

# 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 [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/), 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 [CC BY 4.0 licence](https://creativecommons.org/licenses/by/4.0/).

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

Download for free from the [B.C. Open Collection](#).

**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](https://bccampusopeneducation.ca/) to learn about open education in British Columbia.

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

# Contents

Accessibility Statement	vii
For Students: How to Access and Use this Textbook	xi
About BCcampus Open Education	xiii
Dedication	xv
A Practical Introduction	1
 <u>Chapter 1. Basics</u>	
1.1 GNS3 and Palo Alto	5
1.2 DORA the DHCP Provider	25
1.3 SNAT	47
1.4 DNAT	55
 <u>Chapter 2. Security Tuneup</u>	
2.1 Work with Applications	71
2.2 Deal with Bad Actors	77
2.3 Block Files and Viruses	111
 <u>Chapter 3. Advanced Networking</u>	
3.1 Captive Portal	129
3.2 Remote Access VPN	155
3.3 Site-to-Site VPN	183
 <u>Chapter 4. Cloud Technologies</u>	
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
 <u>Capstone Project</u>	
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 [web version of this resource](#) has been designed to meet [Web Content Accessibility Guidelines 2.0](#), level AA. In addition, it follows all guidelines in [Appendix A: Checklist for Accessibility](#) of the [Accessibility Toolkit – 2nd Edition](#). 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.

### Accessibility Checklist

Element	Requirements	Pass?
<b>Headings</b>	Content is organized under headings and subheadings that are used sequentially.	Yes
<b>Images</b>	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
<b>Images</b>	Images and text do not rely on colour to convey information.	Yes
<b>Images</b>	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
<b>Tables</b>	Tables include row and/or column headers that have the correct scope assigned.	Yes
<b>Tables</b>	Tables include a title or caption.	Yes
<b>Tables</b>	Tables do not have merged or split cells.	Yes
<b>Tables</b>	Tables have adequate cell padding.	Yes
<b>Multimedia</b>	Videos have captions of all speech content and relevant non-speech content that has been edited by a human for accuracy.	Yes
<b>Links</b>	The link text describes the destination of the link.	Yes
<b>Links</b>	Links do not open new windows or tabs. If they do, a textual reference is included in the link text.	Yes
<b>Links</b>	Links to files include the file type in the link text.	Yes
<b>Font</b>	Font size is 12 point or higher for body text.	Yes
<b>Font</b>	Font size is 9 point for footnotes or endnotes.	Yes
<b>Font</b>	Font size can be zoomed to 200% in the webbook or eBook formats.	Yes

## Known Accessibility Issues and Areas for Improvement

- The book relies heavily on screenshots from 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: [Report an Error](#)

This statement was last updated on November 29, 2023.

The Accessibility Checklist table was adapted from one originally created by the [Rebus Community](#) and shared under a [CC BY 4.0 License](#).

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: [Palo Alto Firewall: Practical Guidance and Hands-On Labs](#). To download the book in a different format, look for the “Download this book” drop-down menu and select the file type you want.

### How can I use the different formats?

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

## Tips for Using This Textbook

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

---

## About BCcampus Open Education

*Palo Alto Firewall: Practical Guidance and Hands-On Labs* by Hamid Talebi and Xavier Cawley was funded by BCcampus Open Education.

[BCcampus Open Education](#) began in 2012 as the B.C. Open Textbook Project with the goal of making post-secondary education in British Columbia more accessible by reducing students' costs through the use of open textbooks and other OER. [BCcampus](#) 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 [Ministry of Post-Secondary Education and Future Skills](#) and the [Hewlett Foundation](#).

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

For more information about open education in British Columbia, please visit the [BCcampus Open Education](#) website. If you are an instructor who is using this book for a course, please fill out our [Adoption of an Open Textbook](#) form.

This book was produced using the following styles: [Palo Alto Firewall: Practical Guidance and Hands-On Labs Style Sheet \[Word file\]](#)



## Dedication

This book is dedicated to to our loving parents.



---

# 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 book
- Open 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:

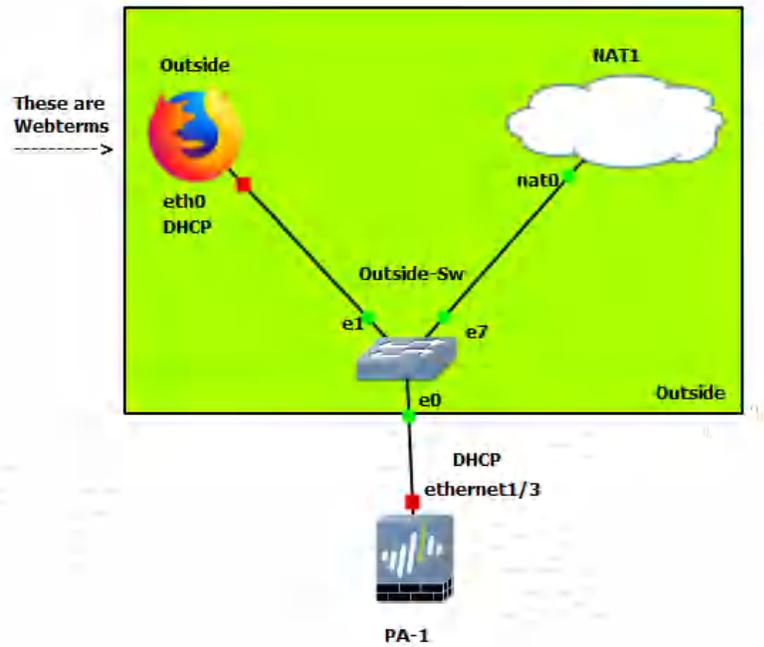


Figure E.1: An example scenario

## 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

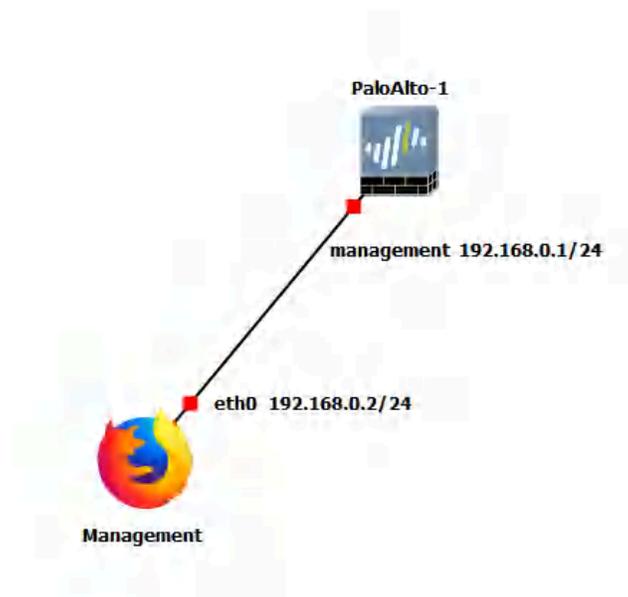


Figure 1.1: Main Scenario

**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.

```

[ 0.905330] md: ... autorun DONE.
[ 0.906307] Using alternate root: /dev/vda2...
[ 0.907927] EXT4-fs (vda2): mounting ext3 file system using the ext4 subsystem
[ 0.912123] EXT4-fs (vda2): mounted filesystem with ordered data mode. Opts:
(null)
[ 0.914112] VFS: Mounted root (ext3 filesystem) readonly on device 253:2.
[ 0.916722] devtmpfs: mounted
[ 0.919799] Freeing unused kernel memory: 2408K
[ 0.928208] Write protecting the kernel read-only data: 22528k
[ 0.930791] Freeing unused kernel memory: 2012K
[ 0.934554] Freeing unused kernel memory: 1496K
[ 0.977518] random: fast init done
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::ec2:90ff:fe58:0 prefixlen 64 scopeid 0x20<link>
    ether 0c:c2:90:58:00:00 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3 bytes 174 (174.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 0c:c2:90:58:00:00 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    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

Master started successfully
vm login: █ No Login!

```

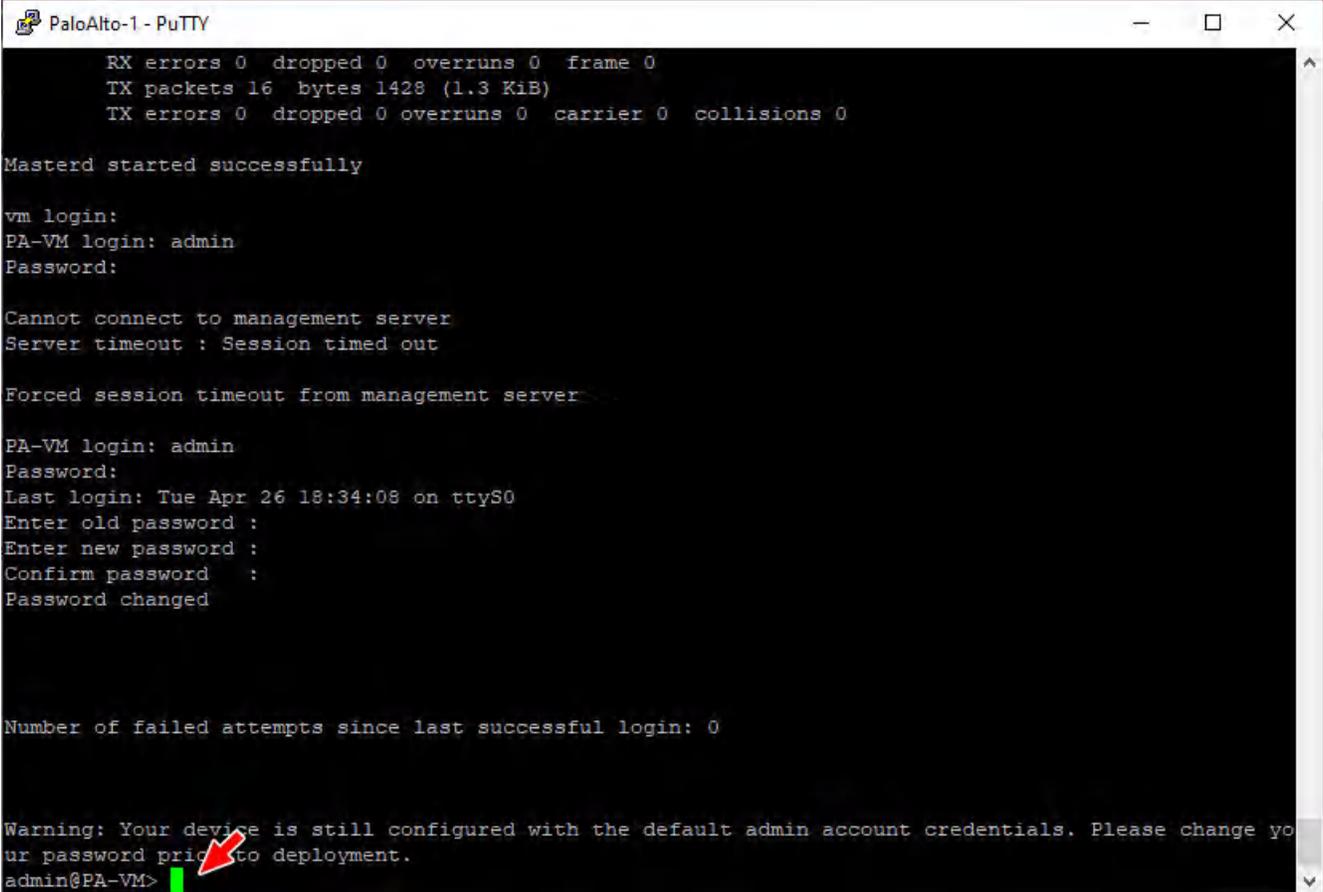
Figure 1.2: No Login

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 prior to 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:

- 1) `configure`
- 2) `set deviceconfig system type static`
- 3) `set deviceconfig system ip-address 192.168.0.1 netmask 255.255.255.0`
- 4) `commit`

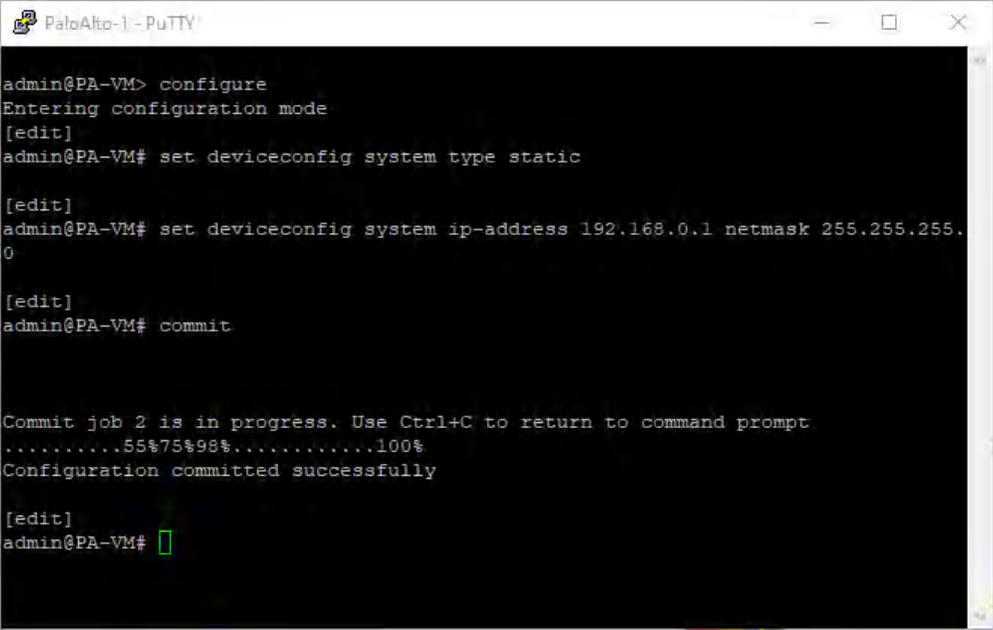
**Line 1:** Gets you into configuration mode.

**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:



```
PaloAlto-1 - PuTTY
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# set deviceconfig system type static

[edit]
admin@PA-VM# set deviceconfig system ip-address 192.168.0.1 netmask 255.255.255.0

[edit]
admin@PA-VM# commit

Commit job 2 is in progress. Use Ctrl+C to return to command prompt
.....55%75%98%.....100%
Configuration committed successfully

[edit]
admin@PA-VM# █
```

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:

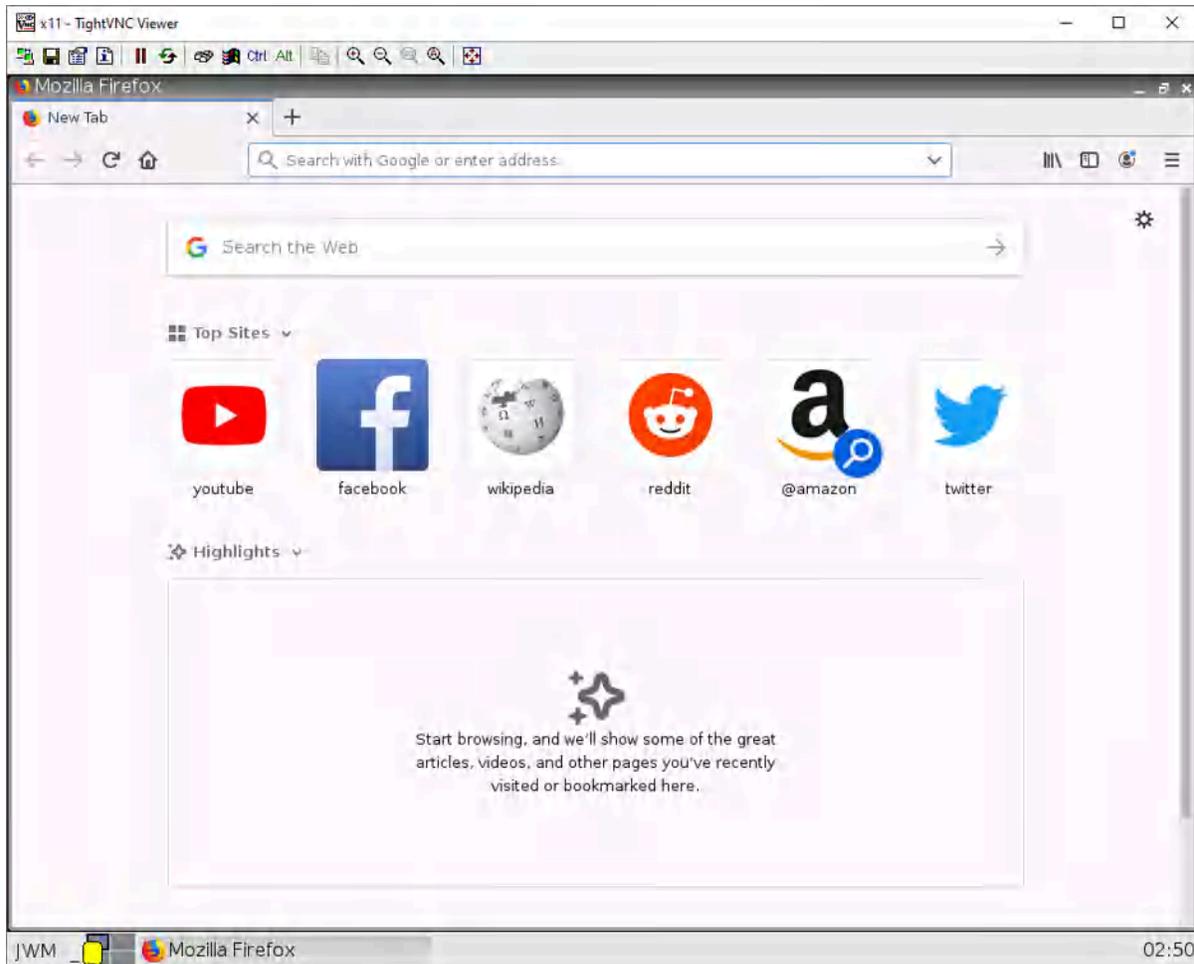


Figure 1.5: WebTerm Firefox browser

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

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

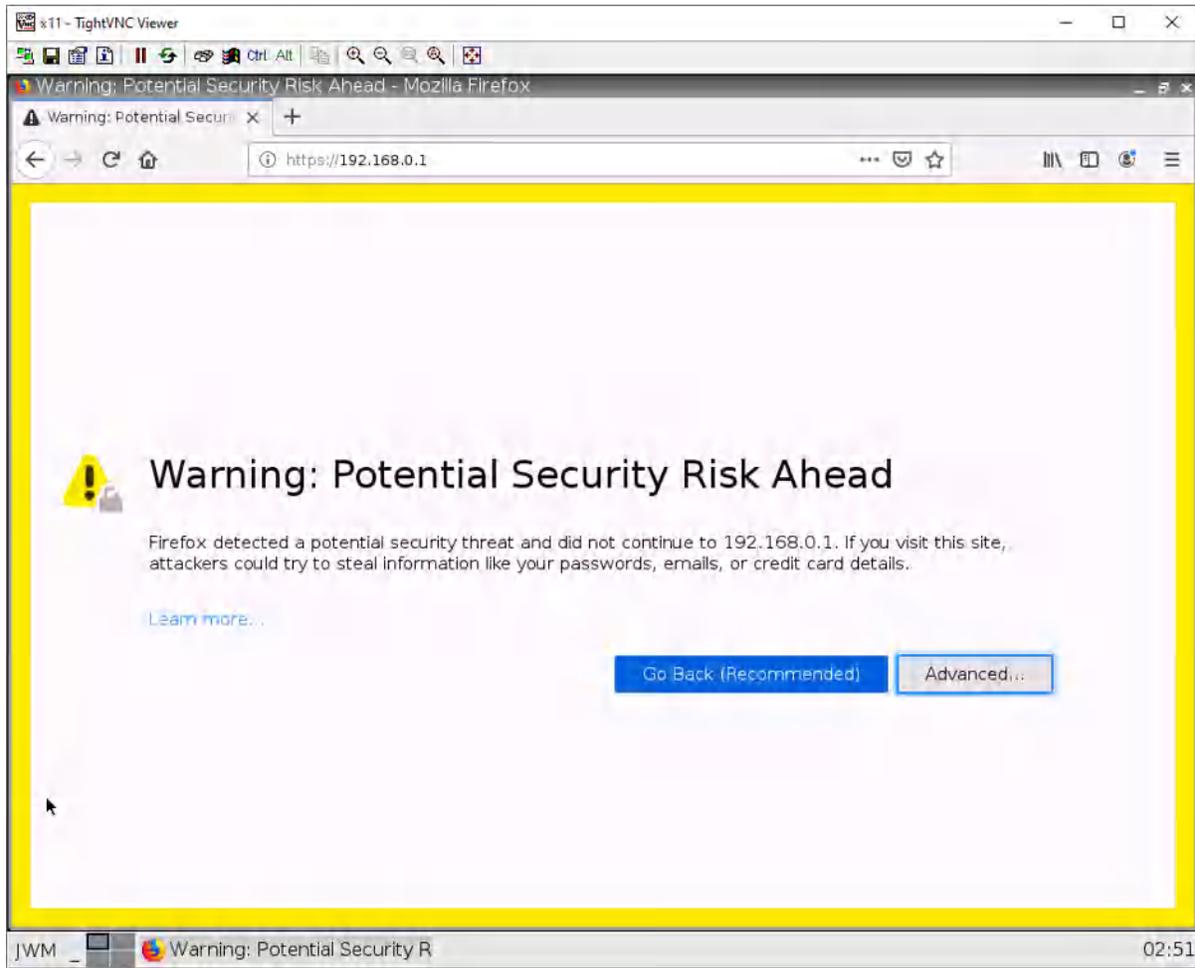


Figure 1.6: Type IP address of Palo Alto

To get past this, click advanced, then click **“Accept the Risk”**.

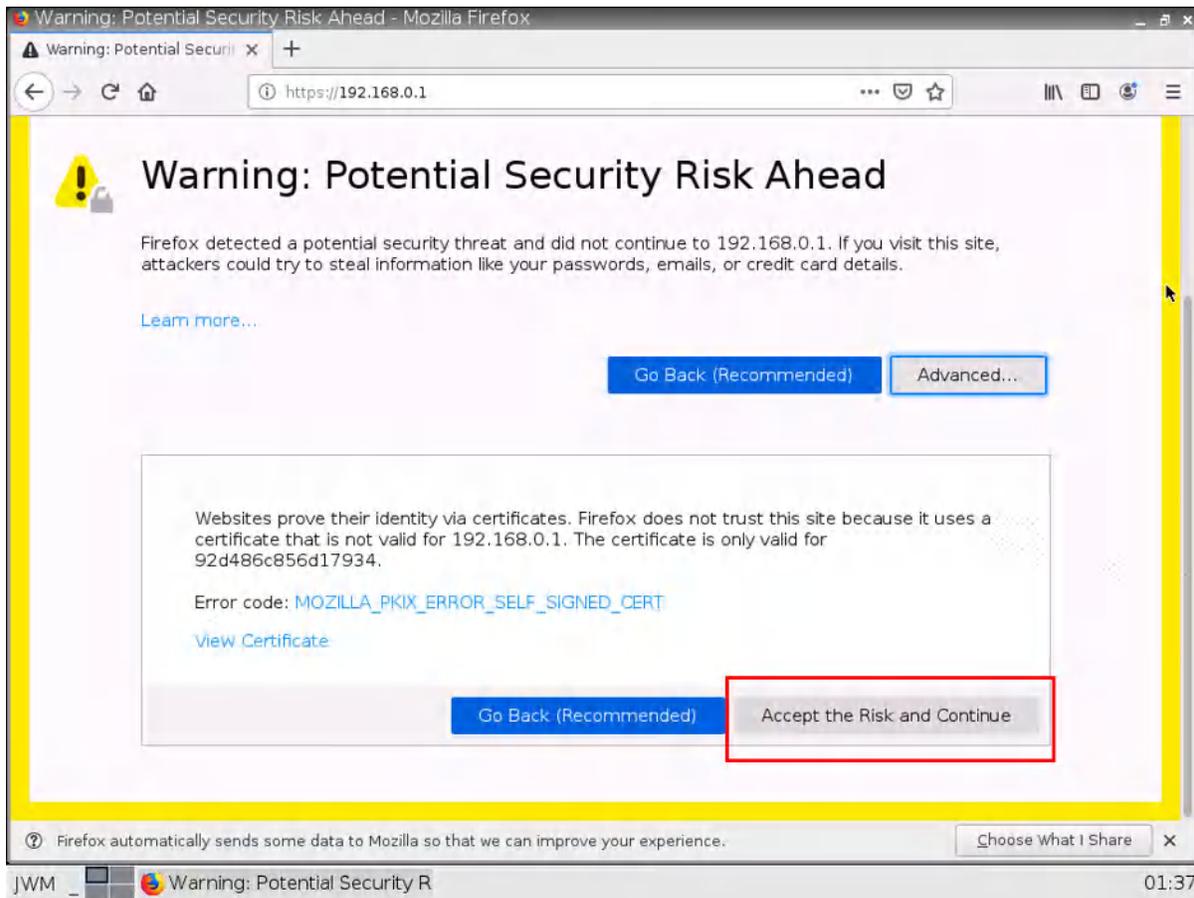


Figure 1.7: Past of security warning

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.

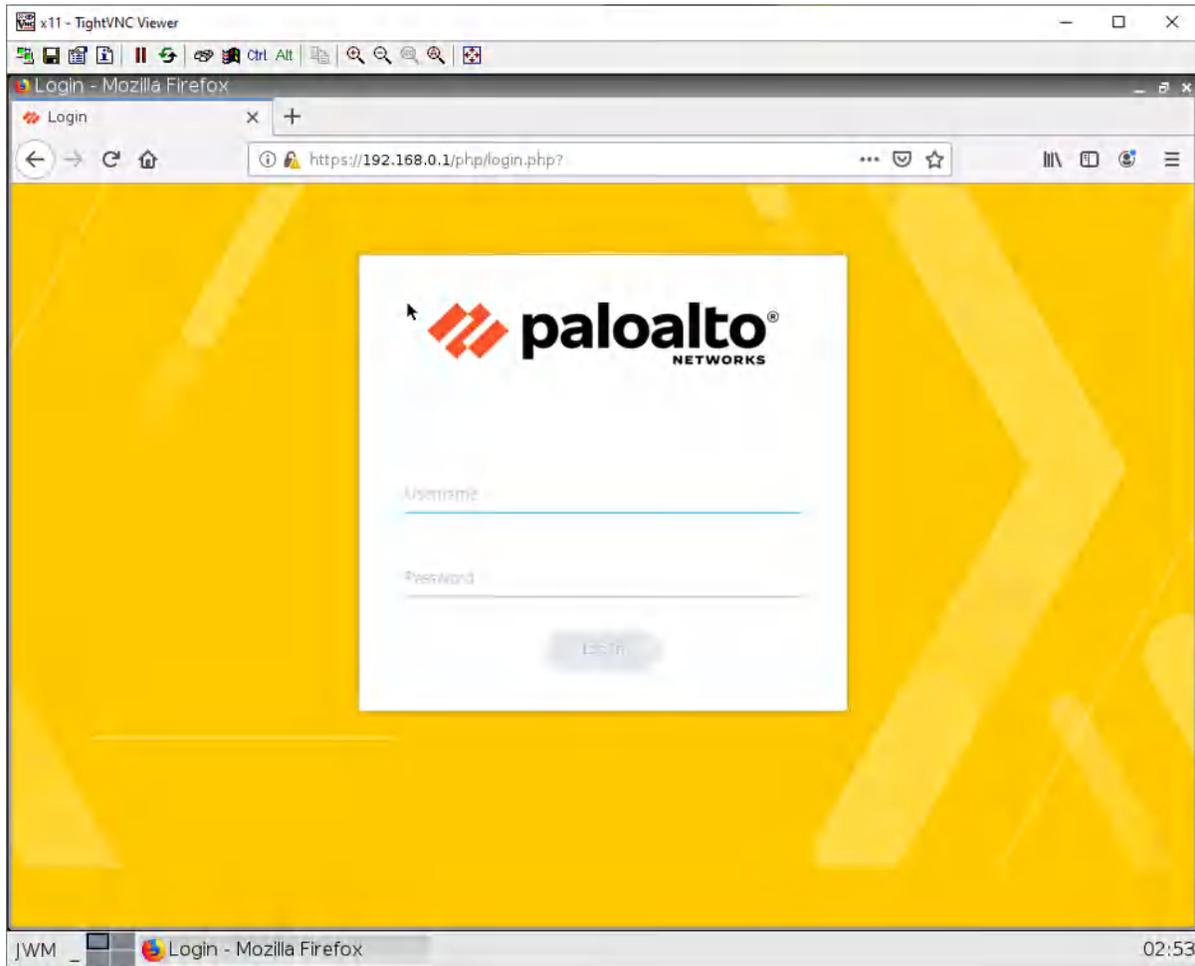


Figure 1.8: Enter credentials

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

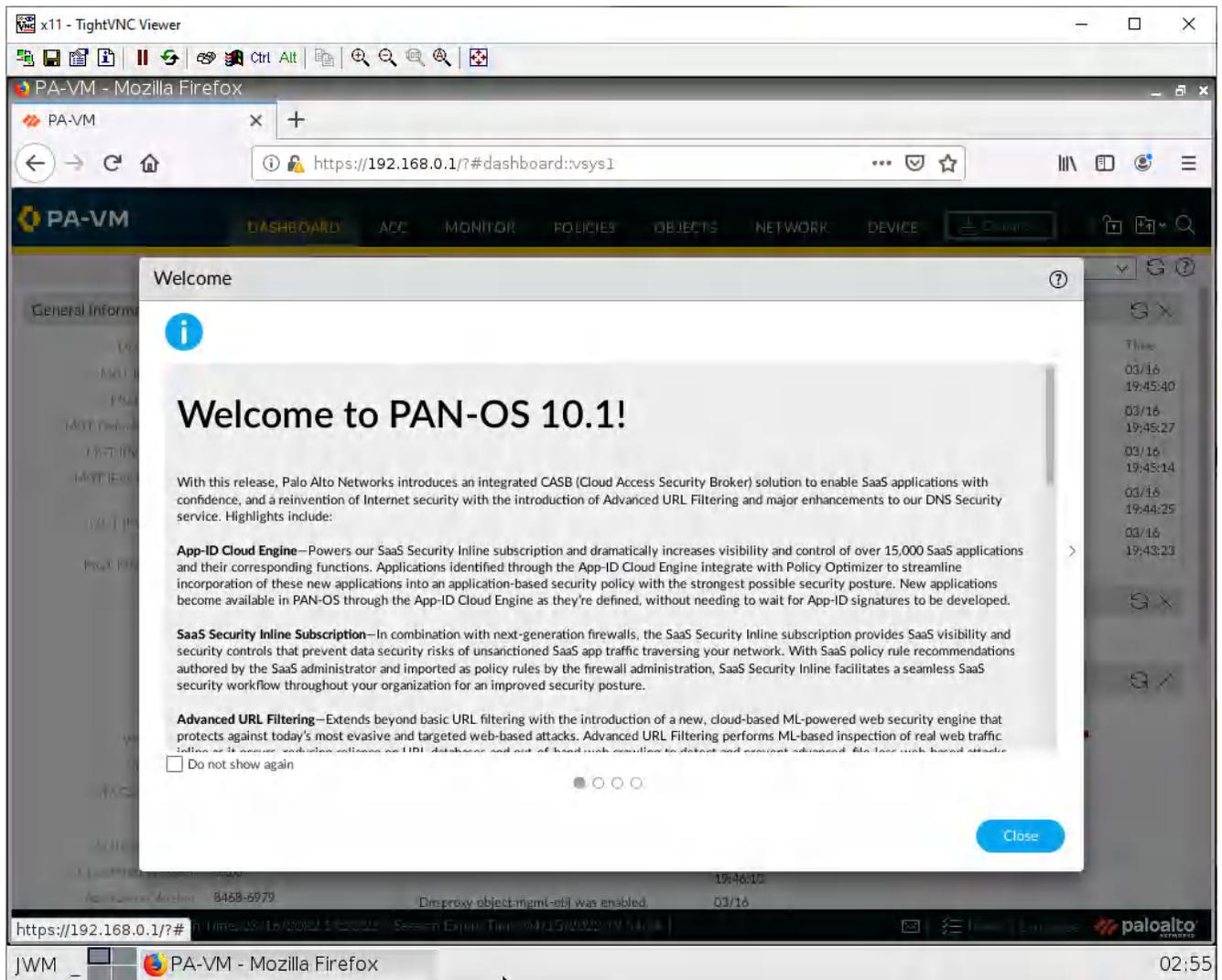


Figure 1.9: First page of Palo Alto

## Explore the Web Interface

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

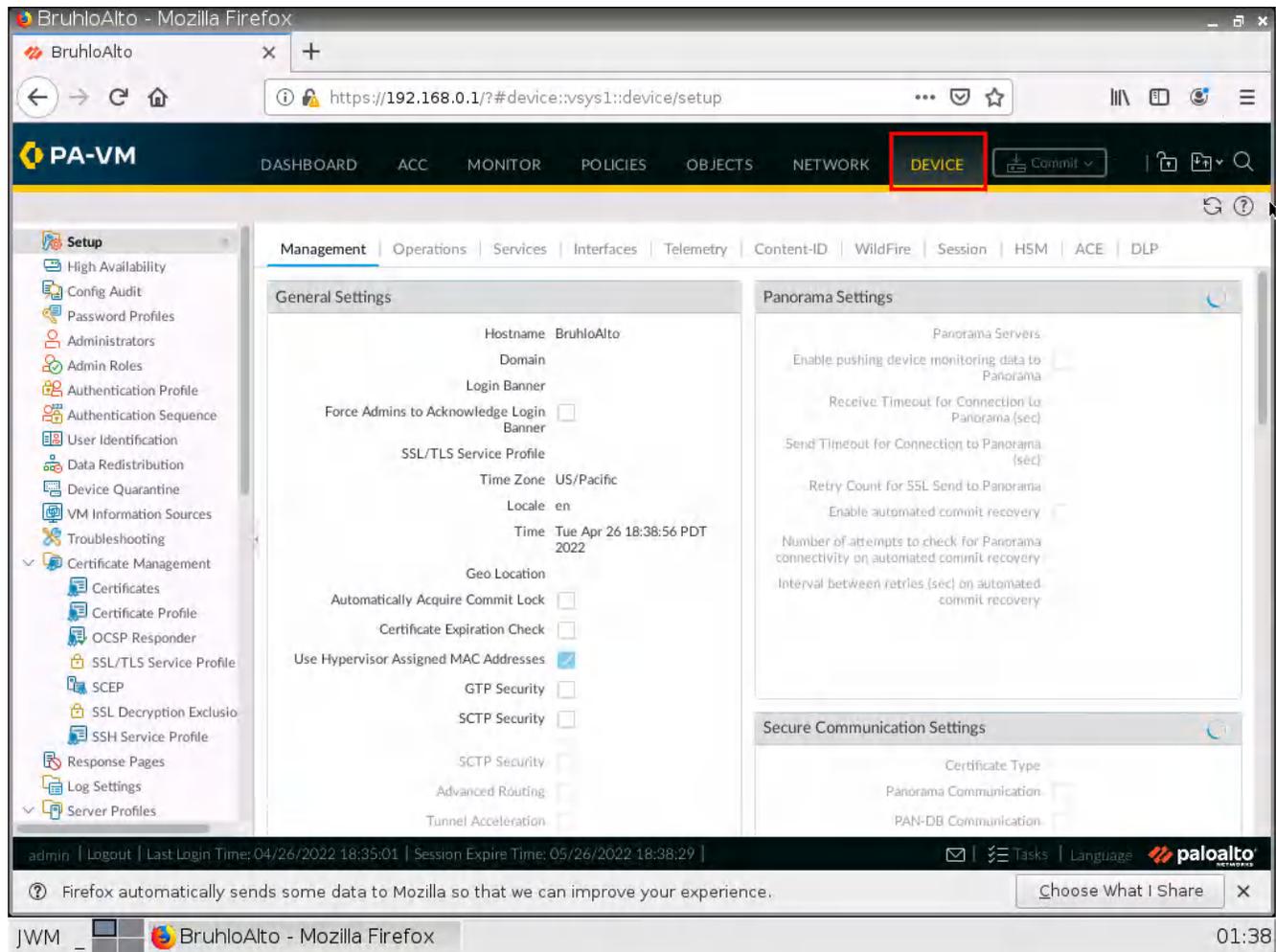


Figure 1.10: Device Settings

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.

The screenshot displays the Palo Alto VM (PA-VM) Network Interfaces Settings page. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK' (highlighted), and 'DEVICE'. The left sidebar shows a tree view of configuration options, with 'Network Profiles' expanded. The main content area shows a table of 8 Ethernet interfaces. The 'VIRTUAL ROUTER' field for 'ethernet1/7' is highlighted with a mouse cursor.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL
ethernet1/1			none	none	none	Untagged	none
ethernet1/2			none	none	none	Untagged	none
ethernet1/3			none	none	none	Untagged	none
ethernet1/4			none	none	none	Untagged	none
ethernet1/5			none	none	none	Untagged	none
ethernet1/6			none	none	none	Untagged	none
ethernet1/7			none	none	none	Untagged	none
ethernet1/8			none	none	none	Untagged	none

admin | Logout | Last Login Time: 04/26/2022 18:35:01 | Session Expire Time: 05/26/2022 18:38:29 | Tasks | Language | paloalto

Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share

JWM BruhloAlto - Mozilla Firefox 01:39

Figure 1.11: Network Interfaces Settings

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

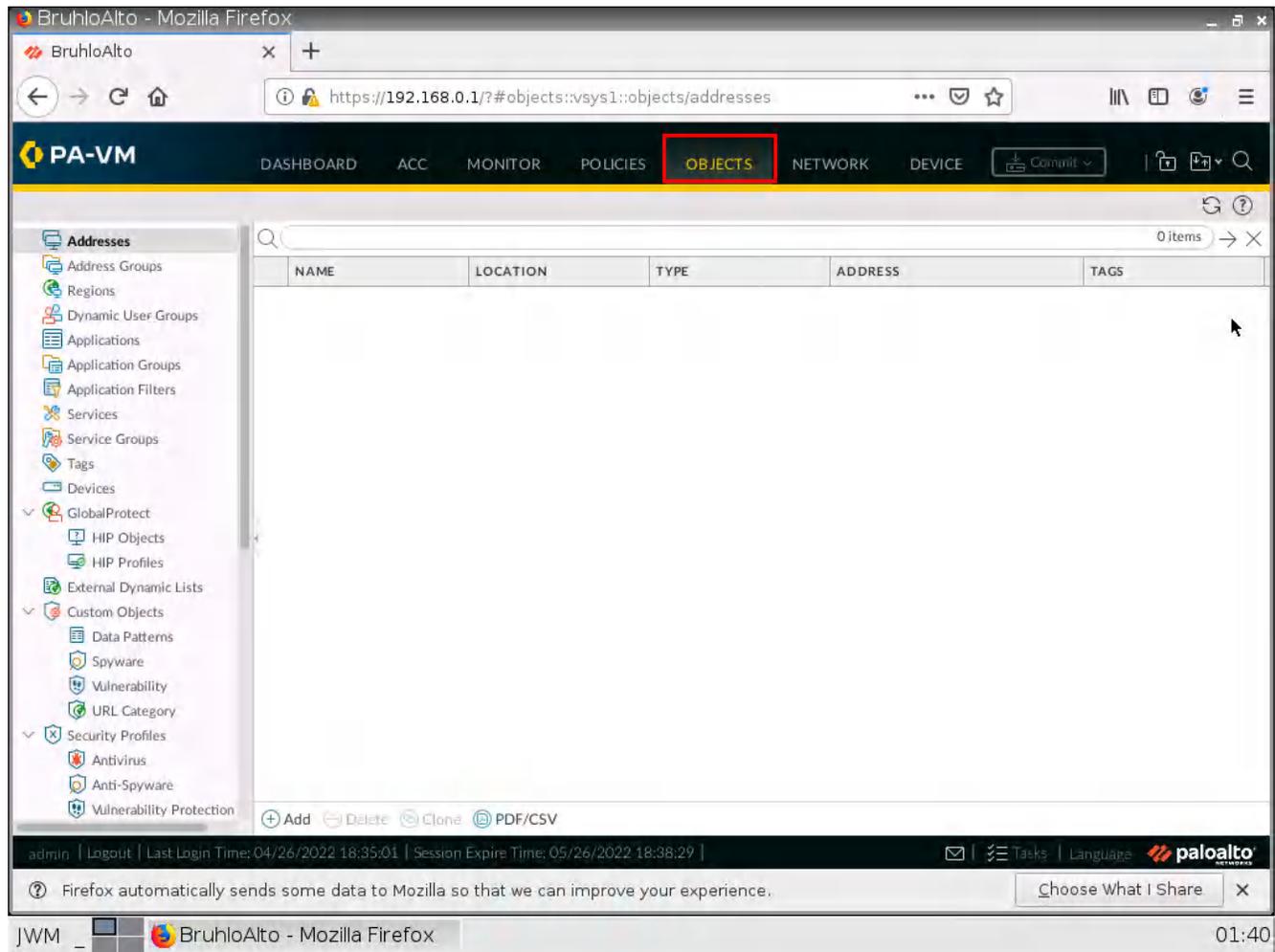


Figure 1.12: Objects Settings

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.

The screenshot shows the Palo Alto VM web interface. The 'POLICIES' tab is highlighted in red. The main content area displays a table of security policies. The table has the following structure:

	NAME	TAGS	TYPE	Source				
				ZONE	ADDRESS	USER	DEVICE	ZONE
1	intrazone-default	none	intrazone	any	any	any	any	(intrazone)
2	interzone-default	none	interzone	any	any	any	any	any

The left sidebar shows a navigation menu with categories like Security and Policy Optimizer. The bottom of the interface includes a toolbar with actions like Add, Delete, Clone, and a footer with user information and session details.

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.

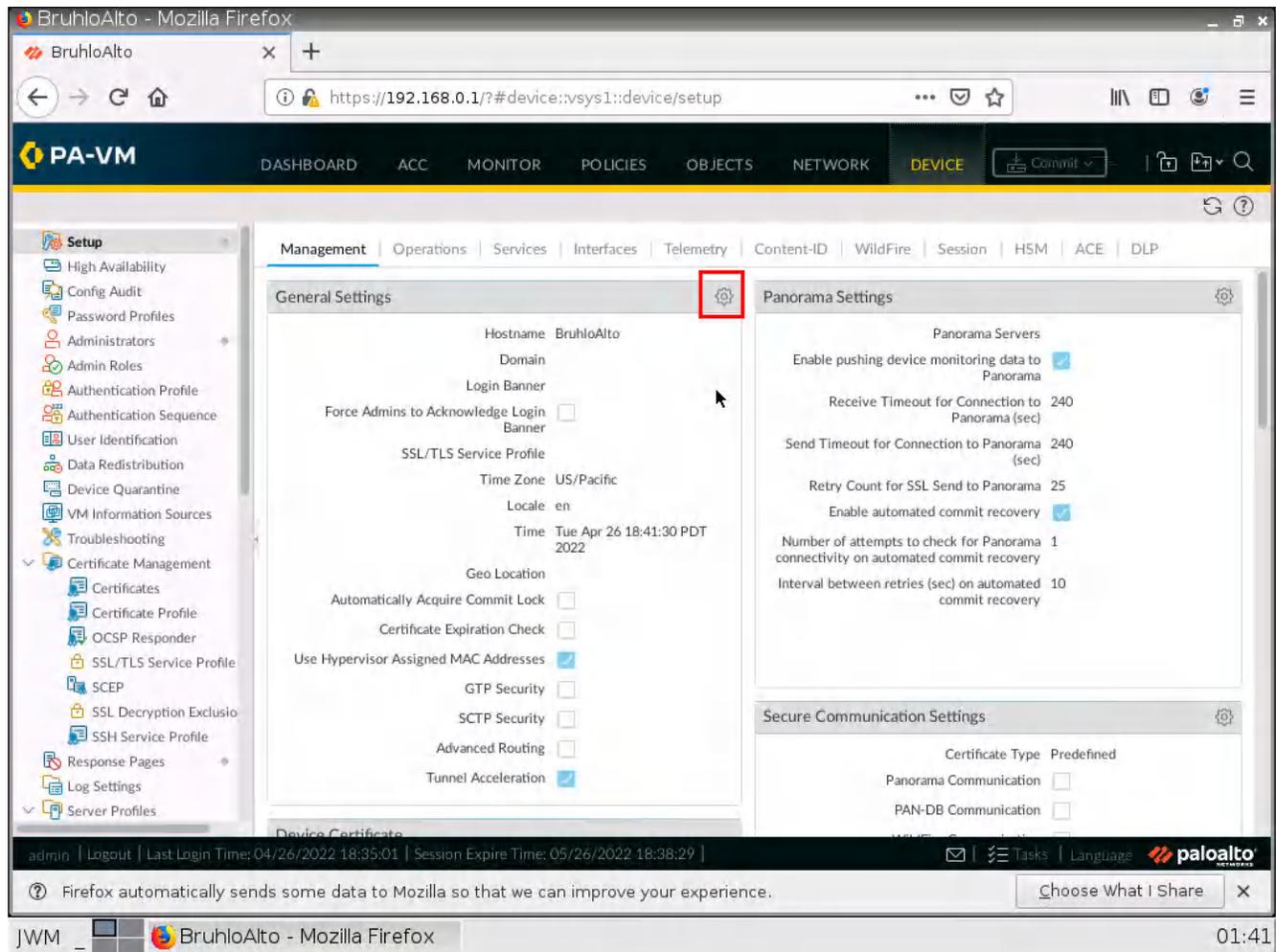


Figure 1.14: Changing hostname

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.

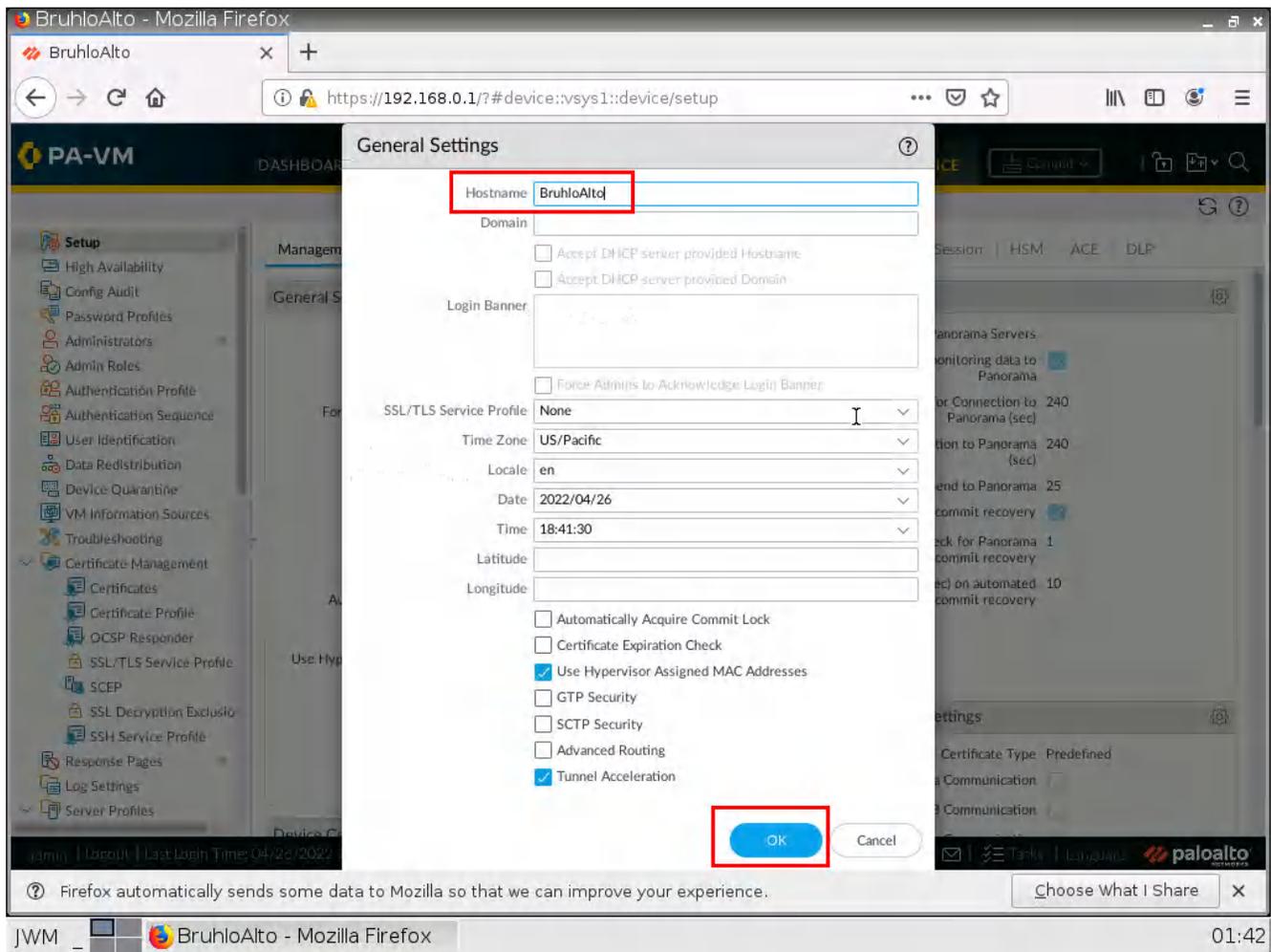


Figure 1.15: General Settings

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.

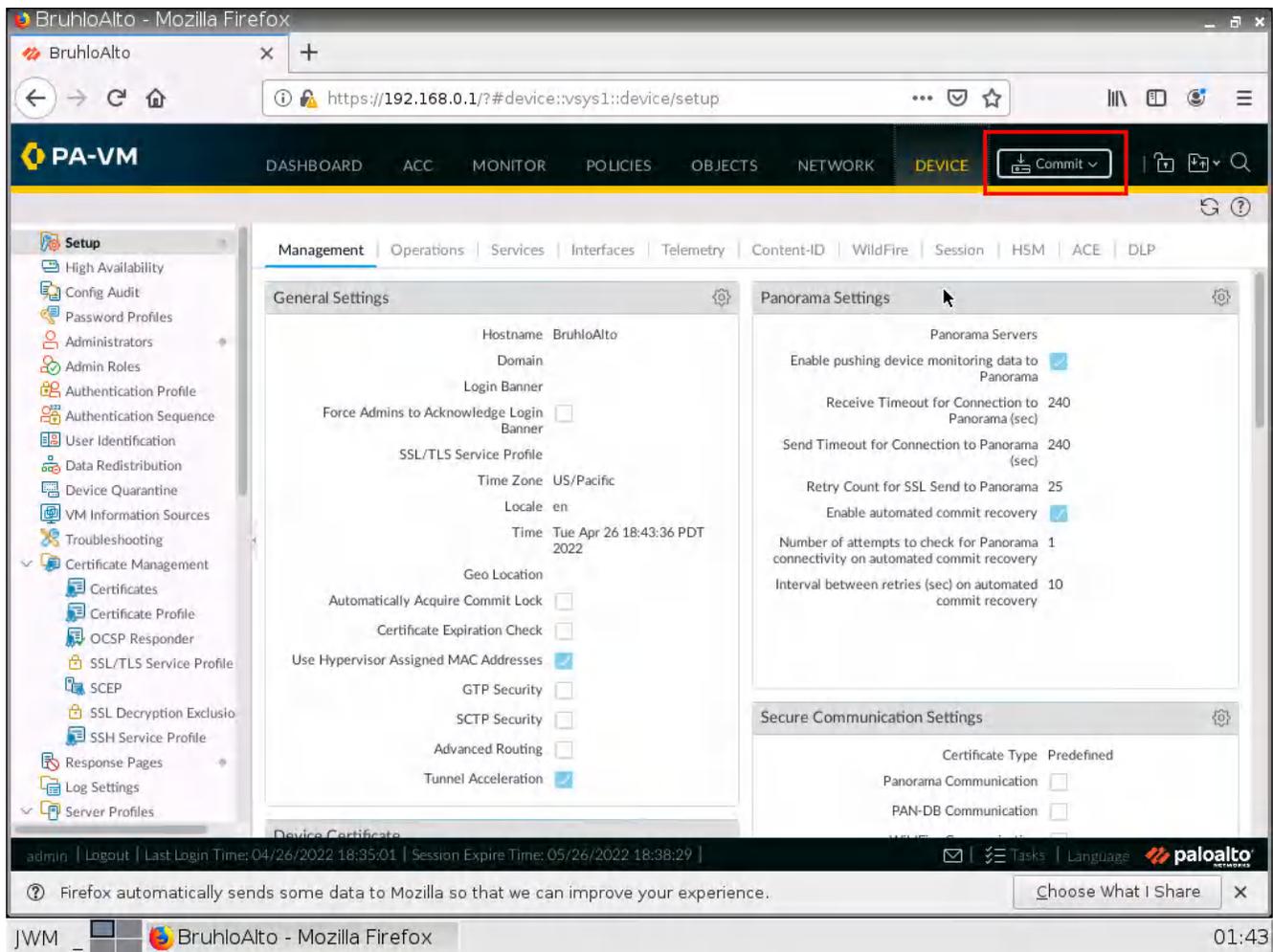


Figure 1.16: Commit Configuration

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.

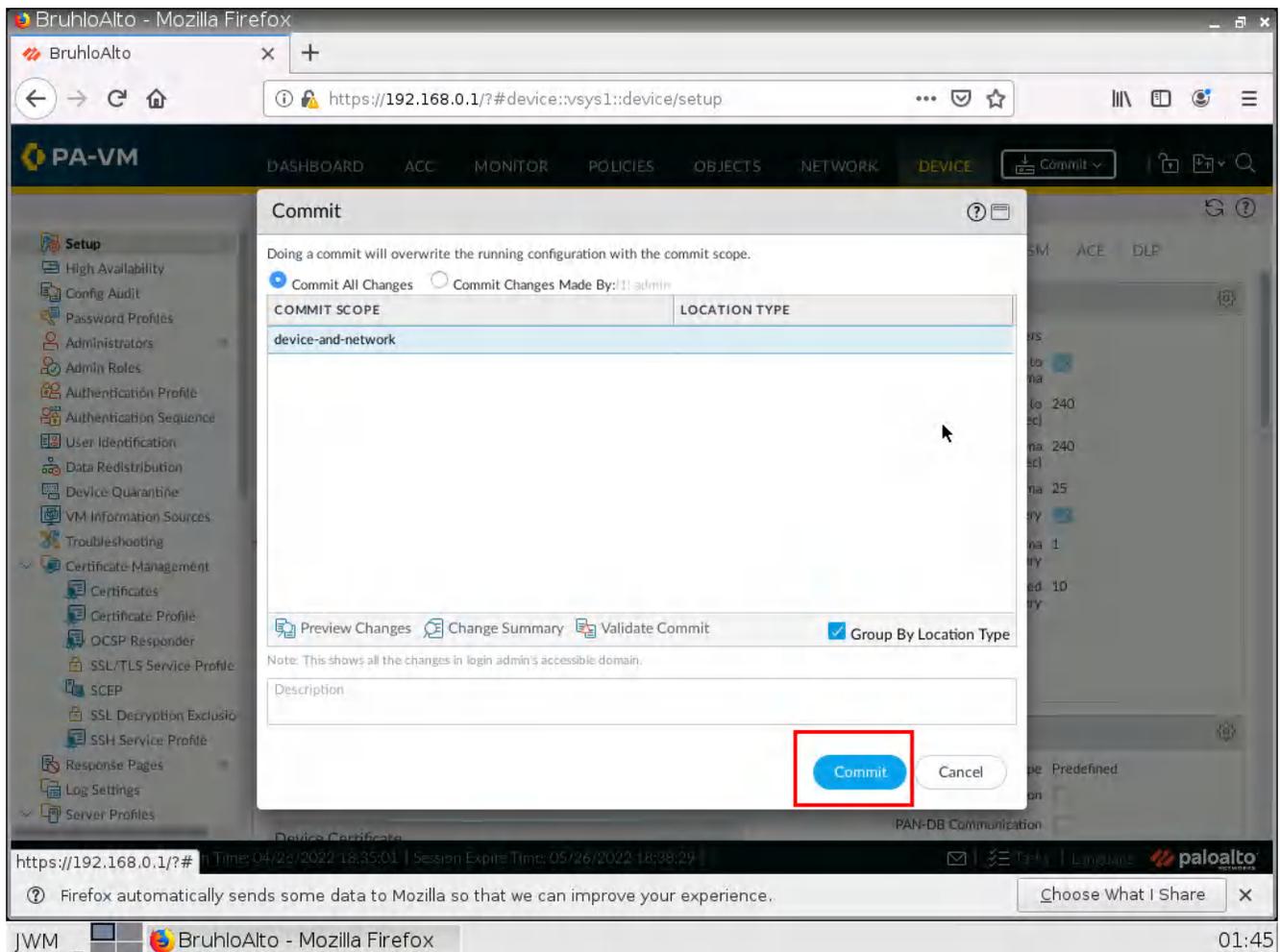


Figure 1.17: Commit all changes

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

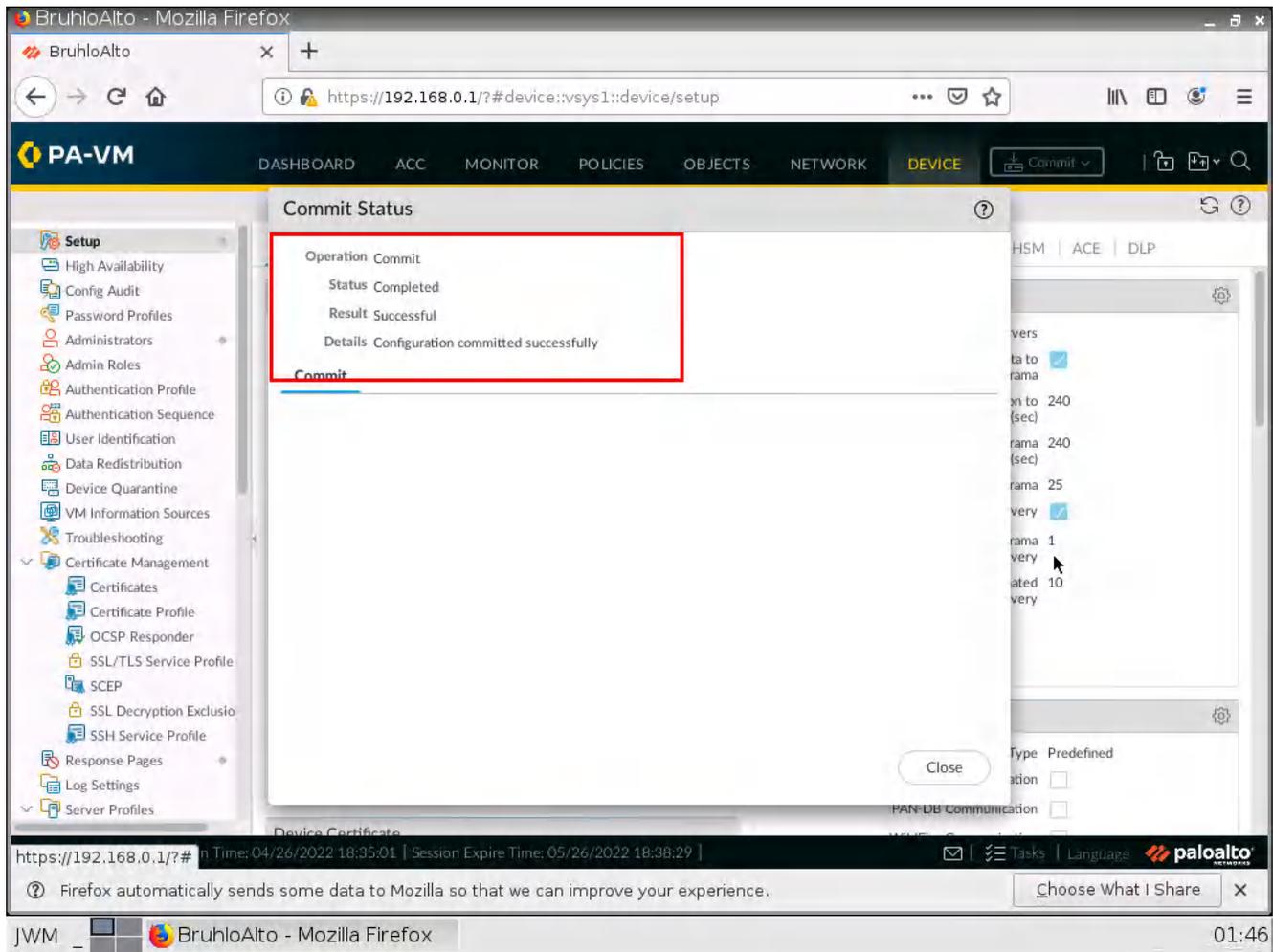


Figure 1.18: Configuration committed successfully

## 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.

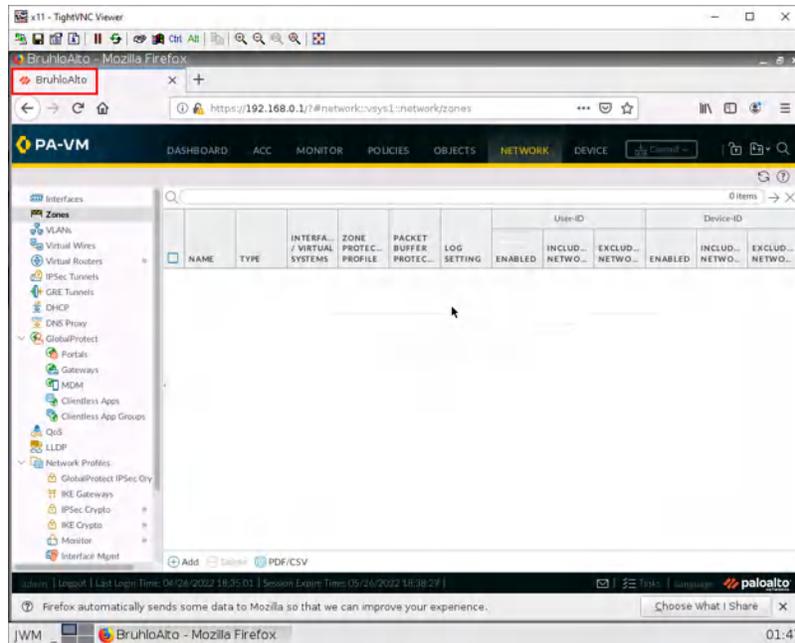


Figure 1.19: Verify configuration

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

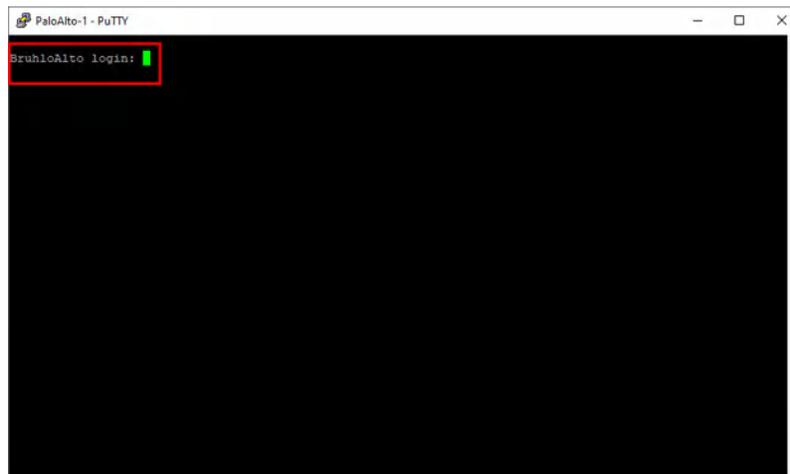


Figure 1.20: Verify configuration in CLI



## 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).

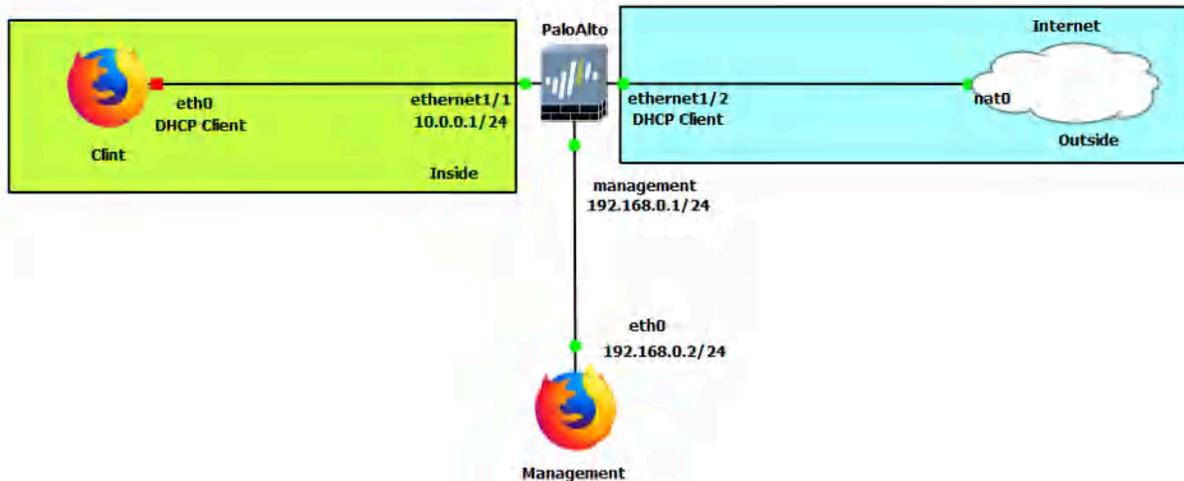


Figure 1.21: main scenario

**Table 1.2: Addressing Table**

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 1.3: 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.

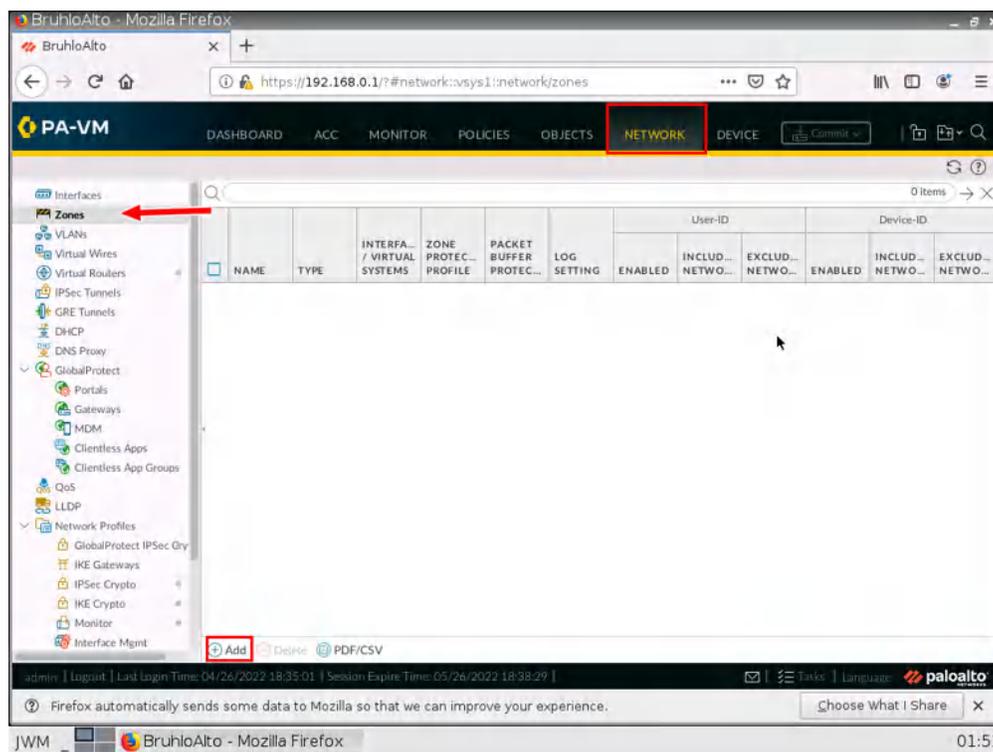


Figure 1.22: Creating zones

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!)

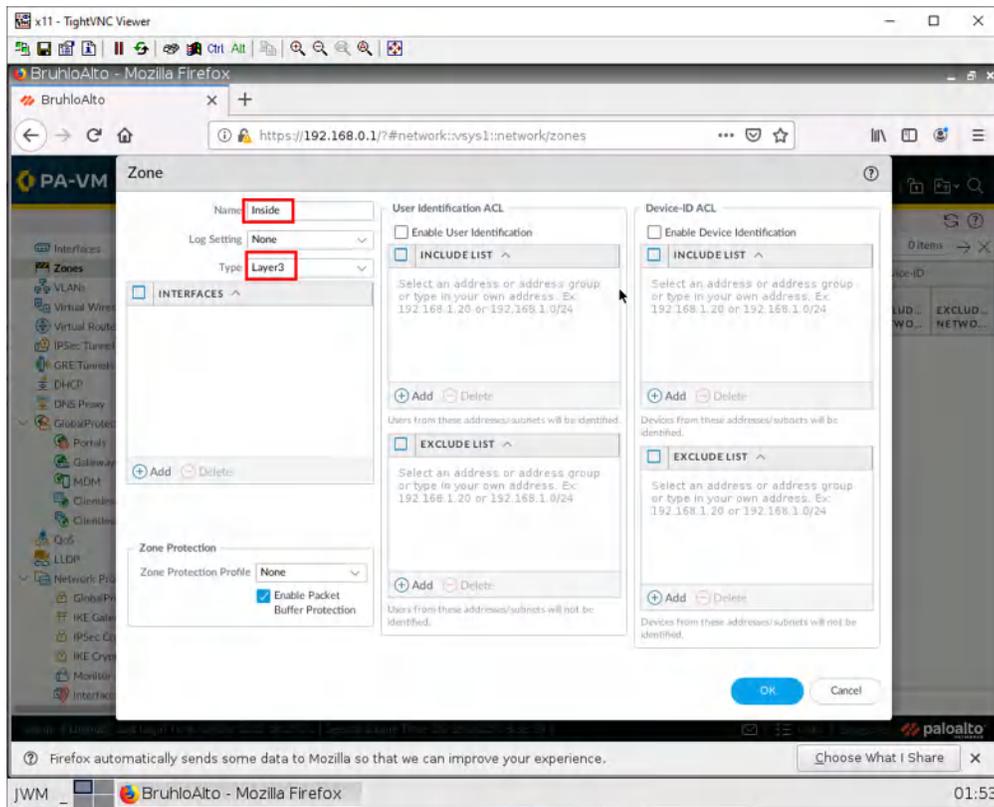


Figure 1.23: Create a zone Inside as a layer3

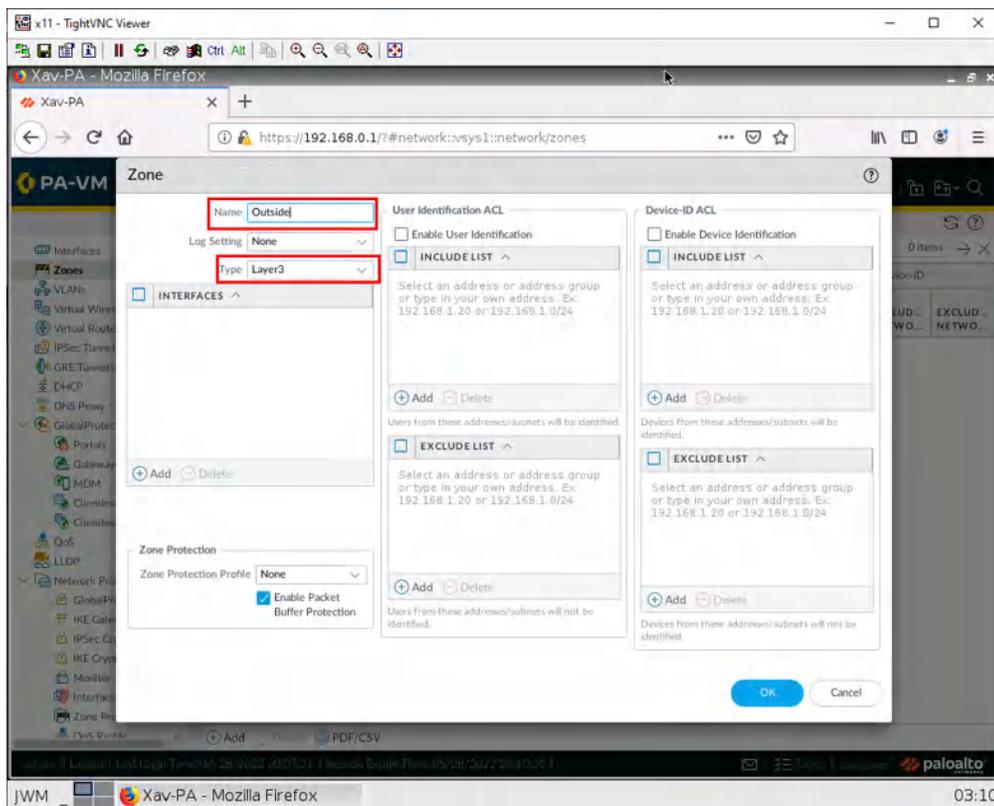


Figure 1.24: Create a zone Outside as a layer3

## Set Up a Static Interface IP Address in Palo Alto

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

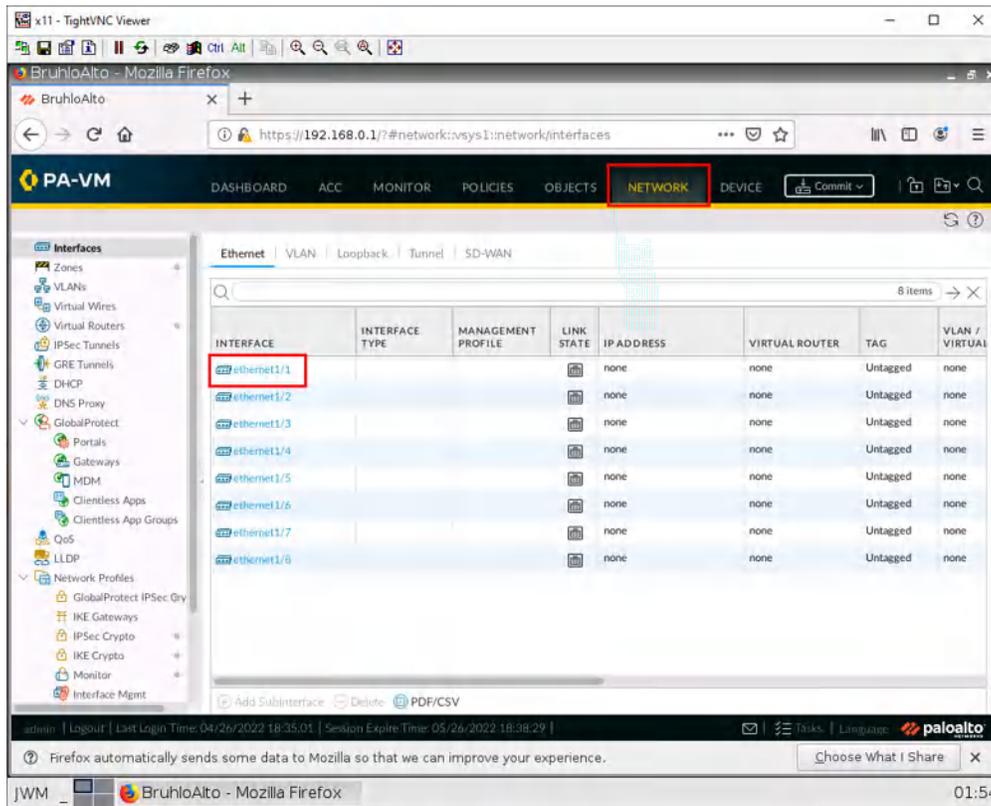


Figure 1.25: Select Ethernet 1/1

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.

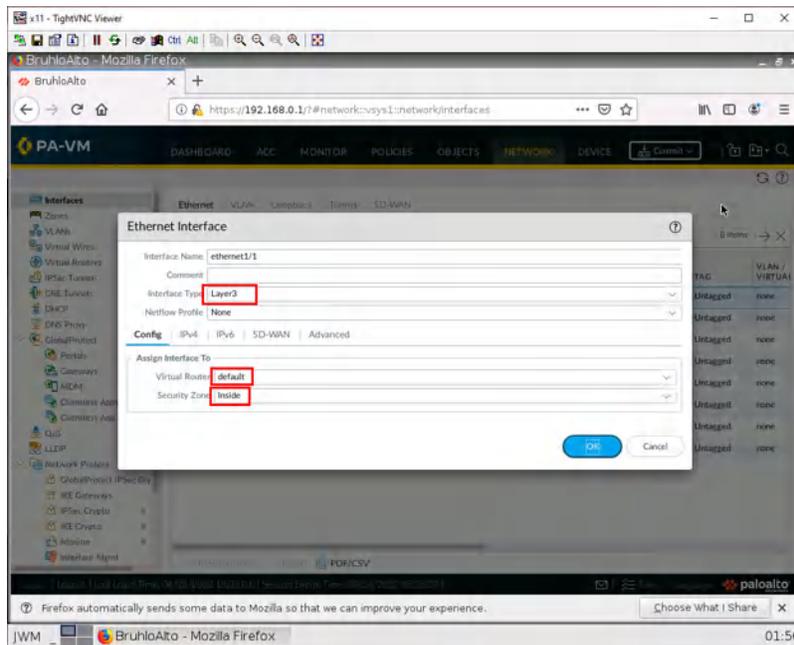


Figure 1.26: Ethernet 1/1 Configuration

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

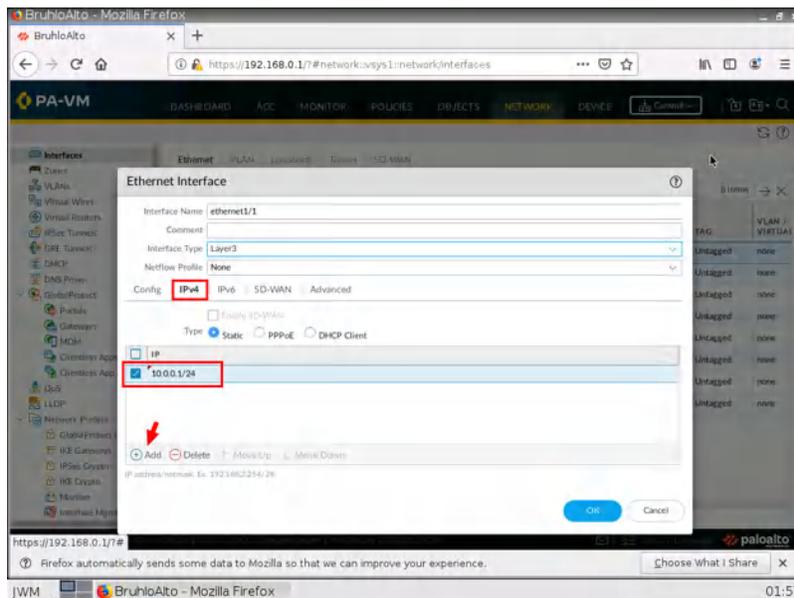


Figure 1.27: Set an IP address for Ethernet 1/1

## 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**.

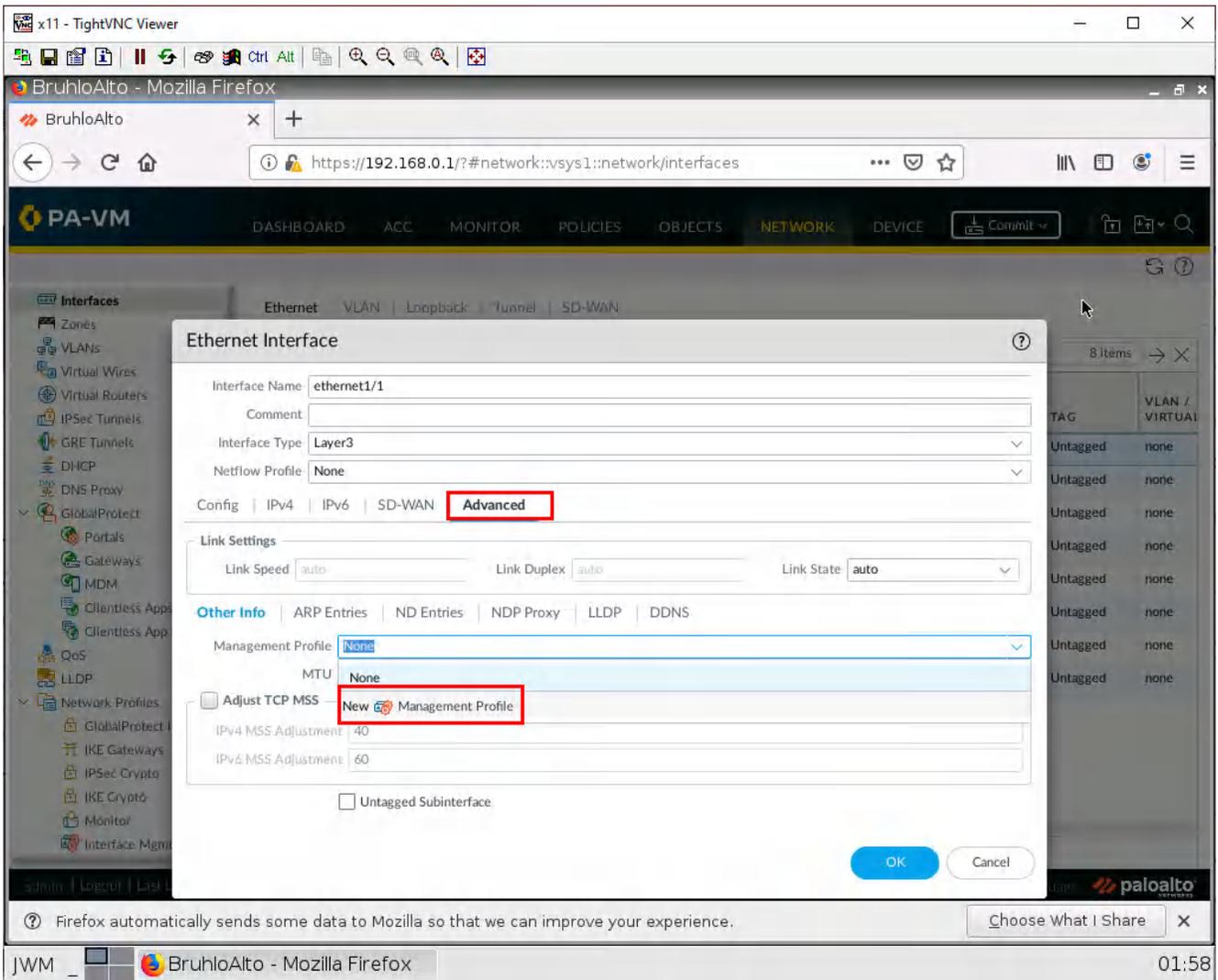


Figure 1.28: Ethernet 1/1 configuration – Advanced Tab

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

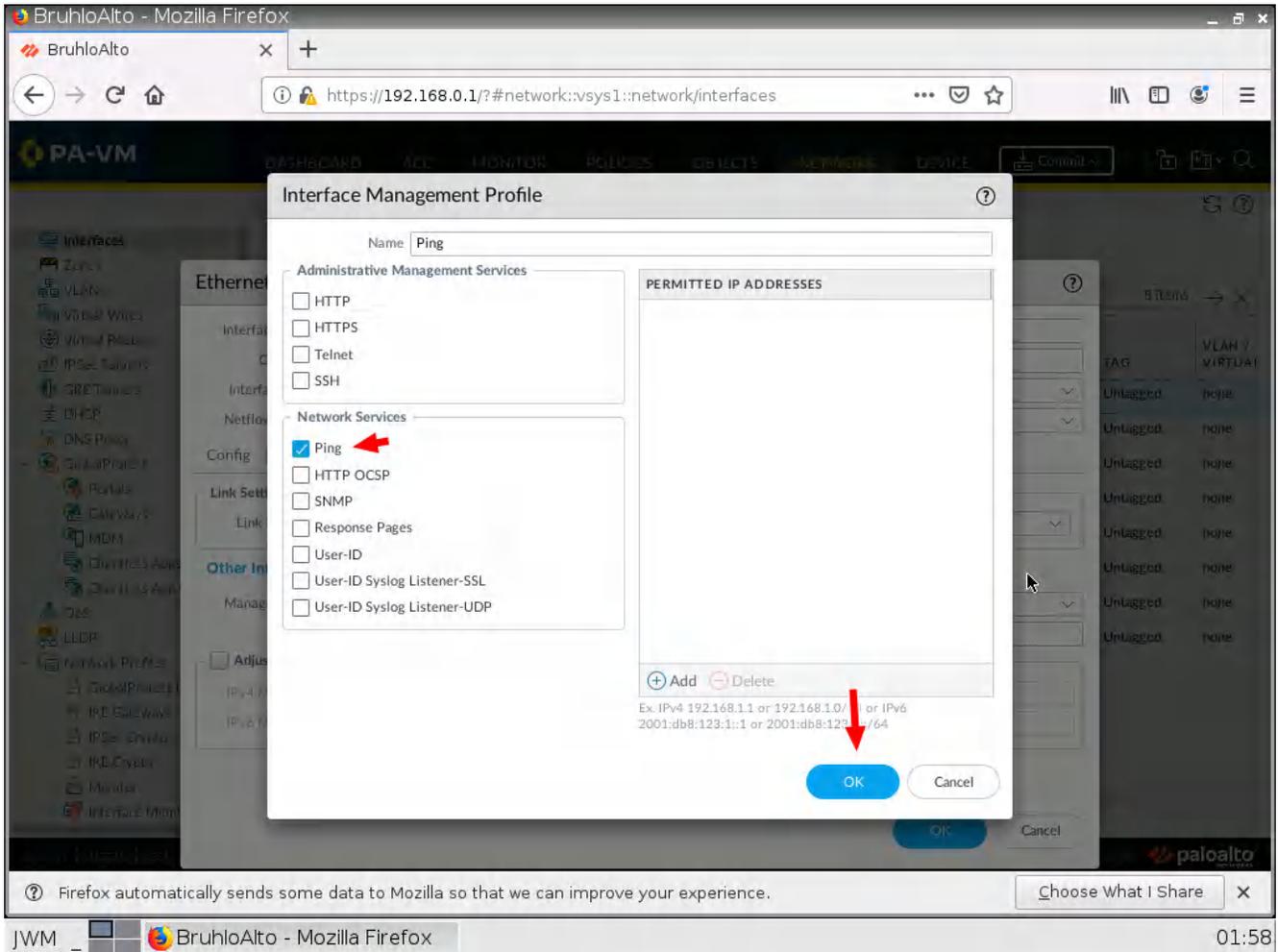


Figure 1.29: Enable Ping under Interface Management Profile

## 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.

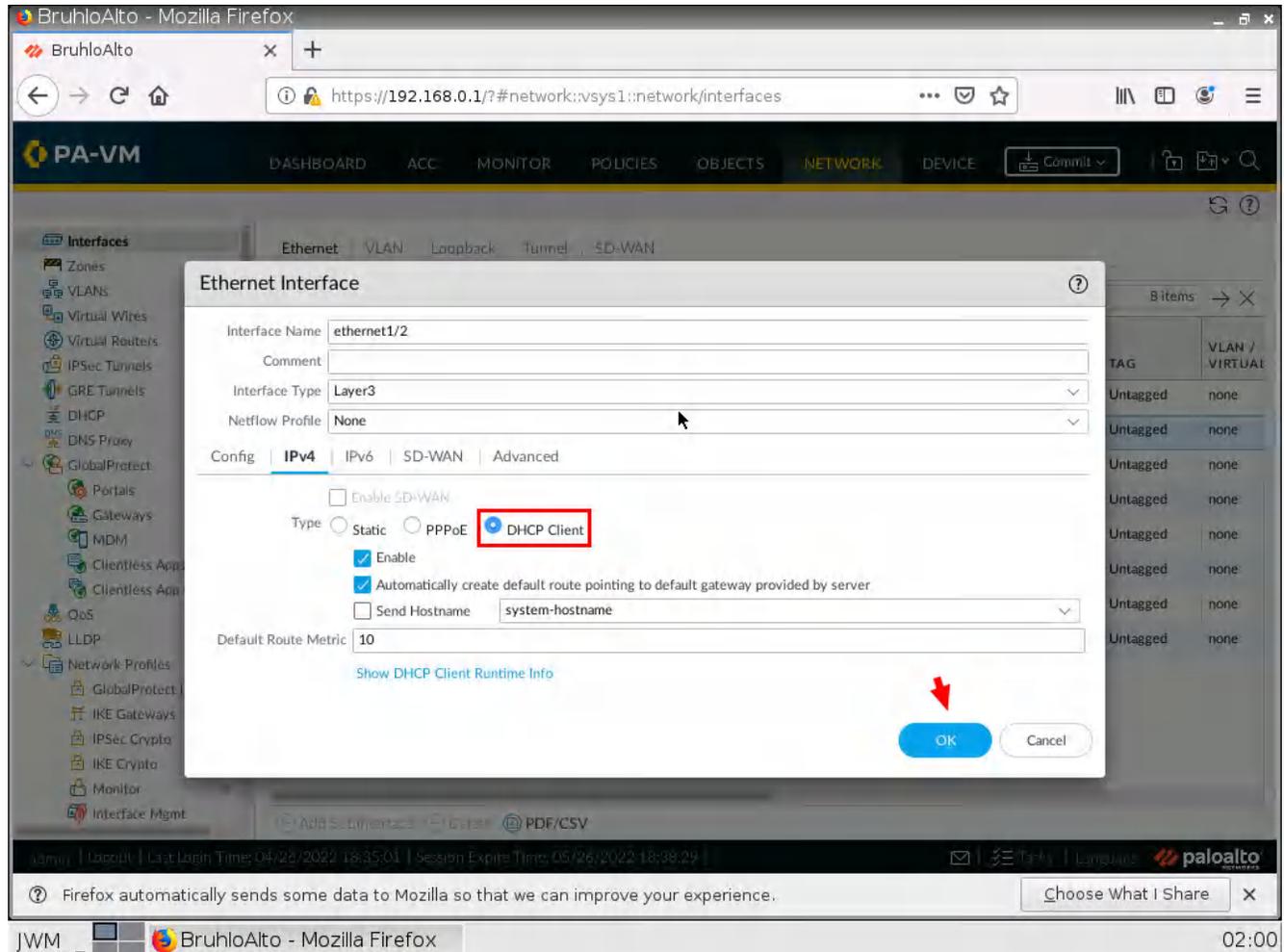


Figure 1.30: Enable DHCP Client on Ethernet 1/2

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.

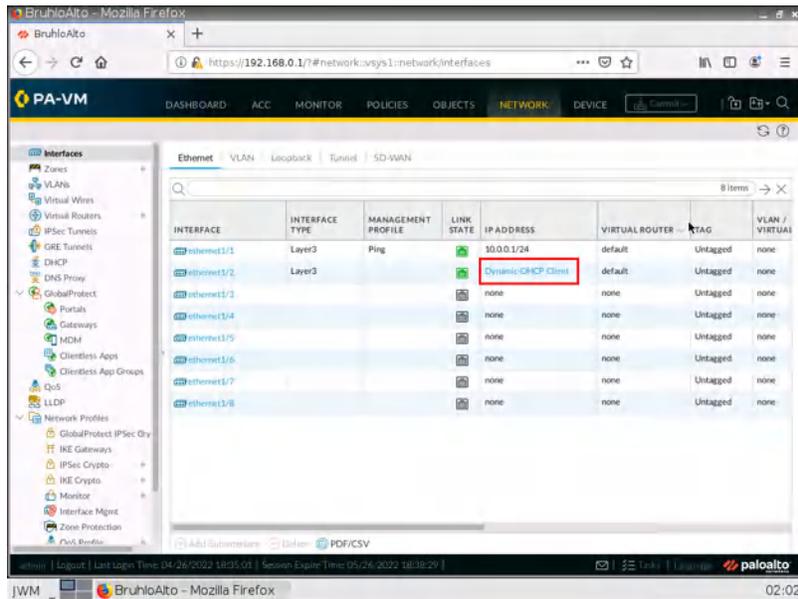


Figure 1.31: Dynamic DHCP Client- Receive an IP address from DHCP Server

Here is an example of that:

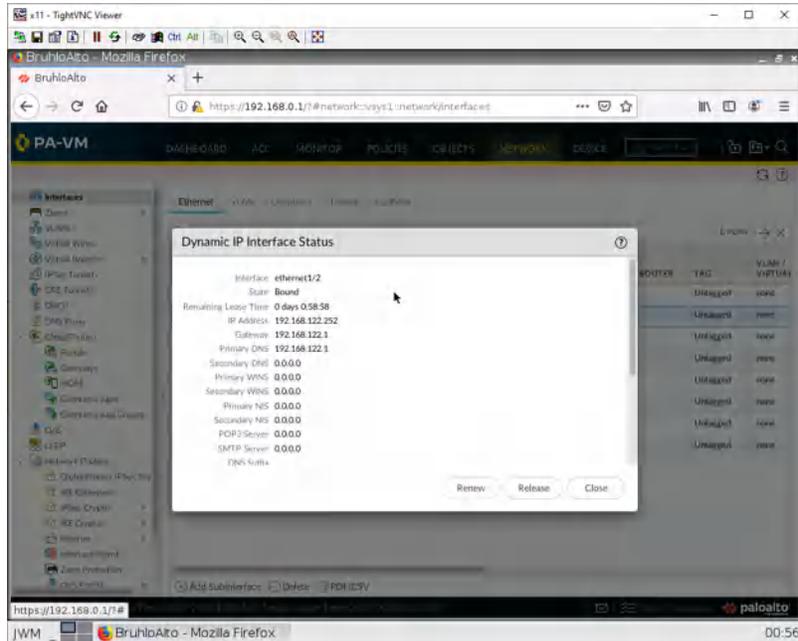


Figure 1.32: IP Address of Interface 1/2

## Set Up a DHCP Server in Palo Alto

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

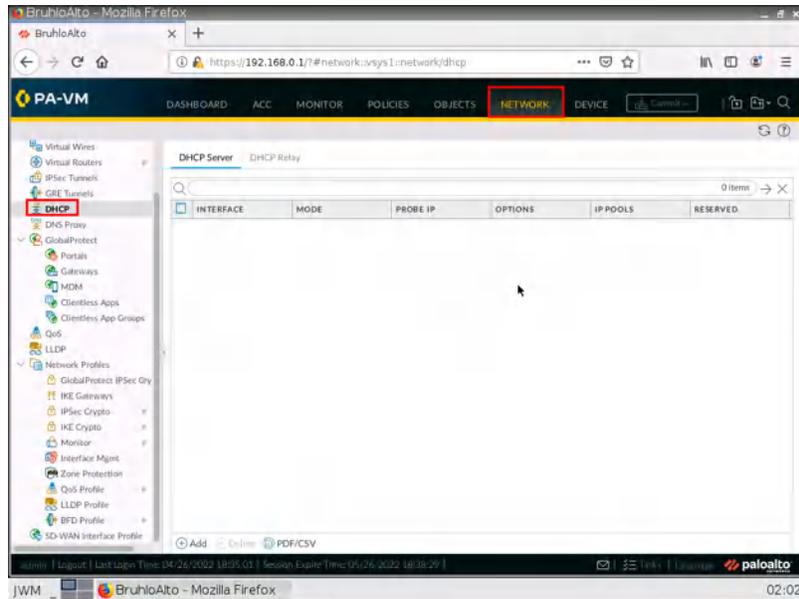


Figure 1.33: Add a DHCP Server

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.

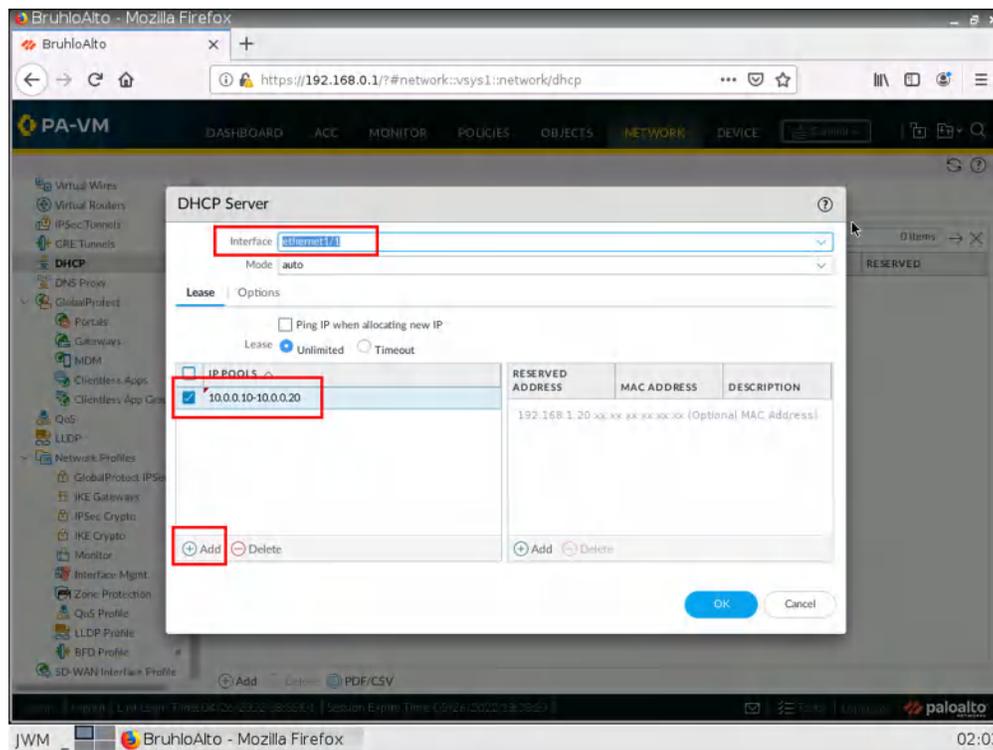


Figure 1.34: Set an IP Pools for Interface 1/1

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.

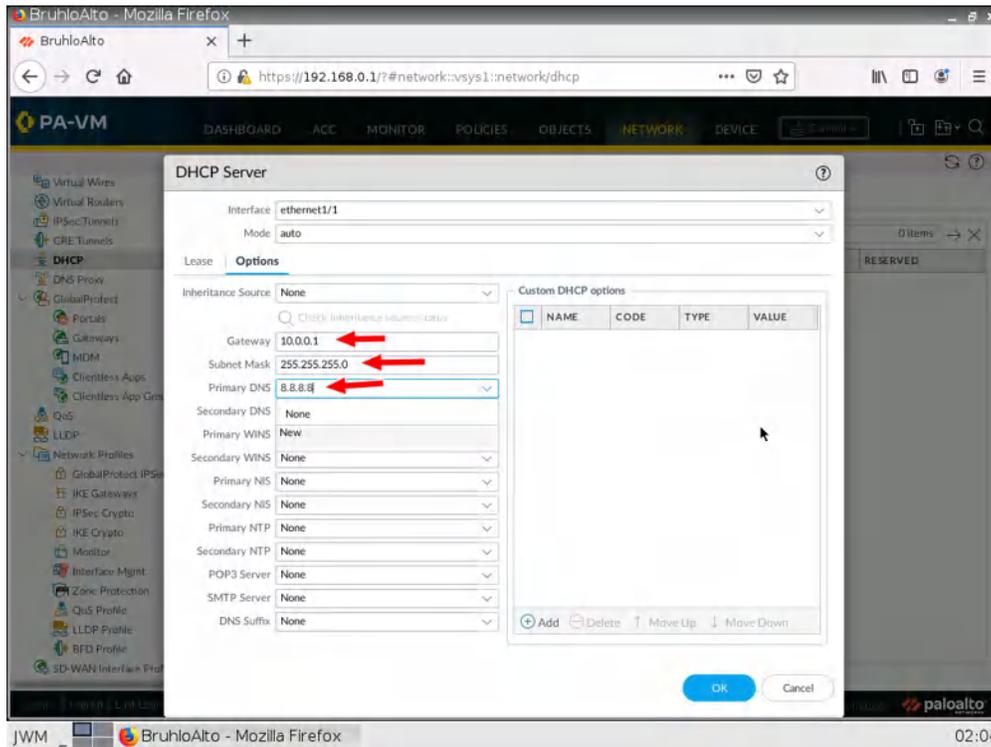


Figure 1.35: Set a Gateway and a primary DNS

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.

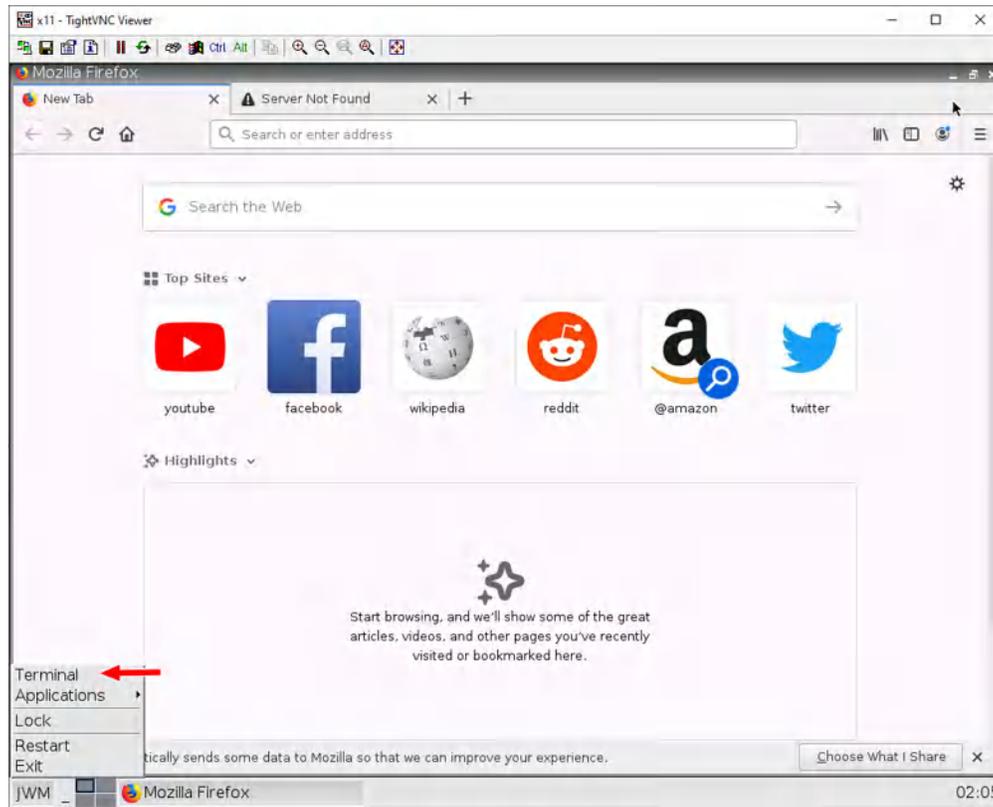


Figure 1.36: Open Terminal in WebTerm1

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

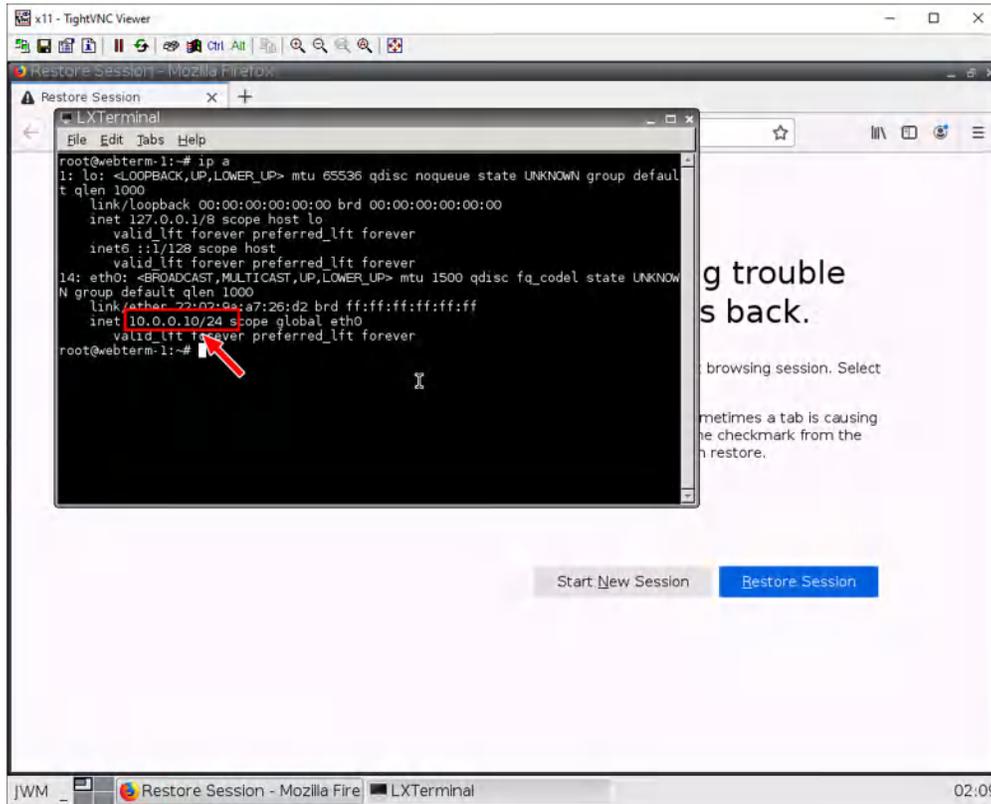


Figure 1.37: Check the IP address in Terminal

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

```

x11 - TightVNC Viewer
Restore Session - Mozilla Firefox
Restore Session
LX Terminal
File Edit Tabs Help
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
14: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
  link/ether 22:02:9a:a7:26:d2 brd ff:ff:ff:ff:ff:ff
  inet 10.0.0.10/24 scope global eth0
    valid_lft forever preferred_lft forever
root@webterm-1:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data:
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=3.66 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.843 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.756 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.727 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=0.703 ms
^C
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4052ms
rtt min/avg/max/mdev = 0.703/1.339/3.667/1.165 ms
root@webterm-1:~#

```

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.

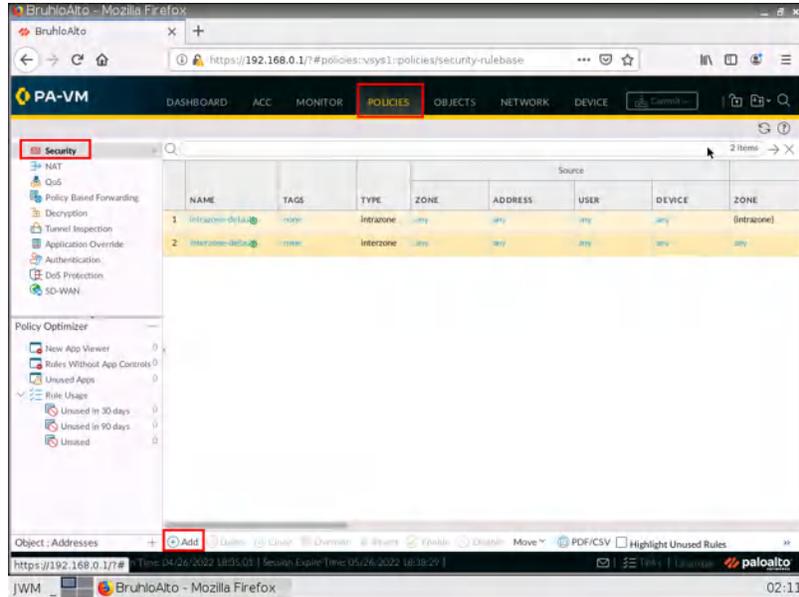


Figure 1.39: Add a Security Policy

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

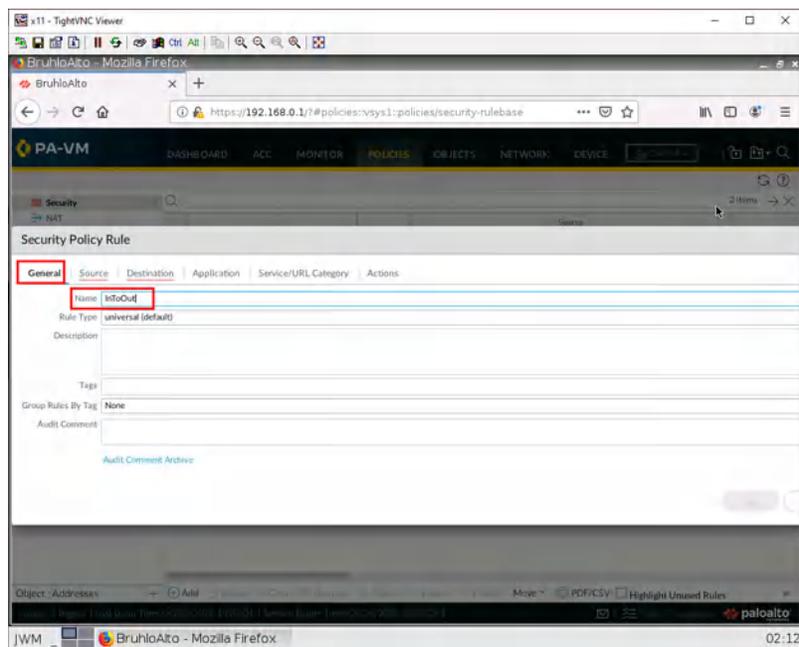


Figure 1.40: Set a Name for Security Policy

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

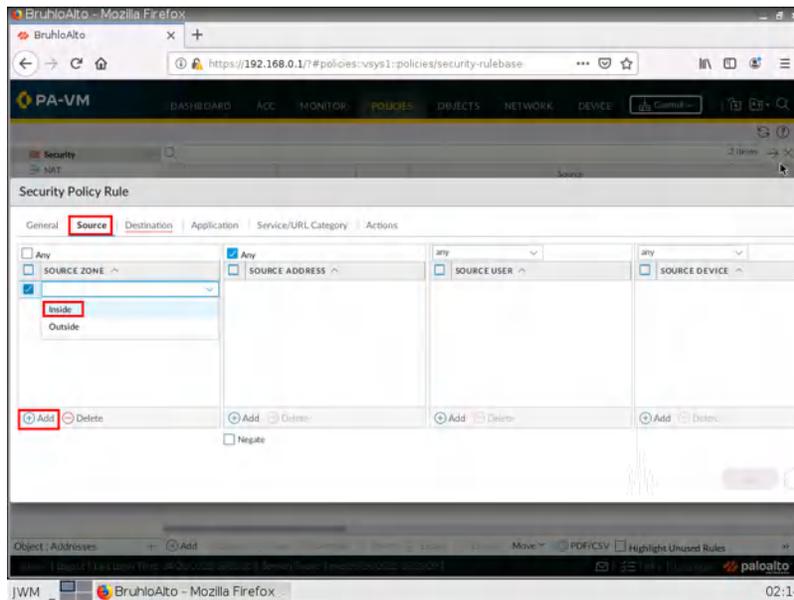


Figure 1.41: Set a Source Zone for Security Policy

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

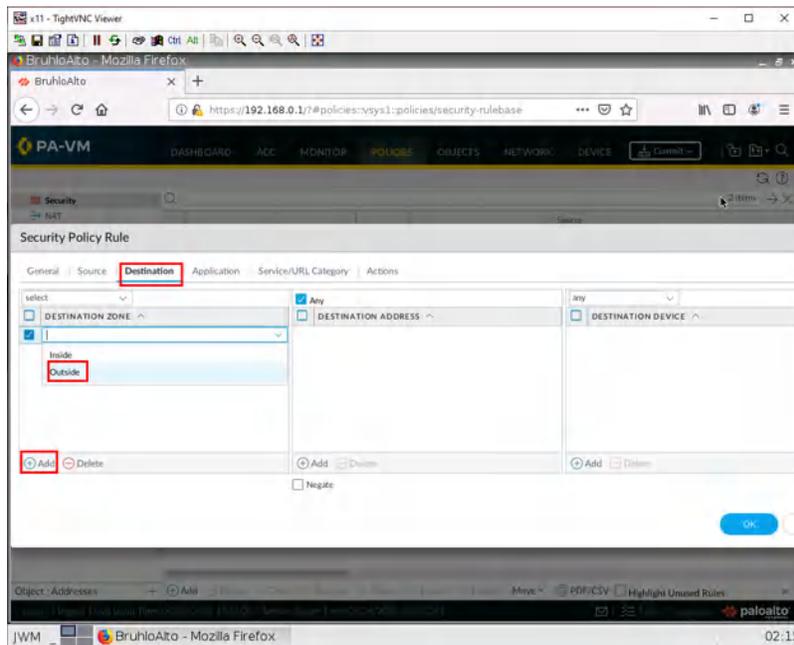


Figure 1.42: Set a Destination Zone for Security Policy

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

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

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

The screenshot shows the Palo Alto VM web interface. The left sidebar is expanded to the 'Security' section, where 'NAT' is highlighted with a red box. Below the sidebar, the 'Policy Optimizer' section shows 'Rule Usage' with three entries: 'Unused in 30 days' (0), 'Unused in 90 days' (0), and 'Unused' (0). The main content area is a table with the following columns: NAME, TAGS, SOURCE\_ZONE, DESTINATION\_ZONE, DESTINATION\_INTERFACE, SOURCE\_ADDRESS, and DESTINATION\_ADDRESS. The table is currently empty. At the bottom of the page, the 'Add' button is highlighted with a red box. The bottom status bar shows 'Object : Addresses' and 'Add' button. The bottom right corner shows '02:16'.

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.

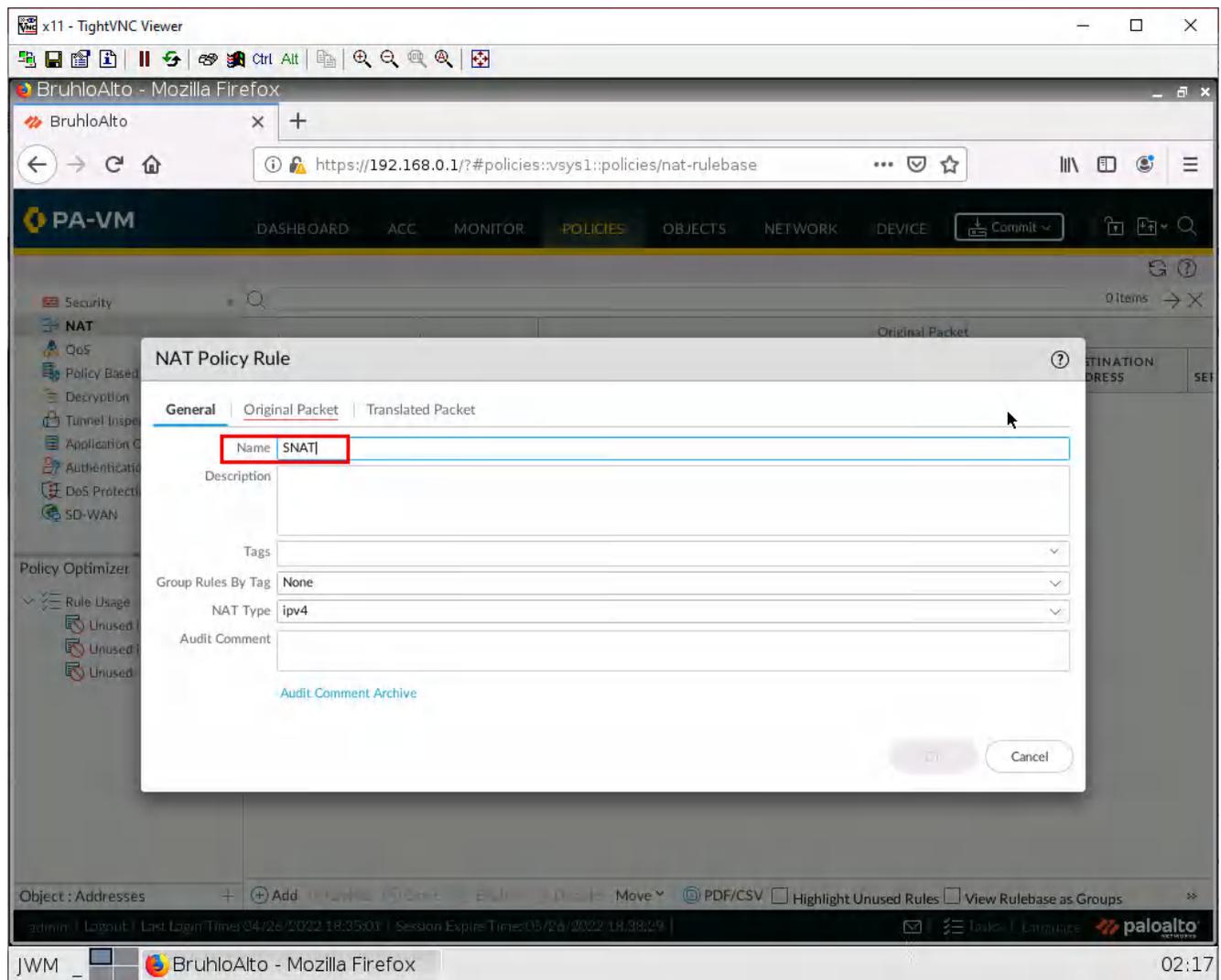


Figure 1.44: Set a Name for NAT

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

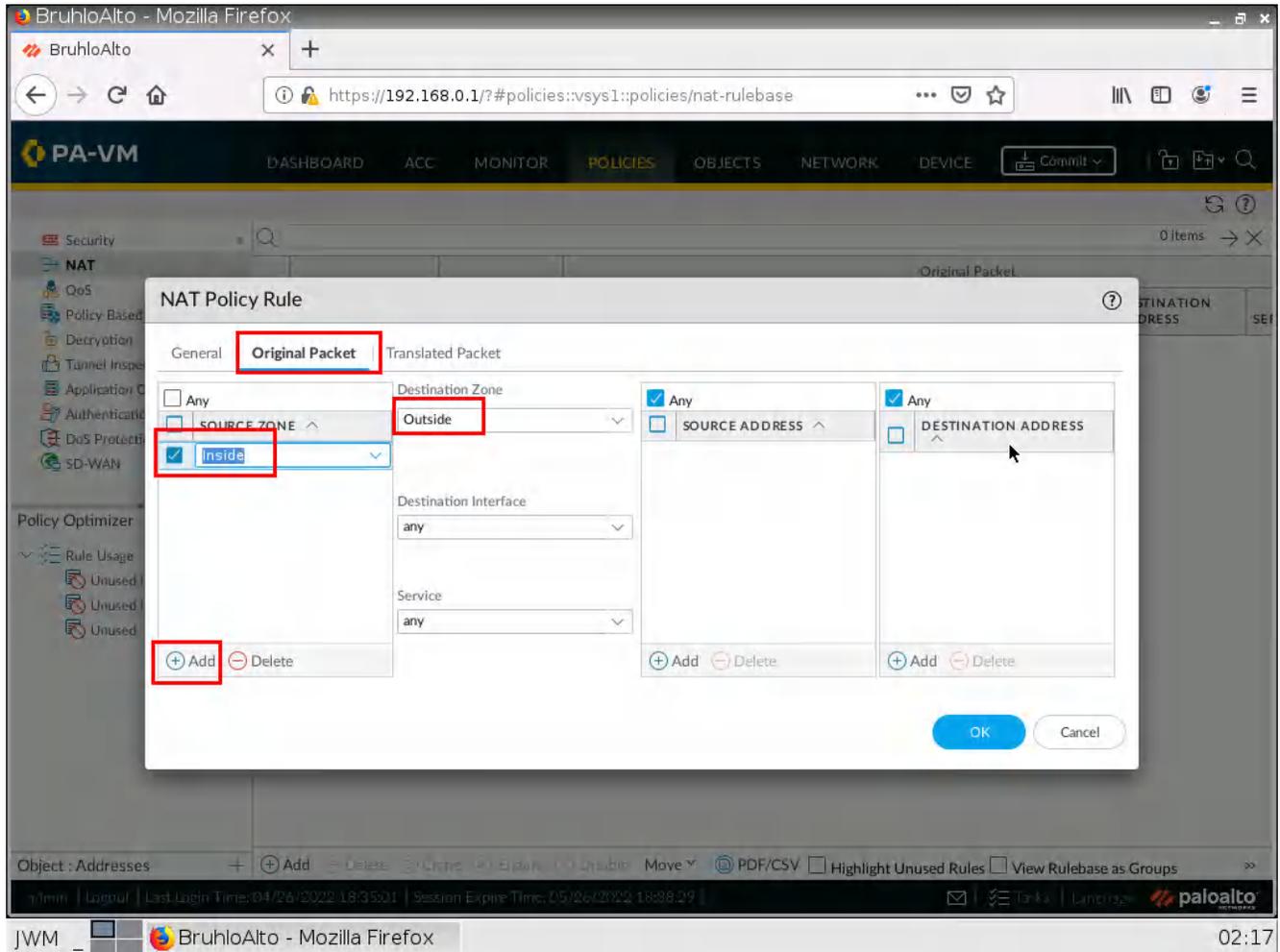


Figure 1.45: Set a Source Zone and Destination Zone for NAT

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**.

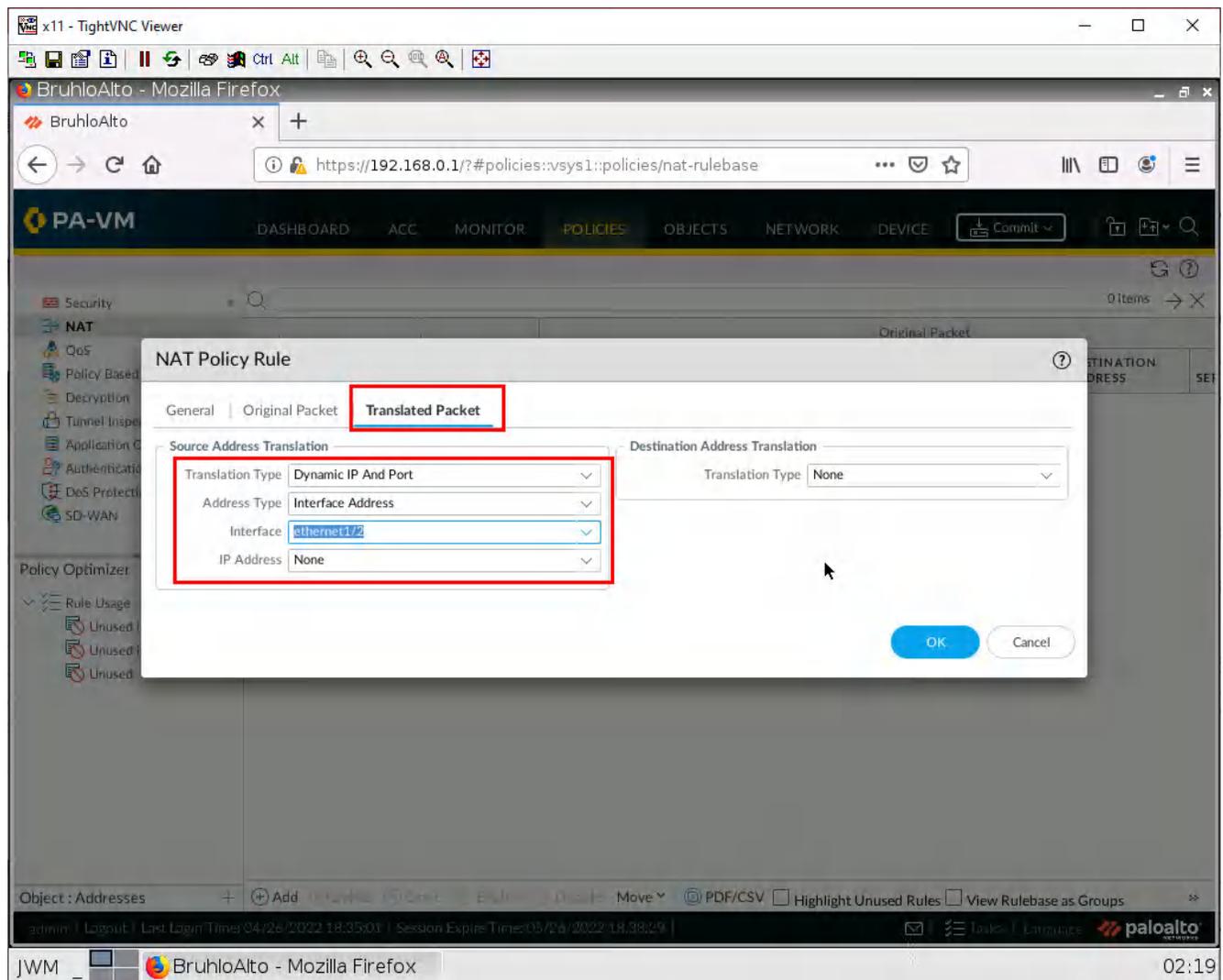
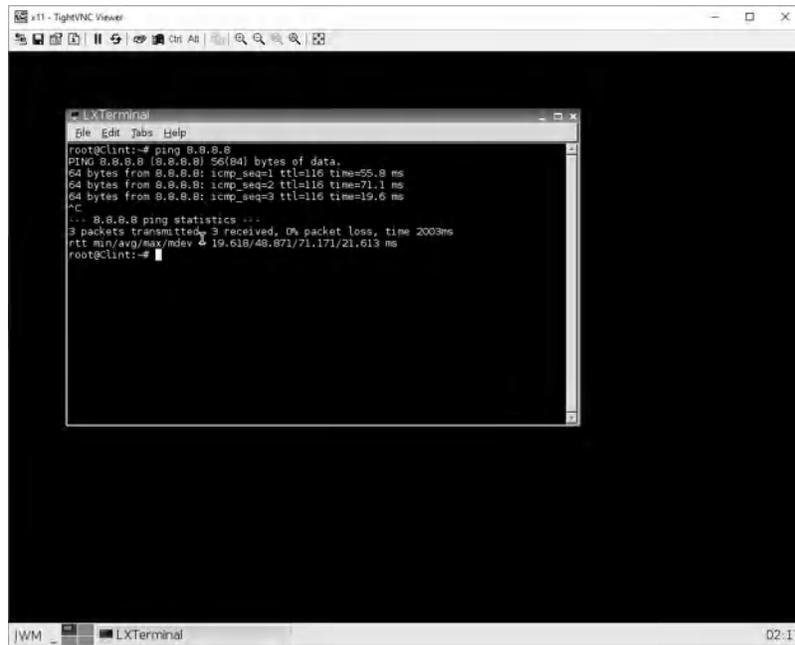


Figure 1.46: Set a Translated Packet

Don't forget to commit!

## Check Internet Connectivity on Webterm

In webterm, you could test pinging 8.8.8.8 like so:



```

x11 - TightVNC Viewer
file Edit Jobs Help
root@clint:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=55.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=71.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=19.6 ms
^C
... 8.8.8.8 ping statistics ...
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 19.618/48.871/71.171/21.613 ms
root@clint:~#
  
```

Figure 1.47: Verify your configuration

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

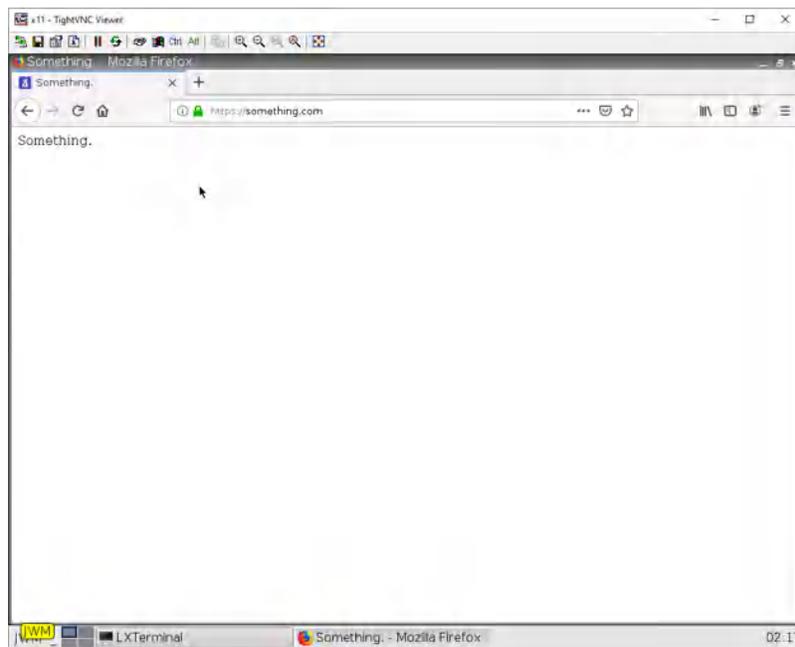


Figure 1.48: Verify your connectivity to the Internet

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



## 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!

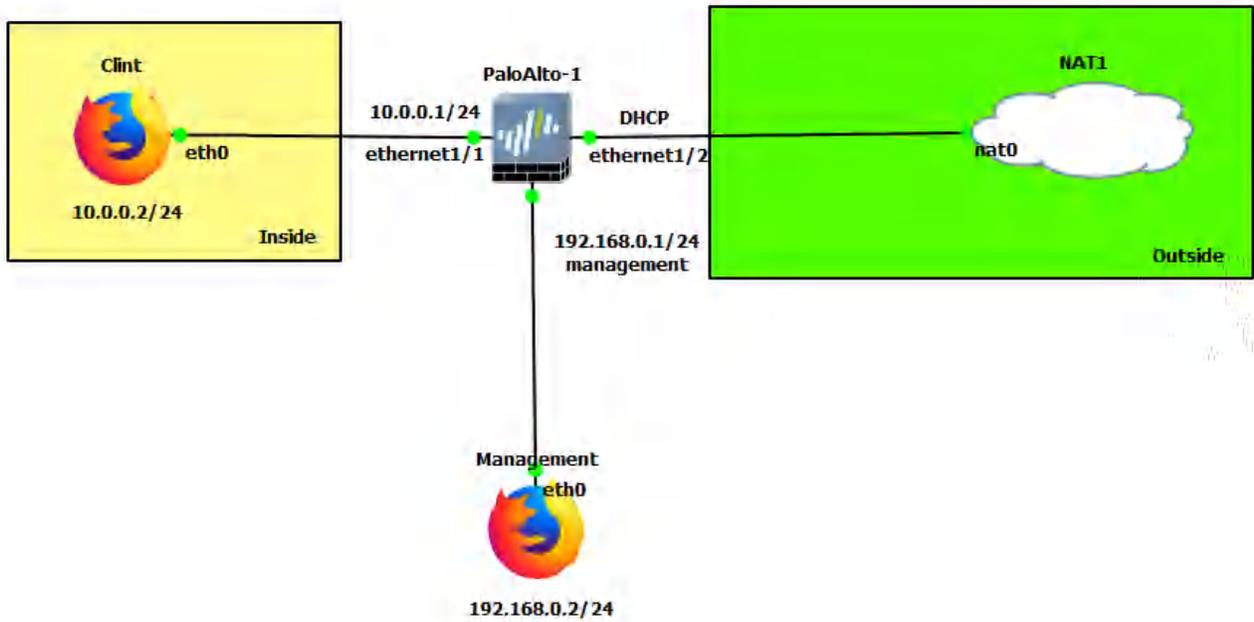


Figure 1.49: Main Scenario

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)

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

The screenshot shows the Palo Alto VM web interface. The left sidebar has a 'Security' menu with 'NAT' highlighted in red. The main content area displays a table with one rule named 'SNAT'. The table has columns for NAME, TAGS, SOURCE\_ZONE, DESTINATION\_ZONE, DESTINATION\_INTERFACE, SOURCE\_ADDRESS, and DESTINATION\_ADDRESS. The rule 'SNAT' has a TAGS value of 'none', SOURCE\_ZONE of 'Inside', DESTINATION\_ZONE of 'Outside', and DESTINATION\_INTERFACE of 'any'. The SOURCE\_ADDRESS and DESTINATION\_ADDRESS are both 'any'. The table is titled 'Original Packet'.

	NAME	TAGS	SOURCE_ZONE	DESTINATION_ZONE	DESTINATION_INTERFACE	SOURCE_ADDRESS	DESTINATION_ADDRESS	SE
1	SNAT	none	Inside	Outside	any	any	any	any

At the bottom of the interface, the 'Add' button in the toolbar is highlighted in red. The toolbar also includes buttons for Delete, Clone, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, and View Rulebase as Groups.

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.

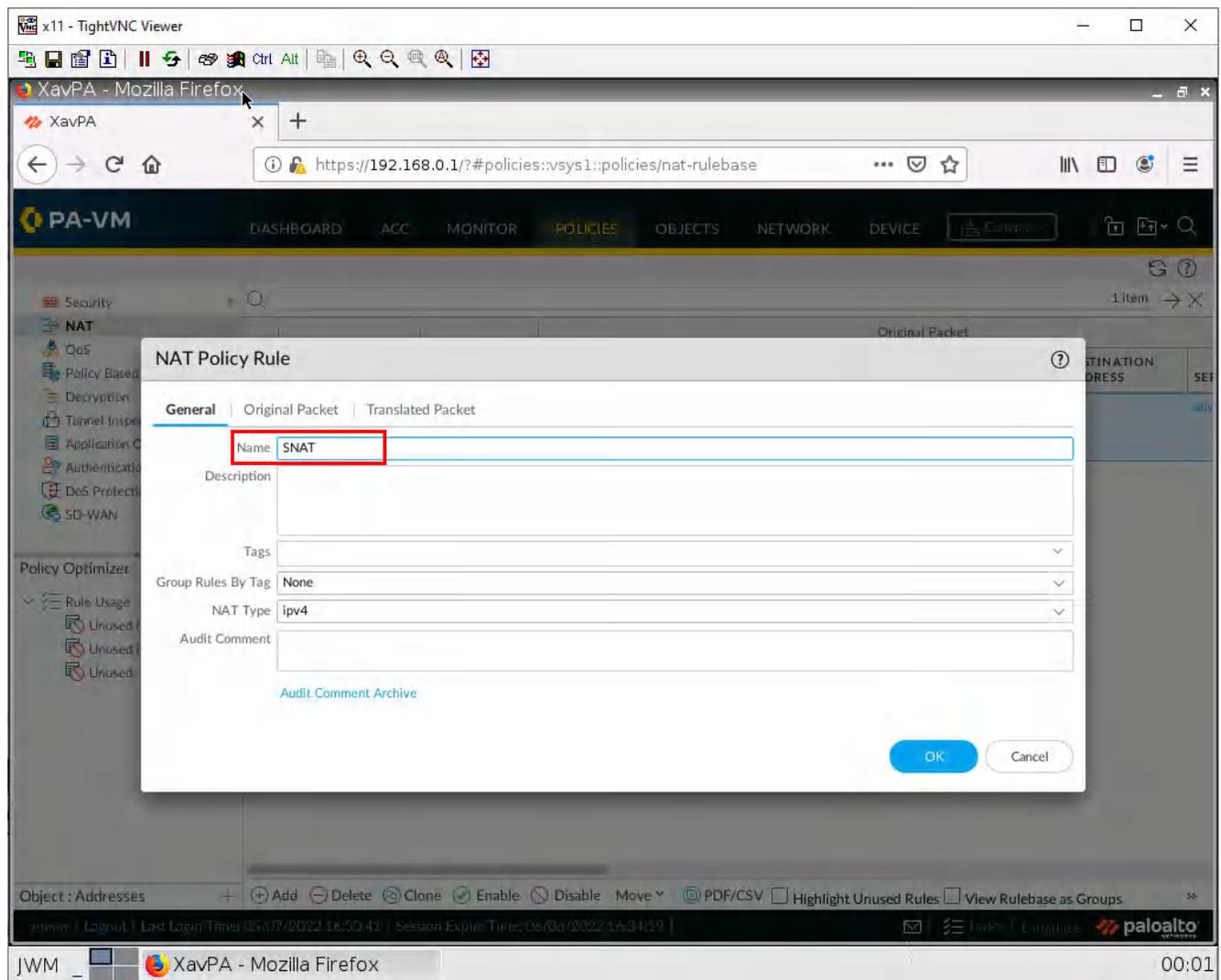


Figure 1.51: Set a Name for NAT

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

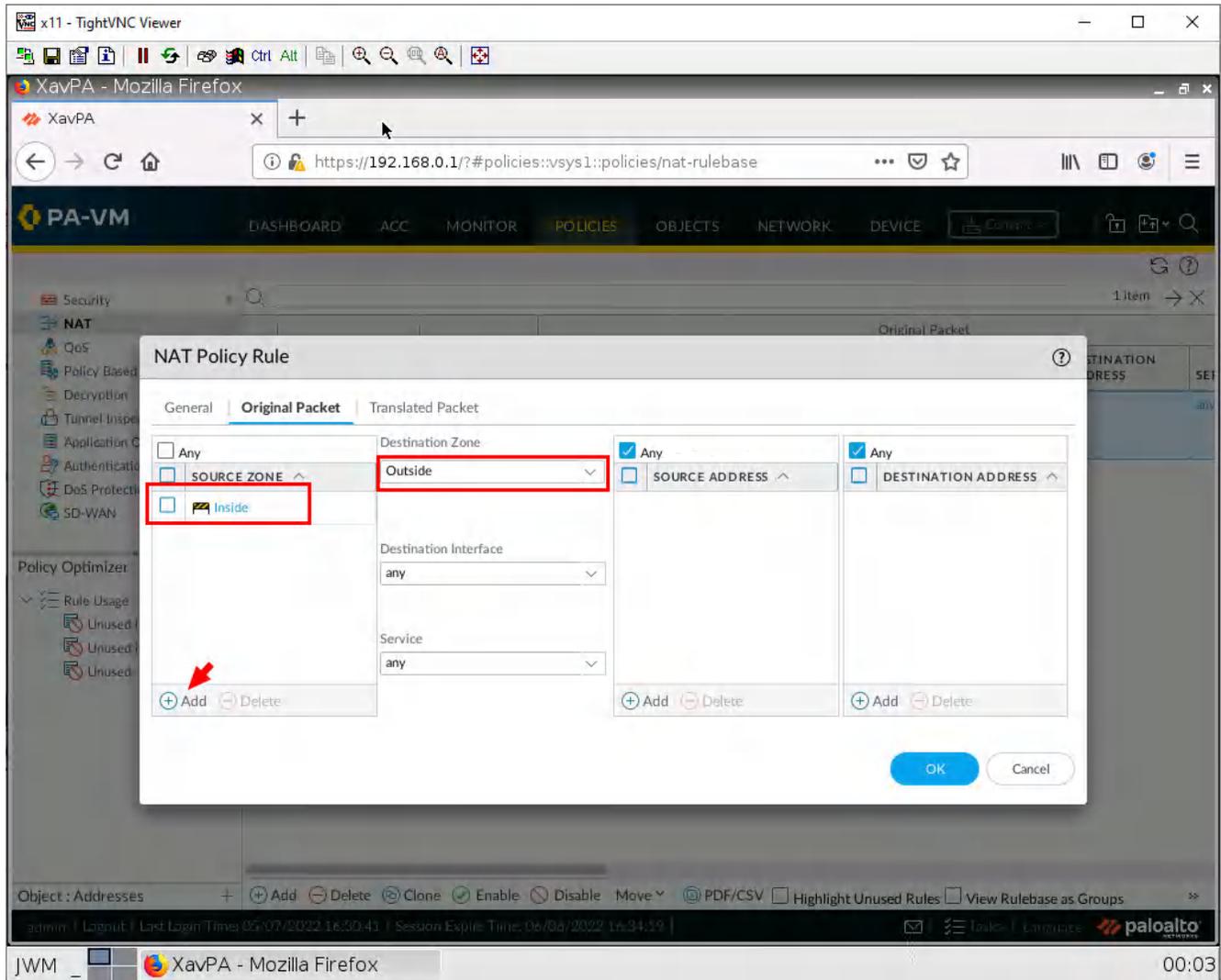


Figure 1.52: Set a Source Zone and Destination Zone for NAT

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

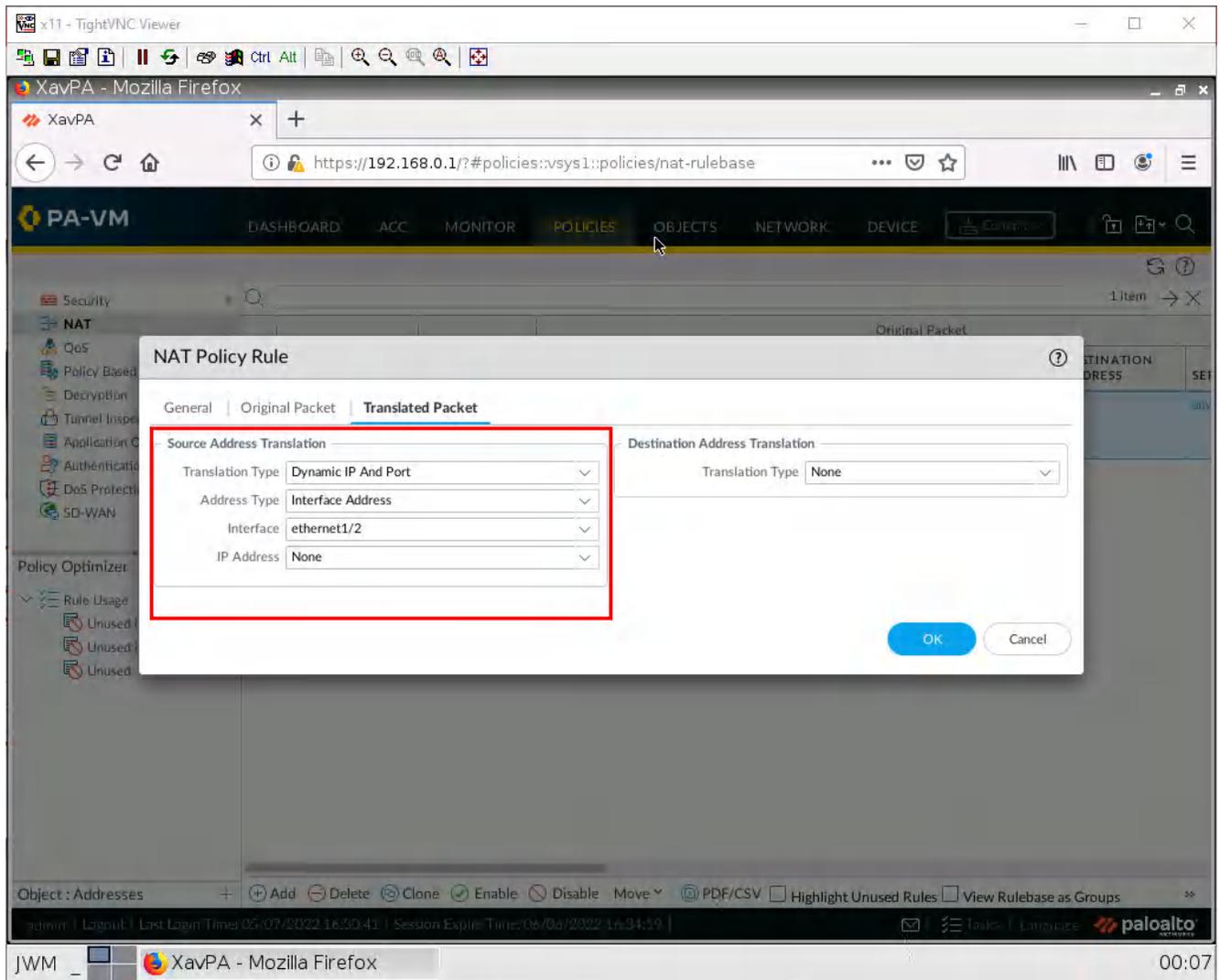


Figure 1.53: Set a Translated Packet

Don't forget to commit!

## Check Internet Connectivity on Webterm

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

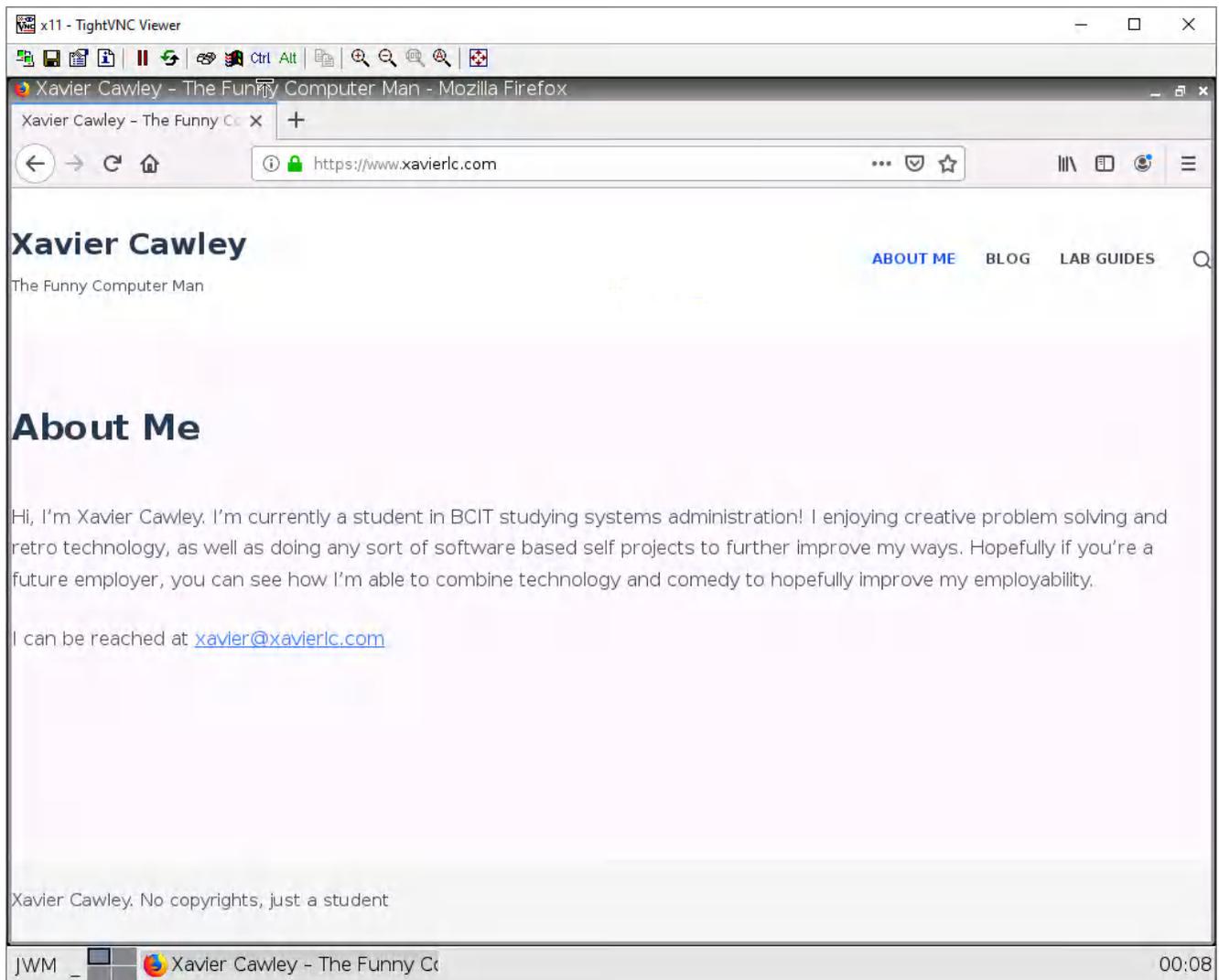


Figure 1.54: Verify your connectivity to the Internet

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



## 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.

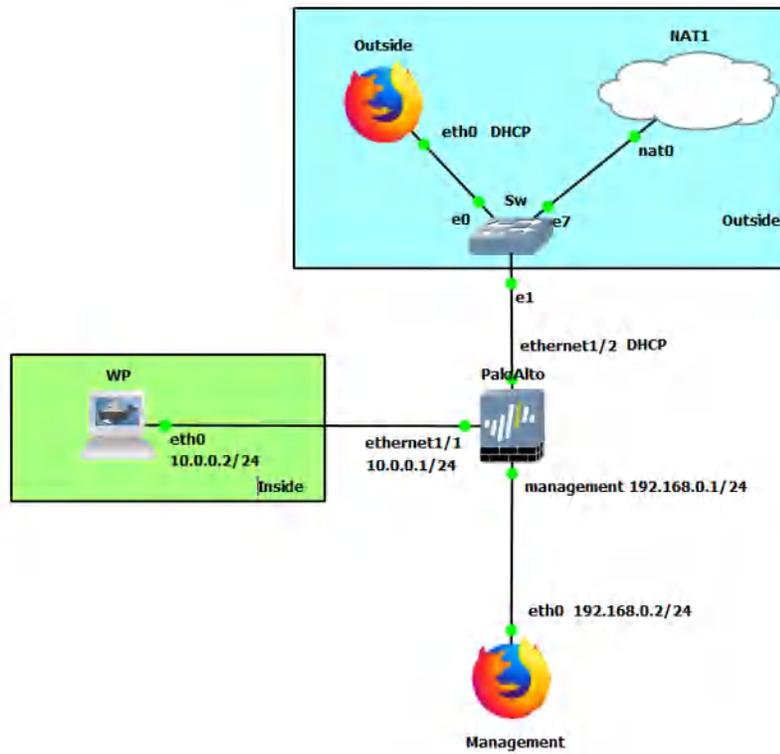


Figure 1.55: Main scenario

Table 1.7: Addressing Table

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**.

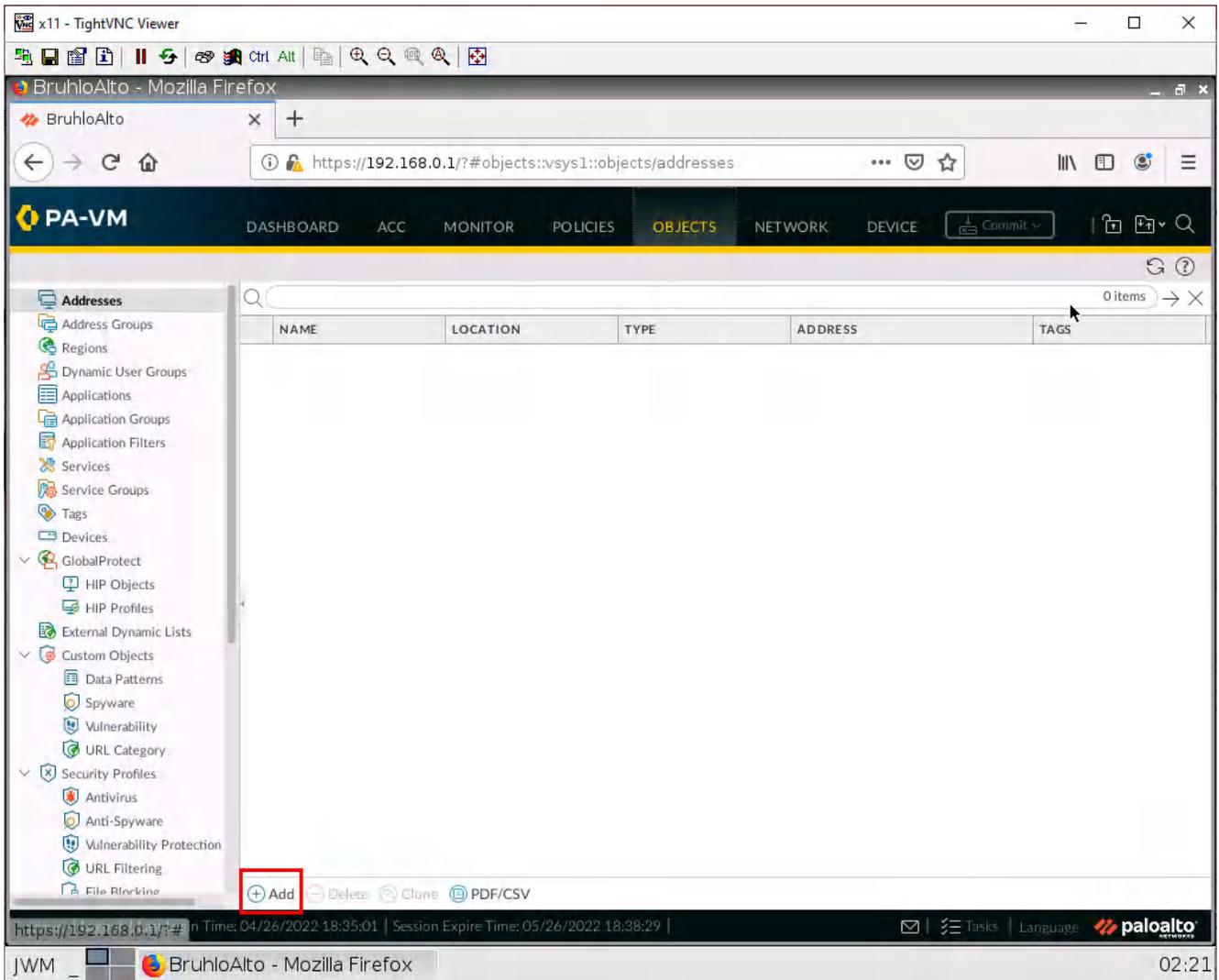


Figure 1.56: Add an address

In this window, we will add the IP of the WordPress server to reference it easier.

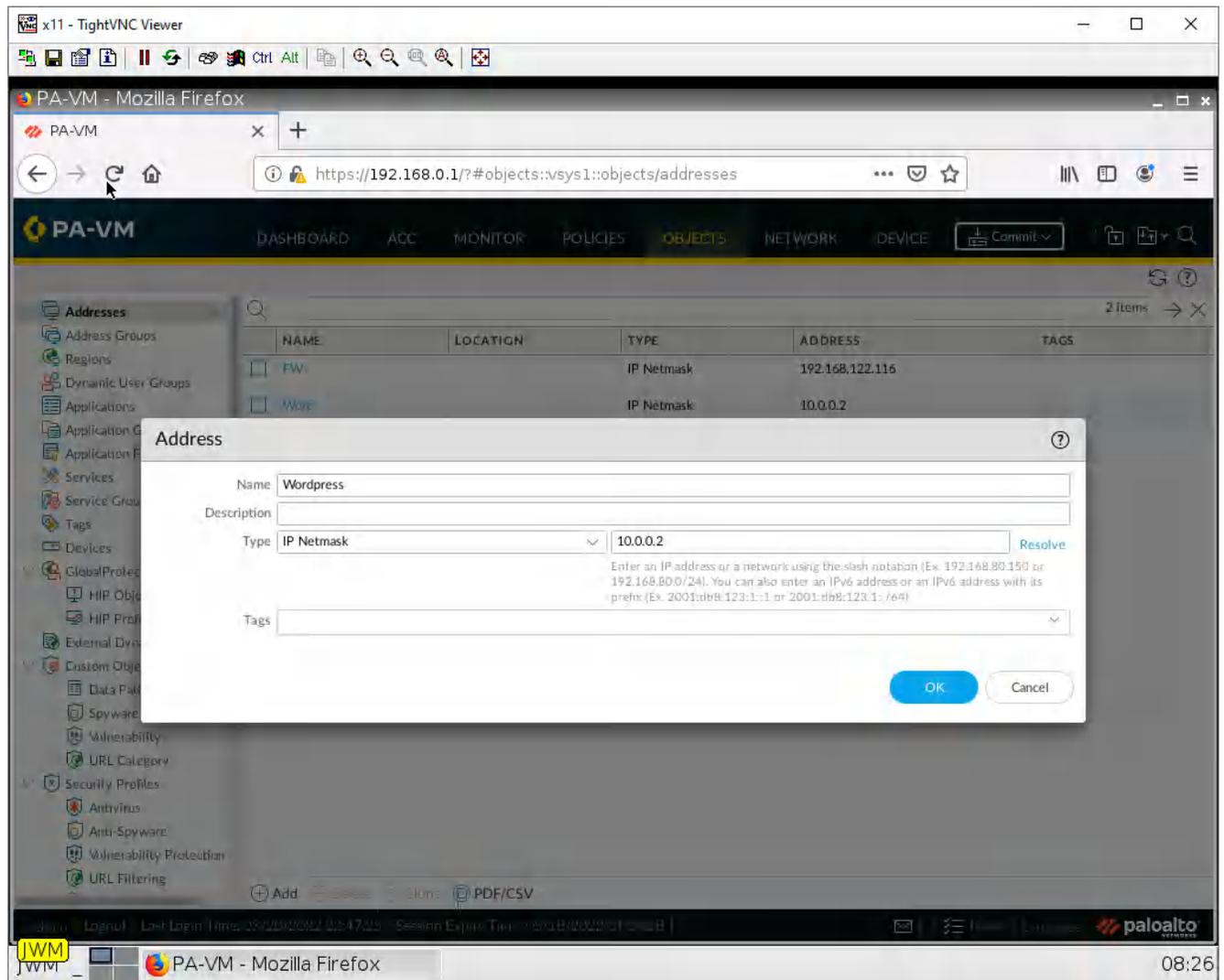


Figure 1.57: WordPress IP address

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:

The screenshot displays the PA-VM web interface in Mozilla Firefox. The browser address bar shows the URL `https://192.168.0.1/?#network:vsys1:network/interfaces`. The interface configuration page is titled "Ethernet" and shows a table of 8 interfaces. The "IP ADDRESS" column for the "ethernet1/2" interface is highlighted with a red box, indicating a link to "Dynamic-DHCP Client".

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL
ethernet1/1	Layer3	Ping		10.0.0.1/24	default	Untagged	none
ethernet1/2	Layer3			<a href="#">Dynamic-DHCP Client</a>	default	Untagged	none
ethernet1/3				none	none	Untagged	none
ethernet1/4				none	none	Untagged	none
ethernet1/5				none	none	Untagged	none
ethernet1/6				none	none	Untagged	none
ethernet1/7				none	none	Untagged	none
ethernet1/8				none	none	Untagged	none

Figure 1.58: Dynamic-DHCP Client IP address

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

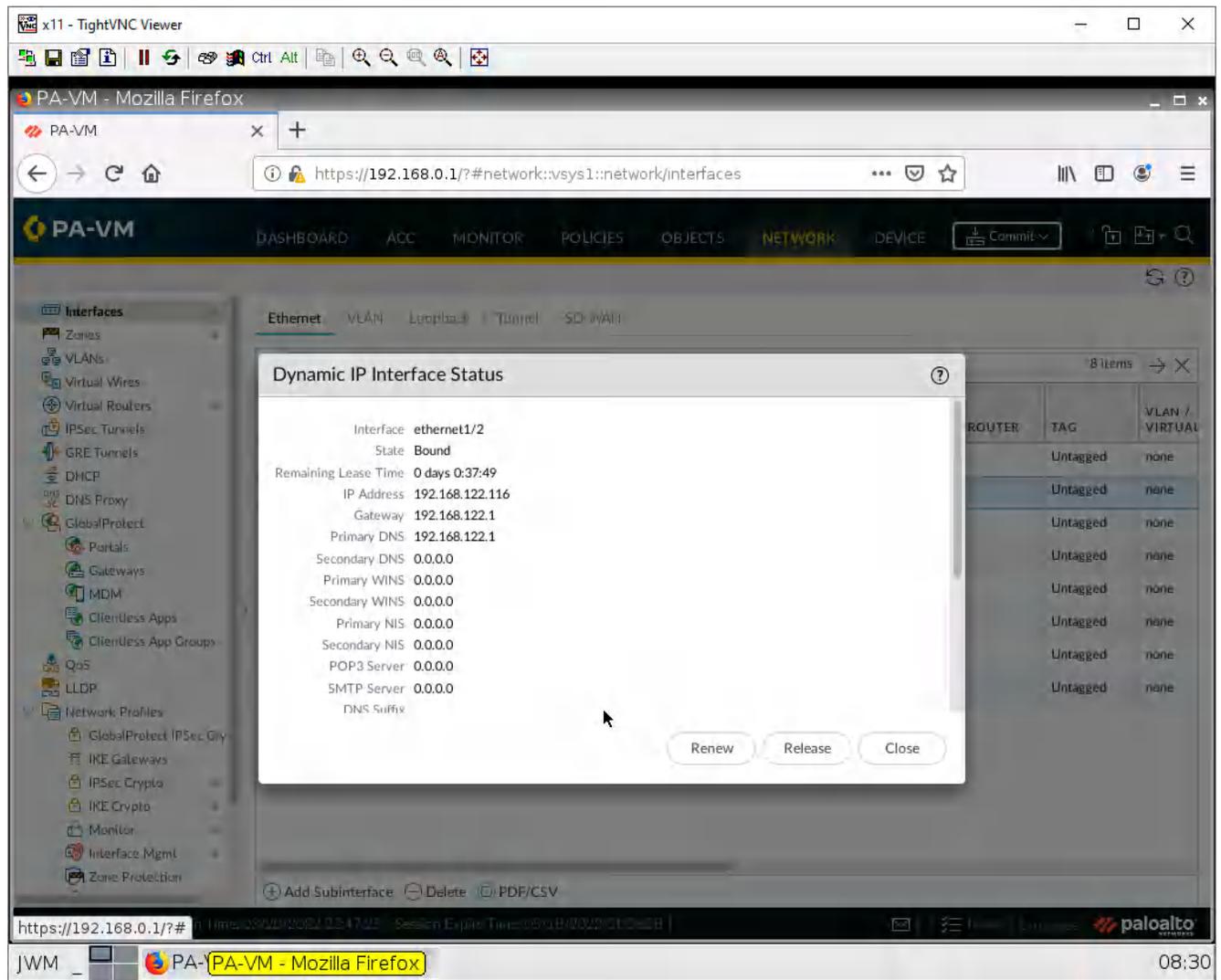


Figure 1.59: Verify Dynamic-DHCP Client IP address

## Create a DNAT Policy

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

The screenshot shows the PA-VM web interface in Mozilla Firefox. The URL is <https://192.168.0.1/?#policies::vsys1::policies/nat-rulebase>. The interface displays the NAT policy configuration page with the 'Original Packet' tab selected. A table lists the policy details:

NAME	TAGS	Original Packet					
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SE...
1 SNAT	none	Inside	Outside	any	any	any	any

At the bottom of the interface, the 'Add' button is highlighted with a red box. Other buttons include Delete, Clone, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, and View Rulebase as Groups. The bottom status bar shows the user 'admin', last login time, session expire time, and the Palo Alto logo.

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)

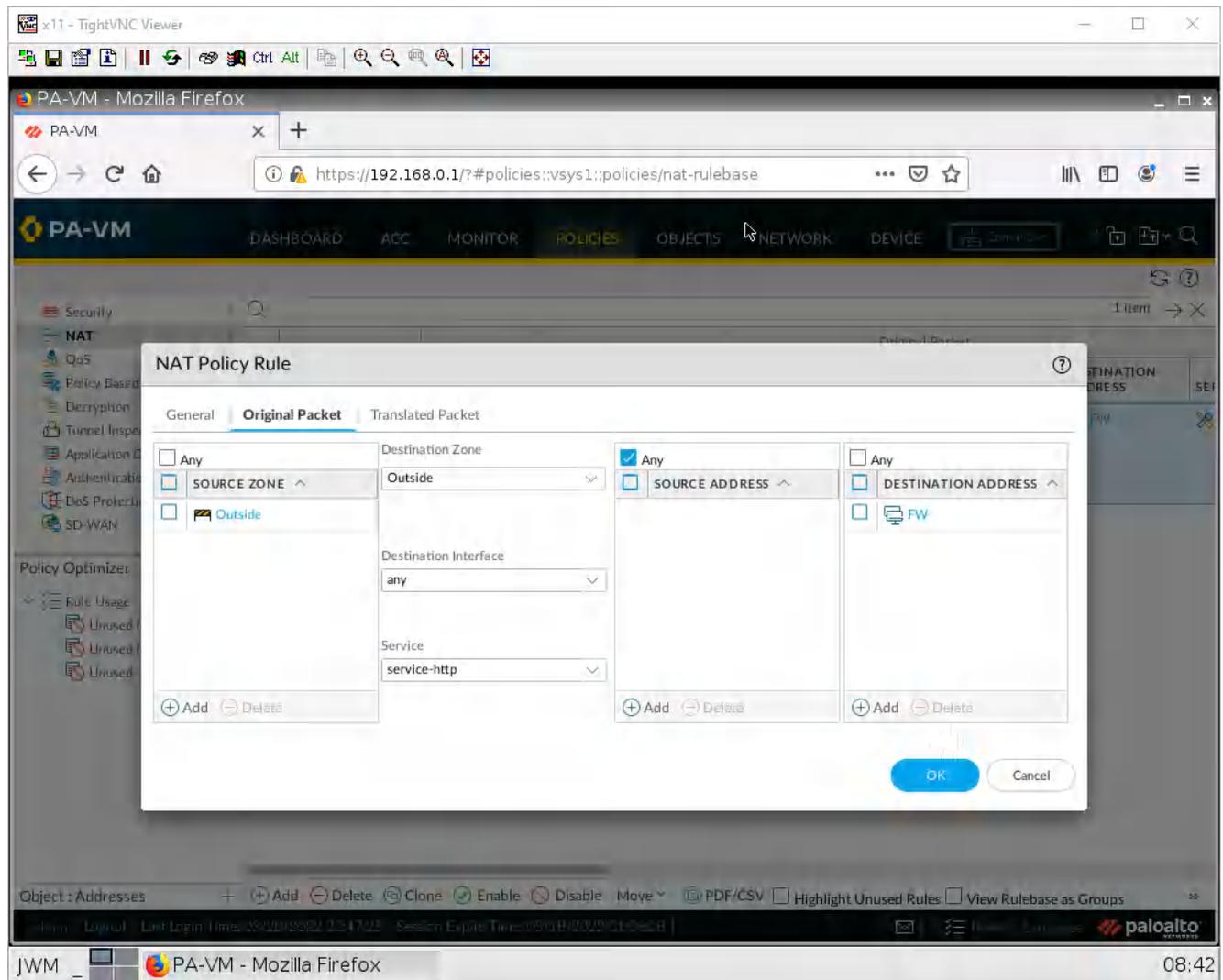
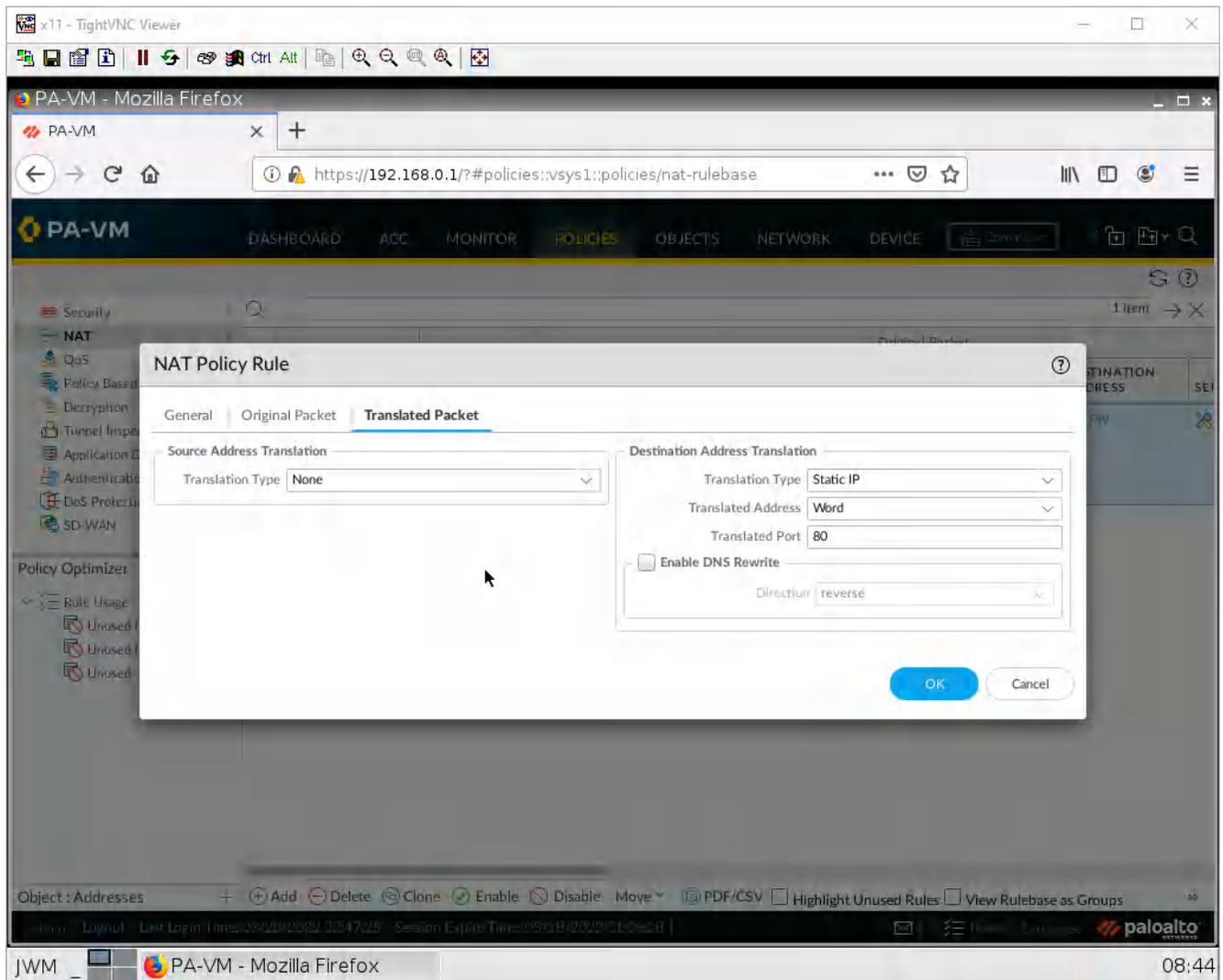


Figure 1.61: DNAT Policy Rule- Original Packet

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

**Table 1.10: DNAT Translated Packet Configuration**

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



*Figure 1.62: DNAT Policy Rule- Translated Packet*

Then, press **OK**.

## Security Policy for DNAT

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

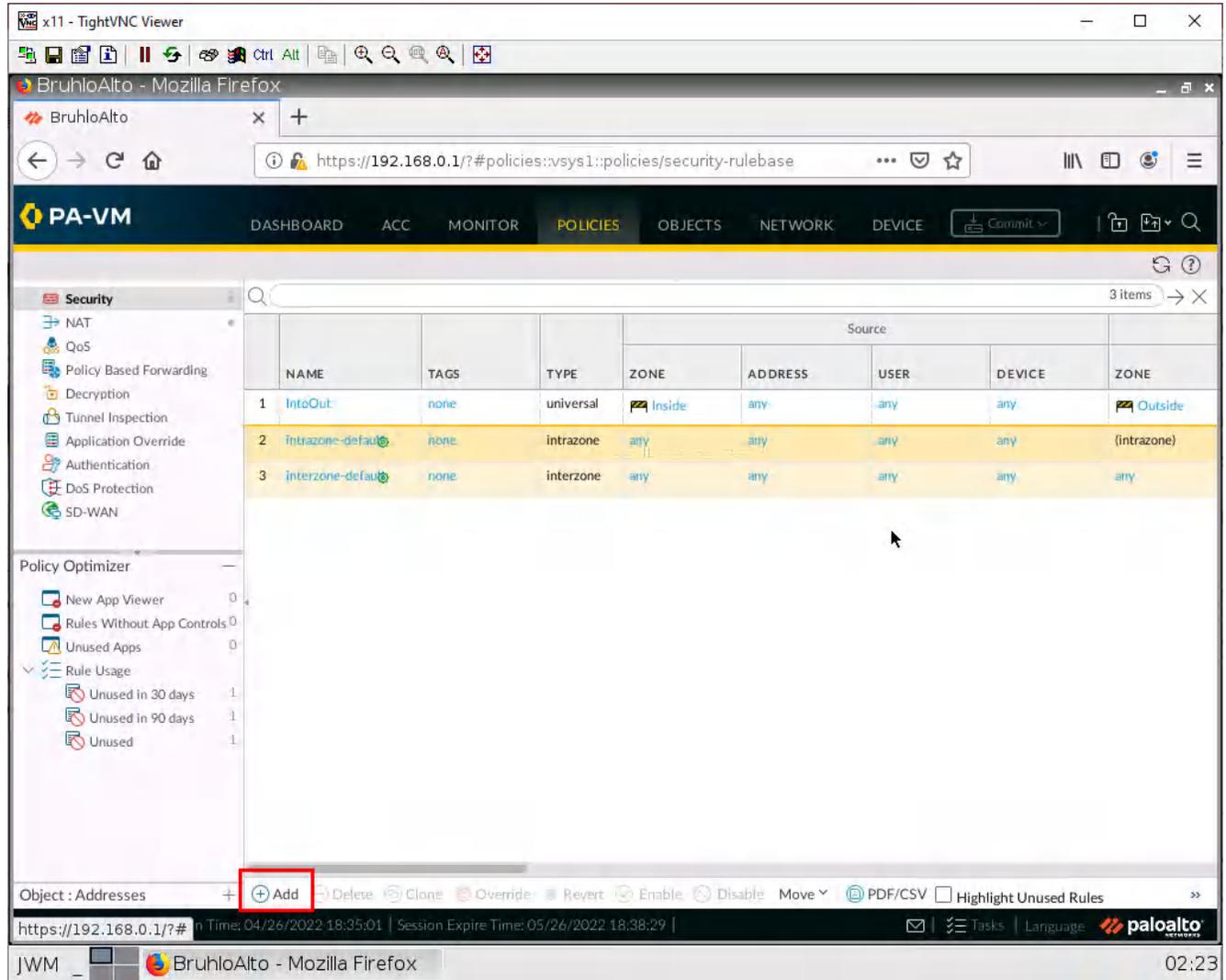


Figure 1.63: Add a Security Policy

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

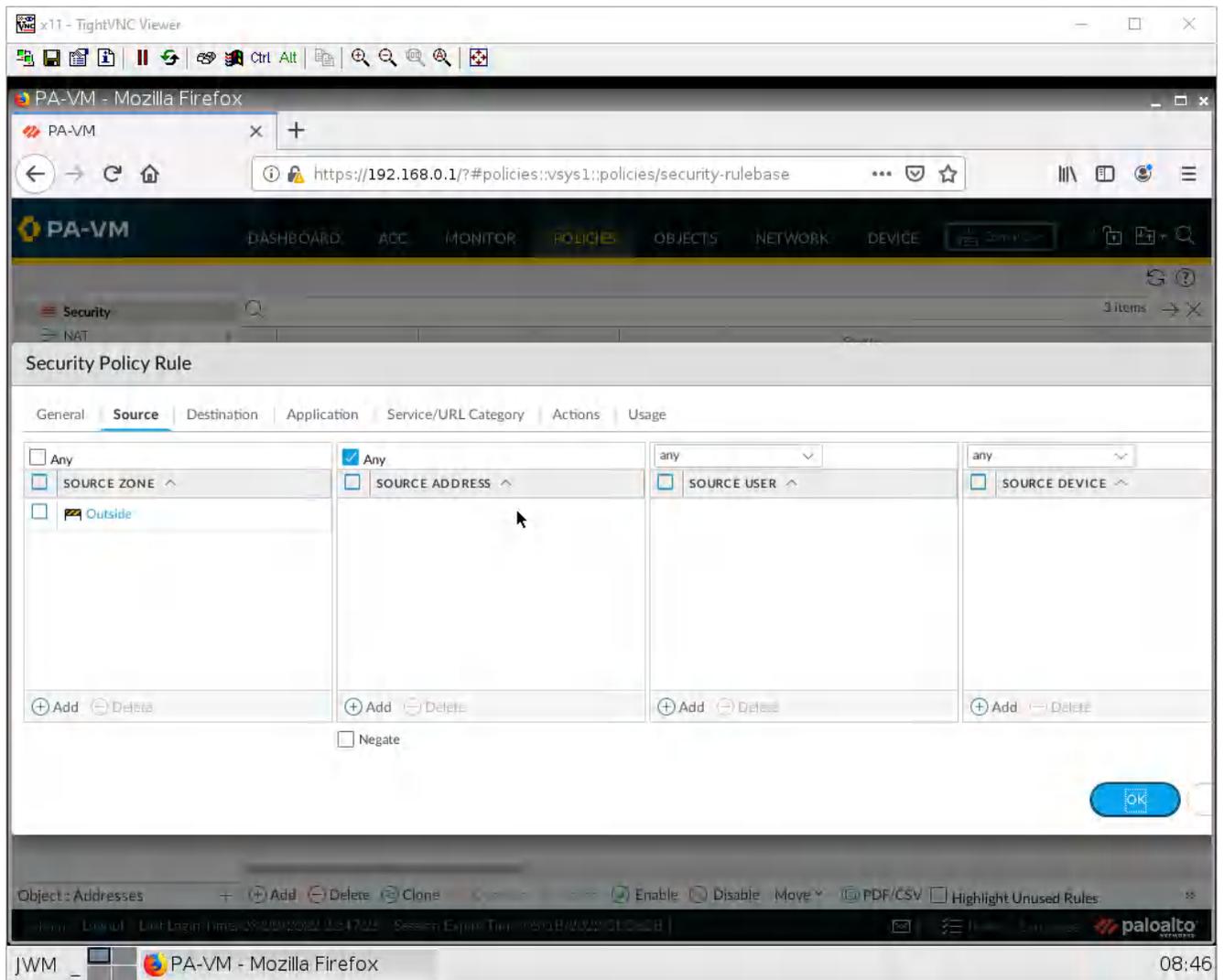


Figure 1.64: Configuring the Source Zone

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

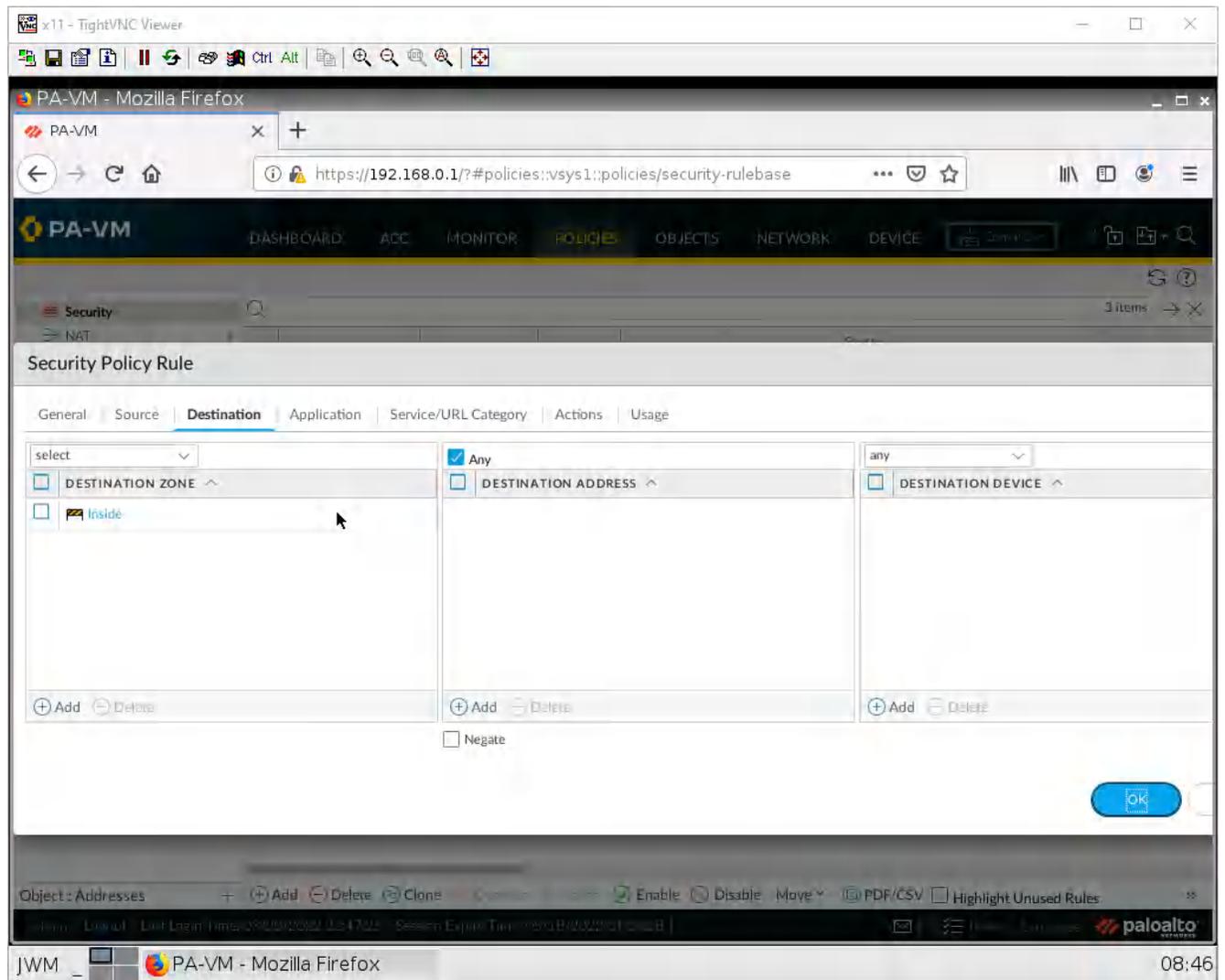


Figure 1.65: Configuring the Destination Zone

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!

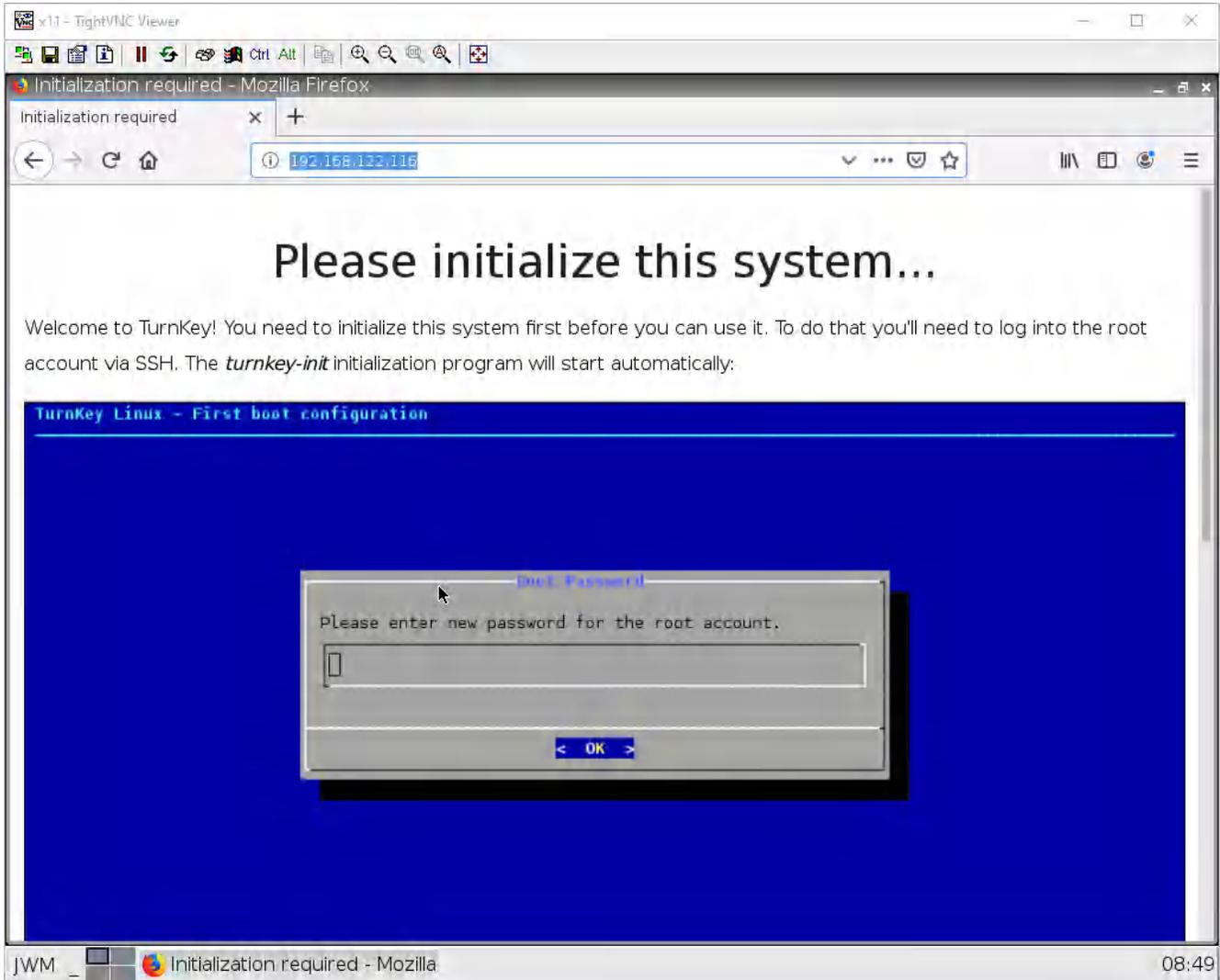


Figure 1.66: Verify your configuration



# Chapter 2. Security Tuneup



---

## 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.

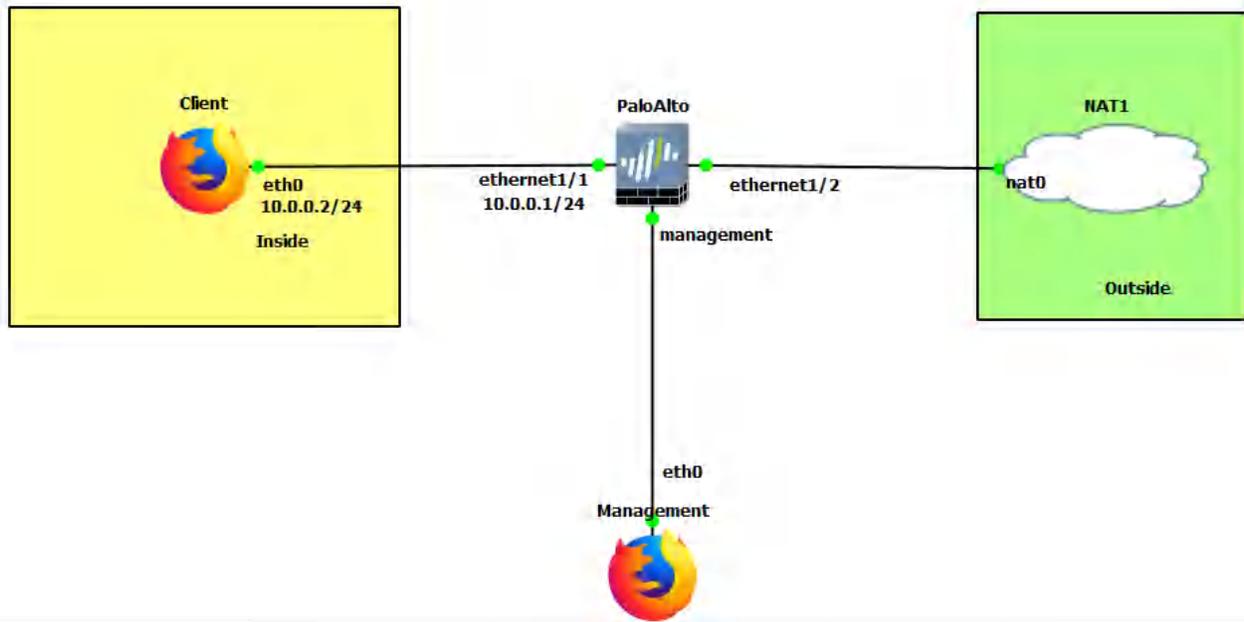


Figure 2.1: Main scenario

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

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

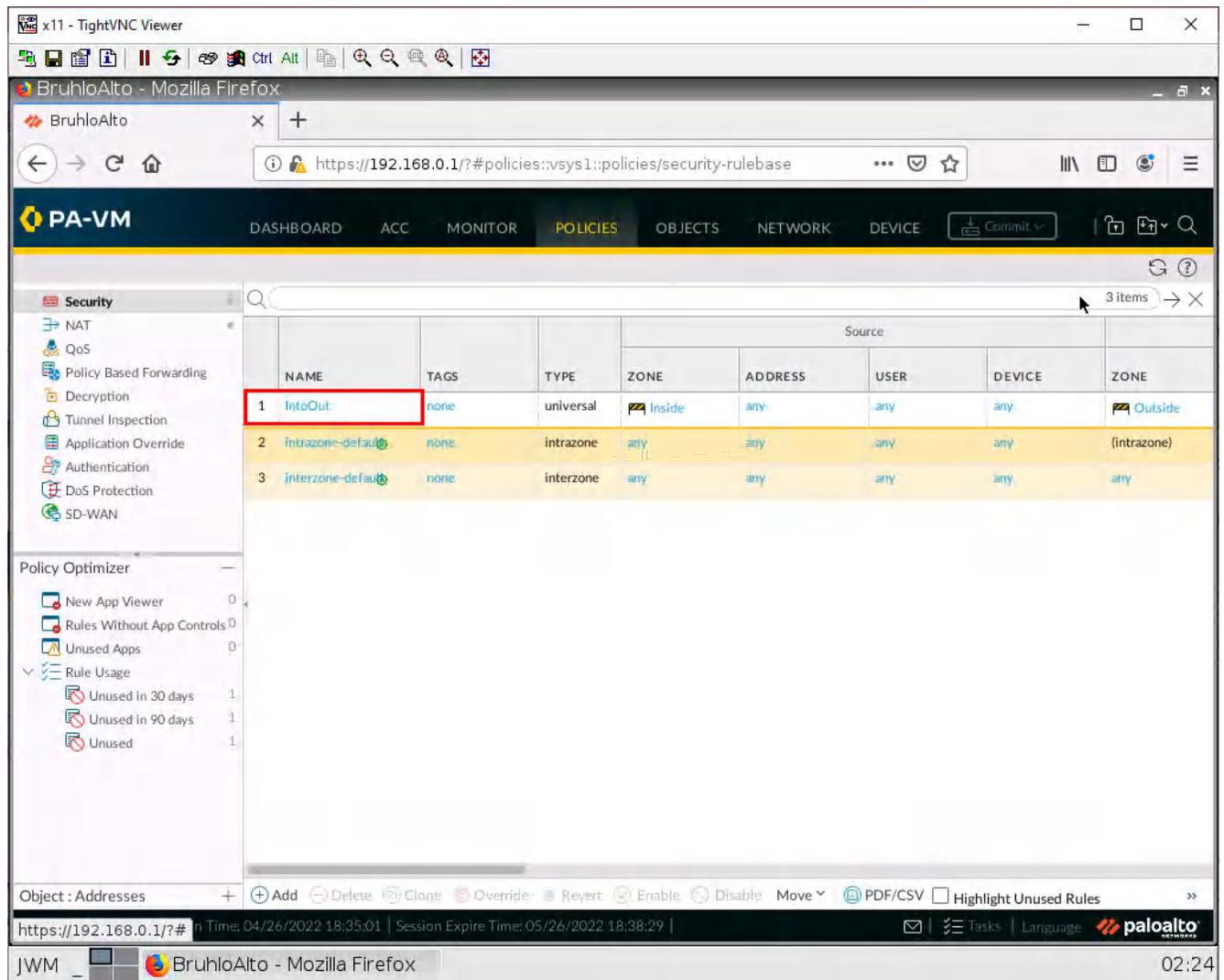


Figure 2.2: Create a Security Policy

Under the application tab, add these under applications:

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

These will allow only basic web browsing.

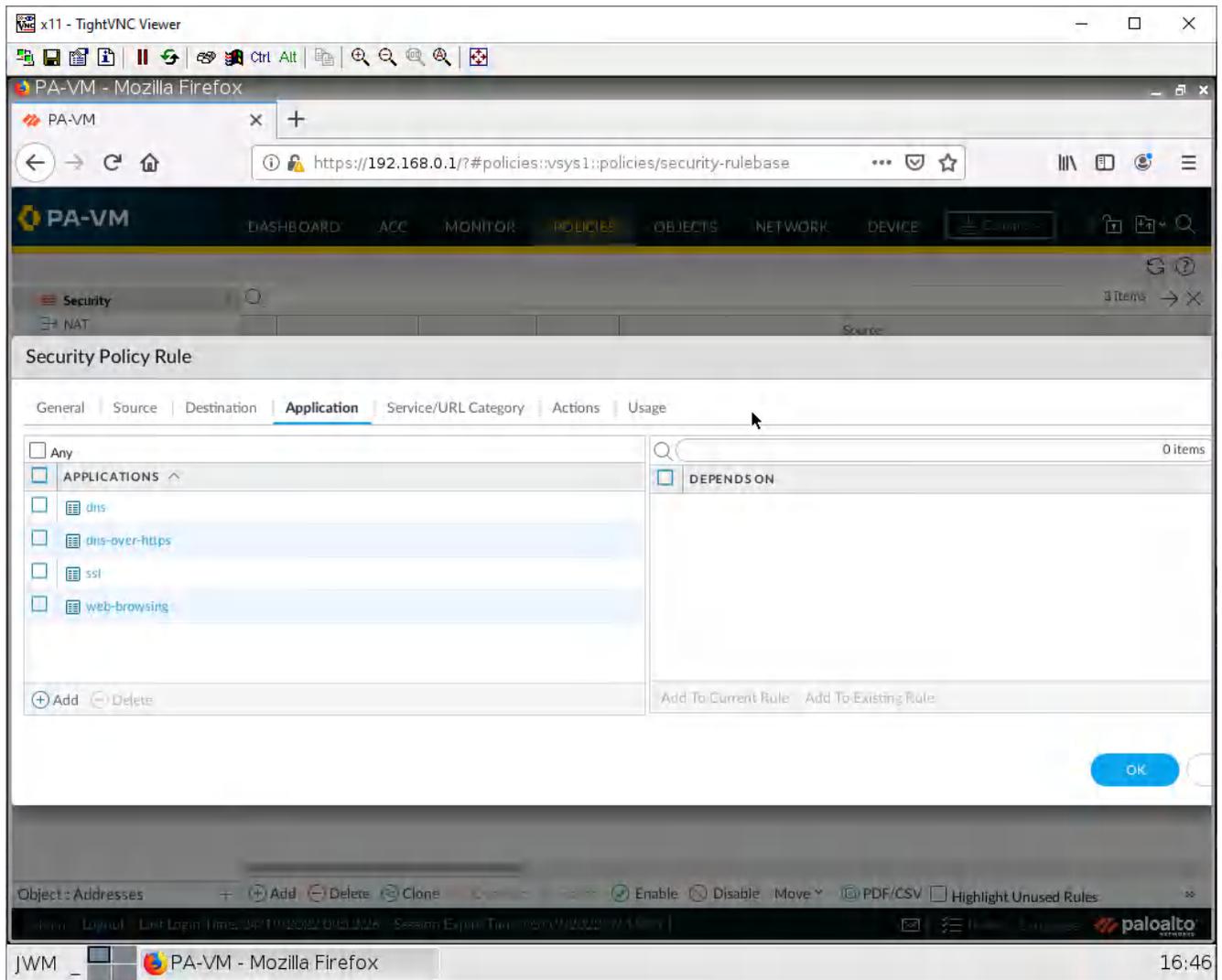


Figure 2.3: Set a custom application

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

## Test the Policy

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

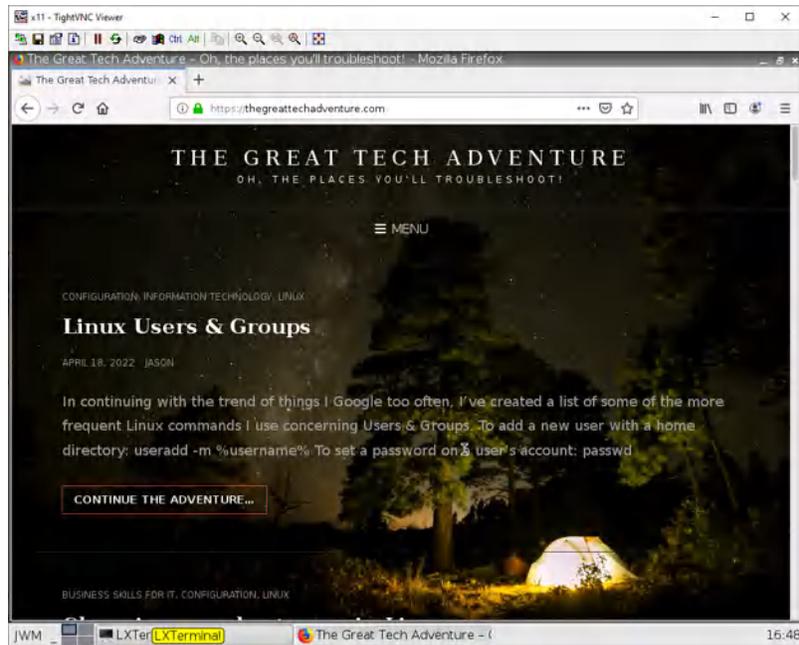


Figure 2.4: Verify your configuration

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

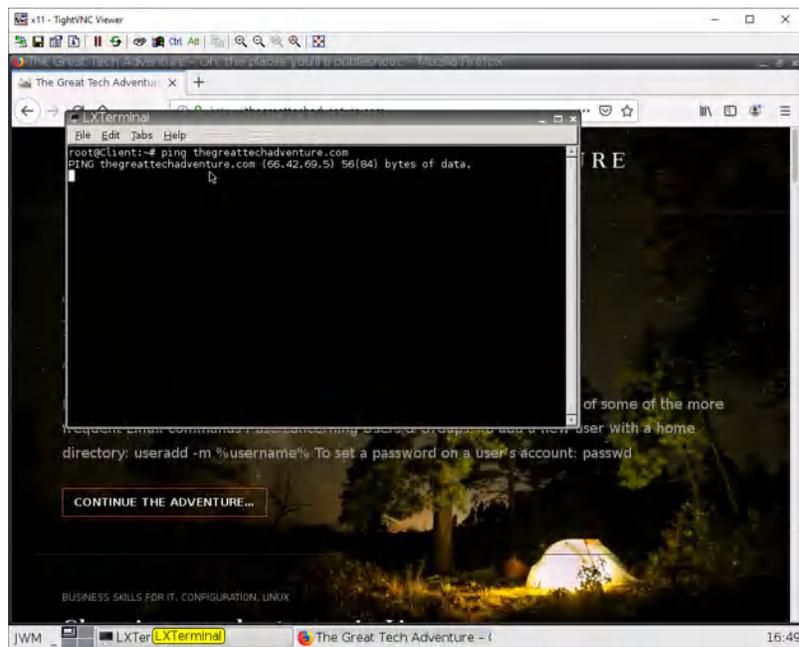


Figure 2.5: Verify Ping

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



---

## 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.

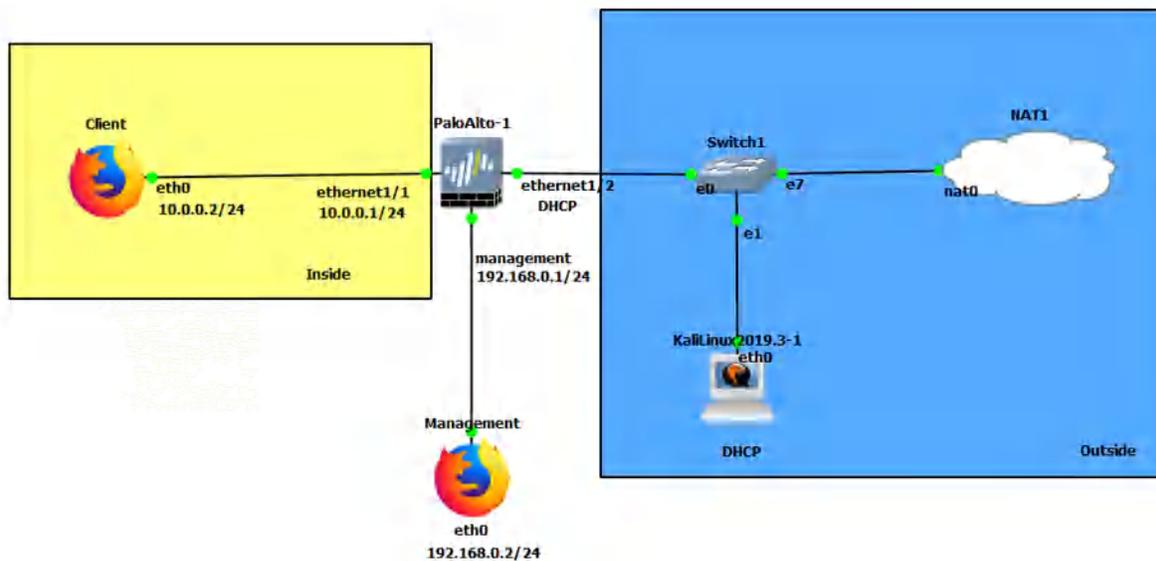


Figure 2.6: Main scenario

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.

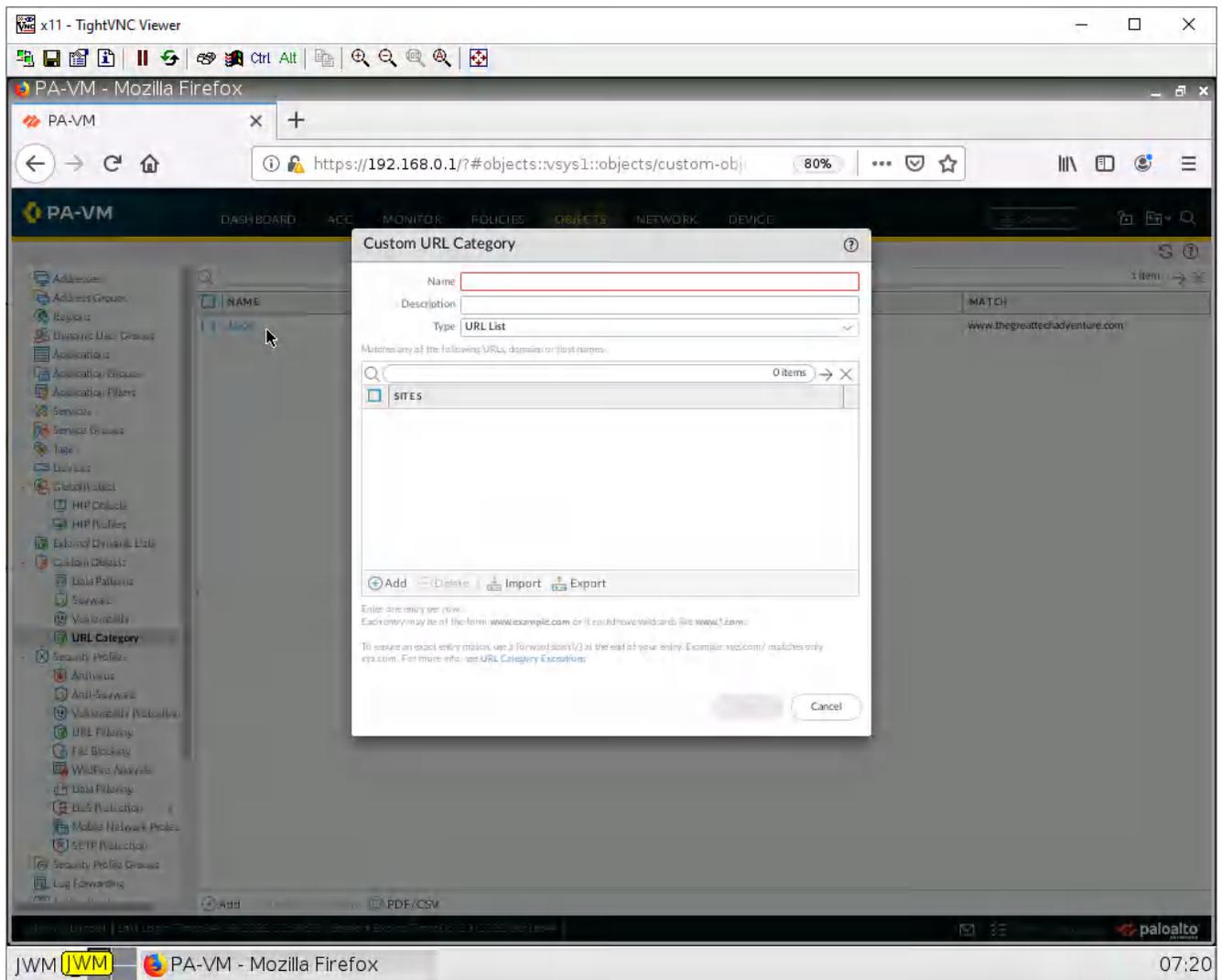


Figure 2.7: Create a Custom URL Category

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

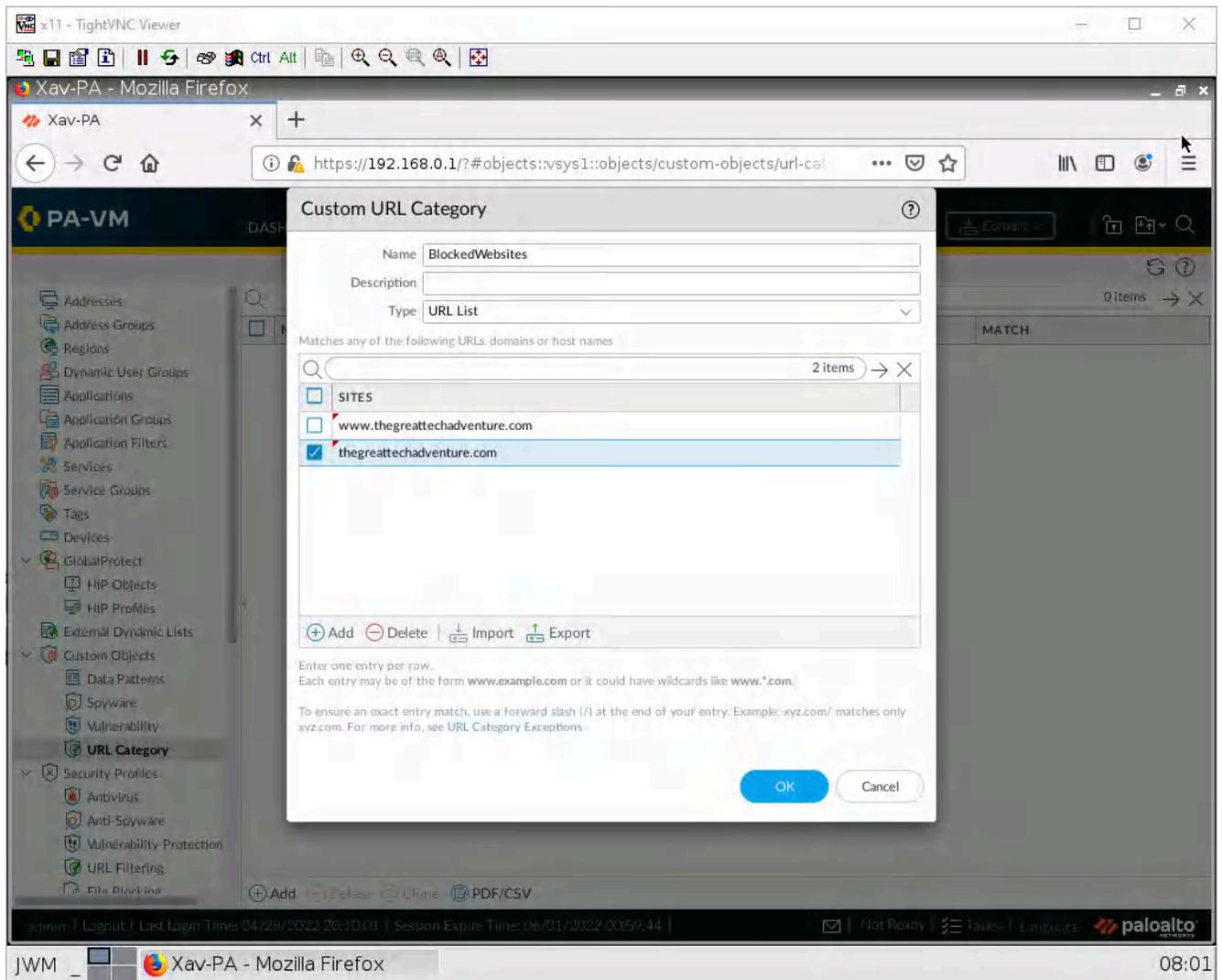


Figure 2.8: Add a CustomURL Category

Enter some websites you would like to block. Here I have added a sample website ([www.thegreattechadventure.com](http://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**:

The screenshot shows the Palo Alto VM console interface. The main content area displays a table of security policies. The table has columns for NAME, TAGS, TYPE, ZONE, ADDRESS, USER, DEVICE, and ZONE. Three policies are listed:

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
1	IntoOut	none	universal	Inside	any	any	any	Outside
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)
3	interzone-default	none	interzone	any	any	any	any	any

At the bottom of the console, the 'Object : Addresses' section is visible, and the '+ Add' button is highlighted with a red box. The console also shows the session time as 04/26/2022 18:35:01 and the session expire time as 05/26/2022 18:38:29.

Figure 2.9: Add a security policy

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

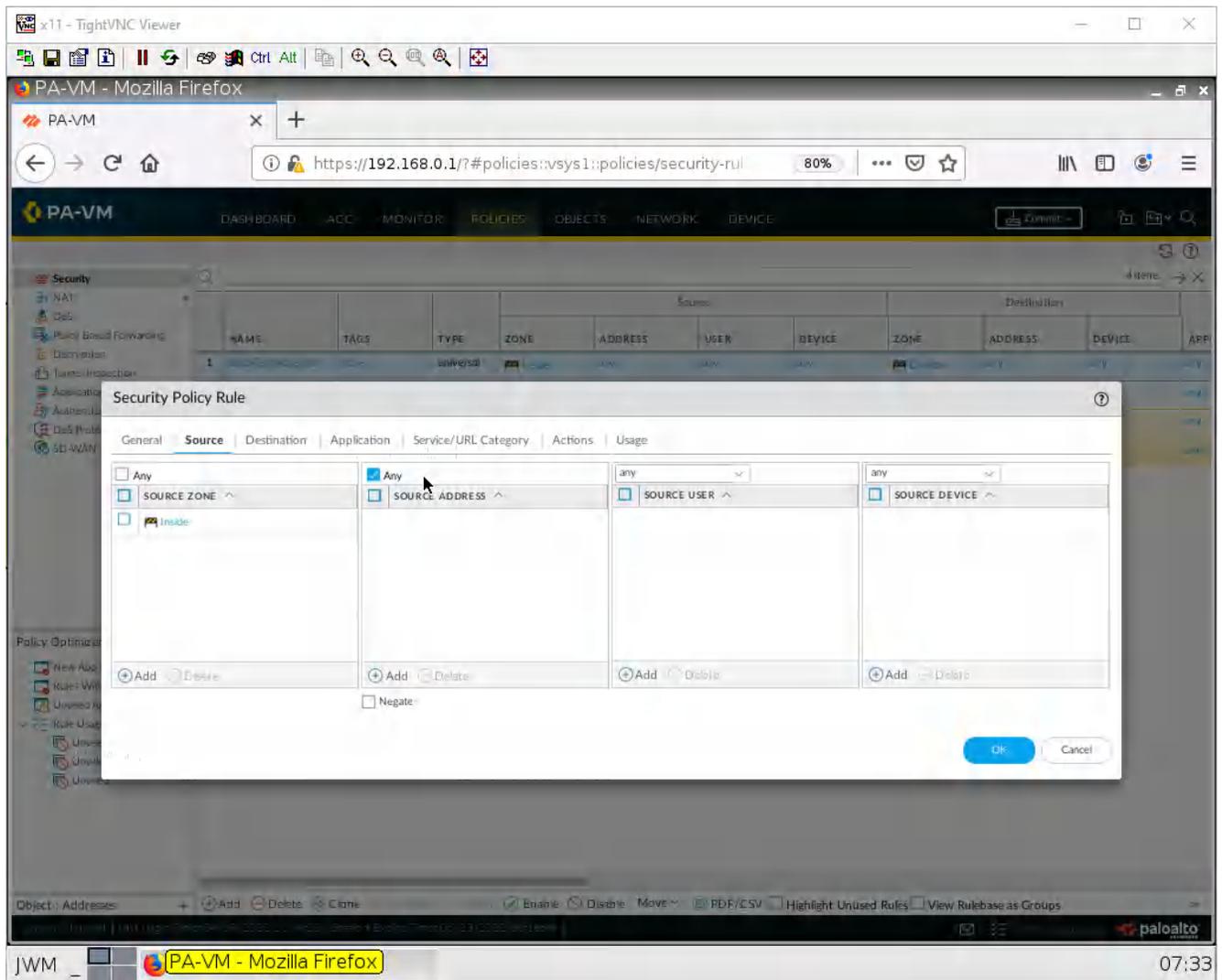


Figure 2.10: Add a Source Zone

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

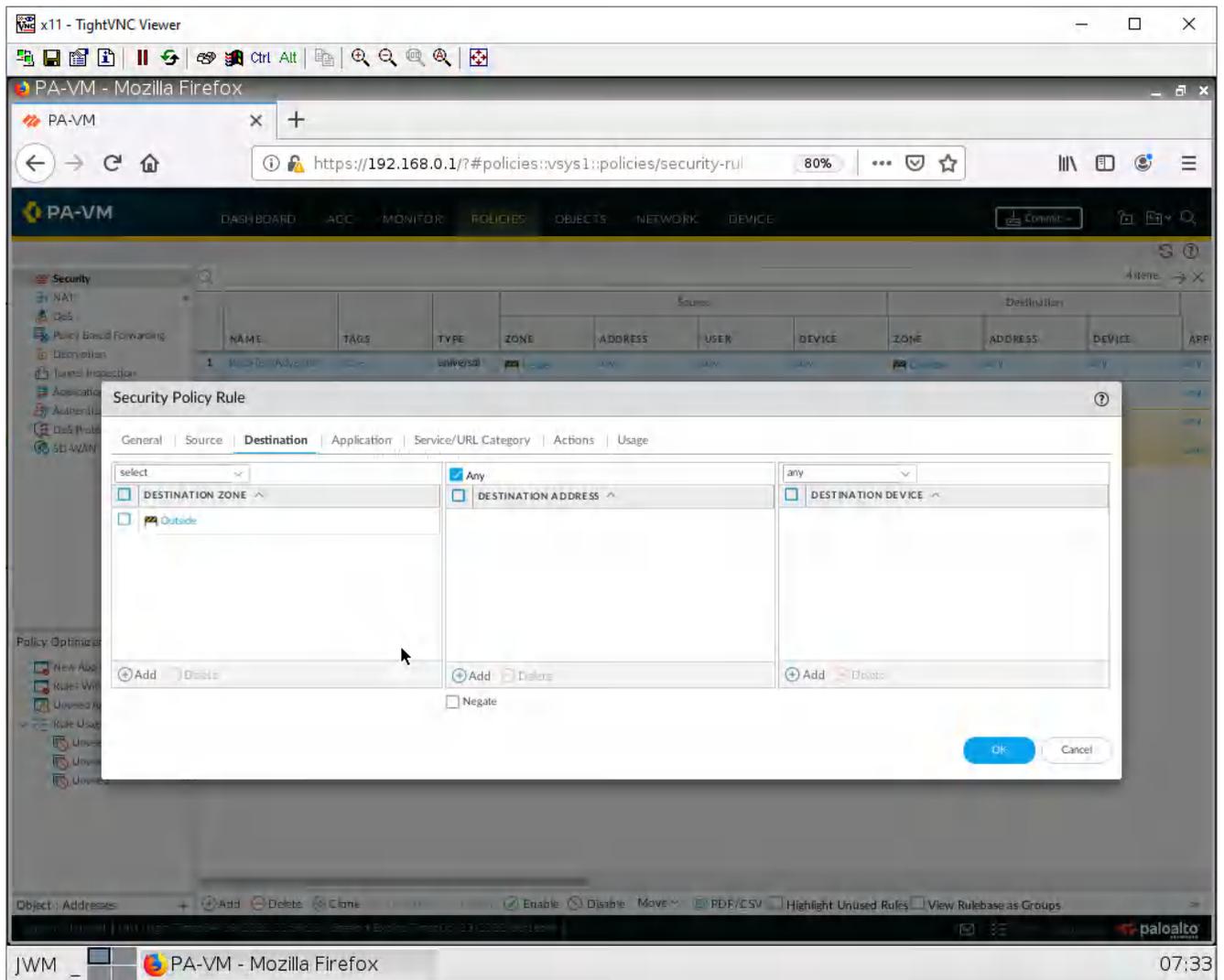


Figure 2.11: Add a Destination Zone

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

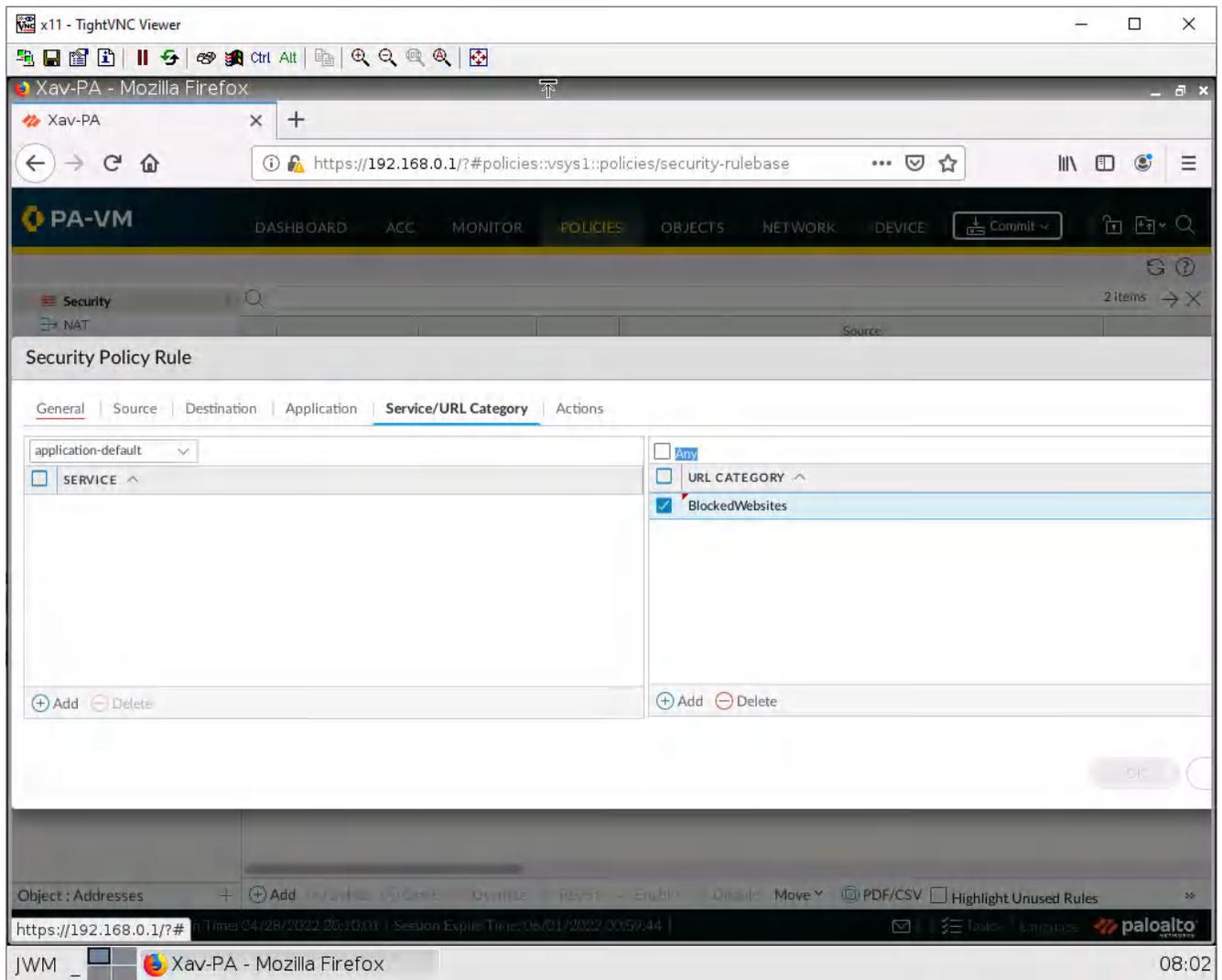


Figure 2.12: Assign URL Category

Under the actions page, set the action to deny.

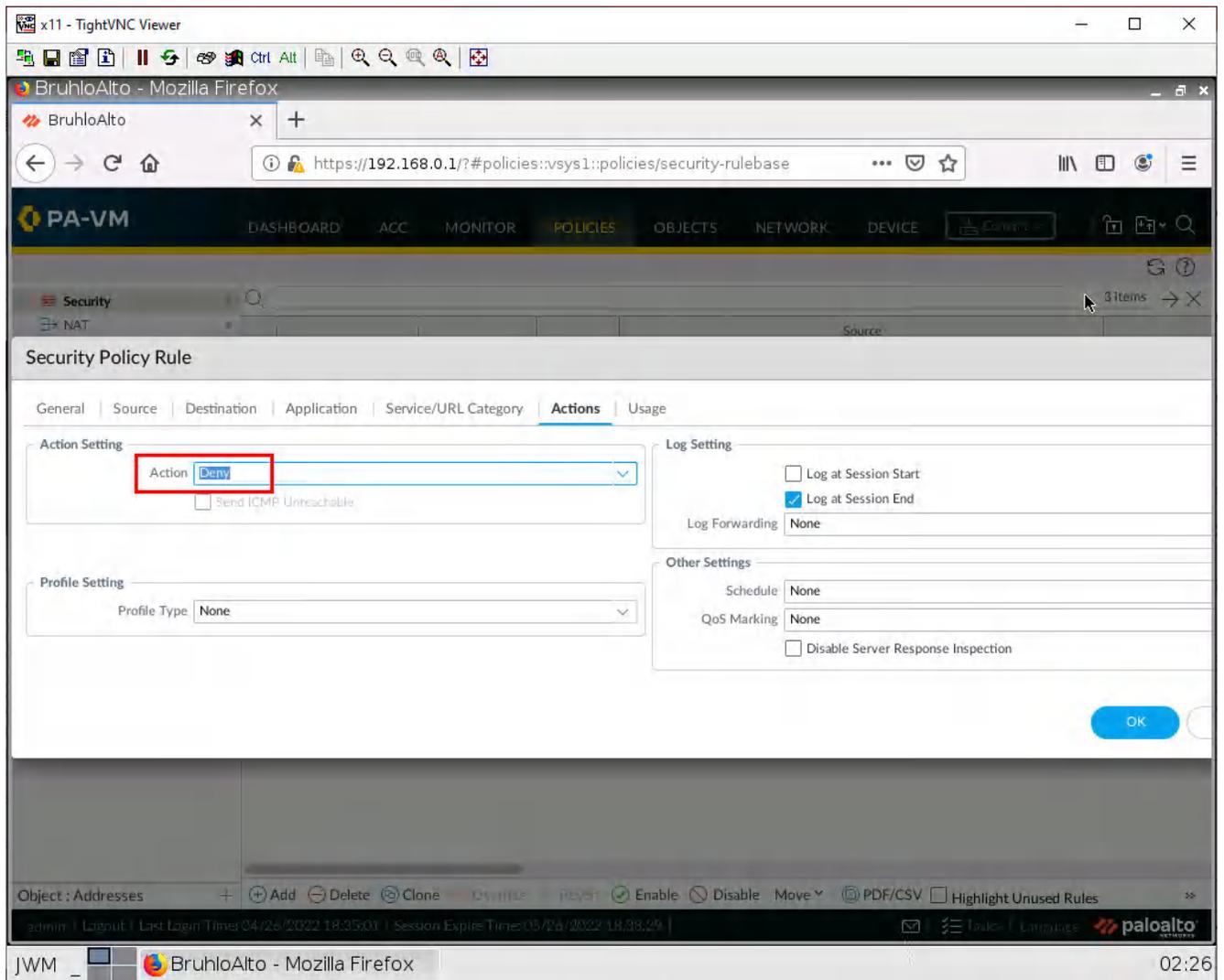


Figure 2.13: Set an Action to Deny

Then click **OK**.

## Enable Block Pages

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

The screenshot shows the Palo Alto VM configuration interface in a Mozilla Firefox browser window. The browser address bar shows the URL: `https://192.168.0.1/#device::vsys1::device/block-pages`. The interface has a navigation menu on the left with 'Response Pages' selected. The main content area displays a table of block pages.

TYPE	ACTION	LOCATION	NAME
Antivirus / Anti-spyware Block Page		Default	
Application Block Page	Disabled	Default	
Captive Portal Comfort Page		Default	
Data Filtering Block Page		Default	
File Blocking Continue Page		Default	
File Blocking Block Page		Default	
GlobalProtect App Help Page		Default	
GlobalProtect Portal Login Page		Default	
GlobalProtect Portal Home Page		Default	
GlobalProtect App Welcome Page		Default	
MFA Login Page		Default	
SAML Auth Internal Error Page		Default	
SSL Certificate Errors Notify Page		Default	
SSL Decryption Opt-out Page	Disabled	Default	
URL Filtering and Category Match Block Page		Default	
URL Filtering Continue and Override Page		Default	
URL Filtering Safe Search Block Page		Default	
Anti Phishing Block Page		Default	
Anti Phishing Continue Page		Default	

The 'Application Block Page' row is highlighted, and the word 'Disabled' in the 'ACTION' column is enclosed in a red rectangular box. The interface also shows a search bar at the top right of the table area with '19 items' and a search icon.

Figure 2.14: Enabling Application Block Page

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

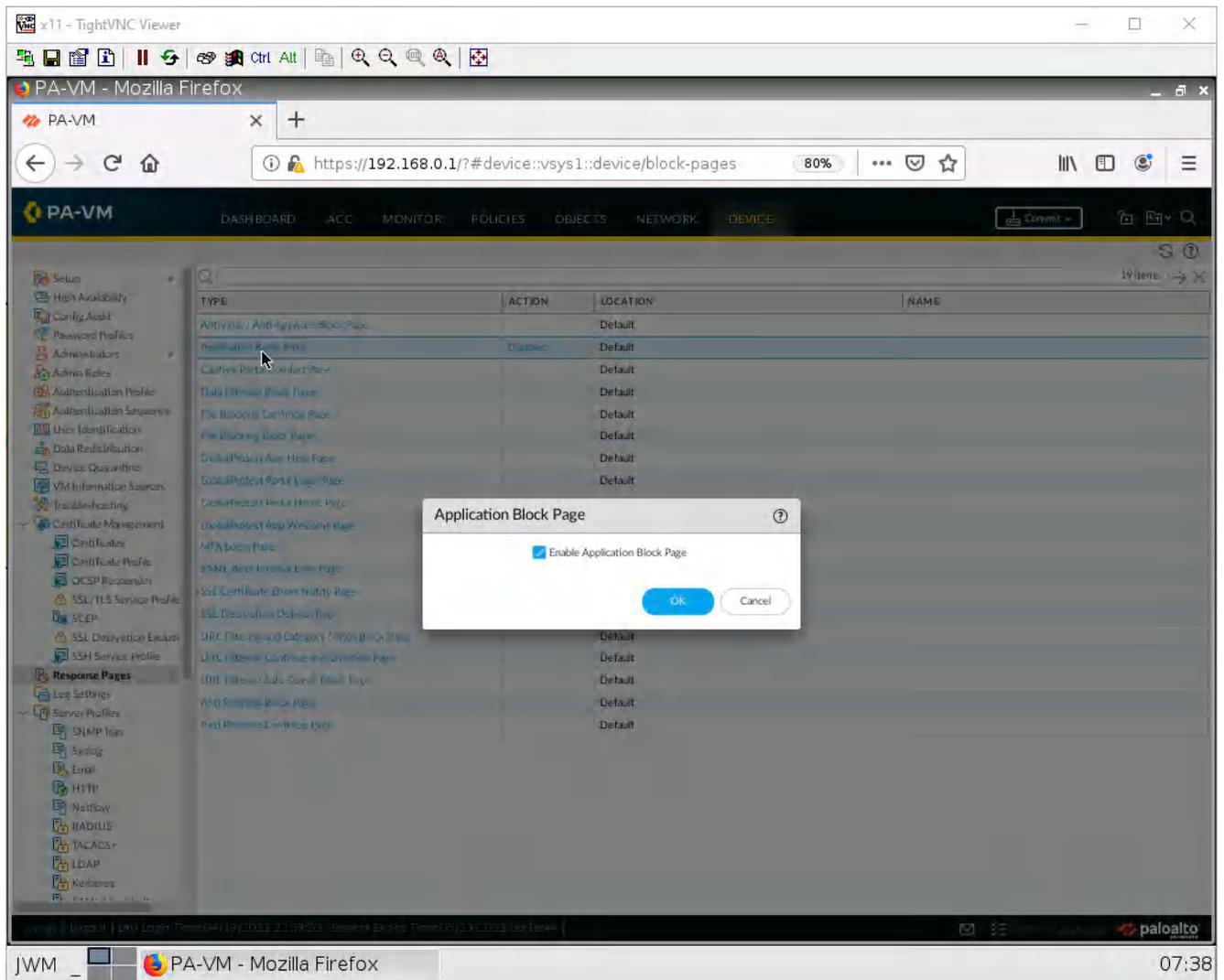


Figure 2.15: Enabling Application Block Page

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.

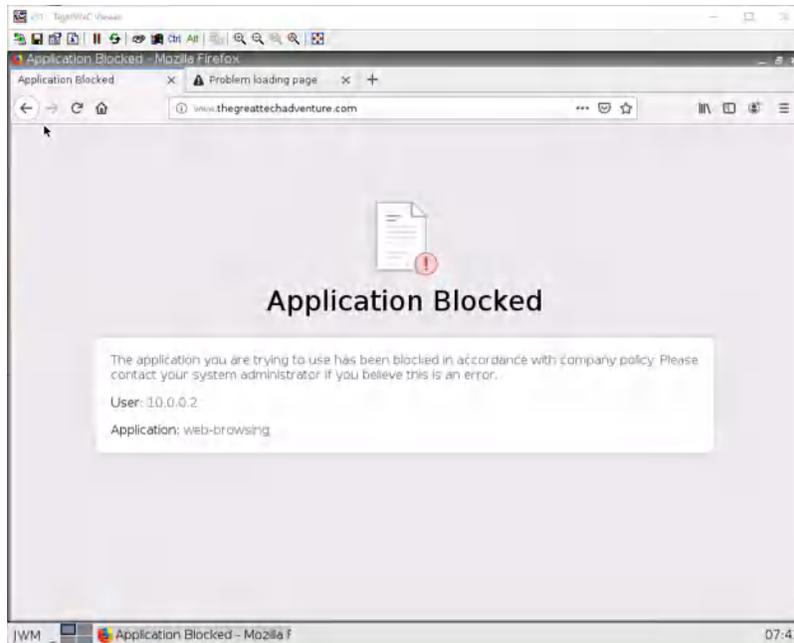


Figure 2.16: Application Block Page

If you see this page, that is alright too!

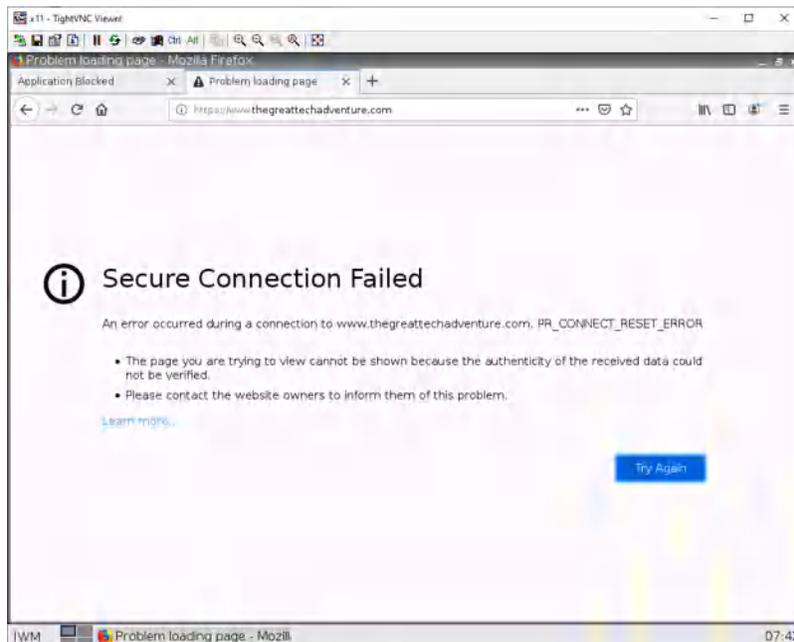


Figure 2.17: Application Block Page

## Set Up Kali to Be a Bad Actor

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

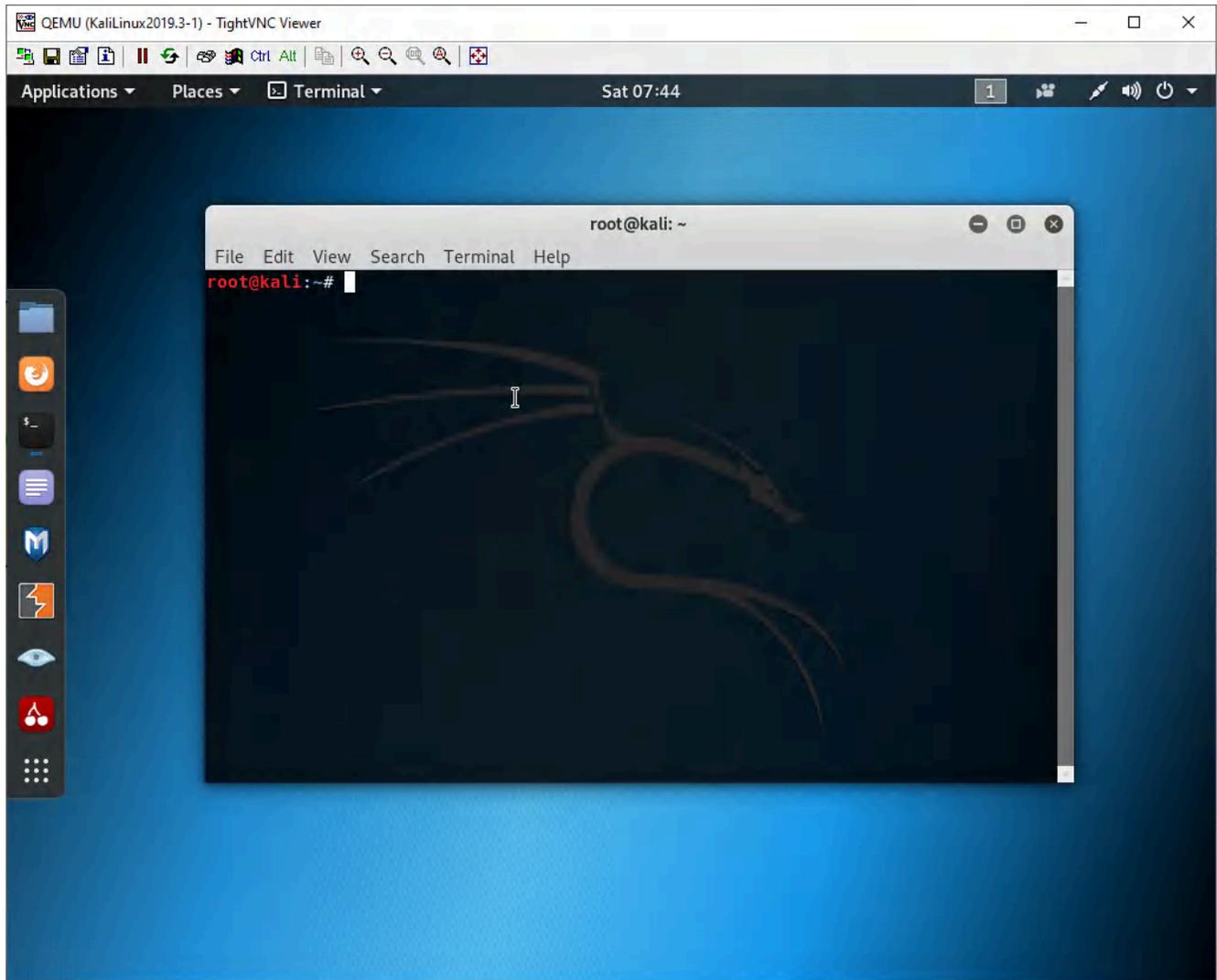


Figure 2.18: Open up Terminal in Kali

We will be using [Pentmenu by GinjaChris](#) 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
```

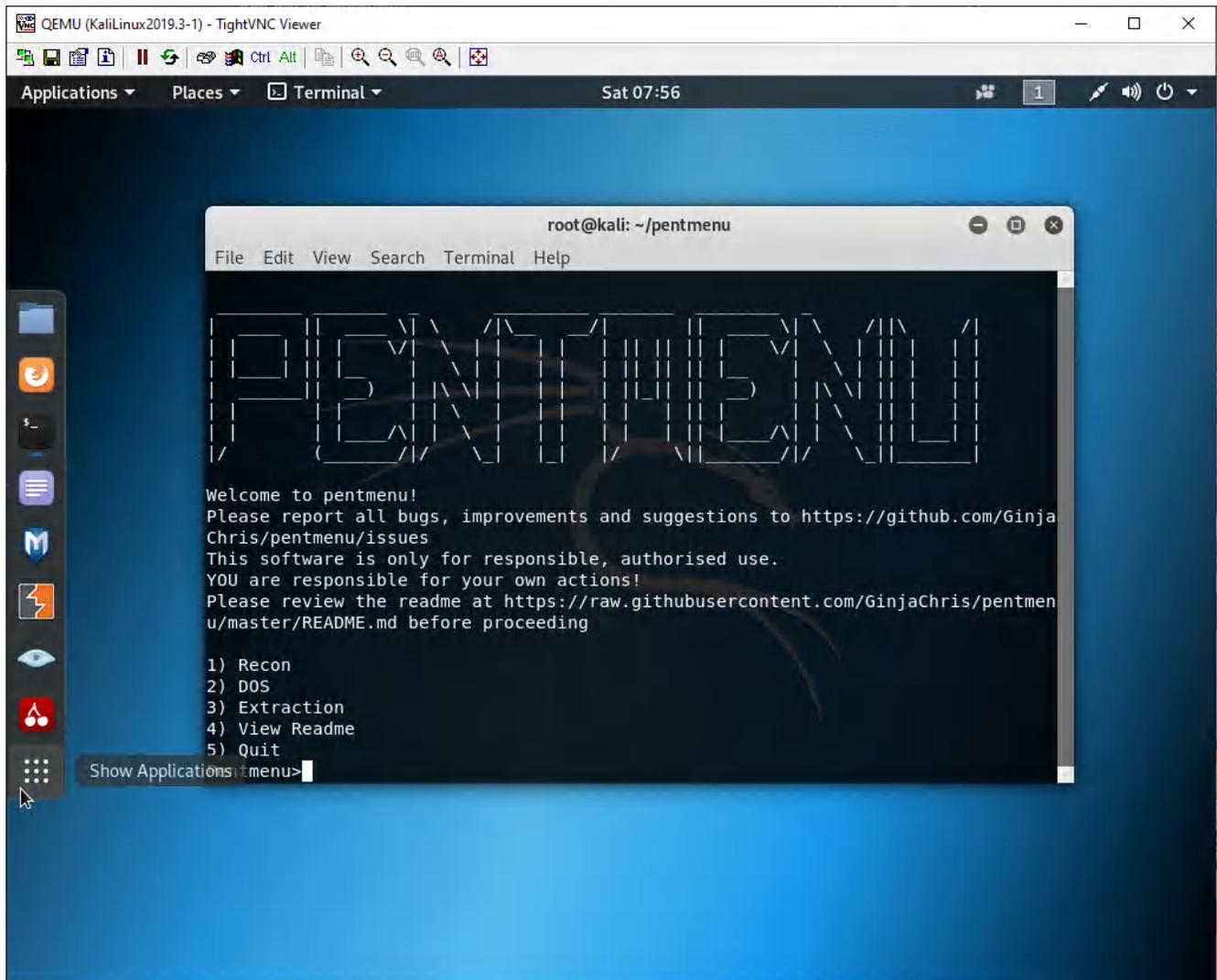


Figure 2.19: PentMenu app

Select option 2 for DoS attack.

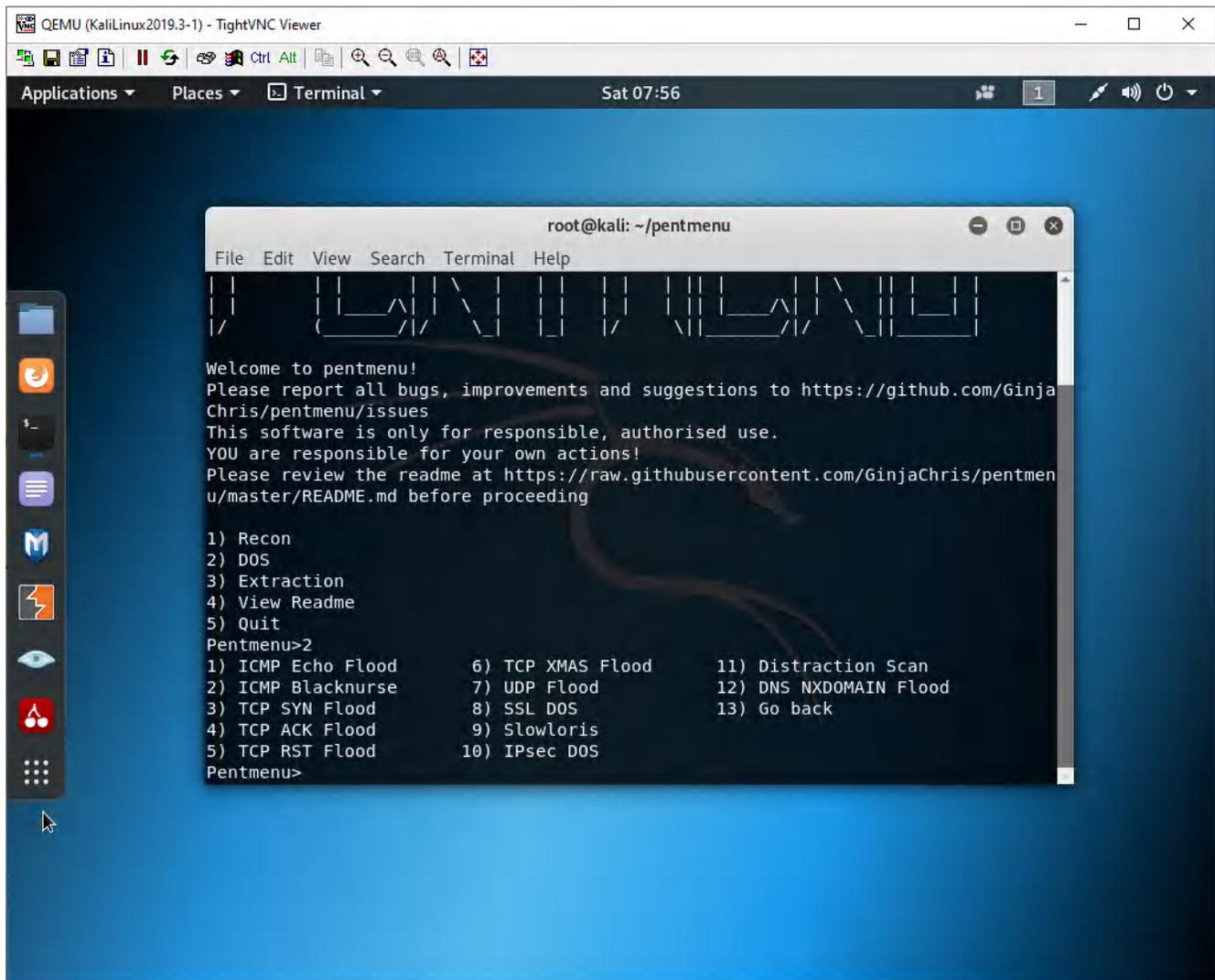


Figure 2.20: PentMenu app – Select DoS (2)

Select option 1 for ICMP Echo Flood.

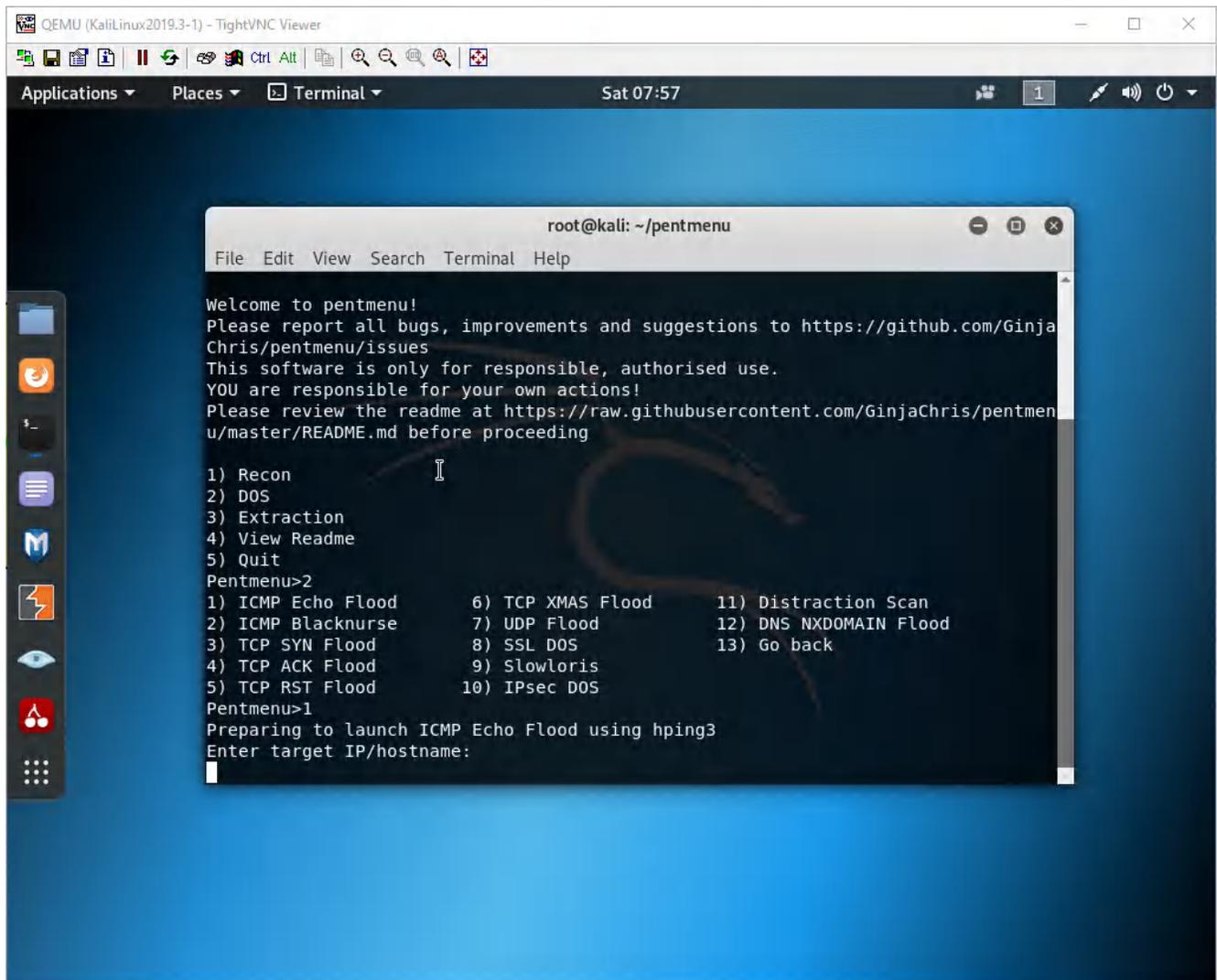


Figure 2.21: PentMenu app – Select ICMP Echo Flood(1)

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

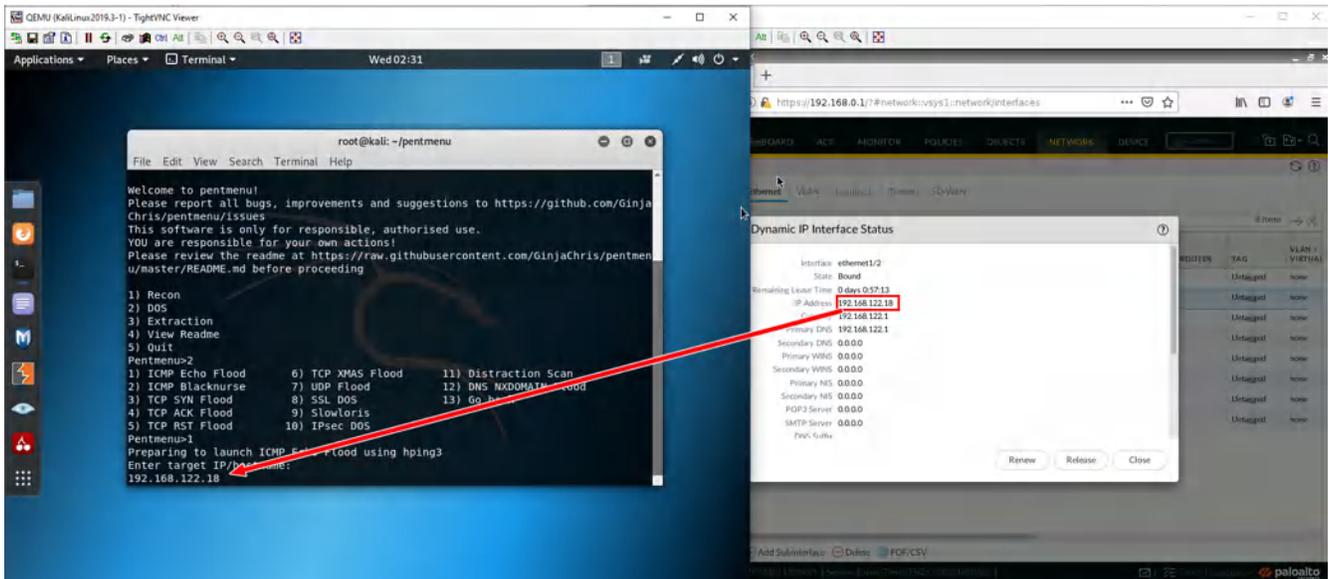


Figure 2.22: PentMenu app – Enter Target IP address

Select r for random IP address.

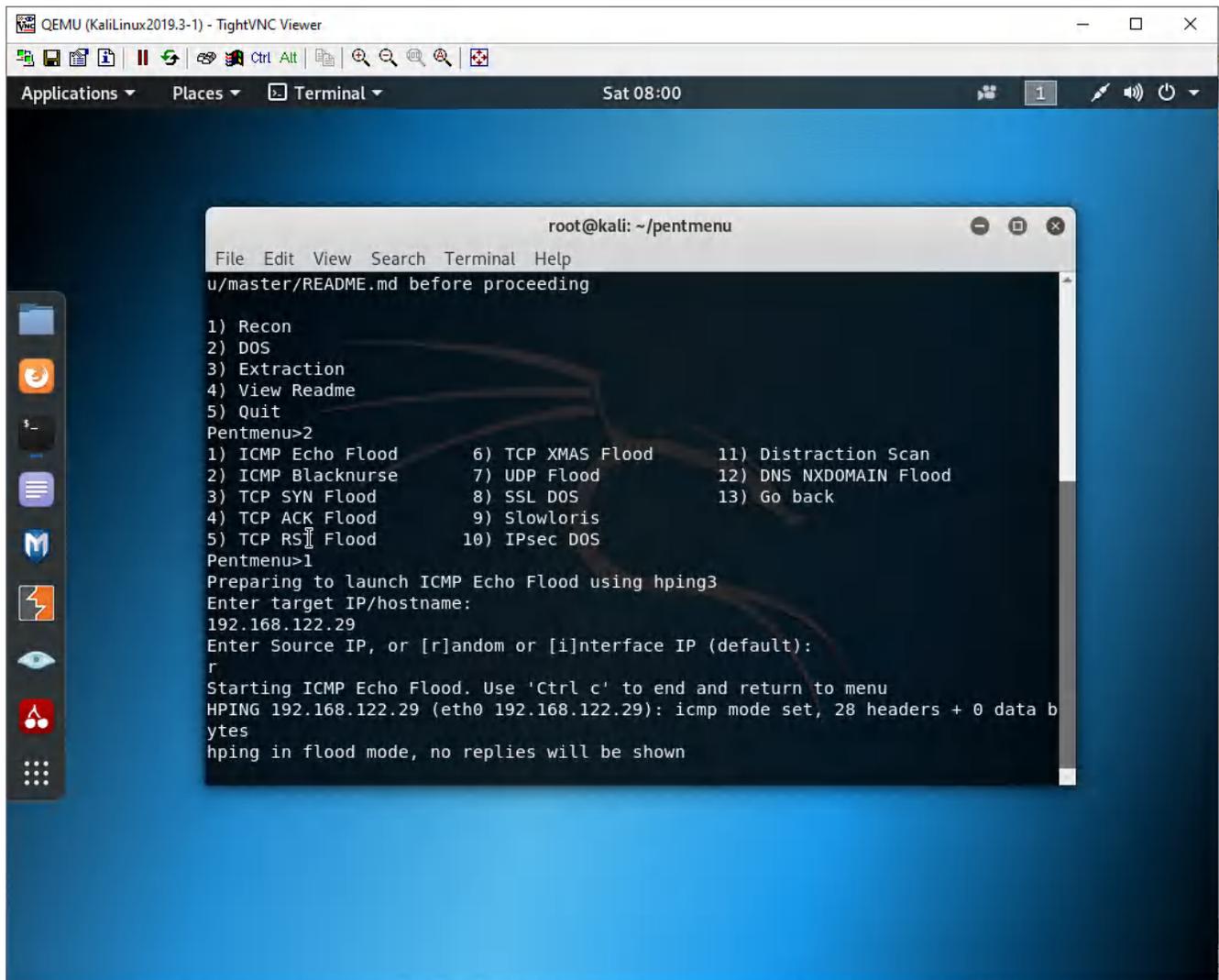


Figure 2.23: PentMenu app – Enter r for random IP address

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

## Analyze the ICMP Flood

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

START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PRO...	APPLICATI...	RULE	INGRESS I/F	EGR... I/F	BYTES	VIRTUAL SYSTEM	CL...
04/23 01:04:16	Outs...	Outside	89.66.199.94	192.168.122.29	62213	27648	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	210.217.255.126	192.168.122.29	62213	29184	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	57.100.45.117	192.168.122.29	62213	11520	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	176.203.8.82	192.168.122.29	62213	32768	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	46.118.185.136	192.168.122.29	62213	23296	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	209.187.54.219	192.168.122.29	62213	513	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	117.46.147.166	192.168.122.29	62213	9216	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	32.208.162.166	192.168.122.29	62213	50432	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	64.91.241.46	192.168.122.29	62213	2816	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	131.24.224.202	192.168.122.29	62213	8144	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	59.118.203.191	192.168.122.29	62213	48640	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	216.75.47.244	192.168.122.29	62213	4608	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	46.251.113.2	192.168.122.29	62213	46080	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	75.229.120.69	192.168.122.29	62213	64512	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	174.135.54.54	192.168.122.29	62213	14592	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	205.4.105.59	192.168.122.29	62213	14848	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>
04/23 01:04:16	Outs...	Outside	188.151.230.236	192.168.122.29	62213	37888	1	ping	intrazone-default	ether...	ether...	60	vsys1	<input checked="" type="checkbox"/>

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

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

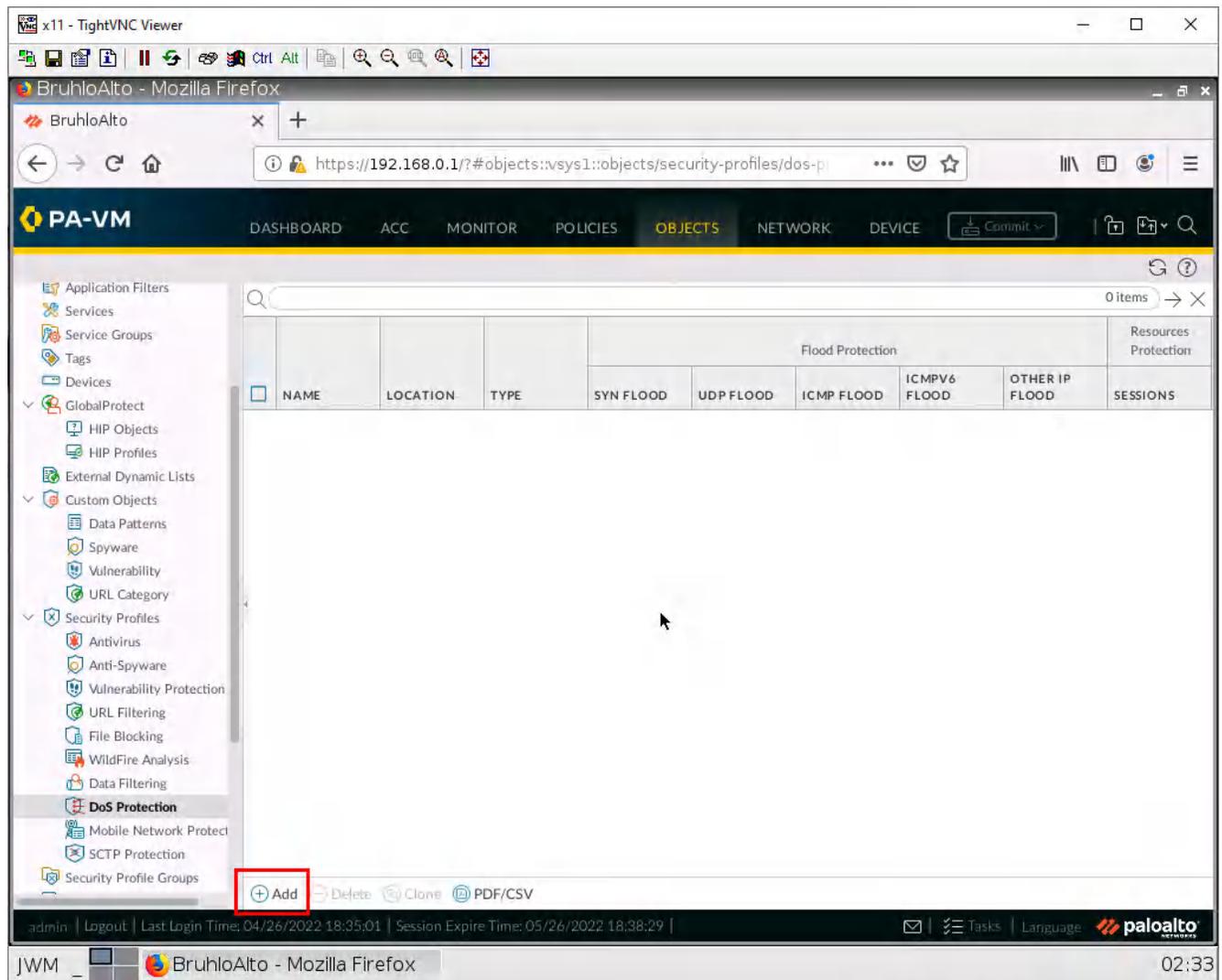


Figure 2.25: Create a DoS Protection

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

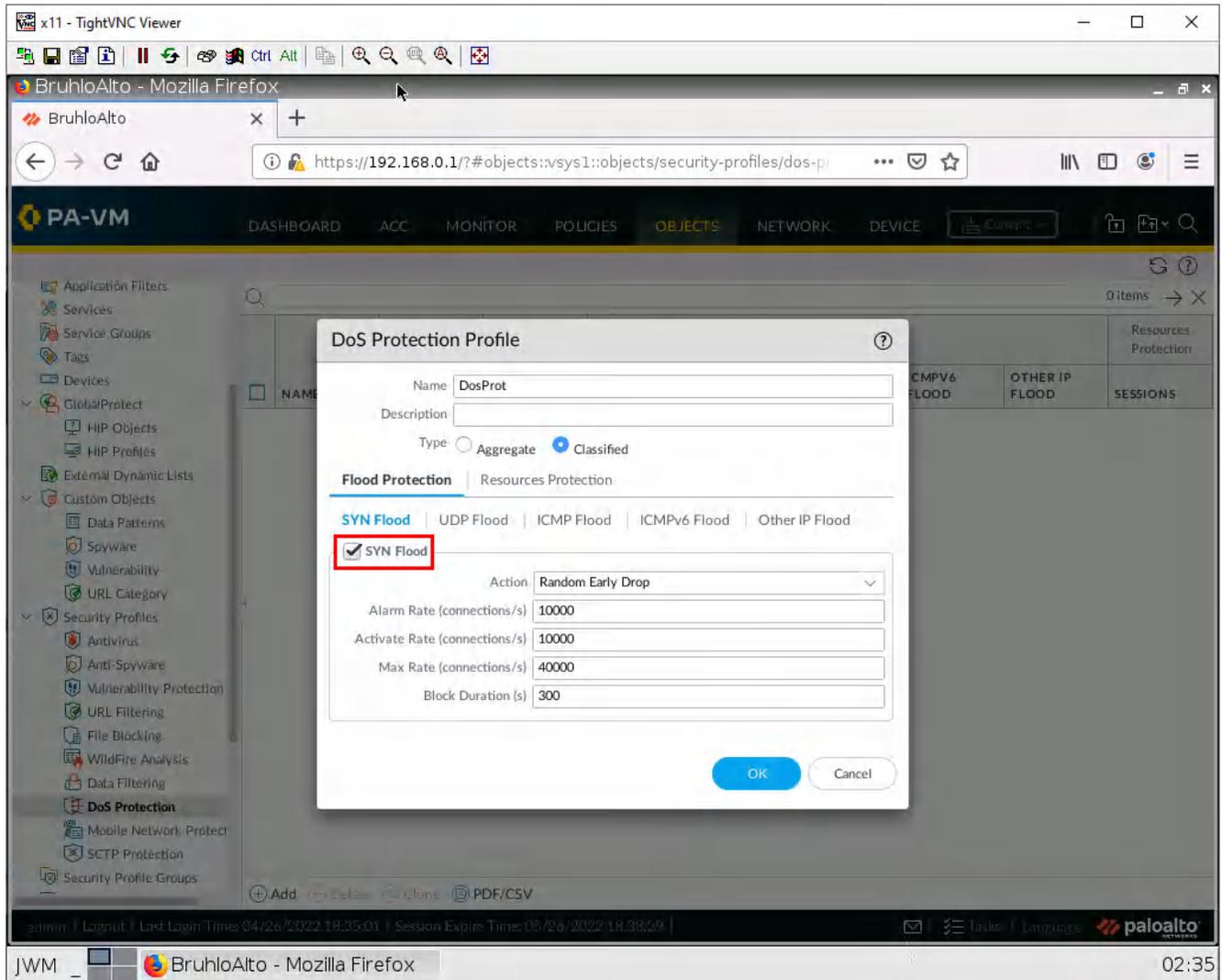


Figure 2.26: SYN Flood Protection

After that, click **OK**.

## Apply the DoS Protection Profile

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

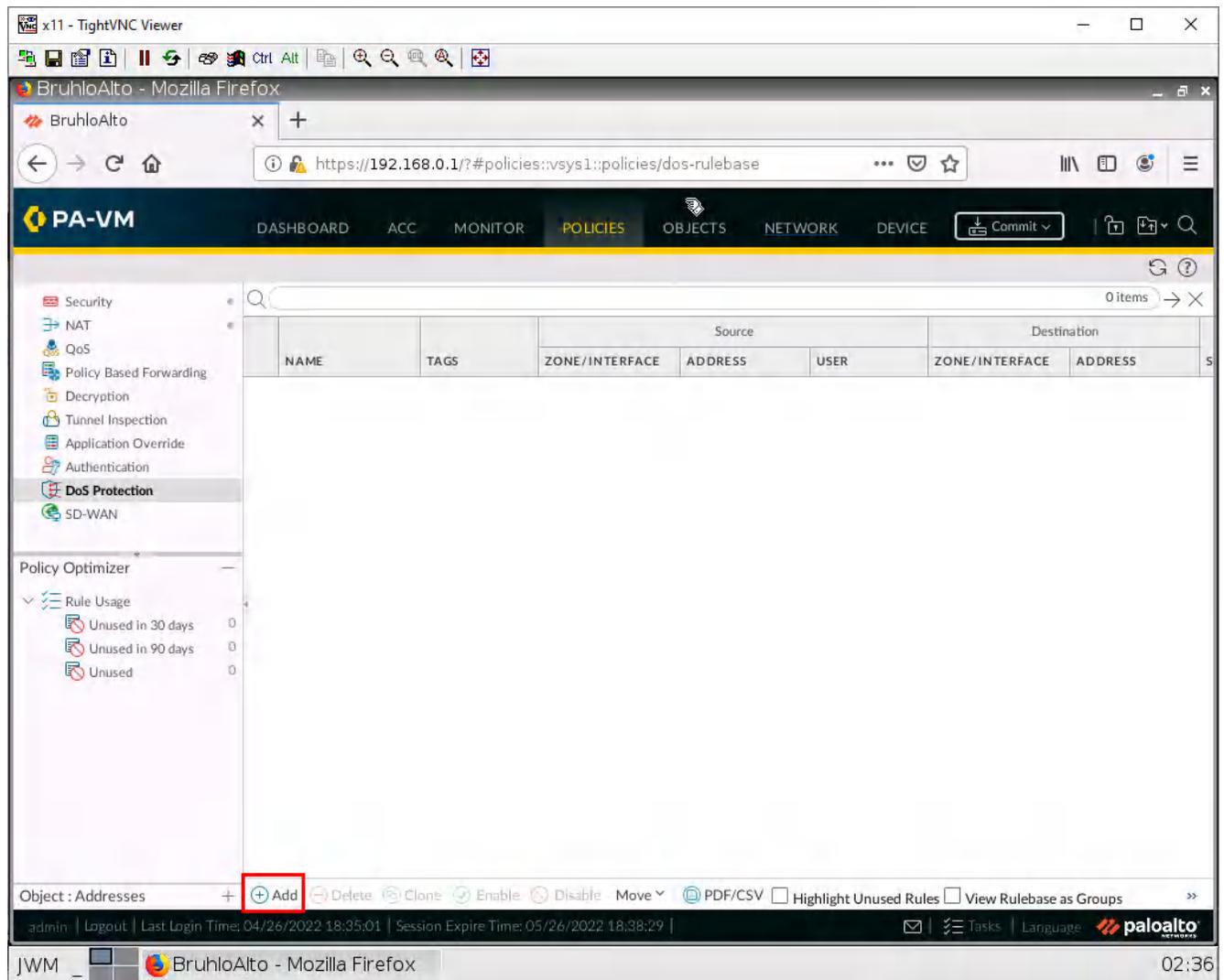


Figure 2.27: Add a DoS Protection Rule

Under the Source tab, add the Outside zone.

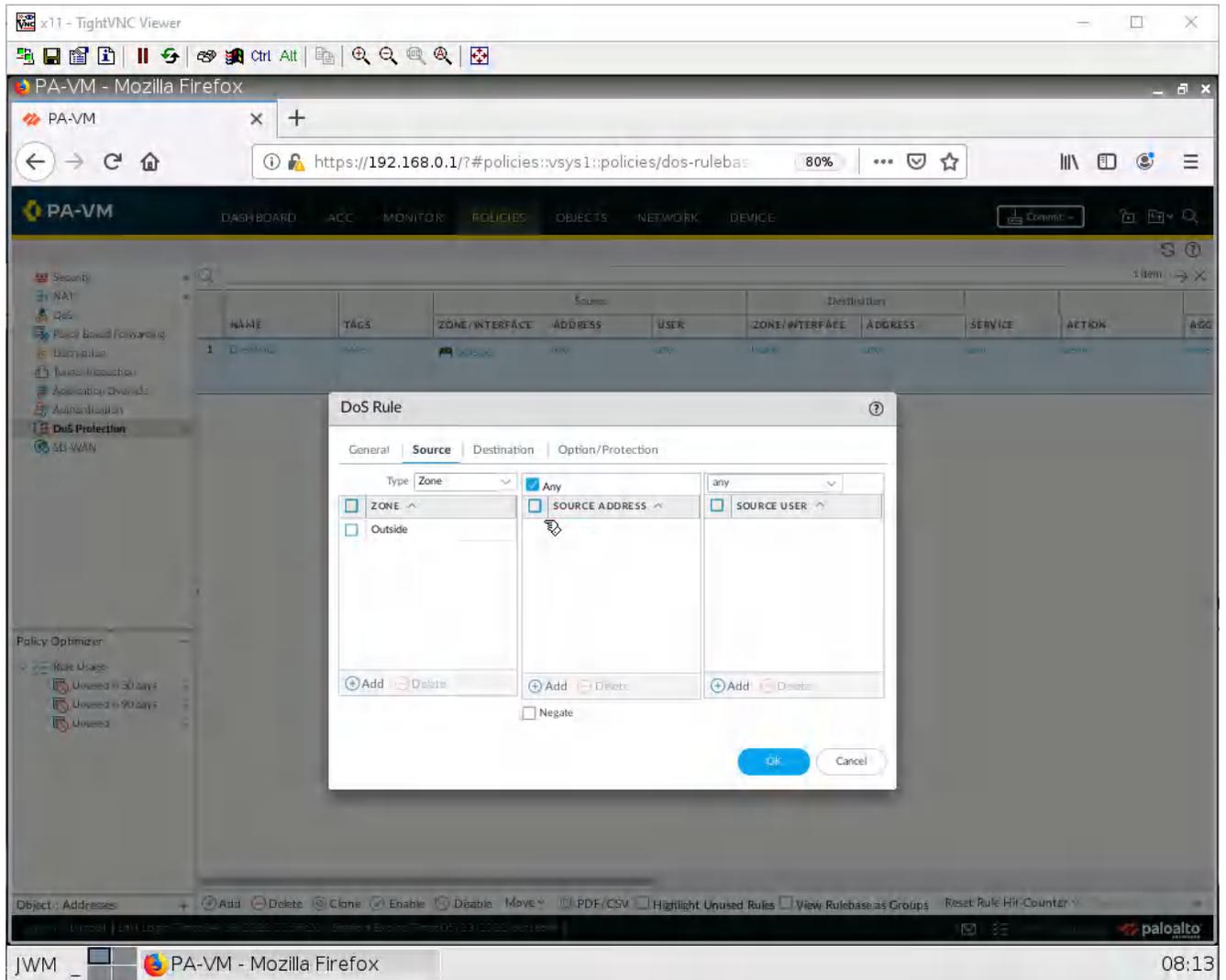


Figure 2.28: Add the Source Zone

Under the Destination tab, add the Inside zone.

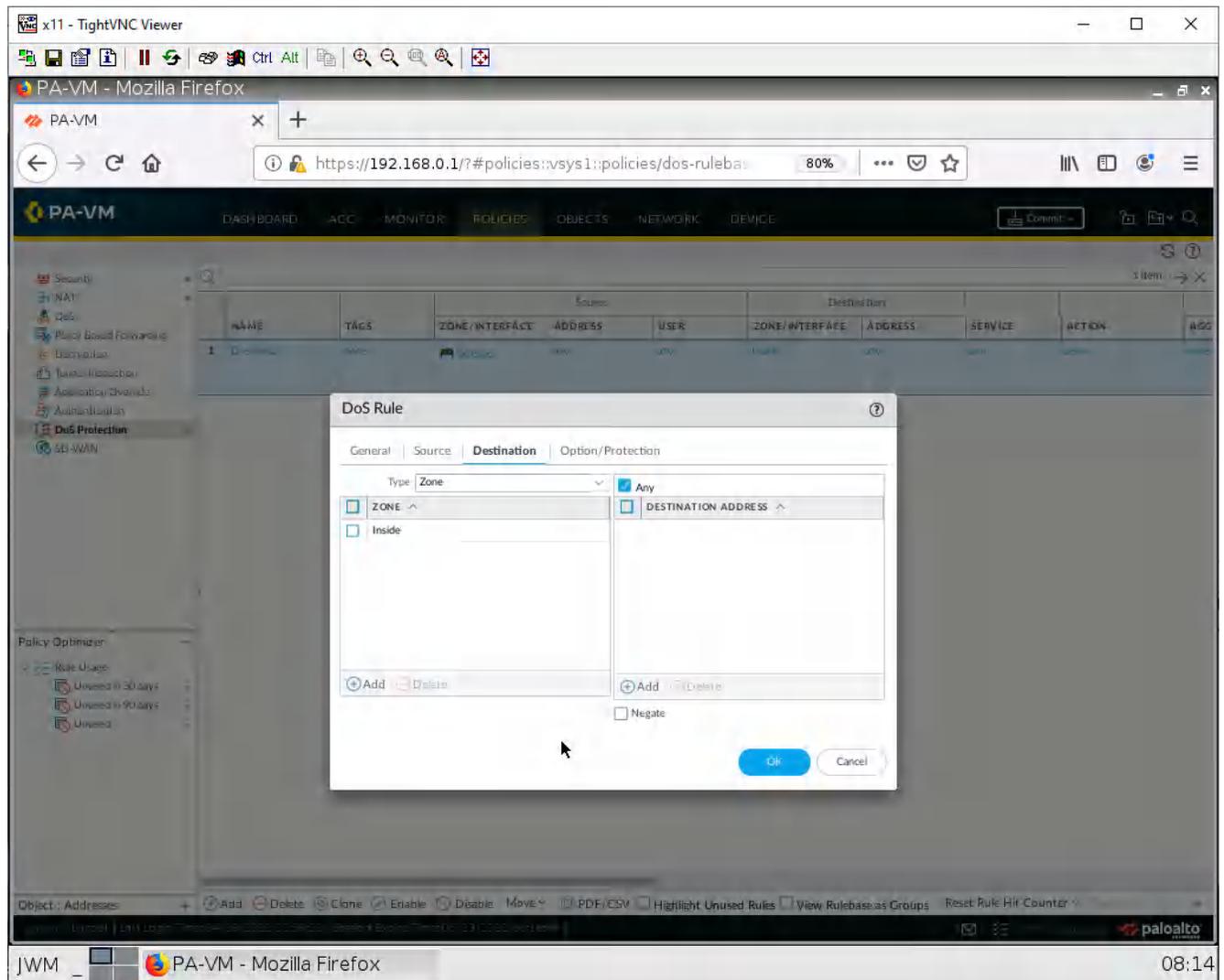


Figure 2.29: Add the Destination Zone

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	<i>Tick this box</i>
Profile	<i>The name of the one you created</i>
Address	source-IP-only

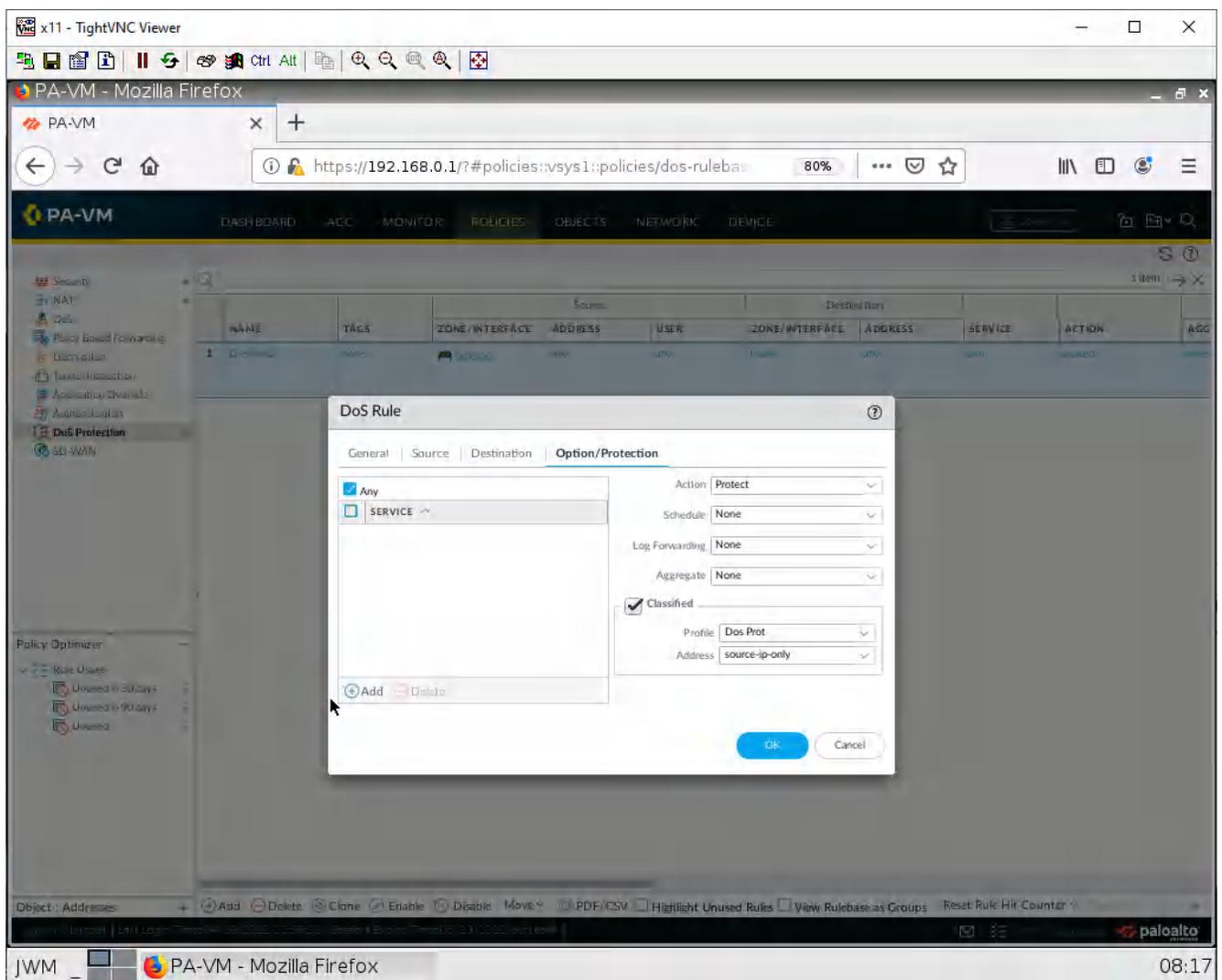


Figure 2.30: DoS Rule – Option/Policies

Then click **OK**.

## Create a Zone Protection Profile

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

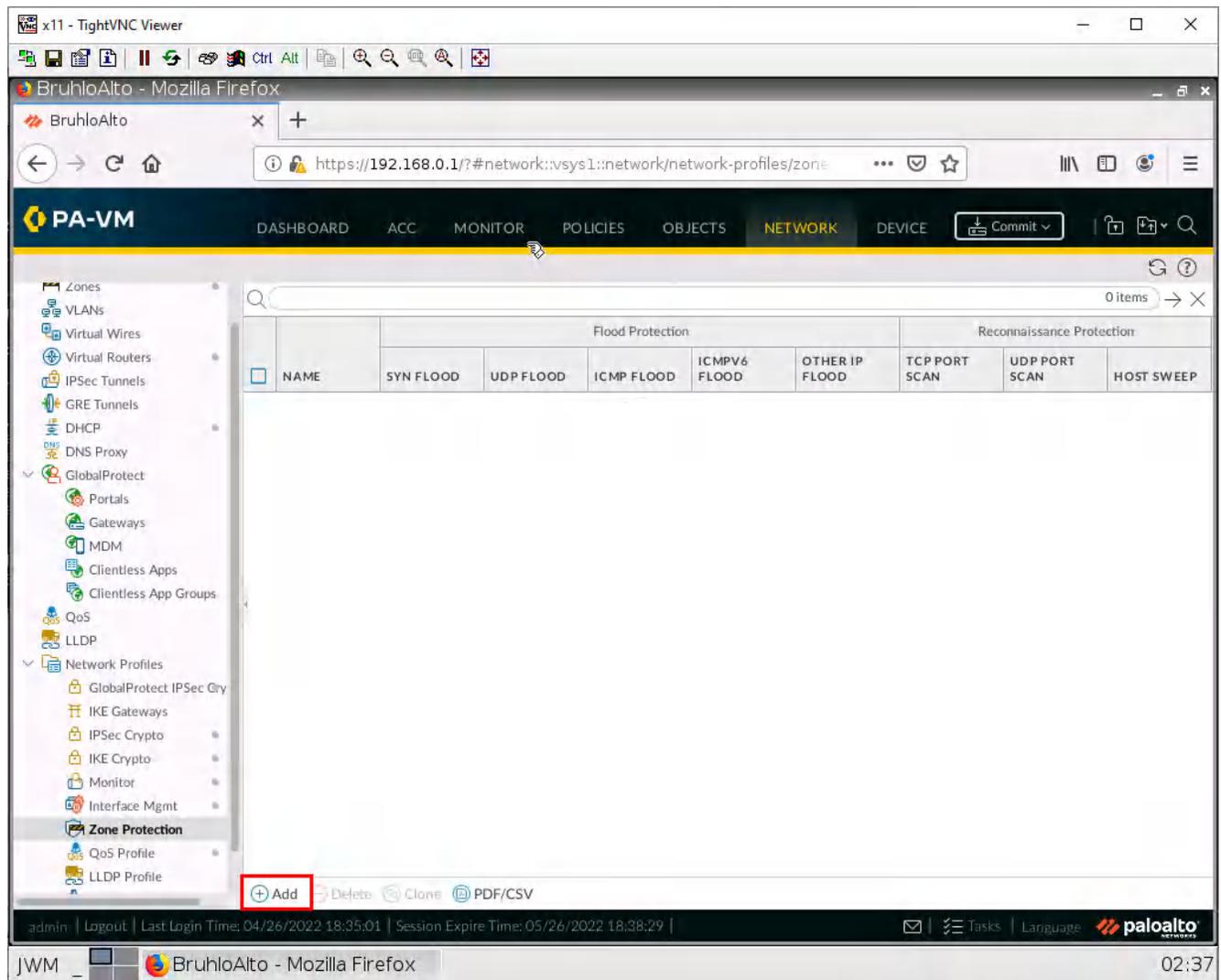


Figure 2.31: Add a Zone Protection

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

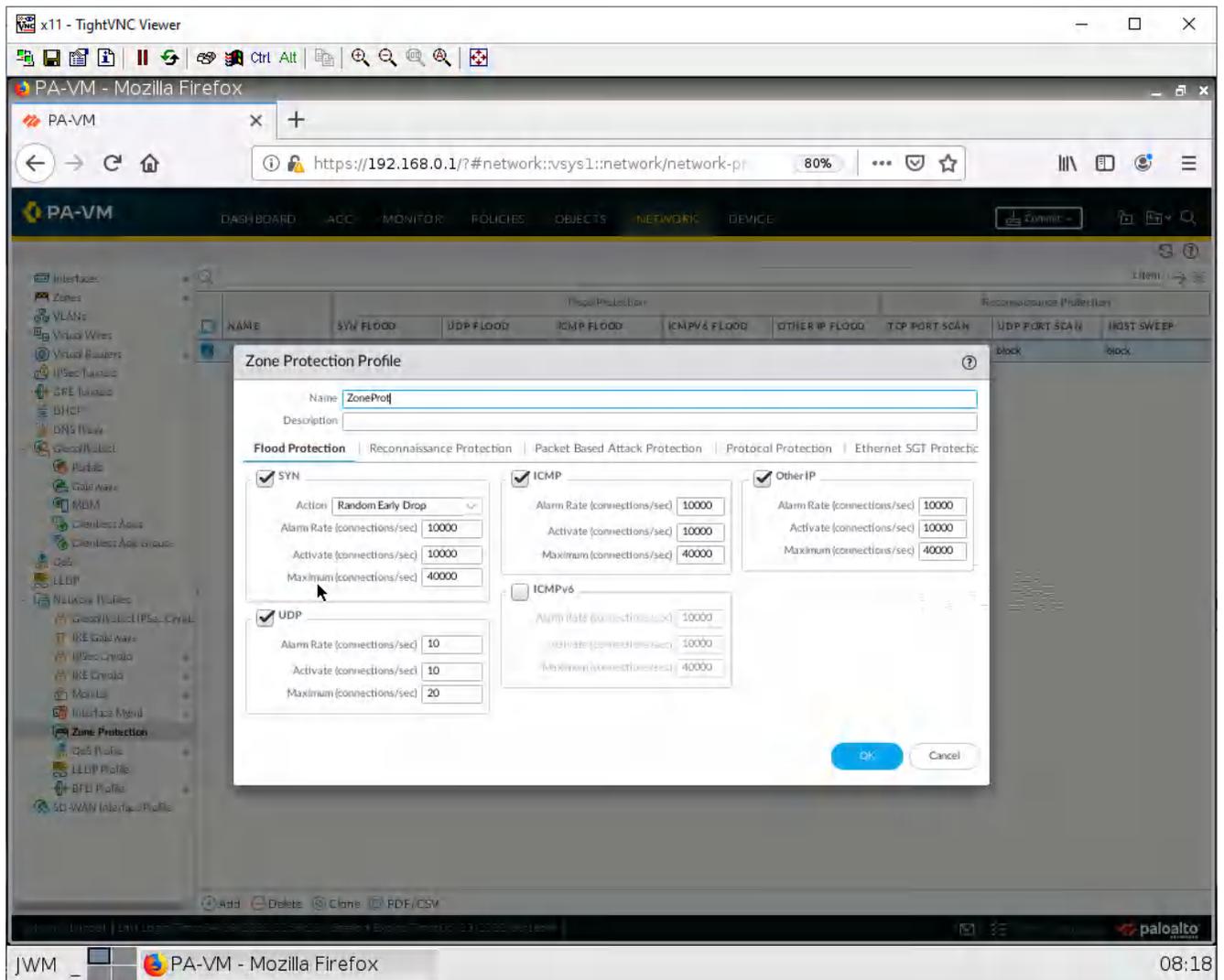


Figure 2.32: Add a Flood Protection

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

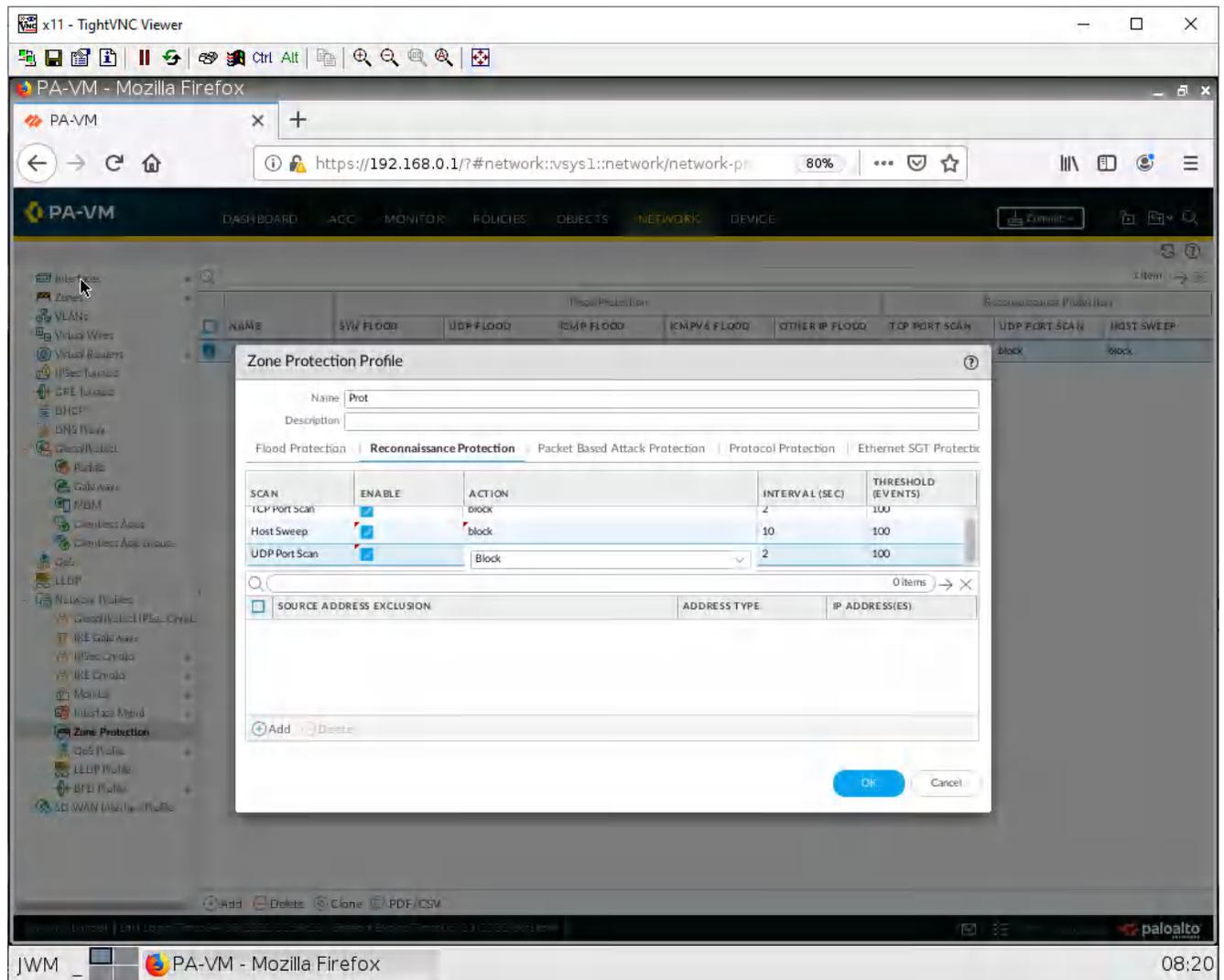


Figure 2.33: Set UDP Port Scan

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

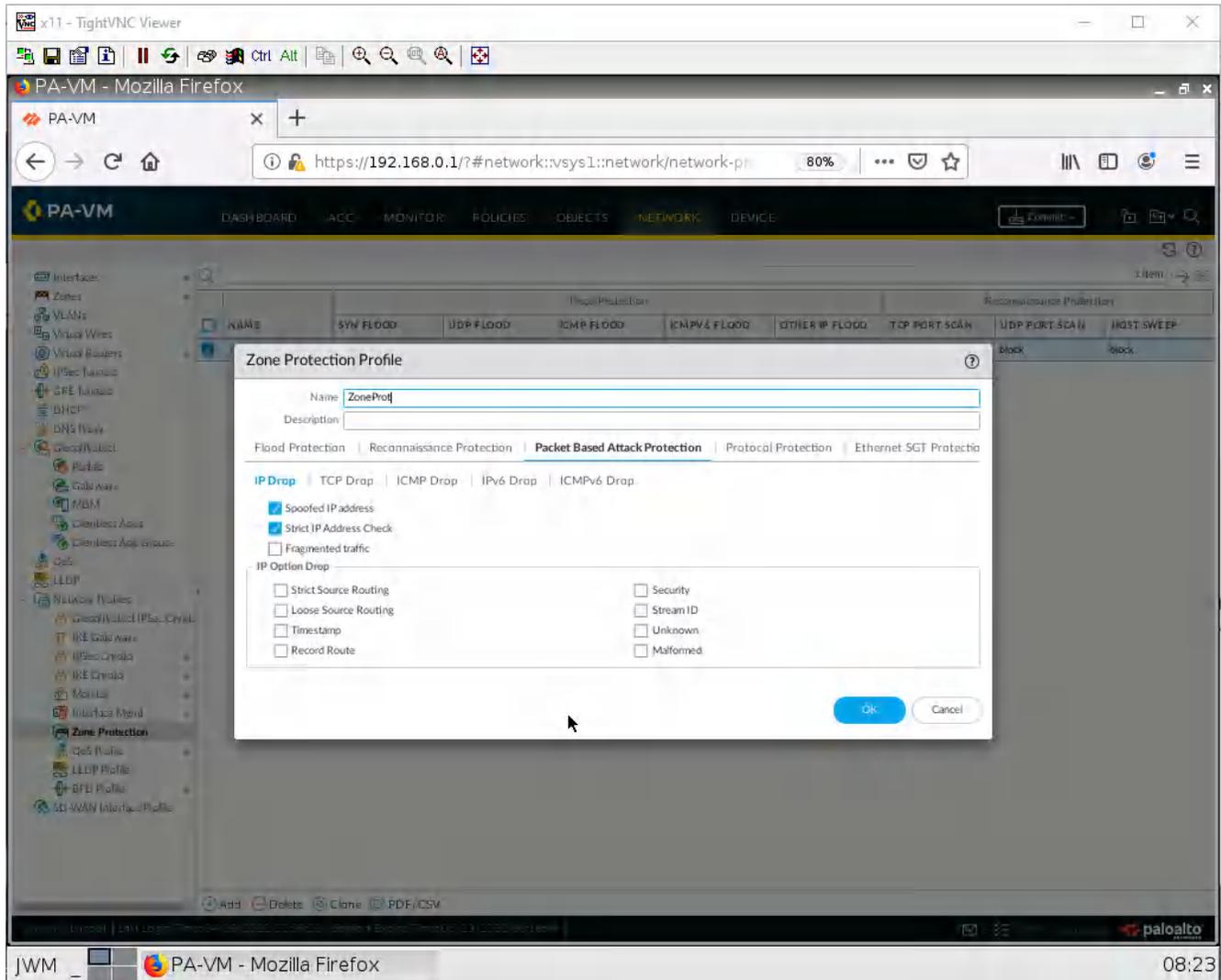


Figure 2.34: Enable Spoof IP address and Strict Address Check

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

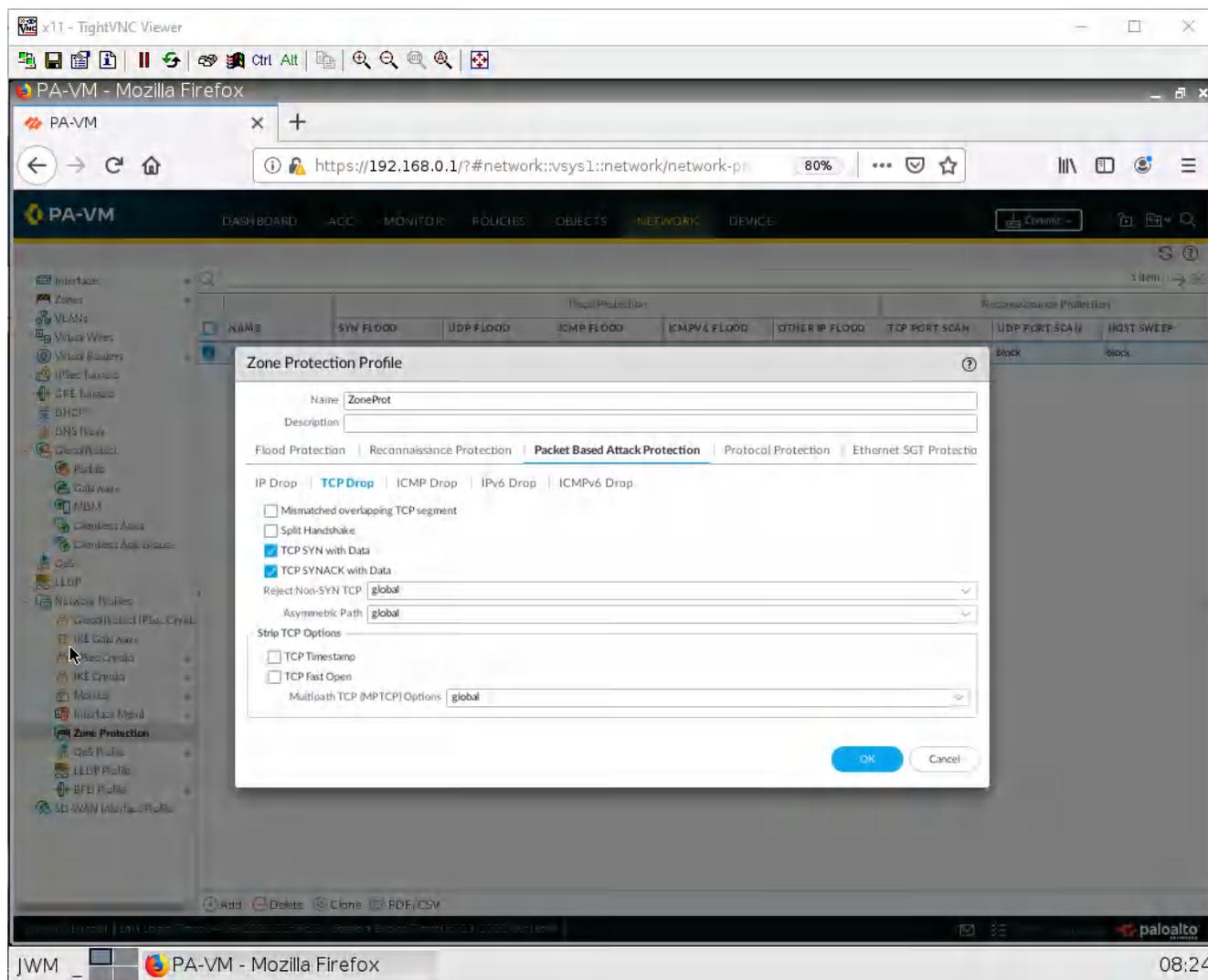


Figure 2.35: Enable TCP SYN with Data

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)**.

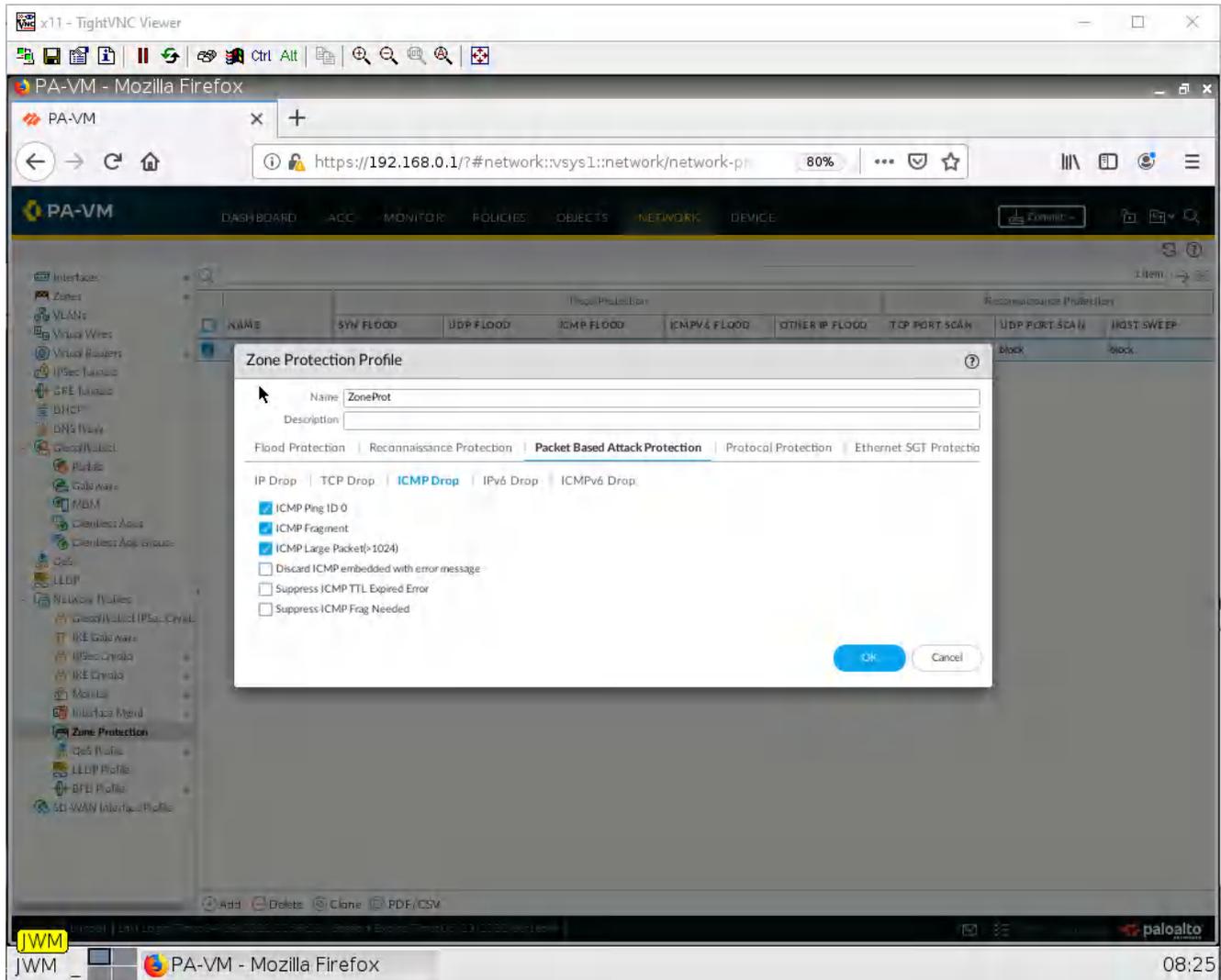


Figure 2.36: Enable ICMP Ping ID 0, ICMP Fragment

Then click **OK**.

## Apply a Zone Protection Profile

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

The screenshot shows the Palo Alto Networks PA-VM web interface. The left sidebar contains a navigation menu with categories like Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, and Network Profiles. The main content area displays a table of zones. The 'Outside' zone is highlighted with a red box.

NAME	TYPE	INTERFA... / VIRTUAL SYSTEMS	ZONE PROTEC... PROFILE	PACKET BUFFER PROTEC...	LOG SETTING	User-ID			Device-ID		
						ENABLED	INCLUD... NETWO...	EXCLUD... NETWO...	ENABLED	INCLUD... NETWO...	EXCLUD... NETWO...
Inside	layer3	ethernet1...		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
Outside	layer3	ethernet1...		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none

At the bottom of the interface, there is a status bar showing the URL, session time (04/26/2022 18:35:01), session expire time (05/26/2022 18:38:29), and the Palo Alto Networks logo. The user's name 'JWM' and the time '02:38' are also visible.

Figure 2.37: Create an Outside zone

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

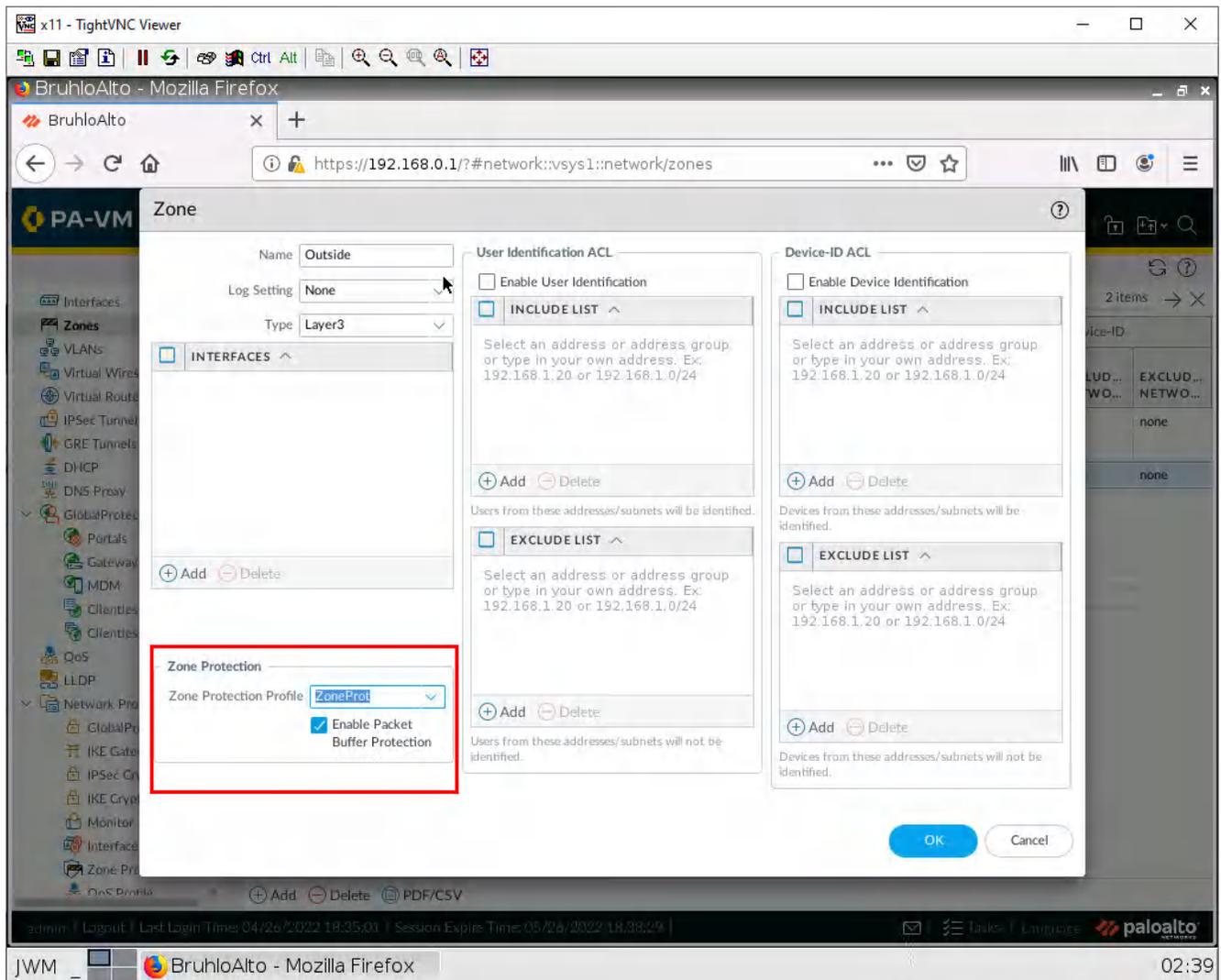


Figure 2.38: Enable Zone Protection under Outside Zone

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.

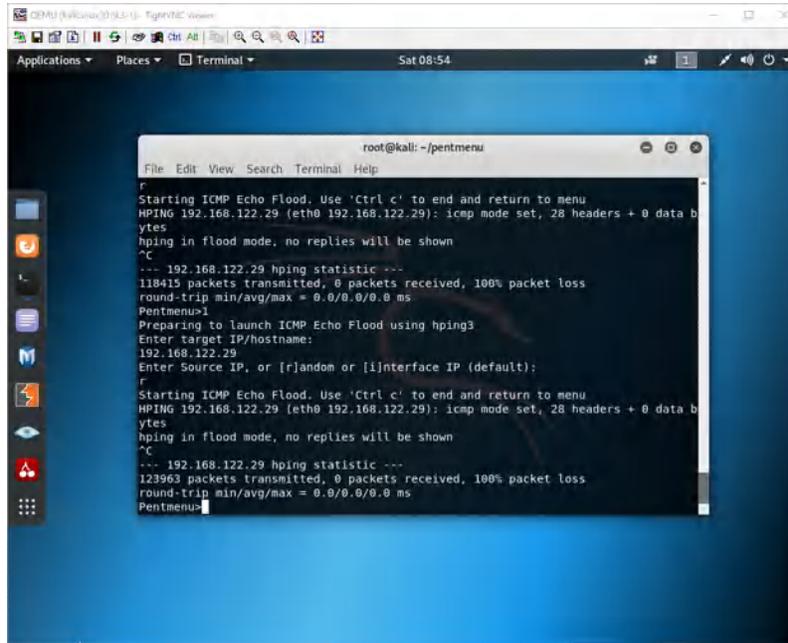


Figure 2.39: Running PentMenu

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

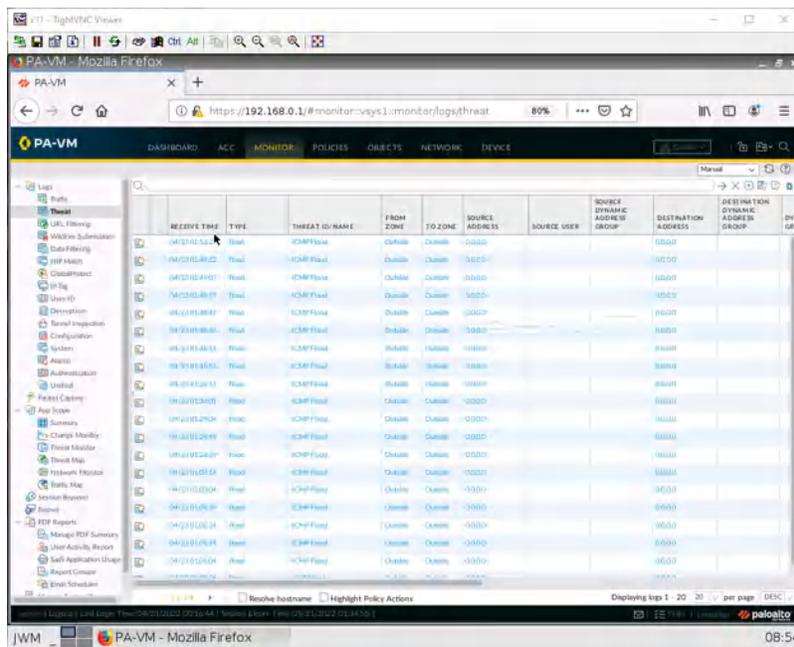


Figure 2.40: Verify logs

## 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 antispysware solution. We’ll also be “testing” wildfire. A feature that thwarts new exploits from happening.

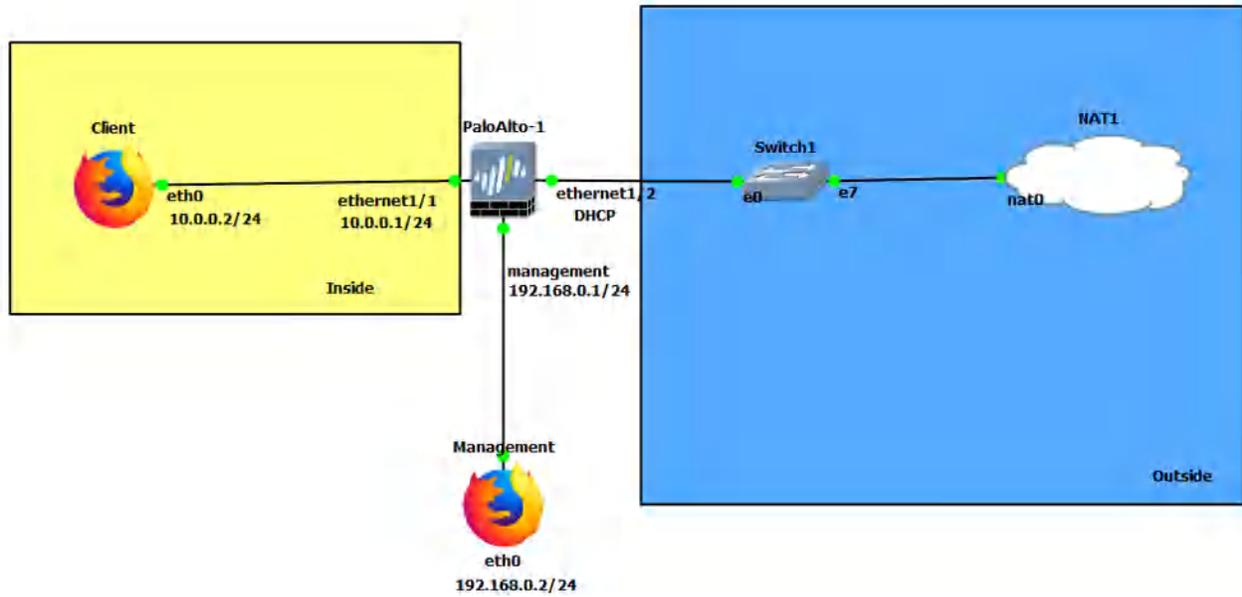


Figure 2.41: Main scenario

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

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

The screenshot shows the Palo Alto VM console interface. The left sidebar displays a tree view of configuration objects, with 'Security Profiles' expanded to show 'Antivirus'. The main content area displays a table of Antivirus profiles. The 'default' profile is selected, and the 'Clone' button at the bottom is highlighted with a red box.

NAME	LOCA...	PACKET CAPTU...	Decoders				Application Exceptions		WildFire Inline ML		SIGNATURE EXCEPTIONS	WILD FIRE IN LINE ML EXCEPTIONS
			PROT...	SIGNA... ACTIO...	WILD... SIGNA... ACTIO...	WILD... IN LINE ML ACTIO...	APPLI...	ACTIO...	MODEL	ACTIO... SETTI...		
<input checked="" type="checkbox"/> default	Predef...	<input type="checkbox"/>	http	default (reset-both)	default (reset-both)	default (reset-both)			Windo... Execut...	enable (inherit per-protocol actions)	0	0
			http2	default (reset-both)	default (reset-both)	default (reset-both)			Power... Script 1	enable (inherit per-protocol actions)		
			smtp	default (alert)	default (alert)	default (alert)			Power... Script 2	enable (inherit per-protocol actions)		
			imap	default (alert)	default (alert)	default (alert)			Execut... Linked Format	enable (inherit per-protocol actions)		
			pop3	default (alert)	default (alert)	default (alert)			MSOffi...	enable (inherit per-protocol actions)		
			ftp	default (reset-both)	default (reset-both)	default (reset-both)						

Buttons: Add, Delete, Clone, PDF/CSV

Threat Prevention License required for antivirus, anti-spyware, and vulnerability protection to function.

Session Info: Time: 04/26/2022 18:35:01 | Session Expire Time: 05/26/2022 18:38:29

Language: paloalto

Figure 2.42: Creating an Antivirus Profile

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

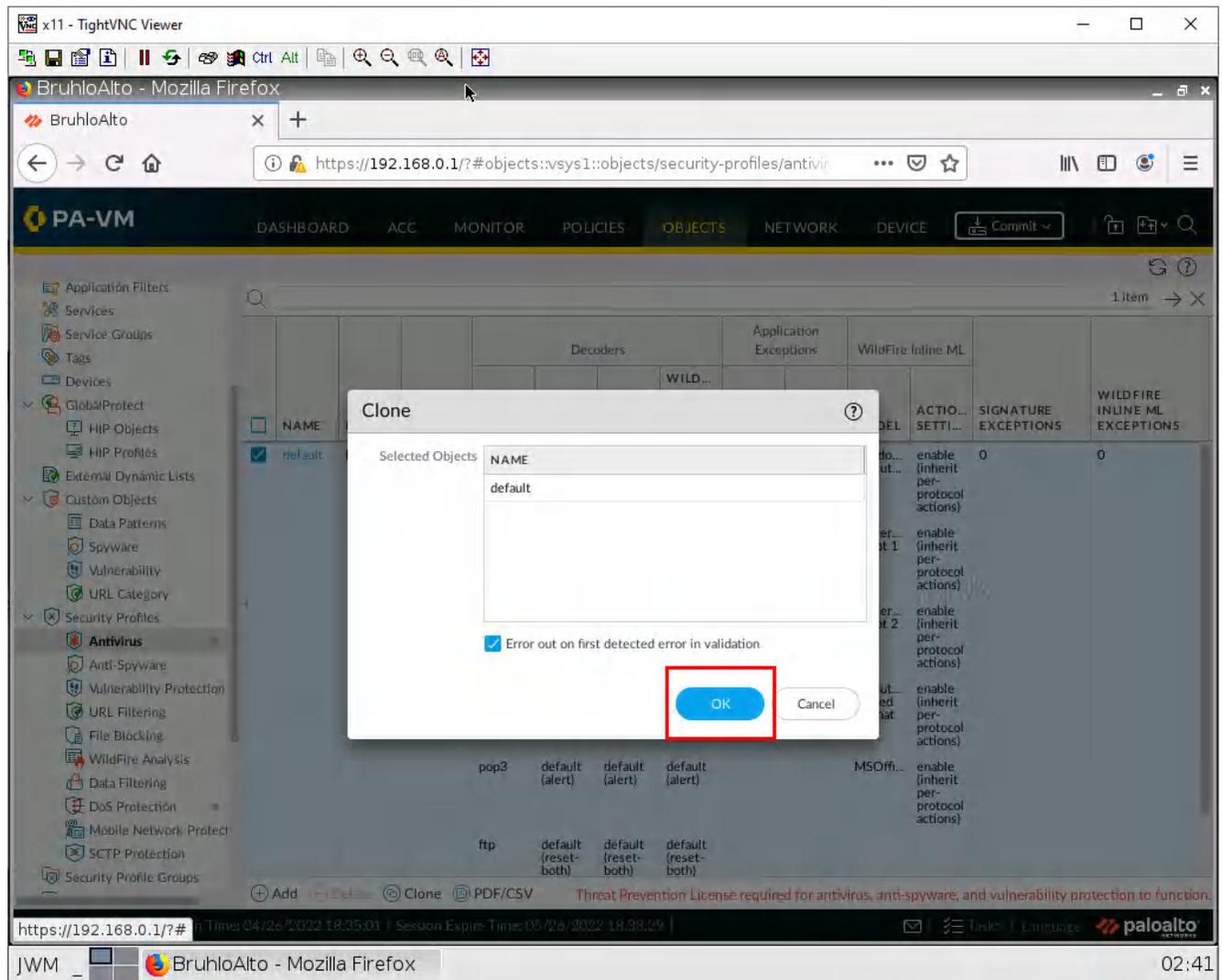


Figure 2.43: Cloning the Antivirus profile

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

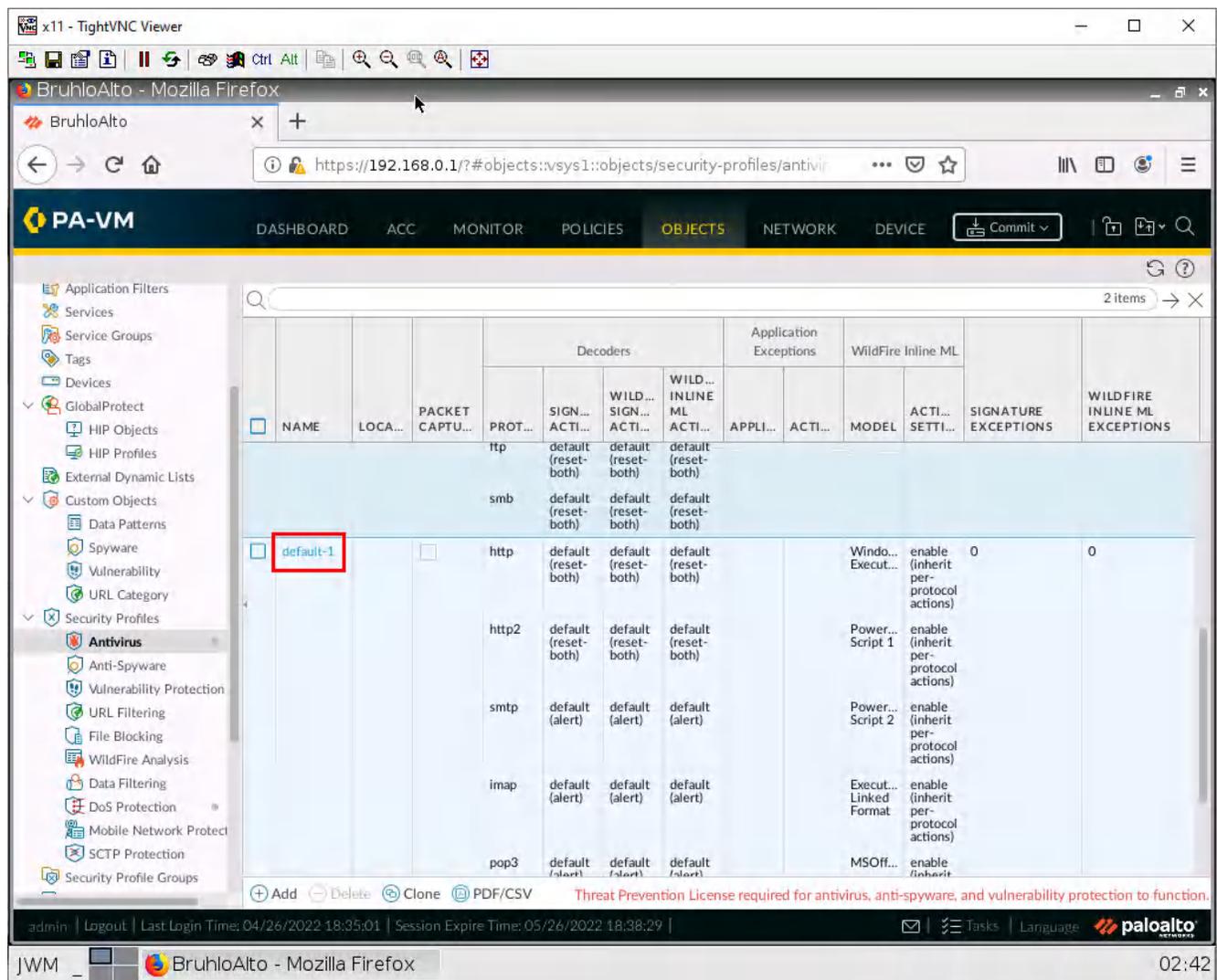


Figure 2.44: Verify the Antivirus profile

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

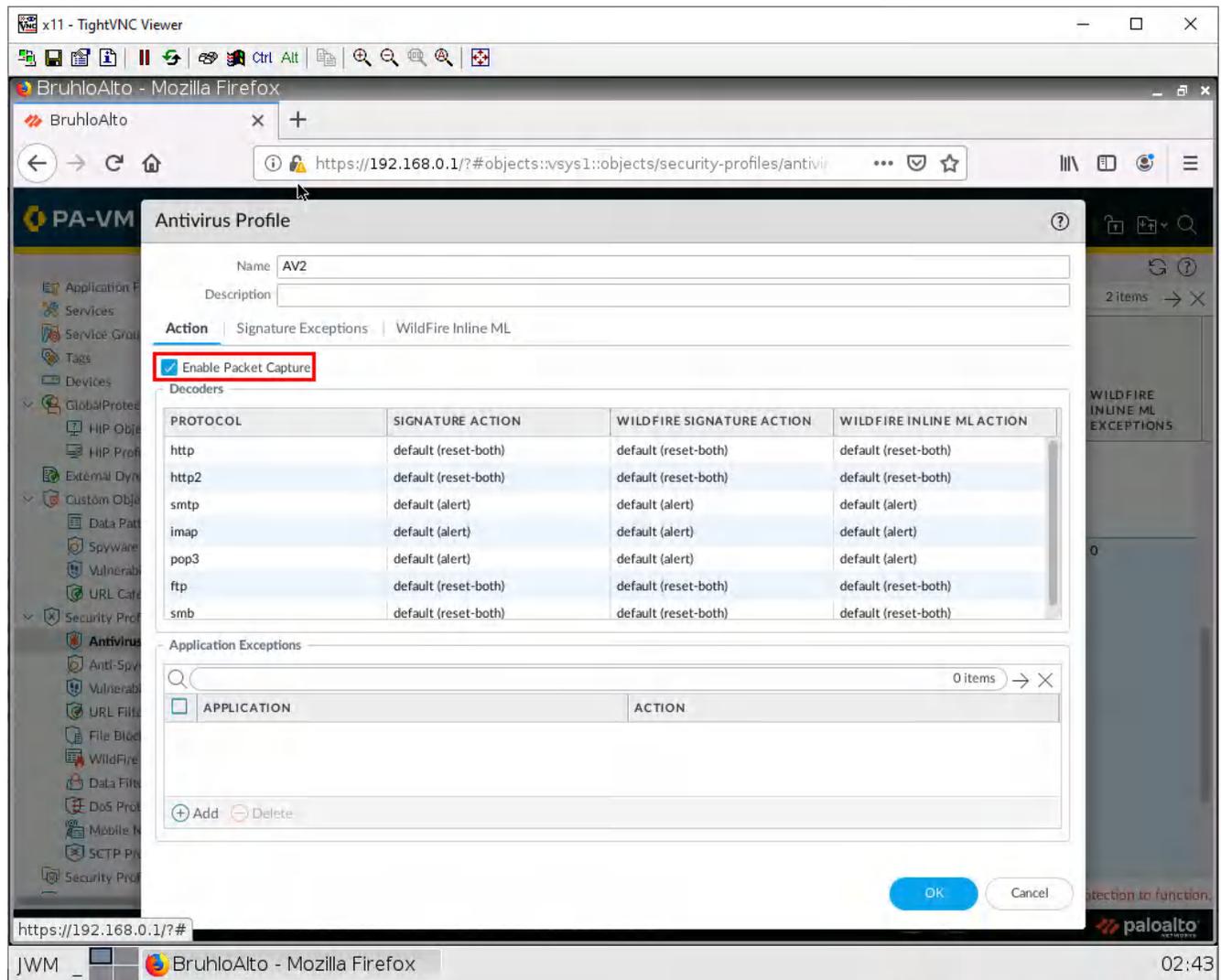


Figure 2.45: Enable Packet Captures under Antivirus Profile

Then press **OK**.

## Create an Anti-Spyware Profile

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

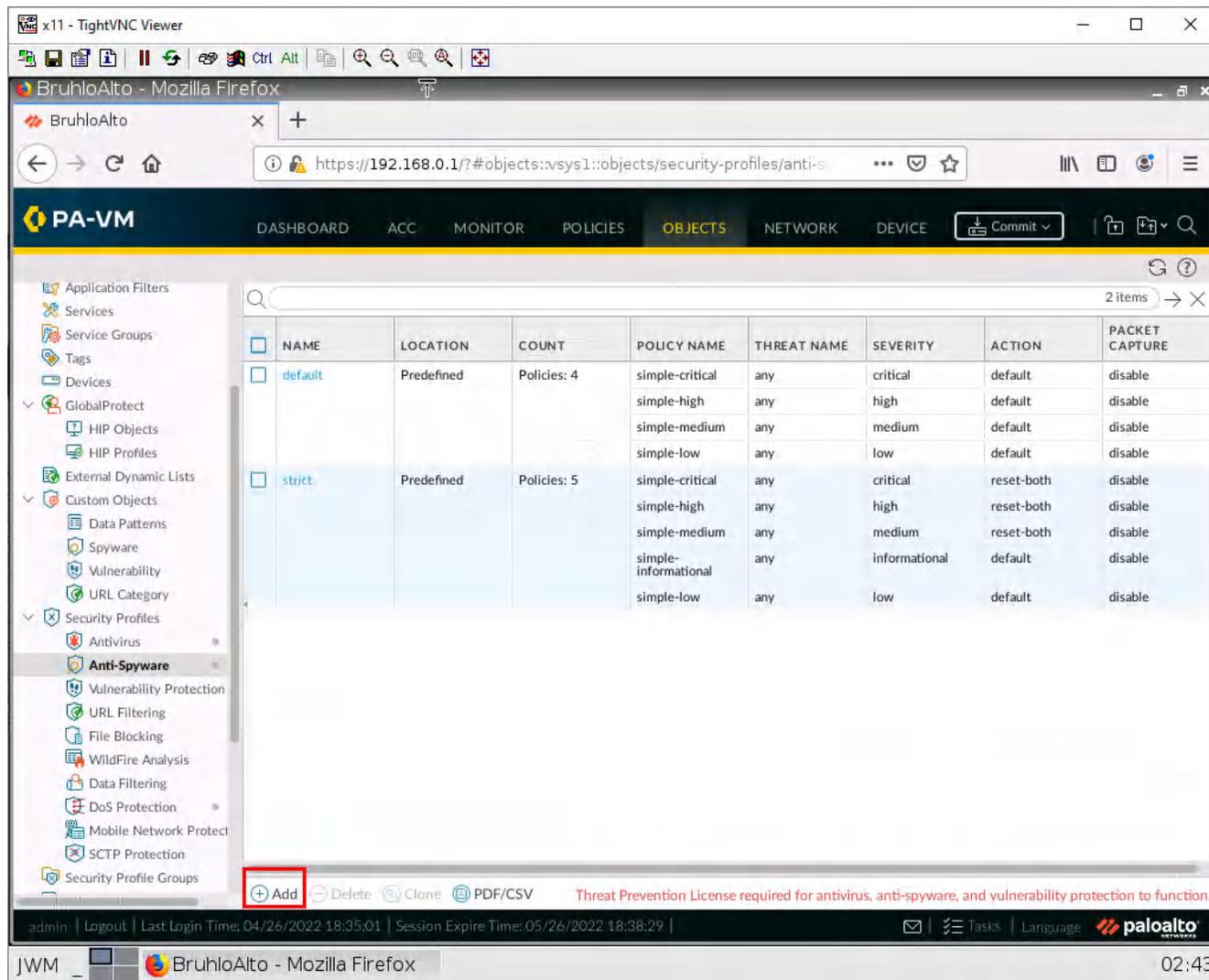


Figure 2.46: Add an Anti-Spyware Profile

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: <i>Drop</i> Severity: <i>Critical, High</i>

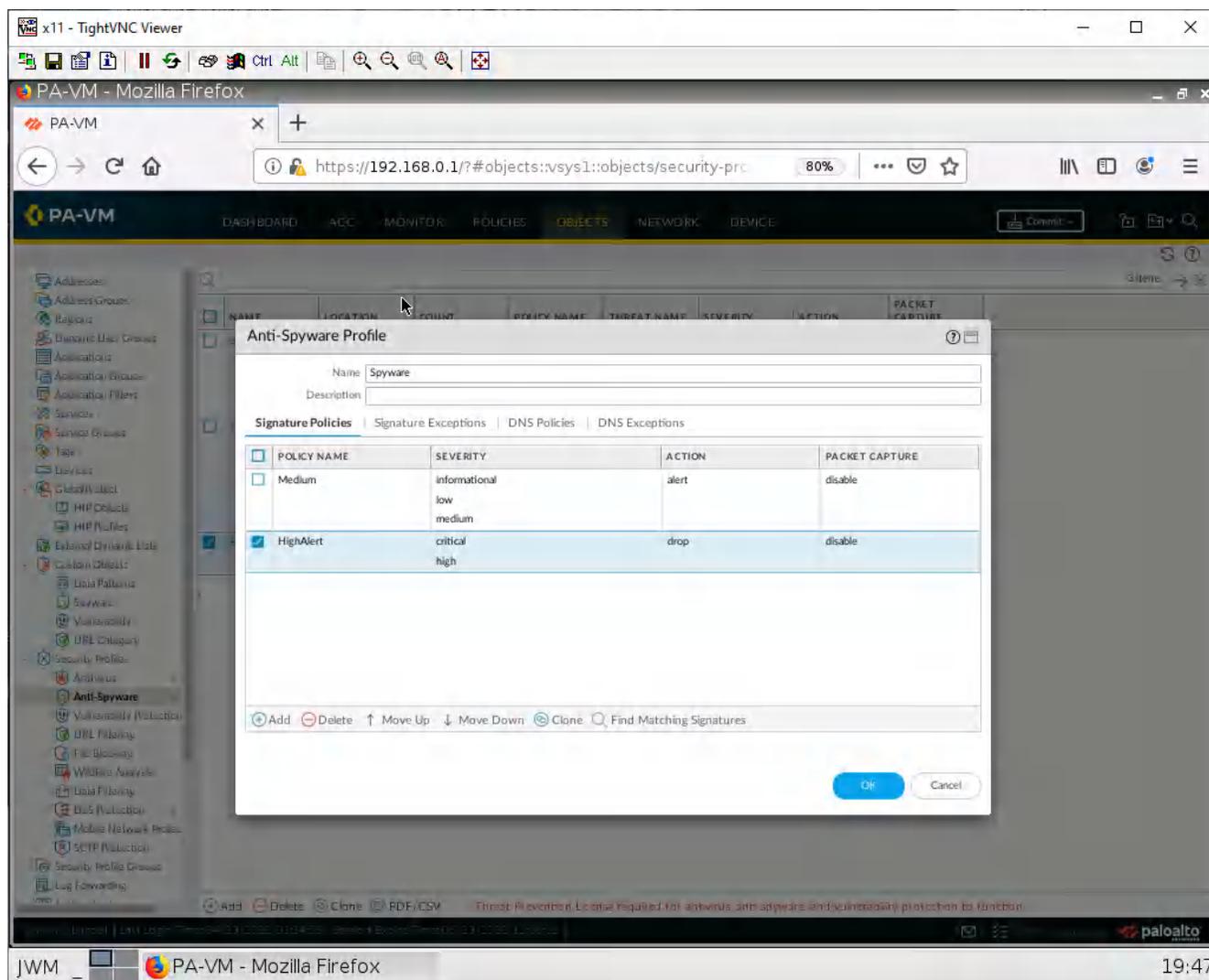


Figure 2.47: Verify an Anti-Spyware Profile

Then press **OK**.

## Create a File Blocking Profile

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

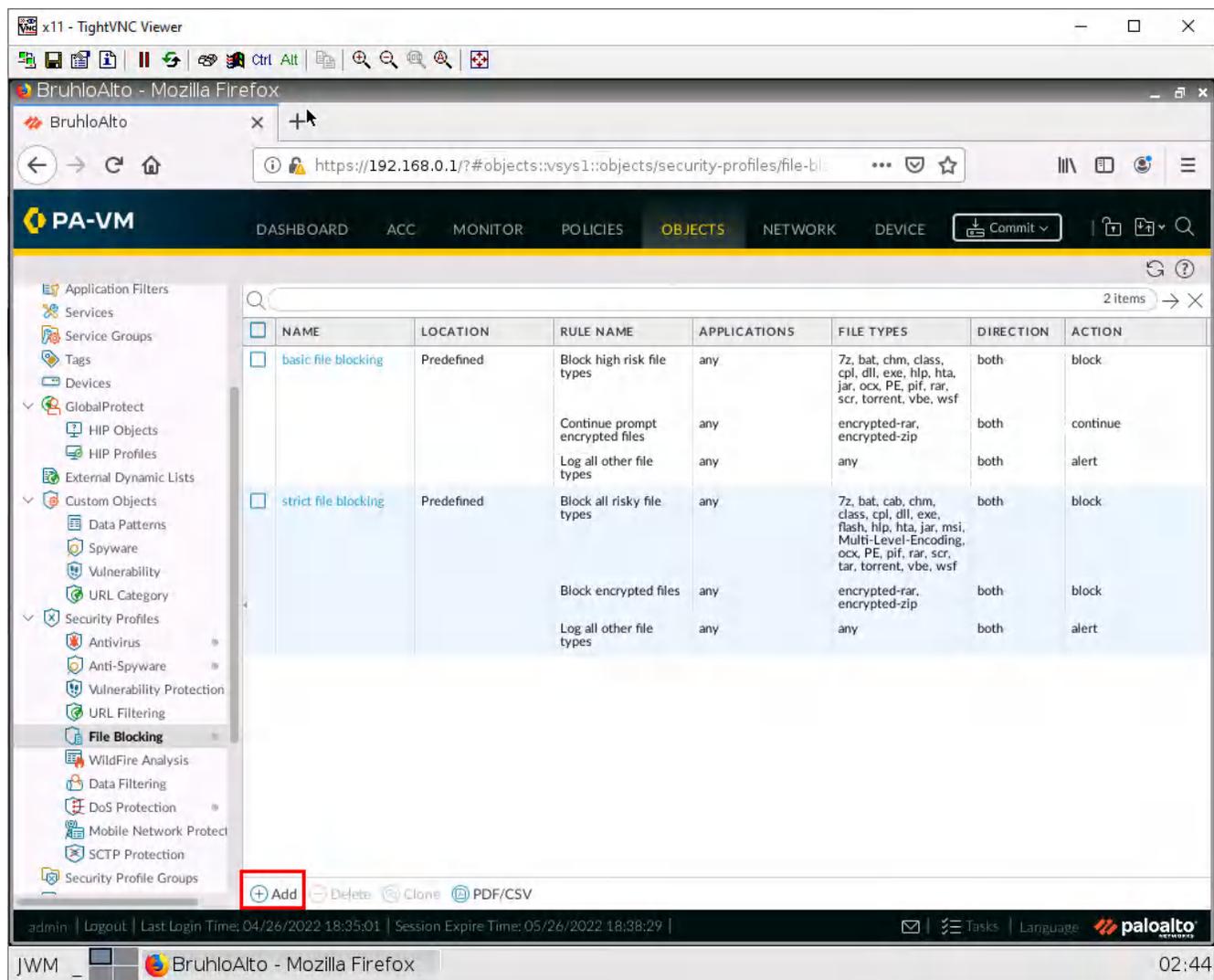


Figure 2.48: Add File blocking Profile

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

Table 2.9: File Blocking Configuration

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

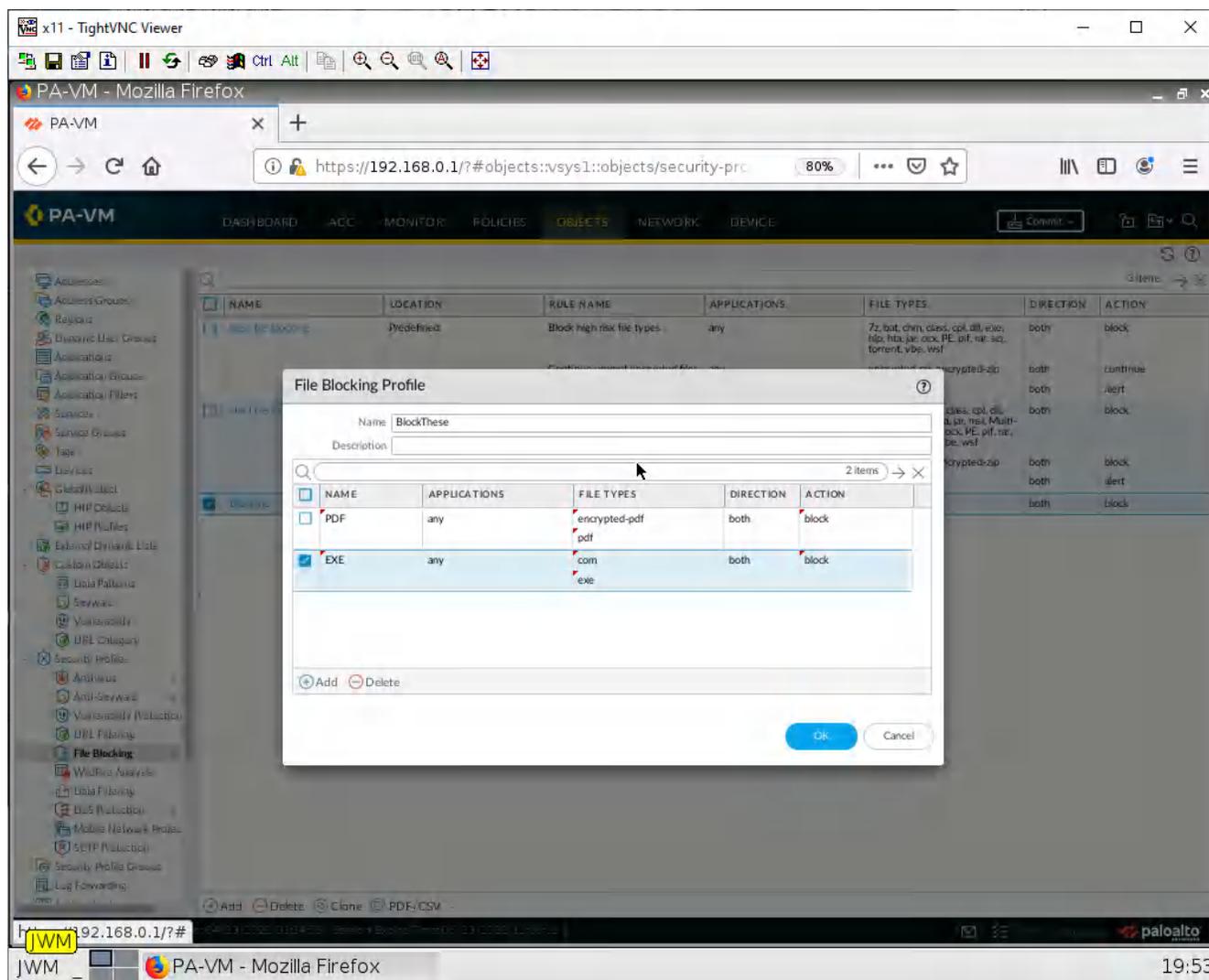


Figure 2.49: Configure the File blocking profile

Then click **OK**.

## Create a WildFire Profile

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

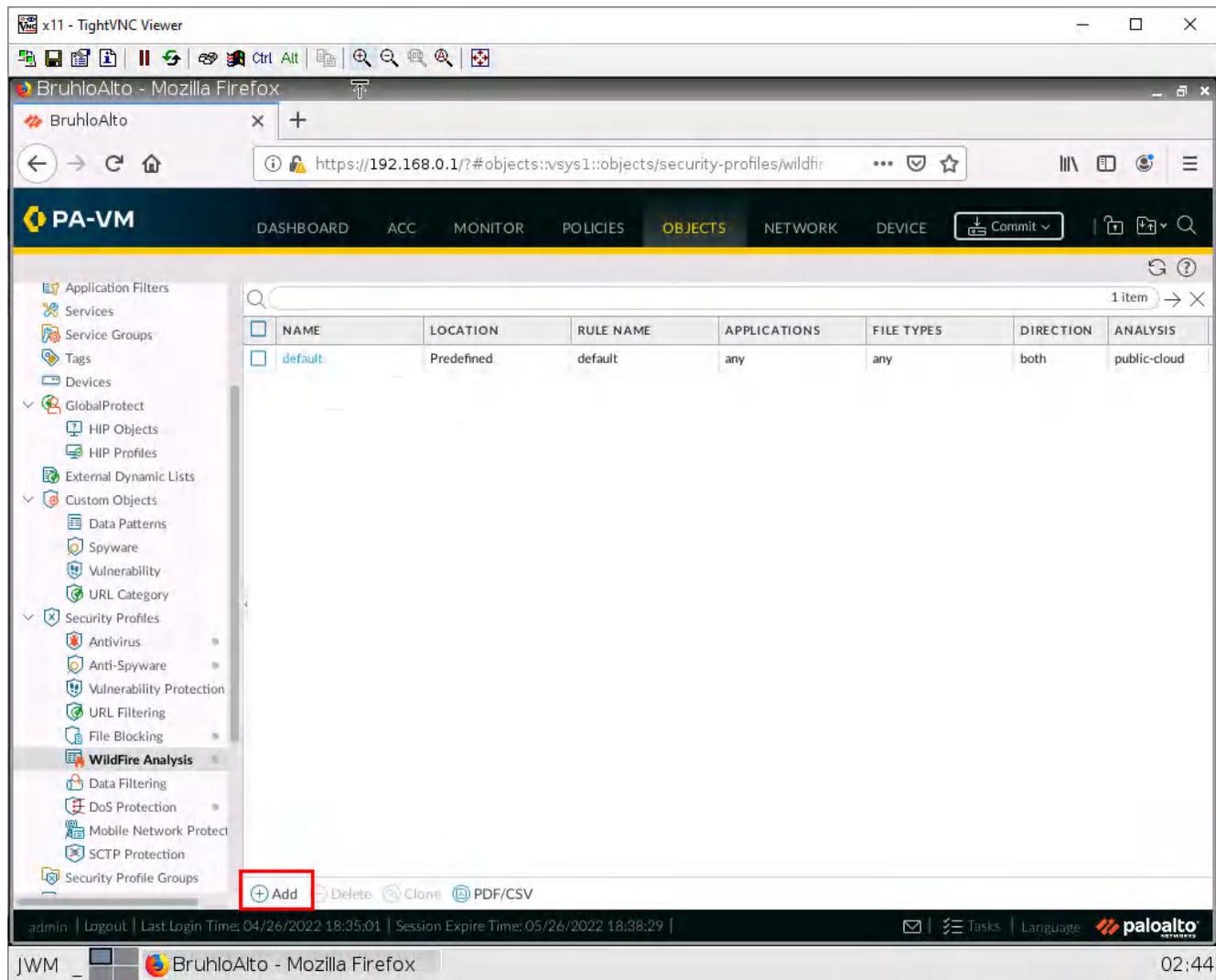


Figure 2.50: Add a WildFire Profile

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>

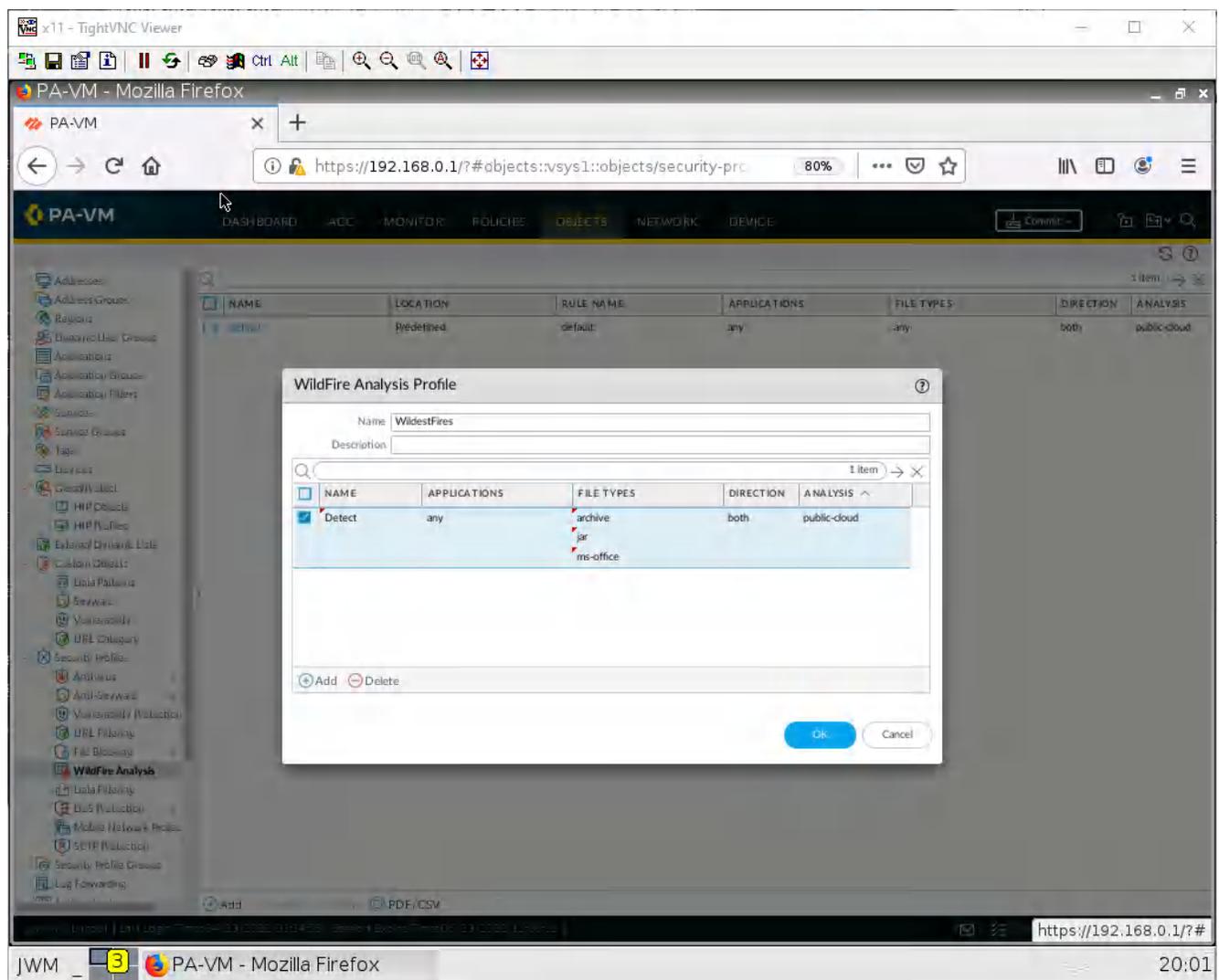


Figure 2.51: Add a WildFire Profile

Then press **OK**.

## Apply Security Profiles to a Security Policy

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

The screenshot shows the Palo Alto VM (PA-VM) web interface. The browser address bar displays `https://192.168.0.1/#policies::vsys1::policies/security-rulebase`. The interface includes a navigation menu with options like DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The 'POLICIES' tab is active, and the 'Security' section is expanded, showing a list of policies. A table displays the following data:

	NAME	TAGS	TYPE	Source				
				ZONE	ADDRESS	USER	DEVICE	ZONE
1	IntoOut	none	universal	Inside	any	any	any	Outside
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)
3	interzone-default	none	interzone	any	any	any	any	any

The 'IntoOut' policy (row 1) is highlighted with a red box. Below the table, there is a 'Policy Optimizer' section with various options like 'New App Viewer', 'Rules Without App Controls', and 'Rule Usage'. At the bottom, there are action buttons such as 'Add', 'Delete', 'Clone', 'Override', 'Revert', 'Enable', 'Disable', 'Move', 'PDF/CSV', and 'Highlight Unused Rules'. The user 'admin' is logged in, and the session expires on 05/26/2022 at 18:38:29. The Palo Alto logo is visible in the bottom right corner.

Figure 2.52: Add a Security Policy

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

**Table 2.11: Security Policy Actions Configuration**

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

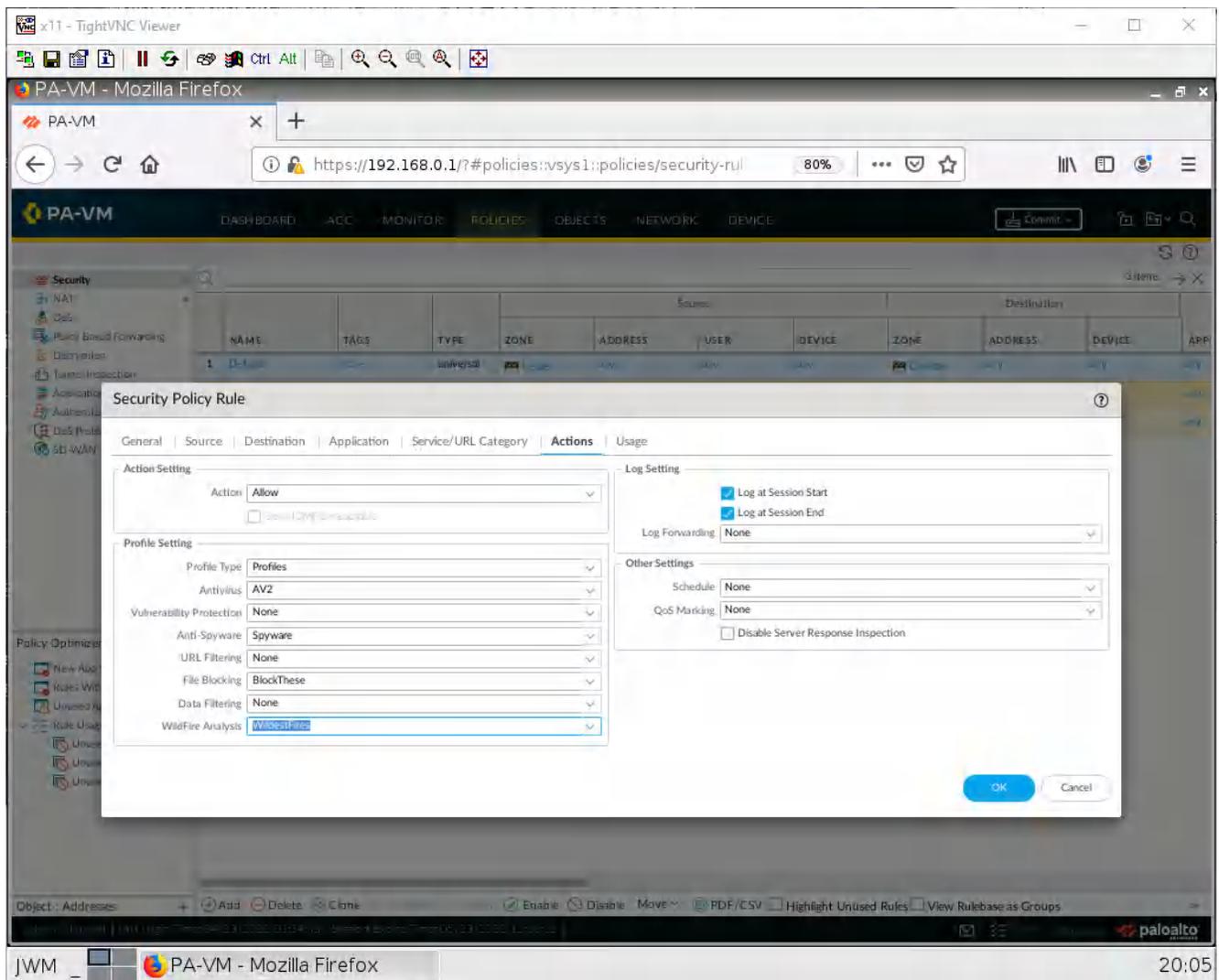


Figure 2.53: Assigning security profiles

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.

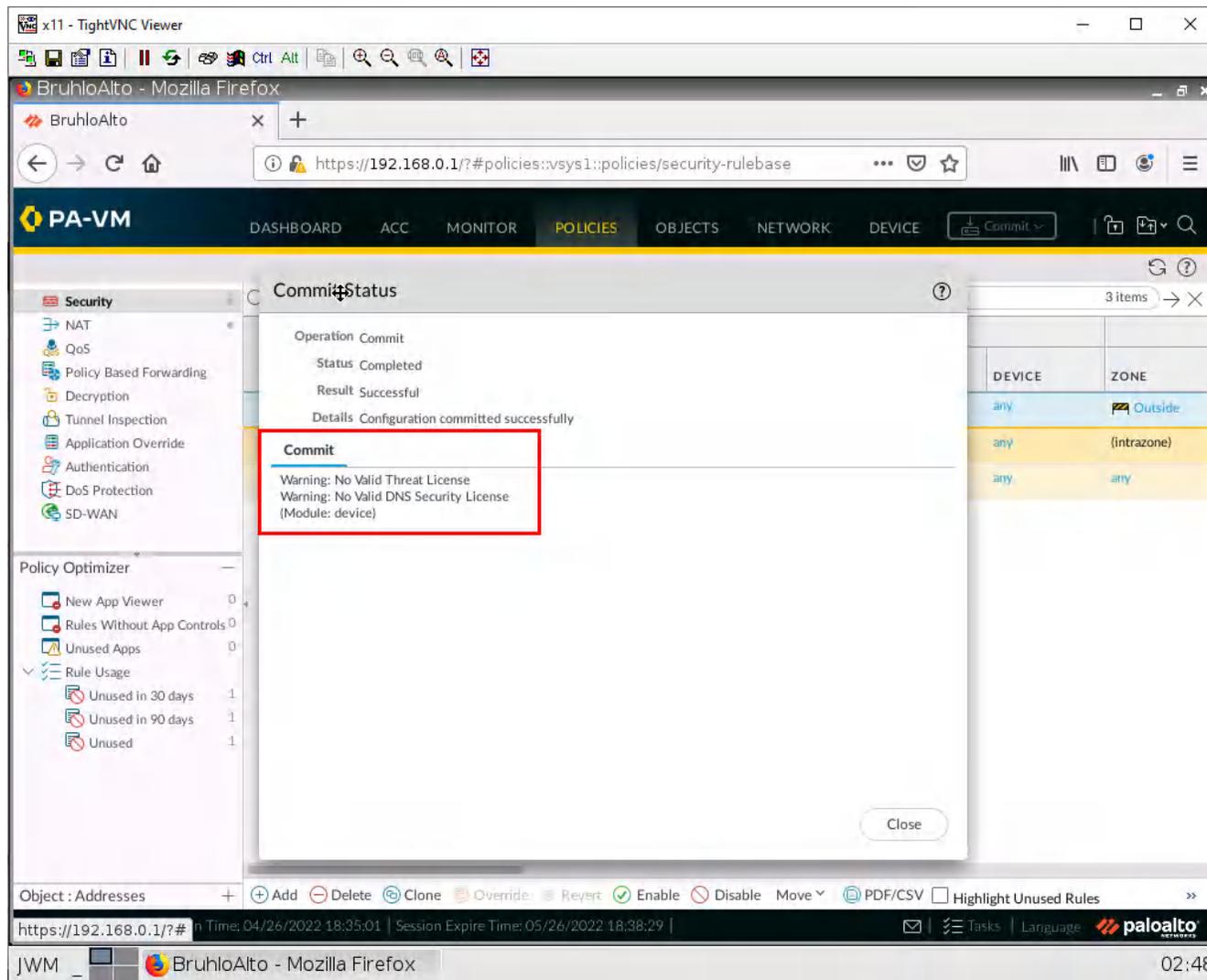


Figure 2.54: Commit the configuration

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 [panedufiles.com](http://panedufiles.com)).

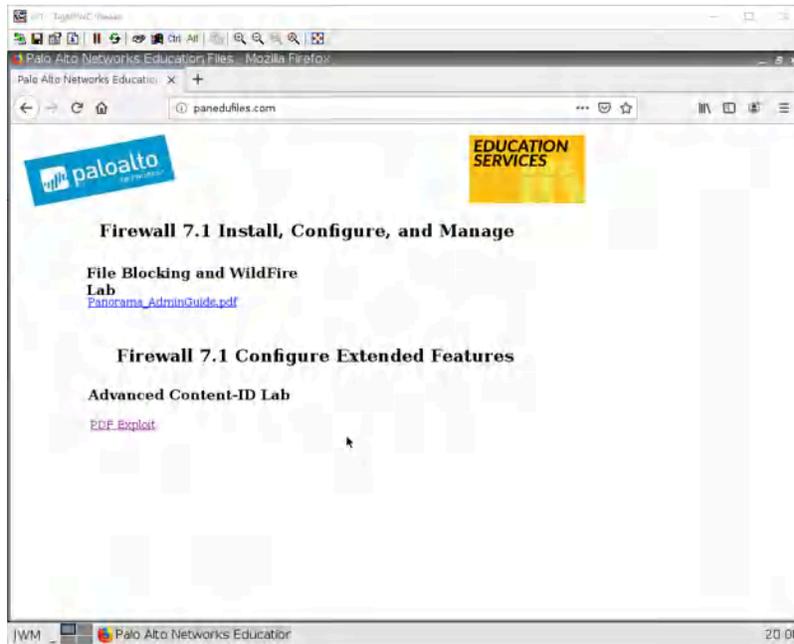


Figure 2.55: Verify the configuration

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

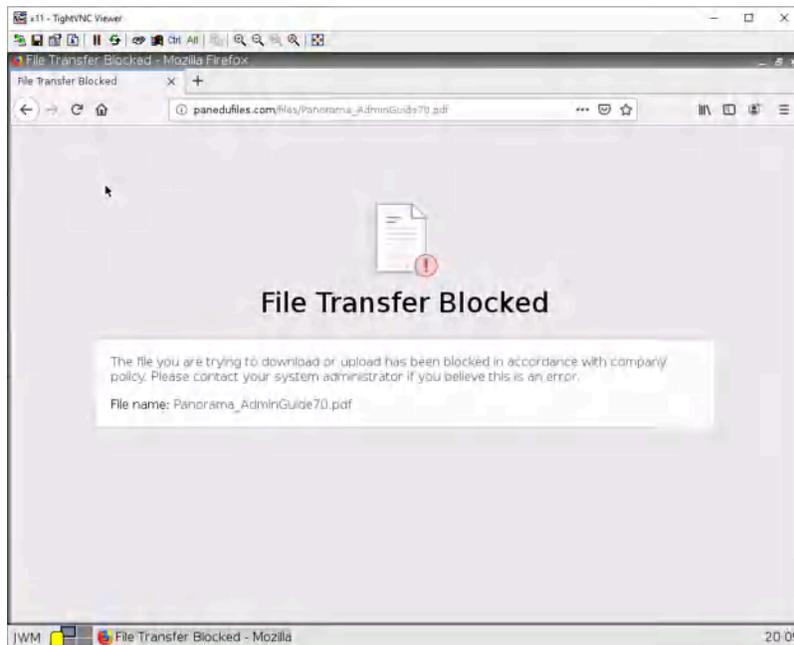


Figure 2.56: File Transfer Blocked

# Chapter 3. Advanced Networking



## 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.

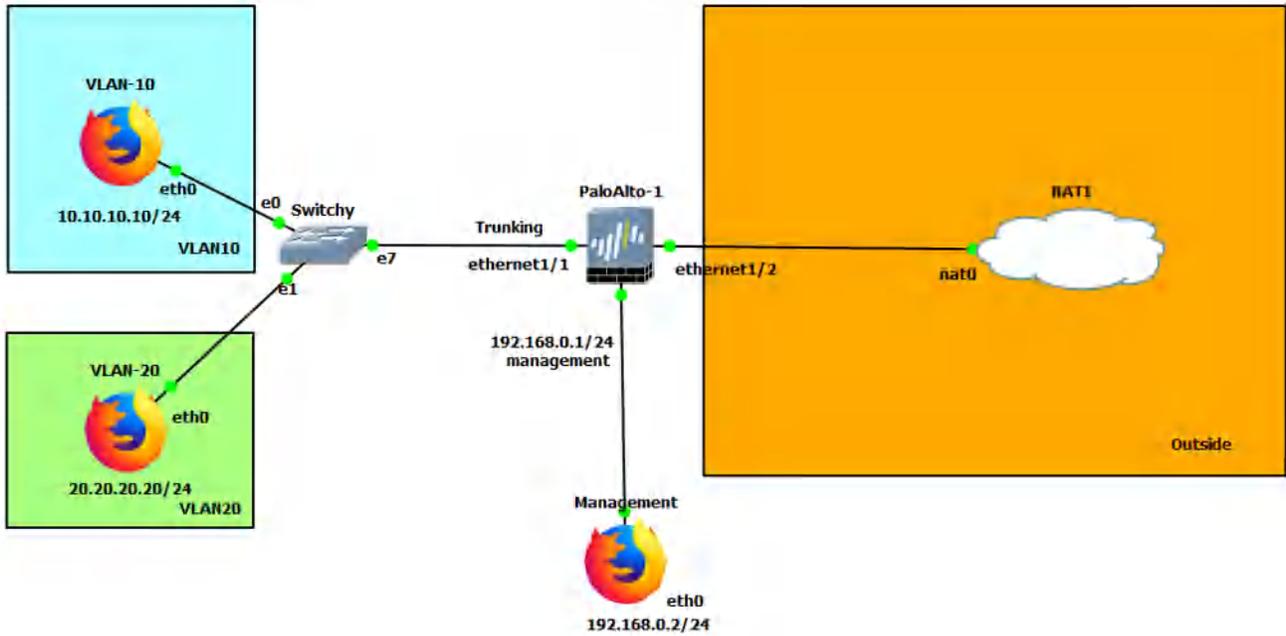


Figure 3.1: Main scenario

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**.

The screenshot shows the Palo Alto VM configuration interface in a web browser. The left sidebar displays the navigation menu with 'Interfaces' selected. The main content area shows the 'Ethernet' configuration page with a table of subinterfaces. The 'ethernet1/1' row is highlighted with a red box.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL
ethernet1/1	Layer3			none	none	Untagged	none
ethernet1/2	Layer3			Dynamic-DHCP Client	default	Untagged	none
ethernet1/3				none	none	Untagged	none
ethernet1/4				none	none	Untagged	none
ethernet1/5				none	none	Untagged	none
ethernet1/6				none	none	Untagged	none
ethernet1/7				none	none	Untagged	none
ethernet1/8				none	none	Untagged	none

At the bottom of the interface, there are buttons for 'Add Subinterface', 'Delete', and 'PDF/CSV'. The bottom status bar shows the user 'admin', session information, and the Palo Alto logo.

Figure 3.2: Ethernet 1/1 configuration

In this window, we just want to set the interface type to **layer 3**.

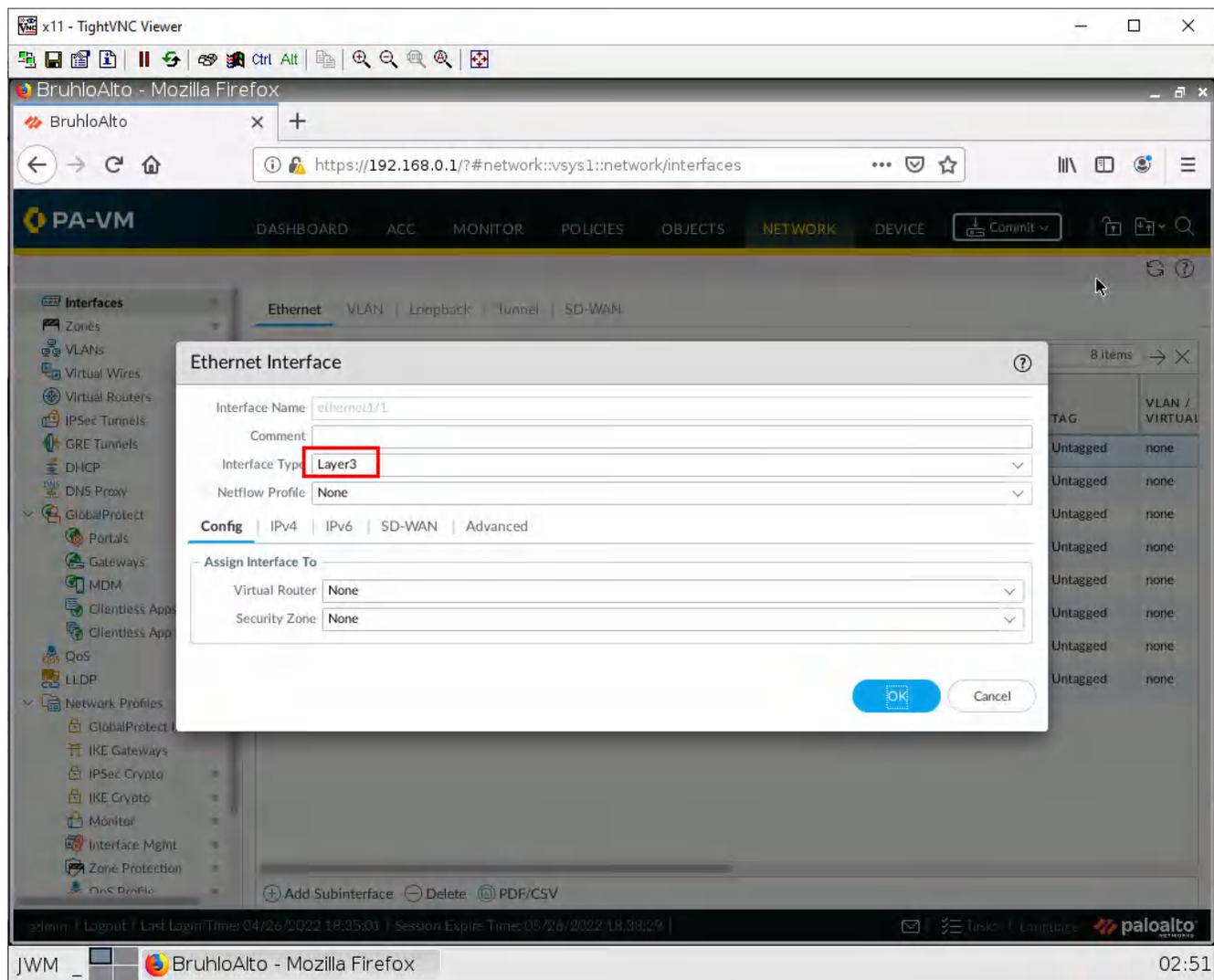


Figure 3.3: Set Interface type to Layer3

Then press **OK**.

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

The screenshot shows the Palo Alto VM configuration interface in a Mozilla Firefox browser window. The URL is `https://192.168.0.1/?#network::vsys1::network/interfaces`. The interface is currently set to "Ethernet". A table lists 8 Ethernet subinterfaces (ethernet1/1 through ethernet1/8). The "Add Subinterface" button at the bottom left is highlighted with a red box.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL
ethernet1/1	Layer3			none	none	Untagged	none
ethernet1/2	Layer3			Dynamic-DHCP Client	default	Untagged	none
ethernet1/3				none	none	Untagged	none
ethernet1/4				none	none	Untagged	none
ethernet1/5				none	none	Untagged	none
ethernet1/6				none	none	Untagged	none
ethernet1/7				none	none	Untagged	none
ethernet1/8				none	none	Untagged	none

Buttons at the bottom: **+ Add Subinterface** (highlighted), **- Delete**, **PDF/CSV**

Footer: admin | Logout | Last Login Time: 04/26/2022 18:35:01 | Session Expire Time: 05/26/2022 18:38:29 | Tasks | Language | paloalto

Figure 3.4: Add Sub interfaces

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

**Table 3.3: Sub Interface Configuration**

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> – IP: <i>10.10.10.1/24</i>
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> – IP: <i>20.20.20.1/24</i>

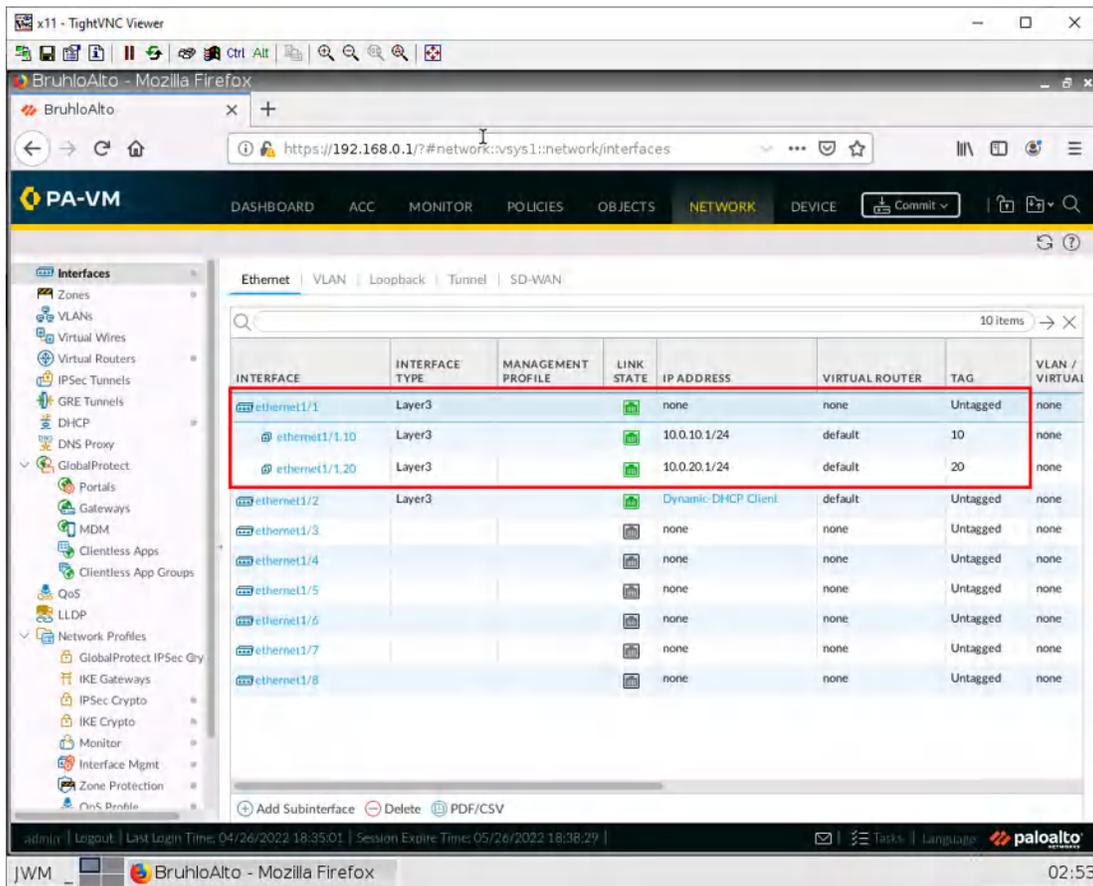


Figure 3.5: Verify Sub interfaces

## Semi-Advanced Security Policies

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

The screenshot shows the Palo Alto VM web interface in Mozilla Firefox. The URL is `https://192.168.0.1/#policies::vsys1::policies/security-rulebase`. The interface displays a list of security policies under the 'Security' tab. The 'Add' button is highlighted with a red box.

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
1	IntoOut	none	universal	Inside	any	any	any	Outside
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)
3	interzone-default	none	interzone	any	any	any	any	any

Object : Addresses + **Add** Delete Clone Override Revert Enable Disable Move PDF/CSV Highlight Unused Rules

admin | Logout | Last Login Time: 04/26/2022 18:35:01 | Session Expire Time: 05/26/2022 18:38:29 | Tasks | Language | paloalto

JWM BruhloAlto - Mozilla Firefox 02:54

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.

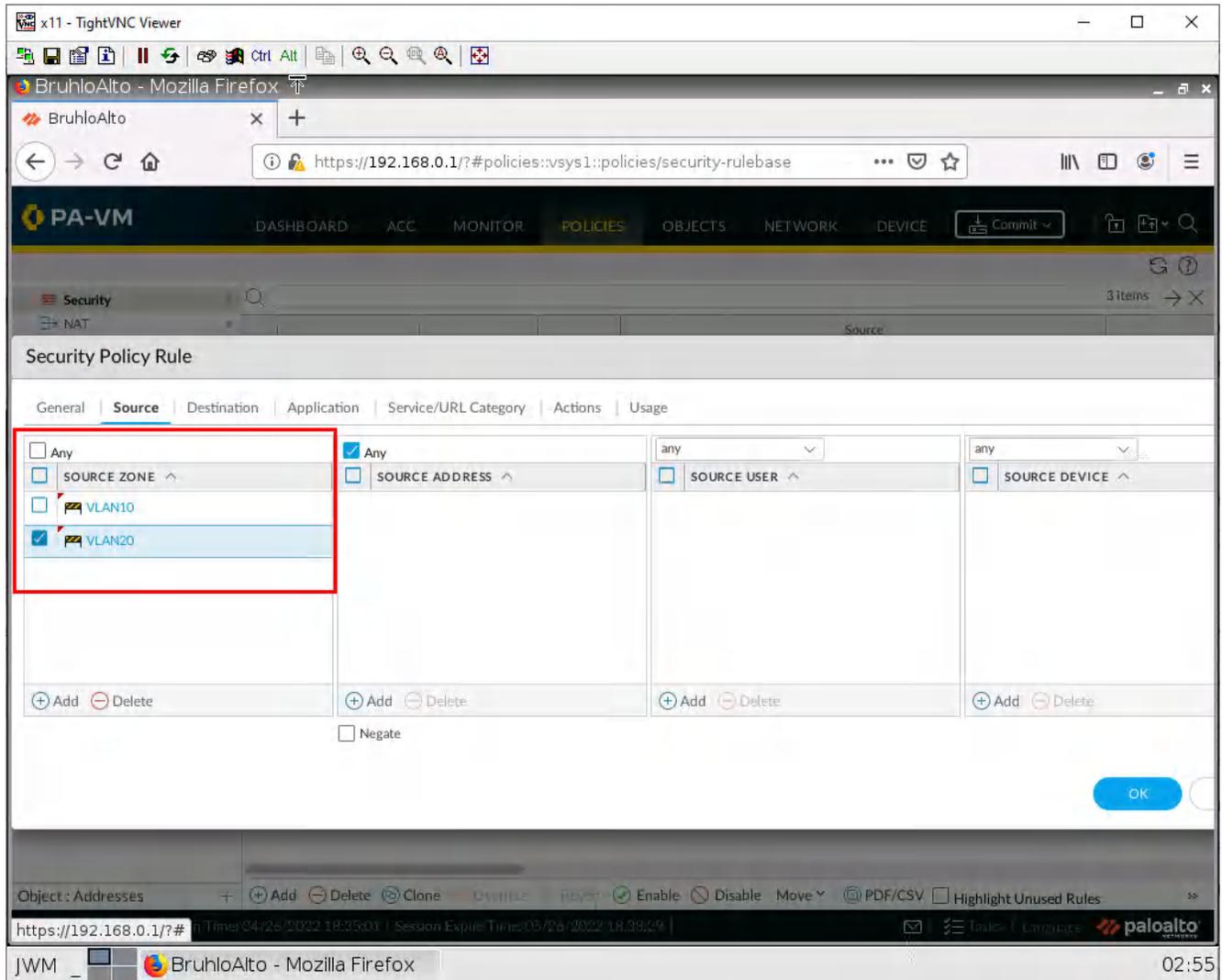


Figure 3.7: Security Policy Rule – Source Zone

Then click **OK**.

## Semi-Advanced NAT Policies

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

The screenshot shows the Palo Alto VM configuration interface in a Mozilla Firefox browser window. The URL is `https://192.168.0.1/?#policies::vsys1::policies/nat-rulebase`. The interface is in the 'POLICIES' section, specifically for NAT. The left sidebar shows a tree view with 'NAT' selected. The main area is a table for NAT rules, currently empty. At the bottom, the 'Object : Addresses' dropdown is open, and the '+ Add' button is highlighted with a red box. Other buttons include 'Delete', 'Clone', 'Enable', 'Disable', 'Move', 'PDF/CSV', 'Highlight Unused Rules', and 'View Rulebase as Groups'. The bottom status bar shows the user 'admin', login time '04/28/2022 20:10:01', session expire time '06/01/2022 00:59:44', and the Palo Alto logo.

NAME	TAGS	Original Packet					
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SE...

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.

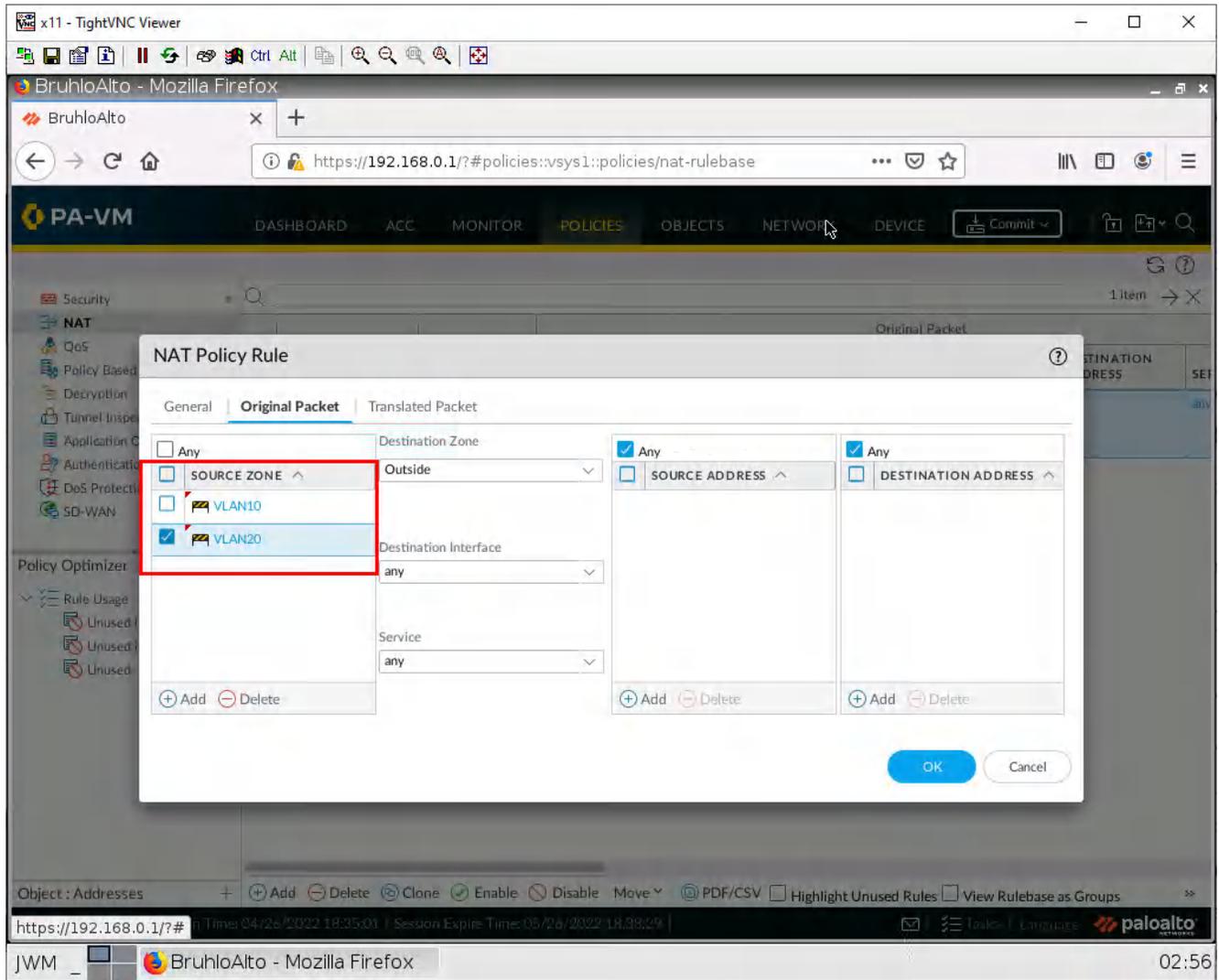


Figure 3.9: Select the Source Zone

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

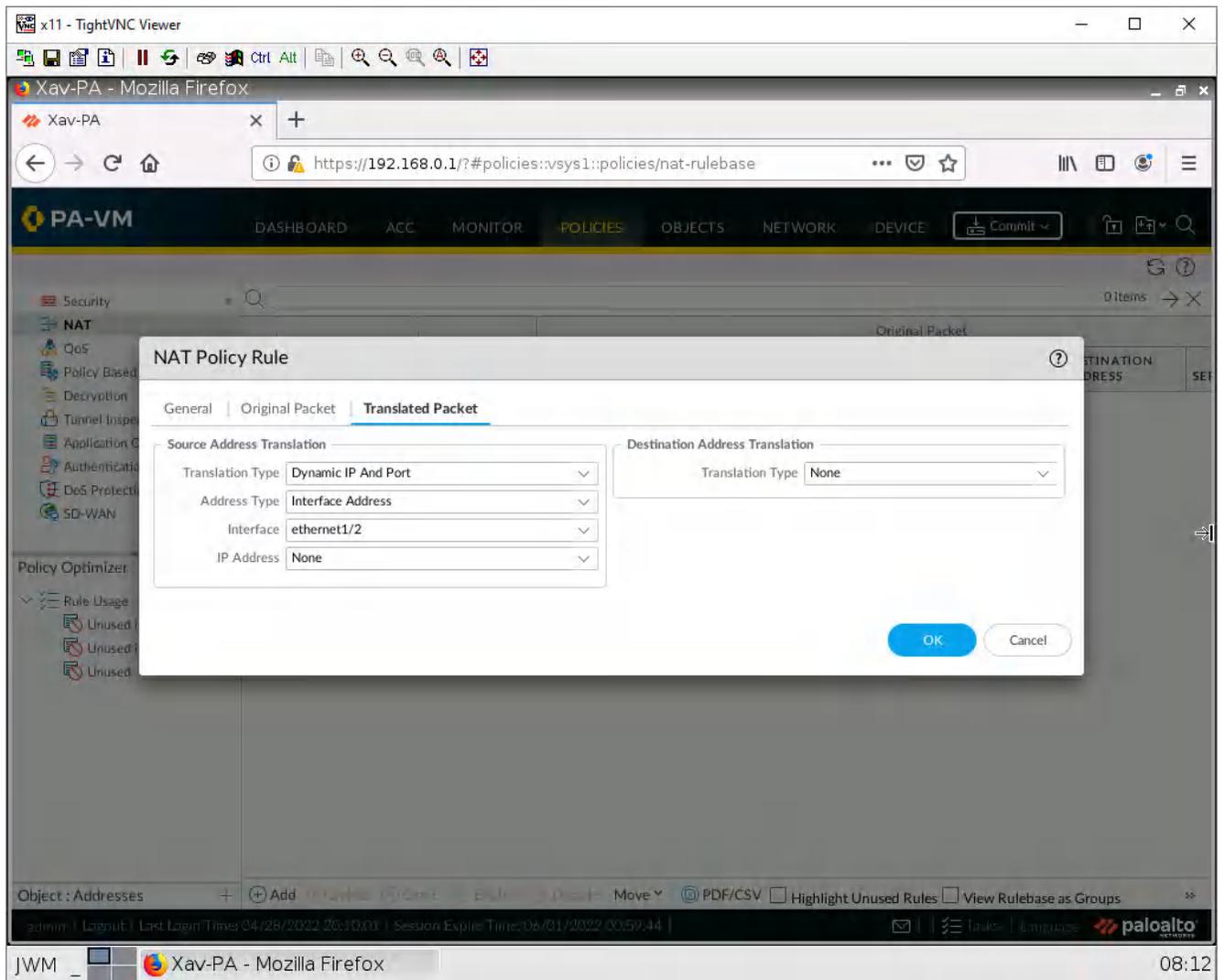


Figure 3.10: SNAT Translated Packet Tab

## Add a User

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

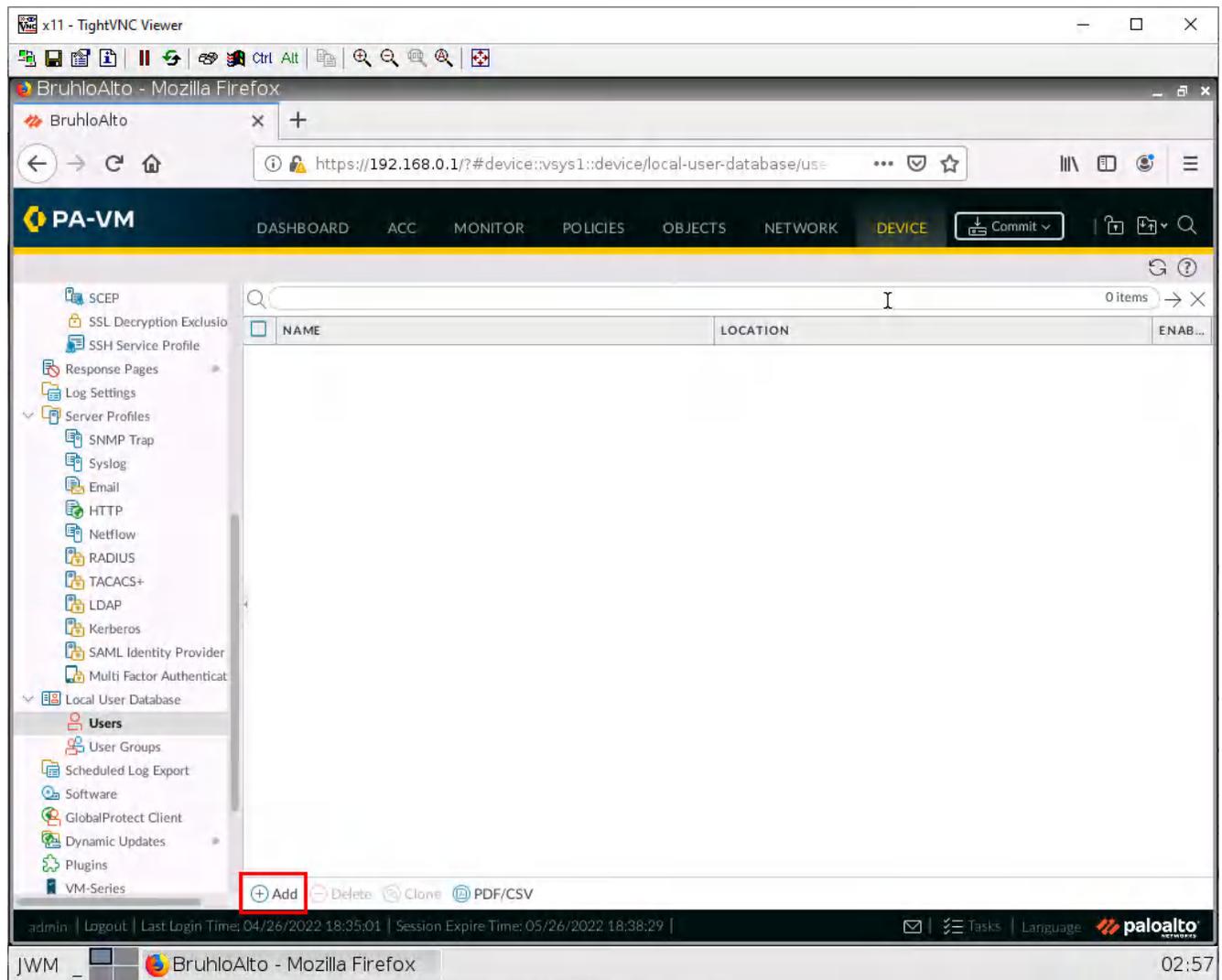


Figure 3.11: Add Users

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

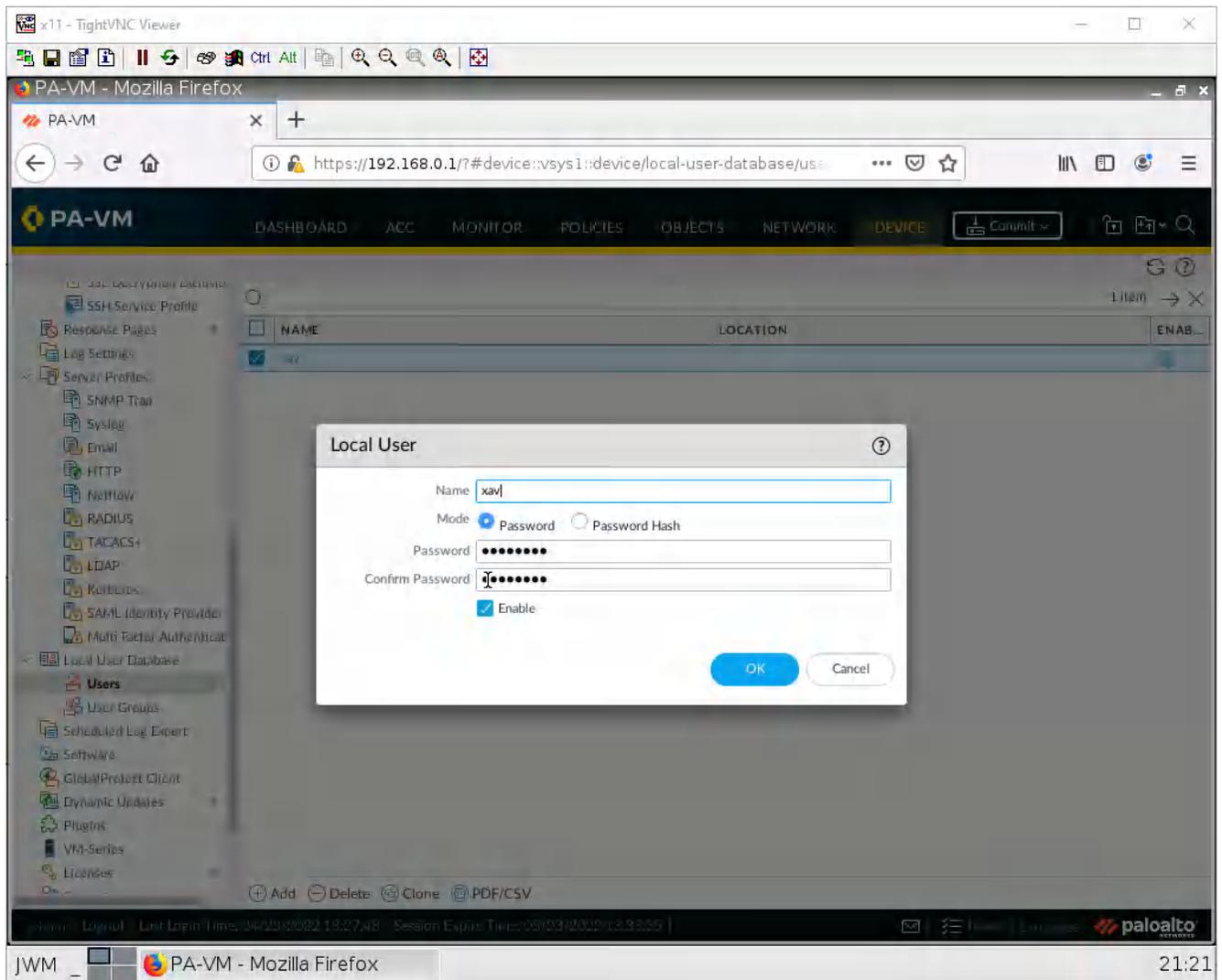


Figure 3.12: Add a user xav

Then click **OK**.

## Create an Authentication Profile

Under **Device** > **Authentication Profile**, click **Add**.

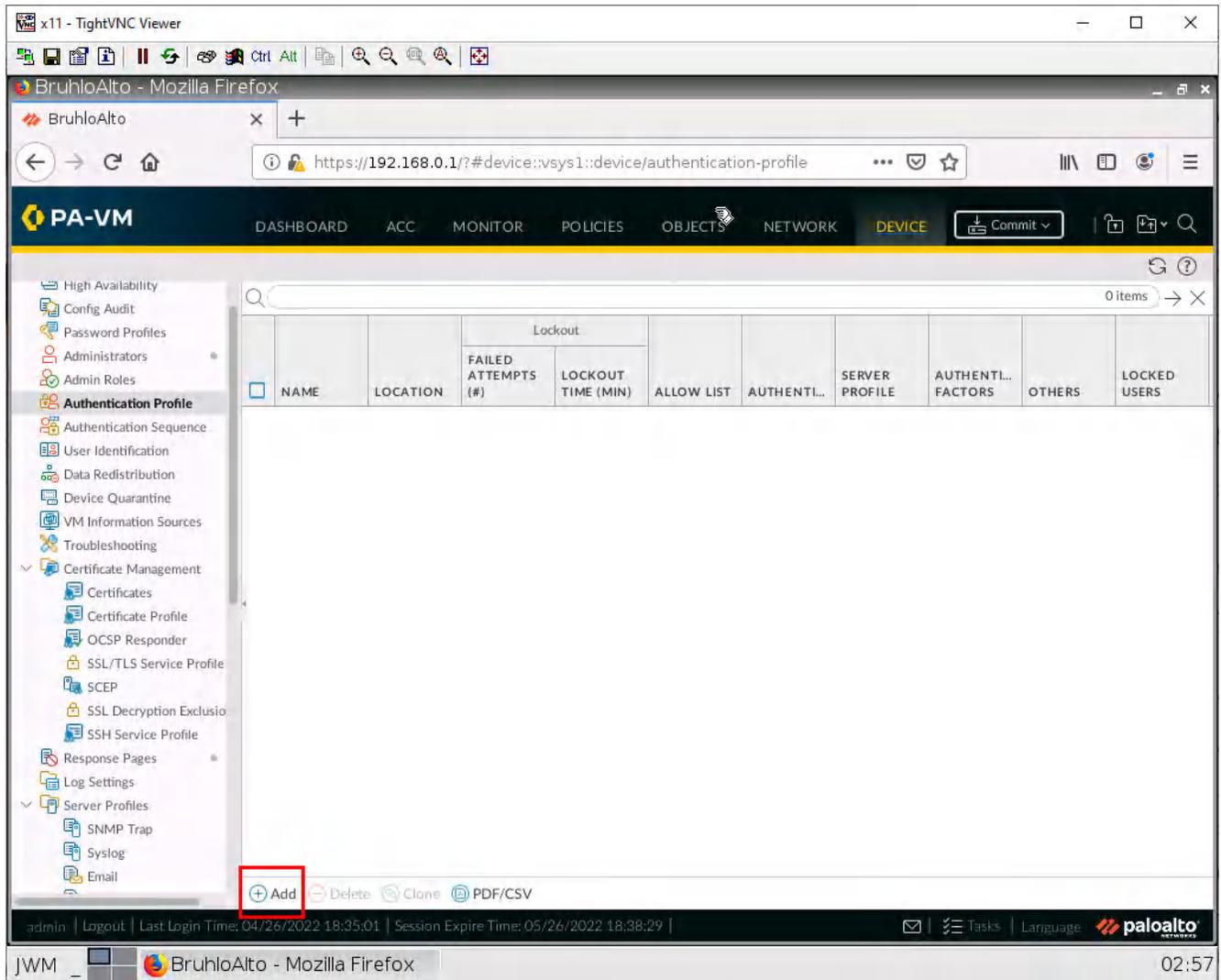


Figure 3.13: Add an Authentication Profile

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

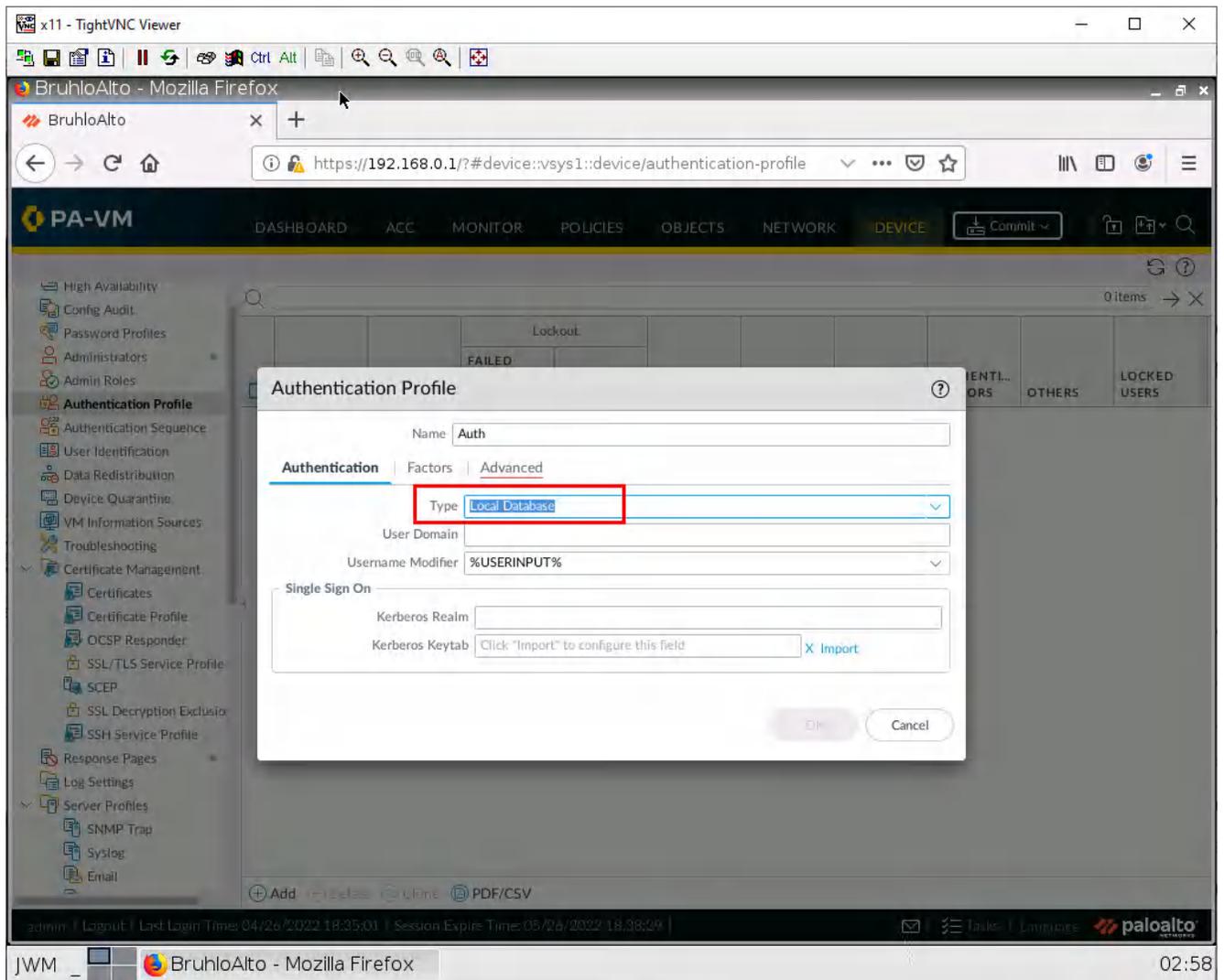


Figure 3.14: Select Local Database

Under the Advanced tab, add your user.

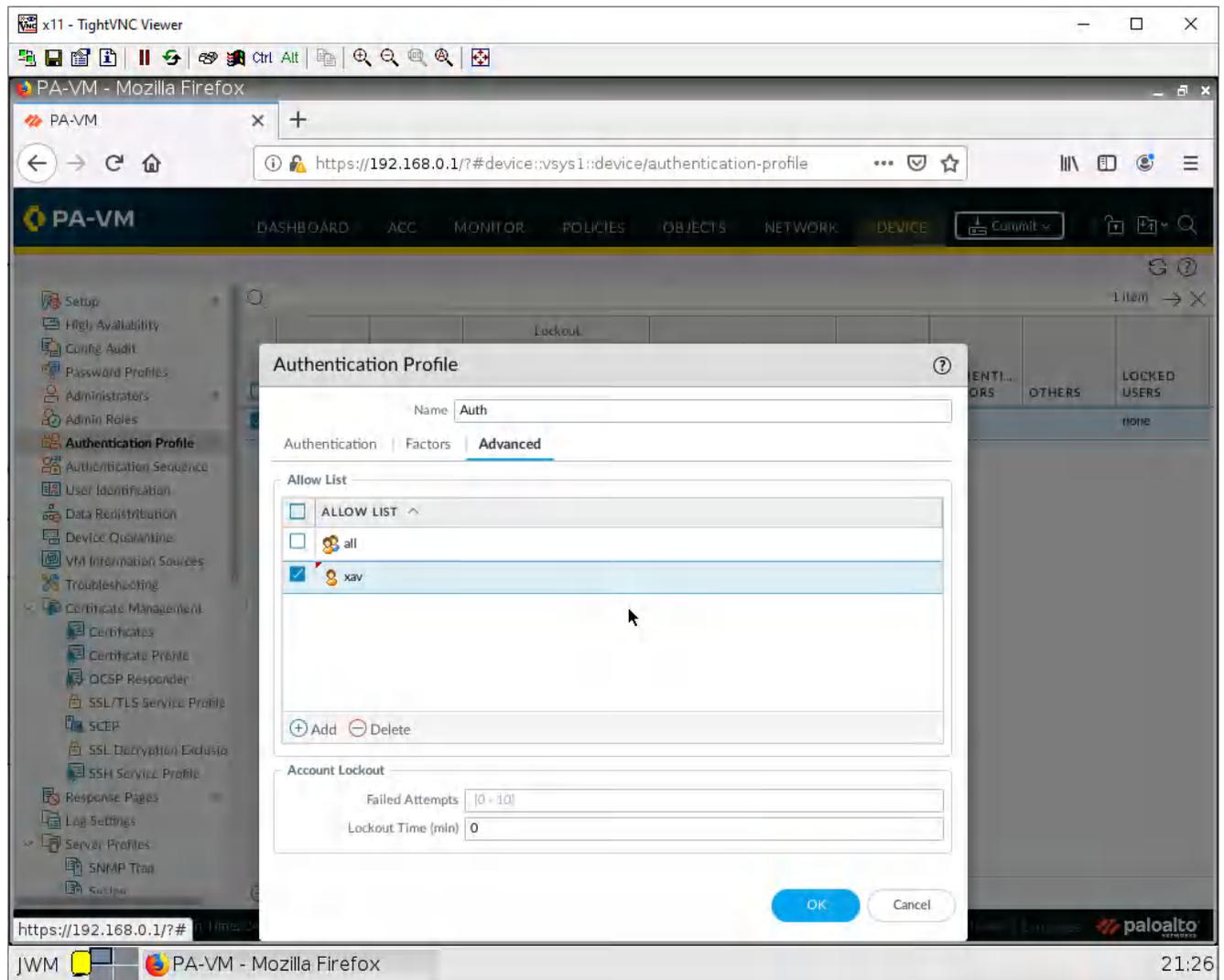


Figure 3.15: Add user xav as Allow List

Then press **OK**.

## Configure the Captive Portal

Under Device, User Identification in the Authentication Portal Settings tab, click the settings icon.

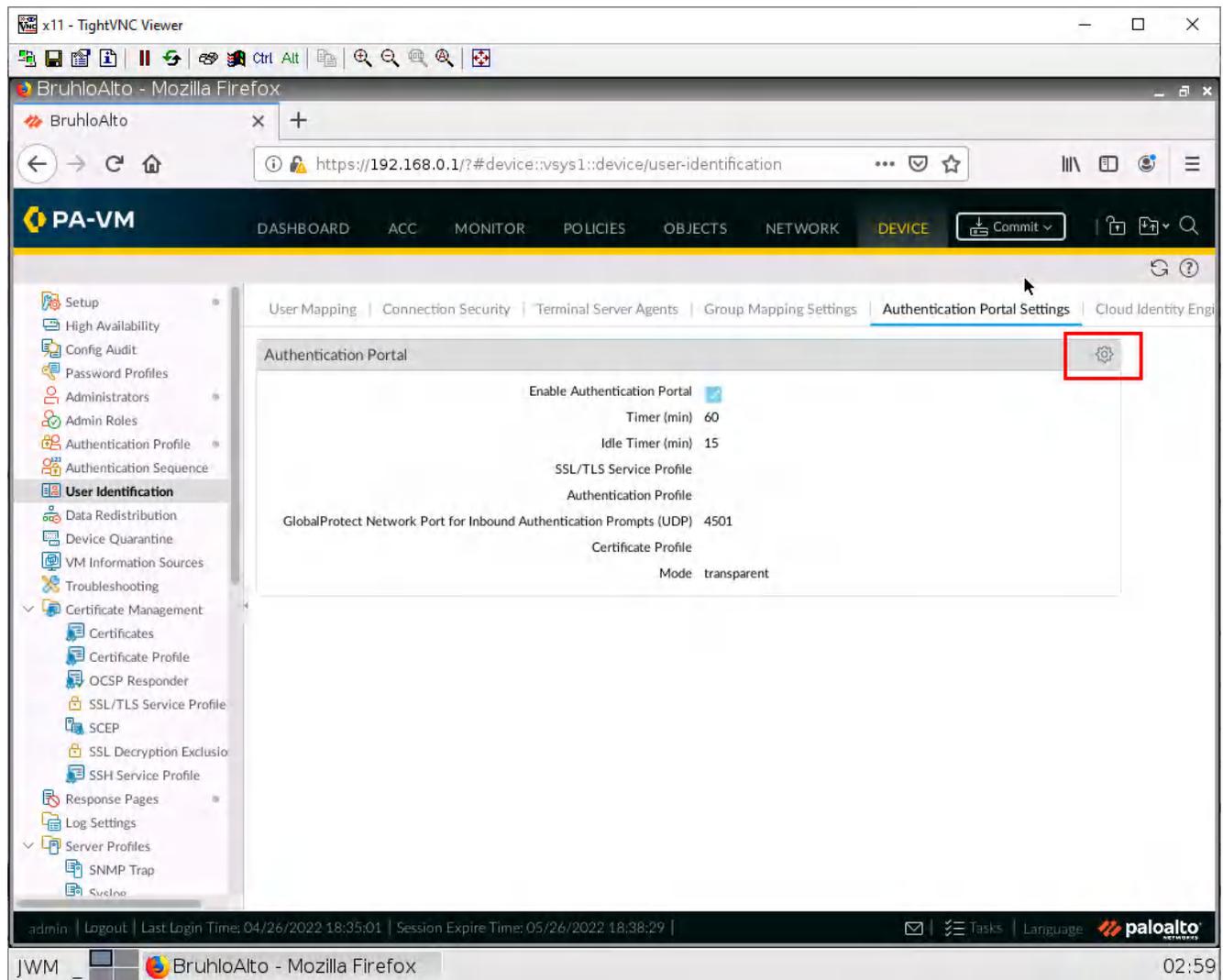


Figure 3.16: Authentication Portal Settings

Configure these settings:

Table 3.4: Authentication Portal Configuration

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

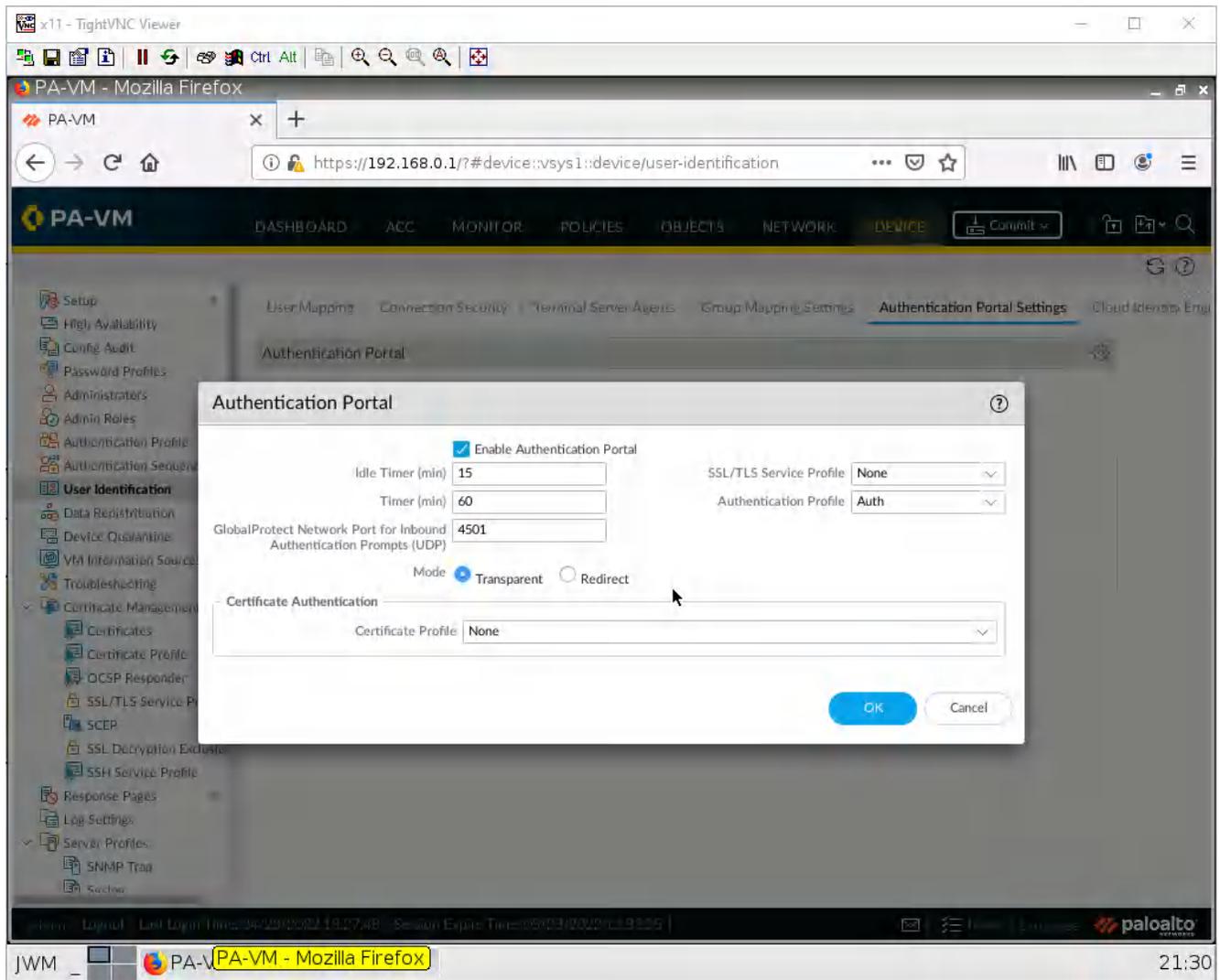


Figure 3.17: Authentication Portal Settings – Select Transparent

Then press **OK**.

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

The screenshot shows the Palo Alto VM configuration interface. The 'Zones' section is expanded in the left navigation menu. The 'VLAN10' zone is selected and highlighted with a red box. The main content area displays a table of zone configurations.

NAME	TYPE	INTERFA... / VIRTUAL SYSTEMS	ZONE PROTEC... PROFILE	PACKET BUFFER PROTEC...	LOG SETTING	User-ID			Device-ID		
						ENABLED	INCLUD... NETWO...	EXCLUD... NETWO...	ENABLED	INCLUD... NETWO...	EXCLUD... NETWO...
<input type="checkbox"/> Inside	layer3	ethernet1...		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
<input type="checkbox"/> Outside	layer3		ZoneProt	<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
<input checked="" type="checkbox"/> VLAN10	layer3	ethernet1...		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
<input type="checkbox"/> VLAN20	layer3	ethernet1...		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none

The interface also shows a search bar at the top right of the table area with '4 items' and a search icon. At the bottom of the table area, there are buttons for '+ Add', '- Delete', and 'PDF/CSV'. The bottom status bar shows the user 'admin', session information, and the Palo Alto logo.

Figure 3.18: Select Vlan 10

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

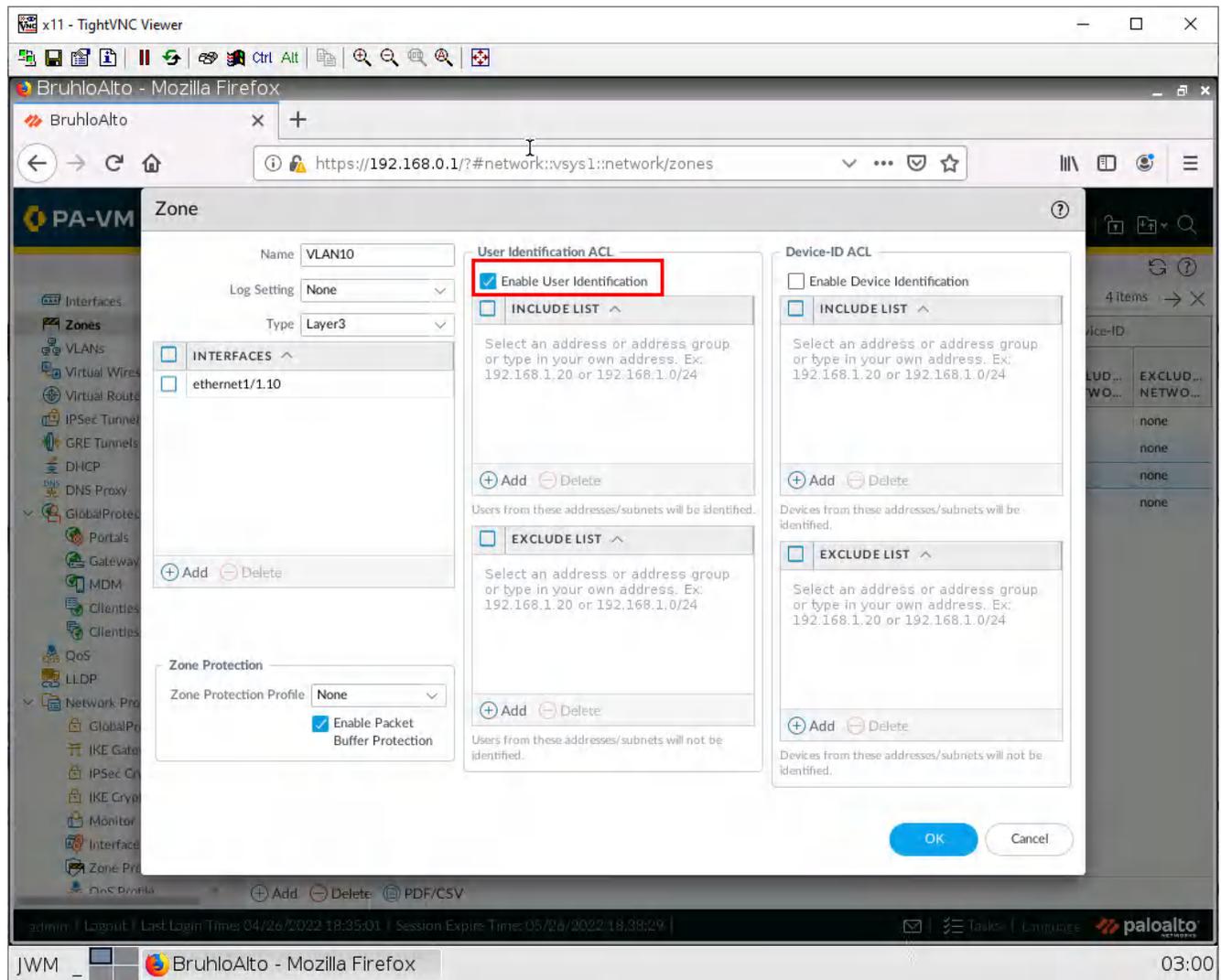


Figure 3.19: Enable User Identification

Then press **OK**.

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

The screenshot shows the Palo Alto VM web interface in Mozilla Firefox. The browser address bar shows the URL: `https://192.168.0.1/#policies::vsys1::policies/authentication-rulebase`. The interface has a dark blue header with navigation tabs: DASHBOARD, ACC, MONITOR, **POLICIES**, OBJECTS, NETWORK, and DEVICE. A 'Commit' button is visible on the right. On the left, a sidebar menu lists various security features, with 'Authentication' selected and highlighted. Below the sidebar is a 'Policy Optimizer' section showing 'Rule Usage' with three categories: 'Unused in 30 days' (0), 'Unused in 90 days' (0), and 'Unused' (0). The main content area is a table with columns for NAME, TAGS, and Source (ZONE, ADDRESS, USER, DEVICE), and Destination (ZONE, ADDRESS). At the bottom of the table, there is a toolbar with an 'Add' button (a plus sign in a circle) highlighted with a red box, along with other actions like Delete, Clones, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, and View Rulebase as Groups. The footer shows the user 'admin', a 'Logout' link, login and session expire times, and the Palo Alto logo.

Figure 3.20: Add an authentication Policy

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

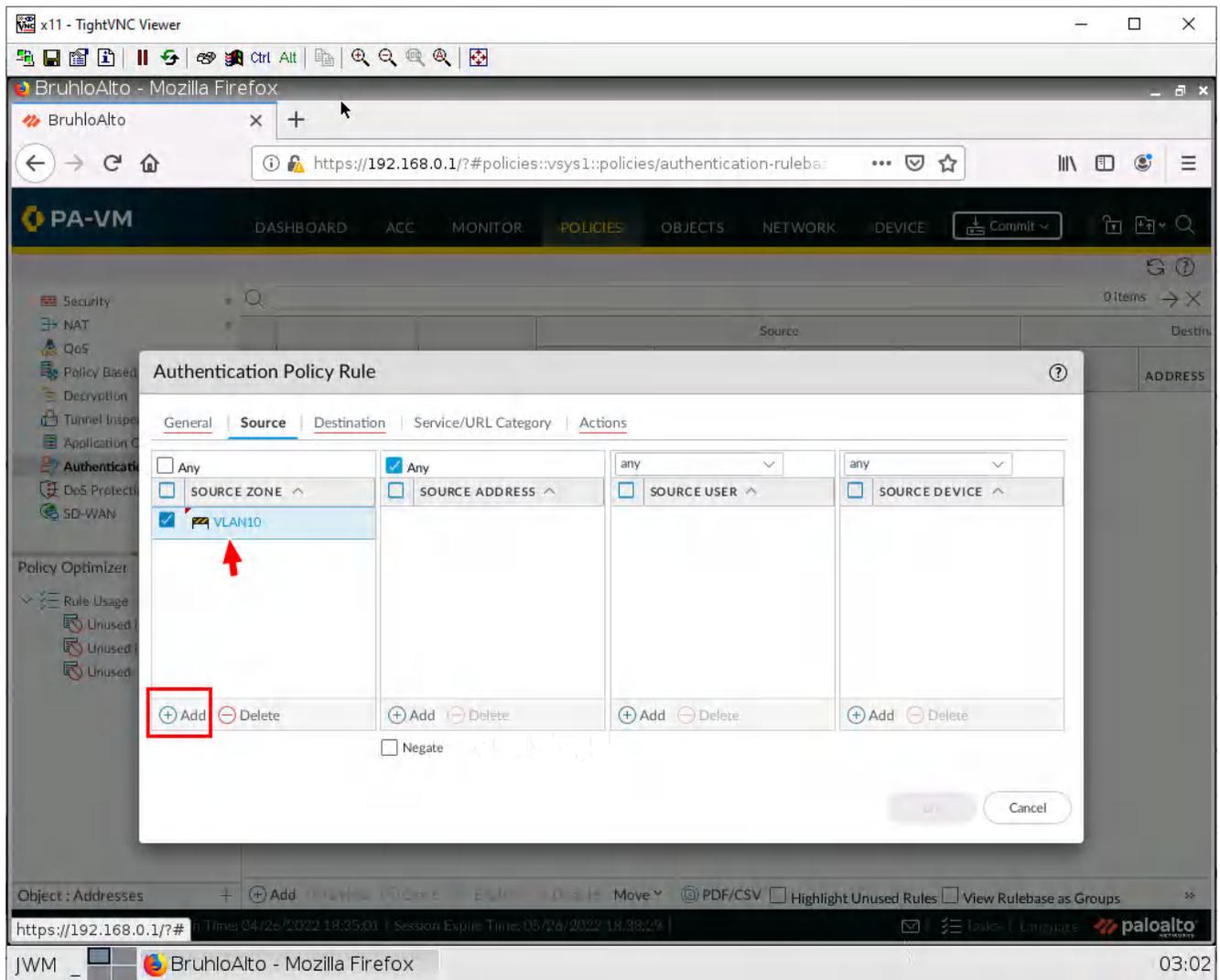


Figure 3.21: Add the Source Zone

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

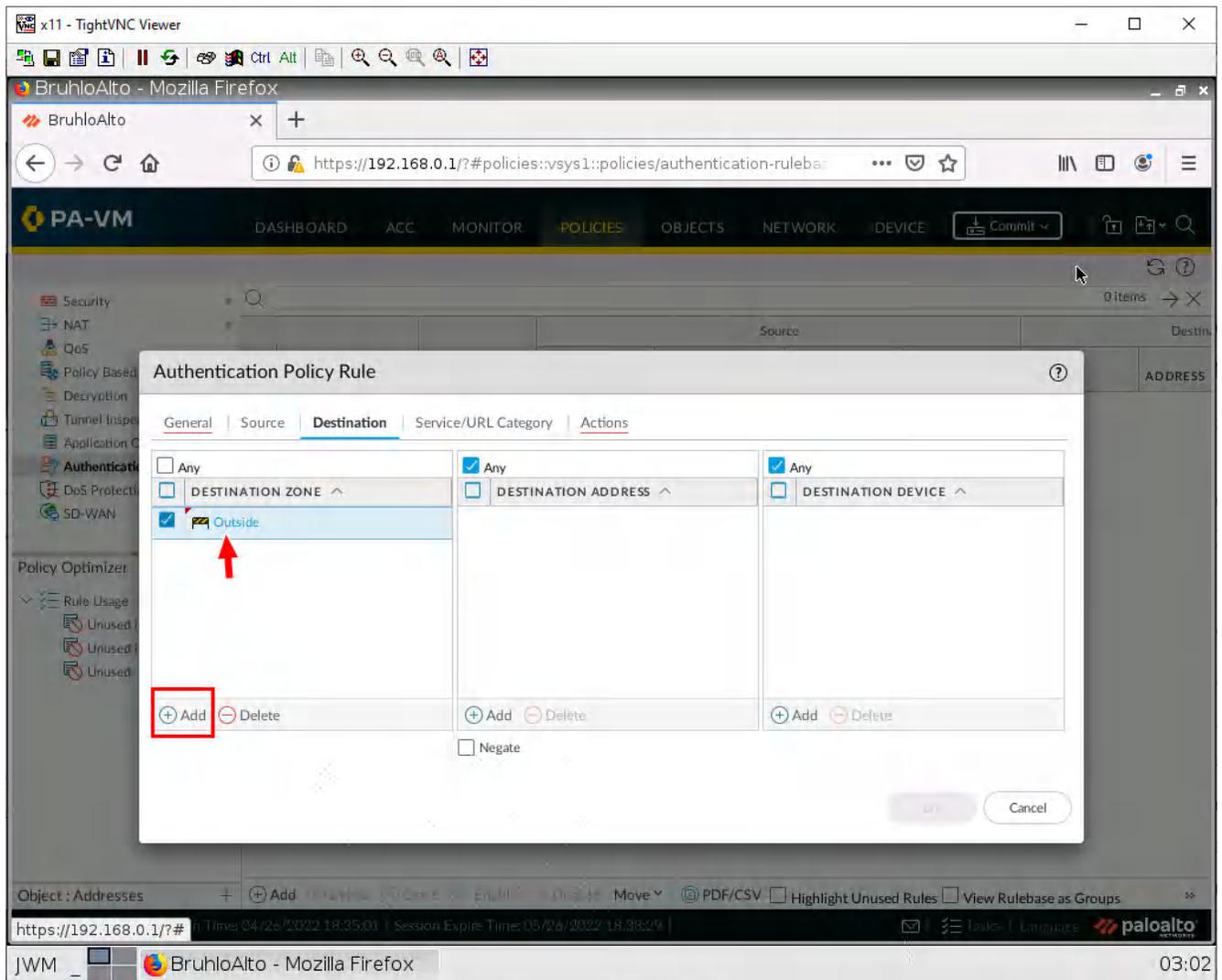


Figure 3.22: Add the Destination Zone

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

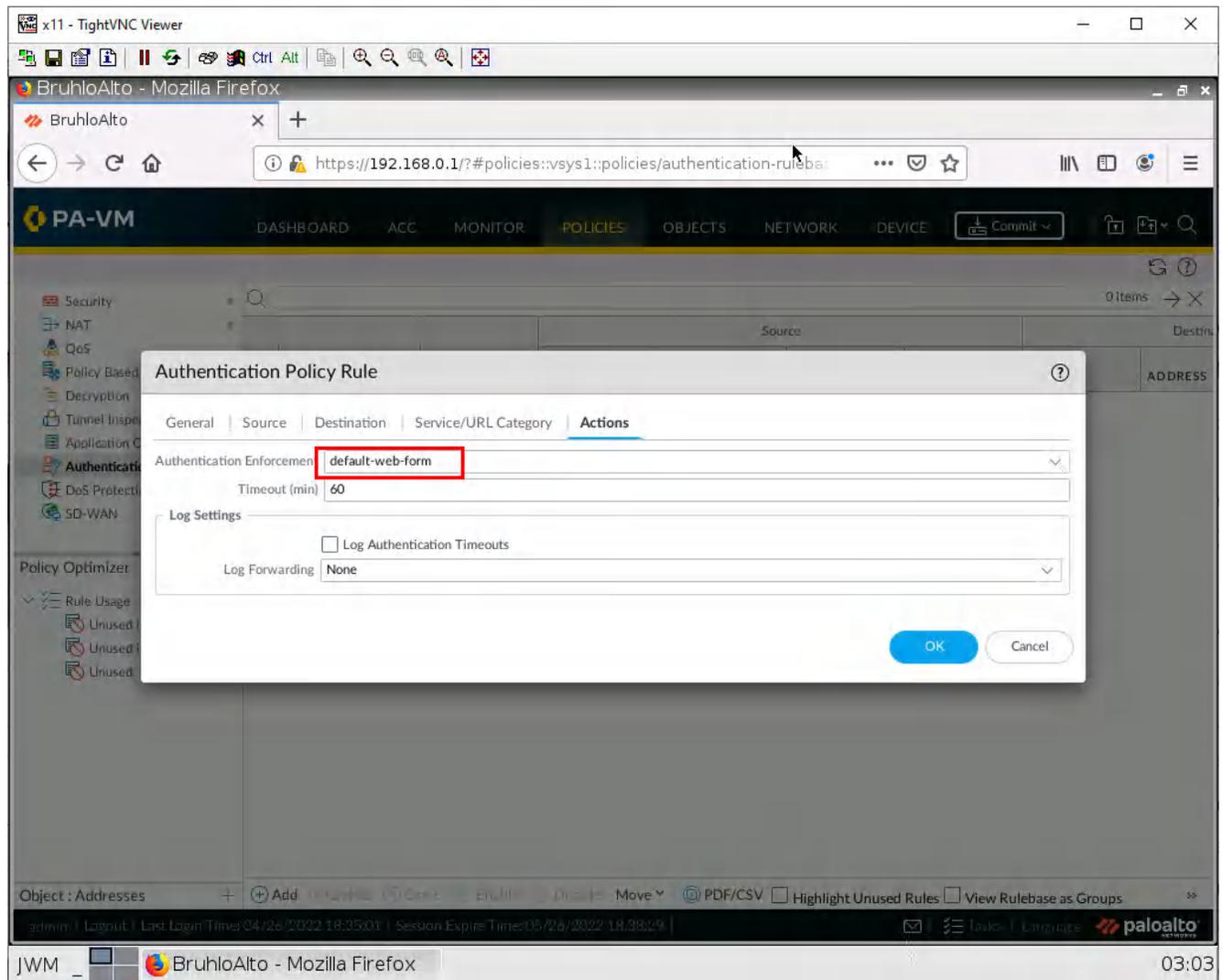


Figure 3.23: Select default-web-form

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.

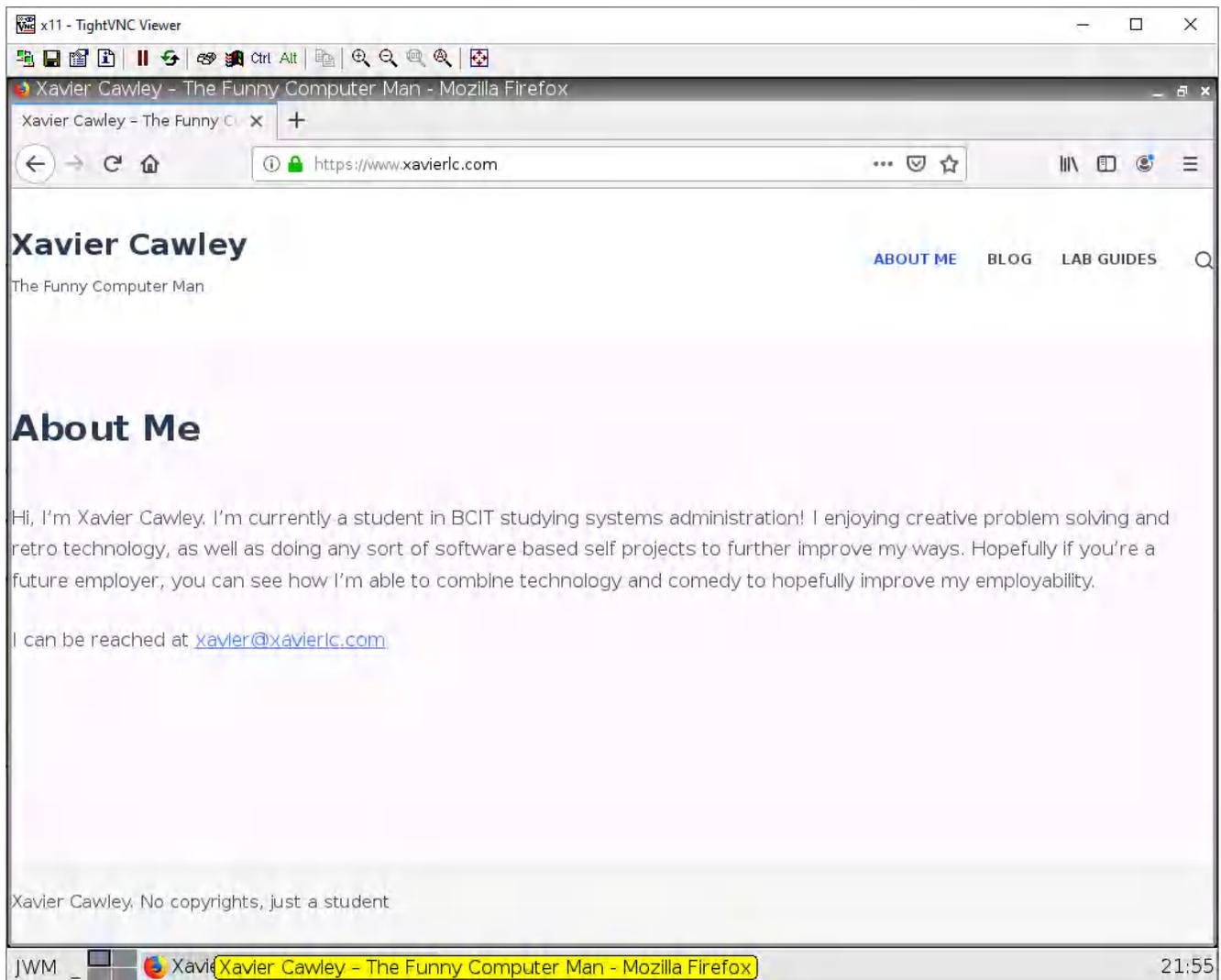


Figure 3.24: Verify your configuration

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.

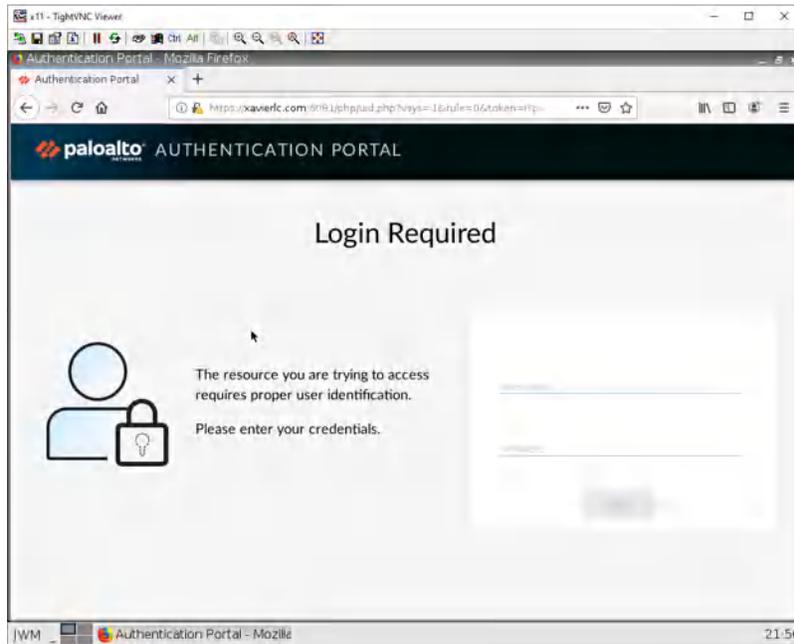


Figure 3.25: Login Page

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

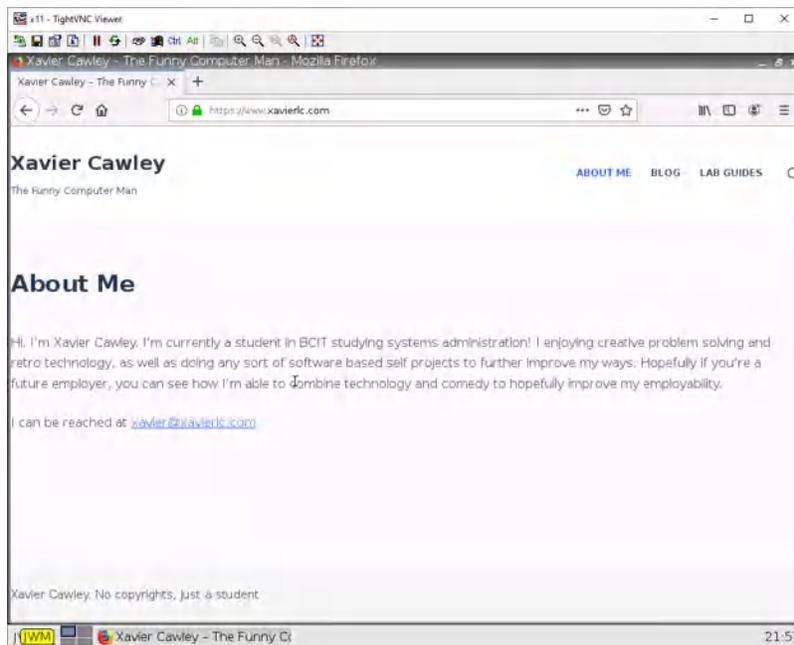


Figure 3.26: Verify your configuration

## 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.

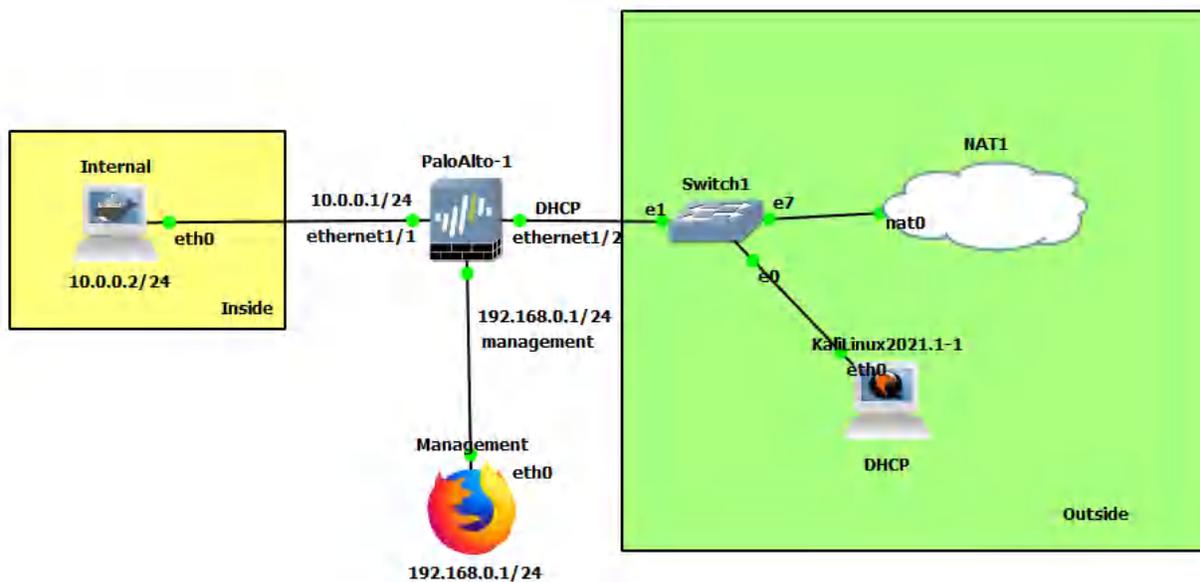


Figure 3.27: Main scenario

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

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

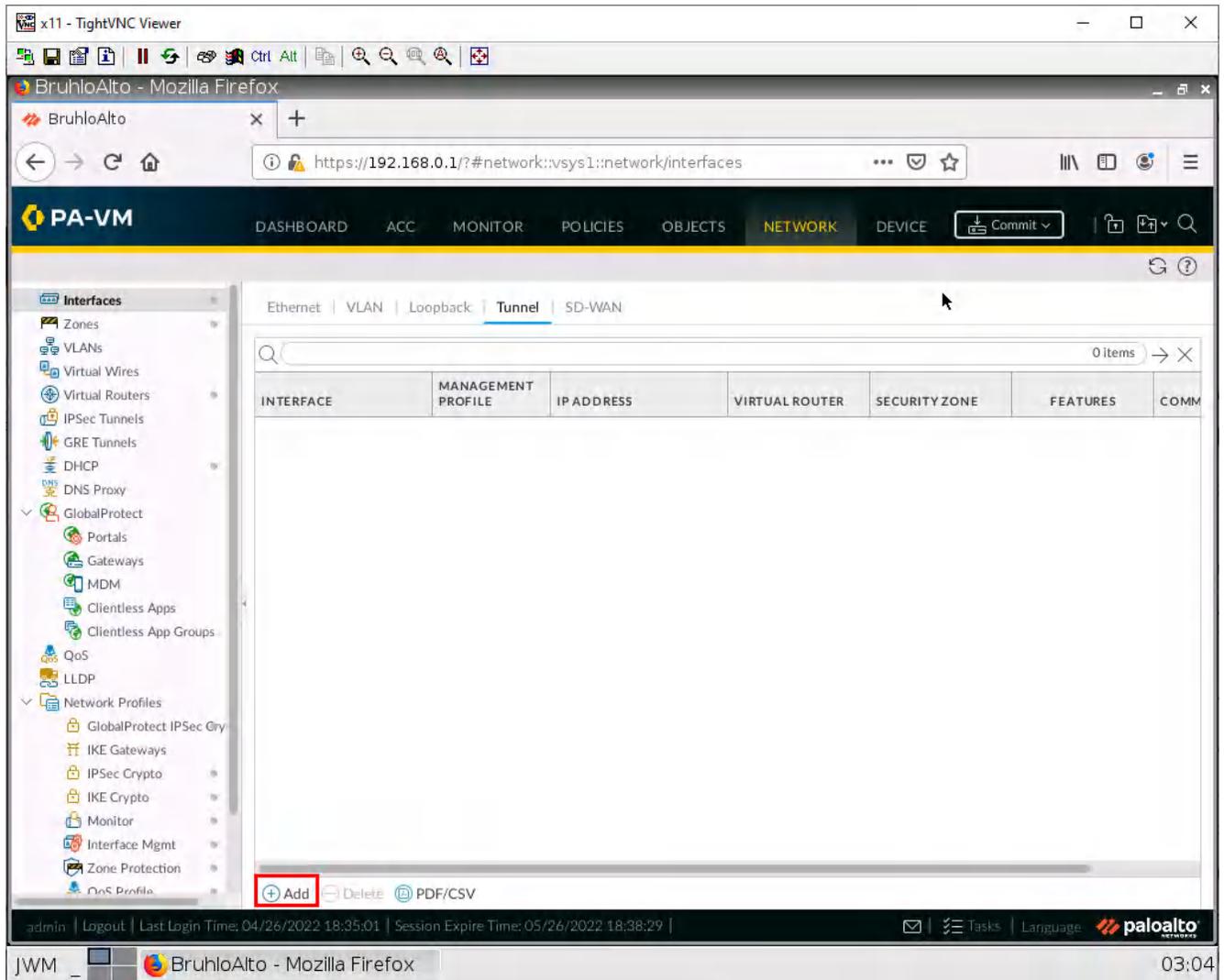


Figure 3.28: Creating a Tunnel

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

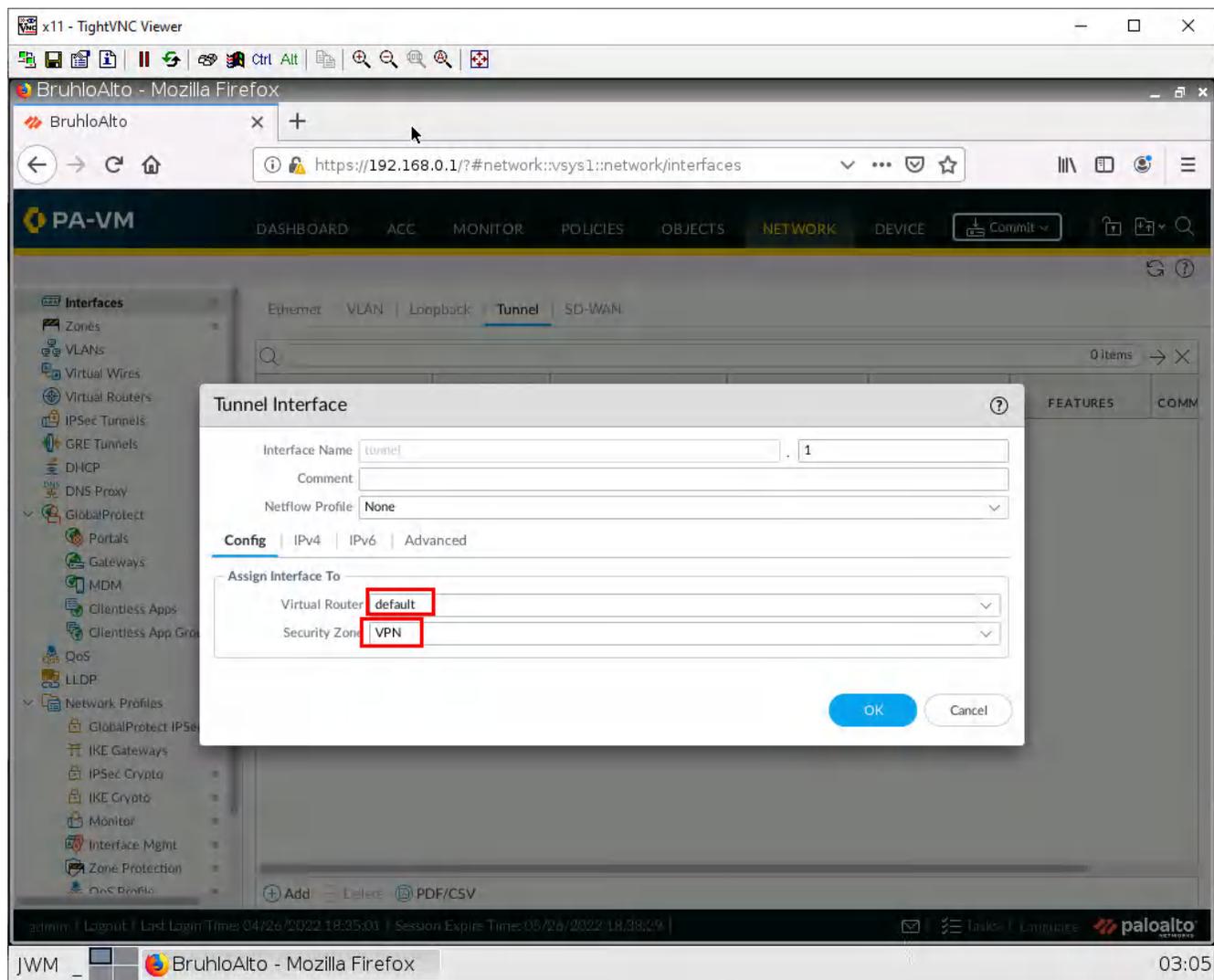


Figure 3.29: Tunnel Interface

Then click **OK**.

## Enable User ACL for a Zone

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

The screenshot shows the Palo Alto Networks PA-VM interface. The left sidebar displays a tree view with 'Zones' expanded. The main content area shows a table of zones. The 'VPN' zone is highlighted with a red box. The table has columns for NAME, TYPE, INTERFA... / VIRTUAL SYSTEMS, ZONE PROTEC... PROFILE, PACKET BUFFER PROTEC..., LOG SETTING, and two sections for User-ID and Device-ID, each with ENABLED, INCLUD..., and EXCLUD... columns.

	NAME	TYPE	INTERFA... / VIRTUAL SYSTEMS	ZONE PROTEC... PROFILE	PACKET BUFFER PROTEC...	LOG SETTING	User-ID			Device-ID		
							ENABLED	INCLUD... NETWO...	EXCLUD... NETWO...	ENABLED	INCLUD... NETWO...	EXCLUD... NETWO...
<input type="checkbox"/>	Inside	layer3	ethernet1...		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
<input type="checkbox"/>	Outside	layer3		ZoneProt	<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
<input type="checkbox"/>	VLAN10	layer3	ethernet1...		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
<input type="checkbox"/>	VLAN20	layer3	ethernet1...		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
<input type="checkbox"/>	VPN	layer3	tunnel.1		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none

At the bottom of the interface, there are buttons for '+ Add', '- Delete', and 'PDF/CSV'. The status bar at the very bottom shows 'admin | Logout | Last Login Time: 04/26/2022 18:35:01 | Session Expire Time: 05/26/2022 18:38:29 | Tasks | Language | paloalto'.

Figure 3.30: Create a VPN Zone

Tick the **Enable user identification** box.

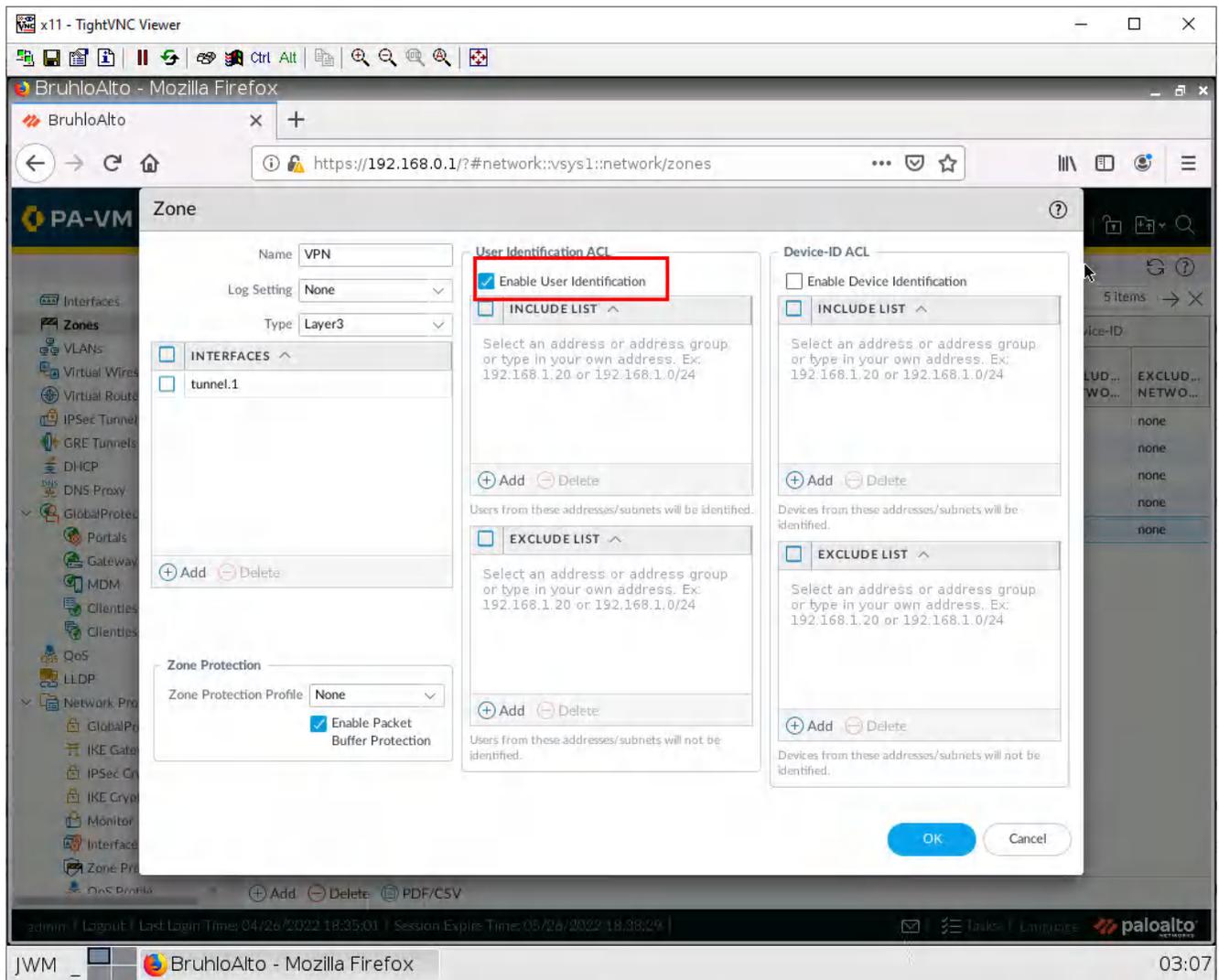


Figure 3.31: Enable User Identification under VPN Zone

Then press **OK**.

## Generate Certs

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

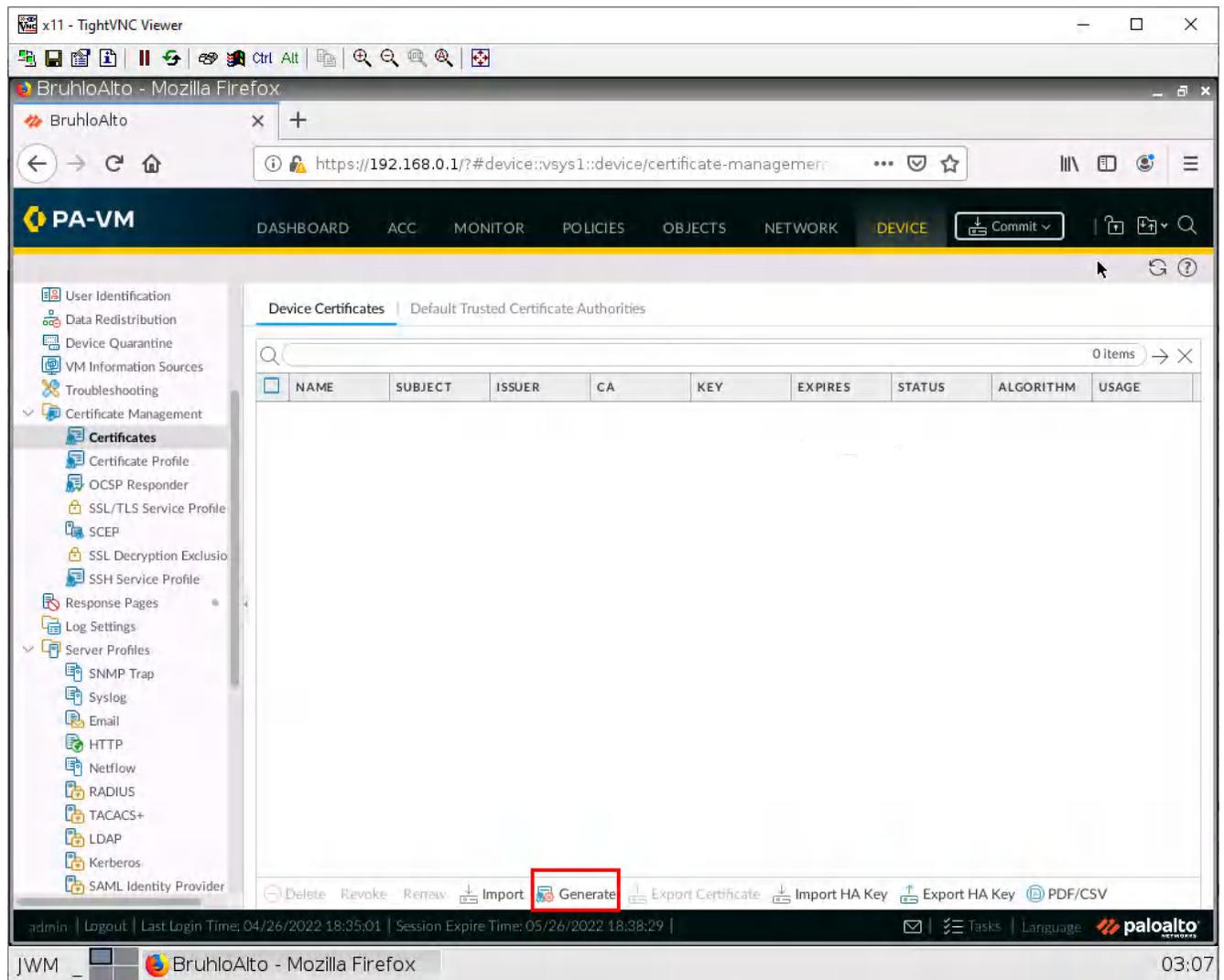


Figure 3.32: Generate a certificate

Configure these settings in the new window:

**Table 3.7: Certificate Generation**

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

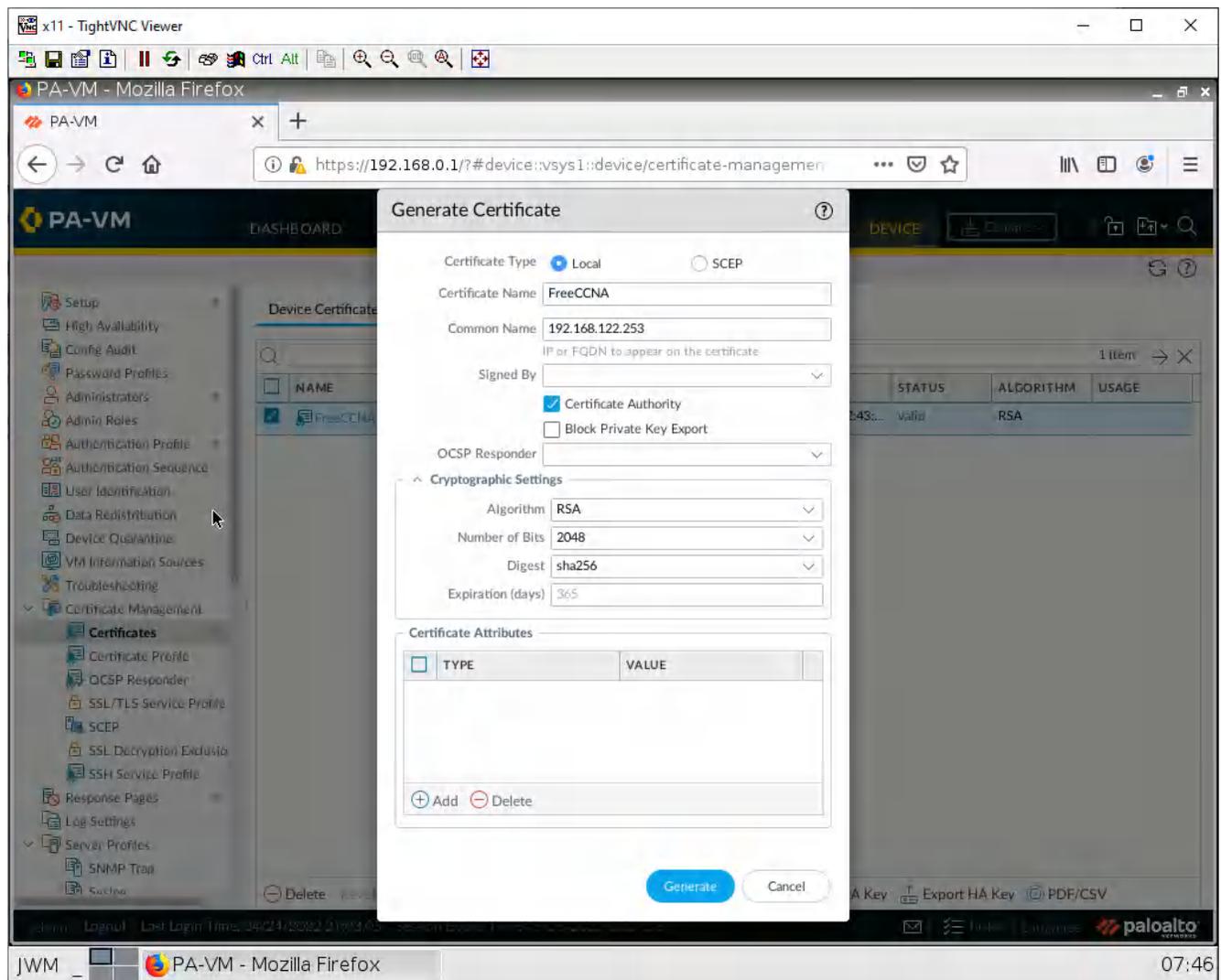


Figure 3.33: Generate a certificate

Then click **Generate**.

## Create an SSL/TLS Service Profile

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

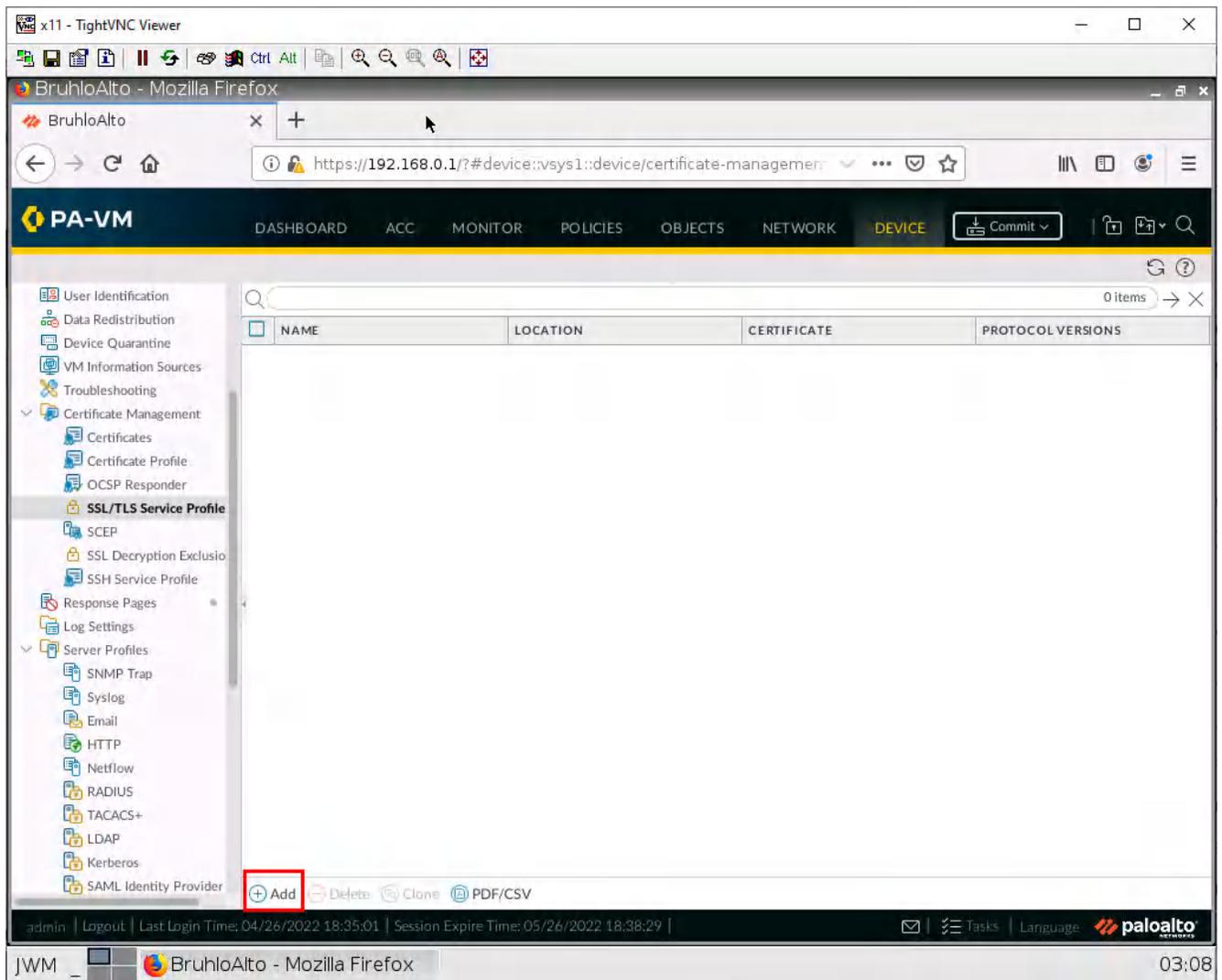


Figure 3.34: Add SSL/TLS Service Profile

In the new window, add the certificate you generated.

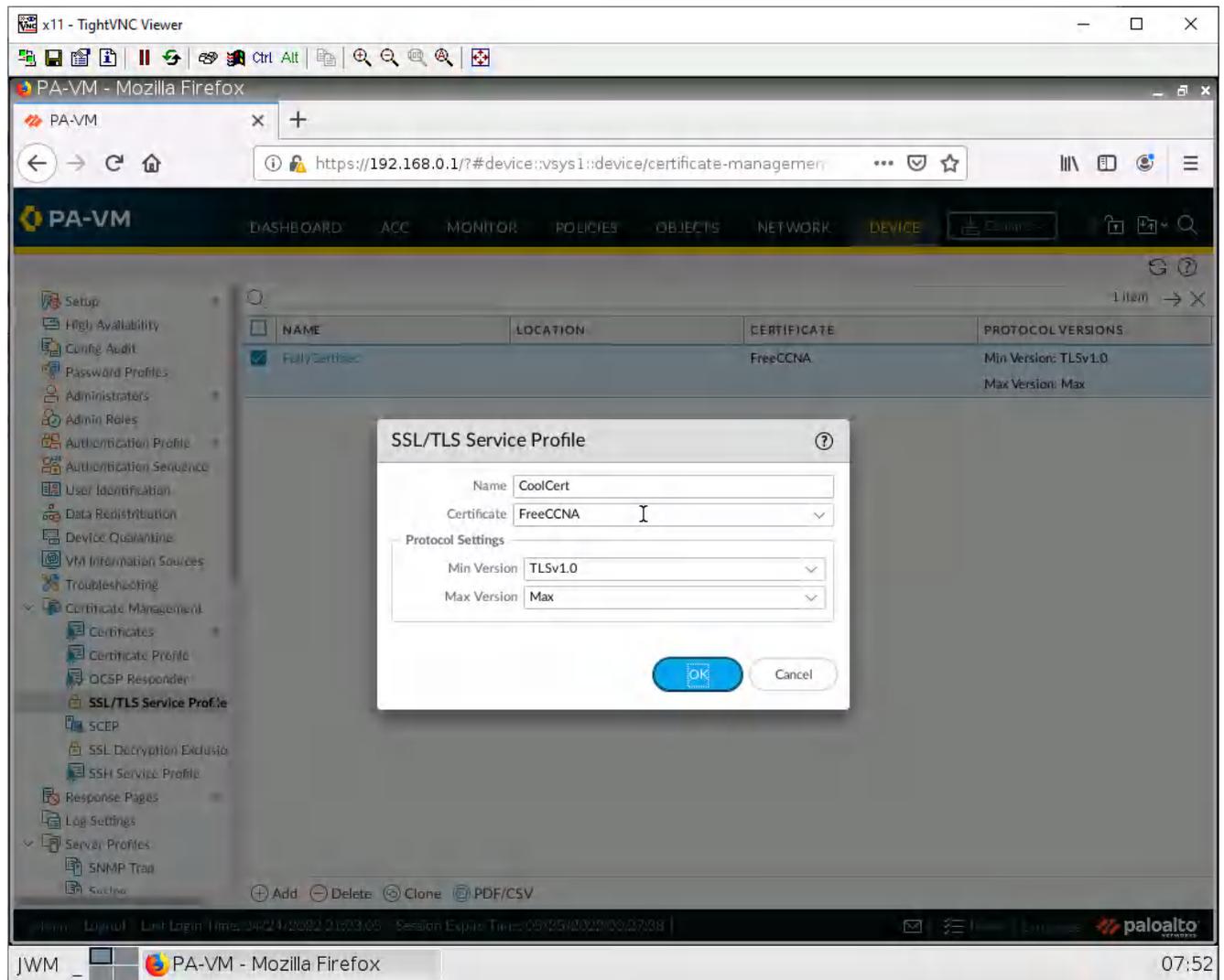


Figure 3.35: Configure SSL/TLS Service Profile

Then click **OK**.

## Create a GlobalProtect Portal

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

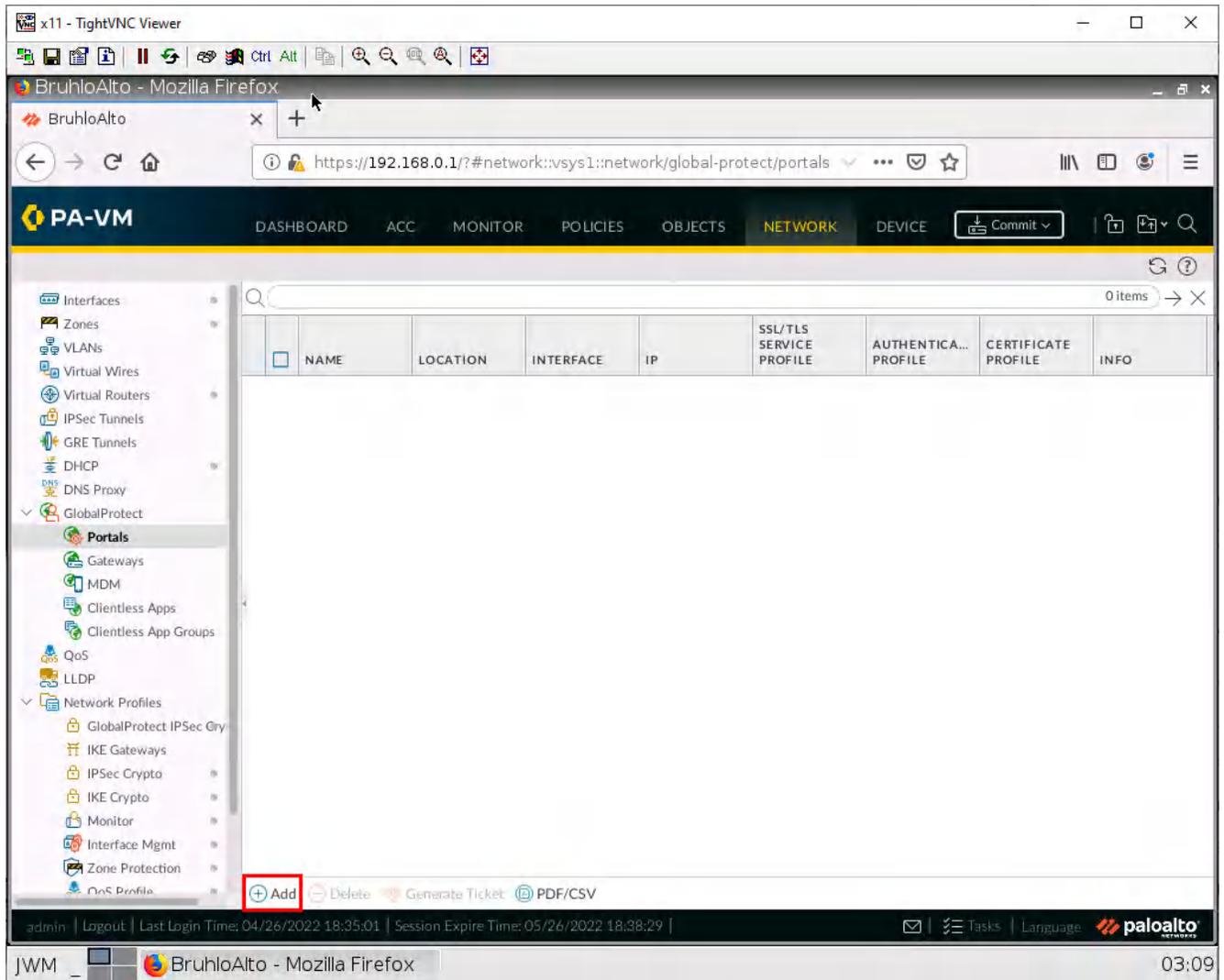


Figure 3.36: Add a Portal

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

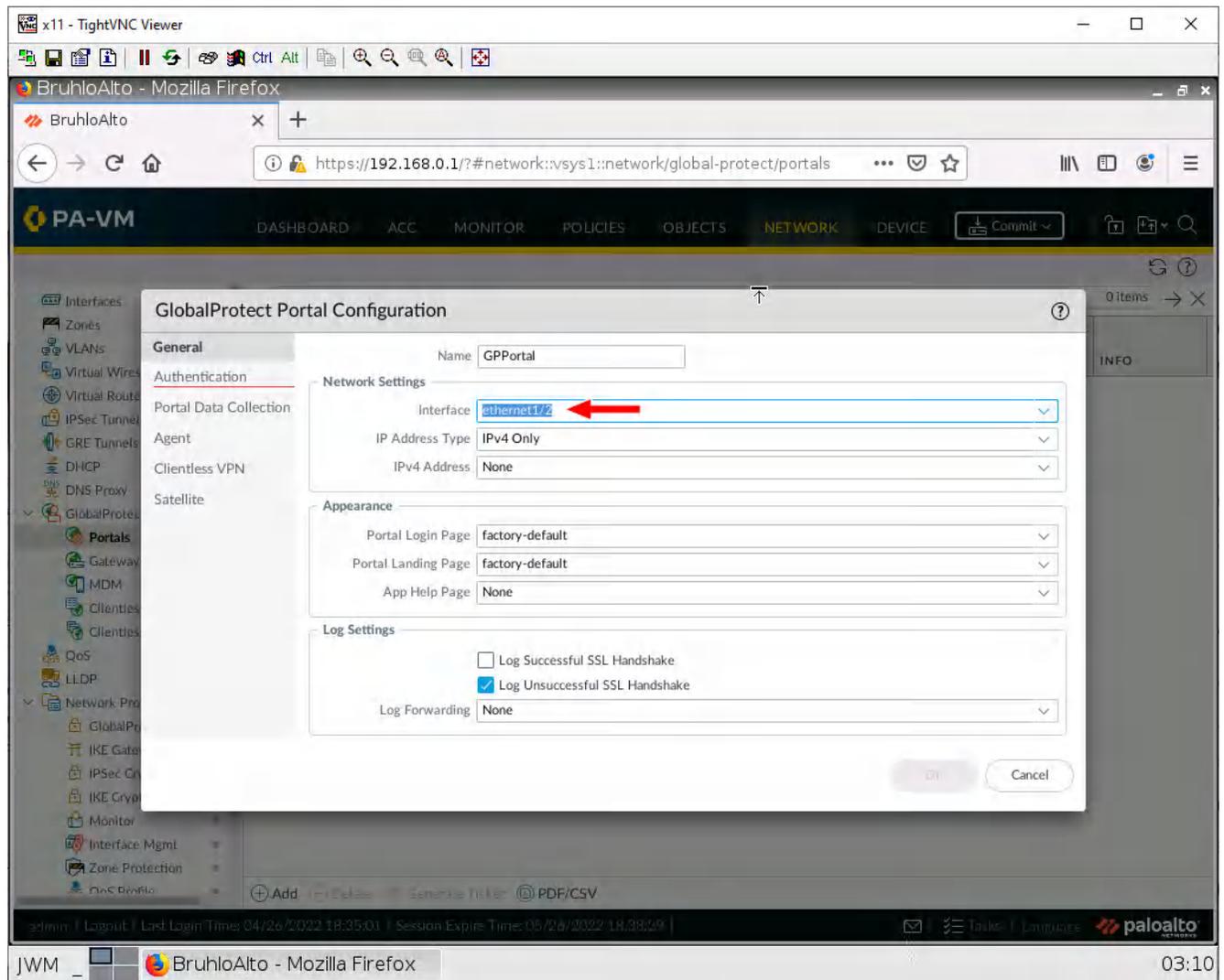


Figure 3.37: GlobalProtect Portal Configuration

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

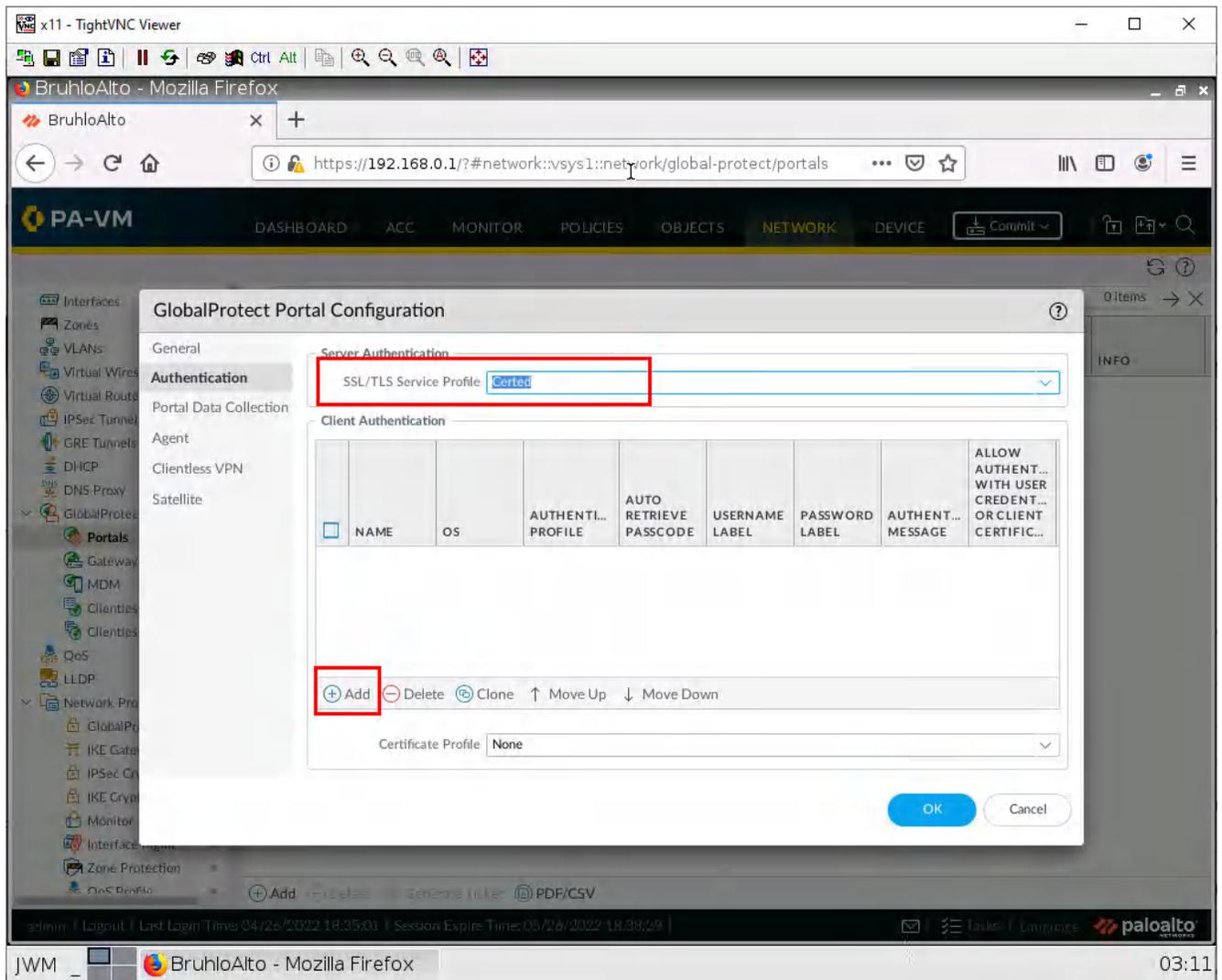


Figure 3.38: Adding SSL/TLS Profile

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

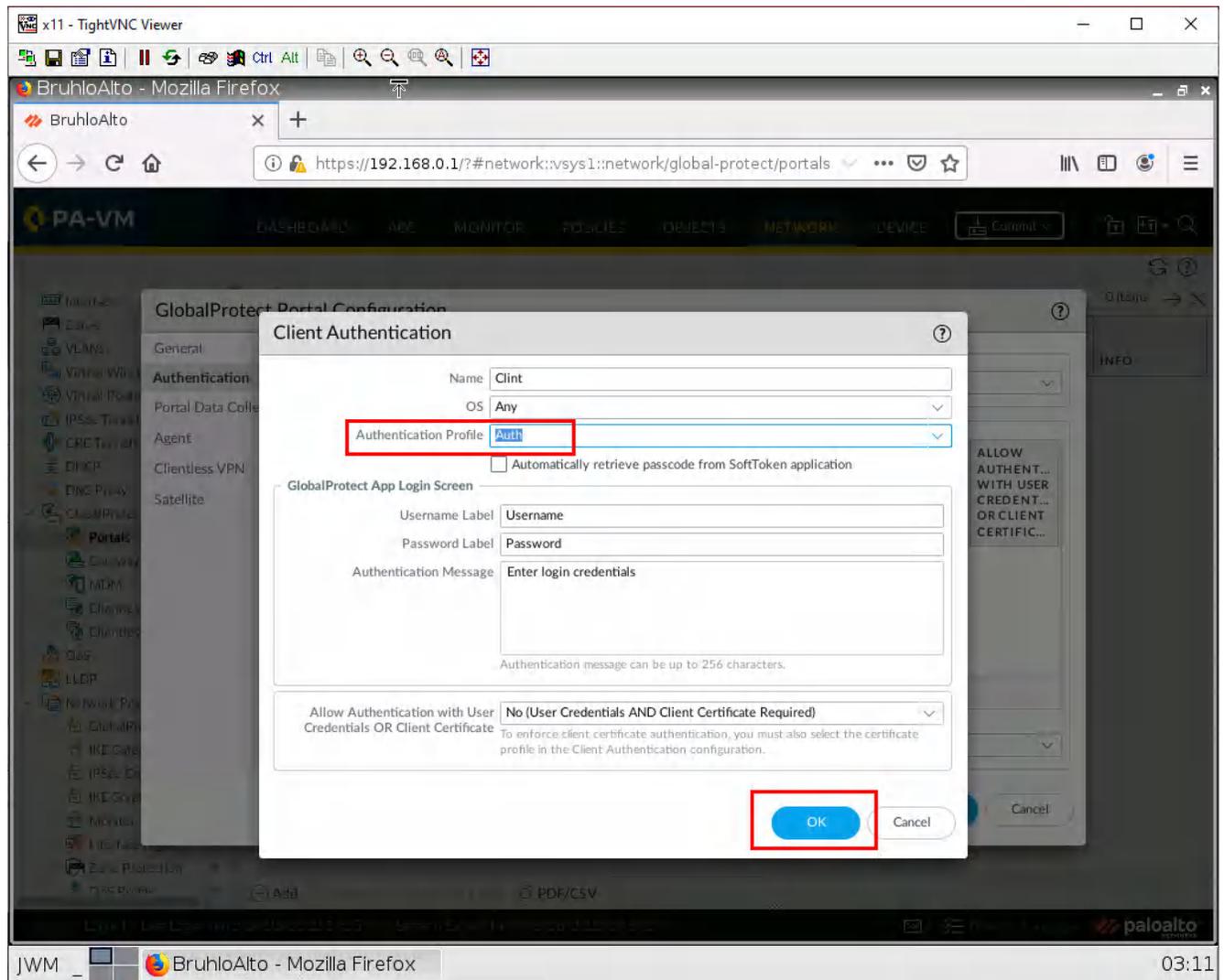


Figure 3.39: Adding Authentication Profile

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

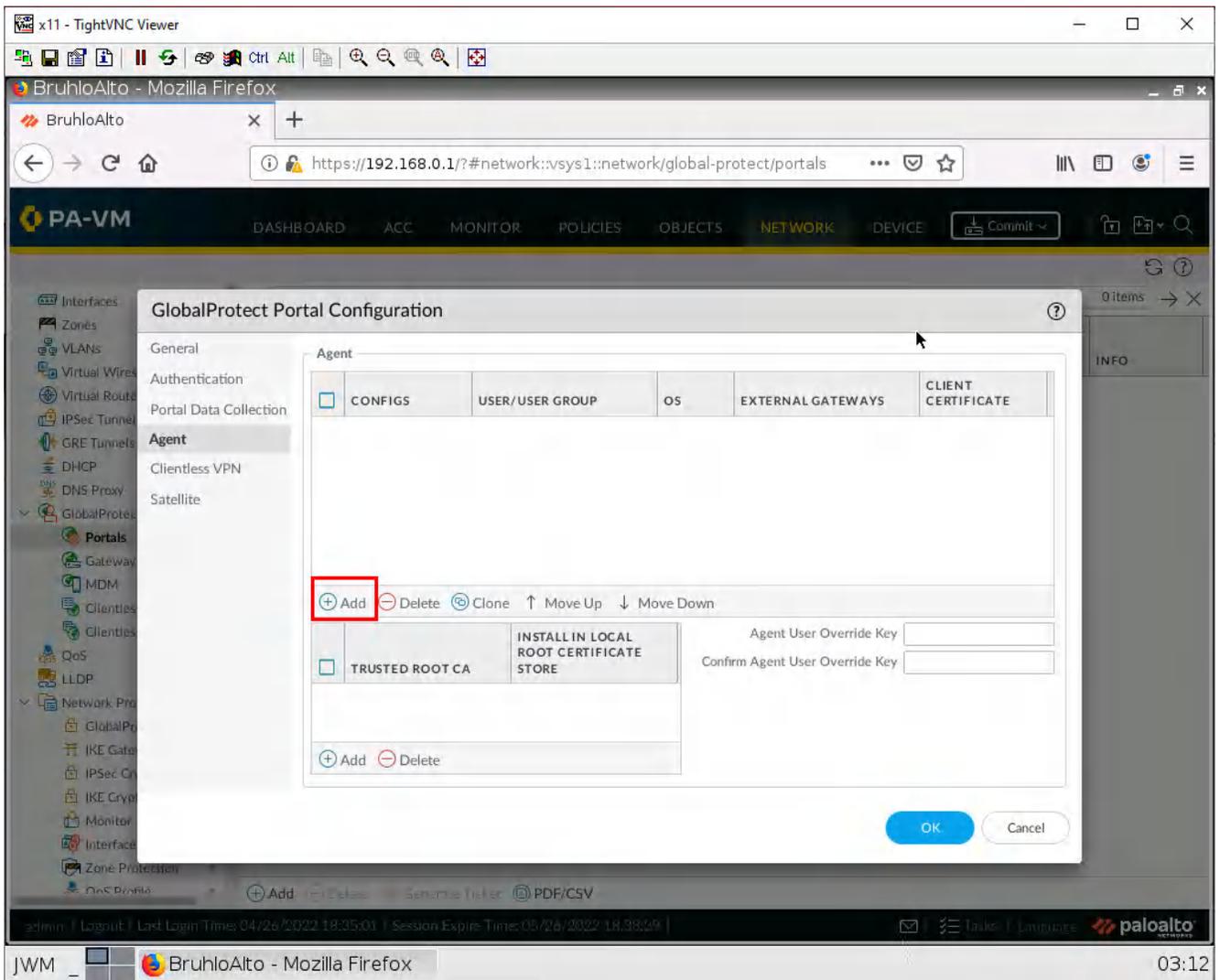


Figure 3.40: Adding the agent

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

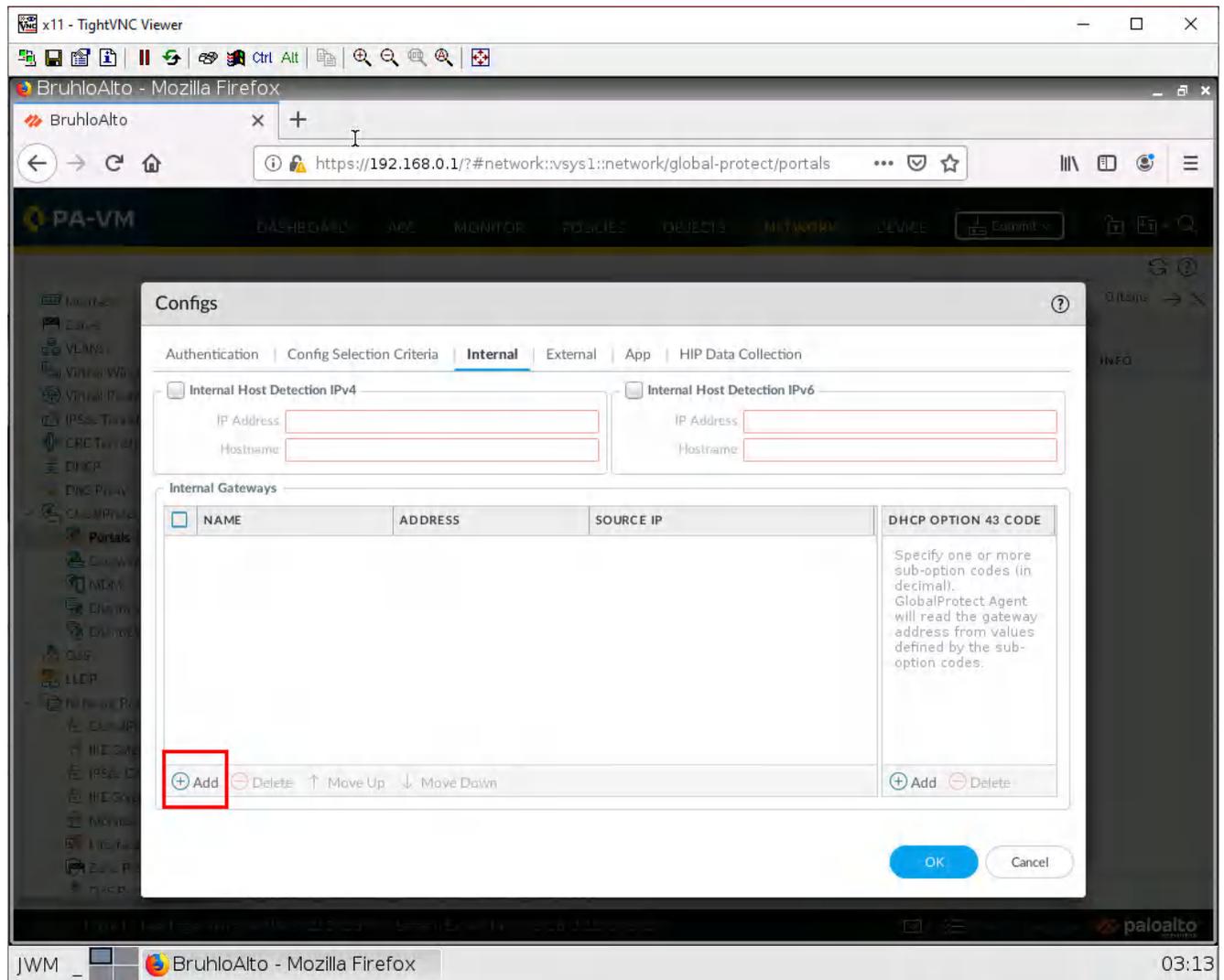


Figure 3.41: Configure Internal Gateway

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

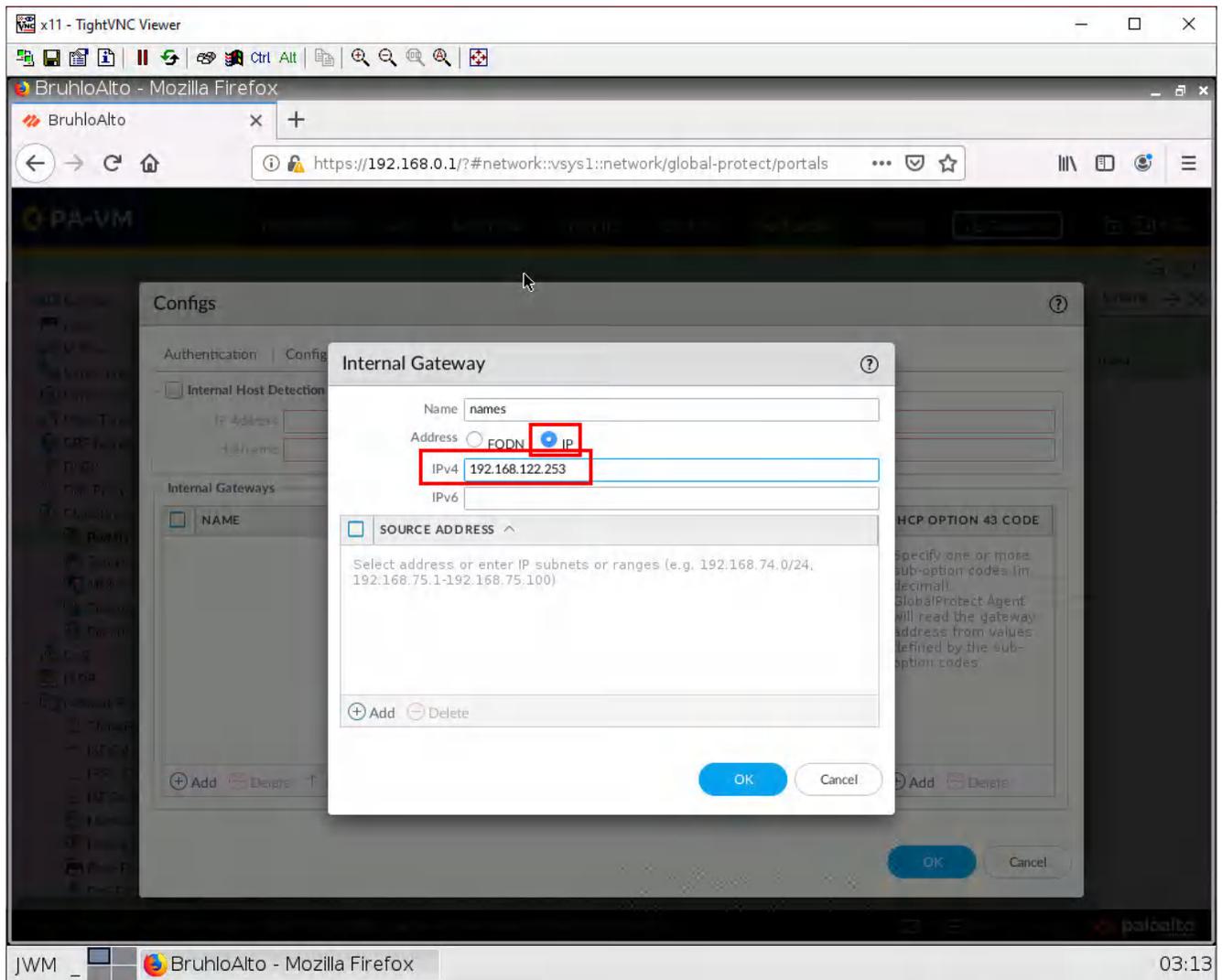


Figure 3.42: Set the IP address for Internal Gateway

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.

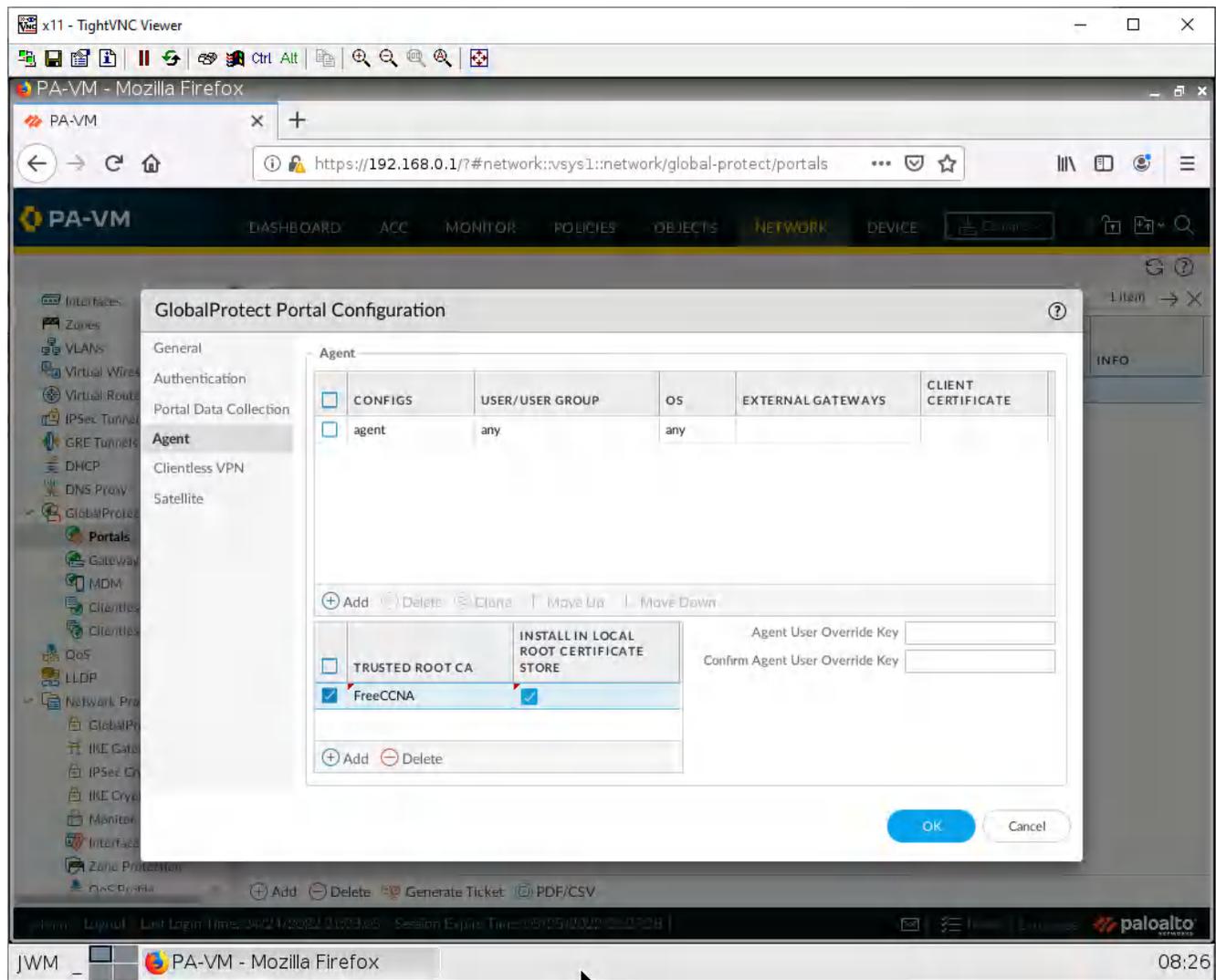


Figure 3.43: Add the Root CA certificate

Then press **OK**.

## Create a GlobalProtect Gateway

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

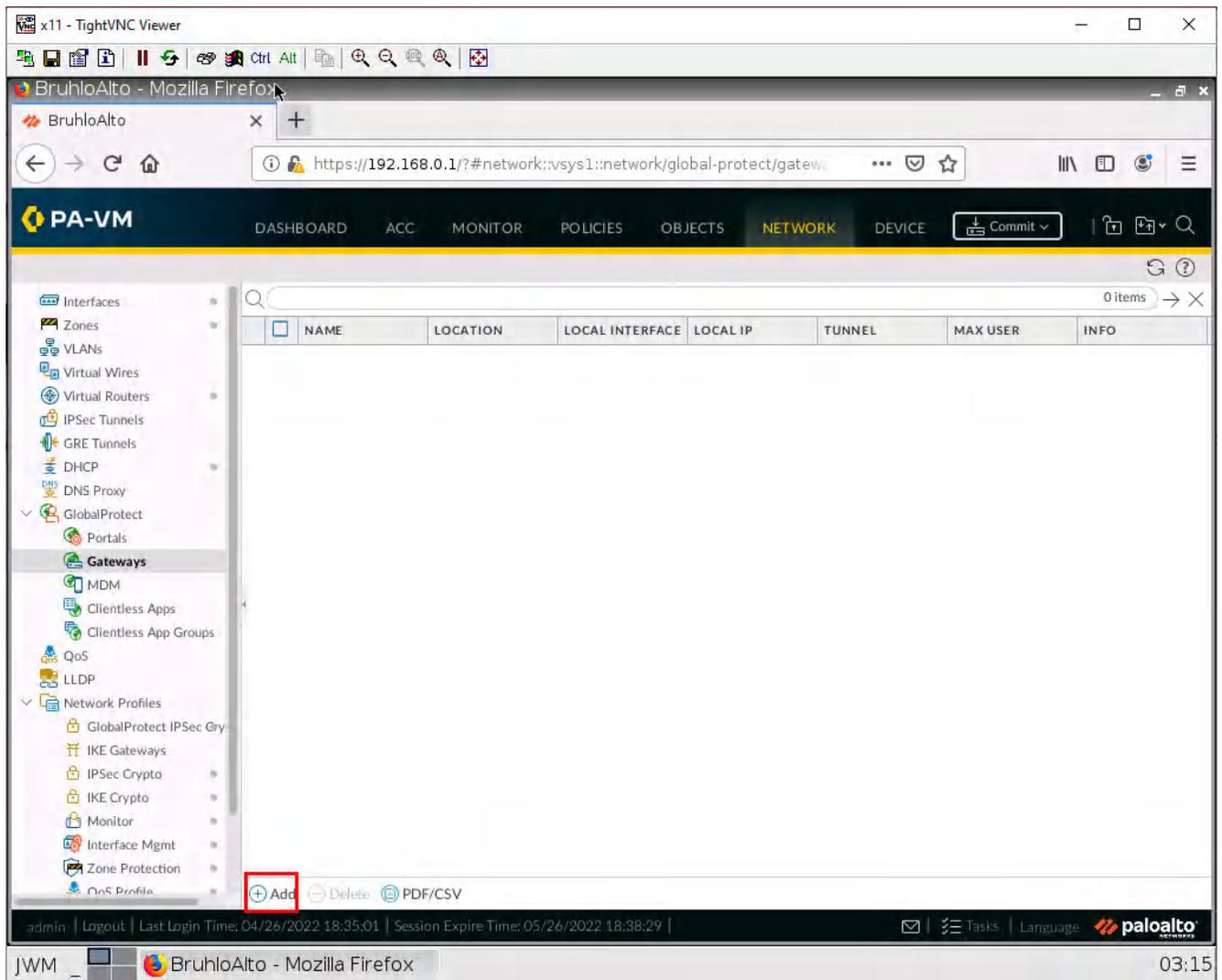


Figure 3.44: Add a Gateway

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

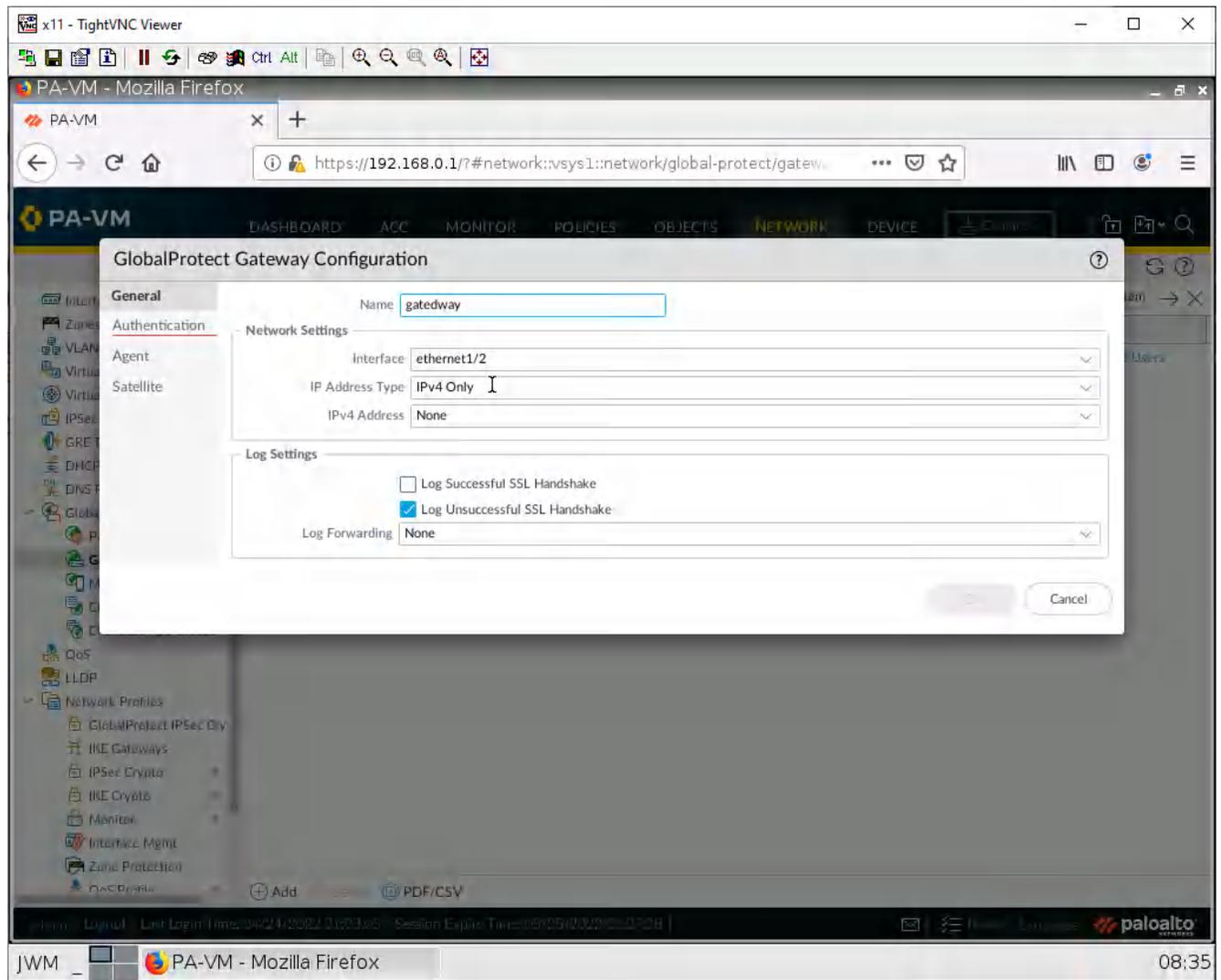


Figure 3.45: GlobalProtect Gateway Configuration

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

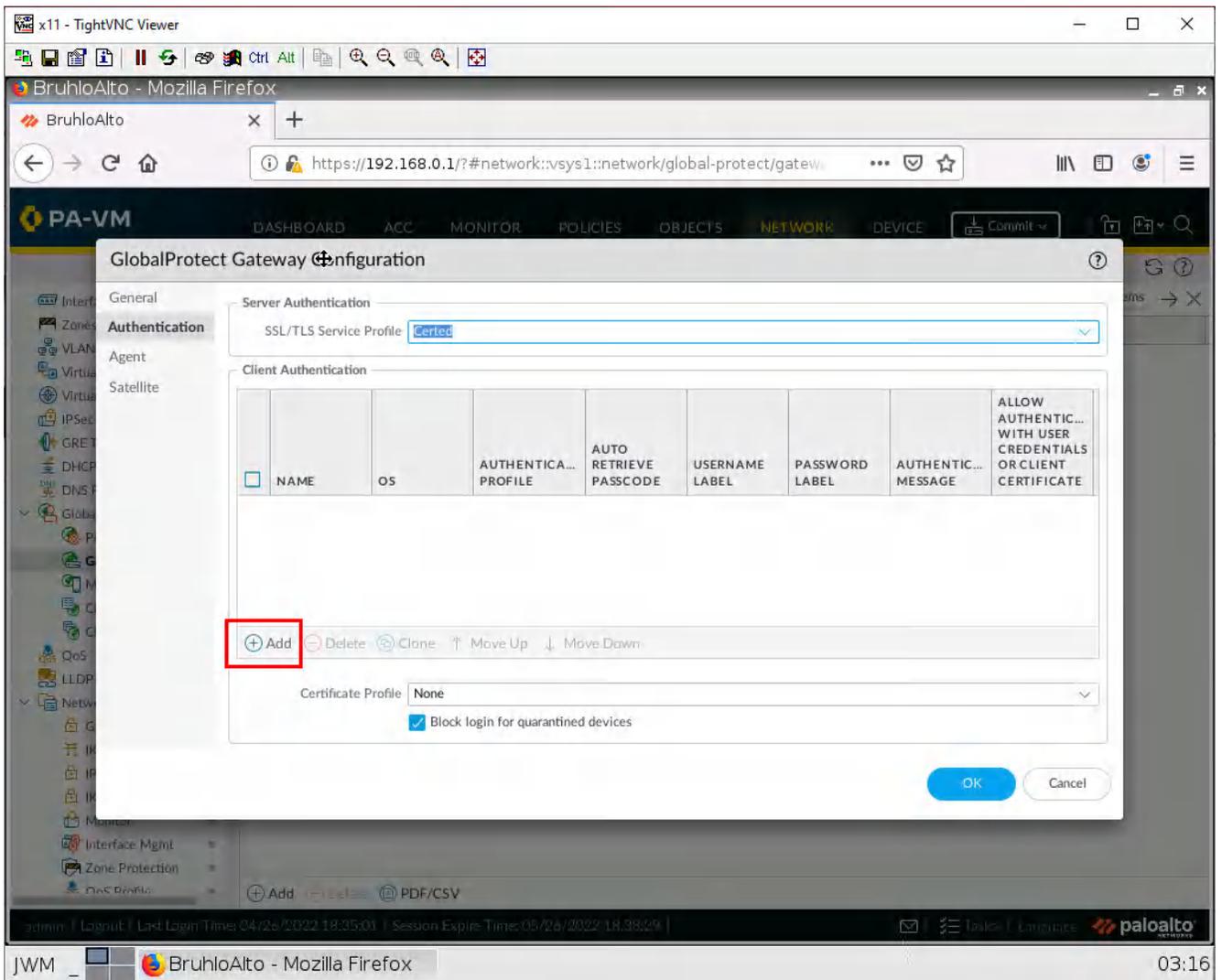


Figure 3.46: SSL/TLS Service Profile

In the new window, select your authentication profile, then click **OK**.

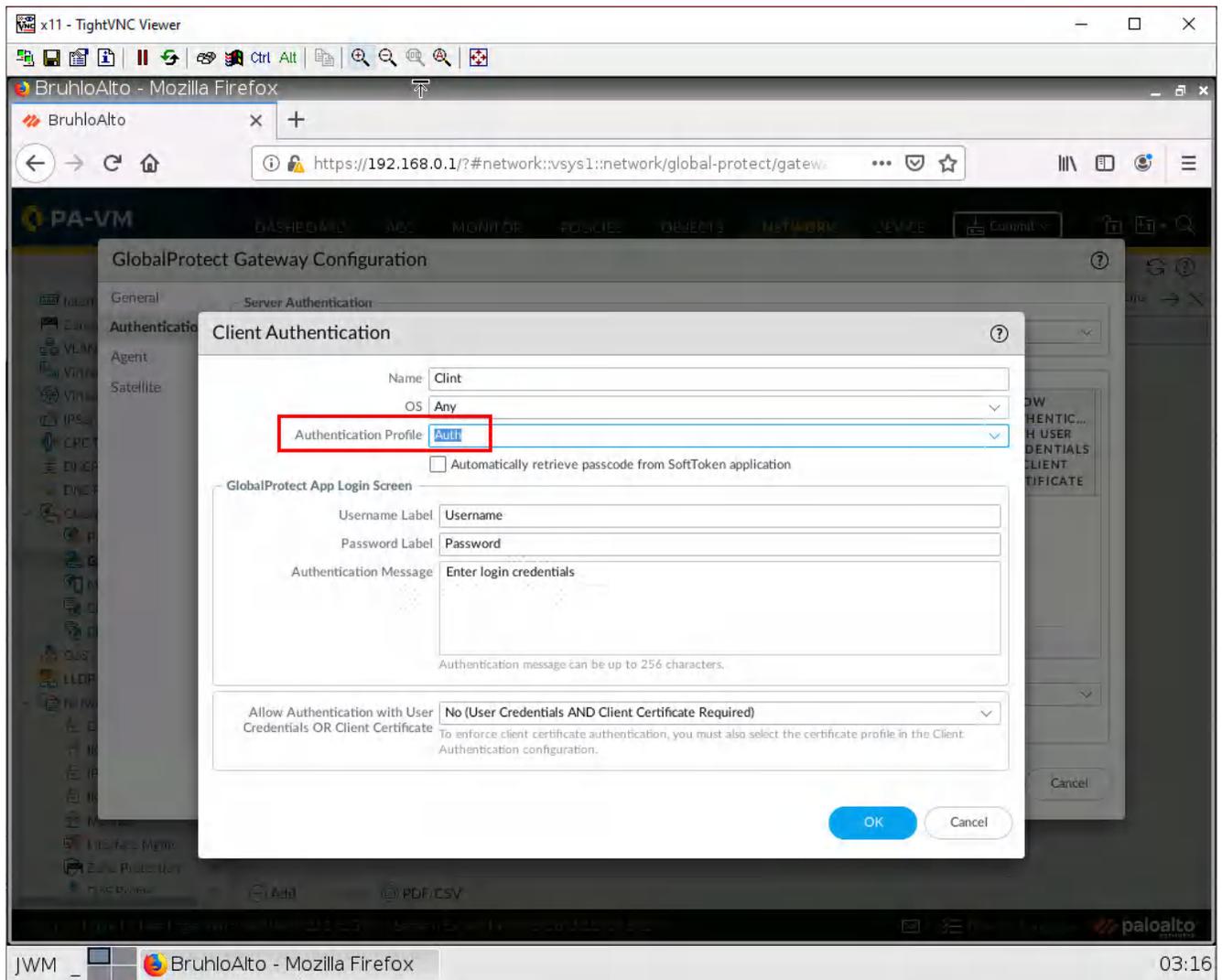


Figure 3.47: Authentication Profile

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

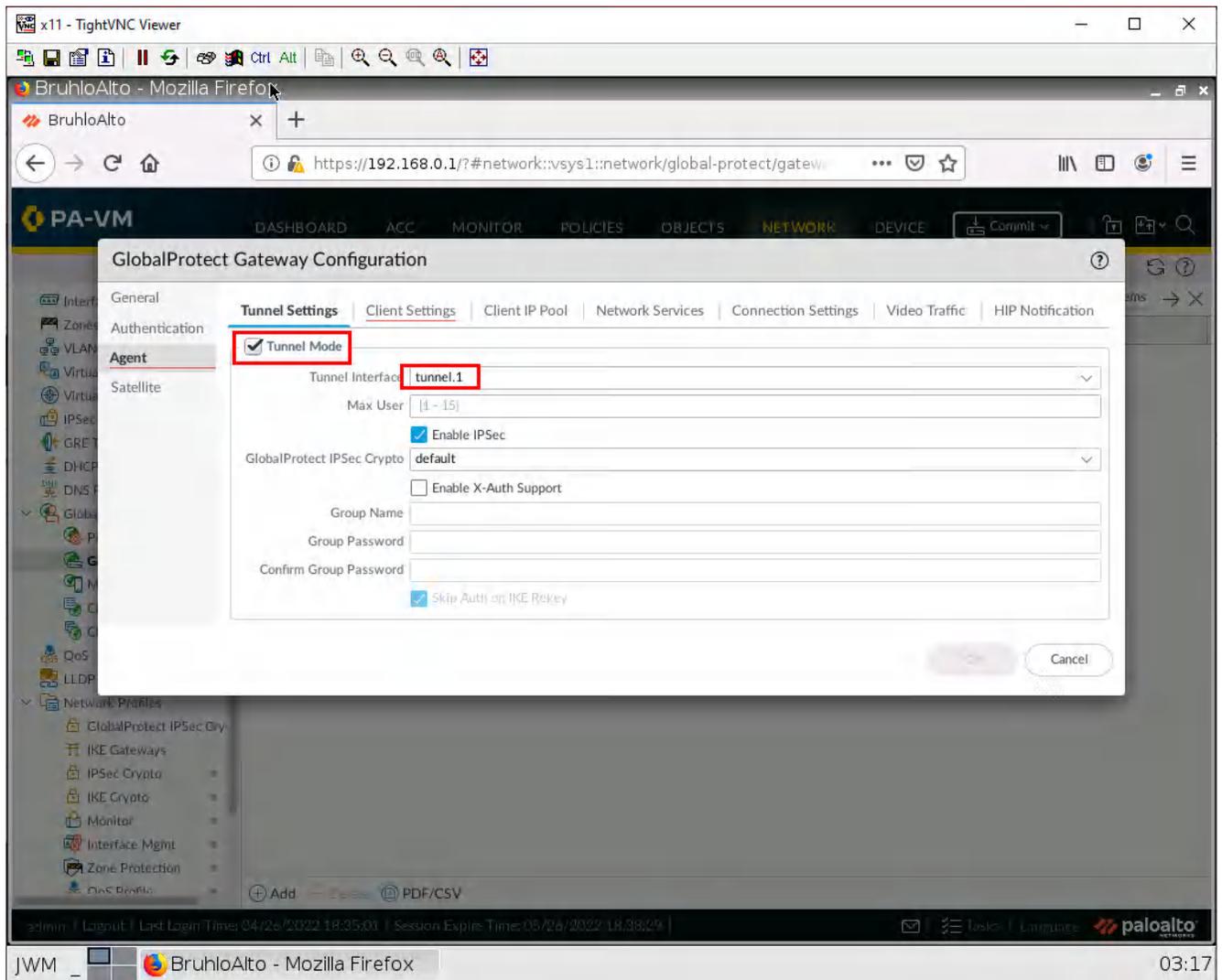


Figure 3.48: Tunnel Mode and Interface

In client settings, click **Add**.

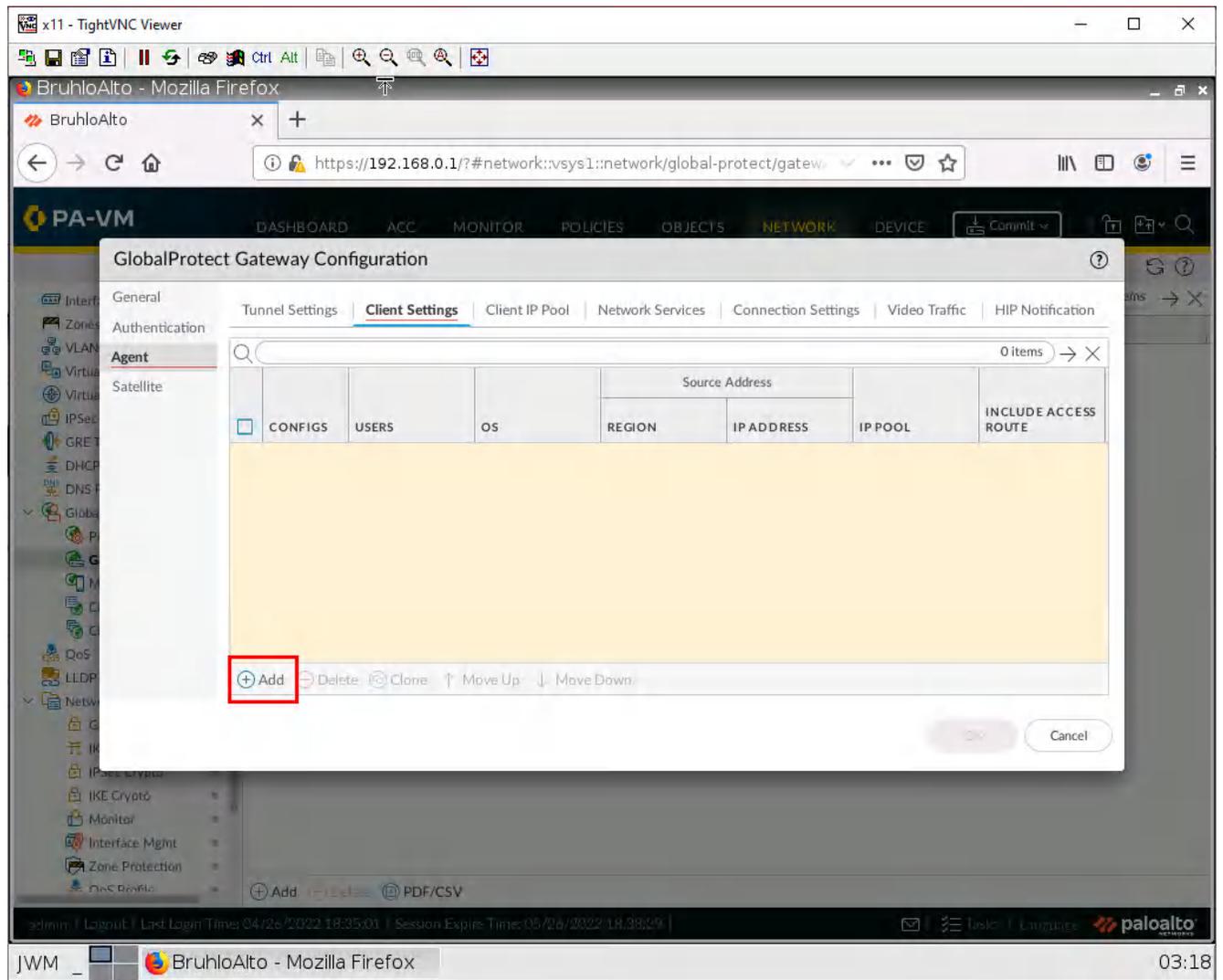


Figure 3.49: Client Settings

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

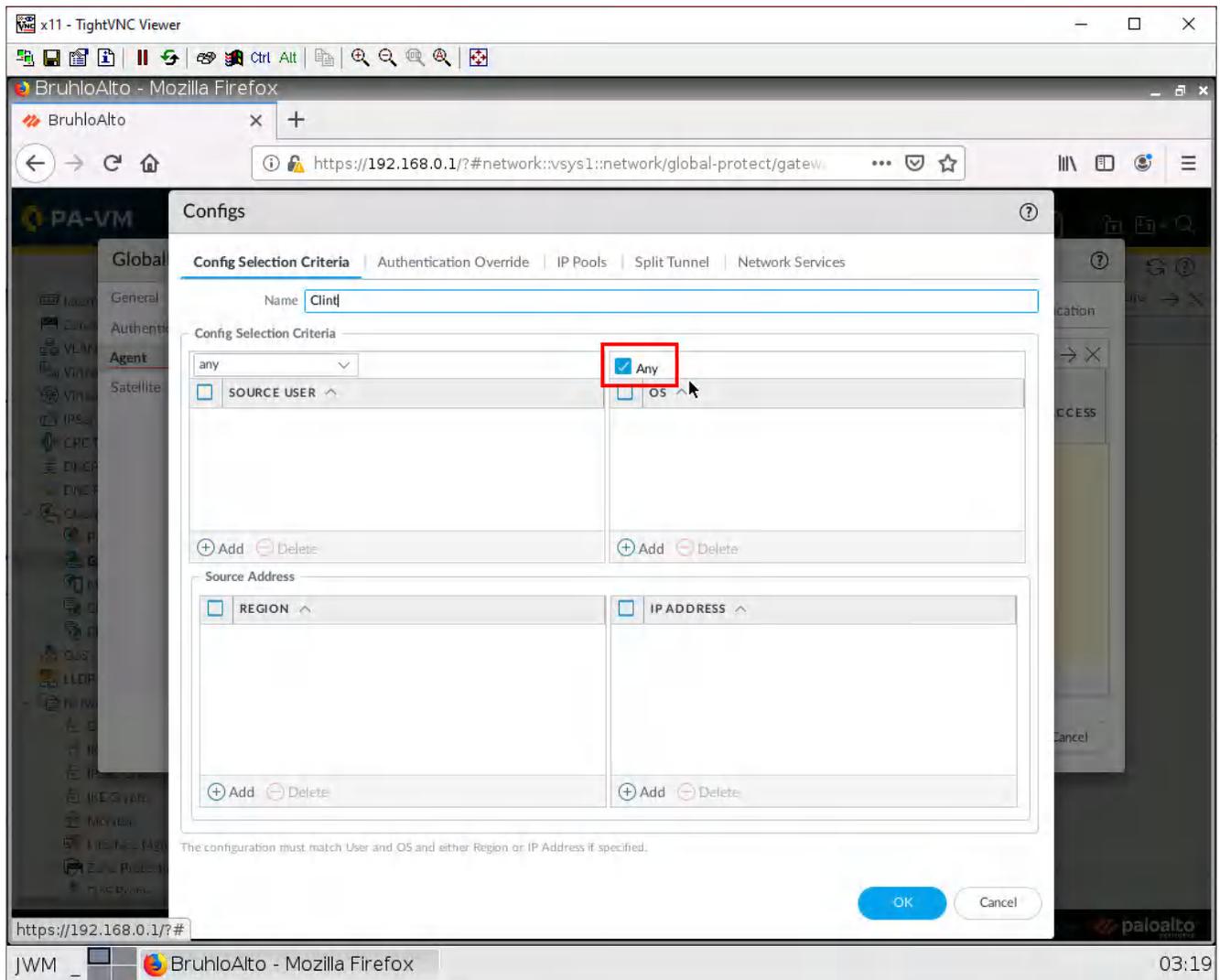


Figure 3.50: Select Client as Any

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

**172.16.10.1-172.16.10.10**

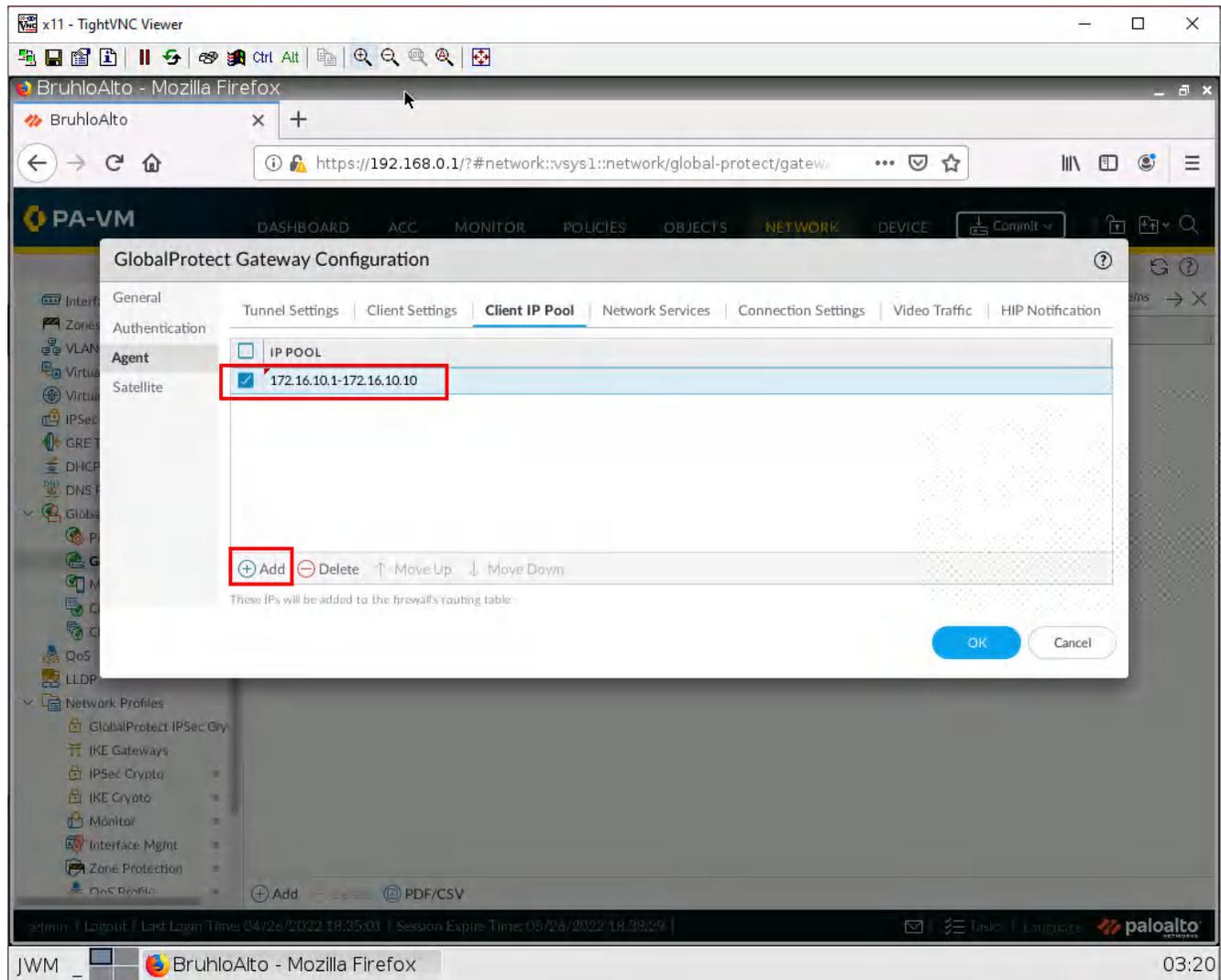


Figure 3.51: IP Pool Configuration

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

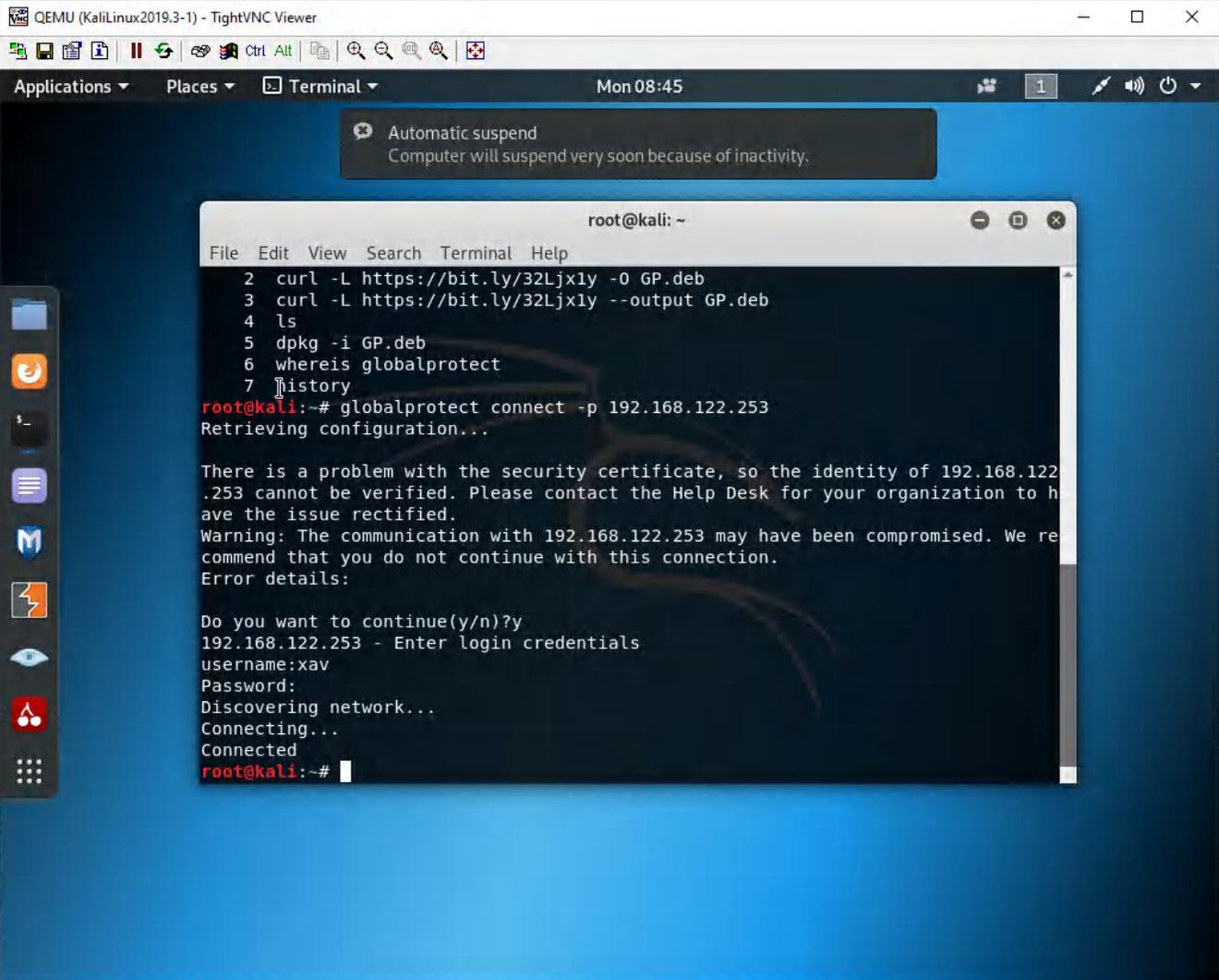
## Install the GlobalProtect Client on Kali

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.



```
QEMU (KaliLinux2019.3-1) - TightVNC Viewer
Applications Places Terminal Mon 08:45
Automatic suspend
Computer will suspend very soon because of inactivity.

root@kali: ~
File Edit View Search Terminal Help
2 curl -L https://bit.ly/32Ljx1y -o GP.deb
3 curl -L https://bit.ly/32Ljx1y --output GP.deb
4 ls
5 dpkg -i GP.deb
6 whereis globalprotect
7 history
root@kali:~# globalprotect connect -p 192.168.122.253
Retrieving configuration...

There is a problem with the security certificate, so the identity of 192.168.122.253 cannot be verified. Please contact the Help Desk for your organization to have the issue rectified.
Warning: The communication with 192.168.122.253 may have been compromised. We recommend that you do not continue with this connection.
Error details:

Do you want to continue(y/n)?y
192.168.122.253 - Enter login credentials
username:xav
Password:
Discovering network...
Connecting...
Connected
root@kali:~#
```

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).

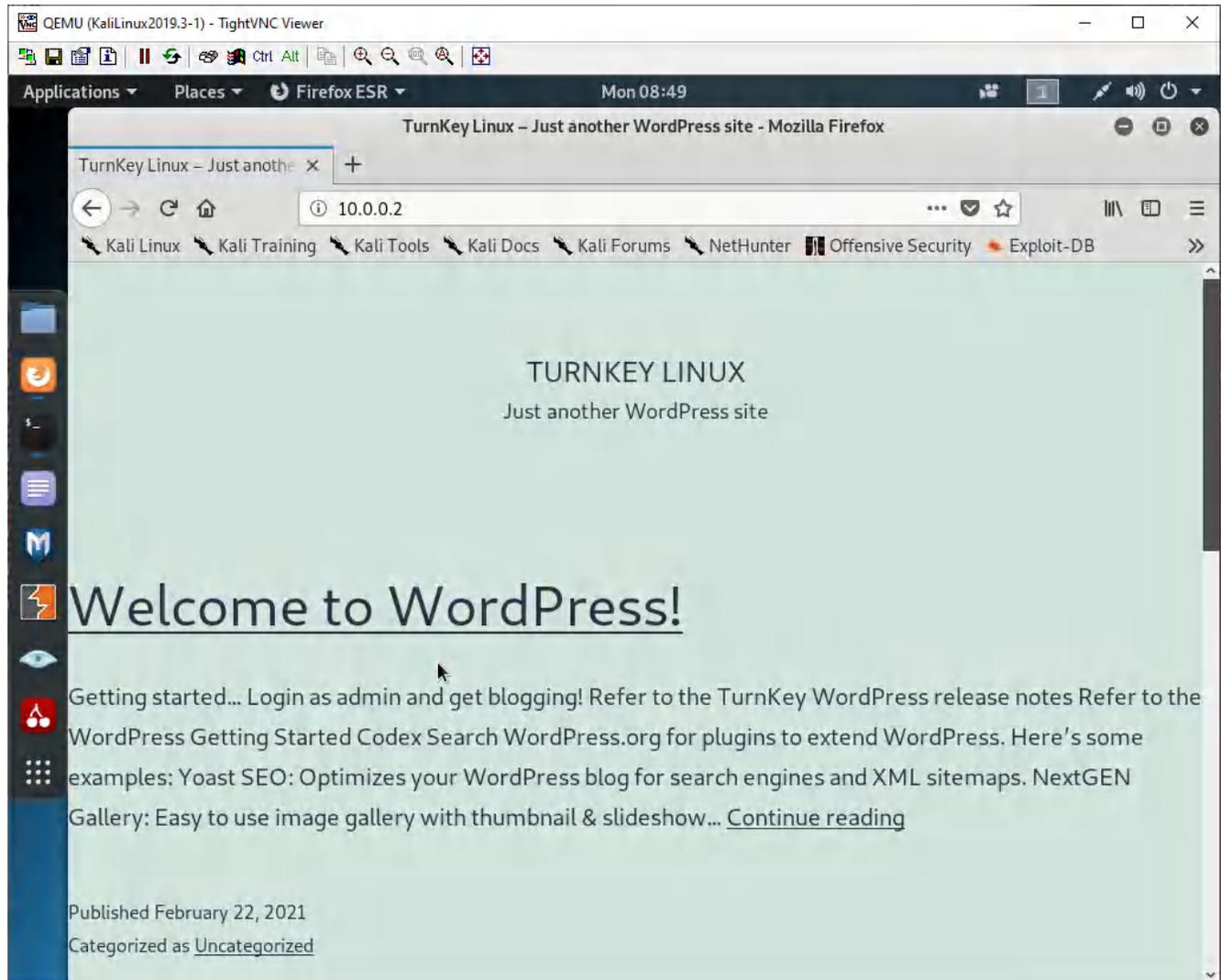


Figure 3.53: Verify your configuration

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.

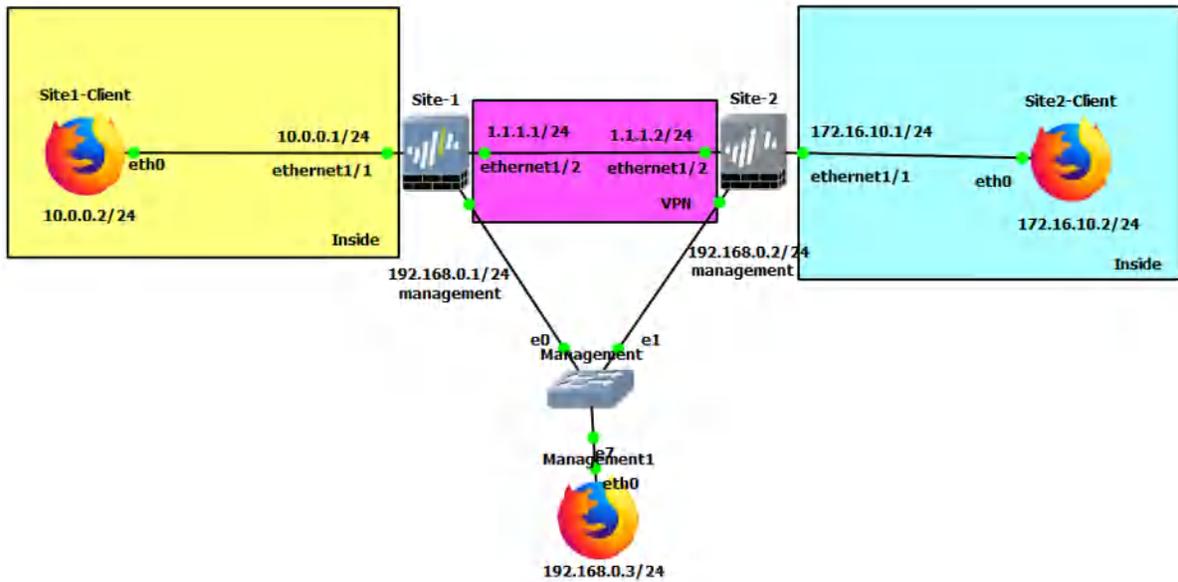


Figure 3.54: Main scenario

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

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

The screenshot shows the Palo Alto VM web interface. The left sidebar contains a navigation tree with 'IKE Gateways' selected under 'Network Profiles'. The main content area displays a table with columns for NAME, PEER ADDRESS, LOCAL ADDRESS (INTERFACE, IP), PEER ID (ID, TYPE), and LOCAL ID (ID, TYPE). The table is currently empty. At the bottom of the table, there is a row of action buttons: '+ Add', '- Delete', 'Enable', 'Disable', and 'PDF/CSV'. The 'Add' button is highlighted with a red box. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. The bottom status bar shows the user 'admin', session information, and the Palo Alto logo.

	NAME	PEER ADDRESS	Local Address		Peer ID		Local ID	
			INTERFACE	IP	ID	TYPE	ID	TYPE
0 items								

Figure 3.55: Add an IKE Gateway

On the Site1 firewall, configure these settings:

**Table 3.11: Site1 IKE Gateway Configuration**

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	<i>Password Here</i>
Confirm Pre-shared key	<i>Confirm Password Here</i>

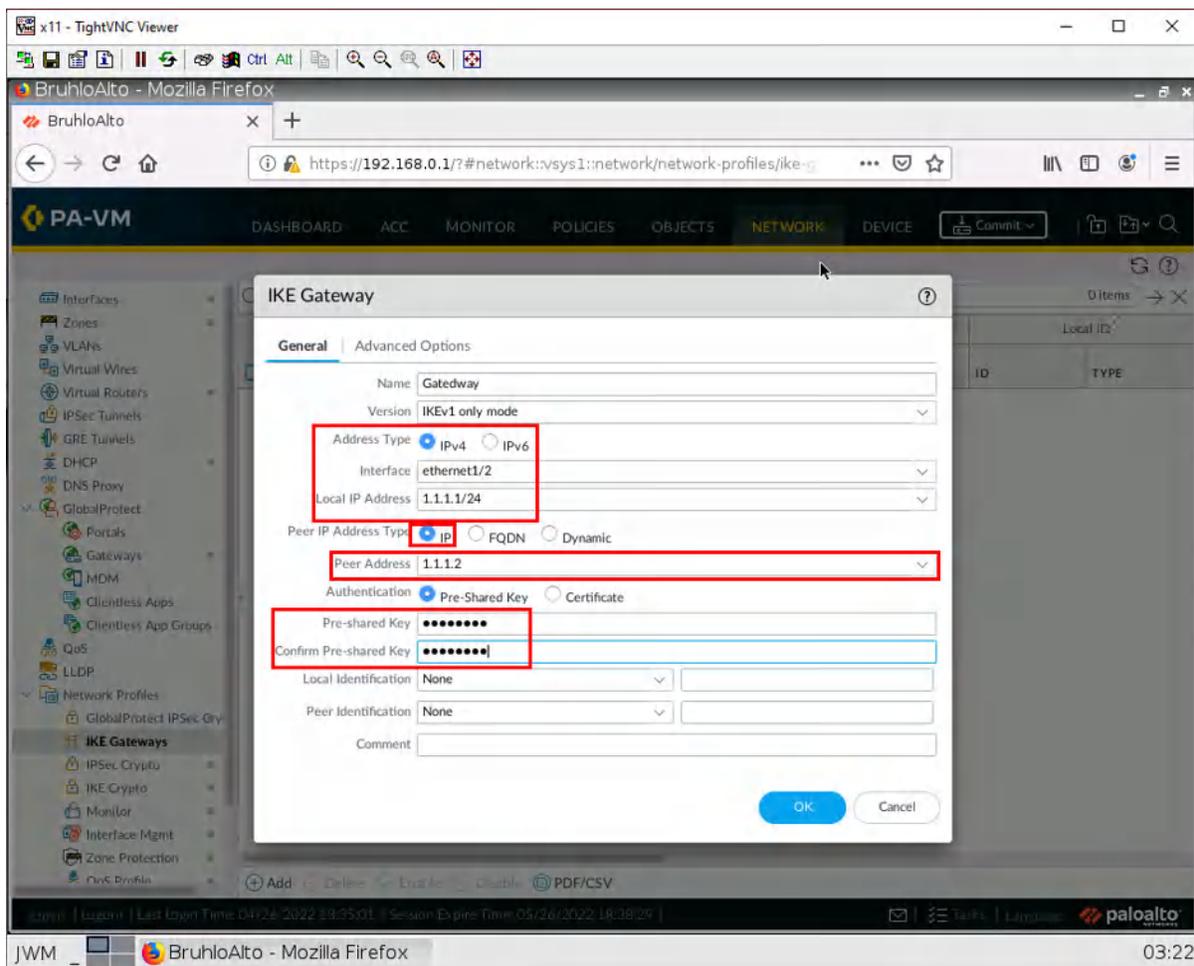


Figure 3.56: Site1 Firewall: IKE Gateway Configuration

Then press **OK**.

On the Site2 firewall, configure these settings:

**Table 3.12: Site2 IKE Gateway Configuration**

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	<i>Same Password as before here</i>
Confirm Pre-shared key	<i>Confirm same password as before here</i>

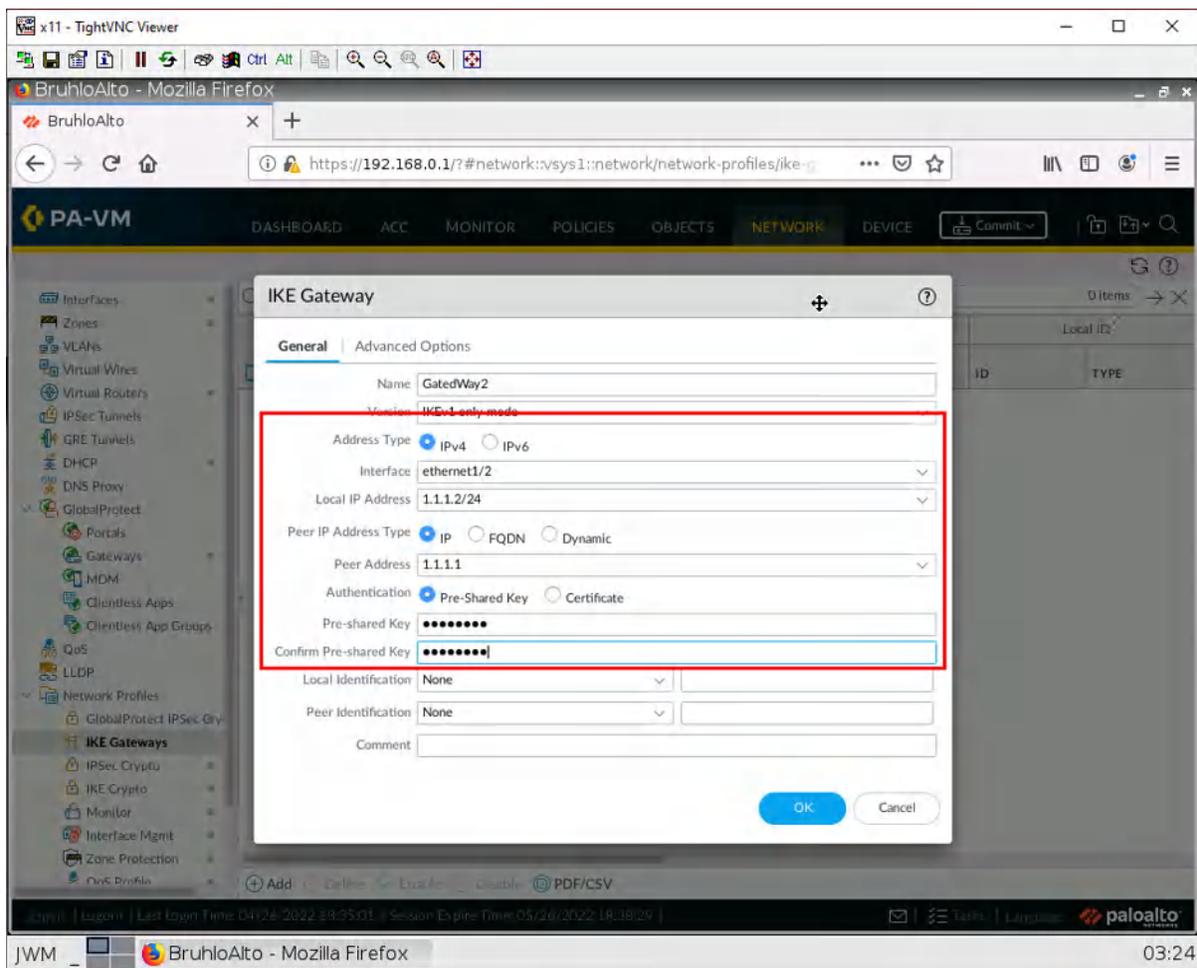


Figure 3.57: Site2 Firewall: IKE Gateway Configuration

Then press **OK**.

## Create an IPsec Tunnel

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

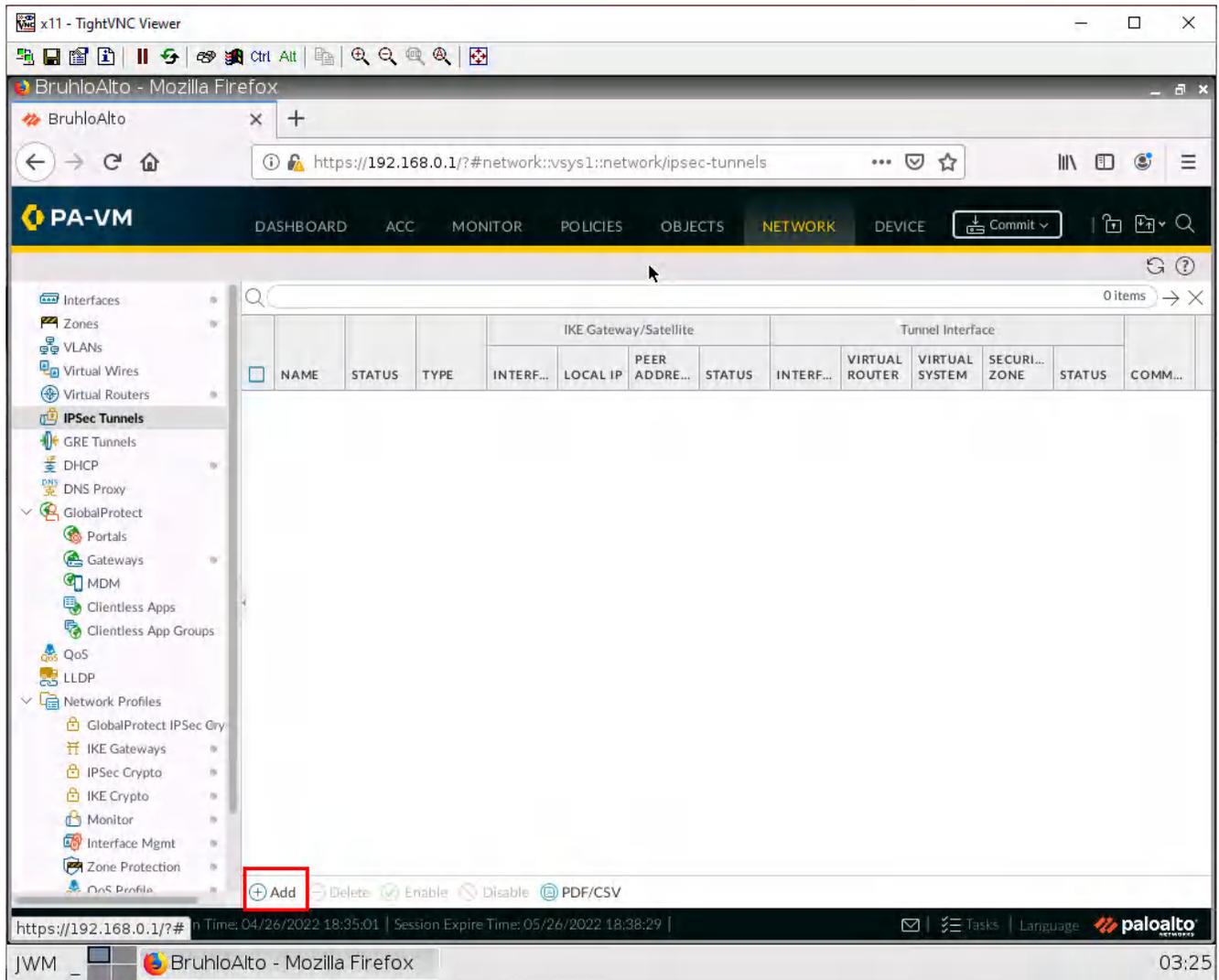


Figure 3.58: Site1 Firewall: Add an IPsec Tunnel

On both firewalls, configure these settings:

**Table 3.13: IPsec Tunnel Configuration**

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

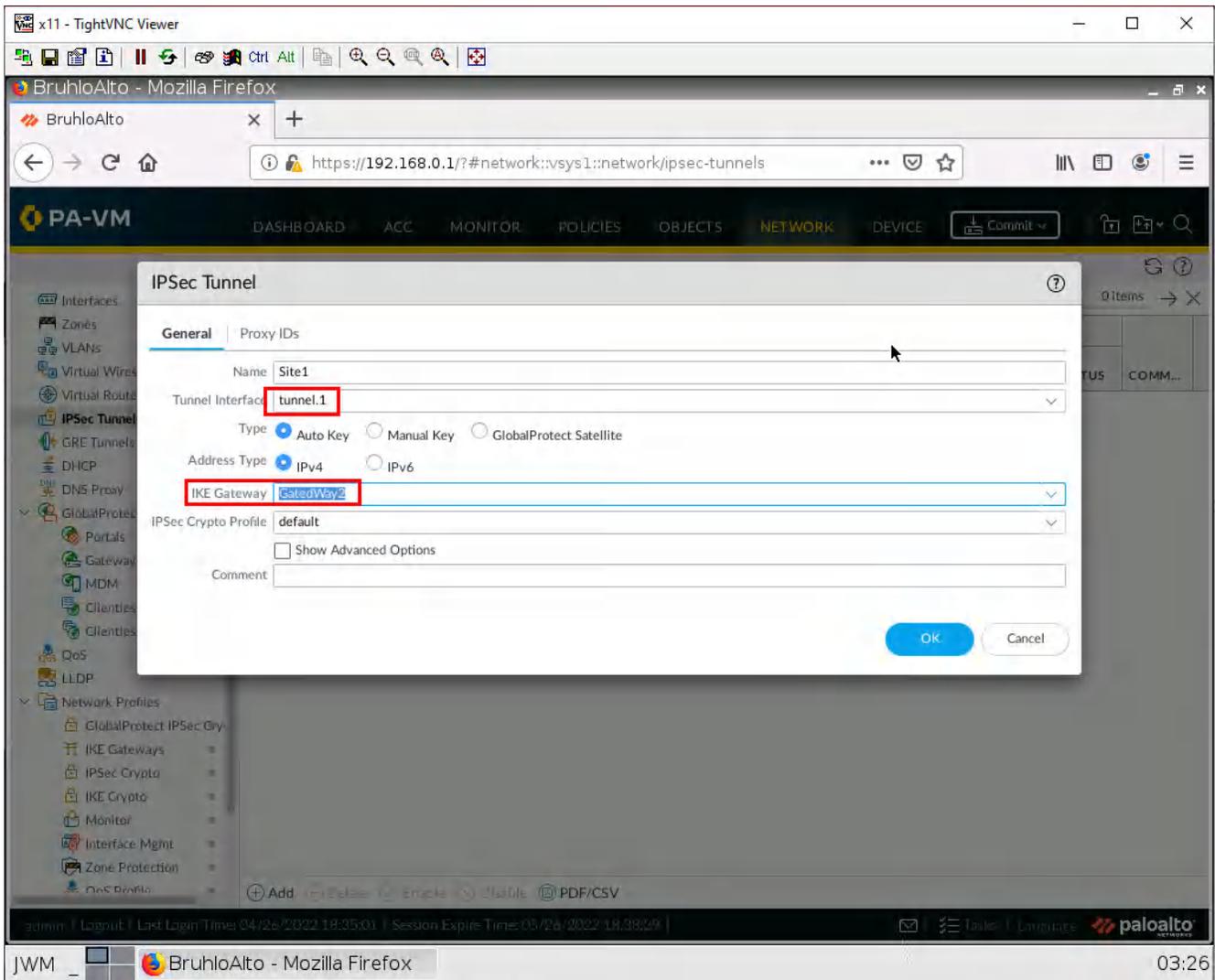


Figure 3.59: Site1 and Site2 Firewall: IPsec Tunnel Configuration

## Create Static Routes

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

The screenshot displays the Palo Alto VM configuration interface in a Mozilla Firefox browser window. The URL is `https://192.168.0.1/#network:vsys1::network/virtual-routers`. The interface shows a sidebar with various configuration categories, and the main area displays a table of virtual routers. The 'default' virtual router is selected and highlighted with a red box. The table shows the following configuration:

NAME	INTERFACES	CONFIGURA...	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
default	ethernet1/2 ethernet1/1.10 ethernet1/1.20 tunnel.1	ECMP status: Disabled						More Runtime Stats

The interface also includes a search bar, a 'Commit' button, and a status bar at the bottom showing the login time (04/26/2022 18:35:01) and session expire time (05/26/2022 18:38:29). The Palo Alto logo is visible in the bottom right corner.

Figure 3.60: Virtual Routers Configuration

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

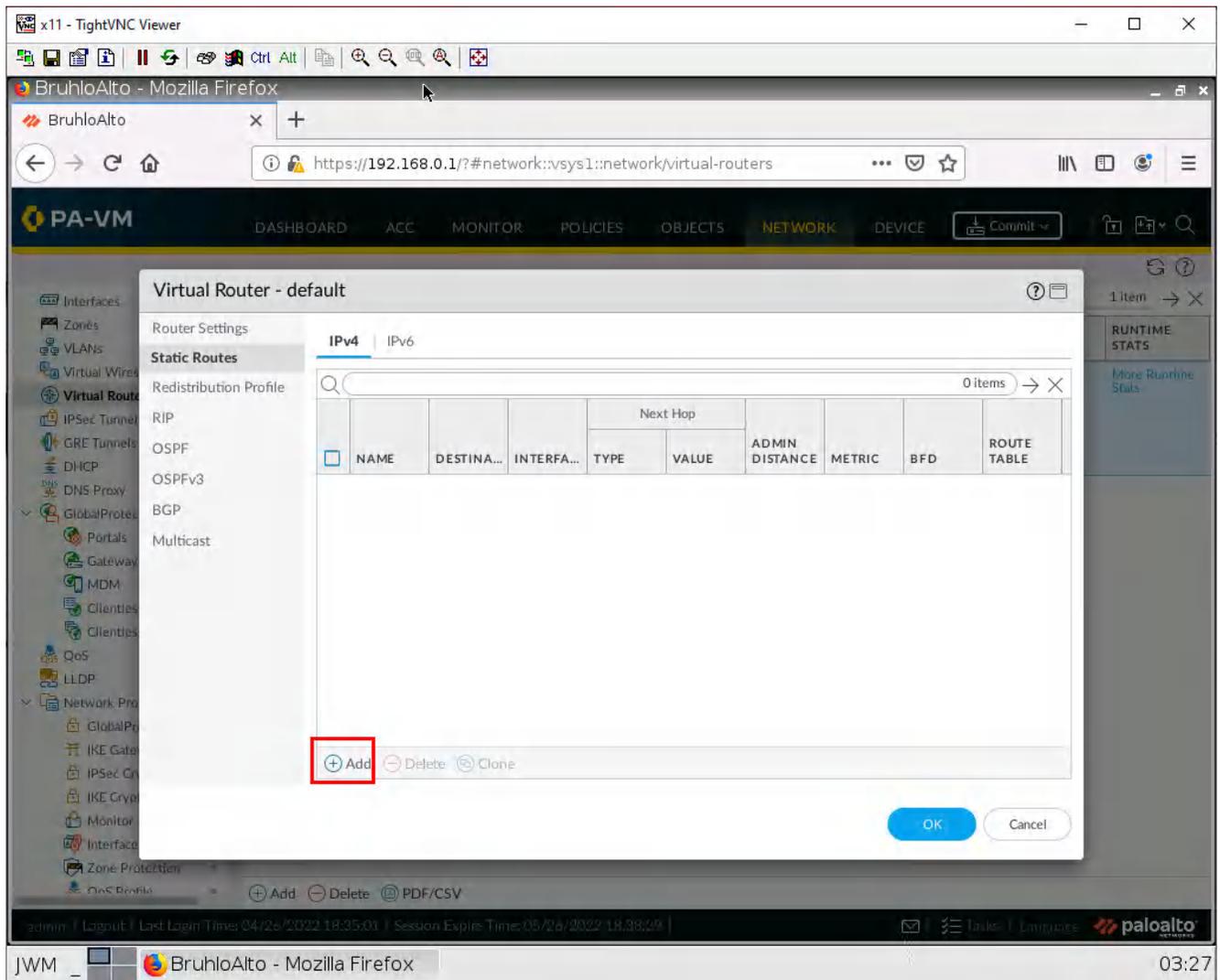


Figure 3.61: Add a Static Route in the Site1

On the Site1 firewall, configure these settings:

**Table 3.14: Site1 Static Route Configuration**

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

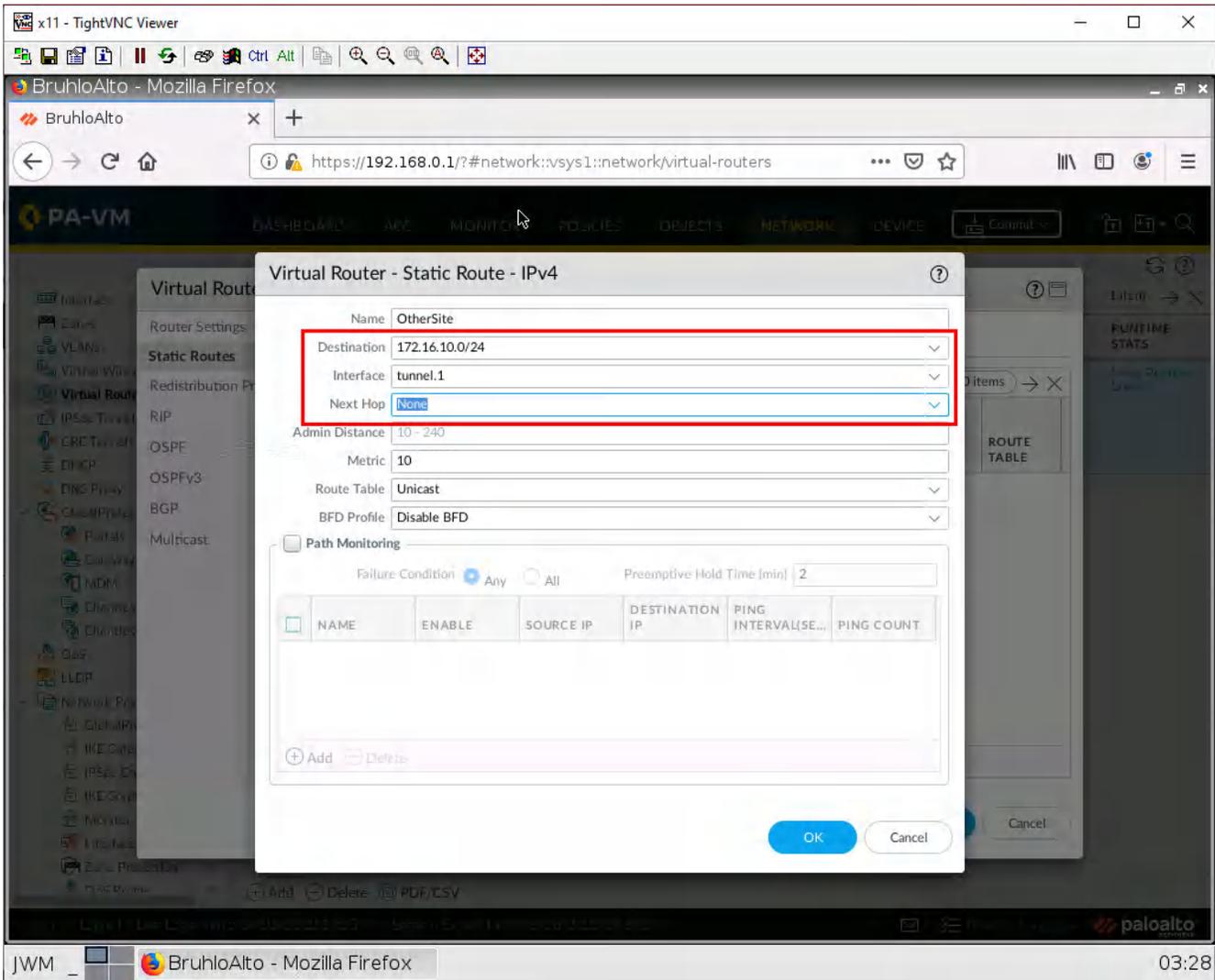


Figure 3.62: Static Route Configuration in the Site1

On the Site2 firewall, configure these settings:

**Table 3.15: Site2 Static Route Configuration**

Parameters	Value
Destination	10.0.0.0/24
Interface	tunnel.1
Next Hop	None

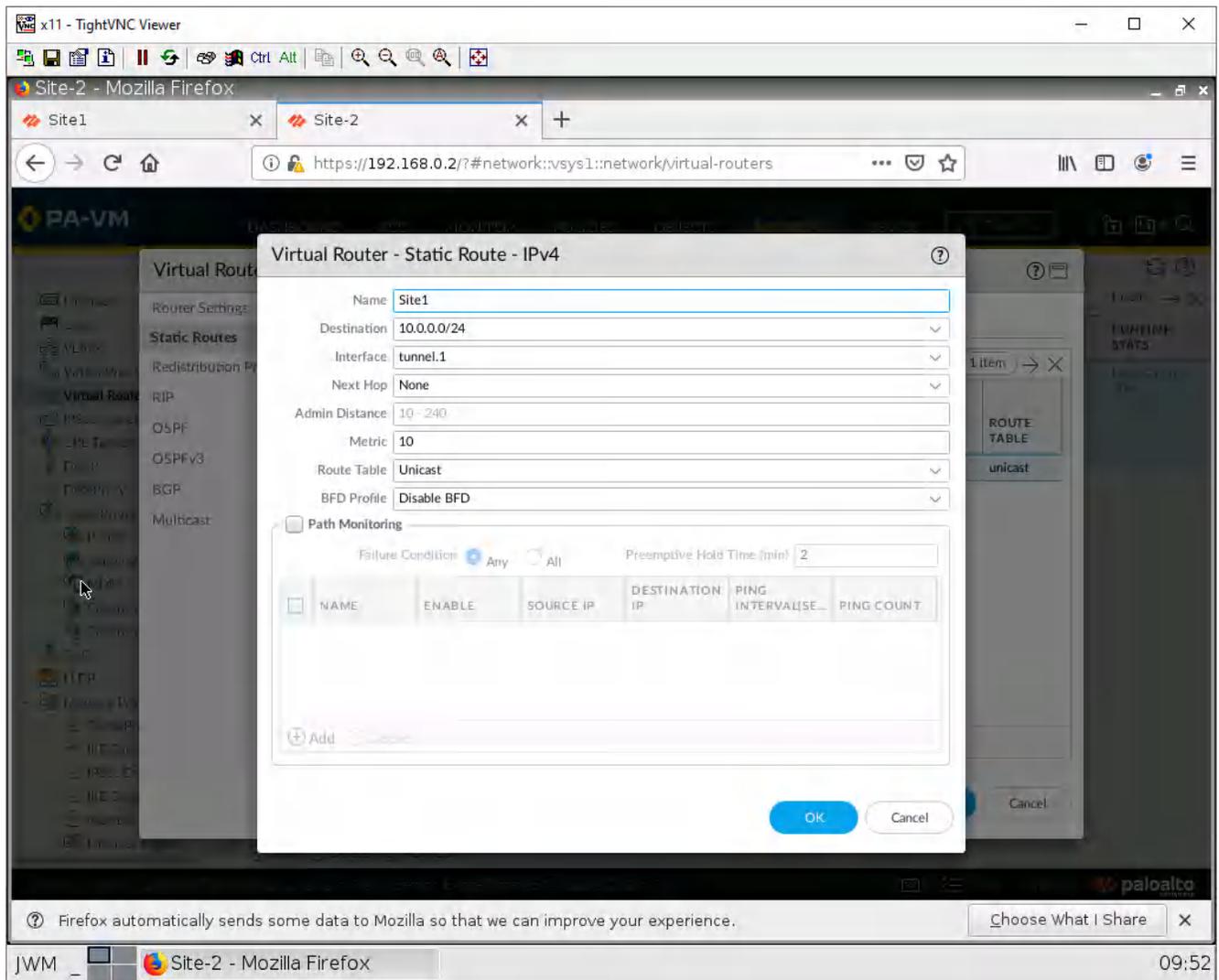


Figure 3.63: Static Route Configuration in the Site 2

Then press **OK**.

## Test the Site-to-Site

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

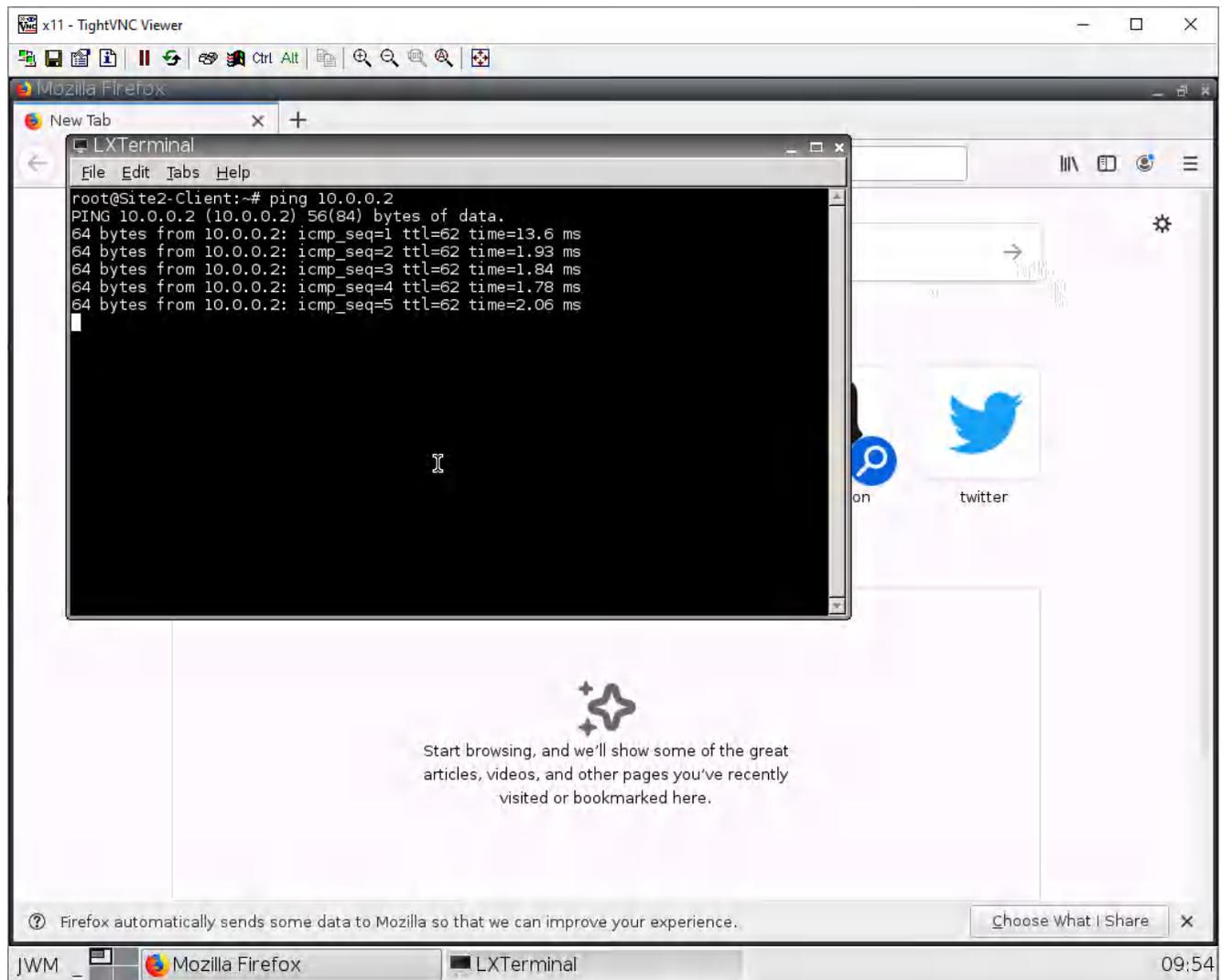


Figure 3.64: Verify your configuration

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

# Chapter 4. Cloud Technologies



## 4.1 IPsec VPN between Palo Alto on Premise and Microsoft 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:** We are going to connect on-premise Palo Alto to Azure Virtual Gateway. This is going to be IPsec VPN between Palo Alto and Azure. First, we'll configure Azure and then connect Palo Alto through Port1 to Azure Virtual Gateway.

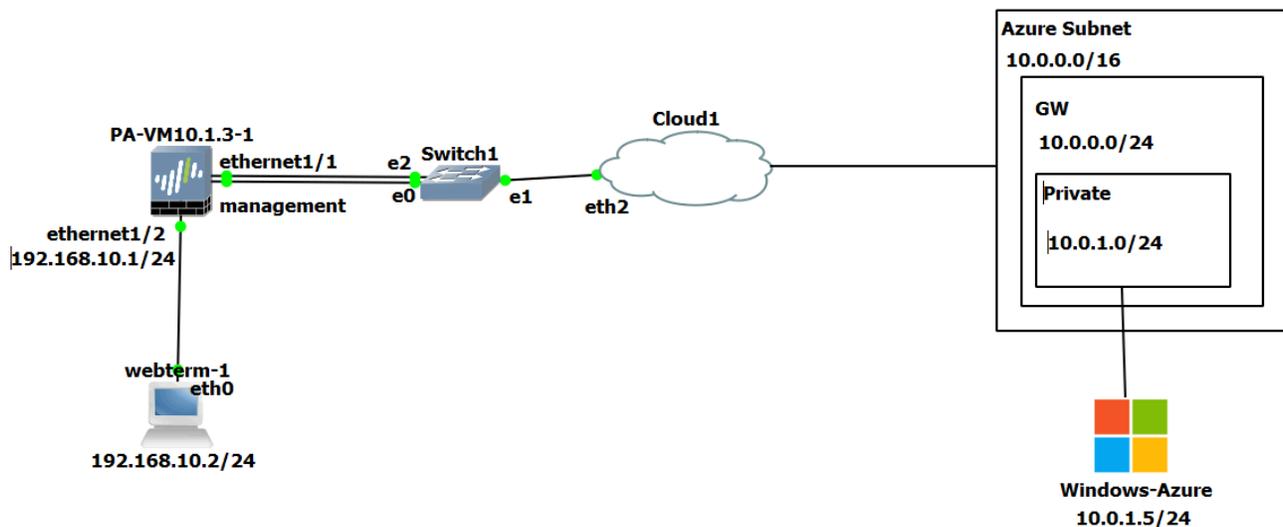


Figure 4.1: Main scenario

## Azure Configuration

1. Create a resource group in Azure as follows:

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

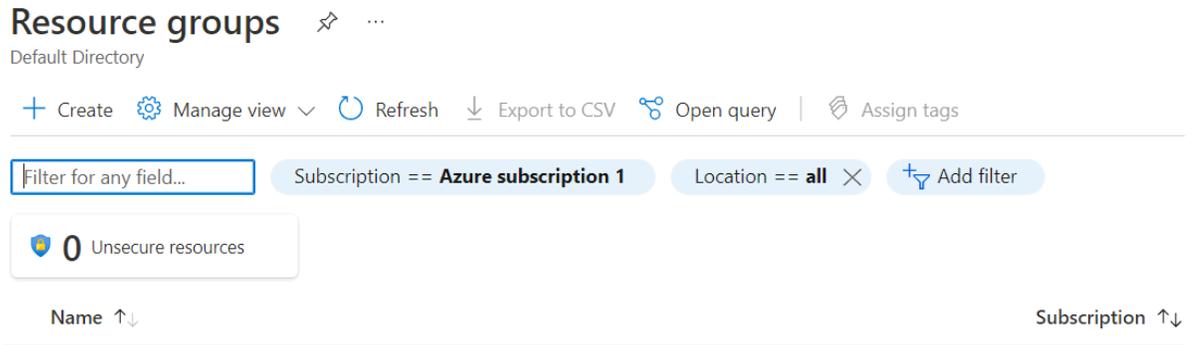


Figure 4.2: Create a resource group

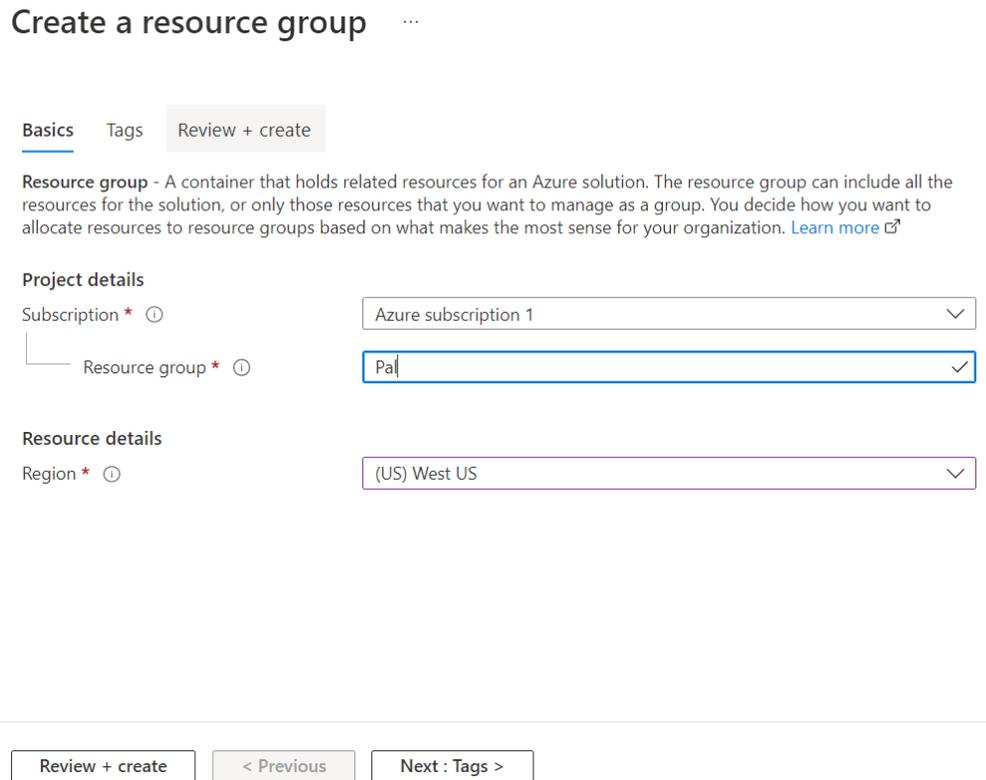


Figure 4.3: Create a resource group

✔ Validation passed.

Basics   Tags   Review + create

Basics

Subscription	Azure subscription 1
Resource group	Pal
Region	West US

Tags

None

---

        [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 network ...

Basics IP Addresses Security Tags Review + create

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

### Project details

Subscription \* ⓘ Azure subscription 1

Resource group \* ⓘ Pal  
[Create new](#)

### Instance details

Name \* Azure-Pa|

Region \* West US

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

Figure 4.5: Create a virtual network

Home > Virtual networks >

### Create virtual network ...

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

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

**IPv4 address space**

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

Add IPv6 address space ⓘ

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

+ Add subnet + Remove subnet

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

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

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

#### Edit subnet

Subnet address range \* ⓘ

10.0.1.0/24 ✓  
 10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

**NAT GATEWAY**

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

NAT gateway  
 None

**SERVICE ENDPOINTS**

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

Services ⓘ  
 0 selected

Save
Cancel

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

### Create virtual network

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

BastionHost  Disable  Enable

DDoS Protection Standard  Disable  Enable

Firewall  Disable  Enable

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

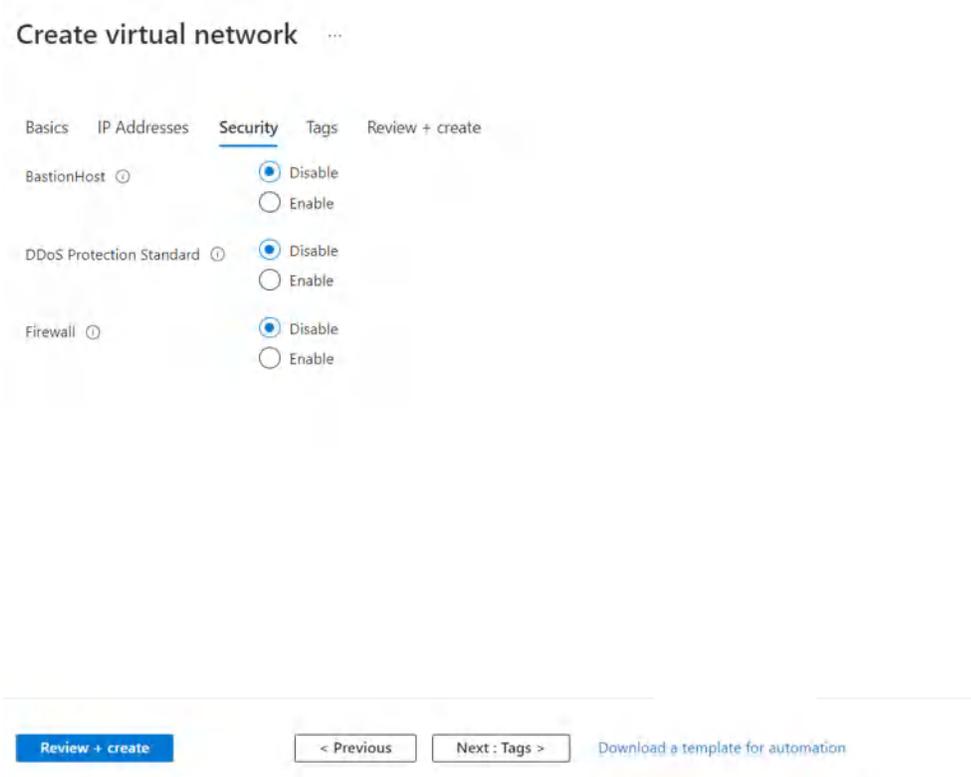


Figure 4.7: Create a virtual network

### Create virtual network

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

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

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

Name  Value

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

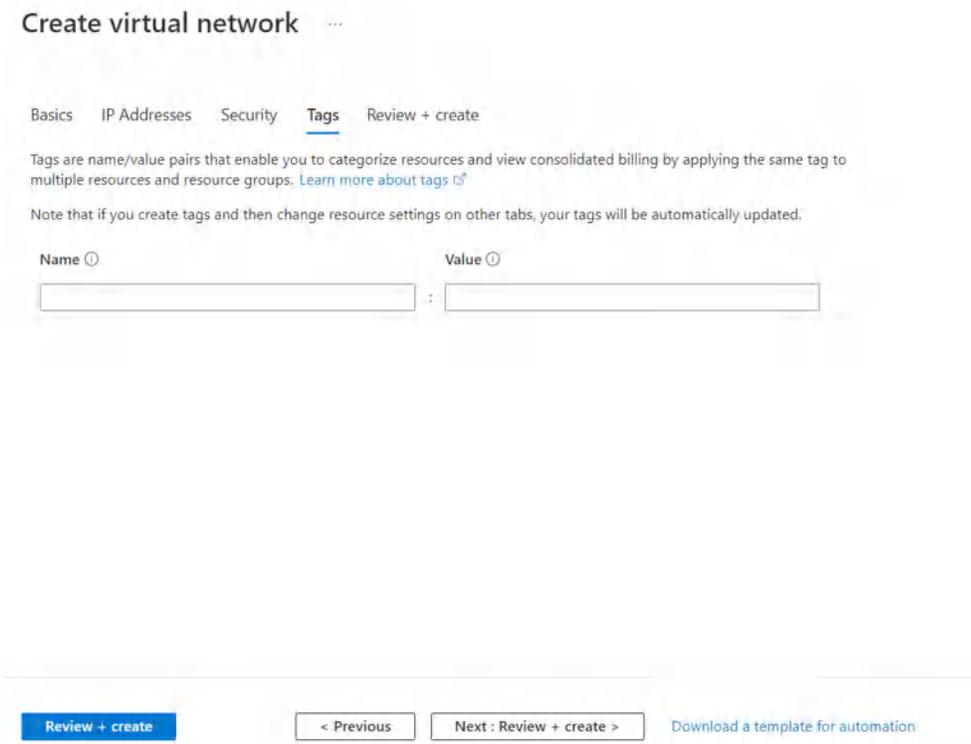


Figure 4.8: Create a virtual network

## Create virtual network ...

✓ Validation passed

Basics IP Addresses Security Tags Review + create

### Basics

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

### IP addresses

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

### Tags

None

  
**Create**

< Previous

Next >

[Download a template for automation](#)

Figure 4.9: Create a virtual network

3. Create a virtual network gateway as following:

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

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

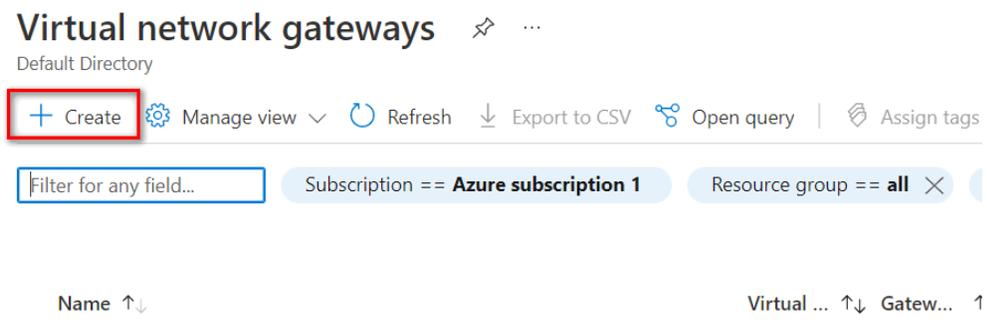


Figure 4.10: Create a virtual network gateway

## Create virtual network gateway ...

Subscription \*

Resource group ⓘ Pal (derived from virtual network's resource group)

**Instance details**

Name \*

Region \*

Gateway type \* ⓘ  VPN  ExpressRoute

VPN type \* ⓘ  Route-based  Policy-based

SKU \* ⓘ

Generation ⓘ

Virtual network \* ⓘ

[Create virtual network](#)

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

[Review + create](#) [Previous](#) [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 - 10.0.1.255 (256 addresses)

Public IP Address Type \* ⓘ  Basic  Standard

**Public IP address**

Public IP address \* ⓘ  Create new  Use existing

Public IP address name \*

Public IP address SKU Standard

Assignment  Dynamic  Static

Enable active-active mode \* ⓘ  Enabled  Disabled

Configure BGP \* ⓘ  Enabled  Disabled

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

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

Figure 4.12: Create a virtual network gateway

## Create virtual network gateway

Validation passed

Basics Tags **Review + create**

**Basics**

Subscription	Azure subscription 1
Resource group	Pal
Name	Azure-VPN-Pal
Region	West US
SKU	VpnGw2
Generation	Generation1
Virtual network	Azure-Pal
Subnet	GatewaySubnet (10.0.1.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP	Disabled
Public IP address	AzurePublic

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

Figure 4.13: Create a virtual network gateway

We'd love your feedback! →

Deployment is in progress


 Deployment name: Microsoft.VirtualNetworkGateway-202205011... Start time: 5/1/2022, 12:03:41 PM  
 Subscription: [Azure subscription 1](#) Correlation ID: 4b078a9d-11d3-4f4b-91fa-5bf1042e8a4c  
 Resource group: [Pal](#)

Deployment details ([Download](#))

Resource	Type	Status	Operation details
----------	------	--------	-------------------

Figure 4.14: Create a virtual network gateway (deployment)

Your deployment is complete


 Deployment name: Microsoft.VirtualNetworkGateway-202205011... Start time: 5/1/2022, 12:03:41 PM  
 Subscription: [Azure subscription 1](#) Correlation ID: 4b078a9d-11d3-4f4b-91fa-5bf1042e...  
 Resource group: [Pal](#)

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

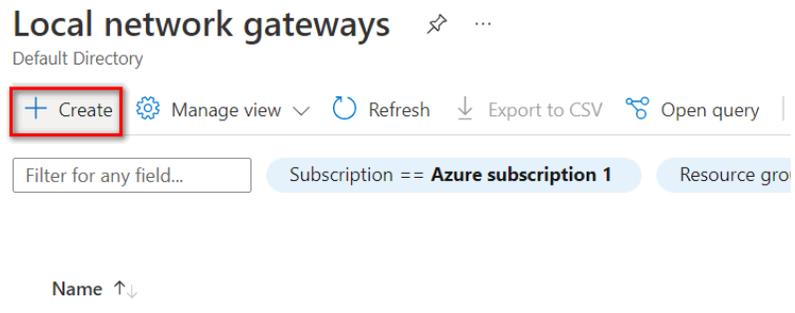


Figure 4.16: Create a local network gateway

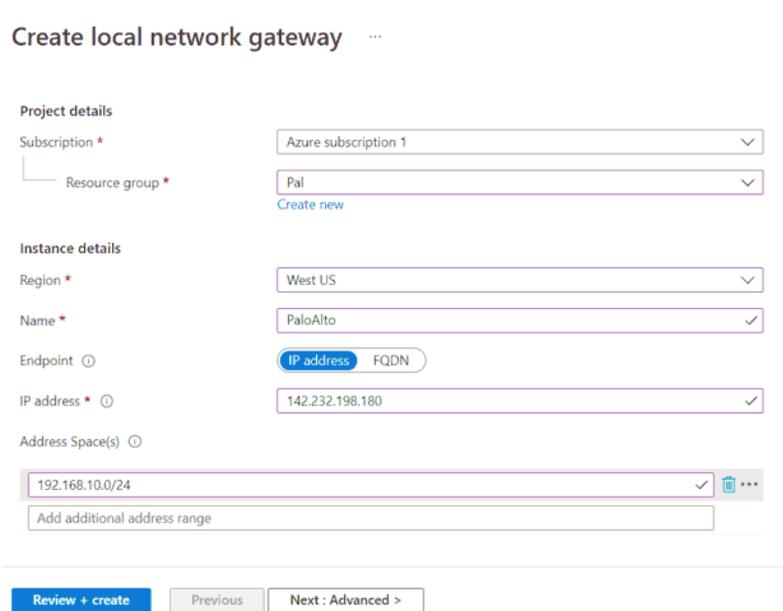


Figure 4.17: Create a local network gateway

## Create local network gateway ...

 Validation passed

Basics   Advanced   **Review + create**

Summary

Name	PaloAlto
Subscription	Azure subscription 1
Resource group	Pal
Region	West US
Endpoint	IP address
IP address	142.232.198.180
Address Space(s)	192.168.10.0/24

[Create](#)   [Previous](#)   [Next](#)

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

 **Your deployment is complete**

 Deployment name: LocalNetworkGatewayCreate-20220501123...   Start time: 5/1/2022, 12:31:33 PM  
Subscription: [Azure subscription 1](#)   Correlation ID: a3a1a10b-d87b-4f9a-bac0-6d05f50b6...  
Resource group: [Pal](#)

∨ **Deployment details** ([Download](#))

∧ **Next steps**

[Go to resource](#)

Figure 4.19: Verify local network gateway deployment

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

**Add connection** ...  
Azure-VPN-Pal

Name \*  
AzureVPN ✓

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

\*Virtual network gateway ⓘ  
Azure-VPN-Pal 🔒

\*Local network gateway ⓘ  
PaloAlto >

Shared key (PSK) \* ⓘ  
123456789 ✓

Use Azure Private IP Address ⓘ

Enable BGP ⓘ

IKE Protocol ⓘ  
 IKEv1  IKEv2

Ingress NAT Rules

**OK**

Figure 4.20: Connection configuration

Based on the Microsoft article [“About cryptographic requirements and Azure VPN gateways”](#), 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** ...  
Virtual network gateway

Search (Ctrl+/) << Refresh → Move ▾ Delete

**Overview**

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

**Essentials**

Resource group (move) : Pal  
 Location : West US  
 Subscription (move) : Azure subscription 1  
 Subscription ID : 9170d5fe-6ca8-4257-9a4b-462d6b7ab3cd

SKU : VpnGw2  
 Gateway type : VPN  
 VPN type : Route-based  
 Virtual network : Azure-Pal  
 Public IP address : 23.101.203.248 (AzurePublic)

Tags (edit) · Click here to add tags

Figure 4.21: Verify the public IP address

## Palo Alto Configuration

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

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/1'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. Under the 'Assign Interface To' section, the 'Virtual Router' is set to 'default' and the 'Security Zone' is set to 'VPN'. There are 'OK' and 'Cancel' buttons at the bottom right.

Figure 4.22: Ethernet 1/1 Config

The screenshot shows the 'Ethernet Interface' configuration window with the 'IPv4' tab selected. The 'Interface Name' is 'ethernet1/1'. Under the 'Type' section, 'DHCP Client' is selected. The 'Enable' checkbox is checked, and 'Automatically create default route pointing to default gateway provided by server' is also checked. The 'Send Hostname' checkbox is unchecked, and the 'Default Route Metric' is set to '10'. There is a 'Show DHCP Client Runtime Info' link below the metric field. There are 'OK' and 'Cancel' buttons at the bottom right.

Figure 4.23: Ethernet 1/1 IPV4

**Ethernet Interface** ⓘ

Interface Name: ethernet1/2  
Comment:   
Interface Type: Layer3  
Netflow Profile: None

**Config** | IPv4 | IPv6 | SD-WAN | Advanced

**Assign Interface To**

Virtual Router: default  
Security Zone: LAN

OK Cancel

Figure 4.24: Ethernet 1/2 Config

**Ethernet Interface** ⓘ

Interface Name: ethernet1/2  
Comment:   
Interface Type: Layer3  
Netflow Profile: None

**Config** | **IPv4** | IPv6 | SD-WAN | Advanced

Enable SD-WAN  
Type:  Static  PPPoE  DHCP Client

<input type="checkbox"/>	IP
<input checked="" type="checkbox"/>	192.168.10.1/24

+ Add - Delete ↑ Move Up ↓ Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

Figure 4.25: Ethernet 1/2 IPv4

Then, create a tunnel.

**Tunnel Interface** ?

Interface Name  .

Comment

Netflow Profile  v

**Config** | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router  v

Security Zone  v

Figure 4.26: Create a tunnel 1

Ethernet | VLAN | Loopback | **Tunnel** | SD-WAN

Q

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY
tunnel		none	none	none
tunnel.1		none	default	VPN

Figure 4.27: Verify Tunnel1

Then, **commit the configuration!**

2. Create a static route to tunnel1 and ethernet1/1 as following figures. Traffic related to **10.0.0.0/16** should go through the tunnel. The rest of the traffic should go through the default Gateway.

Virtual Router - Static Route - IPv4
?

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

BFD Profile

Path Monitoring

Failure Condition  Any  All

Preemptive Hold Time (min)

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
<input type="checkbox"/>						

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

Virtual Router - Static Route - IPv4 ?

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

BFD Profile

Path Monitoring

Failure Condition  Any  All Preemptive Hold Time (min)

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

Figure 4.29: Create a static route to tunnel.1

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

The screenshot shows the 'IKE Crypto Profile' configuration interface. At the top, the title bar reads 'IKE Crypto Profile'. Below it, the 'Name' field is populated with 'IKE'. The configuration is organized into three main sections, each with a list of items and control buttons (Add, Delete, Move Up, Move Down):

- DH GROUP:** Contains one item, 'group2'.
- AUTHENTICATION:** Contains one item, 'sha1'.
- ENCRYPTION:** Contains one item, 'aes-128-cbc'.

To the right of these sections is a 'Timers' section with the following settings:

- Key Lifetime:** Set to 'Seconds' with a value of '28800'. A note below indicates 'Minimum lifetime = 3 mins'.
- IKEV2 Authentication Multiple:** Set to '0'.

At the bottom right of the window, there are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

Figure 4.30: Create an IKE Crypto Profile

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

The screenshot shows the 'IPsec Crypto Profile' configuration interface. At the top, the title bar reads 'IPsec Crypto Profile'. Below it, the 'Name' field is populated with 'IPSEC'. The 'IPsec Protocol' is set to 'ESP'. The 'DH Group' is 'group2' and 'Lifetime' is '27000'. A note below indicates 'Minimum lifetime = 3 mins'. There are three main sections with lists and control buttons:

- ENCRYPTION:** Contains one item, 'aes-128-cbc'.
- AUTHENTICATION:** Contains one item, 'sha1'.
- Enable:** Contains one item, 'Lifsize' set to 'MB' with a value of '[1 - 65535]'. A note below indicates 'Recommended lifsize is 100MB or greater'.

At the bottom right of the window, there are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

Figure 4.31: Create an IPsec Crypto Profile

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

The screenshot shows the 'IKE Gateway' configuration page in the Palo Alto Networks management interface. The 'General' tab is selected. The configuration includes:

- Name:** IKE-GW
- Version:** IKEv2 only mode
- Address Type:** IPv4 (selected), IPv6
- Interface:** ethernet1/1
- Local IP Address:** None
- Peer IP Address Type:** IP (selected), FQDN, Dynamic
- Peer Address:** 23.101.203.248
- Authentication:** Pre-Shared Key (selected), Certificate
- Pre-shared Key:** [Redacted]
- Confirm Pre-shared Key:** [Redacted]
- Local Identification:** None
- Peer Identification:** None
- Comment:** [Empty]

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

Figure 4.32: Create an IKE Gateway

The screenshot shows the 'IKE Gateway' configuration page in the Palo Alto Networks management interface, with the 'Advanced Options' tab selected. The configuration includes:

- Common Options:**
  - Enable Passive Mode
  - Enable NAT Traversal
- IKEv2:**
  - IKE Crypto Profile:** IKE (selected)
  - Strict Cookie Validation
- Liveness Check:**
  - Liveness Check
  - Interval (sec):** 5

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

Figure 4.33: Select IKE Crypto Profile

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

Figure 4.34: Create an IPsec Tunnel

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

Figure 4.35: Create a security policy “LAN-AZ”

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

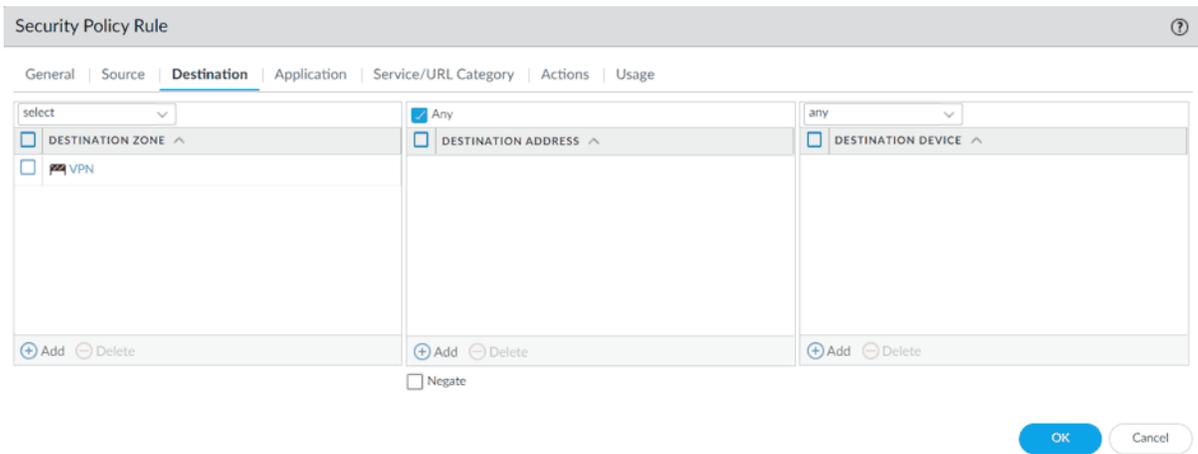


Figure 4.37: Create a security policy “LAN-AZ.” Select destination zone as VPN.

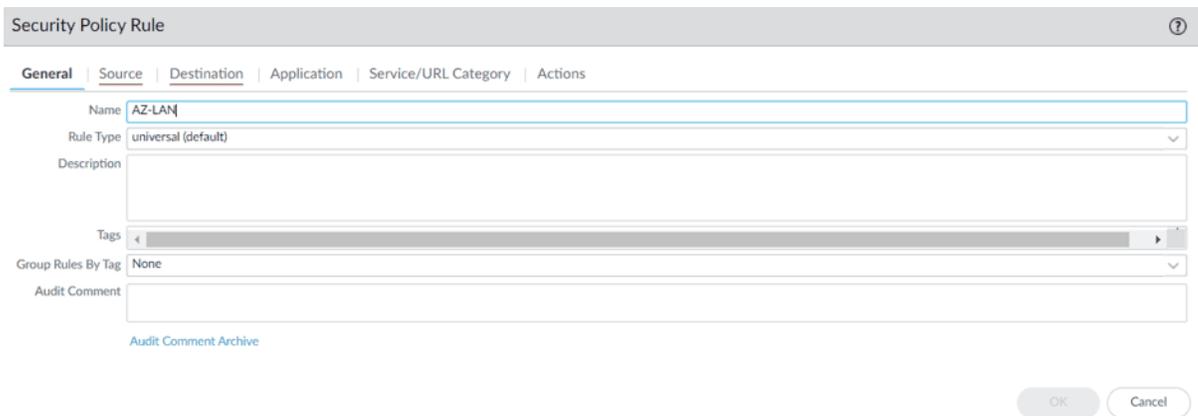


Figure 4.38: Create a security policy “AZ-LAN”

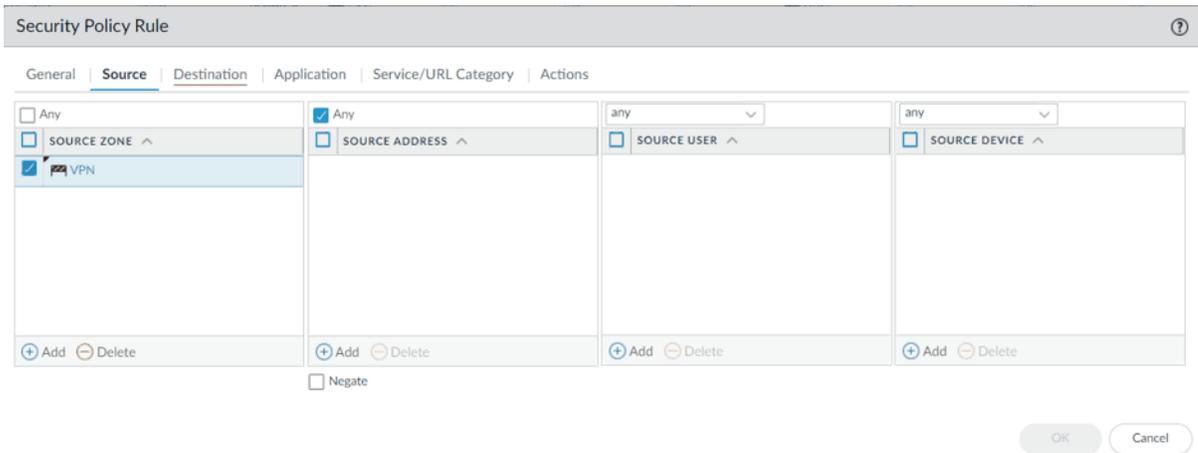


Figure 4.39: Create a security policy “AZ-LAN.” Select source zone as VPN.

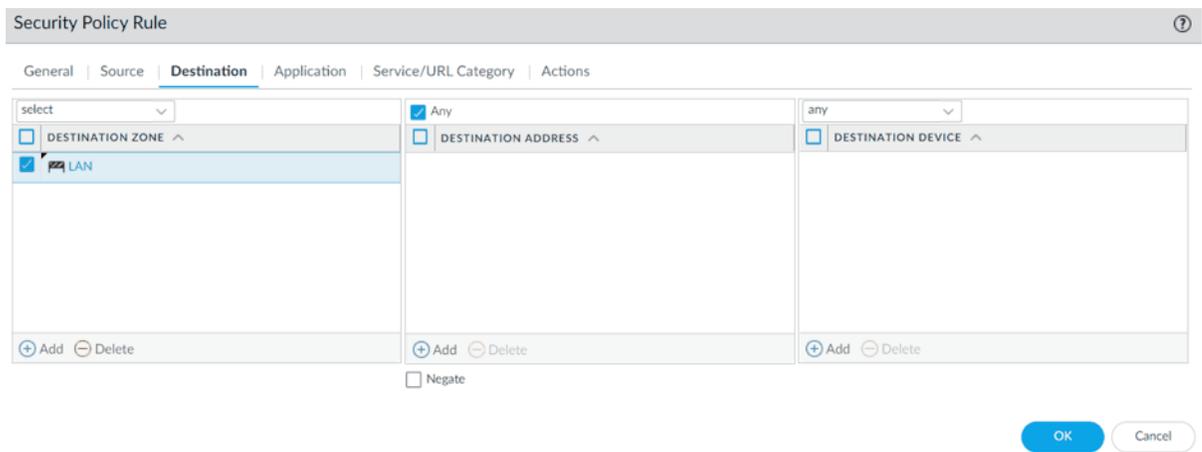
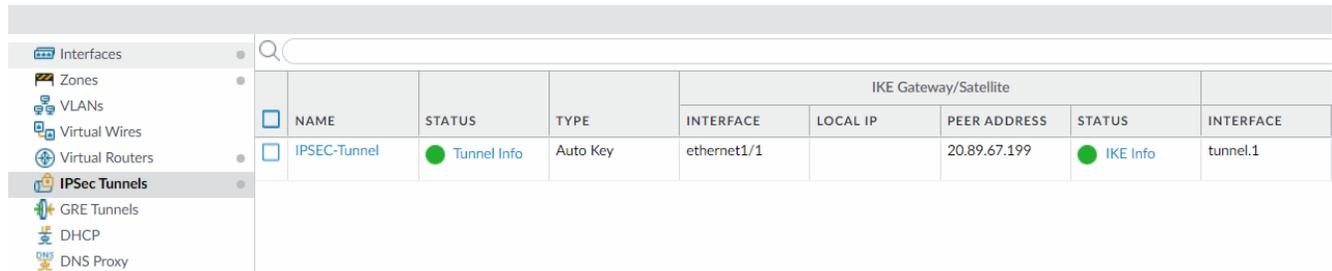


Figure 4.40: Create a security policy “AZ-LAN.” Select destination zone as LAN.

Don't forget to commit the configuration!

## Verify Connections

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



NAME	STATUS	TYPE	IKE Gateway/Satellite			
			INTERFACE	LOCAL IP	PEER ADDRESS	STATUS
IPSEC-Tunnel	Tunnel Info	Auto Key	ethernet1/1		20.89.67.199	IKE Info

Figure 4.41: Verify IPsec Tunnel

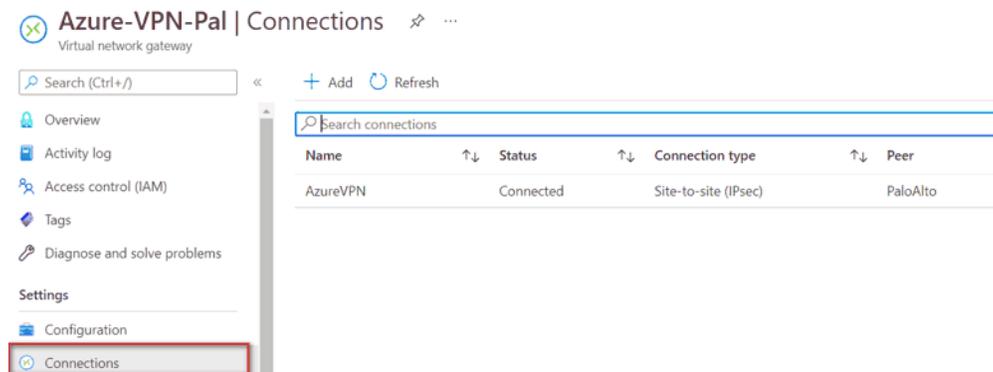


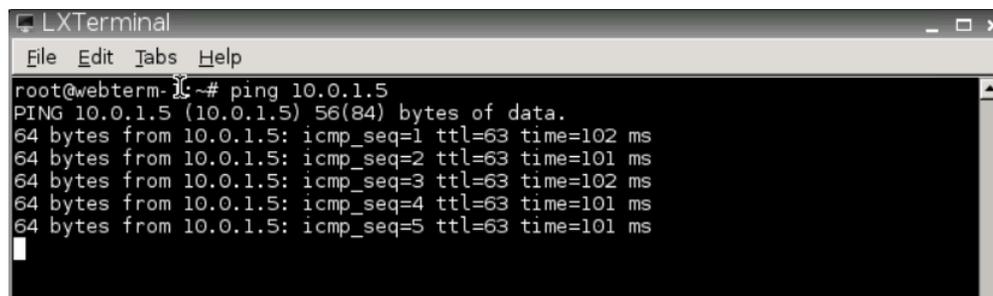
Figure 4.42: Verify connections in Azure

```

hamid@windows2:~$ ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=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
^C

```

Figure 4.43: Verify ping from Windows to webterm



```

root@webterm-1:~# ping 10.0.1.5
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
64 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



## 4.2 Deploy Palo Alto to 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'll learn how to deploy Palo Alto Firewall to Azure.

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

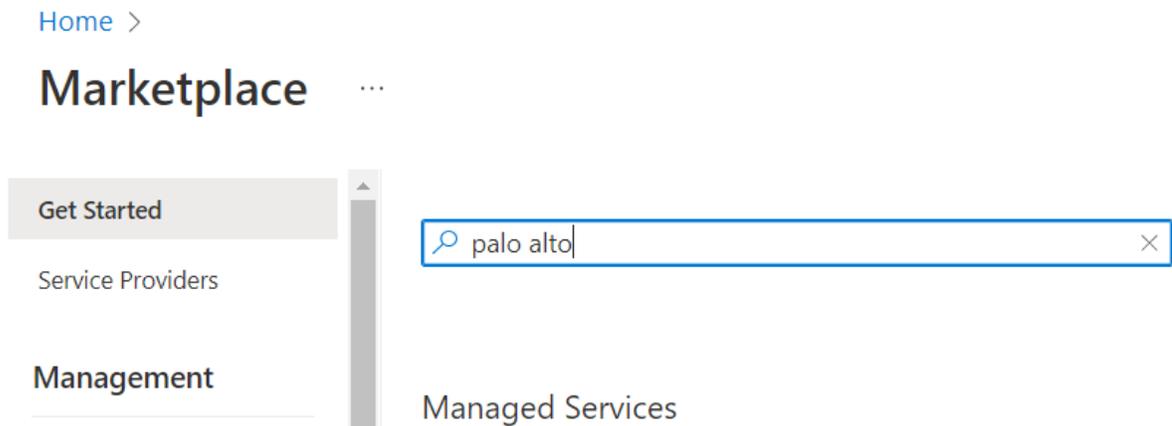


Figure 4.45: Search for Palo Alto

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

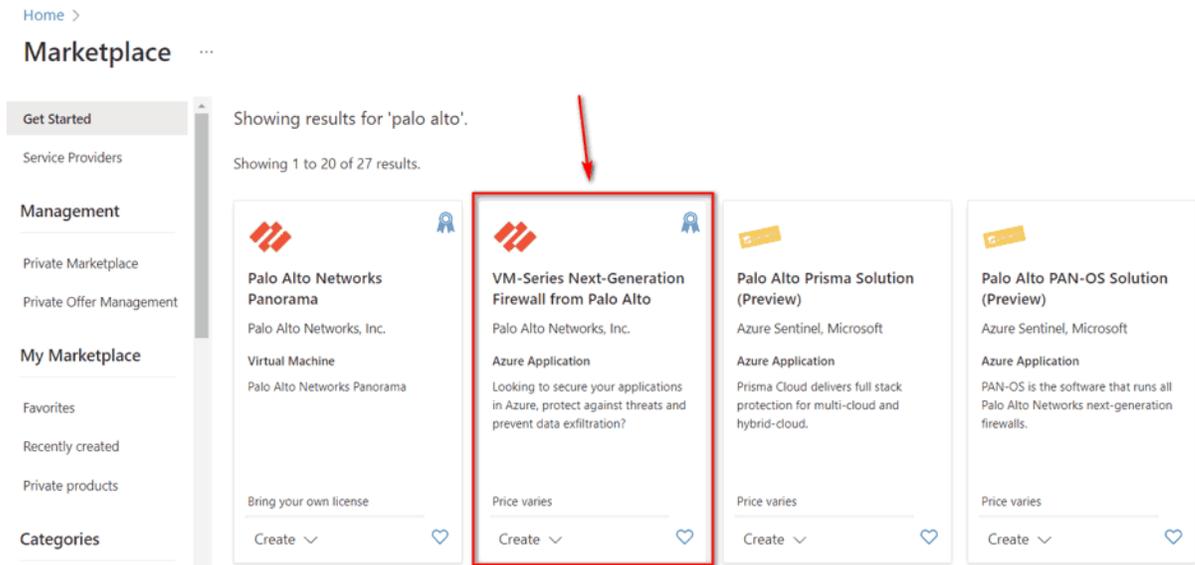


Figure 4.46: Select VM Series Next-Generation Firewall

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

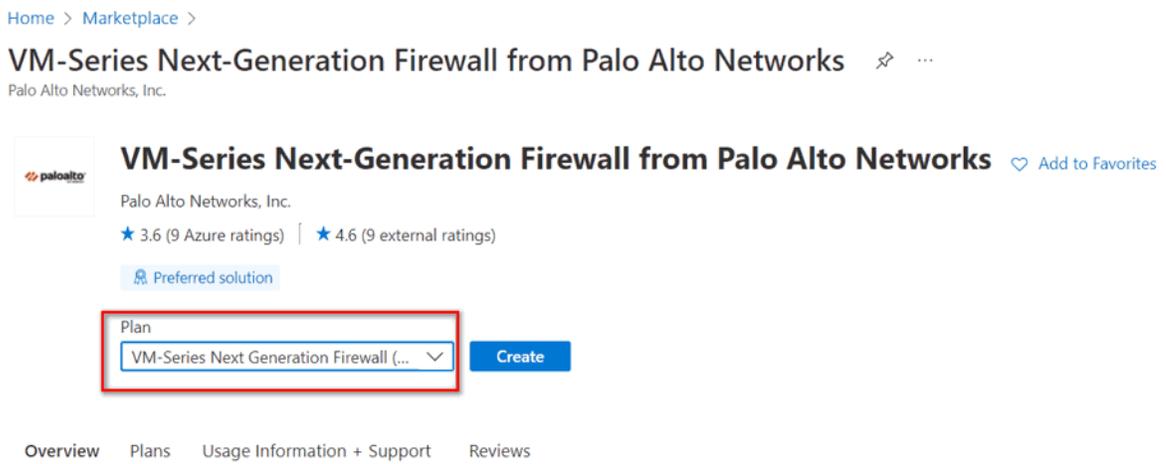


Figure 4.47: Select VM-Series Next Generation Firewall

## 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 *	<input type="text" value="Azure subscription 1"/>
Resource group *	<input type="text" value="Pal"/> <a href="#">Create new</a>
<b>Instance details</b>	
Region *	<input type="text" value="UK West"/>
Username *	<input type="text" value="hamid"/>
Authentication type *	<input checked="" type="radio"/> Password <input type="radio"/> SSH Public Key
Password *	<input type="password" value="....."/>
Confirm password *	<input type="password" value="....."/>

[Review + create](#)

[< Previous](#)

[Next : Networking >](#)

Figure 4.48: Create a VM-Series Palo Alto

Basics Networking VM-Series Configuration Review + create

### Configure virtual networks

Virtual network *	<input type="text" value="(new) fwVNET"/> <a href="#">Create new</a>
Management Subnet *	<input type="text" value="(new) Mgmt (10.0.0.0/24)"/>
Untrust Subnet *	<input type="text" value="(new) Untrust (10.0.1.0/24)"/>
Trust Subnet *	<input type="text" value="(new) Trust (10.0.2.0/24)"/>
Network Security Group: inbound source IP *	<input type="text" value="0.0.0.0/0"/>

Figure 4.49: Networking configuration

Basics   Networking   **VM-Series Configuration**   Review + create

Public IP address \* ⓘ (new) fwMgmtPublicIP [Create new](#)

DNS Name \* ⓘ hamid .ukwest.cloudapp.azure.com

VM name of VM-Series \* ⓘ hamidpaloalto

VM-Series Version ⓘ latest

Enable Bootstrap ⓘ  yes  no

Virtual machine size \* ⓘ **1x Standard D3 v2**  
4 vcpus, 14 GB memory [Change size](#)

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

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.

✓ Validation Passed

Basics   Networking   VM-Series Configuration   **Review + create**

PRODUCT DETAILS

VM-Series Next-Generation Firewall  
from Palo Alto Networks  
by Palo Alto Networks, Inc.  
[Terms of use](#) | [Privacy policy](#)

TERMS

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

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

Figure 4.51: Create a firewall

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

The screenshot shows the Azure portal interface for a deployment. At the top, the deployment name is 'paloaltonetworks.vmseries-ngfw-20220516153314 | Overview'. Below the name is a search bar and several action buttons: Delete, Cancel, Redeploy, and Refresh. A navigation menu on the left includes Overview (selected), Inputs, Outputs, and Template. A feedback banner reads 'We'd love your feedback! →'. The main content area displays 'Deployment is in progress' with a progress indicator. Below this, the deployment details are shown: Deployment name: paloaltonetworks.vmseries-ngfw-2022051615..., Subscription: Azure subscription 1, and Resource group: Pal.

Figure 4.52: Deployment is in progress

The screenshot shows the Azure portal interface after the deployment is complete. A feedback banner reads 'We'd love your feedback! →'. The main content area displays 'Your deployment is complete' with a green checkmark icon. Below this, the deployment details are shown: Deployment name: paloaltonetworks.vmseries-ngfw-2022051615..., Subscription: Azure subscription 1, Resource group: Pal, Start time: 5/16/2022, 3:38:01 PM, and Correlation ID: 5a6d9bc6-d224-43f9-b0f8-8ac39aa296dc. There are also links for 'Deployment details (Download)' and 'Next steps', and a blue button labeled 'Go to resource group'.

Figure 4.53: Deployment is complete

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

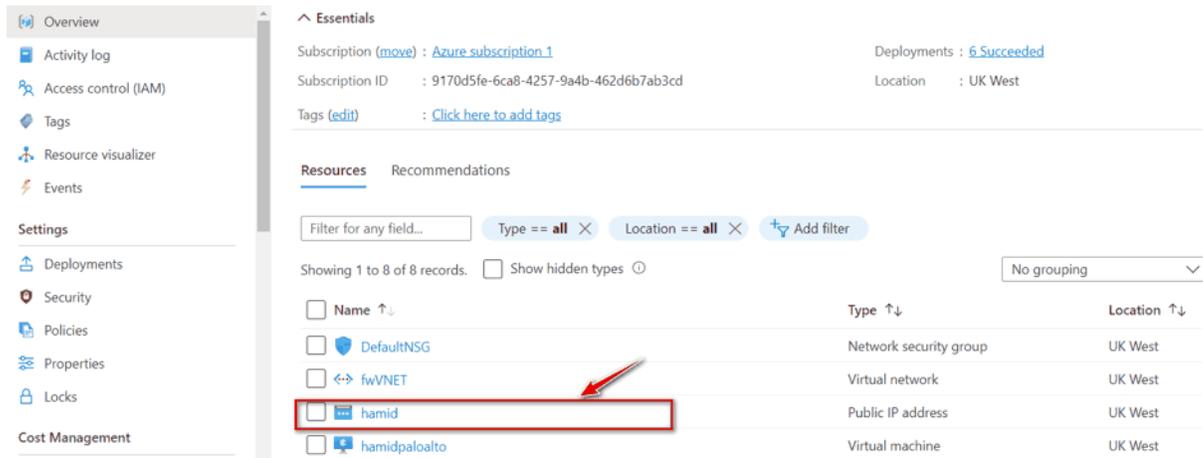


Figure 4.54: Palo Alto Public IP Address



Figure 4.55: Palo Alto Public IP Address

- 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.

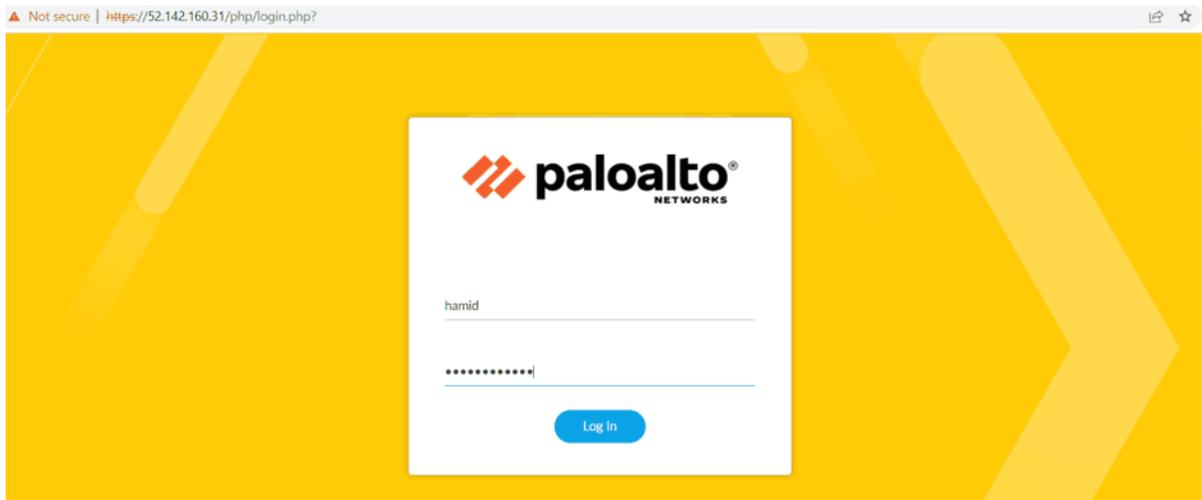


Figure 4.56: Palo Alto Firewall Credential Page

- 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 provided by server.”

**Ethernet Interface** ⓘ

Interface Name: ethernet1/1  
 Comment:   
 Interface Type: Layer3  
 Netflow Profile: None

Config | **IPv4** | IPv6 | SD-WAN | Advanced

Enable SD-WAN  
 Type:  Static  PPPoE  DHCP Client

Enable  
 Automatically create default route pointing to default gateway provided by server  
 Send Hostname: system-hostname

Default Route Metric: 10

[Show DHCP Client Runtime Info](#)

**OK** Cancel

*Figure 4.58: Ethernet1/1 configuration*

**Ethernet Interface** ⓘ

Interface Name: ethernet1/2  
 Comment:   
 Interface Type: Layer3  
 Netflow Profile: None

Config | **IPv4** | IPv6 | SD-WAN | Advanced

Enable SD-WAN  
 Type:  Static  PPPoE  DHCP Client

Enable  
 Automatically create default route pointing to default gateway provided by server  
 Send Hostname: system-hostname

Default Route Metric: 10

[Show DHCP Client Runtime Info](#)

**OK** Cancel

*Figure 4.59: Ethernet1/2 configuration*

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

The screenshot shows the configuration page for an Ethernet interface named 'ethernet1/1'. The interface type is set to 'Layer3' and the netflow profile is 'None'. Under the 'Assign Interface To' section, the virtual router is set to 'default' and the security zone is set to 'Untrust'. The 'Config' tab is selected, and there are 'OK' and 'Cancel' buttons at the bottom right.

Ethernet Interface	
Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None
<b>Config</b>   IPv4   IPv6   SD-WAN   Advanced	
Assign Interface To	
Virtual Router	default
Security Zone	Untrust

Figure 4.60: Ethernet1/1 zone and virtual router

The screenshot shows the configuration page for an Ethernet interface named 'ethernet1/2'. The interface type is set to 'Layer3' and the netflow profile is 'None'. Under the 'Assign Interface To' section, the virtual router is set to 'default' and the security zone is set to 'Trust'. The 'Config' tab is selected, and there are 'OK' and 'Cancel' buttons at the bottom right.

Ethernet Interface	
Interface Name	ethernet1/2
Comment	WAN
Interface Type	Layer3
Netflow Profile	None
<b>Config</b>   IPv4   IPv6   SD-WAN   Advanced	
Assign Interface To	
Virtual Router	default
Security Zone	Trust

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

**Administrative Management Services**

- HTTP
- HTTPS
- Telnet
- SSH

**Network Services**

- Ping
- HTTP OCSP
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

**PERMITTED IP ADDRESSES**

+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.10/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

Figure 4.62: Ethernet1/1 Management Profile

## 12. Create a static route to 10.0.1.1.

Virtual Router - Static Route - IPv4

Name: static

Destination: 0.0.0.0/0

Interface: ethernet1/1

Next Hop: IP Address

Next Hop: 10.0.1.1

Admin Distance: 10 - 240

Metric: 10

Route Table: Unicast

BFD Profile: Disable BFD

Path Monitoring

Failure Condition:  Any  All Preemptive Hold Time (min): 2

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
+ Add - Delete						

OK Cancel

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 IP addresses

Default Directory

+ Create Manage view Refresh Export to CSV Open query Assign tags Delete

Filter for any field... Subscription == Azure subscription 1 Resource group == all Location ==

<input type="checkbox"/>	Name ↑↓	Resource group ↑↓
<input type="checkbox"/>	hamid	PAL

Figure 4.64: Create a public IP address

## Create public IP address ...

SKU \* ⓘ

Standard  Basic

Tier

Regional  Global

### IPv4 IP Address Configuration

Name \*

Untrust

IP address assignment \*

Dynamic  Static

Idle timeout (minutes) \* ⓘ

DNS name label ⓘ

Subscription \*

**Create** Automation options

Figure 4.65: Create a public IP address (set SKU and name)

The screenshot shows the Azure portal interface for configuring IP settings on a network interface. On the left, the 'All resources' pane shows a list of resources, with 'hamidpaloalto-hamid-eth1' selected and highlighted with a red box. The main pane displays the 'IP configurations' settings for 'hamidpaloalto-hamid-eth1'. The 'IP forwarding settings' are shown as 'Enabled'. The 'Subnet' is set to 'Untrust (10.0.1.0/24)'. A message indicates that the associated virtual machine must be stopped or deallocated to edit the subnet. At the bottom, a table lists the IP configurations:

Name	IP Version	Type	Private IP address	Public IP address
ipconfig-untr...	IPv4	Primary	10.0.1.4 (Dynamic)	-

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

**i** 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.



## 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.

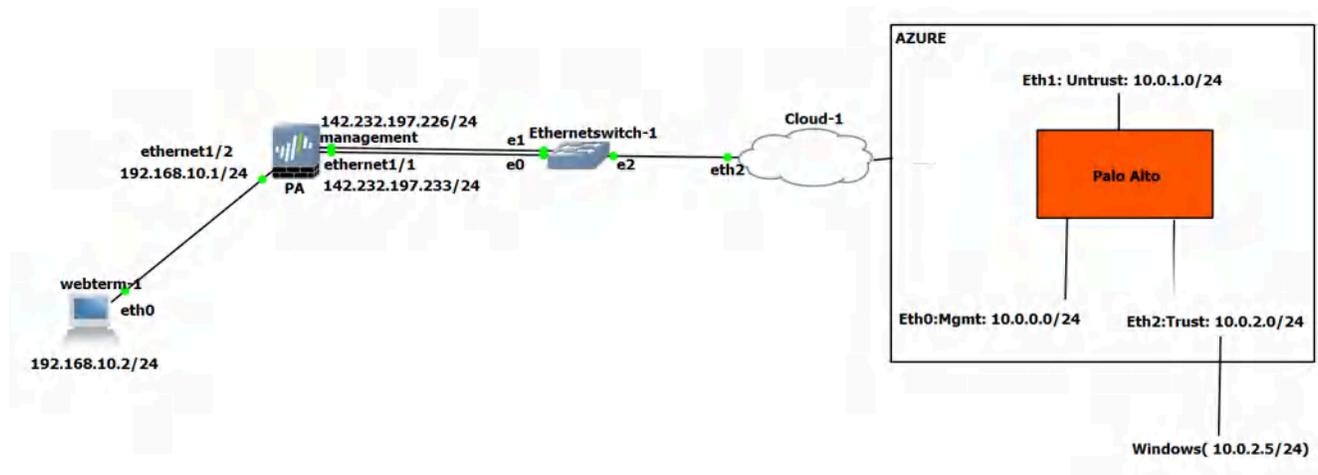


Figure 4.68: Main scenario

## On-Premise Palo Alto Configuration

Devices	Interface	IP address
Palo Alto	Management	DHCP Client
	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.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1	Layer3		🟢	Dynamic-DHCP Client	default	Untagged	none	Untrust
ethernet1/2	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.

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES
tunnel		none	none	none	
tunnel.1		none	default	Untrust	🔒

Figure 4.70: Create a tunnel

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

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

BFD Profile

Path Monitoring

Failure Condition  Any  All Preemptive Hold Time (min)

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
--------------------------	------	--------	-----------	----------------	--------------------	------------

Figure 4.71: Create a static route to default gateway

### Virtual Router - Static Route - IPv4 ?

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

BFD Profile

Path Monitoring

Failure Condition  Any  All      Preemptive Hold Time (min)

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
--------------------------	------	--------	-----------	----------------	--------------------	------------

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** | Advanced Options

Name

Version

Address Type  IPv4  IPv6

Interface

Local IP Address

Peer IP Address Type  IP  FQDN  Dynamic

Peer Address

Authentication  Pre-Shared Key  Certificate

Pre-shared Key

Confirm Pre-shared Key

Local Identification

Peer Identification

Comment

Figure 4.73: Create an IKE Gateway

**IPsec Tunnel** ⓘ

**General** | Proxy IDs

Name

Tunnel Interface

Type  Auto Key  Manual Key  GlobalProtect Satellite

Address Type  IPv4  IPv6

IKE Gateway

IPsec Crypto Profile

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.

	NAME	TAGS	TYPE	Source				Destination		
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEV
1	Trust	none	universal	Trust	any	any	any	Untrust	any	any
2	Untrust	none	universal	Untrust	any	any	any	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.

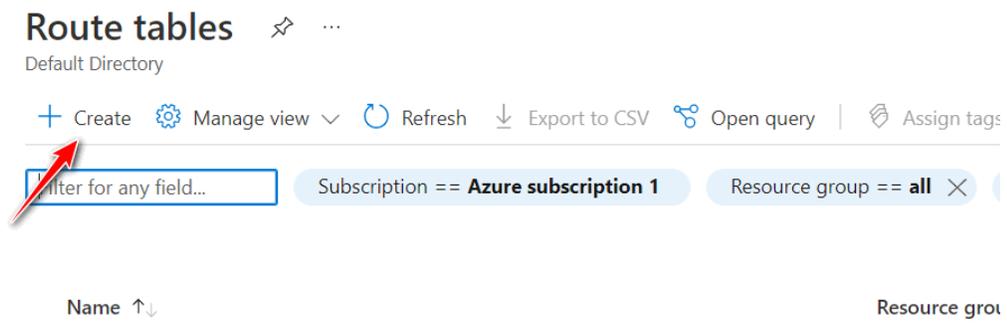


Figure 4.76: Create a route table

## 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 \* ⓘ Pal ✓  
[Create new](#)

**Instance details**

Region \* ⓘ UK West ✓

Name \* ⓘ Trust ✓

Propagate gateway routes \* ⓘ  Yes  No

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

Figure 4.77: Create a route table

## Create Route table ...

✓ Validation Passed

**Basics** Tags **Review + create**

**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)

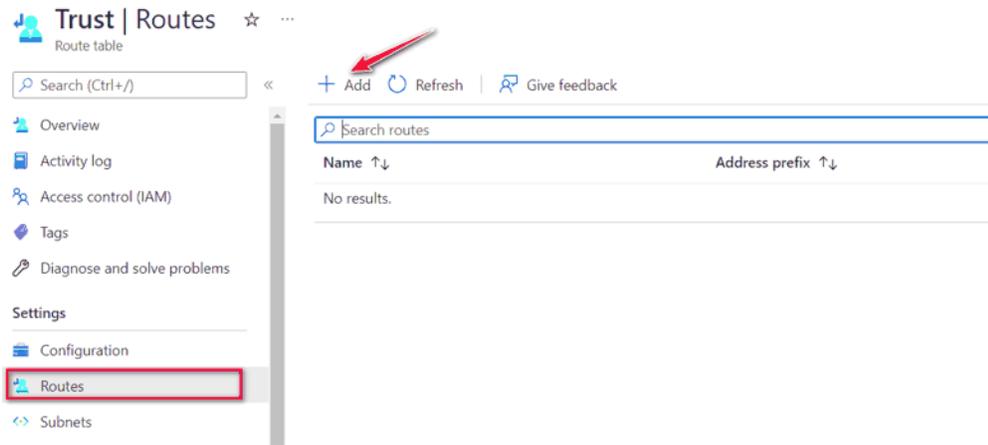


Figure 4.79: Add a Route

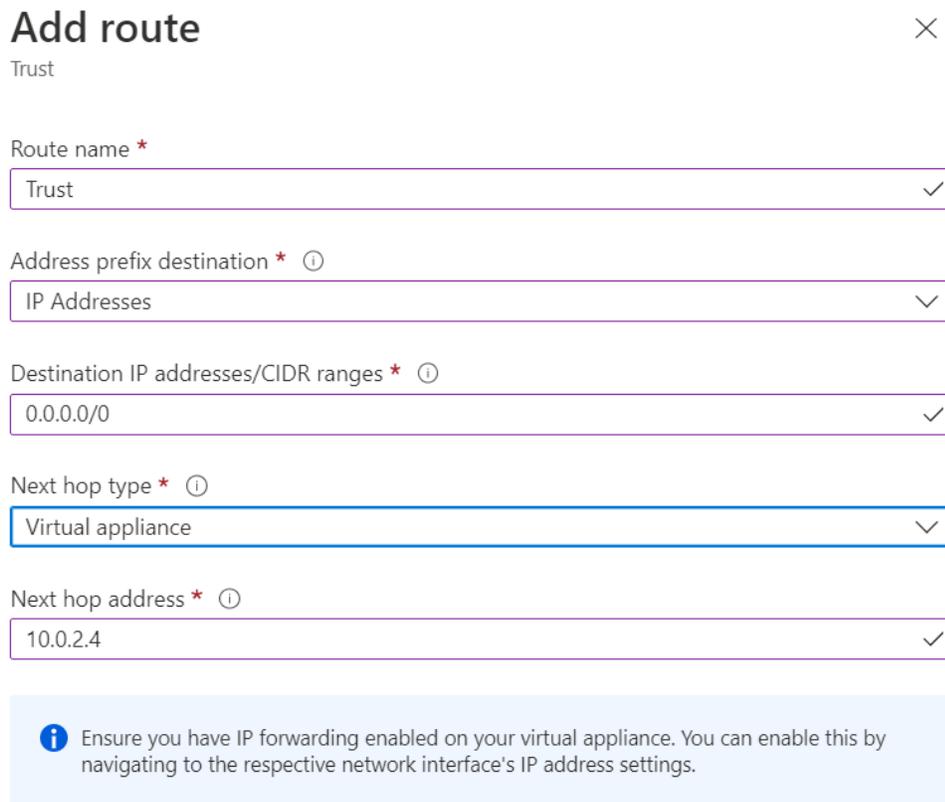


Figure 4.80: Add a default route pointing to 10.0.2.4 (Trust Interface)

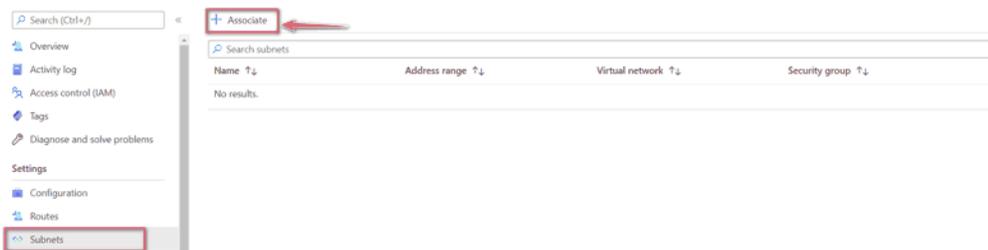


Figure 4.81: Associate Trust route to Trust Subnet

## Associate subnet



Trust

Virtual network ⓘ

fwVNET



Subnet ⓘ

Trust



Figure 4.82: Associate fwVNET to Trust Subnet

- Set static routes as figures 4.83 and 4.84.

Virtual Router - Static Route - IPv4
?

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

BFD Profile

Path Monitoring

Failure Condition  Any  All
Preemptive Hold Time (min)

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

Figure 4.83: Static route pointing to default gateway

### Virtual Router - Static Route - IPv4 ?

Name:

Destination:

Interface:

Next Hop:

Admin Distance:

Metric:

Route Table:

BFD Profile:

Path Monitoring

Failure Condition:  Any  All      Preemptive Hold Time (min):

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
--------------------------	------	--------	-----------	----------------	--------------------	------------

Figure 4.84: Static route pointing to tunnel

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** | Advanced Options

Name

Version

Address Type  IPv4  IPv6

Interface

Local IP Address

Peer IP Address Type  IP  FQDN  Dynamic

Peer Address

Authentication  Pre-Shared Key  Certificate

Pre-shared Key

Confirm Pre-shared Key

Local Identification

Peer Identification

Comment

Figure 4.85: Create an IKE Gateway

**IPsec Tunnel** ⓘ

**General** | Proxy IDs

Name

Tunnel Interface

Type  Auto Key  Manual Key  GlobalProtect Satellite

Address Type  IPv4  IPv6

IKE Gateway

IPsec Crypto Profile

Show Advanced Options

Comment

Figure 4.86: Create an IPsec Tunnel

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

	NAME	TAGS	TYPE	Source				Destination		
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEV
1	Trust	none	universal	Trust	any	any	any	Untrust	any	any
2	Untrust	none	universal	Untrust	any	any	any	Trust	any	any

Figure 4.87: Create two security policies

- 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.

### Create a virtual machine

your resources.

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

**Instance details**

Virtual machine name \* ⓘ

Region \* ⓘ

Availability options ⓘ

Security type ⓘ

Image \* ⓘ  [See all images](#) | [Configure VM generation](#)

Azure Spot instance ⓘ

Size \* ⓘ  [See all sizes](#)

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

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](#)

### Network interface

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

Virtual network *	<input type="text" value="fwVNET"/>
	<a href="#">Create new</a>
Subnet *	<input type="text" value="Trust (10.0.2.0/24)"/>
	<a href="#">Manage subnet configuration</a>
Public IP	<input type="text" value="None"/>
	<a href="#">Create new</a>
NIC network security group	<input checked="" type="radio"/> None <input type="radio"/> Basic <input type="radio"/> Advanced
Delete NIC when VM is deleted	<input type="checkbox"/>
Accelerated networking	<input checked="" type="checkbox"/>

### Load balancing

Figure 4.89: Assign Trust subnet with no public IP

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

```

root@webterm-1:~# ifconfig
eth0      Link encap:Ethernet  Hwaddr 52:54:34:8e:7a:dc
          inet addr:192.168.10.2  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::5054:34ff:fe8e:7adc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:51 errors:0 dropped:0 overruns:0 frame:0
          TX packets:277 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4702 (4.5 KiB)  TX bytes:26674 (26.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4432 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4432 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:374224 (365.4 KiB)  TX bytes:374224 (365.4 KiB)

root@webterm-1:~# ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=62 time=140 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=62 time=145 ms
    
```

Figure 4.90: Ping from WebTerm to Azure

```

System load: 0.0          Processes:                119
Usage of /:   4.9% of 28.90GB  Users logged in:        1
Memory usage: 7%          IPv4 address for eth0: 10.0.2.5
Swap usage:  0%

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri May 20 02:00:05 2022 from 10.0.0.4
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

hamid@linux:~$ ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=62 time=141 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=62 time=143 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=62 time=142 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=62 time=145 ms
    
```

Figure 4.91: Ping from Azure to WebTerm

NAME	STATUS	TYPE	IKE Gateway/Satellite				Tunnel Interface		
			INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM
IPSEC	<span style="color: green;">●</span> Tunnel Info	Auto Key	ethernet1/1		51.141.71.81	<span style="color: green;">●</span> IKE Info	tunnel.1	default (Show Routes)	vsys1

Figure 4.92: Tunnel Status

# Capstone Project



# Capstone Project

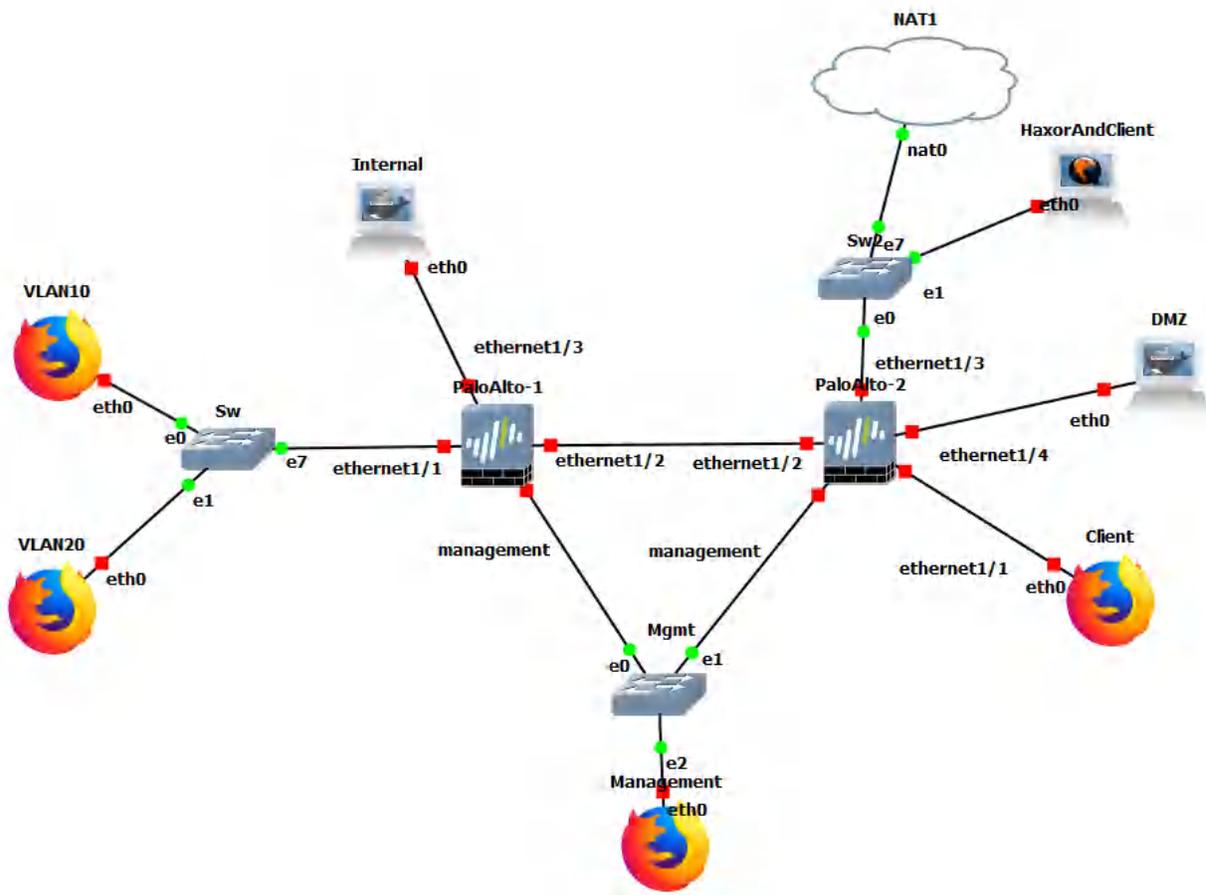


Figure C.1: Capstone Topology

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. [Download Captions](#)



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





## 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”.

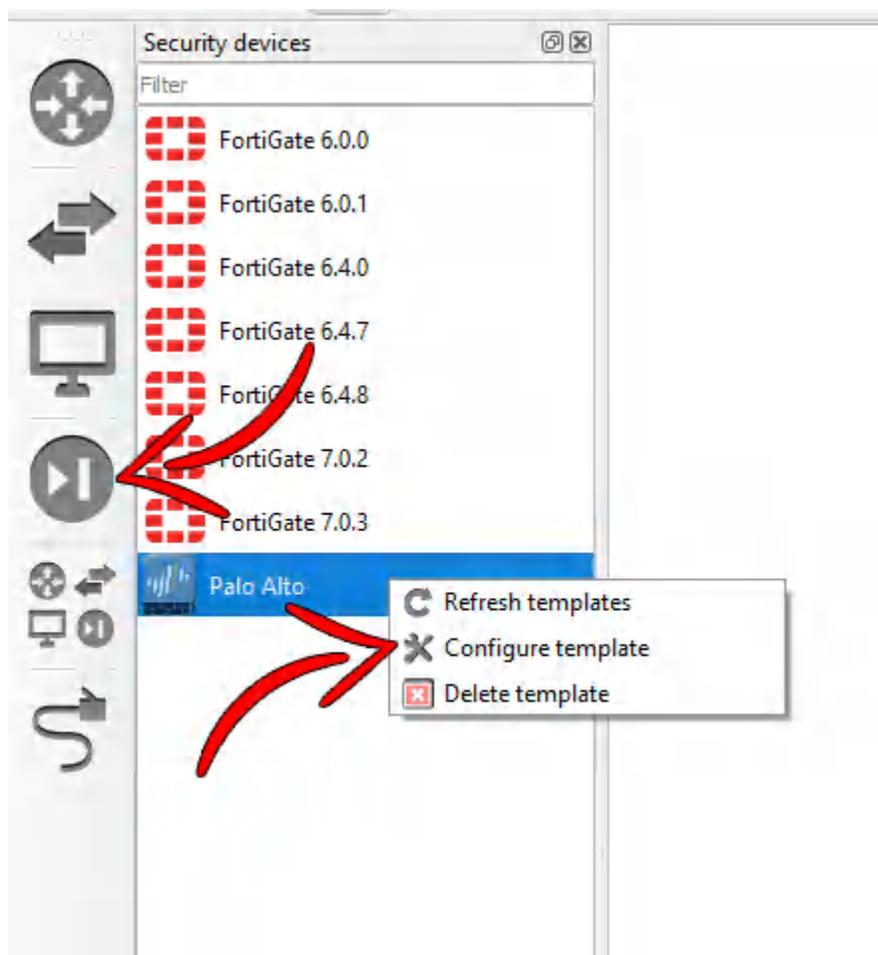


Figure A.1: Configure template

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

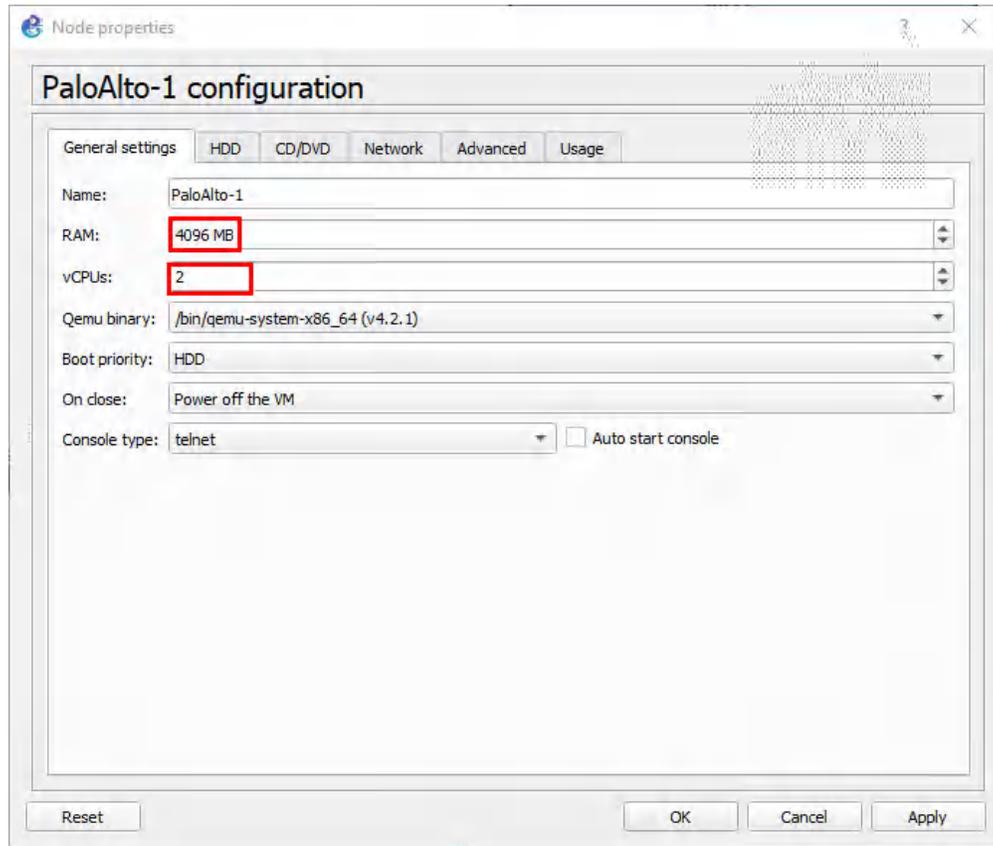


Figure A.2: Configure RAM and vCPUs

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".

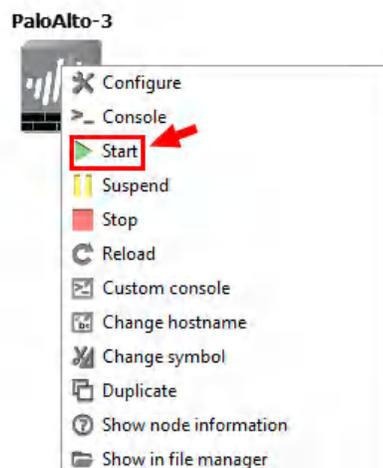


Figure A.4: Starting the Palo Alto

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.

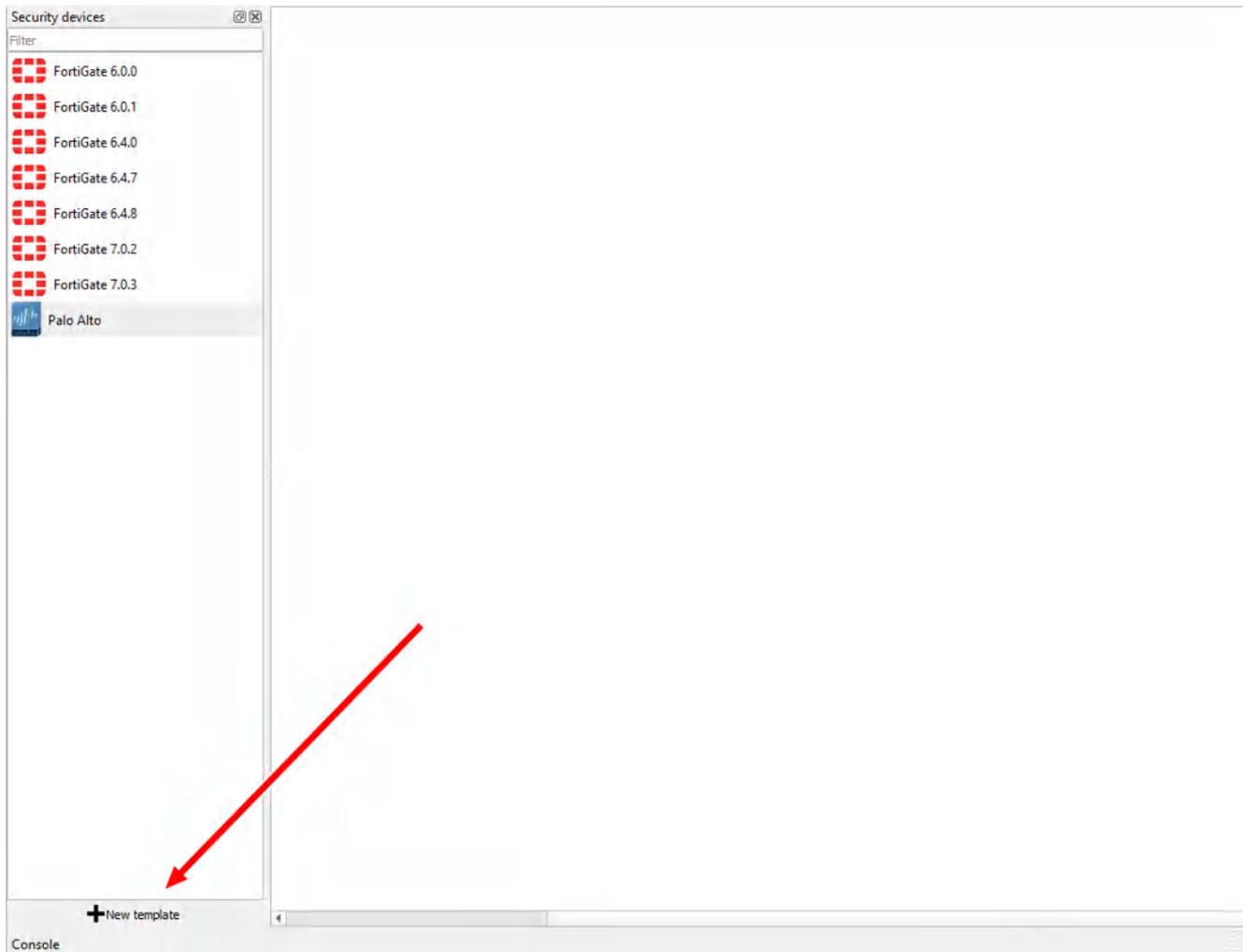


Figure A.5: Add a new template

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

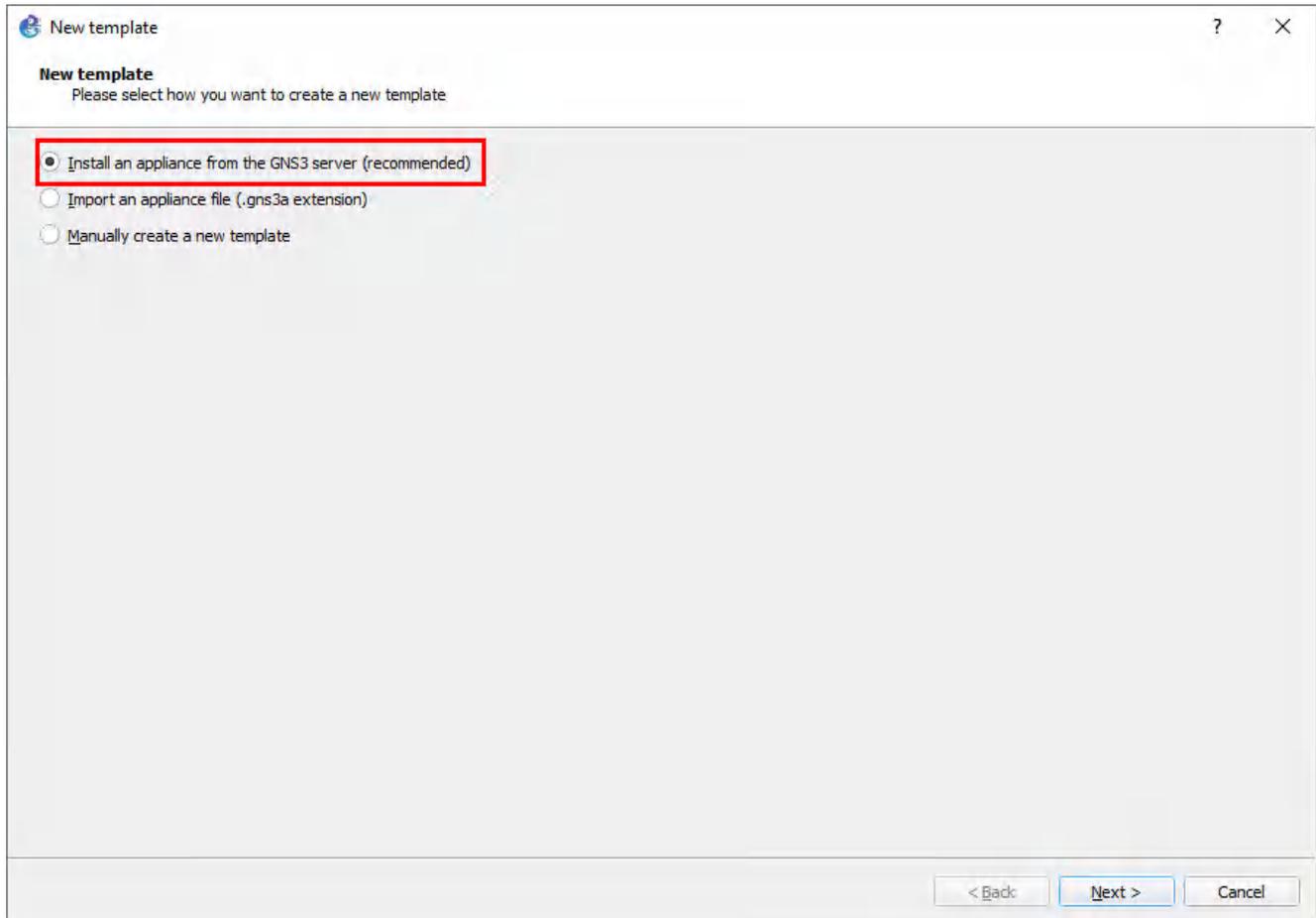


Figure A.6: Select “Install an appliance from the GNS3 server”

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

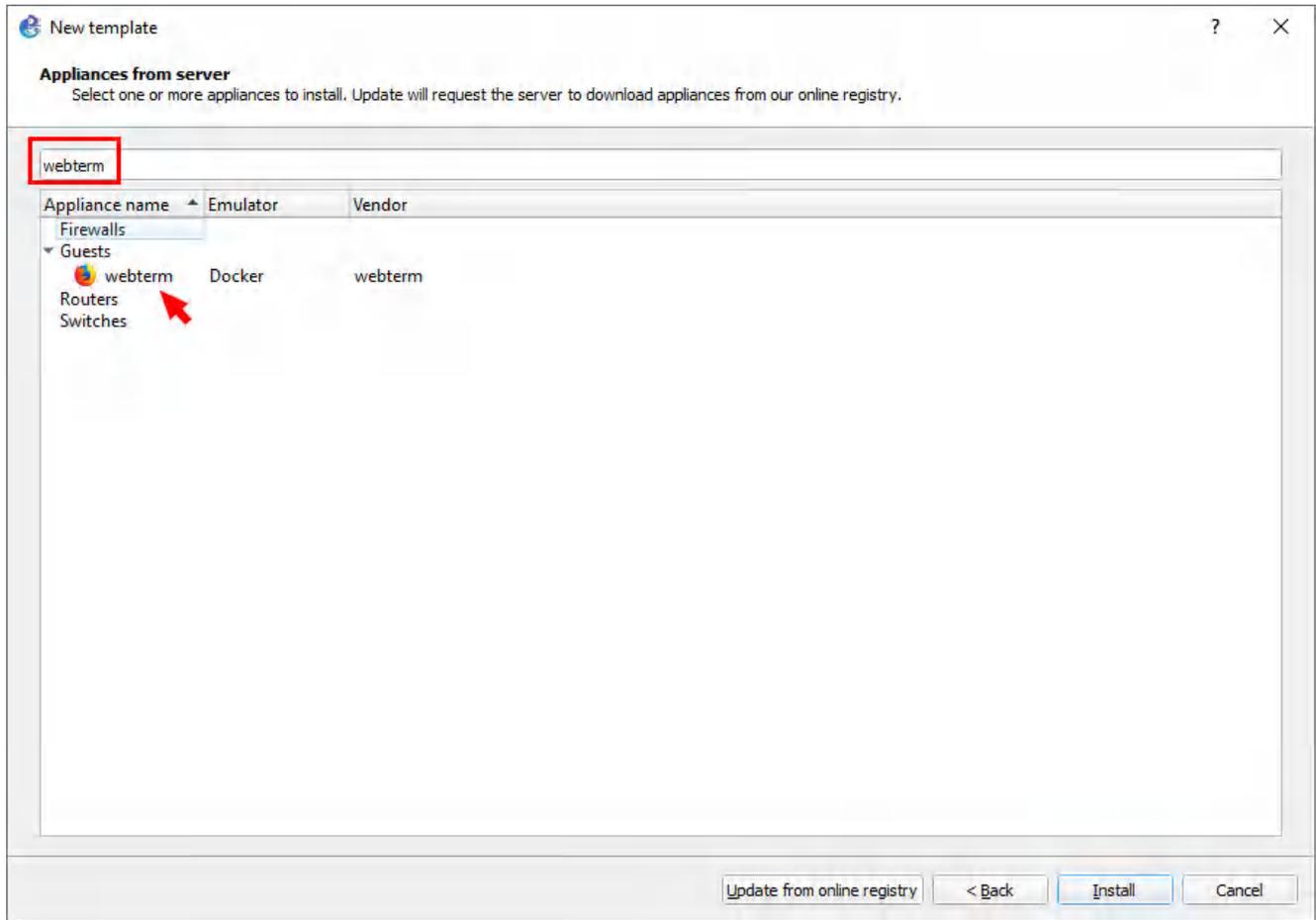


Figure A.7: Search for “webterm”

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

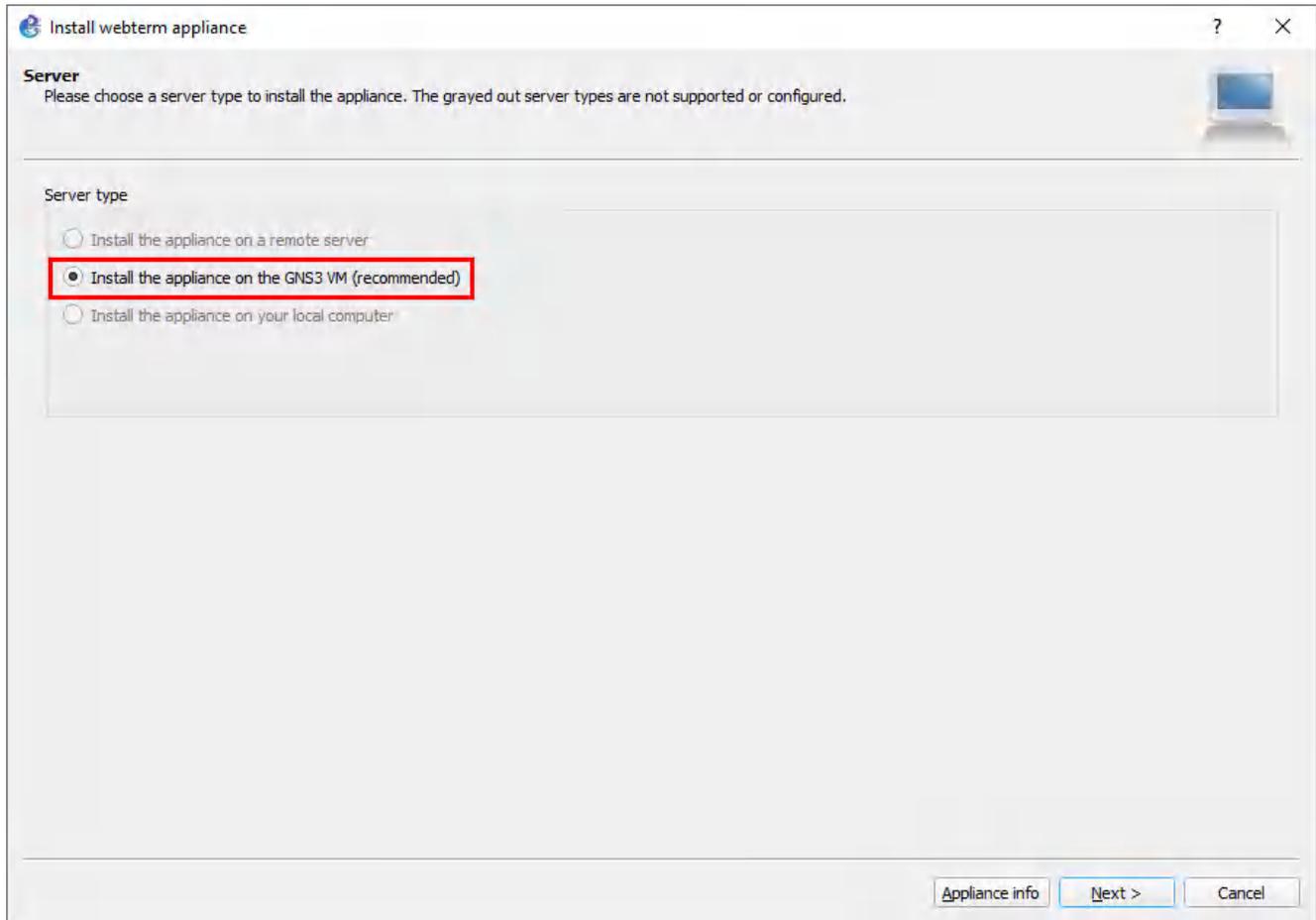


Figure A.8: Select “Install the appliance on the GNS3 VM”

On the next screen, click Finish.

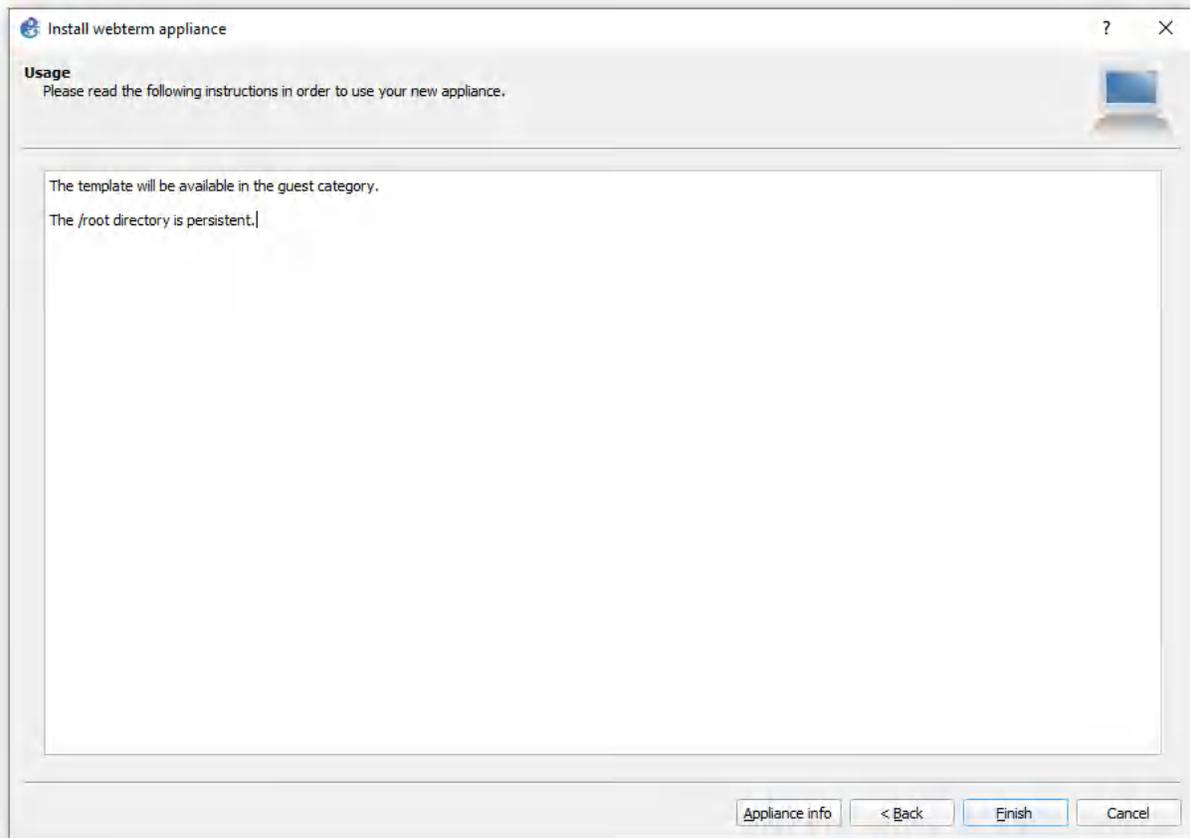


Figure A.9: Final step of Installation of webterm

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”.

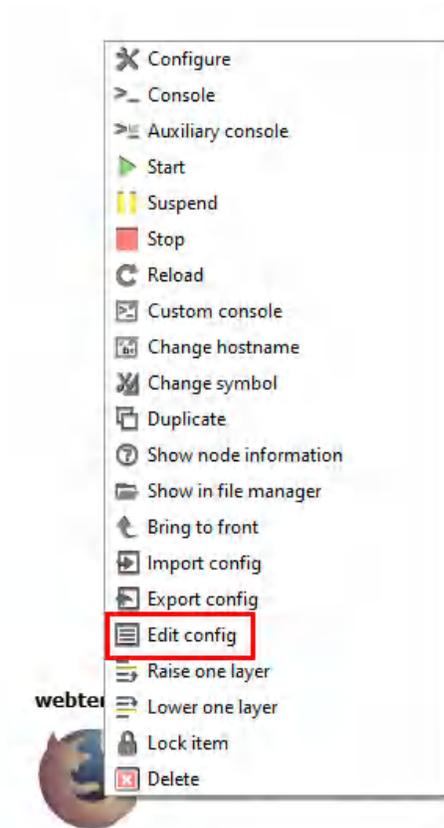
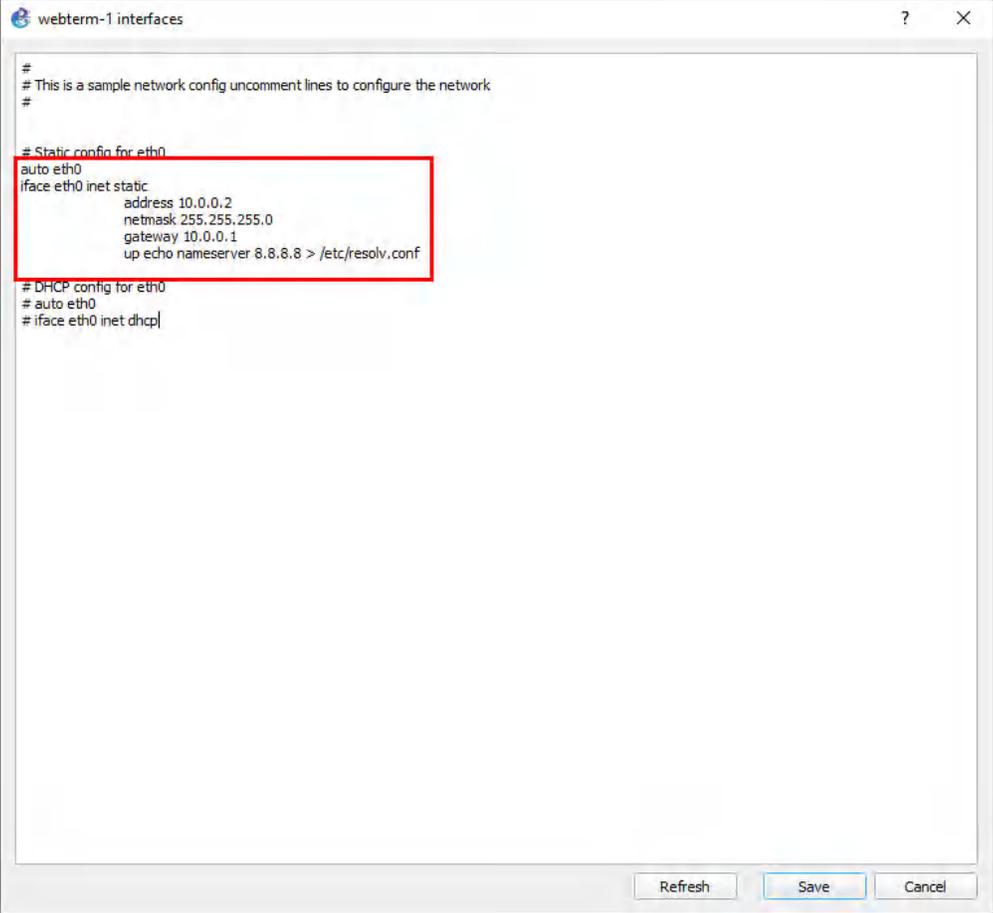


Figure A.10: Edit config

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:



```
webterm-1 interfaces ? X
#
# 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 255.255.255.0
    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 Cancel
```

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.

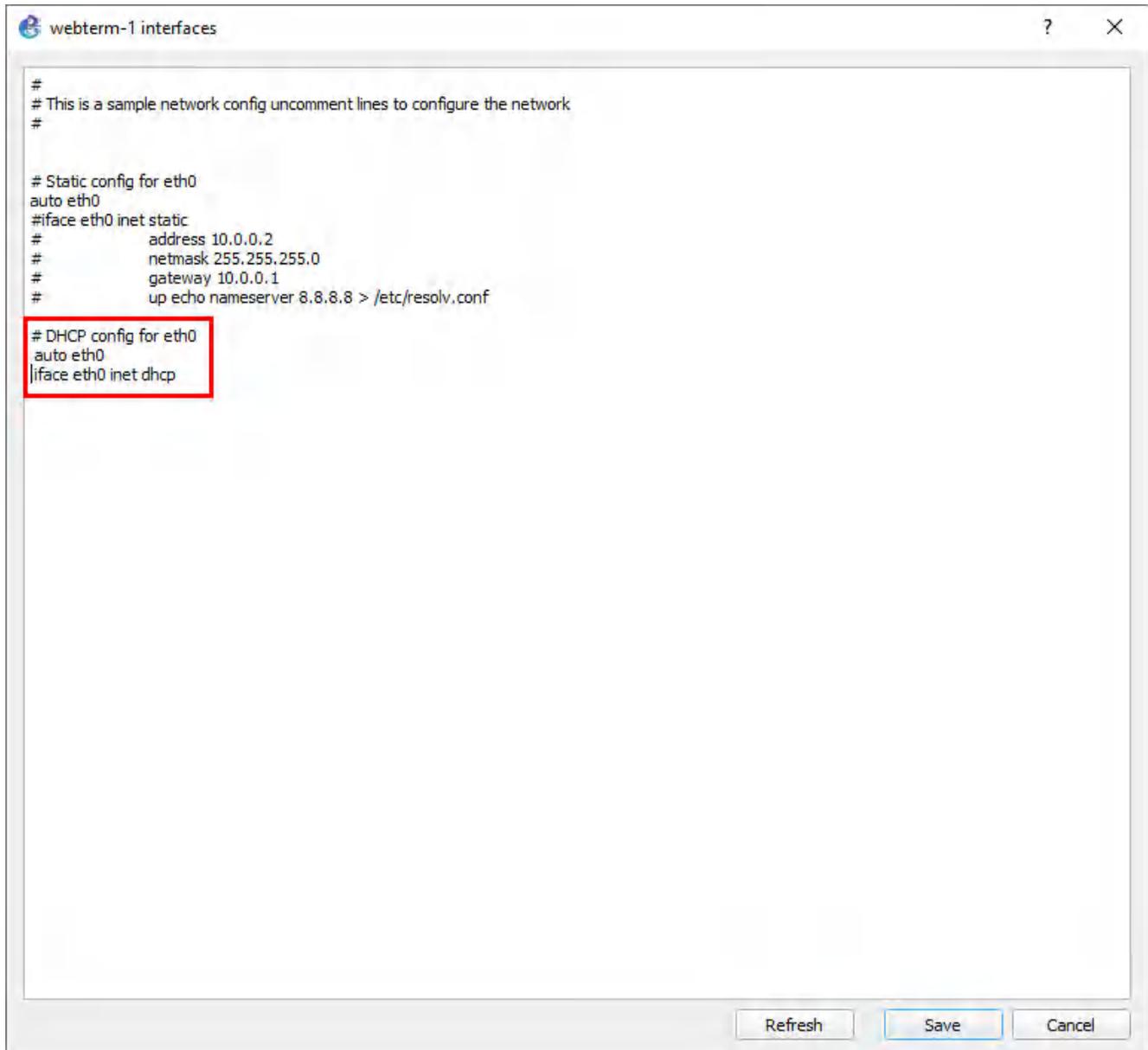


Figure A.12: Configure the DHCP IP address

## Connect Devices in GNS3

Please see the example in the GIF below (if using an offline version of this book, go to the [web version of the appendix of Palo Alto Firewall](#)):

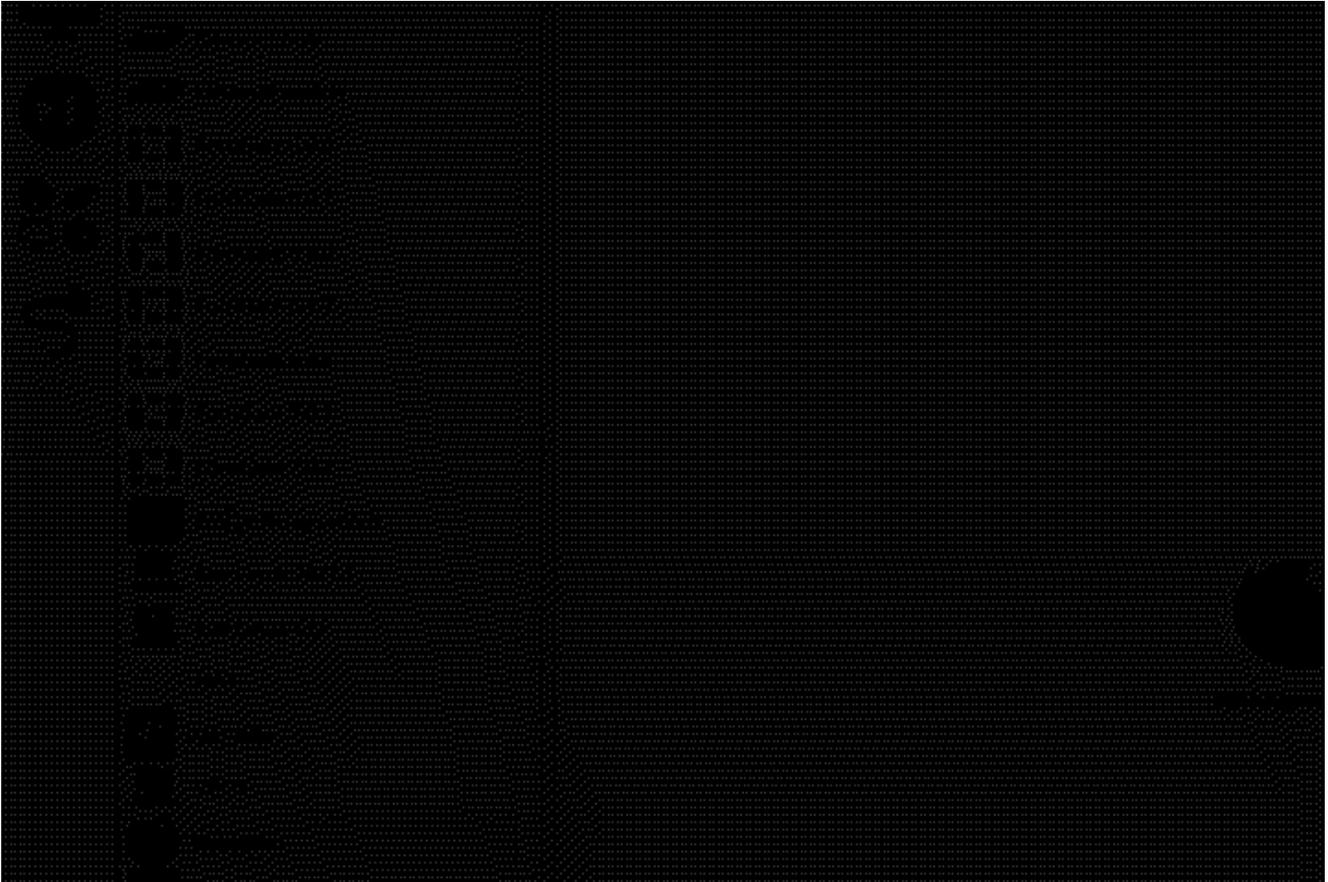


Figure A.13: Connecting devices

## 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.

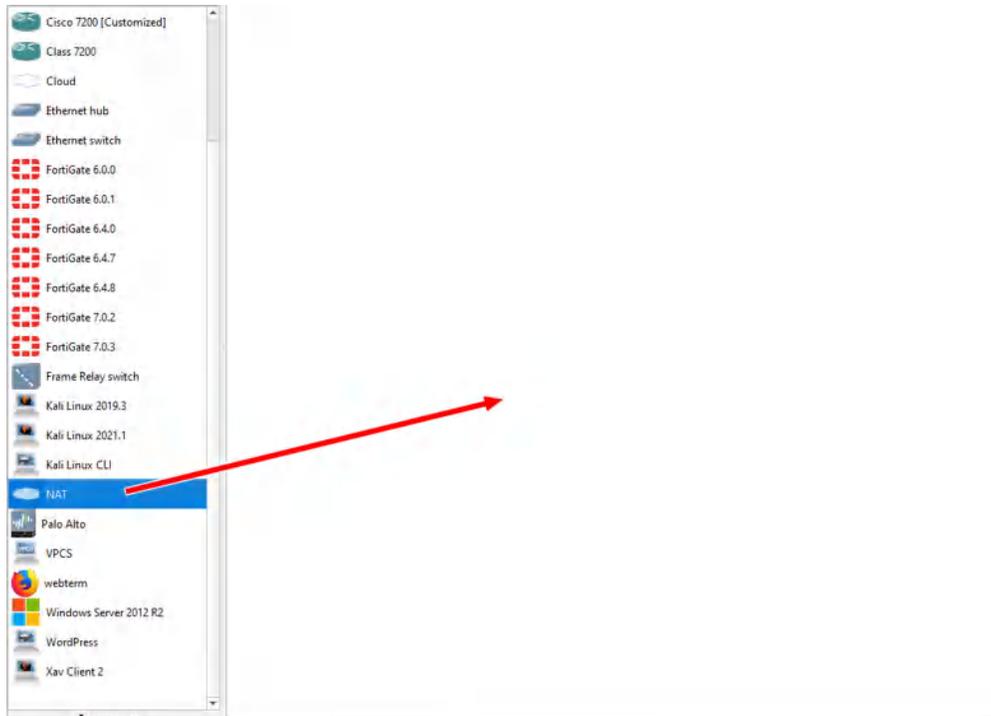


Figure A.14: Using NAT

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

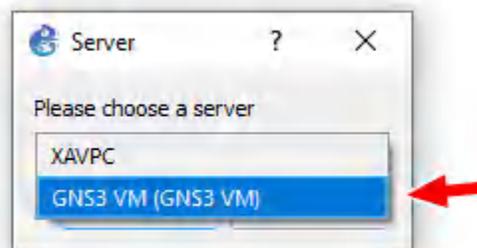


Figure A.15: Select GNS3 VM

## 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.

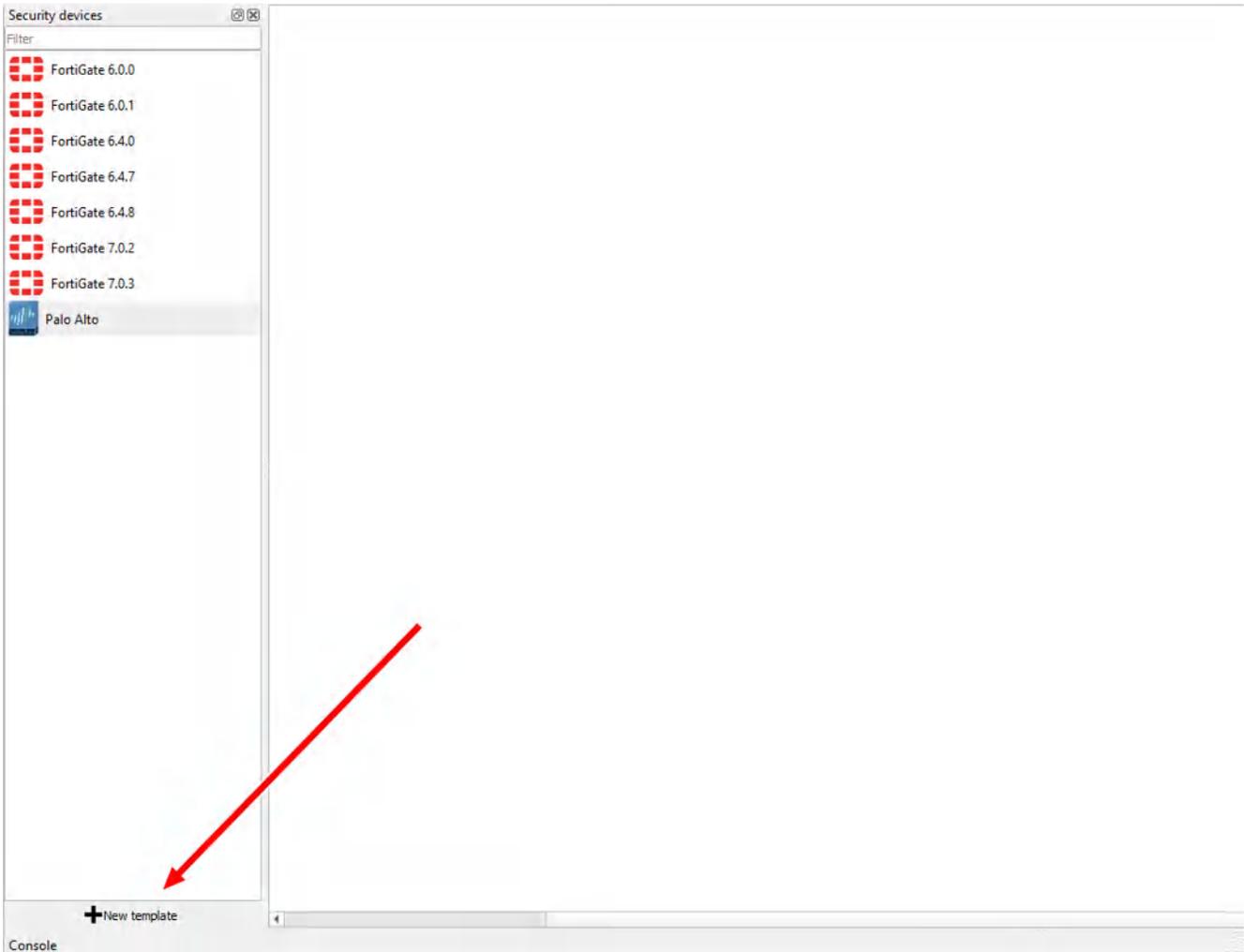


Figure A.16: Create a new template

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

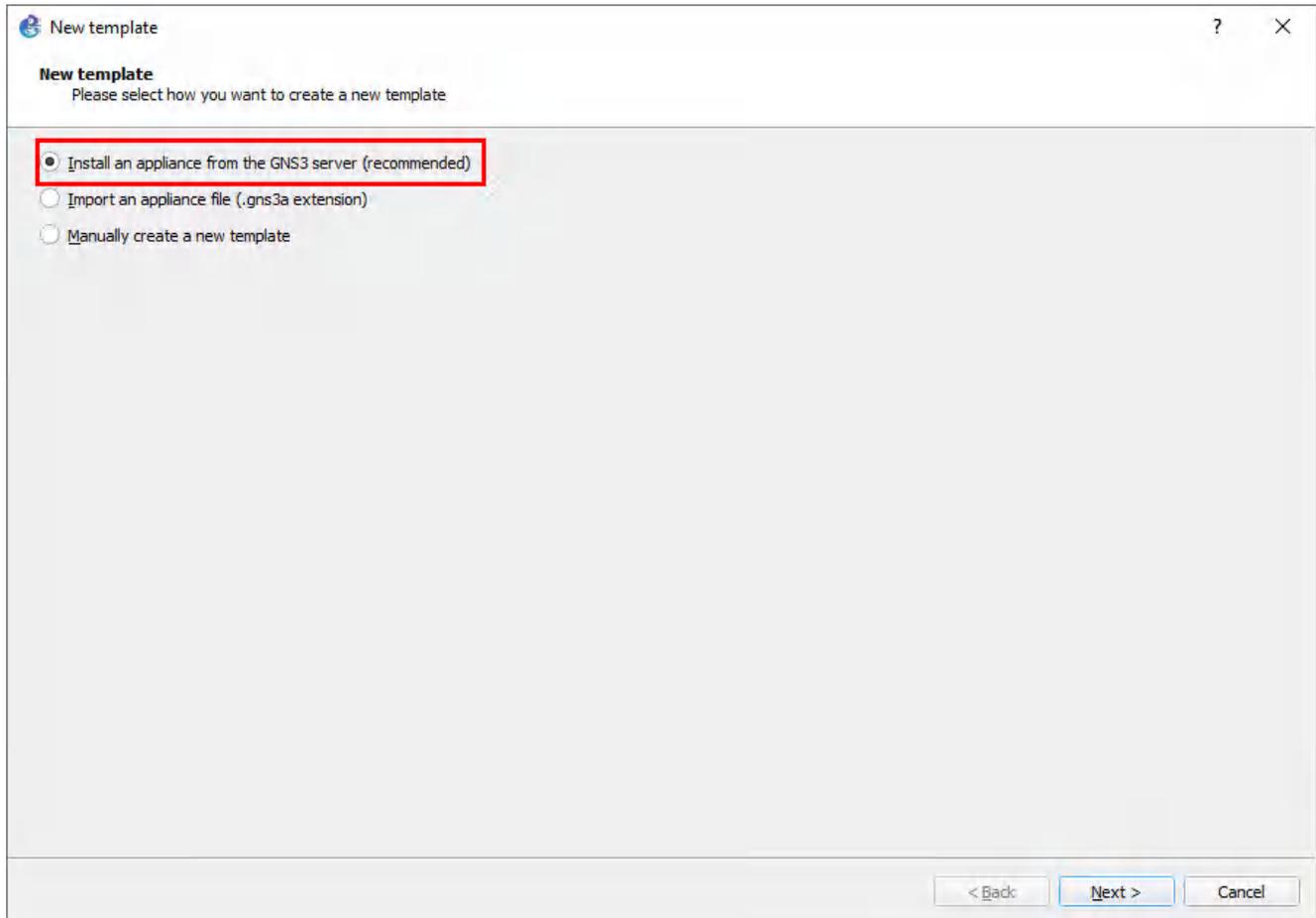


Figure A.17: Select “Install an appliance from the GNS3 server”

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

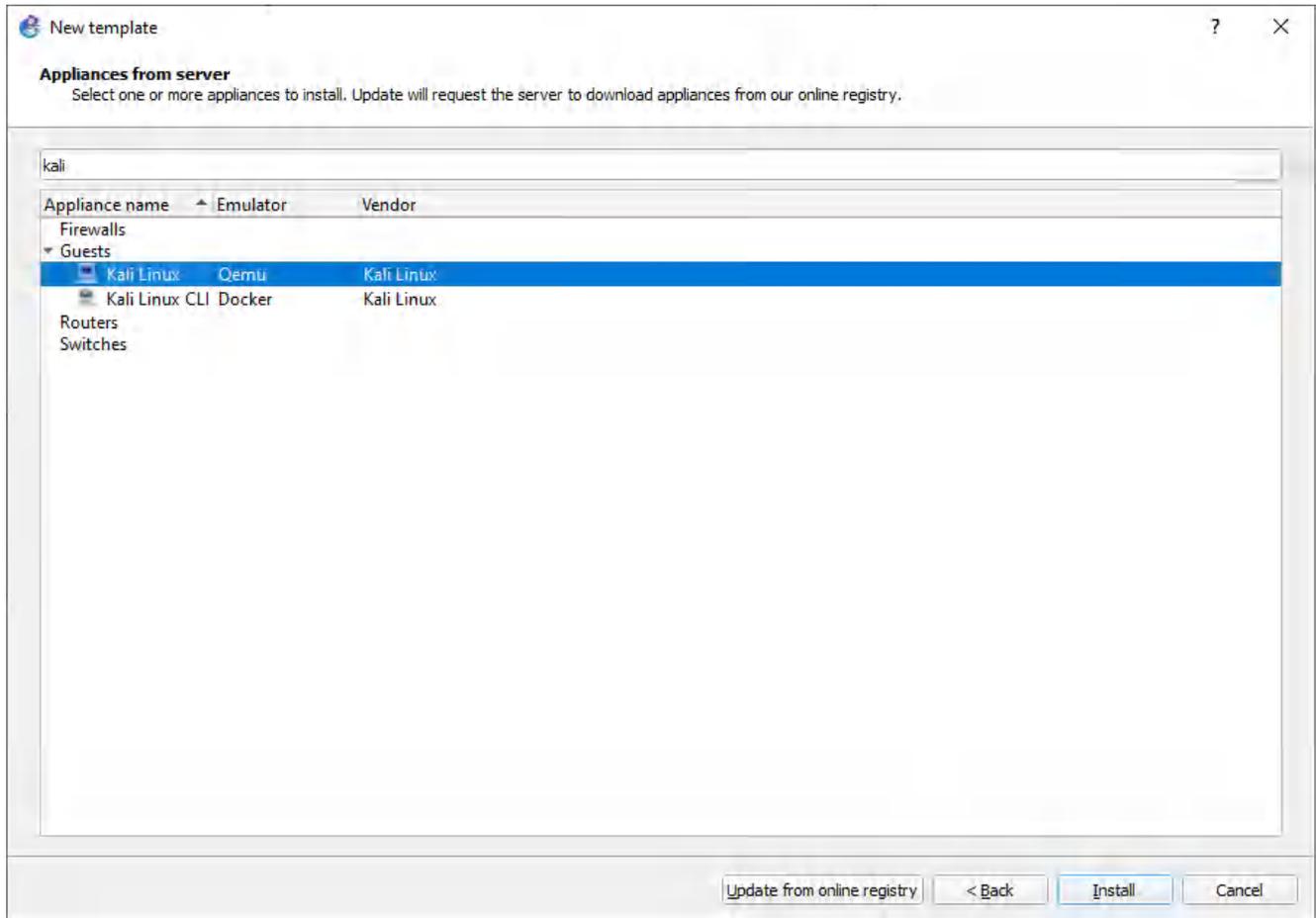


Figure A.18: Search for “kali”

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

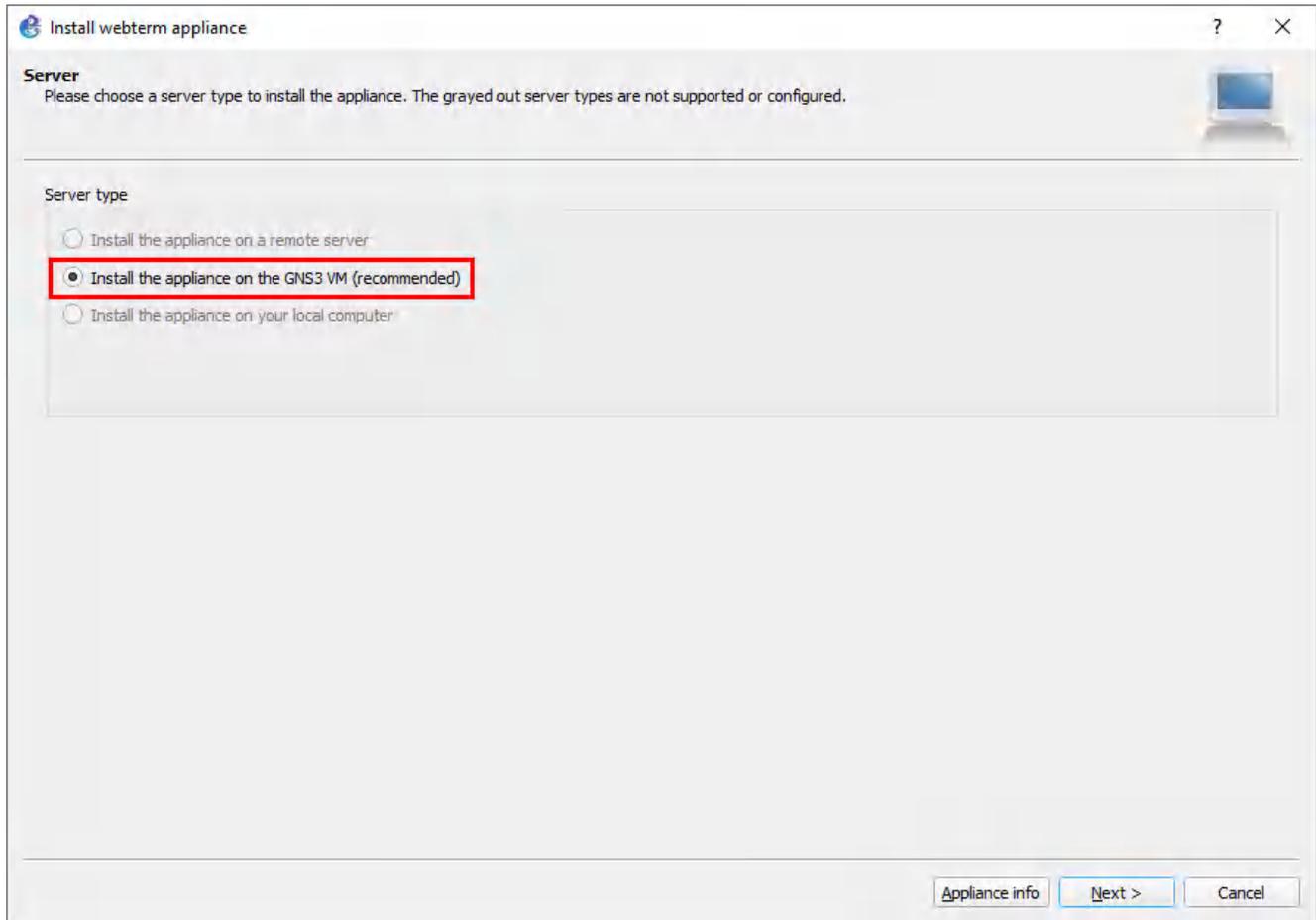


Figure A.19: Select “Install the appliance on the GNS3 VM”

Next again.

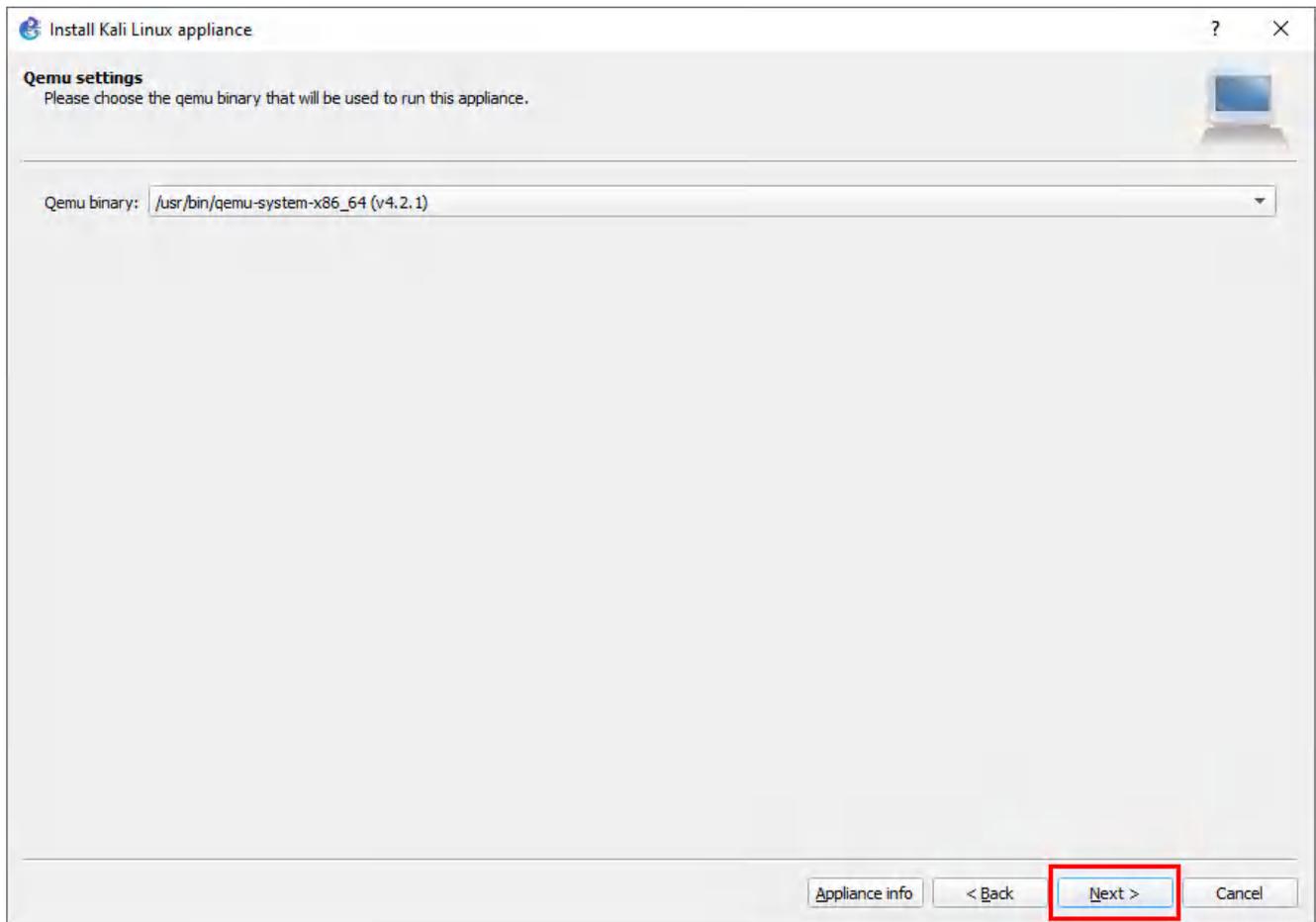


Figure A.20: Select Qemu binary

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

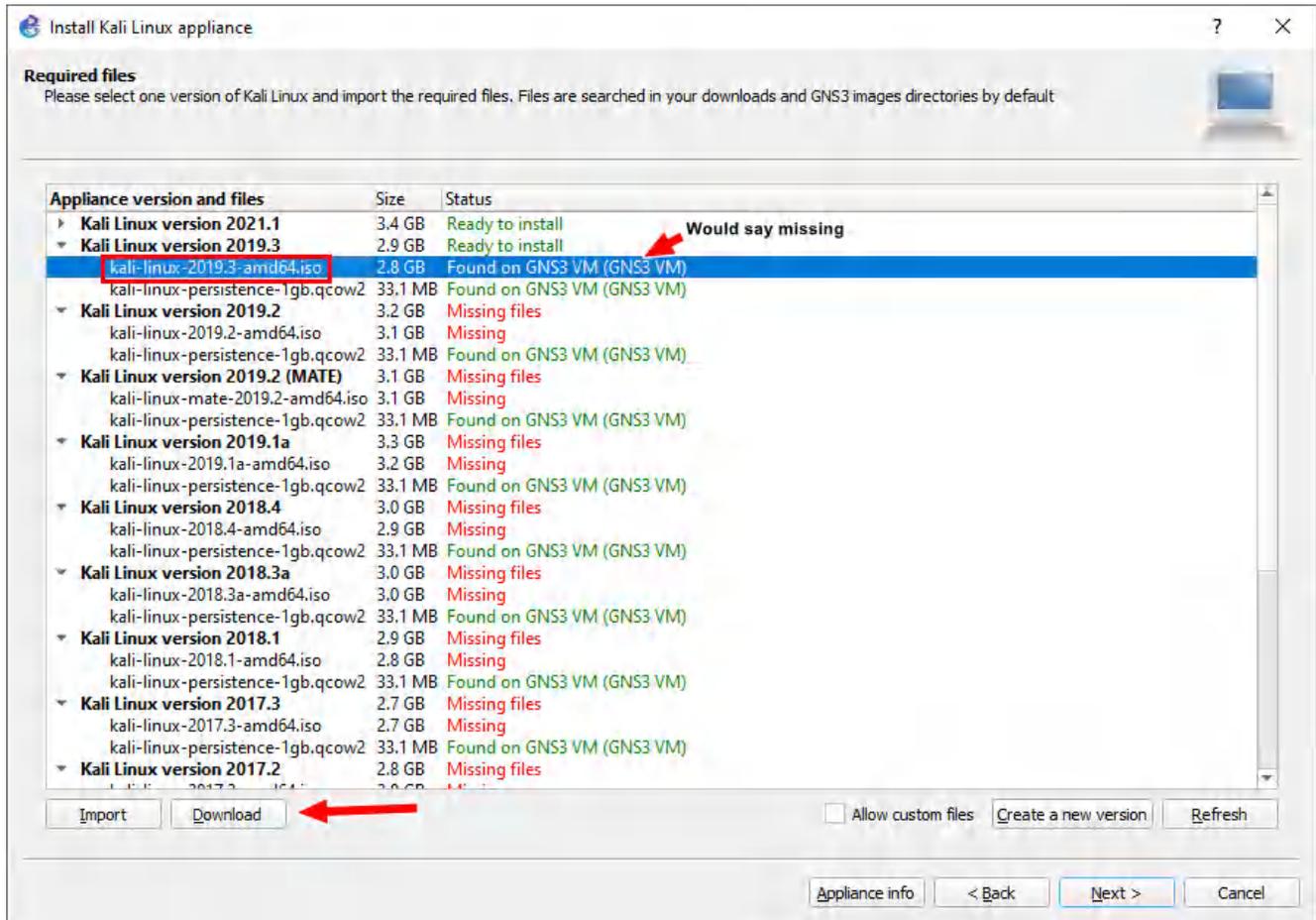


Figure A.21: Select “kali-linux-2019.3-amd64.iso”

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

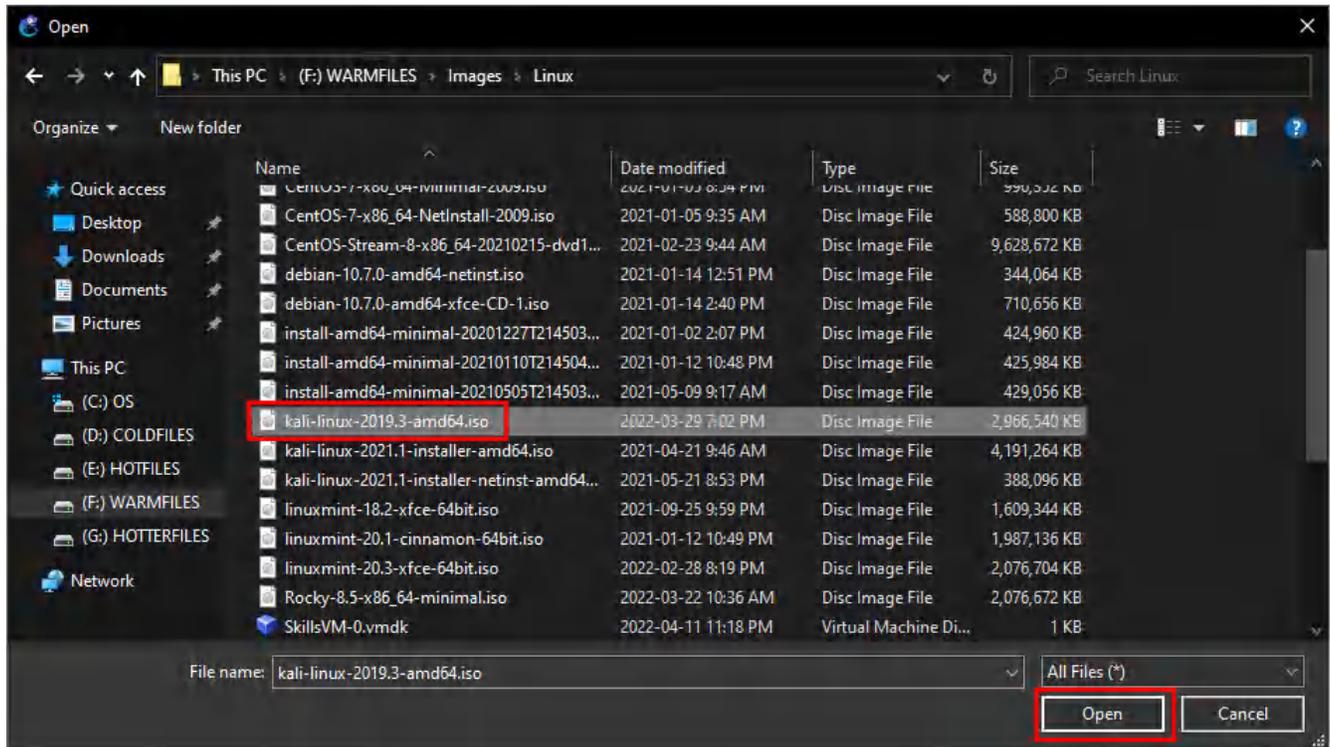


Figure A.22: Select "kali-linux-2019.3-amd64.iso"

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

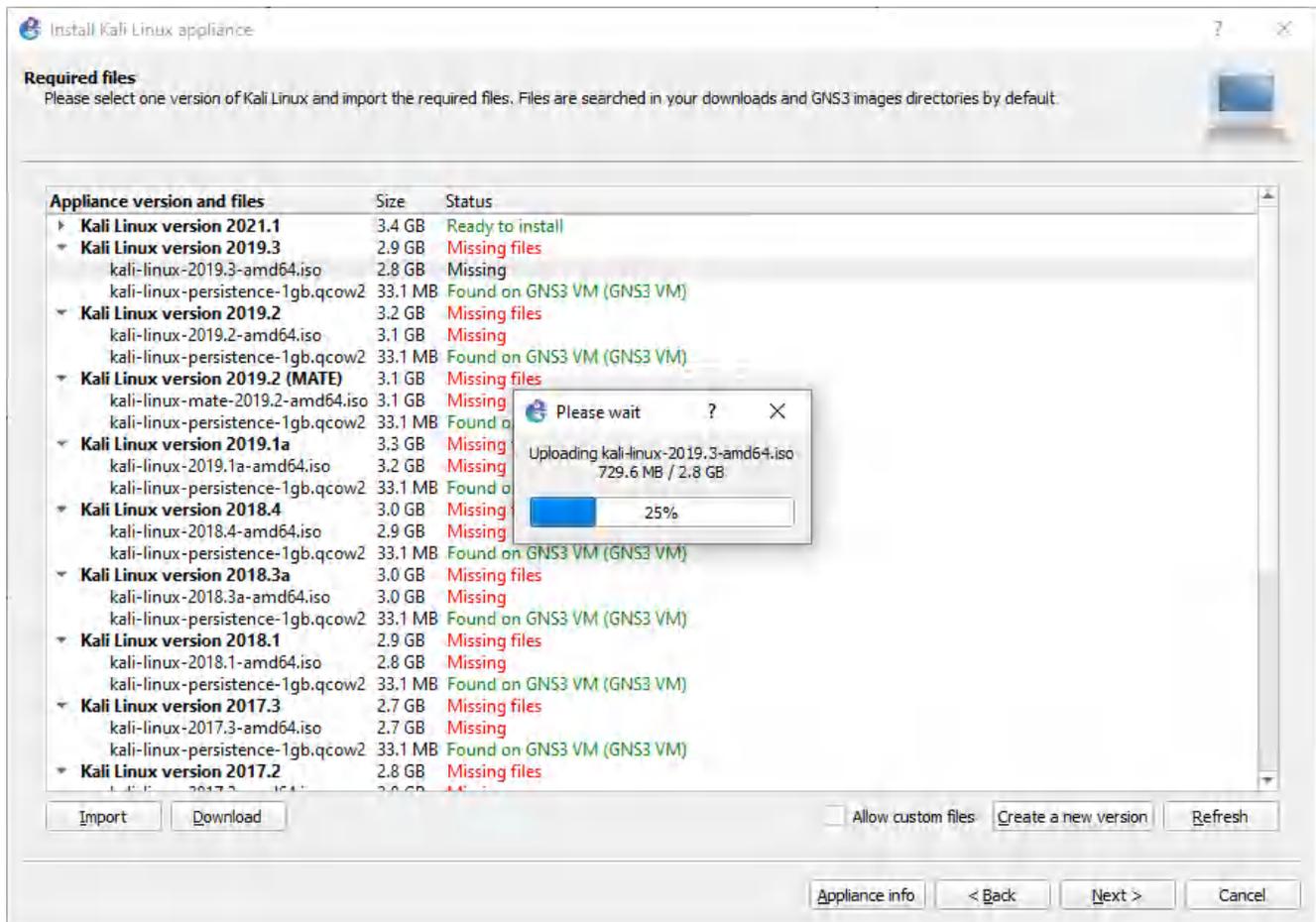


Figure A.23: Loading the ISO image

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

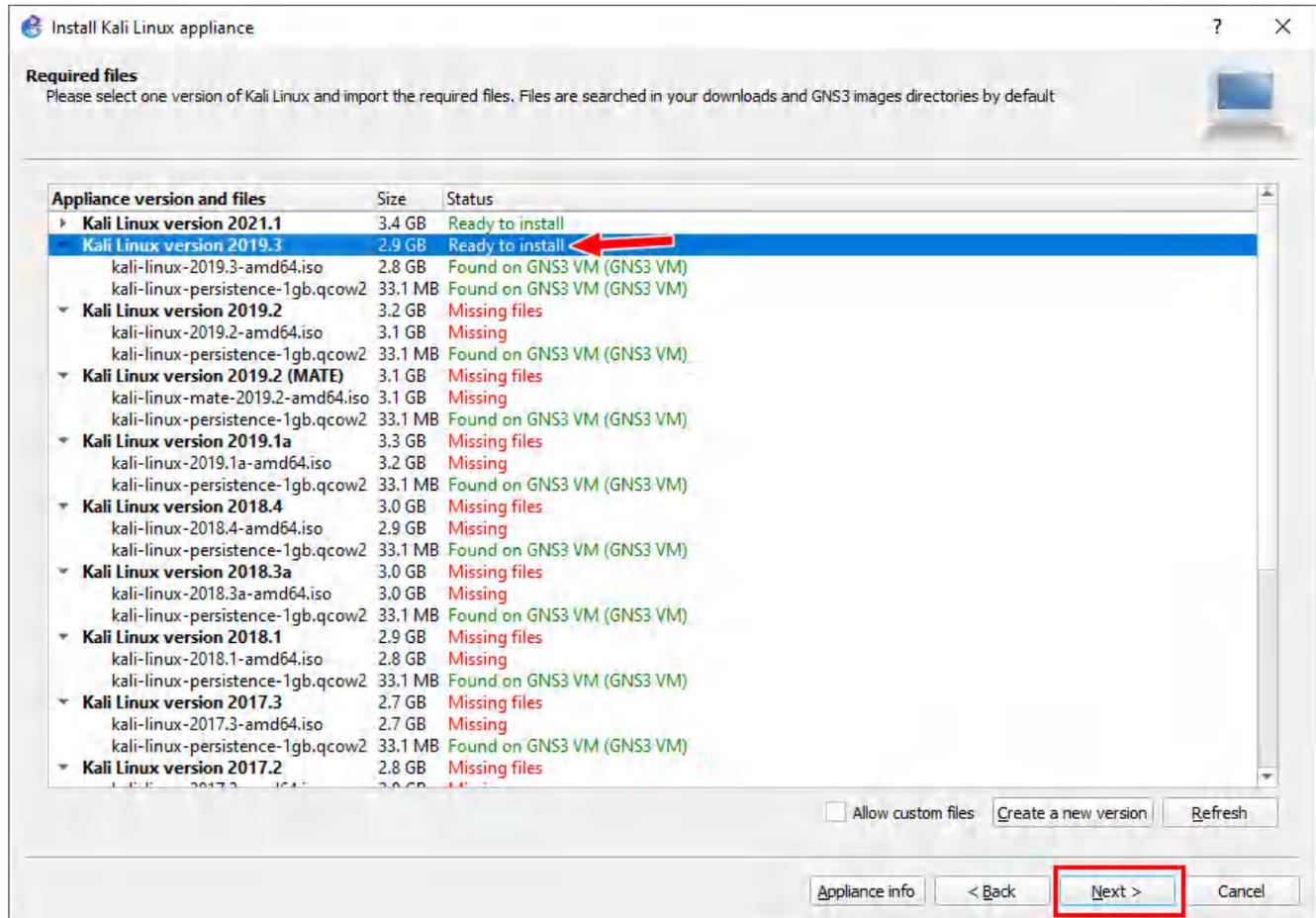


Figure A.24: Ready to install

Then click Finish.

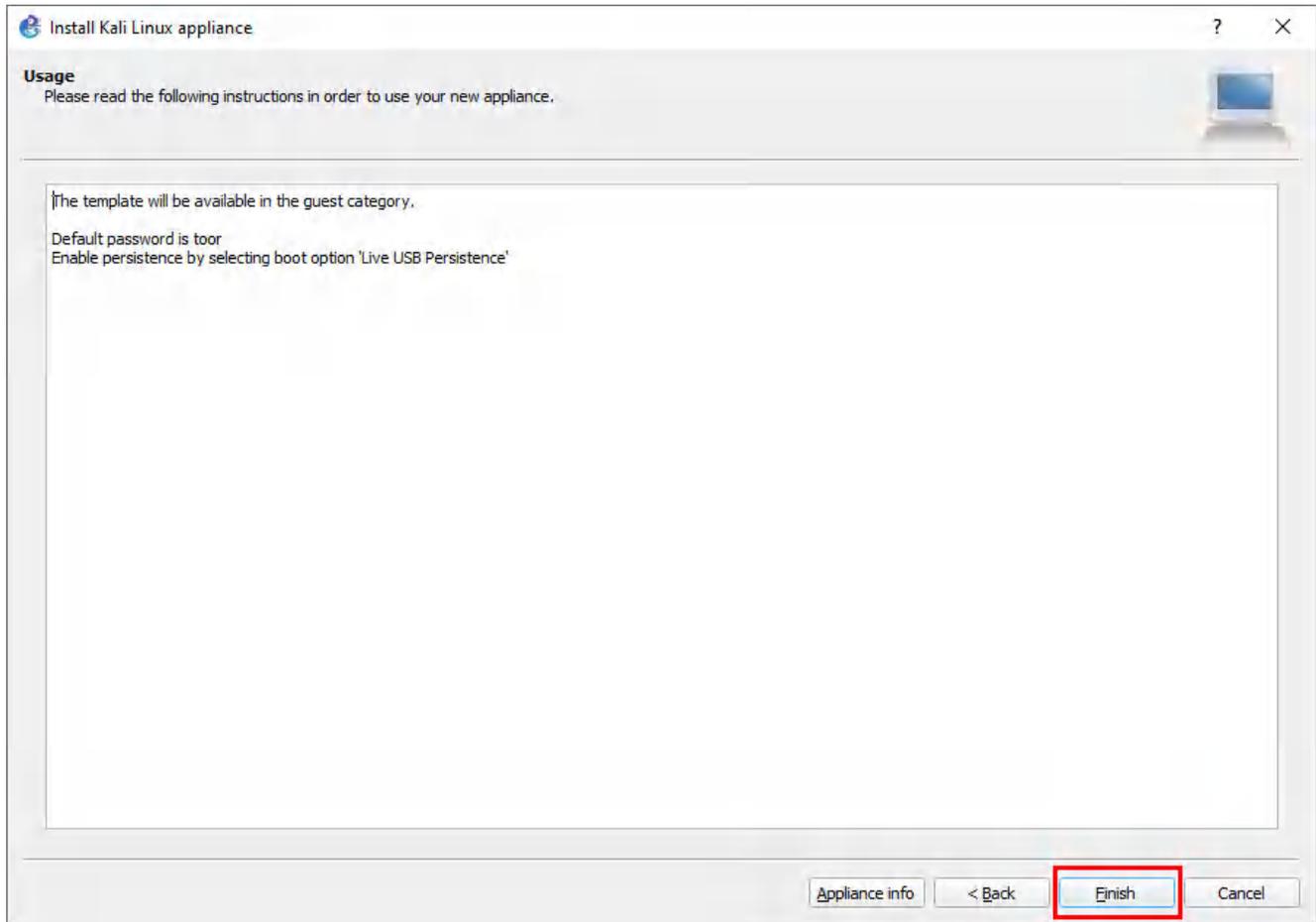


Figure A.25: Final step of configuration

## 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.

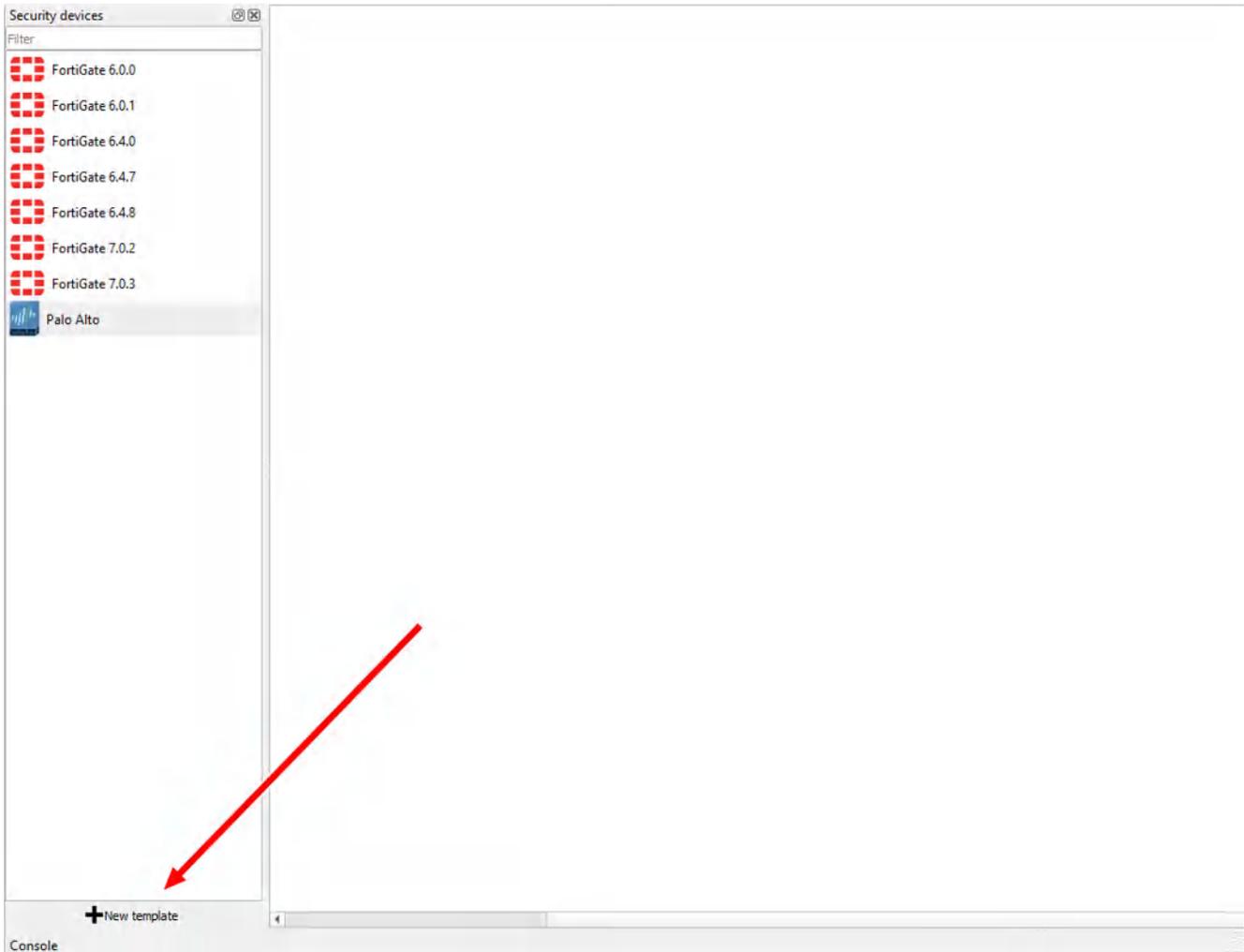


Figure A.26: Create a new template

We want to install an appliance from the GNS3 server.

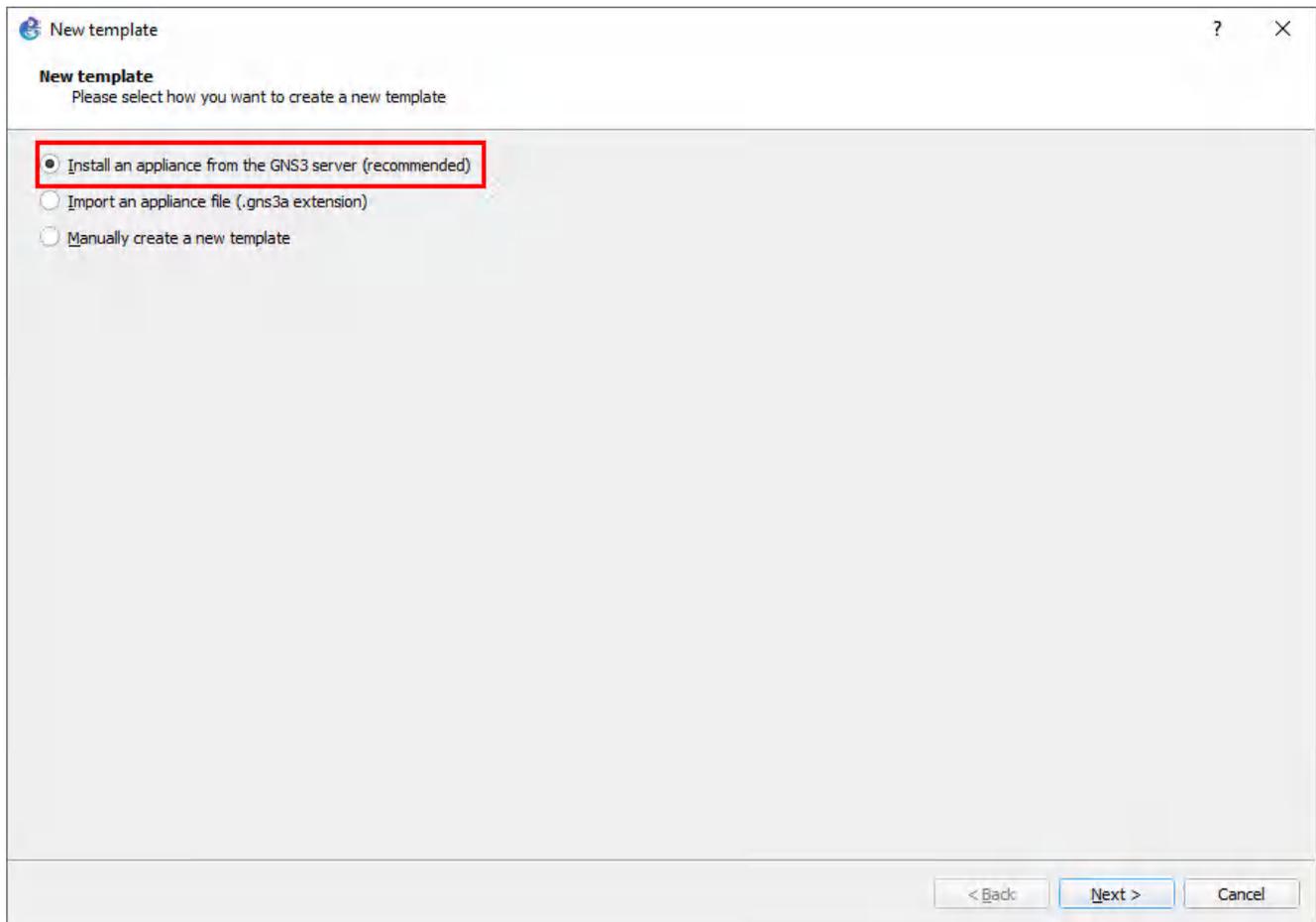


Figure A.27: Select “Install an appliance from the GNS3 server”

Lookup “WordPress”, then click Install.

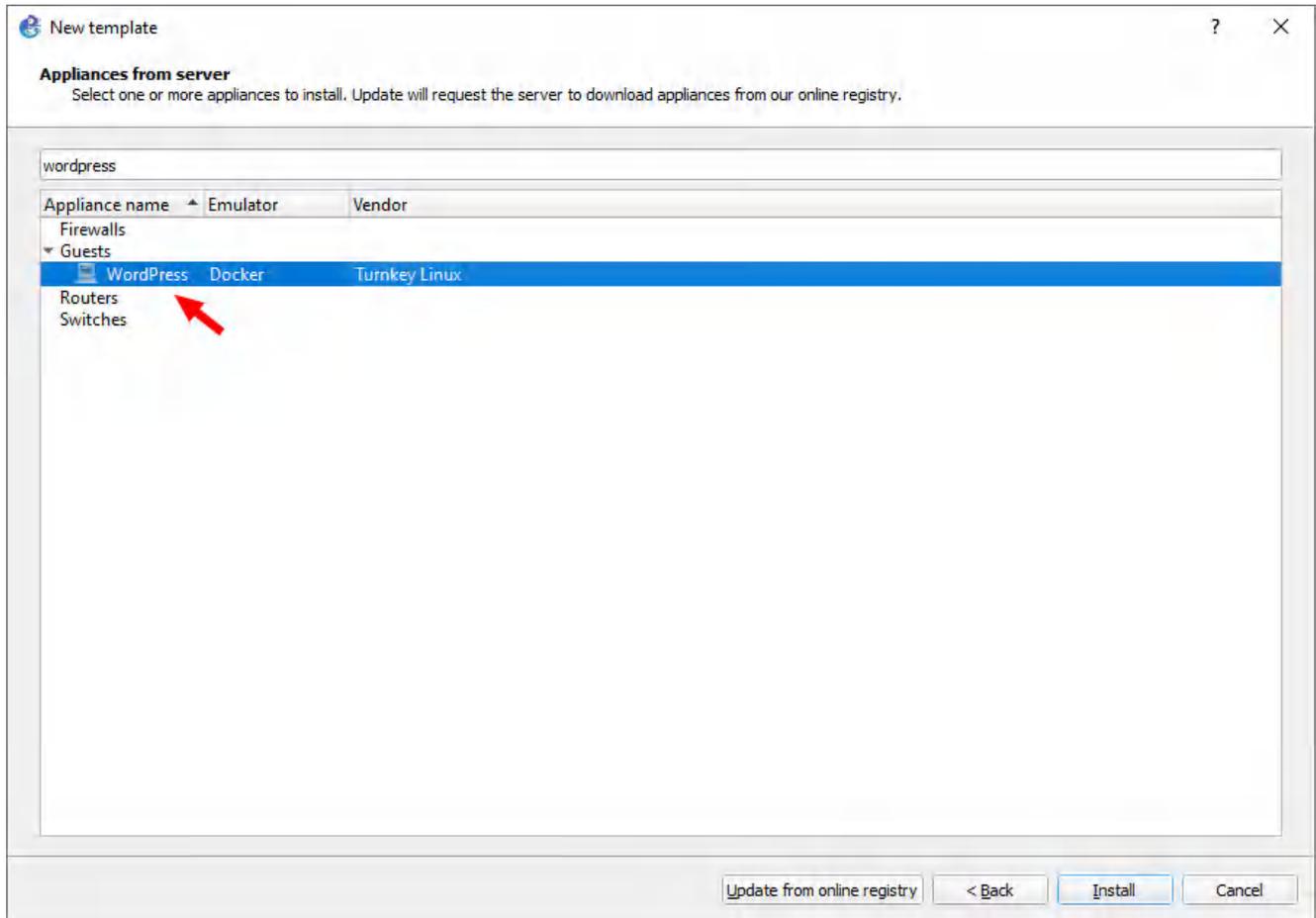


Figure A.28: Search for “WordPress”

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

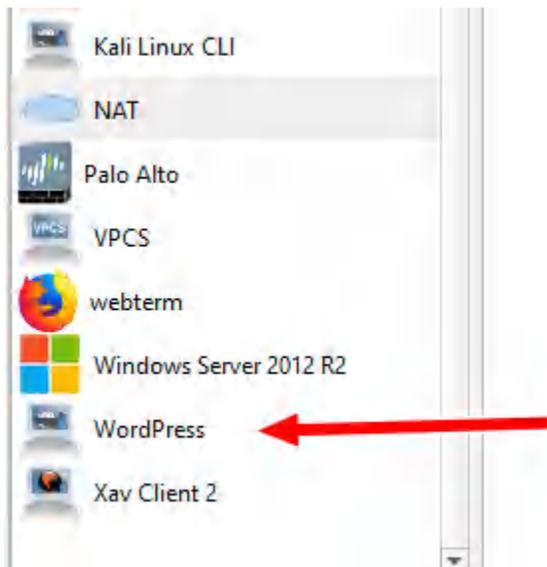


Figure A.29: Verify WordPress Installation

## Configure WordPress

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

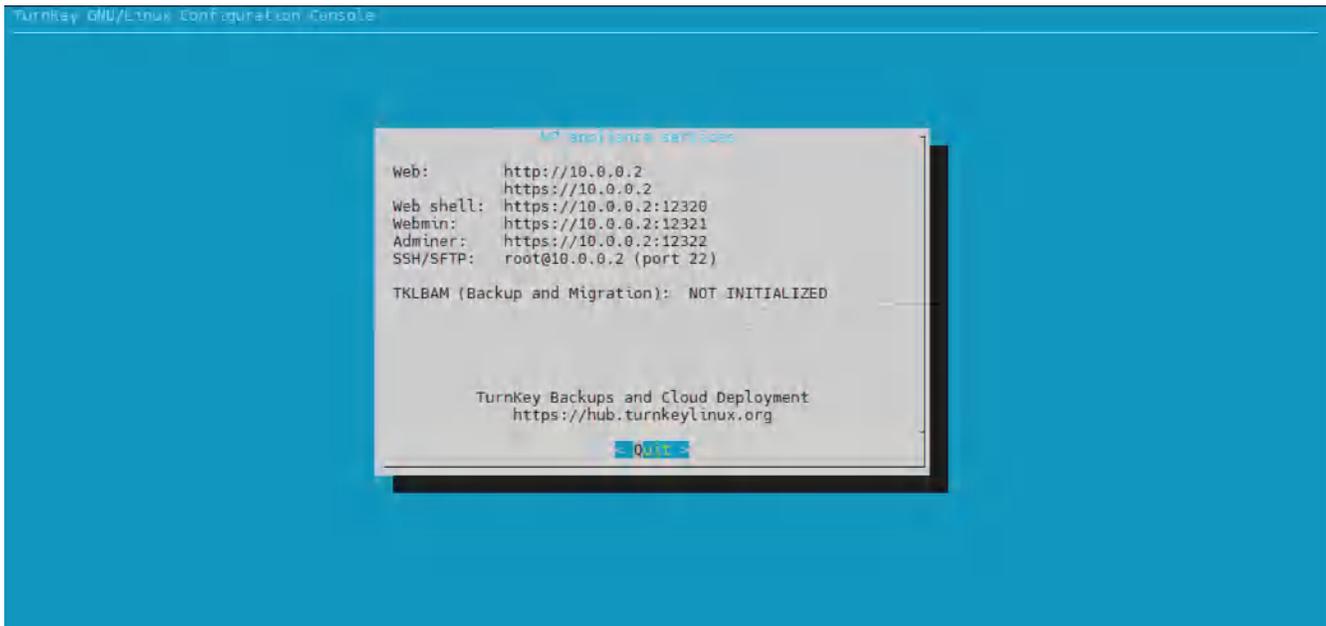


Figure A.30: Running WordPress

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!

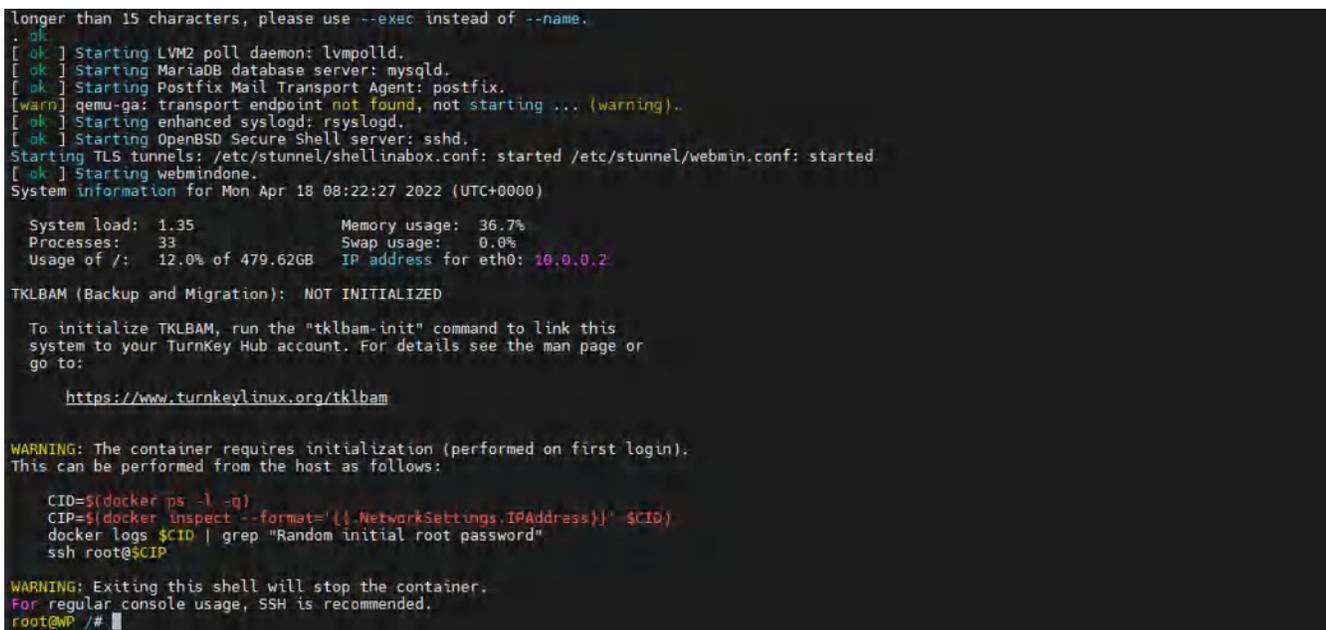


Figure A.31: WordPress is Ready!

## 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.

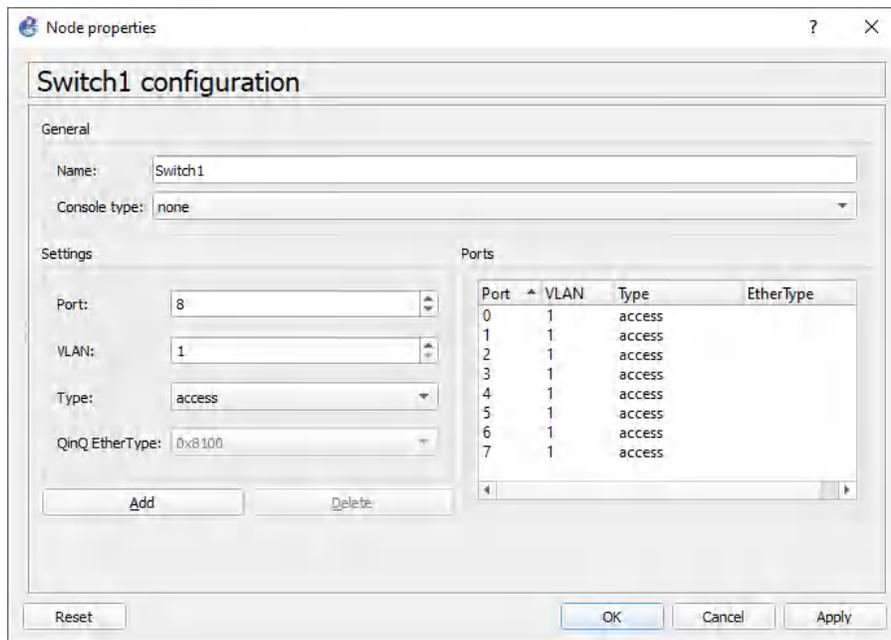


Figure A.32: Switch Configuration

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

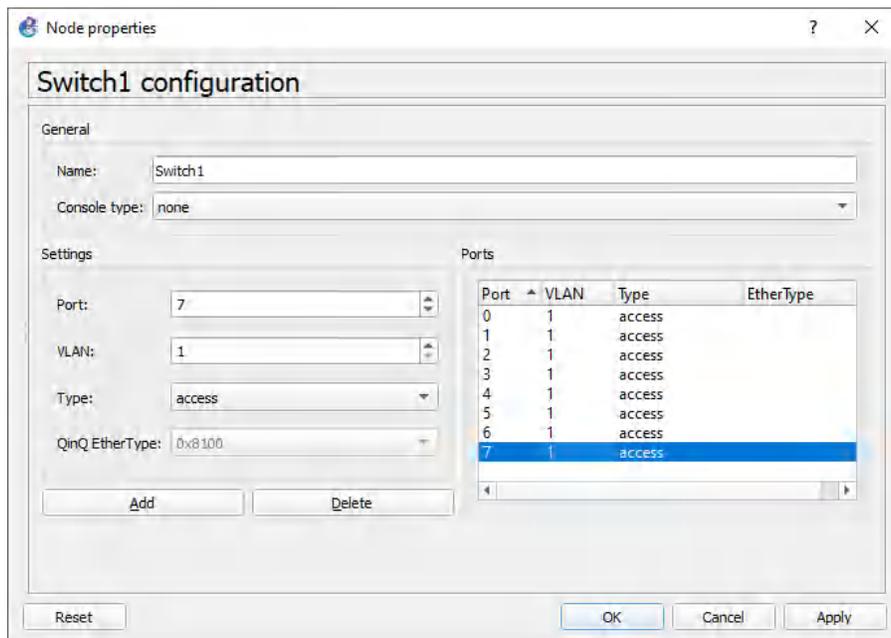


Figure A.33: Double click on port7

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

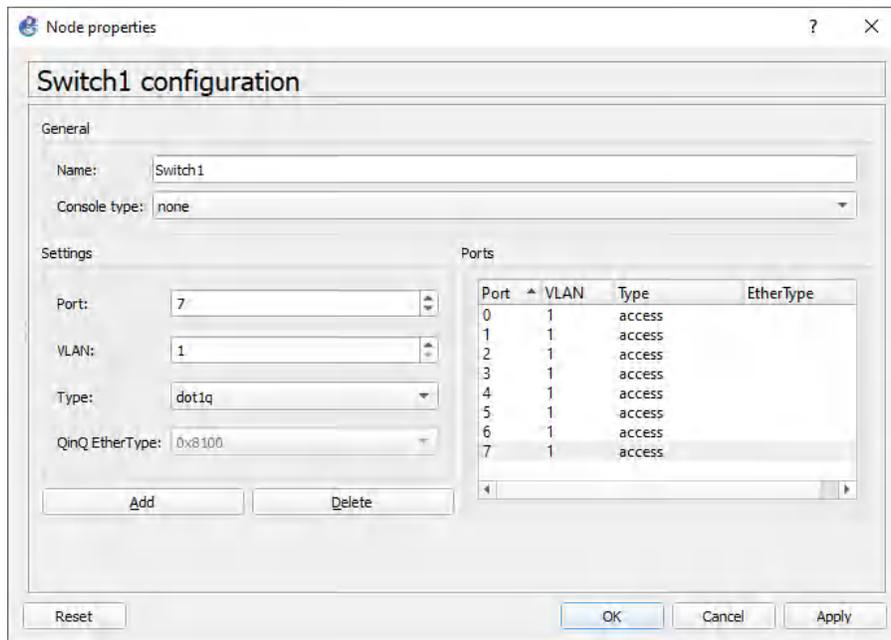


Figure A.34: Select port7 as dot1q

Click on add to apply the changes.

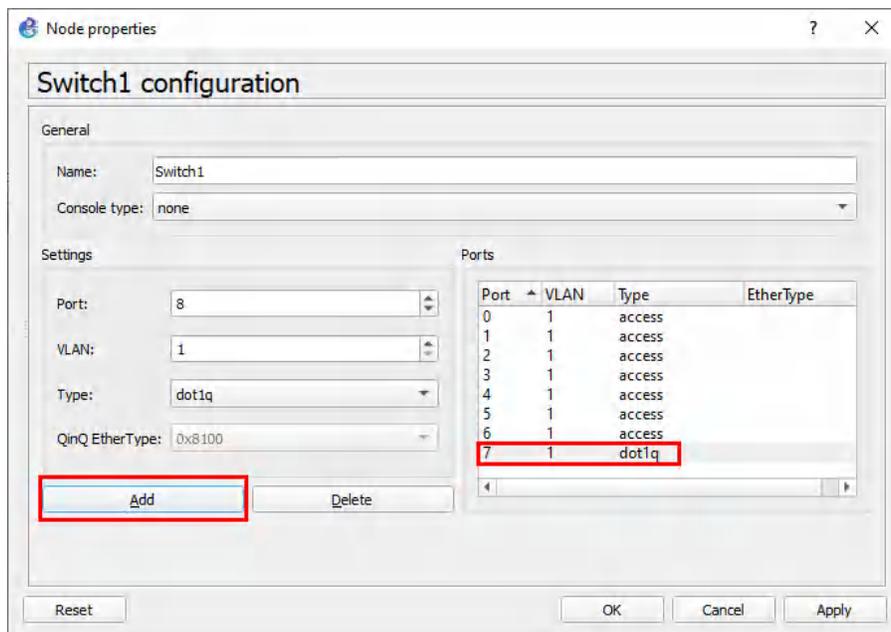


Figure A.35: Click on Add to apply the changes

Then click Apply and OK.



## Acknowledgements

We would like to thank Kacem Habiballah and Tim Carson for their great support during the project. Also, I appreciate [BCcampus](#) 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.



---

## 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.





---

## Versioning History

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

The files posted by this book always reflect the most recent version. If you find an error in this book, please fill out the [Report an Error](#) form.

Version	Date	Change	Details
1.00	November 29, 2023	Book published.	First version.