortiView Sessions**. Verify your result.

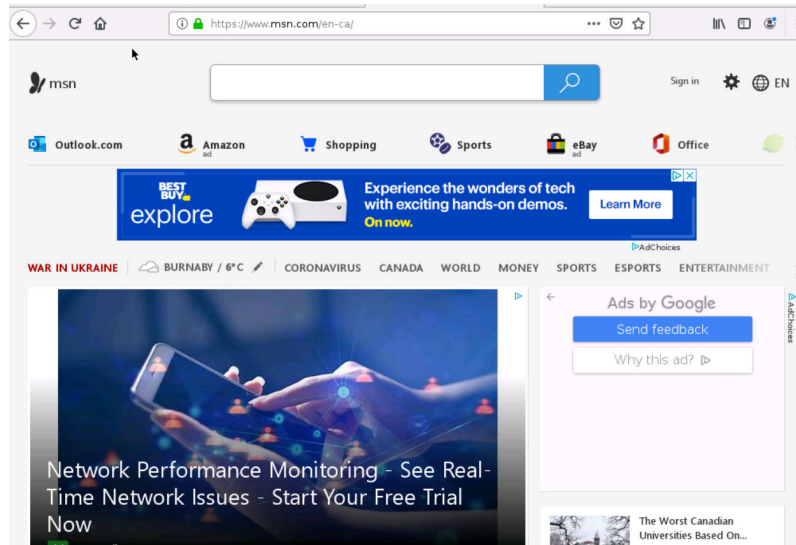


Figure 9.24: Verify configuration

The image shows the FortiView Sessions interface. On the left is a navigation menu with options like Dashboard, Status, Security, Network, Users & Devices, FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Policies, FortiView Sessions (highlighted), Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System, and Security Fabric. The main area displays a table of sessions with columns for Source, Device, Destination, Application, Protocol, Source Port, and Destination Port.

Source	Device	Destination	Application	Protocol	Source Port	Destination Port	
192.168.20.2		4.2.2.4	UDP/53	UDP	50235	53	4
192.168.20.2		4.2.2.4	UDP/53	UDP	50449	53	5
192.168.20.2		23.20.201.44	TCP/443	TCP	35418	443	8.4
192.168.20.2		4.2.2.4	UDP/53	UDP	50345	53	4
192.168.20.2		4.2.2.4	UDP/53	UDP	50426	53	4
192.168.20.2		4.2.2.4	UDP/53	UDP	50736	53	4
192.168.20.2		4.2.2.4	UDP/53	UDP	50779	53	3
192.168.20.2		4.2.2.4	UDP/53	UDP	50582	53	4
192.168.20.2		50.18.10.184	TCP/443	TCP	53074	443	37.5
192.168.20.2		142.250.191.66	TCP/443	TCP	33034	443	91.0
192.168.20.2		4.2.2.4	UDP/53	UDP	49176	53	4
192.168.20.2		4.2.2.4	UDP/53	UDP	49042	53	3
192.168.20.2		4.2.2.4	UDP/53	UDP	49128	53	3
192.168.20.2		4.2.2.4	UDP/53	UDP	49439	53	2
192.168.20.2		4.2.2.4	UDP/53	UDP	49465	53	5

Figure 9.25: FortiView Sessions

14. Go to **Log & Report > Event > SD-WAN Event**. Verify your result.

Date/Time	Level	Message	Log Description
8 minutes ago	Info	Service prioritized by performance metric will ...	SDWAN status
8 minutes ago	Warning	Member link is unreachable or miss threshold. ...	SDWAN status
8 minutes ago	Info	SD-WAN health-check member changed state.	SDWAN SLA notification
8 minutes ago	Info	Service prioritized by performance metric will ...	SDWAN status
8 minutes ago	Info	Member link is available. Start forwarding traff...	SDWAN status
8 minutes ago	Info	SD-WAN health-check member changed state.	SDWAN SLA notification
8 minutes ago	Info	Service prioritized by performance metric will ...	SDWAN status
8 minutes ago	Warning	Member link is unreachable or miss threshold. ...	SDWAN status
8 minutes ago	Info	SD-WAN health-check member changed state.	SDWAN SLA notification
9 minutes ago	Info	Service prioritized by performance metric will ...	SDWAN status
9 minutes ago	Info	Member link is available. Start forwarding traff...	SDWAN status
9 minutes ago	Info	Member link is available. Start forwarding traff...	SDWAN status
9 minutes ago	Info	SD-WAN health-check member changed state.	SDWAN SLA notification
9 minutes ago	Info	SD-WAN health-check member changed state.	SDWAN SLA notification
15 minutes ago	Warning	Service disabled caused by no outgoing path.	SDWAN status warning
15 minutes ago	Info	Service failover to other available interface(s).	SDWAN status
15 minutes ago	Warning	Member link is unreachable or miss threshold. ...	SDWAN status

Figure 9.26: SD-WAN Events

Chapter 10. Cloud Technologies

10.1 IPsec VPN from FortiGate (on Premise) to Azure

Learning Objectives

- Configure a Virtual Network Gateway in Azure
- Configure a local network gateway
- Create an IPSEC VPN between Firewall on-Premise and Azure

Scenario: We are going to connect on premise FortiGate to Azure Virtual Gateway. This is going to be IPsec VPN between FortiGate and Azure. First, we will configure Azure and then connect FortiGate through Port1 to Azure Virtual Gateway.

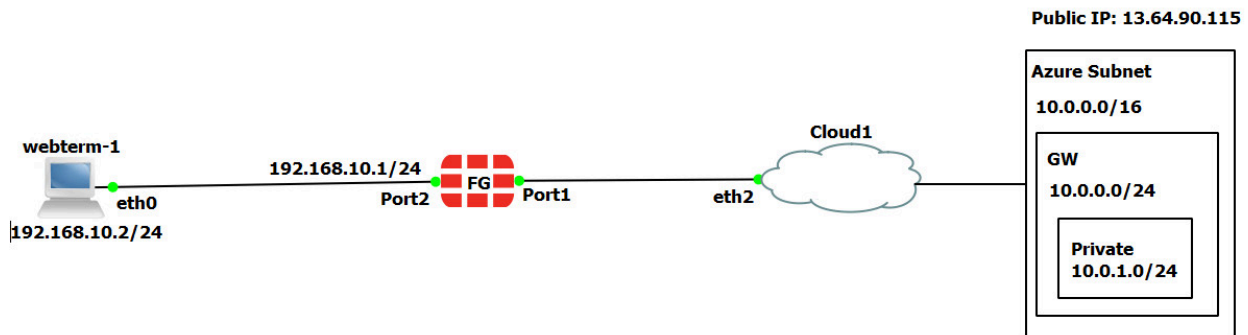


Figure 10.1: Main scenario

Table 10.1: On-premise devices configuration

Device	Configuration	Access
FortiGate	Port 1: DHCP Client Port 2: 192.168.10.1/24	Port1: HTTP, HTTPS, PING
WebTerm1	192.168.10.2/24	–

Azure Configuration

1. Create a resource group in Azure as following:

- Resource group: **FG**
- Region: **West US**

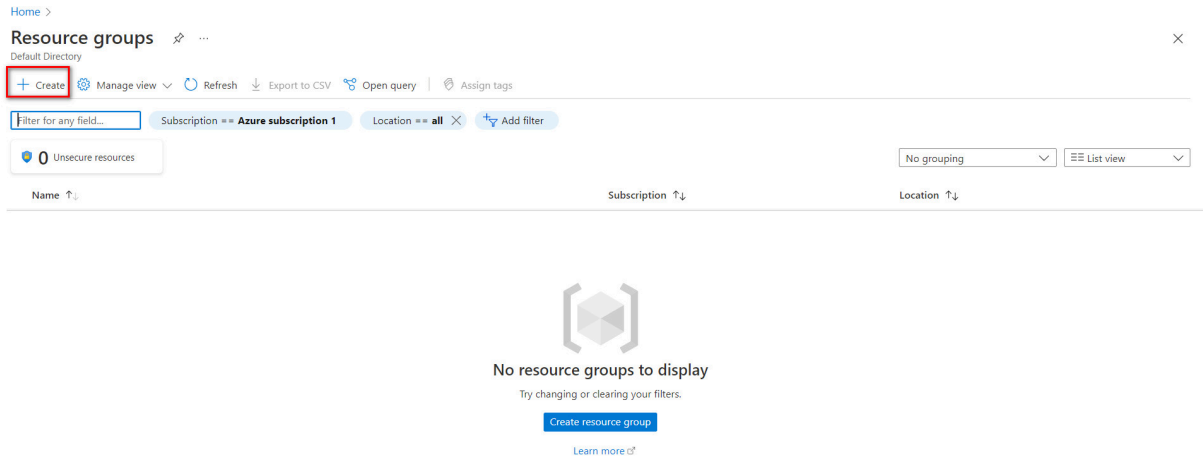


Figure 10.2: Create a resource group

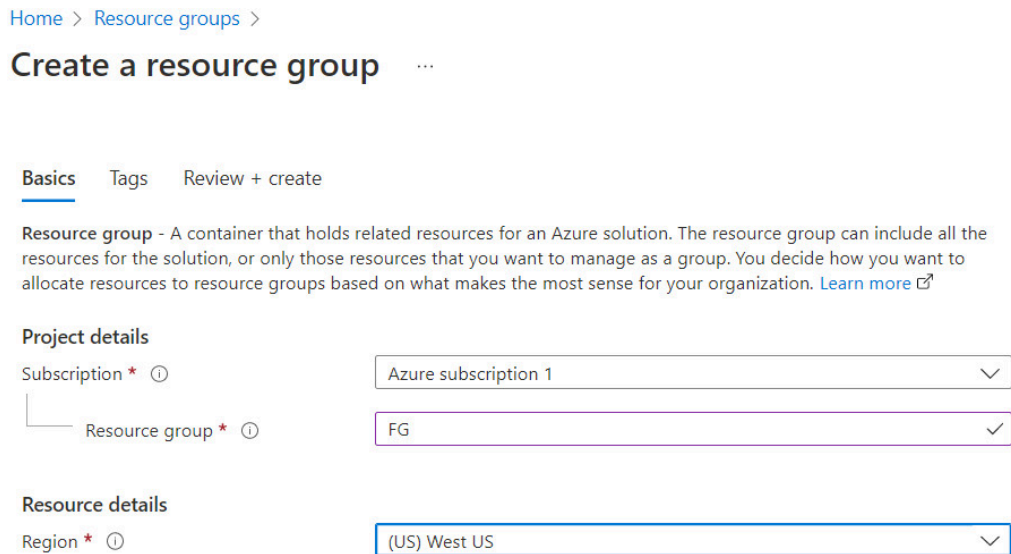


Figure 10.3: Create a resource group

Create a resource group ...

✓ Validation passed.

Basics Tags Review + create

Basics

Subscription	Azure subscription 1
Resource group	FG
Region	West US

Tags

None

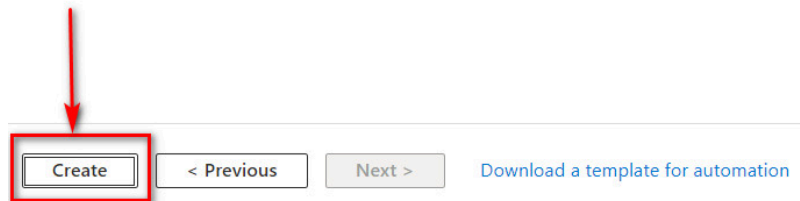


Figure 10.4: Create a resource group

2. Create a virtual network as following:

- Resource group: **FG**
- Name: **Azure-FG**
- Region: **West US**
- Change the default subnet: **10.0.1.0/24**

Create virtual network ...

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ FG [Create new](#)

Instance details

Name * Azure-FG ✓

Region * West US

[Review + create](#) [< Previous](#) [Next : IP Addresses >](#) [Download a template for automation](#)

Figure 10.5: Create a virtual network

Create virtual network ...

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses) [✕](#)

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

[+](#) Add subnet [✕](#) Remove subnet

Subnet name	Subnet address range	NAT gateway
<input checked="" type="checkbox"/> default	10.0.0.0/24	-

ⓘ Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#)

[Review + create](#) [< Previous](#) [Next : Security >](#) [Download a template for automation](#)

Edit subnet ✕

Subnet name * default

Subnet address range * ⓘ 10.0.1.0/24 ✓

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

NAT GATEWAY

Simplify connectivity to the internet using a network address translation gateway. Outbound connectivity is possible without a load balancer or public IP addresses attached to your virtual machines. [Learn more](#)

NAT gateway None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ 0 selected

[Save](#) [Cancel](#)

Figure 10.6: Create a virtual network (change default subnet)

Create virtual network ...

Basics IP Addresses **Security** Tags Review + create

BastionHost ⓘ Disable
 Enable

DDoS Protection Standard ⓘ Disable
 Enable

Firewall ⓘ Disable
 Enable

[Review + create](#)

[< Previous](#)

[Next : Tags >](#)

[Download a template for automation](#)

Figure 10.7: Create a virtual network

Create virtual network ...

Basics IP Addresses Security **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ
<input type="text"/>	<input type="text"/>

[Review + create](#)

[< Previous](#)

[Next : Review + create >](#)

[Download a template for automation](#)

Figure 10.8: Create a virtual network

Create virtual network ...

✓ Validation passed

Basics IP Addresses Security Tags Review + create

Basics

Subscription	Azure subscription 1
Resource group	FG
Name	Azure-FG
Region	West US

IP addresses

Address space	10.0.0.0/16
Subnet	default (10.0.1.0/24)

Tags

None

Security

BastionHost	Disabled
-------------	----------

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#)

Figure 10.9: Create a virtual network

3. Create a virtual network gateway as following:

- **Name:** Azure-VPN-FG
- **Region:** West US
- **Generation:** Generation1
- **Gateway subnet address range:** 10.0.0.0/24
- **Public IP address name:** AzurePublic

Click on “Create and Review”. It takes around 25 minutes to deploy a virtual network gateway in Azure.

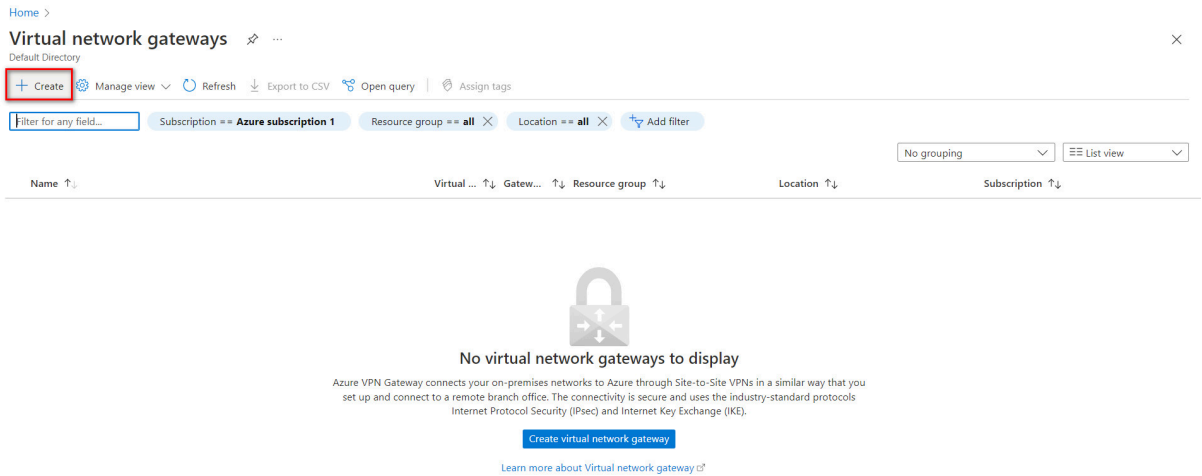


Figure 10.10: Create a virtual network gateway

Create virtual network gateway

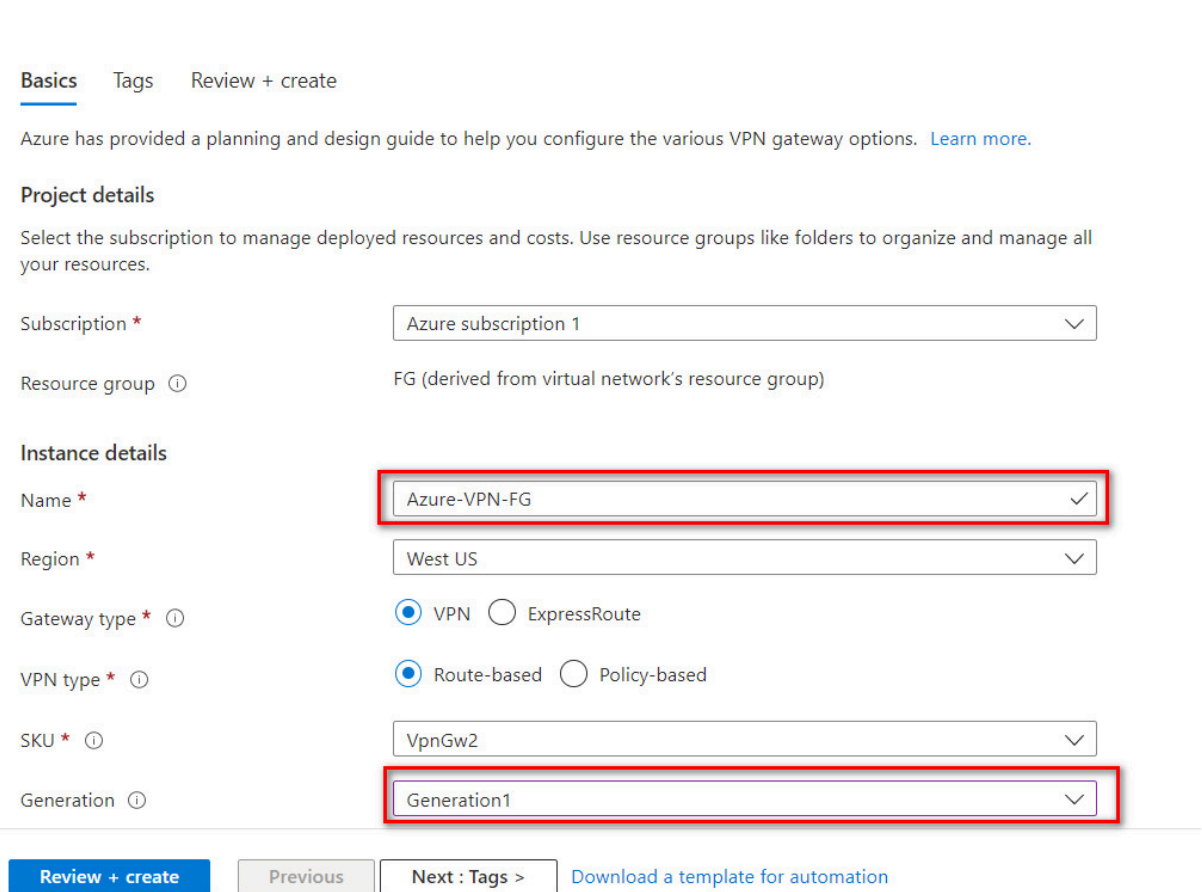


Figure 10.11: Create a virtual network gateway

Create virtual network gateway ...

[Create virtual network](#)

i Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range * ⓘ ✓
10.0.0.0 - 10.0.0.255 (256 addresses)

Public IP Address Type * ⓘ Basic Standard

Public IP address

Public IP address * ⓘ Create new Use existing

Public IP address name * ✓

Public IP address SKU Standard

Assignment Dynamic Static

Enable active-active mode * ⓘ Enabled Disabled

Configure BGP * ⓘ Enabled Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

[Review + create](#)[Previous](#)[Next : Tags >](#)[Download a template for automation](#)

Figure 10.12: Create a virtual network gateway

Create virtual network gateway

Validation passed

Basics Tags **Review + create**

Basics

Subscription	Azure subscription 1
Resource group	FG
Name	Azure-VPN-FG
Region	West US
SKU	VpnGw2
Generation	Generation1
Virtual network	Azure-FG
Subnet	GatewaySubnet (10.0.0.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP	Disabled
Public IP address	AzurePublic

Tags

Create Previous Next [Download a template for automation](#)

Figure 10.13: Create a virtual network gateway (review + create)

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft.VirtualNetworkGateway-20220427143943 | Overview

Deployment

Search (Ctrl+/) Delete Cancel Redeploy Refresh

We'd love your feedback! →

Deployment is in progress

Deployment name: Microsoft.VirtualNetworkGateway-2022042714... Start time: 4/27/2022, 2:42:51 PM
 Subscription: Azure subscription 1 Correlation ID: 489b63db-2c37-4721-a926-cc
 Resource group: FG

Deployment details (Download)

Resource	Type	Status
AzurePublic	Microsoft.Network/publicIPAddresses	Created
Azure-FG/GatewaySubnet	Microsoft.Network/virtualNetworks/subnets	OK

Notifications

More events in the activity log → Dismiss all

- Deployment in progress... Running ×
Deployment to resource group 'FG' is in progress. a few seconds ago
- Successfully deleted subnet ×
Successfully deleted subnet 'Gateway'. 4 minutes ago
- Successfully added subnet ×
Successfully added subnet 'Gateway' to virtual network 'Azure-FG'. 8 minutes ago
- Deployment succeeded ×
Deployment 'Microsoft.VirtualNetwork-20220427142905' to resource group 'FG' was successful.

Figure 10.14: Create a virtual network gateway (deployment)

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft.VirtualNetworkGateway-20220427143943 | Overview

Deployment

Search (Ctrl+/) Delete Cancel Redeploy Refresh

We'd love your feedback! →

Your deployment is complete

Deployment name: Microsoft.VirtualNetworkGateway-2022042714... Start time: 4/27/2022, 2:42:51 PM
 Subscription: Azure subscription 1 Correlation ID: 489b63db-2c37-4721-a926-cc
 Resource group: FG

Deployment details (Download)

Next steps

[Go to resource](#)

Notifications

More events in the activity log → Dismiss all

- Deployment succeeded ×
Deployment 'Microsoft.VirtualNetworkGateway-20220427143943' to resource group 'FG' was successful. [Go to resource](#) [Pin to dashboard](#) a few seconds ago
- Successfully deleted subnet ×
Successfully deleted subnet 'Gateway'. 25 minutes ago
- Successfully added subnet ×
Successfully added subnet 'Gateway' to virtual network 'Azure-FG'. 30 minutes ago

Figure 10.15: Deployment of virtual network gateway

4. Create a local network gateway as following:

- **Resource Group:** FG
- **Region:** West US
- **Name:** FortiGate
- **IP Address:** IP_Address_of_Port1_FortiGate (On premise)
- **Address Space:** IP_Address_LocalNetwork

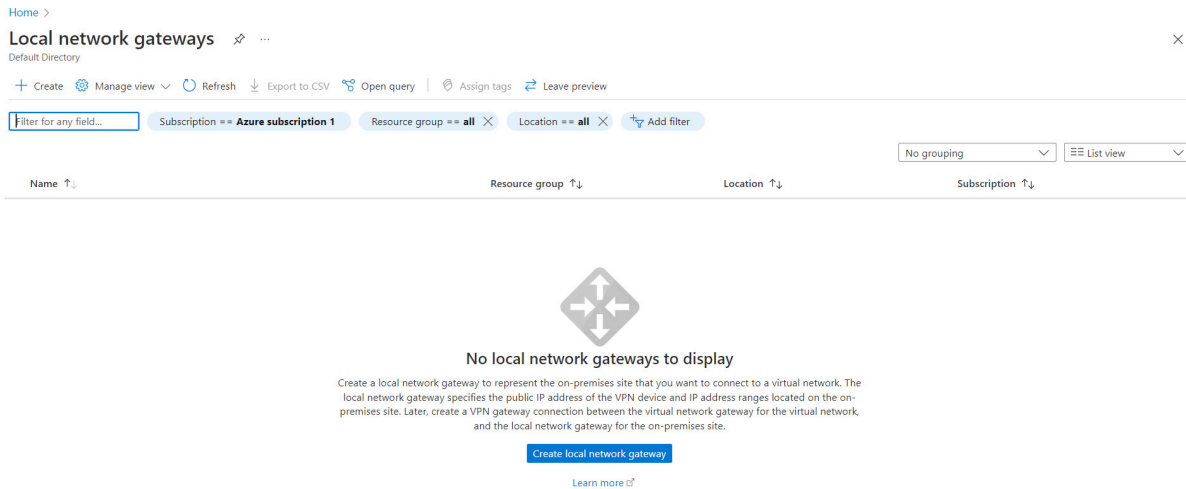


Figure 10.16: Create a local network gateway

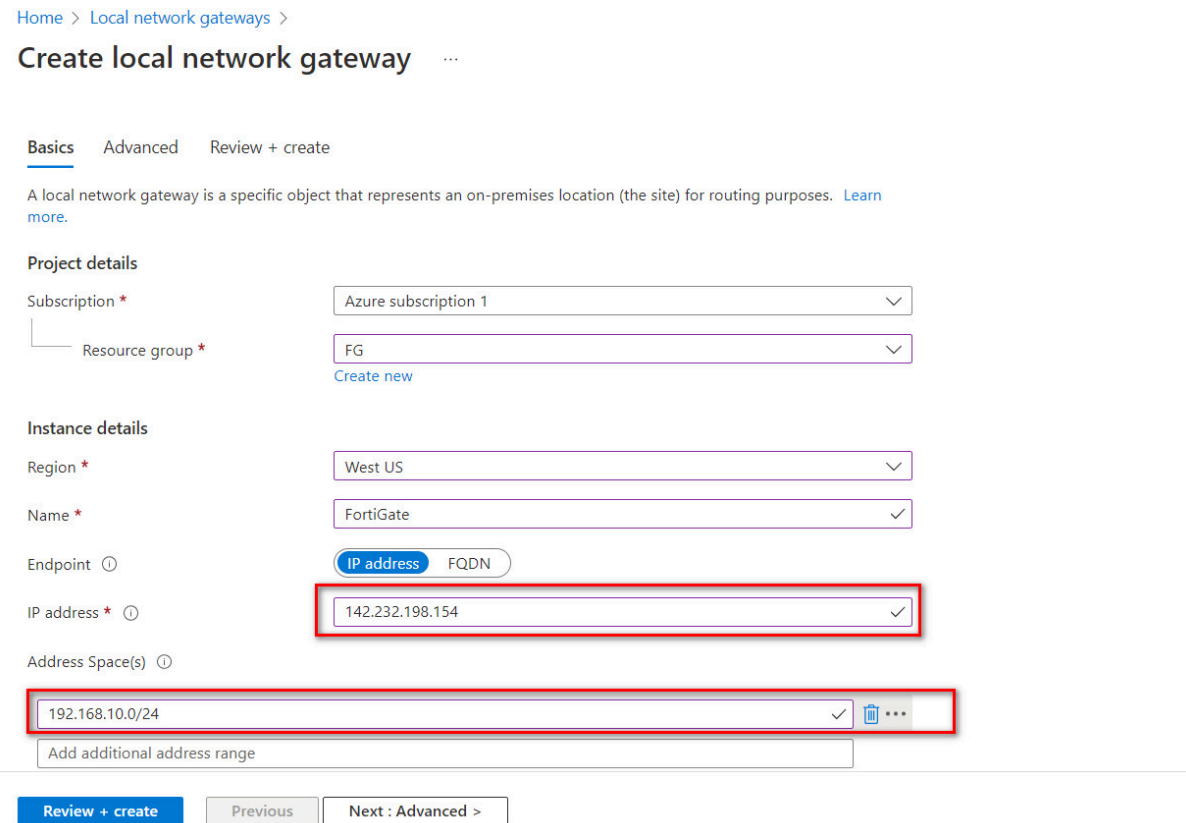


Figure 10.17: Create a local network gateway

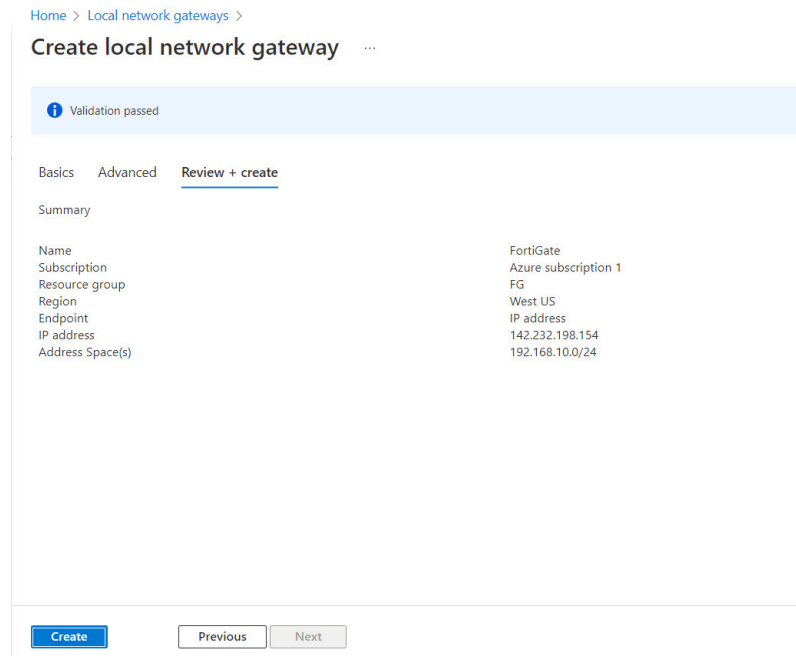


Figure 10.18: Create a local network gateway (review + create)

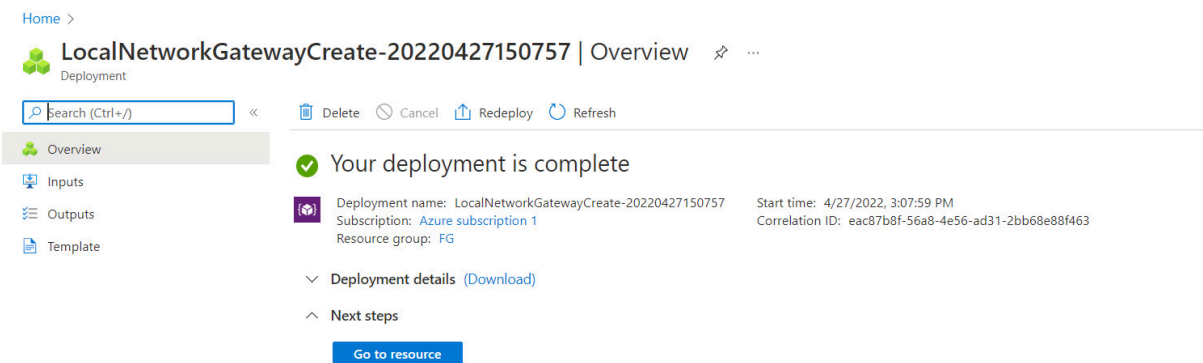


Figure 10.19: Verify local network gateway deployment

5. Go to Virtual network gateway and create a connection in **Virtual network gateways > connections > Add:**

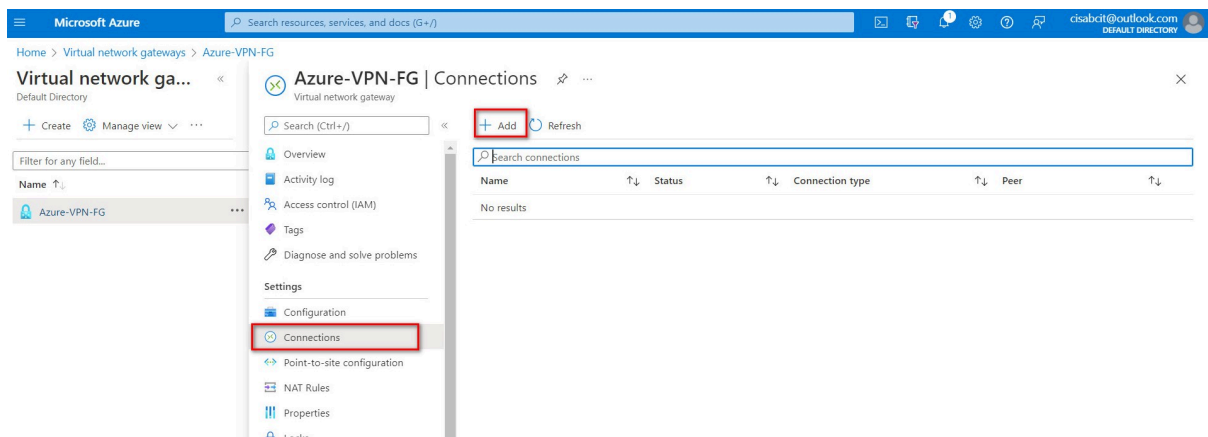


Figure 10.20: Add connections

Home > Virtual network gateways > Azure-VPN-FG >

Add connection ...
Azure-VPN-FG

Name *
VPNAZ ✓

Connection type ⓘ
Site-to-site (IPsec) ✓

*Virtual network gateway ⓘ
Azure-VPN-FG

*Local network gateway ⓘ
FortiGate

Shared key (PSK) * ⓘ
123456789 ✓

Use Azure Private IP Address ⓘ

Enable BGP ⓘ

IKE Protocol ⓘ
 IKEv1 IKEv2

Ingress NAT Rules

Figure 10.21: Connection configuration

Based on the Microsoft article “About cryptographic requirements and Azure VPN gateways” (<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-compliance-crypto>), by default, integrity is SHA384, SHA256, SHA1, MD5 and encryption is AES256, AES192, AES128, DES3, DES. So, we will select SHA1 and AES128 in FortiGate. After doing this step, you should receive a Public IP address in Overview tab.

Azure-VPN-FG Virtual network gateway

Search (Ctrl+F) Refresh Move Delete

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings Configuration Connections Point-to-site configuration NAT Rules Properties Locks

Essentials JSON View

Resource group (move) : FG SKU : VpnGw2
Location : West US Gateway type : VPN
Subscription (move) : Azure_subscription_1 VPN type : Route-based
Subscription ID : 9170d5fe-6ca8-4257-9a4b-462d6b7ab3cd Virtual network : Azure-FG
Public IP address : 13.64.90.115 (AzurePublic)

Tags (edit) : Click here to add tags

Health check Perform a quick health check to detect possible gateway issues
[Go to Resource health](#)

Advanced troubleshooting Run a troubleshooting tool to investigate failure causes and perform repair actions
[Go to VPN Troubleshooting](#)

Documentation View guidance on helpful topics related to VPN gateway
[View documentation](#)

Show data for last 1 hour 6 hours 12 hours 1 day 7 days 30 days

Figure 10.22: Verify public IP address

FortiGate Configuration

1. First, we will configure port 2 IP address.

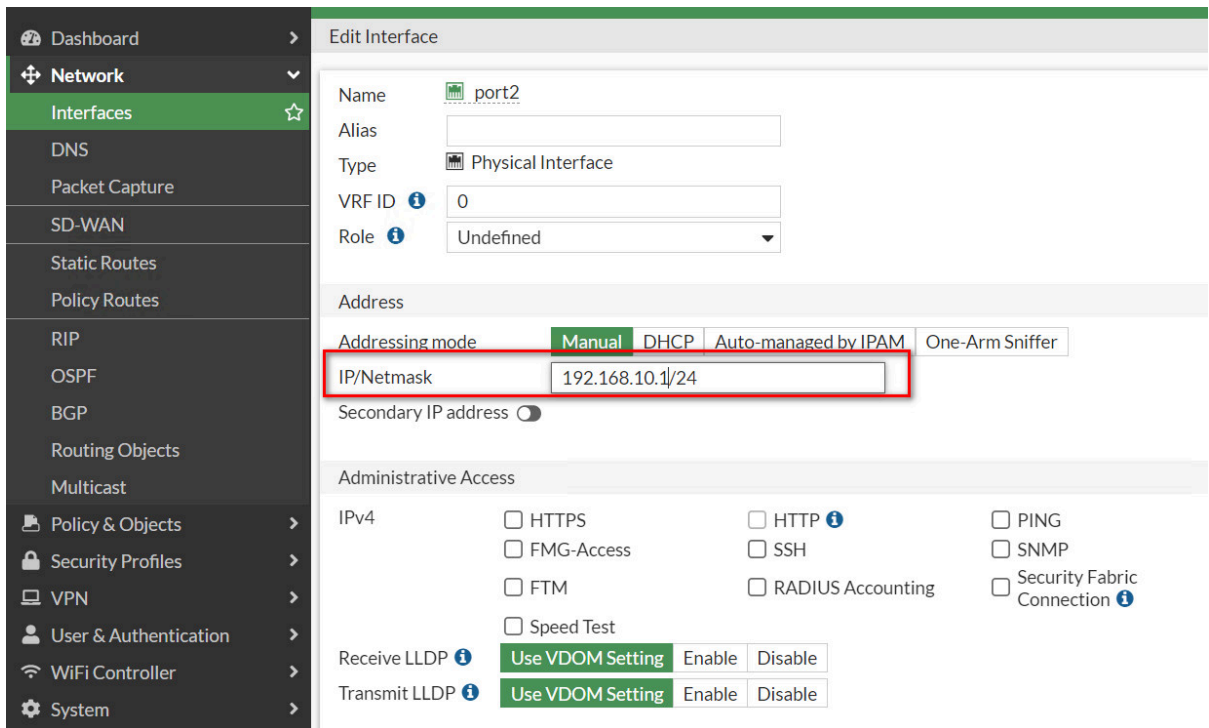


Figure 10.23: Set an IP address for port2

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 10				
port1	Physical Interface		142.232.198.154/255.255.255.0	HTTPS HTTP
port2	Physical Interface		192.168.10.1/255.255.255.0	
port3	Physical Interface		0.0.0.0/0.0.0.0	
port4	Physical Interface		0.0.0.0/0.0.0.0	
port5	Physical Interface		0.0.0.0/0.0.0.0	
port6	Physical Interface		0.0.0.0/0.0.0.0	
port7	Physical Interface		0.0.0.0/0.0.0.0	

Figure 10.24: Port1 and Port2 IP addresses

2. Create a static route to port1 (WAN Port) as Figure 10.25.

The screenshot shows the 'New Static Route' configuration page in the FortiGate web interface. The left sidebar shows the 'Network' menu with 'Static Routes' selected. The main content area has the following fields:

- Automatic gateway retrieval:
- Destination: Subnet (selected), Internet Service. Value: 0.0.0.0/0.0.0.0
- Gateway Address: Dynamic (selected), Specify. Value: 142.232.198.254
- Interface: port1
- Administrative Distance: 10
- Comments: Write a comment... (0/255)
- Status: Enabled (selected), Disabled
- Advanced Options: + (collapsed)

At the bottom right, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted in green.

Figure 10.25: Create a static route

3. Create a IPsec Wizard as a custom.

The screenshot shows the 'VPN Creation Wizard' configuration page in the FortiGate web interface. The left sidebar shows the 'VPN' menu with 'IPsec Wizard' selected. The main content area has the following fields:

- VPN Setup: 1 (step indicator)
- Name: FG-Azure
- Template type: Site to Site, Hub-and-Spoke, Remote Access, Custom (selected)
- Navigation buttons: < Back, Next > (highlighted in green), Cancel

Figure 10.26: Create a custom VPN

- **Remote Gateway IP Address:** *Public_IP_Address_Azure_Virtual_Gateway*
- **Nat Traversal:** Disable
- **Pre-shared Key:** *The same as Azure key (123456789)*
- **Local Address:** 192.168.10.0/24
- **Remote Address:** 10.0.0.0/16
- **Phase 1:** Encryption: AES128, Authentication: SHA-1, DH: 2, lifetime: 28800
- **Phase 2:** Encryption: AES128, Authentication: SHA-1, DH: 2, lifetime: 27000

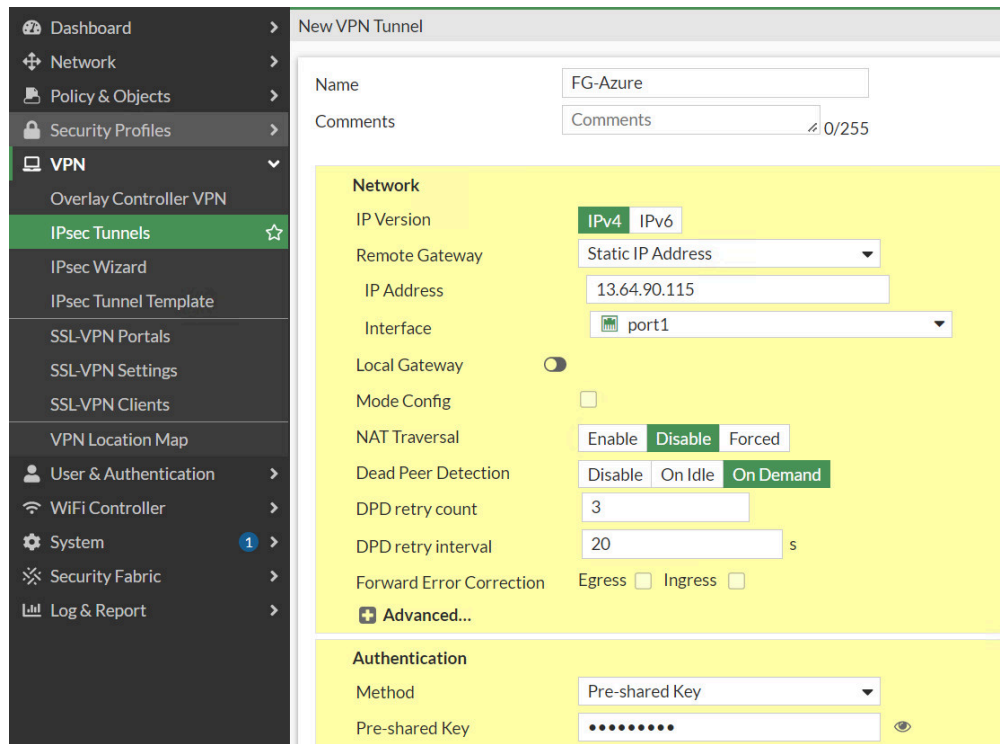


Figure 10.27: Create a custom VPN

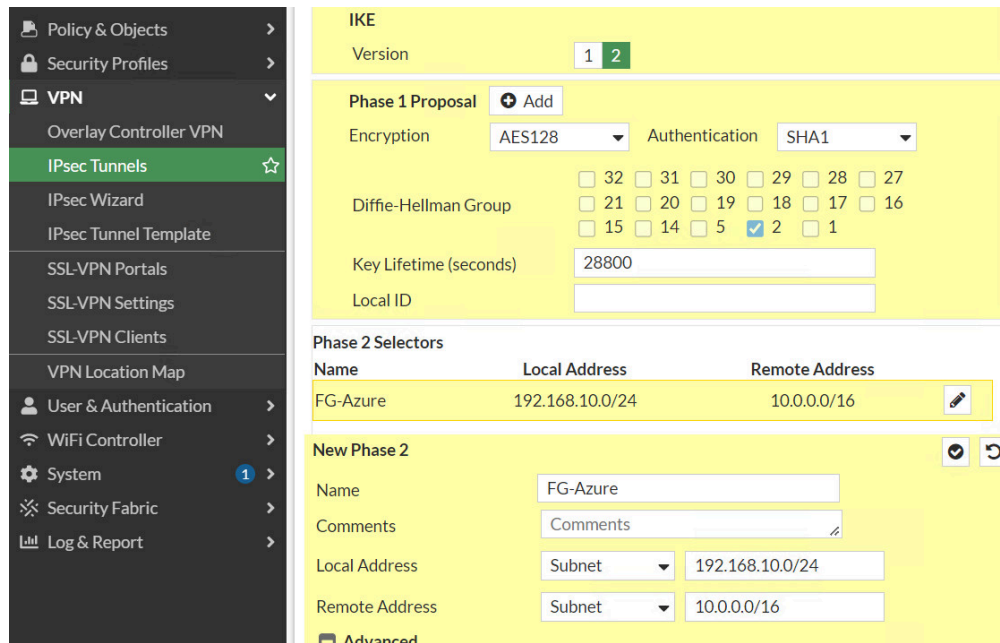


Figure 10.28: Create a custom VPN

Figure 10.29: Create a custom VPN

4. Create a firewall policy from Port 2 to Tunnel and from Tunnel to Port2. We will create a subnet for LAN on premise and a subnet for Microsoft Azure. Like site-to-site VPN we learned previously, NAT should be disabled here.

Figure 10.30: Create a subnet for local network

New Address

Name: AZ-LAN

Color: Change

Type: Subnet

IP/Netmask: 10.0.0.1/24

Interface: any

Static route configuration:

Comments: Write a comment... 0/255

OK Cancel

Figure 10.31: Create a subnet for Azure local

FGVM01TM19008000

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Log & Report

FG-AZURE

port2

FG-Azure

FG-LAN

AZ-LAN

always

ALL

ACCEPT DENY

Flow-based Proxy-based

NAT

Protocol Options: default

Security Profiles

AntiVirus

Web Filter

DNS Filter

OK Cancel

FG-FORTINET v7.0.3

Figure 10.32: Create a policy from port2 to FG-Azure Tunnel

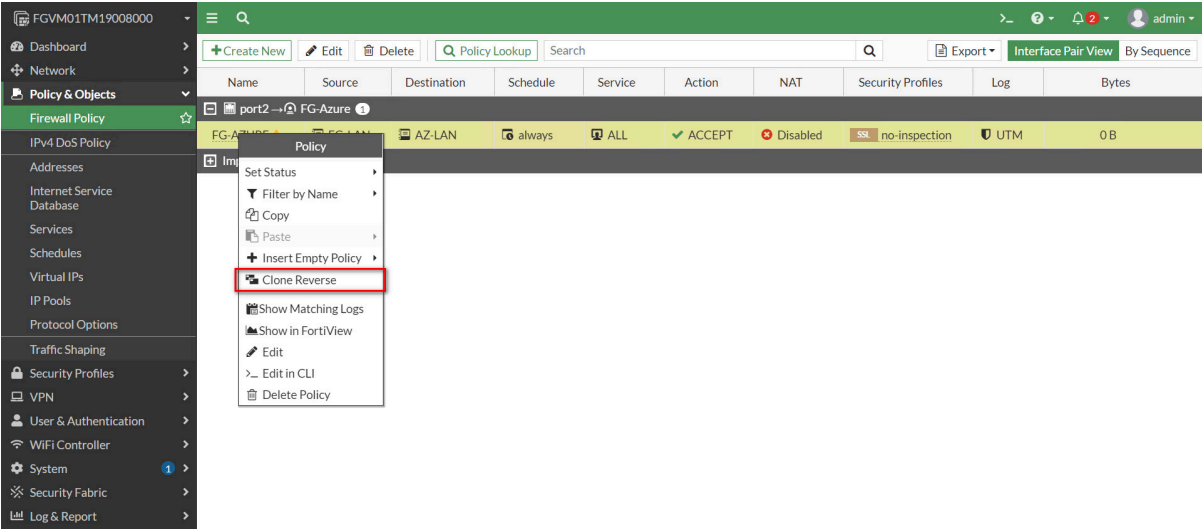


Figure 10.33: Create a policy from FG-Azure Tunnel to port2

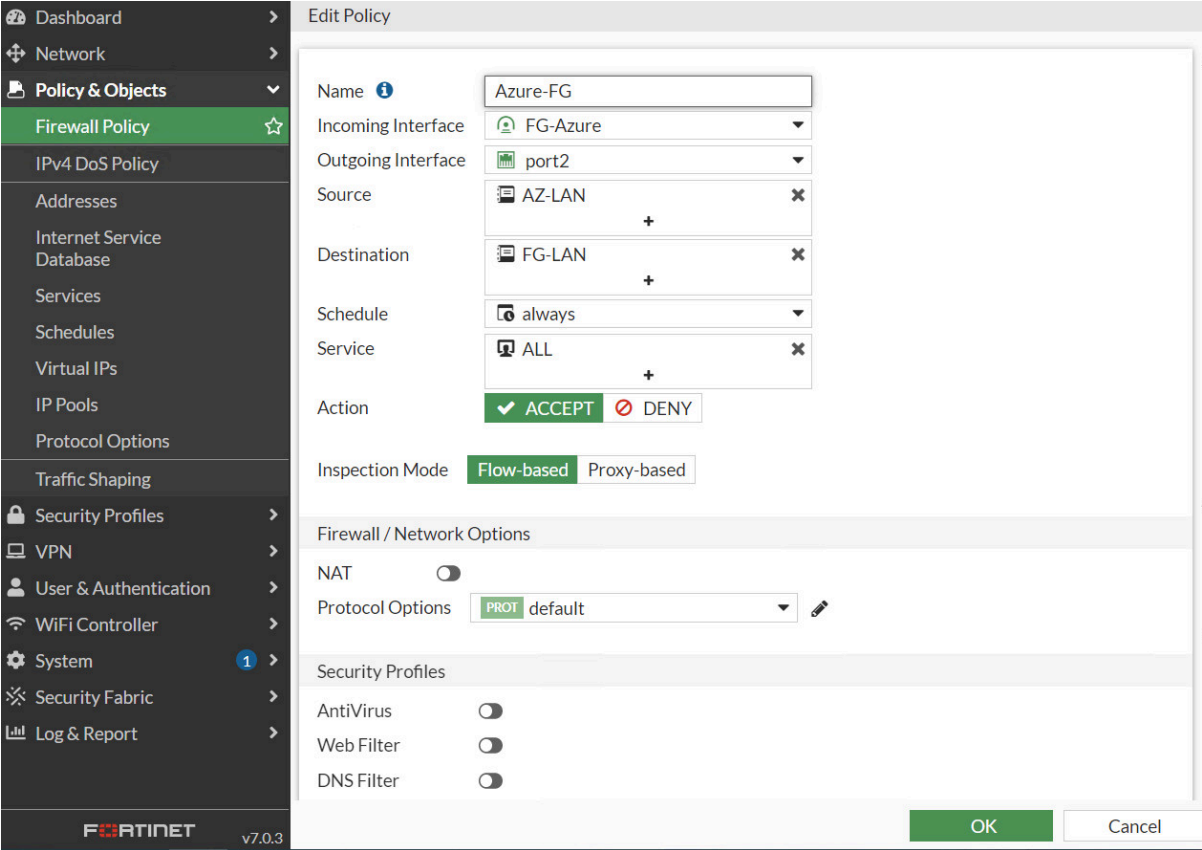


Figure 10.34: Create a policy from FG-Azure Tunnel to port2

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Azure-FG	AZ-LAN	FG-LAN	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
port2 -> FG-Azure	FG-Azure	port2							
FG-AZURE	FG-LAN	AZ-LAN	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
Implicit									

Figure 10.35: Firewall Policies

Verify Connections

If you navigate to IPsec Tunnel, the status should be up.

Tunnel	Interface Binding	Status	Ref.
FG-Azure	port1	Up	3

Figure 10.36: Verify status in FortiGate

Home > Virtual network gateways > Azure-VPN-FG

Virtual network ga... << Azure-VPN-FG | Connections >>

Virtual network gateway

Name	Status	Connection type	Peer
VPNAZ	Connected	Site-to-site (IPsec)	FortiGate

Figure 10.37: Verify status in Azure

10.2 Deploy FortiGate in Azure

Learning Objectives

- Create a FortiGate firewall in Azure through Marketplace
- Identify FortiGate subnets in Azure

Scenario: In this lab, we'll learn how to deploy FortiGate in Azure.

1. Go to Azure Marketplace and search for FortiGate.

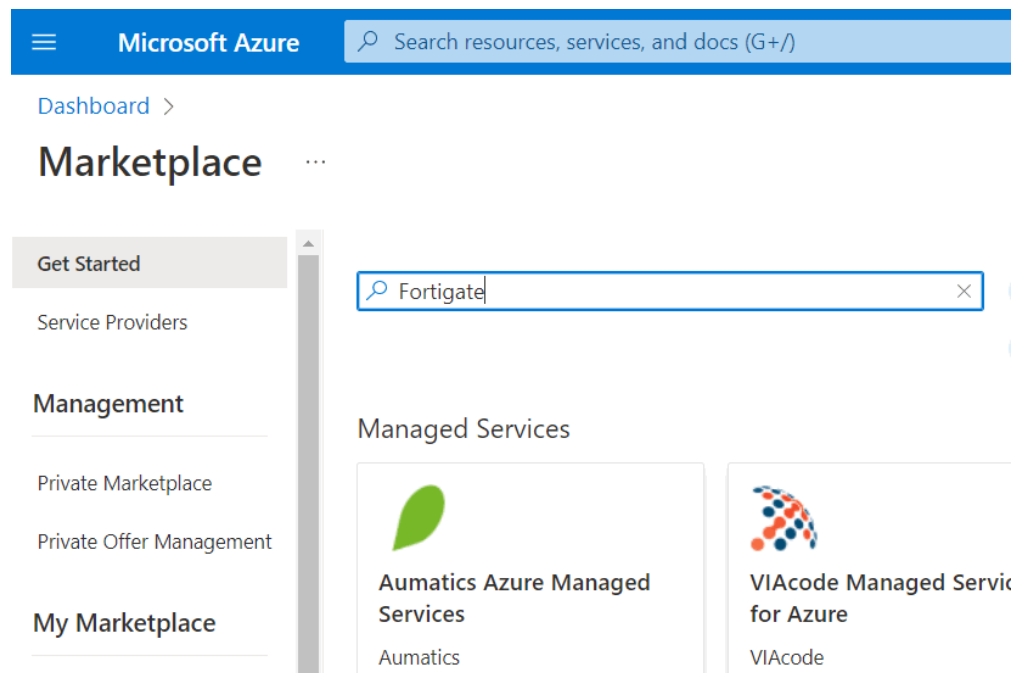


Figure 10.38: Search for FortiGate

2. Select Fortinet FortiGate Next-Generation Firewall.

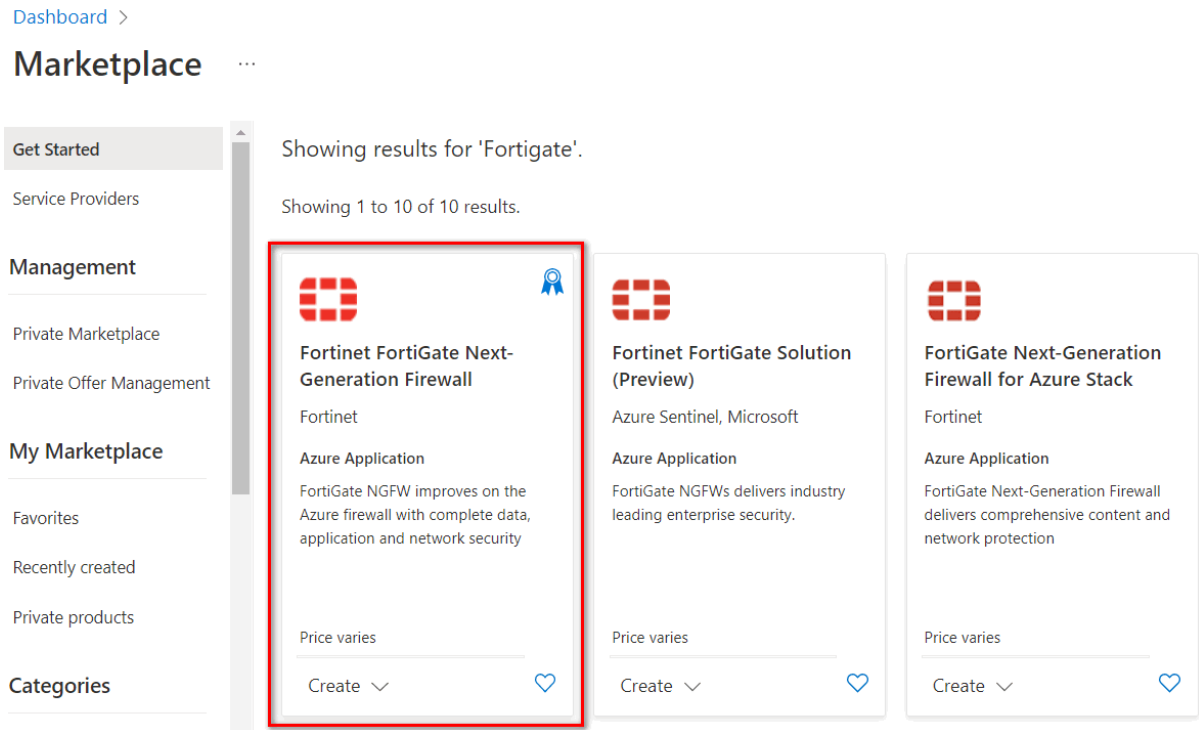


Figure 10.39: Select Fortinet FG Next-Gen

3. Then, Select Single VM from dropdown list.



Figure 10.40: Select Single VM

4. Create a firewall information as Figure 10.41.

Create Fortinet FortiGate Next-Generation Firewall ...

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ (New) FortiGate
[Create new](#)

Instance details

Region * ⓘ UK West

FortiGate administrative username * ⓘ hamid

FortiGate password * ⓘ

Confirm password * ⓘ

Fortigate Name Prefix * ⓘ hamid

Fortigate Image SKU ⓘ Pay As You Go

Fortigate Image Version ⓘ latest

[Review + create](#) [< Previous](#) [Next : Instance Type >](#)

Figure 10.41: Create a Fortinet firewall

5. Leave other tabs as default and press on **“Review+ create”**. It will validate your information and then you can create a FortiGate Firewall.

✓ Validation Passed

Basics Instance Type Networking Public IP Advanced Review + create

PRODUCT DETAILS

Fortinet FortiGate Next-Generation Firewall
 by Fortinet
[Terms of use](#) | [Privacy policy](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.


Name Hamid Talebi

[Create](#) [< Previous](#) [Next](#) [Download a template for automation](#)





Figure 10.42: Validate configuration


6. Then, it will start deployment of FortiGate. It takes around **5 minutes** to deploy FortiGate.


Dashboard >


fortinet.fortinet-fortigate-20220513160337 | Overview  ...


Deployment


<<  Delete  Cancel  Redeploy  Refresh

 Overview


 Inputs

 Outputs

 Template

 We'd love your feedback! →

Deployment is in progress

 Deployment name: fortinet.fortinet-fortigate-20220513160337 Start time: 5/13/2022, 4:05:30 PM
Subscription: [Azure subscription 1](#) Correlation ID: b143bd4f-1aa4-4
Resource group: [FortiGate](#)

Deployment details (Download)





Resource	Type	Status
 hamid-FGT-A	Microsoft.Compute/virtualMachines	Created
 hamid-FGT-A-Nic2	Microsoft.Network/networkInterfaces	Created
 hamid-FGT-A-Nic1	Microsoft.Network/networkInterfaces	Created

Figure 10.43: Deployment is in progress

 **Your deployment is complete**

 Deployment name: fortinet.fortinet-fortigate-20220513160... Start time: 5/13/2022, 4:05:30 PM
Subscription: [Azure subscription 1](#) Correlation ID: b143bd4f-1aa4-4c1a-9905-7ce0dbfed0a5 
Resource group: [FortiGate](#)

Deployment details (Download)

Next steps

[Go to resource group](#)

Figure 10.44: Deployment is complete

7. After deployment is completed, go to **Resource group > FortiGate > Overview** and look for FortiGate Public IP address.

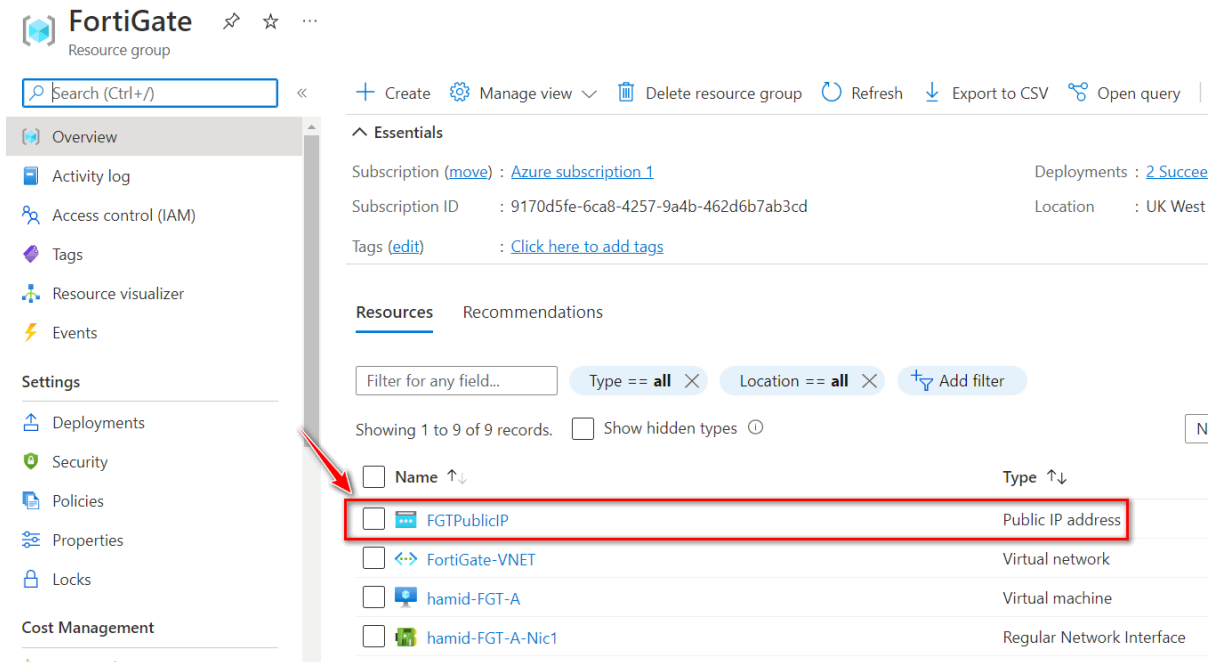


Figure 10.45: FortiGate public IP address

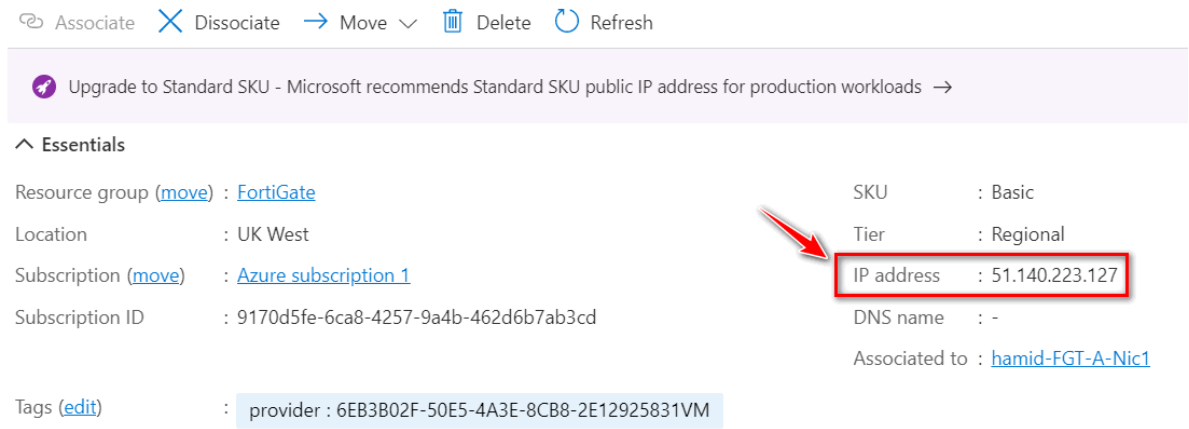


Figure 10.46: FortiGate public IP address

8. Type the IP address in the browser. You should be able to see the FortiGate credentials page. Enter your username and password to login in the firewall.

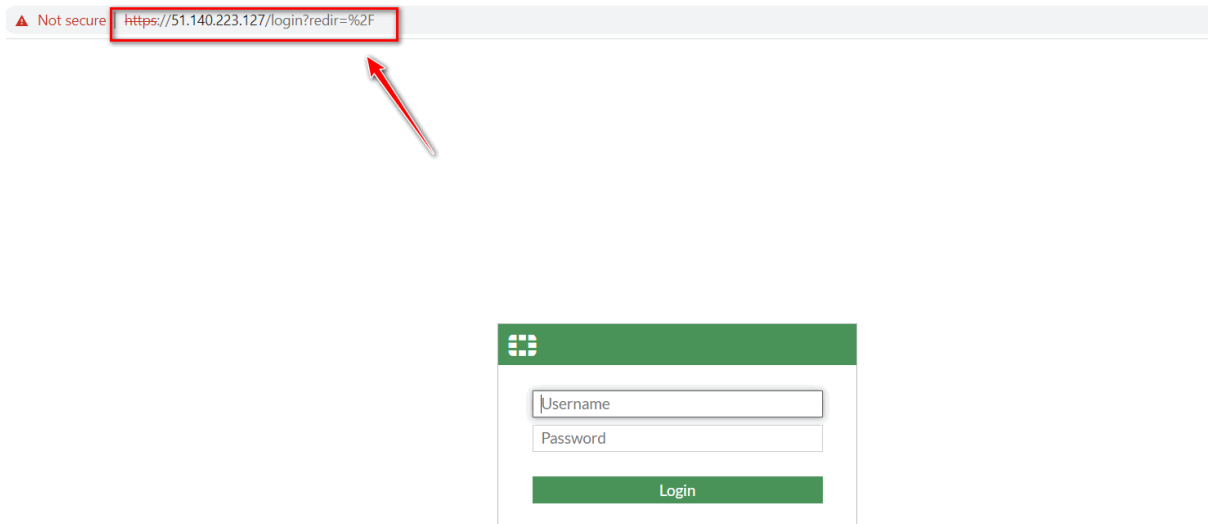


Figure 10.47: FortiGate firewall credential page

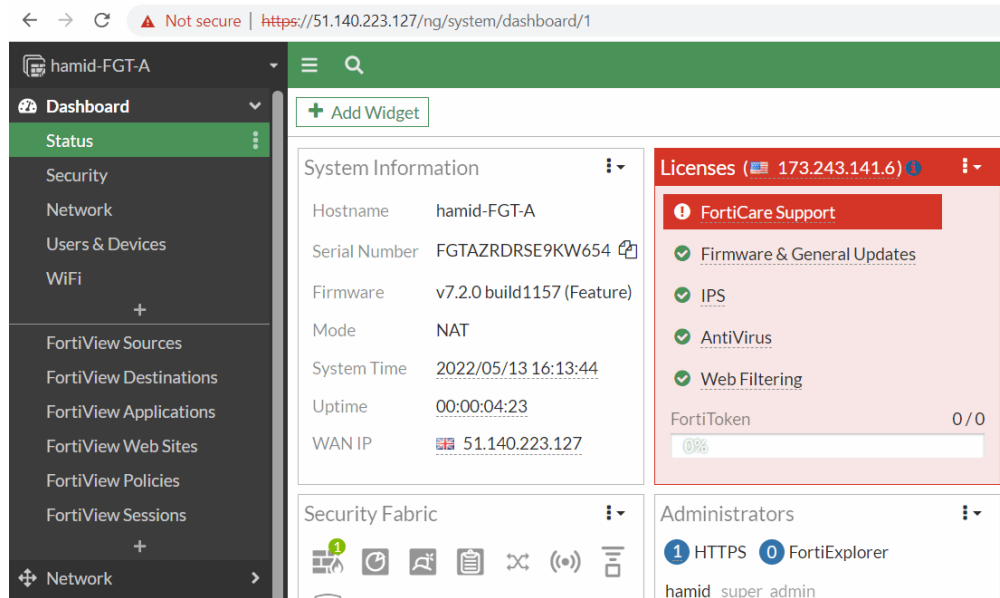


Figure 10.48: FortiGate dashboard

- Based on Fortinet description, we have three subnets in Azure for FortiGate. **External**, **Internal** and **Protected**. If you are planning to connect a new virtual machine to the firewall internal interface, you should connect it to the Protected subnet.

Table 10.2: FortiGate Subnet description in Azure

Subnet	Description
Subnet1	External subnet used to connect the FortiGate-VM to the Internet.
Subnet2	Internal subnet used as a transit network to one or multiple protected networks containing backend services, such as the web server.
Subnet3	Protected subnet used to deploy services. You can deploy multiples of these subnets. The traffic is sent to the FortiGate for inspection using UDR.

10.3 Site to Site VPN between FortiGate on Premise and FortiGate in the Azure

Learning Objectives

- Configure a VPN Wizard in Azure
- Configure site-to-site VPN between FortiGate on premise and Azure
- Identify FortiGate subnets in Azure

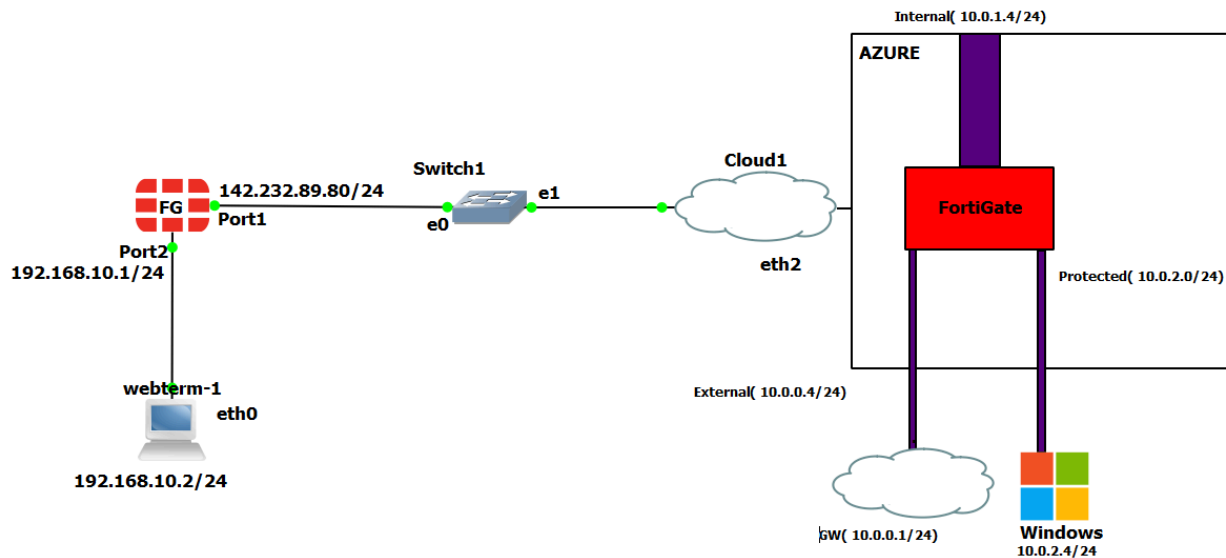


Figure 10.49: Main scenario

Scenario: In this lab, we are going to create a site-to-site VPN from FortiGate on premise to FortiGate in the Azure. Knowing the configuration from section 10.2 is necessary for this lab. Port1 is set as a DHCP, so they will receive an IP address from Cloud.

Table 10.3: Devices configuration

Device	Interface	IP address
FortiGate	Port 1	DHCP Client
	Port 2	192.168.10.1/24
WebTerm	Eth0	192.168.10.2/24

1. On Premise FortiGate Configuration. Follow these steps:

1. Configure the interfaces of the firewall. Port2 by default is an internal interface and name as a “LAN” and Port1 is an external interface and name as a “WAN”.

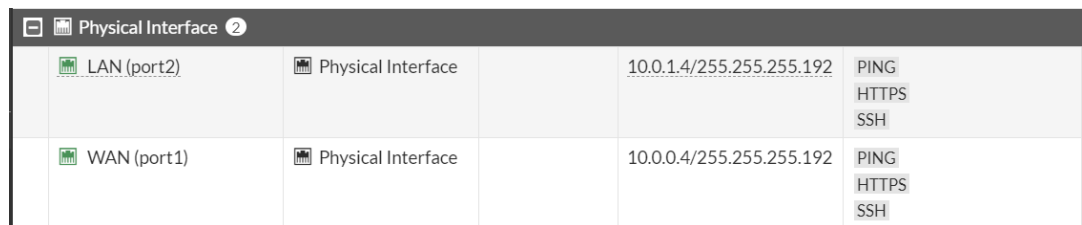


Figure 10.50: Firewall interfaces

2. Create a site-to-site VPN from IPsec Wizard as Figures 10.51 to 10.53.

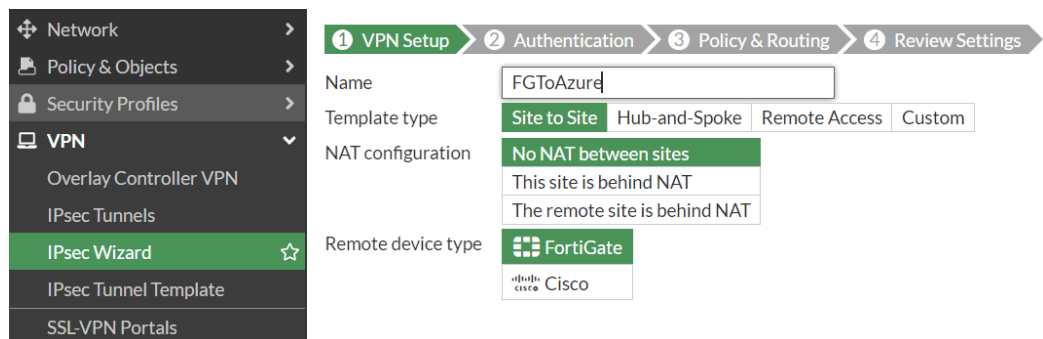


Figure 10.51: Select VPN name

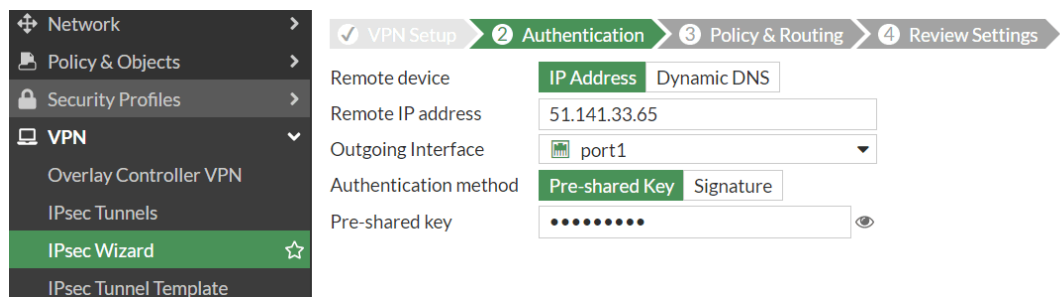


Figure 10.52: Set remote IP address

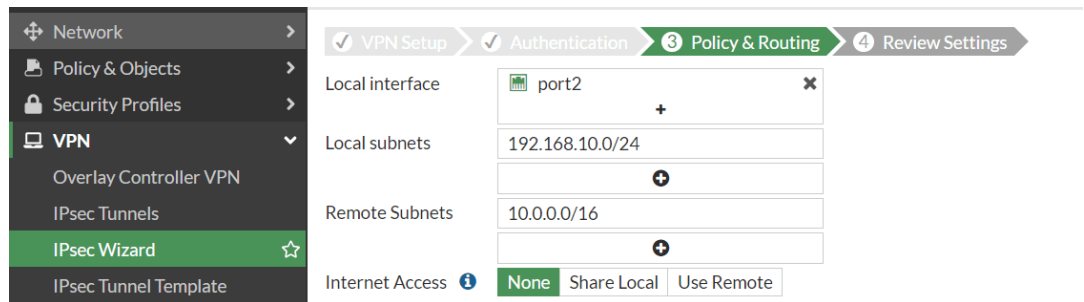


Figure 10.53: Set Policy & Routing

3. Create a static route to the default gateway.

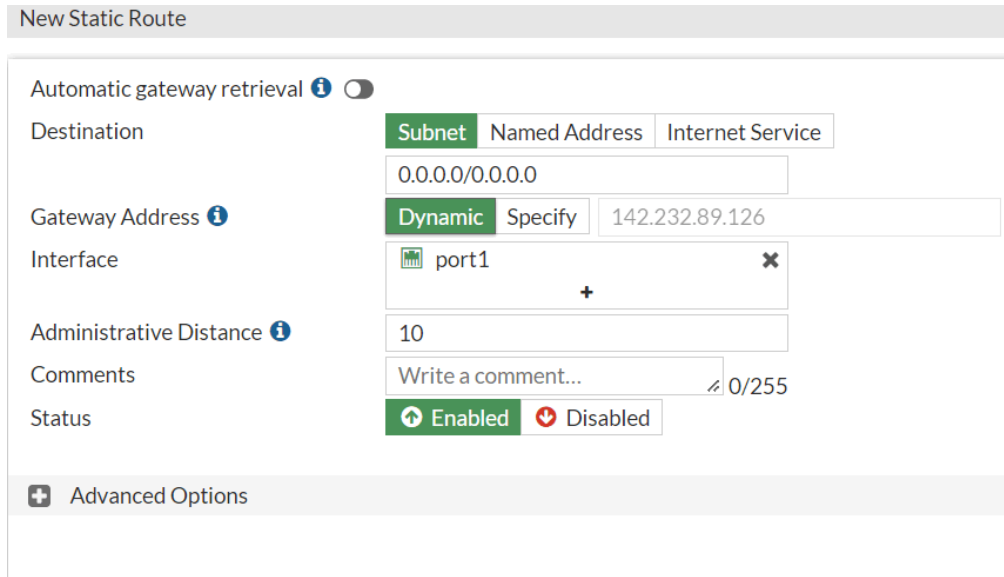


Figure 10.54: Set a default gateway

2. Azure Configuration. Follow these steps:

1. Create a FortiGate firewall in Azure and configure the interfaces. You need to do all steps found in section 10.1.
2. Create a VPN from IPsec Wizard as Figures 10.55 to 10.57.

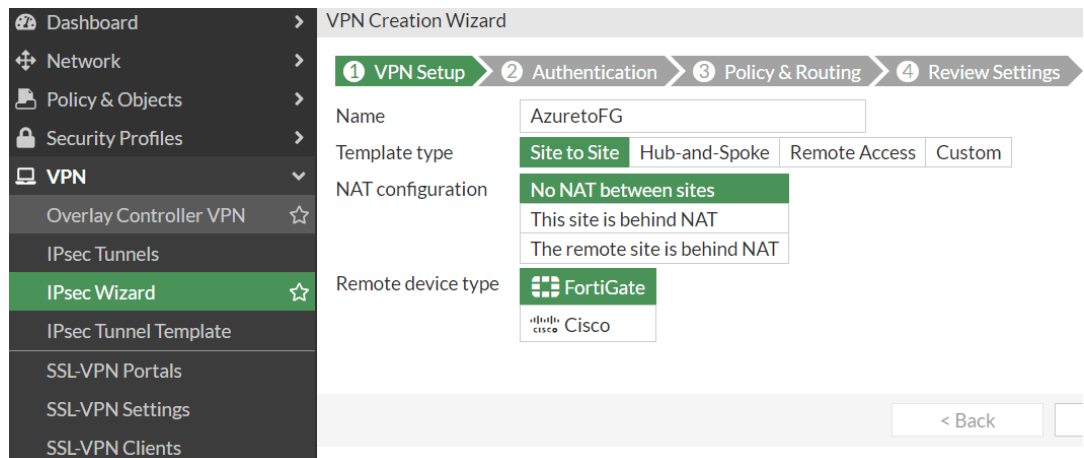


Figure 10.55: Select VPN name

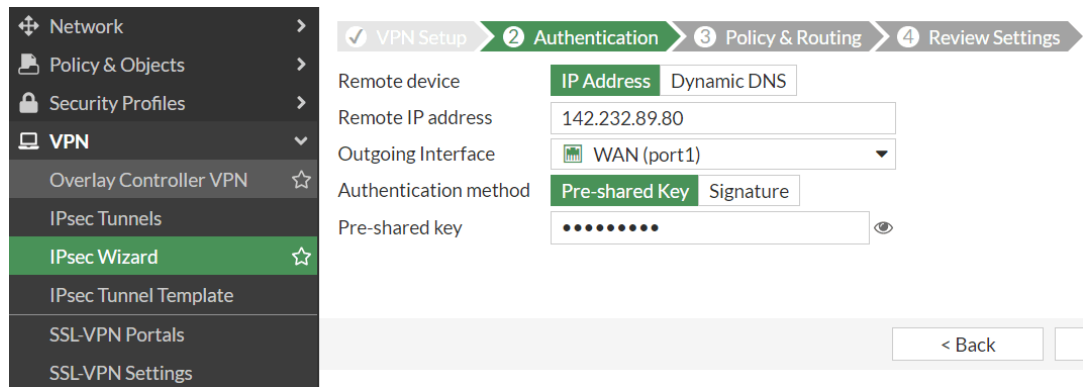


Figure 10.56: Set a remote IP address

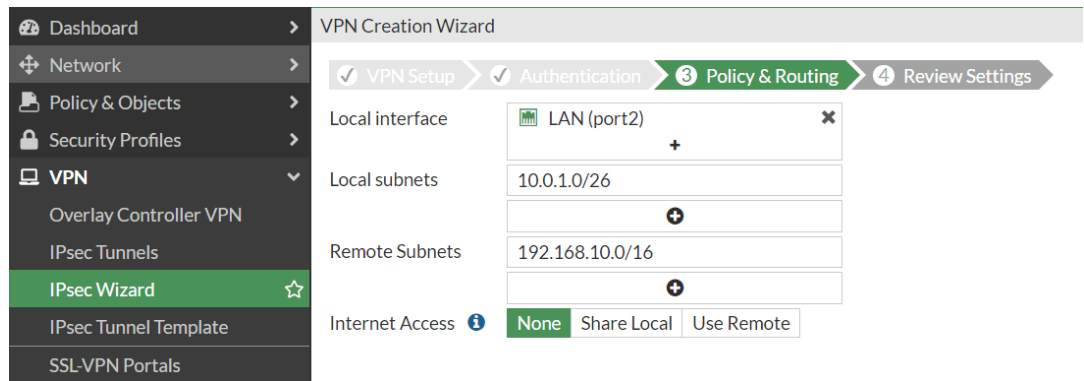


Figure 10.57: Set Policy & Routing

3. Add a Linux or Windows Virtual Machine to **Protected subnet**. You don't need to enable public IP address. Your private IP address should be in the range of 10.0.2.0/24.
4. Go to **VPN > IPsec Tunnels** and check status of the tunnel.

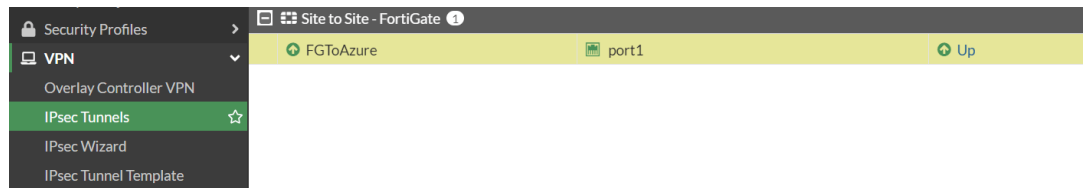


Figure 10.58: Check status of tunnel

5. You should be able to ping from WebTerm to the Virtual Machine.

```
root@webterm-1 ~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.033 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.046 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.044 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.047 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.048 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.048 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=0.052 ms
..
```

Figure 10.59: Ping from WebTerm to Windows VM

10.4 IPsec VPN from FortiGate (on Premise) to AWS

Learning Objectives

- Configure a Customer Gateway in AWS
- Configure a Virtual Private Gateway
- Create an IPsec VPN between FortiGate on-Premise and AWS

Scenario: We are going to connect on premise FortiGate to AWS Virtual Gateway. This is going to be IPsec VPN between FortiGate and AWS. First, we will configure AWS and then connect FortiGate through Port1 to AWS Virtual Gateway

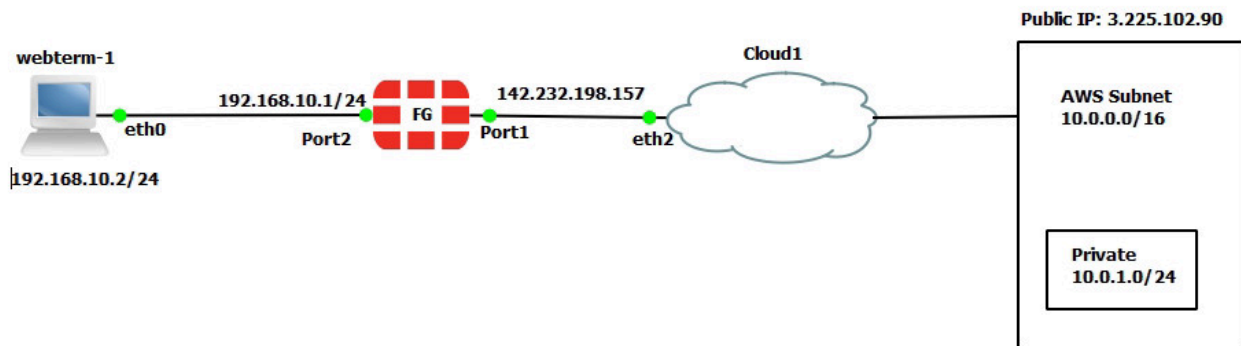


Figure 10.60: Main scenario

Table 10.4: On-premise devices configuration

Device	Configuration	Access
FortiGate	Port 1: DHCP Client Port 2: 192.168.10.1/24	Port1: HTTP, HTTPS, PING
WebTerm1	192.168.10.2/24	–

AWS Configuration

1. Create a VPC for AWS as follows:

- **Name tag:** AWS Subnet
- **IPv4 CIDR:** 10.0.0.0/16

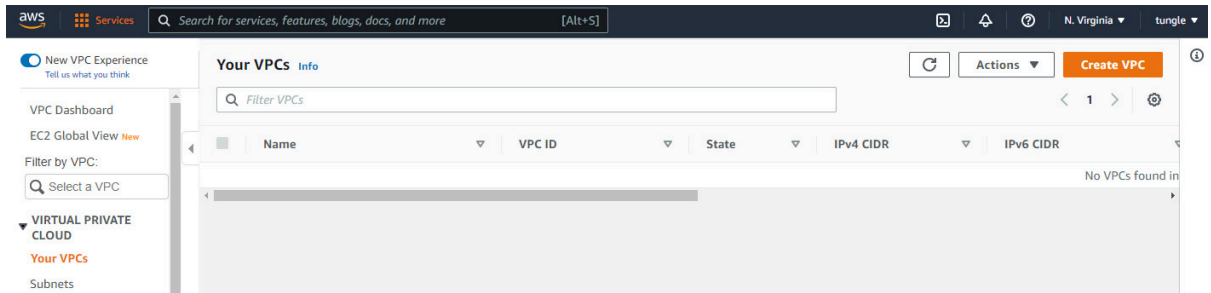


Figure 10.61: Create a VPC

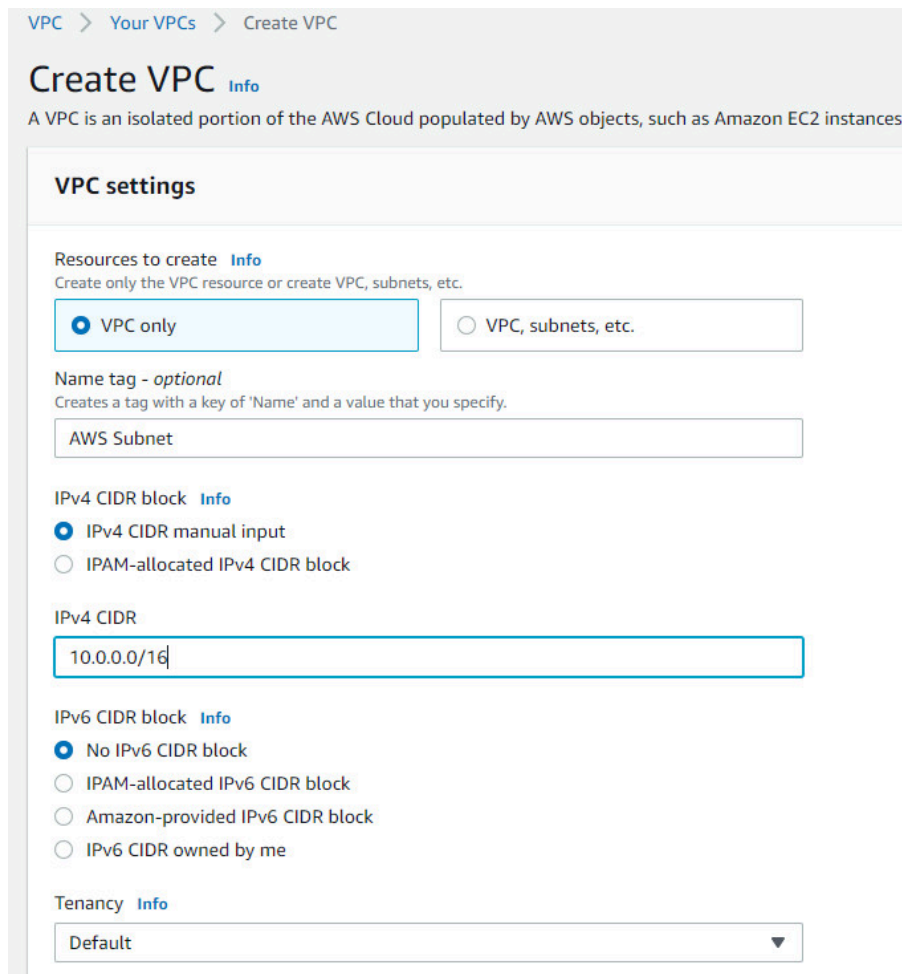


Figure 10.62: Create a VPC named “AWS Subnet”

2. Create a private subnet under AWS VPC as follows:

- **VPC:** AWS Subnet

- Subnet Name: **Private**
- IPv4 CIDR block: **10.0.1.0/24**

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-0a92013e3d2c88ae4 (AWS Subnet) ▼

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

Private

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference ▼

IPv4 CIDR block [Info](#)

10.0.1.0/24 ✕

Figure 10.63: Create a subnet under AWS VPC

3. Create an internet gateway as follows:



Figure 10.64: Create an internet gateway

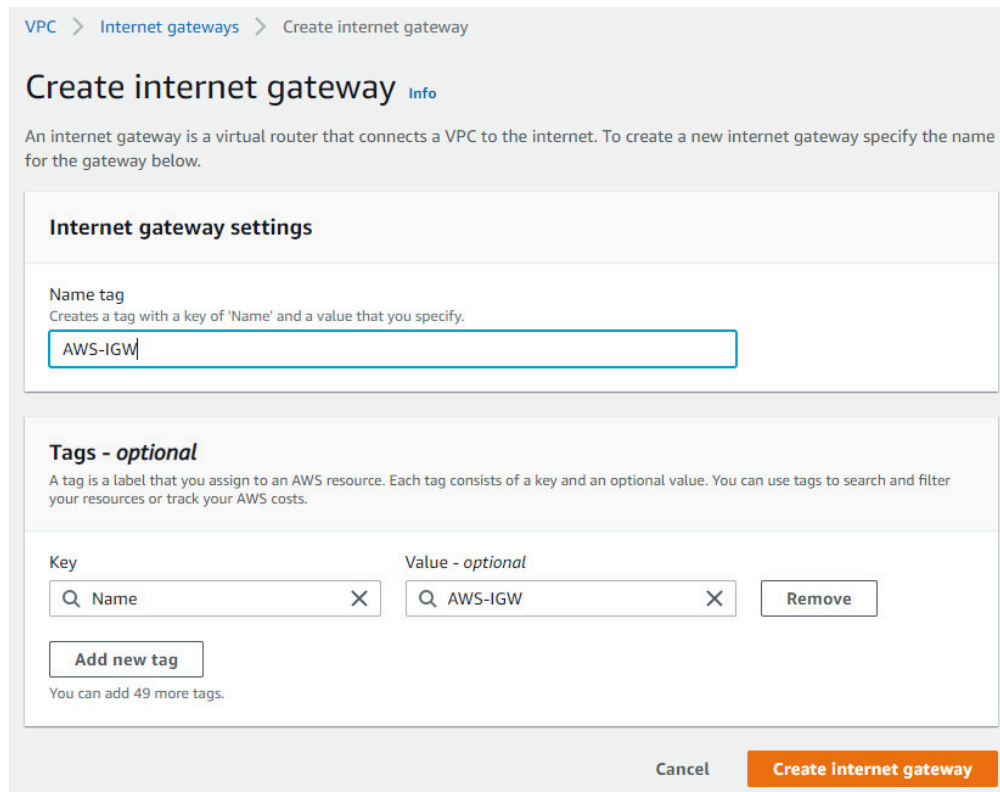


Figure 10.65: Select Name as AWS-IGW

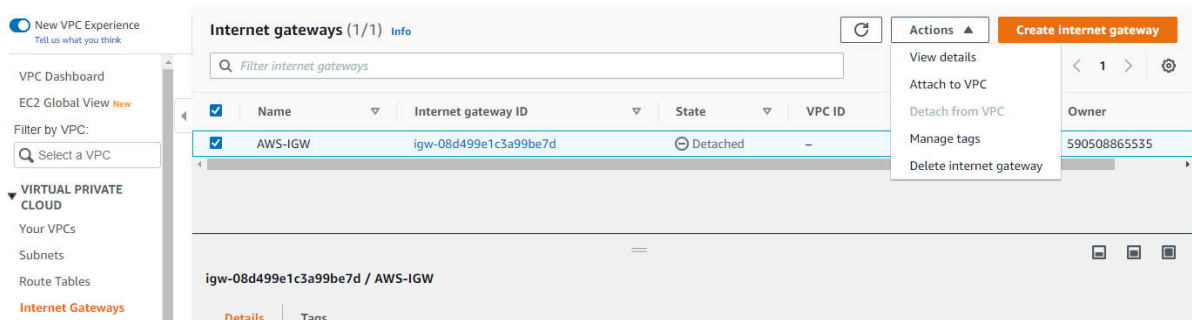


Figure 10.66: Attach the internet gateway to VPC

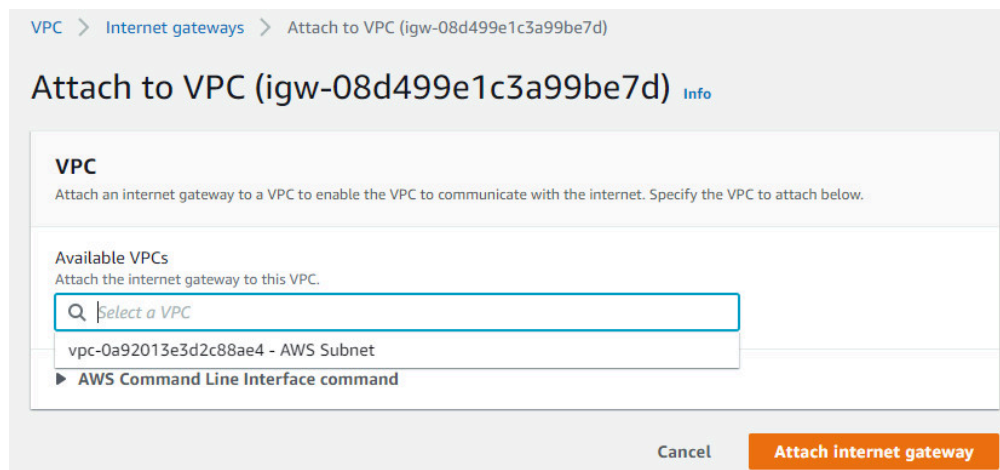


Figure 10.67: Attach the internet gateway to VPC

4. Create a static route to the internet gateway (AWS-IGW). Edit Routes as follows:

The screenshot shows the AWS Management Console interface for editing routes in a VPC. The left sidebar contains navigation options like 'VPC Dashboard', 'Subnets', 'Route Tables', and 'Internet Gateways'. The main content area displays the 'Route tables (1/1)' for the VPC 'vpc-0a92013e3d2c88ae4'. The 'Routes (1)' section shows a table with one route:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

The 'Edit routes' button is highlighted with a red box and an arrow.

Figure 10.68: Edit routes

The screenshot shows the 'Edit routes' page with a dropdown menu open for the 'Target' field. The dropdown menu lists various target options, and 'Internet Gateway' is highlighted with a red box.

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0		-	No

The dropdown menu options include: Carrier Gateway, Core Network, Egress Only Internet Gateway, Gateway Load Balancer Endpoint, Instance, Internet Gateway, local, NAT Gateway, Network Interface, Outpost Local Gateway, Peering Connection, Transit Gateway, and Virtual Private Gateway.

Figure 10.69: Add a new route 0.0.0.0/0 to your internet gateway

The screenshot shows the 'Edit routes' page with the dropdown menu closed. The 'Internet Gateway' option is selected, and its ID 'igw-08d499e1c3a99be7d (AWS-IGW)' is displayed in the 'Target' field.

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-08d499e1c3a99be7d (AWS-IGW)	-	No

Figure 10.70: Add a new route 0.0.0.0/0 to your internet gateway

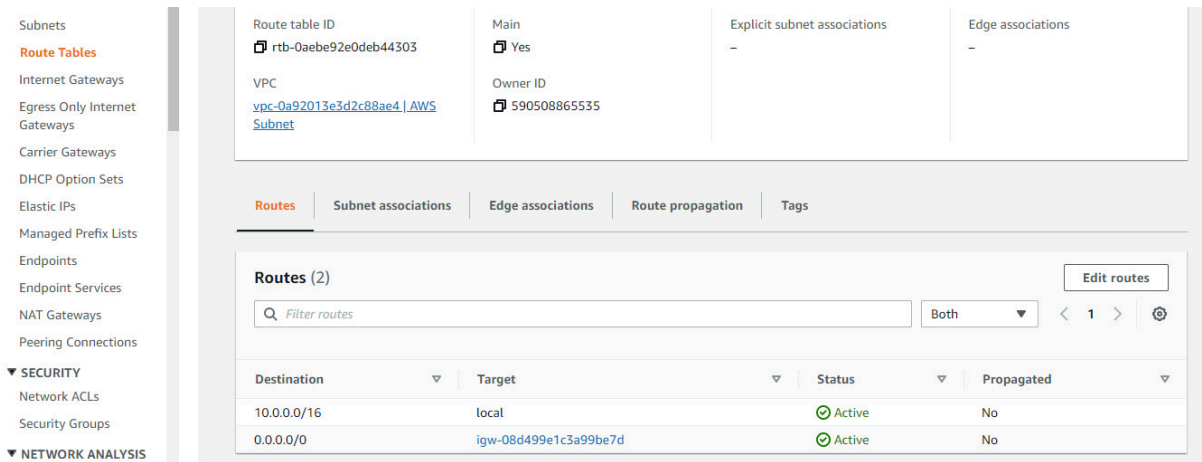


Figure 10.71: Route tables overview

5. Create a customer gateway as follows:

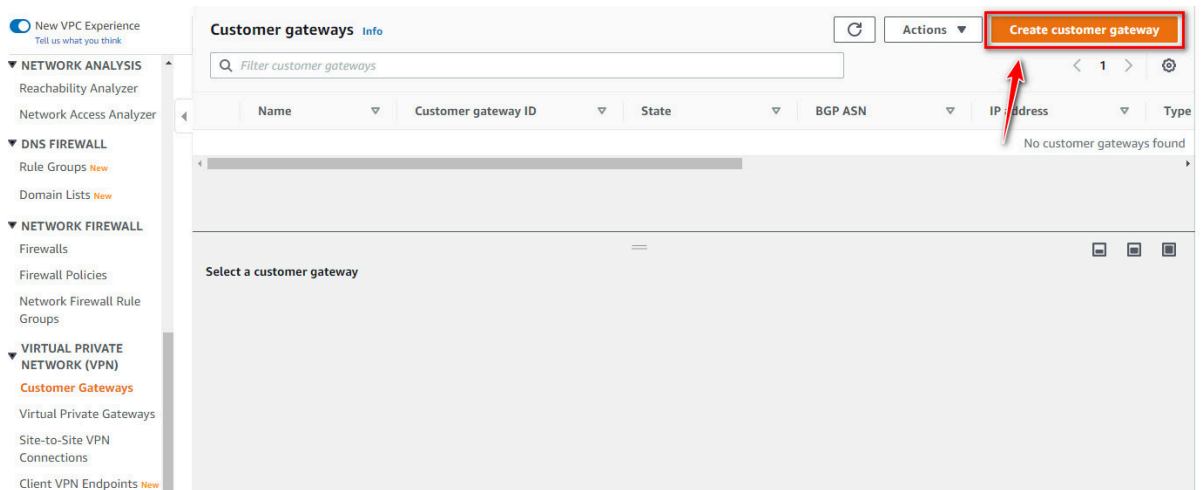


Figure 10.72: Create a customer gateway

Create customer gateway Info

A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network.

Details

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

Value must be 256 characters or less in length.

BGP ASN Info
The ASN of your customer gateway device.

Value must be in 1 - 2147483647 range.

IP address Info
Specify the IP address for your customer gateway device's external interface.

Certificate ARN
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).

Device - optional
Enter a name for the customer gateway device.

Figure 10.73: Create a customer gateway

6. Create a virtual private gateway as follows:

The screenshot shows the AWS Management Console interface for 'Virtual private gateways'. The page title is 'Virtual private gateways Info'. There is a search bar and a table with columns: Name, Virtual private gateway ID, State, Type, and VPC. The table is empty with the message 'No virtual private gateways found'. A red arrow points to the 'Create virtual private gateway' button in the top right corner. The left sidebar shows the navigation menu with 'Virtual Private Gateways' highlighted.

Figure 10.74: Create a virtual private gateway

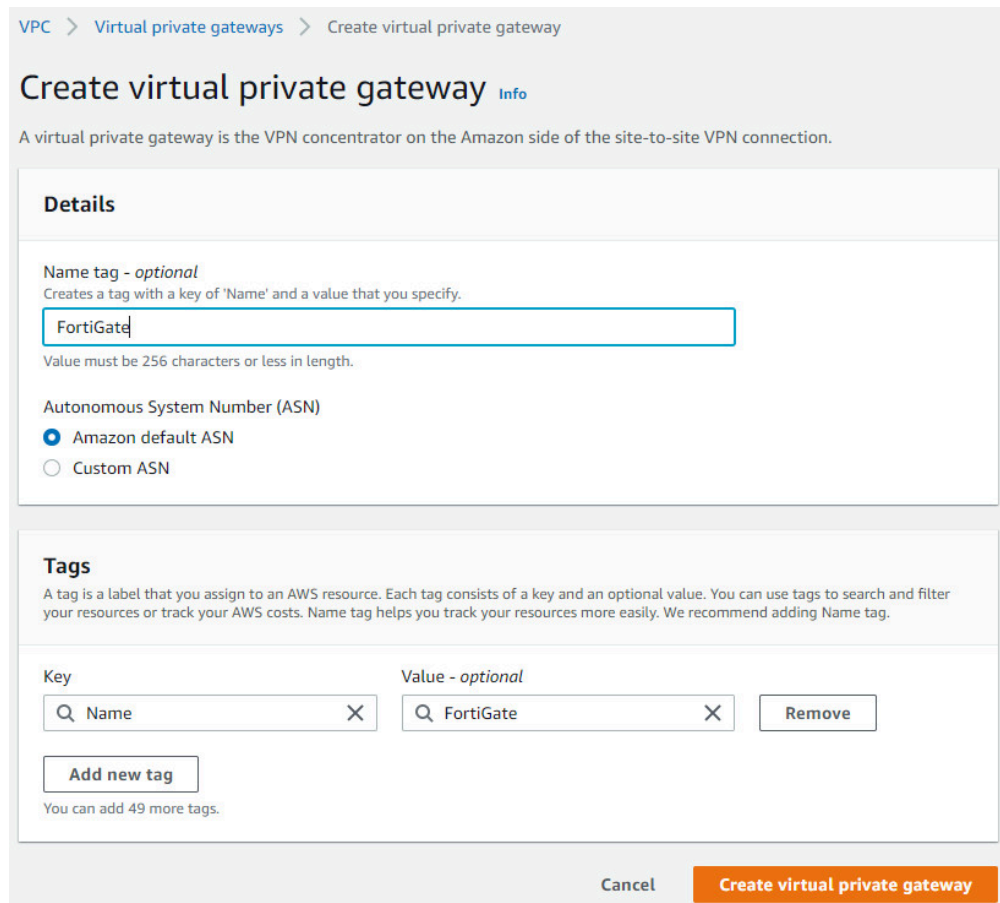


Figure 10.75: Create a virtual private gateway on FortiGate

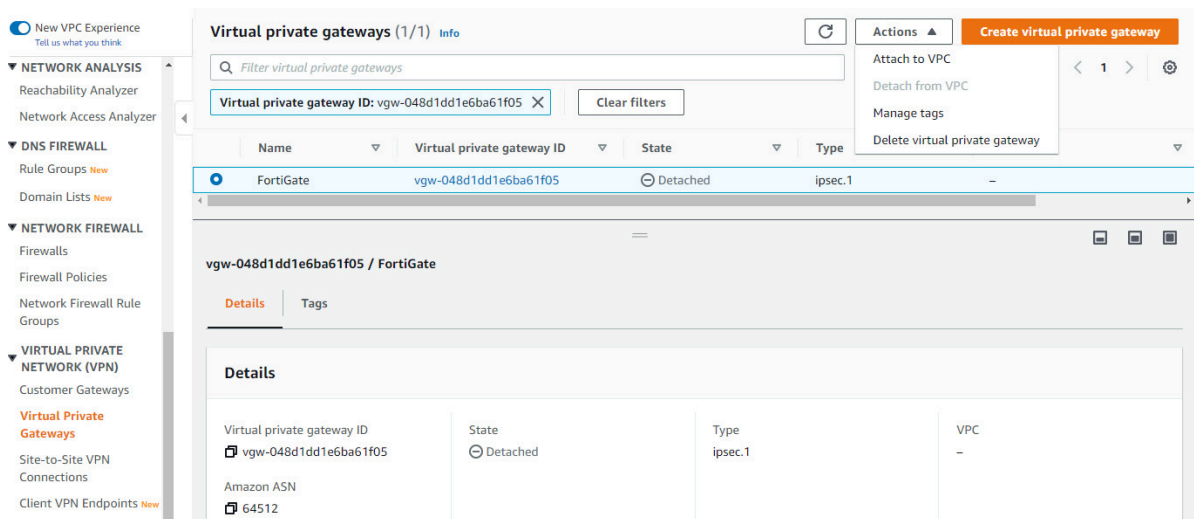


Figure 10.76: Attach virtual private gateway to VPC

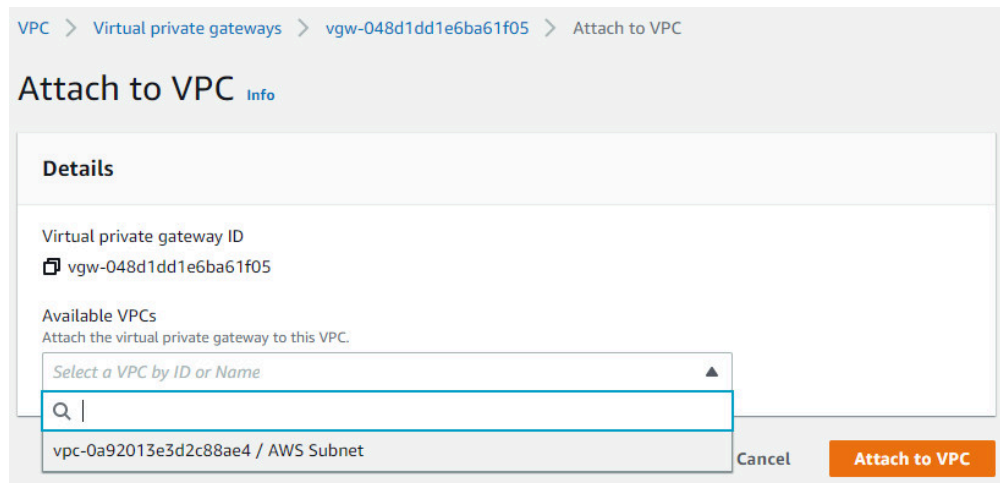


Figure 10.77: Attach virtual private gateway to VPC

7. Create a Site-to-Site VPN connection as follows:

- **Name Tag:** VPNAWS
- **Target gateway type:** Virtual private gateway
- **Virtual Private Gateway:** FortiGate
- **Customer Gateway ID:** AWS-VPN-FG
- **Routing options:** Static
- **Static IP prefixes:** 192.168.10.0/24
- **Local IPv4 network CIDR:** 192.168.10.0/24
- **Remote IPV4 network CIDR:** 10.0.1.0/24
- **Tunnel 1 and Tunnel 2 options:** leave it as default

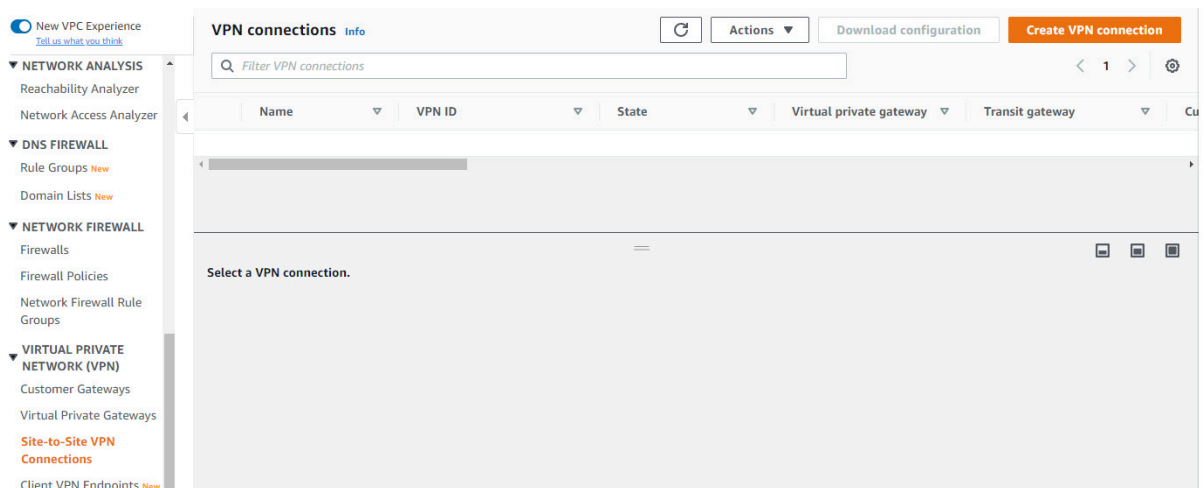


Figure 10.78: Create a site-to-site VPN connection

VPC > VPN connections > Create VPN connection

Create VPN connection [Info](#)

Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.

Details

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

Value must be 256 characters or less in length.

Target gateway type [Info](#)

Virtual private gateway
 Transit gateway
 Not associated

Virtual private gateway

Customer gateway [Info](#)

Existing
 New

Customer gateway ID

Routing options [Info](#)

Dynamic (requires BGP)
 Static

Figure 10.79: Create a site-to-site VPN connection with FortiGate

Static IP prefixes [Info](#)

Local IPv4 network CIDR - *optional*

The IPv4 CIDR range on the customer gateway (on-premises) side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

Remote IPv4 network CIDR - *optional*

The IPv4 CIDR range on the AWS side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

▶ **Tunnel 1 options** - *optional* [Info](#)

▶ **Tunnel 2 options** - *optional* [Info](#)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key Value - *optional*

You can add 49 more tags.

Figure 10.80: Create a site-to-site VPN connection with FortiGate

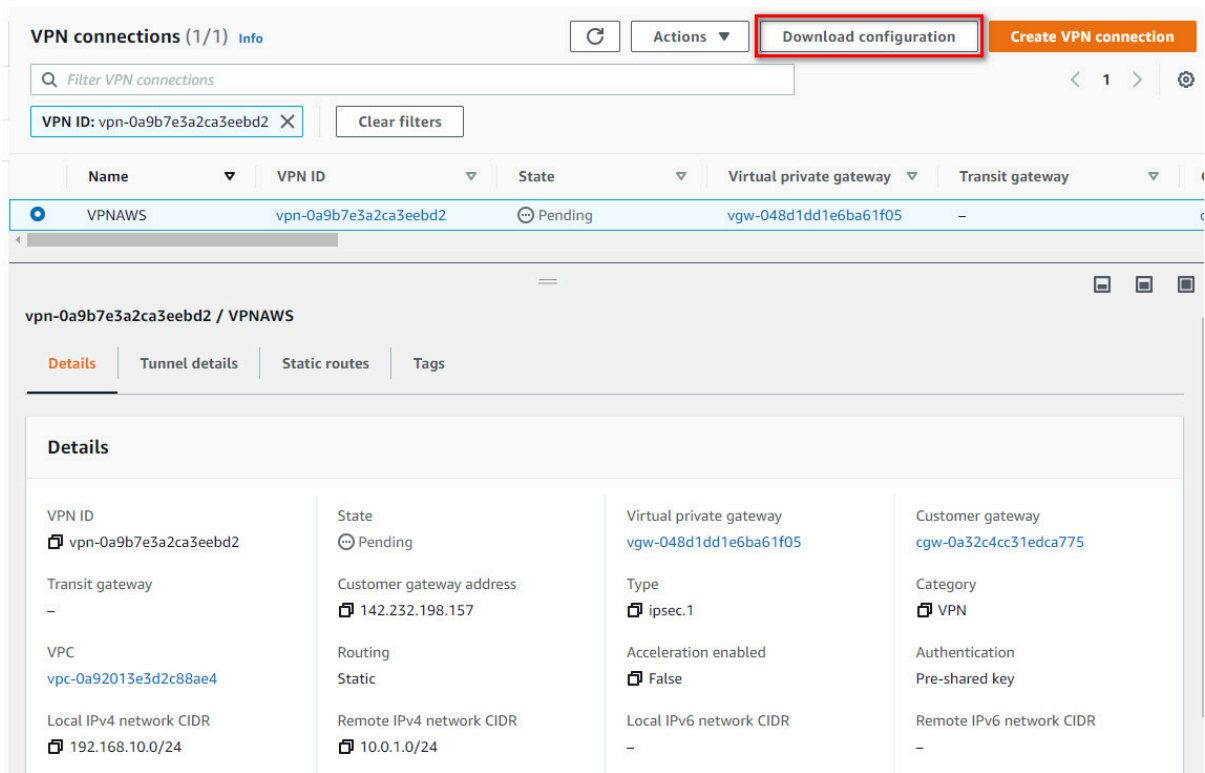


Figure 10.81: Create a site-to-site VPN connection with FortiGate

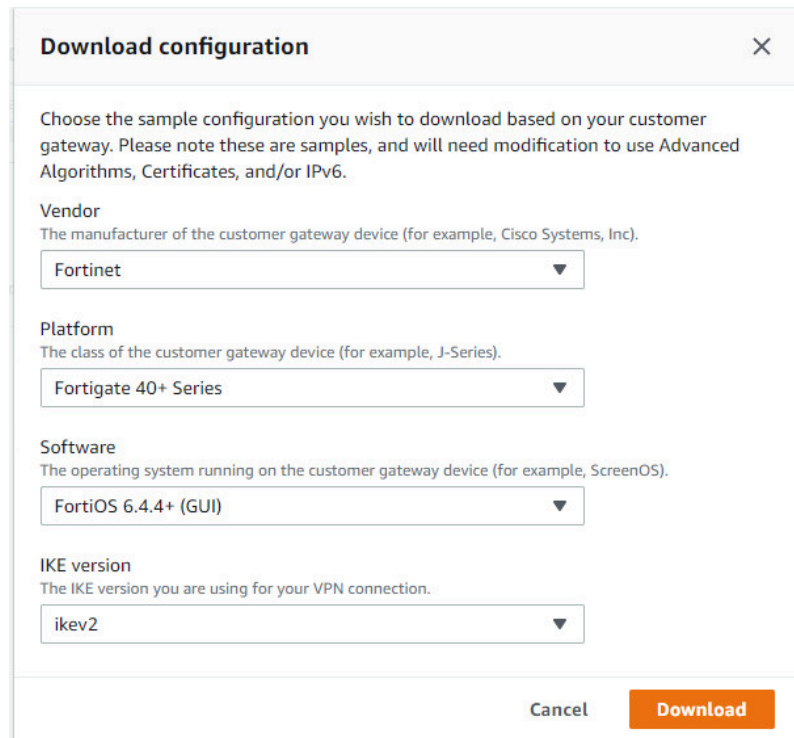


Figure 10.82: Download configuration

The screenshot shows the AWS IAM console interface for VPN connections. At the top, there are buttons for 'Actions', 'Download configuration', and 'Create VPN connection'. A search bar is present with the filter 'VPN ID: vpn-0a9b7e3a2ca3eebd2'. Below the search bar, a table lists the VPN connections. The connection 'VPNAWS' is highlighted, with a state of 'Pending' and a virtual private gateway of 'vgw-048d1dd1e6ba61f05'. Below the table, the 'Tunnel details' tab is selected, showing a table of tunnel states. Both Tunnel 1 and Tunnel 2 are listed with a status of 'Down' and a last status change of 'May 30, 2022, 9:07:13 (UTC-07:00)'. Tunnel 1 has an outside IP address of 3.225.102.90 and an inside IPv4 CIDR of 169.254.72.192/30. Tunnel 2 has an outside IP address of 54.83.91.6 and an inside IPv4 CIDR of 169.254.143.60/30.

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details
Tunnel 1	3.225.102.90	169.254.72.192/30	-	Down	May 30, 2022, 9:07:13 (UTC-07:00)	-
Tunnel 2	54.83.91.6	169.254.143.60/30	-	Down	May 30, 2022, 9:07:13 (UTC-07:00)	-

Figure 10.83: Verify public IP address

- Open the file that you have downloaded on AWS. It will show phase 1 and phase 2 configuration.

```

vpn-0a9b7e3a2ca3eebd2.txt - Notepad
File Edit Format View Help
! IPsec Tunnel #1
! -----
! #1: Internet Key Exchange (IKE) Configuration

Go to VPN --> IPSEC Tunnels --> Create New (drop down) --> Select IPSEC Tunnel

VPN Creation Wizard Window appears

Select Template Type as "Custom"

Provide a Name for the VPN connection (Name must be shorter than 15 chars, best if shorter than 12): vpn-0a9b7e3a2ca3ee

New VPN Tunnel Window Appears (Here we configure the VPN settings):

Under "Network" Section:
a. IP Version: IPv4
b. Remote Gateway: Static IP Address
c. IP address: 3.225.102.90
d. Local Interface: wan1
e. Local Gateway: Select Specify and enter WAN port IP (Public IP)
f. Dead Peer Detection: Enable by selecting On Idle/ On Demand
g. Authentication Method: Pre-shared Key
h. Pre-Shared Key: rt11zQj5aWoSdpACxy_HBYGBX62c4fIS
i. IKE Version: 2
Phase 1 Proposal:
j. Encryption: aes128
k. Authentication: sha1
l. DH group: 2 ! and deselect 5
m. Keylife: 28800 seconds

```

Figure 10.84: IPsec Phase 1

```

vpn-0a9b7e3a2ca3eebd2.txt - Notepad
File Edit Format View Help
! #2: IPsec Configuration

Under Phase 2 Selectors --> New Phase 2
a. Name: vpn-0a9b7e3a2ca3eebd2-0
b. Local Address: LAN subnet behind Fortigate/0.0.0.0/0
c. Remote Address: AWS Private Subnet/0.0.0.0/0

Under Advanced
d. Encryption: aes128
e. Authentication: sha1
f. Select Enable Replay Detection
g. Select Perfect Forward Secrecy
h. DH Group: 2 ! and deselect 5
i. Keylife: 3600 seconds
j. Enable Auto-negotiate ! Autokey Keep Alive is enabled automatically when Auto-negotiate is enabled
k. Click Ok

```

Figure 10.85: IPsec Phase 2

FortiGate Configuration

1. First, we will configure port1 and port2 IP addresses. port1 should be set as DHCP client and port2 should be set as 192.168.10.1/24.

The screenshot shows the FortiGate configuration page for the 'port2' interface. The left sidebar contains a navigation menu with options like Dashboard, Network, Interfaces, DNS, Packet Capture, SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, and System. The main content area is titled 'Edit Interface' and shows the following configuration:

- Name: port2
- Alias: (empty)
- Type: Physical Interface
- VRF ID: 0
- Role: Undefined
- Addressing mode: Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask: 192.168.10.1/24
- Secondary IP address: (disabled)
- Administrative Access:
 - IPv4: HTTPS, FMG-Access, FTM, Speed Test
 - HTTP, SSH, RADIUS Accounting
 - PING, SNMP, Security Fabric Connection
- Receive LLDP: Use VDOM Setting, Enable, Disable
- Transmit LLDP: Use VDOM Setting, Enable, Disable

Figure 10.86: Set an IP address for port2

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 10				
port1	Physical Interface		142.232.198.157/255.255.255.0	HTTPS HTTP
port2	Physical Interface		192.168.10.1/255.255.255.0	
port3	Physical Interface		0.0.0.0/0.0.0.0	
port4	Physical Interface		0.0.0.0/0.0.0.0	

Figure 10.87: Port1 and Port2 IP addresses

2. Create a static route to port1 (WAN Port) as Figure 10.88.

New Static Route

Automatic gateway retrieval

Destination **Subnet** Internet Service
0.0.0.0/0.0.0.0

Gateway Address **Dynamic** Specify 142.232.198.254

Interface port1

Administrative Distance 10

Comments Write a comment... 0/255

Status Enabled Disabled

Advanced Options

OK Cancel

Figure 10.88: Create a static route

3. Create an IPsec Wizard as a custom as follows:
 - **Remote Gateway IP Address:** *Public_IP_Address_AWS_Virtual_Gateway*
 - **Nat Traversal:** Disable
 - **Pre-shared Key:** *The same as AWS key(psWvIznNXaD3e1bWB9mVrODkrYALmrBO)*
 - **Local Address:** 192.168.10.0/24
 - **Remote Address:** 10.0.0.0/16

- **Phase 1:** Encryption: AES128, Authentication: SHA-1, DH: 2, lifetime: 28800
- **Phase 2:** Encryption: AES128, Authentication: SHA-1, DH: 2, lifetime: 3600
- **IKE:** version 2

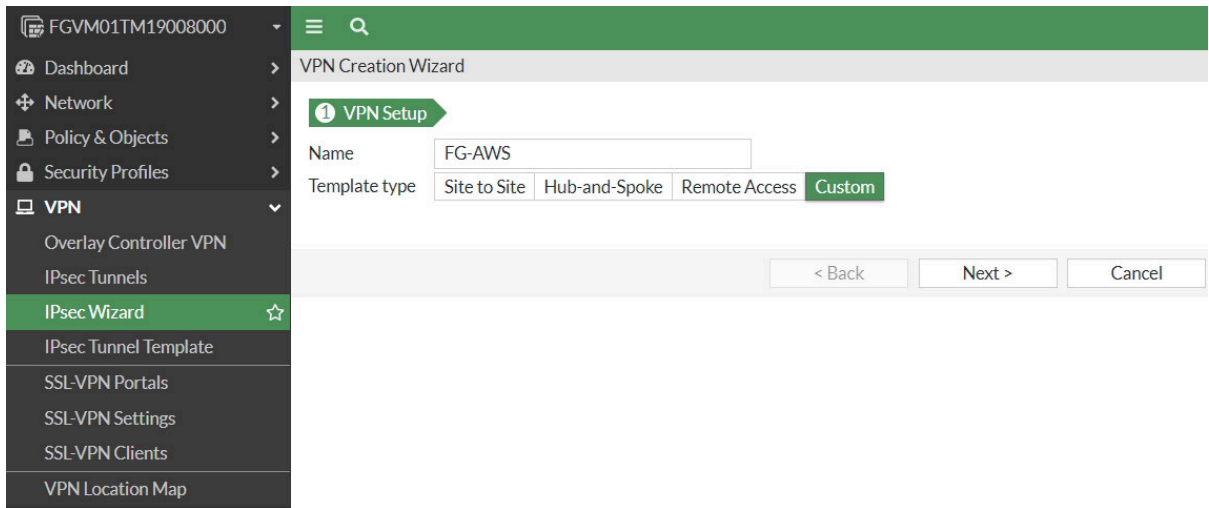


Figure 10.89: Create a custom VPN

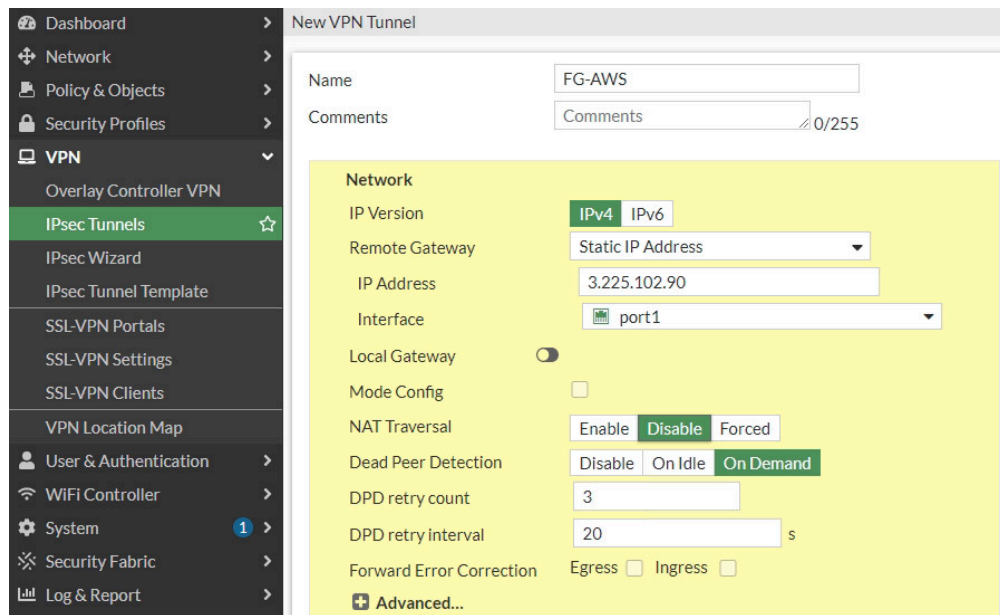


Figure 10.90: Create a custom VPN

Authentication

Method: Pre-shared Key

Pre-shared Key: [Redacted]

IKE

Version: 1 2

Phase 1 Proposal + Add

Encryption: AES128 Authentication: SHA1

Diffie-Hellman Group: 32 31 30 29 28 27
 21 20 19 18 17 16
 15 14 5 2 1

Key Lifetime (seconds): 28800

Local ID: [Empty]

Name	Local Address	Remote Address
FG-AWS	192.168.10.0/24	10.0.0.0/16

New Phase 2

Name: FG-AWS

Comments: [Empty]

Local Address: Subnet 192.168.10.0/24

Remote Address: Subnet 10.0.0.0/16

Figure 10.91: Create a custom VPN

New Phase 2

Name: FG-AWS

Comments: [Empty]

Local Address: Subnet 192.168.10.0/24

Remote Address: Subnet 10.0.0.0/16

Advanced...

Phase 2 Proposal + Add

Encryption: AES128 Authentication: SHA1

Enable Replay Detection

Enable Perfect Forward Security (PFS)

Diffie-Hellman Group: 32 31 30 29 28 27
 21 20 19 18 17 16
 15 14 5 2 1

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds

Seconds: 3600

OK Cancel

Figure 10.92: Create a custom VPN

- Set an IP address for FG-AWS tunnel. We will set the IP address based on the configuration file.

```

vpn-0a9b7e3a2ca3eebd2.txt - Notepad
File Edit Format View Help
! #3: Tunnel Interface Configuration

! A tunnel interface is configured to be the logical interface associated
! with the tunnel. All traffic routed to the tunnel interface will be
! encrypted and transmitted to the VPC. Similarly, traffic from the VPC
! will be logically received on this interface.
!
!
! The address of the interface is configured with the setup for your
! Customer Gateway. If the address changes, the Customer Gateway and VPN
! Connection must be recreated with Amazon VPC.
!
! This is required in order for tunnel failover via gwdetect to function
!
! Perform this from the Global VDOM.

Go to Network Tab --> Interface --> wan1 and edit vpn-0a9b7e3a2ca3eebd2-0

a. IP : 169.254.72.194
b. Remote IP: 169.254.72.193/30
c. Select Ping
d. Administrative Status: Up
e. Select Ok.
    
```

Figure 10.93: Configuration file for setting an IP address for FG-AWS tunnel

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 11				
port1	Physical Interface		142.232.198.157/255.255.255.0	HTTPS HTTP
FG-AWS	Tunnel Interface		0.0.0.0/0.0.0.0	
port2	Physical Interface		192.168.10.1/255.255.255.0	
port3	Physical Interface		0.0.0.0/0.0.0.0	

Figure 10.94: Set an IP address for FG-AWS tunnel

Edit Interface

Name FG-AWS

Alias

Type Tunnel Interface

Interface port1

VRF ID 0

Role Undefined

Address

Addressing mode Manual

IP

Remote IP/Netmask

Administrative Access

IPv4

<input type="checkbox"/> HTTPS	<input type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
<input type="checkbox"/> FMG-Access	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP
<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection
<input type="checkbox"/> Speed Test		

DHCP Server

Network

Security mode

Figure 10.95: Set an IP address for FG-AWS tunnel

5. Create a static route from FG-LAN to AWS-LAN. We will set a static route based on the configuration file.

*vpn-0a9b7e3a2ca3eebd2.txt - Notepad

File Edit Format View Help

! #4 Static Route Configuration

Your Customer Gateway needs to set a static route for the prefix corresponding to your VPC to send traffic over the tunnel interface.

! An example for a VPC with the prefix 10.0.0.0/16 is provided below:

!

! This is configured from the root VDOM

Go to Network Tab --> Static Routes --> Create New

a. Destination: Subnet (10.0.0.0/16)

b. Interface: vpn-0a9b7e3a2ca3eebd2-0 ! This is the VPN tunnel interface

c. Click Ok

Figure 10.96: Configuration file for creating a static route from FG-LAN to AWS-LAN

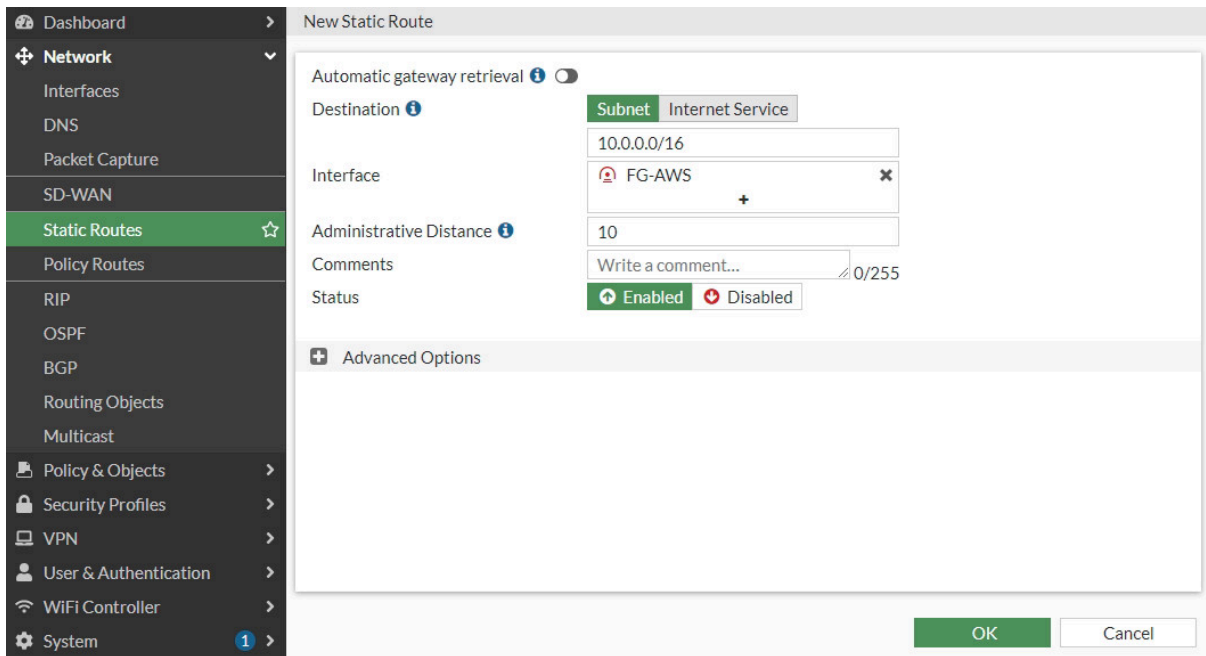


Figure 10.97: Create a static route from FG-LAN to AWS-LAN

Destination	Gateway IP	Interface	Status
0.0.0.0/0	142.232.198.254	port1	Enabled
10.0.0.0/16	3.225.102.90	FG-AWS	Enabled

Figure 10.98: Create a static route from FG-LAN to AWS-LAN

6. Create a firewall policy from Port2 to Tunnel and from Tunnel to Port2. We will create a subnet for LAN on premise and a subnet for AWS. Also, in site-to-site VPN, NAT should be disabled here.

New Address

Name:

Color:

Type:

IP/Netmask:

Interface:

Static route configuration:

Comments: 0/255

Figure 10.99: Create a subnet for local network

New Address

Name:

Color: Change

Type:

IP/Netmask:

Interface:

Static route configuration:

Comments: 0/255

Figure 10.100: Create a subnet for AWS local network

- Dashboard >
- Network >
- Policy & Objects >
- Firewall Policy ☆
- IPv4 DoS Policy
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options
- Traffic Shaping
- Security Profiles >
- VPN >
- User & Authentication >
- WiFi Controller >
- System 1 >
- Security Fabric >
- Log & Report >

New Policy

Name:

Incoming Interface:

Outgoing Interface:

Source: +

Destination: +

Schedule:

Service: +

Action: ACCEPT DENY

Inspection Mode: Flow-based Proxy-based

Firewall / Network Options

NAT:

Protocol Options:

Security Profiles

AntiVirus:

Web Filter:

DNS Filter:

Application Control:

IPS:

OK
Cancel

Figure 10.101: Create a policy from port2 to FG-AWS Tunnel

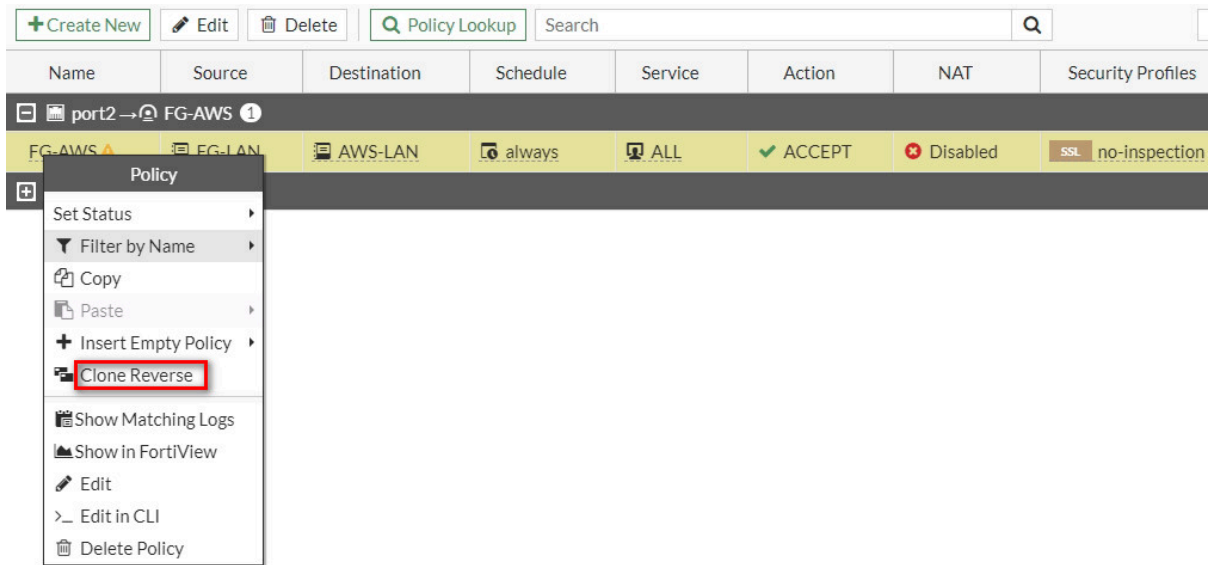


Figure 10.102: Create a policy from FG-AWS Tunnel to port2

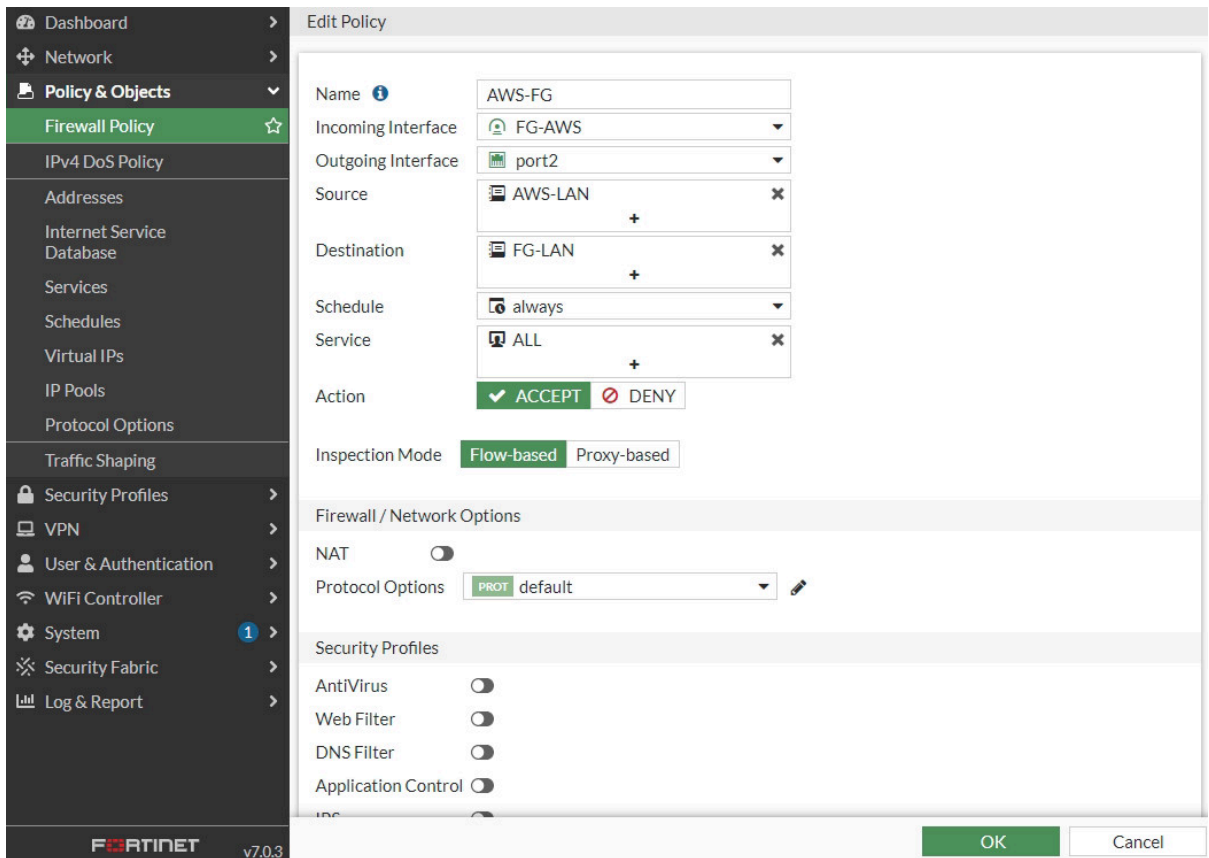


Figure 10.103: Create a policy from AWS-FG Tunnel to port2

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
FG-AWS → port2	AWS-FG	AWS-LAN	FG-LAN	always	ALL	ACCEPT	Disabled, SSL, no-inspection
port2 → FG-AWS	FG-AWS	FG-LAN	AWS-LAN	always	ALL	ACCEPT	Disabled, SSL, no-inspection
Implicit							

Figure 10.104: Firewall Policies Overview

Verify Connections

If you navigate to IPsec Tunnel, the status should be up.

Tunnel	Interface Binding	Status
Custom		
FG-AWS	port1	Up

Figure 10.105: Verify tunnel status in FortiGate (on premise)

VPN connections (1/1) Info

Filter VPN connections

VPN ID: vpn-0a9b7e3a2ca3eebd2

Name	VPN ID	State	Virtual private gateway	Transit gateway
VPNAWS	vpn-0a9b7e3a2ca3eebd2	Available	vgw-048d1dd1e6ba61f05	-

vpn-0a9b7e3a2ca3eebd2 / VPNAWS

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details
Tunnel 1	3.225.102.90	169.254.72.192/30	-	Up	May 30, 2022, 9:29:44 (UTC-07:00)	-
Tunnel 2	54.83.91.6	169.254.143.60/30	-	Down	May 30, 2022, 9:16:00 (UTC-07:00)	-

Figure 10.106: Verify tunnel status in AWS

10.5 Deploy FortiGate in AWS

Learning Objectives

- Create a VPC, public and private subnet, internet gateway, route tables
- Create a FortiGate firewall in AWS through Marketplace
- Identify FortiGate subnets in AWS

Scenario: In this lab, we'll learn how to deploy FortiGate in AWS.

AWS Configuration

1. Create a VPC.

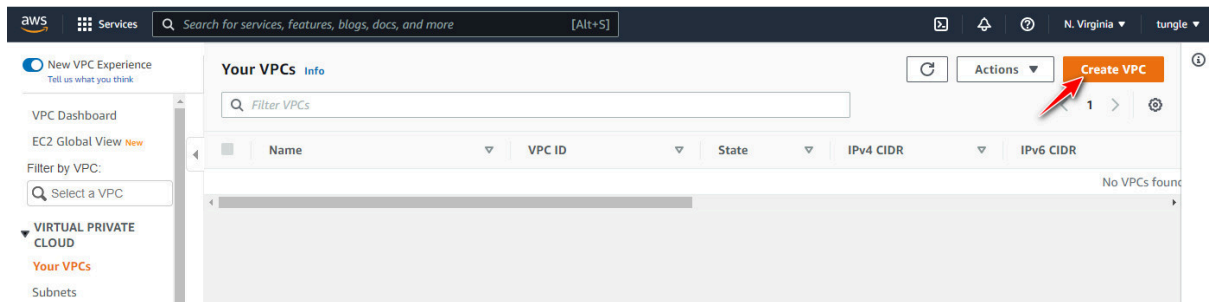


Figure 10.107: Create a VPC

Create VPC [Info](#)
A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or create VPC, subnets, etc.

VPC only VPC, subnets, etc.

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

AWS-VPC

IPv4 CIDR block [Info](#)
 IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16

IPv6 CIDR block [Info](#)
 No IPv6 CIDR block
 IPAM-allocated IPv6 CIDR block
 Amazon-provided IPv6 CIDR block
 IPv6 CIDR owned by me

Tenancy [Info](#)
Default

Figure 10.108: Create a VPC named “AWS-VPC”

2. Create a subnet.

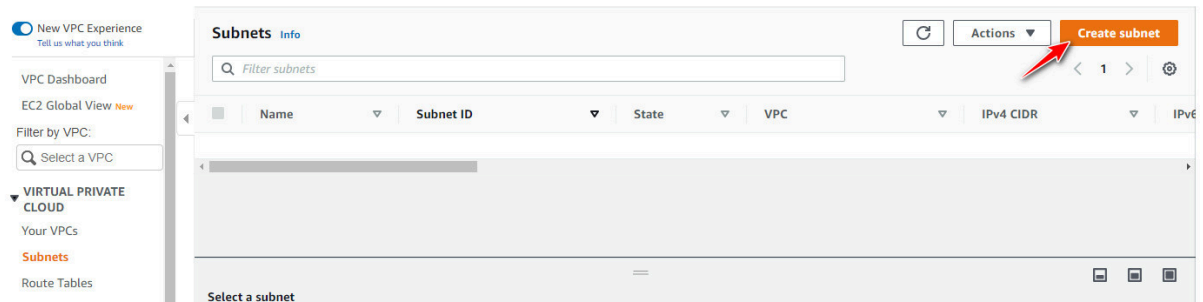


Figure 10.109: Create a subnet

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-060a1e2007366fbf4 (AWS-VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

Public Subnet

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference ▼

IPv4 CIDR block [Info](#)

Q 10.0.0.0/24 X

Figure 10.110: Create a public subnet under AWS-VPC

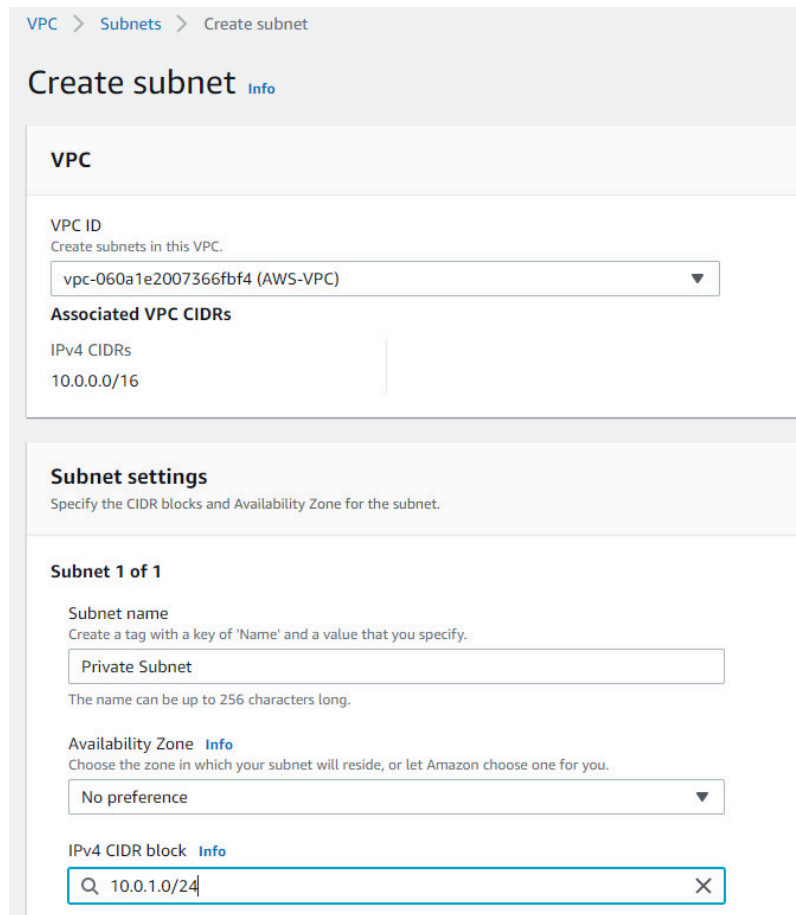


Figure 10.111: Create a private subnet under AWS-VPC

3. Create an internet gateway.

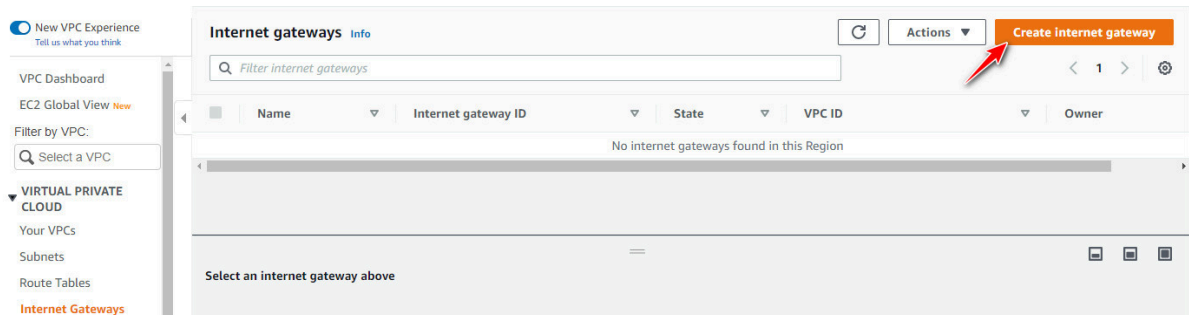


Figure 10.112: Create an internet gateway

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: X

Value - optional: X

You can add 49 more tags.

Figure 10.113: Create an internet gateway

Internet gateways (1/1) Info

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input checked="" type="checkbox"/>	AWS-IGW	igw-0b81c8d93b9e4ea9f	Detached	-

igw-0b81c8d93b9e4ea9f / AWS-IGW

Figure 10.114: Attach an internet gateway to VPC

VPC > Internet gateways > Attach to VPC (igw-0b81c8d93b9e4ea9f)

Attach to VPC (igw-0b81c8d93b9e4ea9f) Info

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

 X

Figure 10.115: Attach an internet gateway to VPC

4. Create a new Public RouteBy default, name of the “built-in route” is “-”. Rename it to Private Route.

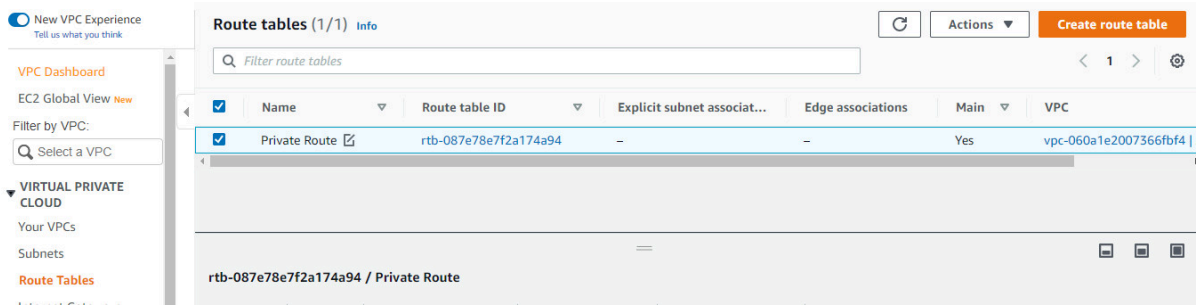


Figure 10.116: Edit private route

Go to **Route tables > create route table.**

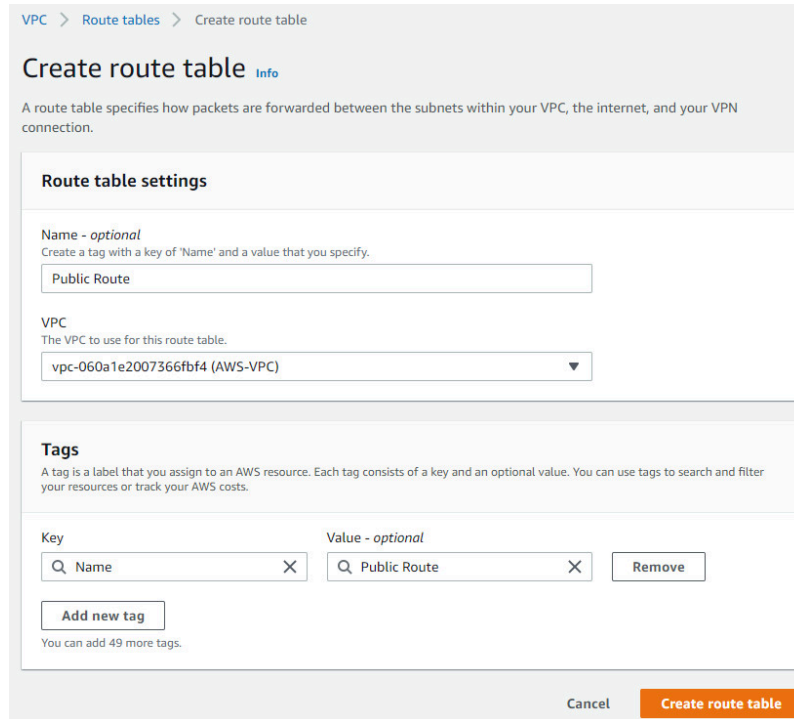


Figure 10.117: Create a public route

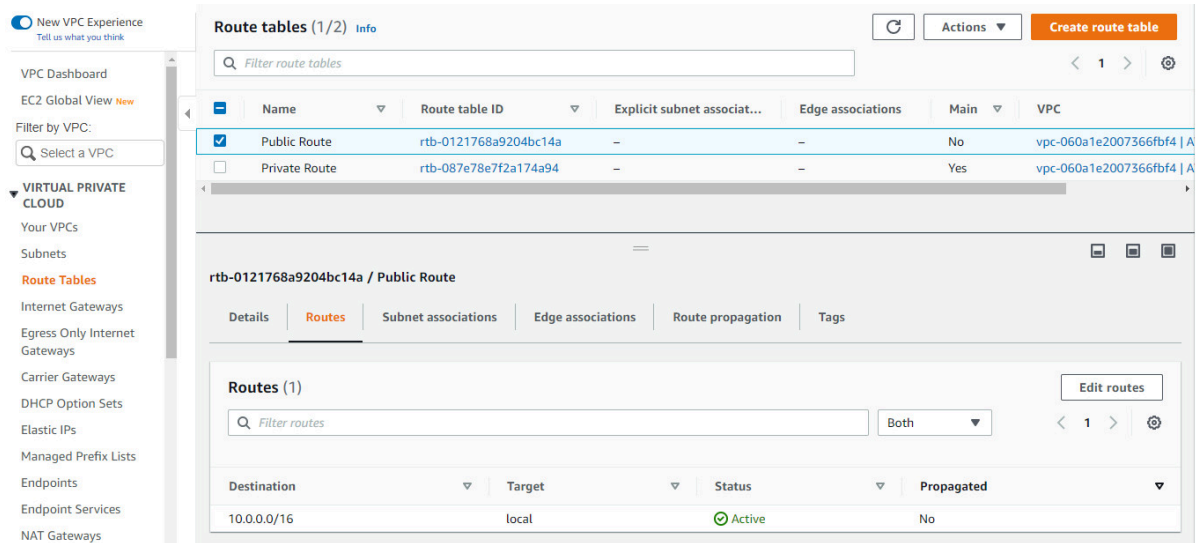


Figure 10.118: Edit routes on Public Route

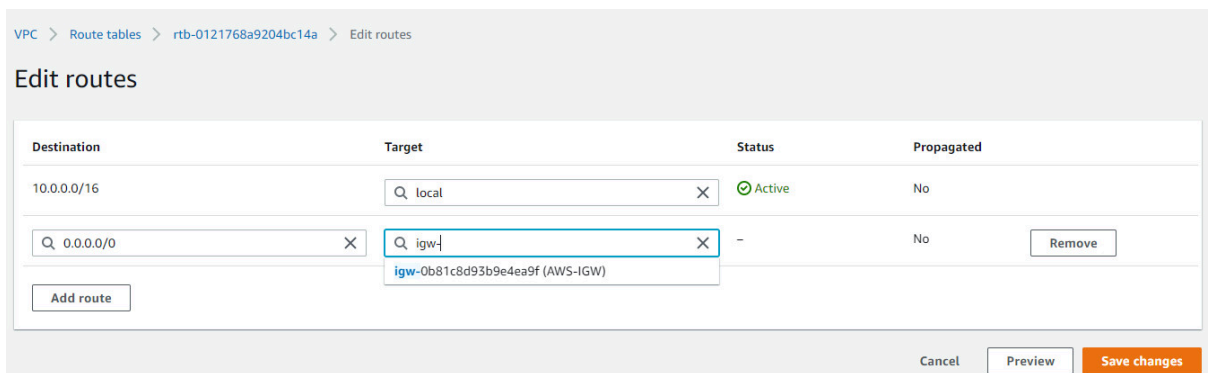


Figure 10.119: Create a new default route to the internet gateway

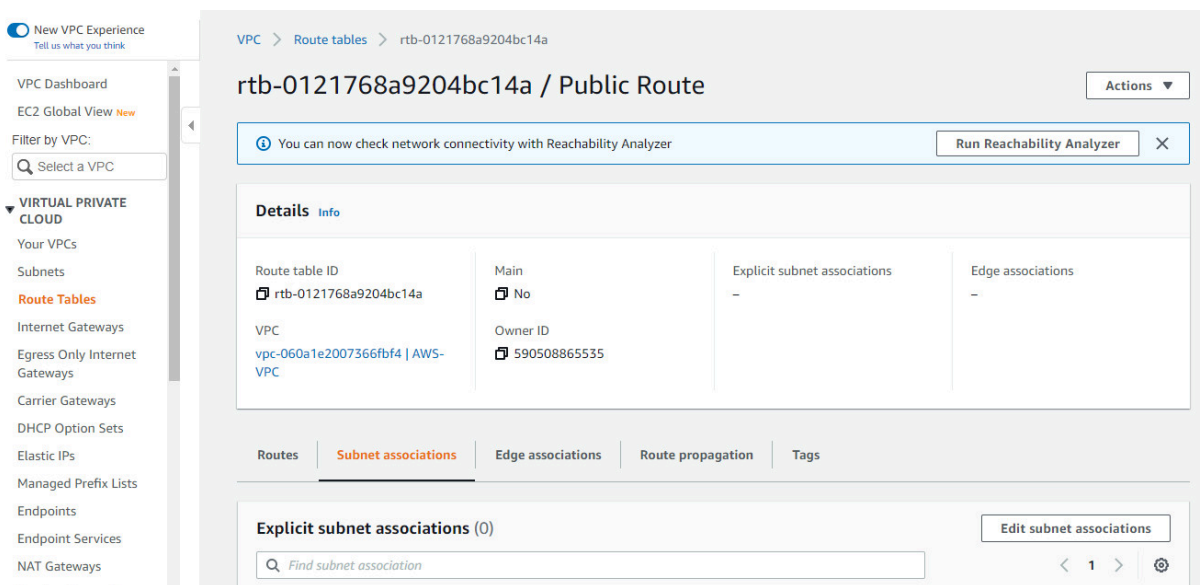


Figure 10.120: Associate Public Subnet to Public Route

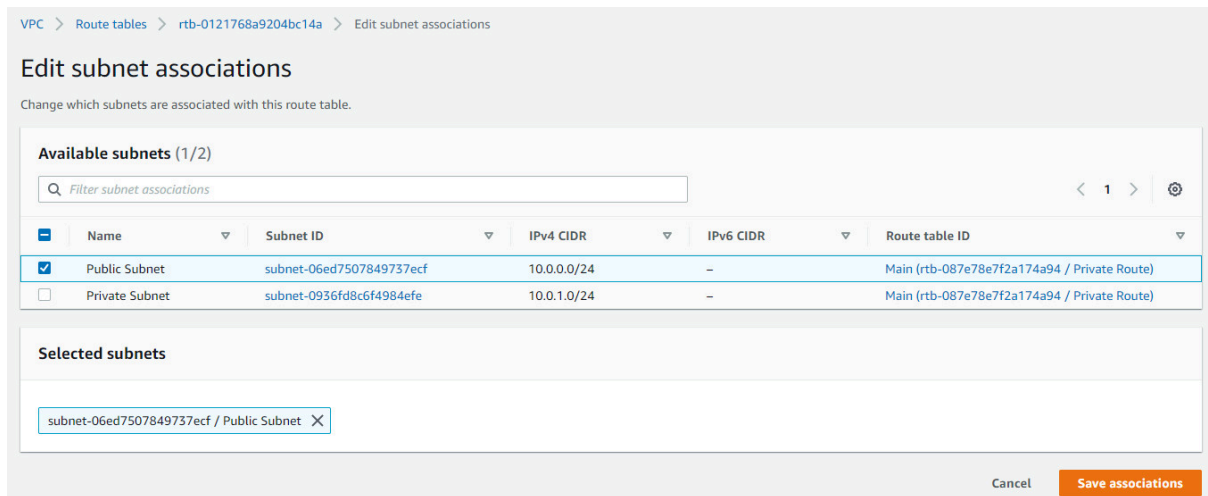


Figure 10.121: Associate Public Subnet to Public Route

5. Create Key Pair. Go to **EC2 – Key Pairs > Create Key Pair**.

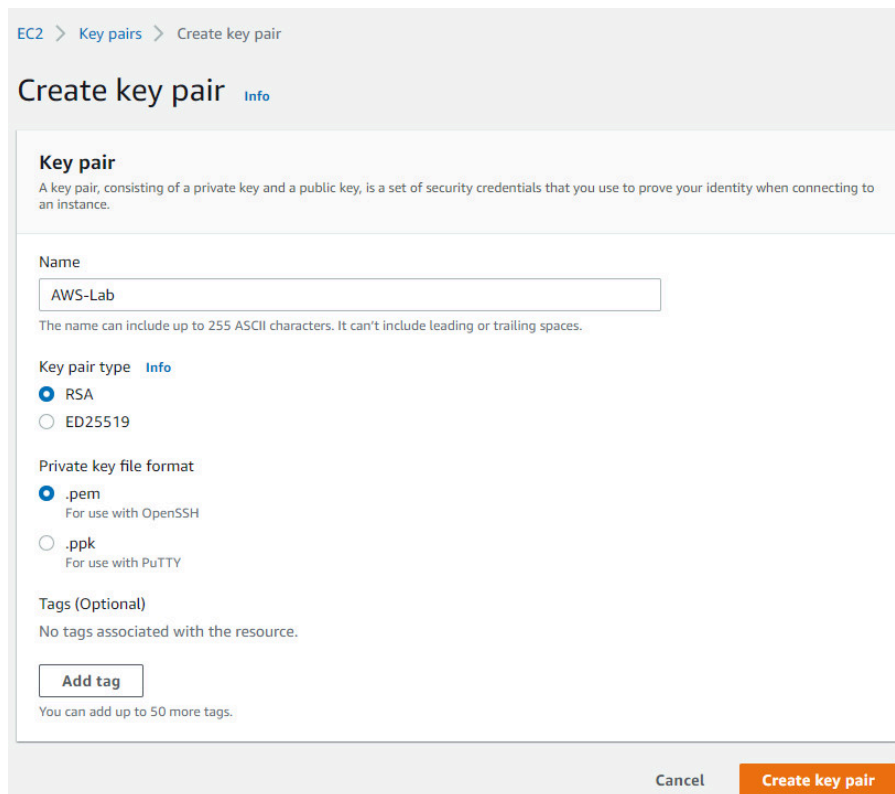


Figure 10.122: Create a key pair

6. Create Instances. Go to **EC2 – Instances > Launch instances**.

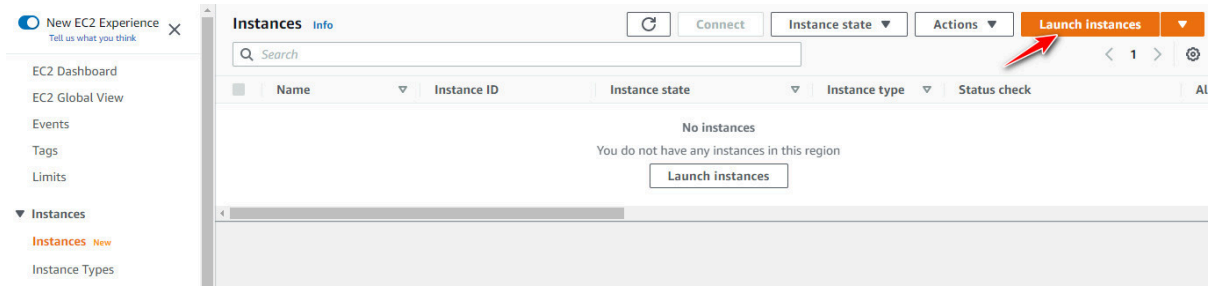


Figure 10.123: Launch a FortiGate instance

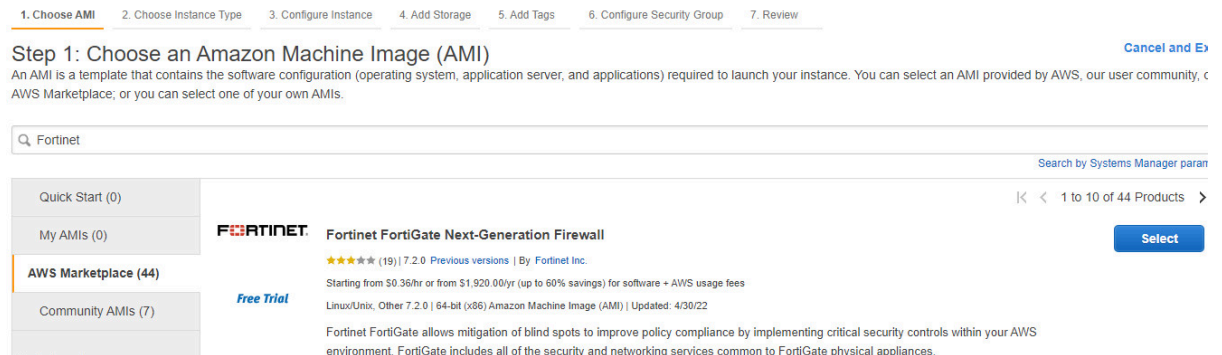


Figure 10.124: Select Fortinet FortiGate Next-Generation Firewall

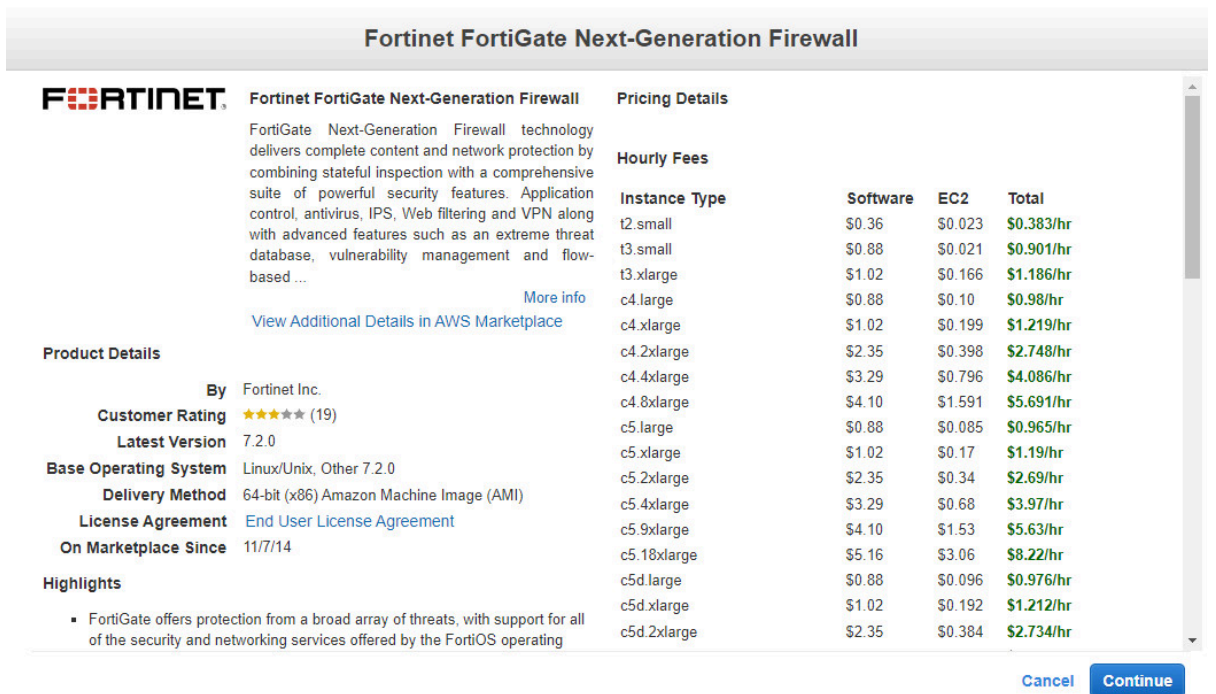


Figure 10.125: Accept FortiGate licence

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applic networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.small (- ECUs, 1 vCPUs, 2.5 GHz, -, 2 GiB memory, EBS only)

Note: The vendor recommends using a **c6i.xlarge** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)
🗑	t2	t2.nano	1	0.5	EBS only
🗑	t2	t2.micro Free tier eligible	1	1	EBS only
🗑	t2	t2.small	1	2	EBS only
🗑	t2	t2.medium	2	4	EBS only
🗑	t2	t2.large	2	8	EBS only

Figure 10.126: Select FortiGate instance type

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take and more.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option Request Spot instances

Network [Create new VPC](#)
No default VPC found. [Create a new default VPC](#).

Subnet [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP

Hostname type

DNS Hostname Enable IP name IPv4 (A record) DNS requests
 Enable resource-based IPv4 (A record) DNS requests
 Enable resource-based IPv6 (AAAA record) DNS requests

Figure 10.127: Select Network is “AWS-VPC”, Subnet is “Public Subnet” and Auto-assign Public IP is “Enable”

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⁱ	Device ⁱ	Snapshot ⁱ	Size (GiB) ⁱ	Volume Type ⁱ	IOPS ⁱ	Throughput (MB/s) ⁱ
Root	/dev/sda1	snap-0ba9f2da5ecf96965	2	General Purpose SSD (gp2)	100 / 3000	N/A
EBS	/dev/sdb	Search (case-insensit)	30	General Purpose SSD (gp2)	100 / 3000	N/A

Add New Volume

Figure 10.128: Leave the Add storage as the default

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key ⁱ (128 characters maximum)	Value ⁱ (256 characters maximum)	Instances ⁱ
Name	FG	<input checked="" type="checkbox"/>

Figure 10.129: Assign Tag with Key is Name and Value is FG

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, to allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing security groups.

Assign a security group: Create a new security group

Select an existing security group

Security group name: FortiGate Security Group

Description: FortiGate Security Group

Type ⁱ	Protocol ⁱ	Port Range ⁱ	Source ⁱ
SSH	TCP	22	Custom 0.0.0.0/0
HTTP	TCP	80	Custom 0.0.0.0/0
HTTPS	TCP	443	Custom 0.0.0.0/0
Custom TCP F	TCP	541	Custom 0.0.0.0/0
Custom TCP F	TCP	3000	Custom 0.0.0.0/0
Custom TCP F	TCP	8080	Custom 0.0.0.0/0
RDP	TCP	3389	Custom 0.0.0.0/0
All ICMP - IPv	ICMP	0 - 65535	Custom 0.0.0.0/0

Add Rule

Figure 10.130: Change to FortiGate Security Group and add RDP and ICMP to the Security Group

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Select a key pair

I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Cancel
Launch Instances

Figure 10.131: Accept key pair and launch instances

The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with options like 'EC2 Dashboard', 'Instances', and 'Images'. The main content area displays the 'Instances (1/1)' page. A table lists one instance named 'FG' with ID 'i-0ff098db861c07b53', which is in a 'Running' state. Below the table, the 'Instance: i-0ff098db861c07b53 (FG)' details are shown, including a summary of its configuration and network settings.

Name	Instance ID	Instance state	Instance type	Status check
FG	i-0ff098db861c07b53	Running	t2.small	Initializing

Instance: i-0ff098db861c07b53 (FG)		
Details	Security	Networking
Instance summary		
Instance ID i-0ff098db861c07b53 (FG)	Public IPv4 address 3.239.117.237 open address	Private IPv4 addresses 10.0.0.22
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-10-0-0-22.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-0-22.ec2.internal	Answer private resource DNS name IPv4 (A)

Figure 10.132: FG instance has been launched successfully

The screenshot shows the AWS Management Console interface for a network interface. The left sidebar contains navigation options like 'Reserved Instances', 'Images', 'Elastic Block Store', and 'Network & Security'. The main content area is titled 'Network interfaces (1/1) Info' and shows a table with one entry: 'FG Public Subnet' with ID 'eni-03b2e198495d21f54'. Below the table, the details for this interface are shown, including its status as 'In-use', VPC ID, Subnet ID, and associated security groups.

Name	Network interface ID	Subnet ID	VPC ID	Availability Zone
FG Public Subnet	eni-03b2e198495d21f54	subnet-06ed7507849737ecf	vpc-060a1e2007366fbf4	us-east-1f

Network interface: eni-03b2e198495d21f54 (FG Public Subnet)

Network interface details

Network interface ID	Name	Description
eni-03b2e198495d21f54	FG Public Subnet	Primary network interface
Network interface status	Interface type	Security groups
In-use	Elastic network interface	sg-09578bdb48a98e906 (FortiGate Security Group)
VPC ID	Subnet ID	Availability Zone
vpc-060a1e2007366fbf4	subnet-06ed7507849737ecf	us-east-1f

Figure 10.133: Change default interface name to FG Public Subnet

7. Add a new private subnet interface.

The screenshot shows the 'Create network interface' page in the AWS Management Console. The page includes a description of an elastic network interface and a form for creating one. The 'Subnet' field is highlighted, showing a list of available subnets. The 'subnet-0936fd8c6f4984efe' (Private Subnet) is selected and highlighted with a red box.

Create network interface

An elastic network interface is a logical networking component in a VPC that represents a virtual network card.

Details Info

Description - optional
A descriptive name for the network interface.
FG Private Subnet

Subnet
The subnet in which to create the network interface.

select subnet

subnet-06ed7507849737ecf	us-east-1f
Public Subnet Owner: 590508865535	
subnet-0936fd8c6f4984efe	us-east-1f
Private Subnet Owner: 590508865535	

Custom

Elastic Fabric Adapter

Enable

► Advanced settings

Figure 10.134: Create FG Private Subnet

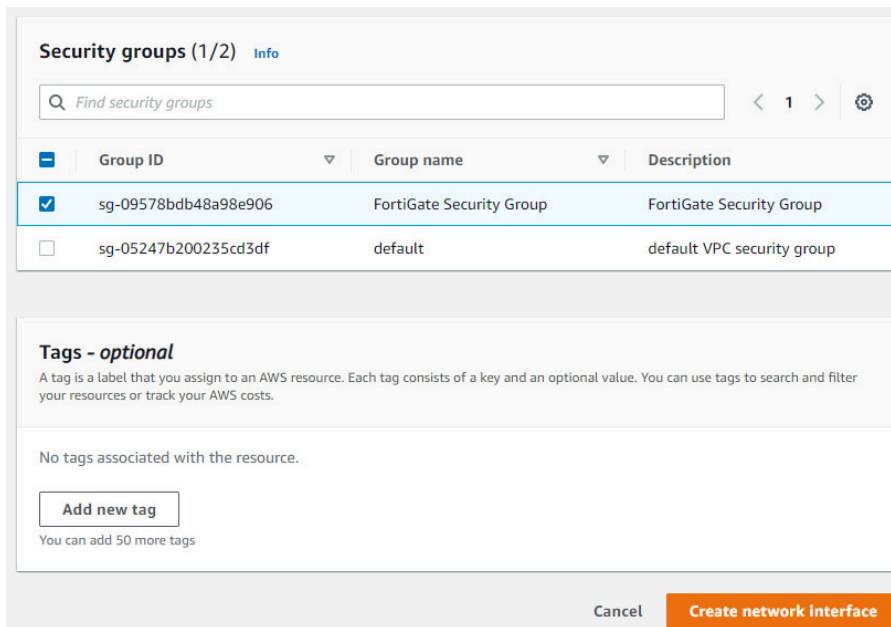


Figure 10.135: Create FG Private Subnet

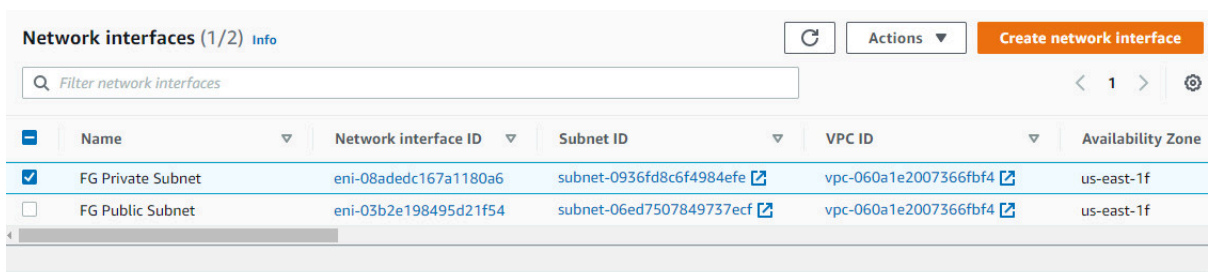


Figure 10.136: Change to FG Private Subnet

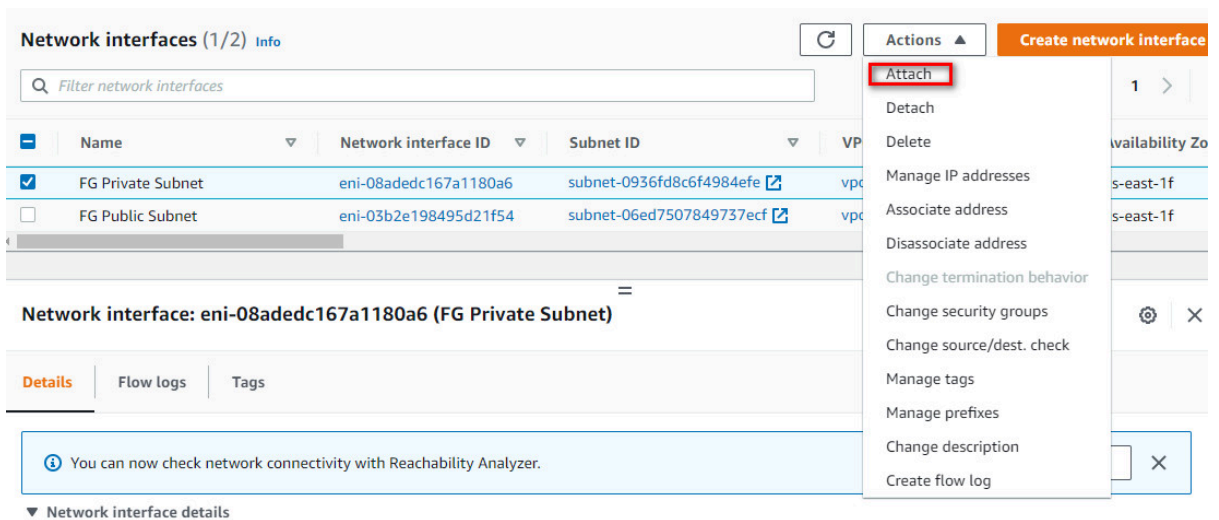


Figure 10.137: Attach the FG Private Subnet to FG

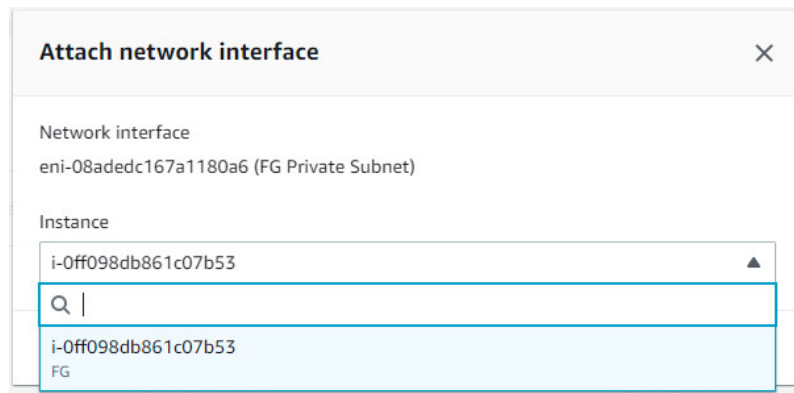


Figure 10.138: Attach the FG Private Subnet to FG

8. Disable Source and Destination check on both FG Private and Public Subnet.

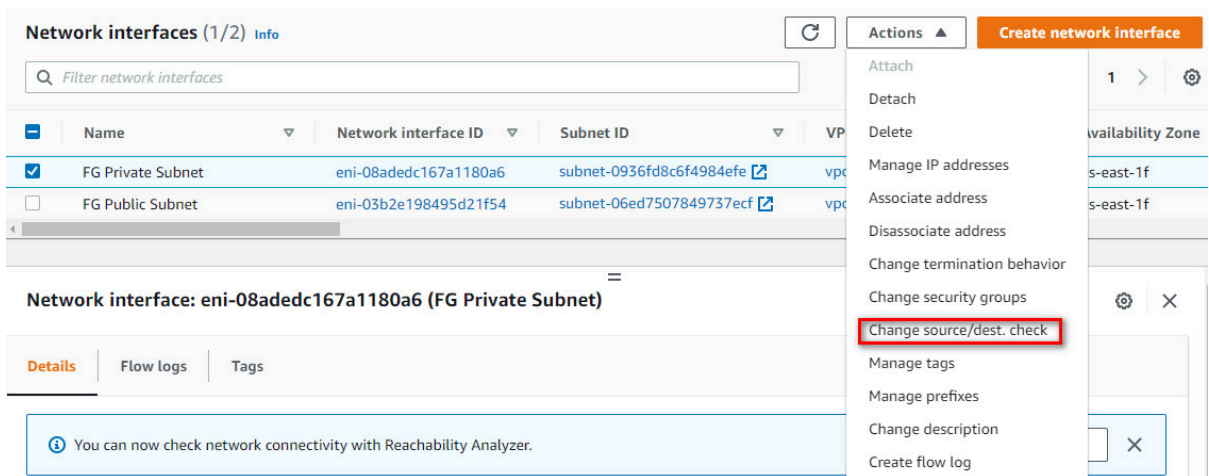


Figure 10.139: Disable source/destination check on FG Private Subnet

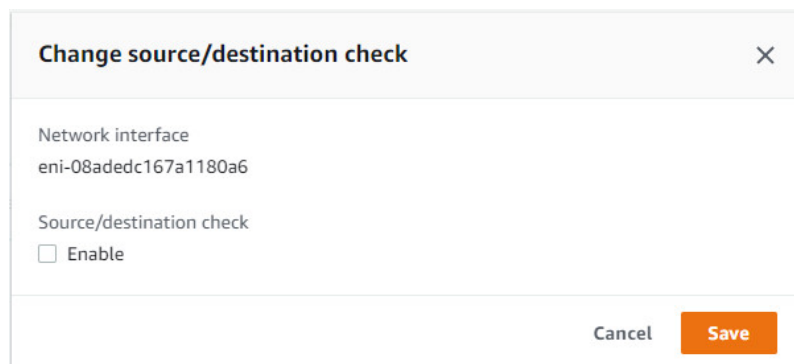


Figure 10.140: Disable source/destination check on FG Private Subnet

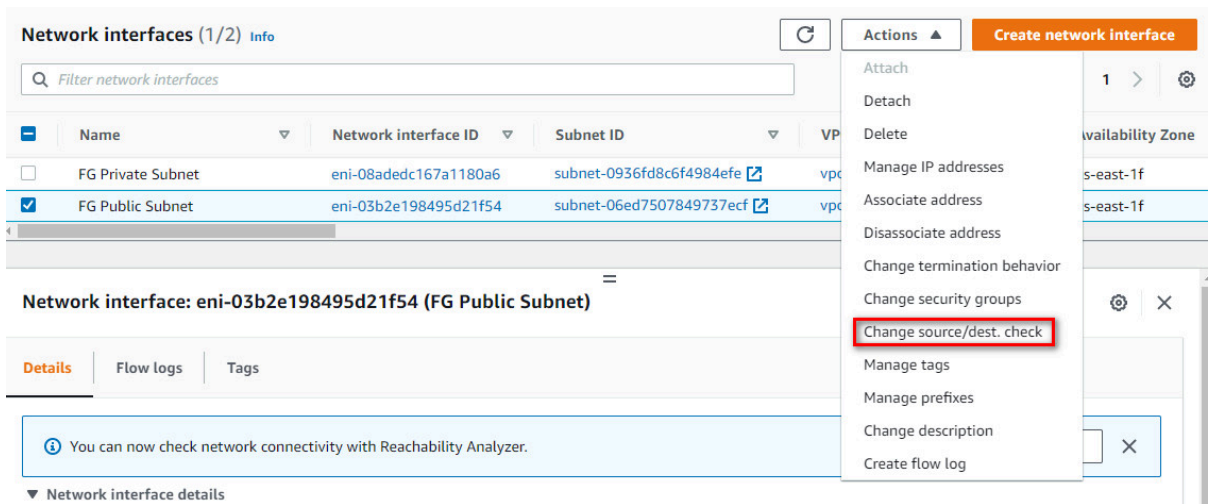


Figure 10.141: Disable source/destination check on FG Public Subnet

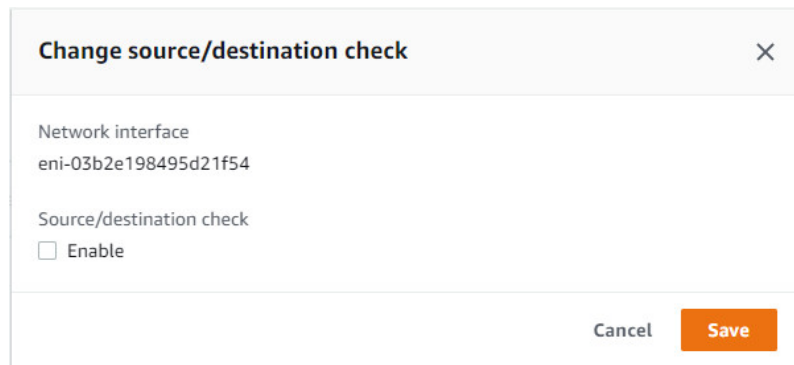


Figure 10.142: Disable source/destination check on FG Public Subnet

9. Edit private route table.

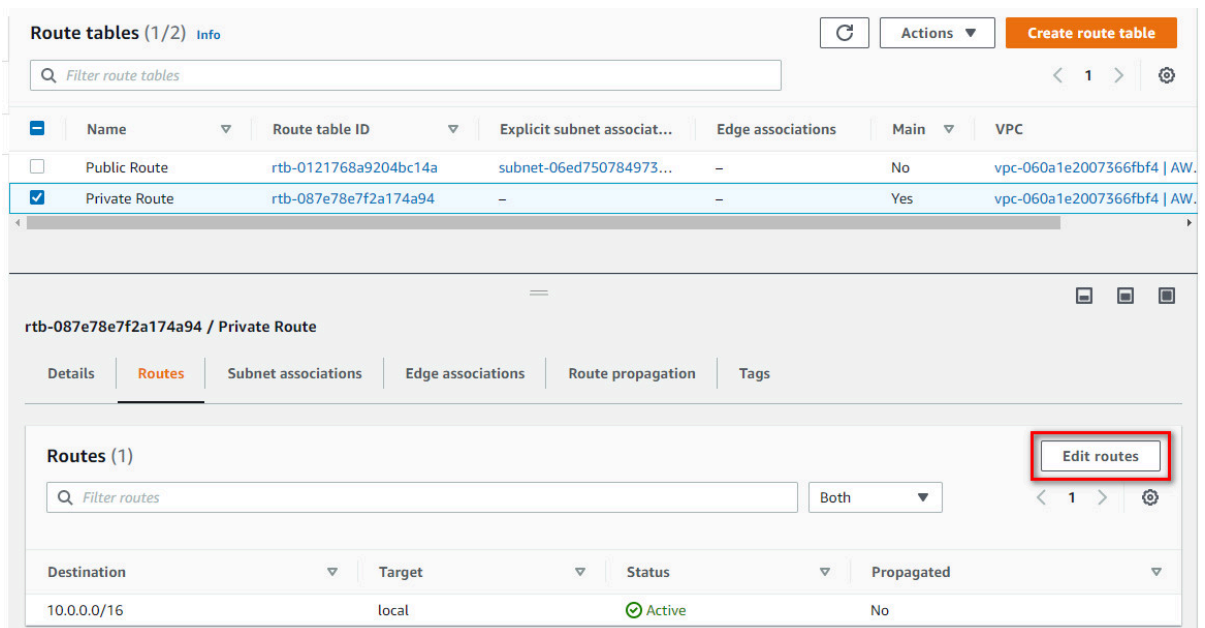


Figure 10.143: Edit Private Route

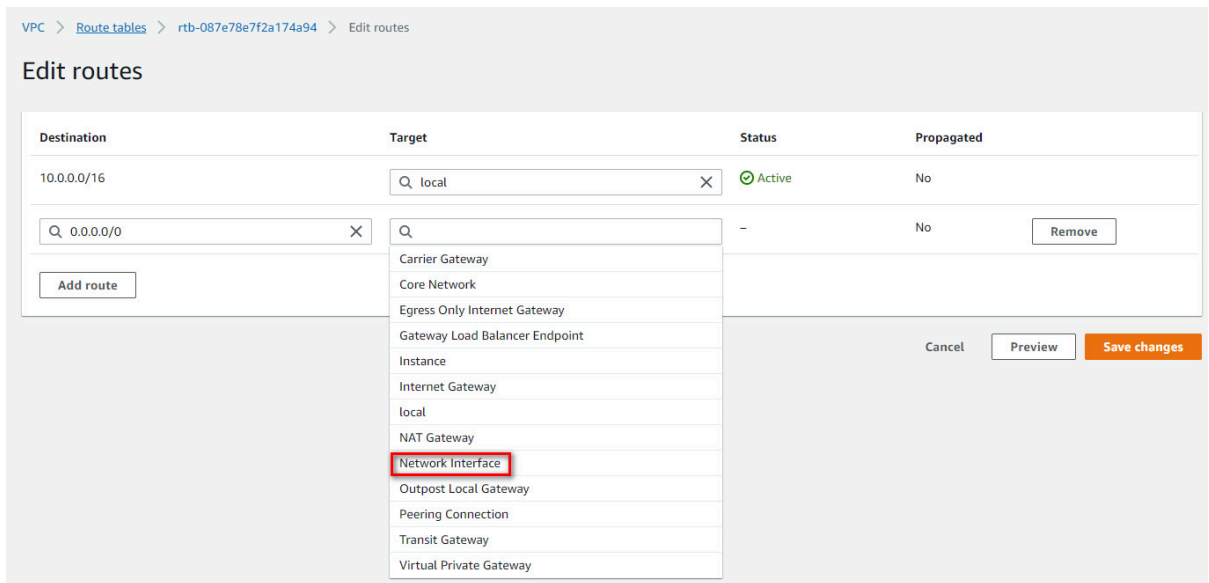


Figure 10.144: Add a default route and select Network Interface

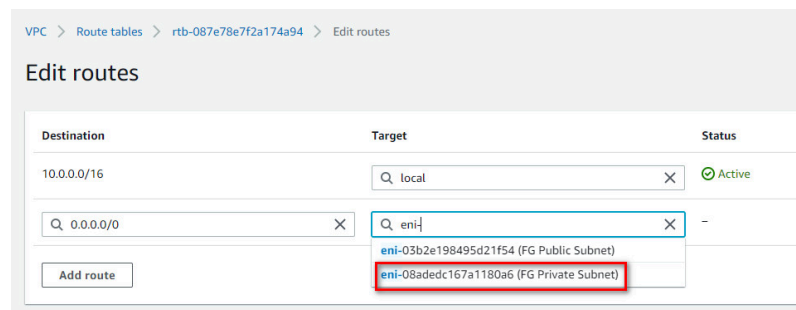


Figure 10.145: Add a default route to target FG Private Subnet

10. Verify Public and Private IP address of FG.

The screenshot displays the AWS Management Console interface for an EC2 instance. At the top, there's a header for 'Instances (1/1)' with a search bar and buttons for 'Connect', 'Instance state', 'Actions', and 'Launch instances'. Below this is a table listing the instance 'FG' with ID 'i-0ff098db861c07b53', state 'Running', and type 't2.small'. The status check shows '2/2 checks passed'. Below the table, the 'Instance: i-0ff098db861c07b53 (FG)' details are shown. The 'Instance summary' section includes: Instance ID (i-0ff098db861c07b53 (FG)), Public IPv4 address (3.239.117.237), Private IPv4 addresses (10.0.0.22, 10.0.1.147), Instance state (Running), Private IP DNS name (ip-10-0-0-22.ec2.internal), Instance type (t2.small), and Elastic IP addresses (none).

Figure 10.146: Verify public and private IP address of FG

11. Accessing FortiGate on AWS. Type the IP address in the browser. You should be able to see the FortiGate credentials page. Enter your username and password to login to the firewall.

The screenshot shows a browser security warning. The address bar indicates a 'Not secure' connection to 'https://3.239.117.237'. A red warning triangle is displayed above the text 'Your connection is not private'. Below this, a message states: 'Attackers might be trying to steal your information from 3.239.117.237 (for example, passwords, messages, or credit cards). Learn more'. The error code 'NET:ERR_CERT_AUTHORITY_INVALID' is visible. A lightbulb icon suggests getting Chrome's highest level of security by turning on enhanced protection. At the bottom, there are 'Advanced' and 'Back to safety' buttons.

Figure 10.147: Access FortiGate

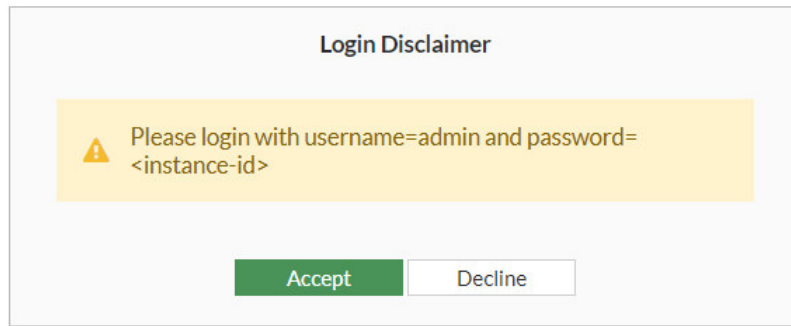


Figure 10.148: Access FortiGate

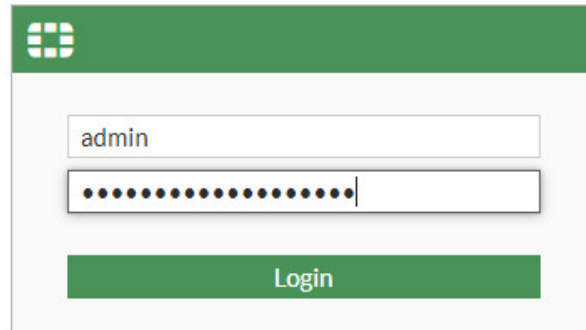


Figure 10.149: Username is admin and password is instance ID of FortiGate

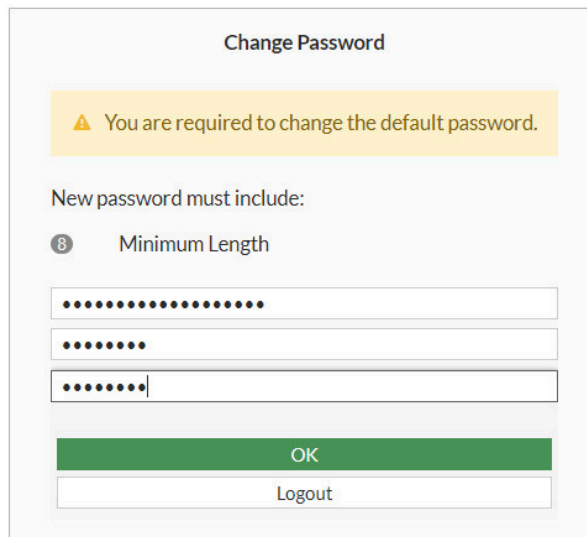


Figure 10.150: Change password

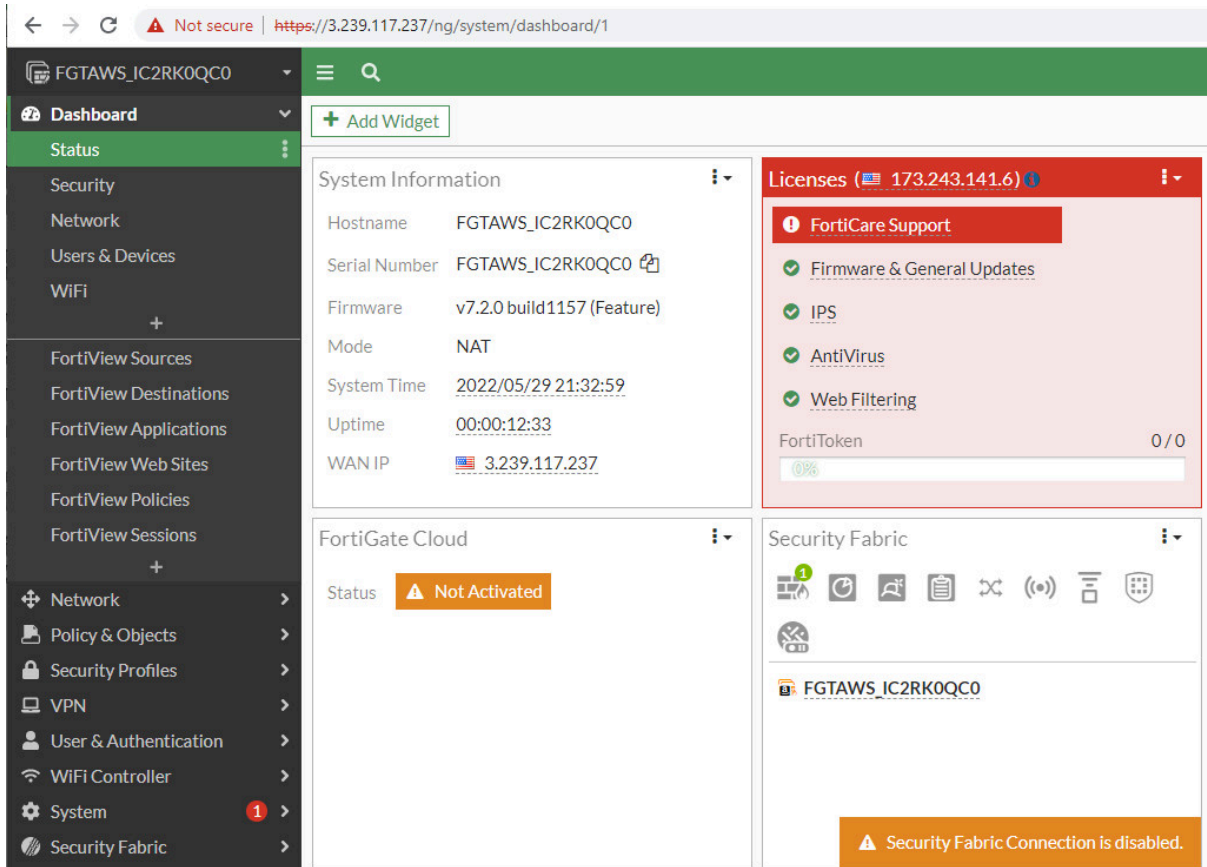


Figure 10.151: FortiGate dashboard

You should set port1 and port2 as DHCP client to receive an IP address from External and LAN subnet. Port1 is belong to External subnet or the internet and port2 is belong to the LAN.

Table 10.5: Port1 and Port2 description

Subnet	Description
Port1	External subnet used to connect the FortiGate-VM to the internet.
Port2	LAN subnet used to deploy services.

Edit Interface

Name:

Alias:

Type: Physical Interface

VRF ID:

Role:

Dedicated Management Port

Address

Addressing mode: Manual DHCP Auto-managed by IPAM One-Arm Sniffer

Retrieve default gateway from server:

Distance:

Override internal DNS:

Administrative Access

IPv4: HTTPS HTTP PING
 FMG-Access SSH SNMP
 FTM RADIUS Accounting Security Fabric Connection
 Speed Test

Receive LLDP: Use VDOM Setting Enable Disable

Figure 10.152: Change port2 to DHCP Client

FortiGate VM64-AWS

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 2				
port1	Physical Interface		10.0.0.22/255.255.255.0	PING HTTPS SSH HTTP FMG-Access
port2	Physical Interface		10.0.1.147/255.255.255.0	
Tunnel Interface 1				
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0	

Figure 10.153: FortiGate interfaces

10.6 Site-to-Site VPN between FortiGate on Premise and FortiGate in the AWS

Learning Objectives

- Configure a VPN Wizard in AWS
- Configure site-to-site VPN between FortiGate on premise and AWS
- Identify FortiGate subnets in AWS

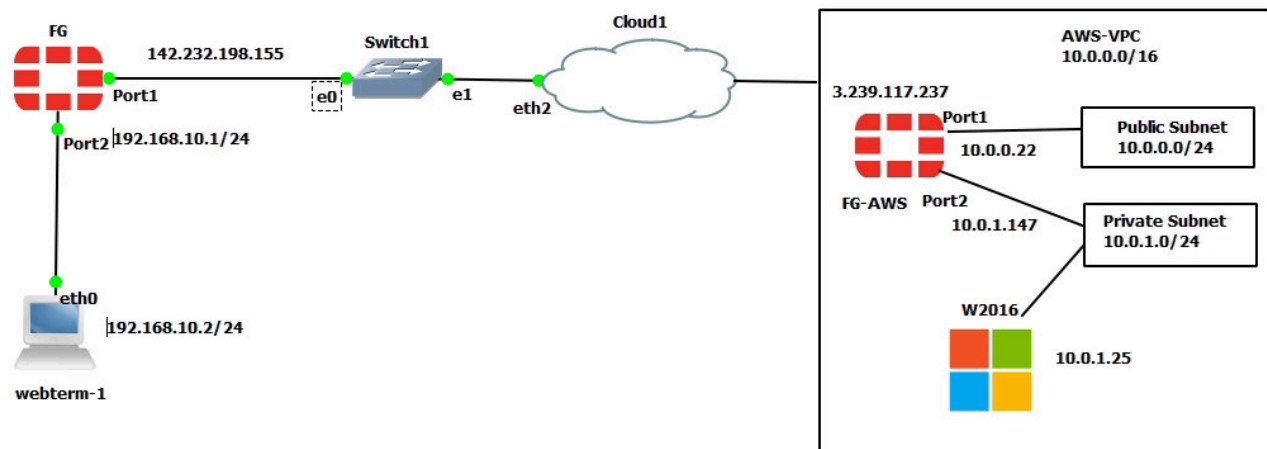


Figure 10.154: Main scenario

Scenario: In this lab, we are going to create a site-to-site VPN from FortiGate on premise to FortiGate in the AWS. Knowing the configuration of section 10.5 is necessary for this lab. Port1 FortiGate on premise is set as a DHCP, so it will receive an IP address from Cloud.

On-Premise FortiGate Configuration

Table 10.6: Devices configuration

Device	Interface	IP address
FortiGate	Port 1	DHCP Client
Port 2	192.168.10.1/24	–
WebTerm	Eth0	192.168.10.2/24

1. Configure the interfaces of the firewall. Port2 by default is an internal interface and named “LAN” and Port1 is an external interface and named “WAN”.

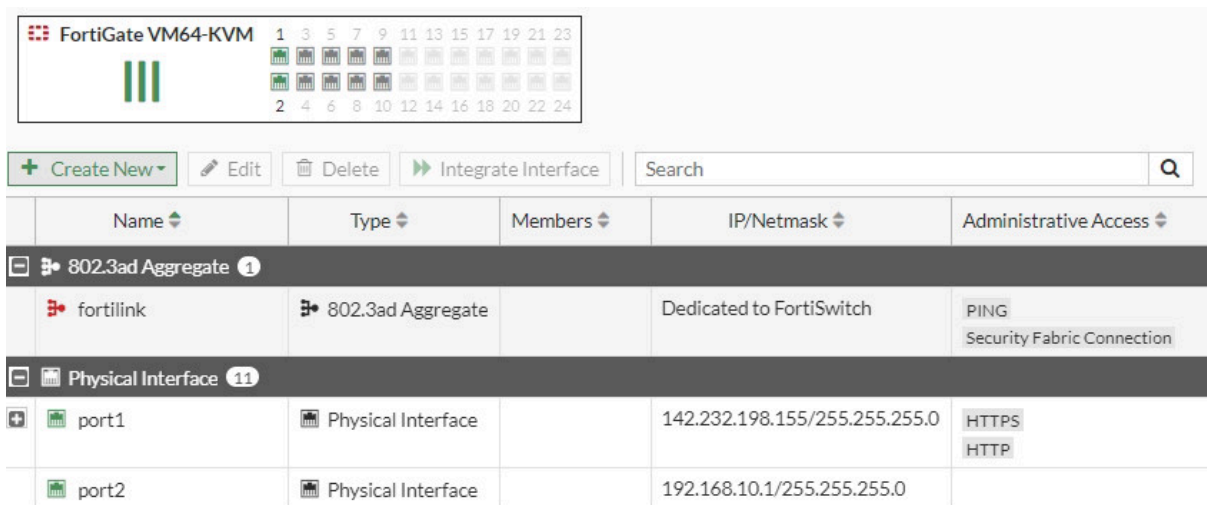


Figure 10.155: Firewall interfaces

2. Create a site-to-site VPN from IPsec Wizard as Figures 10.156 to 10.158.

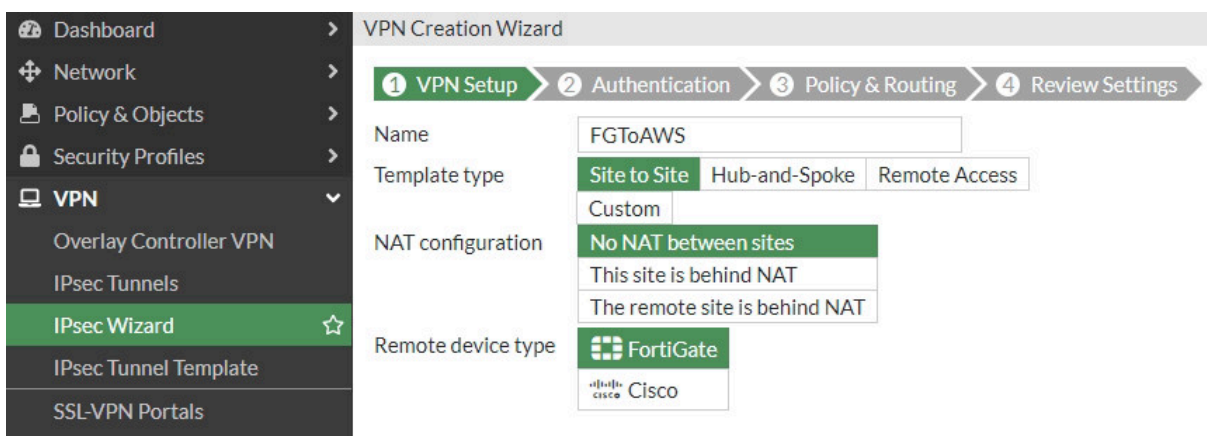


Figure 10.156: Select VPN name

VPN Creation Wizard

VPN Setup 2 Authentication 3 Policy & Routing 4 Review Settings

Remote device: IP Address Dynamic DNS

Remote IP address: 3.239.117.237

Outgoing Interface: port1

Authentication method: Pre-shared Key Signature

Pre-shared key: Pa\$\$w0rd

Figure 10.157: Set remote IP address

VPN Setup Authentication 3 Policy & Routing 4 Review Settings

Local interface: port2

Local subnets: 192.168.10.0/24

Remote Subnets: 10.0.0.0/16

Internet Access: None Share Local Use Remote

Figure 10.158: Set Policy & Routing

3. Create a static route to the default gateway.

Network

Static Routes

Automatic gateway retrieval:

Destination: Subnet Internet Service

0.0.0.0/0.0.0.0

Gateway Address: Dynamic Specify

142.232.198.254

Interface: port1

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled Disabled

Figure 10.159: Set a default gateway

AWS Configuration

1. Create a FortiGate firewall in AWS and configure the interfaces. You need to do all steps in section 10.5.
2. Create a VPN from IPsec Wizard as Figures 10.160 to 10.162.

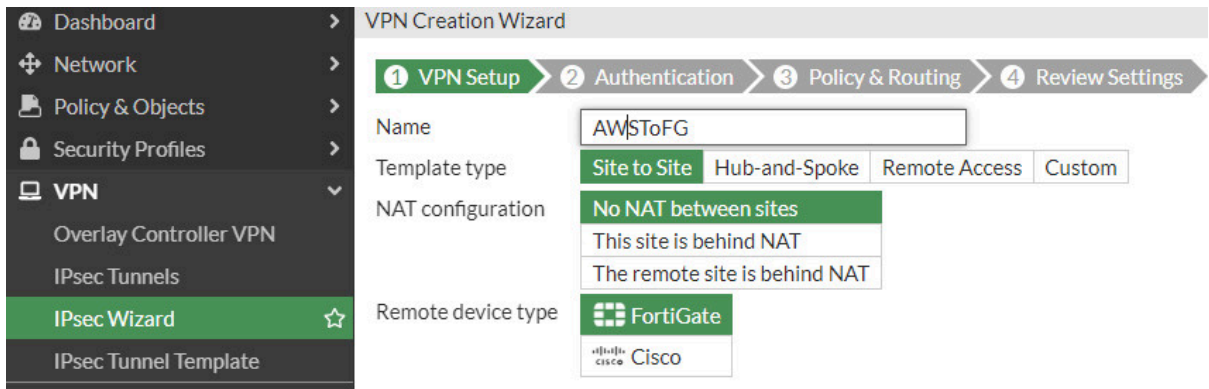


Figure 10.160: Select VPN name

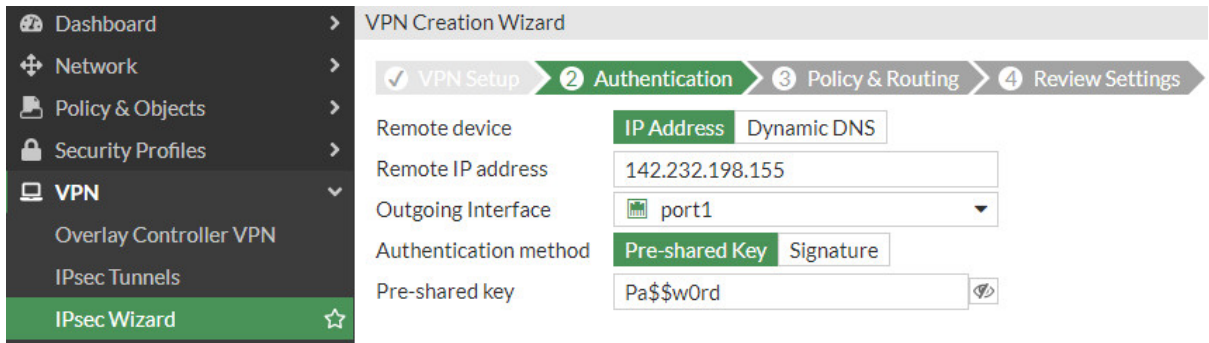


Figure 10.161: Set a remote IP address

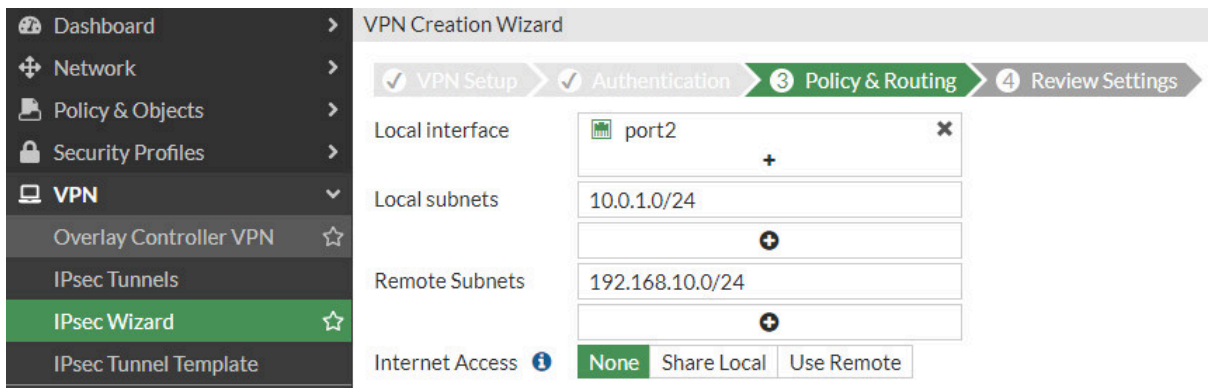


Figure 10.162: Set Policy & Routing

3. Create static routes on FortiGate. We are going to create two static routes as follows:

New Static Route

Automatic gateway retrieval ⓘ

Destination ⓘ Subnet Internet Service
 0.0.0.0/0.0.0.0

Gateway Address ⓘ Dynamic Specify
 10.0.0.1

Interface ⓘ
 port1 + ×

Administrative Distance ⓘ
 10

Comments
 Write a comment... /0/255

Status ⬆️ Enabled ⬆️ Disabled

+ Advanced Options

Figure 10.163: Set a default gateway via 10.0.0.1

New Static Route

Automatic gateway retrieval ⓘ

Destination ⓘ Subnet Internet Service
 10.0.0.0/16

Gateway Address ⓘ Dynamic Specify
 10.0.1.1

Interface ⓘ
 port2 + ×

Administrative Distance ⓘ
 10

Comments
 Write a comment... /0/255

Status ⬆️ Enabled ⬆️ Disabled

+ Advanced Options

Figure 10.164: Create a static route to 10.0.0.0/16 network via 10.0.1.1

Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.0.0.1	port1	Enabled
10.0.0.0/16	10.0.1.1	port2	Enabled
AWSToFG_remote	142.232.198.155	AWSToFG	Enabled
AWSToFG_remote		Blackhole	Enabled

Figure 10.165: Overview of static routes on FortiGate

- Go to **VPN > IPsec Tunnels** and check status of the tunnel.

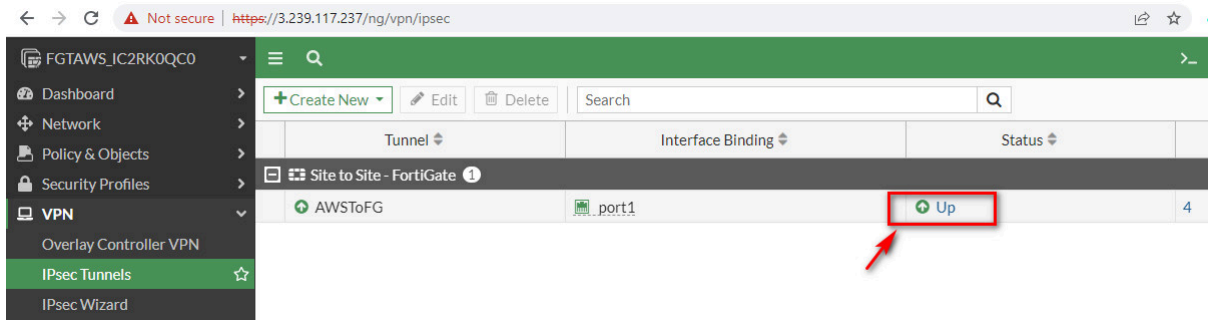


Figure 10.166: Check the status of the tunnel on AWS

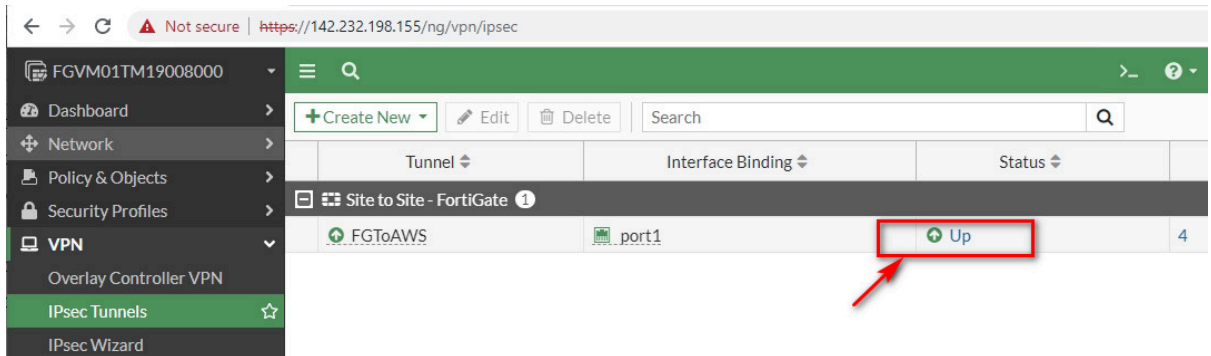


Figure 10.167: Check status of tunnel on FortiGate on premise

5. You should be able to ping from WebTerm to Virtual Machine on AWS and vice versa.

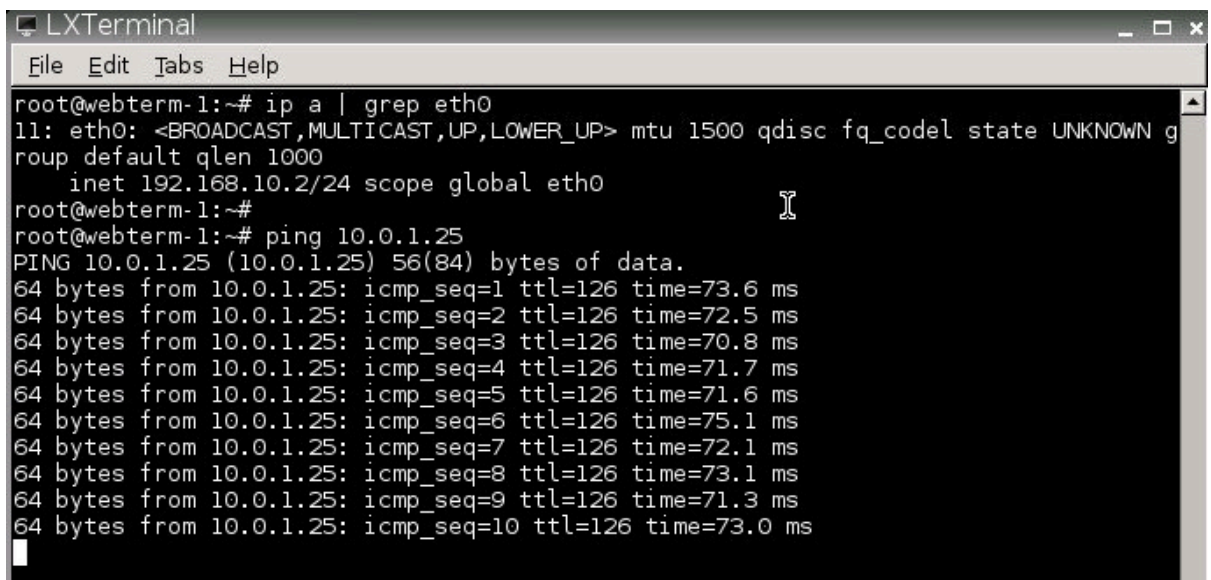


Figure 10.168: Ping from WebTerm to Windows VM

```
3.239.117.237 - Remote Desktop Connection
Administrator: Command Prompt
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : ec2.internal
    Link-local IPv6 Address . . . . . : fe80::d9f1:7627:b99e:2cd2%5
    IPv4 Address. . . . . : 10.0.1.25
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.1.1

Tunnel adapter Local Area Connection* 3:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:34f1:8072:3049:aca:f5ff:fee6
    Link-local IPv6 Address . . . . . : fe80::3049:aca:f5ff:fee6%7
    Default Gateway . . . . . : ::

Tunnel adapter isatap.ec2.internal:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : ec2.internal

C:\Users\Administrator>ping 192.168.10.2 -t

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=69ms TTL=62
Reply from 192.168.10.2: bytes=32 time=69ms TTL=62
Reply from 192.168.10.2: bytes=32 time=73ms TTL=62
Reply from 192.168.10.2: bytes=32 time=73ms TTL=62
Reply from 192.168.10.2: bytes=32 time=72ms TTL=62
Reply from 192.168.10.2: bytes=32 time=72ms TTL=62
Reply from 192.168.10.2: bytes=32 time=72ms TTL=62
Reply from 192.168.10.2: bytes=32 time=72ms TTL=62
```

Figure 10.169: Ping from Windows VM to WebTerm

Appendix: GNS3 Basics

In this chapter, we will be going through the basics in GNS3. Try to play with and familiarize yourself with this environment as this is a good tool for network simulations.

Adding a FortiGate Firewall to GNS3

1. Start by adding a new template.

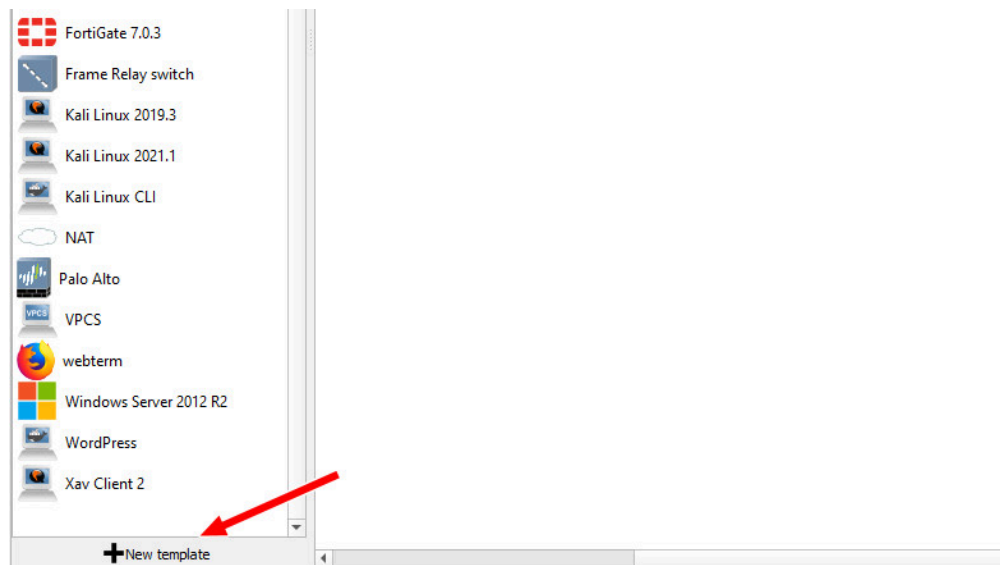


Figure A.1: Create a New template

2. We want to install it from the GNS3 Server, so keep the option default and then press next.

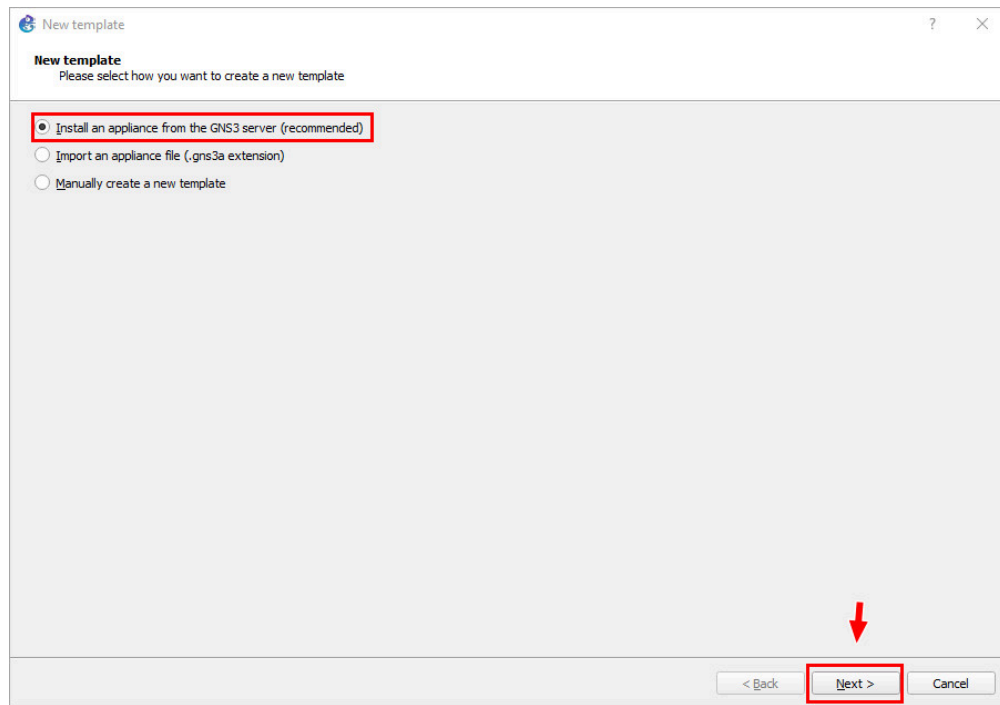


Figure A.2: Select Install an appliance from the GNS3 server

3. On the next window, search for “FortiGate”, and select the option under “Firewalls”, then click “Install.”

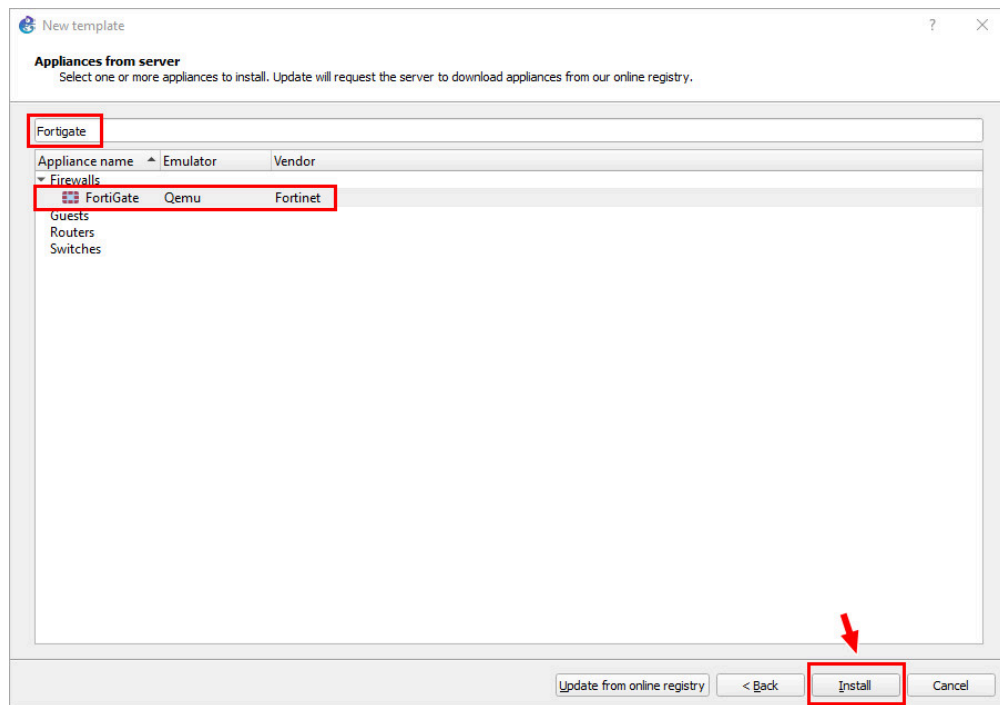


Figure A.3: Search for “FortiGate”

4. Press “Next” on this screen:

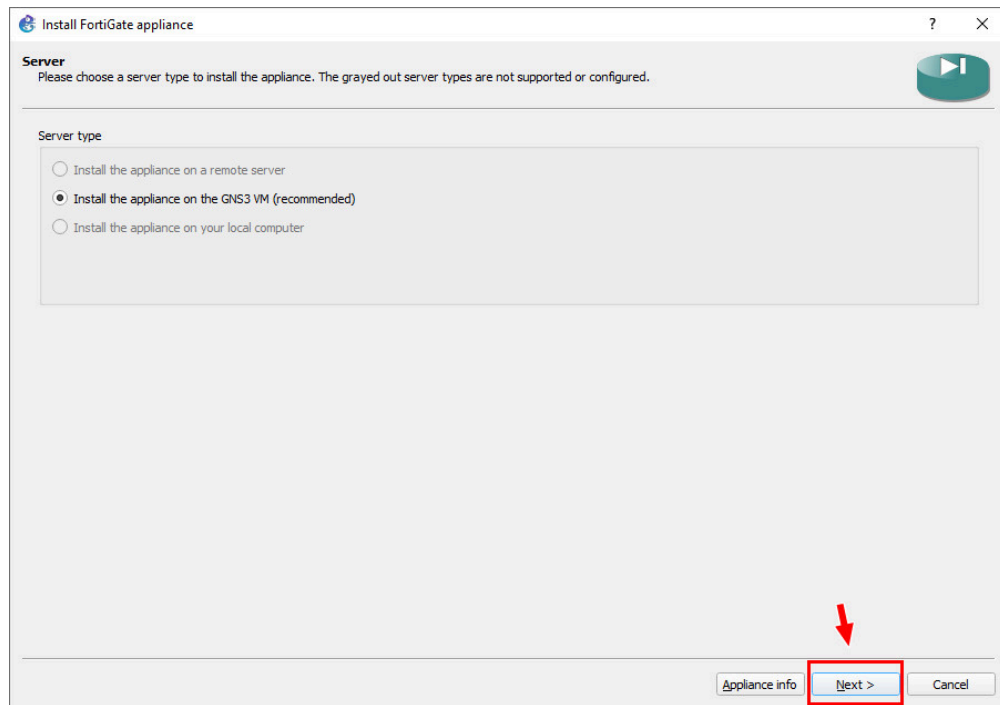


Figure A.4: Install the appliance on the GNS3 VM

5. Press “Next” on this screen:

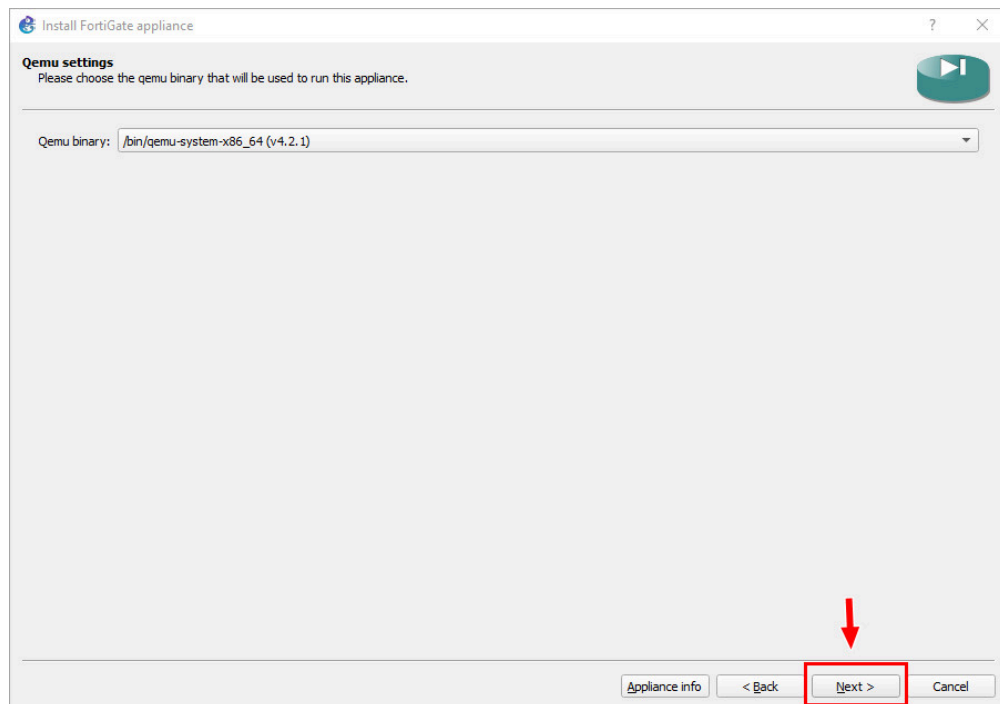


Figure A.5: Qemu settings

6. Tick the “Allow custom files” box.

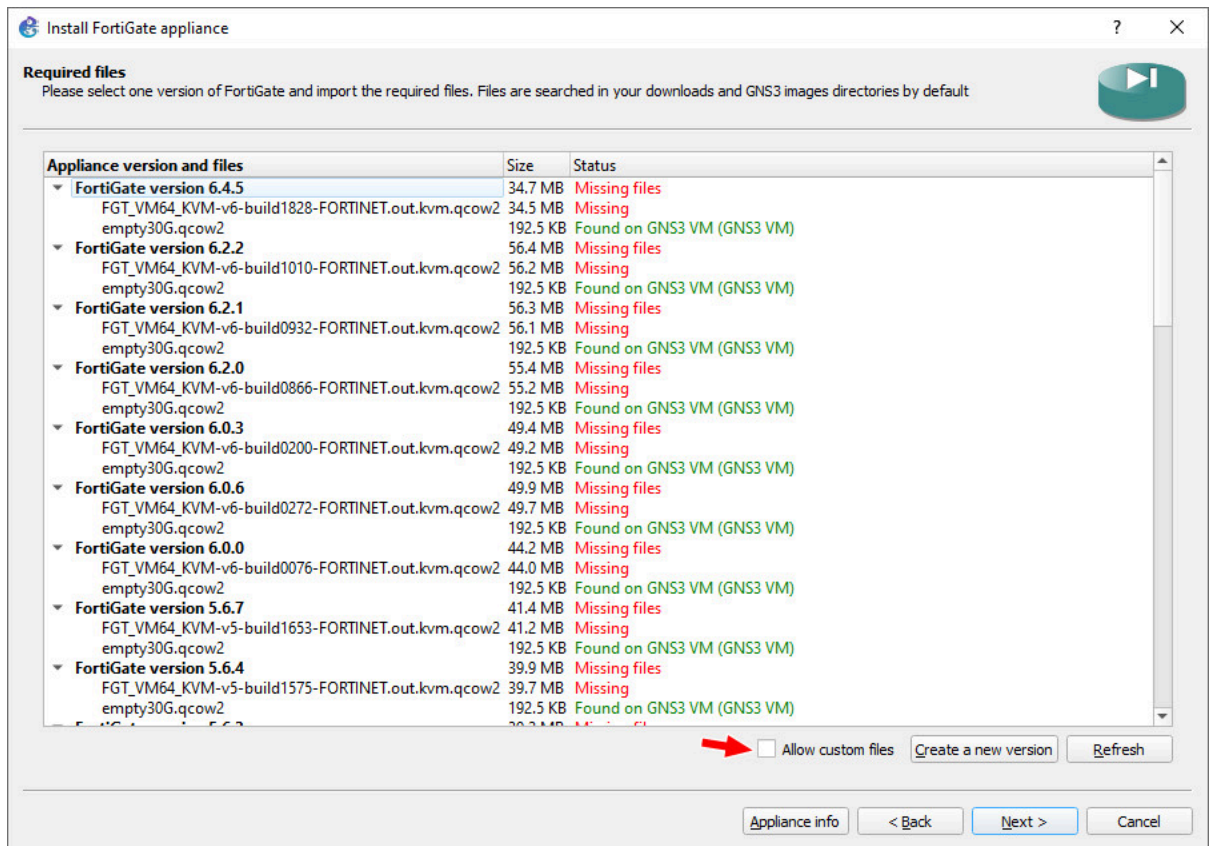


Figure A.6: Tick Allow custom files

7. Click “Yes” on this screen:

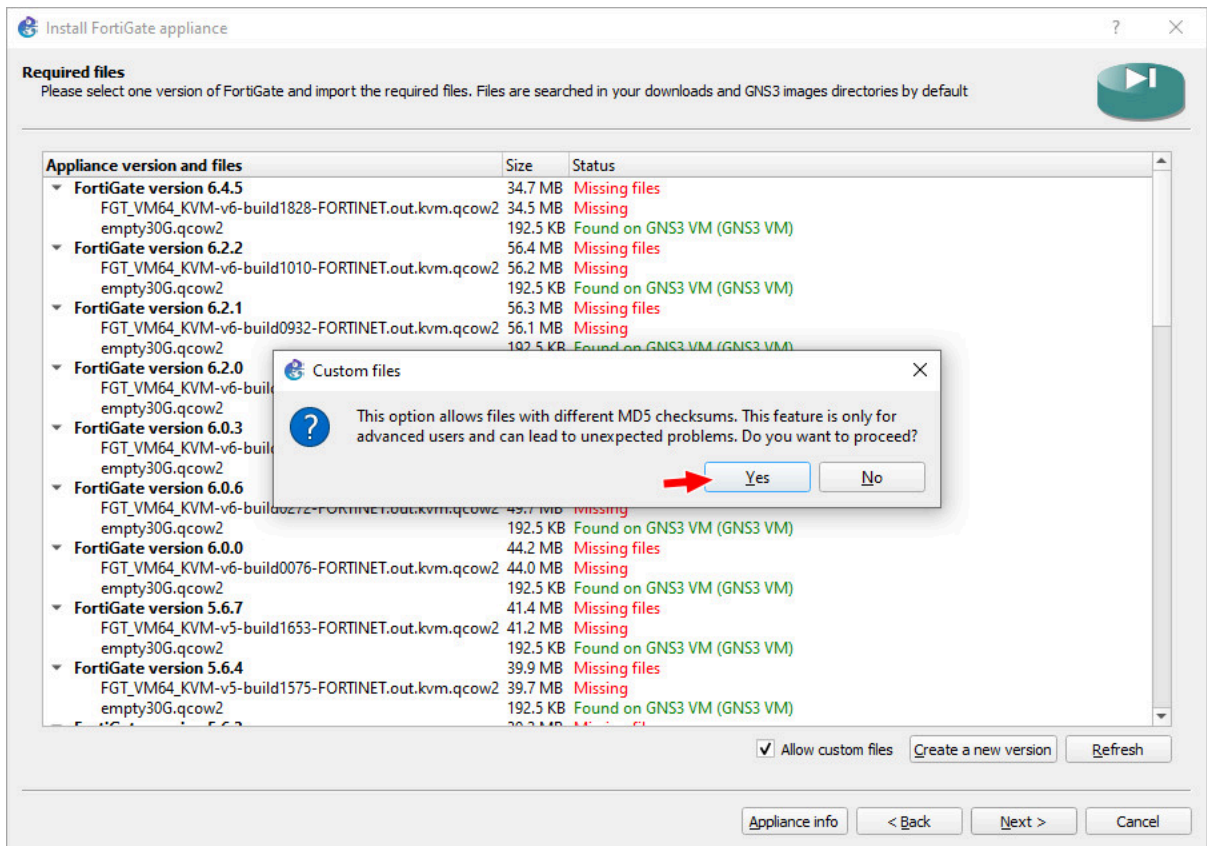


Figure A.7: Click on Yes

8. Highlight a random version.

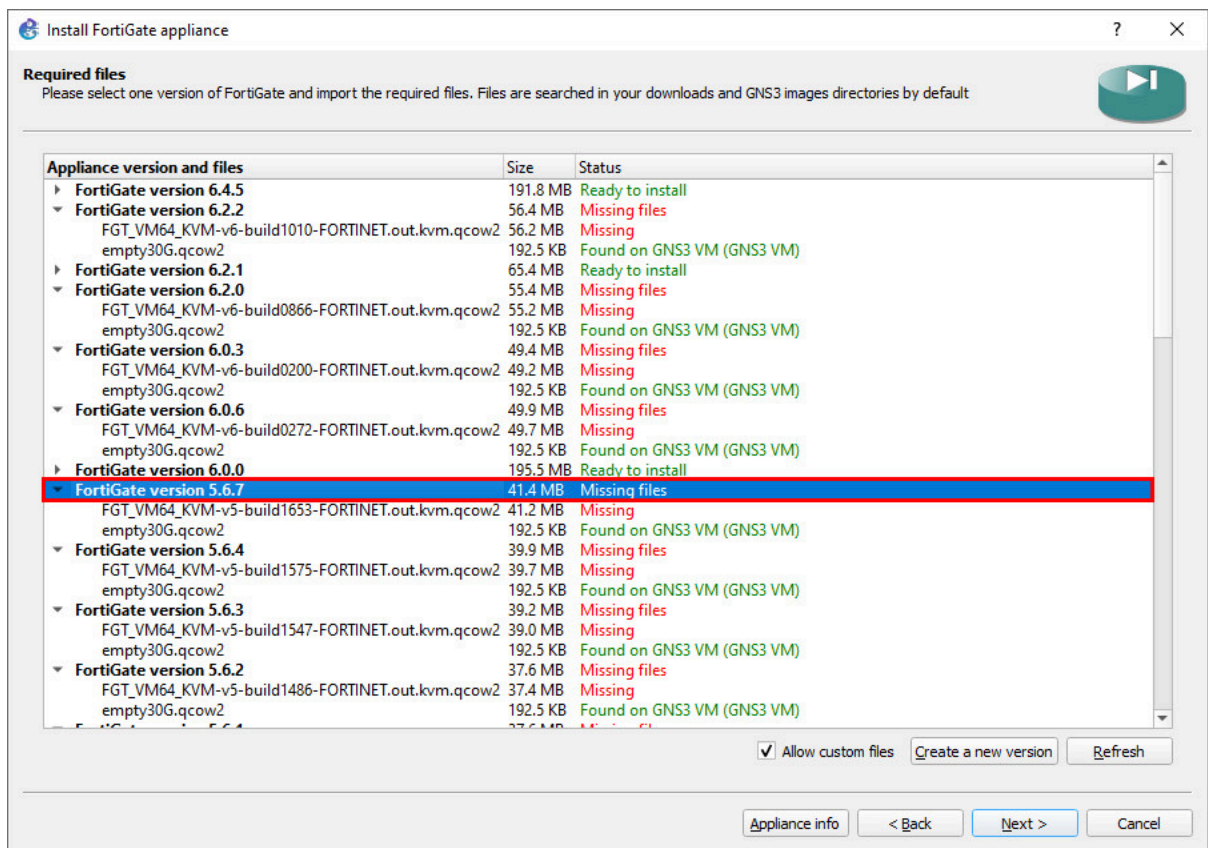


Figure A.8: Highlight a random version

9. Click “Create a new version.”

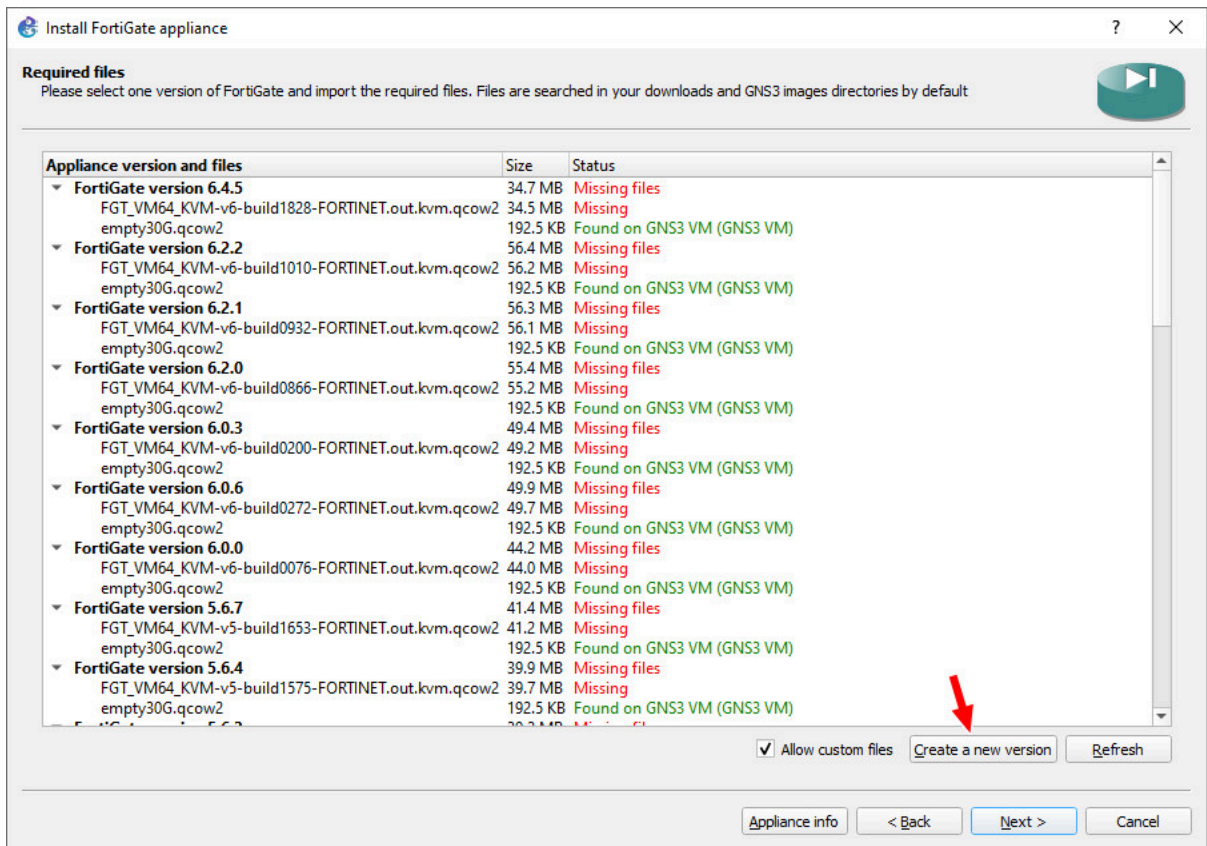


Figure A.9: Create a new version

10. Create a new custom version and select optional name for it.

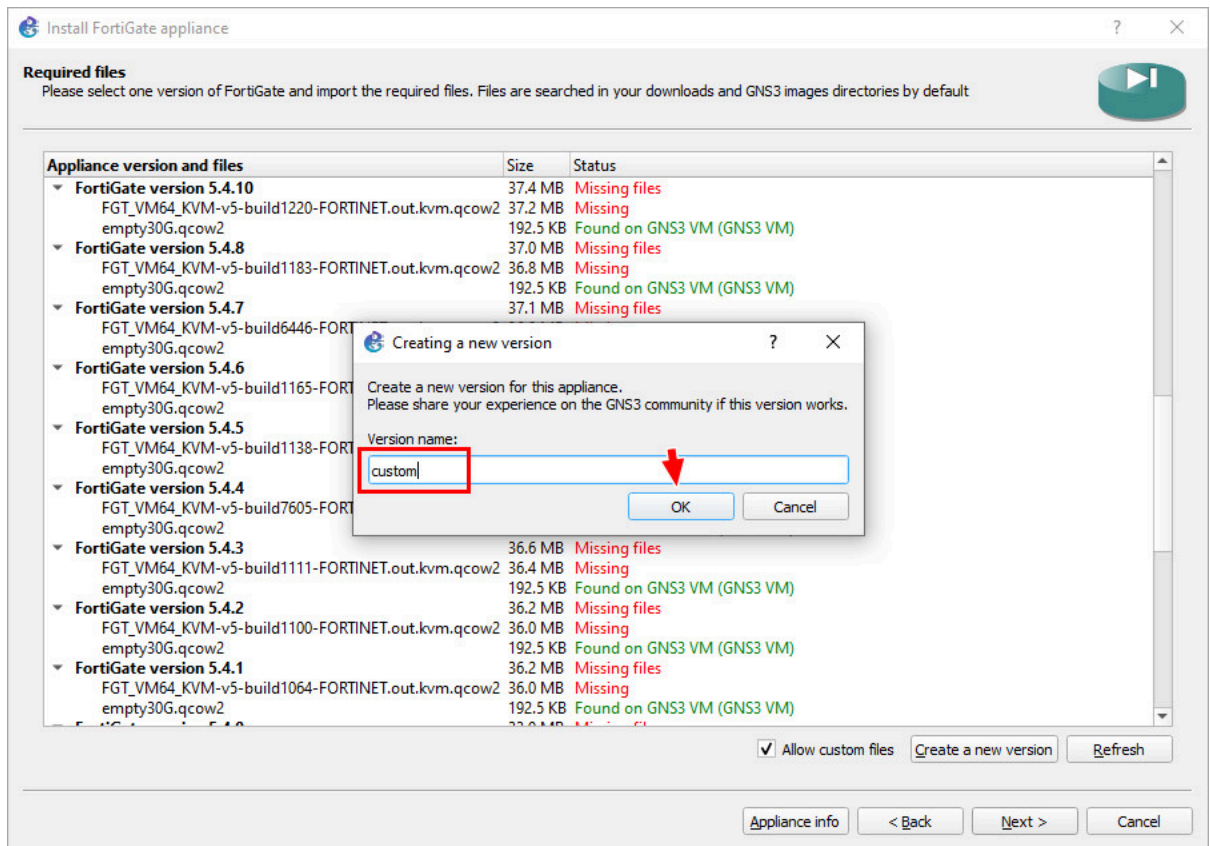


Figure A.10: Create a custom version

11. Press **OK** on this one, too:

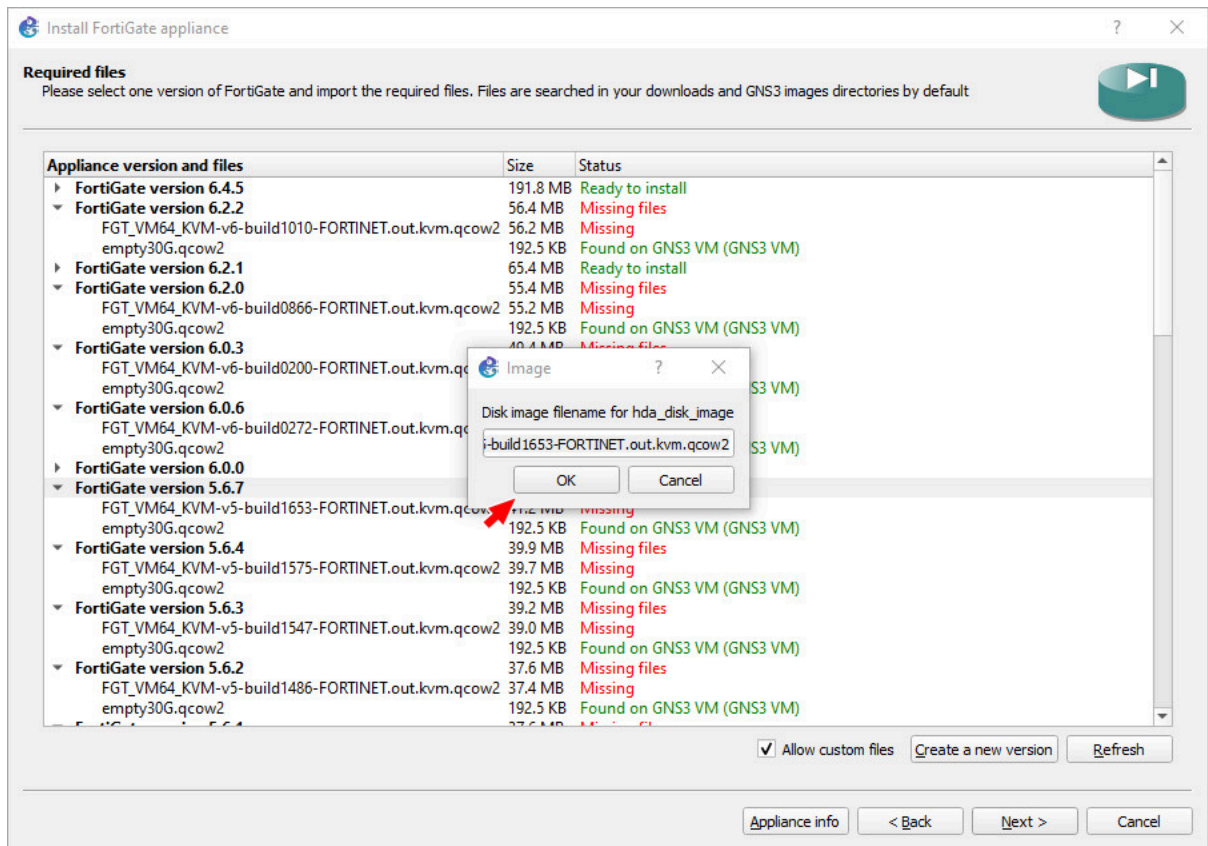


Figure A.11: Click on OK

12. Press **OK** again.

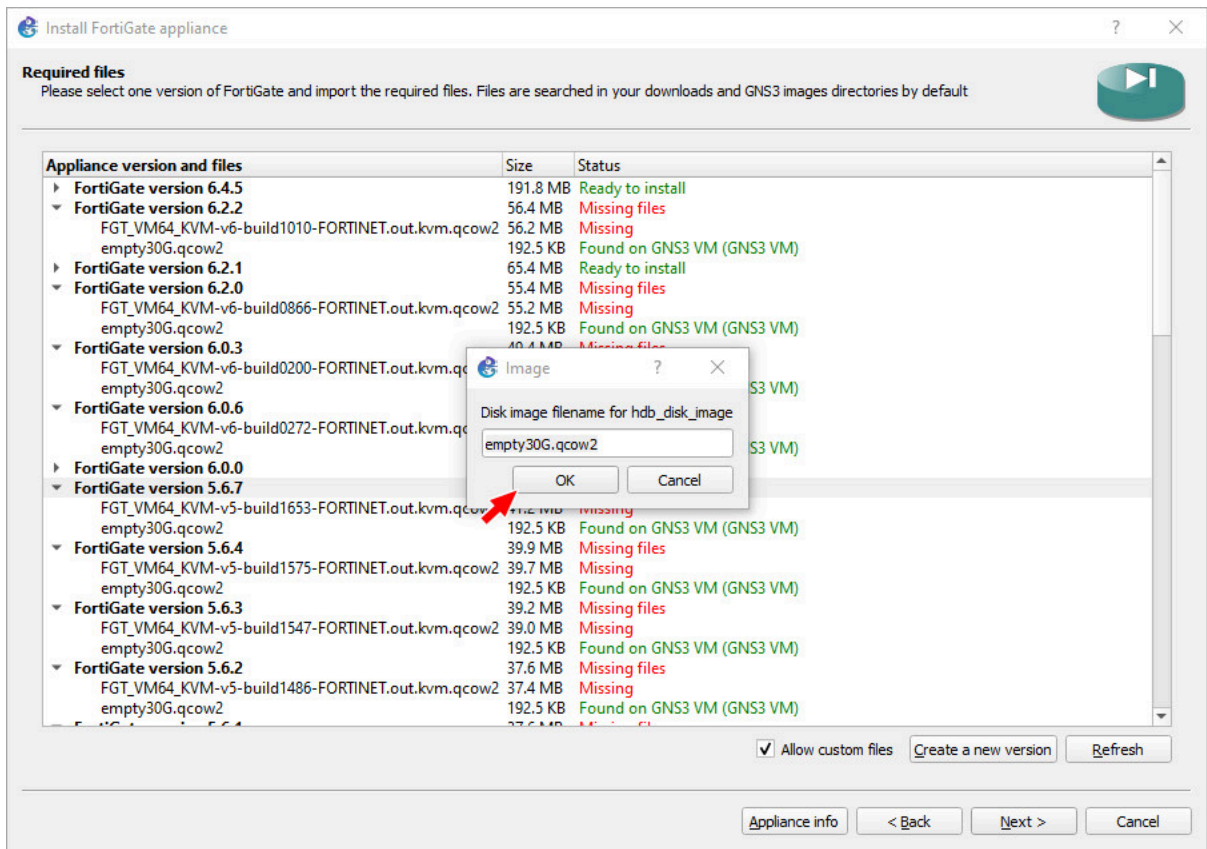


Figure A.12: Click on OK

13. Click on any empty30G file, and click Download. Save that file to your computer.

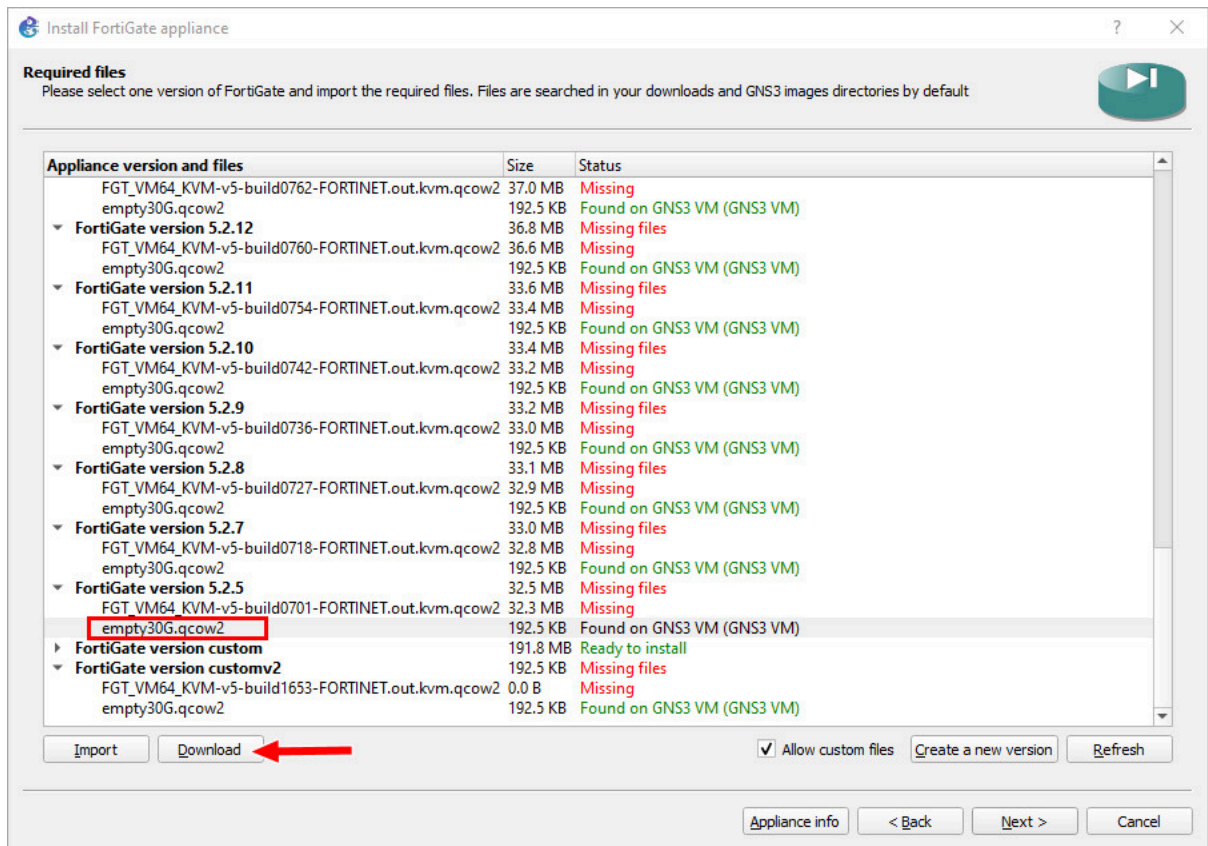


Figure A.13: Download empty30G.qcow2

14. Scroll down to your custom version and click the arrow on the left:

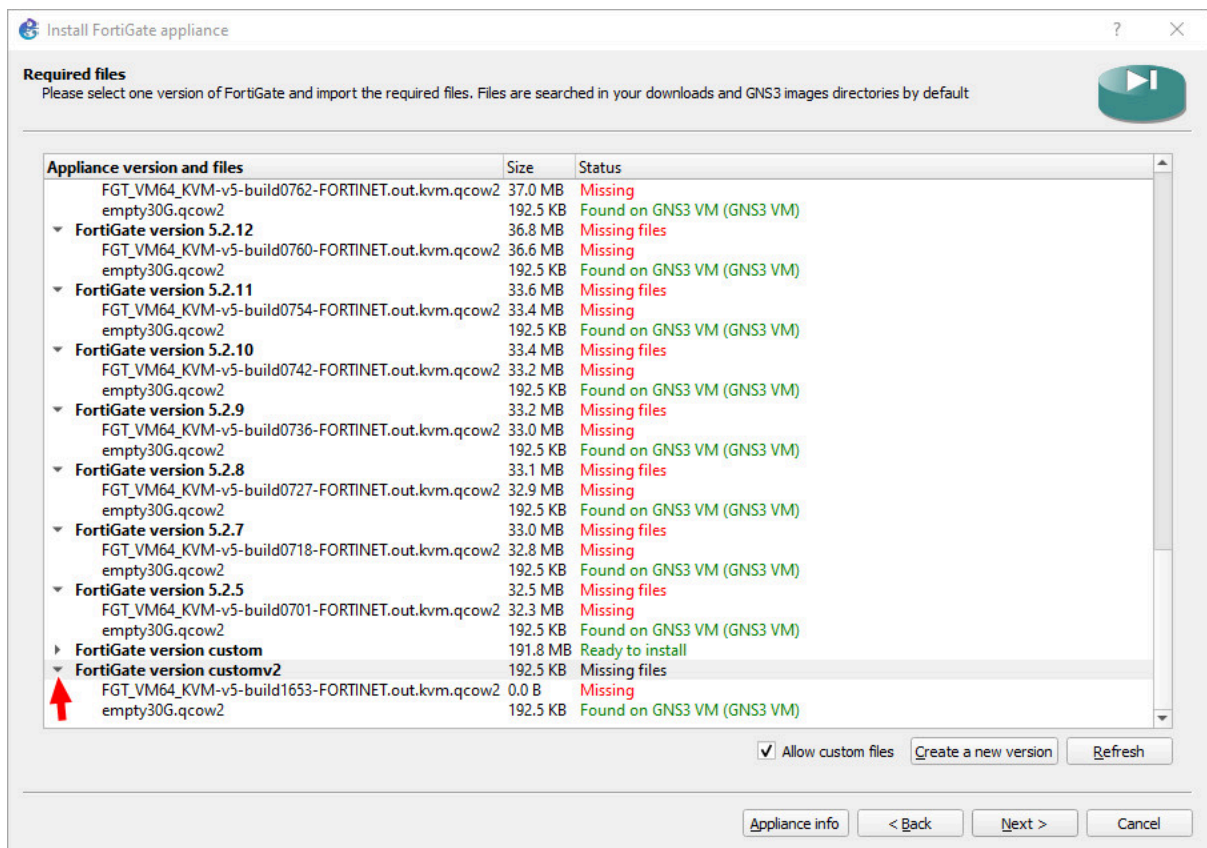


Figure A.14: Select Custom version

15. Click the FGT filename under your custom version and click "Import."

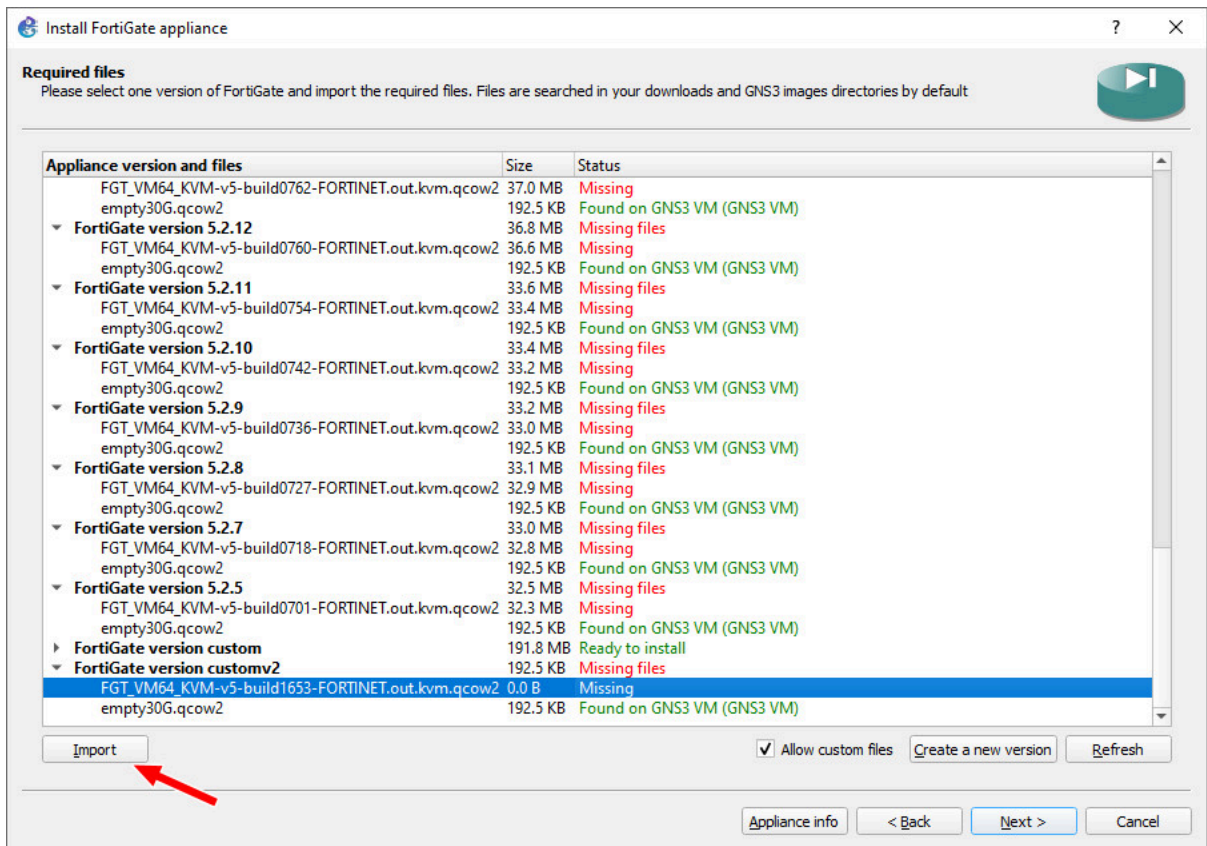


Figure A.15: Import FortiGate Image

16. Navigate to your downloaded FortiGate Firewall image and click “Open.”

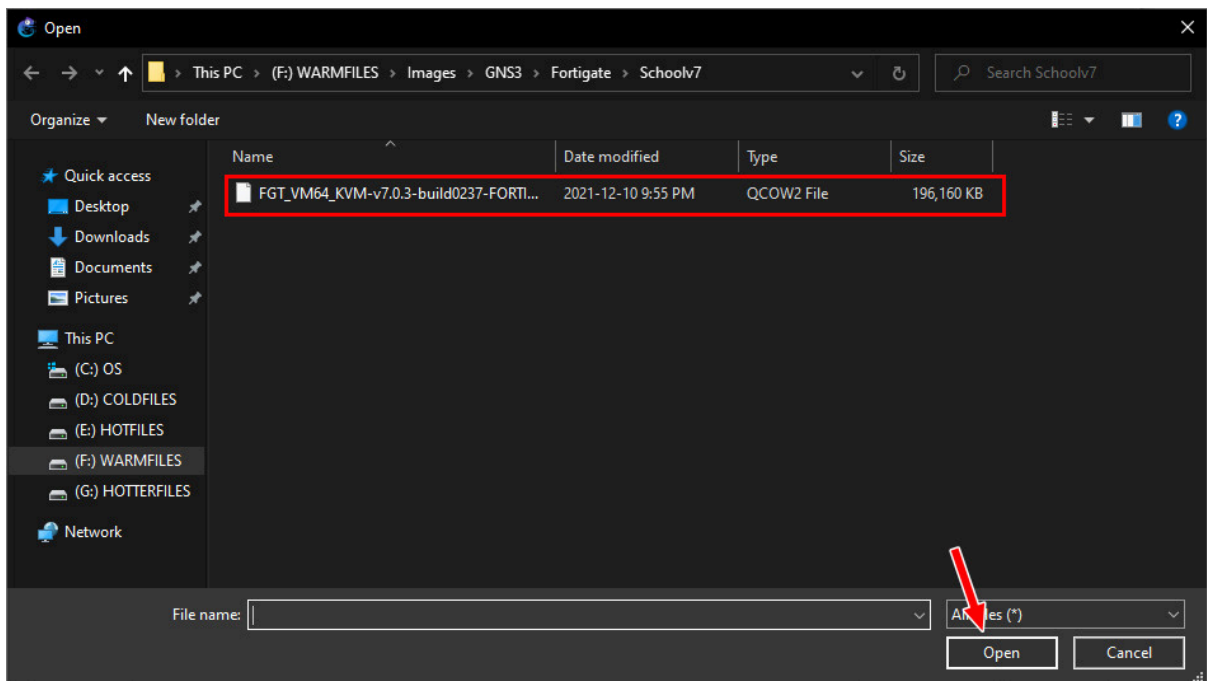


Figure A.16: Select FortiGate Image

17. Still under your custom version, click “Import” on the empty30G file.

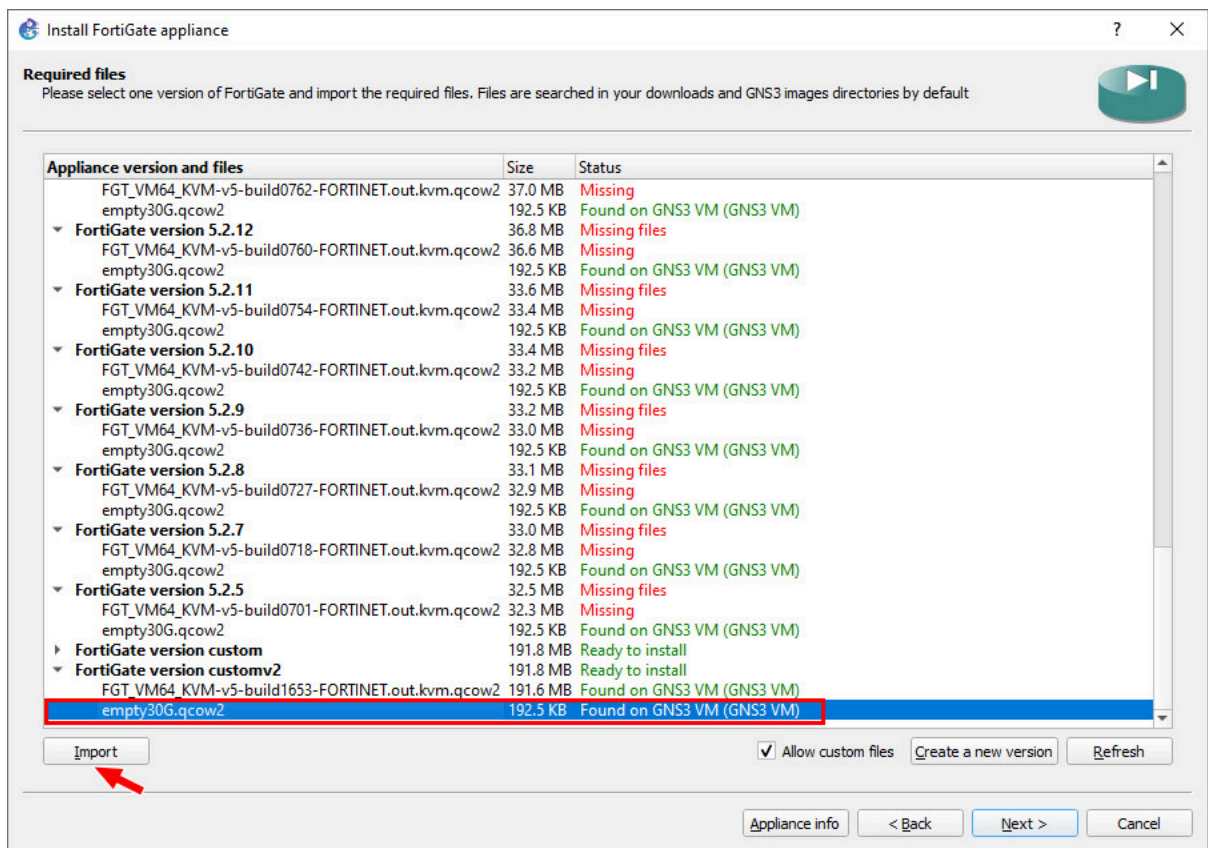


Figure A.17: Select empty30G.qcow2

18. Navigate to your downloaded empty30G file and click “Open.”

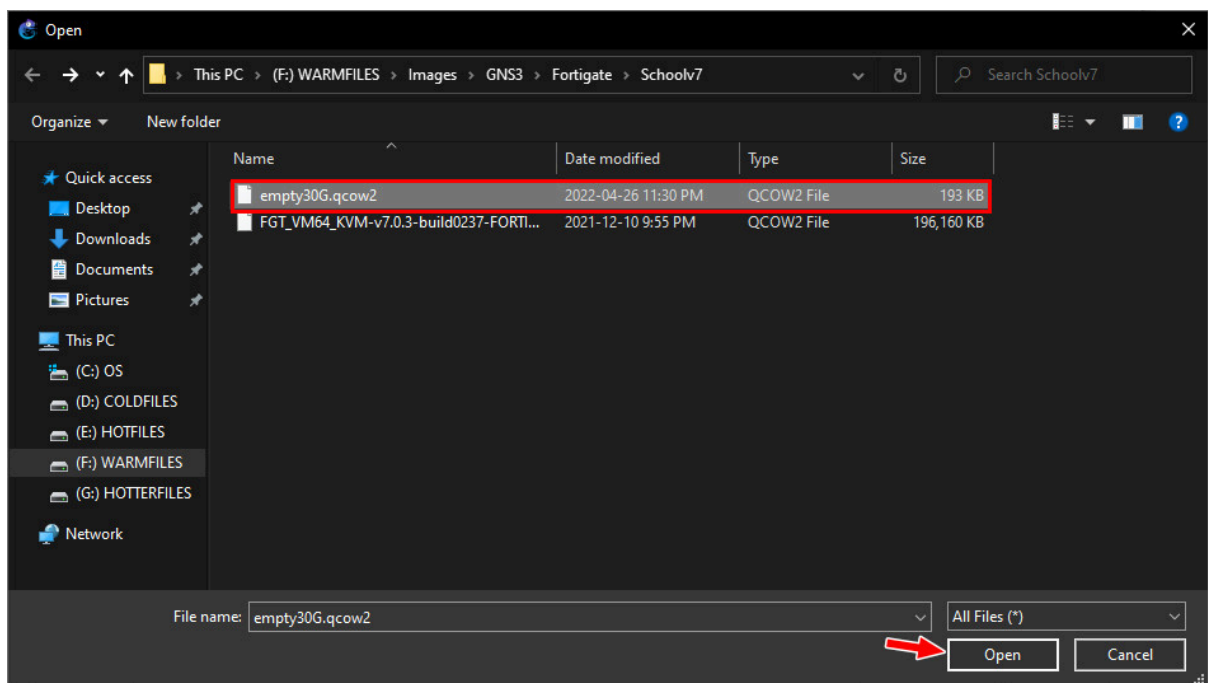


Figure A.18: Import empty30G.qcow2 file

19. After that, highlight the custom version again and click “Next.”

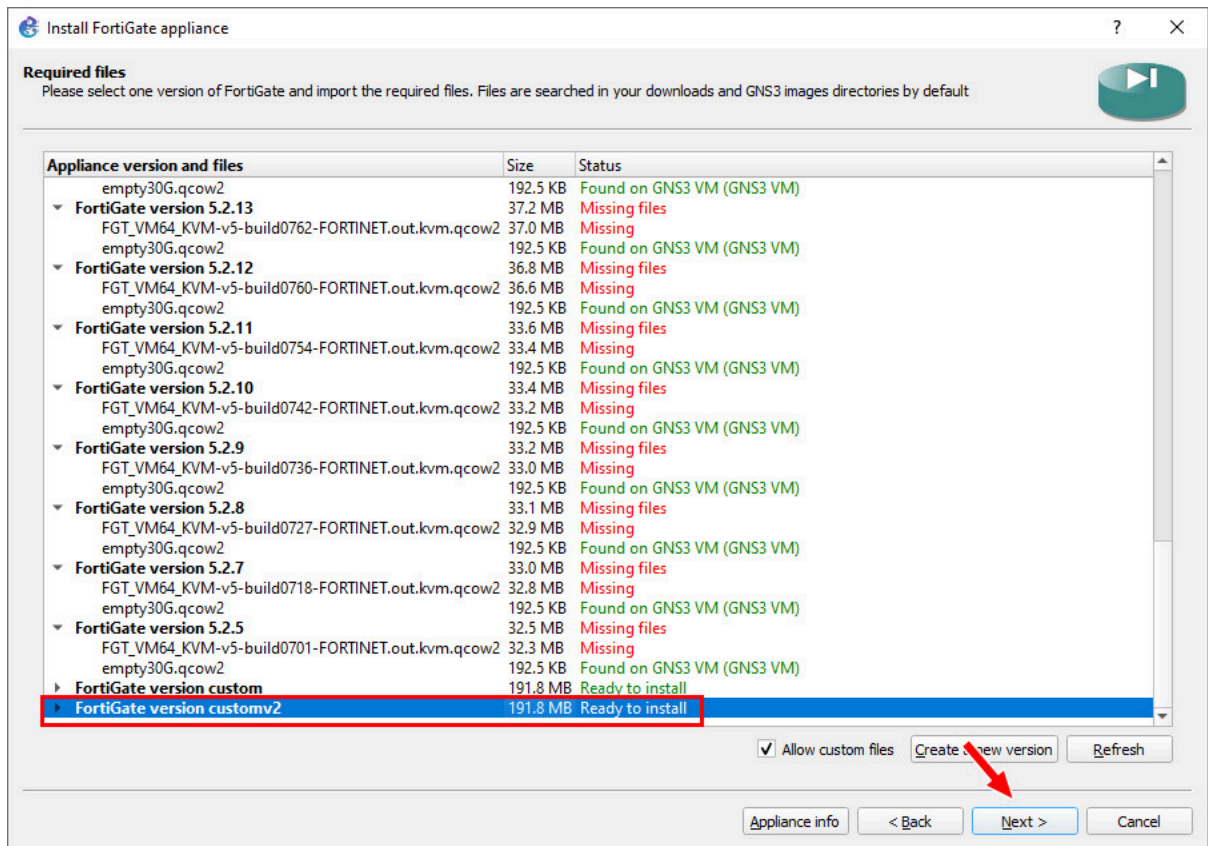


Figure A.19: Select custom version and then click on Next

20. Click “Yes” on this window:

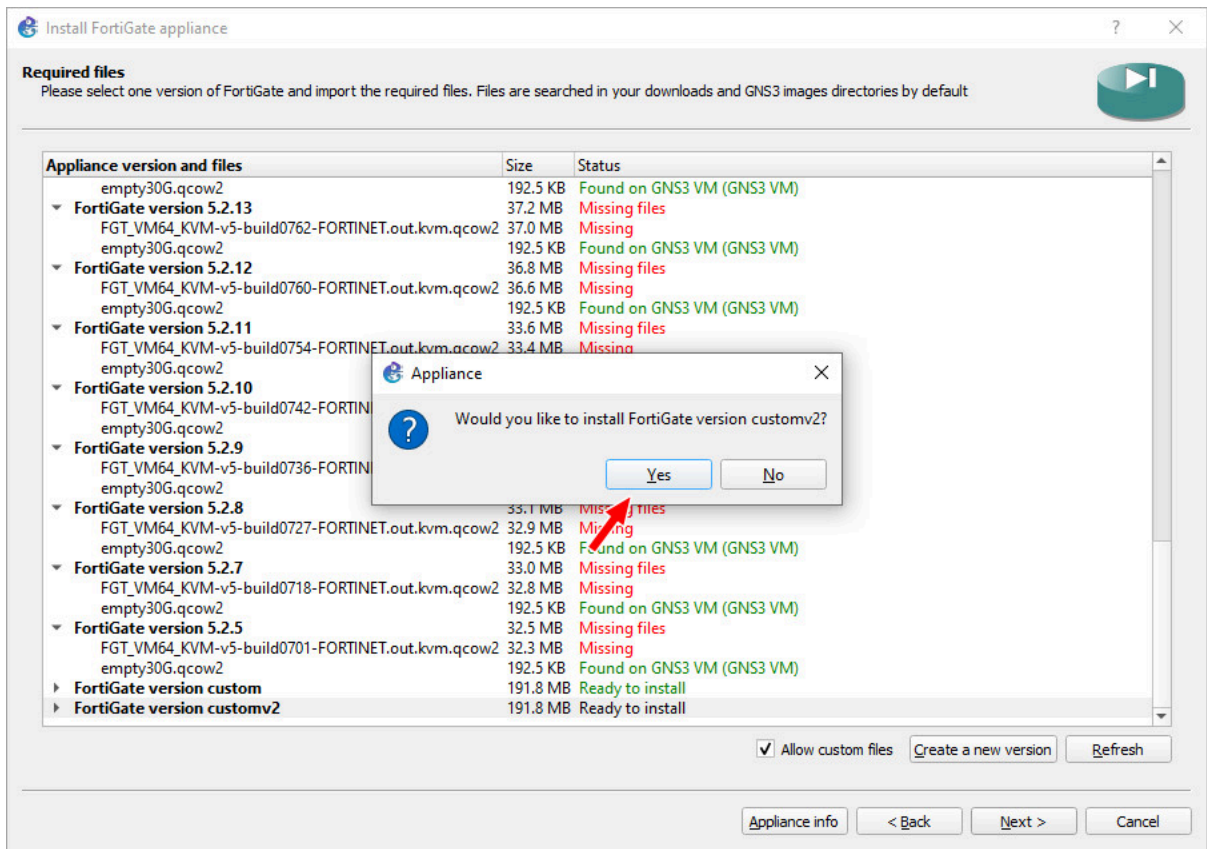


Figure A.20: Click on “Yes”

21. Then click “Finish.”

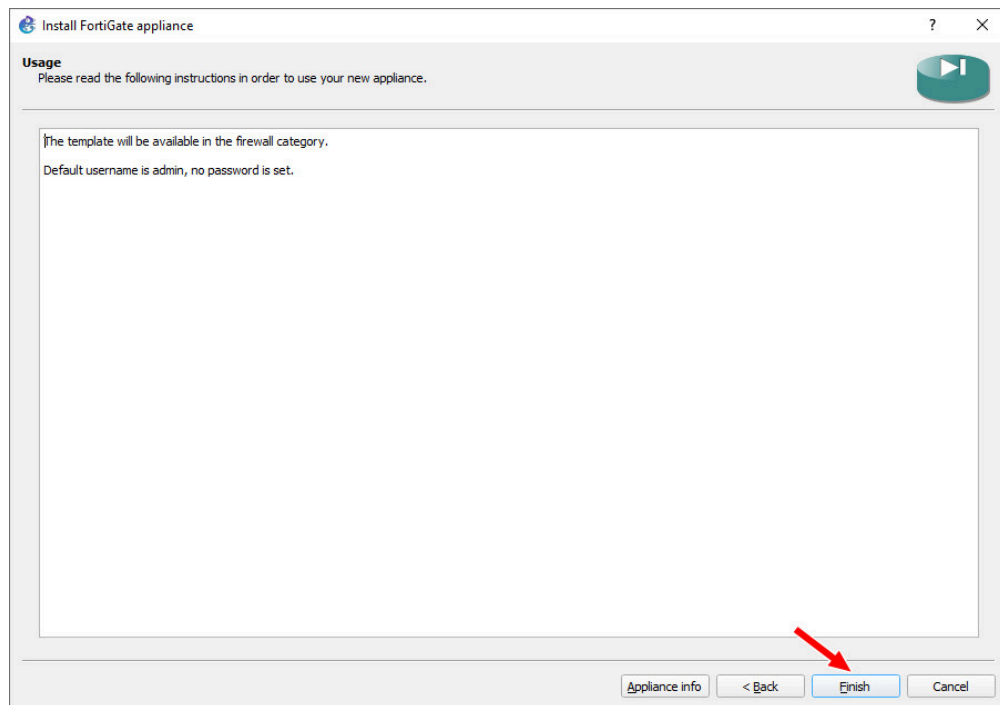


Figure A.21: Click on “Finish”

Configuring Your Palo Alto Firewall Template and Adding the Device

1. Let's start by modifying the GNS3 template of the Palo Alto firewall by right clicking the existing template, and clicking on "Configure template."

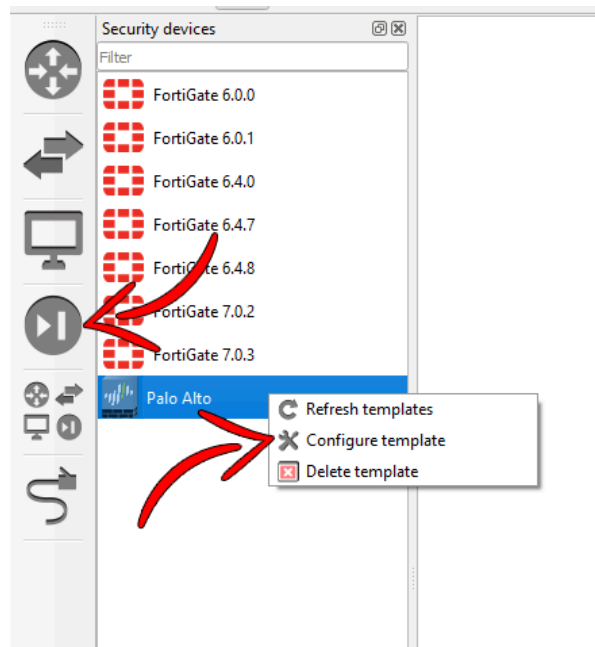


Figure A.22: Configure Palo Alto template

2. Make sure the max amount of RAM is set to at least 4096MB, and the amount of vCPUs are at least 2.

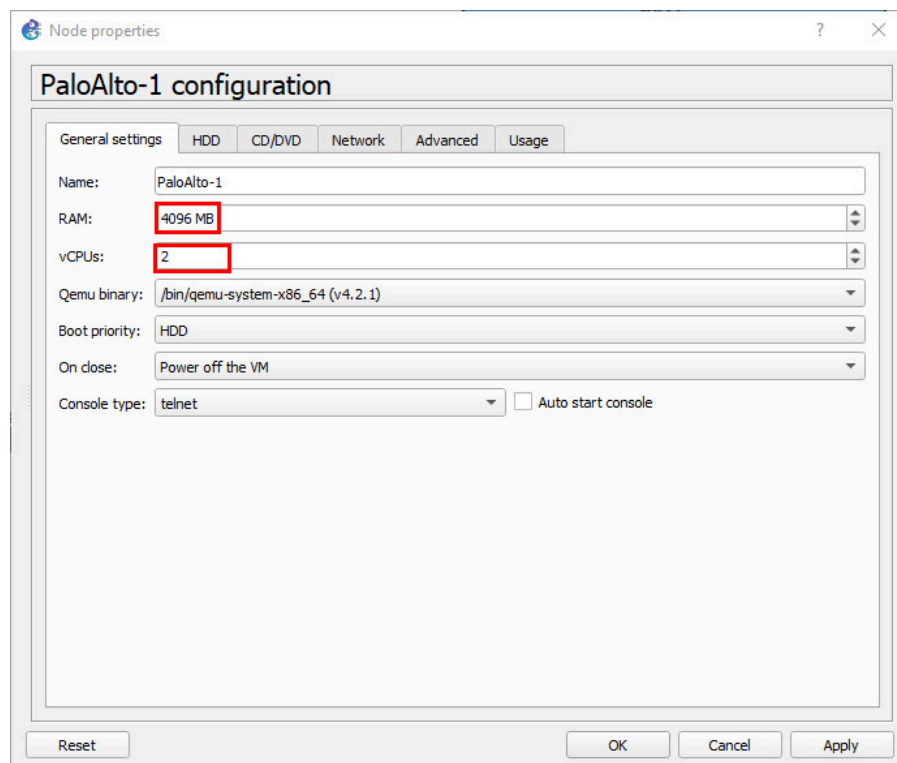


Figure A.23: Configure template

3. Now close the window, and drag in the Palo Alto device from the left hand pane.

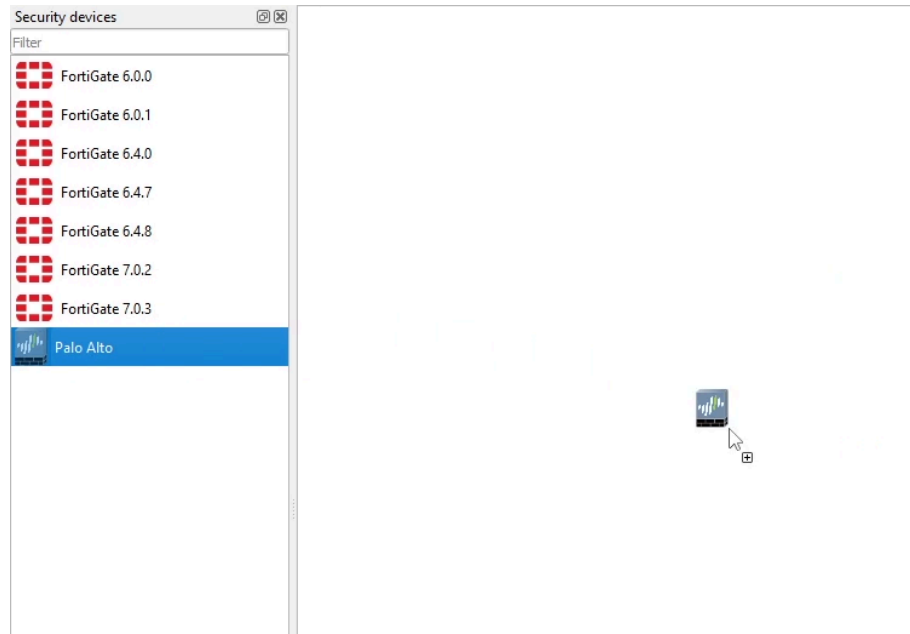


Figure A.24: Drag a Palo Alto in the workspace

4. Once you've dragged in the Palo Alto device, right click it, then click "Start."

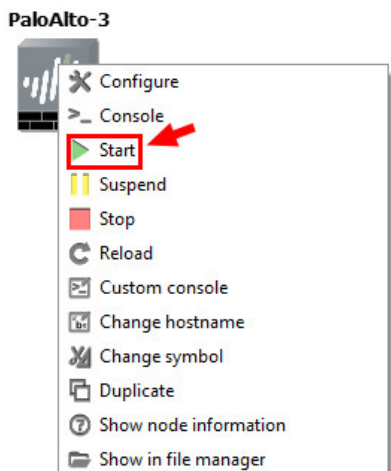


Figure A.25: Start Palo Alto

Keep in mind that this device takes a while to start.

Webterm Installation

1. Let's begin by clicking "New template" on the bottom left hand of GNS3.

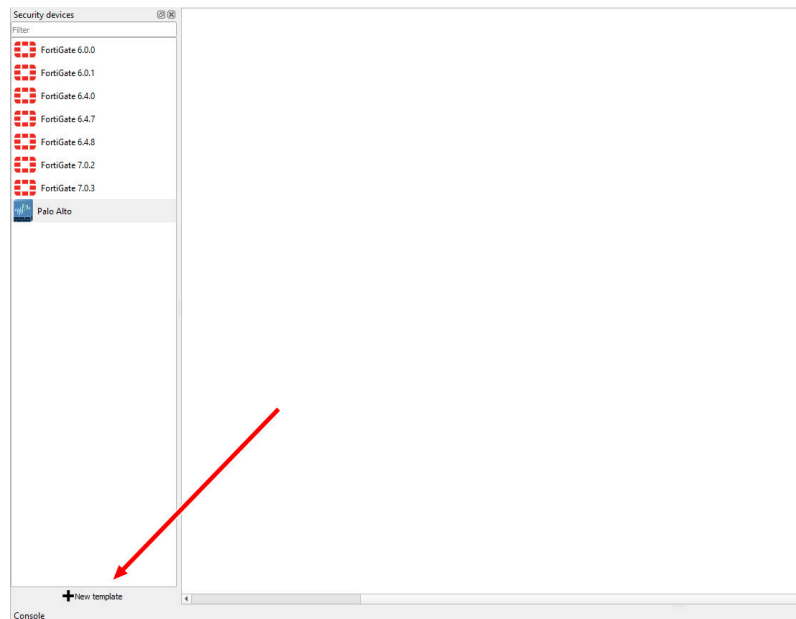


Figure A.26: Create a new template

2. We want to install this into the GNS3 VM. Click on the option to “Install an appliance from the GNS3 Server,” then click next.

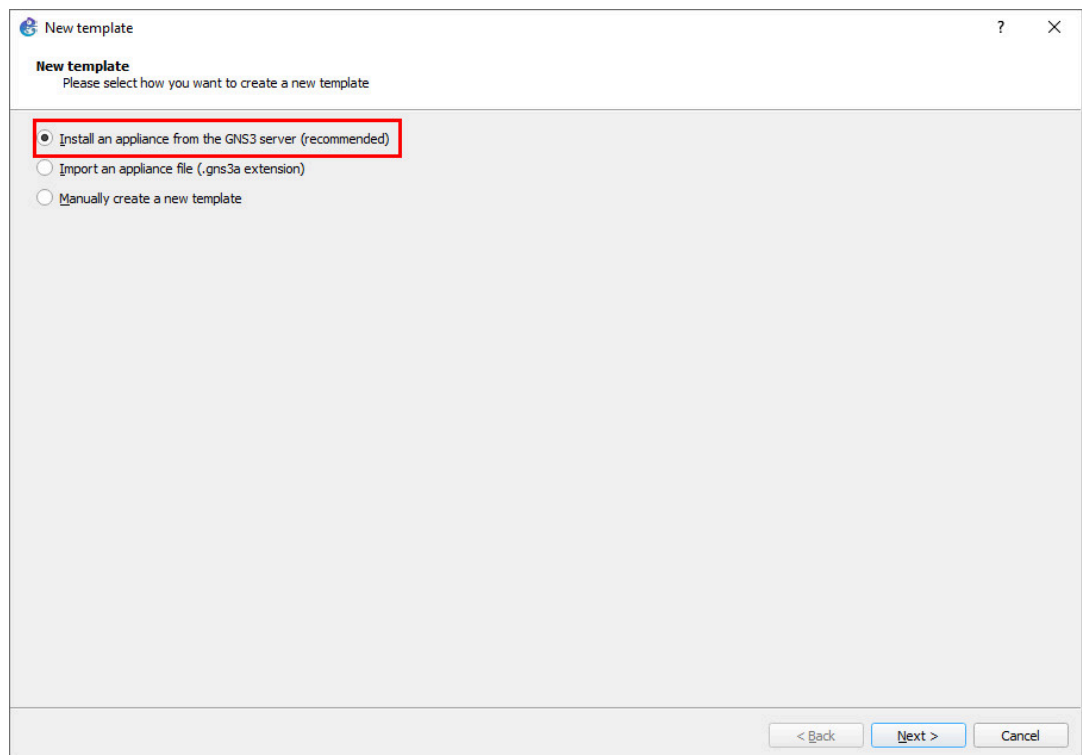


Figure A.27: Install an appliance from the GNS3 server

3. On the next window, search for “webterm,” select the option under “guests,” then click “Install.”

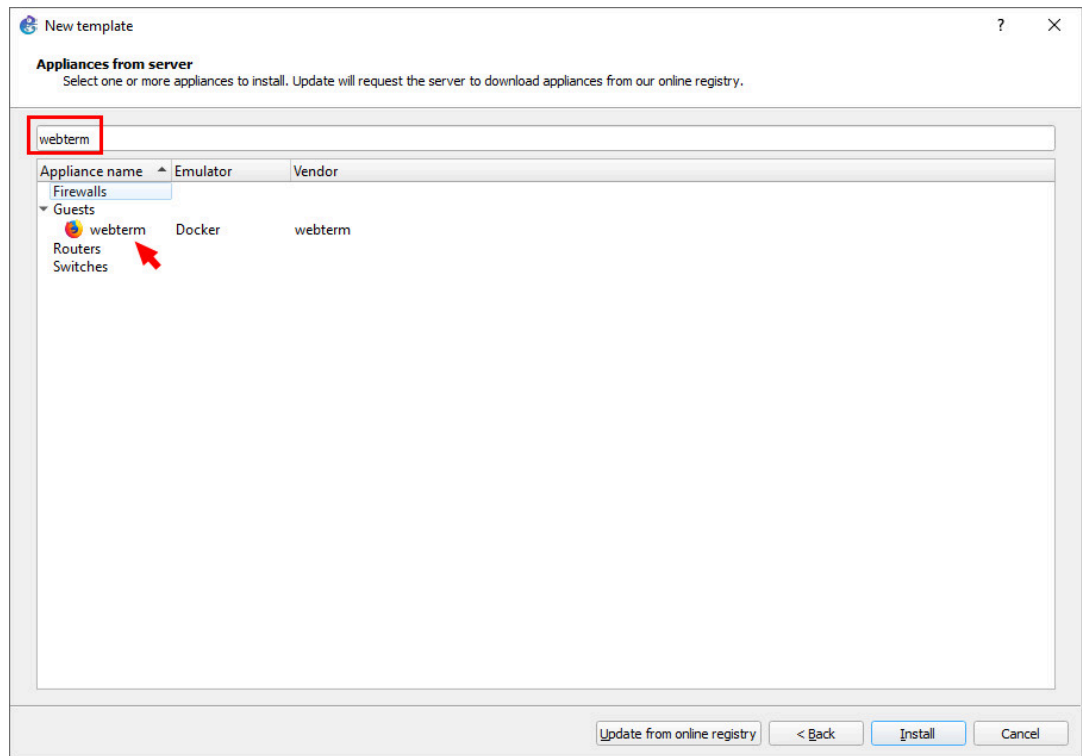


Figure A.28: Search for “webterm”

- On the next screen, ensure that “Install the appliance on the GNS3 VM” is already selected, then click “Next.”

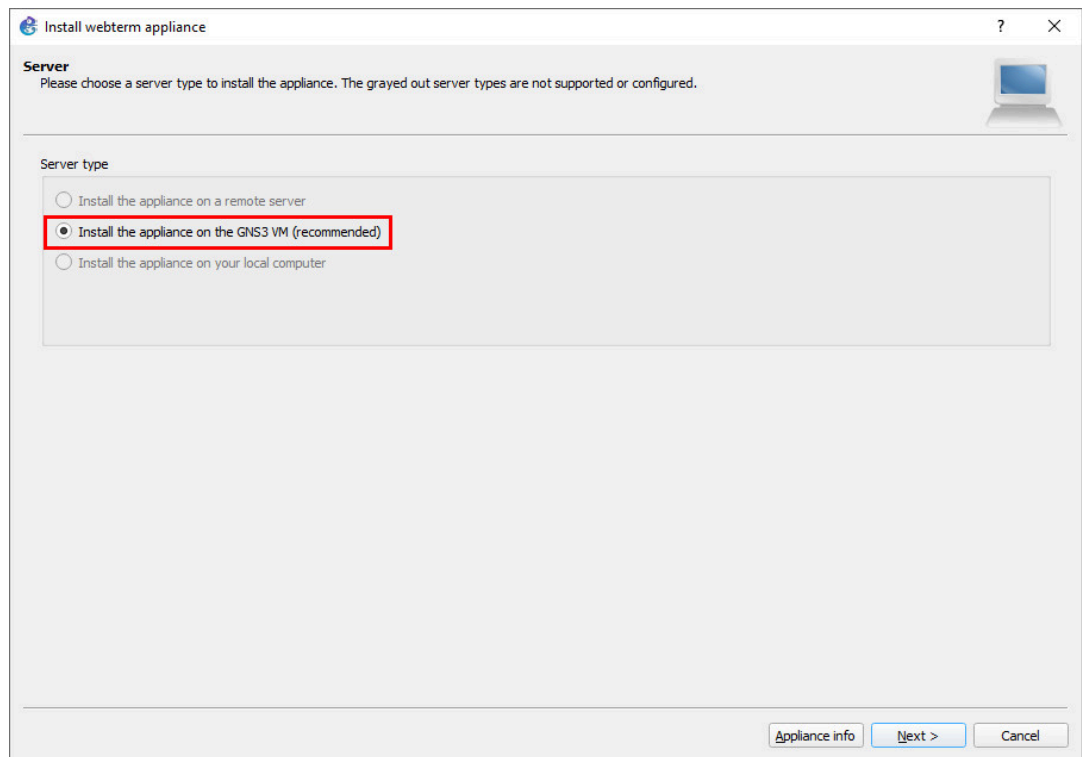


Figure A.29: Select “Install the appliance on the GNS3 VM”

- On the next screen, click “Finish.”

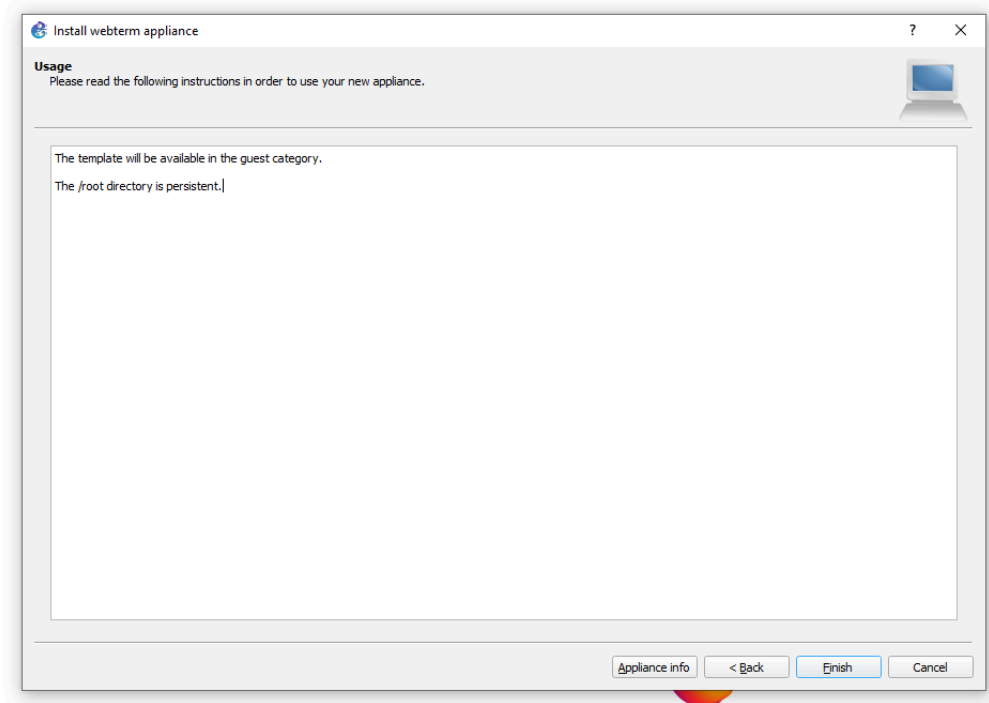


Figure A.30: Click on Finish

After that, it should appear under all devices in GNS3

Configuring Your Webterm Device with a Static IP

1. Drag in the webterm device from the left pane. Then once it finishes downloading the docker file, right click it and select “Edit config.”

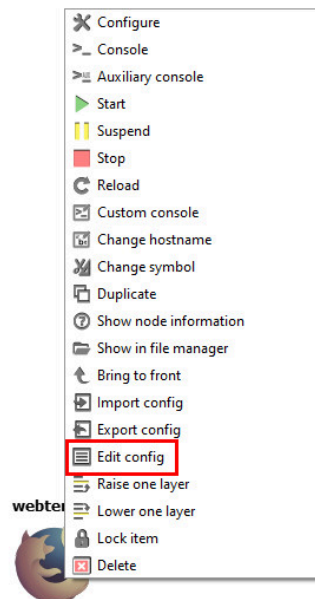


Figure A.31: Edit config

2. A window will pop up containing the device's network configuration. We want to modify this file to match the specified IP address. The final modification should look like a little like this:

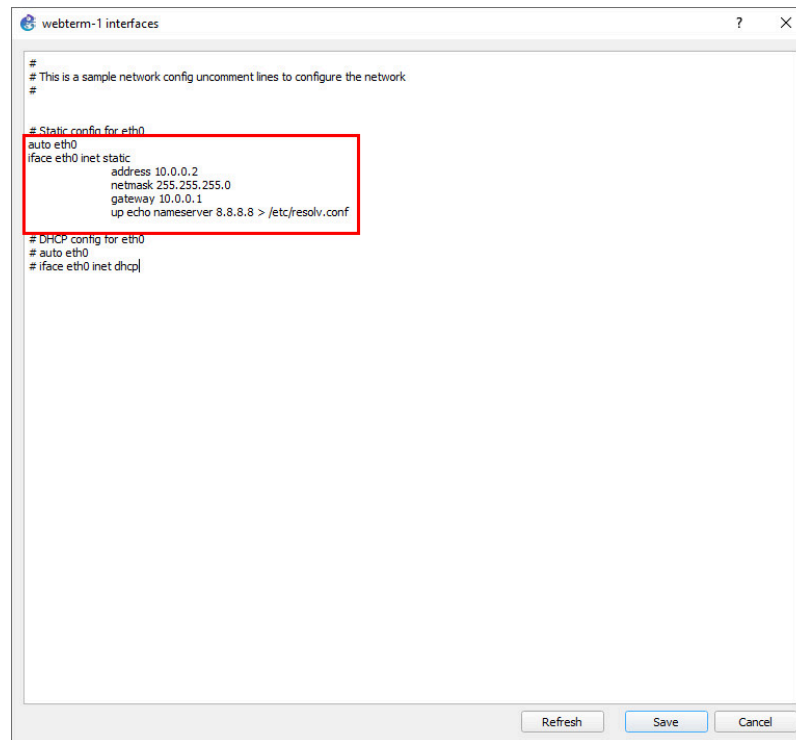


Figure A.32: Static IP address configuration

After these modifications, click on the save button on the bottom right of the window.

Configuring a Webterm DHCP Client

We just need to uncomment these 2 lines to enable DHCP. Click on save and we are done.

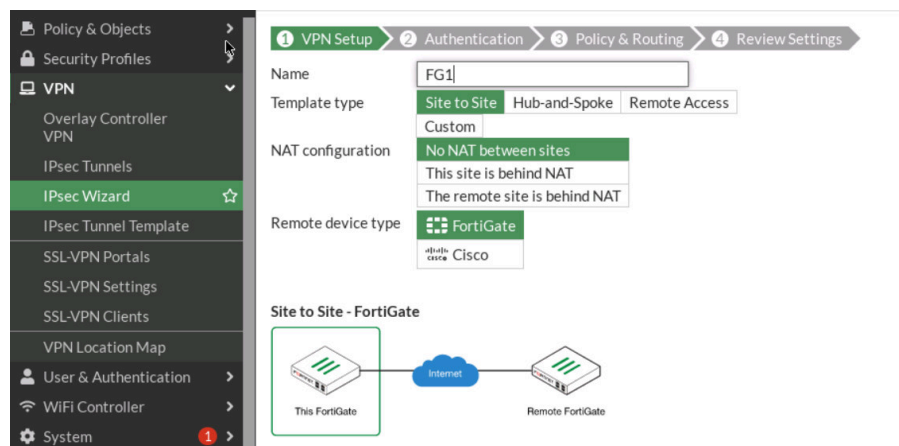


Figure A.33: DHCP IP address configuration

Connecting Devices in GNS3

Please see the example below:¹

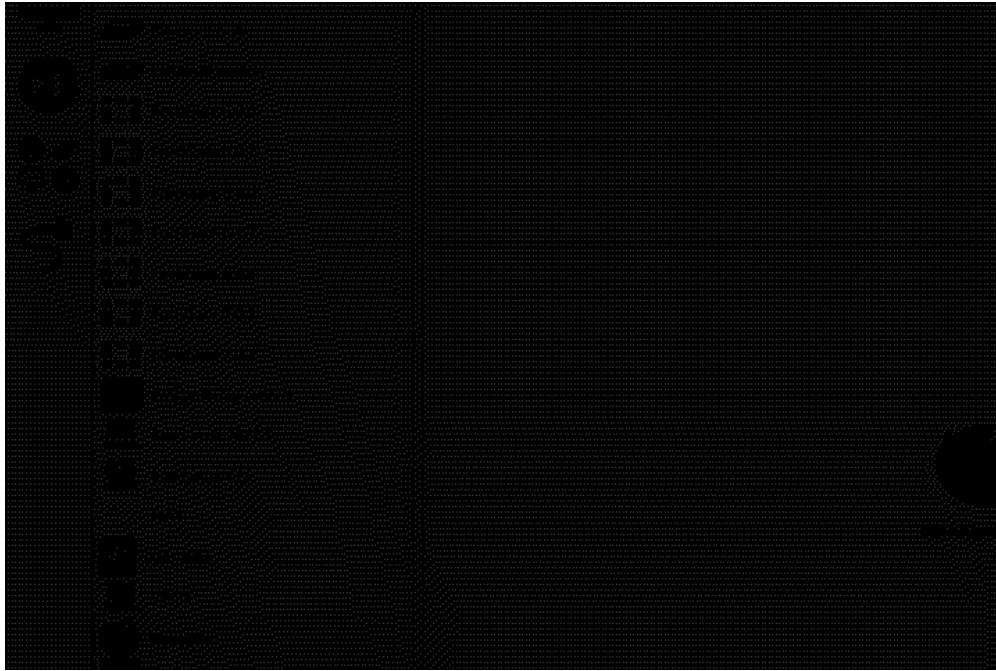


Figure A.34: Connecting devices

Using NAT in GNS3

The NAT device in GNS3 will allow devices in our virtual topology to communicate with the internet. This device is under the all devices section of GNS3.

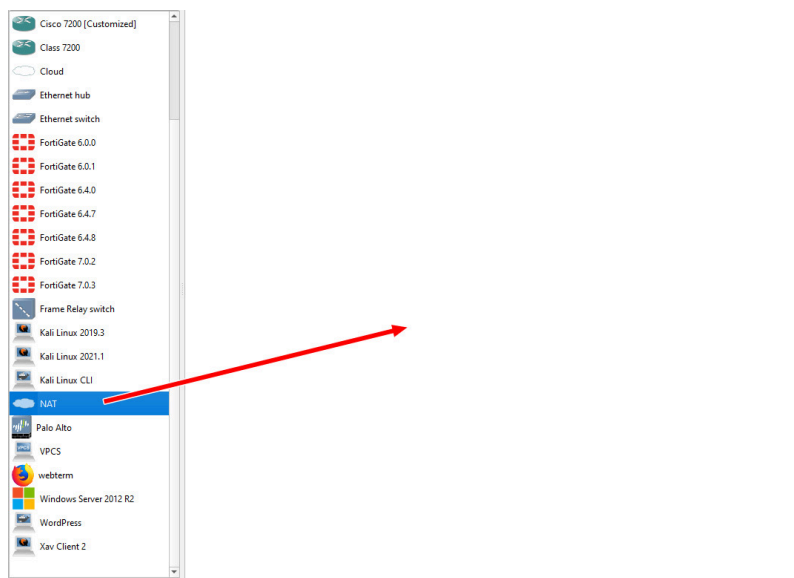


Figure A.35: NAT

1. If using an offline version of the book, navigate to <https://opentextbc.ca/fortigatefirewall/back-matter/appendix/> in order to see this animated example.

Make sure you select the GNS3 VM as the option whenever you see this window (applies for all devices)

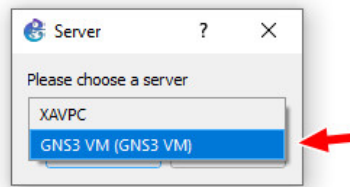


Figure A.36: Choose GNS3 VM

Using Kali in GNS3

Sometimes we need to use Kali to demonstrate an attack. Please keep in mind that Kali is used strictly for testing purposes, and should not be used as a daily driver, to hack your friends, or to pretend to look cool.

1. Let's begin by clicking "New template" on the bottom left hand of GNS3.

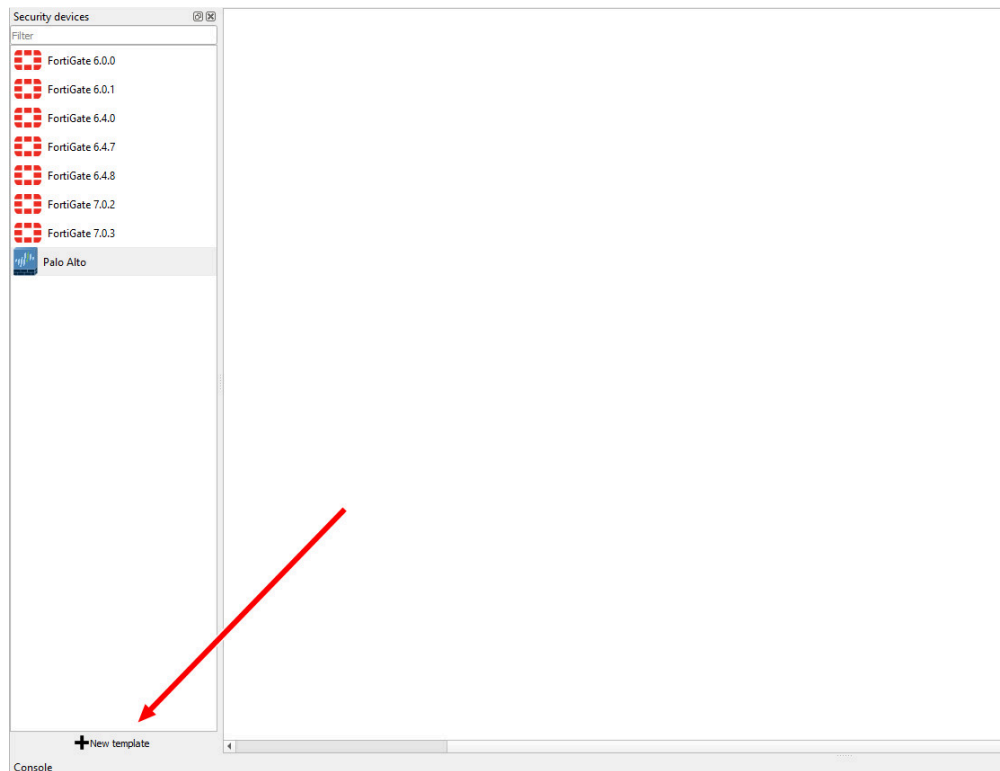


Figure A.37: Create a new template

2. We want to install this into the GNS3 VM. Click on the option to "Install an appliance from the GNS3 Server," then click "Next."

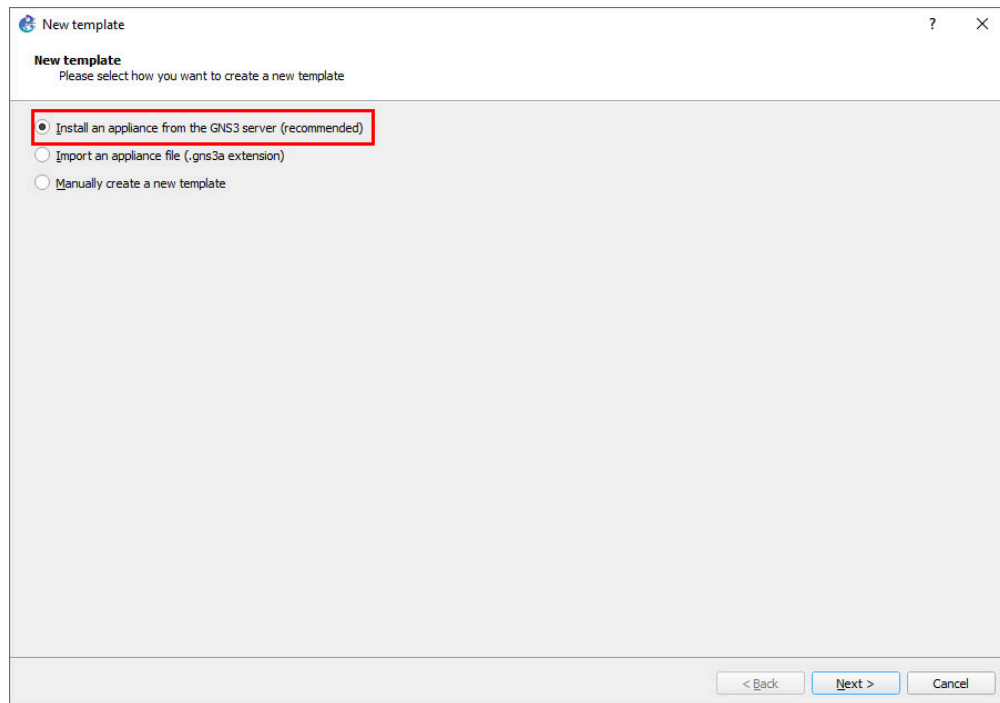


Figure A.38: Select “Install an appliance from the GNS3 Server”

3. On the next window, search for “kali”, and select the non “CLI” option.

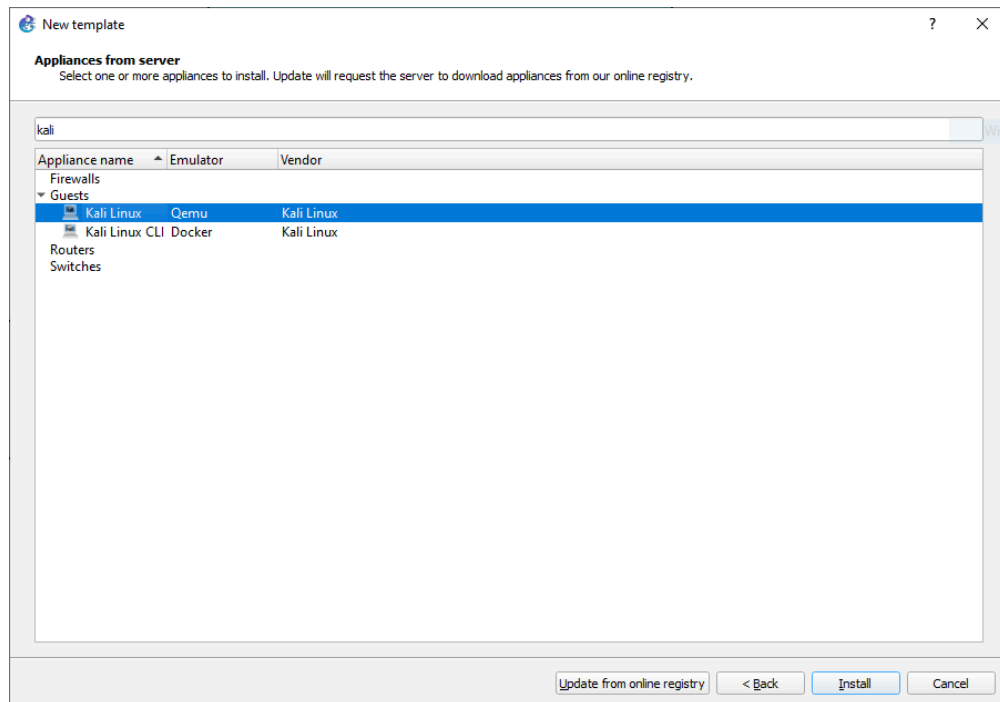


Figure A.39: Select Kali Linux

4. On the next screen, ensure that “Install the appliance on the GNS3 VM” is already selected, then click “Next.”

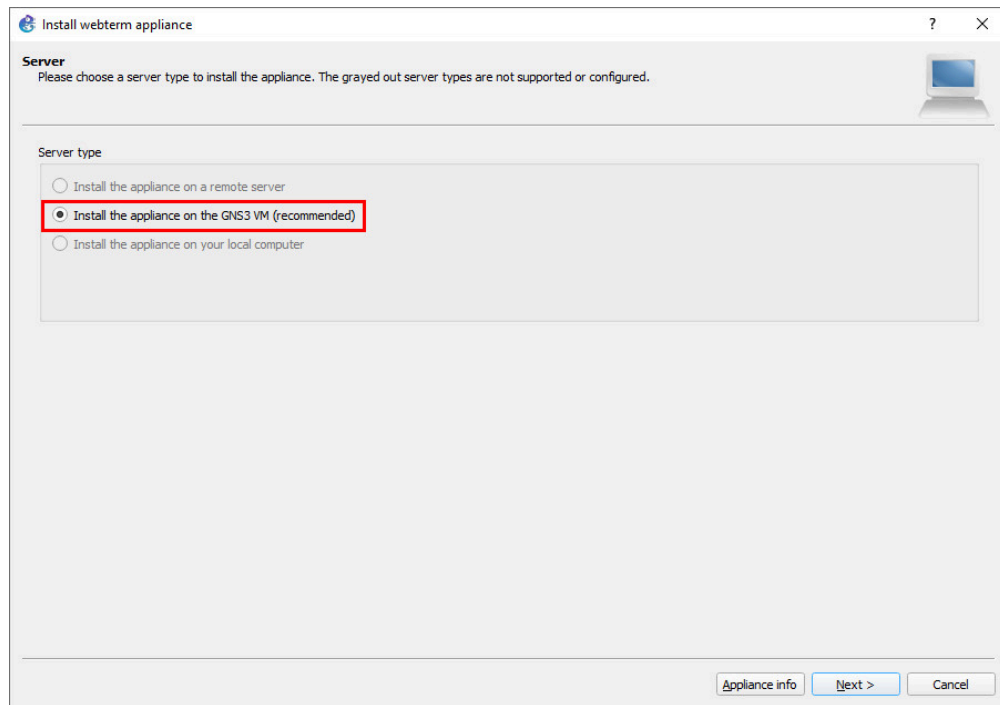


Figure A.40: Install the appliance on the GNS3 VM

5. “Next” again:

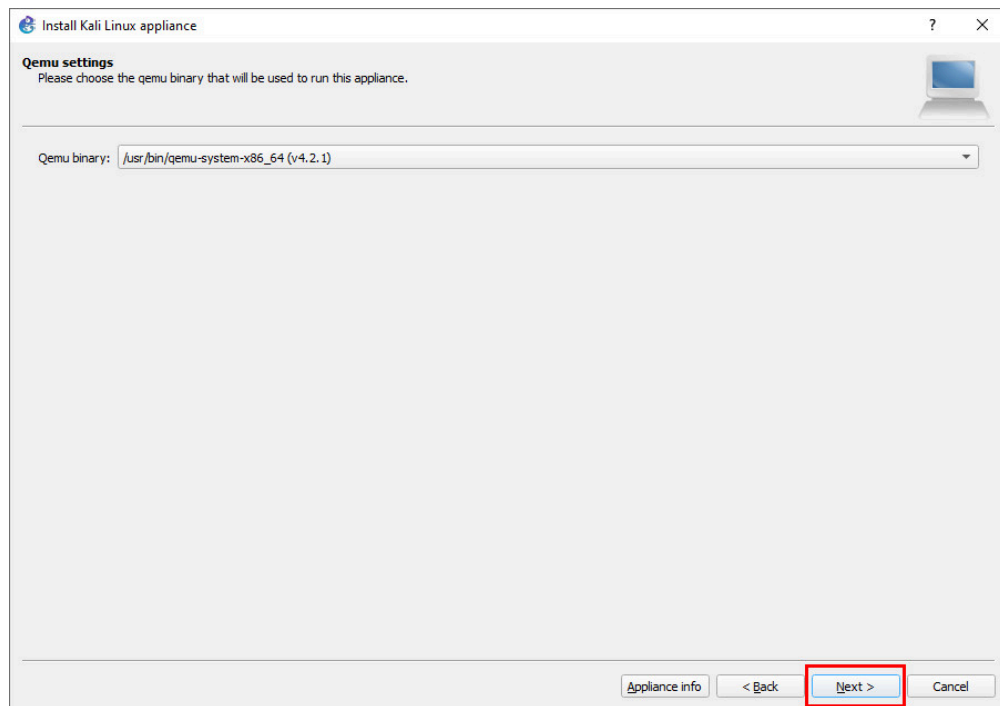


Figure A.41: Qemu binary

6. Expand the “2019” option, and download both missing files.

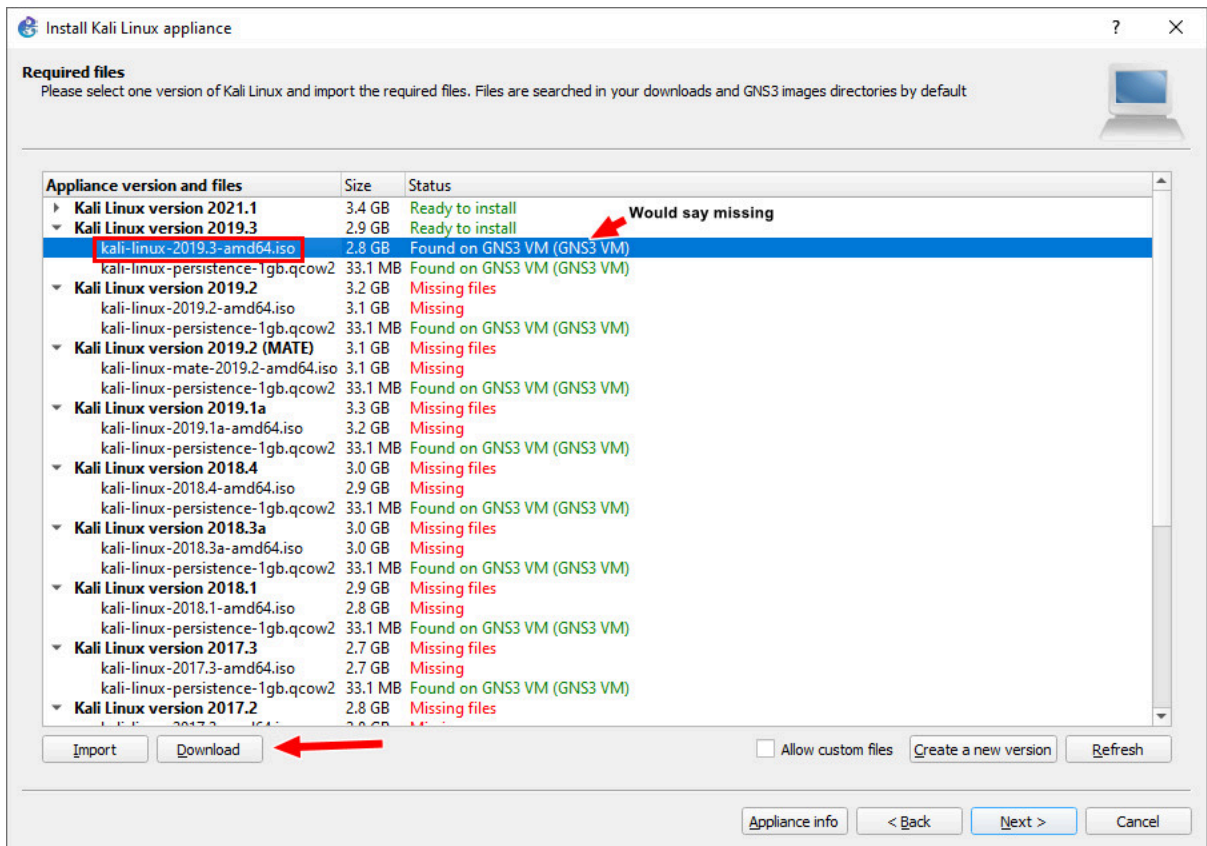


Figure A.42: Select the Kali-Linux version and then Download

- After that, import the downloaded file to the specified 2019 selection.

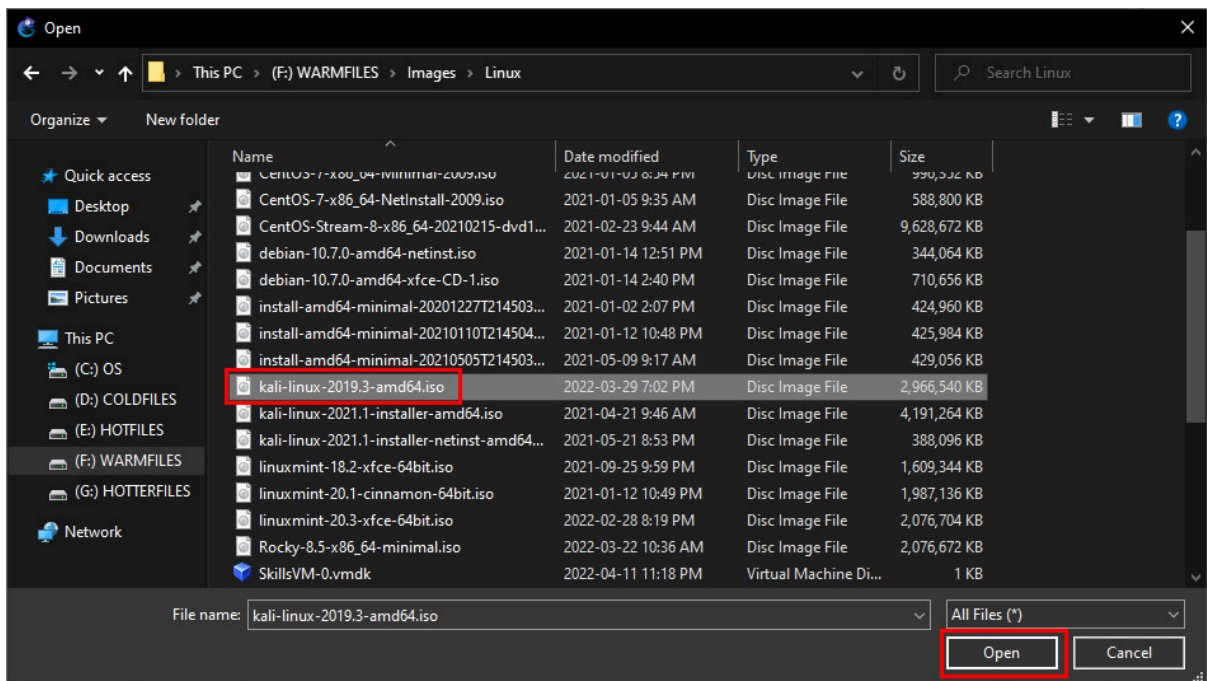


Figure A.43: Select the Kali-Linux downloaded file

- It should take a second, but GNS3 will start to load up the ISO into the GNS3 VM.

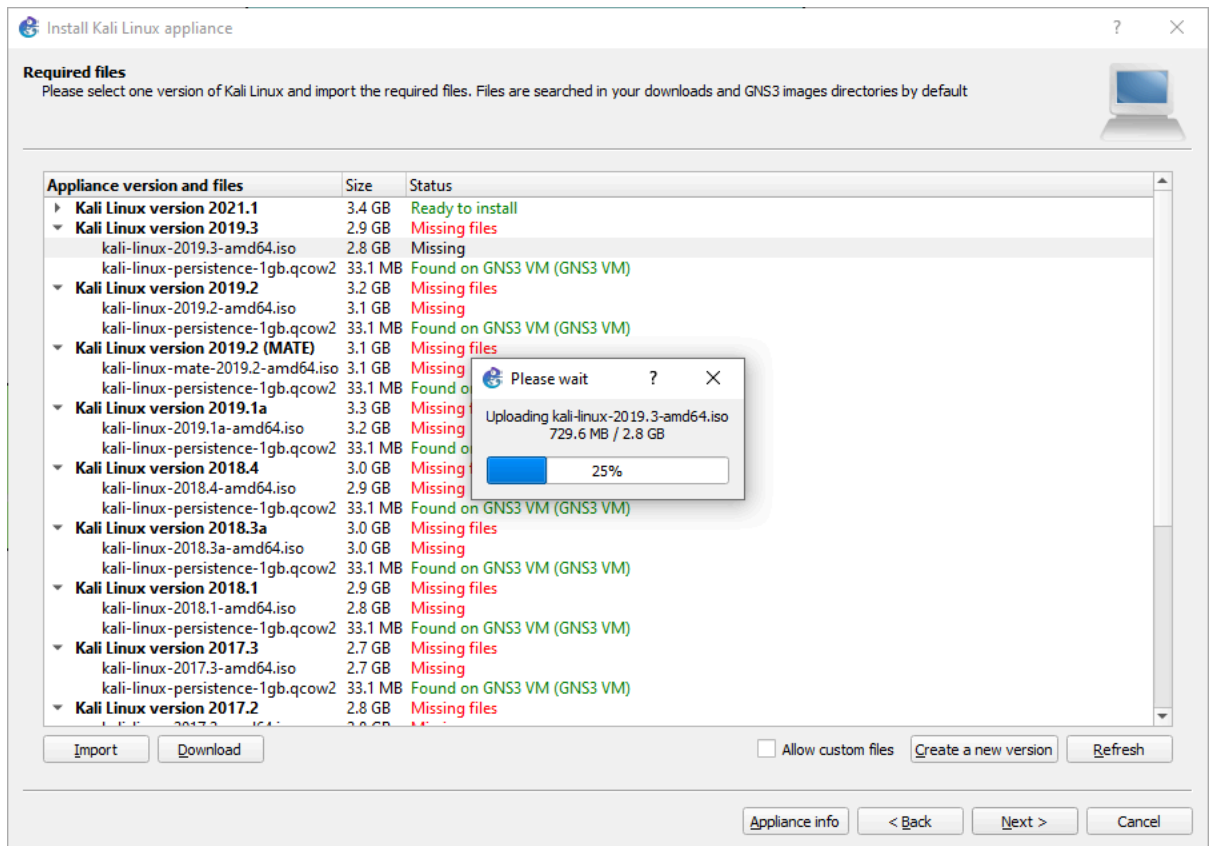


Figure A.44: Load the image

9. After that, click the 2019 version again, then click “Next.”

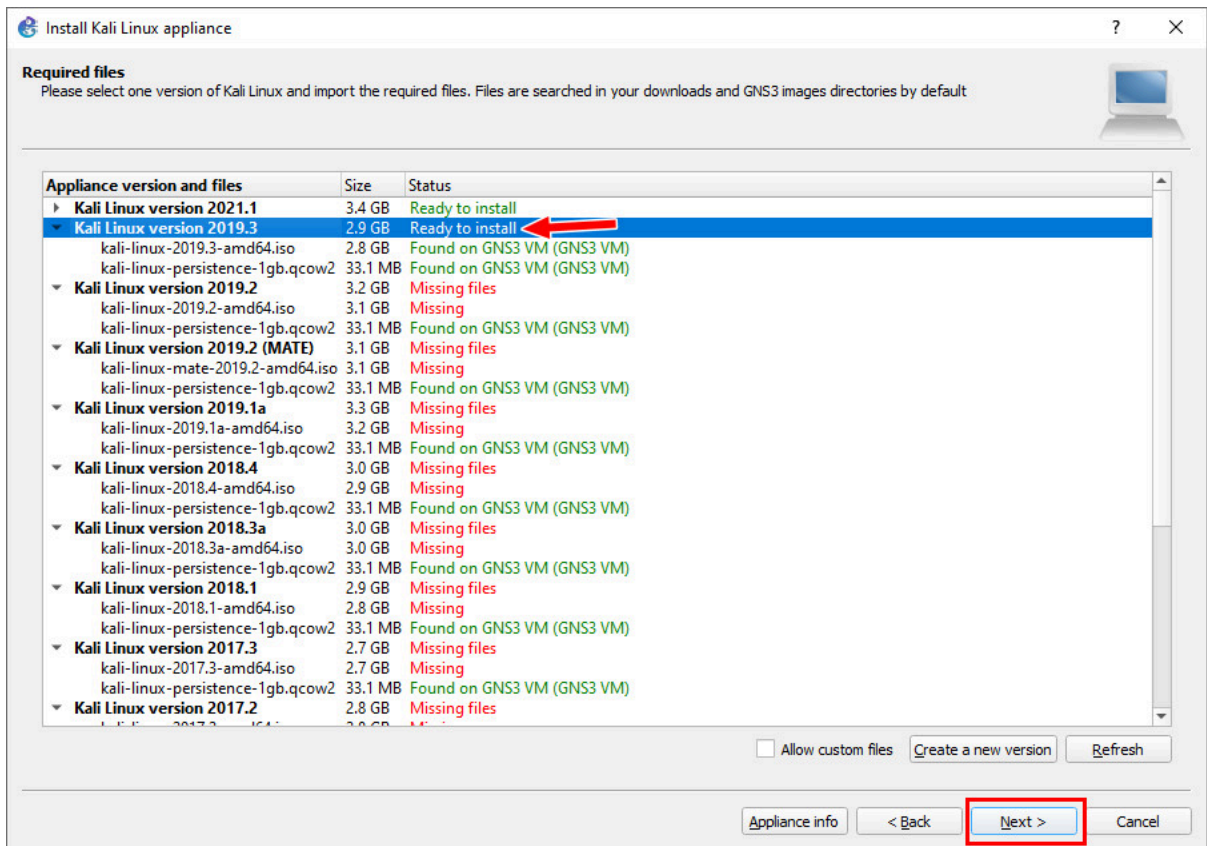


Figure A.45: Ready to install Kali 2019.3

10. Then click “Finish.”

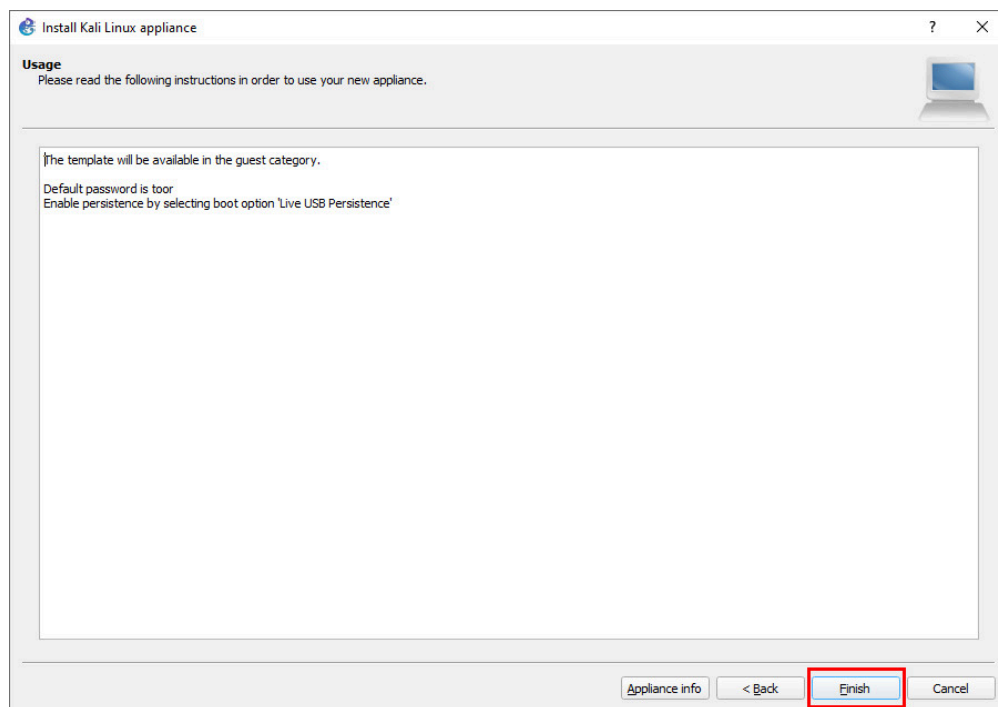


Figure A.46: Click on “Finish”

Using WordPress in GNS3

Sometimes we need a basic webserver to demonstrate website functionality. This can be accomplished using the WordPress appliance in GNS3. Start by clicking the new template button on the bottom of the page.

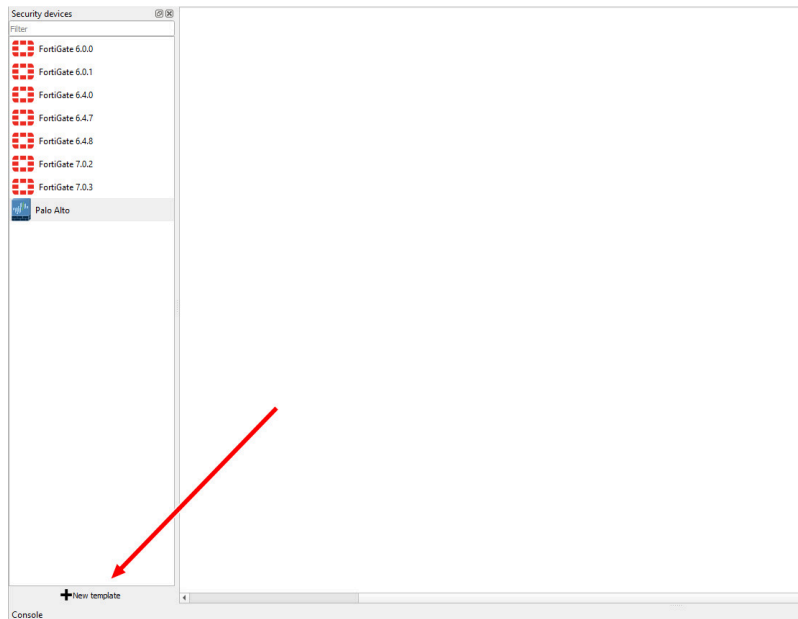


Figure A.47: Create a new template

We want to install an appliance from the GNS3 server.

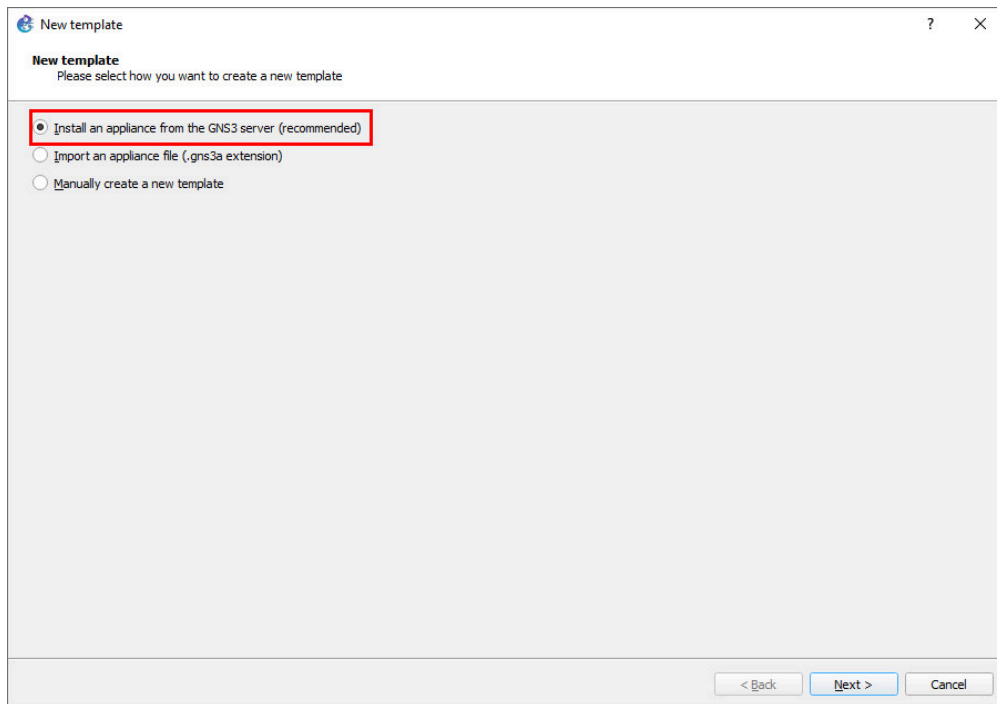


Figure A.48: Install an appliance from the GNS3 server

Look up “WordPress,” then click “Install.”

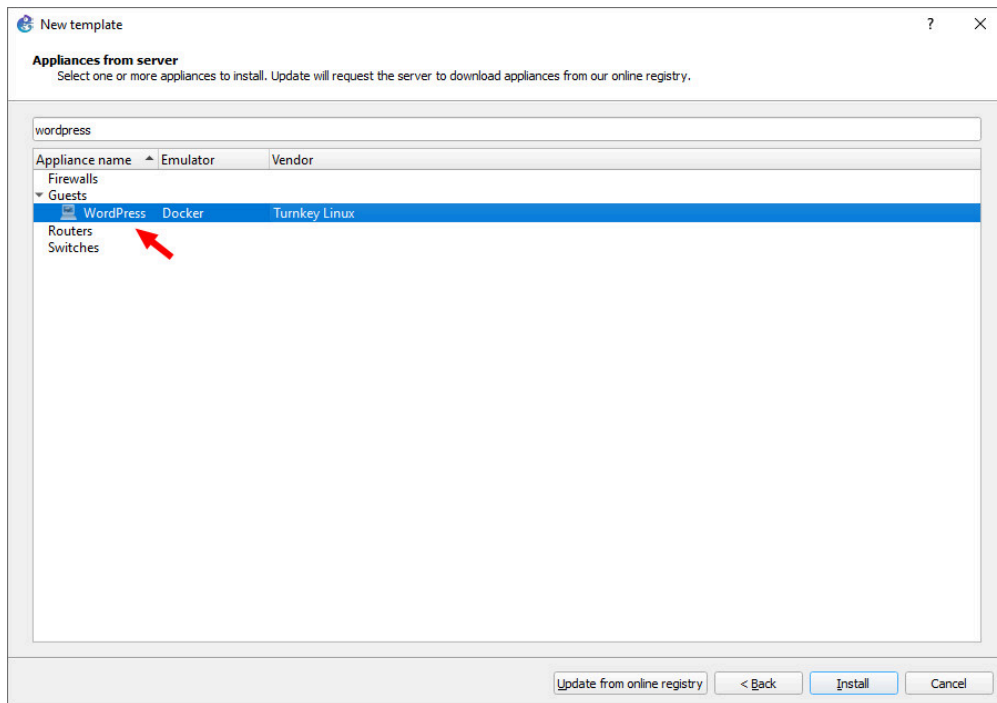


Figure A.49: Search for “WordPress”

Just press next for the following dialogue boxes, and you should now have WordPress!

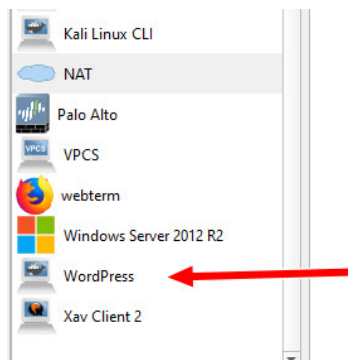


Figure A.50: WordPress installed successfully!

Running WordPress

After changing the interface configuration, start the machine. You will see a dialogue box:

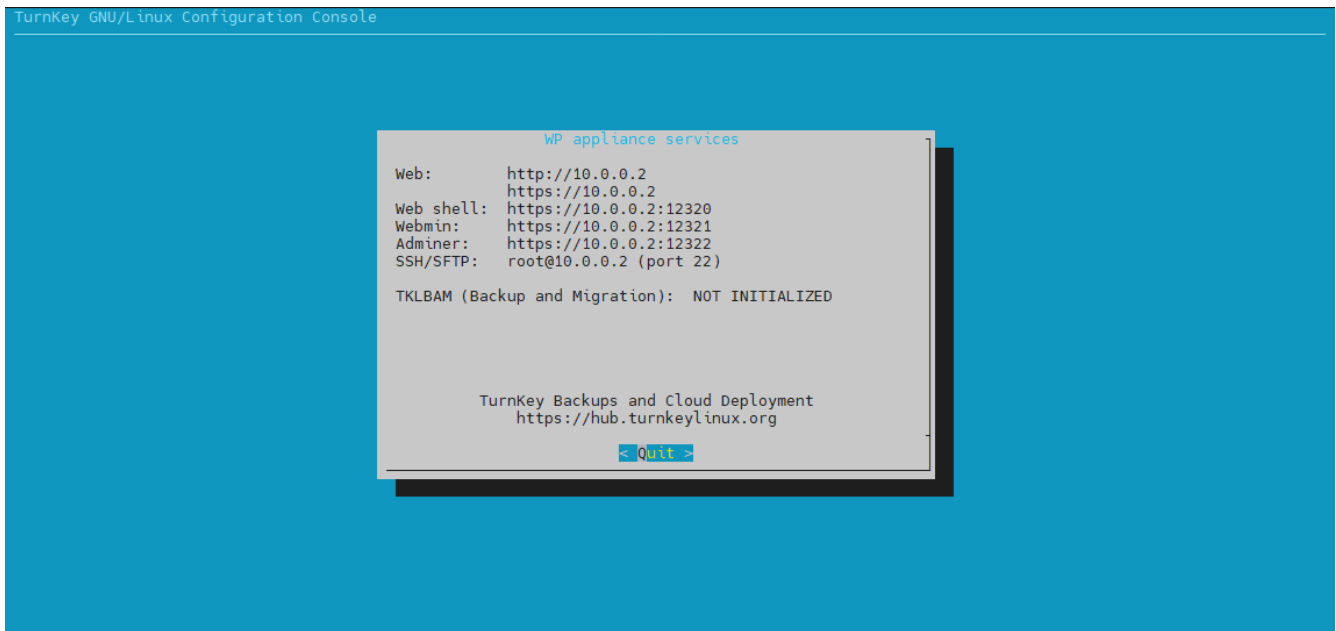


Figure A.51: Running WordPress

Press enter and you'll see the device under some basic configuration. Once you get to the prompt, you can exit that window, and you will have WordPress ready!

```
longer than 15 characters, please use --exec instead of --name.
. ok
[ ok ] Starting LVM2 poll daemon: lvmpolld.
[ ok ] Starting MariaDB database server: mysqld.
[ ok ] Starting Postfix Mail Transport Agent: postfix.
[warn] qemu-ga: transport endpoint not found, not starting ... (warning).
[ ok ] Starting enhanced syslogd: rsyslogd.
[ ok ] Starting OpenBSD Secure Shell server: sshd.
Starting TLS tunnels: /etc/stunnel/shellinbox.conf: started /etc/stunnel/webmin.conf: started
[ ok ] Starting webmin done.
System information for Mon Apr 18 08:22:27 2022 (UTC+0000)

System load:  1.35           Memory usage: 36.7%
Processes:   33             Swap usage:   0.0%
Usage of /:  12.0% of 479.62GB  IP address for eth0: 10.0.0.2

TKLBAM (Backup and Migration): NOT INITIALIZED

To initialize TKLBAM, run the "tklbam-init" command to link this
system to your TurnKey Hub account. For details see the man page or
go to:

https://www.turnkeylinux.org/tklbam

WARNING: The container requires initialization (performed on first login).
This can be performed from the host as follows:

CID=$(docker ps -l -q)
CIP=$(docker inspect --format='{{.NetworkSettings.IPAddress}}' $CID)
docker logs $CID | grep "Random initial root password"
ssh root@$CIP

WARNING: Exiting this shell will stop the container.
For regular console usage, SSH is recommended.
root@WP /# █
```

Figure A.52: WordPress is ready!

Using Switches in GNS3

Usually we just use switches to connect multiple devices together in GNS3. However, it can also be used for VLANs. Start by dragging one in and double clicking it.

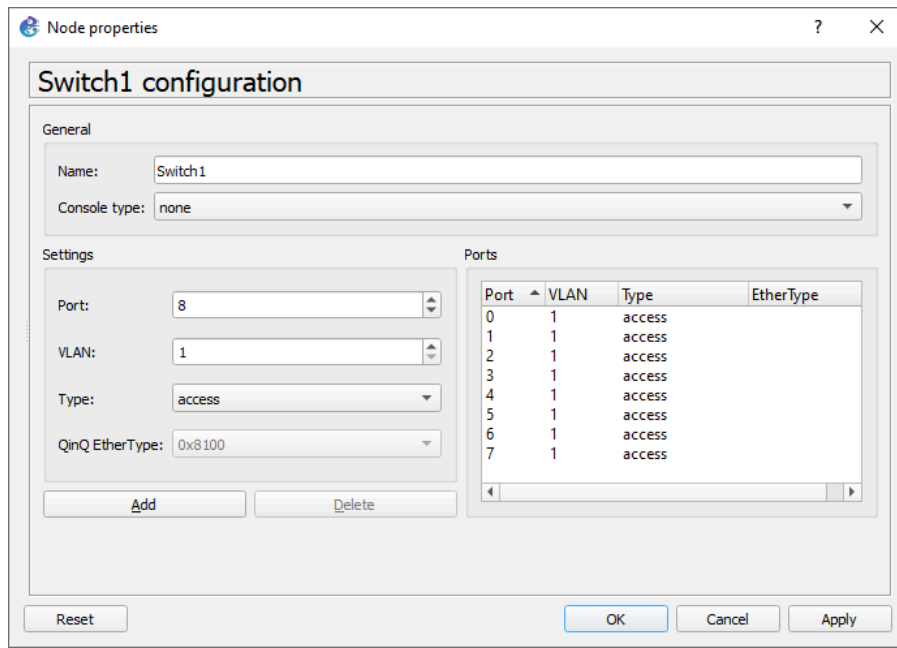


Figure A.53: Switch configuration

Here you can see that they are all basically untagged. To configure a specific port, simply double click your desired port

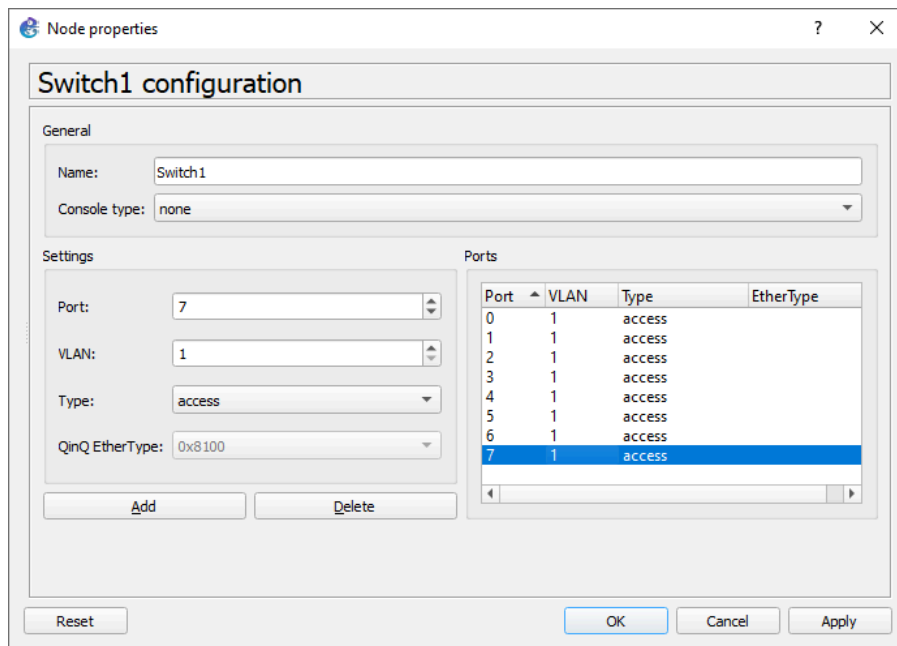


Figure A.54: Switch port configuration

Configure the necessary settings for them (access is for tagging, dot1q is for trunking).

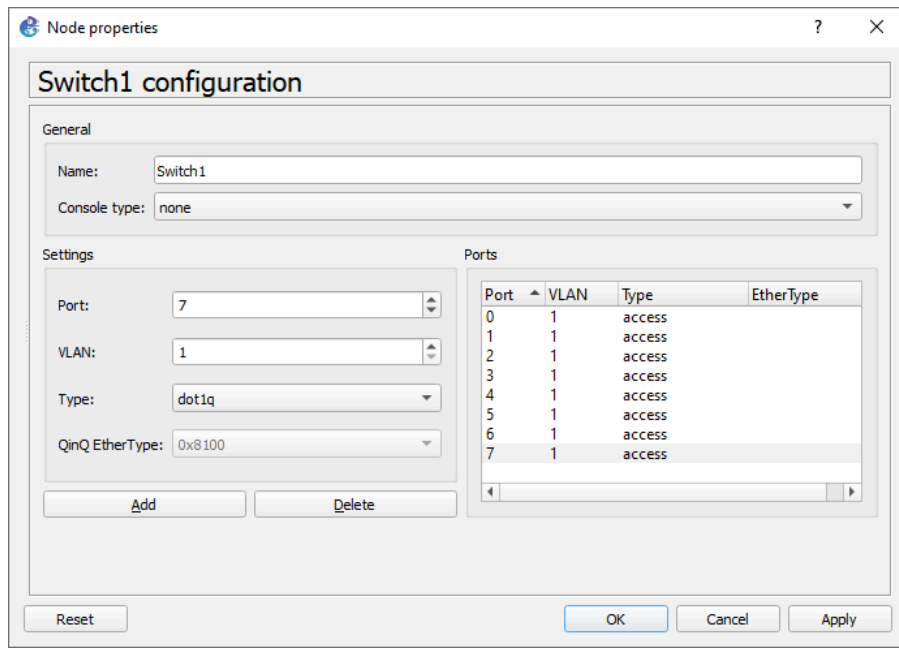


Figure A.55: Switch port configuration

Click on add to **Apply** the changes.

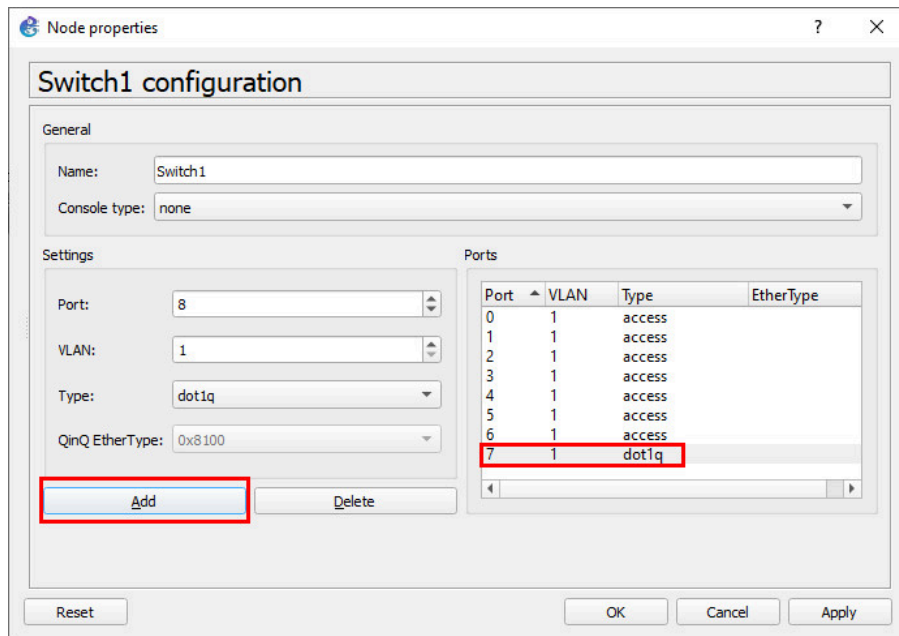


Figure A.56: Switch port configuration

Then click **Apply** and **OK**.

Acknowledgements

I would like to thank Kacem Habiballah and Tim Carson for their great support during the project. Also, I appreciate BCcampus (<https://open.bccampus.ca/>) for the financial support of this project.

I would like to thank my great students and friends Mahdad Zakaria, Michael Kheong, Xavier Cawley, Lewis Saludo, and Tung Lee for their thoughtful feedback and great suggestions during this project.

About the Author

Hamid Talebi (<https://talebi.ca/>) is an IT engineer with 14 years of experience and is a faculty member at Computer Information System Administration (CISA), School of Energy at BCIT. He has a Master of Science (MS) degree in Network Security. He has expertise and experience working with FortiGate and Palo Alto Firewalls, and SIEM software such as Qradar IBM, FortiSIEM, Splunk, and ArcSight.



Before joining BCIT, Hamid held multiple roles IT security roles with a number of reputable organizations, such as the Canadian Institute for Cybersecurity and Bell. He designed and implemented a honeynet for the CIC and created a large IPS/IDS dataset over AWS for the CSE.

He has been working in developing strong information security architectures with an Agile Project Management delivery methodology and assisting in the development of client IT and security strategies. Hamid has taught Network Security Fundamentals, Enterprise Network Security (FortiGate), Advanced Network Security (Palo Alto – Splunk – FortiSIEM), and Network Programming with Python at BCIT.

Versioning History

This page provides a record of edits and changes made to this book since its initial publication. Whenever edits or updates are made in the text, we provide a record and description of those changes here. If the change is minor, the version number increases by 0.01. If the edits involve substantial updates, the version number increases to the next full number.

The files posted by this book always reflect the most recent version. If you find an error in this book, please fill out the Report an Error (<https://collection.bccampus.ca/report-error/>) form.

Version	Date	Change	Details
1.00	August 31, 2023	Book published.	