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 <u>Creative Commons Attribution 4.0 International License</u>, 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.

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 <u>B.C. Open Collection</u>.

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" by Chanut-is-Industries is licensed under a Flaticon licence.

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

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

Visit **BCcampus Open Education** 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
<u>Chapter 3. NAT</u>	
3.1 Source NAT	51
3.2 Destination NAT	57
<u>Chapter 4. VPN</u>	
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

Versioning History

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

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 <u>web version of this resource</u> has been designed to meet <u>Web Content Accessibility Guidelines 2.0</u>, level AA. In addition, it follows all guidelines in <u>Appendix A: Checklist for Accessibility</u> of the <u>Accessibility Toolkit – 2nd Edition</u>. 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.

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

Accessibility Checklist

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: **<u>BCcampus IT Support</u>**
- Web form: <u>Report an Error</u>

This statement was last updated on August 31, 2023.

The Accessibility Checklist table was adapted from one originally created by the <u>Rebus Community</u> and shared under a <u>CC BY 4.0 License</u>.

x Hamid Talebi

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*. To download the book in a different format, look for the "Download this book" drop-down menu and select the file type you want.

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

How can	I	use	the	different	formats?
---------	---	-----	-----	-----------	----------

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.

<u>BCcampus Open Education</u> 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. <u>BCcampus</u> 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 <u>British Columbia</u> <u>Ministry of Post-Secondary Education and Future Skills</u> and the <u>Hewlett Foundation</u>.

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 <u>Creative Commons licence</u> 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 <u>BCcampus Open</u> <u>Education</u> website. If you are an instructor who is using this book for a course, please fill out our <u>Adoption of an Open Textbook</u> form.

This book was produced using the following styles: <u>FortiGate Firewall: Practical Guidance and</u> <u>Hands-On Labs Style Sheet</u> xiv Hamid Talebi

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

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.

4 Hamid Talebi

Chapter 1. Basic Settings

6 FortiGate Firewall

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.

	192 168 10 1/24	webterm-1
FG	Port1	eth0
		192.168.10.2/24

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

Pontifate-Misse-Nik e get system status Certaron: Fortiesce-VMC4-FWRG V7.0 : builders7.220714 (CA) 1012-DS. 1.00000(2018-04-09 15:07) Satisticae DB: 3.00000(2018-04-09-18:07) 27 AI/RE MADE: 0.00000(2001-01-01 00:00) ISC-DB: (.00741:2018-12-01 02:20) 526-MMD21 6.00741(2017-112-01 02:30) APP+18: 6.00041(2015-12-01-02:30) INDUSTRIED-DD: (00741(20,8-12-01 00:30) SFC Maltolous VRL Detabase: 1.00001(2015-01-01 01:01) Settal Hunder: SFREWROVR FLIEL License Ctatus: Valid Evaluation Dicense Expines: Med Mar 20 20:30:13 2020 "H Resources: I CRU/I allowed, 997 MS RAM/2048 MB allowed aldaflaya :keib bean pol Nosthama: SortiGale-VMS-6-XXA Dperacion Mode: NAT Mrrent virtuel domain: root sex number of virtual doubles: 1 Letusl domains platus: I is PAR mode, O in VP sode firtuel donain configuration: disable FIFS-CO mode: disable ussent HA soder standelone Branch point: 0167 Release Vertich Information: GA Fortion 286488: Yes Svaten vine: Woe Mar 8 20:35:38 2002 last reboor 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>

10 Chapter 1. Basic Settings

Network

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

Table 1.2: Routing and firewall policy CLI

Hardware

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

Table 1.3: Hardware CLI

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)

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

Table 1.5: NTP CLI

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
         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	Securit	y_Adn	nin_Pro	ofile					
Comments		<i>∞</i> 0/255							
Access Perm	issions								
Access Co	ontrol			Permis	sions	s Set All 🕶			
Security Fabric		0	None	Read		Read/Write			
FortiView		0	None	Read	ø	Read/Write			
User & Dev	ice	0	None	👁 Read		Read/Write			
Firewall		0	None	💿 Read		Read/Write	¢	Custom	
Log & Report		0	None	Read		Read/Write	¢	Custom	
Network		0	None	Read		Read/Write	0	Custom	
System		0	None	Read		Read/Write	¢	Custom	
Security Pro	ofile	0	None	Read	1	Read/Write	¢	Custom	
VPN		0	None	Read	B ¹	Read/Write			
WAN Opt &	Cache	0	None	Read		Read/Write			
WiFi & Switch		0	None	Read		Read/Write			

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.

Username	admin2			
Туре	Local User			
	Match a user on a remote serve	er group		
	Match all users in a remote ser	ver group		
	Use public key infrastructure (PKI) group		
Password	****	۲		
Confirm Password	****	۲		
Comments	Write a comment		0/255	
Administrator profile	Security_Admin_Profile	+		
Restrict login to tru	usted hosts			
Restrict admin to g	uest account provisioning only			

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

16 Chapter 1. Basic Settings

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**.

Username	Catenbe	A Change Decouverd
Tree	dummz	 Change Password
туре	Match a user on a remote sector group	
	Match all users in a remote server group	
	Use public key infrastructure (PKI) group	-
Comments	Write a comment	/ 0/255
Administrator pr	ofile Security Admin Profile	0/200
C Restrict login Trusted Host 1	to trusted hosts 192.168.10.100/32	
	0	
Restrict adm	in to guest account provisioning only	

3. Click **OK** to save the changes.

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.)

Dashbolind System Stettings Network Host name Hast name Hamid Socurity Profiles System Time VVN Sectings VIFI Controller Set Time System Set Time Set Time Set Time Set Tine Set Time Set Time Set Time Shy Dort 2022/03/25 11:07:02 Three 2009 Set Time USE Consola Set Time Set Time Set Time Set Time Shy Dort 2022/03/25 11:07:02 Minutes (1 - 1440) Set Time Set Time Set Time Set Time Shy Dort 2022/03/25 11:07:02 Minutes (2 - 1440) Set Time Set	FGVM01TM19008000	• = Q					
 Network System Time Current system time 2022/03/25 f1:07:02 Current system time Set Ti	Dashboard	> System Settings					
▲ Scourity Profiles > > VPN > ▲ User & Authentication > ♥ WFI Controller > > System 1000 > ♥ WFI Controller > > Security Profiles > > System 1000 > > Security Profiles > > System 1000 > > Security Profiles > Profile > Profile > Profile # Profile # > Security Fabric > > >	 Network Policy & Objects 	> Host name Hamid					
WIFI Controller System Administrators Firmware 1 Fabric Management Administration Settings HTTP part Replacement Messages FortiGuard FortiGuard HTTPS port HTTPS server certificate Self-sign You are using a default built-in certificate, which will not be able to verify your server's demain me (your users will see a worring). Let's Encrypt on the port SH Dort Create Certificate SSH port SH port SSH port 2424 Teinet port <td>Security Profiles VPN User & Authentication</td> <td>System Time Current system time</td> <td>200</td> <td>22/03/29 11:07:02</td> <td></td> <td></td> <td></td>	Security Profiles VPN User & Authentication	System Time Current system time	200	22/03/29 11:07:02			
Administrators Select server Administrators Solucion (Construction) Administrators 60 Administrators 60 Setup device as local NTP server Isten on Interfaces Firmware Isten on Interfaces Fabric Management Administration Settings HA Administration Settings HA Administration Settings Replacement Messages HTTP port FortiGuard Port conflicts with the SSL-VPN port setting Certificates Port conflicts with the SSL-VPN port setting W Log & Report Variance using a default bull-tin certificate, which will not be able to verify you are using a default bull-tin certificate if you do not have. one. Used S Report SSH point Zedat Teinet port SSH point 2424 Teinet port 1313	⇔ WiFi Controller	> Set Time	(GMT-8:00) Pacific Time (US & Canada) NTP PTP Manual settings				
Firmware 1 Fabric Management Settings HA SNMP Replacement Messages FortiGuard Feature Visibility Certificates Security Fabric HTTPS server certificate Fostion of the state to verify your server's domain mame (your users will see a warring): Let's Encrypt your server's domain mame (your users will see a warring): Let's Encrypt of the state to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your users will see a warring): Let's Encrypt of the set to verify your server's domain mame (your userver wille	Administrators Admin Profiles	Select server Sync interval Setup device as local NTP se	Select server FortiGuerd Custom C Syncinterval 60 Setup device as local NTP server C				
Sectings 17 HA Administration Settings HA SNMP Replacement Messages HTTP port 60 FortiGuard 1 Peature Visibility Image: Certificates Socurity Fabric > HI Log & Report Administration Settings HI Log & Report > SSH port 2424 Telnet port 1313	Firmware 1 Fabric Management	Listen on Interfaces	9	• fartilink •	×	ĸ	
Certificates Security Fabric HTTPS server certificate Image: Security Fabric HTTPS server certificate Vou are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt one. Create Certificate SSH port Zet4 Telnet port	HA SNMP Replacement Messages FortiGuard	Administration Settings HTTP part Redirect to HTTPS HTTPS part	•	80 443			
Eff Log & Report You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt one. Can be used to easily generate a trusted certificate if you do not have one. SSH port 2424 Teinet port 1313	Certificates Security Fabric	> HTTPS server certificate		A Port conflicts with th	e SSL-VPN p	etting	
SSH port 2424 Teinet port 1313 \$	별 Log & Report			You are using a defau your server's domain can be used to easily one. Create Certificate	it built-in ce name (your generate a b	stificate, which will not be able to verify users will see a warning! Let's Encrypt rusted certificate if you do not have	
All Alizability of Al		SSH port Telnet port		2424 1313			

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

18 Chapter 1. Basic Settings

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.

Backup System Config	guration
Backup to Encryption Password	Local PC USB Disk
Confirm password	

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	im port3									
Alias										
Туре	Physical Interface	Physical Interface								
VRFID 0	0									
Role 0	Undefined	•								
Address										
Addressing	mode Manual DF	HCP Auto-managed b	y IPAM One-	Arm Sniffer						
IP/Netmask	192.168.1.1/	/24								
Secondary II	Paddress 🔾									
Administrati	ive Access									
IPv4		T HTTP 6								
	FMG-Access	□ SSH								
	G FTM		Accounting	Security Fabric						
	Speed Test			Connection						
Receive LLD	P 1 Use VDOM Setting	Enable Disable								
Transmit LLI	DP 1 Use VDOM Setting	Enable Disable								
C DHCPS	erver									
DHCP statu	s 🕜 Enabled 🔮 Dis	sabled								
Address ran	ge 192.168.1.20-192.1	68.1.30								
	C)								
Netmask	255.255.255.0									
Default gate	way Same as Interface IP	Specify								
DNS server	Same as System DNS	S Same as Interface IF	Specify							
Lease time	604800	second(s)								

Figure 1.11: Enable DHCP Server

20 Chapter 1. Basic Settings

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 <u>FortiGate document library</u> has full resources.

Resources

- Fortinet Fortigate CLI Commands
- FortiGate document library

Chapter 2. Policy

22 FortiGate Firewall

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




Table 2.1: Devices configuration

Device	Configuration			
FortiCata	Port 2: DHCP Server			
FortiGale	Port 3: DHCP Client			
WebTerm	DHCP Client			

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

FGVM01TM19008000	<pre># config system interface</pre>
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

FGVM01TM19008000	≡ Q.				>	0 -	42.
🕰 Dashboard 🔶	Edit Interface						
🕂 Network	C DHCP Server	C DHCP Server					
Interfaces 😭	DHCP status	🖸 Enabled 🔮 Disa					
DNS	Address range	192.168.1.20-192.16	8.1.30				
Packet Capture		0					
SD-WAN	Netmask	255.255.255.0					
Static Routes	Default gateway	Same as Interface IP	Specify				
Policy Routes	DNS server	Same as System DNS	Same as Interface IP	Specify			
RIP	DNS server 1	4.2.2.4	×				
OSPF		0					
BGP	Lease time 🕄 🔘	604800	second(s)				
Routing Objects							
Multicast	Advanced						
Policy & Objects							
Security Profiles	Network						
□ VPN >	Device detection	0					
Luser & Authentication	Security mode	0					

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

Figure 2.4: Enable DHCP Server

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

Address					
Addressing mode	Manual	DHCP	Auto-mana	ged by IPAM	One-Arm Sniffer
Retrieve default gateway from s	server 🔘				
Distance	5		k		
Override internal DNS	0				

Figure 2.5: Enable DHCP Client

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

Destination 1	Subnet Internet Service	
	0.0.0/0.0.0	
Gateway Address 🕄	Dynamic Specify	
	192.168.122.1	
Interface	m port3	×
Administrative Distance 🜖	10	<
Comments	Write a comment	0/255
Status	Enabled ODisabled	0,200
Advanced Options		

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

Name	mylocal			
Color	E Change			
Туре	Subnet	-		
P/Netmask	192.168.1.0/24			
nterface	🗆 any	-		
Static route configurati	on 🕥			
Comments	Write a comment	// 0/255		

Figure 2.7: Set local subnet

Network	>		
Policy & Objects	Vame 1	LocalToInternet	
Firewall Policy	☆ Incoming Interface	m port2	*
IPv4 DoS Policy	Outgoing Interface	m port3	•
Addresses	Source	I mylocal	×
Internet Service Database	Destination	+	×
Services	Schedule		
Schedules	Scriedule		
Virtual IPs	Service	DNS HTTP	×
IP Pools		HTTPS	×
Protocol Options		PING	×
Traffic Shaping	Action		
Security Profiles	>	ACCEPT O DENT	
2 VPN	> Inspection Mode	Flow-based Proxy-based	
User & Authentication	>		
WiFi Controller	> Firewall / Network	Options	
FURTIDET		OK	Cancel

- 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.

		😵 webterm-1 interfaces	?	×
s. 15.2 and PyQt 5. 15.4.	Node Web Gene Name Start Adap Custa Cons VNC 1 HTTP HTTP Envir (KEY: Netw Reset	<pre># # This is a sample network config uncomment lines to configure the network # # Static config for eth0 #auto eth0 #auto eth0 inet static # address 192.168.0.2 # netmask 255.255.255.0 # gateway 192.168.0.1 > /etc/resolv.conf # DHCP config for eth0 auto eth0 face eth0 inet dhcp</pre>		
		Refresh	Save	Cancel

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 traff	c.
--	----

FGVM01TM19008000	= Q,						>_	0· 40-	💄 admin +
Dashboar , v Status	FortiView	Sessions						now •	0 1-
Security	O Add Filt	er							
Network	Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	
Users & Devices	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	
FortiView Sources	192.168.1.2		4.2.2.4	UDP/53	UDP	51594	53	171 B	
FortiView Destinations	192.168.1.2		4.2.2.4	UDP/53	UDP	52754	53	251 B	
FortiView Applications	192.168.1.2		4.2.2.4	UDP/53	UDP	53934	53	251B	
FortiView Web Sites	192.168.1.2		4.2.2.4	UDP/53	UDP	52974	53	278 B	
Fortiview Policies	192.168.1.2		4.2.2.4	UDP/53	UDP	54356	53	162 B	
Fortiview Sessions #	192.168.1.2		4.2.2.4	UDP/53	UDP	57184	53	266 B	
+ Network	192.168.1.2		34.120.237.76	TCP/443	TCP	60838	443	135.04 kB	
Policy & Objects	192.168.1.2		■ 4.2.2.4	UDP/53	UDP	37632	53	266 B	
Security Profiles	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	
🚨 User & Authentication 🔹 🕽	192.168.1.2		4.2.2.4	UDP/53	UDP	43104	53	159 B	
🕆 WiFi Controller	192.168.1.2		4.2.2.4	UDP/53	UDP	43286	53	266 B	
🏟 System 💼 🗴	192.168.1.2		4.2.2.4	UDP/53	UDP	44476	53	245 B	
🔆 Security Fabric	192.168.1.2		4.2.2.4	UDP/53	UDP	46612	53	169 B	
년 Log & Report	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.**

30 Chapter 2. Policy

FGVM01TM19008000	≡Q				>_ 🕢 🗘 🔁 - 👤 admin -
🙆 Dashboard	Edit Policy				
Network				Statistics (since last re-	set)
🛓 Policy & Objects 🔷	Name 0	LocalToInternet		ID	
Firewall Policy	Incoming Interface	m port2	-	10	1
IPv4 DoS Policy	Outgoing Interface	m port3	•	Last used	57 second(s) ago
Addresses	Source	🖀 mylocal	×	Firstused	1 minute(s) ago
Internet Service Database	Destination	🗉 all	×	Active sessions Hit count	76
Services	Schedule	+		Total bytes	10.80 MB
Schedules	Service	DNS	×	Current bandwidth	Obps
Virtual IPs	Service	HTTP	×		
IP Pools		HTTPS	×	Clear Counters	5
Protocol Options		PING +	×		
Traffic Shaping	Action	✓ ACCEPT Ø DENY		Last 7 Days Bytes -	
Security Profiles				15 MB	
D VPN	Inspection Mode	Flow-based Proxy-based		10 MB	
💄 User & Authentication 🔹 🕨					
☆ WiFi Controller	Firewall / Network O	ptions		5 MB	
🗘 System 💶 🕨	NAT	0		OR	
🔆 Security Fabric	IP Pool Configuration	Use Outgoing Interface A	Address Use Dynamic IP Pool	Mar 26 Mar 2	7 Mar 28 Mar 29 Mar 30 Mar 31 Apr 01
년 Log & Report	Preserve Source Port	0			
	Protocol Options	enor default	- 1		
	Increase the second			Additional Informatio	h
	Security Profiles			D API Preview	
FORTIDET V7.0.	3		OK Can	cel	

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.

2.1 Security Policy 31



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>
Enable this policy	<enable></enable>

FGVM01TM19008000	•	≣ Q,		
🕰 Dashboard	>	Edit Policy	F	
Network	>	*		
占 Policy & Objects	~	Name 0	Block_Ping	
Firewall Policy	☆	Incoming Interface	m port2	-
IPv4 DoS Policy		Outgoing Interface	m port3	•
Addresses		Source	I mylocal	×
Internet Service Database		Destination	all	×
Services			+	
Schedules		Schedule	L o always	-
Virtual IPs		Service	PING +	×
IP Pools		Action	✓ ACCEPT Ø DENY	
Protocol Options				
Traffic Shaping				
A Security Profiles	>	C Log Violation Tr	affic	
I VPN	>	Comments Write	e a comment	
💄 User & Authentication	>	Comments With	@ 0/1023	
🗢 WiFi Controller	>	Enable this policy	D	
🔹 System	1 >			

Figure 2.14: Set firewall policy to block ping

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

+ Create New	de Edit	Delete	Q Policy Looku	p Search				Q
Export •	nterface Pair V	/iew By Seque	nce					
Name	Source T	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
🖃 🖩 port2 → 🖩	port3 2			-				
Block_Ping	🔳 mylocal	🔳 all	Co always	PING	Ø DENY			O AI
LocalToInternet	😐 mylocal	💷 all	Co always	DNS HTTP HTTPS PING	✓ ACCEPT	Enabled	sst no-inspection	0 0

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

34 Chapter 2. Policy

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

lew Applica	ation Sensor		
	0 93 0 p	Cloud A olicies a	pplications require deep inspection. re using this profile.
Name	Ban-SocialNetwork		
Comments	5	1. 0/2	255
C			
Categories			
• All C	Categories		
 ● ■ Bus 	iness (179, 🗅 6)	٠.	Cloud.IT (31)
 Col 	laboration (293 , 🗅 6)	٠.	Email (87, 🗅 12)
 ● Gai 	me (124)	•	General.Interest (241, 🛆 9)
👁 • Mo	bile (3)	•	Network.Service (332)
Ø . P2	P (85)	0-	Proxy (106)
 ● + Rer 	mote.Access (91)	0-	Social.Media (150 , 🗅 31)
 ● + Sto 	rage.Backup (296 , 🗅 16)	۰ گ	Update (48)
Ø- Vid	eo/Audio (206 , 🗅 13)	٠)	VoIP (31)
👁 - We	b.Client (18)	0.	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

۹				>_	0· 40-	\rm admin
Edit / Edit C	Verride					>
🥙 Туре	Application	Filter				
Action	Block -					
	Add All Results	YouTube		×	Q Selected	All Clou
0	Na	ame 🕏	Category #	Technology ≑	Popularity 🕏	Risk ‡
	pplication Signatu	ıre 16/2185				
App	YouTube		Video/Audio	Browser-Based	*****	
10	YouTube.D	ownloader.YTD	Video/Audio	Client-Server	*****	
4	YouTube_C	Category.Control	Video/Audio	Browser-Based	*****	
1	C YouTube_C	hannel.Access 🗅	Video/Audio	Browser-Based	*****	
	YouTube_C	hannel.Control 🕰	Video/Audio	Browser-Based	*****	
	YouTube_C	hannel.ID 🗅 🔒	Video/Audio	Browser-Based	*****	
	YouTube_C	Comment.Posting	Video/Audio	Browser-Based	考查自自自	
	YouTube_H	ID.Streaming	Video/Audio	Browser-Based	*****	
-	YouTube_N	Aessenger 🔒	Social.Media	Browser-Based	*****	
Opt	YouTube_S	earch.Safety.Mode	Video/Audio	Browser-Based	****	-
Bloc	YouTube_S	earch.Video 🔒	Video/Audio	Browser-Based	*****	-
Allo	YouTube_V	/ideo.Access 🗅 🔒	Video/Audio	Browser-Based	*****	
QUI					09	6 T 16/2.18
			OK	Cancel		

Figure 2.18: Block YouTube

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

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

≡	۹	k					0-	4 2 -	💄 ad	imin +
+1	Edit /	Edit Override								×
B		Type Ap	plication	Filter						
	۲	Action Ø	Block +							
	0	Add All F	Results	+ Add Selected	facebook	×	Q	Selected 🚺	All	Cloud
	۲	0	Na	me ≑	Category #	Technology 🕏	Pop	ularity 🛱	Risk ‡	;
Inc	۲	 Application 	on Signatu	re 27/2185						
For	0	0 F	acebook		Social.Media	Browser-Based	**	***	-	
	۲		acebook	AppName	Social.Media	Browser-Based	*9	000		1.1
	0	f F	acebook_	Apps	Social.Media	Browser-Based	**	***	-	7
Tel la		f F	acebook_	Chat 🛆 🔒	Social.Media	Browser-Based	**	**0	-	1
	App	f F	acebook_	File.Download 🕰	Social.Media	Browser-Based	**	000		7
		. ₽ F	acebook	File.Upload 🗅 🔒	Social.Media	Browser-Based	**	*22		
	1	f F	acebook	Like.Button 🔒	Social.Media	Browser-Based	**	***	1000	
	11.	f F	acebook_	Login 🗅 🔒	Social.Media	Browser-Based	**	000	-	
		😄 F	acebook_	Messenger,Image	Collaboration	Client-Server	**	*00		
		C F	acebook_	Messenger.Video.T	Collaboration	Client-Server	**	*29		
		😑 F	acebook_	Messenger.VolP.Call	Collaboration	Client-Server	**	*22		
	14	😑 F	acebook_	Messenger.Voice	Collaboration	Client-Server	**	*24		
	Opt							0%	T 27/	/2,185
1.5					ОК	Cancel				

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.

Network	>					1 4224	
Policy & Objects	. 9	8 Source	Destination	Application Name	Action	Application User	App
Security Profiles	\$	192.168.1.2	142.251.46.195 (fonts.gstatic.com)	G Google.Services	pass		
		192.168.1.2	142.251.46.195 (fonts.gstatic.com)	SSL .	pass		
Luser & Authentication	>	192.168.1.2	142.250.191.78 (apis.google.com)	YouTube	block		
🗢 WiFi Controller	>	192.168.1.2	142.251.46.234 (fonts.googleapis.c	G Google.Services	pass		
🗘 System		192.168.1.2	142.251.46.234 (fonts.googleapis.c	SSL SSL	pass		
🔆 Security Fabric	- >	192.168.1.2	172.217.6.78 (www.youtube.com)	 YouTube 	block		
네 Log & Report	~	192.168.1.2	34.120.237.76 (img-getpocket.cdn	HTTPS.BROWSER	pass		
Forward Traffic		192.168.1.2	34.120.237.76 (img-getpocket.cdn	SSL	pass		
Local Traffic		192.168.1.2	34.120.237.76 (img-getpocket.cdn	2 HTTPS.BROWSER	pass		
Sniffer Traffic		192.168.1.2	34.120.237.76 (img-getpocket.cdn	SSL SSL	pass		
Events		192.168.1.2	157.240.22.35 (facebook.com)	Facebook	block		
AntiVirus		192.168.1.2	157.240,22.35 (facebook.com)	SSL .	pass		
Web Filter		192.168.1.2	157.240.22.35 (facebook.com)	Facebook	block		
SSL		192.168.1.2	157.240.22.35 (facebook.com)	SSL SSL	pass		
UNS Query		192.168.1.2	157.240.22.35 (facebook.com)	Facebook	block		
Application Control	~	192.168.1.2	157.240.22.35 (facebook.com)	SSL.	pass		
Intrusion Desugation	м	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

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

Table 2.3: Devices Configuration

- 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:

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

Table 2.4: Create a new Address for WebTerm3

ich rhad coo		
*	In the second	
Name	WebTerm3	
Color	E Change	
Туре	Subnet 👻	
IP/Netmask	192.168.1.21/32	
Interface	🗆 any 🔻]
Static route configurat	ion 👁	
Comments	Write a comment	5
Lomments	Write a comment M 0/255	5
	OK C	ncol

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.

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

42 Chapter 2. Policy

FGVM01TM19008000	- ≡ Q					
🙆 Dashboard	> New Tra	ffic Shaper				
🕂 Network	>	Charad Dev ID Charac				
💄 Policy & Objects	~ News	Shared Per IP Shaper				
Firewall Policy	Name	WebTerm3				
IPv4 DoS Policy	Quality	of Service				
Addresses	Bandwi	dth unit		kbps		•
Internet Service Database	Maxim	um bandwidth	0	10000	~	kbps
Services	Max co	ncurrent connections	0	5000		~
Schedules	Max co	ncurrent TCP connections	•			
Virtual IPs	Max co	ncurrent UDP connections	0			
IP Pools	Forwar	d DSCP	0			
Protocol Options	Reverse	e DSCP	•			
Traffic Shaping						
Security Profiles	>					
₽ VPN	>					
User & Authentication	>					
🗢 WiFi Controller	->			OK	Car	ncel

Figure 2.25: Set traffic shaping

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

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

Name	WebTe	erm3Pc	licy				Additional Information
Status	🖸 Ena	abled	O Disabled				API Preview
Comments	Write	acomm	ient	<i>a</i> 0/255			⑦ Documentation
If Traffic Mat	tches:						 Online Help II Video Tutorials I
Source		Web	Ferm3 +		×		
Destination	1	all	+		×		
Schedule	•						
Service	G	ALL	+		×		
Application	0		+				
URL Categor	γ		+				
Then:							
Outgoing int	erface		i port3	+		×	
Apply shape	r	•					
Shared sha	per	•					
Reverse sha	aper	•					
Per-IP shap	ber	0	WebTerm3			•	
Assign shapii	ng class I	D O					

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.

FGVM01TM19006000	= Q				>_ @• Q 0
Dashboard	Edit Policy				
Network				Statistics (since last res	et)
Policy & Objects	Name 0	WebTerm3		ID	3
Firewall Policy	Incoming Interface	port2	-		5
IPv4 DoS Policy	Outgoing Interface	i port3	•	Lastused	N/A
Addresses	Source	WebTerm3	×	Firstused	N/A
Internet Service	***	+		Active sessions	0
Database	Destination	all +	×	Hitcount	0
Services	Schedule	Co always		Total bytes	OB
Schedules	Service	DNS	×	Current bandwidth	Obps
Virtual IPs	10000	I HTTP	×		
IP Pools		HTTPS	×	Elear Counters	
Protocol Options		PING +	×		
Traffic Shaping	Action	✓ ACCEPT Ø DENY		Additional information	
Security Profiles			4	Additional miterimation	
⊒ VPN >	Inspection Mode	Flow-based Proxy-based		API Preview	
្ម User & Authentication រ				>_ Edit in CLI	
WiFi Controller	Firewall/Network O	ptions		() Demotration	
🗘 System 👔 🕽	NAT	0		Documentation	
Security Fabric	IP Pool Configuration	Use Outgoing Interfa	ice Address Use Dynamic IP Pool	Video Tutorials	2
Log & Report	Preserve Source Port	0		Consolidated Poli	icy Configuration
	Protocol Options	resor default	- 1		
	Security Profiles				
EDBTIDET			OK Can	cel	

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.

dit Applicatio	on Sensor			
Name	WebTerm3			
Comments h		<i>la</i> 0/25	5	
Categories				
Ø- All Cat	regories			
🖉 🕶 Busin	ess (153, 🛆 6)	Ø• 0	loud.IT (66, 🛆 1)	🖉 🕶 Collaboration (268, 🛆 16)
🖉 🕶 Email	(77, 🛆 12)	0 - 0	ame (86)	🖉 🕶 General.Interest (233, 🛆 8)
🖉 • Mobi	le (3)	Ø - N	letwork.Service (333)	⊘ ▼ P2P (56)
Ø . Proxy	(174)	0 - R	emote.Access (95)	🖉 🕶 Social.Media (118, 🛆 32)
Ø + Stora	ge.Backup (161, 🗅 19)	Ø - U	Ipdate (49)	🖉 🔻 Video/Audio (155 . 🗅 17)
Ø ▼ VoIP (23)		0 - v	Veb.Client (24)	⊘ ▼ Unknown Applications
Network Application :	Protocol Enforcement and Filter Overrides	lete	_	
Priority	Details	Туре	Action	
1	 Twitter Twitter.Video Twitter_Login Twitter_Message Twitter_Post Twitter_Post 	Application	C Allow	

Figure 2.30: WebTerm3 Application Control Settings

	Firewall/Network 0	Option	5		
	NAT	0			
0	IP Pool Configuration		Use Outgoing Interface Address	Use D	ynamic IP Pool
Ŀ	Preserve Source Por	rt 🔿			
ŀ	Protocol Options		PROT default	•	1
	Security Profiles				
Ľ	AntiVirus	•			
ŀ	Web Filter	•			
Ŀ	DNS Filter	0			
L	Application Control	0	APP WebTerm3		
L	IPS	0			
ŀ	File Filter	•			
	SSL Inspection		ss certificate-inspection		
	Logging Options				
Ľ	Log Allowed Traffic		C Security Events A	II Session	ns
	Generate Logs when	1 Sessio	on Starts 🔾		
Ľ	Capture Packets		0		



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



Figure 2.32: Priority of policies

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



Figure 2.33: Verify the result in WebTerm1

48 Chapter 2. Policy

Chapter 3. NAT

50 FortiGate Firewall

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

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	ICMP-HTTP-HTTPS	
	Port 4 – 10.10.10.1/24		
WebTerm	10.10.10.2/24	_	

Table 3.1: Devices configuration

Basic Configuration

1. Port configuration in the firewall as follows:

E FortiGate VM64-KVM	1 3 5 7 9 11 12 15 m m m m 2 4 c 3 10 12 14 15	17 19 21 29 18 70 22 24						
+ Create New ▼ 🖋 Edit	🖻 Delete 🕨 Integra	te Interface	Search				Q	Group
Name 🗘	Type ≑	Members 🛱	E).	IP/Netmask 🗘	τ	Administ	rative A	ccess 🛱
🕽 🗜 802.3ad Aggregate 🗊			*					
🗜 fortilink	₿ 802.3ad Aggregate		Dedic	ated to FortiSwitch		PING Security F	abric C	onnection
🛯 🖩 Physical Interface 10								
m port1	🖩 Physical Interface		192.1	.68.0.1/255.255.255.	D	HTTPS HTTP		
m port2	Physical Interface		192.1	68.1.1/255.255.255.	D			
m port3	Physical Interface		192.1	68.122.242/255.255	255.0			
m port4	Physical Interface		10.10	.10.1/255.255.255.0				

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).

C DHCP Server			
DHCP status	🖸 Enabled 🔮 Dis	abled	
Address range	192.168.1.10-192.1	68.1.20	
	0		
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	×	
	0		
Lease time 🗿 🔘	604800	second(s)	
Advanced			
Network			
Device detection	0		
Security mode	0		

Figure 3.3: DHCP Server configuration

3. 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	192.168.122.242/255.255.255.0 Renew
Expiry Date	2022/04/03 00:00:00
Acquired DNS	192.168.122.1
Default gateway	192.168.122.1
Retrieve default gateway from ser	rver 💽
Distance	5
Override internal DNS	0

Figure 3.4: DHCP client configuration

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

Dashboard	> New Static Route	
Network	Automatic gateway retrieval	0
DNIC	Destination 3	Subnet Internet Service
DINS		0.0.0/0.0.00
Packet Capture	Gateway Address ()	Dynamic Specify
SD-WAN		192.168,122.1
Static Routes	1nterface	m port3 X
Policy Routes		+
RIP	Administrative Distance 🕄	10
OSPF	Comments	Write a comment // 0/255
BGP	Status	Enabled Obsabled
Routing Objects	and the second se	
Multicast	Advanced Options	
🛓 Policy & Objects	>	
Security Profiles	>	
U VPN	>	
User & Authentication	>	

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

3.1 Source NAT 55

æ	Dashboard 3	Edit Policy			
+	Network 3				1
B	Policy & Objects	Name 0	LocalToInternet		l
	Firewall Policy 🖌	Incoming Interface	m port2	•	l
	IPv4 DoS Policy	Outgoing Interface	m port3	•	l
	Addresses	Source	🚍 mylocal	×	l
	Internet Service Database	Destination	🗐 all	×	l
	Services	Schedule	Co always	•	l
	Schedules	Service	DNS	×	l
	Virtual IPs		I HTTP	×	l
	IP Pools		HTTPS	×	l
	Protocol Options		+		l
	Traffic Shaping	Action	✓ ACCEPT Ø DENY		þ
•	Security Profiles	Inspection Mode	Flow-based Proxy-based		ľ
묘	VPN >		the state of the state	SNAT	ŀ
2	User & Authentication	Firewall/NetworkO	ptions		ŀ
÷	WiFi Controller	NAT	0		Ŀ
٠	System 🔹 🕽	IP Pool Configuration	n Use Outgoing Interface Ad	dress Use Dynamic IP Pool	ľ
*	Security Fabric	Preserve Source Port	t 🛈		
ш	Log&Report >	Protocol Options	PROT default	• 1	

Figure 3.6: Configure Firewall Policy and enable Source NAT

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



Figure 3.7: Verify your configuration

56 Chapter 3. NAT

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**

🔁 Dashboard	> New	> New Virtual IP					
🕂 Network	>						
Policy & Objects	v VIP	type IPv4					
Firewall Policy	Nar	ne OutsideToI	DMZ				
IPv4 DoS Policy	LT Cor	nments Write a con	nment	<i>a</i> 0/255			
Addresses		or 🖷 Change					
Internet Service Database	Net	work					
Services	Inte	erface	im port4	-			
Schedules	Тур	e	Static NAT FQDN				
Virtual IPs	∰ Ext	ernal IP address/range	0 10.10.10.1				
IP Pools	Ma	p to	incolor and				
Protocol Options	IP	v4 address/range	192.168.1.22				
Traffic Shaping	0	Optional Filters					
A Security Profiles	>						
I VPN	> °	Port Forwarding					
Luser & Authentication	> Pro	tocol	TCP UDP SCTP ICMP				
ℜ WiFiController	> Ext	ernal service port	80				
System	(1) Ma	p to IPv4 port	80				
X Security Fabric	,						

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.

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

Table 3.2: Firewall policy configuration

Click **OK** to save the changes.

Dashboard		New Policy					
🕂 Network	>	-					
💄 Policy & Objects	*	Name 0	Outside-DMZ				
Firewall Policy	습	Incoming Interface	m port4				
IPv4 DoS Policy		Outgoing Interface	m port2	•			
Addresses		Source	🗐 all	×			
Internet Service Database		Destination	OutsideToDMZ	×			
Services		Schedule	Co always	*			
Schedules		Service	П нттр	×			
Virtual IPs		Service	+				
IP Pools		Action	✓ ACCEPT Ø DENY				
Protocol Options			States (March 1977)				
Traffic Shaping		Inspection Mode	Flow-based Proxy-based				
Security Profiles	>						
🖵 VPN	>	Firewall / Network Options					
LUSER & Authentication	, , ,	TAN	0	and the second			
✤ WiFi Controller	>	IP Pool Configuration	Address Use Dynamic IP Pool				
System	•	Preserve Source Port	0				
Security Fabric	,	Protocol Options	rson default	- /			

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:



Figure 3.13: Enable SSH service in Kali



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

2. Repeat the previous steps we have done for DNAT and try to reach Kali from port 8080 (Port Forwarding: $8080 \rightarrow 22$)

Network	VIP type IPv4		FortiGate
Policy & Objects	Name Kali		FGVM01TM19008000
Firewall Policy	Comments Write a comm	nent	Statistics (since last reset)
IPv4 DoS Policy	Color @ Change		
Addresses			ID
Internet Service	Network		Last used N/A
Database	Interface	E port4	Firstused N/A
Services	Туре	Static NAT	Hitcount O
Schedules	External IP address/range	10.10.10.1	
Virtual IPs	A Map to		I Clear Counters
IP Pools	IPv4 address/range	192 168 1 23	Additional Information
Protocol Options	in those cost unge		Adoltonal montation
Traffic Shaping	Optional Filters		 API Preview
A Security Profiles	>		% References
Q VPN	PortForwarding		>_ Edit in CLI
Luser & Authentication	Protocol	TCP UDP SCTP ICMP	
	External service port 0	8080	⑦ Documentation
1 System	Map to IPv4 port	22	Online Help
X Security Enhric			
-X. Security Fabric			Course 1
Log & Report	>	ОК	Cancel

Figure 3.15: Map External port 8080 to local port 22

62 Chapter 3. NAT

2	Policy & Objects 🛛 💙	Name	SSH	
	Firewall Policy	Incoming Intel ace	m port4	*
	IPv4 DoS Policy	Outgoing Interface	m port2	*
	Addresses	Source	🗐 all	×
	Internet Service Database	Destination	la Kali	ж
	Services	Schedule	always	
	Schedules	Service		×
	Virtual IPs	Service	+	-
	IP Pools	Action	✓ ACCEPT Ø DENY	
	Protocol Options	1.1		
	Traffic Shaping	Inspection Mode	Flow-based Proxy-based	
۵	Security Profiles >	E		
	VPN >	Firewall/Network O	ptions	
	User & Authentication >	NAT	C	
÷	WiFi Controller >	IP Pool Configuration	Use Outgoing Interface Addres	s Use Dynamic IP Pool
٠	System 🔹 🗴	Preserve Source Port		
*	Security Fabric >	Protocol Options	default	• /
ш	Log & Report >	Security Profiles		

Figure 3.16: Set Firewall Policy

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



Figure 3.17: Verify SSH connection

64 FortiGate Firewall

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

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

 Table 4.1: Devices configuration

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).

+ Network	 Administrative Acceleration 	cess			FortiGate
Interfaces DNS	☆ 1Pv4	HTTPS FMG-Access	SSH		FGVM01TM19008000
Packet Capture		□ FTM	RADIUS Accounting	Connection	Status O Down
SD-WAN		Speed Test			Down
Static Routes	Receive LLDP ()	Use VDOM Setting Enab	le Disable		MAC address
Policy Routes	Transmit LLDP ()	Use VDOM Setting Enab	le Disable		0c:24:73:53:00:01
RIP	C DUCD C				Additional Information
OSPF	U DHCP Server				API Preview
BGP	DHCP status	C Enabled O Disabled			% References
Routing Objects	Address range	192.168.0.10-192.168.0.20			>_ Edit in CLI
Multicast		0			
Policy & Objects	Netmask	255.255.255.0			⑦ Documentation
A Security Profiles	> Default gateway	Same as Interface IP Speci	ify		Online Help I
	DNS server	Same as System DNS Same	e as Interface IP Specify		
Luser & Authentication	> Lease time 0 C	604800	second(s)		

Figure 4.4: Set DHCP IP address



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

4.1 IPsec VPN 69

🕞 FGVM01TM19008000	- ≡ Q	>_ 😧 • 🗘 🛛 • 🔝 admin •
🕰 Dashboard	> New User Group	
 Network Policy & Objects Security Profiles VPN User & Authentication 	Name VPN_GRP_A00123456 Type Firewall Fortinet Single Sign-On (FSS RADIUS Single Sign-On (RSS Guest Members	D) O) O) O) O) O) O) O) O) O) O) O) O) O)
User Definition User Groups Guest Management LDAP Servers RADIUS Servers Single Sign-On Authentication Settings		 ② Documentation ④ Online Help C ● Video Tutorials C
FortiTokens FortiTokens SwiFi Controller System Security Fabric		OK Cancel

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

We Dashboard		Users/Group	s Creation wizard	
🕂 Network	>		2 Login Credentials	FortiExplorer
🖹 Policy & Objects	>		Contact Info A Extra Info	Manage your devices on IOS or Android, IOS
A Security Profiles	>	11	100100151	users can also manage FortiToken Cloud
U VPN	>	Username	A00123456	Get the and
Luser & Authentication	~	Password	••••••	Oet the app E
User Definition	4			⑦ Documentation
Licar Groups	-			Online Help Online Help Online Help
Greek Margaret				
Guest Management				Contraction of the second
LDAP Servers				
RADIUS Servers				
Single Sign-On				
Authentication Settings				
FortiTokens				
	>			
🌣 System	1 >			
🔆 Security Fabric	>			
Log & Report	>			
FURTIDET	-702		< Back Next	Cancel

Figure 4.11: Configure login credentials for the user

4.1 IPsec VPN 71



Figure 4.12: Contact info

4. Assign User Group to your profile.

20 Dashboard	> Users/Groups (creation vvizard	
🕂 Network	2 2	30	FortiExplorer
🚊 Policy & Objects	>	0 E	xtra Info Manage your devices on IOS or Android. IOS
Security Profiles	> User Account	Status O Enabled O Disabled	subscriptions.
D VPN	> User Group	O WPN GRP A00123456	¥ Get the app
User & Authentication	*	+	Documentation
User Definition			
User Groups			Video Tutorials
Guest Management			
LDAP Servers			
RADIUS Servers			
Single Sign-On			
Authentication Settings			
FortiTokens			
🗢 WiFi Controller	>		
🌣 System	1 >		
🔆 Security Fabric	>		
네 Log & Report	>		
FRETIDET	100	< Back Sub	Cancel

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

FortiGate - FGVM01TM19	< +	-							
€ → ℃ @	() R	https://192.168.0.1/ng/vpn	/ipsec/wizard			… ⊠ ☆	IIIV		\$ ≡
FGVM01TM19008000	•	≣ Q,				>_ 0	· 42-	1	admin +
a Dashboard	>	VPN Creation Wizard							
+ Network			2 30	Authentical		Policy & Rou		ient Oz	tions
🖹 Policy & Objects							S Rev	iew Set	tings
Security Profiles	>	Incoming Interface	m port1			-	_		
II VPN	*	Authentication method	Pre-shared Key	Signature	-	-		-	
Overlay Controller VPN		Pre-shared key	123456		ø	-	_		
IPsec Tunnels		User Group	VPN GRP A00	123456	•		_		
IPsec Wizard	습					-	_		
IPsec Tunnel Template		Dialup - FortiClient (Wi	ndows, Mac OS, And	roid)					
SSL-VPN Portals				_					
SSL-VPN Settings									
SSL-VPN Clients		This FortiCate	EastiCia						
VPN Location Map		The Carles and	- Grinden		1				
User & Authentication	>				- C.				
↔ WiFi Controller	>		< Back	Next >		Cancel			

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

FGVM01TM19008000	+ ≡ Q	>_ 0+	🗛 2 🔹 🦂 admin 🔹
🛛 Dashboard	> VPN Creation Wizard		All and a second
Network Policy & Objects Security Profiles VDN	> > >		Review Settings
Overlay Controller VPN IPsec Tunnels	The following settings should be reviewed prior to creating the VPN. Object Summany		
IPsec Wizard	ADD123456 VPN		
IPsec Tunnel Template	Phase 1 interface A00123456-VPN		
SSL-VPN Portals SSL-VPN Settings SSL-VPN Clients	Address A00123456-VPN_range Remote to local policies vpn_A00123456-VPN_remote	1	
VPN Location Map	Endpoint Registration A00123456-VPN		
🚊 User & Authentication	>		
	> < Back Create	Cancel	
System	>		

Figure 4.18: Review Settings

6. On Windows machine, <u>download FortiClient from Fortinet</u>. 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





Figure 4.21: Accept FortiClient Free Licence

FGVM01TM19008000	•	≣ Q			≻ @• ¢ 2 • 🧘 ad	tmin +
 Dashboard Network. 	*	FortiGate VM64-KVN		12 36 31 25	an machine le	
Interfaces				1.1.201.32.24	We take this address and Apply it to our VPN in our	
DNS				the car see yes	windows Machine	
Packet Capture		+ Create New - & Ed	it 🝵 Delete 🕪 Integ	rate Interface		
SD-WAN		Search		0	Group By Ty	me •
Static Routes		360101		~	Emoloup by 1	pe -
Policy Routes	- 1.	Name 🗘	Туре 🖨	Members \$	IP/Netmask ≑	Adm
RIP	E	🗄 🔚 Physical Interface 🚺	D			
OSPF	2	🕈 🖻 port1	Physical Interface	_	192.168.122.34/255.255.25	
BGP		m port2	Physical Interface		192.168.0.1/255.255.255.0	PI
Routing Objects						H
Multicast		-				н
🛓 Policy & Objects	>	port3	Physical Interface		0.0.0/0.0.0.0	
Security Profiles		m port4	Physical Interface		0.0.0,0/0.0.0.0	
I VPN	>	m port5	Physical Interface		0.0.0.0/0.0.0.0	
💄 User & Authentication	>	port6	Physical Interface		0.0.0.0/0.0.0.0	
🗢 WiEi Canteallar		mort7	Physical Interface		0.0.0.0/0.0.0	

Figure 4.22: Port1 IP Address

9.

4.1 IPsec VPN 77

	New VPN Conne	ection		
	VPN	SELVEN IPsec VPN	XML	
	Connection Name	VPN	-	_
	Description			
	Remote Gateway	192.168.122.34	*	
	the second s	*Add Remote Gateway		_
	Authentication Method	Pre-shared key	~	
				_
	Authentication (XAuth)	Prompt on login O Save login O Dis	able	
	Failover SSL VPN	[None]	~	
	A Advanta of Children			
		85		
•		Cancel Save		
63				

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**.

🔁 Dashboard	> VPN Creation Wizard			
💠 Network	> R VPu Saup > 2 A	uthentication 3 3 F	Policy & Routing	4 Review Settings
🖹 Policy & Objects	> Remote device	IP Address Dynam	ic DNS	
Security Profiles	> Remote IP address	10.10.10.2		
므 VPN	 Outgoing Interface 	m port3	•	
Overlay Controller VPN	Authentication method	Pre-shared Key Sig	gnature	
IPsec Tunnels	Pre-shared key			
IPsec Wizard				
IPsec Tunnel Template	Site to Site - FortiGate			
SSL-VPN Portals		~		
SSL-VPN Settings		nternet	\geq	
SSL-VPN Clients			10-1-	
VPN Location Map	This Porticate	Hemote For	(rusate)	
💄 User & Authentication	>	1		
☆ WiFi Controller	>	< Back	Next >	Cancel

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.

Dashboard	VPN Creation Wizard			
+ Network	1 VPN Setup	Authentication > 3 Policy 8	x Routing > 4	Review Settings
Policy & Objects	Name	FG2		
Security Profiles >>>	Template type	Site to Site Hub-and-Spoke Custom	Remote Access	
Overlay Controller VPN IPsec Tunnels	NAT configuration	No NAT between sites This site is behind NAT		
IPsec Wizard ☆ IPsec Tunnel Template	Remote device type	The remote site is behind NAT		
SSL-VPN Portals SSL-VPN Settings SSL-VPN Clients	Site to Site - FortiGat	e CISCO		
VPN Location Map User & Authentication WiFi Controller System	This FortiGate	Internet Bernote FortiGate		
Security Fabric		< Back N	lext >	Cancel

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

Ð	Dashboard	>	VPN Creation Wizard			
÷	Network	>	10 million 34	Autor antion 30	Policy & Routing	A Review Settings
8	Policy & Objects	>	Local interface	m port2	×	
۵	Security Profiles	>	Local interface	+		
D	VPN	•	Local subnets	192.168.10.0/24		
	Overlay Controller VPN			0		
	IPsec Tunnels		Remote Subnets	192.168.20.0/24		
	IPsec Wizard	쇼		0		
	IPsec Tunnel Template		Internet Access 🚯	None Share Local	Use Remote	
	SSL-VPN Portals					
	SSL-VPN Settings		Site to Site - FortiGa	te		
	SSL-VPN Clients			- /		
	VPN Location Map			Internet		
2	User & Authentication	>	This FortiGate	Remote F	ortiGate	
(:	WiFi Controller	>				
۵	System	2 >		< Back	Next >	Cancel
**	Security Fabric	>				

Figure 4.32: Policy & Routing in FG2

6.

 Network Policy & Objects 	> >	Tunnel \$	Interface Binding 🖨	Status 🕏	Ref. ‡
Security Profiles	, ⊡	🕄 Site to Site - Forti	Gate 1		
	~	O FG2	port3	O Inactive	4
Overlay Controller VPN		Ť		•	
IPsec Tunnels	☆				
IPsec Wizard					

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!

🕞 FGVM01TM19008000	+ ≡ Q			>_ @•	4 3 - 🤳
 Dashboard Hetwork Policy & Objects 	> IPsec > 圖 Reset Stat	tistics O Bring Up •	O Bring Down -	Q Locate on VPN Map	2 3
Security Profiles	> Name 🖨	Remote Gateway 🖨	Peer ID \$	Incoming Data 🖨	Outgoing Dat
II VPN	* 🗆 🗆 🚥	in fartare O			
Overlay Controller VPN IPsec Tunnels IPsec Wizard IPsec Tunnel Template	O FG2	 ♥ FG2 ♥ Reset Statistics ● Bring Up ♥ Phase 2 Selector: FG2 ♥ Bring Down ♥ All Phase 2 Selectors 		0 B or: FG2 ectors	0 B
SSL-VPN Portals SSL-VPN Settings SSL-VPN Clients VPN Location Map User & Authentication	>	C Locate on VPN M.	ap bgs		

Figure 4.34: Bring up IPsec Tunnel

FGVM01TM19008000	+	≡ Q.			>_ 0•	斗 3 • 👤 admin
 Dashboard Network 	> >	IPsec	tics O Bring Un -	Bring Down *	Q Locate on VPN Man	C C' i∙
Policy & Objects Security Profiles VPN	> >	Name + T	Remote Gateway \$	Peer ID \$	Incoming Data \$	Outgoing Data ≑
Overlay Controller VPN IPsec Tunnels IPsec Wizard		• 552	10.10.10.1		0 B	0 B
IPsec Tunnel Template SSL-VPN Portals SSL-VPN Settings						

Figure 4.35: Verify the status of the tunnel

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

æ	Dashboard	> Edit Interface					
\$	Network	Name m port2					
	Interfaces DNS Packet Capture SD-WAN Static Routes Policy Routes	Alias Type Physical Interface VRF ID 0 Role 1 Undefined	Alias Type Physical Interface VRF ID 1 0 Role 1 Undefined •				
	RIP OSPF BGP Routing Objects Multicast	Addressing mode Man IP/Netmask 192. Secondary IP address Administrative Access	ual DHCP Auto-managed by IPAM One-Arm S 168.10.1/24	Sniffer			
	Policy & Objects Security Profiles VPN User & Authentication WiFi Controller System	 > IPv4 > HTTPS > FMG-Act > FTM > Speed Te > Receive LLDP (1) Use VDOM > Transmit LLDP (1) Use VDOM 	cess SSH Constraints SSH Constraints SSH Constraints Enable Disable Disable Disable Disable Disable Constraints Enable Disable	PING SNMP Security Fabric Connection			

Figure 4.36: Verify configuration

You should be able to ping from WebTerm1 to WebTerm2.

ΨL)	(lern	minal	_ 0
<u>F</u> ile	<u>E</u> dit	absHelp	
root(eth0	@wgbt(<pre>term-1:~# ifconfig Link encap:Ethernet HWaddr 5a:3f:le:c3:02:61 inet addr:192.168.20.2 Bcast:0.0.0.0 Mask:255.255.255.0 inet6 addr: fe80::583f:leff: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)</pre>	
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 PING 64 b 64 b	@webt 192. ytes ytes	term-1:~# ping 192.168.10.2 .168.10.2 (192.168.10.2) 56(84) bytes of data. from 192.168.10.2: icmp_seq=1 ttl=62 time=1.76 ms 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

Device	IP address	Access
FortiCate	Port3: 192.168.1.1/24 – DHCP (192.168.1.20 to 192.168.1.30)	ICMD_HTTD_HTTDS
	Port2: DHCP Client	
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	

Table 4.3: Devices configuration

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

1. Port 3 Configuration:

FGVM01TM19008000	<pre># config system interface</pre>
FGVM01TM19008000	(interface) # edit port3
FGVM01TM19008000	(port3) # set ip 192.168.1.1/24
FGVM01TM19008000	(port3) # set allowaccess http https
FGVM01TM19008000	(port3) # end
FGVM01TM19008000	#
<i>Figure 4.39: Port3 settings</i>	

2. Port 2 Configuration:

FGVM01TM19008000	<pre># config system interface</pre>
FGVM01TM19008000	(interface) # edit port2
FGVM01TM19008000	(port2) # set mode dhcp
FGVM01TM19008000	(port2) # end

Figure 4.40: Port2 settings

3. Configure DHCP Server on port3.

🛛 Dashboard	> Edit Interface			
🕂 Network	 Receive LLDP 0 	Use VDOM Setting	Enable Disable	
Interfaces	☆ Transmit LLDP 🕄	Use VDOM Setting	Enable Disable	
DNS	C DHCP Server			
Packet Capture	DHCP status	• Enabled • Disal	bled	
SD-WAN	Address range	192 169 1 20 192 169	9.1.20	
Static Routes	k	0	5.1.50	
Policy Routes	Netmask	255 255 255 0		
RIP	Default gateway	Same as Interface ID	Specify	
OSPF	Default gateway	Same as Suctor DNC	Same as Interface ID	Specify
BGP	Divis server	Same as System DNS	Same as miteriace iP	specify
Routing Objects	Lease time 🗿 🔍	004800	▼ Second(s)	
Multicast	Advanced			

Figure 4.41: Enable DHCP Server on port3

4. Configure user and user group. Go to **User & Authentication** > **User Definition** to create a local user **sslvpnuser1**.



Figure 4.42: Create a local user

🕞 FGVM01TM19008000	•	≣ Q	
🕰 Dashboard	>	Users/Group	s Creation Wizard
🕂 Network	>		User 1 voc 2 Login Credentials
💄 Policy & Objects	>₹	*	3 Contact Info 4 Extra Info
Security Profiles	>	Username	sslvpnuser1
🖵 VPN	>	Deserved	
User & Authentication	~	Password	•••••
User Definition			
User Groups			
Guest Management			

Figure 4.43: Configure login credentials

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

+ ≣ Q,		
> New User G	roup	
> Name	sslvpngroup	
> Type	Firewall Fortinet Single Sign-On (FSSO) RADIUS Single Sign-On (RSSO)	
✓ Members	Guest sslvpnuser1	×
	+	
	 ■ Q New User G Name Type Members 	 ➡ Q New User Group Name sslvpngroup Type Firewall Fortinet Single Sign-On (FSSO) RADIUS Single Sign-On (RSSO) Guest Members 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

4.2 SSL VPN 89



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.

Name	SSH		
ype	SSH	•	
lost	root@192.168.1.21		
escription			

Figure 4.46: Create an SSH bookmark

Name	WordPress	
Гуре	HTTP/HTTPS	
JRL	192.168.1.20	
Description		
Single Sign-On	Disable SSL-VPN Login	Alternative

Figure 4.47: Create an HTTP/HTTPS bookmark

₽	VPN	~	Rewrite Content IP/	UI/ 🔿					
	Overlay Controller VPN		RDP/VNC clipboard	0					
	IPsec Tunnels		Predefined Bookmar	ks					
	IPsec Wizard		+ Create New		盾 De	lete	Search		Q
	IPsec Tunnel Template			-	_				-
	SSL-VPN Portals	습	Name ≑	Type	T	L	ocation 🛱	Description ≑	
	SSL-VPN Settings		SSH	HTTP/HT	TPS	192.	168.1.21		
	SSL-VPN Clients		WordPress	HTTP/HT	TPS	192.	168.1.20		
	VPN Location Map								
*	User & Authentication	>							0

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

Users/Groups	sslvpngroup	×	
	+		
Portal	MyPortal	•	
Portal	MyPortal	•	
		_	
	0	K	Cancel

Figure 4.50: Assign sslvpngroup to MyPortal

IPsec Tunnels		Authentication/Portal Mapping	0		
IPsec Wizard IPsec Tunnel Template		+Create New / Edit	會 Delete	Send SSL-VPN Configuration	
SSL-VPN Portals		Users/Groups 🛱		Portal ≑	
SSL-VPN Settings	습	sslvpngroup		MyPortal	
SSL-VPN Clients		All Other Users/Groups		MyPortal	
VPN Location Map					
Luser & Authentication	>			0	
	>	L			

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.

FGVM01TM19008000	• ≡ Q		
Dashboard	> New Policy		
🕂 Network	>		
🛓 Policy & Objects	Vame 🕄	SSLVPN	
Firewall Policy	☆ Incoming Interface	SSL-VPN tunnel interface (s	sl.roo 🔻
IPv4 DoS Policy	Outgoing Interface	m port3	-
Addresses	Source	💷 all	×
Internet Service Database		sslvpngroup	×
Services	Destination	III all +	×
Schedules	Schedule	Co always	-
Virtual IPs	Service	ALL	ж
IP Pools		+	
Protocol Options	Action	✓ ACCEPT Ø DENY	
Traffic Shaping	1	Chain based Draws based	
Security Profiles	> Inspection Mode	Proxy-based Proxy-based	
I VPN	> Firewall / Network	Options	
💄 User & Authentication	> NAT	•	
♥ WiFi Controller	IP Pool Configuration	on Use Outgoing Interface Ac	dress

Figure 4.52: Create a Firewall Policy for SSLVPN

8. 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

SSL-VPN Por	rtal	
Download FortiClier	nt -	
Bookmarks		
>_		
SSH	WordPress	
	- Mary Deckmark	

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

8	FortiClient Setup	-		¢
Choose Setup	Туре			
Choose the setu	p type that best suits your needs		-	
✓ Zero Ti	ust Telemetry			
Fabric T	elemetry			
✓ Secure	Remote Access			
SSL and	IPsec VPN			
✓ Vulner	ability Scan			
Host vul	nerability scanning and remediation			
Advan	ced Persistent Threat (APT) Components			
FortiSan	dbox detection and cloud scan			
			Course 1	1
	Back Next		Cancel	1

Figure 4.58: FortiClient Installation

8	FortiClient Setup – 🗆 🗙
Addi	tional Security Features
	AntiVirus Real-Time and On-Demand AntiVirus scanning Web Filtering Single Sign-On Mobility Agent Single Sign-On Mobility Agent Anti-Ransomware Anti-Ransomware
	Application Firewall Application Firewall
	Back Next Cancel

Figure 4.59: FortiClient Installation

10. Configure FortiClient.


Figure 4.60: Configure FortiClient

File Help IEUser VN Sturpe Connection Name Sturpe REMOTE ACCESS Natifications Substrate Client Certificate None Client Certificate Client Certificate Cancel Save	Ð	FortiClient	Zero Trust Fabric Agent	- B ×
VPN SSLVPN VPN SSLVPN Ocnnection Name Description Remote Gateway 192 166.122.39 *Add Remote Gateway Customize port Bollo Customize port Bollo Customize port Bollo Customize port Bollo Customize port Customize port Bollo Customize port Bol	File Help	New VPN Conne	ection	×
Setting: Client Certificate: Authentication Prompt on login Setting: Client Certificate: Authentication Prompt on login Save login Cancel	IEUser	VPN Connection Name	SSLVPN IPac VPN 2000	
Activitations Client Certificate Authentication Formpt on login _ Save login Enable Dual-stack IPv4/IPv6 address Cancel Save		Remote Gateway	192.168.122.39 +Add Remote Gateway Customize port 8080 +	*
Cancel Save	Notifications	Client Certificate Authentication	Enable Single Sign On (SSO) for VPN Tunnel None Prompt on login Save login	
Cancel Save	Q Sattings		Enable Dual-stack IPv4/IPv6 address	
			Cancel Save	

Figure 4.61: Configure SSLVPN

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

		1	
	1 12		
B		7	
se contact you	r administrator or connect to l	EMS for license a	activation.
se contact you Jnlicensed VPN	r administrator or connect to l N access is available until May	EMS for license : • 04, 2022 5:47:	activation. 08 PM
se contact you Jnlicensed VPM PN Name	r administrator or connect to l N access is available until May SSLVPN	EMS for license a 04, 2022 5:47:	activation. 08 PM
se contact you Jnlicensed VPM PN Name Isername	r administrator or connect to I N access is available until May SSLVPN sslvpnuser1	EMS for license a 04, 2022 5:47: ~	activation. 08 PM
se contact you Inlicensed VPM PN Name Isername assword	r administrator or connect to I N access is available until May SSLVPN sslvpnuser1	EMS for license ; 04, 2022 5:47: ~	activation. 08 PM] =

Figure 4.62: SSLVPN Credentials

Accept the Certificate Issuer to have a secure connection.

CCESS			Sec	urity Alert		×	
•	This ser The unit	s page require ver authentica e Certificate Is of wr. Do yo	es a secure conne stion. suer for this site is u wish to procee	ection which includes s untrusted or d?	Manufatio	se ac 47:08	tivation 3 PM
	1	165	NU	view Certailcale	MOIE 110		
			Username	SOLVEN	art	~	
			Password	*****			
				Di	sconnect		

Figure 4.63: Click on Yes in Security Alert

 VPN Name
 SSLVPN

 IP Address
 10.212.134.200

 Username
 sslvpnuser1

 Duration
 00:00:03

 Bytes Received
 0 KB

 Bytes Sent
 4.75 KB

Figure 4.64: Verify SSLVPN Connection

VPN Connected

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.



Figure 4.66: Verify SSH



Figure 4.67: Verify SSH connection

100 Chapter 4. VPN

Chapter 5. Authentication

102 FortiGate Firewall

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.





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	_

Table 5.1: Devices configuration

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 Internet IP).

5.1 Captive Portal 105

DNS	New Static Route		
Packet Capture	Automatic gateway retrieval ()	0	1
SD-WAN	Destination 🚯	Subnet Internet Service	
Static Routes 🗘		0.0.0/0.0.0.0	
Policy Routes	Gateway Address 🜖	Dynamic Specify	
RIP		192.168.122.1	
OSPF	Interface	m port1 ★	
BGP	Administrative Distance 🜖	10	
Routing Objects	Comments	Write a comment	
Multicast	Status	• Enabled • Disabled	
Policy & Objects			
Security Profiles	Advanced Options		
U VPN >			

Figure 5.2: Configure a static route

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

💄 Policy & Objects 🛛 🗸 🗸	New Policy		
Firewall Policy 🗘			
IPv4 DoS Policy	Name	Internet	
Addresses	Incoming Interface	m port2	-
Internet Service	Outgoing Interface	m port1	-
Database	Source	😑 all	×
Services		+	
Schedules	Destination	💷 all	×
Virtual IPs	Cabadala		
IP Pools	Schedule	Lo aiways	•
Protocol Options	Service	ALL +	×
Traffic Shaping	Action	ACCEPT Ø DENY	
Security Profiles			
모 VPN >	Inspection Mode	Flow-based Proxy-based	
User & Authentication			
중 WiFi Controller >	Firewall / Network O	ptions	
🌣 System 🛛 🙆 🕨	NAT	0	
🔆 Security Fabric 🔹 🔸	IP Pool Configuration	Use Outgoing Interface Add	dress

Figure 5.3: Set a Firewall Policy

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

# # 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. 1. 2 netmask 255. 255. 255.0 gateway 192. 168. 1. 1 up echo nameserver 4.2.2.4]> /etc/resolv.conf		
# DHCP config for eth0 # auto eth0 # iface eth0 inet dhcp		

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

FGVM01TM19008000	-	≡ Q.
🙆 nashboard	>	Users/Groups Creation Wizard
Network	>	2 User to 2 Login Credentials
💄 Policy & Objects	>	3 Contact Info 3 Extra Info
Security Profiles	>	Username hamid
I VPN	>	Password
User & Authentication	*	
User Definition	습	
User Groups		
Guest Management		
LDAP Servers		
RADIUS Servers		

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.

++ Network	~	UFIM		S Accounting
- Hetwork		Speed Test		
Interfaces	Receive LLDP ()	Use VDOM Setting	Enable Disable	
DNS	Transmit LLDP	Use VDOM Setting	Enable Disable	
Packet Capture	*			
SD-WAN	DHCP Server			
Static Routes	Network			
Policy Routes	Network			
RIP	Device detection	0 0		
OSPF	Security mode	Captiv	e Portal	•
RGD	Authentication po	ortal Local	External	
DOF OLIVIT	User access 🚯	Restric	ted to Groups Allow	w all
Routing Objects	User groups	Cap	tivePortal	×
Multicast			+	
💄 Policy & Objects	> Exempt sources		+	
Security Profiles	> Exempt destinati	ons/services	+	
D VPN	> Redirect after Ca	ptive Portal Origina	I Request Specific	URL

Figure 5.9: Configure Captive Portal on port2

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

Firewall Authentication	× +			
€ → ℃ ŵ	(1) 2 192.168.1.1:1000/fgtauth?0705078f9885eb66	 ◙	☆	IIIV
⑦ You must log in to this	s network before you can access the Internet.		Open 1	Network Lo
	*			
	Authentication Required			
	Please enter your username and password to continue.			
	Username hamid			
	Password eeeee			
	Continue			

Figure 5.10: Verify Captive Portal

110 Chapter 5. Authentication

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.

<u>.</u>		System – 🗆 🛛
🛞 🛞 · 💦 💌	Control Panel System and Security	System v 🖒 Search Control Panel 🔎
Control Panel Home	view basic informati	on about your computer
	System Properties	×
Computer Name Hardwa	are Advanced System Protection Remote	
Windows uses on the network	the following information to identify your compute c.	Windows 8
Computer description:	1	1
	For example: "Kitchen Computer" or "Mary's Computer".	1U Virtual CPU version 2.5+ 2.90 GHz
Full computer name:	IE11WIN8_1	it Operating System v64-based processor
Workgroup:	WORKGROUP	Pen or Touch Input is available for this Display
To use a wizard to join a Network ID.	domain or workgroup, click Network ID	group settings
		WIN8_1 1 Change settings
To rename this computer workgroup, click Change	r or change its domain or 2 Change	WIN8_1
		RKGROUP
		the Microsoft Software License Terms
		AA427 Activate Windows
	OK Cancel App	NY .

Figure 5.11: Join Windows to the Active Directory

Computer Name/Dom	nain Changes 🛛 💌
You can change the name and the me computer. Changes might affect acces	mbership of this s to network resources.
Computer name:	
IE11WIN8_1	
Full computer name: IE11WIN8_1 Member of	More
hamid.local	
Workgroup: WORKGROUP	

Figure 5.12: Enter Domain name

domain.	sine and password of an account with permission to join th
	administrator
	•••••
	Domain: hamid.local

Figure 5.13: Enter username and password of AD administrator

2. Install FSSO Agent on the AD server.



Figure 5.14: Install FSSO Agent

and the second se				
Installing Fortinet SSO Collector Agent v5.	0.0301			
Please wait while the Setup Wizard installs Fortinet SSC	Collector Ag	gent v5.0.0	0301.	
Status: Computing space requirements				

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.

j Monitoling user logon events	Support N	NTLM authentication		Collector Agent Status: RUNNING	
istening ports				Common Tasks	
FortiGate: 8000 FortiGate S	SSL: 8001	DC Agent:	8002	Show Se	ervice Status
Enable SSL DCAgent S	SSL: 8003	Preshared key:		Chow M	onitored DCa
ogging				Show M	ormored DCs
Log level: Warning 🗸 Log fi	ile size limit(MB): 10	0	View Log	Show L	ogon Users
				-	
Log logon events in separate logs	~	View Logon E	vents	Select Dom	ains I o Monitor
		View Logon E	vents	Select Dom Set Directory /	ains To Monitor Access Information
Log logon events in separate logs	om FortiGate	Password:		Select Dom Set Directory A	ains To Monitor Access Information roup Filters
Log logon events in separate logs Authentication Require authenticated connection fro fimers Work station verify interval (minutes):	om FortiGate	View Logon E Password:		Select Dom Set Directory / Set Gr	ains To Monitor Access Information roup Filters
Log logon events in separate logs Authentication Require authenticated connection fro fimers Workstation verify interval (minutes): Dead entry timeout interval (minutes):	om FortiGate	Password:		Select Dom Set Directory A Set Gr	ains To Monitor Access Information roup Filters ore User List
Log logon events in separate logs Authentication Require authenticated connection fro Fimers Workstation verify interval (minutes): Dead entry timeout interval (minutes): IP address change verify interval (second	om FortiGate 5 480 ds): 60	Password:	Dool	Select Dom Set Directory / Set Gr Set Igno Sync Configuratio	ains To Monitor Access Information roup Filters ore User List on With Other Agents
Log logon events in separate logs Authentication Require authenticated connection fro Fimers Workstation verify interval (minutes): Dead entry timeout interval (minutes): IP address change verify interval (second Cache user group lookup result	om FortiGate 5 480 ds): 60	Password:		Select Dom Set Directory / Set Gr Set Igno Sync Configuratio Export C	anns I o Monitor Access Information roup Filters ore User List on With Other Agents Configuration

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.

Endpoint/Identity			
FSSO Agent on Windows AD		Agent Password	
Name	AD		
Primary FSSO agent	142.232.197.27		+
Trusted SSL certificate (
User group source 🚯	Collector Agent Local		
Users/Groups	0		

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.**

1 Network	·	Add Filter			
🖹 Policy & Objects	· · · ·	V Add Filter			
Security Profiles	> Date/Ti	ime Level	User	Action	Message
I VPN	> 49 seconds as	30	👃 HTALEBI	auth-logon	User HTALEBI added to auth logon
Liser &	> 54 seconds ag	30	A HTALEBI	auth-logon	User HTALEBI added to auth logon
Å System	54 seconds ag	go 🔳	HTALEBI	FSSO-logon	FSSO-logon event from AD: user HTALEBI logged
Security Fabric	54 seconds ag	ço 🔳		server-connect	FSSO server AD(142.232.197.27) is connected
Log & Report	.				
Forward Traffic					
Local Traffic					
Sniffer Traffic					
Events	\$				
AntiVirus					
Web Filter					
SSL					
DN5 Query					
File Filter					
Application Control					
Intrusion Prevention					
and the second sec					

Figure 5.20: FSSO event logs

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



Figure 5.21: Verify configuration

118 Chapter 5. Authentication

Chapter 6. High Availability

120 FortiGate Firewall

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

122 Chapter 6. High Availability

Device	IP address	Access	
WebTerm1	192.168.1.2/24	-	
WebTerm2	192.168.10.2/24	-	
EthernetSwitch1 –		_	
EthernetSwitch2 –		-	
EC Drimowy	Port 1: 192.168.1.1/24	ICMD LITTD LITTDC	
	Port 5: 192.168.10.1/24		
	Port 1: 192.168.1.1/24		
FG-Secondary	Port 5: 192.168.10.1/24	ПСМР-НТТР-НТТР5	

Table 6.1: Devices configuration

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) # set allowaccess http https ping FG-Primary (port5) # set allowaccess http https ping

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 (port1) # end 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) # 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

Secu VPN User System	rity Profiles & Authentication em 1	> > >	Mode Device priority 1 Cluster Settings	Active-Passive 128	•
Adm Adm Firm	inistrators in Profiles ware		Group name Password Session pickup	HRT 123456	Øs
Fabr Setti	ic Management ngs		Monitor interfaces	m port3	×
HA SNM	P		Heartbeat interfaces	m port4	×
Repl Mes Forti	acement sages Guard 1		Management InteUnicast Heartbeat	erface Reservation at	

Figure 6.2: HA primary configuration

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

🖹 Policy & Objects	> _		
Security Profiles	>	Mode	Active-Passive
🖵 VPN	>	Device priority 🟮	50
💄 User & Authentication	>	and the second second	
🔹 System	1 ~	Cluster Settings	
Administrators		Group name	HRT
Admin Profiles		Password	••••••
Firmware		Session pickup	D
Fabric Management		Monitor interfaces	m port3 ×
Settings		Heartheat interfaces	m port4
HA	☆	Theartheat Interfaces	+
SNMP		and the second	
Replacement Messages		Management Int	erface Reservation
FortiGuard	1	Unicast Heartbea	at

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.

6.1 High Availability 125

🕞 FG-Master	+	≡ Q			HA: 🛕 Primary	>_ @•	4 <mark>3</mark> - 🤱
 Dashboard Network Policy & Objects Security Profiles VPN 	> > > > >	FG-Master (Primar	164-КVМ гу)	1 3 5 7 9 	11 13 15 17 19 21 23 11 13 15 17 19 21 23 11 10 10 10 10 12 14 16 18 20 22 24		
💄 User & Authentication	>	C Refresh	Edit 🗶 I	Remove device f	rom HA cluster		
🏟 System	2 ~	Status	Priority	Hostname	Serial No.	Role	System Uptime
Administrators		Synchronized	128	FG-Master	FGVMEVAAPTTBXN83	Primary	36m 7s
Admin Profiles		Synchronized	50	FG-Slave	FGVMEVRDBBJLEOED	Secondary	36m 7s
Firmware							
Fabric Management							
Settings							
НА	1 ☆						

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

192.168.1.1/login?redir=	x +		
€ ⇒ C @	3 2 192.168.1.1/login?redir=%2Fng%2Fsystem%2Fha%2Fmonitor	… ⊚ ☆	IIN 🖾 📽
	Username Password		
	Landa		
	Login		

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.

🕞 FG-Slave	• ≡ Q		HA: Primary	>_ 😯 -	¢ 2 ∙	🙎 adm	
🖹 Policy & Objects 🔹 🔸	2 🕹 O Ad	d Filter	네 HA Events ㅋ	.	🖽 Det		
Security Profiles	Date/Time	Date/Time Level Action					
User & Authentication	Minute ago	Minute ago		Virtual cluster's member state moved Virtual cluster detected member dead			
System	Minute ago						
Security Fabric	Minute ago			Heartbeat packet	lost		
네 Log & Report 🗸 🗸	11 minutes ago			The sync status w	ith the prin	ne primary	
Forward Traffic	12 minutes ago			The sync status with the primary			
Local Traffic	12 minutes ago			The sync status with the primary			
Sniffer Traffic	14 minutes ago			The sync status with the primary			
Events 🏠	14 minutes ago			Virtual cluster's n	nember sta	te moved	
AntiVirus	14 minutes ago			Virtual cluster detected member join			
Web Filter	14 minutes ago			HA device(interface) peerinfo			
SSL	14 minutes ago			HA activity report	t		
DNS Query	14 minutes ago			Virtual cluster add HA device			
File Filter	14 minutes ago			HA activity report	t		

Figure 6.10: HA Events

128 Chapter 6. High Availability

Chapter 7. Security

130 FortiGate Firewall

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
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	_

Table 7.1: Devices configuration

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 <u>pentmenu repository</u> and run **DOS** > **UDP FLOOD** > **Enter port1 IP address** > **Port 443**.

```
0 0 0
                                       root@kali: ~
     Edit New Search Terminal Help
'oot@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
2022-04-07 23:55:24 (6.52 MB/s) - 'pentmenu' saved [49548/49548]
 oot@kali:~# ls
Desktop Documents Downloads Music pentmenu Pictures Public Templates Videos
coot@kali:~# chmod 777 pentmenu
     ali:~# ls
Desktop Documents Downloads Music pentmenu Pictures Public Templates Videos
 oot@kali:~# ./pentmenu
```

Figure 7.2: Download and execute pentmenu script

```
    Recon

2) DOS
Extraction
View Readme
5) Quit
Pentmenu>2
1) ICMP Echo Flood
                       TCP XMAS Flood 11) Distraction
                       UDP Flood
ICMP Blacknurse
                                             12) DNS NXDOMAIN
                       8) SSL DOS
3) TCP SYN Flood
                                             13) Go back
TCP ACK Flood
                       Slowloris
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):
```

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

💄 Policy & Objects 🛛 🗸	New Policy					
Firewall Policy						
IPv4 DoS Policy 습	Name 1	DO	S			
Addresses	Incoming Interface		port1	*		
Internet Service Database	Source Address	ource Address 🔚 all 🔸				
Services	Destination Addres	estination Address 🔳 all		×		
Schedules			+			
Virtual IPs	Service	Ū	ALL	×		
IP Pools			+			
Protocol Options	L3 Anomalies					
Traffic Shaping			Action			
Security Profiles	Name	Logging	Disable Block	Monitor	Threshold	
🖵 VPN 🔷 💙						
💄 User & Authentication 🔹 🔸	ip_src_session	0	Disable Block	Monitor 5000)	<
중 WiFi Controller >		-		A NUT LAND		
🕸 System 🚺 🔰	ip_dst_session	0	Disable Block	Monitor 5000)	V

Figure 7.4: IPv4 DoS Policy

T	0	A	Action			
Mame	Logging	Disable E	Block	Monitor	Inresh	old
tcp_syn_flood	•	Disable E	Block	Monitor	2000	× 1
tcp_port_scan	•	Disable E	Block	Monitor	1000	(V)
tcp_src_session	0	Disable E	Block	Monitor	5000	
tcp_dst_session	•	Disable B	Block	Monitor	5000	
udp_flood	0	Disable E	Block	Monitor	2000	
udp_scan	0	Disable E	Block	Monitor	2000	
udp_src_session	0	Disable	Block	Monitor	5000	()

Figure 7.5: IPv4 DOS Policy Settings

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

FGVM01TM19008000		≣ Q,					>_ @•	¢ 2 -	🧕 admin 🗝
System 1	\$	C 🛓	• Add Filter	r				•	Details
X Security Fabric	>	Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Nam
ഥ Log & Report	*	20 seconds ago	-	192.168.122.196	17		clear_session	1	udp_flood
Forward Traffic									
Local Traffic									
Sniffer Traffic									
Events									
AntiVirus									
Web Filter									
SSL.									
DNS Query									
File Filter									
Application Control									
Intrusion Prevention									
Anomaly	☆								
Log Settings									

Figure 7.6: View anomaly report

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

Net	work interfaces (1/2)	nfo			C	Actions Create net	work interface
Q	Filter network interfaces					Attach Detach	1 > @
	Name	A	Network interface ID 🛛	Subnet ID	VP	Delete	wailability Zone
¥	FG Private Subnet eni-08adedc167a1180a6 subnet-0936fd8c6f4984efe ☑				vpc	Manage IP addresses	s-east-1f
	FG Public Subnet	vpc	Associate address Disassociate address Change termination behavior	s-east-1f			
Net	work interface: eni-08	adedc	167a1180a6 (FG Private S	= Subnet)		Change security groups Change source/dest. check Manage tags	© ×
0	You can now check networ	connec	tivity with Reachability Analyzer.			Change description Create flow log] × [



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*.

ro	ot@kal	i:~#	ping -c	2000 -i	0.01 1	.92.168.	122.127		
PI	NG 192	.168.	122.127	(192.16	8.122.1	.27) 56(84) byte	s of data.	
64	bytes	from	192.16	8.122.12	7: icmp	_seq=1	ttl=255	time=0.920	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=2	ttl=255	time=0.657	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=3	ttl=255	time=0.737	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=4	ttl=255	time=0.664	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=5	ttl=255	time=0.745	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=6	ttl=255	time=0.678	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=7	ttl=255	time=0.750	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=8	ttl=255	time=0.632	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=9	ttl=255	time=0.688	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=10	ttl=255	time=0.667	ms
64	bytes	from	192.16	8.122.12	7: icmp	seq=11	ttl=255	time=0.628	s ms
64	bytes	from	192.16	8.122.12	7: 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 status	📀 Enabled 🔮 Disab	oled		
Address range	192.168.0.10-192.168	3.0.20		
	0			
Netmask	255.255.255.0			
Default gateway	Same as Interface IP	Specify		
DNS server	Same as System DNS	Same as Int	erface IP	Specify
DNS server 1	4.2.2.4	×		
	0			
Lease time 🕄 🔘	604800	🗧 sec	ond(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

7.2 Security Profile 139

🕞 FGVM01TM19008000	<mark>w</mark> ≡ Q	>_	0 -
🙆 Dashboard	New AntiVirus Profile		
🕂 Network	Name		
💄 Policy & Objects	Name myantivirus		
Security Profiles	Comments Write a comment 1/20/255		
AntiVirus	Facture set		
Web Filter	Feature set Flow-based Proxy-based		
Video Filter	Inspected Protocols		
DNS Filter	HTTP		
Application Control	SMTP O		
Intrusion Prevention	POP3		
File Filter			
SSL/SSH Inspection	FTP C		
Application Signatures	CIFS 💽		
IPS Signatures	APT Protection Options		
Web Rating Overrides	Treat Windows executables in email attachments as viruses A		
Web Profile Overrides	Include mobile malware protection		
I VPN	Quarantine A		
User & Authentication			_
F ORTINET v	0.3 OK Cancel		

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

🙆 Dashboard	>	New Policy		
💠 Network	>	(
💄 Policy & Objects	~	Name	Port2-to-Port1	
Firewall Policy	습	Incoming Interface	m port2	-
IPv4 DoS Policy		Outgoing Interface	m port1	-
Addresses		Source	🗐 all	×
Internet Service Database		Destination	all	×
Services		Schedule	Co always	•
Schedules		Service	I ALL	×
Virtual IPs			+	
IP Pools		Action	✓ ACCEPT Ø DENY	
Protocol Options				
Traffic Shaping		Inspection Mode	Flow-based Proxy-based	
Security Profiles	>			
I VPN	>	Firewall / Network O	ptions	
💄 User & Authentication	>	NAT	0	
🗢 WiFi Controller	>	IP Pool Configuration	N Use Outgoing Interface Address	Use Dynamic IP Pool
🗘 System	1 >	Preserve Source Port		
X Security Fabric	>	Protocol Options	default	- /
네 Log&Report	,	Security Profiles		
		AntiVirus	myantivirus	- 1

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**

7.2 Security Profile 141

FGVM01TM19008000	• =	= (۹							
🕰 Dashboard	> 1	lew I	Create New File I	Filter Rule						
+ Network	>						_			
Policy & Objects	· ·	(darr	Name pdf-zip-block							
Security Profiles	~	Lon	Comments	Writeaco	amment	4 0/0				
AntiVirus		E and	Protocols ()	CIFS			ĸ			
Web Filter		1		FTP		1	ĸ			
Video Filter		Rule		HTTP		1	ĸ			
DNS Filter		1		MAPI (2)			ĸ			
Application Control		14		POP3		3	ĸ			
Intrusion Prevention		R		SMTP			к к			
File Filter				3511	+					
SSL/SSH Inspection			Traffic	Incoming	Outgoing Bo	oth				
Application Signatures										
IPS Signatures			Match Files							
Web Rating Overrides			Password-prote	ected only	0					
Web Profile Overrides			File types		pdf		3	¢		
U VPN					zip	+	,	•		
💄 User & Authentication	•		Action		Monitor	Block		-		
🗢 WiFi Controller	>									
System	•					_		_		
🔆 Security Fabric	>						ÖK	C	ancel	
년 Log&Report	>									



€ FGVM01TM1 08000		≣ Q,						
Dashboard	>	New File Filter	Profile	_				
 Network Policy & Objects Security Profiles AntiVirus Web Filter Video Filter 	* * *	Name Comments Scan archive Feature set Rules	contents 🜑	MyFileFilte Write a con Flow-based	r ament Proxy-base	# 0/255		
DNS Filter Application Control		+ Create	New PE	Edit 🖻 De	lete Searc	h Match Files	Action	Q File Types
File Filter SSL/SSH Inspection	☆	pdf		Both	CIFS FTP	Any	Block	pdf zip
Application Signatures IPS Signatures Web Rating Overrides Web Profile Overrides								0
⊒ VPN ■ User & Authentication 奈 WiFi Controller	> > >					ОК	Car	ncel

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 <u>http://talebi.ca/wp-content/uploads/2021/11/prtgdesktop.pdf</u> 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, Acuntix Web Vulnerability Scanner, Adobe Flash Player CSRF

FGVM01TM19008000	₽ E	E Q.									
🙆 Dashboard	> 1	lew IPS Sensor									
🕂 Network	>										
🛓 Policy & Objects	>	Name Myl	IPS								
Security Profiles	~	Comments	te a comn	nent	//255						
AntiVirus		Block malicious URLs ()	lock malicious ORLs								
Web Filter	Web Filter IPS Signatures and Filters										
Video Filter											
DNSFilter		+Create New & Edit									
Application Control		Details		ExemptIPs	Action	Packet Logging					
Intrusion Prevention		AAEH.Botnet	erability.Scanner	0	Default	Oisabled					
File Filter		Acunetix.Web.Vulnerability.									
SSL/SSH Inspection		Adobe.rlash.Player.CSRF									
Application Signatures						0					
IPS Signatures											
Web Rating Overrides		Botnet C&C									
Web Profile Overrides		Scan Outgoing Connections to B	Botnet Site	S Disable B	Block Monito	or'					
D VPN	>				ALC OF DESIGNATION OF						
🔒 User & Authentication	>										
♥ WiFi Controller	*				ŎК	Cancel					

Figure 7.17: Intrusion Prevention Profile

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

144 Chapter 7. Security



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

Internet Service Database	Service ALL *	
Services	Action 🗸 ACCEPT 🖉 DENY	
Schedules	Inspection Mode Flow-based Proxy-based	
Virtual IPs 💱		
IP Pools	Firewall / Network Options	
Protocol Options	NAT	
Traffic Shaping	IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Po	ol
Security Profiles	Preserve Source Port 🕥	
U VPN	Protocol Options default 🔹 🖋	
💄 User & Authentication 🔹 🔸		
중 WiFi Controller >	Security Profiles	
🗘 System 👩 🔸	AntiVirus 🛈	
🔆 Security Fabric 🔹 🔸	Web Filter 🕥	
년 Log & Report >	Video Filter 🕥	
	DNS Filter 🖤 MyDNS 🔹 🖋	
	Application Control	

Figure 7.19: Assign DNS Filter Profile to Firewall Policy

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

Attention	×	talebi.ca/	×	+		
< → C ŵ	(talebi.ca			… ⊠ ☆	٢

Web Page Blocked!

You have tried to access a web page which belongs to a category that is blocked.

Figure 7.20: Verify configuration

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

146 Chapter 7. Security

+ Network	0 ± 0	Add Filter				🕞 🔹 🔲 Details
Policy & Objects	Date/Time	DNS Type	Source	Domain Name	Query Type	Policy ID
Security Profiles	4 minutes ago	dns-response	192.168.0.4	talebi.ca	A	1
□ VPN >	4 minutes ago	dns-response	192.168.0.4	talebi.ca	A	1
Luser & Authentication	4 minutes ago	dns-response	192.168.0.4	talebi.ca	A	1
* WiFi Controller	6 minutes ago	dns-response	192.168.0.4	talebi.ca	A	1
System U >	6 minutes ago	dns-response	192.168.0.4	fonts.gstatic.com	А	1
M Los Decent	6 minutes ago	dns-response	192.168.0.4	globalurl.fortinet.net	A	1
Enward Traffic	6 minutes ago	dns-response	192.168.0.4	fonts.googleapis.com	A	1
Local Traffic	6 minutes ago	dns-response	192.168.0.4	www.facebook.com	А	1
Sniffer Traffic	6 minutes ago	dns-response	192.168.0.4	www.youtube.com	A	1
Events	6 minutes ago	dns-response	192.168.0.4	getpocket.com	A	1.
AntiVirus	6 minutes ago	dns-response	192.168.0.4	fonts.googleapis.com	A	1
Web Filter	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
DN5Query 🟠	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	ICMP-HTTP-HTTPS	
	Port 2:		
	Vlan 10: 192.168.10.1/24		
	Vlan 20: 192.168.20.1/24		
WebTerm1	DHCP Client	_	
WebTerm2	DHCP Client	-	

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

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

 Table 7.3: Switch configuration

Switch1	configur	ation					
Seneral							
Name:	Switch 1						
Console type:	none						*
iettings			Ports				
Port:	8	\$	Port	+ VLAN	Туре	[E.
VLAN:	20	\$	0	1 10	dot1q access		
Type:	access	-	2	20	access		
QinQ EtherType	: 0x8100	*	3 4	1	access access		*
Add		Delete	•		- P	•	Ė

Figure 7.23: Switch configuration

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

7.3 VLAN and Security Profile 149

Ð	Dashboard	>	New Interface			
+	Network	~	*			
	Interfaces	☆	Name	Vlan10		
	DNS		Alias	1		
	Packet Capture		Туре	Sta VLAN	•	
	SD-WAN		VLAN protocol	802.1Q 802.1AD		
	Static Poutor		Interface	m port2	+	
	Static Routes		VLAN ID	10	•	
	Policy Routes	_	VRFID 0	0	<	
	RIP		Role 🚯	LAN	•	
	OSPF					
	BGP		Address			
	Routing Objects		Addressing mode	e	Manual DH	CP Auto-managed by IPAM
	Multicast		IP/Netmask		192.168.10.1	/24
8	Policy & Objects	>	Create address of	object matching subnet 🗨)	
۵	Security Profiles	>	Name		Vlan10 addr	ress
묘	VPN	>	Destination		192.168.10.1/2	24
-	User & Authentication	>	Secondary IP add	dress a		
¢	System	1 > ⁻				
×	Security Fabric	>				
	FORTIDET	v7.0.5			OK	Cancel

Figure 7.24: Vlan10 Configuration

🙆 Dashboard 🔹 🔊	New Interface			
♣ Network Interfaces ☆	Name	Vlan20		
DNS Packet Capture	Alias Type	蹭 VLAN	•	
SD-WAN	VLAN protocol Interface	802.1Q 802.1AD		
Static Routes Policy Routes		20	 	
RIP OSPF	Role ()	LAN	 V 	
BGP	Address			
Routing Objects Multicast	Addressing mod IP/Netmask	e	Manual DHCP 192.168.20.1/2	Auto-managed by IPAM
 Policy & Objects Security Profiles 	Create address	object matching subnet	Vlan20 addres	is
D VPN	Destination		192.168.20.1/24	
User & Authentication >	Secondary IP ad	dress	•	

Figure 7.25: Vlan20 Configuration

150 Chapter 7. Security

	m port2	Physical Interface	0.0.0/0.0.0	
•••••	📲 vlan10	SH VLAN	192.168.10.1/255.255.255.0	
•	₩ vlan20	鍋 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.

			93 Cloud Applications red 0 policies are using this pr	ofile.	m.
lame	block Youtube-SN	4			
Comments			4 0/255		
ategories					
	ategories				
● ▼ Busir	ness (179, 🗅 6)		● - Cloud.IT (31)	۲	 Collaboration (293, 2 6)
● ▼ Emai	il (87, 🛆 12)		● ▼ Game (124)	۲	• General.Interest (241, 🛆
👁 🕶 Mobi	ile (3)		• Network.Service (332)	0	• P2P (85)
Ø - Prox	y (106)		• Remote.Access (91)		 Social.Media (150,
● ▼ Stora	age.Backup (296, 🗅	16)	● Update (48)		• Video/Audio (206, 🗅 13)
● ▼ VoIP	(31)		• Web.Client (18)	0	 Unknown Applications
		ient			
Networ pplication + Creat	k Protocol Enforcem and Filter Overrides te New Filter	🖻 Delete			
 Networ pplication + Creat Priority 	k Protocol Enforcem and Filter Overrides te New & Edit Details	Delete	Action		
Networ Application + Creat Priority	k Protocol Enforcem and Filter Overrides te New & Edit Details No re	Delete Type sults	Action		

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.

⇒ C ŵk	(i) www.twitter.c	om	… ⊠ ☆
	FortiGa	te Application Control	
	Application	Blocked	
	You have attem	pted to use an application that violates your Internet	t usage policy.
	Application	Twitter	
	Category	Social Media	
	URL	http://www.twitter.com/	
	Username		
	Group Name	2	
	Policy	cf98d74a-b7ca-51ec-edb9-434a2a96fe76	

Figure 7.29: Verify configuration

- 4. Filter .zip, .pdf files on Vlan 10:
 - 1. Create a File filtezr profile. File filter only works on the unencrypted protocol. Set traffic for both and finally set the action to block.

152 Chapter 7. Security

New Policy		New F	Create New File	Filter Rule				
Action	Flow-based Prov	Name Comr Scan	Name Comments	pdf-zip Write a co	mment	<i>≰</i> 0/255		
Firewall / Netwo NAT IP Pool Configura Preserve Source Protocol Options	rk Options o stion Port O ; mm defau	Featu Rules Ru	Protocols () Traffic	CIFS FTP HTTP IMAP POP3 SMTP Incoming	+ Outgoing Both	× × × × × × × ×		
Security Profiles AntiVirus Web Filter	3		Match Files Password-prot	ected only	•			
Video Filter DNS Filter Application Cont			File types Action		pdf zip Monitor	+ Block	××	
File Filter SSL Inspection	C certific					ок		Cancel

Figure 7.30: Block PDF and ZIP files

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

arric		zip-pdf				
omments	5	Write a co	omment	# 0/255		
an archiv	ve contents 🔘					
ature se	t	Flow-base	ed Proxy-base	ed		
iles						
+Crea	ate New	Edit 🗊 D	Delete Sea	rch		Q
Rule	Comments	Traffic	Protocols	Match Files	Action	File Types
Rule pdf	Comments	Traffic Both	Protocols CIFS	Match Files Any	Action Block	File Types
Rule pdf	Comments	Traffic Both	Protocols CIFS FTP	Match Files Any	Action Block	File Types pdf zip

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.

Ð	Dashboard	>	New Policy				
÷	Network	>	Name 0	vlan10			
8	Policy & Objects	*	Incoming Interface	DE vlan10			
	Firewall Policy	습	Outgoing Interface	🗎 port1			
	IPv4 DoS Policy		Source	🔳 all	×		
	Addresses		and the last	-	+		
	Internet Service Database		Destination	😑 all	+ ×		
	Services		Schedule	Co always	*		
	Schedules		Service	ALL ALL	×		
	Virtual IPs		Action	✓ ACCEPT	DENY		
	IP Pools						
	Protocol Options		Inspection Mode	Flow-based Prox	y-based		
	Traffic Shaping						
۵	Security Profiles	>	Firewall / Network C	Options			
₽	VPN	>	NAT	•			
2	User & Authentication	>	IP Pool Configuratio	n Use Outgoir	ng Interface Address	Use Dynamic IP Pool	
(î-	WiFi Controller	>	Preserve Source Por	t 🛈			
۵	System	1>	Protocol Options	PROT defau	lt		
*	Security Fabric	>	Converte Deofiles				
<u>lad</u>	Log & Report	>	Security Promes	-			
			AntiVirus				
			Web Filter				
			Video Filter				
			DNSFilter				
			Application Control				
			IPS				
			File Filter	C FF zip-pdf		8	

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

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



The file "prtgdesktop.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

154 Chapter 7. Security

Chapter 8. VDOM

156 FortiGate Firewall

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
Tubic	0.1.	DUVICUS	configuration

Device	IP address	Access
WebTerm-VDOMA	DHCP Client	HTTPS
WebTerm-VDOMB	DHCP Client	HTTPS
FortiGate	Port 2: DCHP 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:



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

🙆 Das	hboard	>	New Virtual Domain			
🕀 Net	work	>	Virtual Domain	VDOM-B		
🔒 Seci	urity Profiles	>	NGEW Mode	Profile based	Policy based	
🌣 Syst	tem	1 *	Control SNAT	Frome-based	Folicy-based	
VDO	MC			Linited Chater		-
Glol	bal Resources		Comments	United States		-
Adn	ninistrators					11
Adn	nin Profiles					
Firm	nware	1				
Fab	ric Management					
Sett	tings					

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**.

Dashboard	Edit Interface		
Network ✓ Interfaces ☆ DNS ▲ Security Profiles >	Name Alias Type VRF ID ()	 port2 Physical Interface 0 	
🗘 System 🚺 >	Virtual domain	& VDOM-B	·
☆ Security Fabric > ш. Log & Report >	Role 0	Undefined	*
	Address		
	Addressing mod	le	Manual DHCP Auto-managed by IPAM One-Arm Sniffer
	Status		Connected
	Obtained IP/Ne	tmask	192.168.122.53/255.255.25 Renew
	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 🔘	
	Distance		5

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.

 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.

Dashboard >	Edit Interface				
🕂 Network 🗸		W			
Interfaces 🗘	Name	port4			
DNS	Allas	Dhunical Interface			
Security Profiles	Type				
🗘 System 🚺 >	VRFID O	0			
Security Fabric	Virtual domain	6 VDOM-A	· ·		
Hel Log & Report	Role U	Undefined	•		
	Address				
	Address		the second second second second	1	
	Addressing mode	e Manual DHCP Au	to-managed by IPAM One	-Arm Sniffer	
	IP/Netmask	192.168.91.1/255.255	5.255.0		
	Secondary IP add	iress 🔿			
	Administrative A	ccess			
	IPv4	HTTPS	HTTP 0	PING	
		FMG-Access	SSH SSH	SNMP	
		□ FTM	RADIUS Accounting	Security Fabric Connection	
		Speed Test		connection	
	Receive LLDP	Use VDOM Setting Enable	Disable		
	Transmit LLDP	Use VDOM Setting Enable	Disable		
	C DHCP Serve	r			
	DHCP status	Enabled ODisabled			
	Address range	192.168.91.2-192.168.91.254	4		

Figure 8.6: Port4 configuration

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

Network v			
Interfacer A	Name	port3	
	Alias		
UNS	Туре	Physical Interface	
Security Profiles	VRF ID 3	0	
🗱 System 🧾 🕽	Virtual domain	& VDOM-A	-
Security Fabric >	Role 0	Undefined	*
≝ Log & Report. >			
	Address		
	Addressing mod	le	Manual DHCP Auto-managed by IPAM One-Arm Sniffer
	Status		Connected
	Obtained IP/Net	tmask	192.168.122.54/255.255.255.0 Renew
	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	D
	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.

Dashboard	Edit Interface				
	Name	m port5			
Interfaces 🏠	Alias	ports			
DNS	Type	Physical Interface			
Security Profiles	VREID 0	0			
🕸 System 🚺 >	Virtual domain	VDOM-B			
☆ Security Fabric > Log & Report >	Role 🟮	Undefined	•		
	Address				
	Addressing mode	Manual DHCP Aut	to-managed by IPAM One	Arm Sniffer	
	IP/Netmask	192.168.92.1/255.255	.255.0		
	Secondary IP addr	ress 🛈			
	Administrative Ac	Cart			
	Administrative Ac				
	IPV4	FMG-Access			
			RADIUS Accounting	Security Fabric	
		Speed Test	0.00000000000	Connection 1	
	Receive LLDP 0	Use VDOM Setting Enable	Disable		
	Transmit LLDP ()	Use VDOM Setting Enable	Disable		
	DHCP Server				
	DHCR status	C Enabled O Disabled			
	Address range	192.168.92.2-192.168.92.254			
	, indiana and indige	ATELEVOTER ATELEOUTERS			-
FURTINET v7.0.3				OK OK	Cancel

Figure 8.8: Port5 configuration

Creating Administrators for Each VDOM

 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.

Dashboard >	New Administrator					
Network	Username	vdom-a				
Security Profiles	Type	Localliser				
🗘 System 🚺 🗸	1)pc	Match a user on a remote se	rver group			
VDOM		Match all users in a remote	server group			
Global Resources		Use public key infrastructur	e (PKI) group			
Administrators 57	Password		۲			
Admin Drofiles	Confirm Password	******	۲			
Admin Promes	Comments	Write a comment		4 0/255		
Firmware 1	Administrator profile	prof_admin	+	101200		
Fabric Management	Virtual Domains	A root	×			
Settings		& VDOM-A	×			
НА		+				
SNMP						
Poplacement Mercager	Two-factor Authen	tication				
Replacement Messages	C Printer de la la	and the state				
FortiGuard	Restrict login to tru	usted hosts				
Feature Visibility	Restrict admin to g	uest account provisioning only	r.			
Certificates						
☆ Security Fabric >						
Leg & Report >					OK	Cancel

Figure 8.9: Administrators for VDOM-A

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.

Ð	Dashboard >	New Administrator					
÷	Network >						
4	Security Profiles >	Username	vdom-b	_			
ń	System 1 v	Туре	Local User				
T			Match a user on a remote :	erver group			
	VDOM		Match all users in a remote	server group			
	Global Resources	Courses	Use public key infrastructu	re (PKI) group			
	Administrators 🗘	Password		۲			
	Admin Profiles	Confirm Password		۲			
	Firmware	Comments	Write a comment		# 0/255		
		Administrator profile	prof_admin	-			
	Fabric Management	Virtual Domains	o root	×			
	Settings	and a subject of the	O VDOM-B	×			
	HA		+				
	SNMP						
	Replacement Messages	Two-factor Authen	tication				
	FortiGuard	C Restrict login to tru	usted hosts				
	Feature Visibility	Restrict admin to g	uest account provisioning or	lv			
	Certificates						
*	Security Fabric >						
Ш	Log & Report >					OK	Cancel

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, set Device to port3,

+ Network	Automatic gateway retrieval	•		
Interfaces	Destination 1	Subnet Internet Service		
Packet Capture		0.0.0.0/0.0.0.0		
SD-WAN	Gateway Address 0	Dynamic Specify 192.168.122.1		
Static Routes	☆ Interface	m port3 ×		
Policy Routes		+		
RIP	Administrative Distance 0	10		
OSPF	Comments	Write a comment # 0/255		
BGP	Status	Enabled O Disabled		
Routing Objects				
Multicast	Advanced Options			

and set Gateway to the IP of the gateway router.

Figure 8.11: Static route in VDOM-A

2. 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.

🕰 Dashboard	New Policy				
Network	>				
Policy & Objects	Name ()	VDOM-A			
Firewall Policy	Incoming Interface	m port4	•		
IPv4 DoS Policy	Outgoing Interface	m port3	+		
Addresses	Source	🔲 all	×		
Internet Service Database	Destination	all +	×		
Services	Schedule	o always	-		
Schedules	Service	ALL	×		
Virtual IPs		+			
IP Pools	Action	✓ ACCEPT Ø DENY			
Protocol Options	1				
Traffic Shaping	Inspection Mode	Flow-based Proxy-based			
Security Profiles	Firewall / Network O	ptions			
Licer & Authentication	NAT	0			
S WiEi Controllor	IP Pool Configuration	Use Outgoing Interf	ace Address Use Dy	namic IP Pool	
	Preserve Source Port	0			
Security Fabric	Protocol Options	PROT default	•		
년 Log & Report :	Security Profiles				
	AntiVirus	0			
	Web Filter (

Figure 8.12: Firewall Policy in VDOM-A

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

G Google	X Server Not Found X +					
€→℃@	(i) A https://www.google.com/?gws_rd=ssl	∨ ··· ⊠ ☆ Ⅲ\ □ & ≡				
About Store	*	Gmail Images 🔛 Sign in				
	Googl	e				
	Google Search I'm Feeling I Google offered in: Français	Lucky				

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, set Device to port2, and set Gateway to the IP of the gateway router.

	Automatic gateway retrieval 3	
Interfaces	Destination ()	Subnet Internet Service
Packet Capture		0.0.0.0/0.0.0.0
SD-WAN	Gateway Address 0	Dynamic Specify 192.168.122.1
Static Routes 🗳	Interface	m port2 ×
Policy Routes		+
RIP	Administrative Distance 0	10
OSPF	Comments	Write a comment # 0/255
BGP	Status	Enabled ODisabled
Routing Objects		
Multicast	Advanced Options	

Figure 8.14: Static route in VDOM-B

 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.

Dashboard >	New Policy		
Network >	1		
占 Policy & Objects 🛛 🗸 🖌	Name 0	VDOM-B	
Firewall Policy ☆	Incoming Interface	m port5	
IPv4 DoS Policy	Outgoing Interface	m port2	-
Addresses	Source	💷 all 🕂	×
Internet Service Database	Destination	'⊒ all +	×
Services Schedules Virtual IPs	Schedule Service	Co always Q ALL +	×
IP Pools Protocol Options	Action	✓ ACCEPT Ø DENY	
Traffic Shaping	Inspection Mode	Flow-based Proxy-based	
	Firewall / Network C NAT IP Pool Configuration Preserve Source Por Protocol Options	Diptions Use Outgoing Interface A t PROT default	ddress Use Dynamic IP Pool
☆ Security Fabric >			

Figure 8.15: Firewall Policy in VDOM-B

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

Dashboard	> New Traffic Shaper		
 Network Policy & Objects 	Type Shared Per IP Shared Name under h	aper	
Firewall Policy	Vuon-b		
IPv4 DoS Policy	Quality of Service		
Addresses	Traffic priority	High	•
Internet Service Database	Bandwidth unit	kbps	•
Services	Maximum bandwidth	10000	kbps
Schedules	Guaranteed bandwidth	7000	Гкррг
Virtual IPs			
IP Pools			
Protocol Options			
Traffic Shaping	☆		

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**

Network	>	den la			
🖹 Policy & Objects	Name	/dom-b			
Firewall Policy	Status	Enabled	Disabled	- di -	
IPv4 DoS Policy	Comments	Write a commen	t //	0/255	
Addresses	If Traffic Match	es:			
Internet Service Database	Source	🔳 all	+	×	
Services	Destination	🔳 all		×	
Schedules			+		
Virtual IPs	Schedule C	2			
IP Pools	Service	ALL		×	
Protocol Options			+		
Traffic Shaping	☆ LIPL Category		+		
A Security Profiles	>	-			
□ VPN	> Then:				
Loser & Authentication	> Outgoing inter	ace	port2		×
중 WiFi Controller	>			+	
🌣 System	> Apply shaper	0			
🔆 Security Fabric	> Shared shape	r 💽 va	lom-b		•
네 Log & Report	> Reverse shap	er 💽 vo	lom-b		•

Figure 8.17: Traffic Shaping Policy in VDOM-B

5. Now open the browser in WebTerm VDOM-B and go to <u>Fast.com</u> and verify your configuration.



Figure 8.18: Verify configuration in VDOM-B
168 Chapter 8. VDOM

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

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		-

Table 8.2: Devices configuration

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.

🙆 Dashboard	>	New Virtual Domain			
Network	>	Virtual Domain	sales		
 Security Profiles System 	2 ~	NGFW Mode	Profile-based	Policy-based	
VDOM	☆	WiEi country/region	United States		•
Global Resources		Comments	onned States		
Administrators					1.

Figure 8.20: Create a VDOM Sales

Dashboard >	New Virtual Domain			
	Virtual Domain	Accounting		
Security Profiles	NGFW Mode	Profile-based P	olicy-based	
🗘 System 🛛 2 🗸	Central SNAT			
VDOM 🏠	WiFi country/region	United States		
Global Resources	Comments	onited states		
Administrators	Commente			1.

Figure 8.21: Create a VDOM Accounting

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

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

Figure 8.22: Port2 and Port3 IP address configuration

æ	Dashboard	>	Edit Interface						
\$	Network	~	Nama	M nort	2				
	Interfaces	☆	Alios	port	4				
	DNS		Type	Phys	ical Interfac	9			
•	Security Profiles	>	VREID 6	0					
۵	System	2 >	Virtual domain	6 Acc	counting				
*	Security Fabric	>	Role ①	Undefi	ined		-		
Lad	Log & Report	>							
			Address						
			Addressing mod	le	Manual	DHCP	Auto-manage	ed by IPAM	One-Arm Sniffer
			IP/Netmask		172.16.1	1/255.2	55.255.0		
			Secondary IP ad	dress 🔾	•				

Figure 8.23: Port2 configuration

Network Y	Namia	M port?	2				
Interfaces な	Name	ports	2				
DNS	Tupo	Physic	cal Interfac	e			
Security Profiles	VREID 6	0	curinterrae	-			
🗘 System 🛛 😰 🗲	Virtual domain	6 sale	5			-	
Security Fabric	Role 1	Undefin	ned			•	
레 Log & Report >							
	Address						
	Addressing mod	e	Manual	DHCP	Auto-mai	naged by IPAM	One-Arm Sniffer
	IP/Netmask		192.168.	1.1/255.	255.255.0		
	Secondary IP ad	dress 🔿					

Figure 8.24: Port3 configuration

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

Ð	Dashboard	> New VD	OM Link			
+	Network	¥				
	Interfaces	☆ Name	AS			
	DNS	Interface	e 0 (AS0)			
A	Security Profiles	> Virtual E	Domain	Accounting		
•	System	2 > IP/Netm	ask	10.10.10.1/24		
※ 回	Security Fabric Log & Report	Adminis	trative Access	HTTPS HTTPS KG-Access Security Fabric Connection 1	□ HTTP ③ □ SSH	PING SNMP
		Commer	nts	Write a comment	# 0/255	
		Status		Enabled Object Disabled	0,200	
		Interface	e 1 (AS1)			
		Virtual D	Domain	o sales	-	
		IP/Netm	ask	10.10.10.2/24		
		Adminis	trative Access	HTTPS	HTTP 1	D PING
				FMG-Access	SSH	SNMP
				Connection		
		Commer	nts	Write a comment	# 0/255	
		Status		Enabled ODisabled		

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

Destination 🟮	Subnet Internet Service	
	192.168.1.0/24	
Gateway Address	10.10.10.2	
Interface	% AS0 +	×
Administrative Distance 🕚	10	
Comments	Write a comment	# 0/255
Status	Enabled ODisabled	

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

Destination 🕄	Subnet Internet Service	
	172.16.1.0/24	
Gateway Address	10.10.10.2	
Interface	% AS0 +	×
Administrative Distance 🕄	10	
Comments	Write a comment	# 0/255
Status	Enabled ODisabled	

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 🚯	P2	
Incoming Interface	m port2	•
Outgoing Interface	So ASO	•
Source	🗐 all 🕂	×
Destination	💷 all 🕂	×
Schedule	Co always	•
Service	₽ ALL +	×
Action	✓ ACCEPT Ø DENY	
Inspection Mode	Flow-based Proxy-based	
Firewall / Network C	options	
NAT O		
Protocol Options	PROT default	- 6

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

Incoming:

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

Name 1	P1	
Incoming Interface	S ASO	•
Outgoing Interface	m port2	•
Source	🗐 all +	×
Destination	🗐 all +	×
Schedule	o always	•
Service	P ALL +	×
Action	✓ ACCEPT Ø DENY	
Inspection Mode	Flow-based Proxy-based	
Firewall / Network O	ptions	
NAT		
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

Destination 🟮	Subnet Internet Service	
	192.168.1.0/24	
Gateway Address	10.10.10.1	
Interface	% AS1 +	×
Administrative Distance 🜖	10	
Comments	Write a comment	# 0/255
Status	Enabled ODisabled	

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

Destination 🕄	Subnet Internet Service	
	172.16.1.0/24	
Gateway Address	10.10.10.1	
Interface	% AS1	х
	+	
dministrative Distance 🕄	10	
Comments	Write a comment	# 0/255
Status	Enabled ODisabled	

Figure 8.31: Create a static route in Sales VDOM

- 8. In Sales VDOM, Create two Firewall Policies:
 - Incoming: Port3
 - **Outgoing:** AS1
 - NAT Disable

lame 🟮	P1	
ncoming Interface	m port3	-
utgoing Interface	% AS1	-
burce	💷 all 🛨	×
Destination	🗐 all 🕂	×
chedule	Co always	•
ervice	I ALL +	×
ction	✓ ACCEPT Ø DENY	
spection Mode	Flow-based Proxy-based	
ewall / Network C	ptions	
otocol Options	PROT default	- /

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

• Incoming: AS1

- **Outgoing:** Port3
- NAT Disable

Name 🟮	P2	
ncoming Interface	% AS1	-
Outgoing Interface	m port3	-
ource	💷 all 🕂	×
Destination	🗐 all 🕂	×
ichedule	lo always	•
ervice	I ALL +	×
ction	✓ ACCEPT Ø DENY	
nspection Mode	Flow-based Proxy-based	
irewall / Network C	ptions	
AT O		
rotocol Options	PROT 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.

ΨL.	XTern	ninal		
<u>F</u> ile	<u>E</u> dit	Tabs	Help	
root eth0	@webt	Link inet inet UP BF RX pa TX pa coll: RX by	:~# ifconfig encap:Ethernet HWaddr 96:3c:81:44:e4:e5 addr:192.168.1.2 Bcast:0.0.0.0 Mask:255.255.25 6 addr: fe80::943c:81ff:fe44:e4e5/64 Scope:Link ROADCAST RUNNING MULTICAST MTU:1500 Metric:1 ackets:4 errors:0 dropped:0 overruns:0 frame:0 ackets:14 errors:0 dropped:0 overruns:0 carrier:0 isions:0 txqueuelen:1000 oytes:264 (264.0 B) TX bytes:1076 (1.0 KiB)	5.0
lo		Link inet UP LO RX pa TX pa coll: RX by	encap:Local Loopback addr:127.0.0.1 Mask:255.0.0.0 6 addr: ::1/128 Scope:Host OOPBACK RUNNING MTU:65536 Metric:1 ackets:5808 errors:0 dropped:0 overruns:0 frame:0 ackets:5808 errors:0 dropped:0 overruns:0 carrier isions:0 txqueuelen:1000 ytes:492032 (480.5 KiB) TX bytes:492032 (480.5 K	:0 iB)
root PING 64 b 64 b	@webt 172. ytes ytes ytes	erm-1 16.1.2 from 2 from 2 from 2	:~# ping 172.16.1.2 2 (172.16.1.2) 56(84) bytes of data. 172.16.1.2: icmp_seq=1 ttl=62 time=1.85 ms 172.16.1.2: icmp_seq=2 ttl=62 time=3.98 ms 172.16.1.2: icmp_seq=3 ttl=62 time=3.92 ms	

Figure 8.34: Verify configuration

To delete a VDOM link in the CLI:

config system vdom-link delete <VDOM-LINK-Name> end 178 Chapter 8. VDOM

Chapter 9. SD-WAN

180 FortiGate Firewall

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

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
	Port 3: 192.168.20.1/24
FortiGate	Port 4: 10.200.2.1/24
	Port 5: 10.200.3.1/24
	Eth0: connected to WRT Manager
OpenIA/st	Eth1: connected to NAT
Openwitt	Eth2: 10.200.2.254/24
	Eth3: 10.200.3.254/24
NAT	

Table 9.1: Devices configuration

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: <u>http://192.168.1.1</u>, and click on "Login" without entering any password.

OpenWrt - Overview - LuCl 🗙	▲ mozilla.org/privacy/firefox/ × +		
-) > C @ (C	🔏 192.168.1.1/cgi-bin/luci/	ତ ☆	III\ 🗉 🔮
benWrt			
No password set! There is no password set on	this router. Please configure a root password to prote	ect the web interface.	
Authorization	Required		
Username	root		
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	LAN2		
Protocol	Static address		
Device	eth2 ▼		
		Cancel	Create interface

Figure 9.3: Add a new interface

iterraces » L	ANZ	Cathiana	Circuial Pattions	DUICE Consider
Seneral Settings	Advanced	settings	Firewall Settings	DHCP Server
	Status	Devi MAC RX: 0 TX: 0	ce: eth2 : 0C:76:09:C7:00:0 0 B (0 Pkts.) 0 B (0 Pkts.)	2
	Protocol	Static ad	ddress	•
	Device	eth2		•
Bring u	p on boot			
IPv4	4 address	10.200.2	2.254	
IPv4	netmask	255.255	.255.0	*
IPv4	gateway	132,166	τi≥i (wan]	

Figure 9.4: LAN2 IPv4 configuration

184 Chapter 9. SD-WAN

Interfaces » L	AN2		
General Settings	Advanced Set	ings Firewall Setting	DHCP Server
reate / Assign fire	wall-zone	n lan: 🔊	•
	C C C C C C C C C C C C C C C C C C C	choose the firewall zon nterface from the asso nterface to it.	e you want to assign to this interface. Select <i>unspecified</i> to remove the ciated zone or fill out the <i>custom</i> field to define a new zone and attach t
			Dismiss

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

	*
LAN3	
Static address	•
💒 eth3	
	LAN3 Static address

	-
Cancel	Create interface

Figure 9.6: Add a new interface (LAN3)

General Settings	Advanced	Settings	Firewall Settings	DHC	P Server
	Status	Devi MAC RX: TX: (ce: eth3 : 0C:76:09:C7:00:0 0 B (0 Pkts.) 0 B (0 Pkts.)	3	
	Protocol	Static ad	ddress	-	
	Device	eth3		•	
Bring u	p on boot				
IPv4	4 address	10.200.3	3.254		***
IPv4	netmask	255.255	.255.0	*	
IPv4	l gateway	152.165	1.12 (1. (wan)		

Figure 9.7: IP configuration for LAN3

Interfaces » l	LAN3		
General Settings	Advanced Settings	Firewall Settings	DHCP Server
Create / Assign fire	wall-zone lan lan	: 🎜 LAN2: 🖉	*
	Choos interfa	e the firewall zone y ce from the associa ce to it.	you want to assign to this interface. Select <i>unspecified</i> to remove the ated zone or fill out the <i>custom</i> field to define a new zone and attach the
			Dismiss Save

Figure 9.8: Firewall settings for LAN3

Your interfaces in OpenWrt should be like Figure 9.9:

186 Chapter 9. SD-WAN



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**.

Network	~	nort4					
Interfaces	☆ Name	I port4					
DNS	Alias	WAN2	Unterface				
Packet Capture	Type	m Physica	interface				
SD-WAN	VRFID	0			•		
Static Routes	Kole U	Undefine	ed		•		
Policy Routes	Address						
RIP	Addressir	ng mode	Manual	DHCP	Auto-man	aged by IPAM	One-Arm Sniffer
OSPF	IP/Netma	isk	10.200.3	2.1/24		0,	
BGP	Secondar	v IP address C	>				
Routing Objects							

Figure 9.10: Port4 configuration

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

Network	~	Manua	m port5					
Interfaces	合	Alias	WAN3					
DNS	合	Туре	Physical I	nterface				
Packet Capture		VRFID 0	0			~		
Static Routes	_	Role	Undefined			•		
Policy Routes		Address						
RIP		Addressing	mode	Manual	DHCP	Auto-mana	aged by IPAM	One-Arm Sniffer
OSPF		IP/Netmask		10.200.3	.1/24			
BGP		Secondary II	Paddress 🔿					
Routing Objects								

Figure 9.11: Port5 configuration

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

188 Chapter 9. SD-WAN



Figure 9.12: Add port4 as SD-WAN members

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

	Network	~		
1	Interferen	Interface	Im WAN3 (port5)	•
	Interfaces	SD-WAN Zone	virtual-wan-link	-
	DNS	Gateway	10.200.3.254	
	Packet Capture	Cost	0	-
	SD-WAN	Priority	0	-
	Static Routes	Status	Enabled Disabled	(°
	Policy Routes	otatas	C Endored	
	RIP			
	OSPF			
	BGP			
	Routing Objects			
	Multicast			

Figure 9.13: Add port5 as SD-WAN members



Figure 9.14: SD-WAN Zones

6. Create a static route as Figure 9.15.

🙆 Dashboard	>	New Static Route						
Network Interfaces DNS	Ť	Automatic gateway retrieval 🕄 🔿 Destination 🚱 Subnet Internet Service						
Packet Capture SD-WAN		Interface	🗟 virtual-wan-link 🗶					
Static Routes	습	Comments	Write a comment // 0/255					
Policy Routes RIP OSPF BGP Routing Objects Multicast		Status	C Enabled O Disabled					
🚊 Policy & Objects	>							

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

190 Chapter 9. SD-WAN

Đ	Dashboard	>	New Policy			
\$	Network	3>				
B	Policy & Objects	~	Name 🚯	SDWAN		
	Firewall Policy	습	Incoming Interface	m port3		•
	IPv4 DoS Policy		Outgoing Interface	🗟 virtual-wan-l	ink	-
	Addresses		Source	🚍 all		×
	Internet Service Database		Destination	🗉 all	+	×
	Services		Schedule	G always		
	Schedules		Service			~
Ę	Virtual IPs		Service	SP ALL	+	~
	IP Pools		Action	✓ ACCEPT 🥝	DENY	
	Protocol Options					
	Traffic Shaping		Inspection Mode	Flow-based Proxy	v-based	
۵	Security Profiles	>	and the second second second second			
묘	VPN	>	Firewall / Network O	ptions		
	User & Authentication	>	NAT	•		
(:	WiFi Controller	,	IP Pool Configuration	use Outgoi	ng Interface Ad	dress
۵	System	1 >		Use Dynam	ic IP Pool	
	FERTIDET	v7.0.3			ОК	Cancel

Figure 9.16: Create a Firewall Policy

- 8. Go to **Network > SD-WAN Rul**e, 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

Dashboard	> Priority Rule	2			
Network Interfaces DNS	Name N	ИуRule	×		
Packet Capture	Source add	iress 🔳 all	+	×	
Static Routes Policy Routes	User group		+		
RIP	Destination	n			
OSPF	Address	🗐 all	+	×	
Routing Objects	Protocol n	number TCP	UDP ANY Spe	cify 0	
Multicast	> Application	0	+		

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

Zone preference	+	
Measured SLA	Default_AWS	
Quality criteria	Q Search	+ Create
Forward DSCP	Default_AWS	1

Figure 9.18: Add target

New Performance SLA				
NameMySLProbe mode IActiveProtocolPingServer4.2.2.	A I Passive Prefe HTTP DNS	er Passive		
Participants All SD	-WAN Members	Specify		
SLA Target				
Link Status				
Check interval Failures before inactive Restore link after ()	500 5 5 5	() () ()	ms check(s)	
Actions when Inactive				
Update static route 🚯	D			
		(Ж	Cancel

Figure 9.19: Create a SLA

9.1 SD-WAN 193

Interfaces		Outgoing Interfaces			Addi
DNS		Select a strategy for he	ow outgoing interfaces will be ch	osen.	0
Packet Capture SD-WAN	☆	O Manual Manually assign o	outgoing interfaces.		
Static Routes Policy Routes		Best Quality The interface with	h the best measured performanc	e is selected.	
RIP OSPF BGP Routing Objects		 Lowest Cost (SLA The interface tha the interface with Maximize Bandw Traffic is load bala 	A) t meets SLA targets is selected. n the lowest assigned cost is sele ridth (SLA) anced among interfaces that mee	When there is a tie, cted. et SLA targets.	
Multicast Policy & Objects	, ,	Interface preference	WAN2 (port4) WAN3 (port5)	×××	
I VPN	>	Zone preference	+		
User & Authentication	>	Measured SLA	MySLA	•	
중 WiFi Controller	>	Quality criteria	Latency	-	
🗢 System	1>	Forward DSCP			
🔆 Security Fabric	>	Reverse DSCP			
🔟 Log & Report	>	Status	💿 Enable 🔮 Disable		
FERTIDET	v7.0.3			OK Car	ncel

Figure 9.20: SD-WAN Configuration

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

SD-WAN Zones	SD-WAN Ru	les Performance SLAs		
Bandwidth Volume	Sessions			
-		Download		Upload
2 Ter		port4	2 Total	port4
+ Create New -	🖋 Edit 💼	Delete		

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

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



13. 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

🙆 Dashboard 🗸 🗸	FortiView Se	ssions					🕞 now - 🗧	1.
Status Security	• Add Filter							
🗄 Network	Source	Device	Destination	Application	Protocol	Source Port	Destination Port	
Users & Devices	192.168.20.2		4.2.2.4	UDP/53	UDP	50235	53	d
+	192.168.20.2		4.2.2.4	UDP/53	UDP	50449	53	5
FortiView Dectinations	192.168.20.2		23.20.201.44	TCP/443	ТСР	35418	443	8.4
FortiView Applications	192.168.20.2		4.2.2.4	UDP/53	UDP	50345	53	4
FortiView Web Sites	192.168.20.2		4.2.2.4	UDP/53	UDP	50426	53	2
FortiView Policies	192.168.20.2		4.2.2.4	UDP/53	UDP	50736	53	2
FortiView Sessions	192.168.20.2		4.2.2.4	UDP/53	UDP	50779	53	2
+	192.168.20.2		4.2.2.4	UDP/53	UDP	50582	53	4
Network >	192.168.20.2		50.18.10.184	TCP/443	TCP	53074	443	37.5
Policy & Objects	192.168.20.2		142.250.191.66	TCP/443	TCP	33034	443	91.0
Security Profiles	192.168.20.2		4.2.2.4	UDP/53	UDP	49176	53	2
⊒ VPN >	192.168.20.2		4.2.2.4	UDP/53	UDP	49042	53	\$
Super & Authentication	192.168.20.2		4.2.2.4	UDP/53	UDP	49128	53	3
System	192.168.20.2		4.2.2.4	UDP/53	UDP	49439	53	2
Security Fabric	192.168.20.2		4.2.2.4	UDP/53	UDP	49465	53	Ę

Figure 9.25: FortiView Sessions

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

FGVM01TM19008000	• = Q	_	>.	- 😯 - 🗘 🔁 - 🕗 admin -
🕂 Network >	2 ± 0 A	dd Filter	Line SD-W	AN Events • 🕞 • 🗇 Details
Policy & Objects	Date/Time	Level	Message	Log Description
□ VPN >	8 minutes ago	(acces	Service prioritized by performance metric will	SDWAN status
Luser & Authentication	8 minutes ago	•	Member link is unreachable or miss threshold	SDWAN status
	8 minutes ago		SD-WAN health-check member changed state.	SDWAN SLA notification
🗘 System 👔 🔉	8 minutes ago		Service prioritized by performance metric will	SDWAN status
🔆 Security Fabric 🔷 🕨	8 minutes ago	- Cicloide	Member link is available. Start forwarding traff	SDWAN status
년 Log & Report 🛛 🗸 🗸	8 minutes ago	- COOPIE	SD-WAN health-check member changed state.	SDWAN SLA notification
Forward Traffic	8 minutes ago	CCICCIC:	Service prioritized by performance metric will	SDWAN status
Local Traffic	8 minutes ago	- COORC	Member link is unreachable or miss threshold	SDWAN status
Sniffer Traffic	8 minutes ago	in the local data	SD-WAN health-check member changed state.	SDWAN SLA notification
Events 🖍	9 mínutes ago	- accord	Service prioritized by performance metric will	SDWAN status
AntiVirus	9 minutes ago	- LOOD	Member link is available. Start forwarding traff	SDWAN status
Web Filter	9 mínutes ago		Member link is available. Start forwarding traff	SDWAN status
SSL	9 minutes ago		SD-WAN health-check member changed state.	SDWAN SLA notification
DNS Query	9 minutes ago		SD-WAN health-check member changed state.	SDWAN SLA notification
File Filter	15 minutes ago	and a cost of	Service disabled caused by no outgoing path.	SDWAN status warning
Intrucion Provention	15 minutes ago		Service failover to other available interface(s).	SDWAN status
Anomaly	15 minutes ago		Member link is unreachable or miss threshold	SDWAN status

Figure 9.26: SD-WAN Events

Chapter 10. Cloud Technologies

198 FortiGate Firewall

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

Device	Configuration	Access
FortiCato	Port 1: DHCP Client	Port1: HTTP, HTTPS, PING
FULUGALE	Port 2: 192.168.10.1/24	
WebTerm1	192.168.10.2/24	-

Table 10.1: On-premise devices configuration

Azure Configuration

- 1. Create a resource group in Azure as following:
 - Resource group: **FG**
 - Region: West US

+ Create 😟 Manage view 🗸 🕐 Refresh 🞍 Ecopit 10.03		
	51 😚 Open query 🖗 Adago (lug)	
Filter for any hold Subscription == Azure subscriptio	n 1 Location == all X 'Q' Add hiter	
• O Unsecure resources		No grouping V == List view V
Name 📬	Subscription ↑↓	Location †↓
	(e)	
	1. mg	
	Try changing or clearing your filters	
	Creste resource group	
	Learn more of	
Figure 10.2: Create a resour	rce group	
Home > Resource groups >		
Home > Resource groups >	roup	
Home > Resource groups > Create a resource g	roup …	
Home > Resource groups > Create a resource g	roup …	
Home > Resource groups > Create a resource g	roup	
Home > Resource groups > Create a resource groups > Basics Tags Review + creat	roup	
Home > Resource groups > Create a resource group > Basics Tags Review + creat Resource group - A container that I	roup te	group can include all the
Home > Resource groups > Create a resource g Basics Tags Review + creat Resource group - A container that I resources for the solution, or only th	roup te holds related resources for an Azure solution. The resource hose resources that you want to manage as a group. You d	group can include all the lecide how you want to
Home > Resource groups > Create a resource group Basics Tags Review + creat Resource group - A container that H resources for the solution, or only the allocate resources to resource group	roup te holds related resources for an Azure solution. The resource hose resources that you want to manage as a group. You d ps based on what makes the most sense for your organizar	egroup can include all the lecide how you want to tion. Learn more 더
Home > Resource groups > Create a resource group Basics Tags Review + creat Resource group - A container that h resources for the solution, or only th allocate resources to resource group Project details	roup te holds related resources for an Azure solution. The resource hose resources that you want to manage as a group. You d ps based on what makes the most sense for your organizad	group can include all the lecide how you want to tion. Learn more 더
Home > Resource groups > Create a resource group Basics Tags Review + creat Resource group - A container that P resources for the solution, or only the allocate resources to resource group Project details	te holds related resources for an Azure solution. The resource hose resources that you want to manage as a group. You d ps based on what makes the most sense for your organizat	: group can include all the ecide how you want to tion. Learn more ⊡ ³
Home > Resource groups > Create a resource group Basics Tags Review + creat Resource group - A container that I resources for the solution, or only the allocate resources to resource group Project details Subscription * ①	roup te holds related resources for an Azure solution. The resource hose resources that you want to manage as a group. You d ps based on what makes the most sense for your organizat	e group can include all the lecide how you want to tion. Learn more 🗗
Home > Resource groups > Create a resource group Basics Tags Review + creat Resource group - A container that H resources for the solution, or only th allocate resources to resource group Project details Subscription * ① Resource group * ①	roup te holds related resources for an Azure solution. The resource hose resources that you want to manage as a group. You d ps based on what makes the most sense for your organizat Azure subscription 1 FG	e group can include all the lecide how you want to tion. Learn more 🗗
Home > Resource groups > Create a resource group Basics Tags Review + creat Resource group - A container that P resources for the solution, or only the allocate resources to resource group Project details Subscription * ① Resource group * ①	roup te holds related resources for an Azure solution. The resource hose resources that you want to manage as a group. You d ps based on what makes the most sense for your organizat Azure subscription 1 FG	e group can include all the lecide how you want to tion. Learn more 🗗
Home > Resource groups > Create a resource group Basics Tags Review + creat Resource group - A container that + resources for the solution, or only th allocate resources to resource group Project details Subscription * ① Resource group * ① Resource details	roup te holds related resources for an Azure solution. The resource hose resources that you want to manage as a group. You d ps based on what makes the most sense for your organizat Azure subscription 1 FG	e group can include all the lecide how you want to tion. Learn more 🗗

Figure 10.3: Create a resource group

Create	a	resource	group	

Validatio	n passed. gs Review + create	
Basics		
Subscription		Azure subscription 1
Resource gro	qu	FG
Region		West US
Tags		
None		
1		
	Denteur	New Complex distances for an entities

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**

Basics IP Addresses Security	y Tags Review + create	
Azure Virtual Network (VNet) is the for Azure resources, such as Azure Virtua networks. VNet is similar to a traditio benefits of Azure's infrastructure sucl	undamental building block for your private network in Az al Machines (VM), to securely communicate with each oth nal network that you'd operate in your own data center, h as scale, availability, and isolation. Learn more about vi	ure. VNet enables many types of er, the internet, and on-premises but brings with it additional rtual network
Project details		
Subscription * ①	Azure subscription 1	\sim
Resource group * (i)	FG	\sim
	Create new	
Instance details		
Name *	Azure-FG	\checkmark
Region *	West US	~
Review + create	< Previous Next : IP Addresses >	Download a template for automation
Review + create gure 10.5: Create a virtual r	< Previous Next : IP Addresses > network	Download a template for automation Edit subnet
Review + create pure 10.5: Create a virtual r reate virtual network —	<pre> Previous Next : IP Addresses > network </pre>	Download a template for automation Edit subnet
Review + create gure 10.5: Create a virtual r reate virtual network	< Previous Next : IP Addresses > network	Download a template for automation Edit subnet Subnet name *
Review + create gure 10.5: Create a virtual r reate virtual network … asics IP Addresses Security Tags Rev	<pre> Next : IP Addresses > network iew + create </pre>	Download a template for automation Edit subnet Subnet name * default Subnet address range * ①
Review + create gure 10.5: Create a virtual r reate virtual network … asics IP Addresses Security Tags Rev ae virtual network's address space, specified as one or IPv4 address space	< Previous	Download a template for automation Edit subnet Subnet name * default Subnet address range * ① 10.0.1.0/24 10.0.10.101.01.255 (251 + 5 Azure)
Review + create gure 10.5: Create a virtual r reate virtual network asics IP Addresses Security Tags as virtual network's address space, specified as one or IPv4 address space 100.00/16 100.00/16	< Previous Next : IP Addresses > network iew + create more address prefixes in CIDR notation (e.g. 192.168.1.0/24). es)	Download a template for automation Edit subnet Subnet name * default Subnet address range * () 10.0.1.0/24 10.0.1.0/255 (251 + 5 Azure 1) addresses)
Review + create pure 10.5: Create a virtual r reate virtual network … usics IP Addresses Security Tags Rev e virtual network's address space, specified as one or IPv4 address space 10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 address	< Previous Next : IP Addresses > network iew + create more address prefixes in CIDR notation (e.g. 192.168.1.0/24). es)	Download a template for automation Edit subnet Subnet name * default Subnet address range * () 10.0.1.0/24 10.0.1.0/25 (251 + 5 Azure) addresses) NAT GATEWAY
Review + create gure 10.5: Create a virtual r reate virtual network asics IP Addresses Security Tags ne virtual network's address space, specified as one or IP-4 address space 10.0.00/16 10.0.0.0 - 10.0.255.255 (65536 address Add IPv6 address space ©	< Previous	Download a template for automation Edit subnet Subnet name * default Subnet address range * () 10.0.1.0/24 10.0.1.0/24 10.0.1.0/25 (251 + 5 Azure) addresses) NAT GATEWAY Simplify connectivity to the internet usi network address translation gateway. O
Review + create gure 10.5: Create a virtual r reate virtual network reside virtual network asics IP Addresses Security Tags revitual network's address space, specified as one or IPV4 address space 10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 address Add IPv6 address space © The subnet's address range in CIDR notation (e.g. 192 retwork.	< Previous	Download a template for automation Edit subnet Subnet name * default Subnet address range * () 10.0.1.0/24 10.0.1.0/24 10.0.1.0/255 (251 + 5 Azure 1 addresses) NAT GATEWAY Simplify connectivity to the internet usi network address translation gateway. G connectivity is possible without a load I or public P addresses attached to your machines. Learn more
Review + create pure 10.5: Create a virtual r reate virtual network resics IP Addresses security Tags revitual network's address space, specified as one or ID0.00.0/16 10.0.00 - 10.0.255.255 (65536 address Add IPv6 address space O The subnet's address range in CIDR notation (e.g. 192 + Add subnet Image Remove subnet	Intervious Next : IP Addresses > network new + create more address prefixes in CIDR notation (e.g. 192.168.1.0/24). resj .168.1.0/24). It must be contained by the address space of the virtual	Download a template for automation Edit subnet Subnet name * default Subnet address range * () 10.0.1.0/24 10.0.10.4 10.0.1.255 (251 + 5 Azure t addresses) NAT GATEWAY Simplify connectivity to the internet us network address transition gateway. O connectivity is possible without a load or public IP addresses attached to your machines. Learn more NAT gateway
Review + create gure 10.5: Create a virtual r reate virtual network reate virtual network asics IP Addresses Security Tags revitual network's address space, specified as one or IP-4 address space 100.00/16 10.0.00 - 10.0.255.255 (65536 address Add IPv6 address space Image: CIDR notation (e.g. 192) Add subnet's address range in CIDR notation (e.g. 192) retwork. Image: Remove subnet Add subnet Image: Remove subnet Subnet name Subnet 1	< Previous	Download a template for automation Edit subnet Subnet name * default Subnet address range * () 10.0.1.0/24 10.0.1.0/24 10.0.1.0/255 (25T + 5 Azure) addresses) NAT GATEWAY Simplify connectivity to the internet us network address translation gateway. O connectivity is possible without a load t or public P addresses attached to your machines. Learn more NAT gateway None
Review + create gure 10.5: Create a virtual r reate virtual network reate virtual network asics IP Addresses Security Tags review rk/s address space, specified as one or IV4 address space 10.0.0.0/16 10.0.255.255 (65536 address Add IPv6 address space Image: CIDR notation (e.g. 192 network: Add subnet Image: Remove subnet Subnet name Subnet a Idefault 10.0.0.0/	< Previous	Download a template for automation Edit subnet Subnet name * default Subnet address range * ① 10.0.1.0/24 10.0.1.255 (251 + 5 Azure to addresses) NAT GATEWAY Simplify connectivity to the internet usi network address translation gateway. O connectivity is possible without a load to or public IP addresses attached to your machines. Learn more NAT gateway None SERVICE ENDPOINTS
Review + create gure 10.5: Create a virtual r reate virtual network asics IP Addresses security Tags Rev he virtual network's address space, specified as one or IPV4 address space Intervertified as one or IN0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 address Add IPv6 address space Intervertified as one or Add subnet Remove subnet Subnet name Subnet a Vise of a NAT gateway is recommended for outbound in a subnet after you create the virtual network. Learn mo	Intermet access from a subnet. You can deploy a NAT gateway and assign it to resident.	Download a template for automation Edit subnet Subnet name * default Subnet address range * () 100.10.40/24 100.10.10.01.255 (251 + 5 Azure ta addresses) NAT GATEWAY Simplify connectivity to the internet us network address translation gateway. O connectivity is possible without a load or public IP addresses attached to your machines. Learn more NAT gateway None SERVICE ENDPOINTS Create service endpoint policies to allor to specific azure resources from your network over service endpoint policies to allor
Review + create gure 10.5: Create a virtual r reate virtual network asics IP Addresses security Tags Rev security asics IP Address space 10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 address Add IPv6 address space Image: Comparison of the subnet's address space Add subnet's address space Image: Comparison of the subnet's address space Add subnet Remove subnet Subnet name Subnet a Idefault 10.0.0.0/ Use of a NAT gateway is recommended for outbound in a subnet after you create the virtual network. Learn more	Intervious Next : IP Addresses > Intervious Intervious <	Download a template for automation Edit subnet Subnet name * default Subnet address range * 100.10/24 100.10/24 100.10/24 100.10/255(251 + 5 Azure taddresses) NAT GATEWAY Simplify connectivity to the internet us network orderes translation gateway. Connectivity is possible without a load to or public IP addresses attached to your machines. Learn more NAT gateway None SERVICE ENDPOINTS Create service endpoint policies to alloi to specific azure resources from your or network over service endpoints. Learn or Services ③

Save Cancel

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

Dasics if Addresses 3c		Neview + create	
BastionHost 🕕	Disable		
	O Enable		
DDoS Protection Standard ①	 Disable 		
	O Enable		
Simul O	Disable		
Firewall 🕕	C Enable		

 Review + create

 Previous
 Next : Tags >
 Download a template for automation

Figure 10.7: Create a virtual network

Create virtual network
asics IP Addresses Se	curity Tags	Review +	+ create	
ags are name/value pairs that outline resources and resources	enable you to ca	tegorize reso	ources and view consolidated	billing by applying the same tag to
ote that if you create tags and	then change re	source settin	ngs on other tabs, your tags wi	ill be automatically updated.
Name ①			Value ①	
]	+	

Figure 10.8: Create a virtual network

Basics IP	Addresses	Security	Tags	Review + create		
Basics						
Subscription			Azure	subscription 1		
Resource grou	up		FG			
Name			Azure	-FG		
Region			West	US		
IP addresses						
Address space	e		10.0.0	.0/16		
Subnet			defau	lt (10.0.1.0/24)		
Tags						
None						
Security						
BastionHost			Disab	led		

Create virtual network

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: 10.0.0/24
 - Public IP address name: AzurePublic

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

Home >					
Virtual network gateways 🔅 … Default Directory					×
+ Create 🕲 Manage view 🗸 🚫 Refresh 🛓 Expon to CSV 🚿	🖇 Open query 👘 🖏 Assign tags				
Filter for any fieldSubscription == Azure subscription 1	Resource group == all \times Location == all \times $*_{\nabla}$ Add filter				
			No grouping	✓ Ist vie	« ~
Name 1	Virtual ↑↓ Gatew ↑↓ Resource group ↑↓	Location 1.1	Sub	scription 14	
	No virtual network gateways to displ	av			
Azu	re VPN Gateway connects your on-premises networks to Azure through Site-to-Site	VPNs in a similar way that you			
3	et up and connect to a remote branch office. The connectivity is secure and uses the Internet Protocol Security (IPsec) and Internet Key Exchange	e industry-standerd protocols (IKE).			
	Create virtual network gateway				
	Learn more about Virtual network gateway 13*				

Figure 10.10: Create a virtual network gateway

Create virtual network gateway

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Azure subscription 1	\sim
Resource group ①	FG (derived from virtual network's resource group)	
Instance details		
Name *	Azure-VPN-FG	~
Region *	West US	\checkmark
Gateway type * 🛈	● VPN ○ ExpressRoute	
VPN type * 🕕	Route-based Policy-based	
SKU * ①	VpnGw2	~
Generation ①	Generation1	~
Review + create	evious Next : Tags > Download a template for automatio	on

Figure 10.11: Create a virtual network gateway

Create virtual network gateway

Gateway subnet address range * 🕕	10.0.0/24 🗸
	10.0.0.0 - 10.0.0.255 (256 addresses
Public IP Address Type * 🛈	Basic Standard
Public IP address	
Public IP address *	Create new O Use existing
Public IP address name *	AzurePublic 🗸
Public IP address SKU	Standard
Assignment	O Dynamic 💽 Static
nable active-active mode * 🕕	Enabled Oisabled
Configure BGP * 🕕	O Enabled O Disabled
Azure recommends using a validated nstructions for configuration, refer to	VPN device with your virtual network gateway. To view a list of validated devices and Azure's documentation regarding validated VPN devices.

Figure 10.12: Create a virtual network gateway

Create virtual network gateway

Basics Tags Review + crea	te
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	

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

Microsoft Azure		P Search resources services and flocs (5+/)					cisabcit@outlook.com
Home > Microsoft.Vi	irtualNe	etworkGateway-20220427143	943 Overviev	v 🖈 …		Notifications	×
Deployment	*	🗐 Delete 🛇 Cancel 🖄 Redieploy 💙 Re	fresh			More events in the activity log +	Dismiss all 🗸
A Overview		Ø We'd love your feedback! →				 Deployment in progress Deployment to resource group 'FG' is in progress. 	Running ×
🐼 Inputs		-			-	nehodunum in union of drank on in a hodicare	a few seconds ago
Cutputs		Deployment is in progres	s			Successfully deleted subset	
🖹 Template		Deployment name: Microsoft.VirtualNetwo Subscription: Azure subscription 1 Resource group: FG	orkGateway-2022042714	Start time: 4/27/2022, 2:42:5 Correlation ID: 489b63db-2c.	1 PM 37-4721-a926-cc	Successfully deleted subnet 'Gateway'.	4 minutes ago.
						Successfully added subnet	×
		Resource	Type		Status	Successfully added subnet 'Gateway' to virtual netw	iofk 'Azüre-FG'.
		AzurePublic	Microsoft Net	work/publictPAddresses	Created		6 minutes ago
		Azure-FG/GatewaySubnet	Microsoft.Net	work/virtualNetworks/subnets	OK	Deployment succeeded	X

Figure 10.14: Create a virtual network gateway (deployment)



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

Filter for any field	cription 1 Resource group == all \times Location == all \times $\stackrel{+}{\to}$ A	dd filter			
			No grouping	✓ I III List view	`
Name 1	Resource group ↑↓	Location 14	Subscripti	ion 14	
	-				
	66				
	No local network gateway	to display			
	Create a local network gateway to represent the on-premises site that	you want to connect to a virtual network. Th	e		
	local network gateway specifies the public IP address of the VPN den premises site. Later, create a VPN gateway connection between the via and the local network gateway for the o	ce and IP address ranges located on the on- tual network gateway for the virtual network n-premises site.	4		
	Create local network gatew	ay			
	Learn more of				
iaure 10 16 [.] Create a loc	ral network aateway				
igure 10.101 Greate a loc	ar network gate way				
Home > Local network gateways >					
Create lacal network	gatoway				
Create local network	gateway				
Create local network	gateway				
Basics Advanced Review + c	reate				
Basics Advanced Review + c	reate				
Basics Advanced Review + c A local network gateway is a specific of more	reate object that represents an on-premises location (the s	ite) for routing purposes. Le	aarn		
Basics Advanced Review + c A local network gateway is a specific o more.	reate object that represents an on-premises location (the s	ite) for routing purposes. Le	sərn		
Basics Advanced Review + c A local network gateway is a specific of more. Project details	reate object that represents an on-premises location (the s	ite) for routing purposes. Le	earn		
Basics Advanced Review + c A local network gateway is a specific of more. Project details Subscription *	reate object that represents an on-premises location (the s	ite) for routing purposes. Le	sarri V		
Basics Advanced Review + c A local network gateway is a specific or more. Project details Subscription *	Preate Azure subscription 1	ite) for routing purposes. Le	earn V		
Basics Advanced Review + ct A local network gateway is a specific or more. Project details Subscription * Resource group *	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new	ite) for routing purposes. Le	earn V		
Basics Advanced Review + c A local network gateway is a specific of more. Project details Subscription * Resource group *	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new	ite) for routing purposes. Le	earn V		
Basics Advanced Review + c A local network gateway is a specific or more. Project details Subscription * Resource group *	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new	ite) for routing purposes. Le	earn V		
Basics Advanced Review + cl A local network gateway is a specific or more. Project details Subscription * Resource group * Instance details Region *	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new West US	ite) for routing purposes. Le	earn ~		
Basics Advanced Review + cl A local network gateway is a specific or more. Project details Subscription * Resource group * Instance details Region * Name *	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new West US FortiGate	ite) for routing purposes. Le			
Basics Advanced Review + c A local network gateway is a specific or more. Project details Subscription * Resource group * Instance details Region * Name * Endmaint On	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new West US FortiGate	ite) for routing purposes. Le	earn		
Basics Advanced Review + cl A local network gateway is a specific or more. Project details Subscription * Resource group * Instance details Region * Name * Endpoint ①	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new West US FortiGate IP address FQDN	ite) for routing purposes. Le	Parn		
Basics Advanced Review + cl A local network gateway is a specific or more. Project details Subscription * Resource group * Instance details Region * Name * Endpoint ① IP address * ①	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new West US FortiGate (P address FQDN) 142.232.198.154	ite) for routing purposes. Le	earn > > >		
Basics Advanced Review + cl A local network gateway is a specific or more. Project details Subscription * Resource group * Instance details Region * Name * Endpoint ① IP address * ① Address Space(s) ①	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new West US FortiGate IP address FQDN 142.232.198.154-	ite) for routing purposes. Le	earn		
Basics Advanced Review + c A local network gateway is a specific of more. Project details Subscription * Resource group * Instance details Region * Name * Endpoint ① IP address * ① Address Space(s) ①	reate object that represents an on-premises location (the s Azure subscription 1 FG Create new West US FortiGate IP address FQDN 142.232.198.154	ite) for routing purposes. Le			

Figure 10.17: Create a local network gateway

Basics Advanced Review + create	
Summary	
Name FortiGate	
Subscription Azure subscription	1
Region FG West US	
Endpoint IP address	
P address 142.232.198.154 Address Space(s) 192.168.10.0/24	

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 gateway	s > Azure-VPN-FG >
Add connection	r en
Name *	
VPNAZ	~
Connection type ①	
Site-to-site (IPsec)	\sim
*Virtual network gateway ①	A
Azure-VPN-FG	
*Local network gateway ①	>
FortiGate	
Shared key (PSK) * 🛈	
123456789	~
Use Azure Private IP Address	
Enable BGP ①	
IKE Protocol ①	
◯ IKEv1	
Ingress NAT Rules	

Figure 10.21: Connection configuration

Based on the Microsoft article <u>"About cryptographic requirements and Azure VPN</u> <u>gateways</u>", 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 🖈						×
P Search (Ctrl+/)	\bigcirc Refresh \rightarrow M	love 🗸 📋 Delete				
Q Overview	∧ Essentials					ISON View
Activity log	Resource group (mos	(c) ; EG		SKU : Vpr	nGwZ	
Access control (IAM)	Location	; West US		Gateway type : VPM	N	
Taris	Subscription (move)	: Azure subscription 1		VPN type : Rou	ute-based	
	Subscription ID	: 9170d5fe-6ca8-4257-9a4b-4	62d6b7ab3cd	Virtual network : Azu	ne-FG	
Diagnose and solve problems				Public IP address : 13.	64.90.115 (AzurePublic)	
Settings	Tags (edit)	: Click here to add tags				
Configuration					States and a second second	
Connections	Health chi	eck quick health check to detect	Advanced troublesho	eshooting oting tool to invesigate	Documentation View guidance on helpful topics rel	ated to
• Point-to-site configuration	possible gi	ateway issues	failure causes and	perfom repair actions	VPN gateway	
🐨 NAT Rules	Go to Res	ource health	Go to VPN Trout	bleshooting	View documentation	
III Deparation						
A Locks	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.

Dashboard	> Edit Interface	_		
Network	Name	m port2		
Interfaces	☆ Alias			
DNS	Type	Physical Interface		
Packet Capture	VREID 0	0		
SD-WAN	Role 0	Undefined		
Static Routes		ondenned		
Policy Routes	Address			
RIP	Addressing	node Manual DHCP	Auto-managed by IPAM On	ne-Arm Sniffer
OSPF	IP/Netmask	192.168.10.1/24		
BGP	Secondary IF	address 🕥		
Routing Objects				
Routing Objects Multicast	Administrati	ve Access		
Routing Objects Multicast Policy & Objects	Administrati	ve Access	HTTP ()	PING
Routing Objects Multicast Policy & Objects Security Profiles	Administrati	re Access HTTPS FMG-Access	HTTP () SSH	PING SNMP
Routing Objects Multicast Policy & Objects Security Profiles VPN	Administrati	re Access HTTPS FMG-Access FTM	HTTP HTTP KSH RADIUS Accounting	PING SNMP Security Fabric Connection ①
Routing Objects Multicast Policy & Objects Security Profiles VPN User & Authentication	Administrati	e Access HTTPS FMG-Access FTM Speed Test	 HTTP () SSH RADIUS Accounting 	 PING SNMP Security Fabric Connection 3
Routing Objects Multicast Policy & Objects Security Profiles VPN User & Authentication WiFi Controller	Administrati	Pe Access HTTPS FMG-Access FTM Speed Test Use VDOM Setting E	 HTTP ① SSH RADIUS Accounting nable Disable 	 PING SNMP Security Fabric Connection ⁽¹⁾

Figure 10.23: Set an IP address for port2

FortiGate VM64-KVM	1 3 5 7 9 11 13 15 1 m m m m m m m m 2 4 6 8 10 12 14 16 1	7 19.21 23 9 20 22 24		
+ Create New ▼ @ Ed	dit 💼 Delete 🕨 Integra	te Interface	Search	
Name ≑	Type ≑	Members 🖨	IP/Netmask ≑	Administrative Acces
🗄 🗜 802.3ad Aggregate (1			
➔ fortilink	➔ 802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Conne
🔄 🔚 Physical Interface 🚺	0			
🕅 port1	Physical Interface		142.232.198.154/255.255.255.0	HTTPS HTTP
m port2	Physical Interface		192.168.10.1/255.255.255.0	
m port3	Physical Interface		0.0.0/0.0.0.0	
m port4	Physical Interface		0.0.0/0.0.0.0	
m port5	Physical Interface		0.0.0/0.0.0.0	
m port6	Physical Interface		0.0.0/0.0.0.0	
m 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.

FGVM01TM19008000	- E	Q				
Dashboard	> New	v Static Route				
 Network Interfaces DNS Packet Capture 	✔ Aut De Ga	tomatic gateway retrieval 🕄 stination 🕄 teway Address 🕄	Subnet Internet Se 0.0.0.0/0.0.0.0 Dynamic Specify	ervice 142.232.198.254		_
SD-WAN	Int	erface	m port1	×		
Static Routes			+	-		
Policy Routes	Adı	ministrative Distance 🟮	10			
RIP	Col	mments	Write a comment	<i>#</i> 0/255		
OSPF	Sta	itus	Enabled ODis	sabled		
BGP Routing Objects Multicast	0	Advanced Options				
🛃 Policy & Objects	>					
Security Profiles	>					
므 VPN	>					
User & Authentication	>					
	>				OK	Cancel

Figure 10.25: Create a static route

3. Create a IPsec Wizard as a custom.

🔁 Dashboard	> VPN Creation W	Vizard				
Network	> 1 VPN Setup					
Policy & Objects	> Name	FG-Azure	_			
Security Profiles	> Template type	Site to Site Hub-and-Spoke	Remote Access	Custom		
III VPN	*					
Overlay Controller VPN	_			2 Deals	Marita	Connel
IPsec Tunnels				* Back	Next >	Cancel
IPsec Wizard						
IPsec Tunnel Template						
SSL-VPN Portals						
SSL-VPN Settings						
SSL-VPN Clients						
VPN Location Map						

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:** 10.0.0/16
- **Phase 1:** Encryption: AES128, Authentication: SHA-1, DH: 2, lifetime: 28800
- Phase 2: Encryption: AES128, Authentication: SHA-1, DH: 2, lifetime: 27000

Dashboard >	New VPN Tunnel		
Network Network Policy & Objects	Name	FG-Azure	
Security Profiles	Comments	Comments // 0/255	
VPN Voverlay Controller VPN	Network		
IPsec Tunnels ☆	IP Version Remote Gateway	IPv4 IPv6 Static IP Address	
IPsec Tunnel Template	IP Address	13.64.90.115	
SSL-VPN Portals SSL-VPN Settings	Interface Local Gateway		
SSL-VPN Clients VPN Location Map	Mode Config NAT Traversal	Enable Disable Forced	
Luser & Authentication → ↔ WiFi Controller →	Dead Peer Detection DPD retry count	Disable On Idle On Demand	
✿ System 1 > ☆ Security Fabric > Lett Log & Report >	DPD retry interval Forward Error Correction	20 s Egress Ingress	
	Authentication Method Pre-shared Key	Pre-shared Key	۲

Figure 10.27: Create a custom VPN

Policy & Objects Security Profiles	IKE Version		1 2				
VPN Verlay Controller VPN	Phase 1 Proposal Encryption	• Add AES128	- /	Authentication	SHA1	•	
IPsec Tunnels ☆ IPsec Wizard IPsec Tunnel Template	Diffie-Hellman Gro	oup	32 21 15	31 30 30 20 19 14 5 2	29 28 2 18 17 1 2 1	7 6	
SSL-VPN Portals SSL-VPN Settings SSL-VPN Clients	Key Lifetime (seco Local ID Phase 2 Selectors	nds)	28800				
VPN Location Map User & Authentication	Name FG-Azure	Local 192.16	Address 3.10.0/24	Rei	mote Address 10.0.0.0/16		
 ♥ WiFi Controller > ✿ System 1 > ※ Security Fabric > 	New Phase 2 Name	FG	-Azure			0	5
네 Log & Report >	Comments Local Address	Su	bnet	 ✓ 192.168.10 ■ 100.00/1/ 	0.0/24		
		50	Difet	• 10.0.0.0/10			

Figure 10.28: Create a custom VPN

Dashboard	>	New VPN Tunnel									
+ Network	>	New Phase 2								0	C
🛃 Policy & Objects	>	Name		FG-Azure							
Security Profiles	Security Profiles >		Comments		Comments						
I VPN	~	Local Address		Cubaa		102.1	49 10 0/2	A			
Overlay Controller VPN		Local Address		Subre	. •	192.1	08.10.0/2	4			
IPsec Tunnels	☆	Remote Address		Subne	t 🕶	10.0.0	0.0/16				
IPsec Wizard		Advanced									
IPsec Tunnel Template		Phase 2 Proposal	O Add								
SSL-VPN Portals		Encryption	AES128		Authentic	ation	SHA1	-			
SSL-VPN Settings		Enable Replay Det	ection 🛃								
SSL-VPN Clients		Enable Perfect For	ward Secre	cy (PFS)	2						
VPN Location Map				32	31 - 3	30	29 🔲 28	27			
User & Authentication	>	Diffie-Hellman Gro	pup	21	20 2	19	18 17	16			
	>			15	14 1		2 1				
System	1 >	Local Port		All 🗾							
🔆 Security Fabric	>	Remote Port		All 🗾							
Log & Report	>	Protocol		All 🗾							
		Auto-negotiate									
		Autokey Keep Aliv	e								
		Key Lifetime		Second	ds			•			
		Seconds		27000							

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.

lame	FG-LAN		
olor	Change		
/pe	Subnet	-	
P/Netmask	192.168.10.0/24		
nterface	🗆 any	-	
tatic route configura	tion 🛈		
Comments	Write a comment	# 0/255	
		OK	Cancel

Figure 10.30: Create a subnet for local network

Name	AZ-LAN		
lor	Change		
pe	Subnet	*	
P/Netmask	10.0.0/16		
Interface	🖸 any	-	
Static route configura	ation 🕥		
Comments	Write a comment	# 0/255	
		ОК	

Figure 10.31: Create a subnet for Azure local

🕞 FGVM01TM19008000	= Q				
Dashboard	New Policy				
Network]
🖹 Policy & Objects 🗸 🗸	Name 🟮	FG-AZURE			
Firewall Policy 🖸	Incoming Interface	m port2	•		
IPv4 DoS Policy	Outgoing Interface	G FG-Azure	+		
Addresses	Source	E FG-LAN	×		
Internet Service Database	Destination	AZ-LAN	×		
Services	Schedule	G always			
Schedules	Service	I ALL	×		
Virtual IPs	Par recep	+			
IP Pools	Action	✓ ACCEPT Ø DENY			
Protocol Options	and the second				
Traffic Shaping	Inspection Mode	Flow-based Proxy-based			
Security Profiles	Firewall / Network C	Options			
	NAT 🔿				
Ser & Authentication Ser & Authentication WiFi Controller	Protocol Options	PROT default	- #		
🌣 System 👔 🔉	Security Profiles				
Security Fabric	AntiVirus	•			
Leg & Report >	Web Filter	0			
	DNS Filter	0			
	3			ОК	Cancel

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



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

Ð	Dashboard	>	Edit Policy				
÷	Network	>					
8	Policy & Objects	*	Name 0	Azure-FG			
	Firewall Policy	☆	Incoming Interface	FG-Azure	-		
	IPv4 DoS Policy		Outgoing Interface	m port2	-		
	Addresses		Source	AZ-LAN	×		
	Internet Service Database		Destination	FG-LAN	×		
	Services		Schedule				
	Schedules		Service		*		
	Virtual IPs		Service	+	~		
	IP Pools		Action	✓ ACCEPT ⊘ DENY			
	Protocol Options						
	Traffic Shaping		Inspection Mode	Flow-based Proxy-based			
•	Security Profiles	>	Firewall / Network (Intions			
므	VPN	>	NAT	Sprions			
•	User & Authentication	>	NAI O	more defende			
(;-	WiFi Controller	>	Protocol Options	PROT default			
۰	System	1 >	Security Profiles				
**	Security Fabric	>	AntiVirus	•			
ы	Log & Report	>	Web Filter	0			
			DNS Filter	0			
	FEIRTINET	v7.0.3	Constant of			OK	Cancel

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

FGVM01TM19008000		≡ Q.								>_ (9 • 🗘 🛛 • 🛃 admin •
2 Dashboard		+ Create New	/ Edit 1	Delete Q Po	olicy Lookup Se	arch			Q E	Export - Inter	rface Pair View By Sequence
Network		Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	log	Bytes
Policy & Objects	٠		re - F port?	Destination	Genedate	Service	Filteron	14.0	second fromes	EOB	of the
Firewall Policy	슈	E 12 TO ALL		Trestan	-		in the second	· ·	and a second second second	Euris	
IPv4 DoS Policy		Azurero	AZ-LAN	FG-LAN	Lo always	W ALL	ALCEPT	O Disabled	no-inspection	U UIM	08
Addresses		□ □ port2→	FG-Azure 1	1-							
Internet Service		FG-AZURE	FG-LAN	AZ-LAN	Lo always	ALL ALL	✓ ACCEPT	O Disabled	no-inspection	UTM UTM	0 B
Database		🛨 Implicit 🕦									
Services											

Figure 10.35: Firewall Policies

Verify Connections

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





Default Directory	Virtual network gateway	onnections	\$P			×
🕂 Create 🔞 Manage view 🗸 \cdots	Ø Search (Ctrl+/) ≪	+ Add 🕐 R	efresh			
Filter for any field	Overview	Search conne	ctions			
Name 1	Activity log	Name	↑↓ Status	↑↓ Connection type	↑↓ Peer	↑↓
Azure-VPN-EG ***	Access control (IAM)	VPNAZ	Connected	Site-to-site (IPsec)	FortiGate	
-	🗳 Tags					
	Diagnose and solve problems					
	Settings					
	Configuration					
	Connections					
	✤ Point-to-site configuration					
	🖂 NAT Rules					
	II Properties					
	A Locks					
	Monitoring					

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 10.50. 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.

Subscription * 🕕	Azure subscription 1	\sim
Resource group * ①	(New) FortiGate Create new	\sim
Instance details		
Region * (i)	UK West	\sim
FortiGate administrative username * 🛈	hamid	\checkmark
FortiGate password * 🛈		\checkmark
Confirm password * 🛈		\checkmark
Fortigate Name Prefix * 🕕	hamid	\checkmark
Fortigate Image SKU ①	Pay As You Go	\sim
Fortigate Image Version ①	latest	\sim
Review + create < Previous	Next : Instance Type >	

Create Fortinet FortiGate Next-Generation Firewall

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.

🕑 Vali	dation Passed						
Basics	Instance Type	Networking	Public IP	Advanced	Review + create		
PRODUC	CT 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	< Previou	IS Next	Dov	wnload a templa	ate 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 Č	Refresh					
👶 Overview	3	We'd love your feedback! \rightarrow						
😫 Inputs								
š≣ Outputs		Deployment is in progr	ress					
Template Deployment name: fortinet.fortinet-fortigate-20220513160337 Start time: 5/* Subscription: Azure subscription 1 Correlation ID: Resource group: FortiGate Correlation ID:				Start time: 5/13, Correlation ID: b	13/2022, 4:05:30 PN : b143bd4f-1aa4-4			
	^	Deployment details (Download)						
		Resource	Туре		Status			
		😌 hamid-FGT-A	Microsoft.Compute/v	virtualMachines	Created			
		Annid-FGT-A-Nic2	Microsoft.Network/n	etworkInterfaces	Created			
		hamid-FGT-A-Nic1	Microsoft.Network/n	etworkInterfaces	Created			

Figure 10.43: Deployment is in progress



Figure 10.44: Deployment is complete

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

FortiGate ☆ ☆ Resource group		
₽ Search (Ctrl+/)	« 🕂 🕂 Create 🚳 Manage view 🗸 💼 Delete resource group 🖒 Refresh 🞍 Expor	t to CSV 🛛 😤 Open query 🛛
(🖻 Overview	↑ ► Essentials	
Activity log	Subscription (move) : Azure subscription 1	Deployments : <u>2 Succee</u>
Access control (IAM)	Subscription ID : 9170d5fe-6ca8-4257-9a4b-462d6b7ab3cd	Location : UK West
🗳 Tags	Tags (edit) : Click here to add tags	
👫 Resource visualizer	Description of the second s	
Events	Resources Recommendations	
Settings	Filter for any field Type == all \times Location == all \times $+_{\nabla}$ Add filter	er
1 Deployments	Showing 1 to 9 of 9 records. Show hidden types ①	Ν
Q Security	Name ↑↓	Type ↑↓
Policies		Public IP address
🔁 Properties		Virtual network
🔒 Locks	hamid-EGT-A	Virtual machine
Cost Management	hamid-FGT-A-Nic1	Regular Network Interface
 A second s		-

Figure 10.45: FortiGate public IP address

ං Associate 🗙 Di	ssociate $ ightarrow$ Move \checkmark 🛍 Delete 🖒 Refresh					
🧭 Upgrade to Standard SKU - Microsoft recommends Standard SKU public IP address for production workloads $ ightarrow$						
∧ Essentials						
Resource group (move) : FortiGate SKU : Basic						
Location	: UK West	Tier	: Regional			
Subscription (<u>move</u>)	: Azure subscription 1	IP address	: 51.140.223.127			
Subscription ID	: 9170d5fe-6ca8-4257-9a4b-462d6b7ab3cd	DNS name	:-			
Associated to : hamid-FGT-A-Nic1						
Tags (<u>edit</u>)	provider : 6EB3B02F-50E5-4A3E-8CB8-2E12925831VM					

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.

Not secure https://51.140.223.127/login?redir=%2F		
<u> </u>		
	•	
	Username Password	
	Login	

Figure 10.47: FortiGate firewall credential page

← → C A Not secure https://51.140.223.127/ng/system/dashboard/1							
🕞 hamid-FGT-A 🔹 🔍							
🔁 Dashboard 🛛 🗸 🖌	+ Add Widget						
Status		1					
Security	System Inform	nation 🗜	Licenses (= 173.243.141.6) 👨	1.			
Network	Hostname	hamid-FGT-A	I FortiCare Support				
Users & Devices	Serial Number	FGTAZRDRSE9KW654 🕰	Firmware & General Updates				
WiFi	Firmware	v7.2.0 build1157 (Feature)	IPS				
T FortiView Sources	Mode	NAT	AntiVirus				
FortiView Destinations	System Time	2022/05/13 16:13:44	Web Filtering				
FortiView Applications	Uptime	00:00:04:23	FortiToken	0/0			
FortiView Web Sites	WAN IP	38 51.140.223.127	0%				
FortiView Policies							
FortiView Sessions	Security Fabri	c I-	Administrators	1-			
+			1 HTTPS 0 FortiExplorer				
			hamid super_admin				

Figure 10.48: FortiGate dashboard

9. 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.

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.

Table 10.2: FortiGate Subnet description in Azure

10.3 Site to Site VPN between FortiGate on Premise and FortiGate in the 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 <u>section 10.2</u> is necessary for this lab. Port1 is set as a DHCP, so they will receive an IP address from Cloud.

Table	10.3:	Devices	configurat	ion
-------	-------	---------	------------	-----

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".

Physical Interface 2			
🔚 LAN (port2)	Physical Interface	10.0.1.4/255.255.255.192	PING HTTPS SSH
MAN (port1)	Physical Interface	10.0.0.4/255.255.255.192	PING HTTPS SSH

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

💠 Network	VPN Setup	Authentication 3 Policy & Routing	4 Review Settings
🖹 Policy & Objects	Local interface	M port2	
Security Profiles	Cocarinternace	+	
묘 VPN ·	Local subnets	192.168.10.0/24	
Overlay Controller VPN		0	
IPsec Tunnels	Remote Subnets	10.0.0/16	
IPsec Wizard ۲	2	0	
IPsec Tunnel Template	Internet Access	None Share Local Use Remote	

Figure 10.53: Set Policy & Routing

3. Create a static route to the default gateway.

New Static Route				
Automatic gateway retrieval 🟮 🕥				
Destination	Subnet	Named Ad	dress	Internet Servic
	0.0.0/0.	0.0.0		
Gateway Address 🟮	Dynamic	Specify	142.	232.89.126
Interface	🔳 port1			×
		+		
Administrative Distance 🛈	10			
Comments	Write a co	omment		<i>«</i> 0/255
Status	🔂 Enable	ed 🔮 Dis	sabled	
Advanced Options				

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 <u>section 10.1</u>.
 - 2. Create a VPN from IPsec Wizard as Figures 10.55 to 10.57.

孢 Dashboard	>	VPN Creation Wizard					
🗘 Network	>	1 VPN Setup	Authenticat	tion 3 Policy	& Routing 🔰 4	Review Set	ttings
Policy & Objects	>	Name	AzuretoFG				
Security Profiles	>	Template type	Site to Site	Hub-and-Spoke	Remote Access	Custom	
	~	NAT configuration	No NAT bet	ween sites			
Overlay Controller VPN	☆	C C	This site is b	ehind NAT			
IPsec Tunnels			The remote	site is behind NAT			
IPsec Wizard	☆	Remote device type	FortiGa	te			
IPsec Tunnel Template			cisco Cisco				
SSL-VPN Portals							
SSL-VPN Settings						< Back	
SSL-VPN Clients							

Figure 10.55: Select VPN name



Figure 10.56: Set a remote IP address

Dashboard	VPN Creation Wizard		
Network	🗸 VPN Setup 🔪	Authentication 3 Policy & Routing	A Review Settings
Policy & Objects	l ocal interface	M LAN (port2)	
Security Profiles	Local Internace	+	
므 VPN ·	Local subnets	10.0.1.0/26	
Overlay Controller VPN		0	
IPsec Tunnels	Remote Subnets	192.168.10.0/16	
IPsec Wizard ර		0	
IPsec Tunnel Template	Internet Access 🕚	None Share Local Use Remote	
SSL-VPN Portals			

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=0.048 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

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

Table 10.4: On-premise devices configuration

AWS Configuration

- 1. Create a VPC for AWS as follows:
 - **Name tag:** AWS Subnet
 - **IPv4 CIDR:** 10.0.0/16

aws	III Services	Q Sear	ch for services, features, blogs, docs,	and more [Alt+5]				D	4	0 4	N. Virginia 🔻	tungi	e 🔻
New Tell up	VPC Experience		Your VPCs Info					C	A	tions 🔻	Create	VPC	٩
VPC Da	ashboard	÷.	Q. Filter VPCs								< 1 >	۲	
EC2 Glo Filter by	obal View New	4	Name	V VPC ID	 State	v	IPv4 CIDR		~	IPv6 CID	R		
Q Sele	ect a VPC										No VPC	is found in	
VIRTU CLOUD	AL PRIVATE D												
Subnet	5												

Figure 10.61: Create a VPC

VPC settings	
Resources to create Info Create only the VPC resource or create VPC,	subnets, etc.
• VPC only	VPC, subnets, etc.
Name tag - <i>optional</i> Creates a tag with a key of 'Name' and a valu	ue that you specify.
AWS Subnet	
 IPv4 CIDR block Info IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block 	
IPv4 CIDR	
10.0.0/16	-
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	

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**

vrc	
/PC ID Create subnets in this VPC	
vpc-0a92013e3d2c88ae4 (AWS Subnet)	
Associated VPC CIDRs	
Pv4 CIDRs	
Subnet settings Specify the CIDR blocks and Availability Zone for the subnet.	
Subnet settings Specify the CIDR blocks and Availability Zone for the subnet. Subnet 1 of 1	
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.	
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	
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.	
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.	

Figure 10.63: Create a subnet under AWS VPC

3. Create an internet gateway as follows:

New VPC Experience Tell us what you think.	Internet gateways Info
VPC Dashboard	Q. Alter-Internet gateways (1) .
EC2 Global View New	Name 🗢 Internet gateway ID 🗢 State 🗢 VPC ID 🗢 Owner
Q Select a VPC	No internet gateways found in this Region
VIRTUAL PRIVATE	
Subnets	
Route Tables	Select an internet gateway above
Internet Gateways	

Figure 10.64: Create an internet gateway

internet gateway is a virtual the gateway below.	router that connects a VPC to the internet. To c	reate a new internet gateway specify the nar
Internet gateway set	tings	
Name tag	s' and a value that you specify.	
Creates a tag with a key of 'Name		
Creates a tag with a key of 'Nam AWS-IGW	Contractor and the second	
AWS-IGW		
AWS-IGW		
AWS-IGM Tags - optional Atag is a label that you assign to your resources or track your AWS	han AWS resource. Each tag consists of a key and an opti	ional value. You can use tags to search and filter
Creates a tag with a key of Nam AWS-IGW Tags - optional A tag is a label that you assign to your resources or track your AWS Key	an AWS resource. Each tag consists of a key and an opt costs. Value - <i>optional</i>	ional value. You can use tags to search and filter
Creates a tag with a key of Nam AWS-IGW Tags - optional A tag is a label that you assign to your resources or track your AWS Key Q. Name	van AWS resource. Each tag consists of a key and an opticosts. Value - optional X Q. AWS-IGW	Ional value. You can use tags to search and filter
Creates a tag with a key of Nam AWS-IGW Tags - optional A tag is a label that you assign to your resources or track your AWS Key Q. Name	A an AWS resource. Each tag consists of a key and an opticosts. Value - <i>optional</i> X Q AWS-IGW	Ional value. You can use tags to search and filter

Figure 10.65: Select Name as AWS-IGW

New VPC Experience Tell us what you think		Inter	net gateways	s (1/1) u	nta				C	Actions 🔺 Create	e Internet gateway	
VPC Dashboard	1	9	Filter Internet gote	nways						View details Attach to VPC	< 1 > 0	0
EC2 Global View New	4	~	Name	v	Internet gateway ID	v	State	7	VPC ID	Datach from VPC	Owner	
Filter by VPC: Q Select a VPC	E		AWS-IGW		igw-08d499e1c3a99be7d		⊖ Detached		-	Manage tags	590508865535	
VIRTUAL PRIVATE										Delete internet gateway	_	Í
Your VPCs												_
Subnets						-						
Route Tables	1	igw-08	3d499e1c3a99b	e7d / AW	S-IGW							
Internet Gateways		Det	ails Tags									

Figure 10.66: Attach the internet gateway to VPC

PC > Internet gateways > Attach to VPC (igw-08d499e1c3a99be7d)	
ttach to VPC (igw-08d499e1c3a99be7d) Info	
VPC Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the Vi	PC to attach below,
Available VPCs Attach the internet gateway to this VPC.	
Q. Select a VPC	
vpc-0a92013e3d2c88ae4 - AWS Subnet	
AWS Command Line Interface command	

Figure 10.67: Attach the internet gateway to VPC

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

New VPC Experience Tell us what you think		Route t	ables (1/1)	Info					C	Actions	Crea	te route (table
VPC Dashboard	ň.,	Q. Filte	a route tibles								3	1.0	0
EC2 Global View New	ā.		lame	V	Route table IC	⊽ ⊽	Explicit subnet	associat	Edge associations	Main 🔻	VPC		
Q Select a VPC		-			rtb-0aebe92e0	0deb44303	-		-	Yes	vpc-0a920)13e3d2c	88ae4 AW
VIRTUAL PRIVATE	11	-											
Your VPCs		_											
Subnets													
Route Tables		rtb-0aebe	e92e0deb443	03									
Internet Gateways		Datalla	1			1 million	intertaine main		-				
Egress Only Internet Gateways	U	Details	Routes	Su	ionet associations	Edge ass	ociations kour	e propagation	lags				
Carrier Gateways		Pout	11)							-		Edit cout	
DHCP Option Sets		Koutt	is (1)									Eun roui	es
Elastic IPs		Q, P	lter routus						Both	*	<	1.2	0
Managed Prefix Lists													
Endpoints		Destin	ation		~	Target	~	Status	∀	Propagated			
Endpoint Services		10.0.0.	0/16			local		O Active		No			

Figure 10.68: Edit routes

Destination		Target		Status	Propagated	
10.0.0/16		Q local	×	O Active	No	
Q, 0.0.0.0/0	×	Q		в	No	Remove
		Carrier Gateway				
Add route		Core Network				
		Egress Only Internet Gateway				
		Gateway Load Balancer Endpoint			Gandal	Bravious Faus change
		Instance			cancer	Save chang
		Internet Gateway				
		local				
		NAT Gateway				
		Network Interface				
		Outpost Local Gateway				
		Peering Connection				
		Transit Gateway				
		Virtual Private Gateway				

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

VPC > Route tables > rtb-Oaebe92e0deb44303 Edit routes) Edit	routes					
Destination		Target		Status	Propagated		
10.0.0.0/16		Q, local	×	⊘ Active	No		
Q, 0.0.0.0/0	×	Q igw-	×	7	No	Ren	nove
Add route		igw-08d499e1c3a99be7d (AWS-IGW)	_				
					Cancel	Preview	Save changes

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

Subnets	Route table ID	Main	Explicit subnet associations	Edge associations
Route Tables	Ttb-0aebe92e0deb44303	🗗 Yes	-	
Internet Gateways	VPC	Owner ID		
Egress Only Internet Gateways	vpc-0a92013e3d2c88ae4 AWS Subnet	D 590508865535		
Carrier Gateways				
DHCP Option Sets				
Elastic IPs	Routes Subnet associations	Edge associations Route	propagation Tags	
Managed Prefix Lists				
Endpoints	Gradual -			
Endpoint Services	Routes (2)			Edit routes
NAT Gateways	Q Filter routes			Both v < 1 > ③
Peering Connections				
* SECURITY	Destination V	Target		
Network ACLs				
Security Groups	10.0.0/16	local	O Active	No
* NETWORK ANALYSIS	0.0.0.0/0	igw-08d499e1c3a99be7d	⊘ Active	No

Figure 10.71: Route tables overview

5. Create a customer gateway as follows:

New VPC Experience Tell us what you think	Customer gateways	Info		C	Actions 🔻	Create customer gateway
NETWORK ANALYSIS Reachability Analyzer	Q Filter customer gatewa	ays.				1 < 1 > @
Network Access Analyzer	Name			♥ BGP ASN	~	IP dress 🔻 Type
▼ DNS FIREWALL Rule Groups New Domain Lists New	<			-		No customer gateways found
 NETWORK FIREWALL Firewalls 			-			
Firewall Policies	Select a customer gateway					
Network Firewall Rule Groups						
VIRTUAL PRIVATE NETWORK (VPN)						
Customer Gateways						
Virtual Private Gateways						
Site-to-Site VPN Connections						
Client VPN Endpoints New						

Figure 10.72: Create a customer gateway

reate customer gateway տ	
ustomer gateway is a resource that you create in AWS that represent twork.	its the customer gateway device in your on-premises
Details	
Name tag - optional Creates a tag with a key of 'Name' and a value that you specify.	
AWS-VPN-FG	
Value must be 256 characters or less in length.	
BGP ASN Info The ASN of your customer gateway device.	
65000	
Value must be in 1 - 2147483647 range.	
IP address Info Specify the IP address for your customer gateway device's external interface.	
142.232.198.157	
Certificate ARN The ARN of a private certificate provisioned in AWS Certificate Manager (ACM)	
Select certificate ARN	▼
Device - optional Enter a name for the customer gateway device.	
Enter device name	

Figure 10.73: Create a customer gateway

6. Create a virtual private gateway as follows:

New VPC Experience	Virtual privat	e gateways	Info				C	Actions 🔻	Create v	irtual priva	ite gate	way
* NETWORK ANALYSIS *	Q Filter virtual	private gateway	ş						1	<	1.>	0
Reachability Analyzer Network Access Analyzer	Name	4	Virtual private gateway ID	4	State	~	Туре		VPC			~
DNS FIREWALL Rule Groups New Domain Lists New	4	_		-	-	No virtual private g	gateways fo	ound				,
NETWORK FIREWALL Firewalls				-	_							
Firewall Policies	Select a virtual pri	vate gateway										
Network Firewall Rule Groups												
VIRTUAL PRIVATE NETWORK (VPN)												
Customer Gateways												
Virtual Private Gateways												
Site-to-Site VPN Connections												

Figure 10.74: Create a virtual private gateway

	e VPN concentrator o	on the Amazon side of the	site-to-site VPN co	nnection.
Details				
Name tag - <i>optional</i> Creates a tag with a key of 'Na	me' and a value that you	specify.		
FortiGate				
Value must be 256 characters	or less in length.			
Autonomous System Num	ber (ASN)			
Amazon default ASN				
Custom ASN				
Tags			And the second second	the second s
Tags A tag is a label that you assign your resources or track your AV	to an AWS resource. Eacl VS costs. Name tag helps	n tag consists of a key and an you track your resources mor	optional value. You ca e easily. We recomme	n use tags to search and filte nd adding Name tag.
Tags A tag is a label that you assign your resources or track your AV	to an AWS resource. Eacl VS costs. Name tag helps	n tag consists of a key and an you track your resources mor	optional value. You ca e easily. We recommen	n use tags to search and filte nd adding Name tag.
Tags A tag is a label that you assign your resources or track your AV Key	to an AWS resource. Eacl VS costs. Name tag helps V	n tag consists of a key and an you track your resources mor alue - optional	optional value. You ca e easily, We recomme	n use tags to search and filte nd adding Name tag.
Tags A tag is a label that you assign your resources or track your AV Key Q. Name	to an AWS resource. Eacl VS costs. Name tag helps V	n tag consists of a key and an you track your resources mor alue - <i>optional</i> Q FortiGate	optional value. You ca e easily. We recommen	n use tags to search and filte nd adding Name tag.
Tags A tag is a label that you assign your resources or track your AV Key Q. Name	to an AWS resource. Eacl VS costs. Name tag helps V	n tag consists of a key and an you track your resources mor alue - <i>optional</i> Q. FortiGate	optional value. You ca e easily. We recommend	n use tags to search and filte nd adding Name tag.

Figure 10.75: Create a virtual private gateway on FortiGate

New VPC Experience	Virtual private gateways (1/1) Info C Actions A Create virtual p	private gateway
NETWORK ANALYSIS Reachability Analyzer Network Access Analyzer	Q. Filter virtual private gateways Attach to VPC Virtual private gateway ID: vgw-048d1dd1e6ba61f05 X Clear filters Manage tags	< 1 > @
▼ DNS FIREWALL	Name Virtual private gateway ID V State V Type Delete virtual private gateway	⊽
Rule Groups New	O FortiGate vgw-048d1dd1e6ba61f05 ⊙Detached ipsec.1 -	
Domain Lists New		,
NETWORK FIREWALL Firewalls Firewall Policies Network Firewall Rule Groups	vgw-048d1dd1e6ba61f05 / FortiGate Details Tags	
VIRTUAL PRIVATE NETWORK (VPN) Customer Gateways	Details	
Virtual Private Gateways Site-to-Site VPN Connections	Virtual private gateway ID State Type VPC	
Cuent VPN Endpoints New	D 64512	

Figure 10.76: Attach virtual private gateway to VPC

/PC > Virtual private gateways > vgw-048d1dd1e6ba61f05 > Attach	to VPC		
Attach to VPC info			
Details			
Virtual private gateway ID			
Available VPCs Attach the virtual private gateway to this VPC.			
Select a VPC by ID or Name	*	1	
Q			
vpc-0a92013e3d2c88ae4 / AWS Subnet		Cancel	Attach 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

New VPC Experience	VPN connections Info	C Actions ¥	Download configuration Create VPN connection
▼ NETWORK ANALYSIS * Reachability Analyzer	Q Filter VPN connections		< 1 > ⊚
Network Access Analyzer	Name VPN ID	⊽ State ⊽ Vi	rtual private gateway 🔻 Transit gateway 🗢 Cu
DNS FIREWALL Rule Groups New Domain Lists New			,
NETWORK FIREWALL Firewalls		1	
Firewall Policies	Select a VPN connection.		
Network Firewall Rule Groups			
VIRTUAL PRIVATE NETWORK (VPN)			
Customer Gateways			
Virtual Private Gateways			
Site-to-Site VPN Connections			
Client VPN Endpoints New			

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

	nt to use for the site-to-site VPN connec
Details	
Name tag - optional Creates a tag with a key of 'Name' and a value that you specify.	
VPNAWS	
Value must be 256 characters or less in length.	
Target gateway type Info	
 Virtual private gateway 	
O Transit gateway	
O Not associated	
Virtual private gateway	
vgw-048d1dd1e6ba61f05 / FortiGate	
Customer gateway Info	
• Existing	
O New	
Customer gateway ID	
cgw-0a32c4cc31edca775 / AWS-VPN-FG	•
Routing options Info	

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

Q Add static IP prefix			
192.168.10.0/24 🗙			
.ocal IPv4 network CIDR - optional The IPv4 CIDR range on the customer gateway (on- 10.0.0/0.	premises) side that is allowed to communi	cate over the	VPN tunnels. The default is
Q 192.168.10.0/24		×	
Remote IPv4 network CIDR - optional The IPv4 CIDR range on the AWS side that is allowe	d to communicate over the VPN tunnels. T	he default is (0.0.0/0.
Q 10.0.1.0/24		×	
 Tunnel 1 options - optional Info Tunnel 2 options - optional Info 			
Tunnel 1 options - optional Info Tunnel 2 options - optional Info Fags Itag is a label that you assign to an AWS resource. Four resources or track your AWS costs. Name tag h	Each tag consists of a key and an optional elps you track your resources more easily.	value. You ca We recommer	n use tags to search and filter Id adding Name tag.
Tunnel 1 options - optional Info Tunnel 2 options - optional Info Tags It ag is a label that you assign to an AWS resource. Your resources or track your AWS costs. Name tag h	Each tag consists of a key and an optional elps you track your resources more easily. Value - optional	value. You ca We recommer	n use tags to search and filter Id adding Name tag.
Tunnel 1 options - optional Info Tunnel 2 options - optional Info Tags Itag is a label that you assign to an AWS resource. Our resources or track your AWS costs. Name tag h Key Q Name X	Each tag consists of a key and an optional lelps you track your resources more easily. Value - <i>optional</i> Q. VPNAWS	value. You ca We recommer	n use tags to search and filter Id adding Name tag. Remove
Tunnel 1 options - optional Info Tunnel 2 options - optional Info Tags A tag is a label that you assign to an AWS resource. rour resources or track your AWS costs. Name tag h Key Q. Name X Add new tag	Each tag consists of a key and an optional lelps you track your resources more easily. Value - optional Q VPNAWS	value. You ca We recommer	n use tags to search and filter Id adding Name tag. Remove
Tunnel 1 options - optional Info Tunnel 2 options - optional Info Tags Atag is a label that you assign to an AWS resource. Nour resources or track your AWS costs. Name tag h Cey Q. Name X Add new tag You can add 49 more tags.	Each tag consists of a key and an optional lelps you track your resources more easily. Value - <i>optional</i> Q, VPNAWS	value. You ca We recommer	n use tags to search and filter Id adding Name tag.
Tunnel 1 options - optional Info Tunnel 2 options - optional Info Fags I tag is a label that you assign to an AWS resource. I tag is a label that you assign to an AWS resource. I tag is a label that you assign to an AWS resource. I tag is a label that you assign to an AWS resource. Add new tag You can add 49 more tags.	Each tag consists of a key and an optional leps you track your resources more easily. Value - optional Q. VPNAWS	value. You ca We recommer	n use tags to search and filter nd adding Name tag.

Figure 10.80: Create a site-to-site VPN connection with FortiGate
					connectio	п
Q Filter VPN connections				5	1 >	0
VPN ID: vpn-0a9b7e3a2ca3eebd2	2 X Clear filters					
Name 🗸	VPN ID 🗢	State		teway 🔻 Transit gateway	V	
VPNAWS	vpn-0a9b7e3a2ca3eebd2	Pending	vgw-048d1dd1e6b	oa61f05 –		
		-				
on-0a9b7e3a2ca3eebd2 / VPNA	aws					-
Details Tunnel details	Static routes lags					
Details						
Details VPN ID	State		Virtual private gateway	Customer gateway		
Details VPN ID O vpn-0a9b7e3a2ca3eebd2	State		Virtual private gateway vgw-048d1dd1e6ba61f05	Customer gateway cgw-0a32c4cc31edca775		
Details VPN ID vpn-0a9b7e3a2ca3eebd2 Transit nateway	State O Pending	45	Virtual private gateway vgw-048d1dd1e6ba61f05 Tvne	Customer gateway cgw-0a32c4cc31edca775		
Details VPN ID vpn-0a9b7e3a2ca3eebd2 Transit gateway	State Pending Customer gateway addre 142.232.198.157	55	Virtual private gateway vgw-048d1dd1e6ba61f05 Type D ipsec.1	Customer gateway cgw-0a32c4cc31edca775 Category D VPN		
Details VPN ID vpn-0a9b7e3a2ca3eebd2 Transit gateway - VPC	State Pending Customer gateway addre 142.232.198.157 Bouting	55	Virtual private gateway vgw-048d1dd1e6ba61f05 Type: D ipsec.1 Acceleration enabled	Customer gateway cgw-0a32c4cc31edca775 Category O VPN Authentication		
Details VPN ID Vpn-0a9b7e3a2ca3eebd2 Transit gateway - VPC vpc-0a92013e3d2c88ae4	State	55	Virtual private gateway vgw-048d1dd1e6ba61f05 Type D ipsec.1 Acceleration enabled D False	Customer gateway cgw-0a32c4cc31edca775 Category VPN Authentication Pre-shared key		
Details VPN ID vpn-0a9b7e3a2ca3eebd2 Transit gateway - VPC vpc-0a92013e3d2c88ae4 Local IPv4 network CID8	State Pending Customer gateway addre 142.232.198.157 Routing Static Remote IPv4 network CIE	55	Virtual private gateway vgw-048d1dd1e6ba61f05 Type D ipsec.1 Acceleration enabled D false Local IPv6 network CIDR	Customer gateway cgw-0a32c4cc31edca775 Category D VPN Authentication Pre-shared key Remote IPv6 network CIDR		

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

Download configuration		×
Choose the sample configuration you wish to d gateway. Please note these are samples, and wi Algorithms, Certificates, and/or IPv6.	ownload based on your customer Il need modification to use Advanced	
Vendor The manufacturer of the customer gateway device (for	example, Cisco Systems, Inc).	
Fortinet	•	
Platform The class of the customer gateway device (for example	, J-Series).	
Fortigate 40+ Series	•	
Software The operating system running on the customer gatewa	y device (for example, ScreenOS).	
FortiOS 6.4.4+ (GUI)		
IKE version The IKE version you are using for your VPN connection.		

Figure 10.82: Download configuration

Q Filter VPN connection	ons					\$	1 >
VPN ID: vpn-0a9b7e3a	a2ca3eebd2 X	lear filters					
Name	VPN ID		itate 🗸 🗸	Virtual private	gateway 🗢 Trans	sit gateway	4
VPNAWS	vpn-0a9b7e3	a2ca3eebd2	Pending	vgw-048d1dd1	e6ba61f05 -		
n-0a9b7e3a2ca3eeb	d2 / VPNAWS						
Details Tunnel	details Static routes	s Tags					
Details Tunnel	details Static routes	s Tags					
Details Tunnel state	details Static routes	s Tags Inside IPv4 CIDR	⊽ Inside IPv6 CIDR ⊽	Status 🔻	Last status change	~	Detai
Details Tunnel	Outside IP address ♥ 3.225,102.90	s Tags Inside IPv4 CIDR 169.254.72.192/30	▽ Inside IPv6 CIDR ▽) ~	Status ⊽ ⊛Down	Last status change May 30, 2022, 9:07:13	⊽ (UTC-07:00)	Detai
Details Tunnel Tunnel state Tunnel number ▼ Tunnel 1 Tunnel 2	Outside IP address v 3.225.102.90 54.83.91.6	5 Tags Inside IPv4 CIDR 169.254.72.192/30 169.254.143.60/30	▼ Inside IPv6 CIDR ▼) -) -	Status ♥ ② Down ③ Down	Last status change May 30, 2022, 9:07:13 May 30, 2022, 9:07:13	v (UTC-07:00) (UTC-07:00)	Detai -

Figure 10.83: Verify public IP address

8. 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			
! #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-4	ða9b7	e3a2ca	i3ee
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			
u. Local Interface: Wani			
E. Local Dear Dearting, Select Specify and enter wan port in (round in) f Dear Dear Dearting, Frahle by selecting On Idle (On Demand			
a. Authentication Method: Pre-shared Key			
h. Pre-Shared Key: rt11zQj5aWoSdpACxy HBYGBX62c4fIS			
i. IKE Version: 2			
Phase 1 Proposal:			
j. Encryption: aes128			
k. Authentication: shal			
1. DH group: 2 ! and deselect 5			
m. Keyiire: 28800 seconas			
Figure 10.84: IPsec Phase 1			

🛄 vp	on-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
с.	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.

Ð	Dashboard	>	Edit Interface						
\$	Network	*	law in the second						
	Interfaces	습	Name	рогт2					
	DNS		Alias	Dhurica	Interface				
	Packet Capture		Type	E Physica	Interface				
	SD-WAN		VRFID 0	0					
	Static Routes		Kole U	Undefine	d		•		
	Policy Routes		Address						
	RIP		Addressing m	node	Manual DH	CP Au	to-managed by IPAM	One-Ar	m Sniffer
	OSPF		IP/Netmask		192.168.10.1	/24			
	BGP		Secondary IP	address Q					
	Routing Objects								
	Multicast		Administrativ	ve Access					
B	Policy & Objects	>	IPv4		HTTPS		HTTP 0		D PING
4	Security Profiles	>			FMG-Access		SSH SSH		SNMP
₽	VPN	>			FTM		RADIUS Accounti	ng	Connection
	User & Authentication	>			Speed Test				connection o
ŵ	WiFi Controller	>	Receive LLDF	0 Us	e VDOM Setting	Enable	Disable		
\$	System	1 >	Transmit LLD	P 🚺 Us	e VDOM Setting	Enable	Disable		

Figure 10.86: Set an IP address for port2

FortiGate VM64-KVM	1 3 5 7 8 11 13 75 A A A A A A A A A 2 4 6 8 10 12 14 26	18 20 22 24			
+ Create New • Edi	it 🛍 Delete 🕨 Integr	ate Interface	Search		Q
Name ≑	Type 🗢	Members 🖨	IP/Netmask 🜩	Administrative Access	\$
🗗 802.3ad Aggregate 🧃					
₽ fortilink	₽ 802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connect	tion
E Physical Interface 10)				
m port1	Physical Interface		142.232.198.157/255.255.255.0	HTTPS HTTP	
im port2	Physical Interface		192.168.10.1/255.255.255.0		
🔳 port3	Physical Interface		0.0.0.0/0.0.0.0		
m 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.

Ð	Dashboard	>	New Static Route				
+	Network Interfaces	*	Automatic gateway retrieval 3				
	DNS		Destination 1	Subnet Internet Se	rvice		
	Packet Capture			0.0.0/0.0.0			
	SD-W/AN		Gateway Address 🚯	Dynamic Specify	142.232.198.254		
-	SU-WAIN	~	Interface	m port1	×		
	Static Routes	ម		+			
	Policy Routes		Administrative Distance 🕄	10			
	RIP		Comments	Write a comment	// 0/255		
	OSPF		Status	Enabled ODis	abled		
	BGP						
	Routing Objects		Advanced Options				
	Multicast						
B	Policy & Objects	>					
•	Security Profiles	>					
묘	VPN	>					
	User & Authentication	>					
(:	WiFi Controller	>					
\$	System	1 >				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:** 10.0.0/16

- 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

FGVM01TM19008000	+ ≡ Q,						
20 Dashboard	> VPN Creation W	lizard					
 Policy & Objects 	> ① VPN Setup > Name	FG-AWS					
Security Profiles VPN Overlay Controller VPN	 Template type 	Site to Site	Hub-and-Spoke	Remote Access	Custom		
IPsec Tunnels					< Back	Next >	Cancel
IPsec Wizard							
IPsec Tunnel Template							
SSL-VPN Portals							
SSL-VPN Settings							
SSL-VPN Clients							
VPN Location Map							

Figure 10.89: Create a custom VPN

Ð	Dashboard	>	New VPN Tunnel					
Ф	Network	>	Cak	les nue l				
8	Policy & Objects	>	Name	FG-AWS				
۵	Security Profiles	>	Comments	Comments 0/255				
묘	VPN	~						
	Overlay Controller VPN		Network					
	IPsec Tunnels	습	IP Version	IPv4 IPv6				
	IPsec Wizard		Remote Gateway	Static IP Address 🔹				
	IPsec Tunnel Template		IP Address	3.225.102.90				
	SSL-VPN Portals		Interface	im port1	•			
	SSL-VPN Settings		Local Gateway	•				
	SSL-VPN Clients		Mode Config					
	VPN Location Map		NAT Traversal	Enable Disable Forced				
2	User & Authentication	>	Dead Peer Detection	Disable On Idle On Demand				
(:-	WiFi Controller	>	DPD retry count	3				
۵	System	1 >	DPD retry interval	20 s				
*	Security Fabric	>	Forward Error Correction	Egress Ingress				
Lui	Log & Report	>	Advanced					

Figure 10.90: Create a custom VPN

Dashboard >	New VPN Tunnel						
✤ Network >	Authentication						
Policy & Objects	Method		Pre-shared Key 🔹				
Security Profiles	Pre-shared Key				•••••	۲	
모 VPN Y	IKE						
Overlay Controller VPN	Version		1 2				
IPsec Tunnels 습	Dhace 1 Proposal	O Add					
IPsec Wizard	Encryption	• AUG		theatiestica	CUAA	-	
IPsec Tunnel Template	Encryption	AE5128	· Au	Intentication	SHAI		
SSL-VPN Portals	D/// 11.11				29 28	27	
SSL-VPN Settings	Dime-Heilman Gr	oup		14 5 2	2 1	10	
SSL-VPN Clients	Key Lifetime (seco	nds)	28800				
VPN Location Map	Local ID						
User & Authentication >							
	Name	Local A	Address	Rem	note Address	5	
System 1 >	FG-AWS	192.168	3.10.0/24	1	0.0.0/16		
☆ Security Fabric >			Company.				
년 Log & Report >	New Phase 2						0 0
	Name	FO	5-AWS				
	Comments	C	omments		11		
	Local Address	Su	ibnet 🔹	192.168.10	.0/24		
	Remote Address	Su	ibnet 👻	10.0.0/16			

Figure 10.91: Create a custom VPN

2 Dashboard	> New VPN Tunnel		
+ Network	New Phase 2		0 0
Policy & Objects Security Profiles	Name	FG-AWS	
	Comments	Comments	
Overlay Controller VPN	Local Address	Subnet - 192.168.10.0/24	
IPsec Tunnels	Remote Address	Subnet - 10.0.0/16	
IPsec Wizard	Advanced		
IPsec Tunnel Template	Phase 2 Proposal O Add		
SSL-VPN Portals	Encryption AES12	8 • Authentication SHA1 •	
SSL-VPN Settings SSL-VPN Clients	Enable Replay Detection	1	
VPN Location Map	Enable Perfect Forward Sec	erecy (PFS) 🛃	
Luser & Authentication	> Diffie-Hellman Group	32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1	
🗘 System 🚺	> Local Port	All 🛃	
🔆 Security Fabric	Remote Port	All 🛃	
Leg & Report	> Protocol	All 💽	
	Auto-negotiate		
	Autokey Keep Alive		
	Key Lifetime	Seconds 🗸	
	Seconds	3600	
	1.3		OK Cancel

Figure 10.92: Create a custom VPN

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

ypn-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.
1
! 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
1
! 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

	FortiGate VM64-KVM 1	3 5 7 9 81 13 15 17 19 M M M M M M M M M M 4 5 6 10 12 1 ⁴ 16 18 20	21 23		
+	Create New - & Edit	Delete 🕨 Integrate In	iterface	Search	Q
	Name ≑	Type ≑	Members #	IP/Netmask 🛱	Administrative Access 🖨
) 3	• 802.3ad Aggregate 1				
	✤ fortilink	₽ 802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
	Physical Interface 11	The second second			
	m port1	Physical Interface		142.232.198.157/255.255.255.0	HTTPS HTTP
	• G FG-AWS	Tunnel Interface		0.0.0.0/0.0.0.0	
	m port2	Physical Interface		192.168.10.1/255.255.255.0	
	m port3	Physical Interface		0.0.0/0.0.0.0	

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

Name	FG-A	AWS		
Alias Type Interface	Tunne	el Interface		
VRFID 0	0			
Role	Undefi	ned	-	
Addressing	mode	Manual		
IP	mode	169 254 72	194	
Remote IP/N	Netmask	169.254.72	.193/30	
Administrat	ive Access			
IPv4		S Access		PING SNMP
	Speed	Test	□ RADIUS Accounting	Connection 3
DHCPS	erver			
Network				

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

Ð	Dashboard	->-	New Static Route				
\$	Network Interfaces	~	Automatic gateway retrieval ① C Destination ①	Subnet Internet Service			
	Packet Capture SD-WAN	_	Interface	10.0.0/16 FG-AWS +	×		
	Static Routes	☆	Administrative Distance 🚯	10			
	Policy Routes		Comments	Write a comment.,,	/ 0/255		
	RIP		Status	Senabled Obisabled			
	OSPF BGP Routing Objects Multicast		Advanced Options				
B	Policy & Objects	>					
•	Security Profiles	>					
	VPN	>					
1	User & Authentication	>					
(:-	WiFi Controller	>					
۵	System	(1) >				OK	Cancel

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

≡ Q.					
+Create New & Edit 🗇 C	lone 🖹 D	elete Search		Q	
Destination 🗢	T	Gateway IP 🖨	Interface ≑		Status ≑
0.0.0/0	142.2	32.198.254	port1		Enabled
10.0.0/16	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.

Name	FG-LAN	
Color	Change	
Туре	Subnet	•
IP/Netmask	192.168.10.0/24	
Interface	any	•
Static route configura	tion O	
Comments	Write a commont	

Figure 10.99: Create a subnet for local network

Name	AWS-LAN	
Color	Change	
Туре	Subnet	•
IP/Netmask	10.0.0/16	
Interface	🗆 any	+
Static route configura	tion 🔿	
Comments	Write a comment	0/259

Figure 10.100: Create a subnet for AWS local network

Ð	Dashboard	> New Policy				
+	Network	>				
B	Policy & Objects	Vame ()	FG-AWS			
	Firewall Policy	1 Incoming Interface	m port2	+		
	IPv4 DoS Policy	Outgoing Interface	G FG-AWS	· •		
	Addresses	Source	E FG-LAN	×		
	Internet Service Database	Destination	aws-lan	×		
	Services		+			
	Schedules	Schedule	Lo always	•		
	Virtual IPs	Service	ALL +	×		
	IP Pools	Action	✓ ACCEPT Ø DENY			
	Protocol Options					
	Traffic Shaping	Inspection Mode	Flow-based Proxy-based			
4	Security Profiles	> Firewall / Network C	Options			
브	VPN	NAT O				
•) (•	User & Authentication WiFi Controller	> Protocol Options	PROT default	- 1		
*	System 1	Security Profiles				
~~	Security Fabric	AntiVirus				
[Log & Report	Web Filter				
		DNS Filter				
		Application Control	0			
		inc.	~			
	FURTINET .	7.0.3			OK	Cancel

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

+Create New	🖋 Edit 📋	Delete Q Police	y Lookup Search	i		Q	
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
🖃 🔳 port2 → 🧟	FG-AWS 1						
FG-AWS Po	E FG-LAN	AWS-LAN	Co always	ALL	✓ ACCEPT	O Disabled	ss. no-inspection
Set Status							
T Filter by I	Name +						
Copy							
Paste	÷-						
+ Insert Em	npty Policy 🔸						
Clone Re	verse						
Bhow Mat	tching Logs						
Show in Fe	ortiView						
🖋 Edit							
>_ Edit in CL							
Delete Po	olicy						

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

Ð	Dashboard	>	Edit Policy					
4	Network	>						
8	Policy & Objects	~	Name ()	AWS-FG				
	Firewall Policy	☆	Incoming Interface	G FG-AWS		-		
	IPv4 DoS Policy		Outgoing Interface	m port2		•		
	Addresses		Source	AWS-LAN		×		
	Internet Service Database		Destination	FG-LAN		×		
	Services		6 h . d . h	+				
	Schedules		Schedule	Lo always		•		
	Virtual IPs		Service	ALL +		×		
	IP Pools		Action	✓ ACCEPT Ø	DENY			
	Protocol Options							
	Traffic Shaping	Ĩ	Inspection Mode	Flow-based Proxy-based	ased			
	Security Profiles VPN	> >	Firewall / Network C	Options				
1	User & Authentication	>	NAT O					
((.	WiFi Controller	>	Protocol Options	PROT default		•		
•	System	1 >	Security Profiles					
1.11	Log C Deport	ĺ.	AntiVirus	•				
	Log & Report	ĺ.	Web Filter	•				
			DNS Filter	•				
			Application Control	•				
			100	~				1
	FORTIDET	v7.0.3					ОК	Cancel

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

FGVM01TM19008000	• ≡ Q,							
Dashboard	> + Create N	ew 🖋 Edit 🗐	Delete Q Polic	y Lookup Searc	:h			Q
Network Network Delicy & Objects	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Firewall Policy	🔓 🖻 🚇 FG-AV	VS→🖾 port2 ①						
IPv4 DoS Policy	AWS-FG	AWS-LAN	E FG-LAN	to always	ALL ALL	✓ ACCEPT	O Disabled	ss. no-inspection
Addresses	🖃 🔚 port2	→ FG-AWS			- Friday			
Internet Service	FG-AWS	E FG-LAN	aws-lan	to always	I ALL	V ACCEPT	O Disabled	ss. no-inspection
Database	🛨 Implicit	D					-	
Services								

Figure 10.104: Firewall Policies Overview

Verify Connections

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

Dashboard	>	+Create New - Fd	it 🖻 Delete	Search		Q		
Network	>	Tunnel			Interface Diading +		Status #	
💄 Policy & Objects	>	Tuhiner	*		Interrace photing +		Status +	
Security Profiles	>	□ □ Custom 1				and the second second		
I VPN	~	G FG-AWS		🔳 port1		O Up		4
Overlay Controller VPN								
IPsec Tunnels								
IPsec Wizard								
IPsec Tunnel Template								

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

, Filter VPN connecti	lons					<	1 >
PN ID: vpn-0a9b7e3a	a2ca3eebd2 X Cle	ar filters					
Name	VPN ID	⊽ Sta	te 🗸	Virtual private	e gateway 🔻 🛛 Tra	ansît gateway	~
VPNAWS	vpn-0a9b7e3a2	ca3eebd2 🔘	Available	vgw-048d1dd	1e6ba61f05 -		
-Oa9b7e3a2ca3eeb	Dd2 / VPNAWS						
-Oa9b7e3a2ca3eeb	od2 / VPNAWS						
Details	details Static routes	Tags					
Details	details Static routes	Tags					
-Oa9b7e3a2ca3eeb Details Tunnel	details Static routes	Tags					
Details Tunnel	details Static routes	Tags					
Details Tunnel	details Static routes	Tags	is not highly available a	nd we strongly rec	commend you configure	e your second tuni	nel. X
Details Tunnel	details Static routes	Tags	is not highly available a	nd we strongly rec	commend you configure	e your second tuni	nel. X
Details Tunnel	details Static routes	Tags.	is not highly available a	nd we strongly rea	commend you configure	e your second tuni	nel. X
Details Tunnel Tunnel Tunnel state	details Static routes	Tags.	is not highly available a	nd we strongly red	commend you configure	e your second tuni	nel. X
Details Tunnel This VPN connect Tunnel state	details Static routes	Tags.	is not highly available a	nd we strongly rea	commend you configure	e your second tuni	nel. X
Cageb7e3a2ca3eeb Details Tunnel This VPN connect Tunnel state Funnel number ♥	details Static routes	Tags This mode of operation	is not highly available an Inside IPv6 CIDR 🛛	nd we strongly red	commend you configure Last status change	e your second tunn	nel. X Detail
Cageb7e5a2ca3eeb Details Tunnel M This VPN connect Funnel state Funnel number ⊽ Funnel 1	details Static routes ion is not using both tunnels Outside IP address ▼ 3.225.102.90	Tags This mode of operation Inside IPv4 CIDR ▼ 169.254.72.192/30	is not highly available an Inside IPv6 CIDR 🔻	nd we strongly red Status ⊽ ⊘ Up	commend you configure Last status change May 30, 2022, 9:29:	e your second tunn ⊽ :44 (UTC-07:00)	nel. X Detail
Cageb7e5a2ca3eeb Details Tunnel This VPN connect Tunnel state Funnel number ♥ Funnel 1	details Static routes ion is not using both tunnels Outside IP address V 3.225.102.90	Tags This mode of operation Inside IPv4 CIDR ♥ 169.254.72.192/30	i is not highly available ar Inside IPv6 CIDR マ -	nd we strongly red Status ⊽ ⊘ Up	commend you configure Last status change May 30, 2022, 9:29:	e your second tunn ⊽ :44 (UTC-07:00)	nel. X Detail
Petails Tunnel Tunnel state Funnel number ♥ Funnel 1 Funnel 2	details Static routes ion is not using both tunnels Outside IP address ▼ 3.225.102.90 54.83.91.6	Tags This mode of operation Inside IPv4 CIDR ♥ 169.254.72.192/30 169.254.143.60/30	i is not highly available ar Inside IPv6 CIDR 호 -	nd we strongly red Status ♥ ⓒ Up ⓒ Down	commend you configure Last status change May 30, 2022, 9:29: May 30, 2022, 9:16:	e your second tuni マ :44 (UTC-07:00) :00 (UTC-07:00)	nel. X Detail

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.

aws	Services	Q Sear	ch for s	ervices, features,	blags, docs, and mo	e	[Alt+5	1					D	¢	0	N. Virginia 🔻	tungle 🔻
New VI	PC Experience		You	Ir VPCs Info									C	Actio	ns 🔻	Create V	e C
VPC Dash	board		Q	Filler VPC1											1	1 2	0
EC2 Glob	al View New PC:	i	×.	Name		~	VPC ID		v	State	~	IPv4 CIDR		~	IPv6 C	CIDR	
Q Select	t a VPC		4	_	_		_		-							No VF	Cs found
VIRTUAL CLOUD	PRIVATE																
Subnets																	

Figure 10.107: Create a VPC

PC settings		
esources to create Info reate only the VPC resource or cre	ate VPC, subnets, etc.	
• VPC only	🗇 VPC, subnets, etc.	
ame tag - optional reates a tag with a key of 'Name' i	and a value that you specify.	
AWS-VPC		
4 CIDR block Info		
IPv4 CIDR manual input		
IPAM-allocated IPv4 CIDR	block	
v4 CIDR		
10.0.0/16		
v6 CIDR block Info		
No IPv6 CIDR block		
IPAM-allocated IPv6 CIDR	block	
Amazon-provided IPv6 CIE	DR block	
IPv6 CIDR owned by me		
onancy late		
chancy uno		

Figure 10.108: Create a VPC named "AWS-VPC"

2. Create a subnet.

New VPC Experience Tell us what you think	Subnets Infe		C Actions V Crea	ate subn	et
VPC Dashboard	Q Filter subnets		1 ×	1 2	0
EC2 Global View New Filter by VPC:	4 Name V Subnet ID V State	♥ VPC	V IPv4 CIDR	Ŧ	IPvé
Q Select a VPC					
VIRTUAL PRIVATE					
Your VPCs					
Subnets					-
Route Tables	Select a subnet		6		

Figure 10.109: Create a subnet

/PC ID reate subnets in this VPC.	
vpc-060a1e2007366fbf4 (AWS-VPC)	
Associated VPC CIDRs	
Pv4 CIDRs	
0.0.0/16	
Subnet settings pecify the CIDR blocks and Availability Zone for the subnet.	
Subnet settings pecify 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.	
Subnet settings pecify 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	
Subnet settings pecify 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.	
Subnet settings pecify 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.	

Figure 10.110: Create a public subnet under AWS-VPC

VPC	
PC ID reate subnets in this VPC.	
vpc-060a1e2007366fbf4 (AWS-VPC)	*
Associated VPC CIDRs	
Pv4 CIDRs	
0.0.0.0/16 Subnet settings pecify the CIDR blocks and Availability Zone for the subnet.	
10.0.0.0/16 Subnet settings specify the CIDR blocks and Availability Zone for the subnet. Subnet 1 of 1 Subnet name	
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.	
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 Subnet	
10.0.0.0/16 Subnet settings Subnet 1 of 1 Subnet name Create a tag with a key of 'Name' and a value that you specify. Private Subnet The name can be up to 256 characters long.	
10.0.0.0/16 Subnet settings Subnet 1 of 1 Subnet name Create a tag with a key of 'Name' and a value that you specify. Private 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	

Figure 10.111: Create a private subnet under AWS-VPC

3. Create an internet gateway.

New VPC Experience Tell us what you think	Internet gateways Info	ateway
VPC Dashboard EC2 Global View New Filter by VPC: Q Select a VPC	Q. Filter internet galeways Name ▼ Internet galeway ID ▼ State ▼ VPC ID ▼ Owner No internet galeways found in this Region	> ()
VIRTUAL PRIVATE CLOUD Your VPCs		
Subnets Route Tables Internet Gateways	Select an internet gateway above	

Figure 10.112: Create an internet gateway

reate internet gateway	Info		
n internet gateway is a virtual router that con or the gateway below.	nects a VPC to the internet. To	create a new inte	met gateway specify the nam
Internet gateway settings			
Name tag Creates a tag with a key of 'Name' and a value that	you specify.		
AWS-IGW			
Tags - optional		stianal value Vauca	n use tags to search and filter
A tag is a label that you assign to an AWS resource. your resources or track your AWS costs.	Each tag consists of a key and an op	prional value. You ca	
A tag is a label that you assign to an AWS resource. your resources or track your AWS costs. Key Q. Name	Value - optional	X	Remove

Figure 10.113: Create an internet gateway

New VPC Experience Tell as what you think	Internet gateways (1/1) Info	C	Actions 🔺 Create	internet gateway
VPC Dashboard	Q, Fliter Internet gatewaya		View details Attach to VPC	< 1 > @
EC2 Global View New	🔞 🗹 Name 🤍 Internet gateway ID 🦁 State 🔍 VPC ID		Derach from VPC	Owner
Q Select a VPC	AWS-IGW igw-0b81c8d93b9e4ea9F O Detached -		Manage tags	590508865535
VIRTUAL PRIVATE CLOUD Your VPCs			Delete internet gateway	
Subnets				
Route Tables	igw-0b81c8d93b9e4ea9f / AWS-IGW			
Internet Gateways	Detaile			
Egress Only Internet Gateways	and and and			

Figure 10.114: Attach an internet gateway to VPC

PC			
ttach an internet gateway to	a VPC to enable the VPC to communit	ate with the internet. Specify the VP	C to attach below.
vailable VPCs ttach the internet gateway to	this VPC.		
Q vpc-060a1e2007366	fbf4	×	

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.

New VPC Experience. Tall us what you think		Rou	te tables (1/1	Info				[C	Actions 🔻	Create route table
VPC Dashboard	Ê	Q	Filter joute tables								<1> 0
EC2 Global View North	Ā		Name	~	Route table ID	4	Explicit subnet associat	Edge associat	ions	Main 🛛	VPC
Q Select a VPC			Private Route	Z	rtb-087e78e7f2a174a94		-	-		Yes	vpc-060a1e2007366fbf4
VIRTUAL PRIVATE	L										
Your VPCs	14										
Subnets							-				
Route Tables	Ľ	rtb-0	87e78e7f2a174a	94 / Priv	ate Route						

Figure 10.116: Edit private route

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

oute table specifies how pac nection.	kets are forward	ed between the subnets within	your VPC, the in	ternet, and your VPN
Route table settings				
Name - optional Create a tag with a key of Name	and a value that y	ou specify.		
Public Route				
/PC The VPC to use for this route tat	ile.			
vpc-060a1e2007366fbf4	(AWS-VPC)		Ψ.	
Tags tag is a label that you assign to our resources or track your AW Key	o an AWS resource. 5 costs.	Each tag consists of a key and an op Value - optional	tional value. You ca	n use tags to search and filter
Tags A tag is a label that you assign to nour resources or track your AW Gey Q. Name	o an AWS resource. 5 costs.	Each tag consists of a key and an op Value - optional Q. Public Route	tional value: You ca	Remove

Figure 10.117: Create a public route

10.5 Deploy FortiGate in AWS 259

New VPC Experience Tell us what you think	Route tables (1/2) Info		CA	ctions V Create route table
VPC Dashboard	Q Filter coute tables			< 1 > @
EC2 Global View New	Name 🔻 Route table ID	♥ Explicit subnet associat	Edge associations	Main 🗢 VPC
O Select a VPC	Public Route rtb-0121768a920	04bc14a -	+	No vpc-060a1e2007366fbf4
C SCICLIA VFG	Private Route rtb-087e78e7f2a	174a94 -	-	Yes vpc-060a1e2007366fbf4
VIRTUAL PRIVATE				
Your VPCs				
Subnets				
Route Tables	rtb-0121768a9204bc14a / Public Route			
Internet Gateways	Post-ile Poster Cohert secolations	Education Burtonica	ten l Tren	
Egress Only Internet Gateways	Details Koutes Subnet associations	Edge associations Route propagat	rags	
Carrier Gateways	Pourtos (1)			Edite courter
DHCP Option Sets	Routes (1)			Edit routes
Elastic IPs	Q Filter routes		Both	▼ <1> ©
Managed Prefix Lists				
Endpoints	Destination 👳 Ti	arget 🛛 Status	⊽ Prop	agated 🗸 🗸
Endpoint Services	10.0.0/16 lo	cal 🥥 Active	No	
NAT Gateways				

Figure 10.118: Edit routes on Public Route

/PC > Route tables > rtb-0121768a9204bc1	4a) Edit	routes.				
Edit routes						
Destination		Target		Status	Propagated	
10.0.0,0/16		Q, local	×	@ Active	No	
Q 0.0.0.0/0	×	Q igw-	×	e.	No	Remove
Add route		igw-0b81c8d93b9e4ea9f (AWS-IGW)				
					Cancel	Preview Save changes

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

New VPC Experience	VPC > Route tables > rtb-012	1768a9204bc14a			
VPC Dashboard EC2 Global View Hew	rtb-0121768a920	4bc14a / Public Ro	ute	Acti	ons 🔻
Filter by VPC:	You can now check network	connectivity with Reachability Analyze	r	Run Reachability Analyzer	X
Q Select a VPC					-
VIRTUAL PRIVATE	Details Info				
Your VPCs					
Subnets	Route table ID	Main	Explicit subnet associations	Edge associations	
Route Tables	Ttb-0121768a9204bc14a	D No	×	8	
Internet Gateways	VPC	Owner ID			
Egress Only Internet Gateways	vpc-060a1e2007366fbf4 AWS- VPC	5 90508865535			
Carrier Gateways					
DHCP Option Sets					
Elastic IPs	Routes Subnet association	ns Edge associations Rou	e propagation Tags		
Managed Prefix Lists					
Endpoints	and the state of the sector				_
Endpoint Services	Explicit subnet association	ons (0)		Edit subnet association	ins
NAT Gateways	Q Find subnet association			× 1 >	0
100 C					

Figure 10.120: Associate Public Subnet to Public Route

Ava	ilable subnets (1/	(2)								
Q	Filter subnet associatio	ans							< 1.2	0
=	Name		Subnet ID	4	IPv4 CIDR	-	IPv6 CIDR	Route table ID		
~	Public Subnet		subnet-06ed7507849737ecf		10.0.0/24		-	Main (rtb-087e78e7f2a1	74a94 / Private Route)
	Private Subnet		subnet-0936fd8c6f4984efe		10.0.1.0/24		-	Main (rtb-087e78e7f2a1	74a94 / Private Route	1
Sele	ected subnets									

Figure 10.121: Associate Public Subnet to Public Route

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

Key pair A key pair, consisting of a private key and a public key, is a set of security credentials t an instance.	that you use to prove your identity when connecting
Name	
AWS-Lab	
The name can include up to 255 ASCII characters. It can't include leading or trailing sp	paces.
Key pair type Info	
O RSA	
O ED25519	
Private key file format	
perm For use with OpenSSH	
For use with PuTTY	
Tags (Optional)	
No tags associated with the resource.	
Add tag	

Figure 10.122: Create a key pair

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

New EC2 Experience X	Instances Info		C Connect	t Instance state 🔻	Actions v	Launch Instance	s 🔻
EC2 Darbbaard	Q. Search						0 < 1
EC2 Global View	Name Name	♥ Instance ID	Instance state			eck	A
Events			No instanc	:05			
Tags			You do not have any instan	nces in this region			
Limits			Launch insta	inces			
▼ Instances	4						
Instances New							
Instance Types							

Figure 10.123: Launch a FortiGate instance

1. Choose AMI	2. Choose Instance Ty	oe 3. Config	ure Instance	4. Add Storage	5: Add Tags	6. Configure Security	Group	7. Review		
Step 1: Ch An AMI is a tempi AWS Marketplace	noose an Am late that contains the e; or you can select or	azon Ma coftware config e of your own	chine In Juration (oper AMIS.	nage (AMI ating system, app	I) plication server,	and applications) requ	uired to la	aunch your insta	nce. You can select an Alv	Cancel and E All provided by AWS, our user community,
Q, Fortinet										Search by Systems Manager para
Quick Start ((0)									K < 1 to 10 of 44 Products
My AMIs (0)	F	RTINET	Fortinet F	ortiGate Next-	Generation Fi	rewall				Select
AWS Marketp	lace (44)		Starting from	9) 7 2.0 Previous ve \$0.36/hr or from \$1.9	ersions By Fortine 20.00/yr (up to 60%	t Inc. savings) for software + AV/S	S usage fee	5		
Community A	AMIS (7)	Hee Trial	Linux/Unix, O Fortinet For environmen	ther 7.2.0 64-bit (x8 tiGate allows mitig t. FortiGate includ	6) Amazon Machine gation of blind spo les all of the secu	Image (AMI) Updated: 4/3 ots to improve policy cou urity and networking sen	0/22 mpliance vices com	by implementing mon to FortiGate	critical security controls with physical appliances.	in your AWS

Figure 10.124: Select Fortinet FortiGate Next-Generation Firewall

FERTINET	Fortinet FortiGate Next-Generation Firewall	Pricing Details				, î
	FortiGate Next-Generation Firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive	Hourly Fees				
	suite of powerful security features. Application	Instance Type	Software	EC2	Total	
	control, antivirus, IPS, Web filtering and VPN along	t2.small	\$0.36	\$0.023	\$0.383/hr	
	database vulnerability management and flow-	t3.small	\$0.88	\$0.021	\$0.901/hr	
	based	t3 xlarge	\$1.02	\$0.166	\$1.186/hr	
	More info	c4.large	\$0.88	\$0.10	\$0.98/hr	
	View Additional Details in AWS Marketplace	c4.xlarge	\$1.02	\$0.199	\$1.219/hr	
Product Details		c4.2xlarge	\$2.35	\$0.398	\$2.748/hr	
	Factional los	c4.4xlarge	\$3.29	\$0.796	\$4.086/hr	
Ву	Portinet Inc.	c4.8xlarge	\$4.10	\$1.591	\$5.691/hr	
Customer Rating	**************************************	c5.large	\$0.88	\$0.085	\$0.965/hr	
Latest Version	7.2.0	c5.xlarge	\$1.02	\$0.17	\$1.19/hr	
Base Operating System	Linux/Unix, Other 7.2.0	c5.2xlarge	\$2.35	\$0.34	\$2.69/hr	
Delivery Method	64-bit (x86) Amazon Machine Image (AMI)	c5.4xlarge	\$3.29	\$0.68	\$3.97/hr	
License Agreement	End User License Agreement	c5.9xlarge	\$4.10	\$1.53	\$5.63/hr	
On Marketplace Since	11/7/14	c5.18xlarge	\$5.16	\$3.06	\$8.22/hr	
Highlights		c5d.large	\$0.88	\$0.096	\$0.976/hr	
		c5d xlarge	\$1.02	\$0.192	\$1.212/hr	
 FortiGate offers protect 	tion from a broad array of threats, with support for all	c5d.2xlarge	\$2.35	\$0.384	\$2.734/hr	_

Figure 10.125: Accept FortiGate licence

Cancel Continue

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 application 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 familie	s ¥	Current generati	on Y 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	*	Туре -	vCPUs (j)	+ Memory (GiB) +	Instance Storage (GB) $(i) \star$		
0	t2		t2.nano	1	0.5	EBS only		
0	t2		t2 micro Free tier eligible	1	1	EBS only		
	t2		t2.small	1	2	EBS only		
0	t2		t2.medium	2	4	EBS only		
0	12		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	1	1 Launch into Auto Scaling (Group (j)
Purchasing option	1	Request Spot instances	
Network	0	vpc-060a1e2007366fbf4 AWS-VPC C No default VPC found. Create a new default VPC.	Create new VPC
Subnet	1	subnet-06ed7507849737ecf Public Subnet us-eas 251 IP Addresses available	Create new subnet
Auto-assign Public IP		Enable	
Hostname type		Use subnet setting (IP name)	
DNS Hostname	1	Enable IP name IPv4 (A record) DNS requests	
		Enable resource-based IPv6 (AAAA record) DNS request:	s

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 (j)	Device ()	Snapshot ()	Size (GiB) (j)	Volume Type ()	IOPS (\tilde{j})	Throughput (MB/s) ()
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 (128 characters maximum)	Value (256 characters maximum)	Instances (j)
Name	FG	

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, I 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 or security groups.

Secu	rity group name: FortiGate	Security Group	
	Description: FortiGate	Security Group	
Type 🕕	Protocol (i)	Port Range ①	Source (j)
SSH V	TCP	22	Custom ~ 0.0.0.0/0
HTTP V	TCP	80	Custom ~ 0.0.0.0/0
HTTPS ¥	TCP	443	Custom v 0.0.0/0
Custom TCP F 🗸	TCP	541	Custom ~ 0.0.0.0/0
Custom TCP F 🗸	TCP	3000	Custom v 0.0.0/0
Custom TCP F 🗸	TCP	8080	Custom ~ 0.0.0.0/0
RDP 🗸	TCP	3389	Custom v 0.0.0.0/0
All ICMP - IPV V	ICMP	0 - 65535	Custom ~ 0.0.0/0

Add Rule

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

0

▼ Instances

Instances New

Instance Types

Savings Plans

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Reserved Instances New

Launch Templates Spot Requests

50	lect an existing key pair or creat	e a new key pai	r ×	
A ki allo obt sec	ey pair consists of a public key that AWS stores, and w you to connect to your instance securely. For Wind in the password used to log into your instance. For L urely SSH into your instance. Amazon EC2 supports	a private key file that y ows AMIs, the private ke inux AMIs, the private k ED25519 and RSA key	you store. Together, they ey file is required to ey file allows you to pair types.	
Not	e: The selected key pair will be added to the set of ke ut removing existing key pairs from a public AML	eys authorized for this in:	stance. Learn more	
	Choose an existing key pair			
	Select a key pair			
	AWS-Lab RSA		~	
	I acknowledge that I have access to the corresponding file, I won't be able to log into my instance.	nding private key file, an	d that without this	
		Cancel	Launch Instances	
_		Cancel	Launch Instances	
Figur	e 10.131: Accept key pair and launch	Cancel	Launch Instances	
Figur	e 10.131: Accept key pair and launch	Cancel instances C Connect	Launch Instances	unchi
Figur	e 10.131: Accept key pair and launch	Cancel instances	Launch Instances	unch i
Figur	e 10.131: Accept key pair and launch	Cancel instances C Connect Instance state	Launch Instances	unch i
Figur	e 10.131: Accept key pair and launch	Cancel instances C Connect Instance state © Running	Launch Instances	unch i
Figur New EC2 Experience Tell us what you think EC2 Dashboard EC2 Global View Events Tags	e 10.131: Accept key pair and launch	Cancel instances C Connect Instance state O Running	Launch Instances Instance state ▼ Actions ▼ La V Instance type V Status check @Q t2.small ② Initializing	unch i

Details Security Networking Storage Status checks Monitoring

Public IPv4 address

Instance state

⊘ Running

🗇 3.239.117.237 | open address 🗹

=

Tags

Private IPv4 addresses

Answer private resource DNS name

10.0.0.22

Public IPv4 DNS

IPv4 (A)

Private IP DNS name (IPv4 only) Hostname type IP name: ip-10-0-0-22.ec2.internal ▼ Images ip-10-0-0-22.ec2.internal

▼ Instance summary Info

D i-Off098db861c07b53 (FG)

Instance ID

IPv6 address

Instance: i-Off098db861c07b53 (FG)

Figure 10.132: FG instance has been launched successfully

10.5 Deploy FortiGate in AWS 265



Figure 10.133: Change default interface name to FG Public Subnet

7. Add a new private subnet interface.

tastic network interface is a logical networking component in a VPC	. that represents a virti	lat network card.
Details Info		
Description - optional descriptive name for the network interface.		
FG Private Subnet		
FG Private Subnet ubnet he subnet in which to create the network interface.		
FG Private Subnet ubnet he subnet in which to create the network interface. Q Select subnet		C
FG Private Subnet ubnet he subnet in which to create the network interface. Q Select subnet subnet-06ed7507849737ecf Public Subnet Owner: 590508865535	us-east-1f	C
FG Private Subnet ubnet he subnet in which to create the network interface. Q Select subnet subnet-06ed7507849737ecf Public Subnet Owner: 590508865535 subnet-0936fd8c6f4984efe Private Subnet Owner: 590508865535	us-east-1f us-east-1f	C
FG Private Subnet ubnet he subnet in which to create the network interface. Q Select subnet subnet-06ed7507849737ecf Public Subnet Owner: 590508865535 subnet-0936fd8c6f4984efe Private Subnet Owner: 590508865535 C Custom	us-east-1f us-east-1f	C
FG Private Subnet ubnet he subnet in which to create the network interface. Q Select subnet subnet-06ed7507849737ecf Public Subnet Owner: 590508865535 subnet-0936fd8c6f4984efe Private Subnet Owner: 590508865535 Custom dastic Fabric Adapter	us-east-1f us-east-1f	C

Figure 10.134: Create FG Private Subnet

4	Find security groups				< 1 > ©
	Group ID	~	Group name	~	Description
~	sg-09578bdb48a98e906		FortiGate Security Group		FortiGate Security Group
1	sg-05247b200235cd3df		default		default VPC security group
your re	esources or track your AWS costs.	Loui et a	acti tag conside of a Acy and an option	Net Visitor	. The carriese rays to search and meet

Figure 10.135: Create FG Private Subnet

Net	work interfaces (1/2) Info				C Actions V	Create	network interface
Q	Filter network interfaces							< 1 > @
	Name	V	Network interface ID 🛛 🗸	Subnet ID	V	VPC ID	V	Availability Zone
	FG Private Subnet		eni-08adedc167a1180a6	subnet-0936fd8c6f4984	efe 🛃	vpc-060a1e2007366	ifbf4 🛃	us-east-1f
	FG Public Subnet		eni-03b2e198495d21f54	subnet-06ed750784973	7ecf 🛃	vpc-060a1e2007366	ifbf4 🔼	us-east-1f
1								

Figure 10.136: Change to FG Private Subnet

Net	work interfaces (1/2) In	fo			C		Actions Create net	work interface
Q	Filter network interfaces						Attach	1 >
•	Name	Ā	Network interface ID 🛛 🗸	Subnet ID	v	VP	Delete	wailability Zo
	FG Private Subnet		eni-08adedc167a1180a6	subnet-0936fd8c6f4984efe 🖸		vpc	Manage IP addresses	s-east-1f
-	FG Public Subnet		eni-03b2e198495d21f54	subnet-06ed7507849737ecf	3	vpc	Associate address Disassociate address	s-east-1f
Net	work interface: eni-08a	dedc	167a1180a6 (FG Private S	= Subnet)			Change termination behavior Change security groups Change source/dest, check Manage tags Manage prefixes	@ ×
0	You can now check network	connec	tivity with Reachability Analyzer.				Change description Create flow log	×

Network interface details

Figure 10.137: Attach the FG Private Subnet to FG

Attach network interface	×
Network interface eni-08adedc167a1180a6 (FG Private Subnet)	
Instance i-Off098db861c07b53	
Instance i-Off098db861c07b53 Q.	

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

Q. filter network interfaces Attach 1 > ■ Name ▼ Network interface ID ▼ Subnet ID ▼ VP Detech wailability. ■ FG Private Subnet eni-08adedc167a1180a6 subnet-0936fd8c6f4984efe vpc Manage IP addresses s-east-1f ▲ FG Public Subnet eni-03b2e198495d21f54 subnet-06ed7507849737ecf vpc Manage IP addresses s-east-1f ▲ Ssociate address Change termination behavior Change security groups © Change source/dest. check ■ Now can now check network connectivity with Reachability Analyzer. Change description ×	Net	work interfaces (1/2) Info			C	Actions Create net	work interface
Name ▼ Network interface ID ▼ Subnet ID ▼ VP Delete wailability. FG Private Subnet eni-08adedc167a1180a6 subnet-0936fd8c6f4984efe 2 vpr Manage IP addresses s-east-1f FG Public Subnet eni-03b2e198495d21f54 subnet-06ed7507849737ecf 2 vpr Associate address s-east-1f Network interface: eni-03b2e198495d21f54 (FG Public Subnet) Subnet OGed7507849737ecf 2 vpr Change security groups Change security groups Change security groups Security groups	Q	Filter network interfaces					Attach	1 > @
FG Private Subnet eni-08adedc167a1180a6 subnet-0936fd8c6f4984efe vpr Manage IP addresses s-east-1f FG Public Subnet eni-03b2e198495d21f54 subnet-06ed7507849737ecf vpr Associate address s-east-1f Details Flow logs Tags Change security groups Change security groups © Out can now check network connectivity with Reachability Analyzer. Change description ×	•	Name	~	Network interface ID 👳	Subnet ID 👳	VP	Delete	wailability Zone
FG Public Subnet eni-03b2e198495d21f54 subnet-06ed7507849737ecf (2) vpc Associate address Disassociate address Change termination behavior Change security groups Change security groups Change termination behavior Change termination You can now check network connectivity with Reachability Analyzer.	0	FG Private Subnet		eni-08adedc167a1180a6	subnet-0936fd8c6f4984efe 🗹	vpc	Manage IP addresses	s-east-1f
Disassociate address Disassociate address Change termination behavior Change security groups Change security groups Change tags Manage tags Manage prefixes Change description Create flow log	V	FG Public Subnet		eni-03b2e198495d21f54	subnet-06ed7507849737ecf 🖸	vpc	Associate address	s-east-1f
You can now check network connectivity with Reachability Analyzer. Create flow log	Deta	work interface: eni-C	D3b2e19	8495d21f54 (FG Public Si	= ubnet)		Change termination behavior Change security groups Change source/dest. check Manage tags Manage prefixes Change description	© ×
	(You can now check netwo	ork connect	tivity with Reachability Analyzer.			Create flow log	×

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

Change source/destination check		×
Network interface eni-03b2e198495d21f54 Source/destination check		
	Cancel	Save

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

9. Edit private route table.

Q	Filter route tables										4	1.0	٢
	Name	~	Route table ID			Explicit subnet a	associat,	Edge associat	ions	Main 🗢	VPC		
	Public Route		rtb-0121768a9	204bc14a	5	subnet-06ed750	784973			No	vpc-060a1	2007366	fbf4 A
2	Private Route		rtb-087e78e7f	2a174a94	-	-		-		Yes	vpc-060a1	2007366	fbf4 A
Def	87e78e7f2a174a9	/ Privat	e Route et associations	Edge as	sociatio	ions Route	propagation	Tags					
Det	87e78e7f2a174a9 tails Routes	y / Privat	e Route et associations	Edge at	sociatio	ions Route	propagation	Tags					
Det	87e78e7f2a174a9 tails Routes	/ Privat Subn	e Route et associations	Edge at	sociati	ions Route	propagation	Tags				dit route	5
Det	87e78e7f2a174a9 tails Routes putes (1) Q. Filter routes	Subn	e Route et associations	Edge at	sociatio	ions Route	propagation	Tags	Both	Y		idit route	5
Det Ro Des	87e78e7f2a174a9 tails Routes outes (1) Q. Filter routes stination	Subn	e Route et associations	Edge at	sociati	ions Route	propagation	Tags	Both	• Propagated		idit route	5

Figure 10.143: Edit Private Route

VPC > Route tables > rtb-087e78e7f2a174a9	94 🗇 Edit	routes					
Edit routes							
Destination		Target		Status	Propagated		
10.0.0.0/16		Q local	×	O Active	No		
Q, 0.0.0,0/0 Add route	×	Q Carrier Gateway Core Network Excess Only Internet Gateway		-	No	Rem	love
		Gateway Load Balancer Endpoint Instance Internet Gateway Iocal NAT Gateway Network Interface Outpost Local Gateway Peering Connection Transit Gateway			Cancel	Preview	Save changes

Figure 10.144: Add a default route and select Network Interface

lit routes				
Destination		Target		Status
0.0.0/16		Q local	×	O Active
Q, 0.0.0.0/0	×	Q, eni-	×	-
		eni-03b2e198495d21f54 (FG Public Subnet)		
Add route		eni-08adedc167a1180a6 (FG Private Subnet)		

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

10. Verify Public and Private IP address of FG.

Instances (1/1) Info			C Conne	ect Ins	tance state 🔻	Launch instances	
Q	Search						< 1
	Name		Instance state	~	Instance type	Status ch	eck
2	FG	i-Off098db861c07b53	⊘ Running	ଭ୍ର	t2.small	Ø 2/2 ch	ecks passed
1							
			_				
Ins	tance: i-Off098db	861c07b53 (FG)	-				۲
D	etails Security	Networking Storage	Status checks Mo	nitoring	Tags		
	Instance summary	Info					
br.	istance ID	Pub	lic IPv4 address		Private I	Pv4 addresses	
ć	i-Off098db861c07b5	53 (FG)	3.239.117.237 open add	ress 🖸	D 10.0	.0.22	
					D 10.0	.1.147	
IPv6 address			ance state	Public IPv4 DNS			
- 0			Running	-			
Hostname type Priv			ate IP DNS name (IPv4 on	Answer private resource DNS name			
IF	name: ip-10-0-0-22.ec	2.internal	ip-10-0-0-22.ec2.internal		IPv4 (A)		
In	istance type	Etas	stic IP addresses		Auto-ass	igned IP addres	5
tž	.small				1 3.23	9.117.237 [Pub	lic IP1

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.

A
Your connection is not private
Attackers might be trying to steal your information from 3.239.117.237 (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Q To get Chrome's highest level of security, turn on enhanced protection

Figure 10.147: Access FortiGate



Figure 10.148: Access FortiGate

admin	
•••••	

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

4	You are required to change the default password.
New	password must include:
0	Minimum Length
••••	•••••
••••	

	OK

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.

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

Table 10.5: Port1 and Port2 description

Name	port2					
Alias						
Туре	Physical Interface					
VRFID 0	0					
Role 0	Undefined		•			
Dedicated	Management Port					
Address						
Addressing mode		Manual	DHCP	Auto-managed	by IPAM	One-Arm Sniffer
Retrieve defau	It gateway from server 🧲	D				
Distance		5				
Override inter	nal DNS	D				
Administrative	Access					
IPv4	HTTPS	0				
	FMG-Access	0) SSH			
	FTM	C	RADIUS Accounting			urity Fabric inection 🚯
	Speed Test					
Receive LLDP	6 Use VDOM Setting	Enable	Disable			

Figure 10.152: Change port2 to DHCP Client

FortiGate VM64-AWS 1	2 5 7 + Li 5 1 15 1 	17 19 21 33 18 35 21 34		
+ Create New → 🖋 Edit	🖻 Delete 🕨 Integra	ate Interface	Search	
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				
m 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	
① Tunnel Interface ①			والتجاز الجز	
NAT interface (naf.root)	Tunnel Interface		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





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 <u>section 10.5</u> 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

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

Table 10.6: Devices configuration

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

æ	Dashboard	VPN Creation Wizard	
\$	Network	10 1111 Salar 20 A	uthentication 3 3 Policy & Routing 3 4 Review Settings
8	Policy & Objects	Remote device	IP Address Dynamic DNS
4	Security Profiles	Remote IP address	3 239 117 237
묘	VPN	Outgoing Interface	mort1
	Overlay Controller VPN	Authontication method	Dra sharad Kay Signatura
	IPsec Tunnels	Authentication method	
	IPsec Wizard だ	Pre-shared key	Pa\$\$w0rd 92

Figure 10.157: Set remote IP address

Network	2 marshield	Autosanication 3 Policy & Routing 4 Review Settings
Policy & Objects	Local interface	mort2
Security Profiles	Locarinterrace	+
UPN YPN	Local subnets	192.168.10.0/24
Overlay Controller VPN		0
IPsec Tunnels	Remote Subnets	10.0.0/16
IPsec Wizard ರ	7	0
IPsec Tunnel Template	Internet Access (3)	None Share Local Use Remote

Figure 10.158: Set Policy & Routing

3. Create a static route to the default gateway.

+ Network Y		
Interfaces	Destination 1	Subnet Internet Service
DN5 Dacket Capture		0.0.0.0/0.0.0.0
	Gateway Address 🕄	Dynamic Specify
SD-WAN		142.232.198.254
Static Routes 分	Interface	🖮 port1 🗙
Policy Routes	Line and the second second	· · · · · · · · · · · · · · · · · · ·
RIP	Administrative Distance 🕄	10
OSPF	Comments	Write a comment // 0/255
BGP	Status	Enabled ODisabled

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 <u>section 10.5</u>.
- 2. Create a VPN from IPsec Wizard as Figures 10.160 to 10.162.

278 Chapter 10. Cloud Technologies



Figure 10.160: Select VPN name

Dashboard	> VPN Creation Wizard	
Network	> 2	Authentication 3 3 Policy & Routing 3 4 Review Settings
Policy & Objects	Remote device	IP Address Dynamic DNS
Security Profiles	Remote IP address	142.232.198.155
D VPN	Outgoing Interface	m port1
Overlay Controller VPN	Authentication method	Pre-shared Key Signature
IPsec Tunnels	Pre-shared key	Pa\$\$w0rd
IPsec Wizard	☆	

Figure 10.161: Set a remote IP address

🕰 Dashboard	> VPN Creation Wizard	VPN Creation Wizard		
💠 Network	>	3 Policy & Routing	A Review Settings	
📕 Policy & Objects	> Local interface	nort?		
Security Profiles	>	+		
🖵 VPN	 Local subnets 	10.0.1.0/24		
Overlay Controller VPN		0		
IPsec Tunnels	Remote Subnets	192.168.10.0/24		
IPsec Wizard		0		
IPsec Tunnel Template	Internet Access ()	None Share Local Use Remote		

Figure 10.162: Set Policy & Routing

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

10.6 Site-to-Site VPN between FortiGate on Premise and FortiGate in the AWS 279

Automatic gateway retrieval 🕄	
Destination 🕕	Subnet Internet Service
	0.0.0.0/0.0.0.0
Gateway Address 🟮	Dynamic Specify
	10.0.0.1
Interface	m port1 🗶
	+
Administrative Distance 🜖	10
Comments	Write a comment Ø 0/255
Status	Enabled ODisabled

Figure 10.163: Set a default gateway via 10.0.0.1

Subnet Internet Service			
10000/4/			
10.0.0/18			
Dynamic Specify			
10.0.1.1			
m port2	×		
+			
10			
Write a comment			
C Enabled O Disabled			
	Subnet Internet Service 10.0.0/16 Dynamic Specify 10.0.1.1 port2 + 10 Write a comment		

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



Figure 10.165: Overview of static routes on FortiGate

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

← → C ▲ Not secure	https://3.2	39.117.237/ng/vpn/ipsec			6 4
FGTAWS_IC2RK0QC0	· • =	Q			>_
Dashboard	> +	Create New 🔻 🖋 Edit 👘 Delete	Search	Q	
Network Network Dilay & Objects	>	Tunnel 🗢	Interface Binding 🛱	Status ‡	
Security Profiles	, ⊡⊧	🗄 Site to Site - FortiGate 1	The second value of the se		
U VPN	~	O AWSToFG	port1	O Up	4
Overlay Controller VPN				1	
IPsec Tunnels					
IPsec Wizard					

Figure 10.166: Check the status of the tunnel on AWS

← → C ▲ Not secure	https://142.232.198.155/ng/vp	n/ipsec		
FGVM01TM19008000	• ≡ Q			>_ 0*
2 Dashboard	> + Create New +	Edit 🗎 Delete Search		Q
+ Network	> Tunnel 🗘	Interface Bindir	ng 🗘 Status	\$
Policy & Objects Security Profiles	>	Gate 1		
D VPN	 FGToAWS 	port1	O Up	4
Overlay Controller VPN				
IPsec Tunnels			-	
IPsec Wizard				

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.

📮 LXTerminal	. 🗆 ×
<u>F</u> ile <u>E</u> dit <u>T</u> abs <u>H</u> elp	
root@webterm-1:~# ip a grep eth0	*
11: eth0: <broadcast,multicast,up,lower_up> mtu 1500 qdisc fq_codel state UNKNOW</broadcast,multicast,up,lower_up>	/N g
roup default qlen 1000	
inet 192.168.10.2/24 scope global eth0	
root@webterm-1:~# J	
root@webterm-1:~# ping 10.0.1.25	
PING 10.0.1.25 (10.0.1.25) 56(84) bytes of data.	
64 bytes from 10.0.1.25: icmp_seq=1 ttl=126 time=73.6 ms	
64 bytes from 10.0.1.25: icmp_seq=2 ttl=126 time=72.5 ms	
64 bytes from 10.0.1.25: icmp_seq=3 ttl=126 time=70.8 ms	
64 bytes from 10.0.1.25: icmp_seq=4 ttl=126 time=71.7 ms	
64 bytes from 10.0.1.25: icmp_seq=5 ttl=126 time=71.6 ms	
64 bytes from 10.0.1.25: icmp_seq=6 ttl=126 time=75.1 ms	
64 bytes from 10.0.1.25: icmp_seq=7 ttl=126 time=72.1 ms	
64 bytes from 10.0.1.25: icmp_seq=8 ttl=126 time=73.1 ms	
64 bytes from 10.0.1.25: icmp_seq=9 ttl=126 time=71.3 ms	
64 bytes from 10.0.1.25: icmp_seq=10 ttl=126 time=73.0 ms	

Figure 10.168: Ping from WebTerm to Windows VM

5. 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=72ms TTL=62

Figure 10.169: Ping from Windows VM to WebTerm

282 Chapter 10. Cloud Technologies

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.

284 Hamid Talebi

😵 New template		7	×
New template Please select how you want to create a new template			
Install an appliance from the GNS3 server (recommended)			
 Import an appliance file (.gns3a extension) 			
Manually create a new template			
		No. 4 La Consul	
	< gack	Mext > Cancel	_

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."

	7
nload appliances from our online registry.	
low	ownload applances from our online registry.

Figure A.3: Search for "FortiGate"

4. Press "Next" on this screen:

Install FortiGate appliance		?	>
rver Please choose a server type to install the appliance. The grayed out server types are not supported or configured.		•	T
Server type			
① Install the appliance on a remote server			
Install the appliance on the GNS3 VM (recommended)			
O Install the appliance on your local computer.			
	1		
	*		
	 		_

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

5. Press "Next" on this screen:

Install FortiG	Gate	appliance			7 X
emu settings Please choose	e the	e gemu binary that will be used to run this appliance.			
Qemu binary:	1	bin/qemu-system-x86_64 (v4.2.1)			•
				+	
				 (

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."

poliance version and files	Size	Status			14
FortiGate version 6.4.5	34.7 MR	Missing files			-
EGT VM64 KVM-v6-build1828-EORTINET out bym gcow2	34.7 MB	Missing			
empty306 acow2	102 5 KB	Found on GNS3 VM (GNS3 VM	n -		
FortiGate version 6.2.2	56.4 MB	Missing files	9		
EGT VM64 KVM-v6-build1010-EORTINET.out.kvm.gcow2	56.2 MB	Missing			
empty30G.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM	0		
FortiGate version 6.2.1	56.3 MB	Missing files			
FGT_VM64_KVM-v6-build0932-FORTINET.out.kvm.gcow2	56.1 MB	Missing			
empty30G.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM	0		
FortiGate version 6.2.0	55.4 MB	Missing files			
FGT_VM64_KVM-v6-build0866-FORTINET.out.kvm.qcow2	55.2 MB	Missing			
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM	D		
FortiGate version 6.0.3	49.4 MB	Missing files			
FGT_VM64_KVM-v6-build0200-FORTINET.out.kvm.qcow2	49.2 MB	Missing			
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		
FortiGate version 6.0.6	49,9 MB	Missing files			
FGT_VM64_KVM-v6-build0272-FORTINET.out.kvm.qcow2	49.7 MB	Missing			
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		
 FortiGate version 6.0.0 	44.2 MB	Missing files			
FGT_VM64_KVM-v6-build0076-FORTINET.out.kvm.qcow2	44.0 MB	Missing			
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM	D.		
FortiGate version 5.6.7	41.4 MB	Missing files			
FGT_VM04_KVM-v5-build1653-FURTINET.out.kvm.qcow2	41.2 MB	Missing	n		
emptysuo.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM	0		
FORTIGATE VERSION 3.0.4	39.9 MB	Missing files			
compt/20G acou/2	102 5 VP	Found on GNS2 VM (GNS2 VM	b.		
emptysoo.qcowz	192.J KD	Found on Grass vivi (Grass vivi	9		- 1

Figure A.9: Create a new version

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

Appliance version and files	Size	Status		1
 FortiGate version 5.4.10 FGT_VM64_KVM-v5-build1220-FORTINET.c empty30G.qcow2 FortiGate version 5.4.8 FGT_VM64_KVM-v5-build1183-FORTINET.c empty30G.qcow2 FortiGate version 5.4.7 FGT_VM64_KVM-v5-build6446-FORT empty30G.qcow2 	37.4 MB but.kvm.qcow2 37.2 MB 192.5 KE 57.0 MB but.kvm.qcow2 36.8 MB 192.5 KE 37.1 MB Creating a new version	 Missing files Missing Found on GNS3 VM (GNS3 VM) Missing files Missing Found on GNS3 VM (GNS3 VM) Missing files 	×	
 FortiGate version 5.4.6 FGT_VM64_KVM-v5-build1165-FORT empty30G.qcow2 FortiGate version 5.4.5 FGT_VM64_KVM-v5-build1138-FORT empty30G.qcow2 FortiGate version 5.4.4 FGT_VM64_KVM-v5-build17605-FORT empty30G.qcow2 FortiGate version 5.4.3 FGT_VM64_KVM-v5-build1111-FORTINET.c empty30G.qcow2 FortiGate version 5.4.2 FGT_VM64_KVM-v5-build1100-FORTINET.c empty30G.qcow2 FortiGate version 5.4.1 	te a new version for this a se share your experience of ion name: 	Appliance. on the GNS3 community if this version work OK Cancel Missing Found on GNS3 VM (GNS3 VM) Missing Found on GNS3 VM (GNS3 VM) Missing Found on GNS3 VM (GNS3 VM) Missing files	ks.	

Figure A.10: Create a custom version

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



Figure A.11: Click on OK

12. Press OK again.

292 Hamid Talebi



Figure A.12: Click on OK

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

pliance version and files	Gize	Ctatur	1
EGT VM64 KVM-v5-build0762-EORTINET out kvm gcow	2 37.0 MB	Missing	
empty30G.g.cow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.12	36.8 MB	Missing files	
FGT VM64 KVM-v5-build0760-FORTINET.out.kvm.acow	2 36.6 MB	Missing	
emptv30G.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.11	33.6 MB	Missing files	
FGT_VM64_KVM-v5-build0754-FORTINET.out.kvm.qcow	2 33.4 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.10	33.4 MB	Missing files	
FGT_VM64_KVM-v5-build0742-FORTINET.out.kvm.qcow	2 33.2 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.9	33.2 MB	Missing files	
FGT_VM64_KVM-v5-build0736-FORTINET.out.kvm.qcow	2 33.0 MB	Missing	
empty30G.qcow2	192,5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.8	33.1 MB	Missing files	
FGT_VM64_KVM-v5-build0727-FORTINET.out.kvm.qcow	2 32.9 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.7	33.0 MB	Missing files	
FGT_VM64_KVM-v5-build0/18-FORTINET.out.kvm.qcow	2 32.8 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.5	32.5 MB	Missing files	
FGT_VIVI04_KVIVI-V3-build0701-FORTINE1.out.kvm.qcow	102 E KD	Found on CNIC2 VAA (CNIC2 VAA)	
Englighte version curter	192.3 KB	Pound on Gives vivi (Gives Vivi)	
FortiGate version customy?	102.5 KB	Missing files	
EGT VM64 KVM-v5-build1653-EORTINET out him acou	2 0 0 B	Missing	
empt/306.gcow2	102 5 KB	Found on GNS3 VM (GNS3 VM)	

Figure A.13: Download empty30G.qcow2

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

294 Hamid Talebi

Inpliance version and files	Size	Ctatur	1	1
FGT VM64 KVM-v5-build0762-EORTINET out hum acow2	37.0 MB	Missing		ł
empty30G.acow?	192.5 KB	Found on GNS3 VM (GNS3 VM)		l
* FortiGate version 5.2.12	36.8 MB	Mission files		l
EGT_VM64_KVM-v5-build0760-EORTINET.out.kvm.acow2	36.6 MB	Missing		l
empty30G.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		l
 FortiGate version 5.2.11 	33.6 MB	Missing files		I
FGT VM64 KVM-v5-build0754-FORTINET.out.kvm.acow2	33.4 MB	Missing		I
emptv30G.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		
 FortiGate version 5.2.10 	33.4 MB	Missing files		
FGT VM64 KVM-v5-build0742-FORTINET.out.kvm.gcow2	33.2 MB	Missing		
empty30G.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		
 FortiGate version 5.2.9 	33.2 MB	Missing files		
FGT VM64 KVM-v5-build0736-FORTINET.out.kvm.gcow2	33.0 MB	Missing		
empty30G.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		
 FortiGate version 5.2.8 	33.1 MB	Missing files		
FGT_VM64_KVM-v5-build0727-FORTINET.out.kvm.gcow2	32.9 MB	Missing		
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		
 FortiGate version 5.2.7 	33.0 MB	Missing files		
FGT_VM64_KVM-v5-build0718-FORTINET.out.kvm.gcow2	32.8 MB	Missing		ł
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		
 FortiGate version 5.2.5 	32.5 MB	Missing files		
FGT_VM64_KVM-v5-build0701-FORTINET.out.kvm.qcow2	32.3 MB	Missing		
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		
FortiGate version custom	191.8 MB	B Ready to install		
FortiGate version customv2	192.5 KB	Missing files		
FGT_VM64_KVM-v5-build1653-FORTINET.out.kvm.qcow2	0.0 B	Missing		
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)		ł

Figure A.14: Select Custom version

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

nnliance version and files	Size	Status	
FGT VM64 KVM-v5-build0762-FORTINET.out.kvm.acow	2 37.0 MB	Missing	
empty30G.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.12	36.8 MB	Missing files	
FGT_VM64_KVM-v5-build0760-FORTINET.out.kvm.gcow	2 36.6 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.11	33.6 MB	Missing files	
FGT_VM64_KVM-v5-build0754-FORTINET.out.kvm.qcow	2 33.4 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.10	33.4 MB	Missing files	
FGT_VM64_KVM-v5-build0742-FORTINET.out.kvm.qcow	2 33.2 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.9	33.2 MB	Missing files	
FGT_VM64_KVM-v5-build0736-FORTINET.out.kvm.qcow	2 33.0 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.8	33.1 MB	Missing files	
FGT_VMb4_KVM-v5-build0/2/-FORTINET.out.kvm.qcow.	2 32.9 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version 5.2.7	33.0 MB	Missing files	
FGT_VIVI04_KVIVI-V3-BUIIdU/18-FORTINET.OUT.KVM.qcow.	100 5 VD	Friend on CNIS2 VAA (CNIS2 VAA)	
EntiGate version 5.2.5	22 5 MD	Missing files	
EGT VM64 KVM-v5-build0701-EORTINET out hom acow	2 32 3 MB	Missing	
empty306.gcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
FortiGate version custom	191.8 MB	Ready to install	
FortiGate version customv2	192.5 KB	Missing files	
FGT_VM64_KVM-v5-build1653-FORTINET.out.kvm.gcow	2 0.0 B	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	

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."

🖑 Open							>	<
← → • ↑	⊁ This	PC > (F:) WARMI	FILES > Images > GNS3 >	Fortigate > Schoolv7		Ö D Sear		
Organize 🕶 Nev	/ folder						10 + 🖬 👔	
🖈 Quick access		Name	<u>^</u>	Date modified	Туре	Size		
Deskton		empty30G.qc	:ow2	2022-04-26 11:30 PM	QCOW2 File	193 KB		
Jownloads	+	FGT_VM64_K	VM-v7.0.3-build0237-FORTI	2021-12-10 9:55 PM	QCOW2 File	196,160 KB		
Documents	*							
Pictures	*							
💻 This PC								
📥 (C:) OS								
COLDFILE	5							
E:) HOTFILES								
👝 (F:) WARMFILE	S							
👝 (G:) HOTTERFIL	ES							
Retwork								
	File nar	me: empty30G.qcd	ow2			All Files (*) ~	
						Oper	Cancel	

Figure A.18: Import empty30G.qcow2 file

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

		Status	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version 5.2.13	37.2 MB	Missing files	
FGT_VM64_KVM-v5-build0762-FORTINET.out.kvm.qc	ow2 37.0 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version 5.2.12	36.8 MB	Missing files	
FGT_VM64_KVM-v5-build0760-FORTINET.out.kvm.qc	ow2 36.6 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version 5.2.11	33.6 MB	Missing files	
FGT_VM64_KVM-v5-build0754-FORTINET.out.kvm.qc	ow2 33.4 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version 5.2.10	33.4 MB	Missing files	
FGT_VM64_KVM-v5-build0742-FORTINET.out.kvm.qc	ow2 33.2 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version 5.2.9	33.2 MB	Missing files	
FGT_VM64_KVM-v5-build0736-FORTINET.out.kvm.qc	ow2 33.0 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version 5.2.8	33.1 MB	Missing files	
FGT_VM64_KVM-v5-build0727-FORTINET.out.kvm.qc	ow2 32.9 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version 5.2.7	33.0 MB	Missing files	
FGT_VM64_KVM-v5-build0718-FORTINET.out.kvm.qc	ow2 32.8 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version 5.2.5	32.5 MB	Missing files	
FGT_VM64_KVM-v5-build0701-FORTINET.out.kvm.qc	ow2 32.3 MB	Missing	
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)	
rtiGate version custom	191.8 MB	Ready to install	

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."

Install FortiGate appliance			?	1
age Please read the following instructions in order to use your new appliance.				
The template will be available in the firewall category.				
Default username is admin, no password is set.				
		X		

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.

General setting	IS HDD	CD/DVD	Network	Advanced	Usage		- 10 M	
Name:	PaloAlto-1							
RAM:	4096 MB							4
vCPUs:	2							
Qemu binary:	/bin/qemu-s	ystem-x86_6	i4 (v4.2.1)					
Boot priority:	HDD							
On close:	Power off th	ne VM						
Console type:	telnet				+ Auto	start console		

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.

🚯 New template	? ×
New template Please select how you want to create a new template	
Install an appliance from the GNS3 server (recommended) Install an appliance flo (one 2- extension)	
Manually create a new template	
	< Back Next > Cancel

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."

New template				?	
ppliances from ser Select one or more	ver appliances to in	stall. Update will request the server t	o download appliances from our online registry.		
ebterm					
ppliance name 🔺	Emulator	Vendor			
Firewalls Guests					
webterm Routers Switches	Docker	webterm			
			in the first state of the	 C. Com	

Figure A.28: Search for "webterm"

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

Install webterm appliance		?	
rver Please choose a server type to install the appliance. The grayed out server types are not supported or configured.		-	
ierver type			
O Install the appliance on a remote server			
Install the appliance on the GNS3 VM (recommended)			
Install the appliance on your local computer			

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

5. On the next screen, click "Finish."

Install webterm appliance.	?
sage Please read the following instructions in order to use your new appliance.	
The template will be available in the guest category.	
The froot directory is persistent.	
	Anniance info < Back Finish Cance

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:

webterm-1 interfaces			?	3
# This is a sample network config uncomment lines to configure the network #				
State confin for eth0 uto eth0 ace eth0 inet state: address 10.0.0.2 netmask 255.255.0				
gateway 10.0.0.1 up echo nameserver 8.8.8.8 > /etc/resolv.conf DHCP contig tor eth0 auto eth0 iface eth0 inet dhcp				
	Refresh	Save	Can	cel

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."

😢 New template	? ×
New template Please select how you want to create a new template	
Install an appliance from the GNS3 server (recommended)	
O Import an appliance file (.gns3a extension)	
O Manually create a new template	
	< Back Next > Cancel

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.

New template				?	
Appliances from server Select one or more appliances to in	tall. Update will request the server to downloa	ad appliances from our online registry.			
kali					
Appliance name	Vendor				
• Guests	10 m m m				
Kali Linux Olemu	Kali Linux Kali Linux				
Routers Switches	Nall Linux				

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."

308 Hamid Talebi

Install webterm appliance	?
ver lease choose a server type to install the appliance. The grayed out server types are not supported or configured.	
erver type	
O Install the appliance on a remote server	
Install the appliance on the GNS3 VM (recommended)	
Install the appliance on your local computer	

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

5. "Next" again:

👶 Install Kali Li	nux appliance				?	×
Qemu settings Please choose	the gemu binary that will be used to run this appliance.					
Qemu binary:	/usr/bin/qemu-system-x86_64 (v4.2.1)				_	•
-		Appliance info	< <u>B</u> ack	Next >	Cance	2

Figure A.41: Qemu binary

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

Innlin	ince version and files	Cize	Statur		-
tppna	Listen and thes	312E	Deskuta install		-
	li Linux version 2021.1	3.4 GD	Would say missing		
* K	all Linux Version 2019.3	2.9 GB	Ready to Install		
	kall-linux-2019:5-amdo4.iso	20 GB	Found on GNS2 VM (GNS2 VM)		
- 1	Linux version 2010.2	2.2 GP	Mireing files		
K	In Linux version 2019.2	3.2 GB	Missing mes		
	kall-linux-2019.2-amd04.Iso	22 1 MD	Friend an CNC2 VM (CNC2 VM)		
- K	Kan-Innux-persistence-igb.qcow2	35.1 MB	Pound on Glubs VIVI (GIVSS VIVI)		
K	In Linux Version 2019.2 (MATE)	21 CP	Missing mes		
	kall-linux-mate-2019.2-amd04.iso	321 140	Trusting		
	kall-linux-persistence-1gb.qcow2	33.1 MB	Found on GINDS VIVI (GINDS VIVI)		
K	Linux version 2019.1a	5.5 GB	IVIISSING TILES		
	kall-linux-2019.1a-amdo4.iso	5.2 GB	IVIISSING		
	kall-linux-persistence-Igb.qcow2	33.1 MB	Found on GNSS VM (GNSS VM)		
K	all Linux version 2018.4	3.0 GB	Missing files		
	kalı-linux-2018.4-amd64.iso	2.9 GB	Missing		
	kalı-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)		
K	ali Linux version 2018.3a	3.0 GB	Missing files		1
	kalı-linux-2018.3a-amd64.iso	3.0 GB	Missing		
1	kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)		
K	ali Linux version 2018.1	2.9 GB	Missing files		
	kali-linux-2018.1-amd64.iso	2.8 GB	Missing		
	kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)		
K	ali Linux version 2017.3	2.7 GB	Missing files		
	kali-linux-2017.3-amd64.iso	2.7 GB	Missing		
	kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)		
· K	ali Linux version 2017.2	2.8 GB	Missing files		18

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

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

🖑 Open					×
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This	s PC → (F:) WARMFILES → Images → Linux			Ö Search L	inut
Organize 🔻 New folde	r.				18 × 🔳 📀
 ✓ Quick access ✓ Desktop ✓ Downloads ✓ Downloads ✓ Documents ✓ Pictures ✓ This PC ✓ (C:) OS (C:) OS 	Name CentOS-7-x80_04-Winimai-2009.is0 CentOS-7-x86_64-NetInstall-2009.is0 CentOS-Stream-8-x86_64-20210215-dvd1 debian-10.7.0-amd64-netinst.is0 debian-10.7.0-amd64-xfce-CD-1.is0 install-amd64-minimal-20201227T214503 install-amd64-minimal-20201227T214503 install-amd64-minimal-202101010T214504 install-amd64-minimal-20210505T214503 kali-finux-2019.3-amd64.iso Kali-finux-2019.3-amd64.iso	Date modified 2021-01-03 03.44 PM 2021-02-23 9:44 AM 2021-02-23 9:44 AM 2021-01-14 12:51 PM 2021-01-14 2:40 PM 2021-01-02 2:07 PM 2021-01-02 2:07 PM 2021-01-12 10:48 PM 2021-05-09 9:17 AM 2022-03-29 7:02 PM	Type visc image rile Disc Image File Disc Image File	Size 990,332 No 588,800 KB 9,628,672 KB 344,064 KB 710,656 KB 424,960 KB 425,984 KB 429,056 KB 2,966,540 KB	
(E) HOTFILES (F:) WARMFILES (G:) HOTTERFILES (G:) HOTTERFILES	 kali-linux-2021.1-installer-amd64.iso kali-linux-2021.1-installer-netinst-amd64 linuxmint-18.2-xfce-64bit.iso linuxmint-20.1-cinnamon-64bit.iso linuxmint-20.3-xfce-64bit.iso Rocky-8.5-x86_64-minimal.iso SkillsVM-0.vmdk 	2021-04-21 9:46 AM 2021-05-21 8:53 PM 2021-09-25 9:59 PM 2021-01-12 10:49 PM 2022-02-28 8:19 PM 2022-03-22 10:36 AM 2022-04-11 11:18 PM	Disc Image File Disc Image File Disc Image File Disc Image File Disc Image File Disc Image File Virtual Machine Di	4,191,264 KB 388,096 KB 1,609,344 KB 1,987,136 KB 2,076,704 KB 2,076,672 KB 1 KB	ļ
File na	me: kali-linux-2019.3-amd64.iso			→ All Files (*) Open	Cancel .:i

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

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

Appliance version and files	Size	Status	
 Kali Linux version 2021.1 Kali Linux version 2019.3 kali-linux-persistence-1gb.qcow2 Kali Linux version 2019.2 kali-linux-persistence-1gb.qcow2 Kali Linux version 2019.2 (MATE) kali-linux-persistence-1gb.qcow2 Kali Linux version 2019.2 (MATE) kali-linux-persistence-1gb.qcow2 Kali Linux version 2019.1a kali-linux-persistence-1gb.qcow2 Kali Linux version 2019.1a kali-linux-2019.1a-amd64.iso kali-linux-persistence-1gb.qcow2 Kali Linux version 2018.4 kali-linux-2018.4-amd64.iso kali-linux-persistence-1gb.qcow2 Kali Linux version 2018.3a kali-linux-persistence-1gb.qcow2 Kali Linux version 2018.1 kali-linux-persistence-1gb.qcow2 Kali Linux version 2018.1 kali-linux-persistence-1gb.qcow2 Kali Linux version 2018.1 kali-linux-persistence-1gb.qcow2 Kali Linux version 2017.3 kali-linux-persistence-1gb.qcow2 	3.4 GB 2.9 GB 3.3 1 MB 3.2 GB 3.1 GB 3.1 GB 3.1 GB 3.1 GB 3.1 GB 3.3 1 MB 3.3 GB 3.2 GB 3.3 1 MB 3.0 GB 3.3 1 MB 2.9 GB 3.1 MB 3.1 MB 3.0 GB 3.1 MB 3.1 MB 3	Keady to install Missing files Missing files Missing files Missing files Missing files Missing Please wait Please wait <th></th>	
I I''' Download	20.00	Allow rustom files	ion Refresh

Figure A.44: Load the image

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

nce version and files	Size	Catalua				
Ellevenetare 2024 4		Status				
IL LINUX VERSION 2021.1	3.4 GB	Ready to install				
li Linux version 2019.3	2.9 GB	Ready to install				
kali-linux-2019.3-amd64.iso	2.8 GB	Found on GNS3 VM (GNS3 VM)				
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)				
li Linux version 2019.2	3.2 GB	Missing files				
kali-linux-2019.2-amd64.iso	3.1 GB	Missing				
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)				
li Linux version 2019.2 (MATE)	3.1 GB	Missing files				
kali-linux-mate-2019.2-amd64.iso	3.1 GB	Missing				
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)				
li Linux version 2019.1a	3,3 GB	Missing files				
kali-linux-2019.1a-amd64.iso	3.2 GB	Missing				
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)				
li Linux version 2018.4	3.0 GB	Missing files				
kali-linux-2018.4-amd64.iso	2.9 GB	Missing				
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)				
li Linux version 2018.3a	3.0 GB	Missing files				
kali-linux-2018.3a-amd64.iso	3.0 GB	Missing				
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)				
li Linux version 2018.1	2.9 GB	Missing files				
kali-linux-2018.1-amd64.iso	2.8 GB	Missing				
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)				
li Linux version 2017.3	2.7 GB	Missing files				
kali-linux-2017.3-amd64.iso	2.7 GB	Missing				
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)				
li Linux version 2017.2	2.8 GB	Missing files				
	kali-linux-2019.3-amd64.iso kali-linux-persistence-1gb.qcow2 i Linux version 2019.2 kali-linux-persistence-1gb.qcow2 i Linux version 2019.2 (MATE) kali-linux-persistence-1gb.qcow2 i Linux version 2019.2 (MATE) kali-linux-persistence-1gb.qcow2 i Linux version 2019.1a kali-linux-2019.1a-amd64.iso kali-linux-2019.1a-amd64.iso kali-linux-2018.4-amd64.iso kali-linux-2018.4-amd64.iso kali-linux-2018.3a-amd64.iso kali-linux-2018.3a-amd64.iso kali-linux-2018.1-amd64.iso kali-linux-2018.1-amd64.iso kali-linux-2018.1-amd64.iso kali-linux-2018.1-amd64.iso kali-linux-2017.3-amd64.iso kali-linux-2017.3-amd64.iso kali-linux-2017.3-amd64.iso kali-linux-2017.3-amd64.iso kali-linux-2017.3-amd64.iso kali-linux-2017.3-amd64.iso kali-linux-2017.3-amd64.iso	kali-linux-2019.3-amd64.iso 2.8 GB kali-linux-persistence-1gb,qcow2 33.1 MB i Linux version 2019.2 32.6 B kali-linux-2019.2-amd64.iso 31.6 B kali-linux-persistence-1gb,qcow2 33.1 MB i Linux version 2019.2 (MATE) 31.6 B kali-linux-persistence-1gb,qcow2 33.1 MB i Linux version 2019.2 (MATE) 31.6 B kali-linux-persistence-1gb,qcow2 33.1 MB i Linux version 2019.1 a 3.3 GB kali-linux-2019.1-a-amd64.iso 3.2 GB kali-linux-2019.1a-amd64.iso 3.2 GB kali-linux-2018.1-a-amd64.iso 2.9 GB kali-linux-2018.4-amd64.iso 2.9 GB kali-linux-2018.3-amd64.iso 3.0 GB <	kali-linux-2019.3-amd64.iso2.8 GBFound on GNS3 VM (GNS3 VM)kali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.23.2 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)3.1 GBMissingkali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)3.1 GBMissingkali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)3.3 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.43.3 GBMissing fileskali-linux-2019.1a3.3 GBMissing fileskali-linux-2019.1a3.3 GBMissing fileskali-linux-2018.43.0 GBMissing fileskali-linux-2018.43.0 GBMissing fileskali-linux-2018.3a3.0 GBMissingkali-linux-2018.3a3.0 GBMissingkali-linux-2018.12.9 GBMissingkali-linux-2018.12.9 GBMissingkali-linux-2018.12.9 GBMissingkali-linux-2018.12.9 GBMissingkali-linux-2018.12.9 GBMissingkali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2017.32.7 GBMissingkali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux-p	kali-linux-2019.3-amd64.iso2.8 GBFound on GNS3 VM (GNS3 VM)kali-linux-persistence-1gb.qcow233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.232. GBMissing fileskali-linux-2019.2-amd64.iso31. GBMissingkali-linux-persistence-1gb.qcow233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)31. GBMissingkali-linux-persistence-1gb.qcow233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)31. GBMissingkali-linux-persistence-1gb.qcow233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.13.3 GBMissing fileskali-linux-2019.1-a-amd64.iso3.2 GBMissing fileskali-linux-2018.1-a-amd64.iso3.2 GBMissing fileskali-linux-2018.4-amd64.iso2.9 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.1-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMissing fileskali-linux-2018.3-a-amd64.iso3.0 GBMi	kali-linux-2019.3-amd64.iso2.8 GBFound on GNS3 VM (GNS3 VM)kali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)kali-linux-2019.2-amd64.iso3.1 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)3.1 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)3.1 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)3.3 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.1a3.3 GBMissing fileskali-linux-2019.1a - amd64.iso3.2 GBMissingkali-linux-2018.4- amd64.iso3.0 GBMissing fileskali-linux-2018.4- amd64.iso3.0 GBMissing fileskali-linux-2018.3a - amd64.iso3.0 GBMissingkali-linux-2018.3a - amd64.iso3.0 GBMissingkali-linux-2018.1- amd64.iso3.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2018.12.9 GBMissingkali-linux-2018.1- amd64.iso2.8 GBMissingkali-linux-2018.1- amd64.iso2.8 GBMissingkali-linux-2018.1- amd64.iso2.8 GBMissingkali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)Linux version 2017.32.7 GBMissing fileskali-linux-persistence-1gb.qcov2	kali-linux-2019.3-amd64.iso2.8 GBFound on GNS3 VM (GNS3 VM)kali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.23.2 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE)3.1 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)kali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)kali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.2 (MATE).3 GBMissing fileskali-linux-persistence-1gb.qcov233.1 MBFound on GNS3 VM (GNS3 VM)i Linux version 2019.1a.3 GBMissing fileskali-linux-2019.1a-amd64.iso.2 GBMissing fileskali-linux-2018.1-amd64.iso.2 GBMissing fileskali-linux-2018.4-amd64.iso.3 GBMissing fileskali-linux-2018.3a-amd64.iso.3 GBMissing fileskali-linux-2018.3a-amd64.iso.3 GBMissing fileskali-linux-2018.1-amd64.iso.3 GBMissing fileskali-linux-2018.1-amd64.iso.3 GBMissing fileskali-linux-2018.1-amd64.iso.3 GBMissing fileskali-linux-2018.1-amd64.iso.3 GBMissing fileskali-linux-2018.1-amd64.iso.3 GBMissing fileskali-linux-2018.1-amd64.iso.3 GBMissing fileskali-linux-persistence-1gb.qcov2.31.1 MBFound on GNS3 VM (GNS3 VM)I Linux vers

Figure A.45: Ready to install Kali 2019.3

10. Then click "Finish."

Install Kali Linux appliance	?
age Please read the following instructions in order to use your new appliance.	
The template will be available in the guest category. Default password is toor Enable persistence by selecting boot option 'Live USB Persistence'	

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.

Security devices	Br be			
Filler				
FortiGate 6.0.0				
FortiGate 5.0.1				
FortiGate 6.4.0				
FortiGate 6.4.7				
FortiGate 6.4.8				
FortiGate 7.0.2				
FortiGate 7.0.3				
Palo Alto				
and the second second				
		- /		
		/		
	/			
	1			
	/			
1				
+New template	41			
Console				

Figure A.47: Create a new template

We want to install an appliance from the GNS3 server.

New template	? >
New template Please select how you want to create a new template	
Install an appliance from the GNS3 server (recommended)	
Import an appliance file (.gns3a extension)	
Manually create a new template	
	and hits
	< Back Next > Cancel

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

Look up "WordPress," then click "Install."

Appliances from server	stall. Undate will request the service	to developed appliances from our college society	
Select one or more appliances to in	stail. Update will request the serve	r to download appliances from our online registry,	
wordpress			
Appliance name A Emulator Firewalls	Vendor		
WordPress Docker	Tueskay Linus		
Routers Switches	amay enter		
			_

Figure A.49: Search for "WordPress"

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

🗮 Kali Linux CLI	
NAT	
pl Palo Alto	
VPCS	
医 webterm	
Windows Server 2012 R2	
🖼 WordPress	
Xav Client 2	
	-

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!



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.

General						
Name:	Switch 1					
Console type:	none					-
Settings			Ports			
	1		Port	+ VLAN	Туре	EtherType
Port:	8	*	0	1	access	
	1		1	1	access	
VLAN:	1	-	2	1	access	
	1		3	1	access	
Type:	access	*	4	1	access	
	A Definition		6	1	access	
QinQ EtherTyp	e: 0x8100	+	7	1	access	
Ad	d	Delete	4) b

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

General						
Name:	Switch 1					
Console type:	none					-
Settings			Ports			
	12	101	Port	VLAN	Туре	EtherType
Port:	1	*	0	1	access	
	1		1	1	access	
VLAN:	1	-	2	1	access	
			3	1	access	
Type:	access	*	4	1	access	
			5	4	access	
QinQ EtherTyp	e: 0×8100	+	7	1	access	
Ad	e 11	Delete				•

Figure A.54: Switch port configuration

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

General						
Name:	Switch 1					
Console type:	none					-
Settings			Ports			
	1		Port	+ VLAN	Туре	EtherType
Port:	/	¥	0	1	access	
	1		1	1	access	
VLAN:	1	+	2	1	access	
	Da.V.		3	1	access	
Type:	dot1q	Ψ.	4	1	access	
	Televis.		6	1	access	
QinQ EtherTyp	e: 0x8100	*	7	1	access	
Ade	1 I	Delete	4			•

Figure A.55: Switch port configuration

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

General							
Name:	Switch1						
Console type:	none						•
Settings			Ports				
			Port	+ VLAN	Туре	EtherType	
Port:	0	Ŧ	0	1	access		
10.001	14		1	1	access		
VLAN:	1	*	2	1	access		
	La de		3	1	access		
Type:	dot1q	*	4	1	access		
	- Internet		5	1	access		
QinQ EtherTyp	e: 0x8100	*	0	1	access dot1a		
			1		uorig		
		p.L.c.	4				Þ.

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 <u>BCcampus</u> 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

<u>Hamid Talebi</u> 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 <u>Report an Error</u> form.

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