Palo Alto Firewall

Palo Alto Firewall

Practical Guidance and Hands-On Labs

Hamid Talebi and Xavier Cawley

BCCAMPUS VICTORIA, B.C.



Palo Alto Firewall by Hamid Talebi, Xavier Cawley is licensed under a <u>Creative Commons Attribution 4.0 International License</u>, except where otherwise noted.

© 2023 Hamid Talebi, Xavier Cawley

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:

Palo Alto Firewall: Practical Guidance and Hands-On Labs by Hamid Talebi and Xavier Cawley is licensed under a <u>CC BY</u> <u>4.0 licence</u>.

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., & Cawley, X. (2023). *Palo Alto firewall: Practical guidance and hands-on labs*. BCcampus. https://opentextbc.ca/paloalto/

Cover image attribution:

"personal firewall" by jiricek72 has been dedicated to the public domain.

Ebook ISBN: 978-1-77420-231-9

Print ISBN: 978-1-77420-230-2

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
Dedication	XV
A Practical Introduction	1
Chapter 1. Basics	
1.1 GNS3 and Palo Alto	5
1.2 DORA the DHCP Provider	25
1.3 SNAT	47
1.4 DNAT	55
Chapter 2. Security Tuneup	
2.1 Work with Applications	71
2.2 Deal with Bad Actors	77
2.3 Block Files and Viruses	111
Chapter 3. Advanced Networking	
3.1 Captive Portal	129
3.2 Remote Access VPN	155
3.3 Site-to-Site VPN	183
Chapter 4. Cloud Technologies	
4.1 IPsec VPN between Palo Alto on Premise and Microsoft Azure	197
4.2 Deploy Palo Alto to Azure	221
4.3 Site-to-Site VPN between Palo Alto on Premise and Palo Alto in the Azure	235
Capstone Project	
Capstone Project	251

Appendix: GNS3 Basics	255
Acknowledgements	285
About the Authors	287
Versioning History	289

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 textbooks 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 text has a linked table of contents and uses headings in each chapter to make navigation easy.
- Accessible images. All images in this text 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
Multimedia	Videos have captions of all speech content and relevant non-speech content that has been edited by a human for accuracy.	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 the Palo Alto firewall software. 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 textbooks more accessible. If you have problems accessing this textbook, please contact us to let us know so we can fix the issue.

Please include the following information:

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

You can contact us one of the following ways:

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

This statement was last updated on November 29, 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 Palo Alto Firewall

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: <u>*Palo Alto Firewall:*</u> <u>*Practical Guidance and Hands-On Labs.*</u> 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	Required apps Accessibility Features	
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

Palo Alto Firewall: Practical Guidance and Hands-On Labs by Hamid Talebi and Xavier Cawley 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>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>Palo Alto Firewall: Practical Guidance and</u> <u>Hands-On Labs Style Sheet [Word file]</u> xiv Palo Alto Firewall

Dedication

This book is dedicated to to our loving parents.

xvi Palo Alto Firewall

A Practical Introduction

The Fundamental Theory

Palo Alto is a next-generation firewall. This means that it uses more advanced techniques to detect threats compared to a traditional firewall. Where a more traditional firewall would inspect source and destination IP addresses and ports, a next generation firewall would detect an application, user, or piece of content. From there we can choose to either allow, block, drop or reset the connection.

Chapter Navigation

Every lab will contain a learning outcome section on the top. Here is an example:

Learning Objectives	
Learn how to navigate this bookOpen up GNS3	

These will contain what the current lab is trying to teach.

A topology of how the lab will look like, will be displayed after the learning outcomes. Here is an example:



Figure E.1: An example scenario

A Practical Introduction

What this book aims to accomplish is a practical understanding of the usage and functionality of Palo Alto firewalls. Learn by doing will be a strong driving force in the coming labs and examples in this book, and I encourage you to try and extend these labs and have fun with them.

Chapter 1. Basics

4 Palo Alto Firewall

1.1 GNS3 and Palo Alto

Learning Objectives

- Configure a static IP for the management port on the firewall
- Change general settings of the firewall using the web interface

Scenario: In this lab, we're only going to start with the basics. Connecting to and configuring basic settings on Palo Alto. There will be a little console usage, but don't fret. The rest of these will involve some sort of GUI based option



Figure 1.1: Main Scenario

Table 1.1: Addressing Table

Device	Configuration
PaloAlto-1	Management: 192.168.0.1/24
WebTerm1-Management	eth0: 192.168.0.2/24

Console into the Palo Alto Device

Make sure to start all your devices, then double click the Palo Alto device. You should see a console window pop up. We need to wait till the prompt changes to "PA-VM". Otherwise, we cannot login.



Figure 1.2: No Login

After about 15 mins, hit enter, and the prompt should change. Login with the following credentials: **Username:** admin **Password:** admin

It will prompt you to change your password. Once you're finished changing your password, you will see the prompt change to this:

```
PaloAlto-1 - PuTTY
                                                                                                  ×
                                                                                             -
        RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16 bytes 1428 (1.3 KiB)
                                                                                                           ~
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Masterd started successfully
vm login:
PA-VM login: admin
Password:
Cannot connect to management server
Server timeout : Session timed out
Forced session timeout from management server
PA-VM login: admin
Password:
Last login: Tue Apr 26 18:34:08 on ttyS0
Enter old password :
Enter new password :
Confirm password
Password changed
Number of failed attempts since last successful login: 0
Warning: Your device is still configured with the default admin account credentials. Please change yo
ur password pristo deployment.
admin@PA-VM>
```

Figure 1.3: Firewall General mode

Configure a Static IP on the Palo Alto Device

I promise you that this is one of the only times we will be interfacing with the command line. But this is necessary for setting up a static IP. Type these commands into the now open console:

```
    configure
    set deviceconfig system type static
    set deviceconfig system ip-address 192.168.0.1 netmask
    255.255.255.0
    commit
```

Line 1: Gets you into configuration mode.

Line 2: Configuration mode command to set the management interface to a static address.

Line 3: Sets IP of the management interface.

Line 4: Every time you make any change in Palo Alto, you must commit the changes for it to take effect.

It should look like this if all commands were successful:



Figure 1.4: Set a static IP address

Access the Web Interface from Webterm



Double click on the webterm device. A Firefox window should immediately pop up:

Figure 1.5: WebTerm Firefox browser

On the top address bar, type in "<u>https://192.168.0.1</u>" (without quotes) then hit enter.

After typing that in, you should see a block page:



Figure 1.6: Type IP address of Palo Alto

To get past this, click advanced, then click "Accept the Risk".



Figure 1.7: Past of security warning

Now that we're past the scary-looking warning screen, type in the credentials to the user: **admin**. The password should be the **password** you set after initially logging in through the command line.



Figure 1.8: Enter credentials

Now, we're in the web interface for the Palo Alto device!



Figure 1.9: First page of Palo Alto

Explore the Web Interface

BruhloAlto - Mozilla Firefo> + 🦔 BruhloAlto × ... ☑ ☆ <) → C û III\ 🗊 🔮 (i) 🐔 https://192.168.0.1/?#device::vsys1::device/setup DPA-VM D - E C NETWORK DEVICE GO Setup Management Operations Services Interfaces Telemetry Content-ID WildFire Session H5M ACE DLP 😬 High Availability Config Audit General Settings Panorama Settings Password Profiles Hostname BruhloAlto Panorama Servers Administrators Enable pushing device monitoring data to Panorama Domain Admin Roles Login Banner Authentication Profile Receive Timeout for Connection Lo Panorama (sec) Force Admins to Acknowledge Login Authentication Sequence Banner B User Identification Send Timeout for Connection to Panorama SSL/TLS Service Profile a Data Redistribution (sec) Time Zone US/Pacific Retry Count for SSL Send to Panorama Device Quarantine Locale en W Information Sources Enable automated commit recovery Time Tue Apr 26 18:38:56 PDT 1 Troubleshooting Number of attempts to check for Panorama connectivity on automated commit recovery 2022 🗸 🧔 Certificate Management Geo Location Interval between retries (sec) on automated Certificates Automatically Acquire Commit Lock E Certificate Profile Certificate Expiration Check OCSP Responder Use Hypervisor Assigned MAC Addresses 🗾 SCEP GTP Security 🔁 SSL Decryption Exclusio SCTP Security Secure Communication Settings 6 SSH Service Profile Response Pages SCTP Security Certificate Type Log Settings Advanced Routing Panorama Communication Server Profiles PAN-DB Communication Tunnel Acceleration ⊠ | ≸∃ Tasks | Language paloalto () Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share 🖲 BruhloAlto - Mozilla Firefox 01:38 IWM

Ξ

×

Let's focus on what we'll actually be used as these labs progress.

Figure 1.10: Device Settings

In device settings, we can change the hostname, create users, generate certs, etc. The bottom line is that it is used for general system administration. We will be delving more into this as the chapters progress.

BruhloAlto - Mozilia Fi BruhloAlto	× +		_	-	_		_				
€ → ♂ û	🛈 🐔 https://192.	⊠ ☆	III\ 🗊	e =							
🚺 PA-VM	DASHBOARD AC	C MONITOR	POLICIES	DBJECTS	NETWORK	DEVICE	」 1[™]	₽ª × Q			
-								G ()			
Zones	Ethernet VLAN	Loopback Tunne	SD-WAN								
	Q	Q Bitems → X									
Virtual Wires Virtual Routers PSec Tunnels	INTERFACE	INTERFACE TYPE	MANAGEMENT	LINK	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUA			
GRE Tunnels	@ ethemet1/1				none	none	Untagged	none			
芝 DHCP 響 DNS Provy	@ ethernet1/2				none	none	Untagged	none			
GlobalProtect	📾 ethernet1/3				none	none	Untagged	none			
Rortals	ethernet1/4				none	none	Untagged	none			
C MDM	ethernet1/5				none	none	Untagged	none			
Clientless Apps	ethernet1/6				none	none	Untagged	none			
Clientless App Groups	ethernet1/7				none	rone	Untagged	none			
	methemet1/8			m	none	none	Untagged	none			
 GlobalProtect IPSec Cry GlobalProtect IPSec Cry IKE Gateways IPSec Crypto IKE Crypto 											
Monitor	-		_								
ag intenace Mgnit	(+) Add Subinterrace	Delete Delete Delete	CSV								
admin Logout Last Login Tim	e: 04/26/2022 18:35:01 9	Session Expire Time: 0	5/26/2022 18:38:29			🖾 🏂 Tasks La	inguagé 🛷	paloalto			
⑦ Firefox automatically set	ends some data to Mo:	zilla so that we ca	n improve your e	xperienc	e.	Choos	se What I Sha	are 🗙			
	Alto Mozilla Firofo	NY.						01.			

Figure 1.11: Network Interfaces Settings

BruhloAlto	×	+									
-) → C @	0) 🔒 https	://192.168	3.0.1/?#objects	::vsys1::obj	ects/addresses		… ⊠ ☆	lır		5
PA-VM	DA	HBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE	≦ Canimit +	1 60 0	ेन् ५ (
Addresses	Q									0 item:	G I
Address Groups Regions Pynamic User Groups Dynamic User Groups Application Groups Application Filters Services Service Groups Tags Devices GlobalProtect HIP Profiles Bio Data Patterns Data Patterns Syyware Wulnerability Wulnerability		NAME		LOCATION		ТҮРЕ	ADDRES	5	TAGS		
Ulnerability Protection	Ð.	Add 😑 Dale	te SClo	ne DF/CSV							
Interio Linnout Last Lonio Time	e: 04/2	6/2022 18:3		on Expire Time: O	5/26/2022 18	:38:29			Tasks Languag	🛛 🥠 pa	loal
intin i togotici case togin nini											-

In network settings, we can change interface IP addresses, create tunnels, and setup routing.

Figure 1.12: Objects Settings

We won't be using the objects tab very much, however, it is important to know about it. Here, we can create pre-defined address objects, define ports, and create security policy templates.

BruhloAlto - Mozilla F	irefox	1								- 8
	×	+) <u> https://1</u>	92.168.0.1/?#po	licies::vsys1::po	olicies/securit	y-rulebase	ເ ☆	lii		5 ≡
🚺 PA-VM	DAS	HBOARD	ACC MONITO	DR POLICIES	OBJECT	S NETWORK	DEVICE	≜ Conimit +	🔁 🗉	∄• Q
									2 items	GO
→ NAT							Source			210
& QoS		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	
Decryption	1	intrazone-defaul	b none	intrazone	any	any	any	any	(intraz	one)
Tunnel Inspection	2	interzone-defaul	8 none:	interzone	any	anv	any	any	any	
DoS Protection DoS Protection Policy Optimizer Rules Without App Controls Unused Apps Rule Usage Wunused in 30 days Wunused in 90 days Wunused	0 0 0 0					*				
Object : Addresses -	+ + A	Add 🕄 Delete	🕞 Clorie 🔞 Ove	rride 💿 Revert 4	🕑 Enable 🛞	Disable Move Y	DF/CSV	ghlight Unused F	lules	»
admin Logout Last Login Tim	ne: 04/26	6/2022 18:35:01	Session Expire Ti	me: 05/26/2022 1	8:38:29]			Tasks Läriguag	e 🥠 pa	loalto
③ Firefox automatically s	ends s	ome data to I	Mozilla so that w	e can improve ;	our experier/	nce.		<u>C</u> hoose Wh	hat I Share	×
WM _ 💻 🍯 Bruhia	Alto -	- Mozilla Fire	efox							01:4

Figure 1.13: Policy Settings

The policies tab is arguably the most important tab of the firewall. Here we will configure security policies and define NAT rules. An important thing to note is these pre-existing security policies. Everything within a zone is allowed, whereas a zone to another zone is not allowed.

Change the Hostname of Palo Alto

Head over to the device tab, and click the cog icon to the right of device settings.



Figure 1.14: Changing hostname

Change the hostname to anything but PA-VM. I will change mine to "BruhloAlto".



After changing the hostname to anything you desire, click on **OK** at the bottom right of the screen.

Figure 1.15: General Settings

After any change in Palo Alto, you will have to commit the changes. When you make changes in Palo Alto, it is put into what we call a "**candidate configuration**." This means that changes do not take effect immediately. After we change some settings, we need to press the commit button on the top right.



Figure 1.16: Commit Configuration

Pressing commit will push the candidate configuration to the running configuration. This is helpful because the Palo Alto device is smart enough to tell you if a configuration won't work without affecting your active network settings. Let's commit these changes by clicking commit again.



Figure 1.17: Commit all changes


If all is well, after a while you should see something similar to this. It means everything worked!

Figure 1.18: Configuration committed successfully

Verify the Changes

Refresh the page by pressing the F5 key (or clicking on the refresh button) on the webterm web browser. If the hostname changed, the tab will change to the hostname you set.

x11 - TightVNC Viewer												-	
	Ctrl	At h	QQ										
🕽 BruhloAlto – Mozilla Fir	refox	κ.											- 6
🏇 BruhloAlto	×	+											
< → C @	G	D 🔒 http	s://192.16	38.0.1/?#ne	twork::vsy	slanetwork	c/zonies		•••	· ⊡ ☆		III\ 🗊	¢
VIUNIBARIO X T C O O DASHEGARD ACC MONITOR POLICES OBJECTS NETWORK DEVACE OBJECT NORK DASHEGARD ACC MONITOR POLICES OBJECTS NETWORK DEVACE OBJECTS NETWORK DEVACE OBJECTS NETWORK DEVACE OBJECTS NETWORK OBJECT DEVACE OBJECT NAME TVYE SYSTEMS PROFILE PROFILE PROFILE NALLED NETWOR Object DEVACE Object Object DEVACE DEVACE DEVACE Object DEVACE DEVACE DEVA													
													90
Tones	20	-				T	1	T				OR	eurs $ ightarrow$
NANK VLANK									User-ID	-	_	Device-ID	
Virtual Wires		NAME	TYPE	/ VIRTUAL SYSTEMS	PROTEC PROFILE	PACKET BUFFER PROTEC_	LOG SETTING	ENABLED	INCLUD	EXCLUD	ENABLED	INCLUD	EXCLU
2 IPSec Tunnels													
GRE Tunnels													
CAS Driver							*						
GlobalProtect													
Portals													
Gateways													
MDM	4												
Clientless Apps													
Clientless App Groups													
👌 QoS													
2 LLDP													
Network Profiles													
GlobalProtect IPSec Ory													
# IRE Gateways													
IPSec Crypto #													
C IKE Crypto.													
Considera Advect													
III - TapAVIK Viewer													
			35.01 Ses	sion Expire Tir	ne: 05/26/2					⊠│注		110 110	paloalt
													ALC: NOTION
⑦ Firefox automatically se	ends s	some dat	a to Mozil	a so that we	e can impr	ove your e	xperience				Choose	What I Sh	arè :

Figure 1.19: Verify configuration

You can also see the changes being reflected on the console interface if you press enter.



Figure 1.20: Verify configuration in CLI

24 Chapter 1. Basics

1.2 DORA the DHCP Provider

Learning Objectives

- Set up a DHCP server on Palo Alto
- Set up zones
- Connect clients to the internet with Palo Alto

Scenario: In this lab, we are going to configure our friend DORA (Discover Offer Request Acknowledge) the hander of addresses. And we'll also be configuring internet access so that clients may finally browse their precious Internet with SNAT (Source Network Address Translation).

6	eth0)HCP Client	ethernet1/1 10.0.0.1/24	ethernet1/2 DHCP Client	nato
Clint		Inside	mänagement	ULSIDE
			192.168.0.1/24	
			eth0	
		-	192.100.0.2/24	



Device	Configuration
PaloAlto	management: 192.168.0.1/24 Ethernet1/1: 10.0.0.1/24 Ethernet1/2: DHCP
Client (WebTerm)	eth0: DHCP
Management (WebTerm)	eth0: 192.168.0.2/24

Table 1.2: Addressing Table

Table 1.3: Zone Configuration

Zones	Interfaces
Inside	Ethernet1/1
Outside	Ethernet1/2

Create Zones in the Palo Alto Web Interface

Under the network tab, click zones, then add on the bottom left of the screen.

🔒 BruhloAlto - Mozilla Fii	refox	6											-	8 >
4 BruhloAlto	×	+												
€ → ୯ ŵ	0) 💪 http:	s:// 192.16	8.0.1/?#ne	twork::vsy	sl:networ	k/zones		•••			III\ 🗊	۲	Ξ
🚺 PA-VM	DAS	HBOARD	ACC	MONITO	R PO	LICIES	OBJECTS	NETWOR	tk DE	VICE	∃.Gommit ~) IE	₽Ŧ,	a
													G	
Contentaces	Q											01	tems .	$\rightarrow \times$
Zanes	-		1						User-ID			Device-IP		
VLANS				11.000	-			-	Given its	1		LANTING IN		
Virtual Wires		NAME	туре	/ VIRTUAL SYSTEMS	PROTEC PROFILE	BUFFER PROTEC	LOG SETTING	ENABLED	INCLUD NETWO	EXCLUD NETWO	ENABLED	INCLUD_ NETWO_	EXC	LUD_ WO
GRE Tunnels GRE Tunnels GRE Tunnels GRE Tunnels														
DNS Proxy										*				
- GlobalProtect														
Portals														
Gateways														
MDM.	×													
Clientless Apps														
Clientless App Groups														
💑 QoS														
S LLDP														
V Retwork Profiles														
GlobalProtect IPSec Gry														
IKE Gateways														
PSec Crypto														
IKE Crypto =														
Monitor =		-												
e Interface Mgmt	€.	Add TOT De	ince 🔘 PD	F/CSV						-				
												uage 🚧	palo	alto
③ Firefox automatically set	ends s	ome data	to Mozilla	a so that we	e can impr	rove your e	xperience				Choose	What I Sh	are	×
	A 14 -	L de cellite	Finatoria										-	01.5
JWM _ Brunio	AILO	- Mozilia	Firefox										(J1:5

Figure 1.22: Creating zones

In here, we just change the name and type of zone. For information's sake. We will only be dealing with (mostly) layer 3 things in Palo Alto for this book. After that, press **OK**. Remember to create Inside and Outside zones (Remember to also commit changes from time to time!)

📓 x11 - TightVNC Viewer ﷺ 🖬 🛍 🚺 📕 🗲 🐲 🏨 Chri. Alt 🕋 🔍 🤍 🥯	Q. Q.		-	- (n x	
9 BruhloAlto - Mozilla Firefox					_ 6 ×	1
⅔ BruhloAlto × +						
← → C ŵ ③ A https://192.16	\$8.0.1/?#network::vsys1::network/zones	··· 🖂 🕁	1IIN		≣ ®	
O PA-VM Zone			0	1771	िन≁ Q	l
Name Inside	User Identification ACL	Device-ID ACL			0.0	
Log Setting None	Enable User Identification	Enable Device Identification			GO	
Interfaces				Olter	$m \rightarrow \times$	
Cover C	Select an address or address group or type in your own address. Ex 192 168 1, 20 or 192, 168 1.0/24	Select an address or address gro or type in your own address. Ex 192 168 1.20 or 192,168,1.0/24	üp	WD	EXCLUD	
S DHCD	Add Delete	⊕ Add ⊖ Delete				
- GobaProtec	Users from these addresses subnets will be identified.	Devices from these addresses/subnets will be				
G. Portals		dentified.	_			
Add Delete	Select an address or address group	EXCLUDE LIST A				
Clientins Clientins Code Zone Protection	or type in your own address. Ec 192 166 1.20 or 192.168.1.0/24	Select an address or address gro or type in your own address. Ex 192.168.1.20 or 192.168.1.0/24	up			
Zone Protection Profile None	Add Oclete	0				
Global Pro Buffer Protect	ion User's from these addresses/subnets will not be identified.	Devices from these addresses/subriets will no	the			
More Can ME Cran Meridae Monikian Monikian Minternece			ancel	40 6	paloalto	
⑦ Firefox automatically sends some data to Mozill	a so that we can improve your experience.	Cho	ose Wha	t I Sha	are X	
JWM _ 🗧 😼 BruhloAlto - Mozilla Firefox					01:53	3

Figure 1.23: Create a zone Inside as a layer3



Figure 1.24: Create a zone Outside as a layer3

Set Up a Static Interface IP Address in Palo Alto

Go under the network tab, and click on ethernet1/1.

x11 - TightVNC Viewer							- 0	x u
	Ciri Ait 🖹 🕀	2000						
👂 BruhloAlto - Mozilla Fir	efox							- 5 >
4 BruhloAlto	× +							
€ ⇒ C û	🛈 🙆 https://	/192.168.0.1/?#networ	k::vsys1::networl	<th>es</th> <th>… ⊠ ☆</th> <th></th> <th>8 Ξ</th>	es	… ⊠ ☆		8 Ξ
🚺 PA-VM	DASHBOARD	ACC MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE		€a v Q
								50
Zones 4	Ethernet VL	AN Loopback Tunne	SD-WAN					
P VLANs	Q(8 items	$\rightarrow \times$
Virtual Routers	INTERFACE	INTERFACE TYPE	MANAGEMENT	LINK	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL
GRE Tunnels	ethernet1/1			m	none	none	Untagged	none
芝 DHCP	Chernet1/2	-			none	none	Untagged	none
V C Global Protect	ethernet1/3				none	none	Untagged	none
C Portais	ethernet1/4			m	none	none	Untagged	none
Gateways	mothemet1/5			1	none	none	Untagged	none
Clientless Apps	and ethernet 1/5				none	none	Untagged	none
Clientless App Groups	mathemat 1/7				0008	Done	Untagged	none
CoS	and a share at 10				0000	0000	Untraned	0000
Construction of the second secon	HAND CONCILING				in re	TAUL C	Unagged	THE .
Monitor ·	-				P			
Mg Interface Mgmt	🕞 Ádd Sublitte	rface 🕞 Delute 🙆 PDF/0	CSV					
admin Logout Last Login Time	04/26/2022 18:35:	01 Session Expire Time: 0	5/26/2022 18:98:2	21		⊠ ≸≣ Tāsks. La	ingulage 🛷 pa	aloalto
⑦ Firefox automatically se	nds some data to	o Mozilla so that we car	n improve your e	xperienc	e,	Choos	se What I Shar	e X
	Alto - Mozilla Fi	irefox		-				01.5
- Dranio	- TOZING TI	in crox						01.0

Figure 1.25: Select Ethernet 1/1

The first thing we want to do when configuring an interface is changing the interface type to layer 3, the virtual router to default, and changing the security zone to the desired zone. In this case, we have to change it to inside for ethernet1/1, and outside for ethernet1/2.

9월 64 Alijing (역 역 역 원	_	_
i Firefox		
× T		
🛈 🔒 https://192.168.0.1/?#network:>sys1::network/interfaces 🛛 😁 💆	lin 🖸	۲
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE	- 10	€ 1 + (
		G
thernet Interface (7		
Teach a Music Patrona M	B Memo	1
Comment	145	VLA
Interface Type Layer3	Untagged	tione
Netflow Profile None	Untaced	ICODE:
config IPv4 IPv6 SD-WAN Advanced	Untagged	ricor
Assign Interface To	Uncapped	IDO
Virtual Router default	Untargetd	riche
Security Zone Inside	Untargent	IDR
	Untieged	INFO
Cincel	Unserred	1004
1g/PDF/CSV		
Trees, Of Male your (ACARADA) Seemen Events Trees. (No. 1) (2012)	- P	aloal
Phase de la companya	what I Sha	rà I
t	A FIREfox × +	A Filedox × • •

Figure 1.26: Ethernet 1/1 Configuration

Now, under the IPv4 tab of the opened window, click on **Add**, then type in the address and prefix of the interface.

BruhloAlto	× +		
€ → ୯ @	③ ♣ https://192.168.0.1/?#network:>vsys1::network(interfaces ☺ ☆)	III\ CD	۲
PA-VM	BASHEGARD ÁCC MONITOR POLICIES DEVECTS NETWORK DEVICE	annt- È	En .
			63
interfaces	Ethemet PLAN Localises Tomms 5D MMM	b ,	
The Zumes	Ethernet Interface	0	
Bat Vinual Wires	and the second se	a den	2 7
Virtual Routers	Interface Name ethemet1/1	-	VLA
PSec Tunnels	Comment Institute Targe Delayer	TAG	VIR
T DHCP	Interface type Layers	Untagged	nbri
E DAS Prom	RECTOR FLORE MARE	Untagged	HOP
Prototel Protoct	Config IPv4 IPv6 SD-WAN Advanced	Lintaggod	1900
C Putter	County (C-synkine	Unsugged	Isola
MDM	Type Q Static 💭 PPPoE 💭 DHCP Client	Lintaged	nore
Cientaray App		Unsuged.	1 Mar
The Cheminess App	10.0.0.1/24	Unterpot	Incre
St Res		Linterent	000
Network Problem			
Glabul Frahers	*		
TT IKE GATENERYS	Add Delete Move Up L Move Down		
M IKE CAVERD	(P.atilres/ntmask. Ex. 1923/662254/24)		
C Marine			
ன transfasé Myra	OK Care	e)	
tps://192.168.0.1/7#			paloa
Erefox automat	cally sends some data to Mozilla so that we can improve your experience.	hoose What I Sh	are

Figure 1.27: Set an IP address for Ethernet 1/1

Ping an Interface in Palo Alto

By default, a Palo Alto interface is not pingable. In a lab environment, checking if pings are working is a good sanity test. Go to the advanced tab, click the drop-down menu next to the management profile, then click **New**.

x11 - TightVNC Viewer		- C	x c
	- 🔊 🏭 Crit Alt 🛍 🔍 🔍 🔍 🍭 🔯		
🟮 BruhloAlto - Mo	zilla Firefox		_ a ×
🦇 BruhloAlto	× +		
€ → C @	🛈 🖍 https://192.168.0.1/?#network::vsys1::network/interfaces 🛛 💀 😒 🟠		≝ ≡
O PA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE	-	+ ₹ + Q
			GØ
Interfaces	Ethernet VLAN Loopback Tunnel SD-WAN	k	
P VLANs	Ethernet Interface ()	8 items	$\rightarrow \times$
Virtual Wires	Interface Name ethernet1/1	TAG	VLAN /
GRE Tunnels	Interface Type Layer3	Untagged	none
n DHCP	Netflow Profile None V	Untagged	none
DNS Proxy	Config IPv4 IPv6 SD-WAN Advanced	Untaged	none
Portals	C Link Settings	Unterped	none
Gateways	Link Speed auto	Untagged	none
Clientiess Apps	Other Info ARP Entries ND Entries NDP Proxy LLDP DDNS	Untagged	none
Clientless App	Management Profile Nome	Untagged	none
dis Qos	MTU None	Untagged	none
V 🗟 Network Profiles	- 🗌 Adjust TCP MSS - New 🚳 Management Profile		
GlobalProtect I	IPv4 MSS Adjustment 40		
E IPSec Crypto	IPv6 MS5 Adjustment 60		
EL IKE Grypto	Untagged Subinterface		
Monitor			
ster internace ingine	OK Cancel		
admin Logour Lasi L		uart 🕠 p	aloalto
⑦ Firefox automat	ically sends some data to Mozilla so that we can improve your experience.	e What I Shai	e X
	BruhloAlto - Mozilla Fírefox		01:58
-			10100

Figure 1.28: Ethernet 1/1 configuration – Advanced Tab

Call this whatever you want, but make sure to tick the ping option under networking services. Then press **OK**.



Figure 1.29: Enable Ping under Interface Management Profile

Enable DHCP on an Interface in Palo Alto

It's almost the same thing as setting up a static interface, but you act differently in the IPV4 menu. Instead of typing in an IP address and mask, you just specify that this is a DHCP client.

BruhloAlto	× +				
	1	https://192.168.0.1/?#network::vsys1::network/interfaces •••• (9 ☆		e =
PA-VM	DASHBO	ARD ACC MONITOR POLICIES OBJECTS NETWORK DEVI	CE 📑 Commit	-) în	₽n v Q
(interfaces	1				50
Zones Be VLANs	Ethernet Interfa	it VLAN Loopback Turmel, SD-WAN ace	0	B items	$\rightarrow \times$
Virtual Wires	Interface Name	ethernet1/2			
Virtual Routers Virtual Routers O GRE Tunnels GRE Tunnels DHCP DNS Proces	Comment			TAĞ	VLAN /
	Interface Type	Layer3	~	Untagged	none
	Netflow Profile	None	~	Untagged	none
GlobalProtect	Config IPv4	IPv6 SD-WAN Advanced		Untagged	none
G Portais		Enable SD-WAN		Untagged	none
Gateways	Туре	Static PPPoE OHCP Client		Untagged	none
Clientiess Apps		Z Enable		Untagged	none
Clientless App		Automatically create default route pointing to default gateway provided by server Send Hostname system-hostname	~	Untagged	none
	Default Route Met	ric 10		Untagged	none
 Network Profiles 日 GlobalProtect i 千 IKE Gateways 日 IPSec Crypts 日 IKE Crypts 		Show DHCP Client Runtime Info	Cancel		
A Manitor	-				
interface Mgmt		Submertadi (E) Giter @ PDF/CSV			
amin Lagolit Last La	gin Time: 04/26/202	2 18:35:01 Session Expire Time: 05/26/2022 18:38:29	213≘ arbi Lun	euros 🥠 p	aloalte
) Firefox automati	cally sends some	data to Mozilla so that we can improve your experience.	Choose	what I Shar	e >
		-We Flasferr			00

Figure 1.30: Enable DHCP Client on Ethernet 1/2

Don't forget to commit your changes!

If all is well after a commit, you will be able to check your DHCP IP address by clicking "dynamic DHCP client" in the main network menu.

🕽 BruhloAlto - Mozilla Fi	refox							_ 8
A BruhloAlto	× +							
€ ⇒ ୯ û	(i) 🔒 https://192	.168.0.1/?#netwo	rk::vsys1::network	nterfac	es -	··· 🖂 🕁	III 🛈	@ ≡
🚺 PA-VM	DASHBOARD AC		POLICIES C	DBJECTS	NETWORK E		- 10	€∎• Q
								GO
interfaces	Ethernet VLAN	Loopback Tunn	d SD-WAN					
VLANs	Q						Biten	»)→×
Virtual Routers	INTERFACE	INTERFACE TYPE	MANAGEMENT	LINK	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUA
GRE Tunnels	conterect1/1	Layer3	Ping		10.0.0.1/24	default	Untagged	none
DHCP DNS Prom	and other set 1/2.	Layer3			Dynamic-DHCP Climit	default	Untagged	none
GlobalProtect	m othermet 1/3				none	none	Untagged	none
Portals	m ethernet 1/4			6	none	none	Untagged	none
Gateways MDM	@Bethernet1/5			8	none	none	Untagged	none
Clientless Apps	and ethernet 1/6-			6	none	none	Untagged	none
Clientless App Groups	methemet1/7			6	nórie	none	Untagged	none
tupe	and ethernet 1/8			199	none	none	Untagged	none
 ✓ Generation Network Profiles ▲ GlobalProtect IPSec City ➡ IKE Gateways ▲ IPSec Crypto ➡ IKE Crypto 								
Monitor +	1							
Zoor Protection								
A Des Profile	(2) Add Subinterlare		CSV		-			
edmin Logout Last Login Time	E 04/26/2022 18:35:01	Session Explite Times to	5/26/2022 18:38:25	4		⊠l ∰ Tasks I i	14	paloalto
		A COLOR						0.0

Figure 1.31: Dynamic DHCP Client- Receive an IP address from DHCP Server

Here is an example of that:

x11 - TightVNC Viewer			- 1	ц)
	🏨 Cht All 🛅 🍳 🍳 🔍 🎕 🔢			
BruhloAlto - Mozilla F	irefox		_	- 8
🏇 BruhloAlto	× +			
€ ⇒ € @	🛈 🐔 https://192.168.0.1/?#network::vsys1unetwork/interfaces	··· 🖂 🔂	III\ 🔟	۲ :
DA-VM				
				a
and interfaces	Ethernet State - Complete - Lands - Complete			
To wante	Concession of the second se	-		
Statute and	Dynamic IP Interface Status	0	0.00	33
C vina water to		1000		VUN
(Play Lonint)	Interface ethernet1/2	ROUVER	TAG	ANEX
Un CAL Furnit	State Bound		Ulderant	tons
E DED TOWN	Remaining Lease Time 0 days 0:58:58		Uniment	int
& Contractor	Gutemay 192.168.122.1		Unliggint	heol
Carl Russie	Primary DNS 192.168.122.1		Indexet	
Company of	Secondary DNS 0.0.0.0		Conceptor	
90 mole	Primary WINS (0000		Unistant	1000
Contract Apr	Primary NIS 0.0.0		Unkargent	Intel
South State Street Stre	Secondary MIS 0.0.00		Unitedant	1000
0.6	POP3Server 0.000		Ilmond	
	SMTP Server 0.00.0		Consequences	100.0
The Challen House of Files, The	and shine			
T all Company	Renew Release	Close		
DI PERSONALI P				
1/7 HE Constant II				
2				
Sector and improve				
En Larm Orema Care	the second s			
Contrast a	(A) Add Subimerface (C) Delete (C) PDI (CSV			

Figure 1.32: IP Address of Interface 1/2

Set Up a DHCP Server in Palo Alto

In the network tab, click on **DHCP**, then click **Add**.



Figure 1.33: Add a DHCP Server

First, we need to define the interface, I set that to ethernet1/1 because it is our LAN. Then, I press **Add** and define a range that fits the network subnet.

🔒 BruhloAlto - Mozi	lla Firefox				_ 8 ×
4 BruhloAlto	× +				
↔ ở ✿ ✿	🛈 🛍 https://192.168.0.1/?#ne	twork::vsys1::network/dhcp		⊚ ☆	III\ © © ≡
🔷 PA-VM	DASHBQARD ACC MONITO	DR POLICIES OBJECTS	NETWORK	DEVICE	- I 色 色 + Q
Real of the local division of the local divi					50
Virtual Routers	DHCP Server			0	-
GRE Tunnels	Interface etilemetal/1			~	N 0 items ⇒ ×
T DHCP	Mode auto			~	RESERVED
DNS Prow	Lease Options				
Portals	Ping IP when allocating r	new IP			
Gateways	Lease O Unlimited O Timeout				
MDM		RESERVED			
Clientless App Gr	10.0.0.10-10.0.0.20	ADDRESS	MAC ADDRESS	DESCRIPTION	
Qu5		192.168.1.20 x	сэх эх эх эх хо (Op)	tional MAC Address	
C LLOP					
GlobalProtect IPS					
T IKE Gateways					
B IPSec Crypto					
IKE Crypto	⊕ Add ⊖ Delete	() Add () Dele	10		
Interface Mgmt					
Zone Protection			-	OK Cancel	
QuS Profile				Cinter	
and ELDP Prohie	1				
SD-WAN Interface Fro	mie Charles Charles				
	Add Lefee OPDF/CSV	- Proto de antes a serio -			the sector is a
					paloaico
JWM _ 🚽 😓 Br	uhloAlto - Mozilla Firefox				02:03

Figure 1.34: Set an IP Pools for Interface 1/1

After that, we need to configure some DHCP options under the options tab. Here we need to define the gateway, (which is usually the interface IP address) subnet mask (which is usually 255.255.255.0), and a DNS server. I just use Google's DNS server as an example.

- C W	U 🖍 htt	rb>//145.108.0.1/:#network:://s/s	L::net	work/ancp	_				
PA-VM	DASHBOAR	D ACC MONITOR POLI	CIES -	OBJECTS	NETWO	DRK DE	VICE	_e Sarani	- Ib B
Virtual Wires	DHCP Server							1	5
Virtual Routers	Interface	ethernet1/1						~	
IPSec Tunnels	Mode	auto						V	Ø items -
DHCP	Lease Option	s							RESERVED
DNS Proxy	Inheritance Source	None		Custom DHCP	options				
GlobalProtect		O Check Internitional Internitional		NAME	CODE	TYPE	VALUE		
GREWays	Gateway	10001		-		1.114	1.000		
MDM	Subnet Mask	255 255 255 0							
Clientless Apps	Primary DNS	8888	51						
Clientless App Gra	Secondary DNS								
Que	Drimony Milhic	None							
Network Dinbles	Primary Wing						*		
C GlobalProtect IPSe	Secondary WINS	None	×						
T IKE Gateways	Primary NIS	None	Y.						
🔁 IPSec Crypto	Secondary NIS	None	~						
C IKE Crypto	Primary NTP	None	~						
Monitor	Secondary NTP	None	~						
By Interface Mgmt	POP3 Server	None	~						
Cas Protection	SMTP Server	None	< 1						
LLDP Profile	DNS Suffix	None	~	⊕ Add ⊖t	Delete T Mi	wellp 11	Mave Dawn		
H BFD Profile									
5D-WAN Interface Frat							_		

Figure 1.35: Set a Gateway and a primary DNS

Again, remember to commit your changes!

Ping Palo Alto from a LAN Device

When opening up your webterm for "Client", click the bottom left button, then click terminal.



Figure 1.36: Open Terminal in WebTerm1

Type in **ip a or ifconfig** on the terminal. If you see an IP address under eth0, the DHCP Server worked!



Figure 1.37: Check the IP address in Terminal

Now, let's ping our Palo Alto device. Type in ping 10.0.0.1. If all works out, you should see this:



Figure 1.38: Ping 10.0.0.1 in the terminal

This means that everything so far worked! Press **Ctrl+C** to stop pinging the Palo Alto device.

Security Profile Basics

In the policies tab, we want to create a new policy. Click on new in the bottom left of the Palo Alto web interface.

BruhloAlto - Mozilla Fir	efox								_ 8
🍄 BruhloAlto	×	+							
€ ⇒ C @	0) 🙈 https://192.1	68.0.1/?#policie	es:vsys1:pc	licies/security-	rulebase	⊡ ☆	10	
🚺 PA-VM	DAS	HBOARD ACC		POLICIES	OBJECTS		DEVICE	E Cumit-	1 to to Q
									G ()
Security -	Q.								$_{2 \text{ items}} \rightarrow \times$
NAT A Das							Source		
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
Decryption	1	Intrazione de Laules	nome	Intrazone	-111	m	ary.	-	(intrazione)
Application Override	z	intercom-dela.	-	interzone	.en	-	ATY	-	-
Policy Optimizer Ass Ado Viswer Mark Without App Contrast Contrast App Contrast App Contrast Contrast App Contrast App Contrast Contrast App Contrast Ap	*								
Object : Addresses + https://192.168.0.1/7#	⊕# 04/20	udd ◯ 0 ,000 (00 C 6/2022 (8:35,01) 5e	inni: Dormati arch Expire Time	6 Praert 05/26 2022 1	g rpaida 🕥 D estaszy	Move *	© PDF/CSV □ Hi	ghlight Unused R	ules » W paloalto
WM - Bruhlo4	Nto -	- Mozilla Firefox	ε						02:1

Figure 1.39: Add a Security Policy

Under the general tab, we just want to give it a name. We will only be working with universal rules.

x11 - TightVNC View	e/	- 🗆 X
	5- 영 論 Chi Ali 뉴 句, 句, 句, 句, 월	
😜 BruhloAlto – M	ozilla Firefox	_ 8
BruhicAlto	× +	
€ → ሮ ŵ	🛈 🔬 https://192.168.0.1/?#policies:vsys1::policies/security-rulebase 🚥 💟 🛱	
🔷 PA-VM	DASHEGARD ACC MONTOR POLICIES CHIECTS NETWORK DEVICE	Sector De Br Q
- Security		G () ≥itims → X
H NAT	Sere Sere	•
Security Policy R	ule	
Rule Type In Rule Type In Description Taga Group Rules By Tag Audit Corresent	sood iversal (kotusto me	
_		
Object : Addresses	+ © Add Move* © PDF/CSV []	Highlight Unused Rules *
man Deserved	kan Tim-Sz. Szz. (19. d) (kan han-Ja-Sz. 20 21. 🔞 🖄	🛟 paloalto
IWM -	BruhloAlto - Mozilla Firefox	02:1:

Figure 1.40: Set a Name for Security Policy

Under the source tab, we specify the inside zone (from). In this case, it will be the "Inside" zone.



Figure 1.41: Set a Source Zone for Security Policy

Under the outside tab (to). Specify the outside zone.

Bruhlokto	BruhloAlto - Mozilla		Q 🔛		-
C C C	🏇 BruhloAlto	× +			
CASHEGAAO ACC MONTOR OSCIENT Lastrecome Control Control <t< th=""><th>€ → ୯ ଇ</th><th>🛈 🙈 https://192.168.</th><th>0.1/?#policies:>ysys1:policies/security-rule</th><th>base ···· 🗵 🔒</th><th>n 🗆 🔹 =</th></t<>	€ → ୯ ଇ	🛈 🙈 https://192.168.	0.1/?#policies:>ysys1:policies/security-rule	base ···· 🗵 🔒	n 🗆 🔹 =
	OPA-VM			NETWORK DEVICE	
Security Policy Rule	Security				Q () P ^{2itims} →)
Central Source Destination Application Service/URL Category Actions	Security Policy Rule			Sector-	
	General Source Dest	ination Application Service	URL Category Actions		
DESTINATION ZONE ^ DESTINATION ADDRESS ^ DESTINATION DEVICE ^	select		M Ann	anv	
Image Image Image Image			DESTINATION ADDRESS	DESTINATION DEVICE	
Inde Outline Outline <		v.			
O Add	Inside				
O Add O Add O Add O Add O Delete	Outside				
CAdd ⊙Deleter					
O Add					
Negule Cline:- Addresses + ⊕ Addi Minge:- Addresses + ⊕ Addi	() Add O Delete		⊕ Add _ Deem	⊕ Add ⊡ Di	
Cilicet : Addresses + @Adda Mine + @PDF/CSV [] Heighlight Unseed Rules			Negate		
GK Digeet Addressev + ⊙Add = Mnye ¹					_
Diger: Addresses + O'Add Burnerd Rules					OK.
Diger: Addresses + O Add B Maye BDF/CSV - Highlight Unseed Rules					
Diljoct : Addresses + ④ Add Meye - ③ PDM7CSV 🗌 Highlight Unused Rules		-			
	biect Addresses	+ (Add		Merve - PDF/CSV Highlight Unused I	Rules ×

Figure 1.42: Set a Destination Zone for Security Policy

After that, press **OK** to confirm.

SNAT (Source NAT: Access the Internet in Palo Alto)

🚾 x11 - TightVNC Viewer							- 0	×
	🔒 Ctri Alt 🐴 🗨	Q @ @ 🔂						
😫 BruhloAlto - Mozilla Fi	refox						-	а×
🊧 BruhloAlto	× +							
↔ ↔ ↔ ↔	🛈 🔏 https://	192.168.0.1/?#policie	es::vsys1::policie	s/nat-rulebase	***	⊠ ☆	III\ 🗊 🔮	Ξ
🚺 PA-VM	DASHBOARD	ACC MONITOR	POLICIES	OBJECTS	NETWORK DEV	/ICE 🛃 Commit →) To Pa	Q
Convitu	0						0 items	
					Orig	inal Packet		
💩 QoS 📑 Policy Based Forwarding	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION	SOURCE ADDRESS	DESTINATION ADDRESS	SEF
Application Override Application Override DoS Protection Solution Policy Optimizer Solution Control Contro Control Control Control Control Co	- 0 0			×				
Object : Addresses	- 🕀 Add 🕘 Delete e: 04/26/2022 18:35:0 Alto - Mozilla Fin	G Clone G Enable D1 Session Expire Time: Crefox	O Disable Mov	e Y () PDF/CSV 29	Highlight Unused	Rules □ View Rulebase ☑	e as Groups Jage 🥢 palox	» alto 02:16

Under the policies tab, go to NAT, then click **Add**.

Figure 1.43: Set a NAT

In this case, we want to translate packets originating from the Inside to go to the outside zone using the interface address of ethernet1/2. This would be Port Address Translation Overload. Under the general tab, just change the name.



Figure 1.44: Set a Name for NAT

Under the original packet tab, click **Add** then make the source zone inside. As for the destination zone, make it outside.



Figure 1.45: Set a Source Zone and Destination Zone for NAT

Under translated packet on source address translation. Specify the translation type as Dynamic IP and port, the address type as interface address, and the interface as ethernet1/2(The interface in the outside zone) After that, click **OK**.



Figure 1.46: Set a Translated Packet

Don't forget to commit!

Check Internet Connectivity on Webterm

In webterm, you could test pinging 8.8.8.8 like so:



Figure 1.47: Verify your configuration

Or you can try navigating to a website for example https://something.com.



Figure 1.48: Verify your connectivity to the Internet

If both of these work. You have successfully configured DHCP and SNAT properly!

46 Chapter 1. Basics

1.3 SNAT

Learning Objectives

• Configure Source NAT (SNAT)

Prerequisites:

- Security policy for Inside to Outside
- Interface configuration
- Knowledge of previous labs

Scenario: Source NAT is what your router does on a daily basis to provide you with Internet access just so you can go on social media and complain about how slow your internet is. Your router at home does this all automatically for you. But since we're real network engineers with a firewall on one hand, and determination on the other. Let's learn how to configure this all by ourselves using Palo Alto! We've already configured this in the previous chapter, so let's just go over it again!

48 Chapter 1. Basics



Figure 1.49: Main Scenario

Table 1.4: Addressing Table

Device	Configuration
Clint	eth0: 10.0.0.2/24 GW: 10.0.0.1 DNS: 8.8.8.8
PaloAlto	Ethernet1/1: 10.0.0.1/24 Ethernet1/2: DHCP Management: 192.168.0.1/24
Management (WebTerm)	eth0: 192.168.0.2/24
Outside (WebTerm)	eth0: DHCP

Table 1.5: Zone Configuration

Zone	Interface
Inside	Ethernet1/1
Outside	Ethernet1/2

SNAT (Source NAT: Access the Internet in Palo Alto)

x11 - TightVNC Viewer								- 🗆	×
B 🖬 🗈 🔳 😏 🛷	😭 Ctri	Alt 📭 🤁	20.00						
😢 XavPA - Mozilla Firefo	х	-					_	-	а×
🊧 XavPA	×	+	k						
$\leftarrow \rightarrow $	(D 🔏 https:,	//192.168.0.1/?#polici	es::vsys1::policie	s/nat-rulebase	~ …		III\ 🗊 🔹	Ξ
🚺 PA-VM	DA	SHBOARD	ACC MONITOR	POLICIES	OBJECTS N	NETWORK DEVI	CE 📋 Commit 🖂	। चि मि	, q
Security	0							G 1 item	:
⇒ NAT	-					Orig	inal Packet		7.43
🐣 QoS 📑 Policy Based Forwarding		NAME	TAGS	SOURCE ZONE	DESTINATION	DESTINATION	SOURCE ADDRESS	DESTINATION ADDRESS	SEF
 Decryption Tunnel Inspection Application Override Authentication 	1	SNAT	none	22 Inside	P2 Outside	any	any	any	Jany
E DoS Protection									
Policy Optimizer -	-								
✓ ⋛ Rule Usage Null Unused in 30 days	4								
Unused in 90 days	1								
E Unused	1								
		-		_					_
Object : Addresses -	+ ①	Add 🕞 Deler	e 19) Clane 💮 Enable.	Disable Mov	e Y 🕒 PDF/CSV	/ 🗌 Highlight Unused	Rules View Rulebase	as Groups	>>
https://192.168.0.1/?# 1	ie: 05/0	17/2022 16:30	:41 Session Expire Time:	06/06/2022 16:34	(1A		⊠ \$= Tasks Langu	lage 🥠 palog	ETHORES
JWM _ WAVPA	4 - Mo	ozilla Firefo	X						23:59

Under the policies tab, go to NAT, then click Add.

Figure 1.50: Set a Source NAT

We want to translate packets originating from the Inside to go to the outside zone using the interface address of ethernet1/2. This would be Port Address Translation Overload. Under the General tab, just change the name.



Figure 1.51: Set a Name for NAT

Under the original packet tab, click add then make the source zone inside. As for the destination zone, make it outside.

🕅 x11 - TightVNC	Viewer				- 🗆 X
		€ 			
XavPA - Mic					×
	A	<u> </u>			
() > G		s://192.168.0.1/?#policies::vsys1::p	oolicies/nat-rulebase	© &	
OPA-VM	DASHBOARD	ACC MONITOR POLICIE	S OBJECTS NETWOR	K DEVICE	्रिम् ग र
					50
Security	Q				$_{1 \text{ item}} \rightarrow \times$
A Dos	Contractory Contractory			Original Packet	
Policy Baser	NAT Policy Rule				() STINATION DRESS SET
E Decryption	General Original Packet	Translated Packet			
Application 1	C	Destination Zone			
Authenticati		Outside v	SOURCE ADDRESS	DESTINATION ADDRESS	~
Dos Protect	Inside				·
A DE VINIY		Destination Istanface			
Policy Optimizer		any ~			
∽ ў⊟ Rule Usage					
Unused		Service			
S Unused	*	any \vee			
	⊕ Add (⊖) Delete				
					_
				OK Cancel	
					~
Object : Addresse	es + 🕀 Add 💬 De	lete 🔞 Clone 🧭 Enable 🚫 Disable	Move *	light Unused Rules 🗍 View Rulebas	e as Groups 🖇
admin Logout	Last Login Time; 05/07/2022 16:	0:41 Session Explin: Time: 06/06/2022	14:34:19	🖾 i 🏭 laakse i Lang	paloalto
JWM	ۏ XavPA - Mozilla Fire	fox			00:03

Figure 1.52: Set a Source Zone and Destination Zone for NAT

Configure these settings under the translated packet tab in the **source address translation** area:

Table 1.6: SNAT Configuration

Parameter	Value
Translation Type	Dynamic IP and Port
Address Type	Interface Address
Interface	Ethernet1/2
IP Address	None

52 Chapter 1. Basics

🗱 x11 - TightVNC	Viewer					-		×
	11 😔 🕾 🎉 Ctrl A		R 🔁					
单 XavPA - Mo	ozilla Firefox						-	а×
🋷 XavPA	×	+						
(←) → C	û (i)	💫 https://192.168	.0.1/?#policies::vsys1::p	oolicies/nat-rulebase	⊠ ☆	101	•	Ξ
🔷 PA-VM	DASE	BOARD ACC	MONITOR POLICI	S OBJECTS NETWORK	DEVICE	L III Dec. 27	ींग मिक	Q
5 Sec. dlu	. 0						1 item	$ \bigcirc $
A NAT		-	Ī		Original Packet			1 20
Qos Re Policy Bases	NAT Policy Rule					0	TINATION	SET
E Decryption	General Origina	Packet Translated	Packet					=01)
Application (- Source Address Tran	slation		 Destination Address Translation — 				
Authenticati	Translation Type	Dynamic IP And Port	~	Translation Type None		\sim		
SD-WAN	Address Type	Interface Address	~					
	Interface	ethernet1/2	~					
Policy Optimizer	IP Address	None	~					
∽ Ž≣ Rule Usage								
Unused R Unused					ок	Cancel		
🐻 Unused		_						
Object : Addresse	es + 🕑 Ac	ld (-) Delete (B) Clar	ne 🅑 Enable 🚫 Disable	Move * (D) PDF/CSV Highlight	Unused Rules View	/ Rulebase as G	roups	>>
admin I Logout I	List Login Timer 05/07/	2022 16:30:41 Sessio	on Explicit nine: 06/06/2022	1634019		e l'Emplace	m palos	AICO.
JWM _	😓 XavPA - Moz	illa Firefox					(00:07

Figure 1.53: Set a Translated Packet

Don't forget to commit!

Check Internet Connectivity on Webterm

Open up webterm, and navigate to any website of your choosing.



Figure 1.54: Verify your connectivity to the Internet

If your desired webpage showed up, you have successfully configured SNAT!

54 Chapter 1. Basics

1.4 DNAT

Learning Objectives

- Configure Destination NAT (DNAT)
- Configure WordPress

Prerequisites:

- SNAT for the Internet
- Security policy for Inside to Outside
- Interface configuration
- Knowledge of previous labs

Scenario: When I think of DNAT (Destination Network Address Translation) I always think of the days of setting up port forwarding for all my favorite games just so I could host server friends can play on. You can think of DNAT like this too if it helps! The goal of this lab is to reach WordPress from the Outside. So, users only enter the IP address of Ethernet 1/2 in the Outside webterm and the firewall redirects the traffic to WordPress.



Figure 1.55: Main scenario

Device	Configuration		
WP (WordPress)	eth0: 10.0.0.2/24 GW: 10.0.0.1		
PaloAlto	Ethernet1/1: 10.0.0.1/24 Ethernet1/2: DHCP Management: 192.168.0.1/24		
Management (WebTerm)	eth0: 192.168.0.2/24		
Outside (WebTerm)	eth0: DHCP		

Table 1.8: Zone Configuration

Zone	Interface
Inside	Ethernet1/1
Outside	Ethernet1/2

Create Reference Addresses

Under **Objects** > **Addresses**, click **Add**.



Figure 1.56: Add an address
In this window, we will add the IP of the WordPress server to reference it easier.

🗱 x11 - TightVNC Viewer							-		×
ª∎∎∎∎ ∎ 9 ∰	tri Alt 📭 🔍 🔍	a a 🔂							
👏 PA-VM - Mozilla Firefox								_	. 🗆 ×
🦇 PA-VM	< +								
← → ¢ ŵ	(i) A https://192.1	.68.0.1/?#objects	::vsysl::o	bjects/addresses		🛛 ☆	lii).	•	Ξ
OPA-VM	DASHBOARD AC		POLICI	es objects	NETWORK		a Commit ∽	म्म म	×Q
								2.000) ())
Addresses	AL A BAS	IDEATION		TYPE	ADDRESS		74.05	2 items	$\rightarrow \times$
Regions	T FW	LOCATION		IP Netmask	192.168.122	.116	TAGS		
B Dynamic User Groups	1 Wear			IP Netmask	100.02				
Application G Address			_				0		
Application F							U		
Nar Nar	wordpress								
Tags Ty	pe IP Netmask		~	10.0.0.2			Recolud		
GlabalProtec				Enter an IP address or a 1 192.168.80.0/24). You ca	network using the slash in also enter an IPv6 ad	notation (Ex. 192.16) dress or an IPv6 addr	8.80.150 pr ess with its		
Fill Prof. Ta	gs			prens (Ex. 20031006.123		1.//84/	*		
External Dyna									
Data Pau						OK.	Cancel		
D Spyware			_						
URL Calegory									
Security Profiles									
Antryinus									
Wilnerability Protection									
URL Filtering	Add back	lion: DPDF/CSV							_
in Lagral Last Lagin Line, W	ourseper lize47.25 Se	sson Elpir Tior - 5	a Britage	at usuali			- 11-11-12	W/palo	alto
<mark>∫WM</mark> €PA-VM - N	Mozilla Firefox							1	08:26

Figure 1.57: WordPress IP address

We also want to put our firewall's "public" IP (the interface facing the NAT cloud) here too. You can find the firewall's DHCP address under **network** > **interfaces**. Then click the hyperlink under IP address:

< → C û	① 🔒 https://192	.168.0.1/?#networ	k::vsys1::network	(interfas	es •	• 🛛 🕁	III (D	@ ≡
0 PA-VM	DASHBOARD AC	C MONITOR	POLICIES C	DBJECTS	NETWORK DI	VICE Barnal	- 10	⊡ • Q
mentaces	Ethemet VLAN	Loopbatk Tunni	SD-WAN					GC
VLANs	QC						8 iten	ns →×
Virtual Routers	INTERFACE	INTERFACE	MANAGEMENT	LINK	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUA
GRE Tunnels	methemet1/1	Layer3	Ping		10.0.0.1/24	default	Untagged	none
DHCP	ethernet1/2	Layer3			Dynamic-DHCP Client	default	Untagged	none
GlobalProtect	methernet1/3			100	none	none	Untagged	none
Portals	Gill ethernet 1/4			100	none	none	Untagged	none
Gateways	(Debeneti)			-	none	note	Untagged	include:
Clientiess Apps	ual enternet to a						the based	
Clientless App Groups	God ethemet 1/6			(m)	none	none	Ownagged	none
A QoS	diffethemet1/7			m	none	none	Untagged	mone
23 LLDP	etherrat1/8			6	none	none	Untagged	none
V La Network Profiles								
GlobalProtect IPSec On	r							
M IPSec Crypto +								
A IKE Crypto +								
Monitor +	A							
10 Interface Mgmt								
Zone Protection								
A Des Reefile is	(P) Add Suborteniare	O Delen 👩 PDF/	csv					
	AL ALIMAN LANS ALL	1	to a state state of					

Figure 1.58: Dynamic-DHCP Client IP address

From there you will find the IP address of the firewall:



Figure 1.59: Verify Dynamic-DHCP Client IP address

Create a DNAT Policy

 BruhloAlto BruhloAlto 	efox	t 🖻 🔍 Q, 🗉	Q 🔂						
🔮 BruhloAlto - Mozilla Fire 🛷 BruhloAlto	efox								
🥋 BruhloAlto								-	а×
	× -	ł							
\leftrightarrow \Rightarrow \bigcirc \textcircled{a}	0	A https://192.16	8.0.1/?#policie	es::vsys1::policie	s/nat-rulebase	*** (∃ ☆	III\ 🗊 🔹	Ξ
🔷 PA-VM	DASHE	BOARD ACC	MONITOR	POLICIES	OBJECTS N	NETWORK DEVIC	E Commit v	T Pr	Q
Security .	a							G 1 item	
						Origin	al Packet	*	
👶 QoS 🕞 Policy Based Forwarding	N	AME	TAGS	SOURCE ZONE	DESTINATION	DESTINATION	SOURCE ADDRESS	DESTINATION ADDRESS	SEF
 Decryption Tunnel Inspection Application Override 	1 5	TAV	none	Magnetic Inside	Magazina Outside	any	any	any	any
部 Authentication (伊 DoS Protection @ SD-WAN									
Policy Optimizer -									
✓ ŽΞ Rule Usage Nulle Usage Nulle Unused in 30 days	4								
C Unused in 90 days									
O charte									
									_
Object : Addresses +	(+) Add		ane 🎅 Enable	C Disable Move	e Y 🔘 PDF/CSV	Highlight Unused R	ules 🗌 View Rulebase	as Groups	>>
admin Logout Last Login Time; (04/26/2	407illa Eirofov	sion Expire Time: (05/26/2022 18:38:	29	Σ	2 ≩∃ Tasks Langi	lage 🥠 palog	11 to

Under **Policies** > **NAT**, click the Add button on the bottom.

Figure 1.60: Add a DNAT Policy

Under the Original Packet tab, configure these settings:

Table 1.9: DNAT Configuration

Parameters	Value
Source Zone	Outside
Destination Zone	Outside
Destination Interface	any
Service	service-http
Destination Address	(Firewall Public Address Here)

× +	s-//192 168 0 1/2#policias-196	vel unolícias/nat-rulabasa	🖸 🛧
	s.//192.106.0.1/!#policiesvs	yst.,policies/hat-fulebase	ш © ш
DASHBOARD	ACC MONITOR B	OLICIES OBJECTS 🗟	NETWORK DEVICE
2			ala la la
NAT Policy Rule			, March 20 Pert
General Original Packet	Translated Packet		
Anv	Destination Zone	Anv	Any
	Outside		ss ~
Outside			□ Ęw
	Destination Interface		
	any	\sim	
	Service-http	~	
		(+) Add (-) Detera	(+) Add (-) Delete
			OK C
_		_	
			_

Figure 1.61: DNAT Policy Rule- Original Packet

Under the translated packet tab, Destination Address Translation. Configure these:

Parameters	Value
Translation Type	Static IP
Translated Address	(IP of WordPress here)
Translated Port	80

Table 1.10: DNAT Translated Packet	Configuration
------------------------------------	---------------

x11 - TightVNC	Viewer	- 🗆	×
	9 1 (1) (1) (1) (1) (1) (1) (1) (1) (1) (
PA-VM - Mo		_	. - ×
A A		ED (18)	
676			=
OPA-VM	DASHBOARD ACC MONITOR ROLICIES OBJECTS NETWORK DEVICE	t E	×Q
		K.	GO
Security	Q	1 isem	$\rightarrow \times$
A Qas	NAT Policy Rule	TINATION	
Policy Based E Decryption	General Original Packet Translated Packet	DRESS	SEI
Tunnel Insper	Source Address Translation Destination Address Translation	144	28
Authenticatio	Translation Type None V Translation Type Static IP V		
SD-WAN	Translated Address Word		
Policy Optimizer	Enable DNS Rewrite		
~ (= Rule Usage	Direction reverse ×		
Unused I			
To Unused	OK Cancel		
Object : Addresses	s + CrAda Concert of Clone Concertor Disable Move * Confidences I Highlight Unused Rules I View Rulebase as	Groups	balto
JWM	S PA-VM - Mozilla Firefox		08:44

Figure 1.62: DNAT Policy Rule- Translated Packet

Then, press **OK**.

Security Policy for DNAT

Under **Policies** > **Security**. Click **Add** at the bottom.

🗱 x11 - TightVNC Viewer									- 🗆 X
≞∎≝∎ ∎ 9 ø ø	Ctrl	Att $ $ \square $ $ \bigcirc \bigcirc	@ @ 🔂						
📦 BruhloAlto - Mozilla Fir	efo:	ĸ							_ a ×
🚧 BruhloAlto	×	+							
← → ⊂ ŵ	0	D 🔏 https://192.1	168.0.1/?#polic	ies::vsysl::p	olicies/securit;	y-rulebase	🖾 🖸		
🚺 PA-VM	DA	SHBOARD ACC	MONITOR	POLICIE	S OBJECTS	6 NETWORK	DEVICE [🖕 Commit 🖂	ੈ∎ €∄ • Q
									G ()
Security	Q		-		1				$3 \text{ items} \rightarrow \times$
							Source		
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
Decryption	1	InteOut	none	universal	22 Inside	any	any	aný	P Outside
Application Override	2	intrazone-defaulto	none	intrazone	atty	ariy	any	any	(intrazone)
Authentication	3	interzone-defaulta	nana	interzone	anv.	anim.		3000	
E DoS Protection		intersone derauge	TROUGE.	interzone	any	any	ant	any	any.
Policy Optimizer -							×		
Object : Addresses + https://192.168.0.1/?# DTime	⊕. :: 04/2 Alto	Add	Clane 💿 Overric ession Expire Time	ier (8 Revert : 05/26/2022 1	③ Enable, ③ 18:38:29 [Disable Move Y	PDF/CSV	Highlight Unused R E Tasks Languag	ules » Maloalto: 02:2

Figure 1.63: Add a Security Policy

x11 - TightVNC Viewer			- 🗆 X
🧏 🖬 😭 🗓 😽 🔊	🏭 Chri Alt 🛅 E. Q. 🔍 🔍 💽		
PA-VM - Mozilla Firef	ox I		_ 🗆 ×
A-VM	x +		
€ → C @	0 M https://192.168.0.1/?#policies::vs	vs1::policies/security-rulebase •	
O PA-VM	DASHBOARD ACC MONITOR	DEGES OBJECTS NETWORK D	DEVICE E Smither D
			G ()
Security	<u>Q</u>		Jitems →×
Security Policy Rule		Course	
General Source Desti	nation Application Service/URL Category Ac	tions Usage	
Anv	Anv	any 🗸	any 💉
		SOURCE USER	
Outside	*		
		⊕Add ⊖ Deter	(+) Add () Delete
	Negate		
			(lok
			- Sound
Object : Addresses	+ (+) Add (-) Delete (-) Clone	🕗 🕗 Enable 🔘 Disable Move * 🕲 PI	DF/CSV Highlight Unused Rules *
	M - Mozilla Firefox		08:46
			00110

Under the source tab, add the outside zone under the source zone:

Figure 1.64: Configuring the Source Zone

66 Chapter 1. Basics

Under the destination tab	, add the inside zone	as the destination zone:
---------------------------	-----------------------	--------------------------

🕱 x11 - TightVNC Viewer				- 🗆 X		
B B B B B B 9 ∞	🎢 Chri Alt 🖿 🔍 🔍					
PA-VM - Mozilla Firef	ox			_ 0		
🗱 PA-VM	× +					
€ → C @	🛈 🔬 https://192	.168.0.1/?#policies::vsys1::policies/security-rulebase	⊠ ☆			
PA-VM	D'ASHBOARD AC	C MONITOR HOUGHE OBJECTS NETWORK	DEVICE En Provension	1 E - Q		
= Security	0			G () Litems → >		
⇒ NAT	1	1 1 1	Sec. 1			
Security Policy Rule						
General Source Destri	nation Application 5	ervice/URI Category Actions Usage				
	A District of the		10-20			
DESTINATION ZONE		DESTINATION ADDRESS	DESTINATION DEVICE			
Kisidé-						
		(+) Add - Dates	Hadd 🗧 Delete			
		Negate				
_			_			
			The second secon			
Object : Addresses	+ (+) Add (-) Delete (3	Clone 2 Enable O Disable Move*	Highlight Unu	ised Rules Standard		

Figure 1.65: Configuring the Destination Zone

After that press **OK**, then **Commit**.

Test DNAT

Using the Outside webterm. Navigate to the public IP address of your firewall. If any webpage shows up, whether it's the WordPress site or the one below. You got DNAT working!



Figure 1.66: Verify your configuration

68 Chapter 1. Basics

Chapter 2. Security Tuneup

70 Palo Alto Firewall

2.1 Work with Applications

Learning Objectives

• Configure security policies

Prerequisites:

- Knowledge of previous labs
- SNAT for internet access
- Security Policy from Inside to Outside

Scenario: Employees can doze off and do other things that they're not supposed to do during work time. If only there was an easy application-aware next-generation firewall that can block these applications! (Hint: It's this firewall!) In this lab, we are going to add applications to the security policy to only allow specific traffic to pass through the firewall.

72 Chapter 2. Security Tuneup



```
Figure 2.1: Main scenario
```

Table 2.1: Addressing Table

Device	Configuration
Client (webterm)	eth0: 10.0.0.2/24 GW: 10.0.0.1
PaloAlto	Ethernet1/1: 10.0.0.1/24 Ethernet1/2: DHCP Management: 192.168.0.1/24
Management (webterm)	eth0: 192.168.0.2/24

Table 2.2: Zone Configuration

Zone	Interface
Inside	Ethernet1/1
Outside	Ethernet1/2

Modify Allowed Applications

🚾 x11 - TightVNC Viewer — 🗆 🗡									
B 🖬 🗈 🔳 😔 🐲 🗲	Ctrl		🔍 🔍 🔂						
🔮 BruhloAlto - Mozilla Firi	efo>	< c							_ @ ×
🊧 BruhloAlto	×	+							
€ → C @	0) 🔏 https://192.1	68.0.1/?#polici	es::vsysl::po	olicies/securit	y-rulebase	⊠ ☆		II 📽 🗉
🚺 PA-VM	DAS	SHBOARD ACC	MONITOR	POLICIES	OBJECT	S NETWORK	DEVICE	📩 Commit 🗸	৳ ∰•Q
									G ()
Security	2				1				$3 \text{ items} \rightarrow \times$
A QoS							Source		
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
Decryption	1	IntoOut	none	universal	M Inside	any	any	any	Moutside
Application Override	2	intrazone-defaul	ROME	intrazone	atiy	any	any	any	(intrazone)
Authentication	3	interzone-defauto	none	interzone	any	any	any	апу	any
C SD-WAN									
Policy Optimizer -									
New App Viewer 0	4								
Rules Without App Controls									
Unused Apps □ V V = Rule Usage									
Unused in 30 days									
Unused in 90 days 1									
Unused 1									
Object : Addresses +	Ð,	Add 🕞 Delete 🛞 C	llone 🙁 Overrid	e 🗿 Revert	🕑 Enable 🚫	Disable Move ~		Highlight Unused R	ules »
https://192.168.0.1/?# n Time	04/2	6/2022 18:35:01 Se	ssion Expire Time:	05/26/2022 1	8:38:29			Tasks Language	🛯 🛷 paloalto
	Alto	- Mozilla Firefo>	(02:24

Under **polices** > **security**, create a new security policy that allows inside to outside.

Figure 2.2: Create a Security Policy

Under the application tab, add these under applications:

- dns
- ssl
- web-browsing
- dns-over-https

These will allow only basic web browsing.

74 Chapter 2. Security Tuneup

🚾 x11 - TightVNC Viewer							-		×
🖹 🖬 🖀 🖺 📕 🔗 🕫	🔊 🗿 Ctri Ait 📴	$ \mathbf{Q} \mathbf{Q} \mathbf{Q} \mathbf{Q} $							
🔮 PA-VM - Mozilla Fire	efox							-	a ×
A-VM	× +							_	
(←) → C @	🛈 🔏 http	://192.168.0.1	1/?#policies::vsys1::	oolicies/security-ruleb	ase	… ⊠ ☆) ©	Ξ
🔷 PA-VM	DASHBOARD	ACC N	MONITOR POLICI	e objects k	NETWORK		or	• PA	Q.
								G	0
Security	0						1	Iten's	$\rightarrow \times$
H NAT					So	nte	_	-	
Security Policy Rule									
General Source Des	stination Application	n Service/UR	RL Category Actions	Usage					
Anv				0					0 items
				DEPENDS	DN				
🔲 🏢 dris									
and dis-over-https									
I II ssi									
web-browsing									
				Add To Current	Rule Add To B	xisting Rule			
								ŎК	D.C.
							_		
Object : Addresses	+ (+) Add (-) De	ete 🛞 Clone	Contract of Space	🕑 Enable 🛞 Disable	Move* (G)	PDF/CSV Highligh	Unused Rules		*
tion Lopiol Lot Login	Hime, 24/10/20/2/005	1126 Session E	apper There is set 979792	WASHY .			100 - 10 M	palo	alto
JWM 0 PA-1	VM - Mozilla Fire	fox							16:46

Figure 2.3: Set a custom application

Press **OK**, and commit the changes.

Test the Policy



On the client machine, navigate to any website, and you'll see it works:

Figure 2.4: Verify your configuration

However, you'll notice that ping will not function:



Figure 2.5: Verify Ping

You can allow Ping application under application settings and then you can verify whether you are able to Ping or not.

76 Chapter 2. Security Tuneup

2.2 Deal with Bad Actors

Learning Objectives

- Restrict certain websites
- Deal with DoS floods

Prerequisites:

- SNAT for the Internet
- Security policy for Inside to Outside
- Interface configuration
- Knowledge of previous labs

Scenario: In this lab, we will learn how to block a specific website and how to prevent script kiddies from succeeding with the infinite ping tool they downloaded from the sketchiest site you've ever seen. Kali acts like an attacker machine and we are going to attack the firewall through port Ethernet1/2. Then, we'll enable DoS Prevention in the firewall to prevent attacks.



Figure 2.6: Main scenario

Table 2.3: Addressing Table

Device	Configuration
PaloAlto-1	management: 192.168.0.1/24 Ethernet1/1: 10.0.0.1/24 Ethernet1/2: DHCP
Client (webterm)	eth0: 10.0.0.2/24 GW: 10.0.0.1 DNS: 8.8.8.8
Management (webterm)	eth0: 192.168.0.2/24
KaliLinux2019-3-1	eth0: DHCP

Table 2.4: Zone Configuration

Zone	Interfaces
Inside	Ethernet1/1
Outside	Ethernet1/2

Create a URL Category

Under **object** > **custom objects** > **URL category**, click **Add**. Click cancel on the pop-up.



Figure 2.7: Create a Custom URL Category

Here we can block 5, 6, or multiple sites. But here we will use just 1. Give it a name, then click **Add**.

x11 - TightVNC Viewer	the second se	- 🗆 X
	🏨 Cri Ali া 📴 🔍 🔍 🔍 🍭 🛛 🔂	
😜 Xav-PA - Mozilla Firef	fox	_ @ ×
🥠 Xav-PA	× +	
↔ ↔ ↔ ↔	🛈 🐔 https://192.168.0.1/?#objects::vsys1::objects/custom-objects/url-cai 🛛 💀 😭	
O PA-VM	Custom URL Category (1)	्ट्राज्यार जिन्म स्त्र≁ Q
	Name BlockedWebsites	0.0
	Description	GO
Addresses	Type URL List	0 items $\rightarrow X$
Reginne	Matches any of the following URLs. domains or host names	MATCH
B Dynamic User Groups	$Q(2items) \rightarrow X$	
Applications	SITES	
Application Groups	www.thegreattechadventure.com	
Application Filters	thegreattechadventure.com	
5 Service Groups		
Tags		
Devices		
V GlobalProtect		
HIP Objects		
External Dynamic Lists		
V 🔞 Custom Objects		
🔟 Data Patterns	Enter one entry per row. Each entry may be of the form www.example.com or it could have wildcards like www.*.com.	
Spyware	To ensure an exact entry match, use a forward slash (/) at the end of your entry. Example: xyz.com/ matches only	
UN Vulnerability	avz.com. For more info, see URL Category Exceptions	
V IX Security Profiles		
Antivirus	OK Cancel	
Anti-Spyware		
Unerability Protection		
URL Filtering		
1 P. File Blocking	HAdd In Celese Conclone @PDF/CSV	
adımın I Logout I Last Login Tim	Control (28/2022 20:10.01) Session Expline Time: 06/01/2022 20:59:44 Control (28/2022 20:10.01) Session Expline Time: 06/01/2022 20:59:44 Control (28/2022 20:10.01) Session Expline Time: 06/01/2022 20:59:44 Control (28/2022 20:10.01) Session Expline Time: 06/01/2022 20:59:44 Control (28/2022 20:10.01) Session Expline Time: 06/01/2022 20:59:44	aiksel Languare 🥠 paloalto
JWM _ 🔜 🍯 Xav-P/	A - Mozilla Firefox	08:01

Figure 2.8: Add a CustomURL Category

Enter some websites you would like to block. Here I have added a sample website (www.thegreattechadventure.com) you can also use wildcards if you want.

After you're done. Click **OK**.

Block a Website

Under **Policies > Security**. Click **Add**:



Figure 2.9: Add a security policy

x11 - Tight	VNC Viewer									- 🗆	×
🧏 🔒 😭 🗈	🖳 🖬 🖺 📕 🖅 av 💐 crit Att 🐘 🔍 🔍 🍭 🍭 🔯										
PA-VM -	Mozilla Firefox			_							_ a ×
🋷 PA-VM	☆ PA-VM × +										
$(\leftrightarrow) \rightarrow ($	C 🙆 🕕 🕄	https://192.16	8.0.1/?#p	oolicies::vsys:	. policies,	/security-rul	80%	… ⊠ ☆	1		; ≡
OPA-VM	DASH BOARD	ACC MONIT	TOR FO	LICIES OBJE	TS NET	WORK DEVICE			1 Longert	- 6	Eq. × Q
20 Seath	5									d ato	50
B NAT						Sales.			Desilinàlian		
Purcy Based	Forwarding MAMS	TĂG.S	TYPE	ZONE	ADDRESS	VSER	DEVICE	ZÓNE	ADDRES5	DEVICE	APP
C Derveden	t sofe soe	2. 22	unive/sal	PR	1.9	1.9	2.9	Mc	_ Y	- Y	- 1
Ace cation	Security Policy Rule									0	
CE Das Prate	General Source Destination	Application 5	ervice/URL C	ategory Action	s. Usage						
		Any	CE ÁDDRESS	*	any SO	⇒ URCE USER ∧		any SOURCE DEVIC	× E ~		
	D M Inside										
Policy Optimizer											
New Aug	(+)Add	(+) Add	Delate		Add	Deble		(+) Add - Delate		_	
C Rules Will	Char Charles	Negate			0.1						
									-		
To Univel	har,								UK I	Cancel	
Object Addresse	s + @Add @Delete	§ Clane		. @ Enable (S)	Disable Mov	re ~ @ PDF/CSV	Highlight Uni	used Rules View Ru	lebase as Groups		-
	Invening of the state of 1222 and the	EL Stept Exche	-::07 20 22	1997 - S. 1 1997 - S. 1997 - S. 19				E	1 35	-	baloalto
JWM _	PA-VM - Mozilla	Firefox									07:33

Under the source tab, add the Inside zone under the source zone:

Figure 2.10: Add a Source Zone

x11 - Tight	tVNC Viewer			- 🗆 X		
🤏 🖬 😭 🖪	🖺 📕 😏 🛷 🙀 Chri Alt 🛅 🔍 🍳 🔍	R. R. 🔂				
😫 PA-VM -	- Mozilla Firefox			_ @ ×		
🊧 PA-VM	× +					
$(\leftrightarrow) \rightarrow 0$	(←) → C ² û î î î https://192.168.0.1/?#policies::vsys1::policies/security-rul 80% •••• ♥ ☆ III II II					
OPA-VN	DASHBOARD ACC MON	ITOR ROLICIES OBJECTS NETWORK DEV	КЕ	id Comme- in Fire Q		
and Country				S ()		
Br NAT		farm.		Desilination		
Purcy Base	ST FORWARDING NAME TAKES	TYPE ZONE ADDRESS USER	DEVICE ZONE	ADDRESS DEVICE APP		
Turne Insp	1 Martie Advention	inniversal page and and	Mi	-1 -1 -1		
Acescation	Security Policy Rule			0		
CE Das Hals	General Source Destination Application	Service/URL Category Actions Usage		~		
ABC OTH ARYNA	select 😪	Any	any 🗸			
		DESTINATION ADDRESS	DESTINATION DEVICE			
Policy Optimic er						
New Aug	Add Deels	() Add Dalats	Add Protein			
Connect Au		Negate		OK Cancel		
Object - Address	es + @Add @Bokts @Clane	. ⊘Enable ⊙ Dianble Move∼ © PDE/ES	M THighlight Unused Rules View Rule	base as Groups		
JWM _	📕 🍯 PA-VM - Mozilla Firefox			07:33		

Under the destination tab, add the Outside zone under the destination zone:

Figure 2.11: Add a Destination Zone

Under the **Service/URL** Category tab, add the created URL category you created in the previous step.

x11 - TightVNC Viewer			- 🗆 X
<u>≞</u> ∎ 🖹 🗎 🗲 🕫) 🏨 Ctri Ait 🖭 🔍 🔍 🔍 🍭 🔯		
🔮 Xav-PA - Mozilla Fire	efox 🖗		_ @ ×
松 Xav-PA	× +		
↔ A C O	(i) 🖍 https://192.168.0.1/?#policies::vsys1::pol	icies/security-rulebase 🛛 💀 😒	III\ 🗊 📽 😑
OPA-VM	DASHBOARD ACC MONITOR POLICIES	OBJECTS NETWORK DEVICE	mmit∼) िर ¥त∙ Q
			60
Security	A A A A A A A A A A A A A A A A A A A		$2 \text{ items} \rightarrow X$
Security Policy Rule		Source	
	and the second second to the second		
General Source Dest	tination Application Service/URL Category Actions		
application-default 🗸			
SERVICE ^		URL CATEGORY ^	
		(+) Add (-) Delete	
			OR C
-			
Object : Addresses	+ (+) Add rough a concrete themate in Revent	English Ontario Move * @ PDF/CSV Highligh	t Unused Rules 🛛 🖇
https://192.168.0.1/?#	mer 04/28/2022 26:10,01 Session Explicit Time: 06/01/2022 00	59344 🗹 🕴 ≸⊟ Laster	Consulate 🦇 paloalto
JWM _ 📕 🍯 Xav-	PA - Mozilla Firefox		08:02

Figure 2.12: Assign URL Category

🗺 x11 - TightVNC Viewer		-					
19. 🖬 🗃 🗈 📕 😔 📾 🏨 Chr. Alt ы 🔍 🔍 🔍 🔍 💀							
赵 BruhloAlto - Mozilla Firefox			_ a ×				
✤ BruhloAlto × +	uhloAlto × +						
← → C û	s/security-rulebas	e … ⊠☆ III\					
PA-VM DASHBOARD ACC MONITOR POLICIES	OBJECTS NET	WORK DEVICE	ी मि× Q				
			GØ				
Security O		k	$3 \text{ items} \rightarrow X$				
Converter Deline Dela		Source	_				
Security Policy Rule							
General Source Destination Application Service/URL Category Actions Use	ige						
Action Setting	Log Setting						
Action Deny		Log at Session Start					
Send ICMP Unreachable	Log Forwarding	Log at Session End					
	Log rormanang	(to be					
Profile Setting	Other Settings	None					
Profile Type None 🗸	OoS Marking	None					
	400 1 10 10	Disable Server Response Inspection					
			ок				
	able O Disable N	AND MORE CON THE MELLING AND	35				
admini Lazout Last Lazon Timer 04/26/2022 18:35:01 Session Explicit Timer 04/26/2022 18:35:01	and O prisable is	M SE Take I Jonus and	🌇 paloalto				
IWM BruhloAlto - Mozilla Firefox			02:26				
			02.20				

Under the actions page, set the action to deny.

Figure 2.13: Set an Action to Deny

Then click **OK**.

Enable Block Pages

Under Device > Response pages .	Click on Disabled beside Application Block Page.

	🕻 Ctri Alt 🔖 🔍 🍳 🔍 🍭 🐼						
👌 BruhloAlto - Mozilla Fir	efox				- 8		
🚧 BruhloAlto	× +						
€ → C @	🛈 🔏 https://192.168.0.1/?#devic	III\ 🗉 😅 =					
🚺 PA-VM	DASHBOARD ACC MONITOR	POLICIE	S OBJECTS NETWORK		ार∽ । नि मि → Q		
					GC		
No Setup	Q				19 items \rightarrow		
🖼 High Availability	ТУРЕ	ACTION	LOCATION	NAME			
Config Audit	Antivirus / Anti-spyware Block Page		Default		4		
Password Profiles	Application Block Page	Disabled	Default				
Administrators	Captive Portal Comfort Page		Default				
Authentication Profile	Data Filtering Block Page		Default				
Authentication Sequence	File Blocking Continue Page		Default				
Suser Identification	File Blocking Block Page		Default				
👶 Data Redistribution	GlobalProtect App Help Page		Default				
Device Quarantine	GlobalProtect Portal Login Page		Default				
W Information Sources	GlobalProtect Portal Home Page		Default				
X Troubleshooting	GlobalProtect App Welcome Page		Default				
Certificates	MFA Login Page		Default				
Certificate Profile	SAMI Auth Internal Error Page		Default				
OCSP Responder	SSI Certificate Errors Notify Page		Default				
SSL/TLS Service Profile	SSI Decryption Ont-out Page	Disabled	Default				
SCEP	LIRI Filtering and Category Match Block Page	a state for a	Default				
SSL Decryption Exclusio	URL Filtering Continue and Override Page		Default				
SSH Service Profile	URI Filtering Safe Search Block Page		Default				
Nor Settings	Anti Phishing Black Page		Default				
Server Profiles SNMP Trap	Anti Phishing Continue Page		Default				
admin Logout Last Login Time	: 04/26/2022 18:35:01 Session Expire Time:	05/26/2022	18:38:29 [⊠ 🐲 Tasks	Language - 200 paloalto		
	Alto Mozilla Eirofox						

Figure 2.14: Enabling Application Block Page

x11 - TightVNC Viewer \times 🖳 🔐 😰 📗 😏 🛷 🙀 Chi Ali 🐘 🔍 🔍 🔍 🐼 😫 PA-VM - Mozilla Firefox аx × + W PA-VM <) → C @ 1 https://192.168.0.1/?#device::vsys1::device/block-pages Ξ 80% ... 🗵 🟠 111\ 🗊 🔅 OPA-VM 1 Der 30 19 tene -> > Setus . Q High Availability TYPE ACTION Antiyot / Anti-syku = Boo new at the type Carties Parts Confect Pace Config Aust Default Password Profiles Default Default Authentication Sequences Default Default Disting Pade of Auto Hera Page Default B Device Qua ortine Detault VM Information Sources In the banking Application Block Page 0 Certificate Management E Certificates Enable Application Block Page Certifunte Profile CKSP Ressender SSL/115 Service Hubb Cancel BA SCEP SSL Decryption Exclusion URL Title ingrand Enterprise france price inc. SSH Service Profile ditter temperature of av Default Response Pages Detault Lug Sattings Default E Server Profiles SNMP has Suciog Di Linal Nation THE TACACS BLUAP Kerberes paloalto 📃 🛑 PA-VM - Mozilla Firefox 07:38 IWM

Tick on the enable checkbox, then press **OK**.

Figure 2.15: Enabling Application Block Page

Make sure to commit your changes!

Test the Blocked URL

Open up Firefox on the Client machine, and try to connect to the URL you blocked. If all is right, you should see a blocked page.



Figure 2.16: Application Block Page

If you see this page, that is alright too!



Figure 2.17: Application Block Page

Set Up Kali to Be a Bad Actor

After entering into the live graphical environment and testing for internet connection. Open up the terminal.



Figure 2.18: Open up Terminal in Kali

We will be using <u>Pentmenu by GinjaChris</u> to demonstrate a flood. Run these commands to download and run the application:

```
#git clone https://github.com/GinjaChris/pentmenu
#cd pentmenu
#chmod +x pentmenu
#./pentmenu
```

90 Chapter 2. Security Tuneup



Figure 2.19: PentMenu app

Select option 2 for DoS attack.

QEMU (KaliLinux2	019.3-1) - TightVNC Viewer				-		×	
🧏 🖬 🖆 📕	중 영광 😹 Ctrl Alt 🖺 🔍 Q, 🔍 (೩ ፼						
Applications 🕶	Places 🔻 🕟 Terminal 🔫	Sat 07:56		, 1	1	1) ()) 🔻	
Applications * Places * Image: Terminal * Sat07:56 Image: Terminal * Sat07:56 Image: Terminal * Sat07:56 Image: Terminal * Sat07:56 Image: Terminal * Image: Terminal * <t< td=""></t<>								
R								

Figure 2.20: PentMenu app – Select DoS (2)

Select option 1 for ICMP Echo Flood.

QEMU (KaliLinux2	019.3-1) - TightVNC Viewer			- 🗆 X
<u>≞∎∎∎</u> II	🗲 🕾 🗿 Chi Alt 🗞 🔍 🔍	Q 🐼		
Applications 🔻	Places 🔻 🕟 Terminal 👻	Sat 07:57		⊯ 1 ≠ •0) U -
		root@kali: ~/pent	menu	600
	File Edit View Search	Terminal Help		
	Welcome to pentmenu! Please report all bug Chris/pentmenu/issues This software is only YOU are responsible f Please review the rea u/master/README.md be	ys, improvements and sugg for responsible, author or your own actions! ndme at https://raw.githu fore proceeding	estions to https://github. ised use. busercontent.com/GinjaChri	com/Ginja
	1) Recon 2) DOS 3) Extraction 4) View Readme 5) Quit Pentmenu>2	I		
	1) ICMP Echo Flood 2) ICMP Blacknurse 3) TCP SYN Flood 4) TCP ACK Flood 5) TCP RST Flood Pentmenu>1	6) TCP XMAS Flood 7) UDP Flood 8) SSL DOS 9) Slowloris 10) IPsec DOS	11) Distraction Scan 12) DNS NXDOMAIN Flood 13) Go back	
	Preparing to launch I Enter target IP/hostr	CMP Echo Flood using hpi name:	ng3	

Figure 2.21: PentMenu app – Select ICMP Echo Flood(1)



For the IP, use the IP of the interface in the outside zone. It should be in the 192.168.122.0/24 range.

Figure 2.22: PentMenu app – Enter Target IP address
Select r for random IP address.



Figure 2.23: PentMenu app – Enter r for random IP address

After about 2 seconds, press **Ctrl+C**.

Analyze the ICMP Flood

PA-VM × → C ŵ PA-VM DASH B PA-VM DASH B C	+	nttps://192 ACC M	2.168.0.1/?#mc	nitor::vsys1::mo	nitor/ses	sion-b				1				
→ C ŵ PA-VM DASHB C Threat. C DAL Filtering WildFire Submissions C Data Filtering Data Filtering C Data Filtering C Data Filtering	1) 🔏 H	nttps://192 ACC M	2.168.0.1/?#mc	nitor::vsys1::ma	nitor/ses	sion-b				1				_
→ C ŵ PA-VM DASHB R: Iráthc ⓒ Theat. ⓒ URL Fitering WildFire Submissions ⓒ Juan Fitering ♥ UNL Fitering ♥ UNL Fitering	 A A	ACC M	2.168.0.1/?#mc	nitor::vsysl::mo	nitor/ses	sion-h								
DA-VM DASHB	DARD	ACC				sion c	IT	80%	☑ ☆	J		101		5
Eig Trathc Filters Threat START START WildFire Submissions Eig 04/23 01/04/10			and the second	IES OBJECTS	NETWORK	¢ D	EVICE			4	g Comeu		1 6	₽ ∎ ~
Threat Filtering START TIME WildFire Submissions Ult Altering														5
WildFire Submissions URL Filtering URL Filte	The second	1	т	Т	Teles	Tes	T	1		→ X 🕑	1 Torrest		Terrere	
Data Filtering 04/23 01:04:16	ZONE	TO ZONE	SOURCE	DESTINATION	PORT	PORT	PRO	APPLICATI	RULE	INGRESS I/F	EGR	BYTES	SYSTEM	c
	Quts	Outside	89.66,199.34	192.168.122.29	62213	27648	i	ong	Intrazone-default	etheri	ether,	60	vsys1	D
ClobalDestact	Outs	Outside	210.217.255.126	192.168.122.29	62213	29184	1	<u>prië</u>	ntrazone-default	etnem	ether	60	vsys1	\geq
C IP-Tag C 04/23 01:04:16 01:04:16	Ouis	Outside	57.100.45.117	192.168.122.29	62213	11520	í.	parts	mbrazone-default	athern	ether	60	vsys1	Þ
Decryption 04/23 01.04:16	Outs.,	Outside	176 203 8.82	192.168.122.29	62213	32768	1	taul g	intrazone-default	ebiein	sther	60	vsys1	D
Configuration	Outs	Outside	46.118.185.136	192168.122.29	62213	23296	i.	one	intrazone-default	ethem	ether	60	vsys1	D
System E 04/23	Öuls	Outside	209.187.54.219	192.168.122.29	62213	513	1	phile	intrazone-defoult	etherna.	ether	60	vsys1	D
Authentication	Outs	Outside	117.46.147.166	192 166 122 29	62213	9216	i.	ONLE	intrazone-default	ethern	ether	60	vsys1	Þ
Packet Capture E 04/23 01/04-16	Ouis	Outside	32 206 162 166	192.168.122.29	62223	50/32	L	ching	inbazone-default	stiem	ether	Ш	vsys1	Þ
App Scope	Ouls	Outside	64.91.241.46	192.168.122.29	62213	2818	1	plag	inbrazone-default	ettern	ether	60	vsys1	D
Change Monitor	Quis	Outside	131.24.226.202	192.168.122.29	62213	ō144	I.	ping.	ntrazone-defourt	ethern	ether	60	vsys1	Ð
Threat Map E 04/23 01:04:16	Quts	Outside	59,118,203,191	192.168.122.29	62213	48640	£	prie.	Intrazone-default	etheriu	ether,	60	vsys1	Þ
C Traffic Map. 04/23 01:04:16	Quis	Outside	216.75.47.244	192.168.122.29	62213	4608	1	pine.	ntrazone-defourt	ethern	ether	60	vsys1	\geq
Botnet 04/23 01:04:16	Ouß	Quiside	46.251.113.2	192.868.122.29	62213	46080	1	puig	intrazone-default	ethern	ether	60	vsys1	D
PDF Reports E 04/23 Manage PDF Summary 01:04:16	Outs	Outside	75.229.120.68	192.168.122.29	62213	64512	1	ong	intrazone-default	etherns	ether	60	vsys1	Þ
Luser Activity Report	Öuts	Outside	174.135.54.54	192.168.122.29	62213	14592	i.	pine:	intrazone-default	ethem	ether	60	vsys1	Þ
Report Groups 04/23 01:04:16	Öuts	Outside	205.4.105.59	192166.122.29	62213	1/18/18	1	pine	intrazone-defourt	ethern	ether	60	vsys1	X
Manage Custom Reports 04/23 01:04:16	Öuts	Outside	168,151,230,236	192.168.122.29	62213	37868	1	pine:	intrazono-default	ethem	ether	60	vsys1	
Reports OPF/CS	v		1						Dame	1 of 1		Displa	wing 1 - 1	26 -

Back on the Management machine, go under **Monitor** > **Session browser**.

Figure 2.24: Verify session logs

As you can see, there are many entries here for ping. We want to prevent floods like these.

Create a DoS Protection Profile

🚾 x11 - TightVNC Viewer									-	
	Ctrl	Alt 📬 '		*						
😢 BruhloAlto - Mozilla Fir	efo:	ĸ			_					_ @ ×
🊧 BruhloAlto	×	+								
€ → C @	0	🕽 🔏 https	://192.168.0.1/?	#objects:	vsys1::objects/sec	urity-profiles/	dos-pi •••	⊠ ☆	1015	□ 🛎 =
OPA-VM	DA	SHBOARD	АСС МО	NITOR	POLICIES OB.	ECTS NET	WORK DE	/ICE	Commit 🛩	৳ E₁+Q
Est Application Filters										G ()
🔀 Services	Q	T.	-							$0 \text{ items} \rightarrow \times$
Service Groups							Flood Protection			Resources Protection
Devices		NAME	LOCATION	TYPE	SYN FLOOD	UDPFLOOD	ICMP FLOOD	ICMPV6	OTHER IP	SESSIONS
 HIP Objects HIP Profiles External Dynamic Lists Custom Objects Data Patterns Spyware Vulnerability URL Category Security Profiles Antivirus Anti-Spyware Vulnerability Protection URL Filtering File Blocking MildFire Analysis Data Filtering So SCTP Protection Security Profile Groups 	•	Add	ete 🛞 Clans 🕲	PDF/CSV	*					
admin Logout Last Login Time	: 04/2	6/2022 18:3	5:01 Session Exp	ire Time: 05	/26/2022 18:38:29 [sks Language	🊧 paloalto
JWM _ 📕 🍯 Bruhlo/	Alto	- Mozilla I	Firefox							02:33
	D (

Under **Objects > Security Profiles > DoS Protection**. Click Add.

Figure 2.25: Create a DoS Protection

Set the type to Classified and under Flood protection, click the checkbox on the **SYN Flood**, **UDP Flood**, and **ICMP Flood** tabs.

x11 - TightVNC Viewer						-	
🧏 🖬 😭 🗓 📕 😔 🗑	Ctrl Alt	ⓑ Q, Q, Q, Q, <mark>ऄ</mark>					
😫 BruhloAlto - Mozilla Fir	refox	k					_ @ ×
🊧 BruhloAlto	× +						
← → C ŵ	(i) 🔏 I	https:// 192.168.0.1 /?#object	s::vsys1::objects/security	-profiles/dos-p	⊠ ☆	IIIN	
🔷 PA-VM	DASHBOA	ARD ACC MONITOR	POLICIES OBJECTS	NETWORK DEV		Econor >	ि म्म⊀ ्
E ¹⁷ Application Filters	Q.						$\begin{array}{c} \mathbb{G} \ \textcircled{0} \\ \text{Oltems} \ \rightarrow \times \end{array}$
Services		DoS Protection Profile		0			Resources Protection
	I NAME	Name DosProt Description Type Aggregate Flood Protection Resource SYN Flood UDP Flood SYN Flood Action Alarm Rate (connections/s) Activate Rate (connections/s) Max Rate (connections/s) Block Duration (s)	e Classified es Protection ICMP Flood ICMPv6 Floo Random Early Drop 10000 10000 40000 300	d Other IP Flood	FLOOD	OTHER IP FLOOD	SESSIONS
SCTP Protection	() Add	- Delase () Clane () PDF/CSV		_		_	
	Alto Mo:	zilla Eirofox	572672022 LH:3529			ne i faninnse	
		2111d T II PTOX					02:55

Figure 2.26: SYN Flood Protection

After that, click **OK**.

Apply the DoS Protection Profile

Under **Policies > Dos Protection**. Click **Add**.

🚾 x11 - TightVNC Viewer								– 🗆 🗙
B 🖬 🗈 📗 😔 🕬	🙀 Ctrl	. Alt 🔤 €	. ् ् ्					
😢 BruhloAlto - Mozilla F	irefo:	x						- 7
🊧 BruhloAlto	×	+						
(←) → C û	0	D 🔏 https://	192.168.0.1/?#policie	es::vsys1::policies/d	os-rulebase	••• (9 th	III\ 🗊 🔹 🗏
O PA-VM		thun a time	Lab Links	Ind Little .	3) . ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
	DA	ASHBOARD	ACC MONITOR	POLICIES	DBJECTS NE	ETWORK DEVIC		
	0							G ()
→ NAT					Source		Dest	ination
🐣 Qo5		NAME	TAGS	ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS
Application Override Authentication DoS Protection SD-WAN Policy Optimizer Rule Usage Unused in 30 days Unused in 90 days Unused	0000							
Object : Addresses	⊢ ⊕. ne: 04/2 oAlto	Add 😔 Delete 26/2022 18;35:0 - Mozilla Fir	G Clone Enable Session Expire Time: refox	○ Disable - Move Y 05/26/2022 18:38:29	PDF/CSV [Highlight Unused R	ules 🗌 View Rulebase 2 👔 🏂 Täsks Larigu	as Groups »

Figure 2.27: Add a DoS Protection Rule

🗱 x11 - TightVNC Viewer									- 🗆	×
🐴 🖬 🛍 🖺 😔 🤉	🔊 😹 Ctri Alt 🖣		Q 🐼							
😫 PA-VM - Mozilla Fire	efox								_	_ @ ×
A-VM	× +									
← → ♂ @	🛈 🔏 h	ttps://192.168	1.0.1/?#polici	ies::vsys1::polic	ies/dos-rul	ebas 80%	*** 🔝			Ξ
O PA-VM	DASH BOARD	ACC MONIT	DR FOLICIE	S OBJECTS	NETWORK	DEVICE		i Con	mir- îr j	±~ Q
										50
Brinat -				form		þ	estinàtion		10	*** - } ×.
Ref.	HAME	TÁGS	ZONE (INTERFAS	CE ADDRESS	USER	ZONE/WTERFAR	E ADDRESS	SERVICE	ACTION	AiGG
e hanvailae	1 Derive		A see							
# According Swands		Def Bule	_	_	_	_	0			_
Dus Protection		DOS Rule					U			
68 541 4VAN		General So	urce Destinati	ion Option/Prote	ction		_			
		Type Zo	one 🗸	Any		any v				
		Outside		SOURCE ADDRE		SOURCE USER				
ū.										
Policy Optimizer -										
Unuesd to 30 days		⊕Add ⊖ D≊	'ete		2	€Add C Deleta				
Unued to 90 days				Negate						
						OK C	Cancel			
							_			
Dbject : Addresses +	Delete 🛞	Clone (@) Enable	Disable Mp	DVE PDF/CSV	- Highlight U	nused Rules View Ru	lebase as Groups	Reset Rule Hit Cou	nter "	aloalto
	VM - Mozilla F	irefox							17 P	08.13
1 ** IVI -	visi sinozilid i	I CIUX								00.15

Under the Source tab, add the Outside zone.

Figure 2.28: Add the Source Zone

Under the Destination tab, add the Inside zone.

🚾 x11 - TightVNC Viewer									- 0	x c
🖹 🖬 🗊 🔳 😏 🛷	😭 Ctrl Alt 🖣		Q 🐼							
😫 PA-VM - Mozilla Firef	ох									_ @ ×
🊧 PA-VM	× +									
← → ⊂ ŵ	🛈 🔏 ht	ttps://192.16	8.0.1/?#policies	evsys1:p	plicies/dos-rule	ba: 80%	🖾 🛉			e =
O PA-VM								1 Long	mit - 1	En v Q
										50
Brivat Cal				Source.		D	etheilten			. dem → ×
Recy Bound Forwarding	MAME .	TAGS	ZONE/INTERFACE	ADDRESS	USER	ZONE/ WTERFAE	E ADDRESS	SERVICE	ACTION-	Also:
the hand incouchion			H MORE							
Acustation Diverside		DoS Rule					0			
Dus Protection		General S	ource Destination	Option/Pr	otection					
		Type	Zone	1						
		ZONE ^			DESTINATION A	ADDRESS A				
		Inside								
Policy Optimizer -		1.00								
Unuesd to 30 days		⊕Add ⊡ 0	siais		⊕Add - Delete					
Covered to 90 days					Negate					
				k		Cotto Co	Cancel			
Object: Addresses + 🛞	Add 🕘 Delete 🍥	Clone Ettabl	e 🕤 Disable Move	· DPDF/E	SV 🗌 Highlight Unu	ised Rulies 🗌 View Ru	lebase as Groups	Reset Rule Hir Cour	nter %	-
and Encode Environmental		Gessio 1 Excine Th	-m05-10(1001.000)						-5	paloalto
JWM _ 📕 🚺 PA-VI	M - Mozilla F	irefox								08:14

Figure 2.29: Add the Destination Zone

Under the **Option/Protection** tab, configure these settings:

Table 2.5: DoS Rule Protection Configuration

Parameter	Value
Action	Protect
Schedule	None
Log Forwarding	None
Aggregate	None
Classified	Tick this box
Profile	The name of the one you created
Address	source-IP-only



Figure 2.30: DoS Rule – Option/Policies

Then click **OK**.

Create a Zone Protection Profile

🚾 x11 - TightVNC Viewer									-		×	
🐴 🖬 😰 📕 😏 🛷 🗑	Ctrl	Att 📴 🕀		æ								
😫 BruhloAlto - Mozilla Fir	refo:	<								-	а×	
🚧 BruhloAlto	×	+										
(←) → C ŵ	0	🕽 🔏 https://	/192.168.0.1/?	#network::vsy	/sl::network/ne	twork-profil	es/zone •		IIIN	•	н	
🚺 PA-VM	D4	SHBOARD	АСС МС		DLICIES OB	JECTS N	IETWORK E	DEVICE	Commit ~	D 🕀	r Q	
				Ø						G		
VI ANS	Q									0 items	$\rightarrow \times$	
Ca Virtual Wires					Flood Protection	¥.		R	econnaissance Pro	issance Protection		
Virtual Routers IPSec Tunnels		NAME	SYN FLOOD	UDPFLOOD	ICMP FLOOD	ICMPV6 FLOOD	OTHER IP FLOOD	TCP PORT SCAN	UDP PORT SCAN	HOST SV	WEEP	
 DHCP DNS Proxy GlobalProtect Portals Gateways MDM Clientless App Groups QoS LLDP GlobalProtect IPSec Crytio GlobalProtect IPSec Crytio IKE Crypto IKE Crypto Monitor Interface Mgmt QoS Profile LLDP Profile 	-1 	Add Defet	e 🔄 Clane 🔘 01 Session Expi	PDF/CSV re Time: 05/26/2	022 18:38:29			⊠ žΞ Tas	ks Language	# palo	alto	
	Alto	- Mozilla Fi	refox								02.37	
	AILO		I EIUX								02:57	

Under **Network > Network Profiles > Zone Protection**. Click **Add**.

Figure 2.31: Add a Zone Protection



Under the flood protection tab, tick **SYN**, **ICMP**, and **UDP**.

Figure 2.32: Add a Flood Protection

Under the Reconnaissance Protection tab, tick enables on all boxes, and change the action to block.

🚾 x11 - TightVNC Viewer						-	
🌯 🔒 😭 🗈 📕 😏 🕫 🙀 Ctri. Att		₽					
💊 PA-VM - Mozilla Firefox							_ a ×
🥐 PA-VM 🗙 🕇							
<>> ℃ ŵ 0 €	https://192.168.0.1	/?#network::vsys1::network/	network-pr	80%	⊠ ☆	10X	🗉 📽 🗉
O PA-VM	ACC MONITOR	FOLICIES OBJECTS NET	ORK DEV	NC E		1 Limmit -	6 BrQ
							30
							zitem 🦂 😥
By VLANS	William W	Proprietore Recipiente de la constant	CHIRULELOOD	citiis pap si		Russianssanse Protekt	HI NAST OVERS
(D) Vital Roaders	the Deck	antiboo annercouo	CMPAG FLOOD	Sames & Fr		DIOCK	OIDCK.
20 Illies Tuntus Zone Prote	ection Profile				0		
BHCF	ame Prot						
DNS IV Law Description	ation	The second states		terret breating a			
Flood Prate	ection Reconnaissance I	Protection Packet Based Attack Pro	ection Prot	ocol Protection	Ethernet SGT Protectic		
Gillewar: SCAN	ENABLE	ACTION		INTERVAL (SEC)	THRESHOLD (EVENTS)		
MBM TCP Port Scan		DIOCK		2	100		
B Dienbest Ace orque		block		10	100		
Geb UDP Port Scan		Block	Ŷ	2	100		
- De Nalaco Nalies				- 1-	0 litems → ×		
Source	ADDRESS EXCLUSION		ADDRESS TYP	PE IP	ADDRESS(ES)		
TT IKE Gale wave							
VY INE Cryata							
Non La							
Se Interface Mend							
Auf Nalas							
ELLIP Insta					OF Cancel		
Sto WAN Merine Photos							
@Att @Dekts (Clane PDF/CSV	and the second s					
Land Date (1997) 1997 (1997) 1997 (1997) 1997	Constant Backer Thread C	23(2020			- E	9E	- paloalto
JWM _ 📕 🍯 PA-VM - Mozilla	Firefox						08:20

Figure 2.33: Set UDP Port Scan

Under the Packet Based Attack Protection tab, under the IP drop subtab, tick on **Spoofed IP address** and **Strict IP Address** Check.



Figure 2.34: Enable Spoof IP address and Strict Address Check

Under the Packet Based Attack Protection tab, under the TCP drop subtab, tick on **TCP SYN with Data** and **TCP SYNACK with Data**.

📸 x11 - TightVNC Viewer		- 🗆 X
<u>≒</u> ∎∎∎∎ 9 ⊛ ≝	🕻 Chi Ali 🛍 🔍 🔍 🍭 🍭 🔂	
📦 PA-VM - Mozilla Firefo:	x	_ a ×
A-VM	x +	
0		
 	(i) 🔓 https://192.168.0.1/?#network::vsys1::network/network-p	
OPA-VM		Limmie- E Eg+ D,
		50
📾 interface: 🔹 🔍 _		sitem 🛶 😥
PR Zapes	The Painter	Recomulation Profession
Eg Vitua Wie:	AME SYN FLOOD UDP FLOOD ICMP FLOOD ICMP FLOOD ICMPV4 FLOOD OTHER IP FLOOD TOP PORT SCAN	UDP PORT SCALL HOST SWEEP
🔘 Visual Busiers 🔹 💻	Zone Protection Profile (2)	DIOCK BROCK
- Of GRE fundes	Name ZooeDrot	
E DHCP	Description	
- CA Georgeout	Flood Protection Reconnaissance Protection Packet Based Attack Protection Protocol Protection Ethernet SGT Protectio	
C Purtate		
Gale way:		
Chenters Acus	Mismatched overlapping TCP segment Selft Handthale	
Thenkess Ass ansus	TCP SYN with Data	
an Gab	Z TCP SYNACK with Data	
CONTRACT IN Day	Reject Non-SYN TCP global	
Ar a confusion (Pares	Asymmetric Path global	
11 18± trake way =	Strip TCP Options	
M Sec Civilia a	TCP Timestamp	
(A IKE Chirala +	TCP Fast Open	
The Montes and the second seco	Multipath TCP (MPTCP) Options global	
Zane Protection		
def Nalis	OK Carrel	
LLLIP Plafile		
BFU Plaffie		
100 DE WANY INDUITING FROME		
(E) HE	d Conte Chine Chine Chine Conternation	
and Direct Divide and a	Sector Control	aloalto
JWM _ 🗧 🌜 PA-VM	- Mozilla Firefox	08:24

Figure 2.35: Enable TCP SYN with Data

Under the Packet Based Attack Protection tab, under the ICMP drop subtab, tick on **ICMP Ping ID 0**, **ICMP Fragment**, and **ICMP Large Packet(>1024)**.



Figure 2.36: Enable ICMP Ping ID 0, ICMP Fragment

Then click **OK**.

Apply a Zone Protection Profile

Under **Network > Zones**. Click on the Outside Zone.



Figure 2.37: Create an Outside zone



Under the Zone Protection category, select the profile you just created.

Figure 2.38: Enable Zone Protection under Outside Zone

Click OK.

Don't forget to commit your changes!

Test the DoS Protection

Run Pentmenu again using the previous options, then **Ctrl+C** after 3 seconds.



Figure 2.39: Running PentMenu

Under **Monitor** > **Logs** > **Threat**. You should see an entry for an ICMP flood.

PA-VM - Mozilia F	refo	<						_			-	8
PA-VM		× +										
€ → @ @		🛈 🔒 htt	ps:// 192 .	168.0.1/#monitor::v	iys1::mór	tor/logs/	threat	80% **	· 🖂 🕁	ÌIIV		=
PA-VM	DÁ	SHBOARD A	10 MB	NITOR POLICIES	OILLECTS	NETWORK	bruce				1 20 120	+ Q
			-							Ma	nat vit	3 0
lines	Q.,										→×⊕∎	0
Thesis		RECEIVE THAT	TYPE	THREAT ID/NAME	FROM	TOZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	
With the Submission	10	04/23/02522	Texat	ICM/Hald	Cuhaie	Cuman	0840	[second days	10000	anoa	- Contraction	-
THE MAN	10	MICHAEL MARK	Texal	high Plan	D.mitt	Change.	5000-			10/200		
CostaPhysict	10	(14/23/02/44/6/1	Text	(CM/Hald	Cubilit	Ch. Harris	0000			anat		
C IF Tag	10	New York Street, Stree	Treal	ICMP Fland	D.mile	Dame:	-0000			1000		
Dereption	10	minimater-	TENA	TOMPRIME	O.mite	Links	000.0			HEOD .		
familimpetion	1	Sections.	Titlet	-ICMP Frank	Double	Desite	3000			NOD O		
System	60	-	These	T.M. Front	(Tablete	11000				-		
Alarm	1	salemater.	Trees	and an internal	10.0.00	1000	-1080			hanna		
United	62	and produced in	These	TOMPTONIA .		1000				(FRAME)		
and Casing	10	01011123401	Red	12477102	Chillin	CLINIC	-0000			Annu.		
to have	0	10121022904	(TIDE)	score root	Chesan	Channe	0000			àuna		11
a Charge Monitor	0	01021922049	final	123477007	DALLE.	Over	-2000			ámu.		
Thread Mulder	D	UNUINT SHIT	fixes.	score fund	Chesan	Change	0000			daman.		
Protivors Incolari	10	OF GENERAL	These	contract (see)	Date	Change	-0.00.0					
Traffic Noe	10	-increased-	-	- Chaptering	Outside	Oump	-0000			0000		
Reprint -	12	04/2101098	Dant	Charlense	0	0	-3000			0.000		
DF Raports	ED-	04/23010104	-	ACM/Print	0	- Ourseller	-3000			0000		
Manage FDF Summary	EQ.	04/22010124	Dani	Child David	Openant	Oumani	-0000			0000		
Sal's Application Lisage	10	04/230104.04	-	Total Plant.	Overhig	Oump	-0000			0000		
Report Groups	-	or the second se	-		- 1.0	1000						
A Constant	_	11.11 F	Resol	ve hostname Hishilshi P	olicy Actions				Displaying	logs 1 - 20 20	v per page D	ESC .
- Harris I Link Lagor Th	- 2423	CHES 0036/44 1	in the second	Tere diversional dealers					100	E THE L	W pale	oalto

Figure 2.40: Verify logs

2.3 Block Files and Viruses

Learning Objectives

- Block specific file types
- Explore and "apply" advanced firewall features

Prerequisites:

- SNAT for the Internet
- Security policy for Inside to Outside
- Interface configuration
- Enable block pages
- Knowledge of previous labs

Scenario: Here we will test out the file blocking, anti-malware, spyware, and spam features of Palo Alto. Sometimes we should block clients from downloading certain file types, and on top of that, implement some sort of antivirus and antispyware solution. We'll also be "testing" wildfire. A feature that thwarts new exploits from happening.



Figure 2.41: Main scenario

Table 2.6: Addressing Table

Device	Configuration
PaloAlto-1	management: 192.168.0.1/24 Ethernet1/1: 10.0.0.1/24 Ethernet1/2: DHCP
Client (webterm)	eth0: 10.0.0.2/24 GW: 10.0.0.1 DNS: 8.8.8.8
Management (webterm)	eth0: 192.168.0.2/24

Table 2.7: Zone Configuration

Zone	Interface
Inside	Ethernet1/1
Outside	Ethernet1/2

Create an Antivirus Profile

) BruhloAlto - Mozilla Fir	efo:	x												- 6
🊧 BruhloAlto	×	+												
\leftrightarrow \rightarrow C \textcircled{a}	0	D 🔏 ht	tps:// 192	.168.0.1/	?#object	s::vsysl	objects	/security	-profiles,	/antivir	***	⊠ ☆	luv	
🚺 PA-VM	D	ASHBOAI	RD A	CC M	ONITOR	POLI	CIES	OBJECT	s ne	TWORK	DEV		↓ Commit ∨	ि ⊬ि≁ (
En Application Filters	Q													G(1item)→
Service Groups Tags					¥.	Dec	oders		Appl Exce	ication ptions	WildFire	Inline ML		
Devices GlobalProtect PHP Objects		NAME	LOCA	PACKET CAPTU	PROT	SIGNA ACTIO	WILD SIGNA ACTIO	WILD INLINE ML ACTIO	APPLI	ACTIO	MODEL	ACTIO SETTI	SIGNATURE	WILDFIRE INLINE ML EXCEPTIONS
HIP Profiles External Dynamic Lists Custom Objects		default	Predefi		http	default (reset- both)	default (reset- both)	default (reset- both)			Windo Execut	enable (inherit per- protocol actions)	0	0
Data Patterns					http2	default (reset- both)	default (reset- both)	default (reset- both)			Power Script 1	enable (inherit per- protocol actions)		
Security Profiles Antivirus Anti-Spyware	4				smtp	default (alert)	default (alert)	default (alert)			Power Script 2	enable (inherit per- protocol actions)		
 Wulnerability Protection URL Filtering File Blocking 					imap	default (alert)	default (alert)	default (alert)			Execut Linked Format	enable (inherit per- protocol actions)		
₩ildFire Analysis ᠿ Data Filtering Œ DoS Protection					рор3	default (alert)	default (alert)	default (alert)			MSOffi	enable (inherit per- protocol actions)		
SCTP Protection					ftp	default (reset- both)	default (reset- both)	default (reset- both)						
Security Profile Groups	Ð	Add (=)	Delete 📀	Clone	PDF/CSV	/ Th	reat Preve	ntion Licer	se require	d for anti-	virus anti-	sovware a	nd vulnerability n	protection to func

Under **Objects > Security Profiles > Antivirus**. Click on default, then **Clone**.

Figure 2.42: Creating an Antivirus Profile

Click on **OK** for the next window.

🚾 x11 - TightVNC Viewer										- 0	×
🖹 🖬 🖆 📗 😏 🖘 🗉	Ctrl Alt	Q Q @ Q E	2								
😢 BruhloAlto - Mozilla Fir	refox	k								-	а×
🊧 BruhloAlto	× +										
€ → C û	🛈 🙇 http	s://192.168.0.1/?#	≠objects∷vsys]	L::objects/s	ecurity-profile	es/antivir	•••	⊠ ☆	10		Ξ
🚺 PA-VM		ACC MO	NITOR POL	LICIES		NETWORK	DEV		↓ Commit ~	के कि	, Q
En Application Filters	0									1 item	
Services			De	coders	A) Ex	oplication sceptions	WildFire	Intine ML			
Devices GlobalProtect HIP Objects		Clone			WILD	() DEL	ACTIO SETTI	SIGNATURE	WILD FIRE INLINE ML EXCEPTION	NS
 HIP Profiles External Dynamic Lists Custom Objects Data Patterns Spyware Vulnerability URL Category Security Profiles 	riefault	Selected Objects	N A ME default				ert1	enable (inherit per- protocol actions) enable (inherit per- protocol actions) enable (inherit	0	0	
Antivirus Anti-Spyware Vulnerability Protection URL Filtering File Blocking WildFire Analysis			Error out on fir	rst detected er	OK	Cancel	ed hat	per- protocol actions) enable (inherit per- protocol actions) enable			
Data Filtering Deta Filtering Deta Protection Mobile Network Protect			(alert)	(alert) (alert)		inacini	(inherit per- protocol actions)			
SCTP Protection	⊕ Add	lass (© Clone (D) F	(reset- both) PDF/CSV Th	(reset- both)	reset- ooth) on License requ	fired for artiv	irus, anti-	spyware, a	nd vulnerability p	rotection to fu	inction.
https://192.168.0.1/?# ******	a 04/26/2022 18	35:01 Session Explin	e Time: 05/26/28	22 18,38,29			ſ		Liske I Language	🦏 palo	alto
JWM _ 📕 🍯 Bruhlo,	Alto - Mozilla	Firefox								(02:41

Figure 2.43: Cloning the Antivirus profile

Control Contro Control Control Control Control Control Control Control Control C	🚾 x11 - TightVNC Viewer														- □ :
Bruhoadto - MOZILE FILETOX +		Ctrl	I Att 🐴	€ Q	@ @ E		_								
	Brunioalto - Mozilia Fir Maruhioalto	rero:	× +	_	k	-	_	_	_	_	_	_	_	_	_ 0
C PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE Convert C C C C C C C C C C C C C C C C C C C			0.111			(- T.)		15.4.4		191	1			1 1	
Image: Control of the stand of the stan	E - C W	6	U 🜇 nttp	s://192.1	168.0.1/?#	FODJECTS	:::vsys1::	objects/	security	-pronies,	antivi	***	© ₩		
Application Filters 2 terms Services 2 terms Test Decoders Decoders Catalafrotect Image: Catalafrotect Image: Catalafrotect Image: Catalafrotect Image: Catalafrotect Image: C	🚺 PA-VM	D	ASHBOARD	D AC	с мо	NITOR	POLIC	CIES	OBJECT	5 NE	TWORK	DEV		≟ Commit ∨	। कि स्तिर (
Services Services Tas Devices Devices Devices Devices HIP Objects HIP Objects HIP Objects Bateman Data Pattems Data Pattems Services Services WildFire Inline ML Actin Actin Actin Services Bate Pattems Sectoral Dynamic Lists Sectoral Dynamic Lists Sectoral Dynamic Lists Sector Notifier Data Pattems Sector Notifier Data Pattems Sector Notifier Of Hitp Orders Sector Notifier Mulnerability Profiles Mulnerability P	Application Filters	Q													G (2 items →
• Wilds • Excertion • Wilds • Excertion • Wilds	X Services Service Groups Tags						Dec	oders		Appl Exce	ication ptions	WildFire	Inline ML		
I HIP Drofiles I HIP Drofiles I Lipport	Contract Co		NAME	LOCA	PACKET CAPTU	PROT	SIGN ACTI	WILD SIGN ACTI	WILD INLINE ML ACTI	APPLI	ACTI	MODEL	ACTI SETTI	SIGNATURE	WILDFIRE INLINE ML EXCEPTIONS
						ttp smb	default (reset- both) default (reset- both)	default (reset- both) default (reset- both)	detault (reset- both) default (reset- both)					Lang of South	The second second
 Security Profiles Anti-Spyware Anti-Spyware Multi-spiware Wulnerability Protection File Blocking Multi-Fire Analysis Data Filtering File Blocking Multi-Fire Analysis Data Filtering Script 1 Anti-Spyware Anti-Spyware Anti-Spyware Multi-Spiware Multi-Spice Anti-Spymare <	Spyware Vulnerability Ø URL Category	-	default-1			http	default (reset- both)	default (reset- both)	default (reset- both)			Windo Execut	enable (inherit per- protocol actions)	0	0
Image: Security Profile Groups	Security Profiles Antivirus Anti-Spyware Multerability Protection					http2	default (reset- both)	default (reset- both)	default (reset- both)			Power Script 1	enable (inherit per- protocol actions)		
	WildFile Analysis					smtp	default (alert)	default (alert)	default (alert)			Power Script 2	enable (inherit per- protocol actions)		
SCTP Protection pop3 default default MSOff enable	안 Data Filtering (任 DoS Protection ** Mobile Network Protect					imap	default (alert)	default (alert)	default (alert)			Execut Linked Format	enable (inherit per- protocol actions)		
→ Add → Delete Image: Clone Image: PDF/CSV Threat Prevention License required for antivirus, anti-spyware, and vulnerability protection to function admin admin Logout Last Login Time: 04/26/2022 18:35:01 Session Expire Time: 05/26/2022 18:38:29 Image: Marguage Image: Marguage Image: Marguage	SCTP Protection					pop3	default	default	default			MSOff	enable /inherit		
admin Logout Last Login Time: 04/26/2022 18;35:01 Session Expire Time: 05/26/2022 18:38:29 🗹 🏂 Tasks Language 🛷 paloalt	Security Profile croups	\oplus	Add 🗇 De	elete 🔞	Clone 🔘 F	PDF/CSV	Thr	eat Preven	tion Licen	nse require	ed for ant	ivirus, anti-	-spyware,	and vulnerability	protection to funct
	admin Logout Last Login Time	: 04/2	26/2022 18:	35:01 Se	ession Expir	e Time: 0!	5/26/202:	2 18:38:29					⊠∣≋	Tasks Langua	👷 🥠 paloalt

Select the new profile it clones (should be something like default-1).

Figure 2.44: Verify the Antivirus profile

x11 - TightVNC	C Viewer				– 🗆 X
- <u>-</u>	📕 😏 🔊 🏨 Ctri Alt 🖷	€, Q, @, Q, 🔂			
🟮 BruhloAlto	- Mozilla Firefox				_ @ ×
🦇 BruhloAlto	× +				
(+) d	∂ (i) ∂ http	ps://192.168.0.1/?#objects::vs	/s1::objects/security-profiles/antivi	⊠ ☆	
0					
OPA-VM	Antivirus Profile				
	Name AV2				50
En Application	F Description				2 items $\rightarrow \times$
Services	Action Signature Except	tions WildFire Inline ML			
Tags	Enable Packet Capture				
Devices	Decoders				WILDFIRE
GlobalProte	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE MLACTION	INLINE ML EXCEPTIONS
HIP Pro	n http	default (reset-both)	default (reset-both)	default (reset-both)	
External Dy	http2	default (reset-both)	default (reset-both)	default (reset-both)	
V 🕞 Custom Obj	le smtp	default (alert)	default (alert)	default (alert)	
🔟 Data Pa	imap	default (alert)	default (alert)	default (alert)	
D Spywan	pop3	default (alert)	default (alert)	default (alert)	0
C URL Cat	ftp	default (reset-both)	default (reset-both)	default (reset-both)	
V 🛞 Security Pro	smb	default (reset-both)	default (reset-both)	default (reset-both)	
	Application Exceptions				
Anti-Spi	(Q($0 \text{ items} \rightarrow 2$	×
URL Fill	APPLICATION		ACTION		
File Blo	d				
WildFin	e				
Data Fill					
Mobile 1	Add Delete				
SCTP P	n				-
Security Pro	4			OK	1 American land
http://100.100	0.1/2#			Cance	maloalto:
nttps://192.168	.0.1//#				1 Perodico
JWM _	🗧 🗧 BruhloAlto - Mozilla	a Firefox			02:43

Rename the profile, and tick the option for packet capture.

Figure 2.45: Enable Packet Captures under Antivirus Profile

Then press **OK**.

Create an Anti-Spyware Profile

🚾 x11 - TightVNC Viewer									- 🗆 ×
- Ricuble Alte - Mezilla Fil	Ctrl	Alt Ba V	<u>य्य</u> ख् ज्ञ	_			_	_	
	ero	х. 	4	_	_	_	_	_	- 8
W BrunioAito	~	Ţ							
←)→ C @		D 陷 https:	//192.168.0.1/?#o	bjects::vsysl::o	bjects/security-pi	rofiles/anti-s	… ⊠ ☆	liiv	
🚺 PA-VM	D/	ASHBOARD	ACC MON	TOR POLICI	ES OBJECTS	NETWORK	DEVICE	≟ Commit ∨	î ⊕r√Q
ET Application Filters	Q								G (2 2 items →)
X Services Service Groups Tags		NAME	LOCATION	COUNT	POLICYNAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
Devices		default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
GlobalProtect					simple-high	any	high	default	disable
HIP Objects					simple-medium	any	medium	default	disable
HIP Profiles					simple-low	any	low	default	disable
External Dynamic Lists		strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	disable
Data Patteros					simple-high	any	high	reset-both	disable
Sovware					simple-medium	any	medium	reset-both	disable
Ulnerability					simple- informational	any	informational	default	disable
G URL Category					simple-low	any	low	default	disable
Security Profiles									
Antivirus 🔹									
Anti-Spyware									
Vulnerability Protection									
File Blocking									
WildFire Analysis									
🖰 Data Filtering									
E DoS Protection									
🞥 Mobile Network Protect									
SCTP Protection		_							
Security Profile Groups	Ð			F/CSV Three	t Prevention License	required for aptivin	us anti-snyware	and vulnerability o	rotection to funct
					to on on 1	required for alltivit	ast at the shyward, a	ana vuniciaunity p	rotection to runce
idmin Logout Last Login Time	:04/2	6/2022 18:35	101 Session Expire	ime: 05/26/2022	18:38:29		MI \$=	Tasks Language	w paloalto
VM 📃 🐻 Bruhlo.	Alto	- Mozilla F	Firefox						02

Under **Objects > Security Profiles > Anti-Spyware**. Click **Add**.

Figure 2.46: Add an Anti-Spyware Profile

Under the signature policies tab, click **Add**, name it, then configure these:

Table 2.8: Anti-Spyware Configuration

Rule	Configuration
Medium	Action: <i>Alert</i> Severity: <i>Medium, Low, Informational</i>
HighAlert	Action: Drop Severity: Critical, High

118 Chapter 2. Security Tuneup



Figure 2.47: Verify an Anti-Spyware Profile

Then press **OK**.

Create a File Blocking Profile

🚾 x11 - TightVNC Viewer								- 🗆 X
≞ 🖬 🖹 📕 🗲 🛷 ⋬	Ctrl		@ @ 🔂					
🕑 BruhloAlto - Mozilla Fir	efo:	ĸ						_ a ×
🊧 BruhloAlto	×	+*						
← → ⊂ ŵ	0	🕽 🔏 https://192.	.168.0.1/?#object	s::vsys1::objects/sec	urity-profiles/file-b	⊠ ☆		
🚺 PA-VM	D/	ASHBOARD AG	CC MONITOR	POLICIES OB.	JECTS NETWO	DRK DEVICE	∳ Commit ∨) ि सि प्
E Application Filters	0							$\begin{array}{c} G \end{array} \\ 2 \text{ items} \end{array} \rightarrow \times \end{array}$
Services		NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
Tags Devices GlobalProtect		basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
IIP Objects				Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
External Dynamic Lists				Log all other file types	any	any	both	alert
Custom Objects		strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
URL Category	4			Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
V Security Profiles				Log all other file types	any	any	both	alert
Anti-Spyware Uulerability Protection UUL Filtering UUL Filtering UUL Filtering UUL Filtering UUL Filtering UUL DoS Protection Mobile Network Protect SCTP Protection Scurity Profile Groups admin Lagout Last Login Time	⊕. : 04/2	Add C Delete (6)	Clane (2) PDF/CSV Gession Expire Time: 0	5/26/2022 18:38:29		⊠ %∃	Tasks Larigu	age <i>4</i> 2 paloalto
JWM _ 🗖 😸 Bruhlo	Alto	- Mozilla Firefo	x					02:4

Under **Objects > Security Profiles > File Blocking**. Click **Add**.

Figure 2.48: Add File blocking Profile

Configure these settings using the add button on the new window that just spawned.

Name	Properties
PDF	Applications: <i>any</i> File Types: <i>pdf</i> , <i>encrypted-pdf</i> Action: <i>Block</i>
EXE	Applications: <i>any</i> File Types: <i>exe</i> , <i>com</i> <i>Action: Block</i>

Table 2.9: File Blocking Configuration

120 Chapter 2. Security Tuneup

🔀 x11 - TightVNC Viewer									÷-	
BBBB B B B	es 🙀 Ctrl	Alt		Q @ Q 🛛 🔂						
😫 PA-VM - Mozilla Fi	refox	_			_					_ @ ×
🊧 PA-VM	×	+								
E > C A	0	£.	https://1	92 168 0 1/2#object	suvsvs]objects/sec	urity-pro	80% *** 💟	52	his	n @ =
		-	neep only 1	211001011/18 00/000	511(3) 511155 5000	sarry pro	0	A	iu v	B @ -
PA-VM									🛓 Commit -	百四十只
										SO
Acu esses	9									Siteme
Aculess Groups	T NAME			LOCATION	RULENAME	APPLICATIONS	FILE TYPES		DIRECTION	ACTION
Bungane Han Ground	1.1 - Head for the	000 m		Pyedefinied	Block high risk file types	any	7z, bat, chm, hlp, hta; jar, o torrent, vbe.	dass, opl. dll, exe, oc. PE. pif, rar. sig. Wsf	both	block,
Accidation Groups				P (1	Postform constant and added 6	ine the	principality of		both	Luntinue
Acustica Filters		File	Blocking	Profile			(?		both	mert
Sumper -	The second		Nam	e BlockThese				diss. cp), di. a. jar. nsil, Mult	both -	block.
Re Lan			Descriptio	n				DEX. PE. pif. tar. DE. wsf		
ES bevert		01					2 items	korypted-zip	both	block.
- Restall Luci	_	n	NAME	APPLICATIONS	FUETVPES	DIRECTION	ACTION		both	dert
Ш ний рышев	Correct Contract	-	DOE	2014	accounted add	both	black		hoth	block
ER HIP Nulles			r Dr	ally	pdf	0001	Proces			
 Extend Dynamic Lists I Coston Objects 		-	EXE	any	com	both	block			
E Linka Palitania					exe					
G Seywar										
W Yomensonity										
- Di Securiti Profile:										
🕼 Antiseus			Add ODe	lete						
😡 Anul-ásywa 🗉										
Vurierated V (Valuation										
File Blocking							Cancel			
WILENE ANAVES						_	_			
(Linka Filenny										
CE Lius Wallaction										
Tel contra Nelva + Prozes										
Construction										
Lug Forwarding										
1000 () · · · · ·		elete l	S Clone E	PDF/CSV -						
hum192.168.0.1/?#	204 - 20 - 20 <u>5 -</u> 2	1114-	Distance of B	verne miner die 201222 dae				M 35		
JWM OPA	-VM - Mo	zilla	Firefox							19:53

Figure 2.49: Configure the File blocking profile

Then click **OK**.

Create a WildFire Profile

🚾 x11 - TightVNC Viewer						-	
≞∎∎∎∎ ∥ 9 ⊗ ≸	Ctrl Att 📭 🤇	R Q @ Q B					
😫 BruhloAlto - Mozilla Fir	refox 7	ř					_ @ ×
🚧 BruhloAlto	× +						
↔ ↔ ↔ ↔	🛈 🔊 https	:// 192.168.0.1 /?#objects	::vsys1::objects/sec	urity-profiles/wildfir	⊘ ☆	lux (
🗘 PA-VM	DASHBOARD	ACC MONITOR	PO LICIES OB	JECTS NETWORK	DEVICE	La Commit →	ቪ ଲେ• ପ
and the second second							G 🛈
En Application Filters	9						$^{\rm 1item} \rightarrow \times$
Service Groups	NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
📎 Tags	default.	Predefined	default	any	any	both	public-cloud
Colorado Devices Colorado De							
 Wulnerability WL Category Security Profiles Antivirus Anti-Spyware 	4						
Ullnerability Protection URL Filtering File Blocking							
Image: WildFire Analysis Image: Object of the second s							
Mobile Network Protect							
SCIP Protection							
C security i tome croups	⊕ Add ⊖ Dele	te Clone DF/CSV					
admin Logout Last Login Time	: 04/26/2022 18:3	5:01 Session Expire Time: 0!	5/26/2022 18:38:29			asks Language 😽	🏷 paloalto
JWM _ 🗧 🌜 Bruhlo	Alto - Mozilla f	Firefox					02:44

Under Objects, **Security Profiles > WildFire Analysis**, click **Add**.

Figure 2.50: Add a WildFire Profile

Configure these settings using the add button on the new window that just spawned.

Table 2.10: WildFire Configuration

Name	Properties
Detect	Applications: <i>any</i> File Types: <i>archive, jar, ms-office</i>

122 Chapter 2. Security Tuneup

x11 - TightVNC Viewer				10-10-10-10-10-	and many res				-	
BBBB B H S	es 🙀 Ctrl	Alt 🖻	€ €	2 @ @ 🔂						
📦 PA-VM - Mozilla F	irefox									_ @ ×
🍻 PA-VM	×	+								
< → ℃ ŵ	0	🏡 hi	ttps://19:	2.168.0.1/?#øbjects	::vsys1::objects/sec	urity-pro 80%	⊠ ☆	9		: ≡
🚯 PA-VM	DASH BDA	RD	ACC A	MONIFOR: POLICIES	OSJECTS NETWO	RK DEMICE		-U	ipmmit -	6 B* Q
	~									SO
Addresses	TI NAME			LOCA DON	DAILE SA MAE	ADDIVATIONS	EN E TYPES		DIRECTON	
Regions	La stat			Predefined	default	any	any		both	public-cloud
Accurations										
Accuration Groups		Wild	Fire Analy	sis Profile			0			
Accuration Filters		· · · · ·	in c / in city	SIST FORM			U			
Sumar Council			Name	WildestFires						
🖗 lage		-	Description							
		QC		Tracilla Isaa	Doursel /	The second second	1 item $\rightarrow \times$			
HIP Course			NAME	APPLICATIONS	FILE TYPES	DIRECTION	SIS ^			
III HIP Nulles			Detect	any	archive	both public-c	loud			
External Dynamic Lists					ms-office					
Enala Partunia										
D Seywar	X									
W Volkerability										
DEL Calugury										
Anike us		() Ar	Id ODele	te						
🗊 Anil-Seywa L		On								
Vonerately Netotion							1000			
Con that Filleway						OK.	Cancel			
WildFire Analysis			_							
din Liala Fillaway										
CE Duá Muluchico										
Andre Helow + Prose										
Construction Construction										
Lug forwarding										
Variat (()Add			PDF/CSV						
Linnet Link Log		16425	Station Ext	ere fren (* 1001111 (.e.,	5				https://192	.168.0.1/?#
JWM _ 3 6 PA	A-VM - Mo	zilla F	irefox							20:01

Figure 2.51: Add a WildFire Profile

Then press **OK**.

Apply Security Profiles to a Security Policy

x11 - TightVNC Viewer									- 🗆 X
	Ctrl		🔍 🔍 🔂						
😢 BruhloAlto - Mozilla Fir	refo:	x							_ @ ×
🊧 BruhloAlto	×	+							
< → ℃ ŵ	0	D 🔏 https://192.3	168.0.1/?#policie	es::vsysl::p	olicies/securit	y-rulebase	… ☑ ☆	111	
🔷 PA-VM	D/	ASHBOARD AC	C MONITOR	POLICI	es objec	TS NETWORK	DEVICE	↓ Commit ∨	ट •स• द
		k							G ()
🔤 Security	Q								$_{3 \text{ items}} ightarrow imes$
⇒ NAT							Source		
🛞 QoS Rolicy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
Decryption	1	IntoOut	none	universal	🚝 Inside	any	any	any	P Outside
Application Override	2	intrazone-defaul@	NORE	intrazone	any	any	any	ariy	(intrazone)
Authentication	3	interzone-defau	none	interzone	any	апу	any	any	any
C SD-WAN									
Policy Optimizer -									
🔁 New App Viewer 🛛 0	4								
Rules Without App Controls									
✓ ² Rule Usage									
Unused in 30 days 1									
💫 Unused in 90 days 🛛 1									
Unused 1									
	-								
Object : Addresses +	Ð	Add (=) Delete 🚳	Clone 💿 Override	Revert	🕑 Enable 🕥	Disable Move Y	PDF/CSV - H	lighlight Unused R	ules »
admin Logout Last Login Time	: 04/2	16/2022 18:35:01 S	ession Expire Time:)	05/26/2022	18:38:29			Tasks Languag	🔹 🦇 paloalto
JWM _ Bruhlo,	Alto	- Mozilla Firefo	x						02:45

Under **Polices** > **Security**. Click the policy for inside to outside you created.

Figure 2.52: Add a Security Policy

Under the Actions tab, in the Profile Setting subsection. Configure these:

Parameters	Value
Profile Type	Profiles
Antivirus	Select the one you created
Anti-Spyware	Select the one you created
File Blocking	Select the one you created
WildFire Analysis	Select the one you created

Table 2.11: S	ecurity Policy	Actions (Configuration
----------------------	----------------	-----------	---------------

۵ (🛈 🔏 https://192.	168.0.1/?#	policies::vsys1::	policies/security	-ru 80%	⊠ ☆	1	1 0
DA	SH BOARD ACC MC	NITOR RO	LICIES OBJECT	s NETWORK	DEVICE		1 Lonomit	-
5								_
				Source I			DeitInätten	
onwarding N	ME. TAGS	TYPE	ZONE	ADDRESS US	ER DEVICE	ZONE	ADDRESS	De
1 []	Age the	anive/sa	-	1.4		Mon	- Y	
ecurity Policy Rul	2						_	G
General Source	Destination Application	Service/URL C	ategory Actions	Usage				
Action Setting				Log Setting				
Actio	Allow		V		🗾 Log at Session Start			
	🔲 in - Corporation				Log at Session End			
Profile Setting				Log Forwardling	None			4
Profile Typ	Profiles	Ŷ	Other Settings					
Antiyiiu	AV2		4	Schedule	None			\sim
Vulnerability Protection	Protection None			QoS Marking	QoS Marking, None			
Anti-Spywan	nti-Spyware Spyware ~				Disable Server Respo	nse Inspection		
URL Filtering	ring None ~							
File Blocking	BlockThese		Ý					
Data Filtering	None		Ý					
WildFire Analysi	Wassifica		~					
								Canada
							OK	ancel
	_	_	_	_	_	_	_	

Figure 2.53: Assigning security profiles

Then click **OK**. Remember to commit your changes!

Test the Security Profiles

Since I do not have a licence, we cannot demonstrate all of these profile features, as you can see when you commit.



Figure 2.54: Commit the configuration

This is ok, we can still test out the file blocking features.

On the client, navigate to a website that hosts PDF files (I used <u>panedufiles.com</u>).



Figure 2.55: Verify the configuration

Try and open one of these. If it shows the file blocking screen, it means that the file blocking worked!



Figure 2.56: File Transfer Blocked

Chapter 3. Advanced Networking

128 Palo Alto Firewall

3.1 Captive Portal

Learning Objectives

- Configure VLANs
- Configure captive portal

Prerequisites:

- Setup Zones
- Some interface configuration
- Configuring VLANs on the GNS3 switch
- Knowledge of previous labs

Scenario: Now let's push for some advanced networking configurations. Sometimes you just have to push departments into their own VLANs for organization and compliance. Say we have a guest and employee network. We want to prevent communication between the two as much as possible. We would also want to implement some sort of login to access the internet for guests, much like hotels.
130 Chapter 3. Advanced Networking



Figure 3.1: Main scenario

Table 3.1: Addressing Table

Device	Configuration
PaloAlto-1	management: 192.168.0.1/24 Ethernet1/1: Trunking Ethernet1/1.10: 10.10.10.1/24 Ethernet1/1.20: 20.20.20.1/24 Ethernet1/2: DHCP
VLAN-10	eth0: 10.10.10.10/24 GW: 10.10.10.1 DNS: 8.8.8.8
VLAN-20	eth0: 20.20.20.20/24 GW: 20.20.20.1 DNS: 8.8.8.8
Management	eth0: 192.168.0.2/24
Switchy	e0: Access mode, VLAN 10 e1: Access mode, VLAN 20 e7: dot1q, VLAN 1

Table 3.2: Zone Configuration

Zone	Interface
VLAN10	Ethernet1/1.10
VLAN20	Ethernet1/1.20
Outside	Ethernet1/2

Configure Sub Interfaces

Under **Network > Interfaces**. Click on **ethernet1/1**.

🚾 x11 - TightVNC Viewer							- [x c
3 🖬 🖆 📗 😏 🛷 🖠	🛚 ctri Ait 📭 🗨	Q @ Q &						
😝 BruhloAlto - Mozilla Fir	efox							_ @ ×
🚧 BruhloAlto	× +		*					
€ → ୯ û	🛈 🔏 https://1	.92.168.0.1/?#networ	k::vsys1::network	/interfac	es ••	· 🛛 🕁	III\ 🗊	≝ ≡
🚺 PA-VM	DASHBOARD	ACC MONITOR	POLICIES	OBJECTS	NETWORK D	DEVICE	t~ Ē	₽ŧ × Q
								G ()
	Ethernet VLA	N Loopback Tunne	SD-WAN					
Go VLANs	Q						8 items	$\rightarrow \times$
Virtual Routers Virtual Routers IPSec Tunnels	INTERFACE	INTERFACE TYPE	MANAGEMENT	LINK	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL
GRE Tunnels	themet1/1	Layer3			none	none	Untagged	none
● DHCP ● ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	ethernet1/2	Layer3			Dynamic-DHCP Client	default	Untagged	none
V 😤 GlobalProtect	ethernet1/3			-	none	none	Untagged	none
Portals	ethernet1/4			画	none	none	Untagged	none
C MDM	ethernet1/5			m	none	none	Untagged	none
Clientless Apps	4 ethernet1/6			m	none	none	Untagged	none
Clientless App Groups	ethernet1/7				none	none	Untagged	none
Cos Qos	ethernet1/8			m	none	none	Untagged	none
V 🕞 Network Profiles								
GlobalProtect IPSec Cry								
H IKE Gateways								
HE Crypto								
A Monitor								
Interface Mgmt								
R Zone Protection				_				
A Oos Profile	+ Add Subinterfa	ace 😑 Delete 🙆 PDF/	CSV					
adının Logout Last Login Time	: 04/26/2022 18:35:0	1 Session Expire Time: 0	5/26/2022 18:38:29	i i		🖂 🎉 Tasks La	nguage 🛷 p	aloalto
IWM	Alto - Mozilla Fir	efox						02:50

Figure 3.2: Ethernet 1/1 configuration

	In t	his	window,	we just	want to	set the	e interfa	ace type	to l	layer	3.
--	------	-----	---------	---------	---------	---------	-----------	----------	------	-------	----

x11 - TightVNC Viewer			- C	ı ×
🧏 🖬 😭 🗈 📕 😔	🏘 🗿 Cri Ait 🔖 🔍 🔍 🔍 🔍 🔯			
😢 BruhloAlto - Mo:	zilla Firefox		_	_ @ ×
🊧 BruhloAlto	× +			
↔ ↔ ↔ ↔	🛈 🔏 https://192.168.0.1/?#network::vsys1::network/interfaces	⊠ ☆		: Ξ
🔷 PA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK	DEVICE	-) 🛅	₽∰ Y Q
Interfaces Page Zones	Ethernet VLAN Loopback Tunnel SD-WAM		R	60
eg VLANs Co Virtual Wires	Ethernet Interface	0	8 items	$\rightarrow \times$
Virtual Routers PSec Tunnels	Interface Name ethermet1/1.		TÁG	VLAN / VIRTUAL
GRE Tunnels	Comment		Untagged	none
こ DHCP 習 DNS Proxy	Netflow Profile None	~	Untagged	none
	Config Dr.4 Dr.4 SD-WAN Advanced		Untagged	none
Portais			Untagged	none
Gateways MDM	- Assign Interface To		Untagged	none
Clientiess Apps	Security Zone None	×	Untagged	none
Clientless App	Security zone Tome	*	Untagged	none
QoS LLDP V R Netwark Profiles		OK Cancel	Untagged	none
 □ GlobalProtect L 〒 IKE Gateways ② IPSec Crypto ☆ INSE Grypto ☆ Monitor ※ Interface Mgmt ※ Const Protection ※ Const Protection 				
stimm Lagout Last La	gin Time: 04/26/2022 18:35:01 Session Expire Time: 05/26/2022 18:38:29	🗹 👔 laska i Lang	uaer 🦘 pa	aloalto
JWM 6	BruhloAlto - Mozilla Firefox			02:51

Figure 3.3: Set Interface type to Layer3

Then press **OK**.

🚾 x11 - TightVNC Viewer							-	o x
	Ctri Alt 🗎 🗎 🔍 🔍	🔍 🍳 🔯						
🔮 BruhloAlto - Mozilla Fir	efox	_						_ a >
🊧 BruhloAlto	× +							
€ → C @	🛈 🔬 https://192	1.168.0.1/?#netwo	rk::vsys1::network	/interfac	:es ••	· 🛛 🕁		🛎 🗉
🚺 PA-VM	DASHBOARD A	CC MONITOR	POLICIES	OBJECTS	S NETWORK D	EVICE	t~) ℃	₽₹×Q
								G ()
Zanes	Ethernet VLAN	Loopback Tunne	el SD-WAN					
g VLANs	Q						8 item	$s \rightarrow X$
	INTERFACE	INTERFACE TYPE	MANAGEMENT	LINK	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL
GRE Tunnels	and ethernet1/1	Layer3			none	none	Untagged	none
DHCP DNS Prove	ethernet1/2	Layer3	1		Dynamic-DHCP Client	default	Untagged	none
V GlobalProtect	ethernet1/3			m	none	none	Untagged	none
C Portais	ethernet1/4			m	none	none	Untagged	none
Gateways	ethernet1/5				none	none	Untagged	none
Clientless Apps	4 methemet1/6				none	none	Untagged	none
Clientless App Groups	methemet1/7				none	none	Untagged	none
🚓 QoS	methemet1/8				none	none	Untagged	none
V C Network Profiles	and ethemet1/0				libite	June	ontagged	Hone
GlobalProtect IPSec Cry								
IPSec Crypto								
IKE Crypto								
Monitor •								
Interface Mgmt								
Zone Protection	0	0						
R OoS Profile	(+) Add Subinterface	Delete PDF/	CSV					_
admin Logout Last Login Time	:04/26/2022 18:35:01	Session Expire Time: 0)5/26/2022 18:38:29			⊠ ≸∃ Tasks La	inguage 🥠	paloalto
JWM 📕 🚺 Bruhlo	Alto - Mozilla Firefo	xc						02:5:

Now while **ethernet1/1** is still selected, click on add sub interface.

Figure 3.4: Add Sub interfaces

We want to add 2 sub-interfaces. Here is what you should configure:

Interface	Configuration
Ethernet1/1.10	Interface Name: 10 Tag: 10 Config tab: – Virtual Router: <i>default</i> – Security Zone: <i>VLAN10</i> IPv4: – Type: <i>Static</i> – <i>IP</i> : 10.10.10.1/24
Ethernet1/1.20	Interface Name: 20 Tag: 20 Config tab: – Virtual Router: <i>default</i> – Security Zone: <i>VLAN20</i> IPv4: – Type: <i>Static</i> – <i>IP</i> : 20.20.20.1/24

Table 3.3: S	bub Interface	Configuration
--------------	---------------	---------------

x11 - TightVNC Viewer							- 0) >
B 🖬 🗈 🗏 号 🐲 🖠	Ctrl Alt 🐴 🔍 🔍 🖉	Q Q 🐼						
BruhloAlto - Mozilla Fir	efox							_ 8
🊧 BruhloAlto	× +							
€⇒ ୯ ଢ	(i) 🖍 https://192.16	58.0.1/?#netwo	I rk::vsys1::network	interfac	es 😒 💀	· 🛛 🕁		8
0 PA-VM	DASHBOARD ACC	MONITOR	POLICIES	OBJECTS	NETWORK D	EVICE	· 16	₽ ₩ ~ (
								G (
Zones 9	Ethernet VLAN 1	oopback Tunn	el SD-WAN					
C VLANS	Q						10 items	$) \rightarrow \rangle$
Virtual Routers	INTERFACE	INTERFACE TYPE	MANAGEMENT	LINK	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN
GRE Tunnels	ethernet1/1	Layer3			none	none	Untagged	none
DHCP P	@ ethernet1/1.10	Layer3			10.0.10.1/24	default	10	none
Global Protect	@ ethernet1/1.20	Layer3		-	10.0.20.1/24	default	20	none
Tortals	con ethernel 1/7	Laver3			Dynamic-DHCP Client	default	Untagged	none
Gateways	Cathernatd /2				0000	none	Untagged	0000
Clientless Apps	+				none	none	Untergood	
Clientless App Groups	ethernet1/4				none	none	Untagged	none
😤 Qo5	ethernel1/5				none	none	Untagged	none
CLOP	methernet1/6			ch	none	none	Untagged	none
GlobalProtect IPSec Cry	ethernet1/7			1	none	none	Untagged	none
H IKE Gateways	ethernet1/8			1	none	none	Untagged	none
PSec Crypto								
🔁 IKE Crypto 🐘								
Monitor •								
Tope Protection				_				
A OnS Profile	(+) Add Subinterface	Delete @PDE/	CSV					
		Frank STON		1				alaali
dinin Thogout Thast Login Time:	04/26/2022 18:35:01 Set	sion Expire time.C	0/20/2022 18:38:29				ingualle 🧼 p	aloal

Figure 3.5: Verify Sub interfaces

Semi-Advanced Security Policies

x11 - TightVNC Viewer								÷	- 🗆 X
≞∎∎∎∎ ∎ 9 ≇	Ctrl	$Att \mid \mathbb{P}_1 \mid \textcircled{\texttt{Q}}, \textcircled{\texttt{Q}}$	🔍 🔍 🔂						
😢 BruhloAlto - Mozilla Fin	efo)	<.							_ @ ×
🊧 BruhloAlto	×	+							
↔ ♥ ✿ ✿	0	D 👰 https://192.	168.0.1/?#policie	savsyslap	olicies/securi	ty-rulebase	••• 🛛 🖞	111	
🚺 PA-VM	DA	ASHBOARD AG	CC MONITOR	PÓLICI	es objec	TS NETWORK	DEVICE	Commit V	ि सि ∙ Q
	0								G ()
B Security → NAT	~						Source		
💩 QoS					-		Jource		
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
Decryption Decryption	1	IntoOut	none	universal	ma Inside	any	any	any	P Outside
Application Override	2	intrazone-defauto	NONE	intrazone	atiy	aniy	any	any	(intrazone)
Authentication	3	interzone-defaut	none	interzone	any	any	any	апу	any
SD-WAN									
Policy Optimizer -									
New App Viewer D	4								
Rules Without App Controls D									
Unused Apps									
✓ [*] ⊂ Rule Usage									
Unused in 30 days									
Unused 1									
Object : Addresses +	÷	Add (=) Delete (6)	Clone 🙁 Override	Revent	🕑 Enable. 🚫	Disable Move Y	PDF/CSV	Highlight Unused Ru	es »
admin Logout Last Login Time;	04/2	6/2022 18:35:01 S	ession Expire Time: 0	5/26/2022	18:38:29			∃Tasks Language	🊧 paloalto
JWM _ 📕 🍯 BruhloA	Alto	- Mozilla Firefo	x						02:54

Well, it's not really advanced, but under **Policies** > **Security**, click **Add**.

Figure 3.6: Add a Security Policy

We will be making a policy to allow **VLAN10** and **VLAN20** into the Outside zone. We can do this by adding multiple zones under the source zone.

🚾 x11 - TightVNC Viewer			- 🗆 X
≞∎≝∎∎ € അ≋	角 Chr. Alt 🐴 🗨 🍳 🔍 🍭 🔂		
👂 BruhloAlto - Mozilla Fi	refox 🐨		_ @ >
🊧 BruhloAlto	× +		
← → C ŵ	🛈 🐔 https://192.168.0.1/?#policies::vsy	vs1::policies/security-rulebase •••	
OPA-VM	DASHBOARD ACC MONITOR P	OLICIES OBJECTS NETWORK DE	VICE 🛓 Commit ~ T 🖣 ~ Q
	~		80
Socurity Policy Pulo		Source	
General Source Destina	ation Application Service/URL Category Ac	tions Usage	any v
	SOURCE ADDRESS	SOURCE USER	
VLAN10			
VLAN20			
		Add (-) Delete	
Orda O balcac		Orada O Botch	Critic Cresting
_	L ivegate		ОК
Object : Addresses + https://192.168.0.1/?# 16 1005	Add Delete Clone Ovinite in	ever 🕑 Enable 🚫 Disable Move Y 🔘 PDF/ 202020114/05224	CSV 🗌 Highlight Unused Rules 🔅
JWM 🔤 🍯 Bruhlo	Alto - Mozilla Firefox		02:5

Figure 3.7: Security Policy Rule – Source Zone

Then click **OK**.

Semi-Advanced NAT Policies

🗱 x11 - TightVNC Viewer								- 0	×
🐴 🖬 🖀 🖺 📕 😔 😂	Ctrl Alt		Q @ @ 🐼						
😫 Xav-PA - Mozilla Firefi	ox	不							. a ×
🚧 Xav-PA	× +	-							
← → ⊂ ŵ	1	https://19	92.168.0.1/?#polici	es::vsys1::policie	s/nat-rulebase	***		III\ 🗊 📽	Ξ
🚺 PA-VM	DASHI	BOARD	ACC MONITOR	POLICIES	OBJECTS	NETWORK DEV	rICE 🚔 Commit ∨) it ti	٠Q
								0	G ()
Security	Q							0 items	$\rightarrow \times$
→ NAT A QoS					1	Orig	inal Packet		_
Policy Based Forwarding	NA	ME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION	SOURCE ADDRESS	DESTINATION ADDRESS	SER
SD-WAN Policy Optimizer - ✓ 注 Rule Usage IN Unused in 30 days IN Unused in 90 days IN Unused in 90 days	- 0 0 0								

Still not really advanced. But under **Policies** > **NAT**, click **Add**.

Figure 3.8: Add a NAT Policy

We want to make a Static NAT policy for the Internet connectivity. But under the Original Packet tab, we can select multiple zones.

🚾 x11 - TightVNC	Viewer					- 0	×				
🌯 🖬 😭 🗈	l 😏 🖘 🖠	B Ctrl Alt Ba €	Q @ Q B								
BruhloAlto	- Mozilla Fir	efox					. a ×				
M BruhloAlto		× +									
(←) → C	۵	🛈 🔏 https://	(192.168.0.1/?#policies::vsys1::	oolicies/nat-rulebase	… ⊠ ☆		Ξ				
🚺 PA-VM		DASHBOARD	ACC MONITOR POLIC	IES OBJECTS NETWO	DEVICE 🔄 Commit ~) <u>t</u> F	×Q				
						E	à D				
Security		Q				1 item	$\rightarrow \times$				
Dos	NATE	P.I.			Original Packet						
Policy Based	NAT Polic	y Rule			C	DRESS	SET				
Decryption	General Original Packet Translated Packet										
Application C	Anv		Destination Zone	Anv	Anv	ī.					
Authenticatio	SOURC	e zone	Outside V		DESTINATION ADDRESS						
SD-WAN		N10									
		N120	Destination Interface								
Policy Optimizer			any ~								
V := Rule Usage											
C Unused 1			Service								
Unused	0			0							
	(+) Add (-)	Delete		(+) Add (-) Delete	(+) Add (-) Delete	1. C					
					OK Cancel	5					
	-										
Object : Addresse	s +		e 🛞 Clone 🅑 Enable 🚫 Disable	Move * (PDF/CSV High	light Unused Rules 🖾 View Rulebase	as Groups	**				
https://192.168.	0.1/? # 11100	04/26/2022 18:35:	01 Session Expire Time: 05/26/2022	18.38:29	🖾 🔮 lasks Lanan	ace 🥢 palo	alto				
JWM _	Bruhlo	Alto - Mozilla Fi	refox		1		02:56				

Figure 3.9: Select the Source Zone

Image:	×
Xav-PA - Mozilla Firefox	×
	-
(→) C' (https://192.168.0.1/?#policies::vsys1::policies/nat-rulebase ···· (□ (https://192.168.0.1/?#policies::vsys1::policies/nat-rulebase (•) PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE Image: Commit and	
OASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE	=
	L
G (2))
📾 Security 🔹 🔍 👘 🔍 👘 🖓	×
In NAT Original Packet	
RESS VOS NAT Policy Rule	SET
General Original Packet Translated Packet	
🖆 Tunnel Juspe	
27 Authentičatio Translation Type Dynamic IP And Port V Translation Type None V	
E Dos Protecti Address Type Interface Address V	
Interface ethernet1/2 v	÷
Policy Optimizer IP Address None V	
₩ ³ Rule Usage	
Thused	
B Unused 1	
40 trinsed	
adimin Lazout Last Lazout Lazout Last Lazout Laz	5
JWM _ 📕 🌜 Xav-PA - Mozilla Firefox 08:	12

Configure the rest for static NAT, then press **OK**.

Figure 3.10: SNAT Translated Packet Tab

Add a User

Under **Device > Local User Database > Users**. Click **Add**.

🚾 x11 - TightVNC Viewer					- 🗆 X
	🕻 ctri Alt 📬 🏵 🔍 🔍				
😫 BruhloAlto - Mozilla Fir	efox				_ a ×
🊧 BruhloAlto	× +				
← → C ŵ	🛈 <u> https://192.168</u>	.0.1/?#device::vsys1::devic	ce/local-user-database/us⊨	⊚ ☆	III\ 🗊 😻 🗏
🚺 PA-VM	DASHBOARD ACC	MONITOR POLICIES	OBJECTS NETWORK		mmit∨ ि ⊮₁∙ Q
Per corre	0			*	G ()
SSL Decryption Exclusio			1	ł	\circ items $\rightarrow \times$
SSH Service Profile	NAME		LOCATION		ENAB
Response Pages					
Log Settings					
Server Profiles					
Email					
НТТР					
Retflow					
RADIUS					
	4				
Kerberos					
SAML Identity Provider					
Multi Factor Authenticat					
V III Local User Database					
Users					
Scheduled Log Export					
G Software					
GlobalProtect Client					
🔁 Dynamic Updates 🔹					
2.5 Plugins					
VM-Series	(+) Add (-) Delete (-) Clor	DE DF/CSV			
admin Logout Last Login Time.	: 04/26/2022 18:35:01 Sessio	in Expire Time: 05/26/2022 18:	38:29 [🖂 🏂 Tasks	Language 🥠 paloalto
JWM _ 📕 🍯 Bruhlo/	Alto - Mozilla Firefox				02:57

Figure 3.11: Add Users



Create any user you want with a username and password. Here is an example:

Figure 3.12: Add a user xav

Then click **OK**.

Create an Authentication Profile

Under Device >	Authentication P	Profile, click Add.
-----------------------	-------------------------	---------------------

🚾 x11 - TightVNC Viewer										÷	
B 🖬 🗈 🔳 😔 🕬 🎽	Ctrl	Att 📭 🤆									
👂 BruhloAlto - Mozilla Fir	efo)	<	_								_ a ×
🚧 BruhloAlto	×	+									
€ → ୯ û	0	🕽 🔏 https:	//192.168.0.1	L/?#device::v	sys1::device	/authenticati	on-profile	*** (פ ב	lux -	□ 🔹 =
🚺 PA-VM	D/	SHBOARD	ACC	MONITOR	POLICIES	OBJECT	NETWOR	K	CE 📑 Com	mit 🗸 🕴	ਰਿ ਦੀ • ⊄
🖽 High Availability											G ()
Config Audit	Q		1			1	1	1	-	1	$0 \text{ items} \rightarrow X$
Password Profiles				Lo	ckout						
Administrators		NAME	LOCATION	FAILED ATTEMPTS		ALLOW LIST	AUTHENTI	SERVER	AUTHENTI	OTHERS	LOCKED
Authentication Profile	-	NAME	LOCATION	(#)	TIME (MIN)	ALLOW LIST	AUTHENTIA	PROFILE	FACTORS	OTHERS	USERS
 Data Redistribution Device Quarantine VM Information Sources Troubleshooting Certificate Management Certificates Certificate Profile OCSP Responder SSL/TLS Service Profile SCEP SSL Decryption Exclusio SSH Service Profile Response Pages Log Settings Server Profiles SNMP Trap 	4										
Email	(Ð)	Add 🕞 Dele	te 🕲 Clone (DF/CSV							
admin Logout Last Login Time:	04/2	6/2022 18:35	i:01 Session E	xpire Time: 05/	26/2022 18:38	:29			Z \$∃ Taskš	Language	🊧 paloalto
JWM _ BruhloA	Alto	- Mozilla F	Firefox								02:57

Figure 3.13: Add an Authentication Profile



Under the Authentication tab, change the type to Local Database.

Figure 3.14: Select Local Database

Under the Advanced tab, add your user.

🗱 x11 - TightVNC Viewer		-	σx
🧏 🖬 🖹 📕 🤧 😻 🖠	🕻 Chi Ali 📴 🔍 🔍 🍭 🍭 🐼		
😫 PA-VM - Mozilla Firefo:	x	_	×
🚧 PA-VM	× +		
← → ⊂ ŵ	🛈 🔏 https://192.168.0.1/?#device::vsys1::device/authentication-profile 🛛 💀 🤝 🏠	n lux e	D 📽 😑
🚺 PA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE	🛓 Cammit 🛪	টি ≞িশ এ
Ve Seno	0		G @ Lillen → X
E Fligh Availability	Lockoul		
Config Audit Password Profiles	Authentication Profile (2)	IENTI ORS OTHERS	LOCKED
Admin Roles	Name Auth		none
Authentication Profile	Authentication Factors Advanced		
Authentication Sequence	Allow List		
Data Redistribution	ALLOW LIST A		
Device Quarantine	S all		
Troubleshuching	S xav		
Contractor Management Contractor Management Certificatos Certificatos Certificatos Provide Contractor Provide Contractor Provide	k		
Ca scep	⊕ Add ⊖ Delete		
🖹 SSL Decryption Exclusio	Account I oclouit		
Response Pages	Failed Attemptr 10 = 10		
Ta Log Settings	lockout Time (min) 0		
	terrational from the second se		
Can Souther	Cancel		
https://192.168.0.1/?# 0.000			// paloalto
JWM 💭 🛑 PA-VM	- Mozilla Firefox		21:26

Figure 3.15: Add user xav as Allow List

Then press **OK**.

Configure the Captive Portal

Under Device.	User Identification in the	ne Authentication Portal	Settings tab	click the settings icon.
Under Device	Osci iucinincunon in u	ic municilituditi i onui	ocumes mo	, cher the settings reon.



Figure 3.16: Authentication Portal Settings

Configure these settings:

Parameter	Value
Enable Authentication Portal	Tick this box
Authentication Profile	Select the one you created
Mode	Transparent

146 Chapter 3. Advanced Networking

x11 - TightVNC Viewer		- 🗆 X
B ∎∎∎ B ∎ S	ෂ 🏨 Chri Alt 📴 වැ. වැ. 🔍 🍭 🔂	
😫 PA-VM - Mozilla Fir	refox	_ @ ×
M PA-VM	× +	
	🛈 🐔 https://192.168.0.1/?#deviceovsys1odevice/user-identification 🛛 💀 😒 🟠	
OPA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK LIVEVICE	्र सि स ्
Setup	User Mapping Convection Security Revisional Server Agents Group Mapping Settings Authentication Portal Set	tings Cloud Identity Engl
Config Audit	Authentication Portal	-3
Administrators	Authentication Portal ①	
Automication Profile Automication Security User Identification Device Qualifying Viol Information Secure You Information Secure Troubleshecting Certificate Management Certificates	Certificate Profile None Certificate Profile	
Certificate Profile COSP Responder SEL/TLS Service Pr SEL SELP SEL SELP SEL SELP SEL SELP SEL SECP SEL SECR SEL SECRE SEL	CK Cancel	
Lopiol Les Lopi	n (me: 94/29/2922/1427/48) Service Equite Trans/19/29/29/29225 🔤 👔 😤 🖂 La	🌕 🎆 paloalto
JWM _ PA	-NPA-VM - Mozilla Firefox	21:30

Figure 3.17: Authentication Portal Settings – Select Transparent

Then press **OK**.

🚾 x11 - TightVNC Viewer												÷	
B B B B I 5 00 5	Ctrl	Att 🐴	Q. Q. @	Q 🐼									
🔮 BruhloAlto - Mozilla Fir	refo:	x	•	-									_ @ ×
🊧 BruhloAlto	×	+	^										
€ → C ŵ	0	D 윮 http	s://192.16	8.0.1/?#net	work::vsys	s1::network	<td></td> <td>v</td> <td>⊠ ☆</td> <td></td> <td></td> <td>🔹 Ξ</td>		v	⊠ ☆			🔹 Ξ
🚺 PA-VM	D#	ASHBOARD	ACC	MONITO	DR PO	LICIES	OBJECTS	NETWO	RK DE		↓ Commit ~] 16	₽₹►Q
													G ()
Interfaces 🔹	Q							-				4 ite	$\xrightarrow{ems} \rightarrow \times$
Zones									User-ID			Device-ID	
VLANS Virtual Wires Virtual Routers		NAME	TYPE	INTERFA / VIRTUAL SYSTEMS	ZONE PROTEC PROFILE	PACKET BUFFER PROTEC	LOG SETTING	ENABLED	INCLUD NETWO	EXCLUD NETWO	ENABLED	INCLUD NETWO	EXCLUD NETWO
DipSec Tunnels		Inside	layer3	ethernet1					any	none	F	any	none
GRE Tunnels		Outside	layer3		ZoneProt			E	any	none		any	none
E DHCP		VLAN10	layer3	ethernet1					any	none		any	none
DNS Proxy		VLAN20	layer3	ethernet1		-		0	any	none		any	none
V 😫 GlobalProtect	-					-							
A Oos Profile	Ð	Add O'De	lete 🙆 PE	DF/CSV									
admin Logout Last Login Time	: 04/2	6/2022 18:	35:01 Ses	sion Expire Tin	ne: 05/26/20	022 18:38:29	2				asks Lang	uage 🚧	paloalto
JWM _ 💻 🍯 Bruhlo.	Alto	- Mozilla	Firefox										02:59

Under **Network > Zones**, click on the VLAN10 zone.

Figure 3.18: Select Vlan 10

x11 - TightVNC Viewer × 1 🖳 🖬 👔 📘 🕖 🛷 😹 ctri Att 🐚 🔍 🔍 🍭 🐼 🔰 BruhloAlto - Mozilla Firefox a x 🊧 BruhloAlto + × 1 https://192.168.0.1/?#network::vsys1::network/zones <) → C @ III\ 🗉 🔮 Ξ ···· · · · ☆ 0 Zone PA-VN User Identification ACL Device-ID ACL Name VLAN10 GO Enable User Identification Enable Device Identification Log Setting None 4 items $\rightarrow \times$ (A) Interfaces INCLUDE LIST A INCLUDE LIST A Zones Type Layer3 Select an address or address group Select an address or address group G VLANS INTERFACES ^ or type in your own address. Ex 192.168.1.20 or 192.168.1.0/24 or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24 Virtual Wire UD... EXCLUD. ethernet1/1.10 I Virtual Route NO. PSec Tunne none GRE Tunnel none E DHCP ⊕ Add ⊖ Delete none (+) Add (-) Delete DNS Proxy Devices from these addresses/subnets will be identified. Users from these addresses/subnets will be identified ~ GiobalProte Portals EXCLUDE LIST A EXCLUDE LIST A 🚑 Galewa Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24 (+) Add (-) Delete MDM D Select an address or address group or type in your own address. Ex 192.168.1.20 or 192.168.1.0/24 Clientie Clientle A Qos Zone Protection LLDP Zone Protection Profile None Network Pr + Add - Delete Enable Packet C GlobalP (+) Add (-) Delete **Buffer Protection** Users from these addresses/subnets will not be identified. H IKE Gate Devices from these addresses/subnets will not be E IPSec C Identified E IKE Cry C Monitor Cancel interfac R Zone Pr + Add Delete DPF/CSV paloalto 🖲 BruhloAlto - Mozilla Firefox 03:00 IWM

In this window, we just want to tick the **Enable User Identification** checkbox.

Figure 3.19: Enable User Identification

Then press **OK**.

🚾 x11 - TightVNC Viewer							-	
🏝 🖬 🖹 📕 😔 🕫	😭 Ctrl Alt 🖻	Q, Q, @ Q ₩						
🔰 BruhloAlto - Mozilla F	Firefox							_ 8 ×
🦔 BruhloAlto	× +							
(← → C @	🛈 🔒 htt	ps://192.168.0.1/?#polic	ies::vsys1::polic	ies/authenticatio	on-ruleba: 🗸	⊘ ☆		
🚺 PA-VM	DASHBOAR	D ACC MONITO	R POLICIES	OBJECTS	NETWORK	DEVICE	Commit ~	Ê ∰√Q
Security	. 0							$G \bigcirc$
⇒ NAT					Source			Destina
👶 QoS	NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
Application Override Authentication C Dos Protection S SD-WAN Policy Optimizer		Jetete Si Clone D Fraible	C Disable Mo	ve Y		nucod Buler 🗌 View	- Bulabaro ar Gra	
admin Logout Last Login Tir	me: 04/26/2022 18	8:35:01 Session Expire Time	: 05/26/2022 18:3	8:29	- 🖂 Hignlight U	nused Rules 🗀 View	s Language 🧳	paloalto
JWM _ 🖶 🍯 Bruhl	oAlto - Mozill	a Firefox						03:01

Finally, under **Policies > Authentication**. Click **Add**.

Figure 3.20: Add an authentication Policy

x11 - TightVNC Viewer _ 🖳 🖬 👔 🗓 📕 😏 🛷 🙀 Chri Ait 🐘 🔍 🔍 🔍 🐼 🔰 BruhloAlto - Mozilla Firefox k × + 🦇 BruhloAlto <) → C @ 🛈 🐔 https://192.168.0.1/?#policies::vsys1::policies/authentication-ruleba ... 🗵 🟠 111\ 🗊 🔹 PA-VM Qitems $\rightarrow \times$ Security TAN +E Source A QOS Policy Bases Authentication Policy Rule 0 E Decryption 🖨 Tunnel Inspe General Source Destination Service/URL Category Actions Application \sim V P Authenticati Any 🗹 Any anv any E Dos Protect SOURCE ZONE SOURCE ADDRESS SOURCE USER SOURCE DEVICE G SD-WAN VLAN10 Policy Optimizer V 🚈 Rule Usage R Unused C Unused C Unused + Add O Delete (+) Add - Delete (+) Add (-) Delete Negate Cancel + (+) Add Object : Addresses

×

а×

Ξ

GO

Desti

ADDRESS

paloalto

03:02

Under the Source tab, add VLAN 10 in the source zone.

Figure 3.21: Add the Source Zone

🖲 BruhloAlto - Mozilla Firefox

https://192.168.0.1/?#

IWM



Under the Destination tab, add Outside in **Destination Zone**.

Figure 3.22: Add the Destination Zone

🚾 x11 - TightVNC V	Viewer	-	
	📙 😏 📾 🏙 Chr. Alt ங 🔍 🔍 🔍 🔍 🔯		
😝 BruhloAlto -	- Mozilla Firefox		_ a ×
🋷 BruhloAlto	× +		
€ → C		lity	□ 🔹 =
OPA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE	nmit ~	ोि मि≁ ⊂
			GO
Security	• Q		${}^{\rm Oltems}\to\times$
Dos	Source	-	Destina
Policy Based	Authentication Policy Rule	(?	ADDRES5
E Depryption	General Source Destination Service/URL Category Actions		
P Authentication	Authentication Enforcemen default-web-form	×.	
Dos Protecti	Timeout (min) 60		
G SD-WAN	Log Settings		
Policy Optimizer	Log Forwarding None	~	
∽ ў⊟ Rule Usage			
Unused		Cancel	
C Unused			
Object : Addresses	s + (17/Add Highlight Unused Rules View R	ilebase as Gro	wips »
		Contraining S	03.03
144141 -			05.05

Under Actions, change the Authentication Enforcement setting, change it to **default-web-form**.

Figure 3.23: Select default-web-form

Then press **OK**.

Test VLANs and Captive Portal

On the VLAN-20 webterm, navigate to any website. If all was right, the desired website should appear.



Figure 3.24: Verify your configuration

On the VLAN-10 webterm, navigate to any website. If all was right, you should see a certificate error, accept this. Then you should see a login page.



Figure 3.25: Login Page

Enter your credentials and log in. If all was successful, you should see the website appear.



Figure 3.26: Verify your configuration

3.2 Remote Access VPN

Learning Objectives

- Configure a tunnel interface
- Configure a remote access VPN

Prerequisites:

- Setup Zones
- Some interface configuration
- Create a new user
- Create an auth policy
- Policy that allows VPN to Inside
- Policy that allows Outside to VPN
- Knowledge of previous labs

Scenario: VPNs aren't just about changing your location like many advertisements say they're for. What it's really used for is to securely access a remote location's resources like your workplace, or even your own home. That is what this lab will focus on. We are going to install GlobalProtect Agent on Kali and then we'll try to reach the Internal through VPN connection.



Figure 3.27: Main scenario

Table 3.5: Addressing Table

Device	Configuration
PaloAlto-1	management: 192.168.0.1/24 Ethernet1/1: 10.0.0.1/24 Ethernet1/2: DHCP
Internal (WordPress)	eth0: 10.0.0.2/24 GW: 10.0.0.1
KaliLinux2019.3-1	eth0: DHCP
Management	eth0: 192.168.0.2/24

Table 3.6: Zone Configuration

Zone	Interface
Inside	Ethernet1/1
Outside	Ethernet1/2
VPN	Tunnel.1

Create a Tunnel Interface

WATCHING THE COLORED OF COLORED						- C	ı x
L 🖬 🛍 📘 🗗 🖅 🛷 🍯	Ctrl Alt 📭 🗨	Q @ Q 🔂					
) BruhloAlto - Mozilla Fir	efox					_	- 8
🊧 BruhloAlto	× +						
	🛈 💫 https://	192.168.0.1/?#network	::vsys1::network/inte	erfaces	⊠ ☆		s =
🚺 PA-VM	DASHBOARD	ACC MONITOR	POLICIES OBJ	ECTS NETWORK	DEVICE	nmit 🗸 🛛 🕇 🖿	±₁• Q
							G ()
E Interfaces	Ethernet VLA	AN Loopback Tunnel	SD-WAN		k		
Zones 👘		an Tredekovera <u>1</u> territer					
	Q(0 items	$\rightarrow \times$
Virtual Routers	INTERFACE	MANAGEMENT	IPADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FFATURES	COMM
🔨 IPSec Tunnels						· Fritenies	
CRE Tunnels							
麦 DHCP ッ							
DNS Proxy							
GlobalProtect							
Co Portais							
Gateways							
MDM							
Clientless Anns							
Concineas Appa							
Clientless App Groups							
Clientless App Groups							
Clientless App Groups							
Clientless App Groups Clientless App Groups Clientless							
Clientless App Groups Clientless App Groups Clientless App Groups Clientless							
Clientless App Groups Clientless App Groups Clientless App Groups Clientless							
Clientless App Groups Clientless App Groups CLDP Control GlobalProtect IPSec Gry Clientles Control GlobalProtect IPSec Gry Clientles Control IPSec Crypto Control IPSec Grypto C							
 Glientless App Groups QoS LLDP Network Profiles GlobalProtect IPSec Gry IKE Gateways IPSec Crypto IKE Crypto Monitor 							
 Glientless App Groups QoS LLDP ColobalProtect IPSec Gry KE Gateways IPSec Crypto IKE Crypto Monitor Interface Mgmt 							
 Glenitless App Groups QoS LLDP Network Profiles GlobalProtect IPSec Gry HKE Gateways IPSec Crypto IKE Crypto Monitor Interface Mgmt Zone Protection 							
 Clientless App Groups QuS LDP Network Profiles GlobalProtect IPSec Gry KE Gateways IPSec Crypto IKE Crypto Monitor Interface Mgmt Zone Protection OS Profile 	• Add - Dele	± □ PDF/CSV					
 Clientless App Groups QoS LLDP ColobalProtect IPSec Gry HKE Gateways IPSec Crypto IKE Crypto IKE Crypto Monitor Interface Mgmt Zone Protection OnS Brofile Startin Opsout Last Login Time 	Add → Dels 04/26/2022 - 18/35/	1 Session Expire Time:05	/26/2022 18:38:29]		⊠ X= jayes	Language 4/10 102	aloalto
 Glenness App Groups Clientless App Groups QoS LLDP Network Profiles GlobalProtect IPSec Cry HKE Gateways IPSec Crypto IKE Crypto IKE Crypto INetwork Profiles Cons Profile Interface Mgmt Cons Profile 	⊕ Add ⊖ Dele 04/26/2022-18;35:0	1 Session Expire Time: 05	/26/2022 18:38:29		⊠ ÿ≘ Ťasks	Language - 🚧 P	aloalto

Under **Network > Interfaces** in the Tunnel tab, click **Add**.

Figure 3.28: Creating a Tunnel

In the new window, change the virtual router to default, and the security zone to the VPN zone.

🚾 x11 - TightVNC Viewer				- 0	X
≞∎∎∎ ∎ 🖌	🌮 🗿 Chi Alt 🖺 🔍 🔍 🔍 🍭 🔂				1
😝 BruhloAlto - Mozil	la Firefox				_ @ ×
🥠 BruhloAlto	× +				
↔ ↔ ↔ ↔	(i) 🖍 https://192.168.0.1/?#network::vsy	/sl::network/interfaces 🗸 🗸	⊠ ☆		S =
OPA-VM	DASHBOARD ACC MONITOR PO	DLICIES OBJECTS NETWORK	DEVICE	it v 🖿 🤅	₽ <u>₹</u> + Q
Interfaces	Ethemer VEAN Loopback Tunnel S	D-WANL			60
	Q			0 items	$\rightarrow \times$
Virtual Routers	Tunnel Interface		0	FEATURES	COMM
CRE Tunnels CRE Tunnels CRE Tunnels CRE GIDBalProtect CRE GibbalProtect CRE Gateways CRE Gateways CRE Gateways CRE Clentless Apps CRE Clentless Apps CRE Clentless CRE Gateways CRE Gatew	Interface Name Comment Netflow Profile None Config IPv4 IPv6 Advanced - Assign Interface To Virtual Router default Security Zone VPN	. 1	× ×		
Interface Mg/nt R Zone Protection	Add Elect @ PDF/CSV	federa di fische I			
admini i Logouit i Last Logi	1 Time: 04/26/2002 18:35:01 - Session Expire Time: 05/26/	2022 LH/36829	M 3= links f i	autolare 🥠 pa	AIOaico
JWM _ 🚽 🔞 Bru	uhloAlto - Mozilla Firefox		J.		03:05

Figure 3.29: Tunnel Interface

Then click **OK**.

Enable User ACL for a Zone

Under Network > Zone,	click the VPN zone.
-----------------------	---------------------

x11 - TightVNC Viewer														
B 🖬 🗈 🔳 😏 🕫	» 🏨	Ctrl	Alt 📳	Q. Q. @	R 🔍 🔂									
🔰 BruhloAlto - Mozilla	Fire	efox	(_ a ×
🚧 BruhloAlto		×	+											
(←) → ⊂ @		0) 🔏 http	s://192.16	8.0.1/?#net	work::vsy	slanetwork	/zones			⊠☆			: Ξ
O PA-VM		DA	SHBOARD	ACC	MONITO	OR PO	LICIES	OBJECTS	NÉTWO	RK DE	VICE B	∔ ⊆ Commit ∨) I 🔁	₽₹×Q
														G 🕐
Interfaces	•	Q											5 ite	$\rightarrow \times$
Zones	5									User-ID	k		Device-ID	
			NAME	ТҮРЕ	INTERFA / VIRTUAL SYSTEMS	ZONE PROTEC PROFILE	PACKET BUFFER PROTEC	LOG	ENABLED	INCLUD NETWO	EXCLUD NETWO	ENABLED	INCLUD NETWO	EXCLUD NETWO
PSec Tunnels		Ē	Inside	laver3	ethernet1					any	none		anv	none
GRE Tunnels			Outside	layer3		ZoneProt			T	any	none		any	none
호 DHCP	•		VLAN10	layer3	ethernet1					any	none		any	none
DNS Proxy			VLAN20	layer3	ethernet1		10		0	any	none		any	none
GlobalProtect		n	VPN	layer3	tunnel.1					any	none		any	none
Cotemous		-					1.0							
C MDM														
Clientless Apps		4												
🔞 Clientless App Group	s													
des QoS														
ELLDP														
V 🛱 Network Profiles														
GlobalProtect IPSec C	3ry													
H IKE Gateways														
Di IPSec Crypto	1													
IKE Crypto	* II.													
Monitor														
Log Interface Mgmt														
Cos Protection		0	u no		FICAL									
THIS PROMP		(±)A	ad B	iete 🔘 PE	JF/CSV									
admin Logout Last Login T	(ime; (04/20	6/2022 18:	35:01 Ses:	sion Expire Tim	ne: 05/26/20	022 18:38:29	2				asks Lang	uage и	paloalto
JWM 📃 🚯 Bruk	NoA	lto -	- Mozilla	Firefox										03:06

Figure 3.30: Create a VPN Zone

Tick the **Enable user identification** box.



Figure 3.31: Enable User Identification under VPN Zone

Then press OK.

Generate Certs

🚾 x11 - TightVNC Viewer								-	- 0	×
🐴 🖬 😭 🗈 📕 😏 🛷 🐲	Ctrl Alt		Q. 🔂							
😫 BruhloAlto - Mozilla Fire	efox	_						_		_ 8 3
🊧 BruhloAlto	× +									
€ → C @	0 🔒 H	nttps://192.168	.0.1/?#device	::vsys1::devic	e/certificate-m	anagemen	⊠ ☆	10N		3 =
🚺 PA-VM	DASHBO	ARD ACC	MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE	↓ ⊆ Commit ~	🔁 🗉	≩• Q
									h.	G 🕐
User Identification Data Redistribution	Device C	Certificates Def	ault Trusted Cert	ificate Authoritie	is.					
Device Quarantine	0								0 items	X
VM Information Sources		AF SUBIE	CT ISSUE	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE	7 ~
Certificate Management		5055	100021		NL1	EATINES	514105	ALGORITHM	USAGE	
Certificates										
Cortificate Profile										
Certificate Profile										
CCSP Responder										
SSL/TLS Service Profile										
La SCEP										
🔒 SSL Decryption Exclusio										
SSH Service Profile										
Response Pages	4									
I on Settings										
Server Promes										
SNMP Trap										
Syslog										
Les Email										
HTTP										
Netflow										
RADIUS										
TACACS+										
Co LDAP										
C Kerberos										
SAML Identity Provider	G Delete	e Revoke Rena	w 🛓 Import	👼 Generate 💡	Export Certific:	ate 🖕 Import HA	Key 👖 Export I	HA Key 🙆 PDF/0	CSV	
admin Logout Last Login Time;	04/26/2022	18:35:01 Sessio	in Expire Time: 0	5/26/2022 18:3	8:29			asks Language	🥠 pa	loalto
JWM _ 📕 🍯 BruhloA	lto - Moz	zilla Firefox								03:0

Under **Device > Certificate Management > Certificates**, click on **Generate**.

Figure 3.32: Generate a certificate

Configure these settings in the new window:

Table 3.7:	Certificate	Generation
------------	-------------	------------

Parameters	Value
Certificate Name	Cert Name Here
Common Name	The DHCP IP of Ethernet1/2
Certificate Authority	Tick this box

162 Chapter 3. Advanced Networking



Figure 3.33: Generate a certificate

Then click Generate.

Create an SSL/TLS Service Profile

x11 - TightVNC Viewer				- 🗆 X
	🕻 Chri Alt 📭 🔍 🍳 🖗	R. Q. 🔂		
🔰 BruhloAlto - Mozilla Fir	refox			_ @ ×
🊧 BruhloAlto	× +	*		
← → ⊂ ŵ	🛈 🔏 https://192.10	58.0.1/?#device::vsys1::device	e/certificate-managemer: 😪 🚥 I	♥☆ ॥\ ₪ \$ ≡
🔷 PA-VM	DASHBOARD ACC	MONITOR POLICIES	OBJECTS NETWORK DEVI	CE (≝ Commit ∨) ि ⊡ v Q
				G O
Ser Identification	Q(0 items ightarrow imes
Data Redistribution Device Quarantine	NAME	LOCATION	CERTIFICATE	PROTOCOL VERSIONS
WM Information Sources				
X Troubleshooting				
💛 🧊 Certificate Management				
📰 Certificates				
Certificate Profile				
OCSP Responder				
SSL/TLS Service Profile				
LIS SCEP				
SSL Decryption Exclusio				
Response Pages				
Log Settings				
Server Profiles				
SNMP Trap				
Byslog				
Email				
НТТР				
I Netflow				
RADIUS				
TACACS+				
LDAP				
Kerberos				
SAML Identity Provider	🕀 Add 🕒 Dielete 💿 C	one DF/CSV		
admin Logout Last Login Time	: 04/26/2022 18:35:01 Ses	sion Expire Time: 05/26/2022 18:38	3:29 0	🗹 🗏 Tasks Language - 🊧 paloalto
JWM _ 🗧 🍯 Bruhlo/	Alto - Mozilla Firefox			03:08

Under **Device > Certificate Management > SSL/TLS** Service Profile, click **Add**.

Figure 3.34: Add SSL/TLS Service Profile

In the new window, add the certificate you generated.



Figure 3.35: Configure SSL/TLS Service Profile

Then click **OK**.

Create a GlobalProtect Portal

🗱 x11 - TightVNC Viewer								- □)
L 🖬 🖆 主 📕 🗲 🕫 🖁	😭 Ctri Alt 📭 🕀							
) BruhloAlto - Mozilla Fi	refox							_ 8
🚧 BruhloAlto	× + *							
A D C A	() & https://	//192 168 0 1/2#petw	orkuveve 1 unet	work/alobal-pro	atact/nortale		lux	m 📧 :
	Ma napsi	7192.100.0.1/:#fietw	DIKUASASTUUG	.work/global-pit	otect/portais	un O M	III V	
OPA-VM	DASHBOARD	ACC MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE	↓ ⊆ Commit ∨	ि िि रि
								GO
📾 Interfaces 🔹 🔹								0 items \rightarrow
Zones 🖤					SSL/TLS		Mar Maria	
	NAME	LOCATION	INTERFACE	IP	PROFILE	PROFILE	PROFILE	INFO
Virtual Wires								
Virtual Routers								
GRE Tunnels								
F DHCP								
DNS Proxy								
GlobalProtect								
S Portals								
🛃 Gateways								
MDM [
Sclientless Apps	-4							
Clientless App Groups								
des QoS								
2 LLDP								
 Network Profiles 								
GlobalProtect IPSec Cry	1							
H IKE Gateways								
IPSec Crypto *								
IKE Crypto								
Monitor •								
Interface Mgmt								
Cone Protection	Course and		00510011					
TOS Proble	HAdd Delet	e 🦷 Generate Ticket 🌘	DF/CSV					_
admin Logout Last Login Time	e: 04/26/2022 18:35:	:01 Session Expire Time:		38:29				🥠 paloalt
MM	Alto - Mozilla Fi	irefox						03

Under **Network > GlobalProtect > Portals**, then click **Add**.

Figure 3.36: Add a Portal
In the general tab, set the interface to Ethernet1/2.

x11 - TightVNC	Viewer				– 🗆 X
3 B f 🗈 🛛	😏 📾 🎉 Ctri Alt		∂		
🟮 BruhloAlto -	Mozilla Firefox				_ = ×
🋷 BruhloAlto	× +	-			
(←) → C ·	a 0 a	https://192.168.0.1/?#	#network::vsys1::network/global-pro	otect/portals 🛛 💀 🔂	III\ 🗉 🛎 🗏
P. DA MAR					
V PA-VM	DASHI	BOARD ACC MO	NITOR POLICIES OBJECTS		mmit~ ि मि≺ Q
					G ()
Interfaces	GlobalProtect Po	rtal Configuration		$\overline{\uparrow}$	$\textcircled{0 items} \rightarrow \times$
G VLANS	General	Name	GPPortal		INFO
Control Wires	Authentication	Network Settings			INPO
() Virtual Route	Portal Data Collection	Interface	ethernet1/2		~
GRE Tunnels	Agent	IP Address Type	IPv4 Only		~
E DHCP	Clientless VPN	IPv4 Address	None		~
DNS Proxy	Satellite	Appearance			_
GiobalProtei		Portal Login Page	factory-default		~
🚑 Gateway		Portal Landing Page	factory-default		~
MDM		App Help Page	None		$\mathbf{\nabla}$
Clienties Clienties		Log Settings			
A Qos			Log Successful SSL Handshake		
LLDP			Log Unsuccessful SSL Handshake		
V La Network Pro		Log Forwarding	None		~
于 IKE Gate					
PA-VM Ans Interfaces Zonés VIANS VIANS VIANS VIANS VIANS VIANS VIANS VIANS VIAN V					Cancel
E IKE Cryp	I - TightVHC Viewer III - TightVHC Viewer IIII - TightVHC Viewer IIIII - TightVHC Viewer IIII - TightVHC Viewer IIIII - TightVHC Viewer IIIII - TightVHC Viewer IIIII - TightVHC Viewer IIIII - TightVHC Viewer IIIIII - TightVHC Viewer IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII				
interface	MgmL				
R Zone Prot	Lection =				
Se Ons Brok	bbA 🕀 🔹	(m) Delais 🥂 Generalia ()	DEF/CSV		
adimin Lagout 1	Last Lagin Time: 04/26/20	022 18:35:01 Session Expli	Time: 05/28/2022 18:38:29		Elaunuare 🧤 paloalto
JWM _	ۏ BruhloAlto - M	lozilla Firefox			03:10

Figure 3.37: GlobalProtect Portal Configuration

x11 - TightVNC Viewer × 1 🖳 📓 🖺 📕 😏 🛷 🙀 Chi Alt 🐚 🔍 🔍 🔍 🐼 😫 BruhloAlto - Mozilla Firefox а× × + 🦇 BruhloAlto <) → C @ III\ 🗊 🔮 Ξ (i) 🚯 https://192.168.0.1/?#network::vsys1::network/global-protect/portals ... 🗵 🟠 PA-VM GO 0 items $\rightarrow \times$ (A) Interfaces **GlobalProtect Portal Configuration** 0 Zonès C VLANS General INFO Virtual Wire Authentication SSL/TLS Service Profile Certed (Virtual Rout Portal Data Collection 1 IPSec Tunne **Client Authentication** GRE Tunnels Agent ALLOW E DHCP Clientless VPN AUTHENT .. WITH USER CREDENT... 党 DNS Proxy Satellite AUTO V GlobalProte AUTHENTI ... RETRIEVE OR CLIENT CERTIFIC... USERNAME PASSWORD AUTHENT ... NAME os PROFILE LABEL LABEL MESSAGE Portals 🚑 Gatewa MDM Cilentie Clientie A Qos LLDP (+) Add ⊖ Delete 🐵 Clone ↑ Move Up ↓ Move Down Network Pr C GlobalP Certificate Profile None H IKE Gate 1 IPSec C E IKE Gry Cancel C Monitor interface R Zone Protection DPDF/CSV (+) Add paloalto 💻 🖲 BruhloAlto - Mozilla Firefox IWM 03:11

In the authentication tab, select SSL/TLS profile you created in the previous step, then click Add.

Figure 3.38: Adding SSL/TLS Profile

In the new window, change the authentication profile, then press **OK**.

躍 x11 - TightVNC Viewer	- 🗆 X
🖳 🖬 🖺 📕 🖅 🛷 🏨 cm Att 🐘 🔍 의, 🧠 🍭 🐼	
😜 BruhloAlto - Mozilla Firefox 🛛 🖗	_ 8 ×
☆ BruhloAlto × +	
← → C û ① A https://192.168.0.1/?#network::vsys1::network/global-protect/portals	
PA-VM DASHEDATO AND MONITOR POLICES DEJECTS METWORK CEVICE	tinnit v Ti Hi = Q
	60
ClobalDestat Destal Configuration	
Client Authentication	
VEANS. General	INFO
Authentication Name Clint	Y
(PSs. Time) Appr Authentication Profile Authentication Profile	
Clientiess VPN Satellite Clientiess VPN Satellite Clientiess VPN Satellite Clientiess VPN Satellite Clientiess VPN Satellite Clienties	ALLOW AUTHENT WITH USER CREDENT OR CLIENT CERTIFIC
INFECTOR profile in the Client Authentication configuration. E (RES) INFECTOR INFECTOR INFECTOR	

Figure 3.39: Adding Authentication Profile

🚾 x11 - TightVNC Viewer						- 🗆 X
🌯 🖬 😭 🖹 📕 😏 🛷 🙀 Ctri Alt		2				
📦 BruhloAlto - Mozilla Firefox						_ @ ×
🊧 BruhloAlto 🗙 🕂	-					
<>> ℃ ŵ 0 €	https://192.168.0.1/?#	fnetwork::vsysl::netwo	rk/global-p	protect/portals •••• (9 ☆	III\ 🗊 🔹 🗏
	BOARD ACC MO	NITOR POLICIES	OBJECTS	NETWORK DEVI	CE 🚺 Commit ~] È ⊮a < Q
						G ()
GlobalProtect Po	rtal Configuration					$\underbrace{\text{0 items}}_{\text{0 items}} \rightarrow \times$
General	Agent				*	
Virtual Wires Authentication Virtual Route Portal Data Collection	CONFIGS	USER/USER GROUP	OS	EXTERNAL GATEWAYS	CLIENT CERTIFICATE	INFO
GRE Tunnels Agent						
E DHCP Clientless VPN						
GlobalProte						
Gateway						
	⊕ Add ⊖ Delete 🔞 0	Clone ↑ Move Up ↓ M	love Down			
Clienties		INSTALL IN LOCAL	1	Agent User Override Key		
A QoS	TRUSTED ROOT CA	STORE	Cor	nfirm Agent User Override Key		
V 🛱 Network Pro						
田 GlobalPo 刊 IKE Gate	() Add () Delete					
台 IPSec Cn	C Aud O Delete					-
A Monitor				-	OK Cancel	5
Tope Profession						×
Add		el er @ PDF/CSV				
edimin Lagout Last Lagin Time: 04/26/20	022 18:35:01 Session Explin	e Time: 05/28/2022 18.38;	295	E	🛛 🛛 👔 Tarks I Laug	uare 🦛 paloalto
JWM _ 📕 😉 BruhloAlto - M	lozilla Firefox					03:12

In the agent tab, in the agent section, click **Add**.

Figure 3.40: Adding the agent

In the internal tab in the Internal gateway, click **Add.**

x11 - TightVNC	Viewer				– 🗆 X
3 B 🖬 🗈	📕 🗲 🕫 🏭 Ctri Alt 🐴	e , e, @, 💀			
😫 BruhloAlto	- Mozilla Firefox				_ @ ×
🊧 BruhloAlto	× +	τ			
€ → C	û 🚯 https	s://192.168.0.1/?#network	::vsys1::network/global-protect/porta	s ••• 🗵 🟠	
Ø PA-VM				RE ELECTE Lander) te e q
in tourist	Configs			(
	Authentication Config Sel	ection Criteria	External App HIP Data Collection		ilvsó
🗐 Vistal P	- Internal Host Detection IPv	4	Internal Host Detection IPv6		
C IPSS. Torres	IP Address		IP Address		
E DISCP	Hostname		Hostname		
DWS Prove	Internal Gateways				
Portals	NAME	ADDRESS	SOURCE IP	DHCP OPTION 43 CODE	
Contraction Contra				Specify one or more sub-option codes (in decimal). GlobalProtect Agent will read the gateway address from values defined by the sub- option codes.	
E IPSA C		ve Up 👃 Move Daiws		⊕ Add ⊖ Delete	
E Monte					
Riterie Riterie				OK Cancel	
and the set	Letter out <u>1977 - 1</u> 5 -	a Secolar In a			🏀 paloalto
JWM _	🍯 BruhloAlto - Mozilla	Firefox			03:13

Figure 3.41: Configure Internal Gateway

x11 - TightVNC Viewer × 1 🖳 📓 🖹 📕 😏 🛷 🙀 Chi Alt 🐚 🔍 🔍 🔍 👰 😫 BruhloAlto - Mozilla Firefox а× 🊧 BruhloAlto × + <) → C @ Ξ () 🚯 https://192.168.0.1/?#network::vsys1::network/global-protect/portals ... 🖾 🟠 111\ 🗉 🔮 1 Configs Authentication Confi Internal Gateway 1 Internal Host Detectio Name names Address O FODN O IP IPv4 192.168.122.253 Internal Gateways IPv6 NAME CP OPTION 43 CODE SOURCE ADDRESS ^ Select address or enter IP subnets or ranges (e.g. 192.168.74.0/24, 192:168.75.1-192.168.75.100) ⊕ Add ⊖ Delete Cancel (+) Add - Denere Cancel 🖲 BruhloAlto - Mozilla Firefox 03:13 IWM

In this window, change the Address to select IP, and in the IPv4 box, type in the IP of Ethernet1/2.

Figure 3.42: Set the IP address for Internal Gateway

Press **OK** twice to get back to the agent tab. Then in the trusted root ca section, add your generated cert, and tick the box to install in local root certificate store.

x11 - TightVNC Viewer							-		×
🖹 🖬 🖀 🖺 🛃 🕾	🔊 🙀 Ctri Alt 📔								
🔮 PA-VM - Mozilla Fire	efox							-	а×
A-VM	× +								
(←) → C @	0 🔏	https://192.168.0.1	/?#network::vsys1::netv	vork/global-	protect/portals •••• (⊴ ☆			Ξ
O PA-VM	DASHBOA	ARD ACC N	IONITOR POLICIES	OBJECTS	NETWORK DEVIC	E E Camp		मे भिके भ	Q
(G	0
Global	Protect Porta	al Configuration					0	1 item -	→×
General General	-	Agent						VFO	
Virtual Wires Authenti	cation ata Collection		USER/USER GROUP	os	EXTERNAL GATEWAYS	CLIENT CERTIFICATE			
CRE Tunnels Agent DHCP Clientless DHCP Stellite Clientless Satellite Portals Converse	s VPN	agent	any	any					
		(+) Add	S Clane T Move Up 1	Mave Dewn					
		TRUSTED ROOT	INSTALL IN LOCAL ROOT CERTIFICAT CA STORE	E Co	Agent User Override Key				
- Ca Network Pro		FreeCCNA							
回 GlobalPn 开 IKE Gato 回 IPSec Gn		⊕ Add ⊖ Delete							
A IKE Ovja						OK Cance	et)		
Zone Protestion	_	_	_	_			_		
A MAS Brofila	E bbA (🔵 Delete 🧠 Generat	e Ticket () PDF/CSV						
Hanni Lopiol Last Lagin	lime, 24/24/202	2 Dir/23.05 Session E	ристин-сэлрэндар — с	828	E			paloa	alto
JWM	VM - Mozilla	Firefox						(08:26

Figure 3.43: Add the Root CA certificate

Then press **OK**.

Create a GlobalProtect Gateway

🚾 x11 - TightVNC Viewer		- 🗆 X
	🕻 cm Att 📭 🔁 🔍 🔍 🔍 🐼	
😫 BruhloAlto - Mozilla Fir	refox	_ @ ×
A BruhloAlto	x +	
(←) → C @	(i) 🗞 https://192.168.0.1/?#network::vsys1::network/global-protect/gatew. 🚥 💟 🏠	
🚺 PA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE 📥 Commit 🗸] ͡ਦ ⊮+ Q
		G (?)
Interfaces •	<u>d</u>	$0 \text{ items} \rightarrow X$
Zones 🔹	NAME LOCATION LOCAL INTERFACE LOCAL IP TUNNEL MAX USER	INFO
Wirtual Positers		
PSec Tunnels		
GRE Tunnels		
호 DHCP ····································		
DNS Proxy		
V 😤 GlobalProtect		
S Portais		
Gateways		
MDM		
Clientless Apps		
Clientless App Groups		
V Retwork Profiles		
GlobalProtect IPSec Crv		
H IKE Gateways		
🔒 IPSec Crypto 👘		
🔁 IKE Crypto 👘		
🖰 Monitor 👘		
interface Mgmt 👘		
Zone Protection		
A Oos Profile	Add Delete Delete PDF/CSV	
admin Logout Last Login Time	: 04/26/2022 18:35:01 Session Expire Time: 05/26/2022 18:38:29 🖂 🖂 🖂 🖂 🖂 🖂 🖂 🖂 🖂 🖄	uage 🛷 paloalto
JWM Sruhlo	Alto - Mozilla Firefox	03:15

Under **Network > GlobalProtect > Gateways**, click **Add**.

Figure 3.44: Add a Gateway

In the general tab, set the interface to Ethernet1/2.

🗱 x11 - TightVNC Viewer				-	□ ×
🖹 🖬 🗊 🔳 😏 🛷	🚮 ctri Att 📭 🔍 🔍	@ @ ₺			
🖕 PA-VM - Mozilla Firef	ox				_ a ×
NA-VM	× +				_
€ → C û	🛈 🔏 https://192.1	68.0.1/?#network::vsysl::network/global-protect/gatews	⊡ ☆		≝ ≡
O PA-VM	DASHBOARD ACC	MONITOR POLICIES OBJECTS NETWORK		· È	₽Q
GlobalProtec	t Gateway Configurati	on		0	60
General	Name	gatedway			x∉ mu
Addictication Agent	- Network Settings	ethernet1/2		×	Maire
Wintue Satellite	IP Address Type	IPv4 Only I		~	
1PSet	IPv4 Address	None		\sim	
GRET	Log Settings			_	
E DHCP	C	Log Successful SSL Handshake			
- Gula		Log Unsuccessful SSL Handshake			
C P	Log Forwarding	None		~	
C M				_	
The C				Cancel	
Dos					
- C Network Profiles					
E GlobalProtect (PSec Dry	e.				
TT INE GATEWAYS					
A INE Crypto					
B Manitor					
Minterface Mgmt					
🕞 Zune Protection					
A nac Brafila	Add . : (ii)	PDF/CSV			
Logical Lost Login Tin	ne, 04/24/20/22/21/23.05 - Se	salon Equile Trans 09/05/00/2010.0208	⊠ / 待 ! — .	1 1 10	paloalto
JWM _ BA-VI	M - Mozilla Firefox				08:35

Figure 3.45: GlobalProtect Gateway Configuration

🚾 x11 - Tigh	tVNC Viewer									-	
B 🖬 🕅 [l 9 @	😭 Ctr	I Alt 🖻	Q Q @	V 🛛 🔁						
Bruhlo/	Alto - Mozilla F	irefo.	x								_ a ×
	Alto	×	+								
$(\epsilon) $	C D		D 🚯 https	://192.168.0	.1/?#network::vsys	1::network/g	lobal-protect/	gatew. •			
0 PA-\	M	D	ASHBOARD	ACC	MONITOR PO	LICIES OI	JECTS NE	TWORR L	DEVICE	Commit ~	T PT × Q
	GlobalProtect	Gate	eway 🕀ni	figuration						0	50
🖾 Interf	General	Serv	ver Authentica	tion							$\times \leftarrow sms$
Cones Cones	Authentication	1	SSL/TLS Servi	ce Profile Certe	łd					×	
Co Virtue	Satellite	Clie	nt Authenticat	ion							
Virtua			NAME	OS	AUTHENTICA PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC MESSAGE	ALLOW AUTHENTIC WITH USER CREDENTIALS OR CLIENT CERTIFICATE	
V C Globa P C C C C C C C C C C C C C C C C C C		÷	Add Del	ete 💿 Clone te Profile None	92.168.0.1/7#network:tvsys1::network/global-protect/gatew V V M ACC MONITÓR POLICIES OBJECTS NETWORK DEVICE COMMENT ration of AUTHENTICA AUTO NOTHERE OS AUTHENTICA AUTO RETRIEVE USERNAME PASSWORD AUTHENTIC WITH USER CERTIFICATE PASSCODE LABEL PASSWORD AUTHENTIC OB CLIENT MESSAGE CERTIFICATE Block login for quarantined devices CERTIFICATE Block login for quarantined devices CERTIFICATE Block login for quarantined devices						
日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日	unica terface Mgint = me Protection =			Z Bi	ock login for quarantine	d devices			ОК	Cancel	
	as straine	(T)		Em Seedon	SV Evnire Turner ()570-140	122-18-38-00-1					a naloalto
	Bruble	Alto	- Mozilla	Firefox	- quire interest and the					Contracting of	03:16

In the Authentication tab, add your **SSL/TLS** profile, then click **Add**.

Figure 3.46: SSL/TLS Service Profile

In the new window, sele	t your authentication	profile, then click OK .
-------------------------	-----------------------	---------------------------------

🚾 x11 - TightVNC Viewer		– 🗆 X
1 🔄 🗃 🖹 📕 😏 🥶 🏨 Ciri Ait 🗈 🍭 옥 🔍 🤆	R 🔁	
📦 BruhloAlto - Mozilla Firefox 🛛 🖓 🖗		_ @ ×
✤ BruhloAlto × +		
(←) → C ⁴	0.1/?#network::vsys1::network/global-protect/gatewa 💀 👽 🛧	III\ 🗊 🔹 🗏
PA-VM DASHEDARD AND		mute निक्ति Q
GlobalProtect Gateway Configuration		0 50
General Server Authentication		uis \rightarrow X
Authentication Client Authentication	0	×
Agent Agent Name Name	Clint	
OS OS	Any	DW HENTIC
Authentication Profile		H USER DENTIALS
GlobalProtect App Login Screen	Automatically retrieve passcode from SoftToken application	TIFICATE
Username Label	Username	
Password Label	Password	
Authentication Message	Enter login credentials	
5 a		
T LLDP	Circleal Server Authentication Authenticatio Authenticatio Agent Satellize Client Authentication Agent Satellize Client Authentication W HENTIC. Satellize U Name Clint Authentication Profile Satellize U Satellize ClobalProtect App Login Screen U Satellize U Satellize ClobalProtect App Login Screen U Satellize ClobalProtect App Login Screen D Satellize D Satellize ClobalProtect App Login Screen D Satellize D Satellize ClobalProtect App Login Screen D Satellize D Satelli	
Allow Authentication with User	No (User Credentials AND Client Certificate Required)	<u> </u>
Credentials OR Client Certificate	To enforce client certificate authentication, you must also select the certificate profile in the Client. Authentication configuration.	
12. IP		Cancel
22 Manual and	OK Cancel	
W I un fam Ment		
The Post of the Control of Contro		
	B h and balance A	// paloalto
		02.16
		05.10

Figure 3.47: Authentication Profile

Under the agent tab, in tunnel settings, tick the tunnel mode checkbox and select the tunnel you made.

🚾 x11 - TightVNC Viewer		- 🗆 X
🏝 🖬 🗊 📕 😏 🛷	🗿 Chi Alt 🗞 🔍 🔍 🔍 🔍 🔀	
🔮 BruhloAlto - Mozilla f	Firefor	_ 8 ×
🥠 BruhloAlto	× +	
← → C ŵ	(i) 🗞 https://192.168.0.1/?#network::vsysl::network/global-protect/gatew ♡ ☆	
OPA-VM		tr म•< Q
GlobalProtec	t Gateway Configuration	0 50
General Authentication VLAN VIAN VIAN VIAN VIAN VIAN VIAN VIAN VI	Tunnel Settings Client IP Pool Network Services Connection Settings Video Traffic HIP Notification Image: Tunnel Interface Tunnel.1 Max User [1 - 15] Image: Tunnel Interface Image: Tunnel Interface Image: Tunnel Interface Image: Tunnel.1 Image: Tunnel Interface Image: Tunnel.1 Image: Tunnel Interface Image: Tunnel.1 Image: Tunnel Interface Imag	ion sns → X
Construction Cons	Y	cel 202117
JWM _ 🚽 🕹 Bruhl	loAlto - Mozilla Firefox	03:17

Figure 3.48: Tunnel Mode and Interface

In client settings, click **Add**.

ightVNC Viewer								-	
1 🗈 🛛 1 🔊	🦛 🛤	tri Alt 🖻		æ					
oAlto - Mozilla	Firefo	xc	1						_ 8
loAlto	×	+							
CÔ		🛈 🔏 http	os://192.168.0.1/	?#network::vsys	s1::network/global-	-protect/gatew	v 🛛 t		۳ =
-\/M								o	
Child	1.6.1	DASHBOARD	D ACC M	ONITOR PO	LICIES OBJECT	5 NETWORK	DEVICE	Commit -	I ₩A + C
GlobalProte	ct Gai	teway Cor	nnguration					0	GO
orf: General	Tur	nnel Settings	Client Settings	Client IP Pool	Network Services	Connection Sett	ings 🕴 Video Tra	ffic HIP Notification	swe $ ightarrow$
Authentication Agent	Q(0 items) $\rightarrow \times$	
Satellite					Source	e Address			
20	-	CONFICS	LISEDS	05	REGION		IRPOOL	INCLUDE ACCESS	
		_							
P.	\oplus	Add Date	ete 🛞 Clone 🕴 I	Move Up J. May	ve Down				
G								Cancel	
IR IP SPECE TABLE									
IKE Crypto									
Monitor									
Zone Protection									
nas Brafile	Œ	Add -	PDF/CSV						
OAS Réafic Lagout I Last Lagan Tr	(me) 04	Add	alaa (i) PDF/CSV 35:01 Session Exp	ire Time: 05/26/26	322 18,38,29			🗄 tasko i Language - 4	paloalto

Figure 3.49: Client Settings

BruhloAlto BruhloAlto Mare Clind Config Selection Criteria Authentication Override IP Pools Split Tunnel Network Services Config Selection Criteria Authentication Override PA-VM Config Selection Criteria Config Selection Criteria Mare Clind Config Selection Criteria Config Selection Criteria Mare Clind Config Selection Criteria Config Selection Criteria Config Selection Criteria Mare Clind Config Selection Criteria Confi
 BruhloAlto - Mozilla Firefox → BruhloAlto × + → C û https://192.168.0.1/?#network::vsys1::network/global-protect/gatew. Configs Configs Configs Config Selection Criteria Authentication Override IP Pools Split Tunnel Network Services Name Config Selection Criteria avy Source USER For an avy Source USER Add Deletic Add Deletic
 BruhloAlto x + BruhloAlto x + BruhloAlto x + BruhloAlto x + BruhloAlto x x
 Configs Configs
Configs
Global Config Selection Criteria Name Clind Name Clind Name Clind Config Selection Criteria Name Clind Name Clind Config Selection Criteria Name Clind Config Selection Criteria Image: Co
Image: Authentic Authentic Config Selection Criteria Image: VLAN Agent Image: Authentic Image: VLAN Source User Image: Authentic Image: VLAN Source User Image: Authentic Image: VLAN Source User Image: Authentic Image: VLAN Image: Authentic Image: Authentic Image: VLAN Source User Image: Authentic Image: VLAN Image: Authentic Image: Authentic Image: VLAN Image: Authentic Image: Authentic Image: VLAN Image: Authentic <td< td=""></td<>
Authenth Config Selection Criteria Image: Virial Satellite Image: Virial Satellite
Agent any Satellite Source user Source user Drop Drop Drop Output Comp Output
Source user A
CRCT EDCP DNCT DNCT Com Com
E Dice Dice Comp (*) Add Obelete (*) Add Obelete
Add ⊖ Delete
Add Delete
Source Address
REGION A IPADDRESS A
25 LLDP
Lance)
Add Delete
2 Meyeta
I II. 14 - Moon The configuration must match User and OS and either Region or IP Address if specified.
8 Tac Burn
https://192.168.0.1/?#

Make sure the **Any** checkbox is ticked on top of the OS category, then press **OK**.

Figure 3.50: Select Client as Any

In client IP pool settings, add an IP pool range of this:

🗱 x11 - TightVNC Viewer		-	
<u>≞∎∎∎∎ ∎ 9</u> @	🙀 Chri Alt 陆 🤁 🔍 🔍 🔍 🔯		
Novilla f BruhloAlto - Mozilla f BruhloAlto	Firefox +		_ a ×
← → ♂ ŵ	🛈 👰 https://192.168.0.1/?#network::vsys1::network/global-protect/gatew/	··· 🛛 🕁 💷	≣ ®
O PA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK	DEVICE	Par Q
GlobalProtec	t Gateway Configuration	0	G ()
General Cones Authentication	Tunnel Settings Client Settings Client IP Pool Network Services Connection Settings IP POOL	Video Traffic HIP Notification	ems → ×
Virtua Virtua Satellite IPSec	172.16.10.1-172.16.10.10		
OHE RET			
G	Add Delete Move Up Move Down		
	These IPs will be added to the firewall's routing table	OK Cancel	
Construction ・ Construction Construction ・ KE GlobalProtect IPSec Con ・ 新 IKE Gateways ・ IPSec Crypto ・ 目的をついます。 ・ KE Crypto	v		
Monitor	⊕ Add @ PDF/CSV		
edimin Lagout Last Lagin Tri	ne: 04/26/2022 18:35:03 Session Expire Time: 05/26/2022 18:38:29	🖂 🎉 Tasko Lauguare 🛷	paloalto
JWM _ Bruh	oAlto - Mozilla Firefox		03:20

172.16.10.1-172.16.10.10

Figure 3.51: IP Pool Configuration

Then press **OK**. Don't forget to commit the configuration!

Install the GlobalProtect Client on Kali

Open up a terminal window and run the following commands:

```
#curl -L https://bit.ly/32Ljx1y --output GP.deb
#sudo dpkg -i GP.deb
#globalprotect connect -p [IP of Palo Alto Ethernet1/2 Here]
```

When connecting, it will show an error about validation. Type in y then press enter.

It will also ask for your username and password. Enter the one you created prior.



Figure 3.52: Installing GlobalProtect on Kali Linux

Test Remote Access VPN

On Kali, after connecting to GlobalProtect, navigate to the IP of the WordPress Server (Internal).



Figure 3.53: Verify your configuration

If everything was correct, it should display the WordPress site!

3.3 Site-to-Site VPN

Learning Objectives

- Configure site-to-site VPN
- Configure static routing

Prerequisites:

- Create Zones on both firewalls
- Create a tunnel interface on both firewalls
- Create a policy to allow VPN to Inside on both firewalls
- Create a policy to allow Inside to VPN on both firewalls
- Interface configuration
- Knowledge of previous labs

Scenario: This one is a bit tricky since you will be managing both devices. A site-to-site VPN is what your company would set up if you had offices in other locations without being directly connected to each other. But in this lab, we'll just take it easy and assume that they have a direct connection to each other. So, we are going to configure site-to-site VPN between two Palo Alto firewalls. Then, you should be able to ping from client-1 to client-2.



Figure 3.54: Main scenario

Table 3.8: Addressing Table

Device	Configuration
Site-1	management: 192.168.0.1/24 Ethernet1/1: 10.0.0.1/24 Ethernet1/2: 1.1.1.1/24
Site-2	management: 192.168.0.2/24 Ethernet1/1: 172.16.10.1/24 Ethernet1/2: 1.1.1.2/24
Site1-Client	eth0: 10.0.0.2/24 GW: 10.0.0.1
Site2-Client	eth0: 172.16.10.2/24 GW: 172.16.10.1
Management1	eth0: 192.168.0.3/24

Table 3.9: Zone Configuration for Site1

Zone	Interface
Inside	Ethernet1/1
VPN	Ethernet1/2, tunnel.1

Table 3.10: Zone Configuration for Site2

Zone	Interface
Inside	Ethernet1/1
VPN	Ethernet1/2, tunnel.1

Create an IKE Gateway

🚾 x11 - TightVNC Viewer									- 0	×
B B B B I 5 8 ;	😭 Ctrl	Att 📭 🕀	Q @ Q .							
🔮 BruhloAlto - Mozilla Fi	refo>	ĸ							-	а×
🊧 BruhloAlto	×	+								
€ → C @	0	D 🔏 https://	/192.168.0.1/?#ne	twork::vsys1::r	etwork/network-	profiles/ike-g	⊚ ☆		III\ 🗉 🔮	Ш
OPA-VM	DA	ASHBOARD	ACC MONIT	OR POLICI	es <u>objects</u>	NETWORK	DEVICE	计 Commit 🗸	_ ाकिस्≁	Q
									G	0
interfaces 🔹	Q								0 items	$\rightarrow \times$
Zones 👘				Loc	al Address	F	Peer ID		Local ID	
gig VLANs Po Virtual Wires		NAME	PEER AD DRESS	INTERFACE	IP	ID	TYPE	ID	TYPE	
Virtual Routers PSec Tunnels CD5 Tunnels										
DHCP ₩										
DNS Proxy										
GlobalProtect										
Cotewovic a										
C MDM										
Clientless Apps	4									
Clientless App Groups										
des QoS										
tldp.										
V 🗟 Network Profiles										
GlobalProtect IPSec Cry										
T IKE Gateways										
IPSec Urypto										
Monitor										
Interface Mgmt										
Zone Protection	-									
A Oos Profile	(H)	Add 🗇 Delete	e 🕅 Enable 🚫 Dis	able 📵 PDF/CS	v					
admin Logout Last Login Tim	e: 04/2	6/2022 18:35:		0						
		() ROFF TO 0000	01 Session Expire Tir	ne: 05/26/2022 1				Tasks Lane	uage 🛷 paloa	lto [.]

Under **Network > Network Profiles > IKE Gateways**, click **Add**.

Figure 3.55: Add an IKE Gateway

On the Site1 firewall, configure these settings:

Parameter	Value
Interface	Ethernet1/2
Local IP Address	1.1.1.1/24
Peer IP Address Type	IP
Peer Address	1.1.1.2
Pre-shared Key	Password Here
Confirm Pre-shared key	Confirm Password Here



Figure 3.56: Site1 Firewall: IKE Gateway Configuration

Then press **OK**.

On the Site2 firewall, configure these settings:

Parameters	Value
Interface	Ethernet1/2
Local IP Address	1.1.1.2/24
Peer IP Address Type	IP
Peer Address	1.1.1.1
Pre-shared Key	Same Password as before here
Confirm Pre-shared key	Confirm same password as before here

Table 3.12: Site2 IKE Gateway Configuration

Image: Image	x11 - TightVNC Viewer		- 🗆 X
BruhloAkto - Mozilla Firefox	BBBB I 9 @	🏚 ctri Att 🐴 🔍 🔍 🔍 🍭 🔂	
BruhloAto X +	🜒 BruhloAlto - Mozilla F	irefox	_ d ×
	🛷 BruhloAlto	× +	
CONTROL ACC MONTOR POLCES Objects NETWORK Device Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control <th>↔ ↔ ↔ ↔</th> <th>🛈 🔬 https://192.168.0.1/?#network::vsys1::network/network-profiles/ik</th> <th>e-g ••• ⊠ ☆ IIN @ © ≡</th>	↔ ↔ ↔ ↔	🛈 🔬 https://192.168.0.1/?#network::vsys1::network/network-profiles/ik	e-g ••• ⊠ ☆ IIN @ © ≡
KE Gateway Wrust Wree Wrust Wree <td>🚯 PA-VM</td> <td>DASHBOARD ACC MONITOR POLICIES OBJECTS NETW</td> <td>ORK DEVICE 🛃 Commit~ 한 편~ Q</td>	🚯 PA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETW	ORK DEVICE 🛃 Commit~ 한 편~ Q
Zones Within Whee Within Whee Within Whee Within Works Within Works <td< td=""><td>Interfaces .</td><td>KE Gateway</td><td>€ ①</td></td<>	Interfaces .	KE Gateway	€ ①
Writelin Writelin Name ID TVPE Writelin Writelin Roberts Writelin Name StatedWay2 Writelin Writelin Made Solutions Name StatedWay2 Writelin Writelin Made Solutions Name StatedWay2 Vortelin Name StatedWay2 Writelin Writelin Writelin Made Solutions Name StatedWay2 Vortelin Vortelin Name StatedWay2 Vortelin Vortelin Name StatedWay2 Vortelin Vortelin <t< td=""><td>VLANS</td><td>General Advanced Options</td><td>Local iD</td></t<>	VLANS	General Advanced Options	Local iD
CRE Tuwels HCP DNS Proxy Coloral Protect Porcials Coloral Protection Porcials Porcials Porcials Porcials Coloral Protection Porcials Porc	Virtual Wires Virtual Routers = dl IPSec Tunnets	Name GatedWay2	ID TYPE
GladestProtect © Rorcals © Gateways © MDM © Cateways © Montess Apps © Olentiess Apps © Confirm Pre-shared Key Local Identification None © Confirm Pre-shared Key © Confirm Pre-shared Key © Confirm Pre-shared Key © Noc Doreflex © Noc Doreflex © Noc Doreflex © Doc Doreflex	GRE Tunnels GRE Tunnels DHCP = ONS Proxy	Address Type O IPv6 Interface ethernet1/2	~
Peer Address 11.1 Authentication Pre-shared Key Clientitess Apps Clientitess App Groups Confirm Pre-shared Key Confirm Pre-shared Ke	GlobalProtect	Local IP Address 1.1.1.2/24 Peer IP Address Type O IP C FQDN Dynamic	Y
Clientless App Groups Quis LLDP Confirm Pre-shared Key None Peer Identification None Comment Confirm Pre-shared Key Confirm Pre-shared Key Comment Confirm Pre-shared Key Confirm Pre-shared Key Comment Confirm Pre-shared Key Confirm Pre-shared Key Confirm Pre-shared Key Comment Confirm Pre-shared Key Confirm Pre-shared Ke	Chentess Apps	Peer Address 11.1.1 Authentication O Pre-Shared Key Certificate	~
W dos Confirm Pre-shared Key ILDP Local Identification None Image: State Crypto INFE Crypto Image: State Crypto Image: NEE Crypto Image: State Crypto Image: State Crypt	Clientless App Groups	Pre-shared Key	
Add Codes Cod	CLUDP	Confirm Pre-shared Key	
IMAR Gateways Comment Image: Protection Image: Protection	ClobalProtect IPSec Gry	Peer Identification None	
	H IKE Gateways	Comment	OK. Cancel
I General Gener	Monitor Monitor	⊕ Add = Delter in Englis = Desplis @/PDF/CSV	
IWM BruhloAlto - Mozilla Firefox 03:24	Server Lugoret Last Loger Ter	na 04/22-2022 23/3501 Session Expire Timm 05/26/2022 18:38:29	🖾 🗄 talk Linear 🥠 paloalto:
		oAlto - Mozilla Firefox	03:24

Figure 3.57: Site2 Firewall: IKE Gateway Configuration

Then press **OK**.

Create an IPsec Tunnel

Under **Network > IPsec Tunnel**, click **Add**.



Figure 3.58: Site1 Firewall: Add an IPsec Tunnel

On both firewalls, configure these settings:

Parameters	Value		
Tunnel Interface	tunnel.1		
IKE Gateway	The one you created on the respective firewall		

Table 3.13: IPsec Tunnel Configuration

🚾 x11 - TightVNC	Viewer		- 🗆 X
-	📕 😔 😹 chi Alt ы 🔍 🔍 🔍 🔍 🕄		
😢 BruhloAlto	- Mozilla Firefox		_ a ×
🦔 BruhloAlto	x +		
(a) a			
6 - 6	1 M Mttps://192.168.0.1//#network::vsys1::network/ipsec-tunnels	@ 꾜	
🚺 PA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK	DEVICE	umit~ Tr Fr Q
🖾 Interfaces	IPSec Tunnel		
Zonès	General Proxy IDs		
Contract Wire	Name Site1	•	
(Virtual Rout			
1 IPSec Tunne	Type O and the O starting of starting		
GRE Tunnels	Address Type		
E DHCP			
	INE Gateway Gatedway		~
Portais	Show Advanced Options		~
Gateway	Comment		
Clientie		OK	Cancel
des QoS		- And -	Cancer
LLDP			
V La Network Pro	hips		
THE IKE Gate	Ways		
E IPSec Cr	nto -		
E IKE Gryp	0		
🕑 Monitor			
interface	Mgint =		
🦻 Zone Pr	tectión =		
📥 Oos Dio	% ● Add (=) Extend () Enacle () Clastile @ PDF/CSV		
admin Lagout	Last Lagin Time: 04/26/2022 18:35:01 Session Expire Time: 05/26/2022 18:38:29	M #Elake	Lanzalaze 🧼 paloalto
JWM _	🕹 BruhloAlto - Mozilla Firefox		03:26

Figure 3.59: Site1 and Site2 Firewall: IPsec Tunnel Configuration

Create Static Routes

Under **Network > Virtual Routers**, click default.



Figure 3.60: Virtual Routers Configuration

Under the static routes tab, click **Add**.

x11 - TightVNC	Viewer											- 0	×
- <u>-</u>	📕 🗲 🔊 🙀 Ctri Alt		Q Q @	۹ 💀									
😫 BruhloAlto	- Mozilla Firefox			R.								-	a×
🤲 BruhloAlto	× H	-											
€ → C	û 🛈	http	s://192.16	8.0.1/?#nei	twork::vsys	slanetwor	k/virtual-ro	uters	•••	⊠ ☆	101	•	Ξ
🚺 PA-VM	DASHI	BOARD	ACC	MONIT	OR PO	LICIES	OBJECTS	NETWO	rk de	VICE	🛓 Commit 🗸	<u>₹</u>	× Q
🖾 Interfaces	Virtual Router - d	efault	:		_	_	_			_	00	1 item	$\rightarrow \times$
Zones	Router Settings	IP	v4 IPv6									RUNTIN	E
Virtual Wires	Redistribution Profile	Q	C							ļ	0 items \rightarrow \times	More Ri Stats	othing
PSec Tunnel	RIP					Ne	ext Hop						
GRE Tunnels	OSPF		NAME	DESTINA	INTERFA	TYPE	VALUE	ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE		
DNS Proxy	OSPFv3												
V CiobalProtei.	Multicast												
Gateway													
Clienties													
Clientles													
V G Network Pro													
H IKE Gate		Ð		lete 🕲 Clor	ie								
回 IPSec Cr 图 IKE Cryp		0	0.5										
Honitor										ок	Cancel		
🐼 Interface	stattien		-	_	_	_	_	_	_				
A Ons Bin	nio 🔹 🕀 Add	ΘDe	elete 🔘 PD	F/CSV									
admin Logorit	Last Login Time: 04/26/20	022 18:	35:01 Sess	ion Expline Tir	ne: 05/26/26	122 18.38,2	8				Tanks I Language	🦏 palo	alto
JWM _	😸 BruhloAlto - M	lozilla	Firefox										03:27

Figure 3.61: Add a Static Route in the Site1

On the Site1 firewall, configure these settings:

Parameters	Value
Destination	172.16.10.0/24
Interface	tunnel.1
Next Hop	None

Table 3.14: Site1 Static Route Configuration

躍 x11 - TightVNC Viewer	- 🗆 X
<u>백</u> 🖬 🖆 📕 😔 😹 Chi Alt 🐚 연 🔍 🔍 🔍 🔂	
😜 BruhloAlto - Mozilla Firefox	_ a ×
(←) → C' (i) https://192.168.0.1/?#network::vsys1::network/virtual-routers ···· ♥	
CPA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE	📥 Commut 🐖 🗇 🖅 - Q
Virtual Router - Static Route - IPv4	0 00
Name OtherSite	
VENVa Statle Parties Destination 172.16.10.0/24	→ STATS
Static Routes Interface tunnel.1	✓ Ditems → ×
Virtual Rout Next Hop Next Hop None	
C CRE To 240	ROUTE
E DISP OSDER	TABLE
Route Table Unicast	\sim
BFD Profile Disable BFD	
Path Monitoring	
Preemptive Hold Time (min) 2	
CALIFICATION PING	
Ages	
EL LLDP	
- Entertained Re-	
T KECAN	
E IPSE E	
E RESAR	and the second se
Cance	Cancel
Protection Production	
Priseburna (†1Add (⊖)Delete (⊕)PDF/CSV	
الم المحمد الم	😑 🥢 paloalto
JWM _ 🔤 BruhloAlto - Mozilla Firefox	03:28

Figure 3.62: Static Route Configuration in the Site1

On the Site2 firewall, configure these settings:

Parameters	Value
Destination	10.0.0/24
Interface	tunnel.1
Next Hop	None

Table 3.15: Site2 Static Route Configuration

🚾 x11 - TightVNC	Viewer								- 🗆 X
🤨 🖬 😭 🗈	📕 🤧 🔊 🙀 ପ	trt Att 📭 🔍 🔾	. @ @ ₽						
🏮 Site-2 - Mo	zilla Firefox	-		-					_ ā ×
🋷 Sitel	×	🛛 🥠 Site-2		× +					
(+) > C	۵	(i) 🔏 https://192	2.168.0.2/?#net	work::vsys1::n	etwork/virtual-r	outers	🗹 🖆	/11/	• • =
								_/	
O PA-VM	t)	And in a second second	an an at an a	a	ne les pe				百四日
	Virtual Route	Virtual Router	- Static Route	- IPv4			(?)	08	60
Ghai	Router Setting:	Name	Site1						$f(\omega)\to\infty$
PP4	Static Routes	Destination	10.0.0/24				~	_	T MINITIANE
E NLWAY	Redistribution Pr	Interface	tunnel.1				~	1 item $\rightarrow \times$	1111.5
Vinual Roa	RIP	Next Hop	None				~		Ter
1 12 18 Same and a	OAPE	Admin Distance	10 - 240					ROUTE	
No. 196 Terror	OSPEV3	Metric	10					TABLE	
E Production of the	BGP	Route Table	Unicast				~	unicast	
and the second second	Multicast	BFD Profile	Disable BFD				Ŷ		
C. P. and	Mundasc	Path Monitoria	ig Condition		Prosmetiva Melri	Time Smirel 2			
		1 pilipi	Any	- All	r reempurve mala	Citize (India)			
L3		NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SE_	PING COUNT		
SILFR									
- El 1/									
	-	() Add							
- 19									
_ 10E T								Cancel.	
E las						ок	Cancel		
									Sector Sector
			Carlos Carlos Carlos						ogo paloalto
 Firefox au 	tomatically sends	some data to Mo	ozilla so that we	can improve	your experience	е.		<u>C</u> hoose Wha	at I Share X
JWM _	ۏ Site-2 - Mo	ozilla Firefox							09:52

Figure 3.63: Static Route Configuration in the Site 2

Then press **OK**.

Test the Site-to-Site

On any client device, try and ping the other client on the other site.



Figure 3.64: Verify your configuration

If you can ping the other client in the other site, everything worked!

Chapter 4. Cloud Technologies

196 Palo Alto Firewall

4.1 IPsec VPN between Palo Alto on Premise and Microsoft Azure





Figure 4.1: Main scenario

Azure Configuration

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

Resource groups Default Directory	☆ …	
+ Create 🐯 Manage view	✓ Č) Refresh ⊥ Export to CSV S Open query Ø Assign tags	
Filter for any field	Subscription == Azure subscription 1 Location == all \times + Add filter	
O Unsecure resources		
Name \uparrow_{\downarrow}		Subscription \uparrow_{\downarrow}

Figure 4.2: Create a resource group

Create a re	esource grou	ib	
Basics Tags	Review + create		
Resource group - resources for the allocate resources	A container that holds solution, or only those r to resource groups ba	related resources for an Azure solution. The reso resources that you want to manage as a group. Yo sed on what makes the most sense for your orga	urce group can include all the ou decide how you want to nization. Learn more C ^a
Project details			
Subscription * 🛈)	Azure subscription 1	\checkmark
Resource	group * 🛈	Pal	\checkmark
Resource details	5		
Region * 🛈		(US) West US	\sim
Review + creat	e < Previous	Next : Tags >	

Figure 4.3: Create a resource group

✓ Validation passed.	
Basics Tags Review + create	
Basics	
Subscription	Azure subscription 1
Resource group	Pal
Kegion	West US
Tags	
None	
Create < Previous Nex	ct > Download a template for automation

Figure 4.4: Create a resource group

- 2. Create a virtual network as follows:
 - **Resource group:** Pal
 - Name: Azure-Pal
 - **Region:** West US
 - Change the default subnet: 10.0.1.0/24

Create virtual netwo	ork …	
Basics IP Addresses Securit	y Tags Review + create	
Azure Virtual Network (VNet) is the f Azure resources, such as Azure Virtu networks. VNet is similar to a tradition benefits of Azure's infrastructure suc	undamental building block for your private network i al Machines (VM), to securely communicate with each onal network that you'd operate in your own data cen thas scale, availability, and isolation. Learn more abo	n Azure. VNet enables many types of o other, the internet, and on-premises iter, but brings with it additional but virtual network
Project details		
Subscription *	Azure subscription 1	\checkmark
Resource group * ①	Pal Create new	
Instance details		
Name *	Azure-Pal	\checkmark
Region *	West US	\sim
Review + create Figure 4.5: Create a virtual ne	<pre>< Previous Next : IP Addresses > twork</pre>	Download a template for automation
Home > Virtual networks >		Edit subnet ×
Create virtual network … Basics IP Addresses Security Tags Review + creation of the virtual network's address space, specified as one or more ad IPv4 address space	ate dress prefixes in CIDR notation (e.g. 192.168.1.0/24).	Subnet address range * () 10.0.1.0/24 10.0.1.0/25 (251 + 5 Azure reserved addresses) NAT GATEWAY
10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)	Î	Simplify connectivity to the internet using a network address translation gateway. Outbound connectivity is possible without a load balancer or public IP addresses attached to your virtual or publics.
Add IPv6 address space O The subnet's address range in CIDR notation (e.g. 192.168.1.0/2 network.	4). It must be contained by the address space of the virtual	NAT gateway None
+ Add subnet 🔋 Remove subnet	ange NAT gateway	SERVICE ENDPOINTS Create service endpoint policies to allow traffic to specific azure resources from your virtual
default 10.0.0.0/24		network over service endpoints. Learn more Services ①
● Use of a NAT gateway is recommended for outbound internet acc a subnet after you create the virtual network. <u>Learn more</u> o [*]	ess from a subnet. You can deploy a NAT gateway and assign it to	0 selected V
Review + create < Previous	Next : Security > Download a template for automation	Save Cancel

Figure 4.6: Create a virtual network (Change default subnet)

asics IP Addresses	Security Tags	s Review + create	
astionHost ①	 Disable 		
	O Enable		
DoS Protection Standard ①) Oisable		
	O Enable		
rewall ①	Oisable		
	O Enable		
Review + create	< \$	Previous Next : Tags > Download a template for automation	
ure 4.7: Create d	a virtual ne	etwork	
ure 4.7: Create d	a virtual ne	etwork	
ure 4.7: Create o reate virtual ne	a virtual ne etwork	etwork	
ure 4.7: Create o reate virtual ne	a virtual ne etwork	etwork	
ure 4.7: Create o reate virtual ne	a virtual ne etwork	etwork	
ure 4.7: Create or reate virtual ne	a virtual ne etwork	etwork s Review + create	
ure 4.7: Create o reate virtual ne asics IP Addresses	a virtual no etwork Security Tags	etwork s Review + create	
nure 4.7: Create of reate virtual ne asics IP Addresses ags are name/value pairs tha nultiple resources and resour	a virtual ne etwork Security Tags at enable you to co rce groups, Learn	etwork s Review + create rategorize resources and view consolidated billing by applying the same tag to more about tags to	
nure 4.7: Create of reate virtual ne asics IP Addresses ags are name/value pairs tha nultiple resources and resour lote that if you create tags a	a virtual ne etwork Security Tags at enable you to ca rce groups. Learn nd then change re	etwork s Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags to ⁿ esource settings on other tabs, your tags will be automatically updated.	
eure 4.7: Create of reate virtual ne asics IP Addresses ags are name/value pairs tha nultiple resources and resour lote that if you create tags a	a virtual ne etwork Security Tags at enable you to ca ree groups. Learn nd then change re	etwork Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags © esource settings on other tabs, your tags will be automatically updated.	
nure 4.7: Create of reate virtual ne asics IP Addresses a ags are name/value pairs tha nultiple resources and resour lote that if you create tags a Name ①	a virtual ne etwork Security Tags at enable you to ca rece groups, Learn nd then change re	etwork s Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags to esource settings on other tabs, your tags will be automatically updated. Value ①	
nure 4.7: Create of reate virtual ne asics IP Addresses a ags are name/value pairs tha nultiple resources and resour lote that if you create tags a Name ()	a virtual ne etwork Security Tags at enable you to ca rece groups. Learn nd then change re	etwork s Review + create stategorize resources and view consolidated billing by applying the same tag to more about tags to esource settings on other tabs, your tags will be automatically updated. Value ①	
nure 4.7: Create of reate virtual ne asics IP Addresses a ags are name/value pairs tha nultiple resources and resour lote that if you create tags a Name ()	a virtual ne etwork Security Tags at enable you to ca rece groups, Learn nd then change re	etwork s Review + create sategorize resources and view consolidated billing by applying the same tag to more about tags © esource settings on other tabs, your tags will be automatically updated. Value ① Yalue ①	
nure 4.7: Create of reate virtual ne asics IP Addresses a sultiple resources and resour lote that if you create tags a Name ()	a virtual ne etwork Security Tags at enable you to ca rece groups. Learn nd then change re	etwork s Review + create sategorize resources and view consolidated billing by applying the same tag to more about tags © esource settings on other tabs, your tags will be automatically updated. Value ①	
ure 4.7: Create of reate virtual ne asics IP Addresses : ags are name/value pairs tha nultiple resources and resour tote that if you create tags a Name ().	a virtual no etwork Security Tags at enable you to co rece groups. Learn nd then change re	etwork s Review + create sategorize resources and view consolidated billing by applying the same tag to more about tags © esource settings on other tabs, your tags will be automatically updated. Value ①	
ure 4.7: Create of reate virtual ne asics IP Addresses : ags are name/value pairs tha nultiple resources and resour tote that if you create tags a Name ().	a virtual no etwork Security Tags at enable you to co cce groups. Learn nd then change re	etwork s Review + create sategorize resources and view consolidated billing by applying the same tag to more about tags of esource settings on other tabs, your tags will be automatically updated. Value ①	
ure 4.7: Create of reate virtual ne asics IP Addresses : ags are name/value pairs tha hultiple resources and resour tote that if you create tags a Name ①	a virtual ne etwork	etwork s Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags © esource settings on other tabs, your tags will be automatically updated. Value ①	
ure 4.7: Create of reate virtual ne asics IP Addresses : ags are name/value pairs tha hultiple resources and resour tote that if you create tags a Name ()	a virtual ne etwork	etwork s Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags © esource settings on other tabs, your tags will be automatically updated. Value ①	
nure 4.7: Create of reate virtual ne asics IP Addresses : ags are name/value pairs tha nultiple resources and resour lote that if you create tags a Name ()	a virtual ne etwork	etwork Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags to esource settings on other tabs, your tags will be automatically updated. Value ①	
nure 4.7: Create of reate virtual net assics IP Addresses : ags are name/value pairs tha nultiple resources and resour lote that if you create tags a Name ()	a virtual ne etwork Security Tags at enable you to ca rece groups, Learn nd then change re	etwork s Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags of esource settings on other tabs, your tags will be automatically updated. Value ①	
nure 4.7: Create of reate virtual net lasics IP Addresses ags are name/value pairs tha nultiple resources and resour lote that if you create tags a Name ()	a virtual ne etwork Security Tags at enable you to ca rece groups, Learn nd then change re	etwork s Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags to esource settings on other tabs, your tags will be automatically updated. Value ①	
pure 4.7: Create of reate virtual ne assics IP Addresses : ags are name/value pairs tha nultiple resources and resour lote that if you create tags a Name ()	a virtual ne etwork Security Tags at enable you to ca rece groups. Learn nd then change re	etwork Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags to esource settings on other tabs, your tags will be automatically updated. Value ①	
gure 4.7: Create of create virtual net associate and the second s	a virtual ne etwork Security Tags at enable you to ca rece groups, Learn nd then change re	etwork Review + create ategorize resources and view consolidated billing by applying the same tag to more about tags to esource settings on other tabs, your tags will be automatically updated. Value ①	

Figure 4.8: Create a virtual network
🕑 Vali	dation passed				
Basics	IP Addresses	Security	Tags	Review + create	
Basics					
Subscript	tion		Azure	subscription 1	
Resource	group		Pal		
Name			Azure	-Pal	
Region			West	US	
IP addre	esses				
Address s	space		10.0.0	.0/16	
Subnet			defau	lt (10.0.0/24)	
Tags					
None	_				
Create		< Pre	vious	Next >	Download a template for automation

Create virtual network

- 3. Create a virtual network gateway as following:
 - Name: Azure-VPN-Pal
 - **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.

Virtual network Default Directory	gateways	☆ …			
🕂 Create 🐯 Manage vie	ew 🗸 🕐 Refresh	\downarrow Export to CSV	😚 Open quei	у 🖗 А	ssign tags
Filter for any field	Subscription == I	Azure subscription 1	Resource	e group == a	all \times
Name 🔨			Virt	ual ↑↓ G	atew 1

Figure 4.10: Create a virtual network gateway

Create virtua	l network	gateway	
---------------	-----------	---------	--

Subscription *	Azure subscription 1
Resource group ①	Pal (derived from virtual network's resource group)
Instance details	
Name *	Azure-VPN-Pal
Region *	West US 🗸
Gateway type * 🛈	VPN C ExpressRoute
VPN type * 🕕	Route-based Policy-based
SKU * 🕕	VpnGw2 ~
Generation ()	Generation1 V
Virtual network * 🛈	Azure-Pal V
	Only virtual networks in the currently selected subscription and region are listed.
Review + create Prev	vious Next : Tags > Download a template for automation

Figure 4.11: Create a virtual network gateway

Create virtual network gateway

Gateway subnet address range * 🕕	10.0.1.0/24
	10.0.1.0 - 10.0.1.255 (256 addresses)
Public IP Address Type * 🛈	O Basic 💿 Standard
Public IP address	
Public IP address * ①	Create new Use existing
Public IP address name *	AzurePublic 🗸
Public IP address SKU	Standard
Assignment	O Dynamic 💿 Static
Enable active-active mode $*$ \bigcirc	C Enabled (Disabled
Configure BGP * 🕕	C Enabled 💿 Disabled

Review + create	Previous	Next : Tags >	Download a template for automation

Figure 4.12: Create a virtual network gateway

Create virtua	l network	gateway	
---------------	-----------	---------	--

	Valio	dation pa	ssed			
	Basics	Tags	Review + create			
	Basics					
	Subscript	ion		Azure subscr	iption 1	
	Resource	group		Pal		
	Name			Azure-VPN-F	al	
	Region			West US		
	SKU			VpnGw2		
	Generatio	on		Generation1		
	Virtual ne	etwork		Azure-Pal		
	Subnet			GatewaySubr	net (10.0.1.0/24)	
	Gateway	type		Vpn		
	VPN type			RouteBased		
	Enable ac	tive-acti	ve mode	Disabled		
	Configure	e BGP		Disabled		
	Public IP	address		AzurePublic		
	Figure 4.	13: Ci	reate a virtual ne	twork gate	way	
🗿 We'd love your	feedback! \rightarrow					
 Deployr 	ment is in pi	rogre	55			
Deployment Subscription: Resource gro	name: Microsoft.Vir : Azure subscription pup: Pal	tualNetwo 1	orkGateway-2022050111	Start time: 5, Correlation II	/1/2022, 12:03:41 PM): 4b078a9d-11d3-4f4b-91fa-5bf1042e8a4c	
Deployment	details (Download	d)				
Resourc	e		Туре		Status	Operation
Resource gro Deployment Resource Gure 4.14: C	oup: Pal details (Download e Create a virtu	ⁱ⁾ al net	^{Туре} work gateway (de	ployment)	Status	
Your c	leployme	nt is	complete			
Deployme Subscript Resource	ent name: Micro ion: Azure subsc group: Pal	soft.Virt ription	ualNetworkGateway-2 1	202205011	Start time: 5/1/2022, 12:03:41 PM Correlation ID: 4b078a9d-11d3-4f4t	o-91fa-5bf1

- $\,\,\,\,\,\,\,$ Deployment details (Download)
- ∧ Next steps

Go to resource

Figure 4.15: Deployment of virtual network gateway

- 4. Create a local network gateway as follows:
 - **Resource Group:** Pal
 - **Region:** West US
 - Name: PaloAlto
 - **IP Address:** IP_Address_of_Port1_FortiGate(On Prem)
 - Address Space: IP_Address_LocalNetwork



Name \uparrow_{\downarrow}

Figure 4.16: Create a local network gateway

Create local network gateway

Project details		
Subscription *	Azure subscription 1	~
Resource group *	Pal Create new	~
Instance details		
Region *	West US	~
Name *	PaloAlto	
Endpoint ①	IP address FQDN	
IP address * 🕕	142.232.198.180	~
Address Space(s) ①		
192.168.10.0/24		✓ 🗊 …
Add additional address range		
Review + create Previous	Next : Advanced >	

Figure 4.17: Create a local network gateway

Create local network gateway

 Validation passed Basics Advanced 	Review + create	
Summary		
Name Subscription Resource group Region Endpoint IP address Address Space(s)		PaloAlto Azure subscription 1 Pal West US IP address 142.232.198.180 192.168.10.0/24
Create	Previous Next	

Figure 4.18: Create a local network gateway (review + create)



Figure 4.19: Verify local network gateway deployment

5. Go to Virtual network gateway and create a connection in **Virtual network gateways** > **Azure-VPN-Pal** > **connections** > **Add**

Add connection	
Name *	
AzureVPN	\checkmark
Connection type ①	
Site-to-site (IPsec)	\sim
*Virtual network gateway ①	A
Azure-VPN-Pal	
*Local network gateway ①	
PaloAlto	
Shared key (PSK) * ()	
123456789	\checkmark
Use Azure Private IP Address 🛈	
Enable BGP ()	
IKE Protocol ①	
◯ IKEv1	
Ingress NAT Rules	
ОК	

Figure 4.20: 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'll select SHA1 and AES128 in FortiGate. After doing this step, you should receive a Public IP address in the Overview tab.

Azure-VPN-Pal	\$				
Search (Ctrl+/)	~	\bigcirc Refresh \rightarrow Mov	ve 🗸 🔟 Delete		
Overview	-	∧ Essentials			
Activity log		Resource group (move)) : <u>Pal</u>	SKU	: VpnGw2
Access control (IAM)		Location	: West US	Gateway type	: VPN
🔮 Tags		Subscription (move)	: Azure subscription 1	VPN type	: Route-based
Diagnose and solve problems		Subscription ID	: 9170d5fe-6ca8-4257-9a4b-462d6b7ab3cd	Virtual network	: <u>Azure-Pal</u>
U blagnose and some problems				Public IP address	: 23.101.203.248 (AzurePublic)
Settings		Taos (edit)	Click here to add taos		

Figure 4.21: Verify the public IP address

Palo Alto Configuration

1. First, we'll configure Ports IP address.

Ethernet Interf	ace	?
Interface Name	ethernet1/1	
Comment		
Interface Type	Layer3	\sim
Netflow Profile	None	\sim
Config IPv4	IPv6 SD-WAN Advanced	
Assign Interface To)	
Virtual Route	r default	\sim
Security Zone	e VPN	~



Cancel

Figure 4.22: Ethernet 1/1 Config

Ethernet Interf	ace		(?)
Interface Name	ethernet1/1		
Comment			
Interface Type	Layer3		\sim
Netflow Profile	None		\sim
Config IPv4	IPv6 SD-WAN	Advanced	
Туре	☐ Enable SD-WAN	DHCP Client	
	Enable		
	Automatically create d	efault route pointing to default gateway provided by server	
	Send Hostname	ystem-hostname	~
Default Route Me	ric 10		
	Show DHCP Client Runtin	ne Info	

Figure 4.23: Ethernet 1/1 IPV4

Ethernet Interf	ace	(?)
Interface Name	ethernet1/2	
Comment		
Interface Type	Layer3	\sim
Netflow Profile	None	\sim
Config IPv4	IPv6 SD-WAN Advanced	
Assign Interface To		
Virtual Route	r default	\sim
Security Zone	LAN	\sim

Cancel

Cancel

Figure 4.24: Ethernet 1/2 Config

Ethernet Interf	ace	?
Interface Name	ethernet1/2	
Comment		
Interface Type	Layer3	\sim
Netflow Profile	None	\sim
Config IPv4	IPv6 SD-WAN Advanced	
	Enable SD-WAN	
Туре	Static OPPoE ODHCP Client	
IP IP		
192.168.10.1/2	24	
+ Add - Delete	e ↑ Move Up ↓ Move Down	
IP address/netmask. Ex.	192.168.2.254/24	

Figure 4.25: Ethernet 1/2 IPv4

Then, create a tunnel.

Cancel

Tunnel Interface		?
Interface Name	tunnel . 1	
Comment		
Netflow Profile	None	\sim
Config IPv4	IPv6 Advanced	
Assign Interface To		
Virtual Route	er default	\sim
Security Zon	e VPN	\sim

Figure 4.26: Create a tunnel 1

Ethernet VLAN	Loopback Tunne	el SD-WAN		
Q				
INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURI
tunnel		none	none	none
tunnel.1		none	default	VPN

Figure 4.27: Verify Tunnel1

Then, commit the configuration!

 Create a static route to tunnel1 and ethernet1/1 as following figures. Traffic related to 10.0.0/16 should go through the tunnel. The rest of the traffic should go through the default Gateway.

Virtual Router	- Static Route -	IPv4				?
Name	static					
Destination	0.0.0/0					\sim
Interface	ethernet1/1					\sim
Next Hop	IP Address					\sim
	142.232.198.254					\sim
Admin Distance	10 - 240					
Metric	10					
Route Table	Unicast					\sim
BFD Profile	Disable BFD					\sim
Path Monitorin	g					
Failure	e Condition 💿 Any		Preemptive Hold	Time (min) 2		
NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT	
🕂 Add 😑 Dele						

Cancel

Figure 4.28: Create a static route to ethernet 1/1

4.1 IPsec VPN between Palo Alto on Premise and Microsoft Azure 213

Virtual Router	- Static Route -	IPv4				?
Name	tunnel					
Destination	10.0.0/16					\sim
Interface	tunnel.1					\sim
Next Hop	None					\sim
Admin Distance	10 - 240					
Metric	10					
Route Table	Unicast					\sim
BFD Profile	Disable BFD					\sim
Path Monitorin	g					
Failure	e Condition 💿 Any) All	Preemptive Hold	Time (min) 2		
	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT	
⊕ Add ⊝ Dek						
				ОК	Canc	el

Figure 4.29: Create a static route to tunnel.1

3. Go to	Network >	Network	Profiles >	Create	an IKE	Crypto.
----------	-----------	---------	-------------------	--------	--------	---------

IKE Crypto Profile	0
Name IKE	
DH GROUP	ENCRYPTION
group2	aes-128-cbc
Add Delete Move Up J Move Down	Timor
AUTHENTICATION	_ Timers
sha1	Key Lifetime Seconds 🗸
	28800
	Minimum lifetime = 3 mins
↔ Add	IKEv2 Authentication 0 Multiple
	OK Cancel

Figure 4.30: Create an IKE Crypto Profile

4. Go to **Network > Network Profiles > Create an IPsec Crypto Profile**.

IPSec Crypto P	Profile					(?)
Name	IPSEQ					
IPSec Protocol	ESP 🗸	DH Group	group2			\sim
ENCRYPTION		Lifetime	Seconds	\sim	27000	
aes-128-cbc		- C Enable	Minimum lifetim	ne = 3 mir	ns	
		Lifesiz	MB	\sim		
			Recommende		is 100MB or greater	
🕀 Add 🕞 Delete	e ↑ Move Up 👃 Move Down					
AUTHENTICAT	TON					
sha1						
	e ↑ Move Up ↓ Move Down					
					ок	Cancel

Figure 4.31: Create an IPsec Crypto Profile

5. Go to **Network > Network Profiles > Create an IKE Crypto Gateways**.

IKE Gateway		(?)
General Advance	ed Options	
Name	IKE-GW	
Version	IKEv2 only mode	~
Address Type	 ● IPv4 ○ IPv6 	
Interface	ethernet1/1	\sim
Local IP Address	None	\sim
Peer IP Address Type	● IP ○ FQDN ○ Dynamic	
Peer Address	23.101.203.248	~
Authentication	• Pre-Shared Key Certificate	
Pre-shared Key	•••••	
Confirm Pre-shared Key	•••••••	
Local Identification	None v	
Peer Identification	None	
Comment		
Figure 4.32: Create	an IKE Gateway	
IKE Gateway		?
General Advance	ed Options	
Common Options		
Enable Passive M	lode	
Enable NAT Trave	ersal	
IKEv2		
IKE Crypto Profile	IKE	~
	Strict Cookie Validation	
Liveness Check		
Interval (sec)	5	
	OK	Cancel

Figure 4.33: Select IKE Crypto Profile

6. Go to **Network** > **IPsec Tunnels** > **Add.** Select the previous profile you have created as Figure 4.34.

IPSec Tunnel		?
General Prox	ty IDs	
Name	IPSEC-Tunnel	
Tunnel Interface	tunnel.1	\sim
Туре	💿 Auto Key 🔹 Manual Key 🔹 GlobalProtect Satellite	
Address Type	O IPv4 ○ IPv6	
IKE Gateway	IKE-GW	\sim
IPSec Crypto Profile	IPSEC	\sim
	Show Advanced Options	
Comment		
	ОК Сапсе	

Figure 4.34: Create an IPsec Tunnel

7. Create a firewall policy from LAN to VPN zone and from VPN to LAN.

Security Policy	Rule	?
General Sou	rce Destination Application Service/URL Category Actions Usage	
Name	LAN-AZ	
Rule Type	universal (default)	\sim
Description		
Tags	4	•
Group Rules By Tag	None	\sim
Audit Comment		
	Audit Comment Archive	



OK Cancel

Figure 4.35: Create a security policy "LAN-AZ"

Security Policy Rule	lication Service/URI Category Actions		Ć
	Any	any 🗸	any
SOURCE ZONE	SOURCE ADDRESS	SOURCE USER A	SOURCE DEVICE A
🛨 Add 😑 Delete	🛨 Add \ominus Delete	🔁 Add \ominus Delete	🕀 Add \ominus Delete
	Negate		

Figure 4.36: Create a security policy "LAN-AZ." Select the source zone as LAN.

Security Policy Rule							
General Source Destination Application Serv	rice/URL Category Actions Usage						
select 🗸	Z Any	any 🗸					
DESTINATION ZONE	DESTINATION ADDRESS	DESTINATION DEVICE					
↔ Add		↔ Add ⊖ Delete					
	Negate Negate						

Figure 4.37: Create a security policy "LAN-AZ." Select destination zone as VPN.

Security Policy	ecurity Policy Rule						
General Sour	rce Destination Application Service/URL Category Actions						
Name	AZ-LAN						
Rule Type	universal (default)	\sim					
Description							
Tags	4						
Group Rules By Tag	None	\sim					
Audit Comment							
	Audit Comment Archive						

OK Cancel

Cancel

Figure 4.38: Create a security policy "AZ-LAN"

Security Policy Rule			0
General Source Destination App	lication Service/URL Category Actions		
Any	Z Any	any 🗸	any 🗸
SOURCE ZONE A	SOURCE ADDRESS A	SOURCE USER A	SOURCE DEVICE A
VPN			
🕀 Add \ominus Delete	↔ Add ⊖ Delete	🕣 Add \ominus Delete	🛨 Add \ominus Delete
	Negate		

OK Cancel

Figure 4.39: Create a security policy "AZ-LAN." Select source zone as VPN.

218 Chapter 4. Cloud Technologies

	Destination address	DESTINATION DEVICE
2 P2 LAN		
€ Add ⊖ Delete	Add ⊖ Delete	Add ⊖ Delete

Cancel

Figure 4.40: Create a security policy "AZ-LAN." Select destination zone as LAN.

Don't forget to commit the configuration!

Verify Connections

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

🚥 Interfaces	Q								
Zones						IKE Gatew	/ay/Satellite		
e Virtual Wires		NAME	STATUS	ТҮРЕ	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE
Virtual Routers		IPSEC-Tunnel	Tunnel Info	Auto Key	ethernet1/1		20.89.67.199	IKE Info	tunnel.1
🔨 IPSec Tunnels									
🐠 GRE Tunnels									
붗 DHCP									
🕎 DNS Proxy									

Figure 4.41: Verify IPsec Tunnel

8	Azure-VPN-Pal C	Con	nections 🖈						
م	Search (Ctrl+/)	K	🕂 Add 💍 Refresh						
۵	Overview	^							
۲	Activity log	L	Name	↑↓	Status	\uparrow_{\downarrow}	Connection type	\uparrow_{\downarrow}	Peer
የአ	Access control (IAM)		AzureVPN		Connected		Site-to-site (IPsec)		PaloAlto
¢	Tags								
Þ	Diagnose and solve problems	L							
Set	tings	L							
	Configuration								
8	Connections								

Figure 4.42: Verify connections in Azure

	1					-					
har	nid@wir	idows2	2:~Ş	pın	g 19	2.	168.10).2			
PIN	NG 192.	168.1	10.2	(19	2.16	58.	10.2)	56(84)	bytes	of data.	
64	bytes	from	192	.168	.10.	2:	icmp_	_seq=1	ttl=63	time=103	ms
64	bytes	from	192	.168	.10.	2:	icmp_	_seq=2	ttl=63	time=106	ms
64	bytes	from	192	.168	.10.	2:	icmp_	_seq=3	ttl=63	time=101	ms
64	bytes	from	192	.168	.10.	2:	icmp_	_seq=4	ttl=63	time=103	ms
64	bytes	from	192	.168	.10.	2:	icmp_	_seq=5	ttl=63	time=102	ms
64	bytes	from	192	.168	.10.	2:	icmp	seq=6	ttl=63	time=102	ms
64	bytes	from	192	.168	.10.	2:	icmp_	_seq=7	ttl=63	time=102	ms
64	bytes	from	192	.168	.10.	2:	icmp	seq=8	ttl=63	time=101	ms
$^{\rm C}$											

Figure 4.43: Verify ping from Windows to webterm

🖷 LXTerminal	-	×
<u>Eile Edit Tabs H</u> elp		
root@webterm-16~# ping 10.0.1.5		٠
PING 10.0.1.5 (10.0.1.5) 56(84) bytes of data.		
64 bytes from 10.0.1.5: icmp_seq=1 ttl=63 time=102 ms		
64 bytes from 10.0.1.5: icmp_seq=2 ttl=63 time=101 ms		
64 bytes from 10.0.1.5: icmp_seq=3 ttl=63 time=102 ms		
64 bytes from 10.0.1.5: icmp_seq=4 ttl=63 time=101 ms		
<u>6</u> 4 bytes from 10.0.1.5: icmp_seq=5 ttl=63 time=101 ms		

Figure 4.44: Verify ping from webterm to Windows in Azure

220 Chapter 4. Cloud Technologies

4.2 Deploy Palo Alto to Azure



1. Go to Azure Marketplace and search for Palo Alto.

Home >			
Marketplace			
-			
Get Started		O pala alta	~
Service Providers	L		~
Management	l	Managed Services	

Figure 4.45: Search for Palo Alto

2. Select VM-Series Next-Generation Firewall from Palo Alto.

Home >				
Marketplace				
Get Started	Showing results for 'palo alto'.			
Service Providers	Showing 1 to 20 of 27 results.	ł		
Management	A	//		
Private Marketplace	Dala Alta Natuarka	VAL Series Next Constation	Dala Alta Drisma Colution	Dala Alta DANI OS Salutian
Private Offer Management	Panorama	Firewall from Palo Alto	(Preview)	(Preview)
	Palo Alto Networks, Inc.	Palo Alto Networks, Inc.	Azure Sentinel, Microsoft	Azure Sentinel, Microsoft
My Marketplace	Virtual Machine	Azure Application	Azure Application	Azure Application
Favorites	Palo Alto Networks Panorama	Looking to secure your applications in Azure, protect against threats and prevent data exfiltration?	Prisma Cloud delivers full stack protection for multi-cloud and hybrid-cloud.	PAN-OS is the software that runs all Palo Alto Networks next-generation firewalls.
Recently created				
Private products	Bring your own license	Price varies	Price varies	Price varies
Categories	Create 🗸 🛇	Create 🗸 🗢 🛇	Create 🗸 🗢	Create 🗸 🛇

Figure 4.46: Select VM Series Next-Generation Firewall

3. Then, Select VM-Series Next Generation Firewall from dropdown list.

```
Home > Marketplace >
```

VM-Series Next-Generation Firewall from Palo Alto Networks 🔅 … Palo Alto Networks, Inc.

d'a paloaito	VM-Series Next-Generation Firewall from Palo Alto Networks 👳 Add to Favorites			
	Palo Alto Networks, Inc.			
	★ 3.6 (9 Azure ratings) 🛛 ★ 4.6 (9 external ratings)			
	R. Preferred solution			
	Dian			
	VM-Series Next Generation Firewall (V			
Overview	Plans Usage Information + Support Reviews			

Figure 4.47: Select VM-Series Next Generation Firewall

4. Create a Firewall information, as Figure 4.48.

Home > Marketplace > VM-Series Next-Generation Firewall from Palo Alto Networks >

Create VM-Series Next-Generation Firewall from Palo Alto Networks

manage all your resources.		
Subscription * 🕕	Azure subscription 1	\sim
Resource group * ①	Pal Create new	\checkmark
Instance details		
Region * 🛈	UK West	\sim
Username * 🛈	hamid	\checkmark
Authentication type *	Password SSH Public Kov	
Password *	•••••	\checkmark
Confirm password *	•••••	\checkmark
Review + create < Previous	s Next : Networking >	

Figure 4.48: Create a VM-Series Palo Alto

Basics Networking VM-Series Co	onfiguration Review + create	
Configure virtual networks		
Virtual network * 🛈	(new) fwVNET	\sim
	Create new	
Management Subnet *	(new) Mgmt (10.0.0/24)	\sim
Untrust Subnet *	(new) Untrust (10.0.1.0/24)	\checkmark
Trust Subnet *	(new) Trust (10.0.2.0/24)	\checkmark
Network Security Group: inbound source	0.0.0.0/0	

Figure 4.49: Networking configuration

224 Chapter 4. Cloud Technologies

Basics Networking	VM-Series Configuration Review + create
Public IP address * (i)	(new) fwMgmtPublicIP
	Create new
DNS Name * 🛈	hamid 🗸
	.ukwest.cloudapp.azure.com
VM name of VM-Series *	hamidpaloalto
VM-Series Version ①	□atest ∨
Enable Bootstrap 🛈	⊖ yes
	• no
Virtual machine size * 🕕	1x Standard D3 v2
Virtual machine size * 🕕	1x Standard D3 v2 4 vcpus, 14 GB memory Change size
Virtual machine size * ①	1x Standard D3 v2 4 vcpus, 14 GB memory Change size

Figure 4.50: VM Configuration (DNS-VM Name)

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

🗸 Vali	dation Passed			
Basics	Networking	VM-Series Configuration	Review + create	
PRODUC	CT DETAILS			
VM-Serie from Pal by Palo A Terms of	es Next-Generat o Alto Networks Ito Networks, Inc use Privacy poli	tion Firewall s cy		
TERMS				
PRODUC VM-Serie from Pal by Palo A Terms of TERMS	CT DETAILS es Next-Generat o Alto Networks lto Networks, Inc use Privacy polic	tion Firewall : :. cy		

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

Figure 4.51: Create a firewall

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

paloaltonetwork	s.vm	series-ngfw-20220516153314 Overview
✓ Search (Ctrl+/)	«	🔟 Delete 🚫 Cancel 📋 Redeploy 💍 Refresh
👶 Overview		𝒞 We'd love your feedback! →
😫 Inputs		
š≡ Outputs		Deployment is in progress
📄 Template		Deployment name: paloaltonetworks.vmseries-ngfw-2022051615 Subscription: Azure subscription 1 Resource group: Pal

Figure 4.52: Deployment is in progress



Figure 4.53: Deployment is complete

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

(*) Overview	∧ Essentials		
Activity log	Subscription (move) : Azure subscription 1	Deployments : 6 Succ	eeded
Access control (IAM)	Subscription ID : 9170d5fe-6ca8-4257-9a4b-462d6b7ab3cd	Location : UK We	st
Tags	Tags (edit) : Click here to add tags		
🛧 Resource visualizer	Persurger Decommondations		
🗲 Events	Resources		
Settings	Filter for any field Type == all \times Location == all \times $+_{\nabla}$ Add filt	ter	
Deployments	Showing 1 to 8 of 8 records. Show hidden types ①	[No grouping V
Security	Name ↑↓	Type ↑↓	Location ↑↓
Policies		Network seguity aroun	LIK West
😂 Properties		Network security group	UK West
🔒 Locks	↓ ↔ fwVNeT	Virtual network	UK West
	L Im hamid	Public IP address	UK West
Cost Management	🗌 🖳 hamidpaloalto	Virtual machine	UK West

Figure 4.54: Palo Alto Public IP Address

🕜 Upgrade to Stand	ard SKU - Microsoft recommends Standard SKU public IP address for production	workloads \rightarrow	
∧ Essentials			
Resource group (move) : <u>Pal</u>	SKU	: Basic
Location	: UK West	Tier	: Regional
Subscription (<u>move</u>)	: Azure subscription 1	IP address	: 52.142.160.31
Subscription ID	: 9170d5fe-6ca8-4257-9a4b-462d6b7ab3cd	DNS name	: hamid.ukwest.cloudapp.azure.com
		Associated to	: <u>hamidpaloalto-hamid-eth0</u>
Tags (<u>edit</u>)	: <u>Click here to add tags</u>		
See more			

Figure 4.55: Palo Alto Public IP Address

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

Not secure https://52.142.160.31/php/login.php?		Le 女
	hamid	
	Log in	

Figure 4.56: Palo Alto Firewall Credential Page

9. Azure will create three interfaces, as Figure 4.57. By default, Eth0 is set as a management port and this port has the public IP address and you can reach the GUI through this IP address. Eth1 is set as an Untrusted interface and to be able to access the firewall through this port, you should set the Public address for this port.



Figure 4.57: Palo Alto Firewall Interfaces by default

10. To set interfaces in the firewall, you should go to Network > Interfaces and set both ethernet1/1 and ethernet1/2 as a DHCP client. Also, uncheck "Automatically create default route pointing to default gateway."

Ethernet Interf	ace		?
Interface Name	ethernet1/1		
Comment			
Interface Type	Layer3		\sim
Netflow Profile	None		\sim
Config IPv4	IPv6 SD-WAN	Advanced	
Туре	Enable SD-WAN	DHCP Client	
	🗸 Enable		
	Automatically create description	efault route pointing to default gateway provided by server	
	Send Hostname	ystem-hostname	\sim
Default Route Me	ric 10		
	Show DHCP Client Runtin	ne Info	

Cancel

Figure 4.58: Ethernet1/1 configuration

Ethernet Interf	ace		?
Interface Name	ethernet1/2		
Comment			
Interface Type	Layer3		\sim
Netflow Profile	None		\sim
Config IPv4	IPv6 SD-WAN	Advanced	
	Enable SD-WAN		
Туре	🔵 Static i PPPoE 💿	DHCP Client	
	🗸 Enable		
	Automatically create	default route pointing to default gateway provided by server	
	Send Hostname	system-hostname	\sim
Default Route Me	tric 10		
	Show DHCP Client Run	time Info	
		ок	Cancel

Figure 4.59: Ethernet1/2 configuration

11. Then, you set a default route and set a zone for each interface.

Ethernet Interf	ace	?
Interface Name	ethernet1/1	
Comment		
Interface Type	Layer3	~
Netflow Profile	None	~
Config IPv4	IPv6 SD-WAN Advanced	
Assign Interface To		
Virtual Route	default	\sim
Security Zone	Untrust	\sim



Cancel

Figure 4.60: Ethernet1/1 zone and virtual router

Ethernet Interf	ace	?
Interface Name	ethernet1/2	
Comment	WAN	
Interface Type	Layer3	\sim
Netflow Profile	None	\sim
Config IPv4	IPv6 SD-WAN Advanced	
Assign Interface To		
Virtual Route	default	~
Security Zone	Trust	\sim

Figure 4.61: Ethernet1/2 zone and virtual router

and then in Ethernet1/1 under the advanced tab, set management interface profile as Figure 4.62.

Interface Management Profile		?
Name access Administrative Management Services HTTP	PERMITTED IP ADDRESSES	
 ✓ HTTPS ☐ Telnet ☐ SSH 		
Network Services Ping HTTP OCSP		
SNMP Response Pages User-ID		
User-ID Syslog Listener-SSL		
	+ Add Oelete	
	Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64	
	OK Cance	

Figure 4.62: Ethernet1/1 Management Profile

12. Create a static route to 10.0.1.1.

L(SEC) PING C	COUNT
AL(SEC) PING	COUNT
	ок

Figure 4.63: Create a static route to 10.0.1.1

13. Create a public IP address and assign the public IP address to interface eth1 (Untrusted interface).

Public I	P address	es 🖈 …				
+ Create	🔅 Manage view	∨ 🕐 Refresh	↓ Export to CSV	😚 Open query	🗟 Assign tags	🔟 Delete
Filter for any	y field	Subscription == A	zure subscription 1	Resource gro	oup == all 🗙	Location ==
Name ↑	\downarrow				Resource grou	р ↑↓
🗌 🖬 ham	id				PAL	

Figure 4.64: Create a public IP address

Create public IP address	
--------------------------	--

	SKU * ① Standard ● Ba Tier ● Regional ● GI	asic				
	IPv4 IP Address Con	figuration				
	Name *					
	Untrust					
	IP address assignment	*				
	🔵 Dynamic 🧿 Sta	atic				
	Idle timeout (minutes)	* ()				
	0					
	DNS name label					
	Subscription *					
	Create Aut	tomation options				
	Figure 4.65: Create a	public IP addres	ss (set SKU	and name)		
	5	1	(,		
All resources «	🚃 hamidpaloalto-har	mid-eth1 IP configu	rations 🖈 …			\times
Default Directory	Network interface	🛨 Add 🗖 Saun 🗸 Direc	and () Refrech			
+ Create 😒 Manage view 🗸 …	Overview	IP forwarding settings				
Filter for any field	Activity log	IP forwarding	Disabled	abled)		
	Access control (IAM)	Virtual network	6w/NET			
	🔷 Tags	ID configurations				
bamid	··· Settings	Subnet	Untrust (10.0.1	0/24)		\sim
Amidpaloalto	IP configurations		- man (100.1			
Amidpaloalto-hamid-eth0	DNS servers					
Amidpaloalto-hamid-eth1	••• Vetwork security group	The associated virtual maching	ne 'hamidpaloalto' must be e	either stopped or deallocated in o	order to be able to edit the subnet.	
Amidpaloalto-hamid-eth2	··· Properties	O Search ID configurations				
hamidpaloalto_OsDisk_1_f224c1820b8e	··· A Locks	Name IP Version	Туре	Private IP address	Public IP address	
NetworkWatcher_ukwest	Monitoring	ipconfig-untrIPv4	Primary	10.0.1.4 (Dynamic)		
	Insights	4		see or prystancy		

Figure 4.66: Select Interface eth1

ipconfig-untrust ···· hamidpaloalto-hamid-eth1
🔚 Save 🗙 Discard
Public IP address settings
Public IP address
Disassociate Associate
Public IP address *
Untrust (51.140.253.110)
Create new
Private IP address settings
Virtual network/subnet fwVNET/Untrust
Virtual machine hamidpaloalto
The associated virtual machine 'hamidpaloalto' must be either stopped or deallocated in order to be able to edit the private IP address.
Assignment Dynamic Static
IP address
10.0.1.4

Figure 4.67: Assign public IP address to Eth1

14. Open the browser and type the public IP address. You should be able to access the firewall.

234 Chapter 4. Cloud Technologies

4.3 Site-to-Site VPN between Palo Alto on Premise and Palo Alto in the Azure

Learning Objectives
Configure a Virtual Network in Microsoft Azure
Set up and configure the Azure VPN Gateway for IPsec VPN
Implement Network Security Groups (NSGs) in Azure for traffic control
Monitor and troubleshoot IPsec VPN connections on Palo Alto

Scenario: In this lab, we will create a site-to-site VPN from Palo Alto on-premise to Palo Alto in the Azure. Knowing the configuration of section 4.2 is necessary for this lab. I have created management and ethernet1/1 as a DHCP, so they will receive an IP address from Cloud.



Figure 4.68: Main scenario

On-Premise Palo Alto Configuration

Devices	Interface	IP address	
	Management	DHCP Client	
Palo Alto	Ethernet 1/1	DHCP Client	
	Ethernet 1/2	192.168.10.1/24	
WebTerm	Eth0	192.168.10.2/24	

1. Configure the interfaces of the firewall. Set Ethernet1/1 as a Untrust Zone and Ethernet1/2 as a Trust Zone.

Interfaces	0	Ethernet VLAN Loopback Tunnel SD-WAN									
Magazine Zones											
💑 VLANs		0									
Contract Wires		~							1		
Wirtual Routers	0			MANAGEMENT	LINK				VLAN / VIRTUAL-		
🔨 IPSec Tunnels	0	INTERFACE	INTERFACE TYPE	PROFILE	STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	WIRE	SECURITY ZONE	
GRE Tunnels		ethernet1/1	Layer3			Dynamic-DHCP Client	default	Untagged	none	Untrust	
DNS Proxy		ethemet1/2	Layer3			192.168.10.1/24	default	Untagged	none	Trust	

Figure 4.69: Firewall Interfaces

2. Create a **tunnel.1** and set the tunnel as Untrust zone.

Interfaces	•	Ethernet VLAN Lo	oopback Tunne	SD-WAN					
Zones E VLANs	•								
Virtual Routers	•	INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES		
SRE Tunnels		tunnel		none	none	none			
물 DHCP		tunnel.1		none	default	Untrust	œ		

Figure 4.70: Create a tunnel

Cancel

3. Create two static routes, one pointing to 142.232.197.254 (on-Prem Default Gateway) and the other one sending the traffic of Azure through the tunnel.

Virtual Router	- Static Route -	IPv4				?		
Name	statid	tatiq						
Destination	0.0.0/0					\sim		
Interface	ethernet1/1					\sim		
Next Hop	IP Address					\sim		
	142.232.197.254					\sim		
Admin Distance	10 - 240							
Metric	10							
Route Table	Unicast					\sim		
BFD Profile	Disable BFD					\sim		
Path Monitorin	g							
Failur	e Condition 💿 Any		Preemptive Hold	Time (min) 2				
NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT			
+ Add - Dele								

Figure 4.71: Create a static route to default gateway
238 Chapter 4. Cloud Technologies

Virtual Router	- Static Route -	IPv4				?
Name	tunnel					
Destination	10.0.0/16					\sim
Interface	tunnel.1					\sim
Next Hop	None					\sim
Admin Distance	10 - 240					
Metric	10					
Route Table	Unicast					\sim
BFD Profile	Disable BFD					\sim
Path Monitorin	g					
Failur	e Condition 🧿 Any		Preemptive Hold	Time (min) 2		
	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT	

Cancel

Figure 4.72: Create a static route to Azure

4. For setting up, site-to-site VPN we will use default IKE Crypto, IPsec Crypto profiles and we will only set IKE Gateway and IPsec Tunnel as following figures. You have to configure local and peer identification.

IKE Gateway				(
General Advance	d Options			
Name	IKE			
Version	IKEv1 only mode			~
Address Type	○ IPv4 ○ IPv6			
Interface	ethernet1/1			\vee
Local IP Address	None			\checkmark
Peer IP Address Type	O IP ○ FQDN	O Dynamic		
Peer Address	51.142.139.28			~
Authentication	 Pre-Shared Key 	Certificate		
Pre-shared Key	•••••			
Confirm Pre-shared Key	•••••			
Local Identification	IP address		\sim	142.232.197.233
Peer Identification	IP address		\sim	51.142.139.28
Comment				
				OK Cancel

Figure 4.73: Create an IKE Gateway

General Prox	y IDs	
Name	IPSEQ	
Tunnel Interface	tunnel.1	~
Туре	O Auto Key O Manual Key O GlobalProtect Satellite	
Address Type	 ● IPv4 ○ IPv6 	
IKE Gateway	IKE	~
IPSec Crypto Profile	default	~
	Show Advanced Options	
Comment		

Figure 4.74: Create an IPsec Tunnel

5. Finally, create two security policies, one from Trust to Untrust zone and the other from Untrust to Trust zone.

🚾 Security 🔹	Q(
⇒ NAT						Sou	irce			Destination	
🙇 QoS											
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEV
Decryption Tunnel Inspection	1	Trust	none	universal	M Trust	any	any	any	Muntrust	any	any
Application Override	2	Untrust	none	universal	Mag Untrust	any	any	any	Mag Trust	any	any

Figure 4.75: Create two security policies

Azure Configuration

- 1. Create a Palo Alto firewall in Azure and configure the interfaces. You need to do all steps in section 4.1 and assign public IP address to Ethernet 1 (Untrust Zone).
- 2. Create a route in Azure pointing to Trust interface.

Route tables ☆ Default Directory		
+ Create 🔅 Manage viev	$v \sim \bigcirc$ Refresh \downarrow Export to CSV	😚 Open query \mid 🧔 Assign tags
liter for any field	Subscription == Azure subscription 1	Resource group == all ×
~		
Name \uparrow_{\downarrow}		Resource grou

Figure 4.76: Create a route table

Create Route table

Basics	Tags	Review	+	create
--------	------	--------	---	--------

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	/
Resource group * ①	Pal	/
	Create new	
Instance details		
Region * ①	UK West	/
Name * 🕕	Trust	~
Propagate gateway routes * 🕠	⊖ Yes	
	No	
Review + create < Previous	Next : Tags >	

Figure 4.77: Create a route table

Create Route table

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.

Basics	
Subscription	Azure subscription 1
Resource group	Pal
Region	UK West
Name	Trust
Propagate gateway routes	No
Create < Previous	Next Download a template for automation

Figure 4.78: Create a route table (verify and create)

242 Chapter 4. Cloud Technologies

Route table	☆ …		
✓ Search (Ctrl+/)	~ ~	+ Add 🕐 Refresh 🔊 Give f	feedback
🖄 Overview	^	₽ Search routes	
Activity log		Name ↑↓	Address prefix \uparrow_{\downarrow}
Access control (IAM)		No results.	
🧳 Tags			
Diagnose and solve problems			
Settings			
a Configuration			
🔽 Routes			
Subnets			

Figure 4.79: Add a Route

Add route	\times
Trust	
Route name *	
Trust	\checkmark
Address prefix destination * ①	
IP Addresses	\sim
Destination IP addresses/CIDR ranges * 🛈	
0.0.0/0	\checkmark
Next hop type * (i)	
Virtual appliance	\sim
Next hop address * 🕕	
10.0.2.4	\checkmark
Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.	

Figure 4.80: Add a default route pointing to 10.0.2.4 (Trust Interface)

Search (Ctrl+/) «	+ Associate			
1 Overview	Search subnets			
 Activity log 	Name 14	Address range ↑↓	Virtual network 14	Security group ↑↓
Access control (IAM)	No results.			
🗳 Tags				
Diagnose and solve problems				
Settings				
Configuration				
🚵 Routes				
• Subnets				

Figure 4.81: Associate Trust route to Trust Subnet

Associate subnet						
Trust						
Virtual network 🛈						
fwVNET	\checkmark					
Subnet ①						
Trust	~					

Figure 4.82: Associate fwVNET to Trust Subnet

3. Set static routes as figures 4.83 and 4.84.

Virtual Router	- Static Route -	Static Route - IPv4							
Name	static								
Destination	0.0.0/0					\sim			
Interface	ethernet1/1	zthernet1/1							
Next Hop	IP Address					\sim			
	10.0.1.1					\sim			
Admin Distance	10 - 240								
Metric	10								
Route Table	Unicast					\sim			
BFD Profile	Disable BFD ~								
Path Monitorin	g								
Failure	e Condition 🧿 Any	🔿 All	Preemptive Hold	Time (min) 2					
NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT				
+ Add Del									

OK Cancel

Figure 4.83: Static route pointing to default gateway

244 Chapter 4. Cloud Technologies

Virtual Router	- Static Route -	tatic Route - IPv4							
Name	tunnel								
Destination	192.168.0.0/16					\sim			
Interface	tunnel.1					\sim			
Next Hop	None					\sim			
Admin Distance	10 - 240	10 - 240							
Metric	10								
Route Table	Unicast	Unicast 🗸 🗸							
BFD Profile	Disable BFD					\sim			
Path Monitorin	Ig								
Failur	e Condition 🧿 Any		Preemptive Hold	Time (min) 2					
NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT				
+ Add Del									

Cancel

4. For setting up, site-to-site VPN we will use default IKE Crypto, IPsec Crypto profiles and we will only set IKE Gateway and IPsec Tunnel as figures 4.85 and 4.86.

IKE Gateway		?
General Advance	ed Options	
Name	IKE	
Version	IKEv1 only mode	\sim
Address Type	 ○ IPv4 ○ IPv6 	
Interface	ethernet1/1	\sim
Local IP Address	None	\sim
Peer IP Address Type	IP ○ FQDN ○ Dynamic	
Peer Address	51.142.139.28	\sim
Authentication	• Pre-Shared Key Certificate	
Pre-shared Key	•••••	
Confirm Pre-shared Key	•••••	
Local Identification	IP address 🗸 142.232.197.233	
Peer Identification	IP address 51.142.139.28	
Comment		
	ОК Са	ancel

Figure 4.85: Create an IKE Gateway

IPSec Tunnel		?
General Prox	y IDs	
Name	IPSEC	
Tunnel Interface	tunnel.1	\sim
Туре	Auto Key O Manual Key O GlobalProtect Satellite	
Address Type	O IPv4 ○ IPv6	
IKE Gateway	IKE	\sim
IPSec Crypto Profile	default	\sim
	Show Advanced Options	
Comment		
	OK Canc	el)

Figure 4.86: Create an IPsec Tunnel

5. Finally, create two security policies, one from Trust to Untrust zone and the other from Untrust to Trust zone.

Security •	Q(
⇒ NAT						Sou	rce			Destination	
🐣 QoS											
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEV
Decryption Tunnel Inspection	1	Trust	none	universal	M Trust	any	any	any	Muntrust	any	any
Application Override	2	Untrust	none	universal	Mag Untrust	any	any	any	Mag Trust	any	any

Figure 4.87: Create two security policies

6. Add windows or Linux VM to Trust Subnet. This VM is for testing ping from Azure side to on-prem. We will not create a public IP address for the VM.

Subscription *	Azure subscription 1	~			
		· ·			
Resource group * 🕕	Pal	\sim			
	Create new				
Instance details					
Virtual machine name * 🛈	linux	\checkmark			
Region * 🛈	(Europe) UK West	\sim			
Availability options 🕕	No infrastructure redundancy required	\vee			
Security type 🕕	Standard	\vee			
Image * 🕕	🖸 Ubuntu Server 20.04 LTS - Gen2 🔊				
	See all images Configure VM generation				
Azure Spot instance ①					
Size * (i)	Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (\$64.02/month)				
	See all sizes				

Create a virtual machine

Figure 4.88: Create a VM

Create a virtual machine

inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more $\ensuremath{\mathbb{C}}^3$

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * 🛈	fwVNET	\sim
Subnet * ①	Trust (10.0.2.0/24) Manage subnet configuration	\checkmark
Public IP ①	None Create new	\checkmark
NIC network security group ①	 None Basic Advanced 	
Delete NIC when VM is deleted ①		
Accelerated networking ①		
Load balancing		
Review + create < Previ	ious Next : Management >	

Figure 4.89: Assign Trust subnet with no public IP

7. Now, you should be able to ping and your tunnel should be green.



Figure 4.90: Ping from WebTerm to Azure



Figure 4.91: Ping from Azure to WebTerm

			IKE Gateway/Satellite						Tunnel Interface
NAME	STATUS	ТҮРЕ	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM
IPSEC	Tunnel Info	Auto Key	ethernet1/1		51.141.71.81	IKE Info	tunnel.1	default (Show Routes)	vsys1

Figure 4.92: Tunnel Status

Capstone Project

250 Palo Alto Firewall

Capstone Project



Figure C.1: Capstone Topology

Well, this is it. The final lab. This will test everything you have learned so far and maybe some more. I will list the requirements and come up with a scenario below. I will not be providing IP addresses or zone information. If you can meet the requirements below, you can consider yourself pretty good at Palo Alto. Good luck!

Scenario: ODI (Openly Deceptive Insurance) is a company looking for a consultant to do all their networking. They have 2 office locations, one in Vancouver, and the other one in England. In the Vancouver site, they want 2 VLANs, VLAN 10 and VLAN 20. VLAN 20 will serve as a login only network, whereas VLAN 10 is for all the employees. Vancouver also hosts their internal webserver where they keep internal records of very important things like their next scam, and list of really good Netflix shows. They also have a site-to-site setup with their England site to access their other resources. But that site-to-site is mainly so that the Vancouver employees have access to British Netflix. The England site is responsible for hosting the public webserver in the DMZ, as well as being the main source of remote access employees so they can access the internal webserver by connecting to the England site online.

Requirements

"Vancouver Site":

- VLAN Configuration
- Captive Portal on VLAN 20
- DHCP Server to provide addressing for VLAN 10 and VLAN 20
- Access Internet through Site to Site VPN
- Site to Site VPN

"England Site":

- Secure DMZ for DMZ webserver
- DoS protection for "public" facing interface
- Site to Site VPN
- Remote Access VPN
- Internet Access

Video Guide

This video will go over how I set it up and maybe some other additional tips and tricks. <u>Download</u> <u>Captions</u>



One or more interactive elements has been excluded from this version of the text. You can view them online here: <u>https://opentextbc.ca/paloalto/?p=331#oembed-1</u>

254 Capstone Project

Appendix: GNS3 Basics

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

Configure Your Palo Alto Firewall Template and Adding the Device

Lets start by modifying the GNS3 template of the Palo Alto firewall by right clicking the existing template, and clicking on "configure template".



Figure A.1: Configure template

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

General setting	s HDD	CD/DVD	Network	Advanced	Usage		
Name:	PaloAlto-1						-
RAM:	4096 MB						4.4
vCPUs:	2						4.4
Qemu binary:	/bin/qemu-s	system-x86_6	54 (v4.2.1)				*
Boot priority:	HDD						+
On dose:	Power off t	he VM					+
Console type:	telnet				Auto start co	onsole	

Figure A.2: Configure RAM and vCPUs

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



Figure A.3: Dragging the Palo Alto

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



Figure A.4: Starting the Palo Alto

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

Webterm Installation

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



Figure A.5: Add a new template

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)	
Import an appliance file (.gns3a extension)	
Manually create a new template	
	<bade next=""> Cancel</bade>

Figure A.6: Select "Install an appliance from the GNS3 server"

On the next window, search for "webterm", select the option under "guests", then click install.

ppliances from ser	ver		and the second			ſ	
Select one or more	appliances to in	all. Update will request the server to download appliances fro	om our online registry,				
Appliance name	Emulator	Vendor					_
Firewalls Guests webterm Routers	Docker	webterm					
Switches 🔷 💊							
		110	data from online registry	e Park	Install	Cap	-

Figure A.7: Search for "webterm"

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

😢 Install webterm appliance		?	×
Server Please choose a server type to install the appliance. The grayed out server types are not supported or configured.		-	
Server type			
 Install the appliance on a remote server 			
Install the appliance on the GNS3 VM (recommended)			
Install the appliance on your local computer			
	Appliance info	Cany	al
		Caric	

Figure A.8: Select "Install the appliance on the GNS3 VM"

On the next screen, click Finish.

Install webterm appliance		?	×
sage Please read the following instructions in order to use your new appliance.		-	Ľ,
The template will be available in the guest category.			
The /root directory is persistent.			
	automatic state and		
	Appliance into < Back Einish	Cano	:el

Figure A.9: Final step of Installation of webterm

After that, it should appear under all devices in GNS3.

Configure Your Webterm Device with a Static IP

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.10: Edit config

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:

3 webterm-1 interfaces		?	×
# # This is a sample network config uncomment lines to configure the network #			
# Static config for eth0			
uto eth0 face eth0 inet static address 10.0.0.2 netmask 255.255.255.0 gateway 10.0.0.1 up echo nameserver 8.8.8.8 > /etc/resolv.conf			
# DHCP config for eth0 # auto eth0 # iface eth0 inet dhcp			
	Refresh Save	Cance	el

Figure A.11: Configure the static IP address

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

Configure a Webterm DHCP Client

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

😚 webterm-1 interfaces	?	×
# # This is a sample network config uncomment lines to configure the network #		
# Static config for eth0 auto eth0 #iface eth0 inet static # 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 config for eth0 auto eth0 liface eth0 inet dhcp		

Figure A.12: Configure the DHCP IP address

Connect Devices in GNS3

Please see the example in the GIF below (if using an offline version of this book, go to the <u>web version</u> <u>of the appendix of *Palo Alto Firewall*):</u>



Figure A.13: Connecting devices

Use 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.14: Using NAT

Make sure you select the GNS3VM as the option whenever you see this window (applies for all devices).



Figure A.15: Select GNS3 VM

Use 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.

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



Figure A.16: Create a new template

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.17: Select "Install an appliance from the GNS3 server"

On the next window, search for "kali", and select the non "CLI" option.

New template						?	
Select one or more	appliances to ins	tall. Update will request the server to do	vnload appliances from our online regi	istry.			
ali							
ppliance name 4 Firewalls	Emulator	Vendor					
Guests							
📃 Kali Linux	Qemü	Kali Linux					
Routers Switches	l Docker	Kali Linux					
Stritenes							
			(Contraction of the				
			Update from online r	registry < <u>B</u> ack	Install	Canc	:e

Figure A.18: Search for "kali"

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

😢 Install webterm appliance	? ×
Server Please choose a server type to install the appliance. The grayed out server types are not supported or or	configured.
Server type	
 Install the appliance on a remote server 	
Install the appliance on the GNS3 VM (recommended)	
Install the appliance on your local computer	
	Appliance info Next > Cancel

Figure A.19: Select "Install the appliance on the GNS3 VM"

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 >	Cancel

Figure A.20: Select Qemu binary

Expand the "2019" option, and download both missing files. Also, you can download the latest version. Version 2019 is more stable in GNS3.

ease select one version of Kall Linux and impo	ort the rec	Jired files. Files are searched in your downloads and GNS3 images directories by default	-
ppliance version and files	Size	Status	
Kali Linux version 2021.1	3.4 GB	Ready to install Would say missing	
 Kali 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)	
 Kali 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)	
Kali 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)	
Kali 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)	
Kali 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)	
 Kali 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)	
 Kali 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)	
Kali 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)	
Kali Linux version 2017.2	2.8 GB	Missing files	
1.1.2 3073 1012	3.0.00		
Import Download		Allow custom files Create a new	v version <u>R</u> efresh

Figure A.21: Select "kali-linux-2019.3-amd64.iso"


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

Figure A.22: Select "kali-linux-2019.3-amd64.iso"

It should take a second, but GNS3 will start to load up the ISO into the GNS3VM.



Figure A.23: Loading the ISO image

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



Figure A.24: Ready to install

Then click Finish.

😢 Install Kali Linux appliance.	? X
Usage 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.25: Final step of configuration

Use WordPress in GNS3

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



Figure A.26: Create a new template

We want to install an appliance from the GNS3 server.

New template	?
lew 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)	
∬ <u>M</u> anually create a new template	
	< Back Next > Cancel

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

Lookup "WordPress", then click Install.

New template		?	
ppliances from server Select one or more applian	es to install. Update will request the server to download appliances from our online reg	jistry.	
ordpress			
ppliance name 🔺 Emulat	or Vendor		
Firewalls			
WordPress Docke	Turnkey Linux		
Routers			
Switches			
	Update from online	registry < Back Install Ca	ancel

Figure A.28: Search for "WordPress"

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



Figure A.29: Verify WordPress Installation

Configure WordPress



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

Figure A.30: 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.31: WordPress is Ready!

Use 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			
			Port	+ VLAN	Туре	EtherType
Port:	8	¥	0	1	access	
10.001			1	1	access	
VLAN:	1	*	2	1	access	
-	Luca de		3	1	access	
Type:	access	· · · · ·	5	1	access	
	o factores		6	1	access	
QinQ Ether i yp	e: 10x8100	-	7	1	access	
	4	Delate				•

Figure A.32: 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:	Switch1					
Console type:	none					-
Settings			Ports			
	-		Port	+ VLAN	Туре	EtherType
Port:	1	¥	0	1	access	
	1.	Tel.	1	1	access	
VLAN:	1		2	1	access	
			3	1	access	
Type:	access	*	4	1	access	
			2	4	access	
QinQ EtherTyp	e: 0x8100	+	7	1	access	
					000000	
		Dalata				
Ad	•	Delete				

Figure A.33: Double click on port7

General						
Name:	Switch 1					
Console type:	none					-
Settings			Ports			
	1-	1.0	Port	+ VLAN	Туре	EtherType
Port:	1	¥	0	1	access	
	1		1	1	access	
VLAN:	1	-	2	1	access	
			3	1	access	
Type:	dot1q	T	4	1	access	
			2		access	
QinQ EtherType	e: 0x8100	π.	0	-	access	
			4		access	
		Public.				
Add		Delete				

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

Figure A.34: Select port7 as dot1q

Click on add to apply the changes.

General							
Name:	Switch1						1
Console type:	none						-
Settings			Ports				
Dort	0		Port	+ VLAN	Туре	EtherType	1
Port	0	T	0	1	access		
VLAN:	1	*	1	1	access		
10.00	1-	1-1	2	1	access		
Type:	dot1a	*	4	1	access		
	(5	1	access		
QinQ EtherType	e: 0x8100	-	6	1	access		
			7	1	dot1q		
Add	1	Delete				1	Þ.

Figure A.35: Click on Add to apply the changes

Then click Apply and OK.

284 Palo Alto Firewall

Acknowledgements

We 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.

We would like to thank my great students and friends Lewis Saludo, Tung Lee, and Jason Manning for their thoughtful feedback and great suggestions during this project.

286 Palo Alto Firewall

About the Authors

Hamid Talebi

Hamid Talebi 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.

Xavier Cawley

Xavier Cawley is a Junior Devops Engineer and recent graduate of the CISA program at BCIT. He has always had an interest in and knack for technology ever since the age of 10, whether it was fiddling with jumpers, or automating some tedious tasks for school. Whilst participating in the CISA program, Xavier was well known for creating guides and documentation for several classes and aiding students on labs and assignments.





288 Palo Alto Firewall

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	November 29, 2023	Book published.	First version.