Palo Alto Firewall

Palo Alto Firewall

Practical Guidance and Hands-On Labs

Hamid Talebi and Xavier Cawley

BCCAMPUS
VICTORIA, B.C.

Sample APA-style citation (7th Edition):

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

Cover image attribution:

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

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

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

Visit BCcampus Open Education to learn about open education in British Columbia.

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

Contents

Accessibility Statement

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

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.

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:

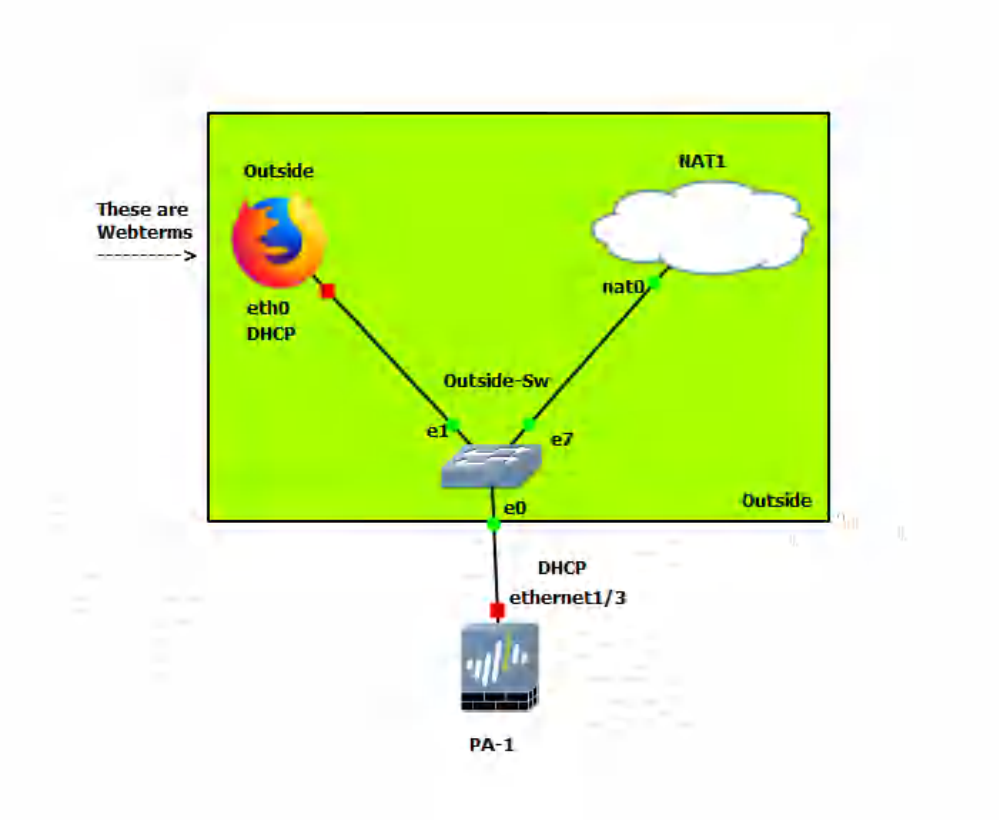


Figure E.1: An example scenario

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

1.1 GNS3 and Palo Alto

Learning Objectives

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

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

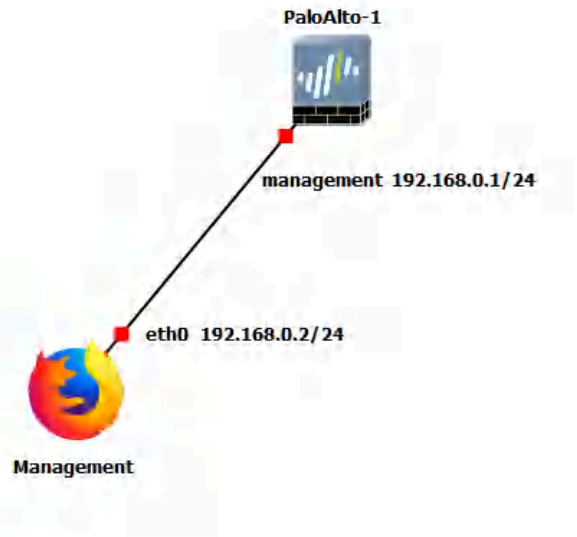


Figure 1.1: Main Scenario

Table 1.1: Addressing Table

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

Console into the Palo Alto Device

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

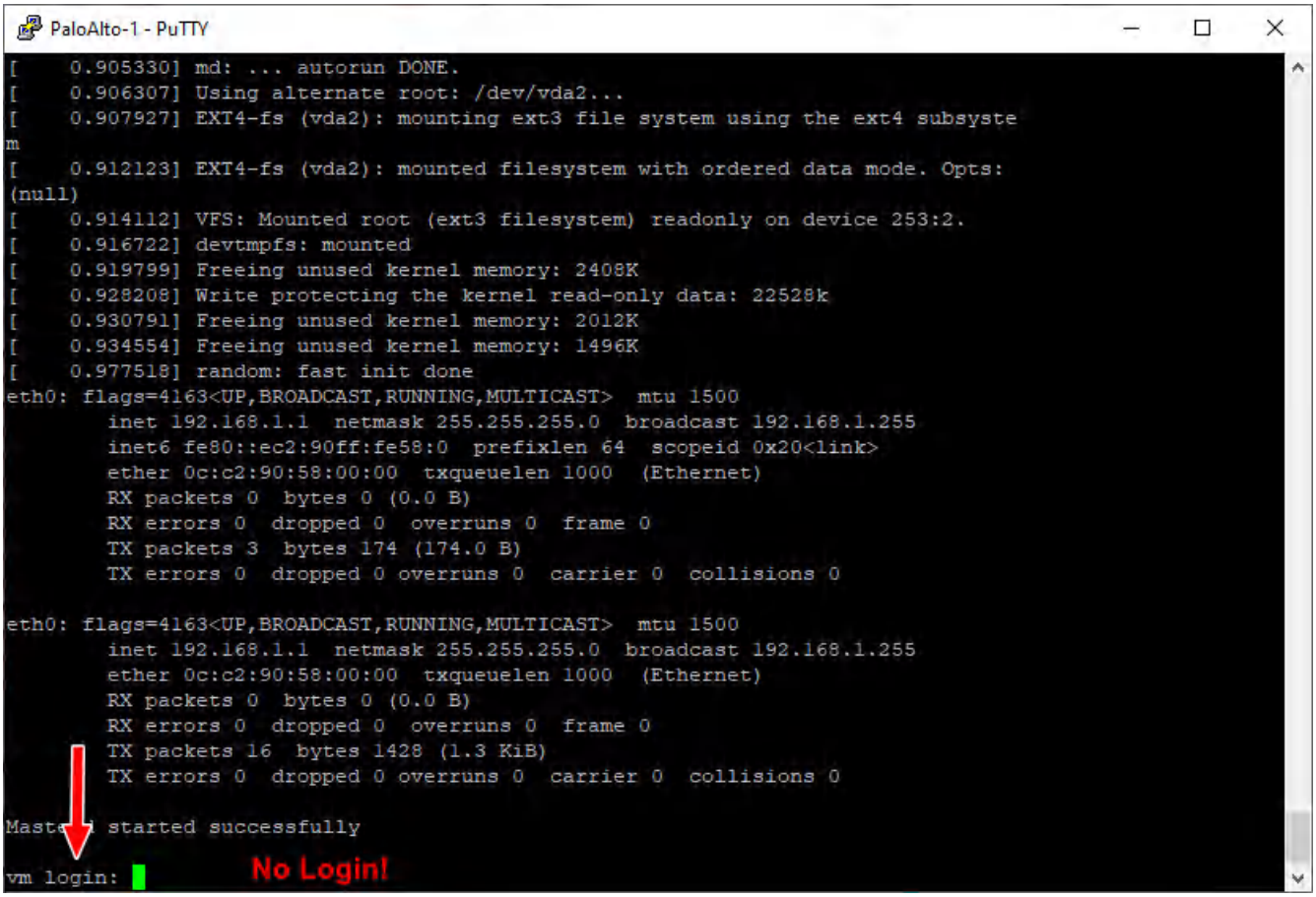


Figure 1.2: No Login

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

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

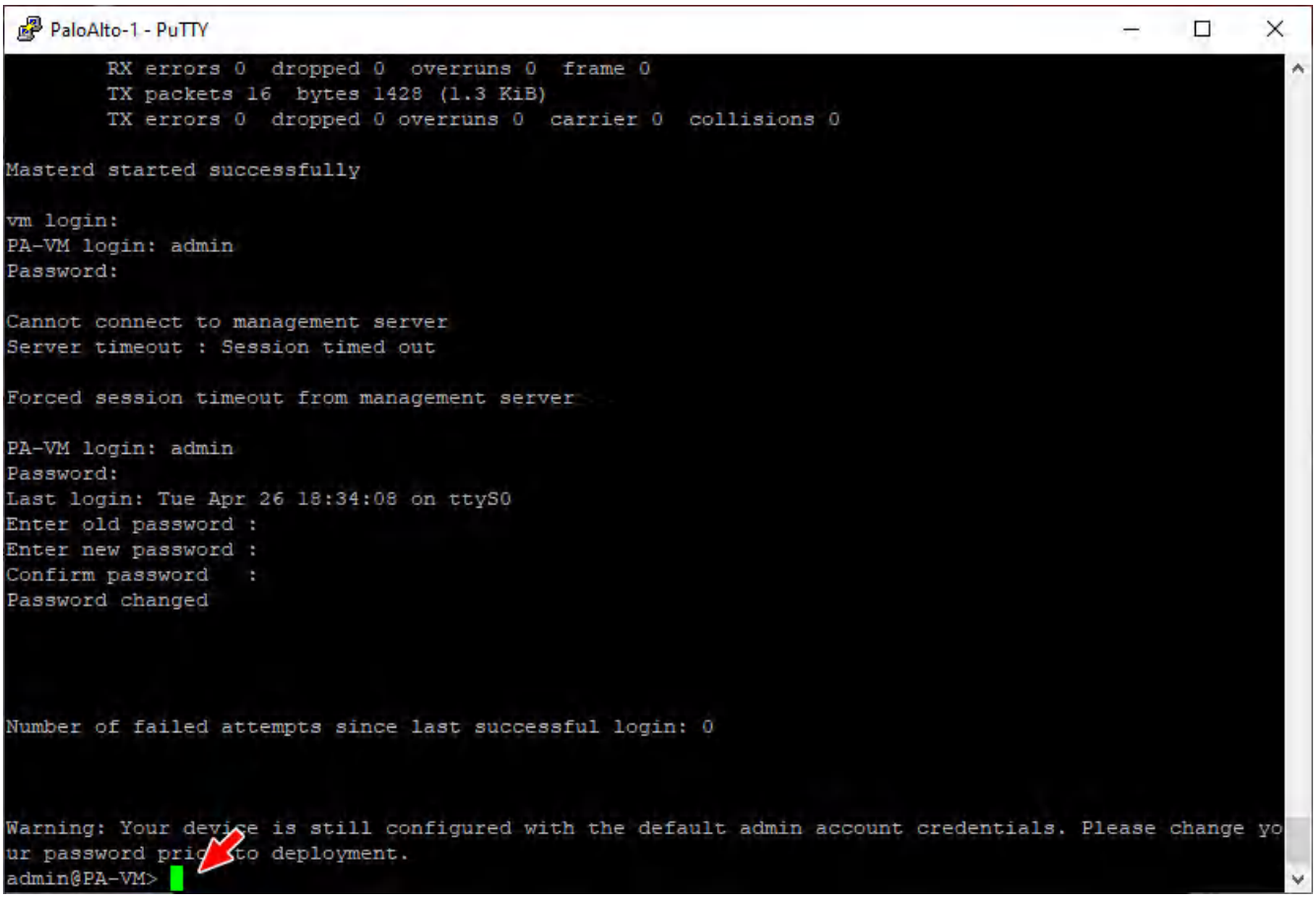


Figure 1.3: Firewall General mode

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:

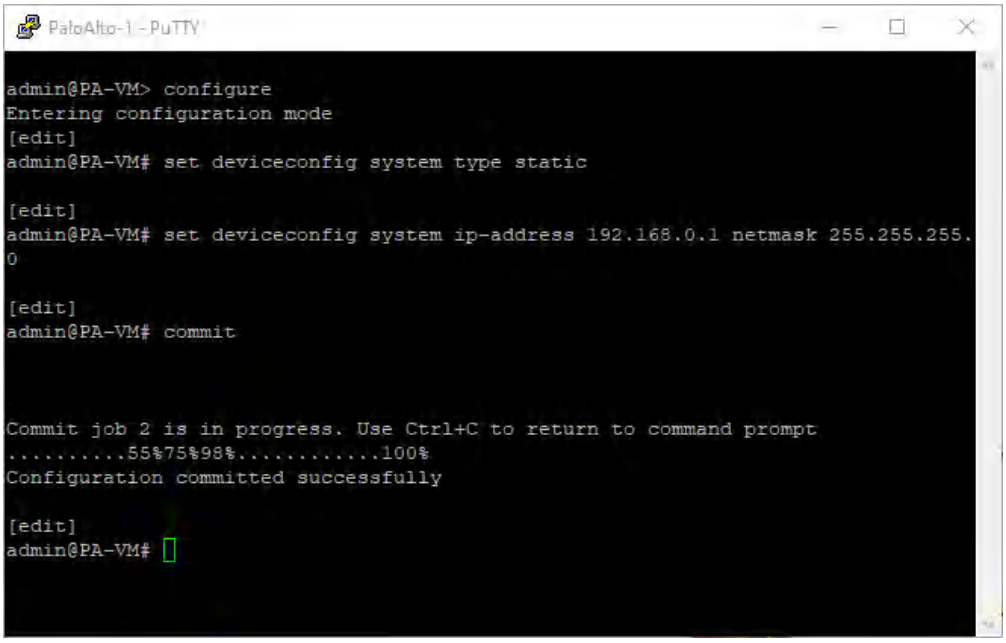


Figure 1.4: Set a static IP address

Access the Web Interface from Webterm

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

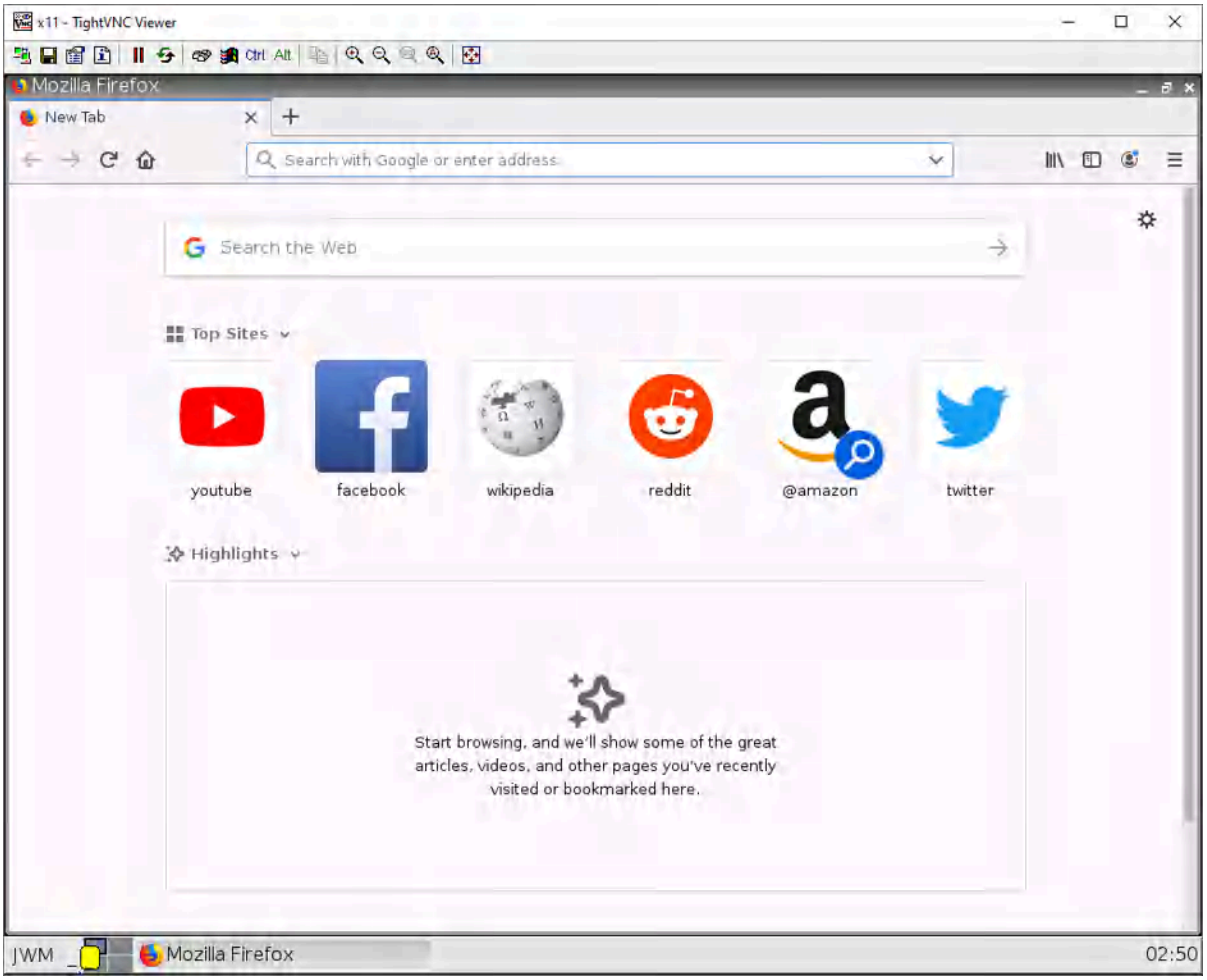


Figure 1.5: WebTerm Firefox browser

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:

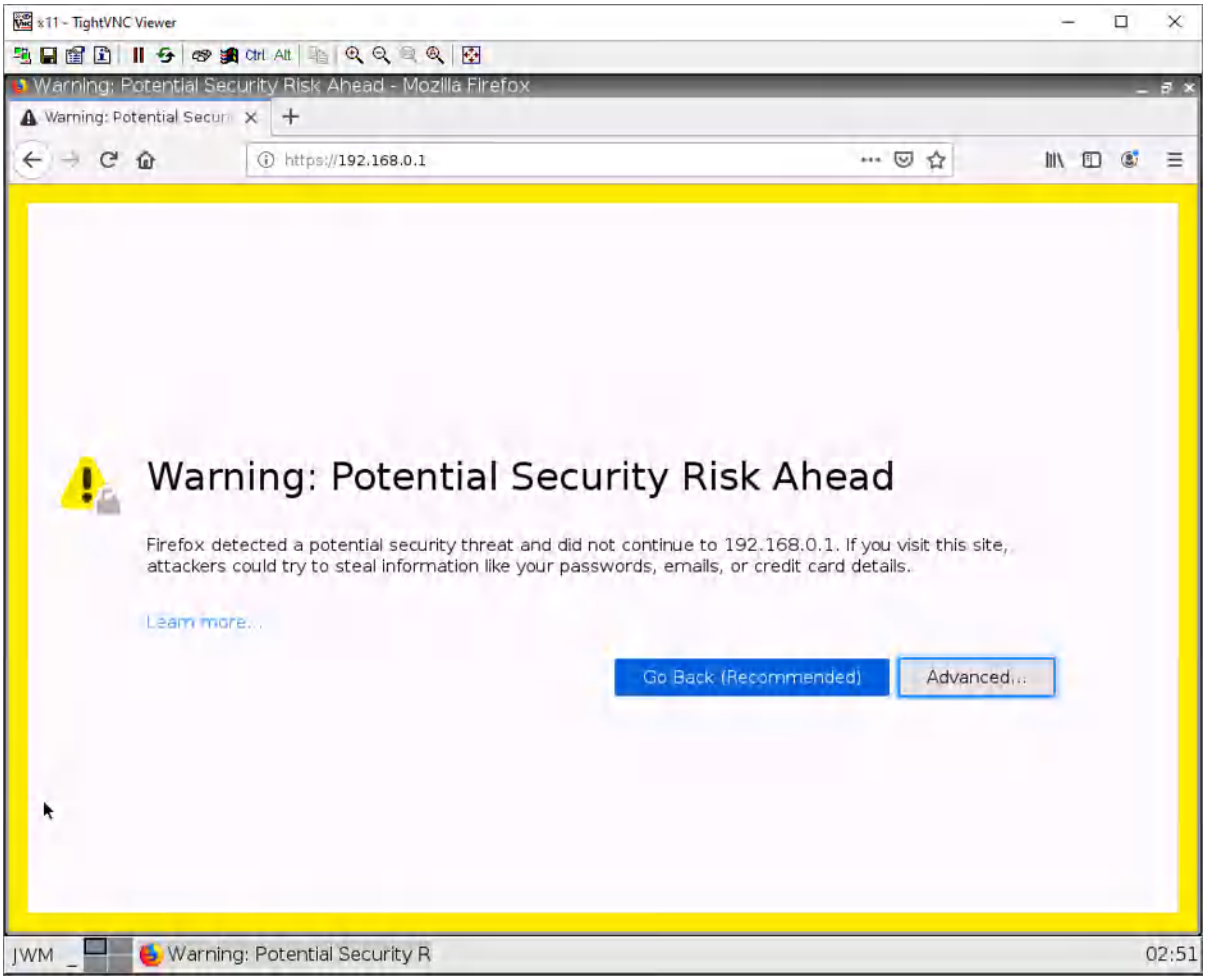


Figure 1.6: Type IP address of Palo Alto

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

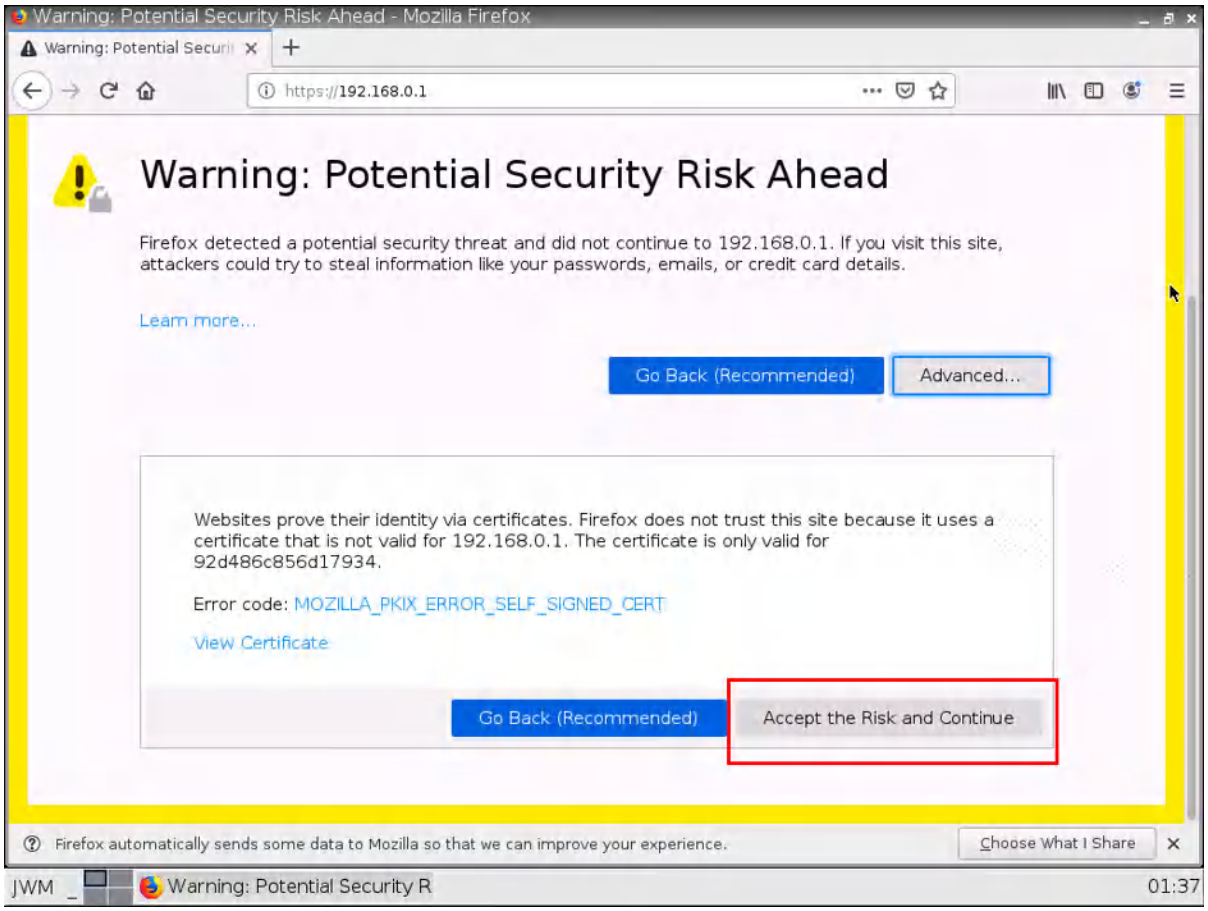


Figure 1.7: Past of security warning

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.

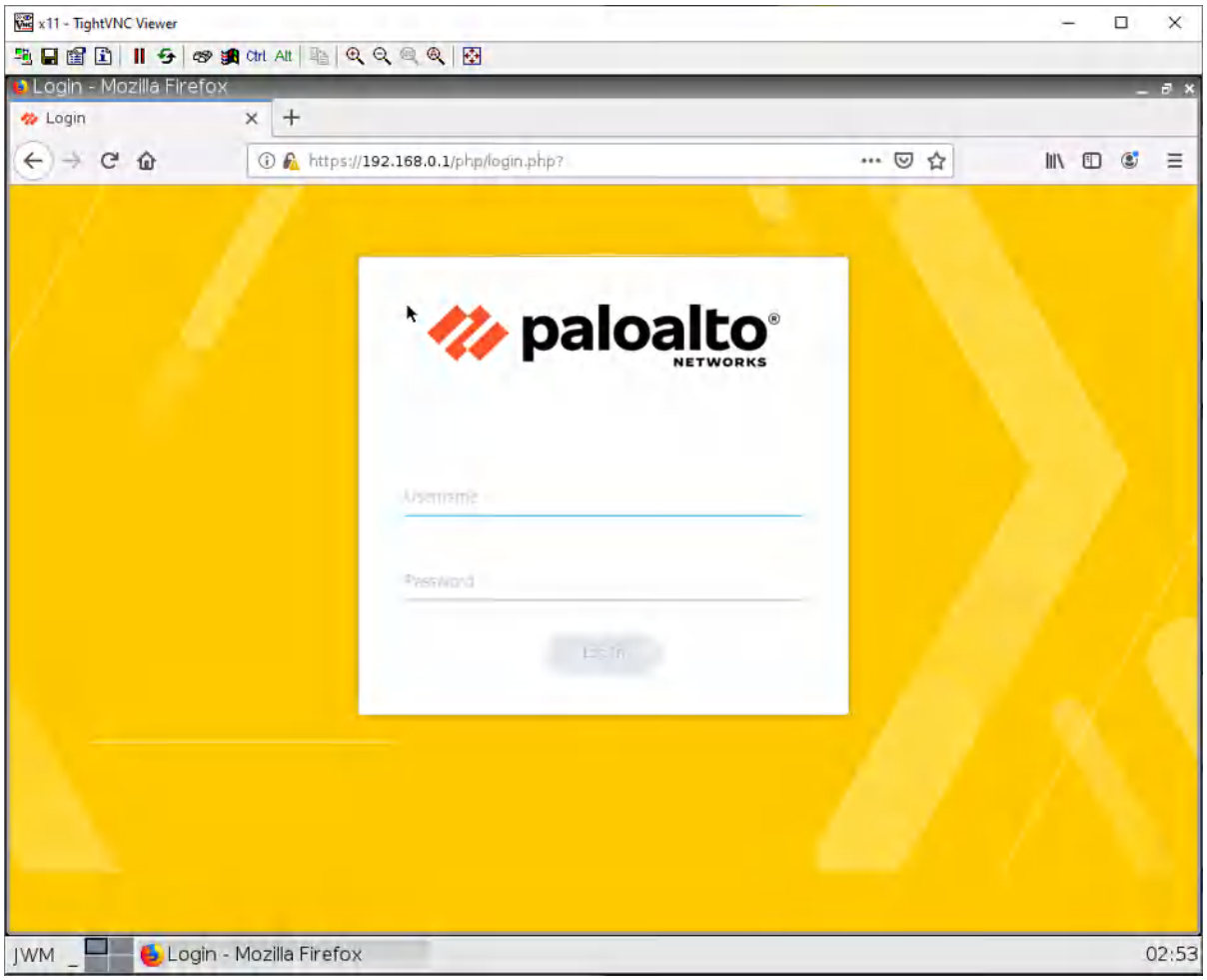


Figure 1.8: Enter credentials

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

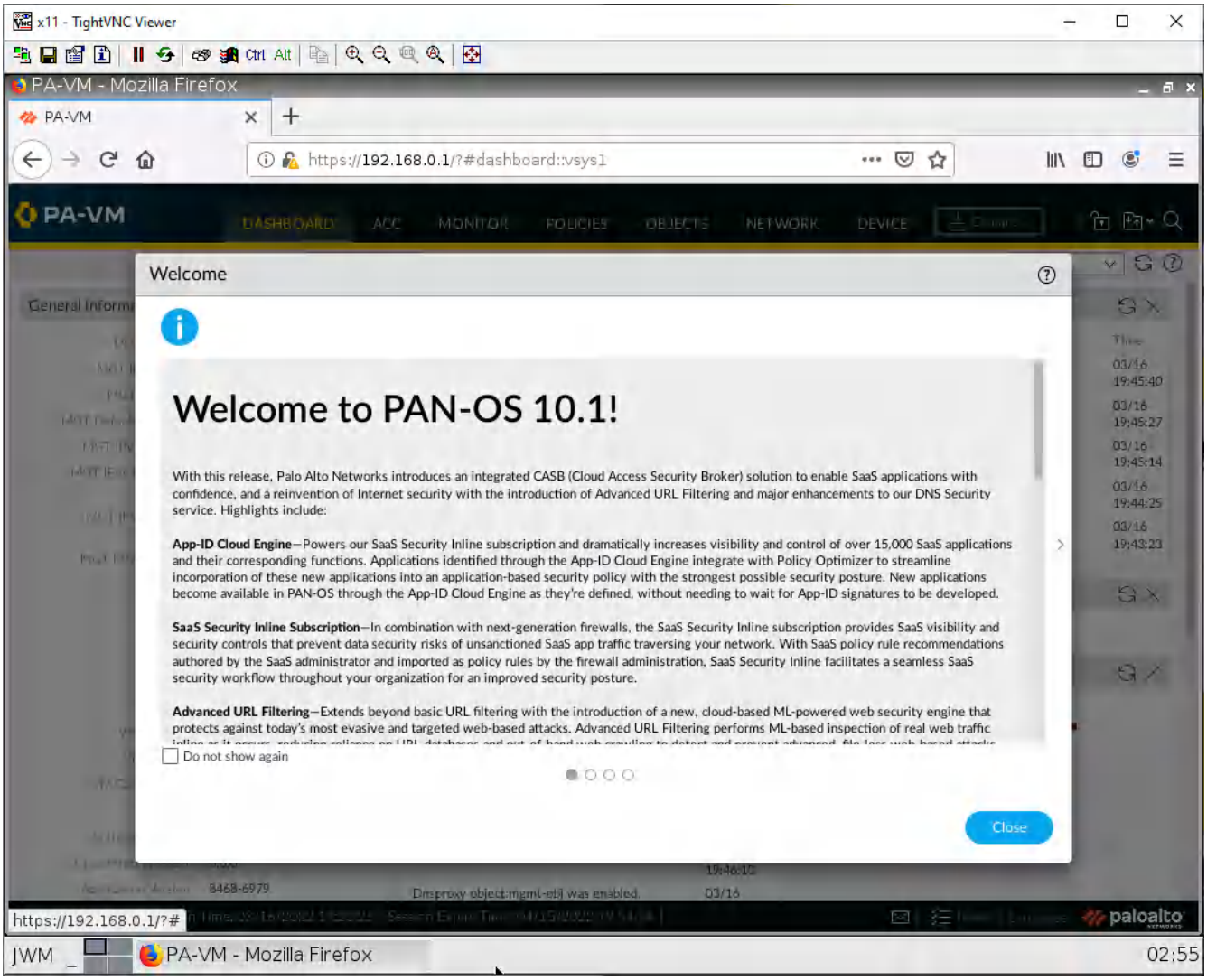


Figure 1.9: First page of Palo Alto

Explore the Web Interface

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

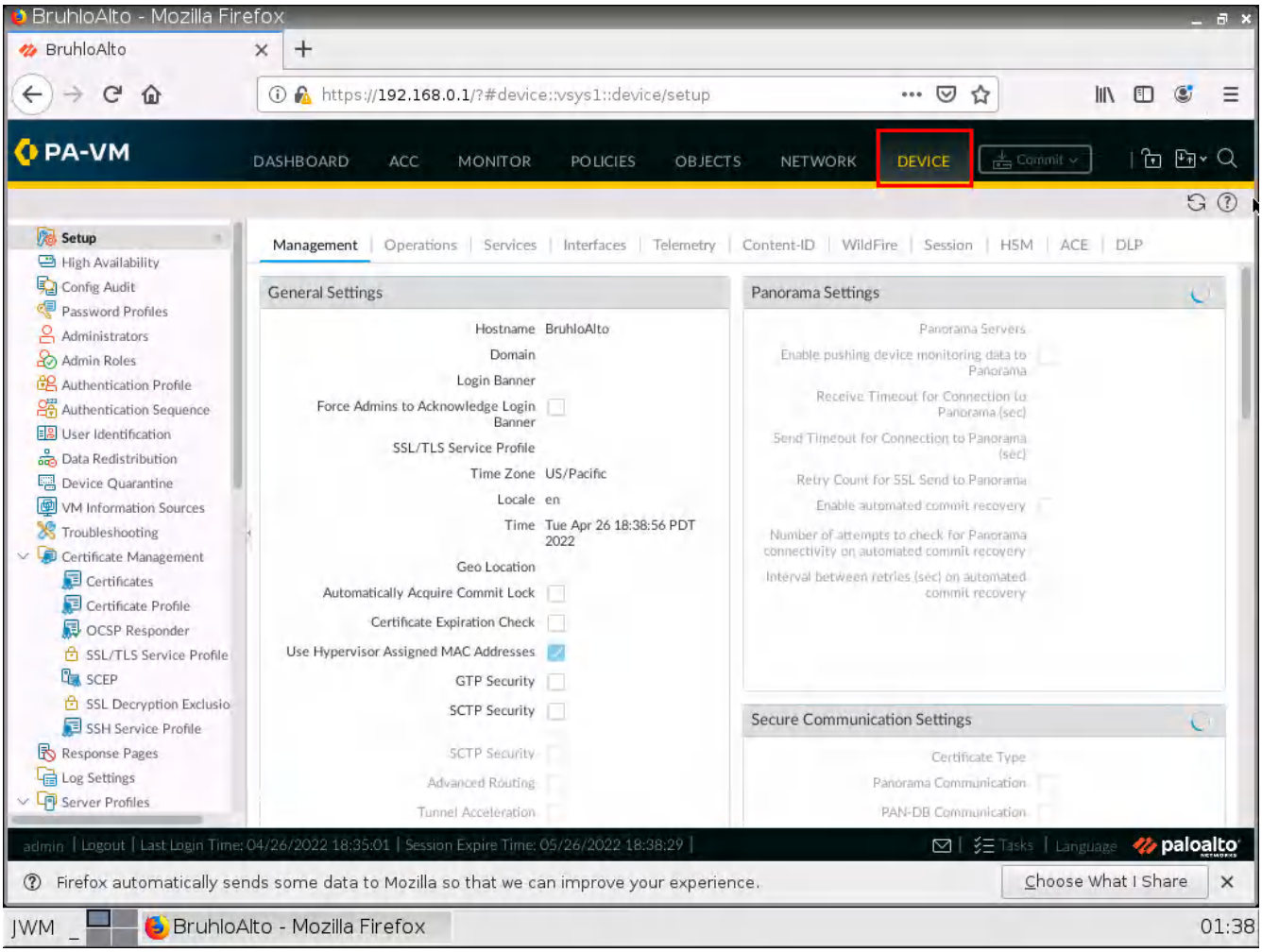


Figure 1.10: Device Settings

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.

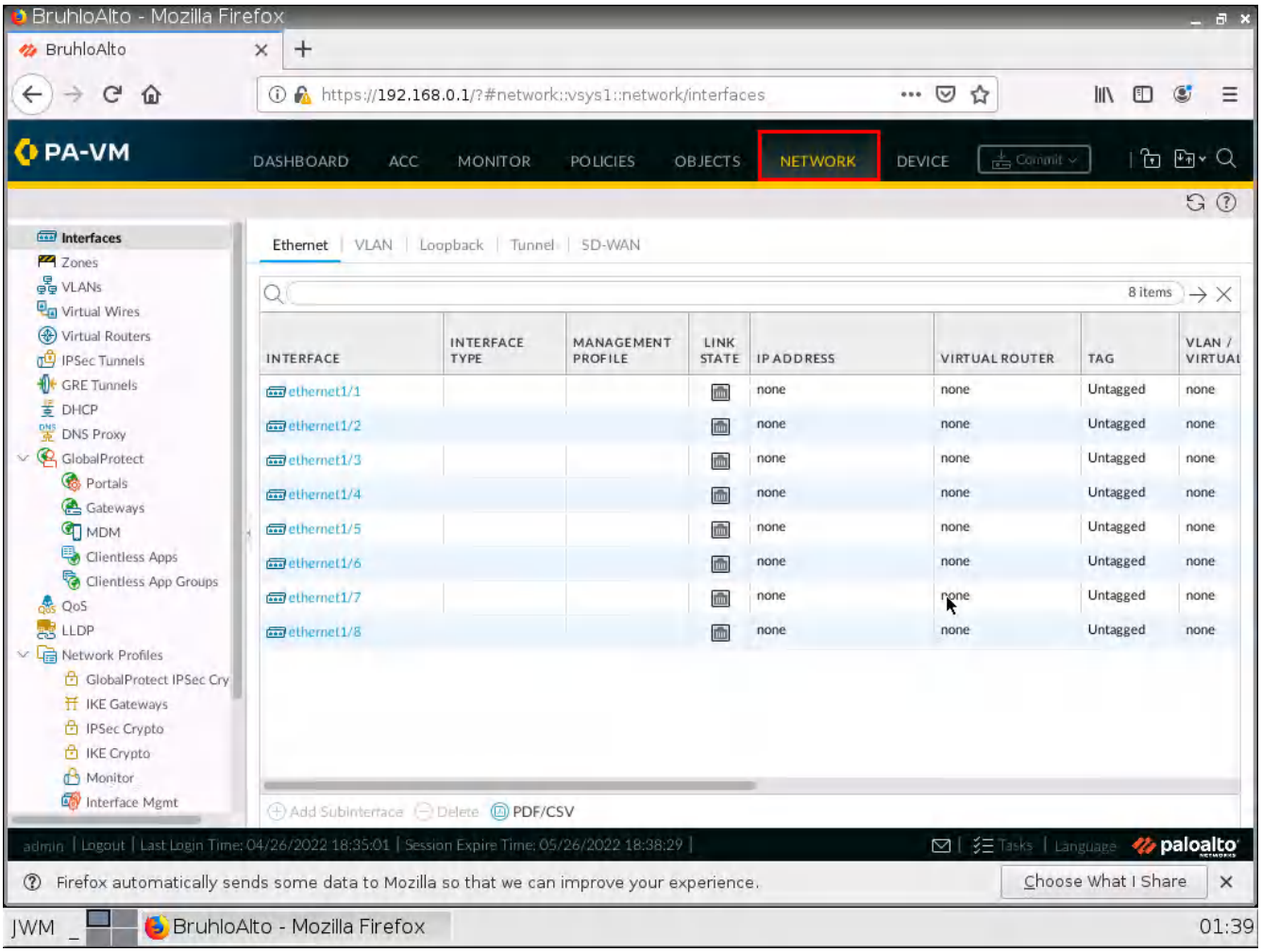


Figure 1.11: Network Interfaces Settings

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

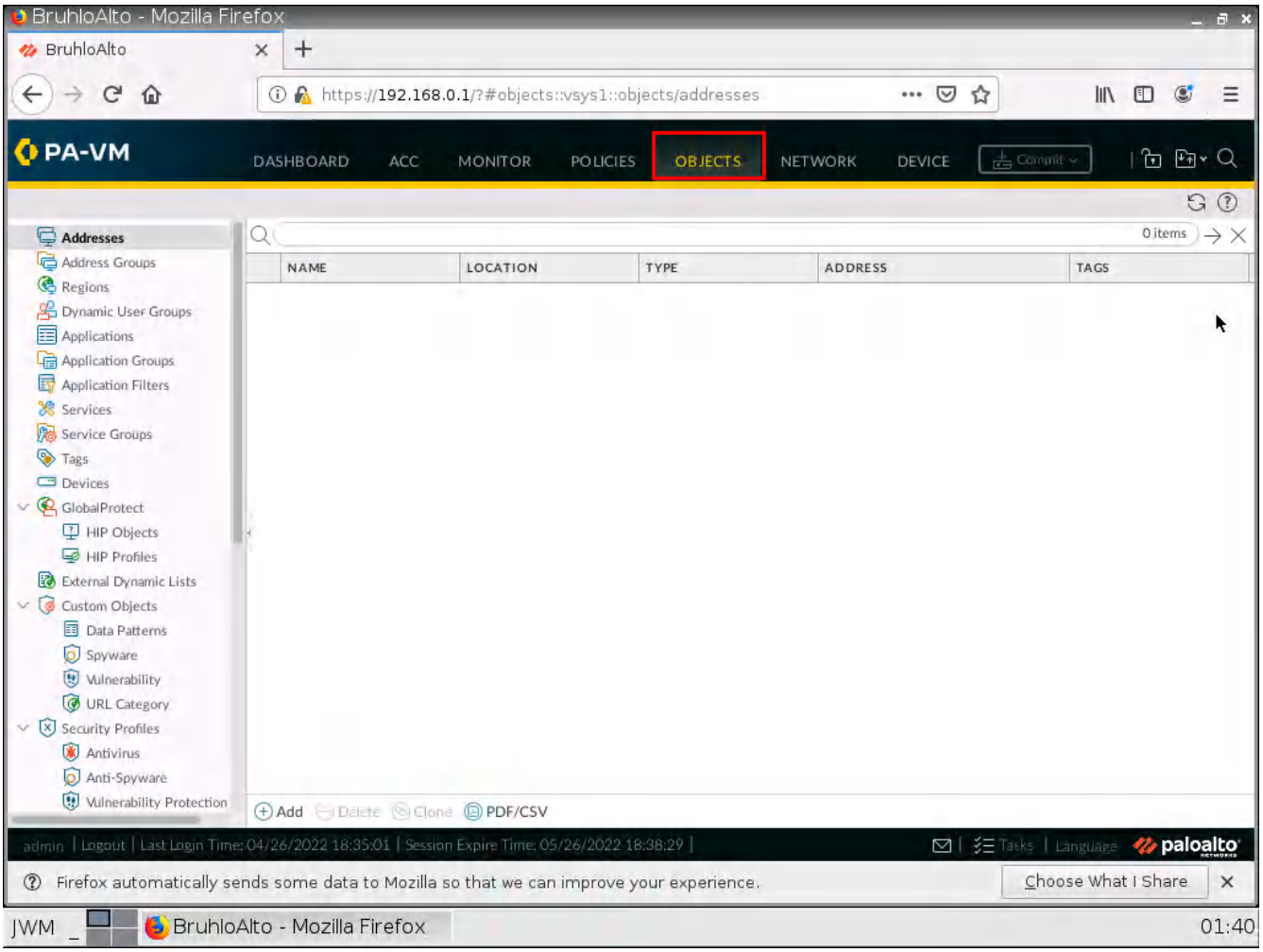


Figure 1.12: Objects Settings

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.

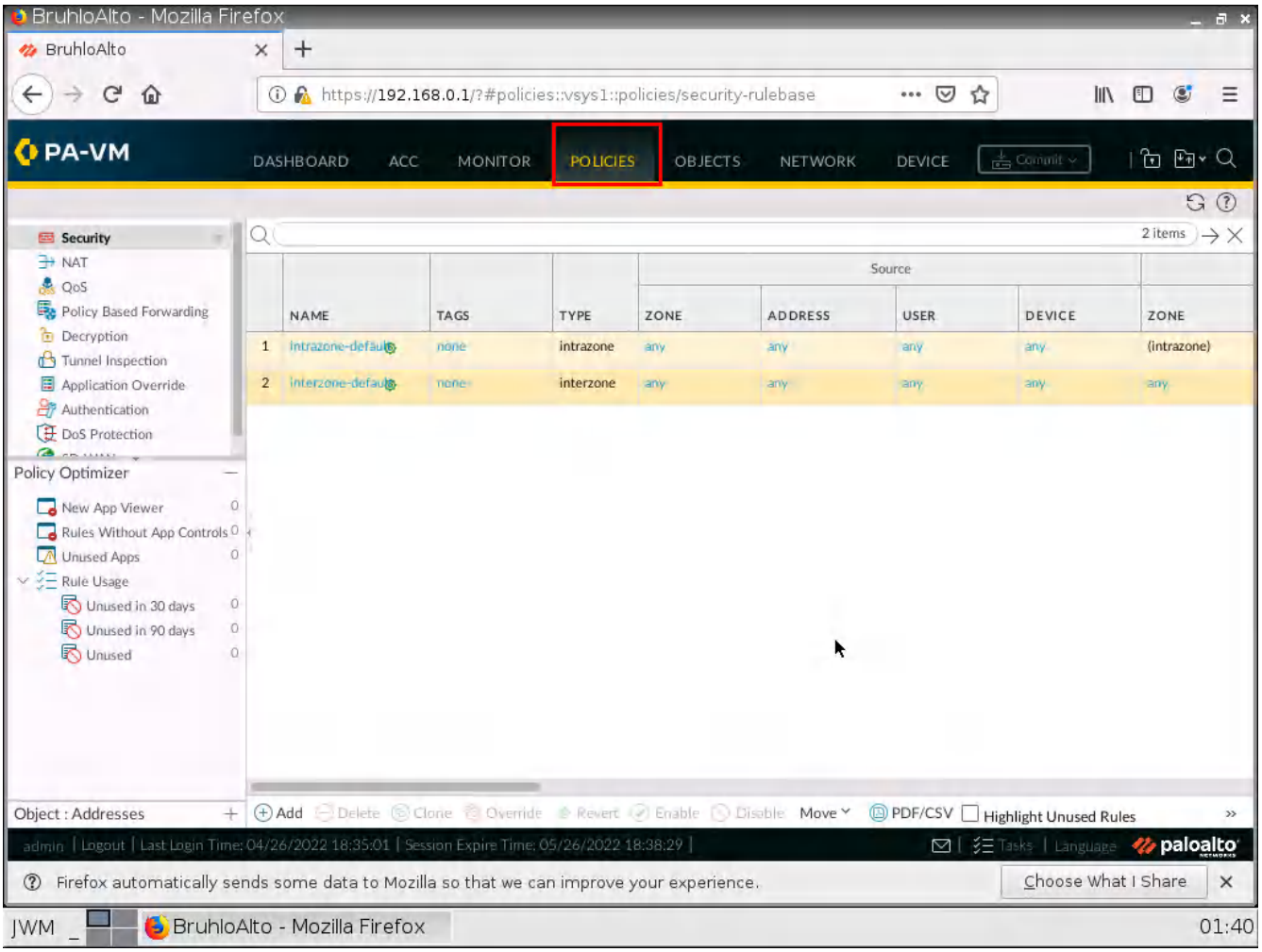


Figure 1.13: Policy Settings

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.

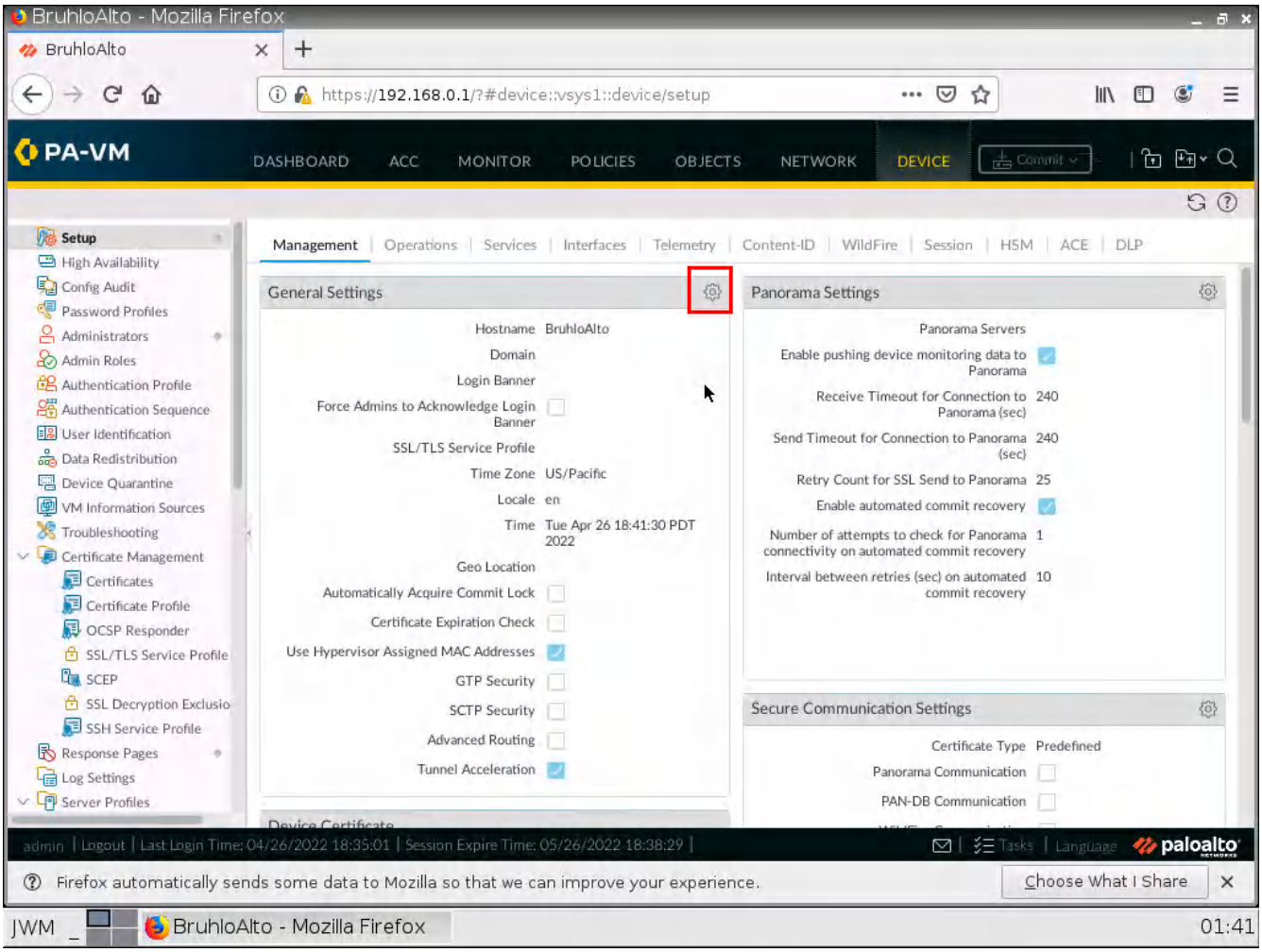


Figure 1.14: Changing hostname

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.

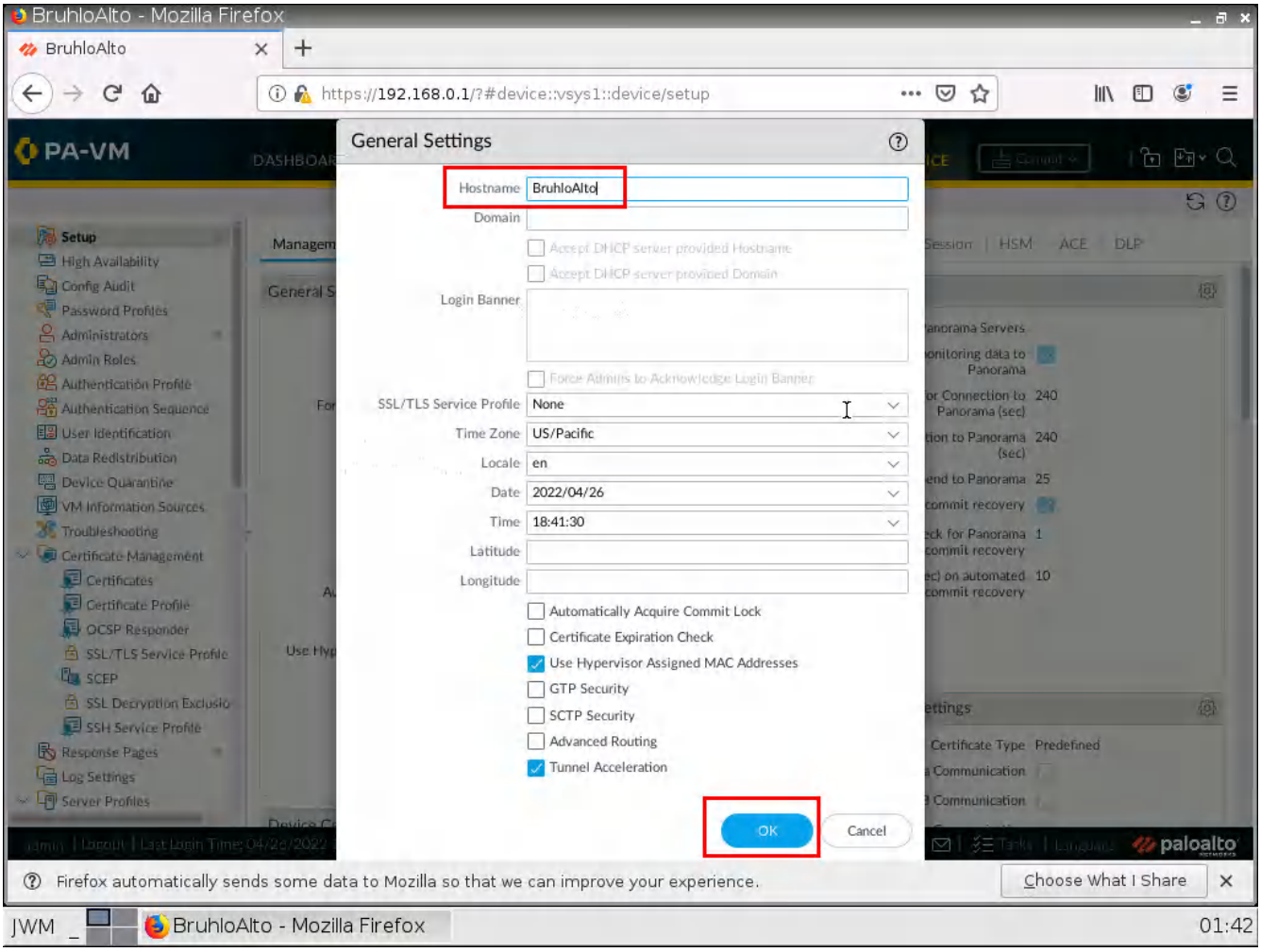


Figure 1.15: General Settings

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.

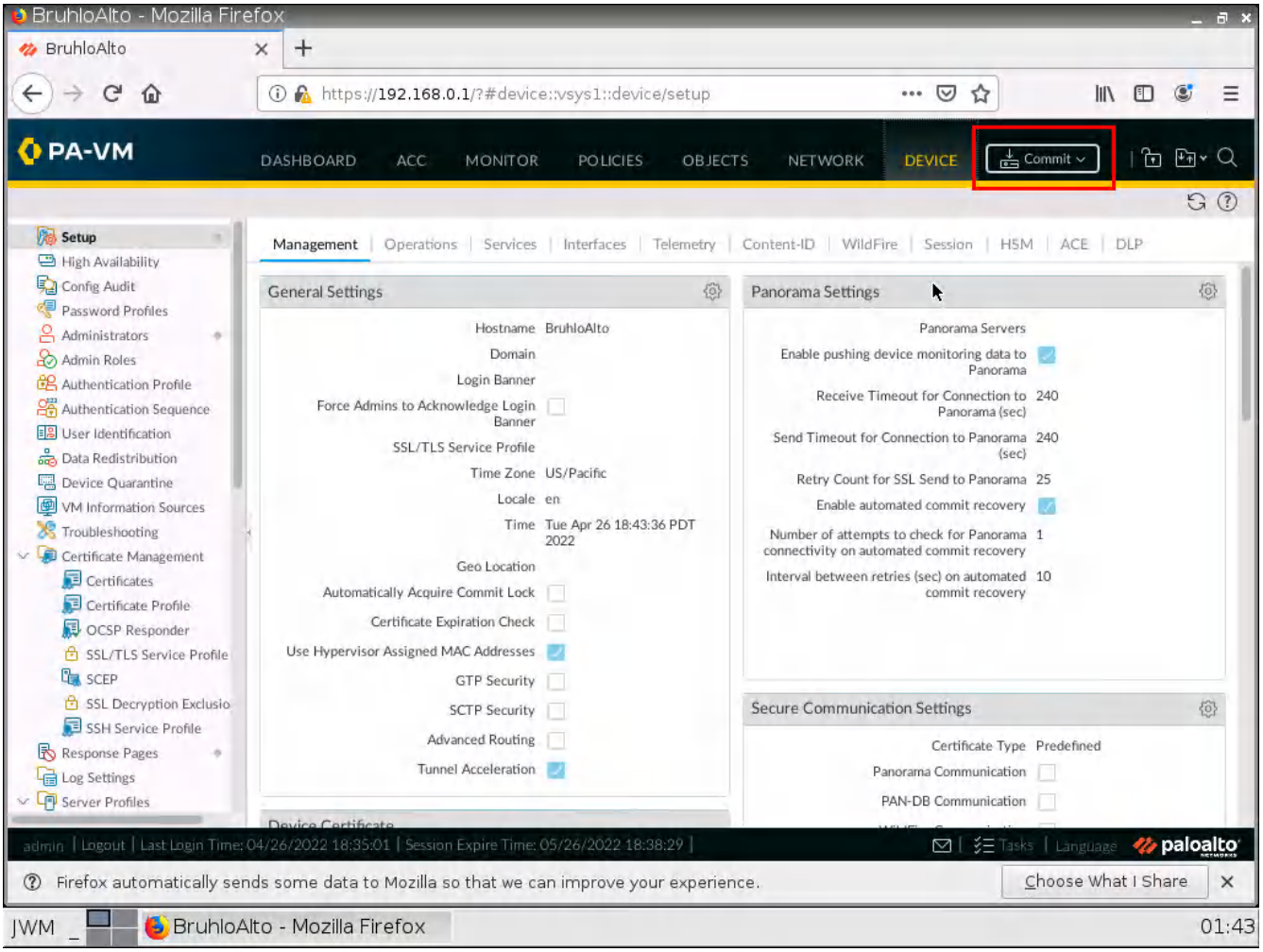


Figure 1.16: Commit Configuration

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.

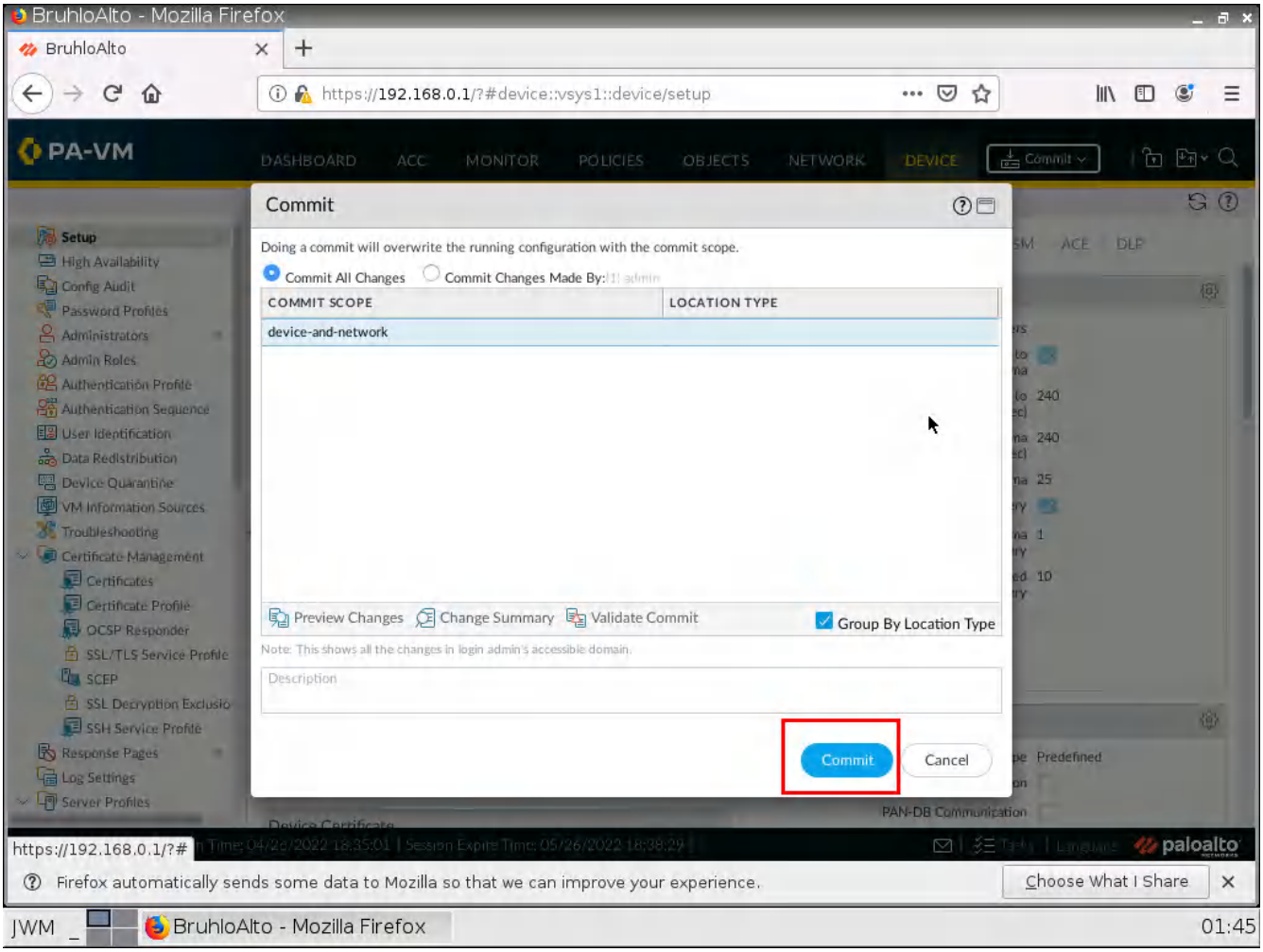


Figure 1.17: Commit all changes

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

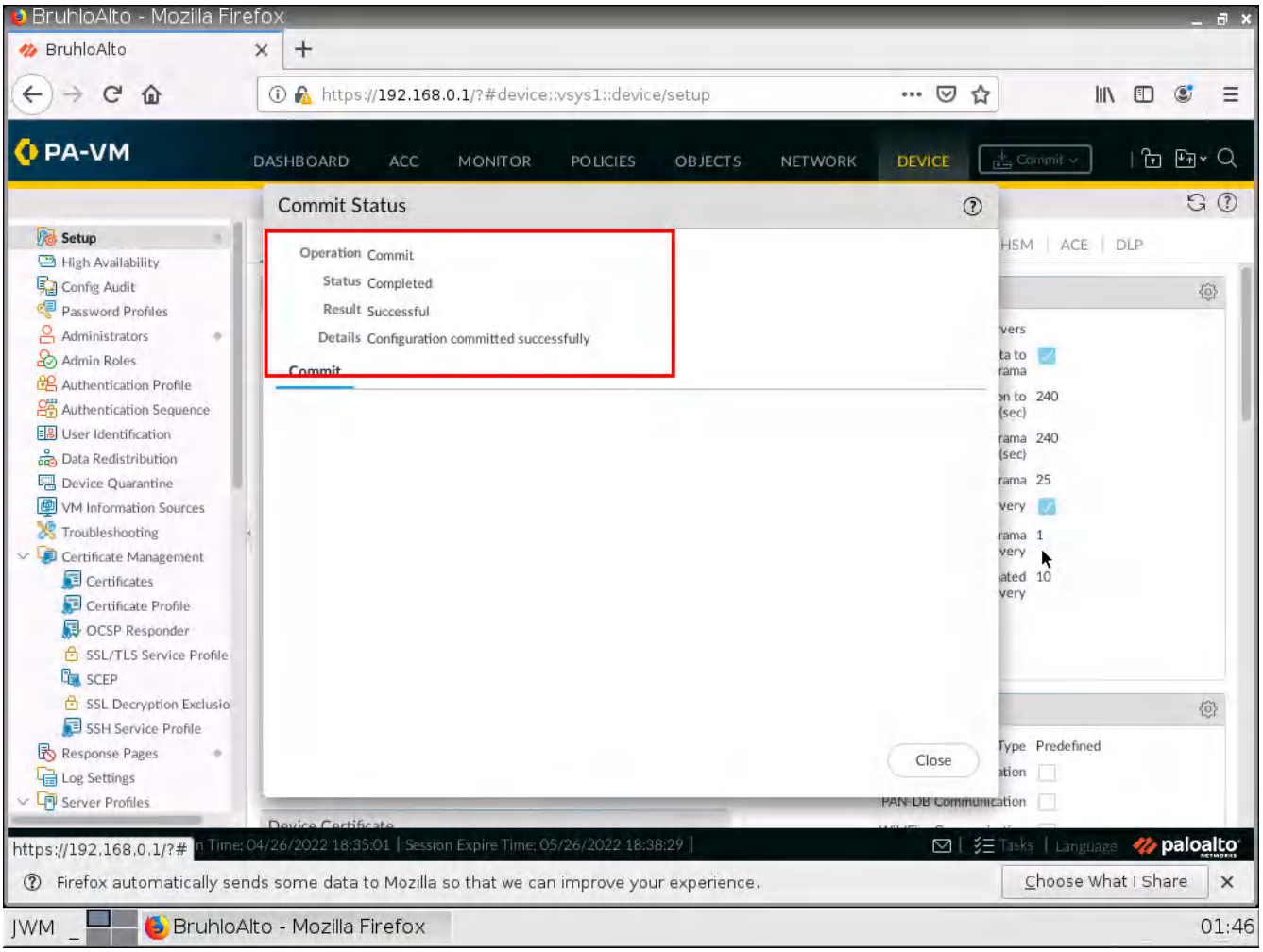


Figure 1.18: Configuration committed successfully

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.

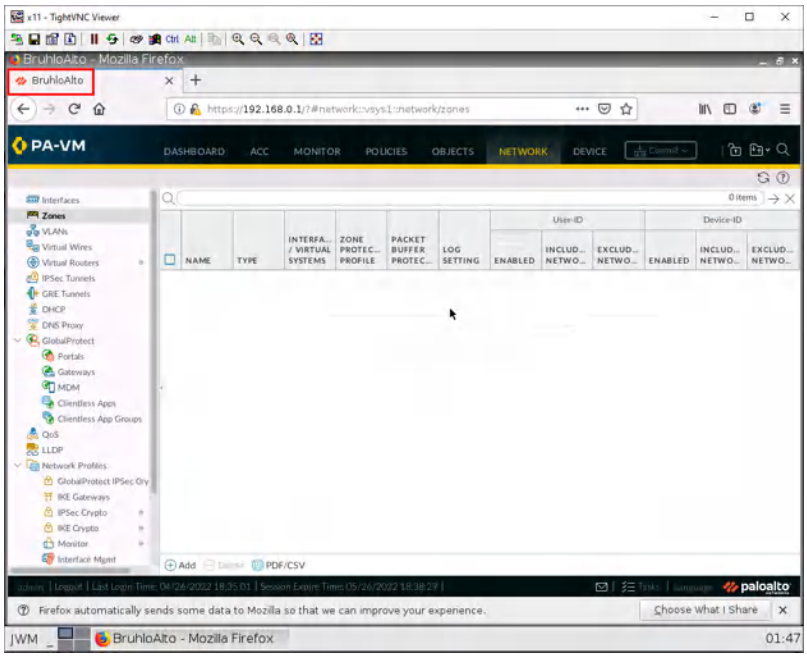


Figure 1.19: Verify configuration

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

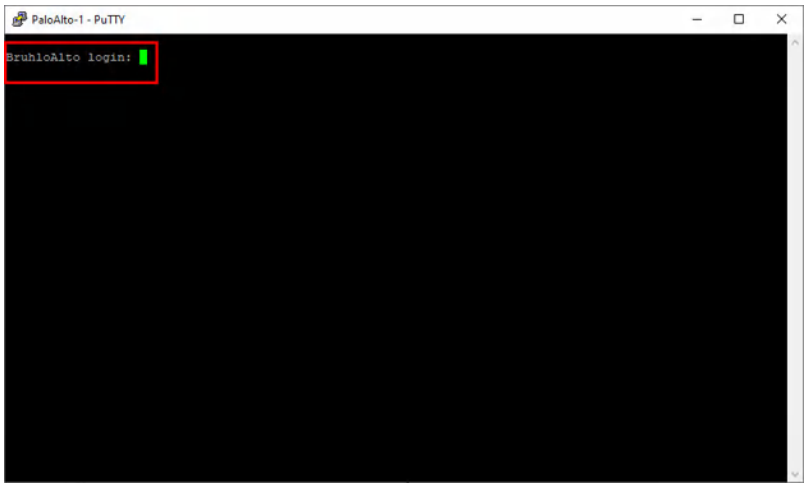


Figure 1.20: Verify configuration in CLI

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).

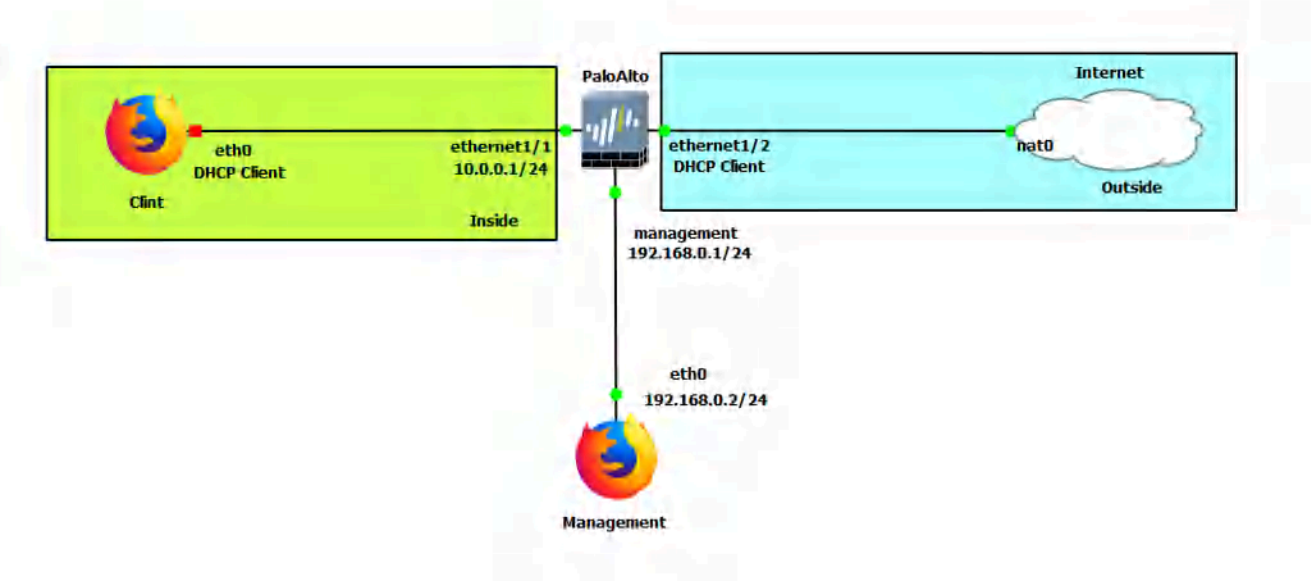


Figure 1.21: main scenario

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.

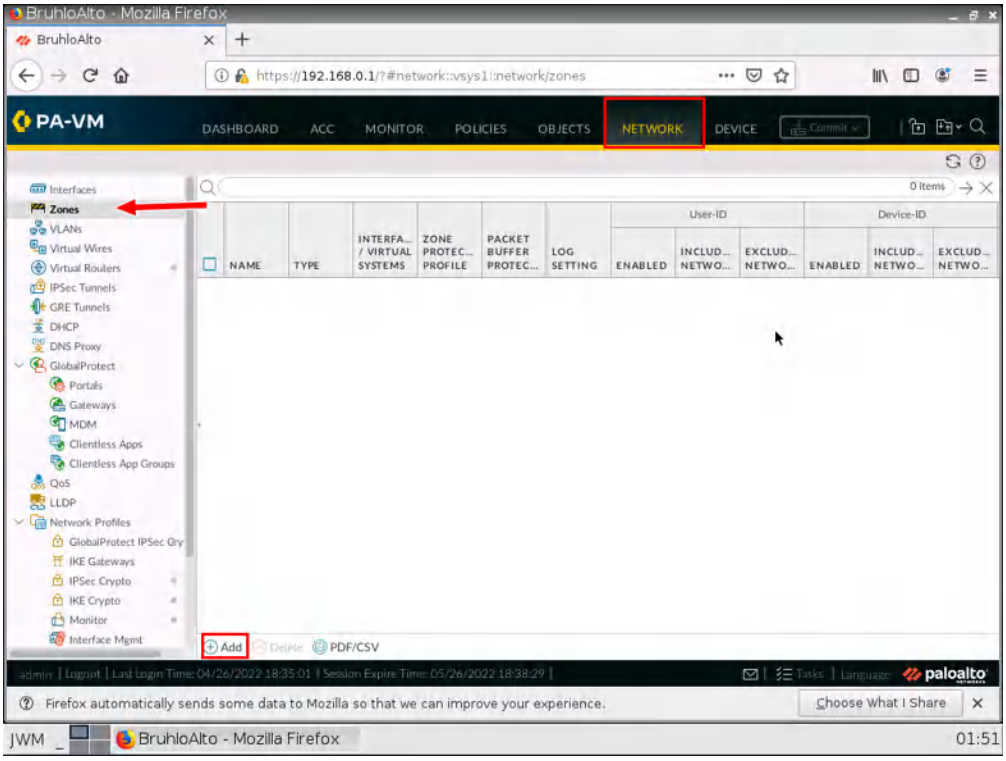


Figure 1.22: Creating zones

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!)

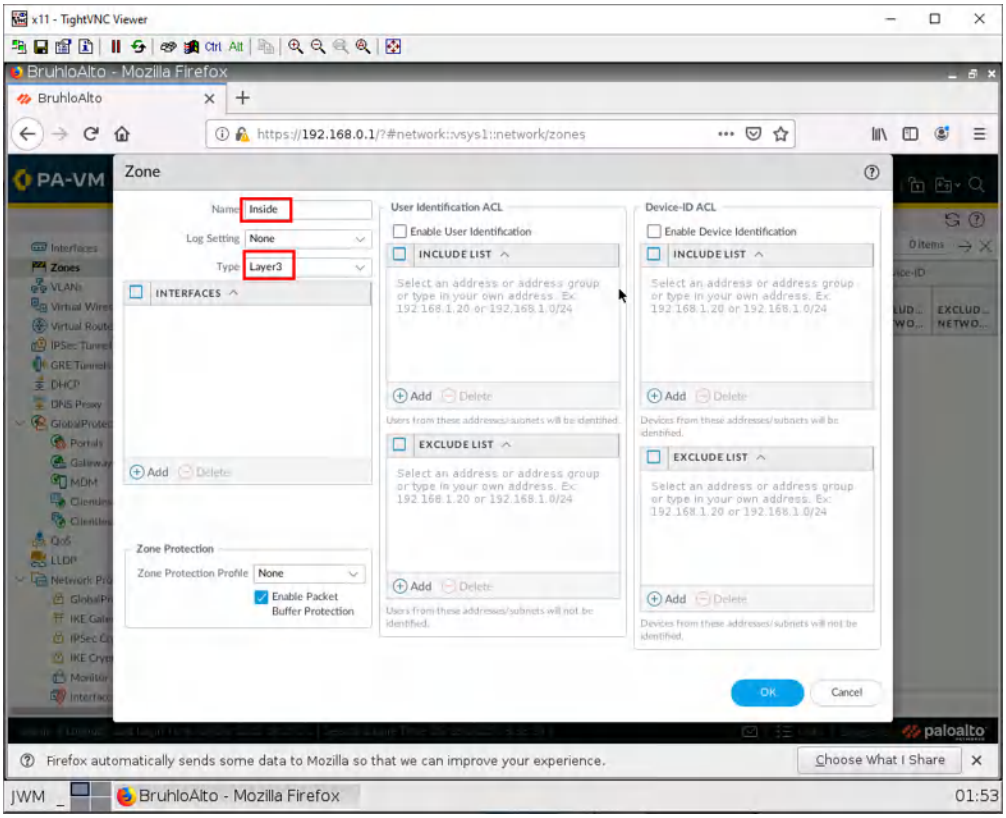


Figure 1.23: Create a zone Inside as a layer3

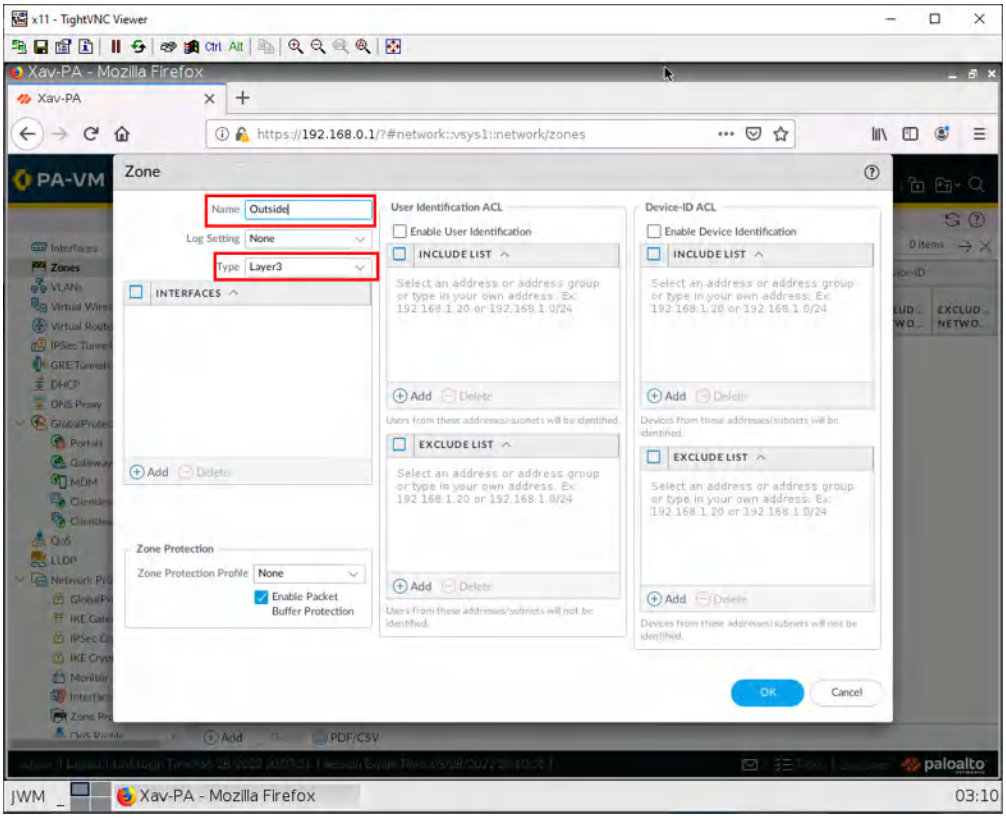


Figure 1.24: Create a zone Outside as a layer3

Set Up a Static Interface IP Address in Palo Alto

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

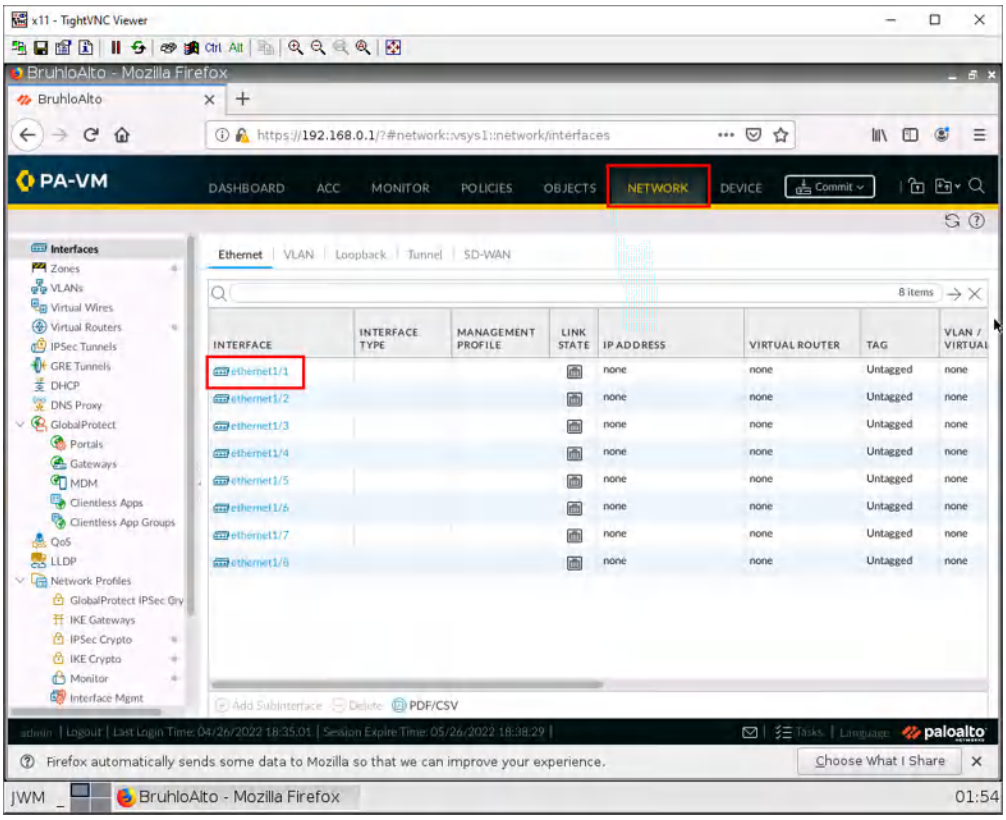


Figure 1.25: Select Ethernet 1/1

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.

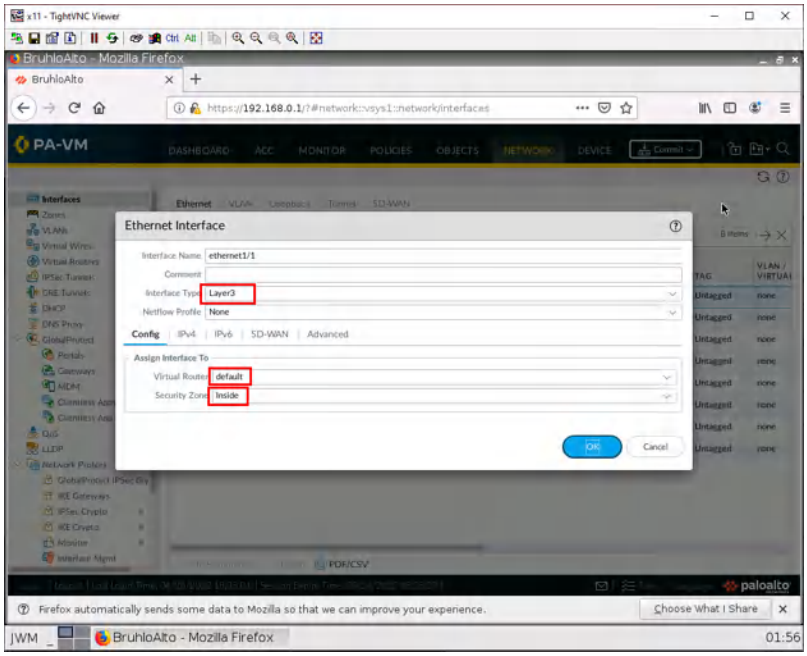


Figure 1.26: Ethernet 1/1 Configuration

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

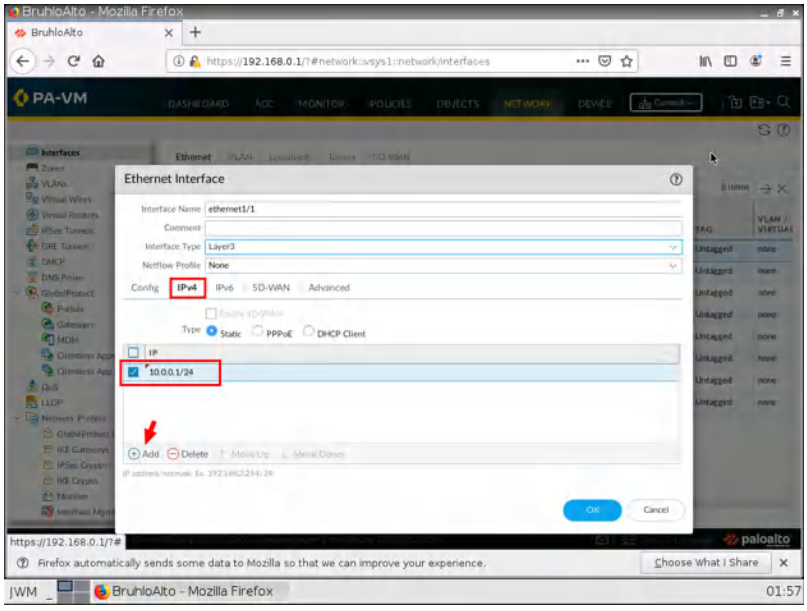


Figure 1.27: Set an IP address for Ethernet 1/1

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**.

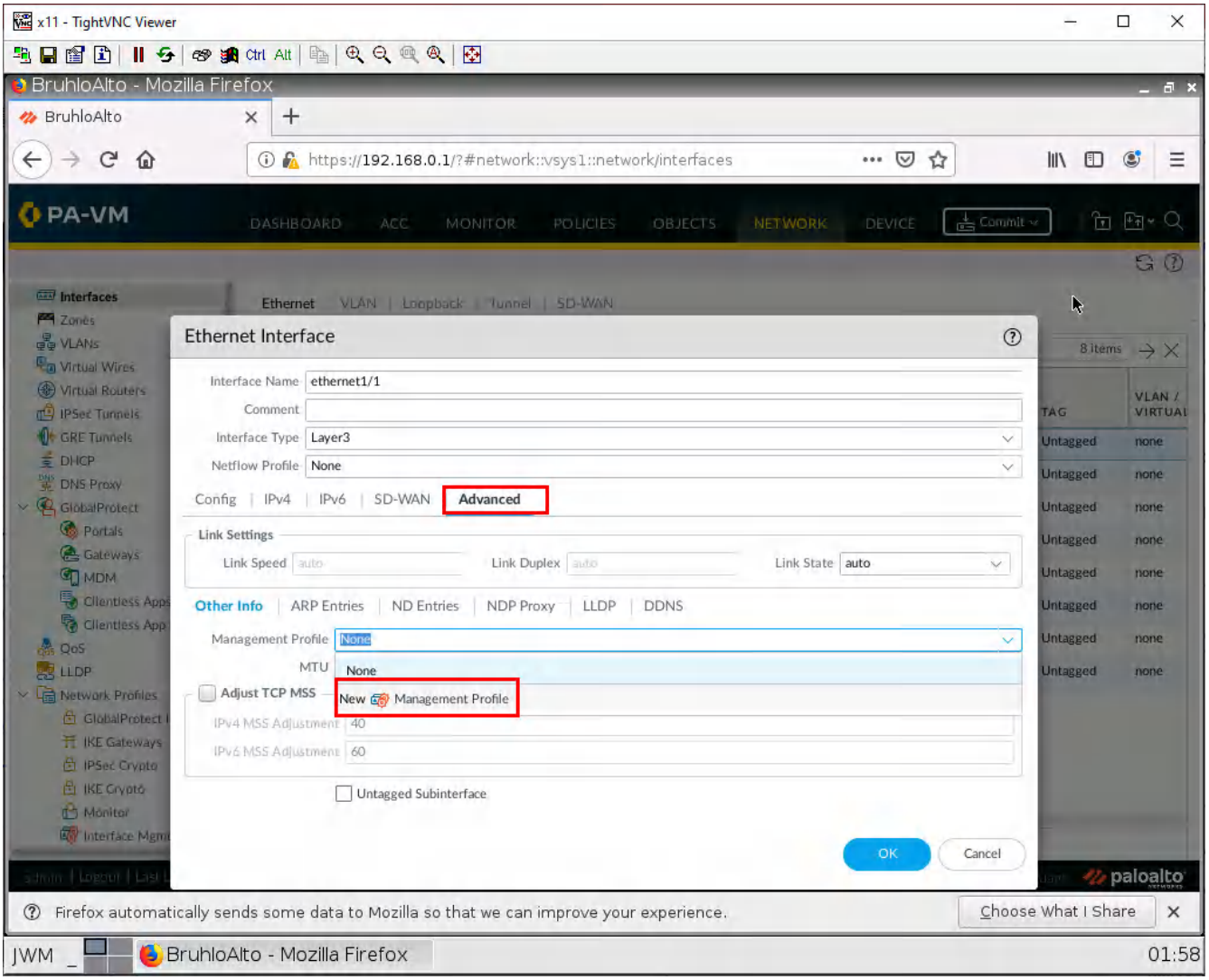


Figure 1.28: Ethernet 1/1 configuration – Advanced Tab

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

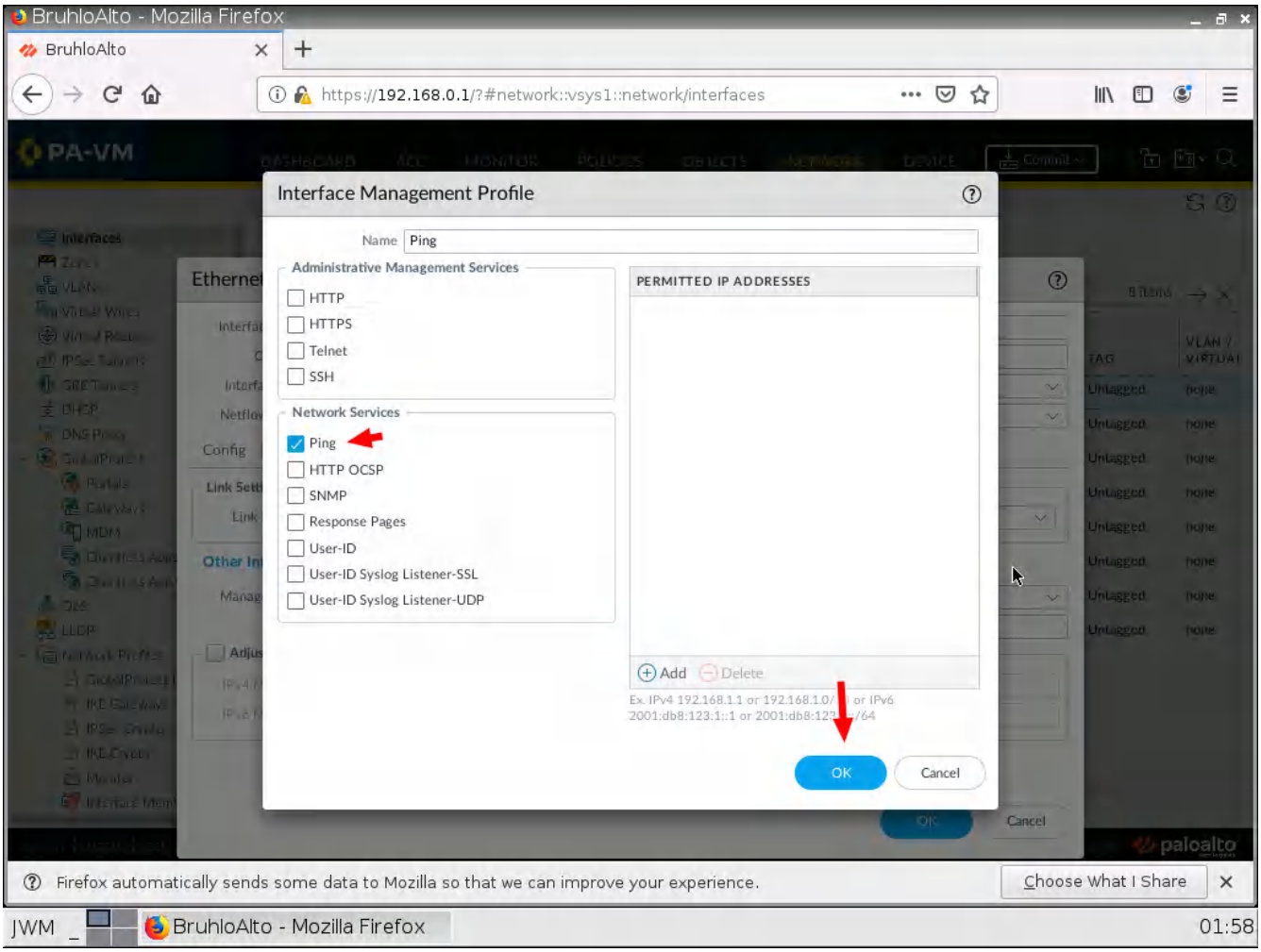


Figure 1.29: Enable Ping under Interface Management Profile

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.

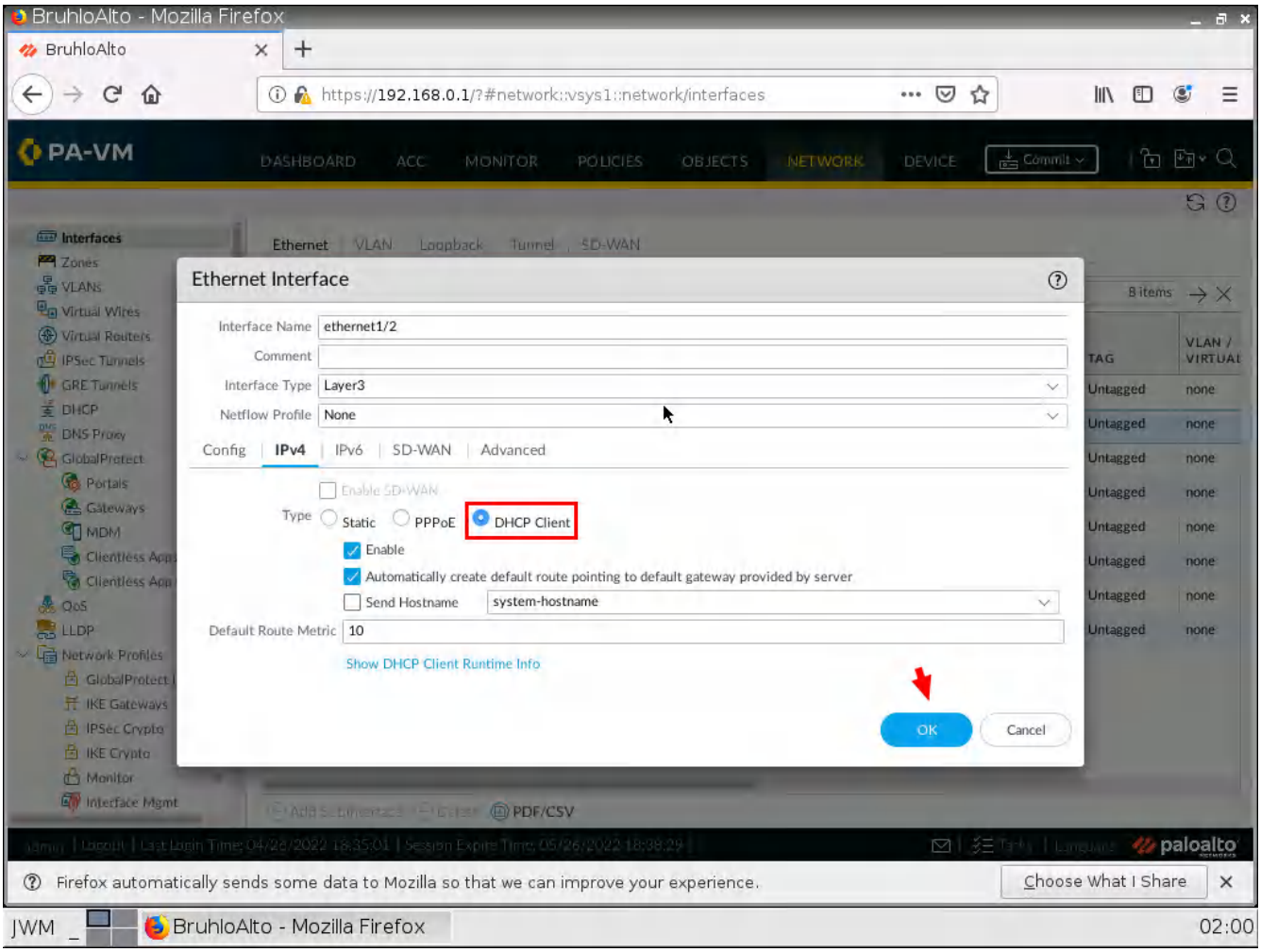


Figure 1.30: Enable DHCP Client on Ethernet 1/2

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.

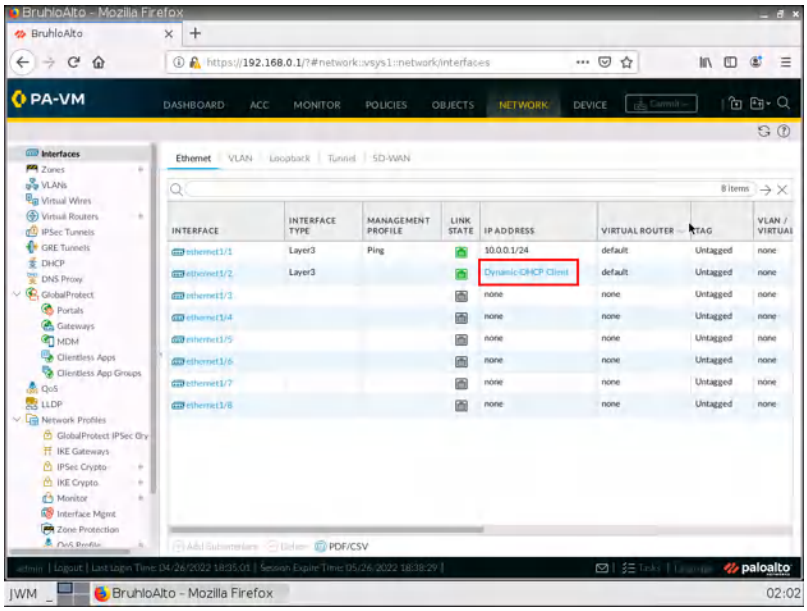


Figure 1.31: Dynamic DHCP Client- Receive an IP address from DHCP Server

Here is an example of that:

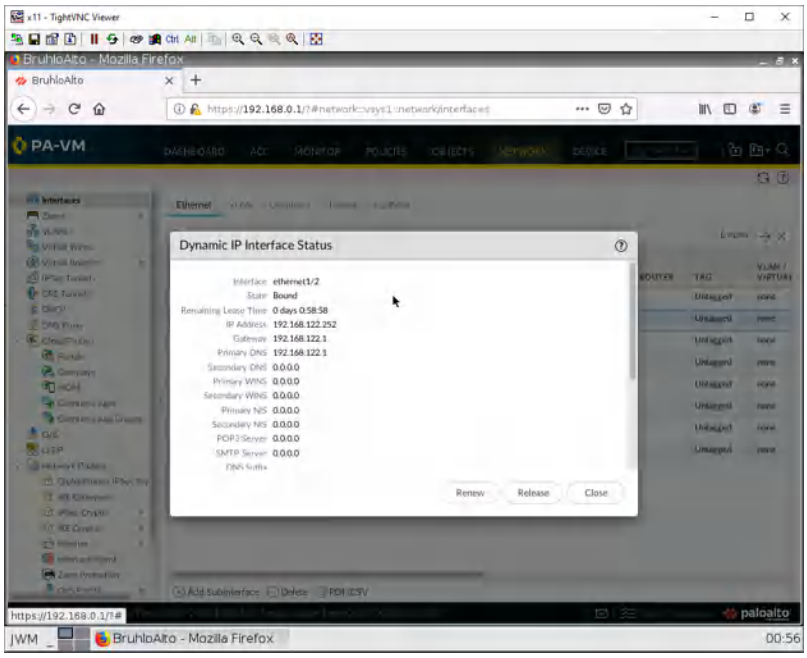


Figure 1.32: IP Address of Interface 1/2

Set Up a DHCP Server in Palo Alto

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

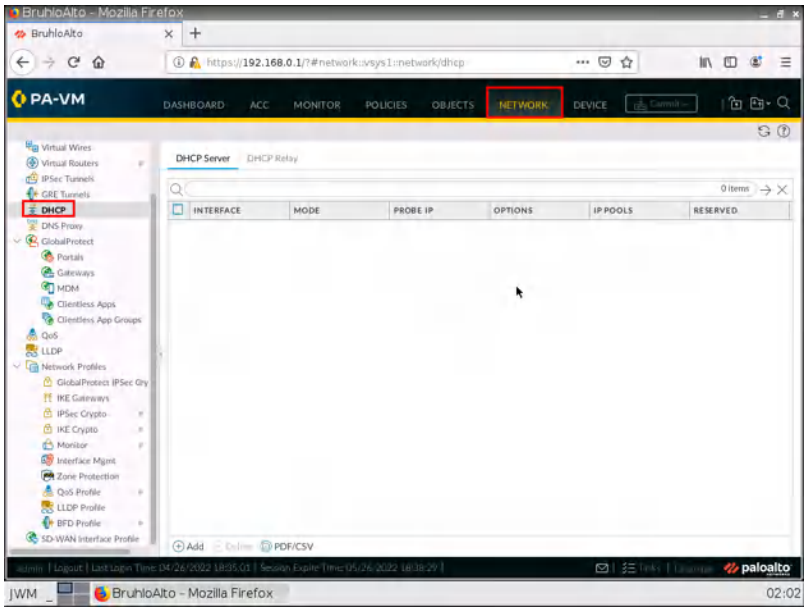


Figure 1.33: Add a DHCP Server

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.

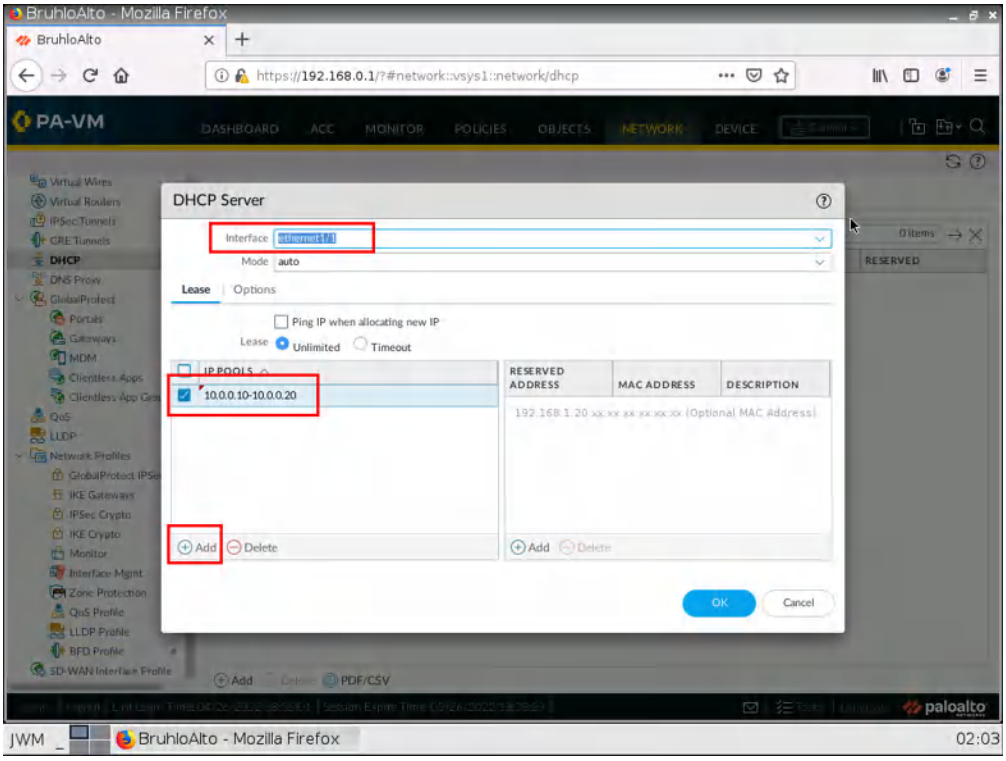


Figure 1.34: Set an IP Pools for Interface 1/1

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.

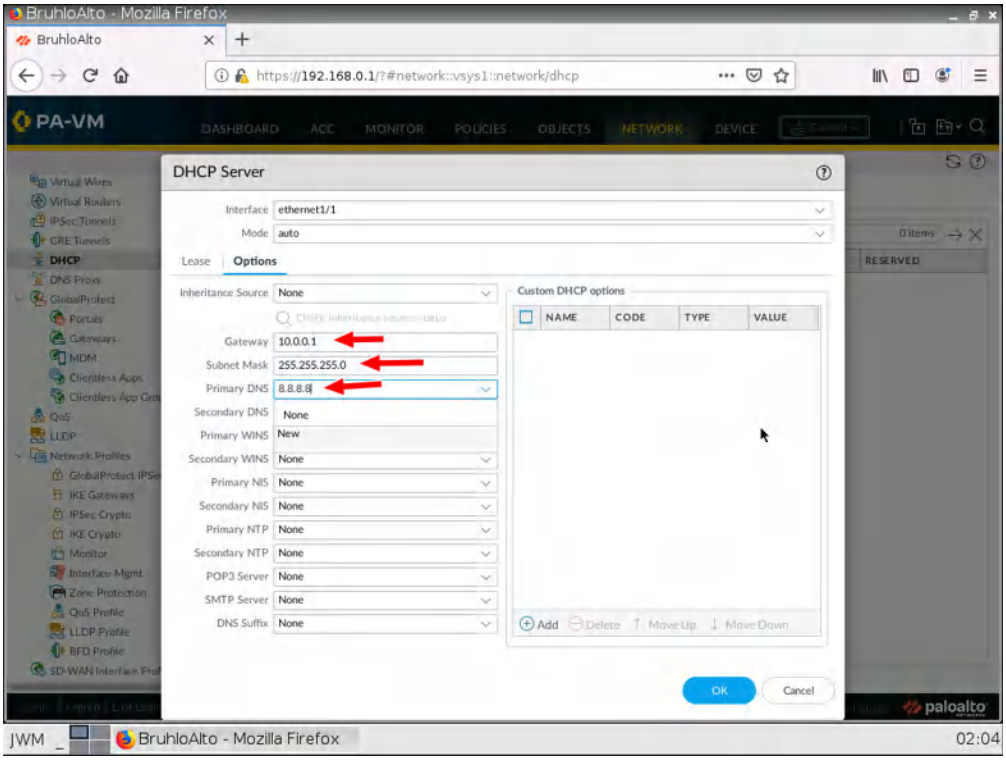


Figure 1.35: Set a Gateway and a primary DNS

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.

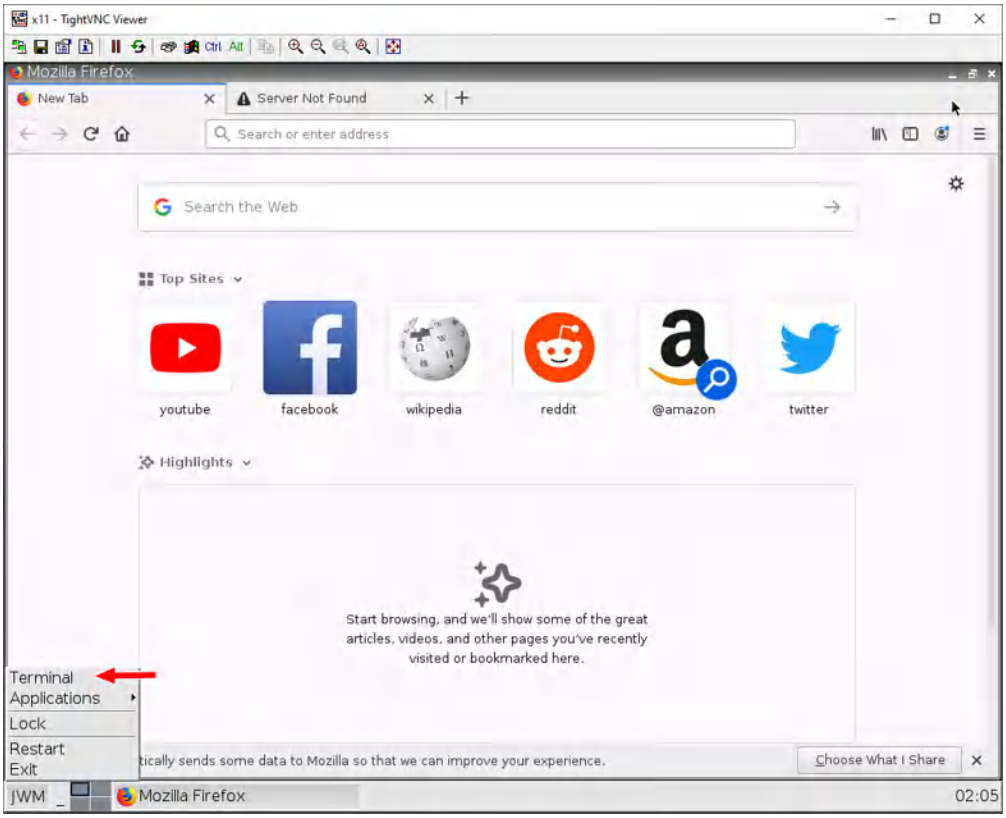


Figure 1.36: Open Terminal in WebTerm1

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

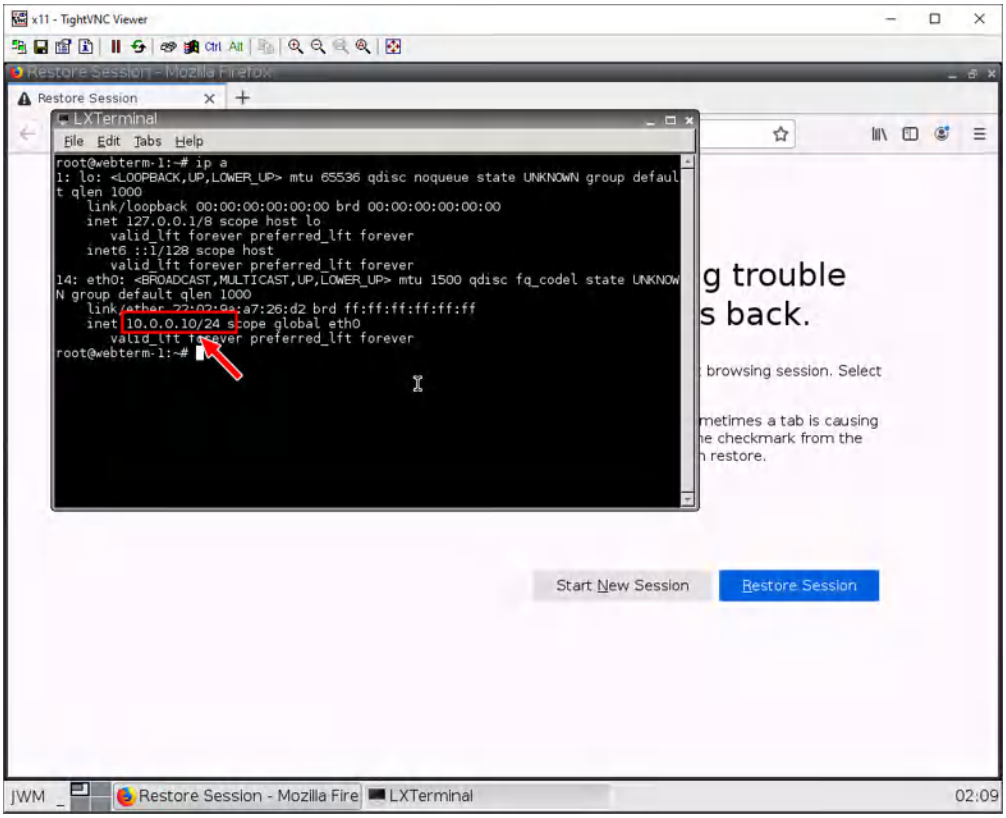


Figure 1.37: Check the IP address in Terminal

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

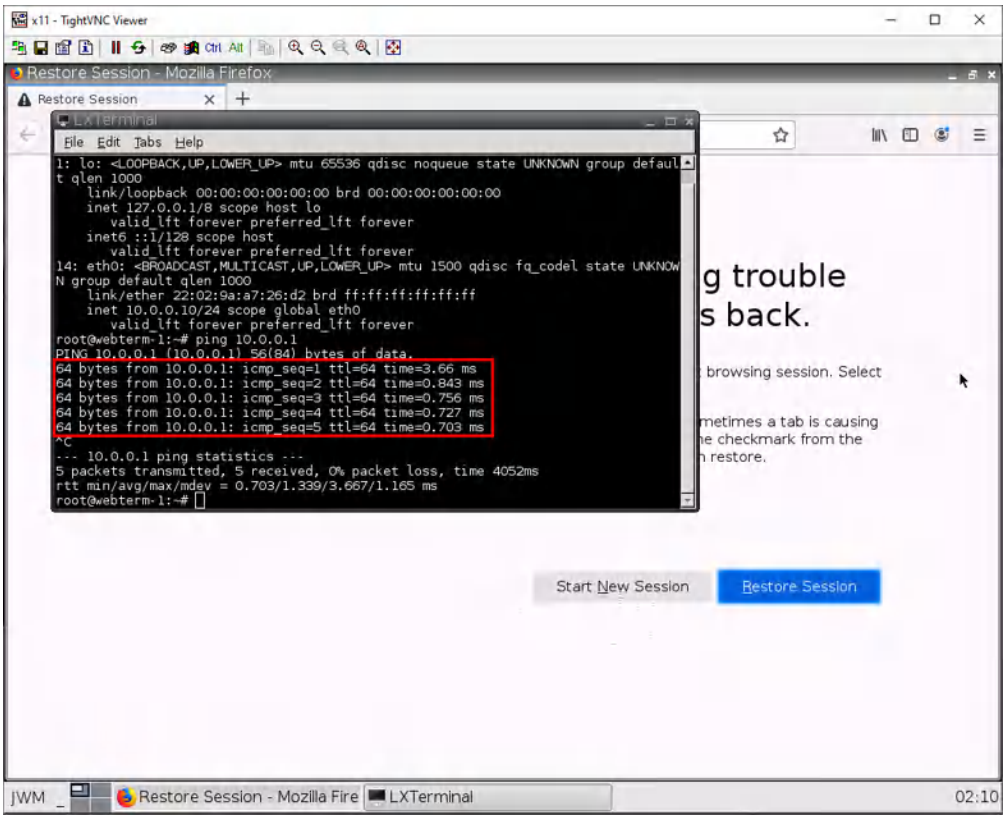


Figure 1.38: Ping 10.0.0.1 in the terminal

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.

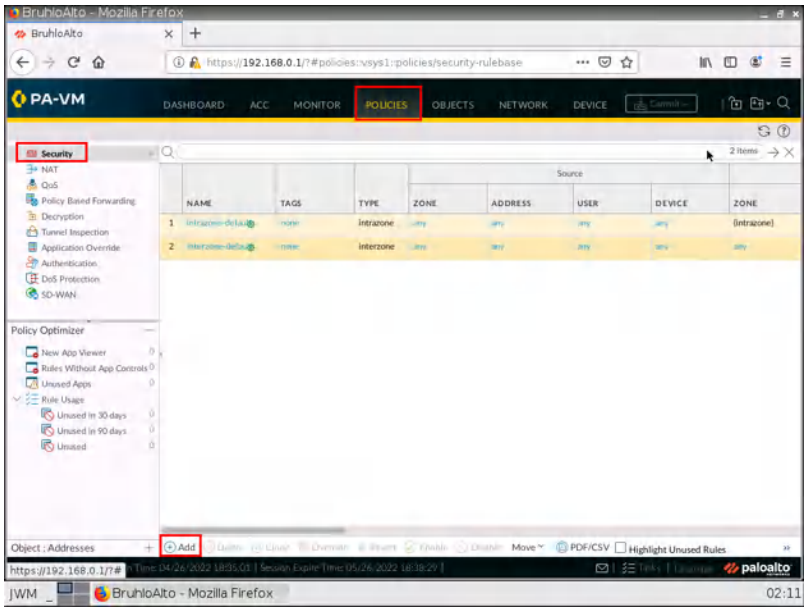


Figure 1.39: Add a Security Policy

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

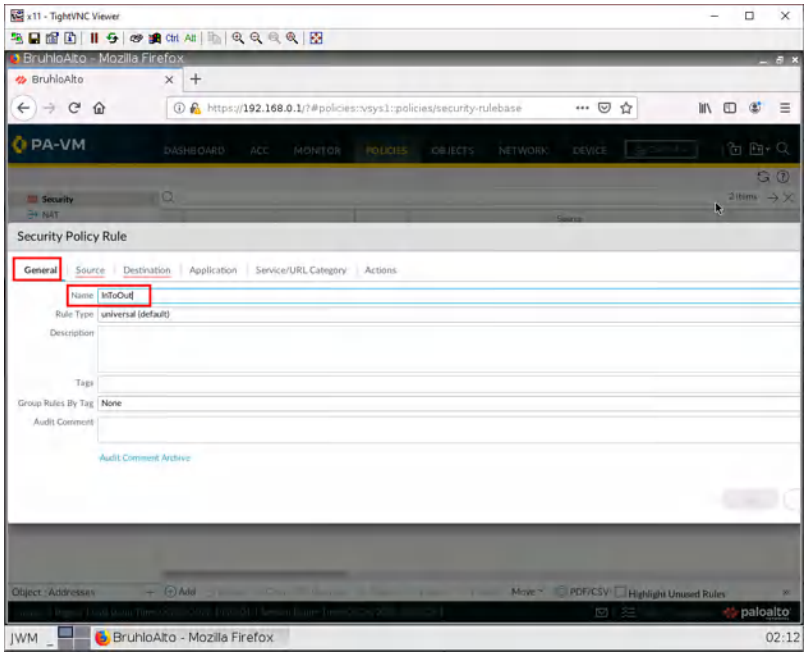


Figure 1.40: Set a Name for Security Policy

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

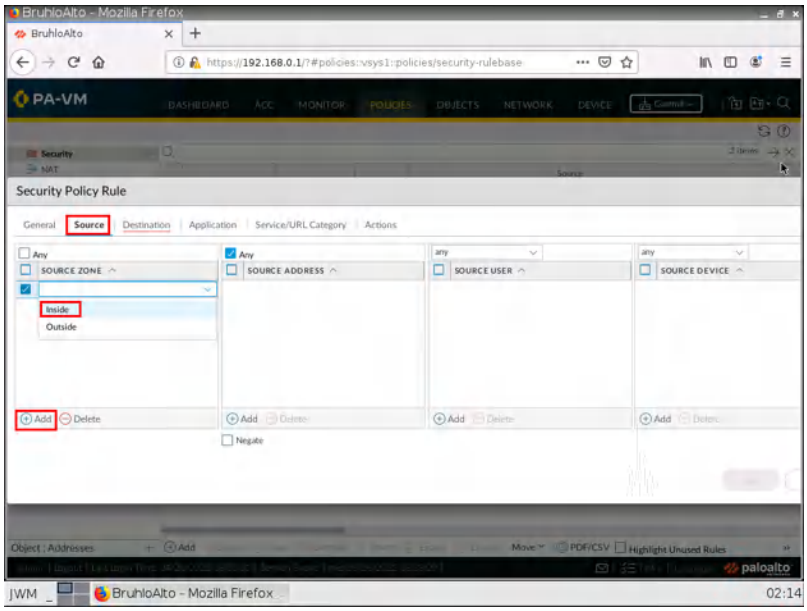


Figure 1.41: Set a Source Zone for Security Policy

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

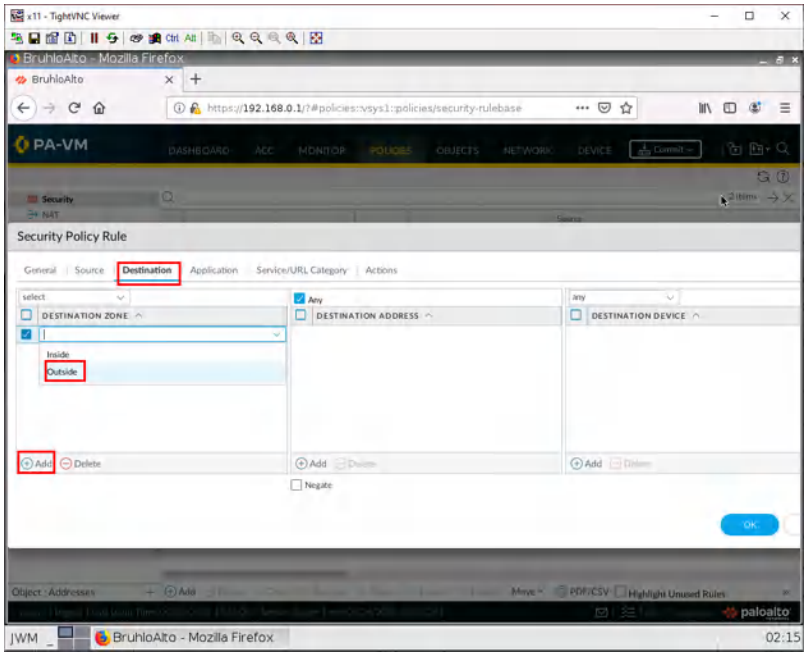


Figure 1.42: Set a Destination Zone for Security Policy

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**.

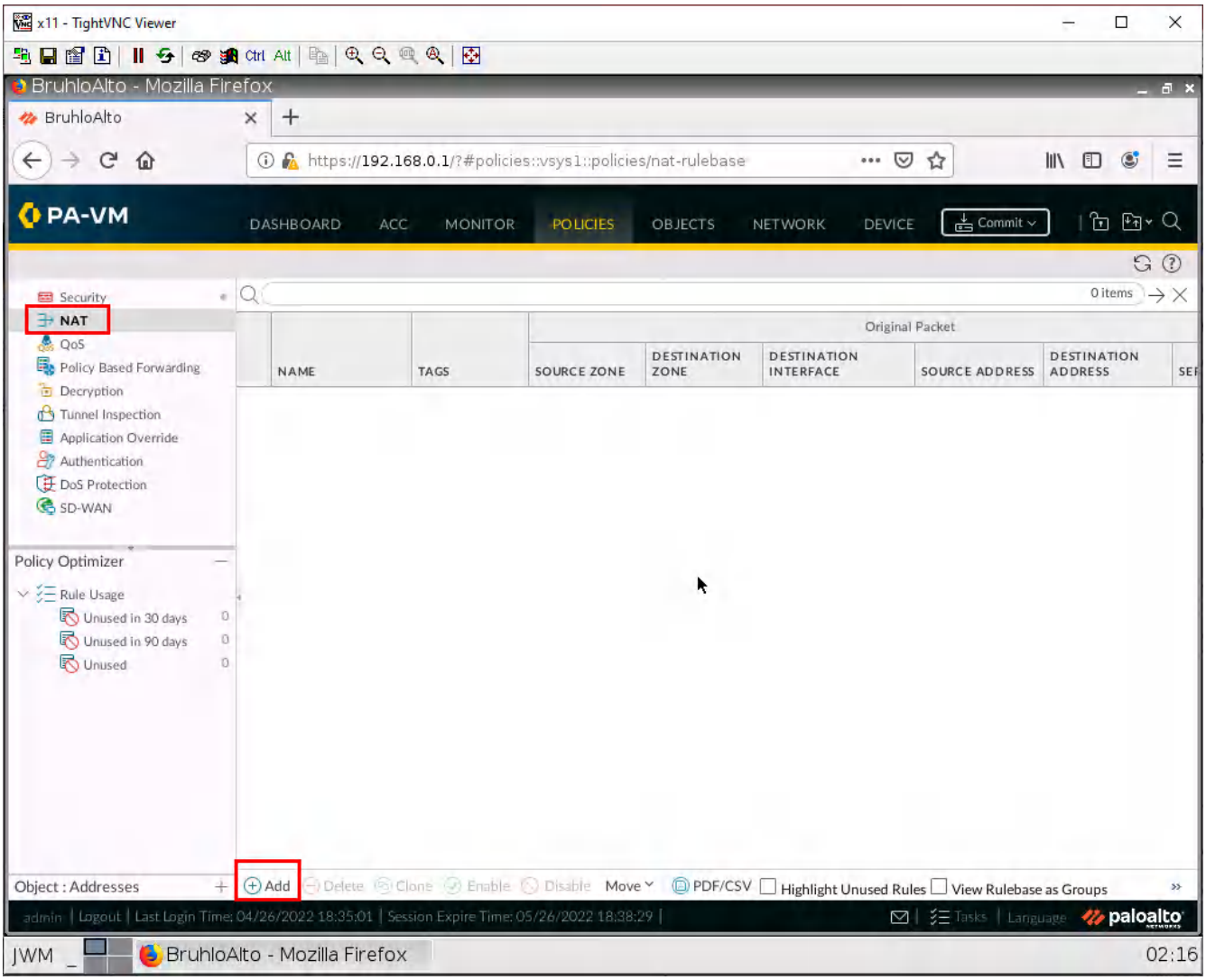


Figure 1.43: Set a NAT

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

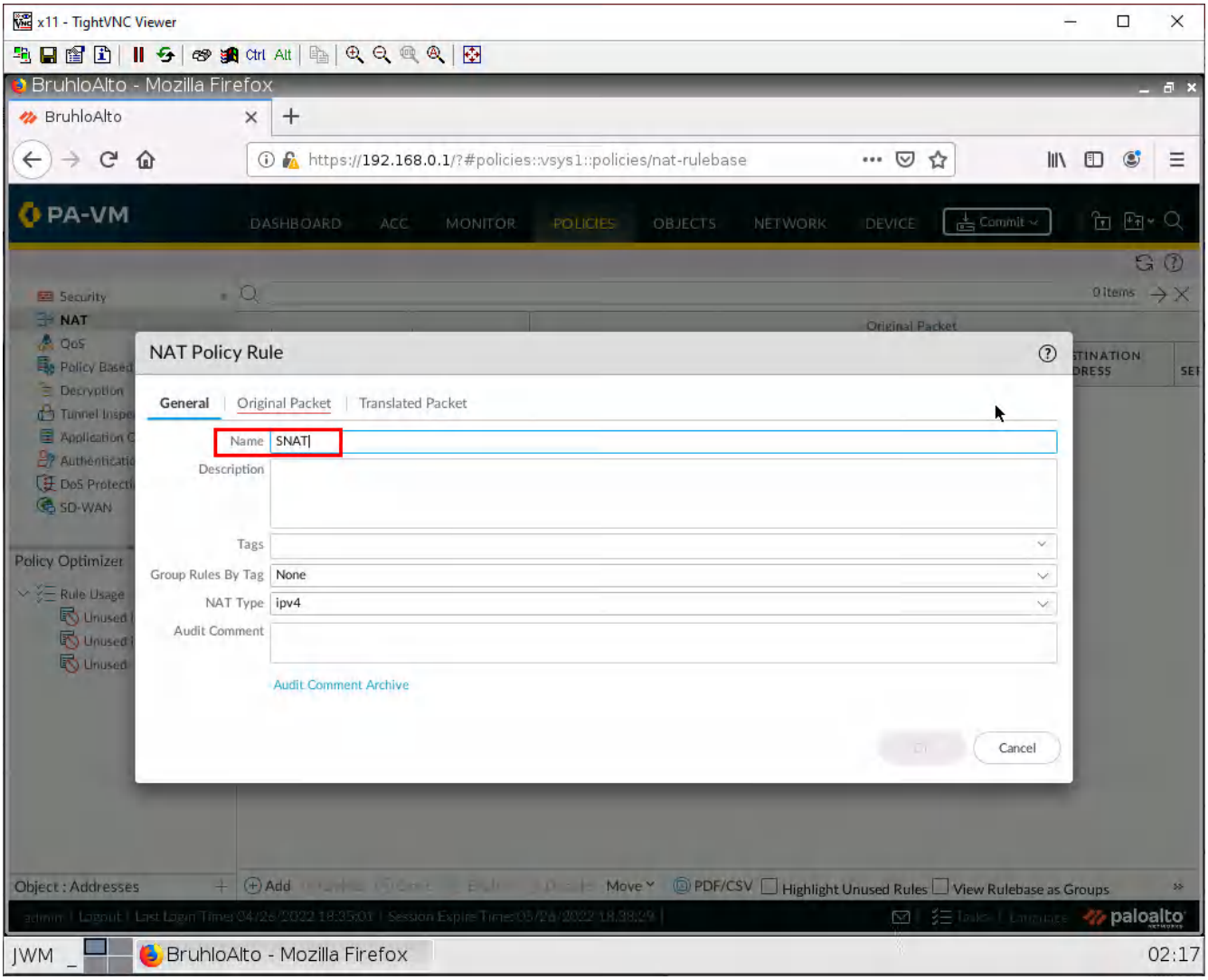


Figure 1.44: Set a Name for NAT

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

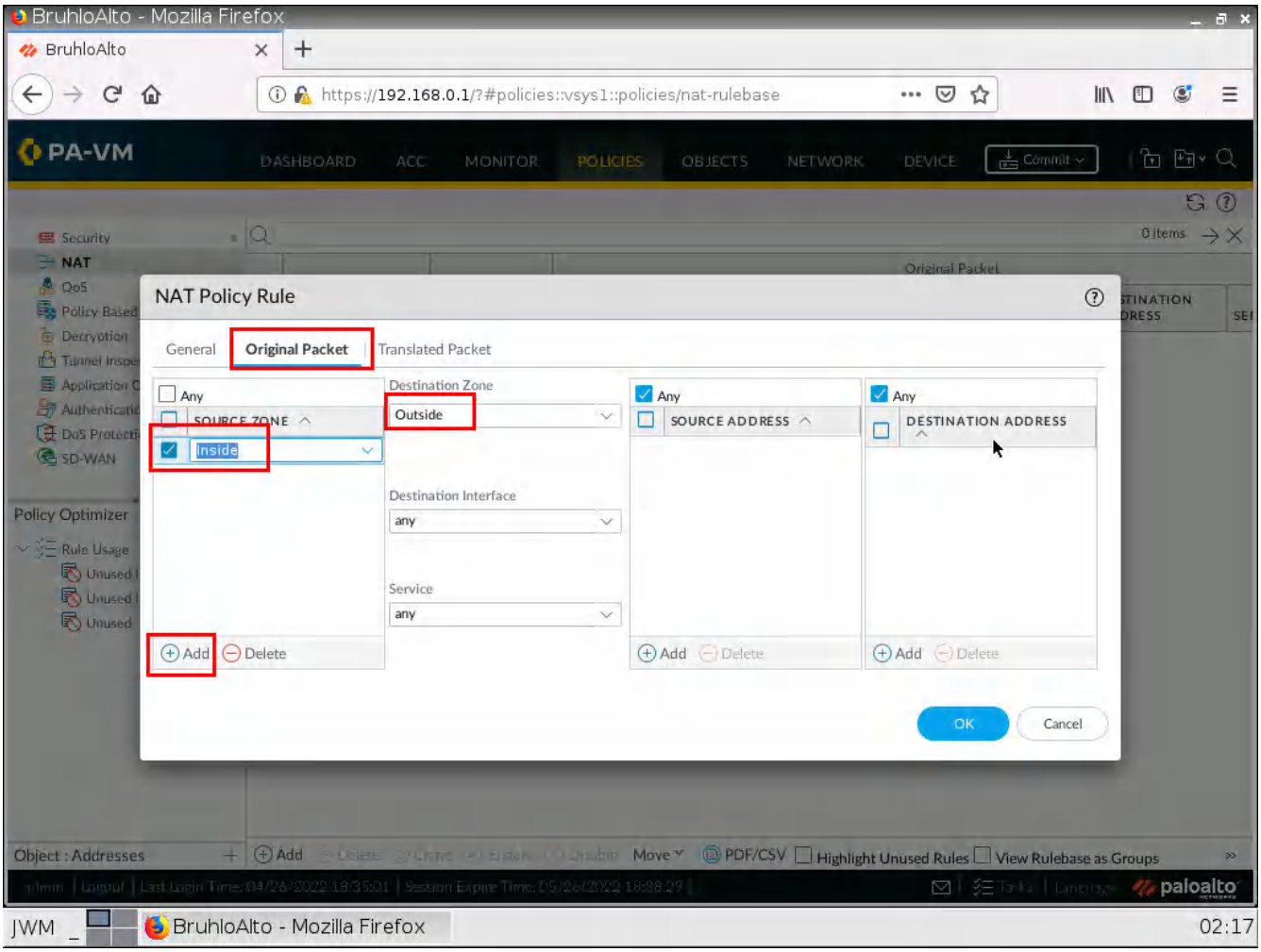


Figure 1.45: Set a Source Zone and Destination Zone for NAT

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

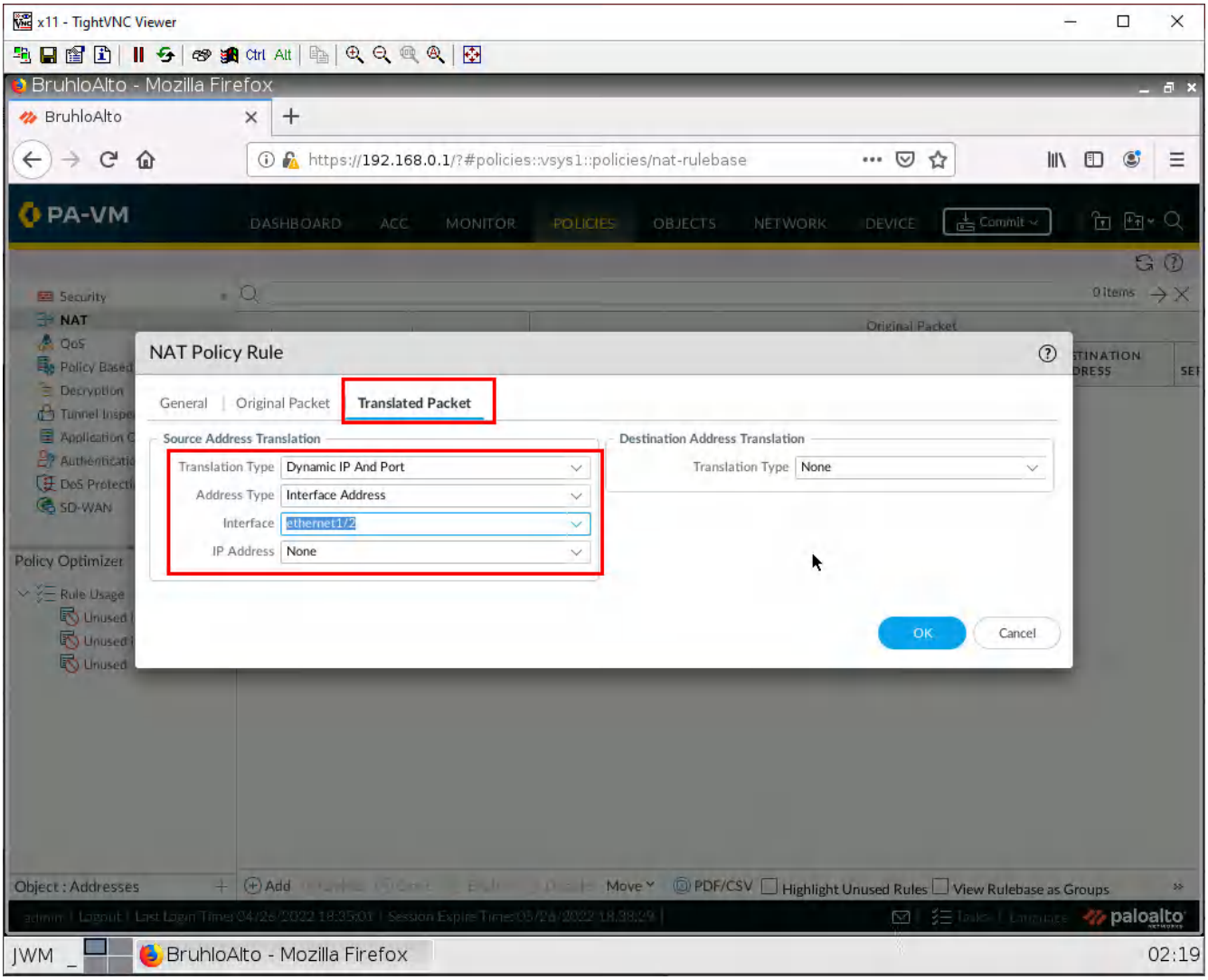


Figure 1.46: Set a Translated Packet

Don’t forget to commit!

Check Internet Connectivity on Webterm

In webterm, you could test pinging 8.8.8.8 like so:

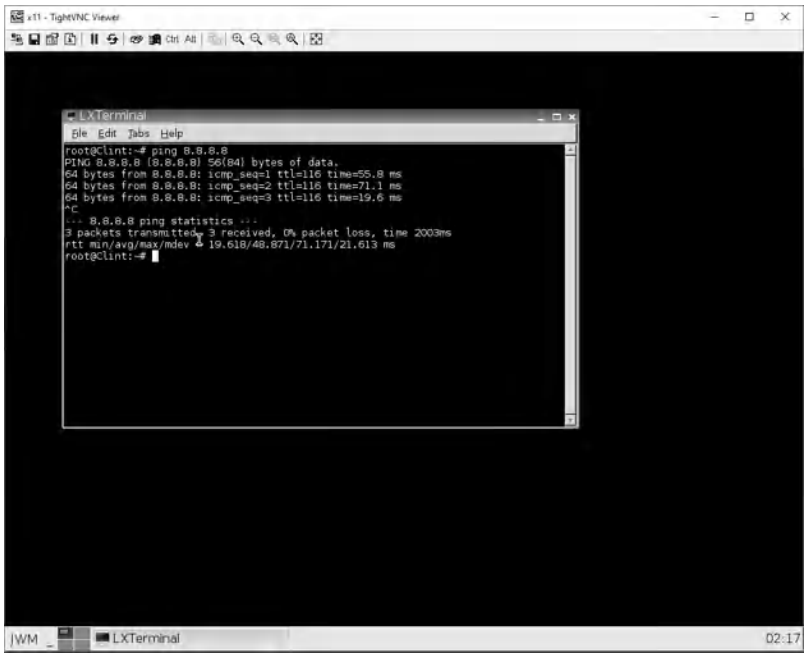


Figure 1.47: Verify your configuration

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

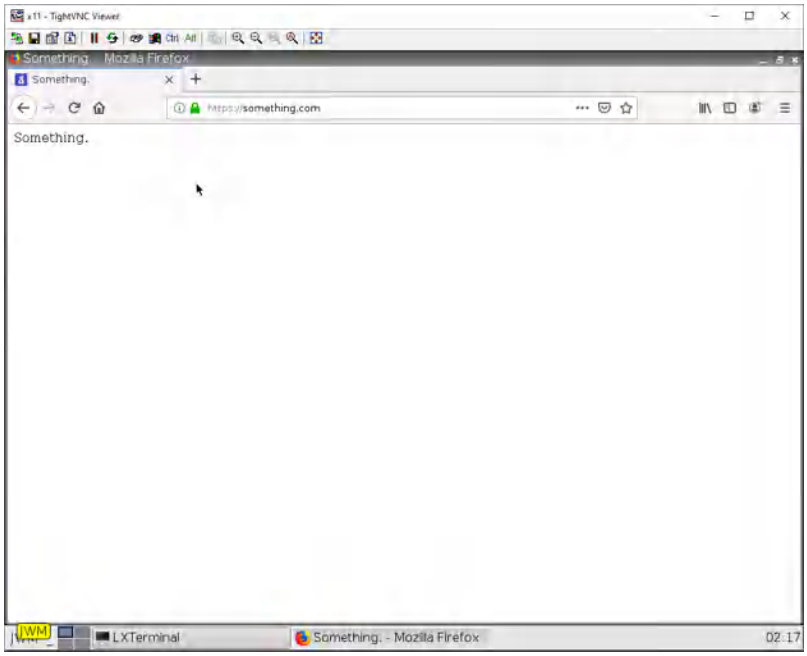


Figure 1.48: Verify your connectivity to the Internet

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

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!

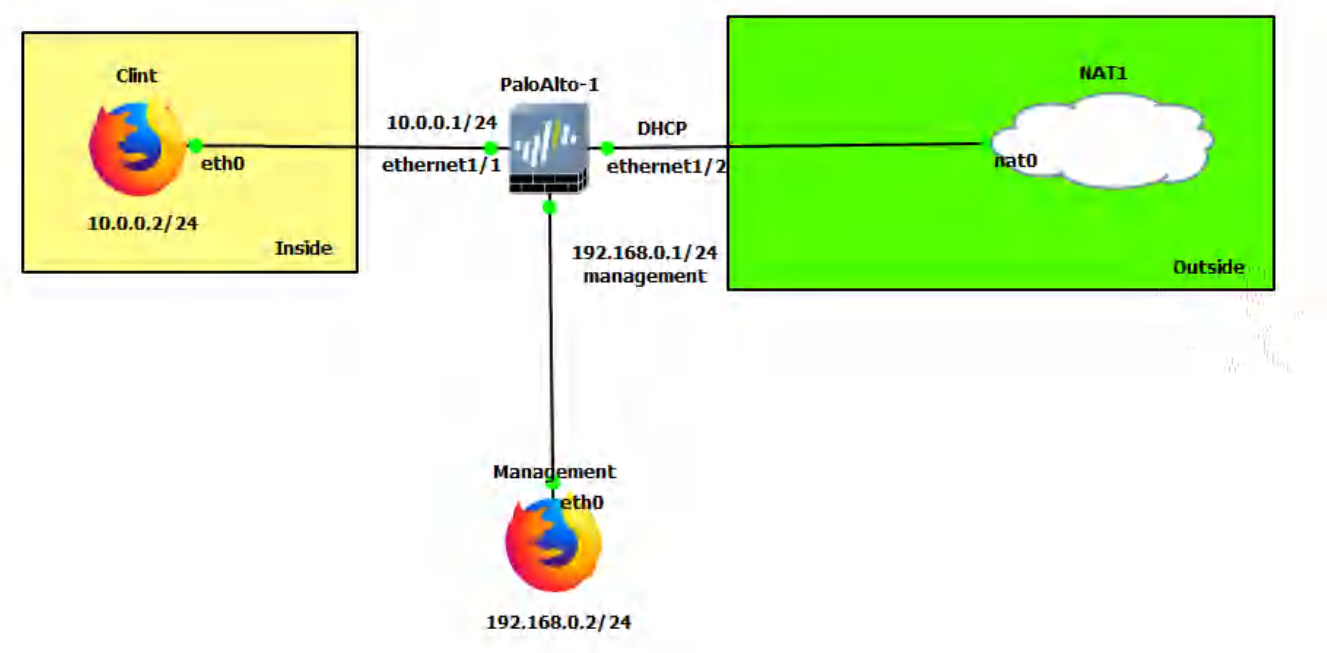


Figure 1.49: Main Scenario

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.

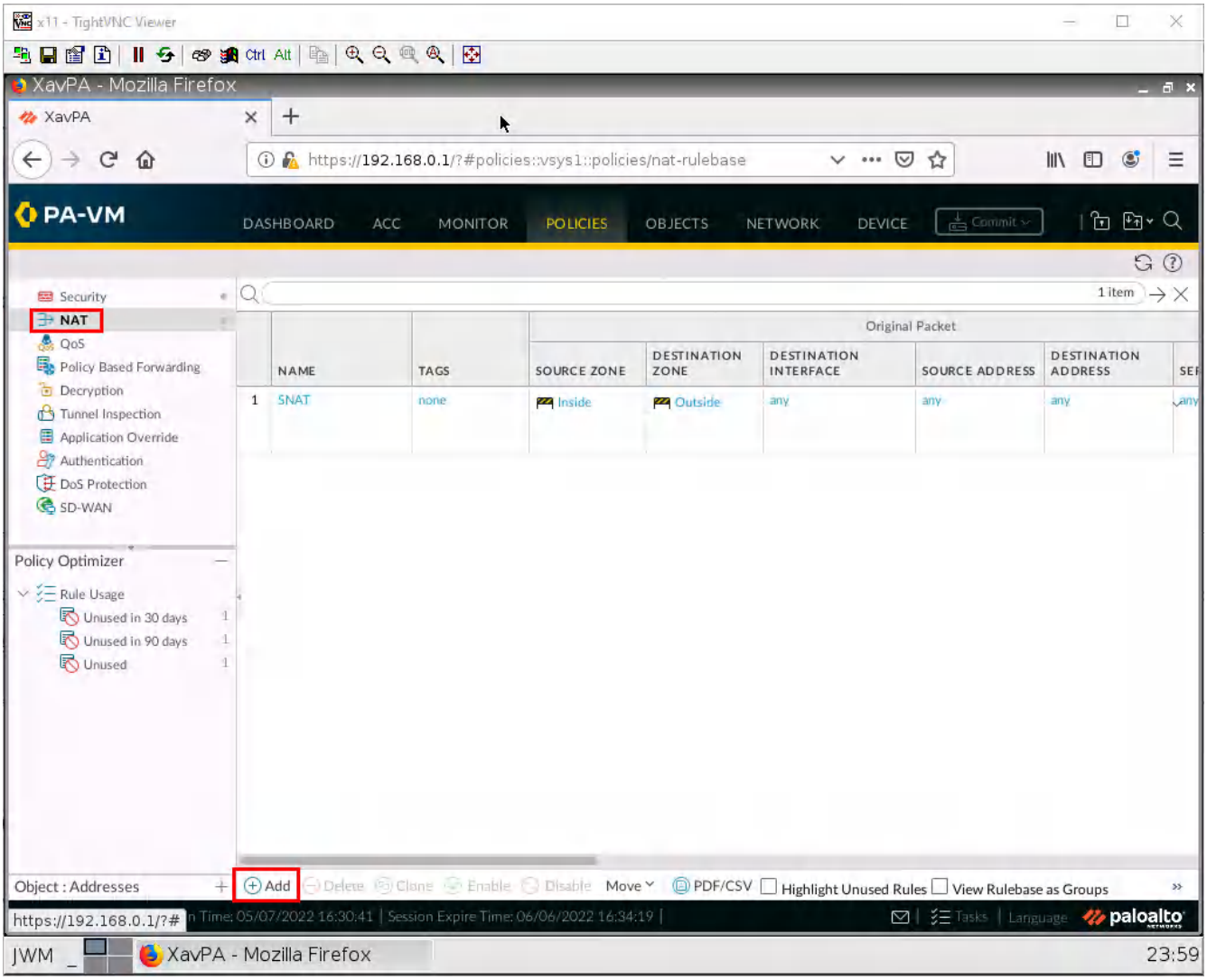


Figure 1.50: Set a Source NAT

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.

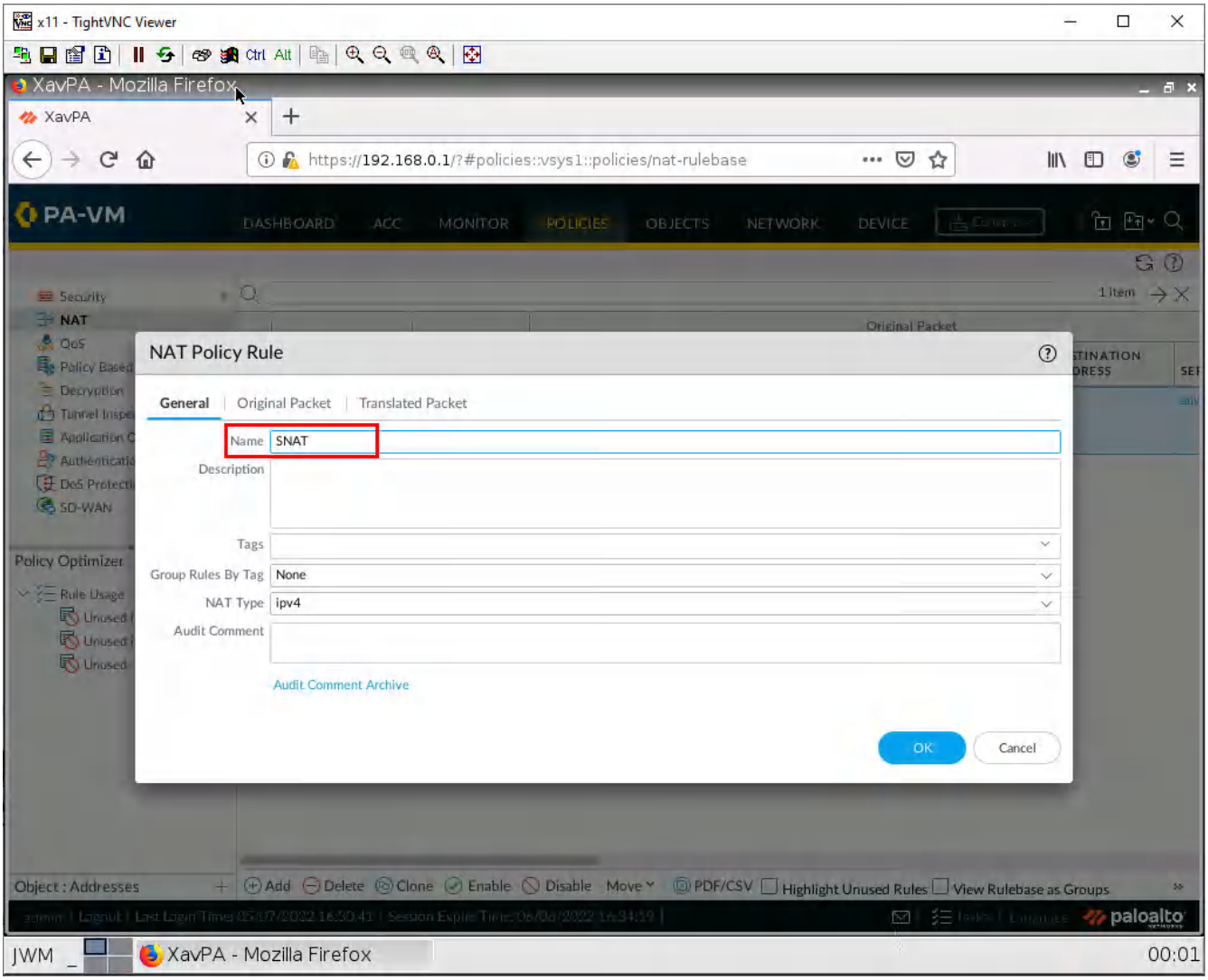


Figure 1.51: Set a Name for NAT

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

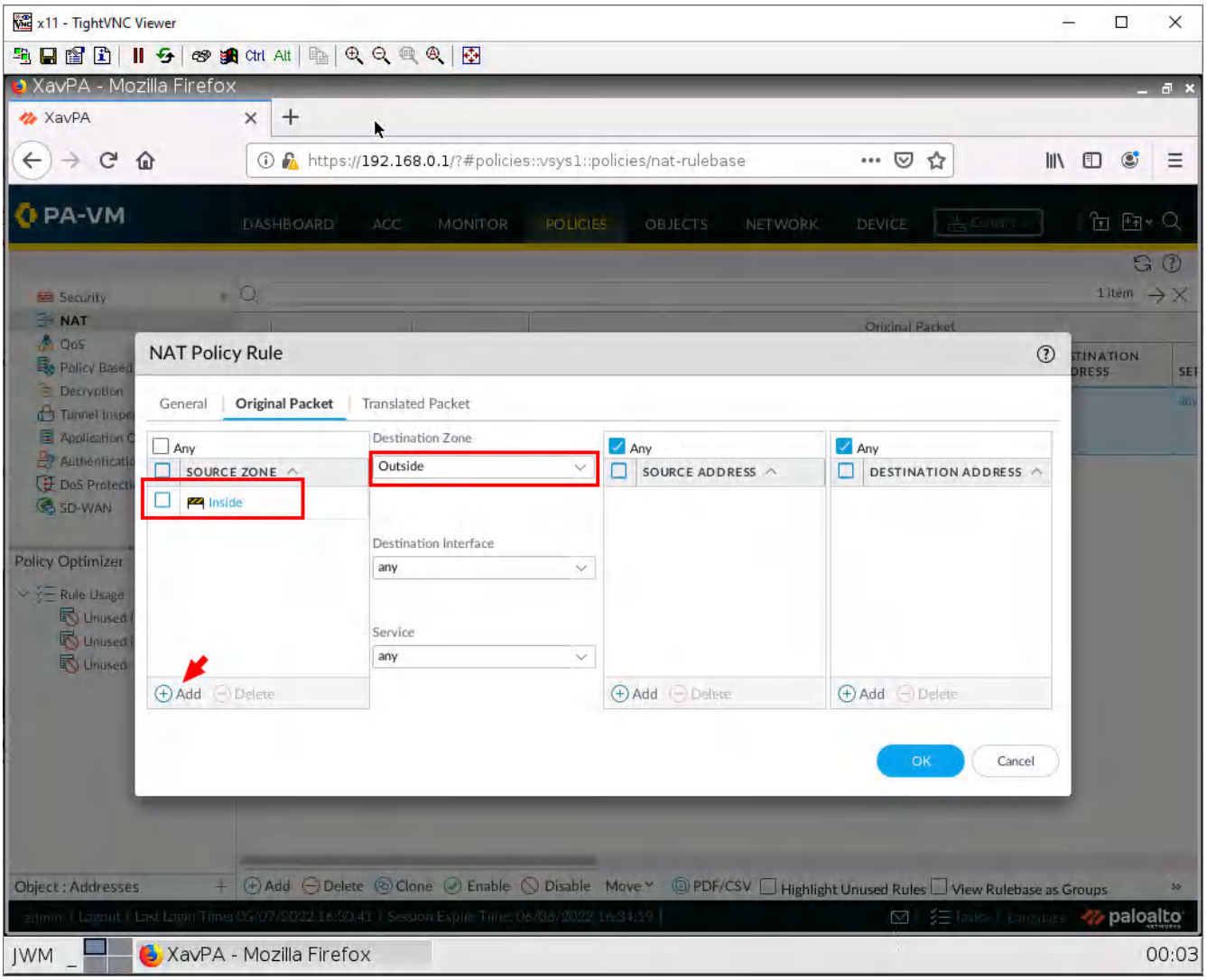


Figure 1.52: Set a Source Zone and Destination Zone for NAT

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

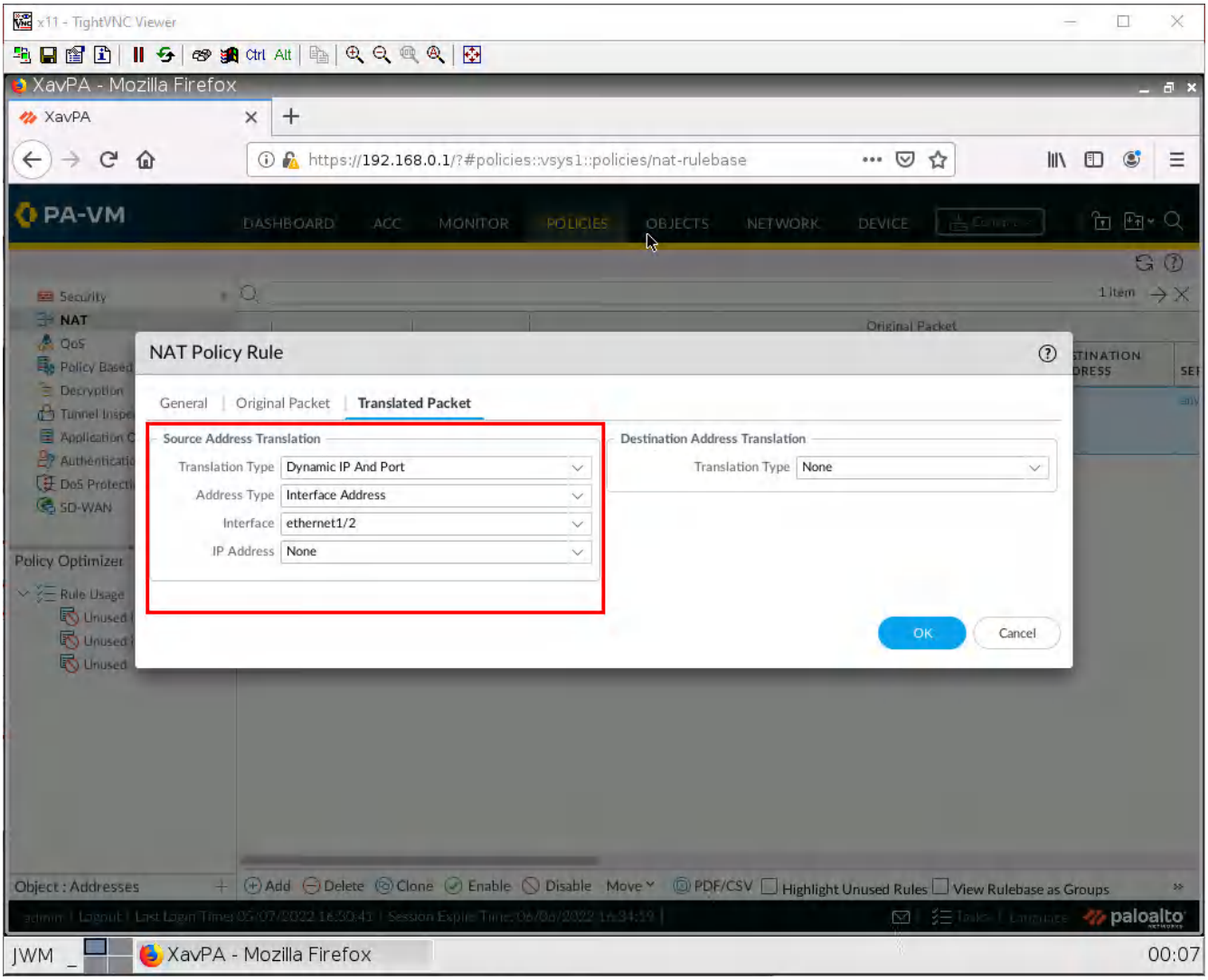


Figure 1.53: Set a Translated Packet

Don’t forget to commit!

Check Internet Connectivity on Webterm

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

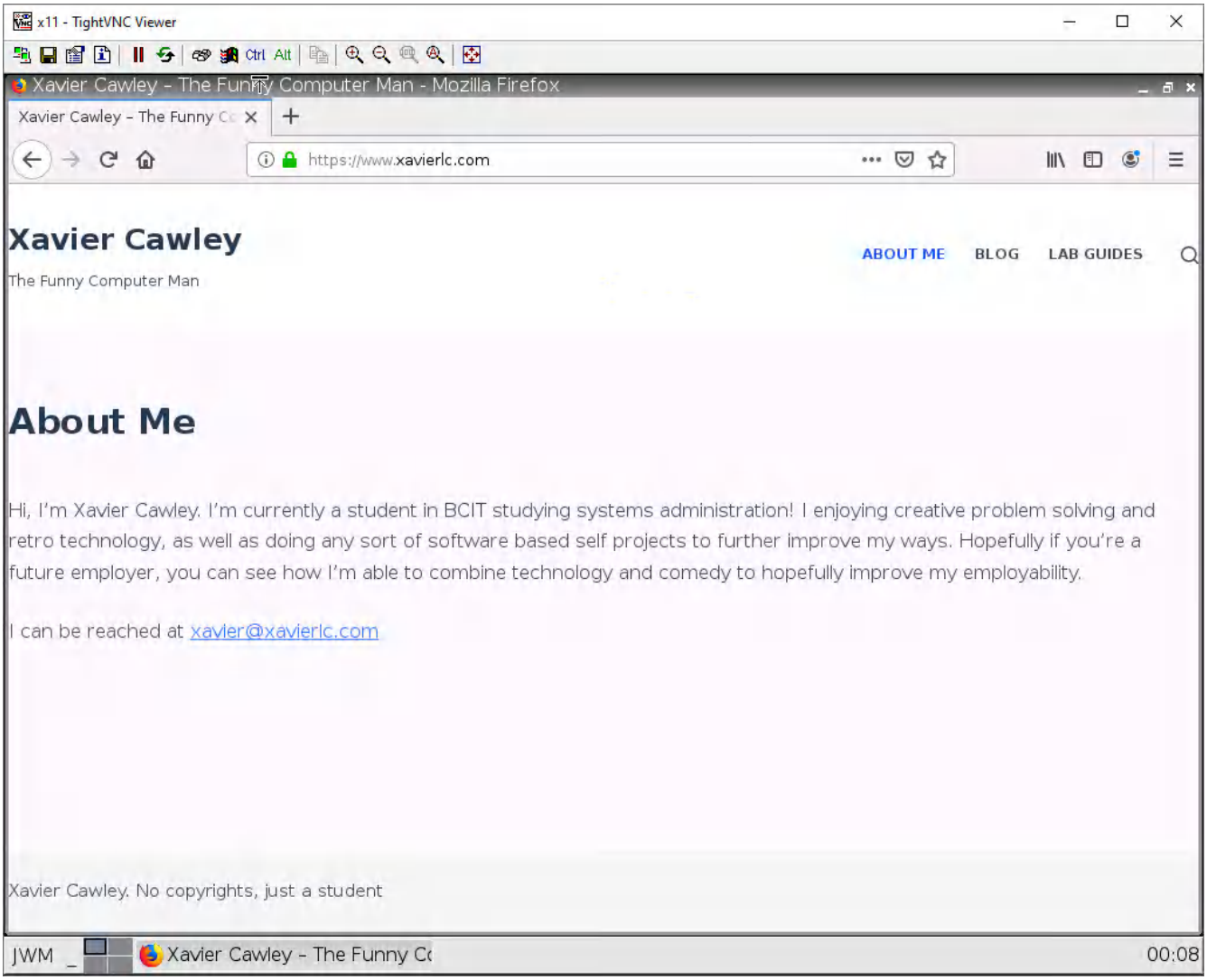


Figure 1.54: Verify your connectivity to the Internet

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.

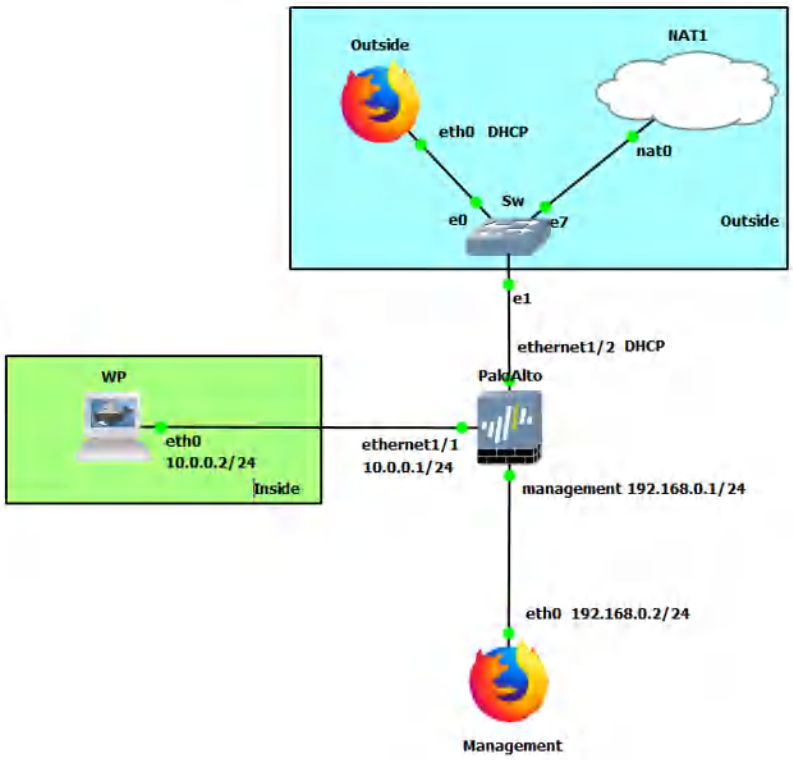


Figure 1.55: Main scenario

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**.

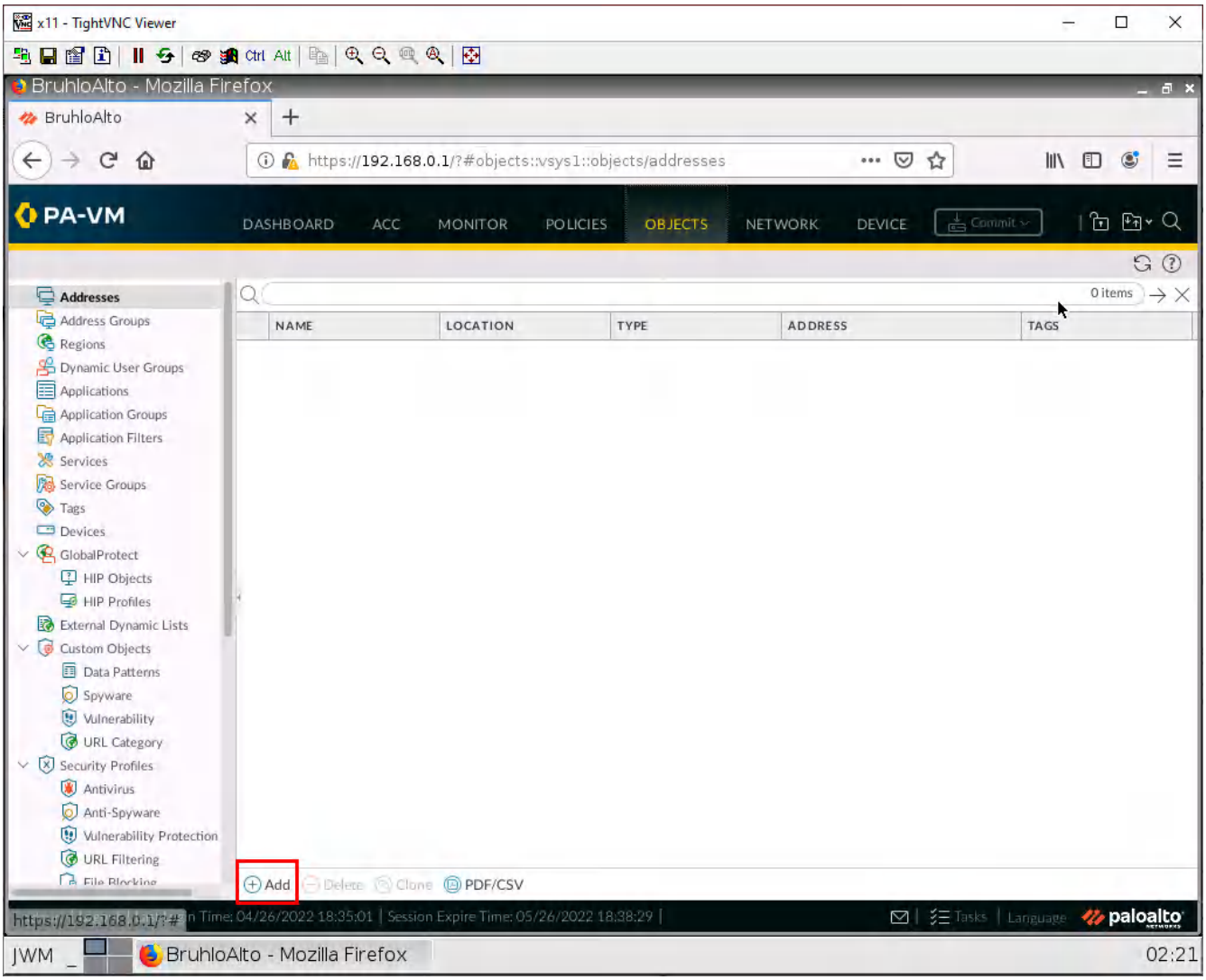


Figure 1.56: Add an address

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

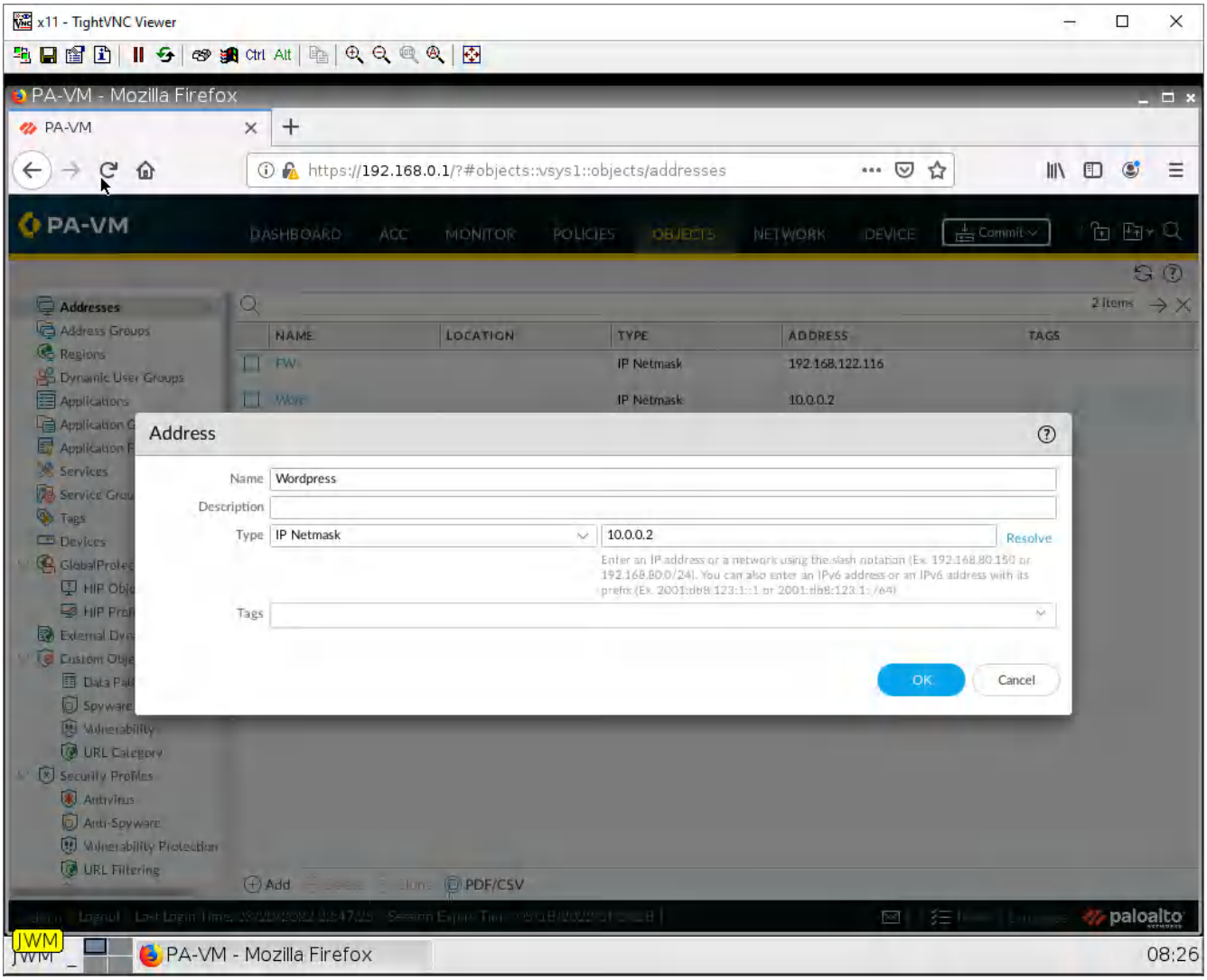


Figure 1.57: WordPress IP address

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:

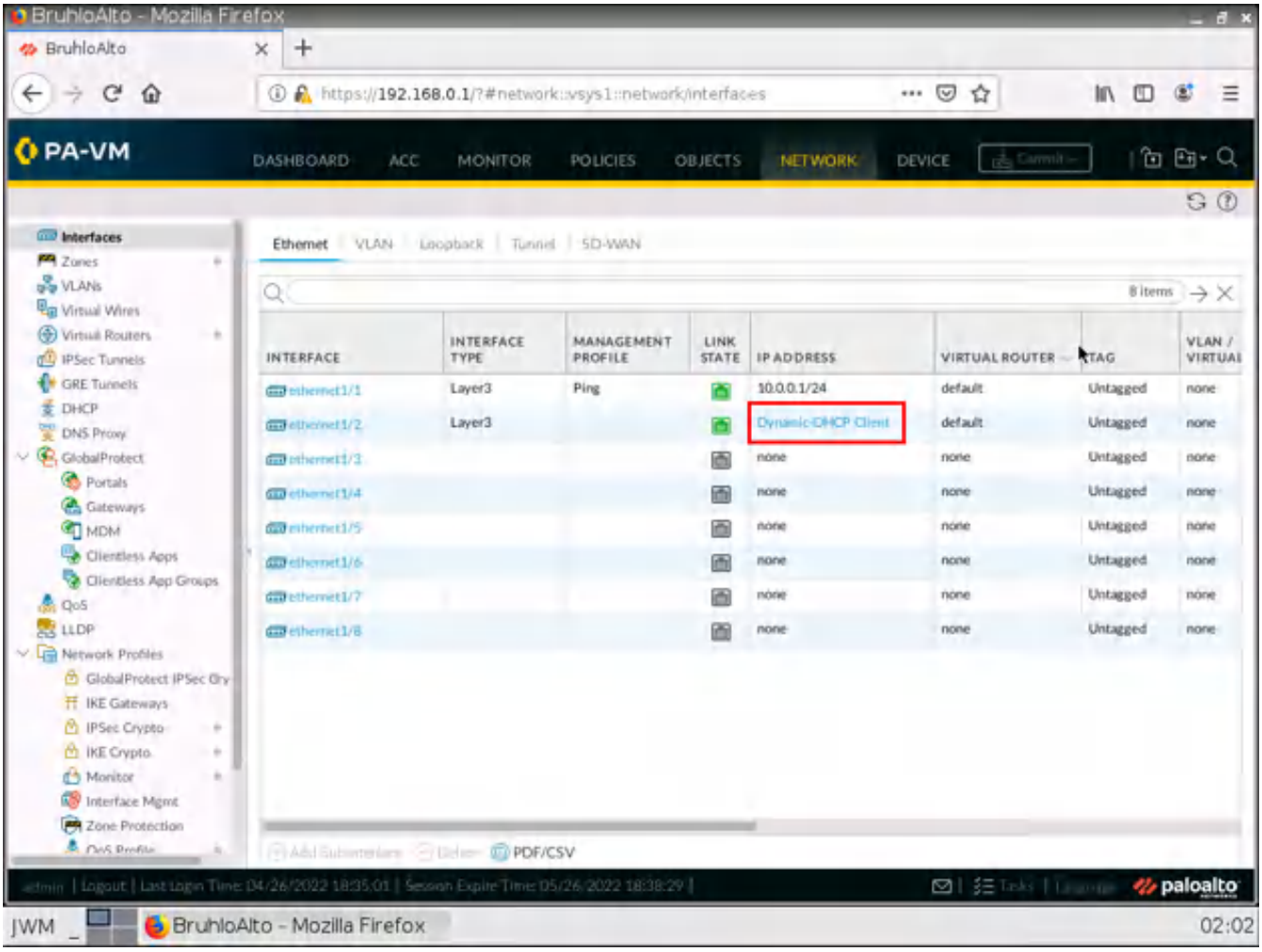


Figure 1.58: Dynamic-DHCP Client IP address

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

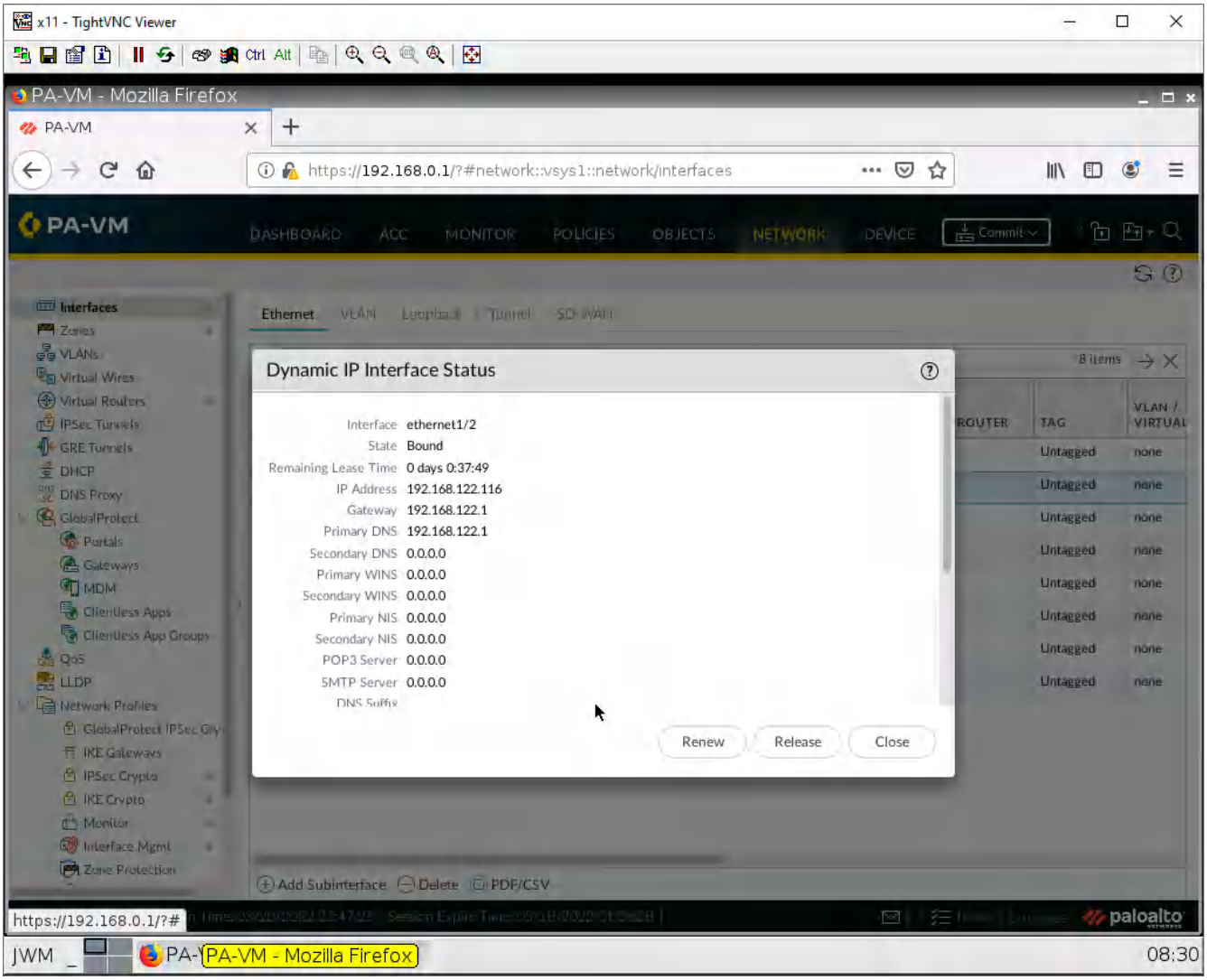


Figure 1.59: Verify Dynamic-DHCP Client IP address

Create a DNAT Policy

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

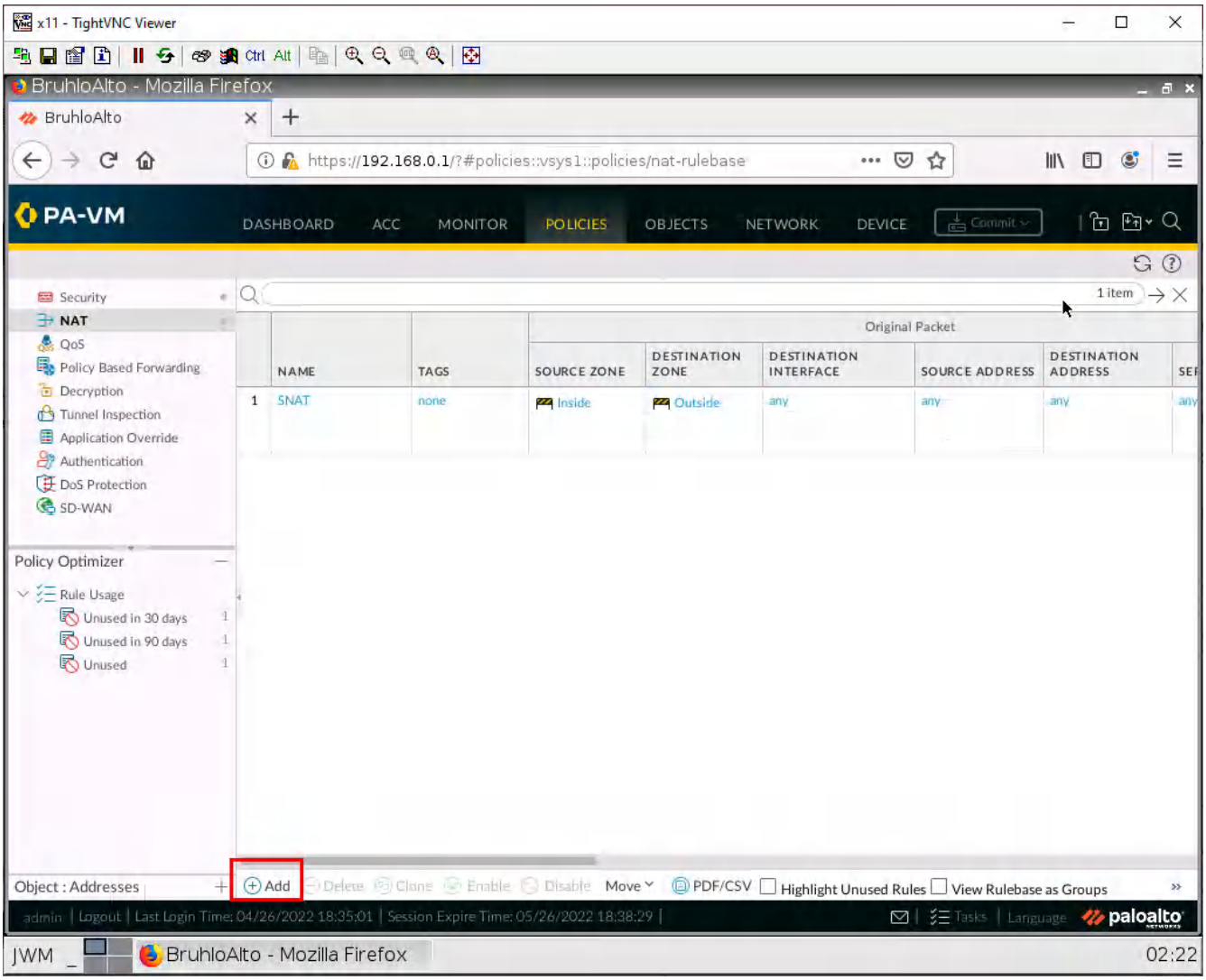


Figure 1.60: Add a DNAT Policy

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)

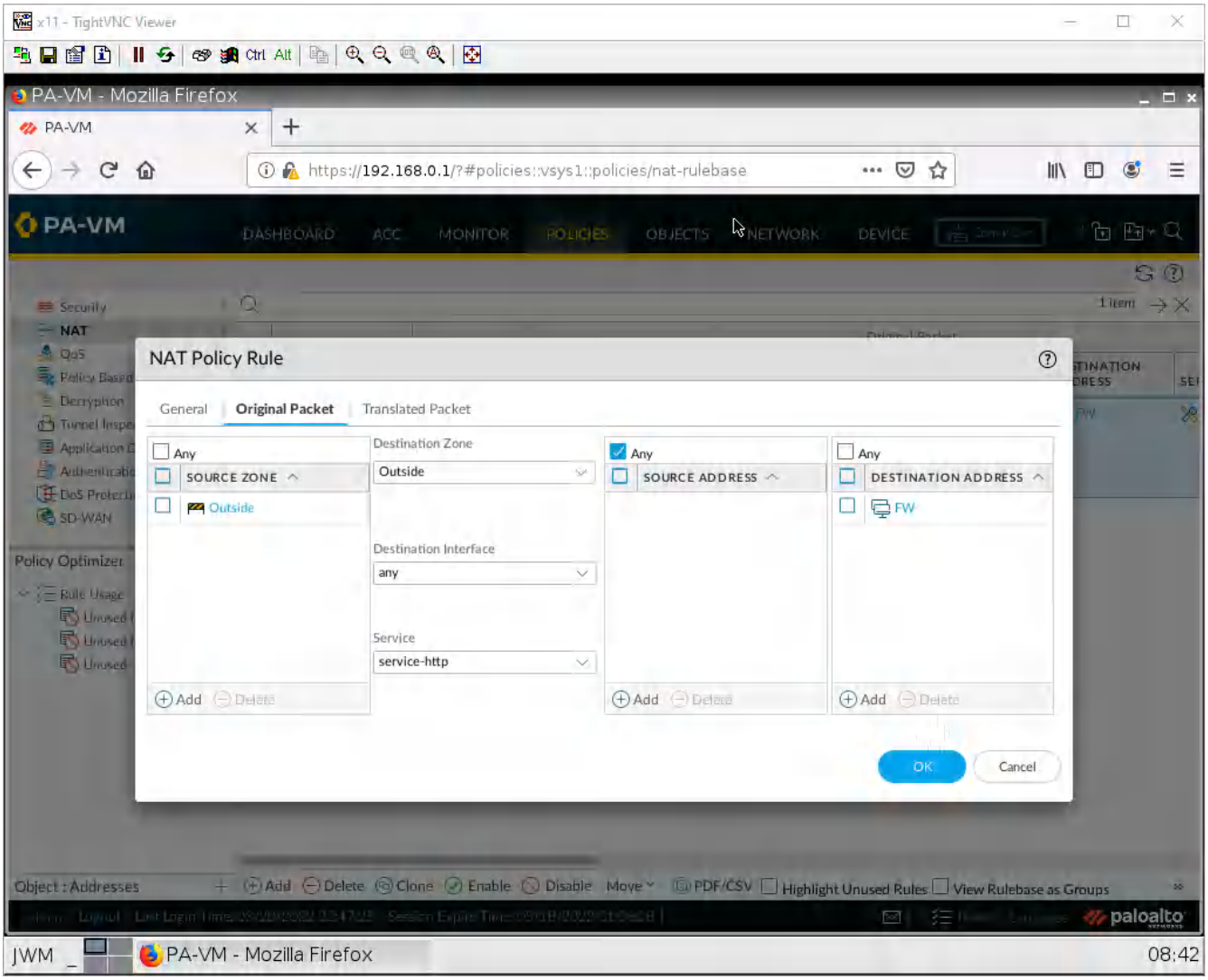


Figure 1.61: DNAT Policy Rule- Original Packet

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

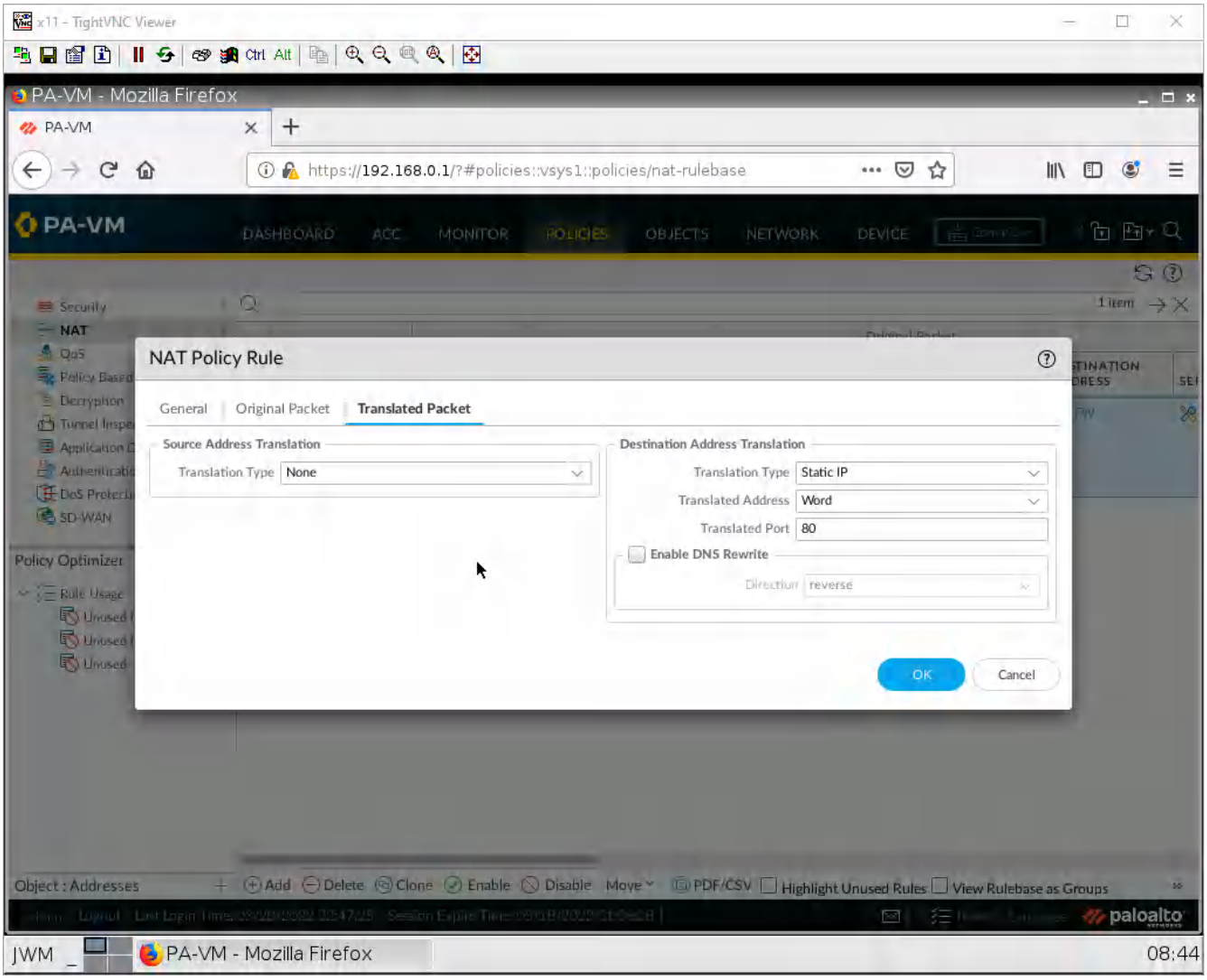


Figure 1.62: DNAT Policy Rule- Translated Packet

Then, press **OK**.

Security Policy for DNAT

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

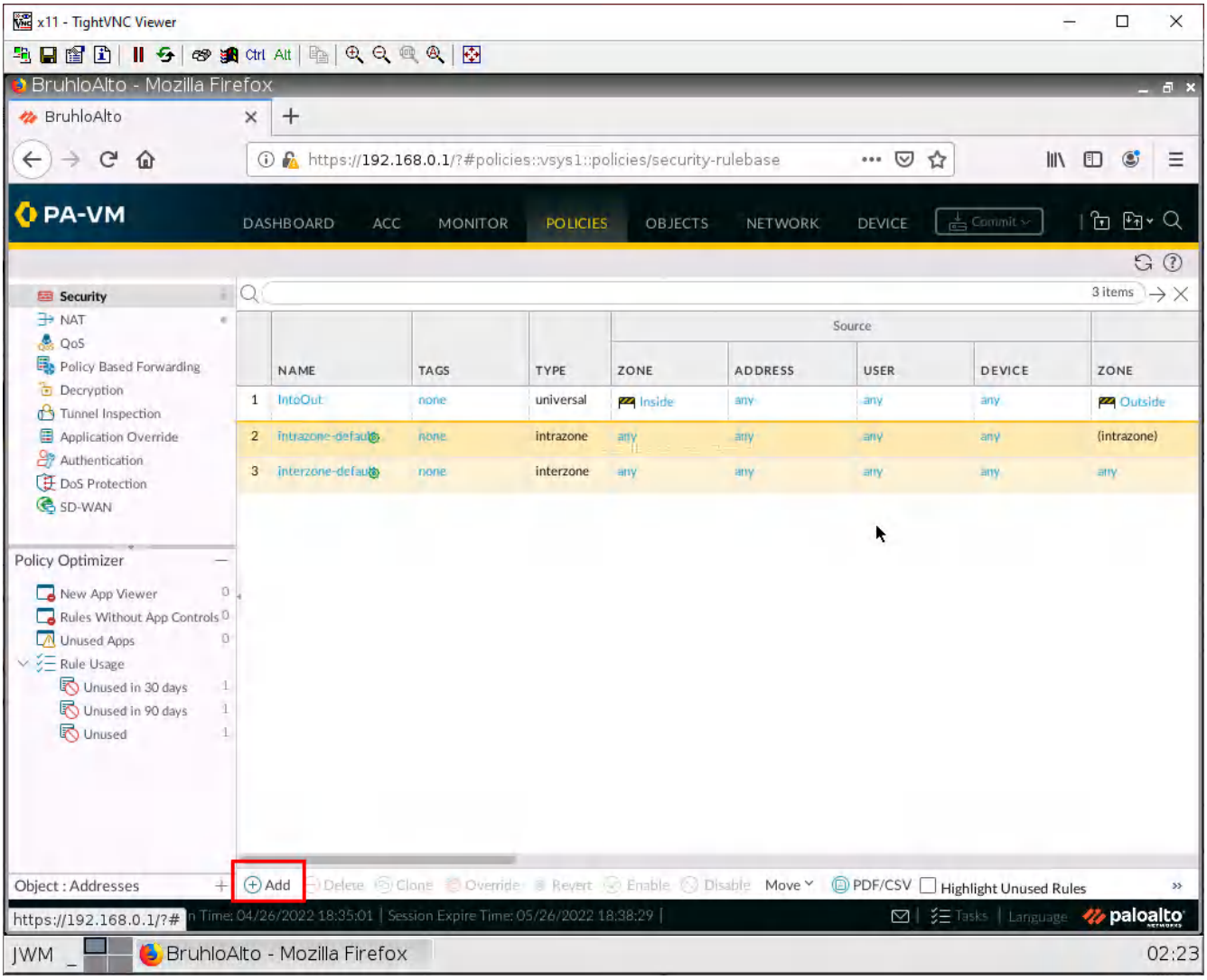


Figure 1.63: Add a Security Policy

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

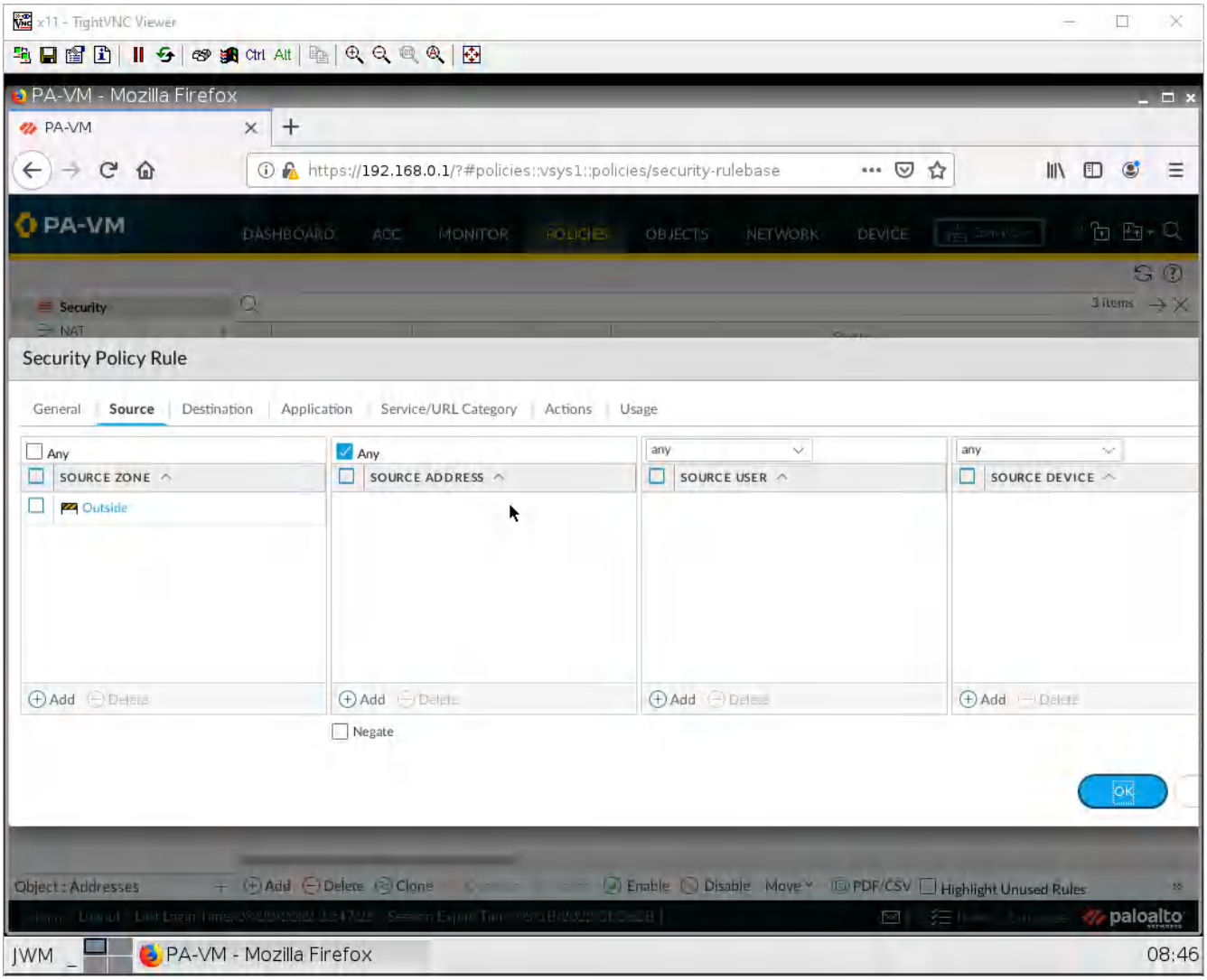


Figure 1.64: Configuring the Source Zone

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

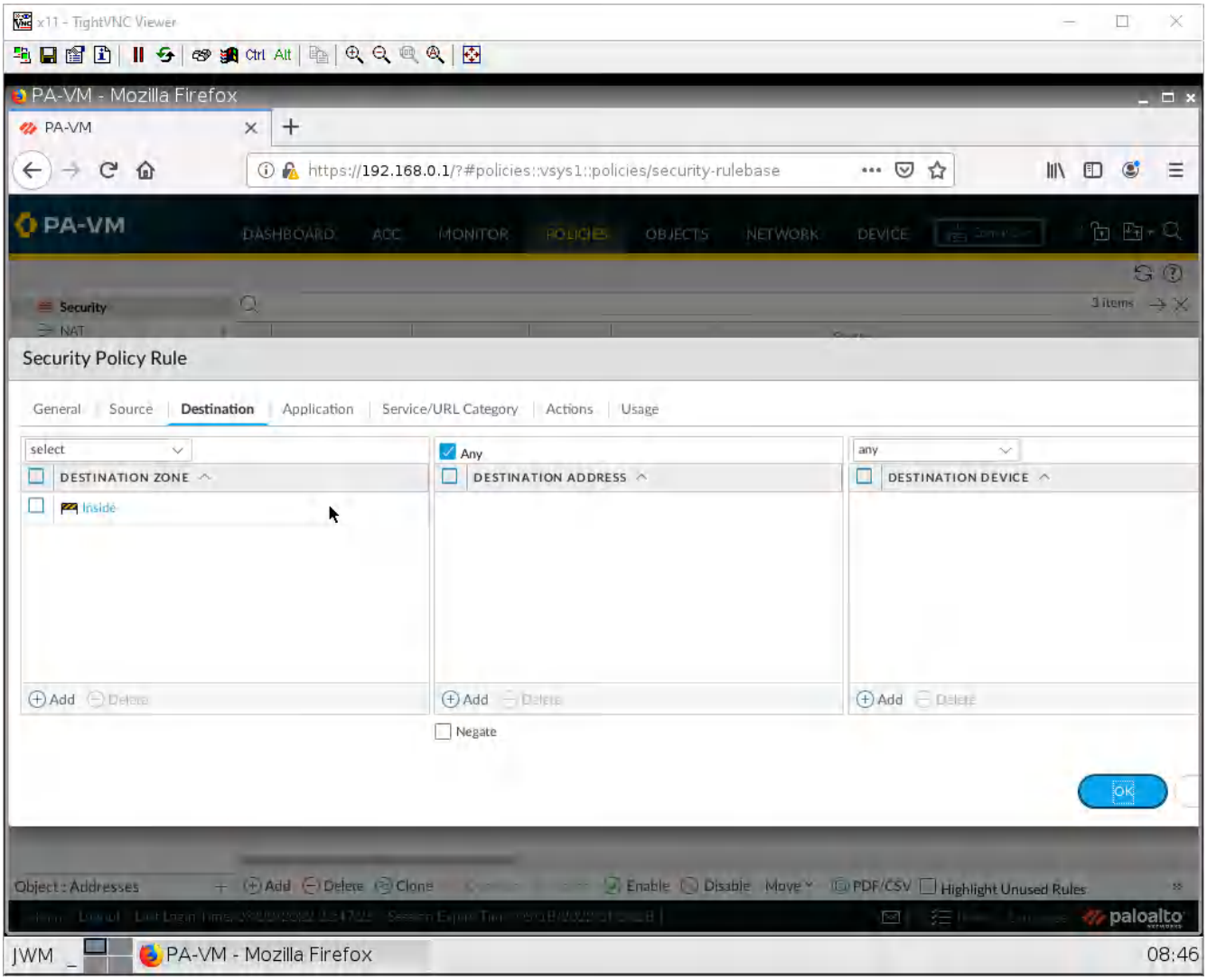


Figure 1.65: Configuring the Destination Zone

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!

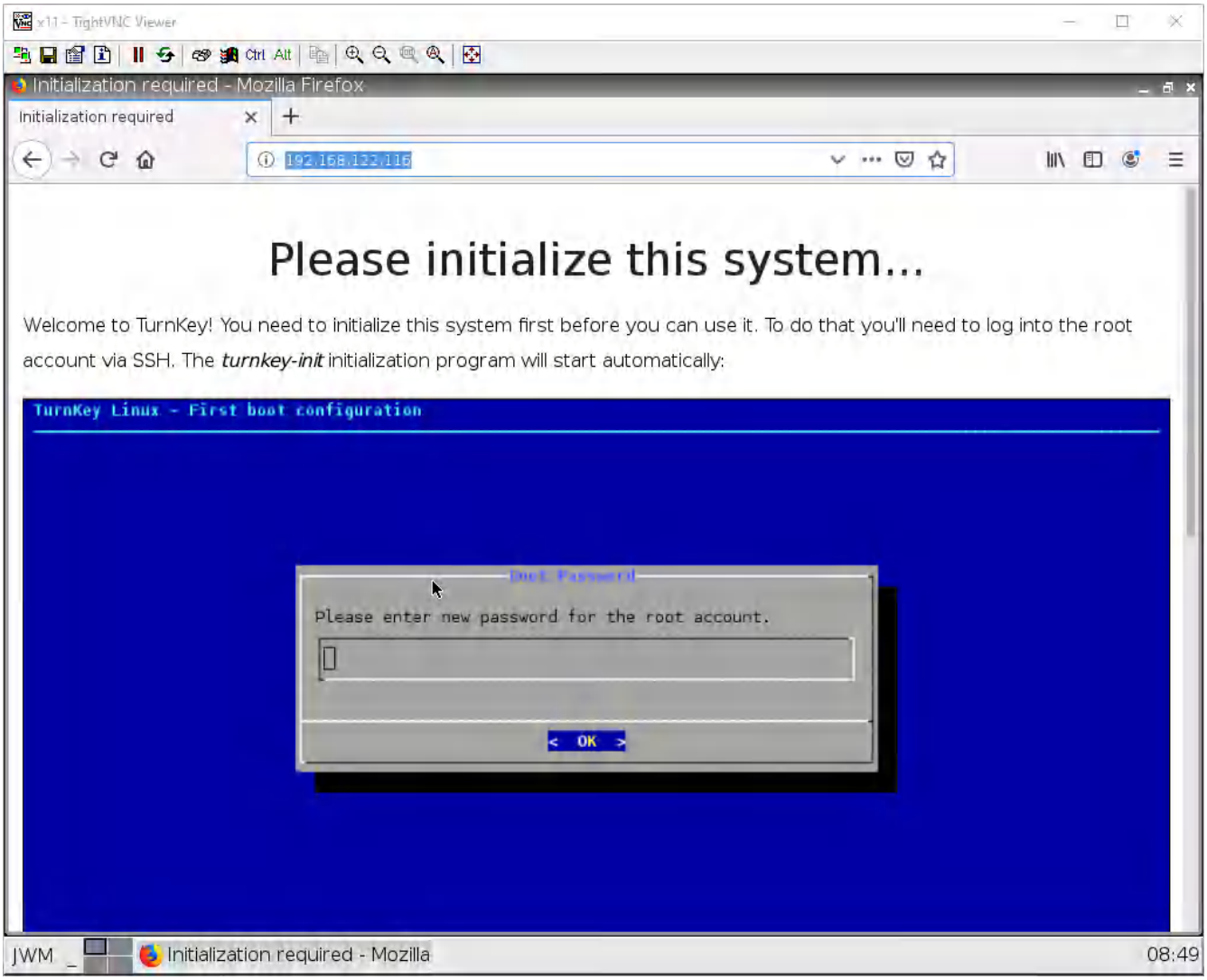


Figure 1.66: Verify your configuration

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.

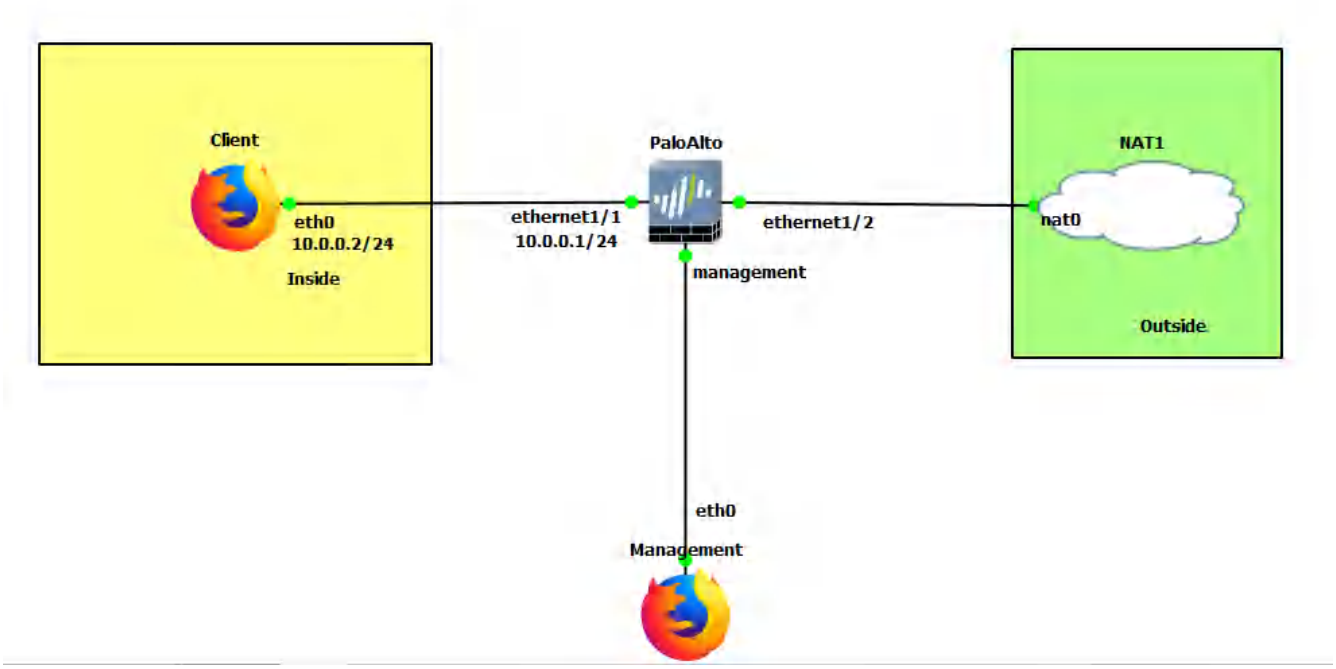


Figure 2.1: Main scenario

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

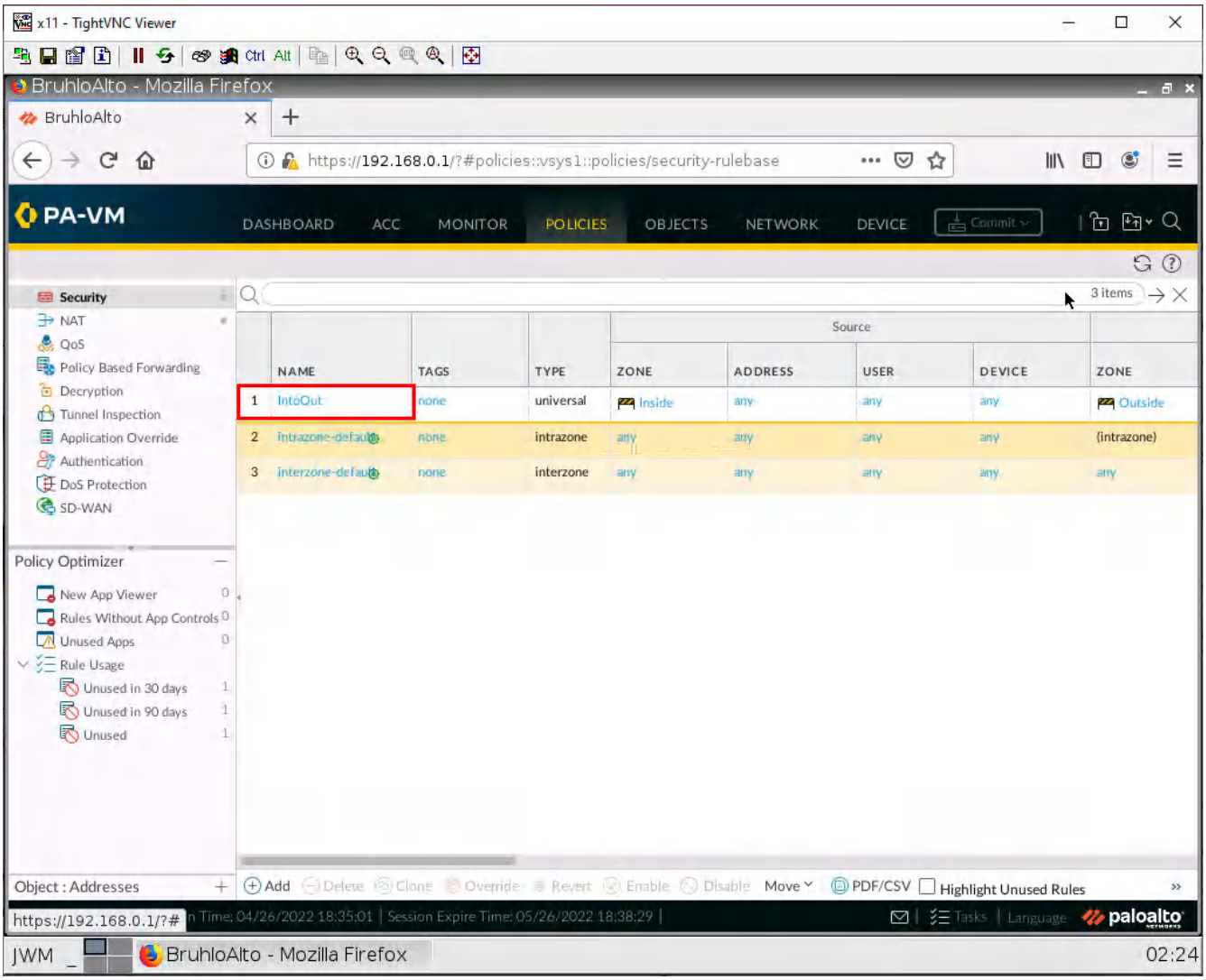


Figure 2.2: Create a Security Policy

Under the application tab, add these under applications:

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

These will allow only basic web browsing.

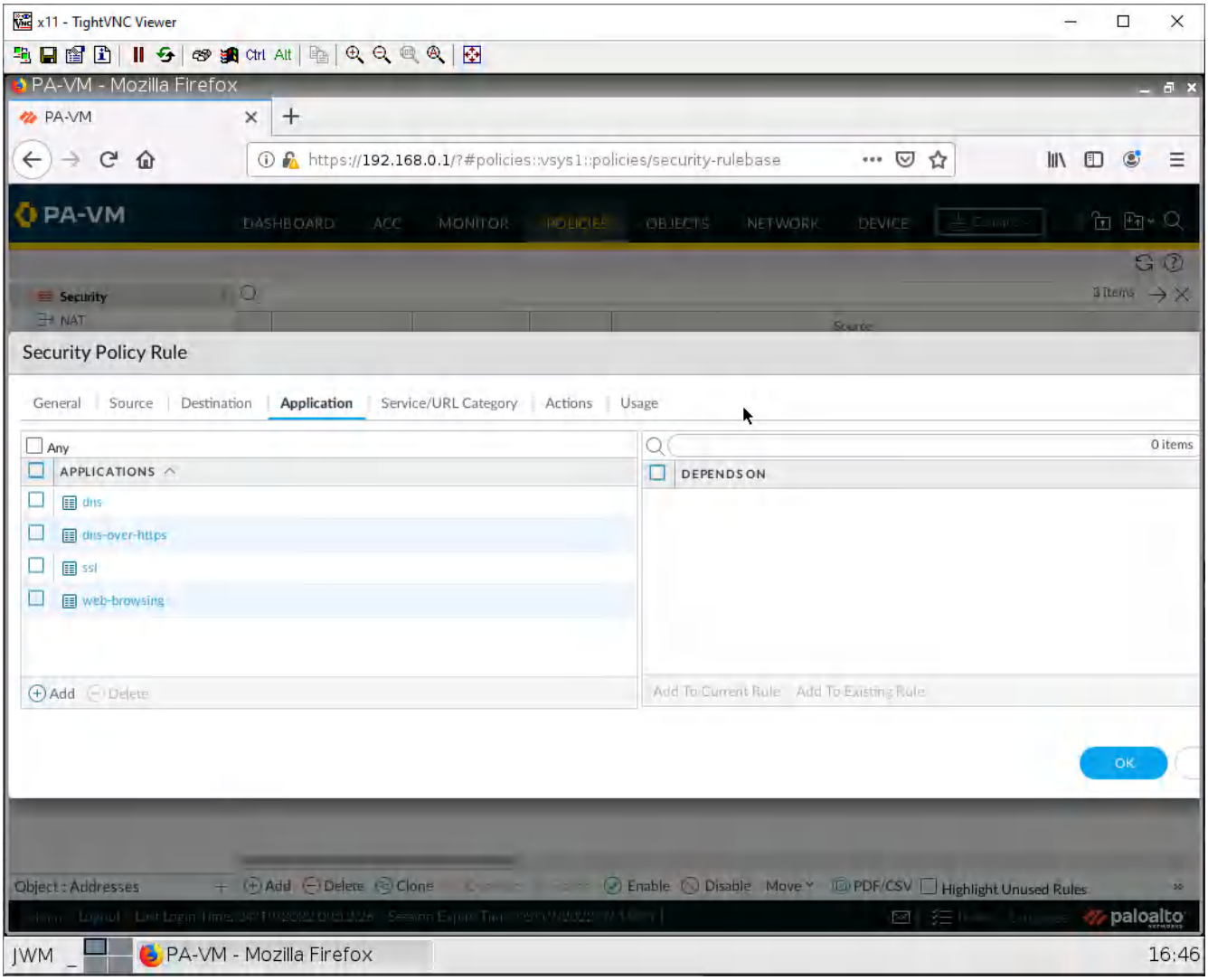


Figure 2.3: Set a custom application

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

Test the Policy

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

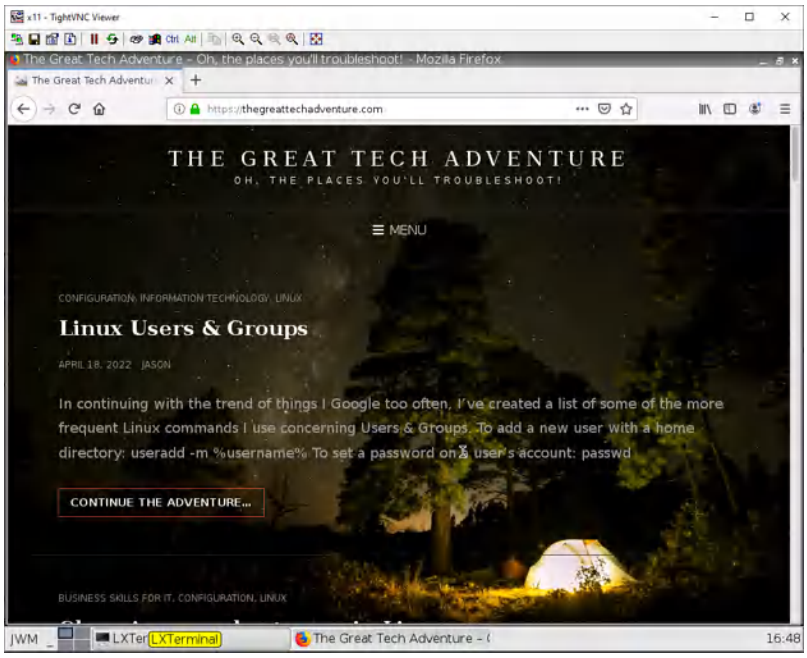


Figure 2.4: Verify your configuration

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

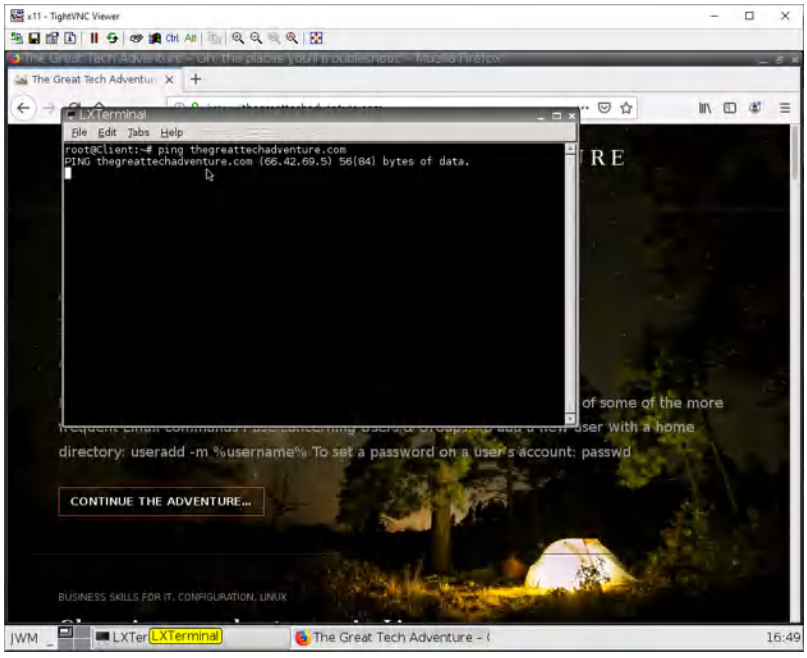


Figure 2.5: Verify Ping

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.

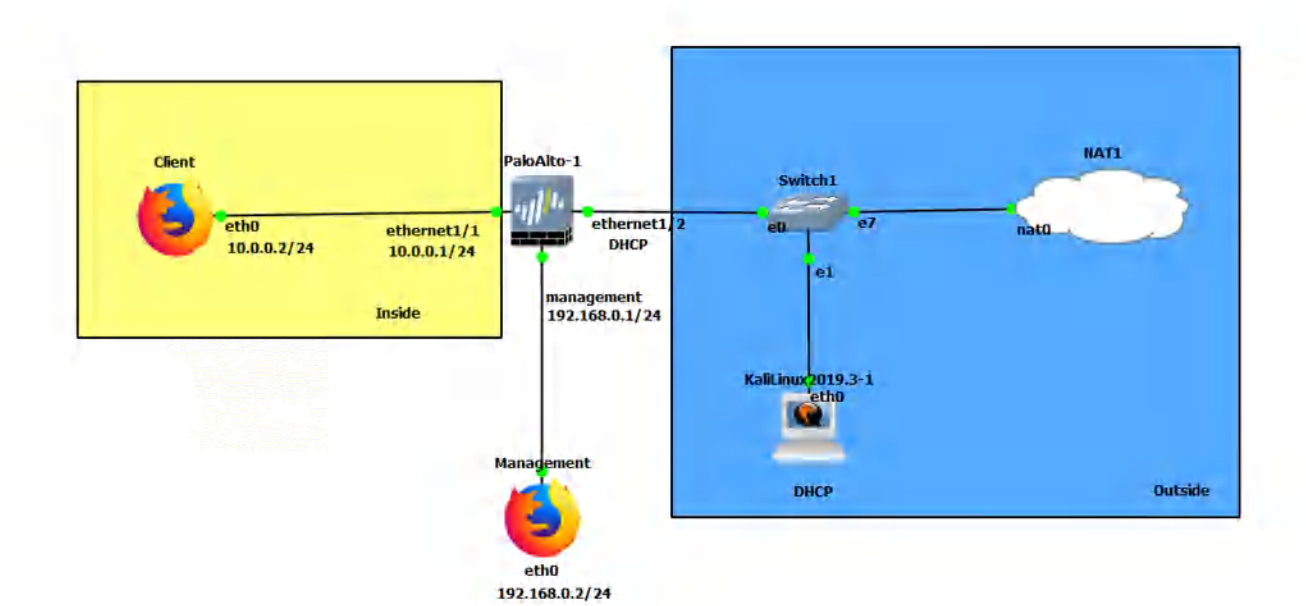


Figure 2.6: Main scenario

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.

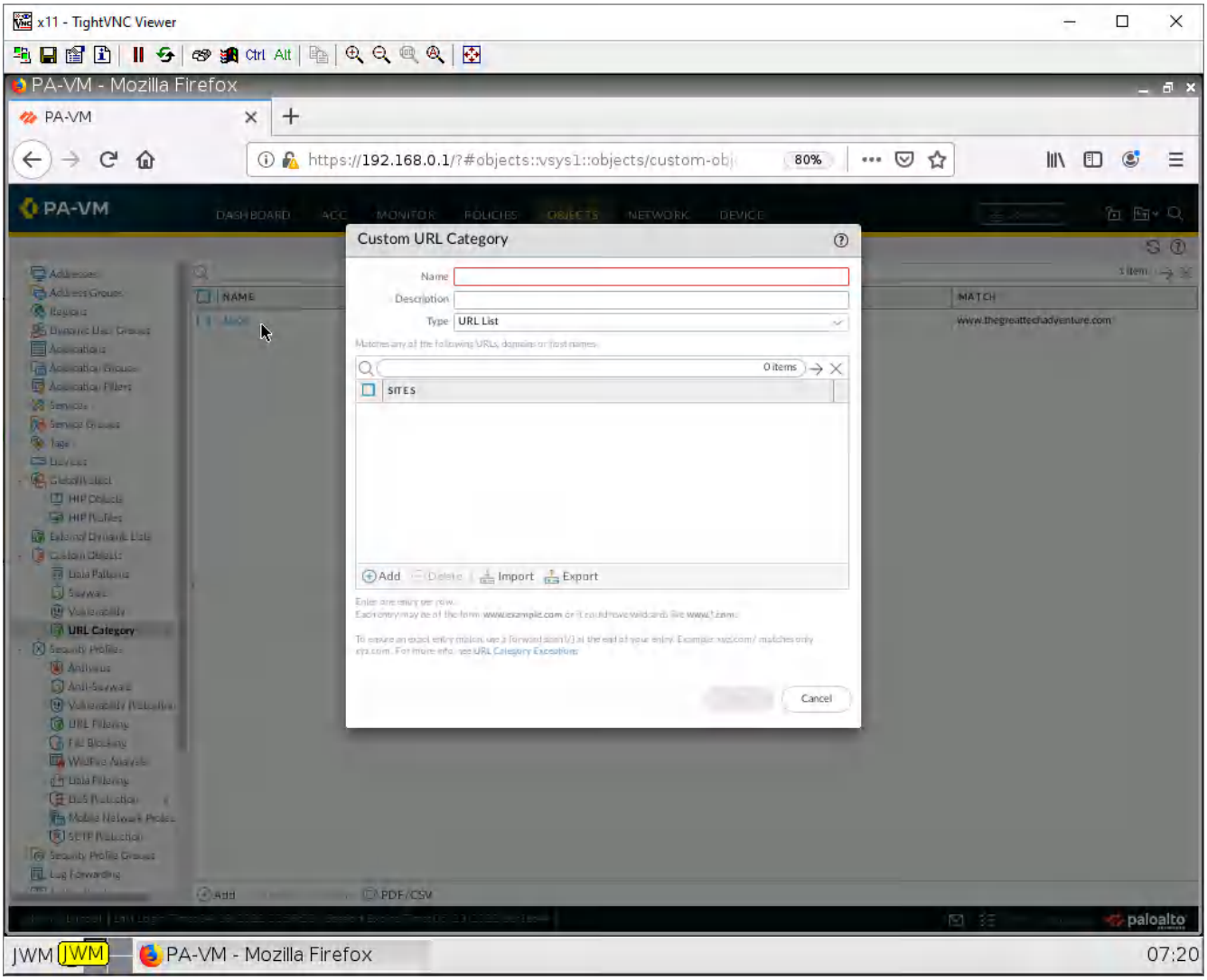


Figure 2.7: Create a Custom URL Category

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

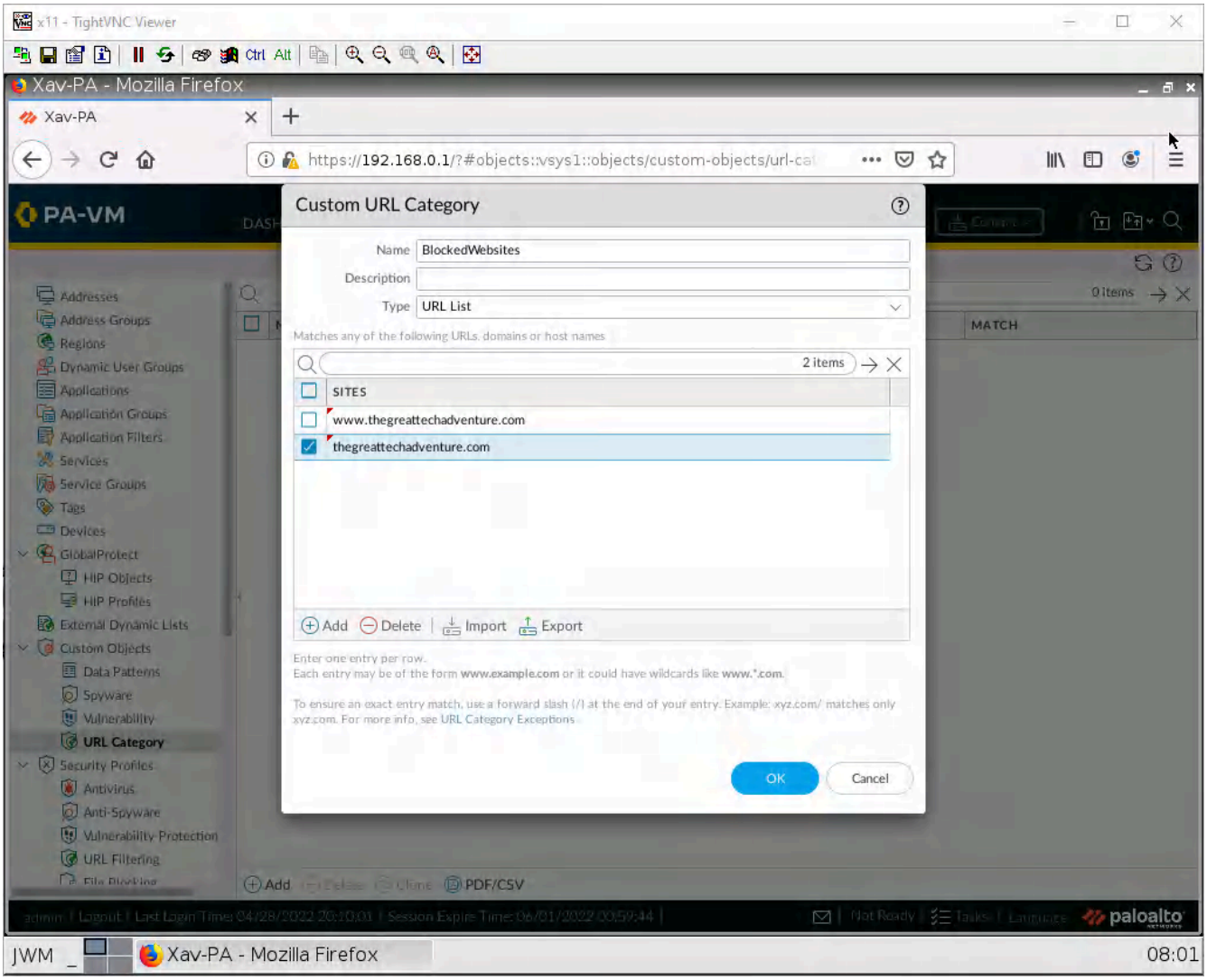


Figure 2.8: Add a CustomURL Category

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

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

Block a Website

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

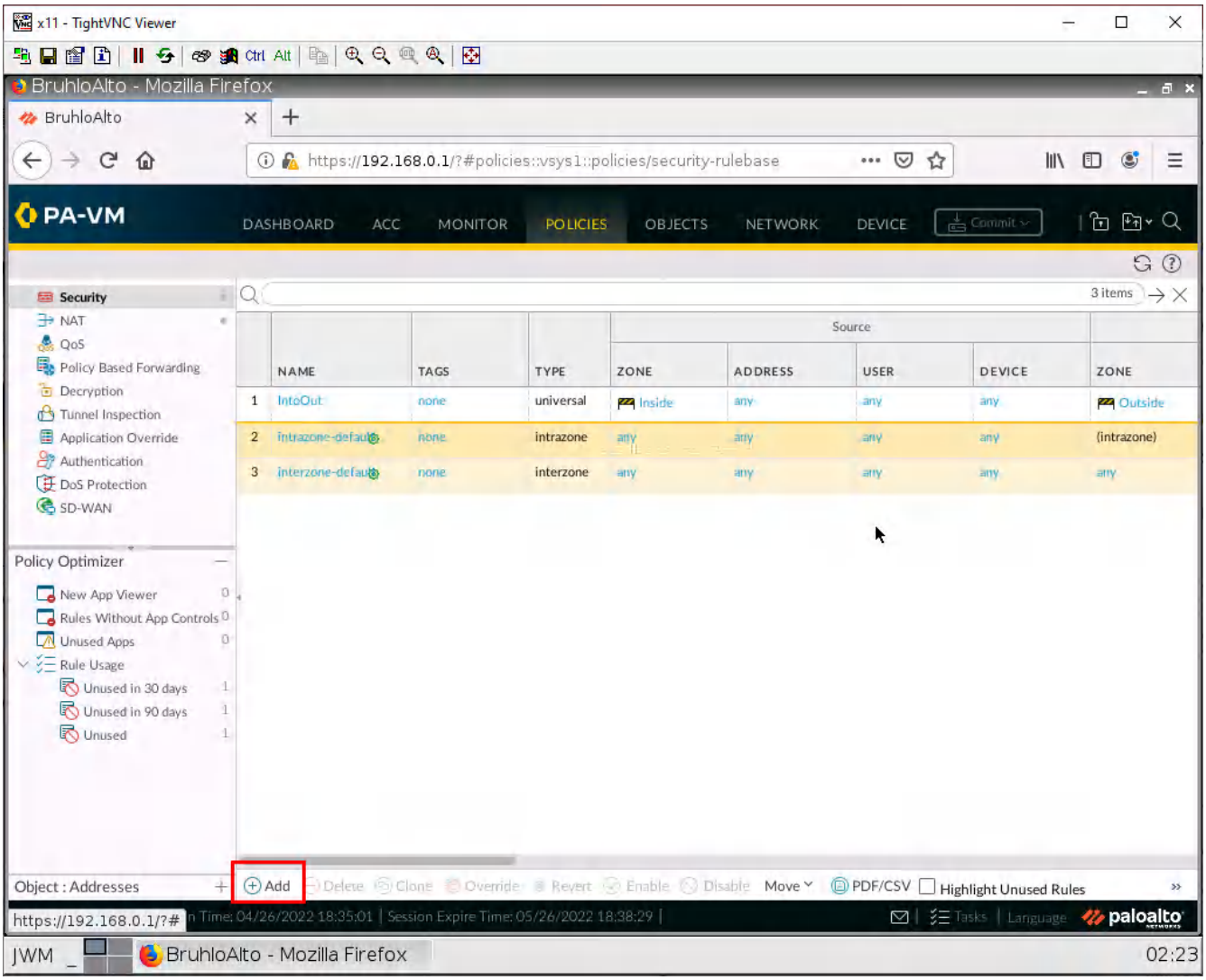


Figure 2.9: Add a security policy

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

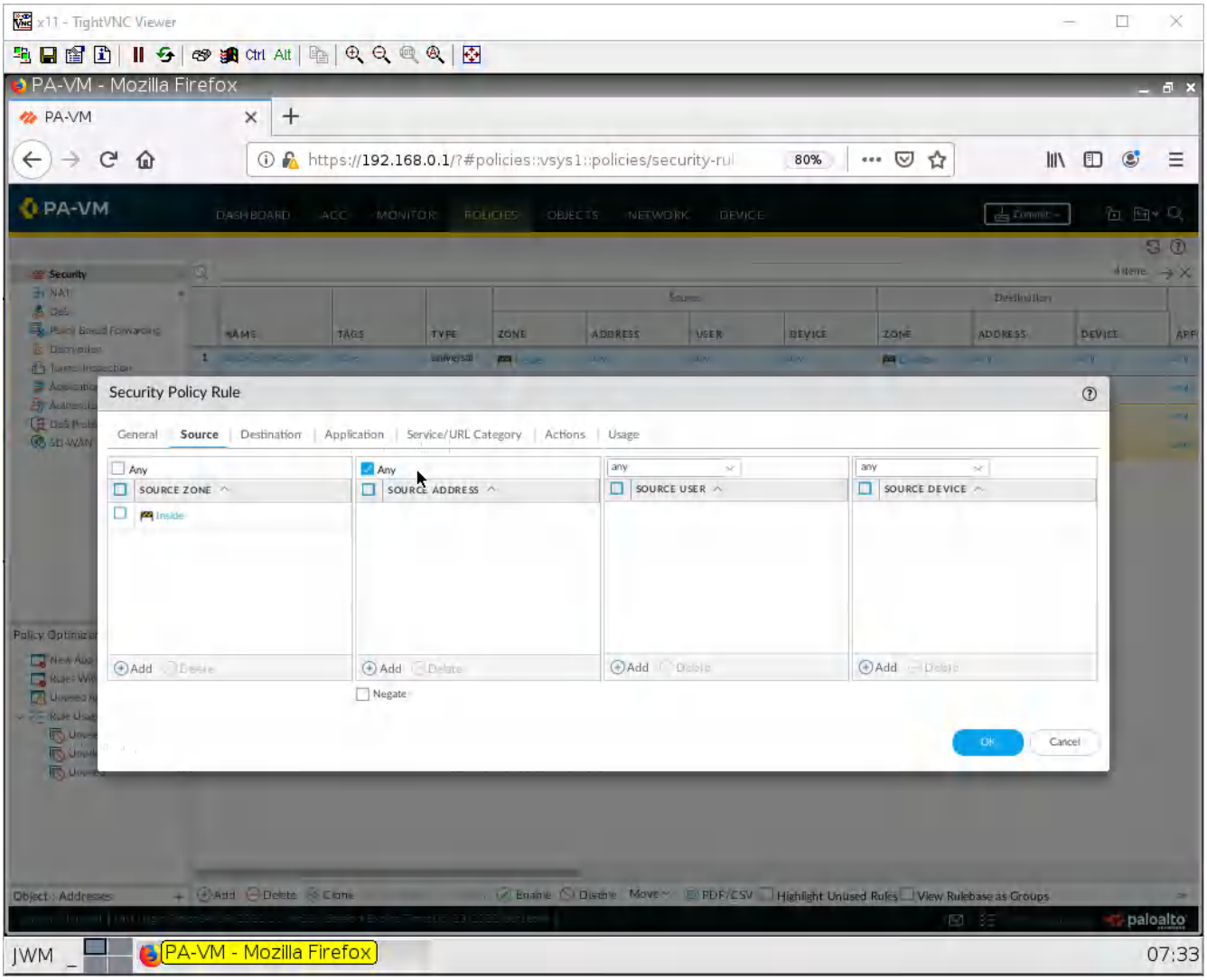


Figure 2.10: Add a Source Zone

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

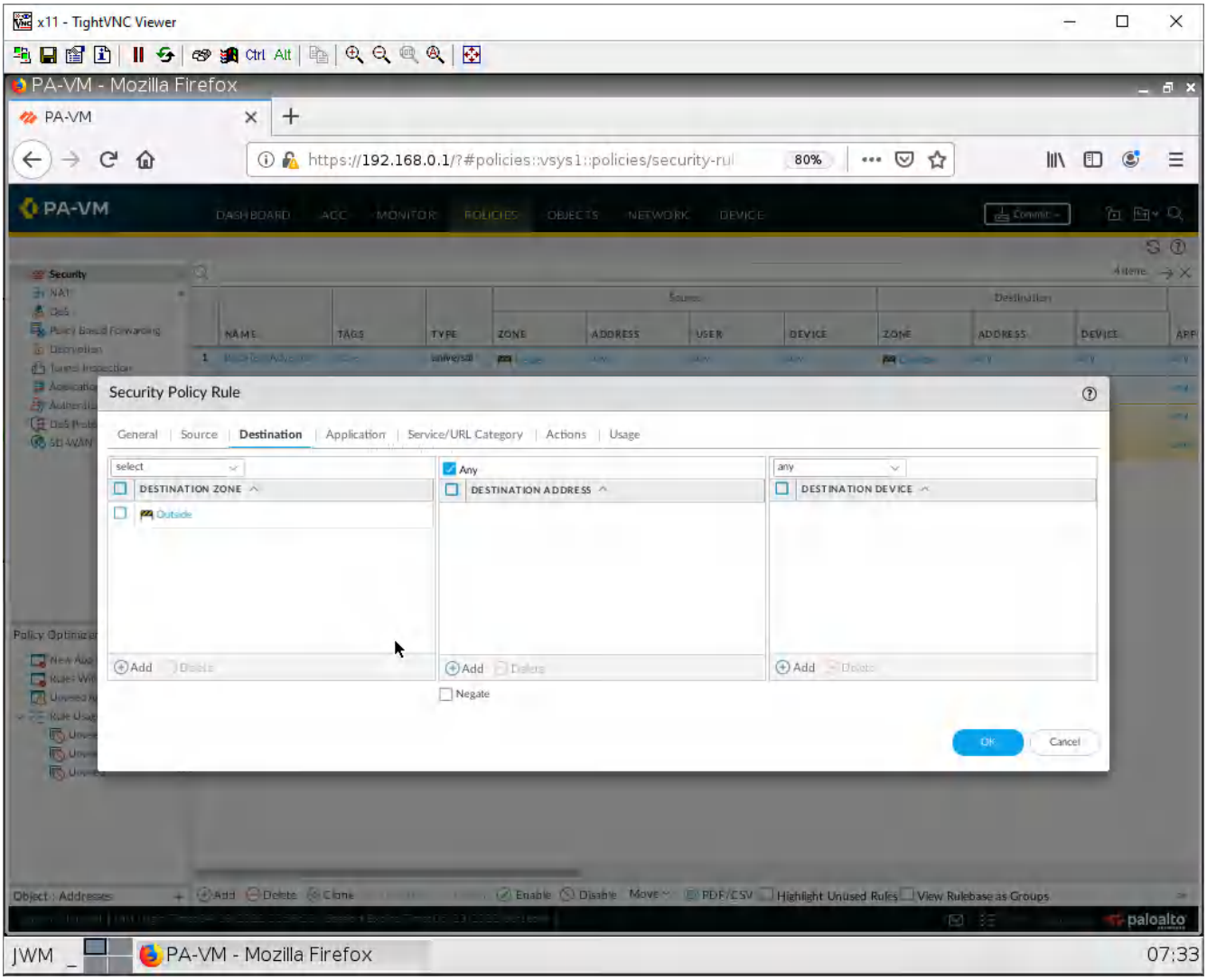


Figure 2.11: Add a Destination Zone

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

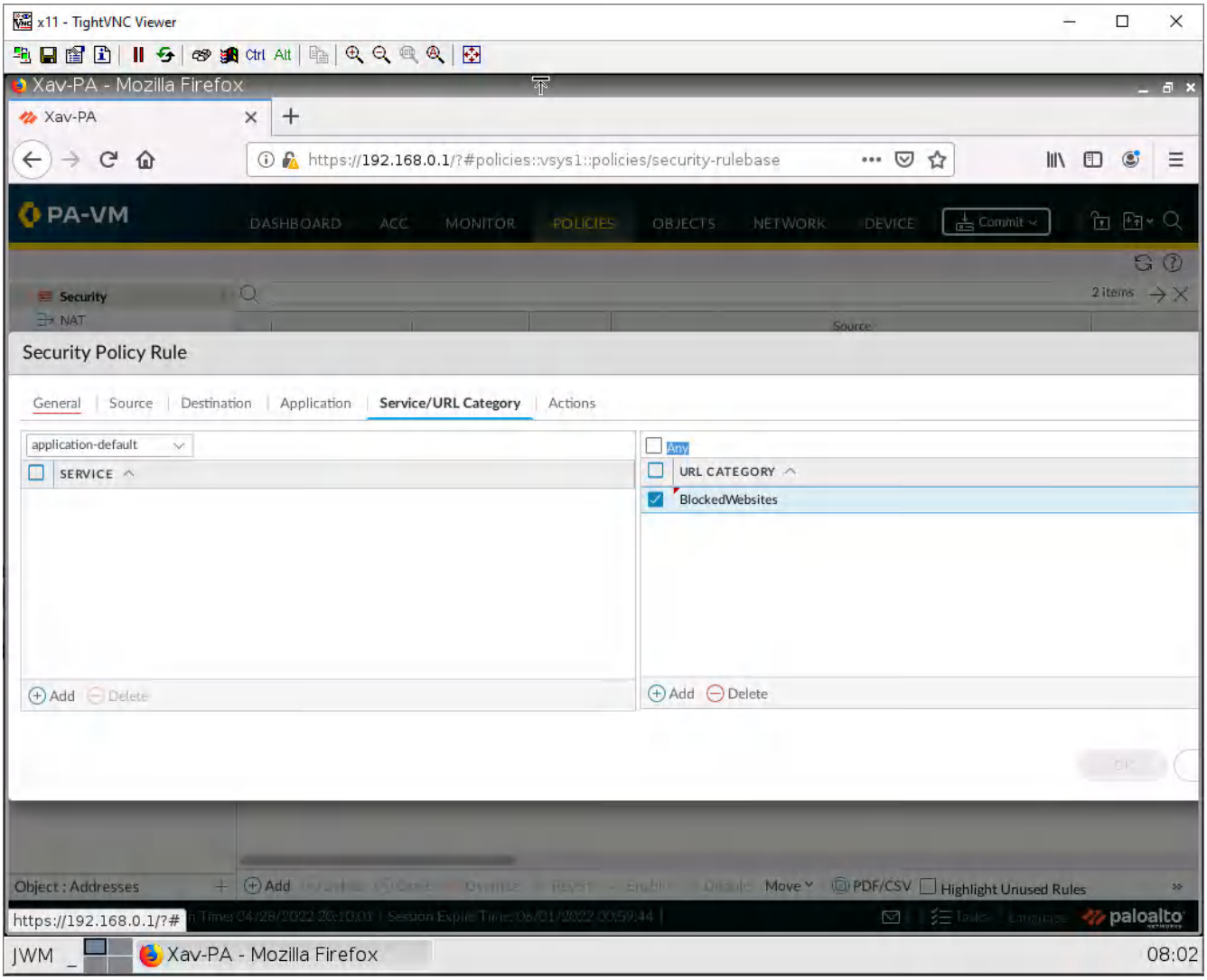


Figure 2.12: Assign URL Category

Under the actions page, set the action to deny.

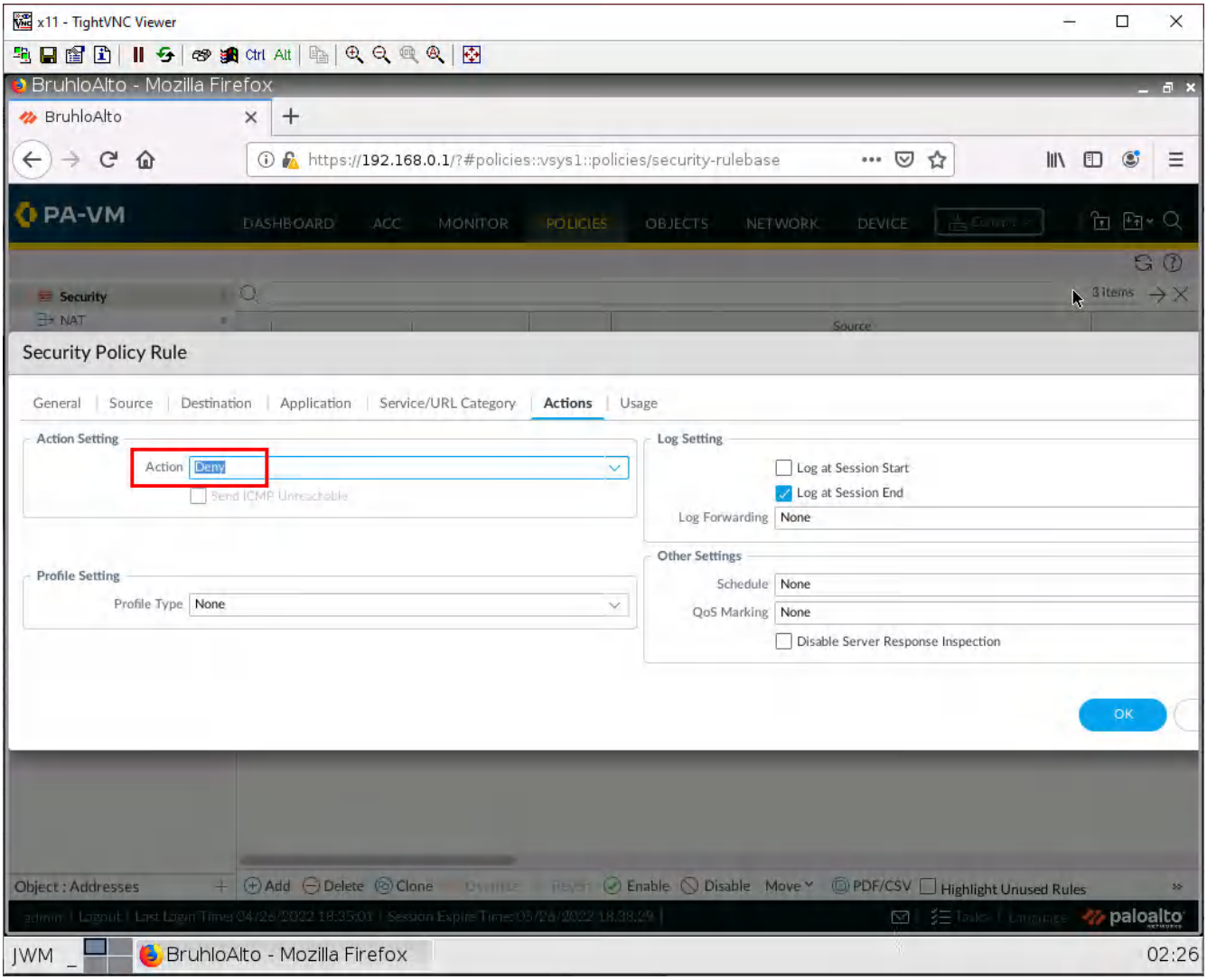


Figure 2.13: Set an Action to Deny

Then click **OK**.

Enable Block Pages

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

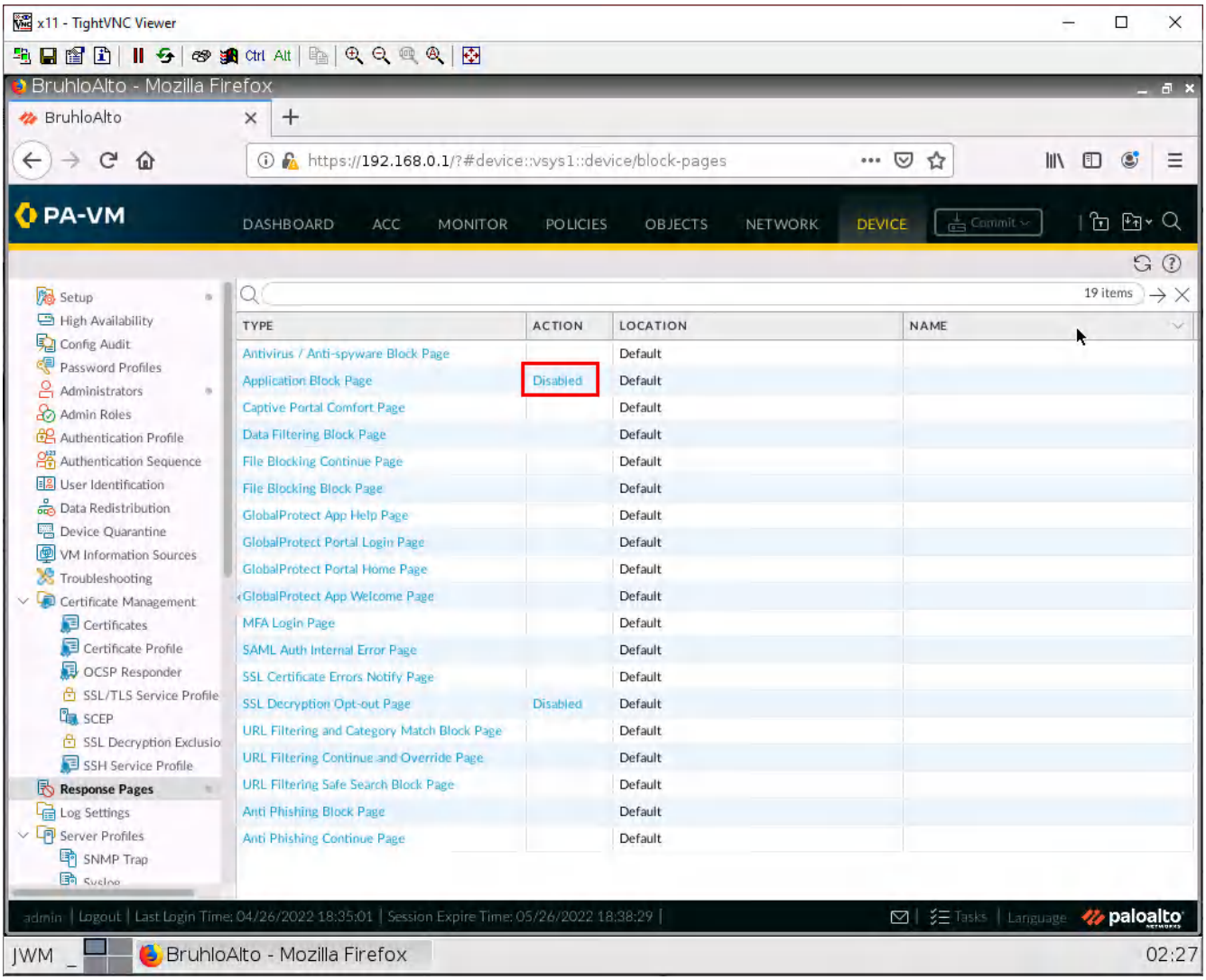


Figure 2.14: Enabling Application Block Page

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

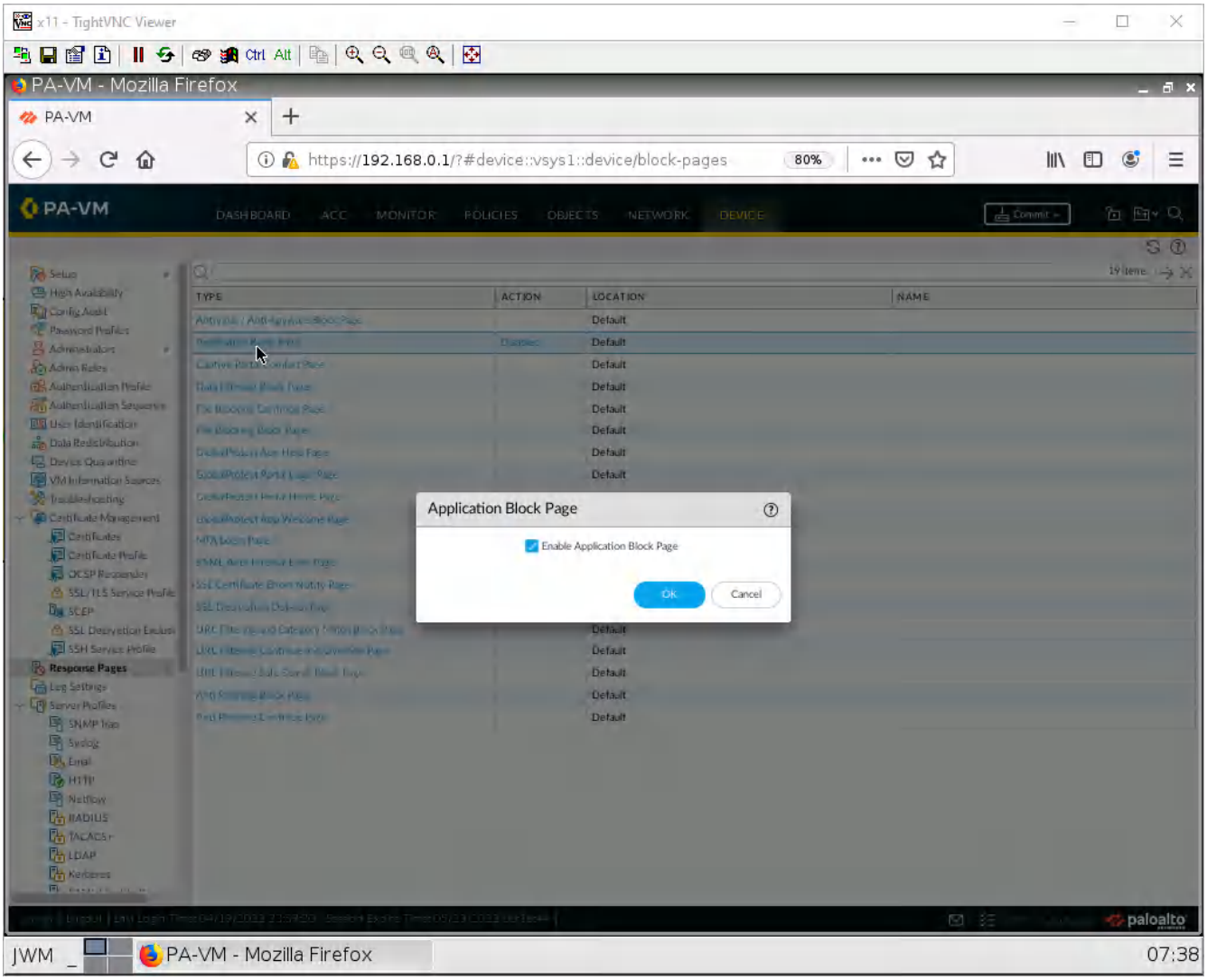


Figure 2.15: Enabling Application Block Page

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.

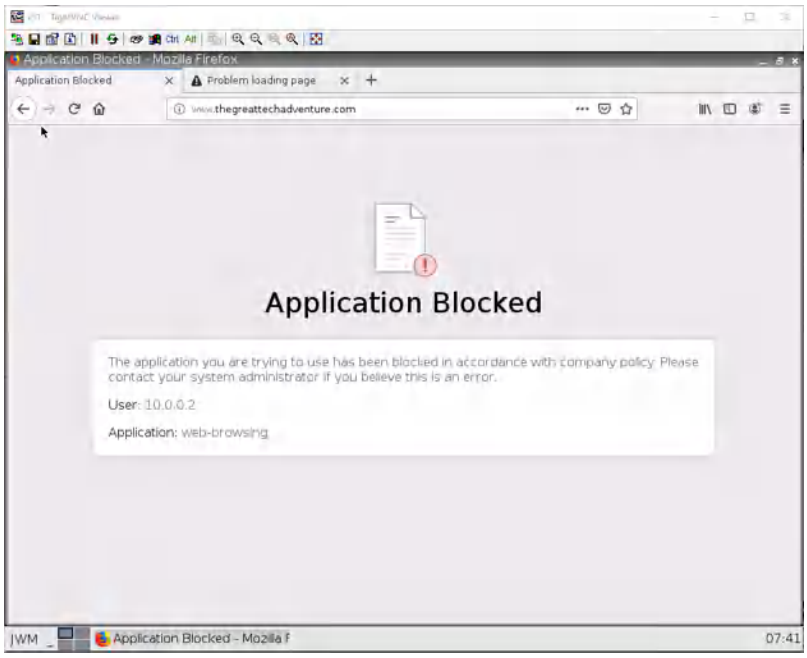


Figure 2.16: Application Block Page

If you see this page, that is alright too!

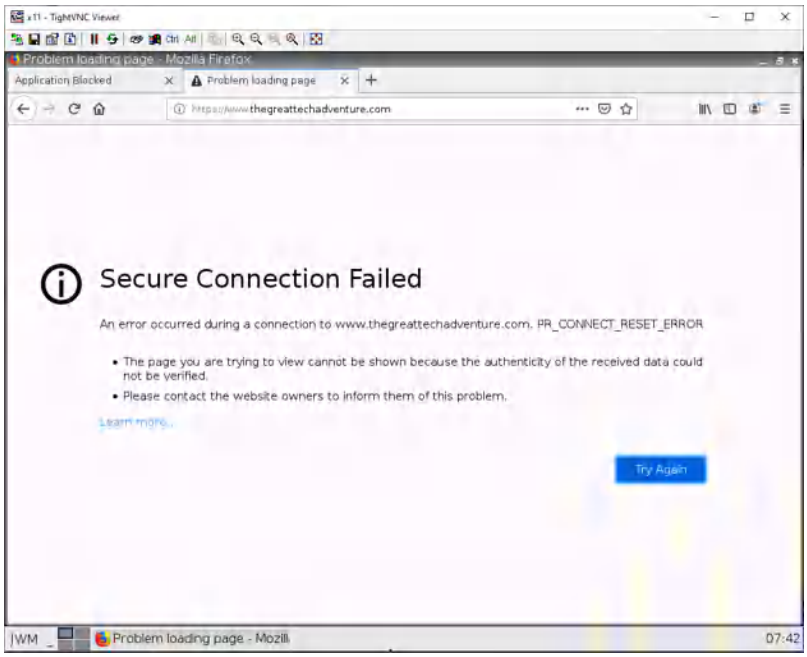


Figure 2.17: Application Block Page

Set Up Kali to Be a Bad Actor

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

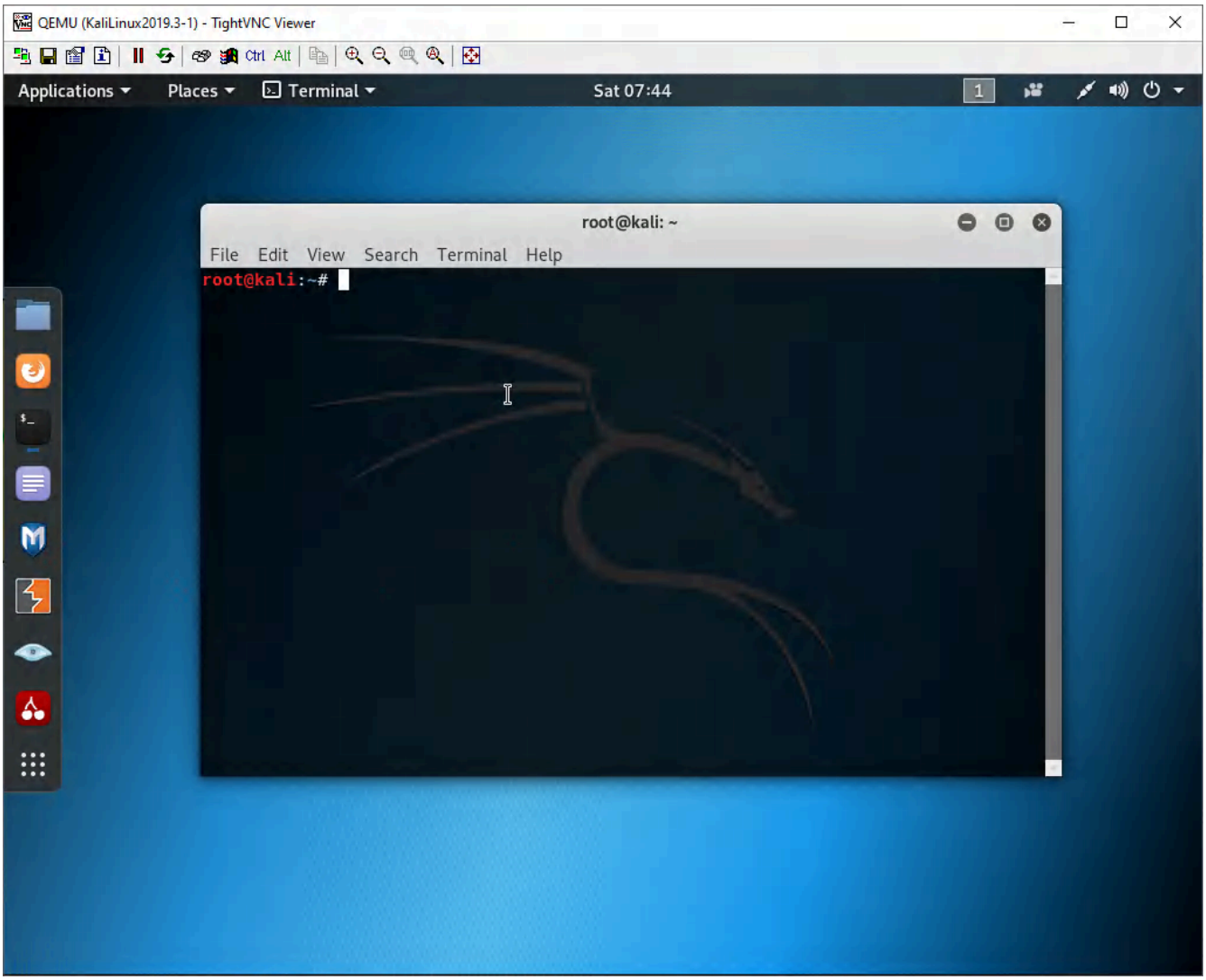


Figure 2.18: Open up Terminal in Kali

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
```

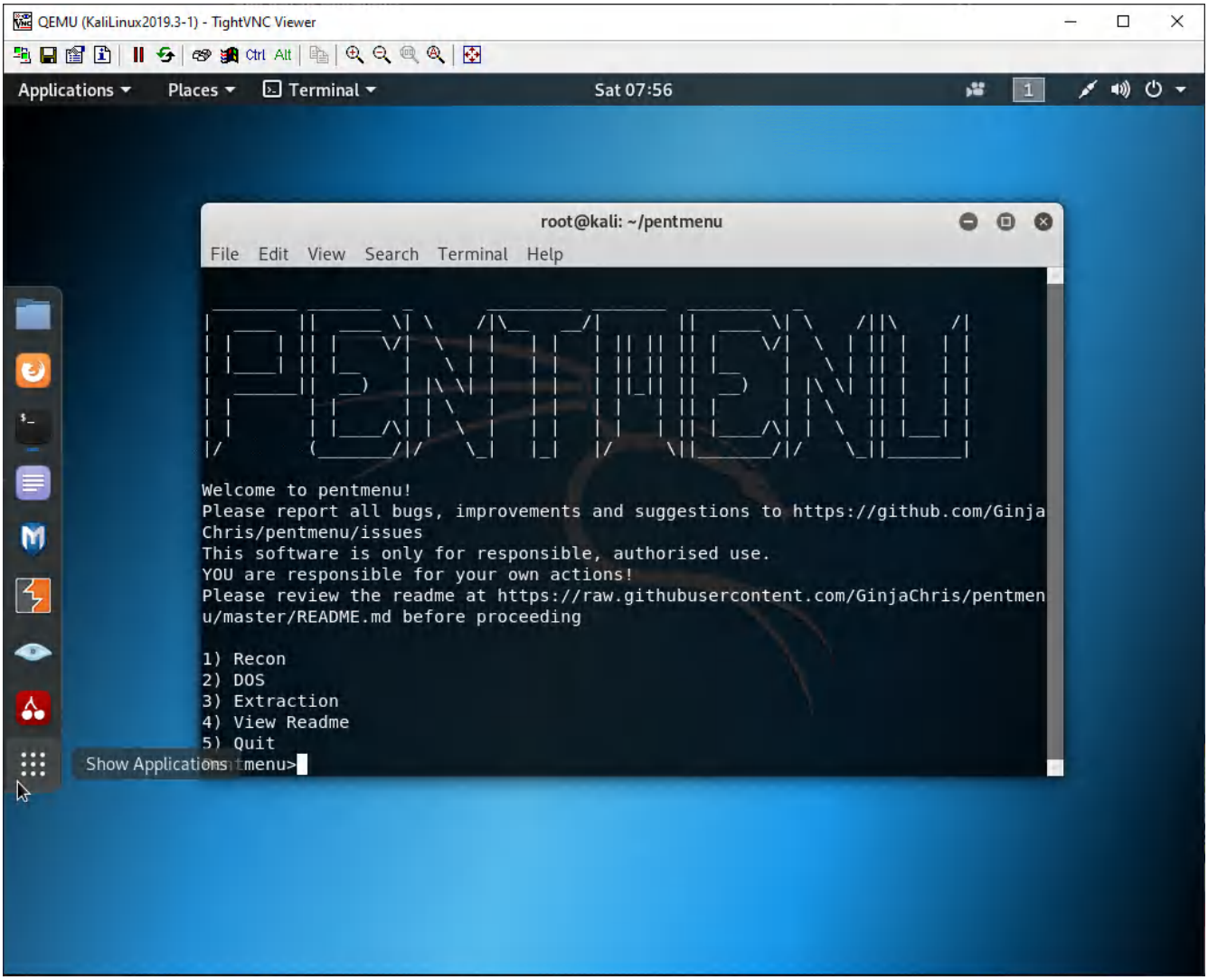


Figure 2.19: PentMenu app

Select option 2 for DoS attack.

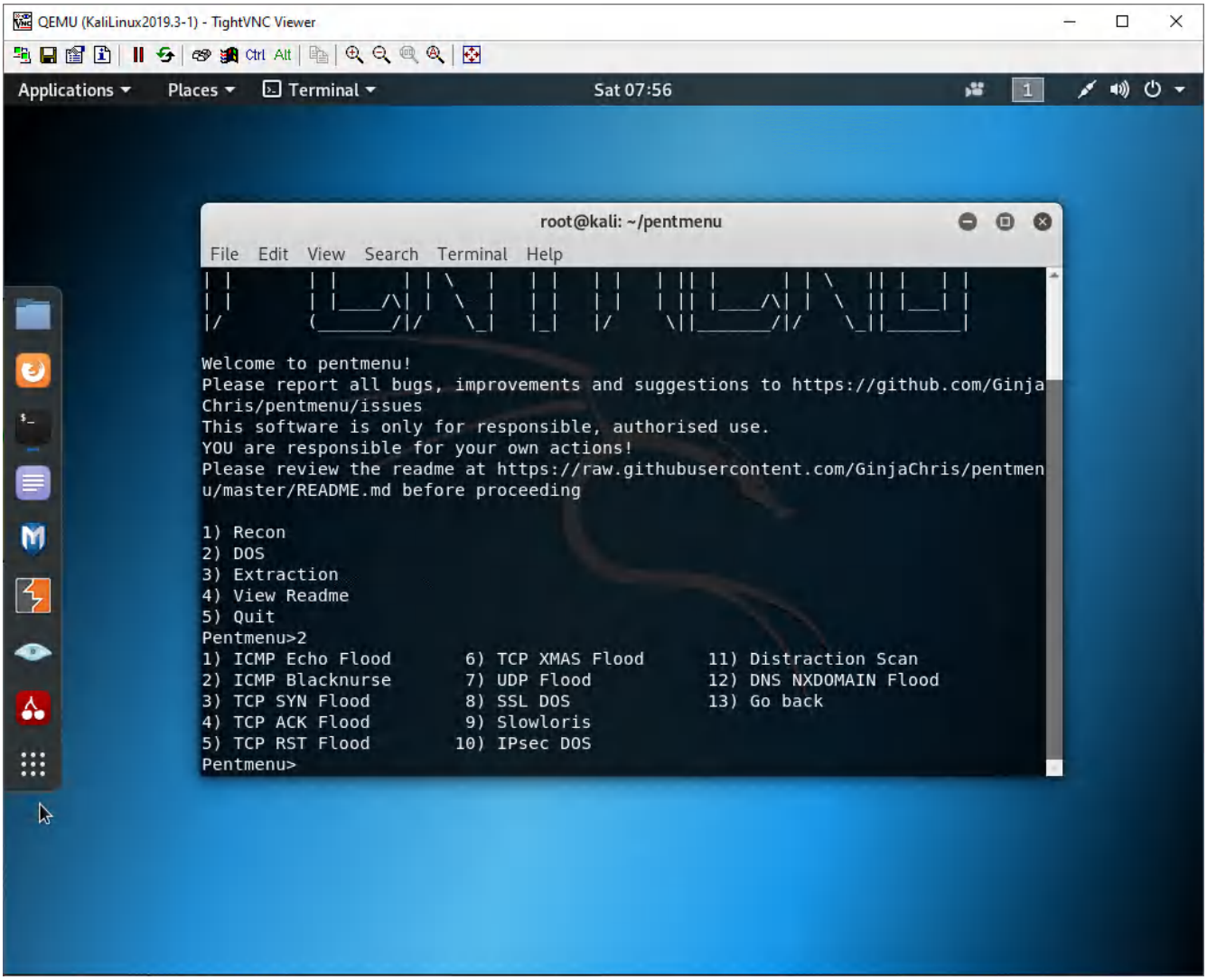


Figure 2.20: PentMenu app – Select DoS (2)

Select option 1 for ICMP Echo Flood.

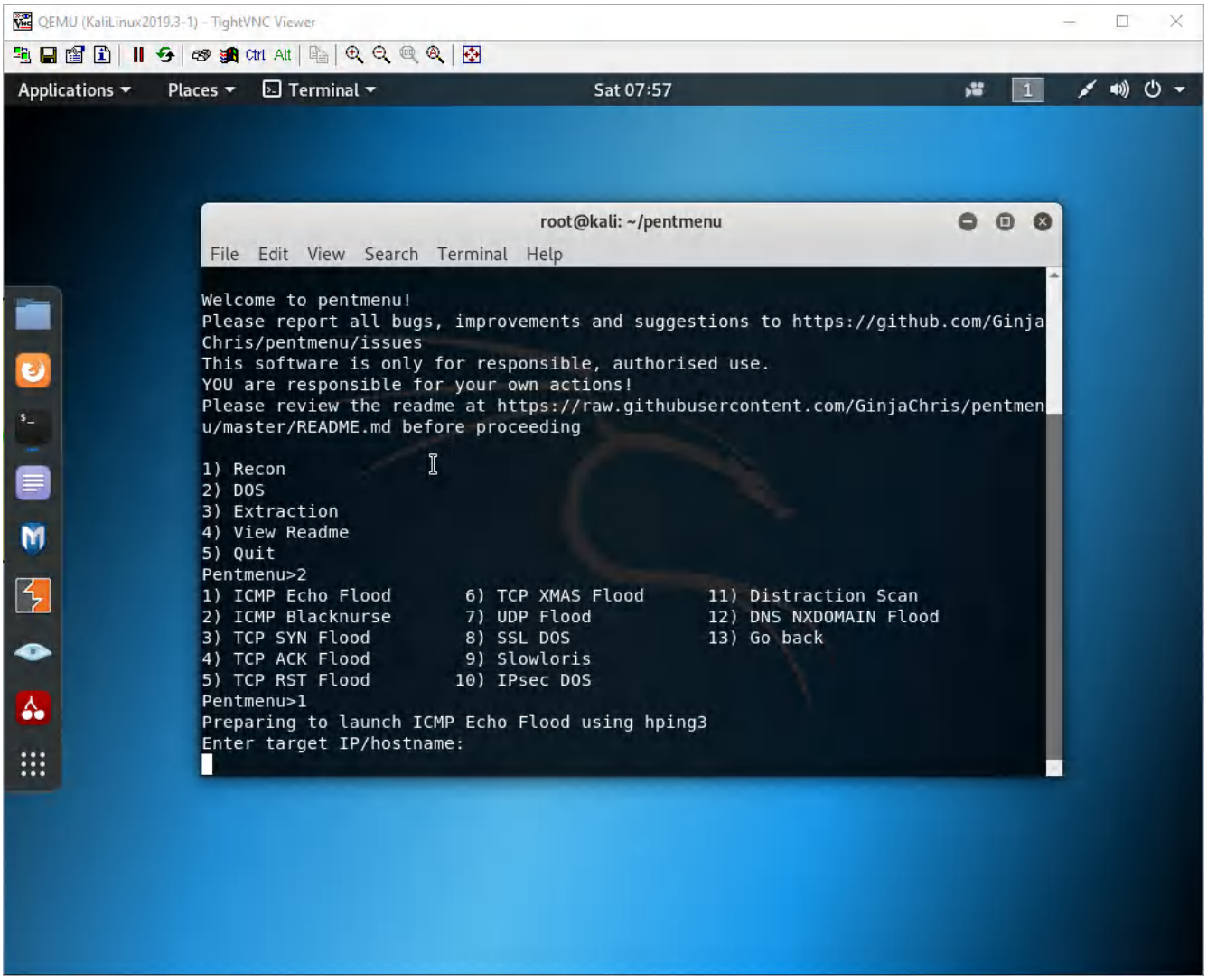


Figure 2.21: PentMenu app – Select ICMP Echo Flood(1)

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

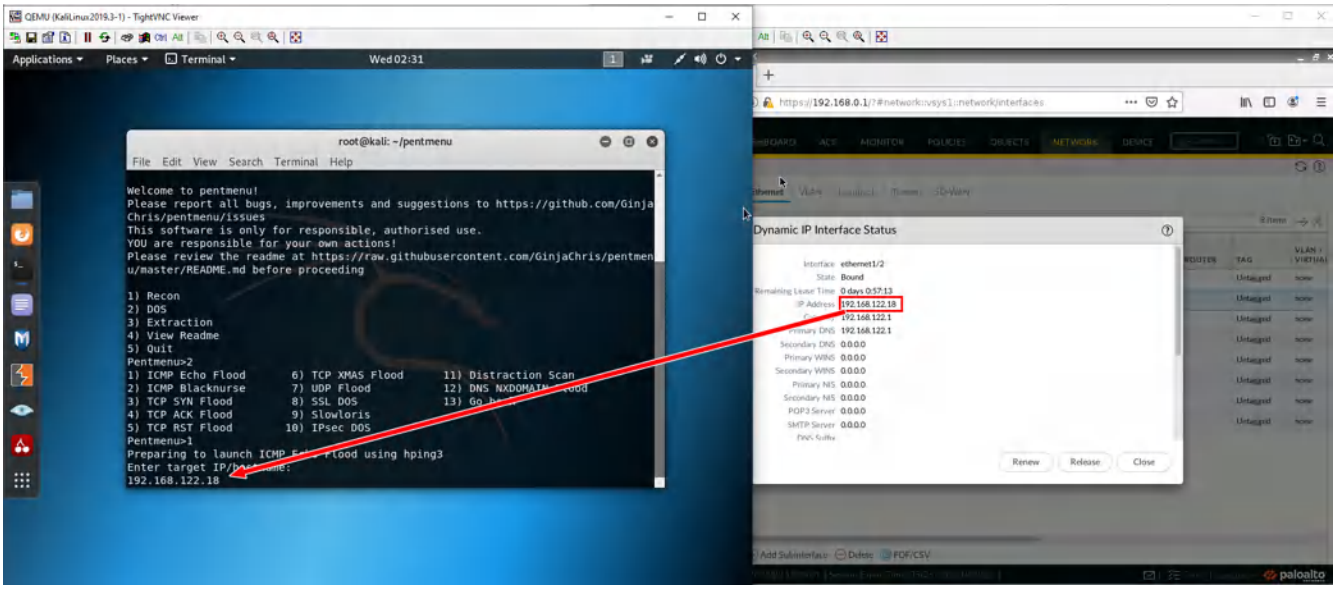


Figure 2.22: PentMenu app – Enter Target IP address

Select r for random IP address.

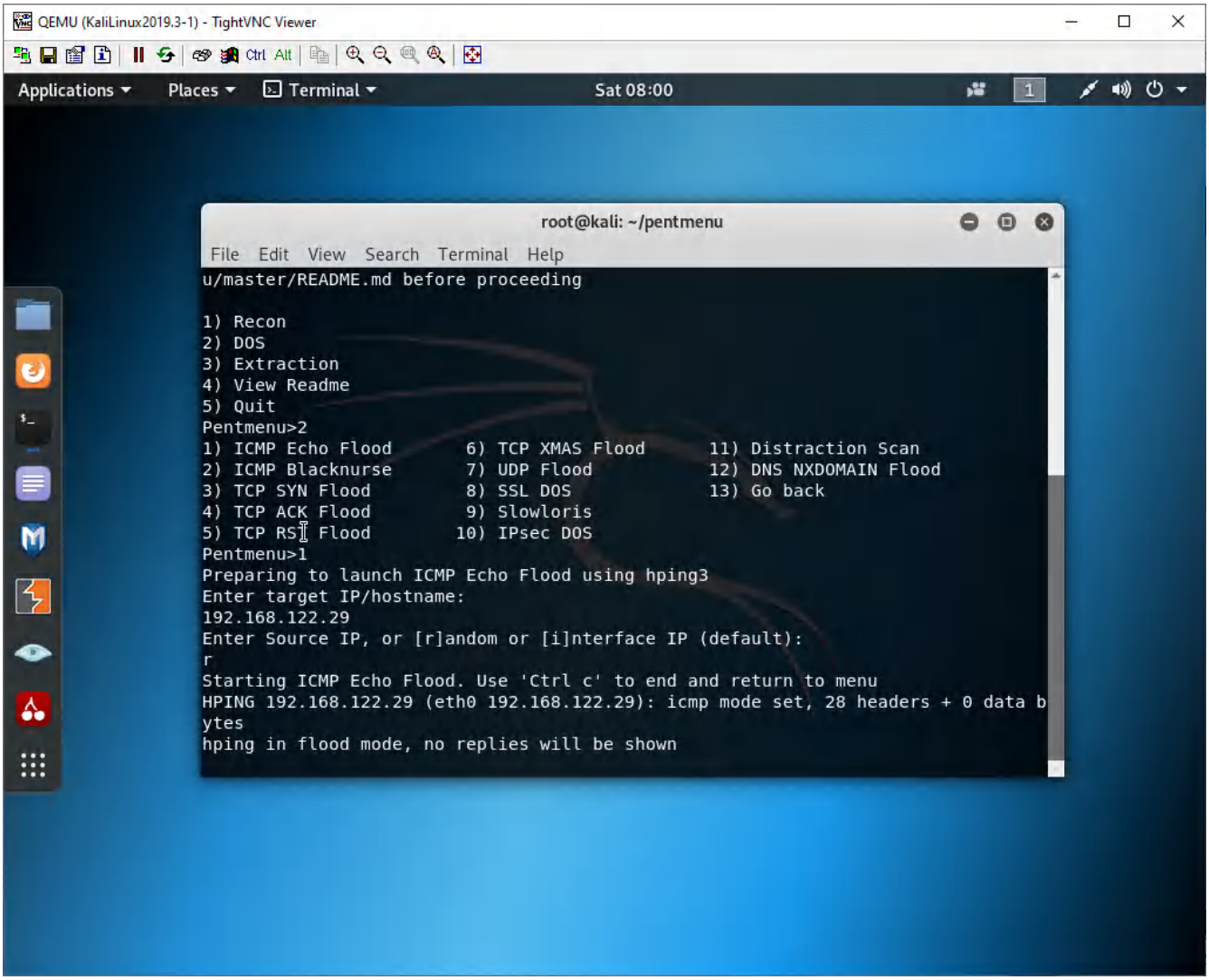


Figure 2.23: PentMenu app – Enter r for random IP address

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

Analyze the ICMP Flood

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

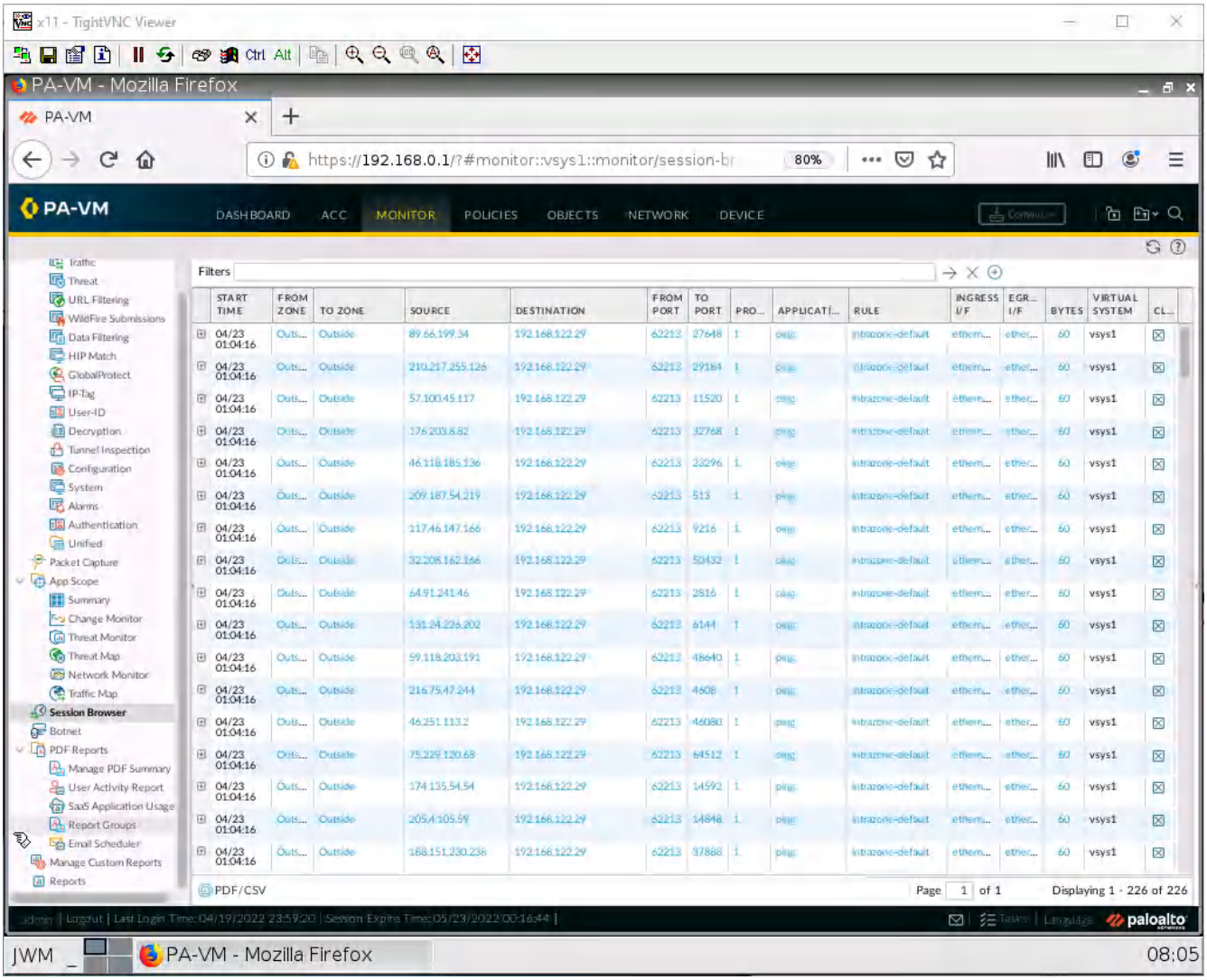


Figure 2.24: Verify session logs

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.

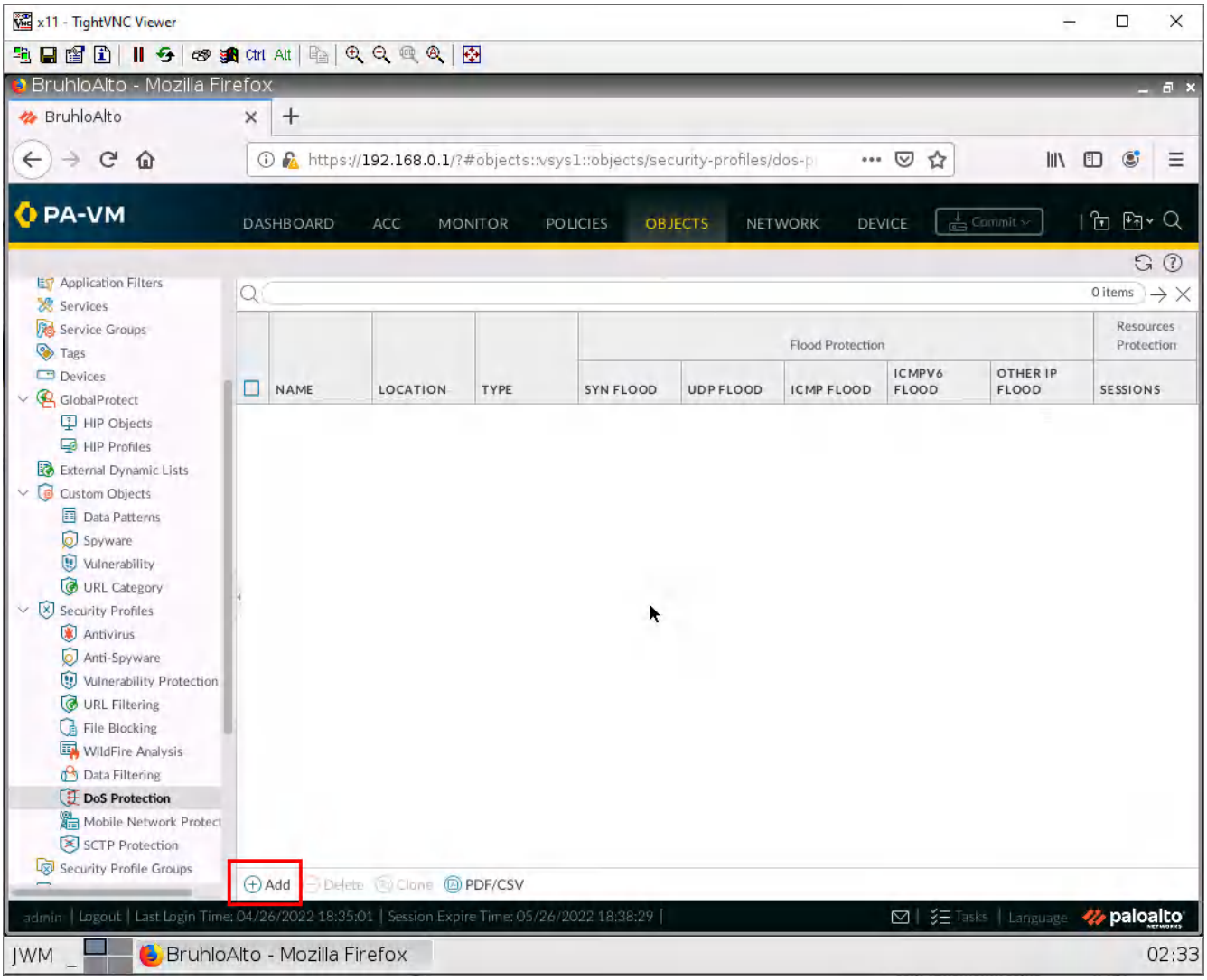


Figure 2.25: Create a DoS Protection

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

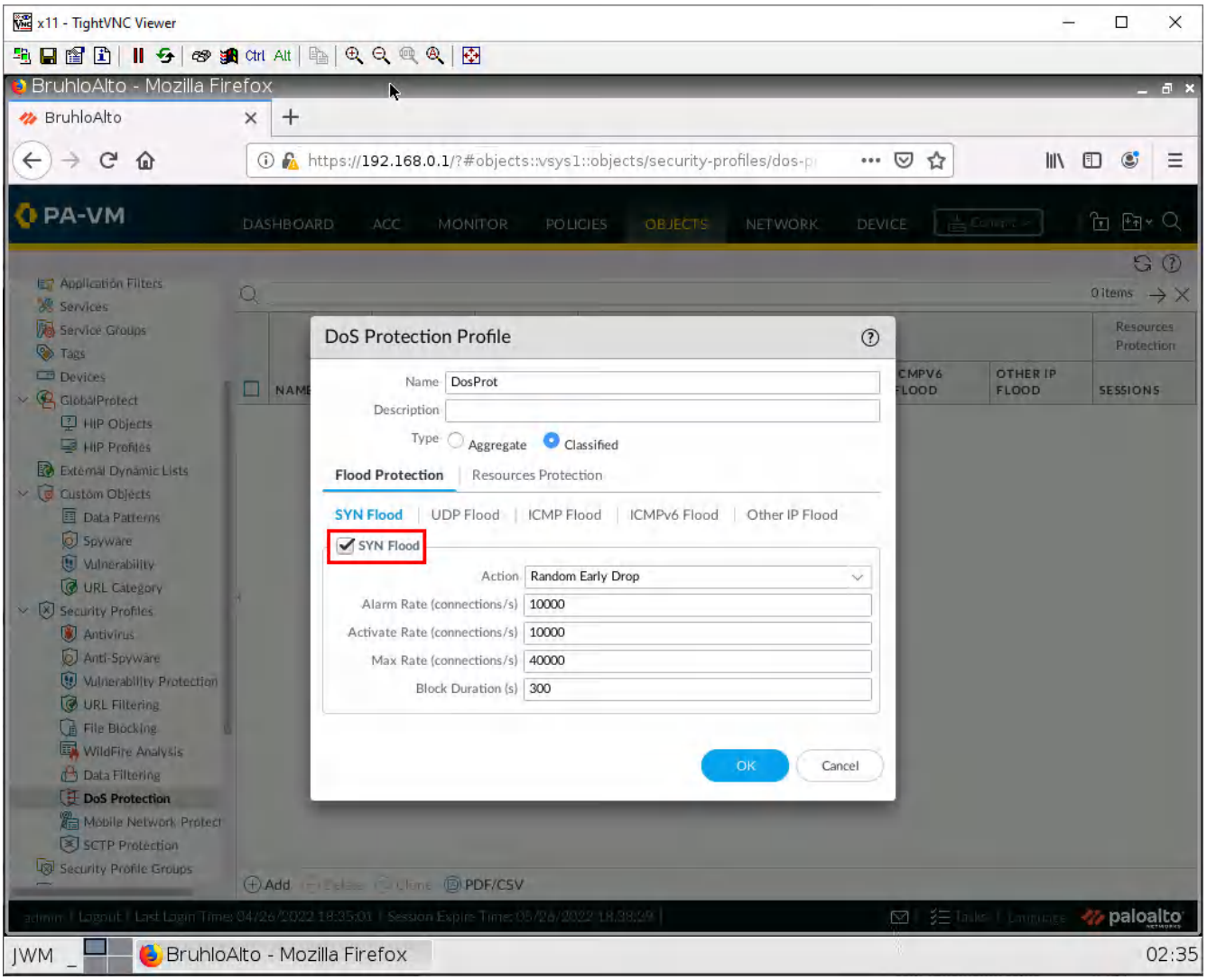


Figure 2.26: SYN Flood Protection

After that, click **OK**.

Apply the DoS Protection Profile

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

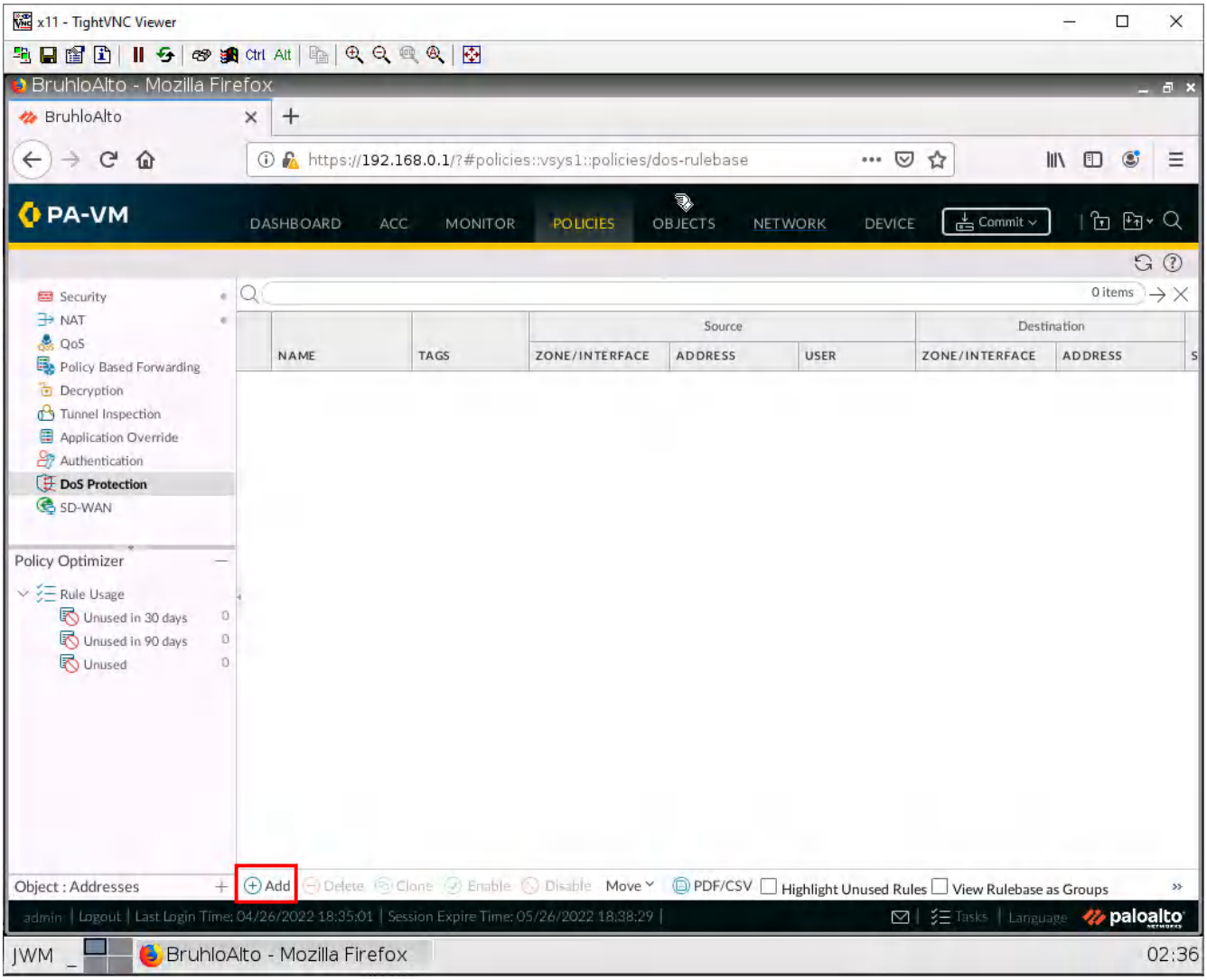


Figure 2.27: Add a DoS Protection Rule

Under the Source tab, add the Outside zone.

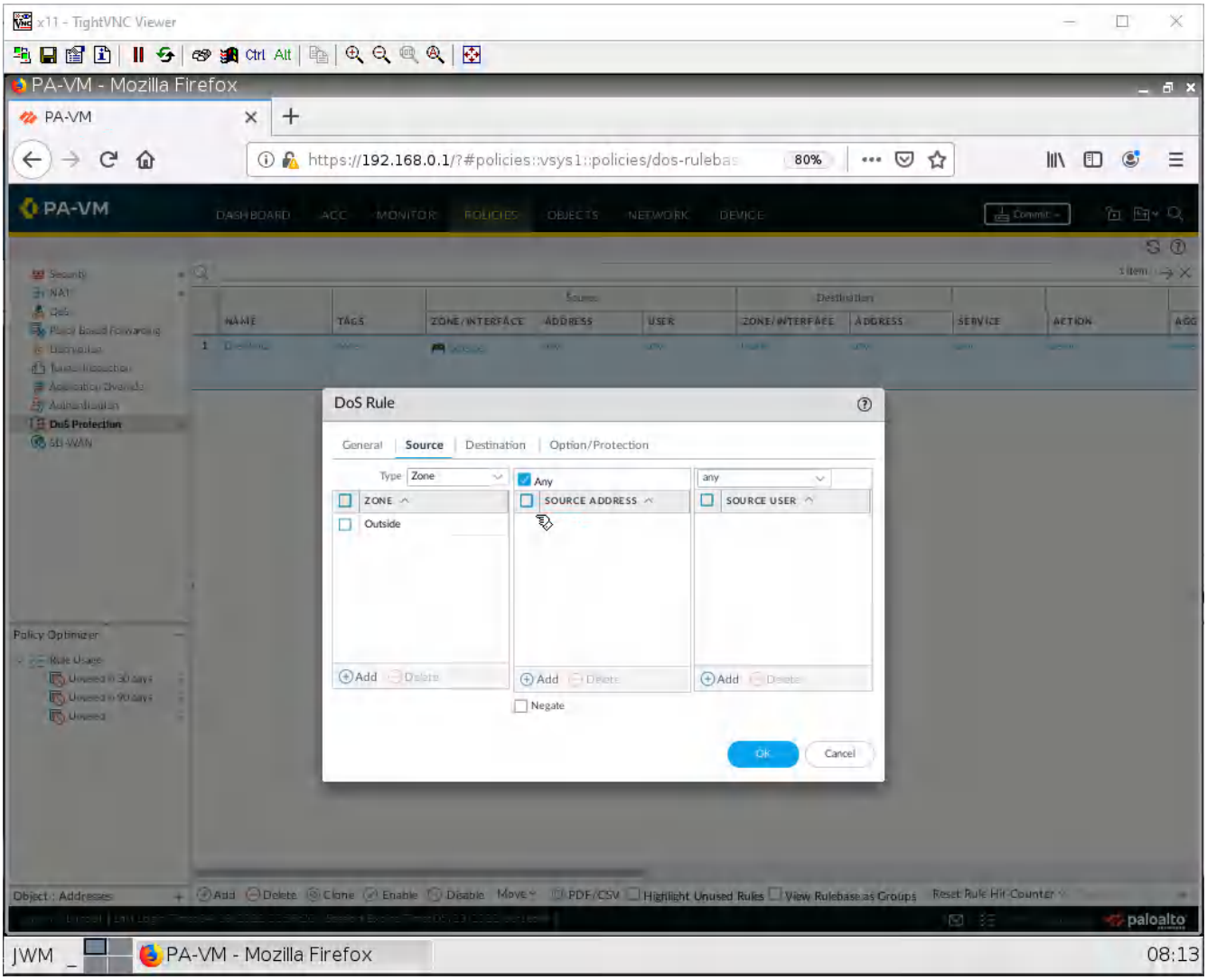


Figure 2.28: Add the Source Zone

Under the Destination tab, add the Inside zone.

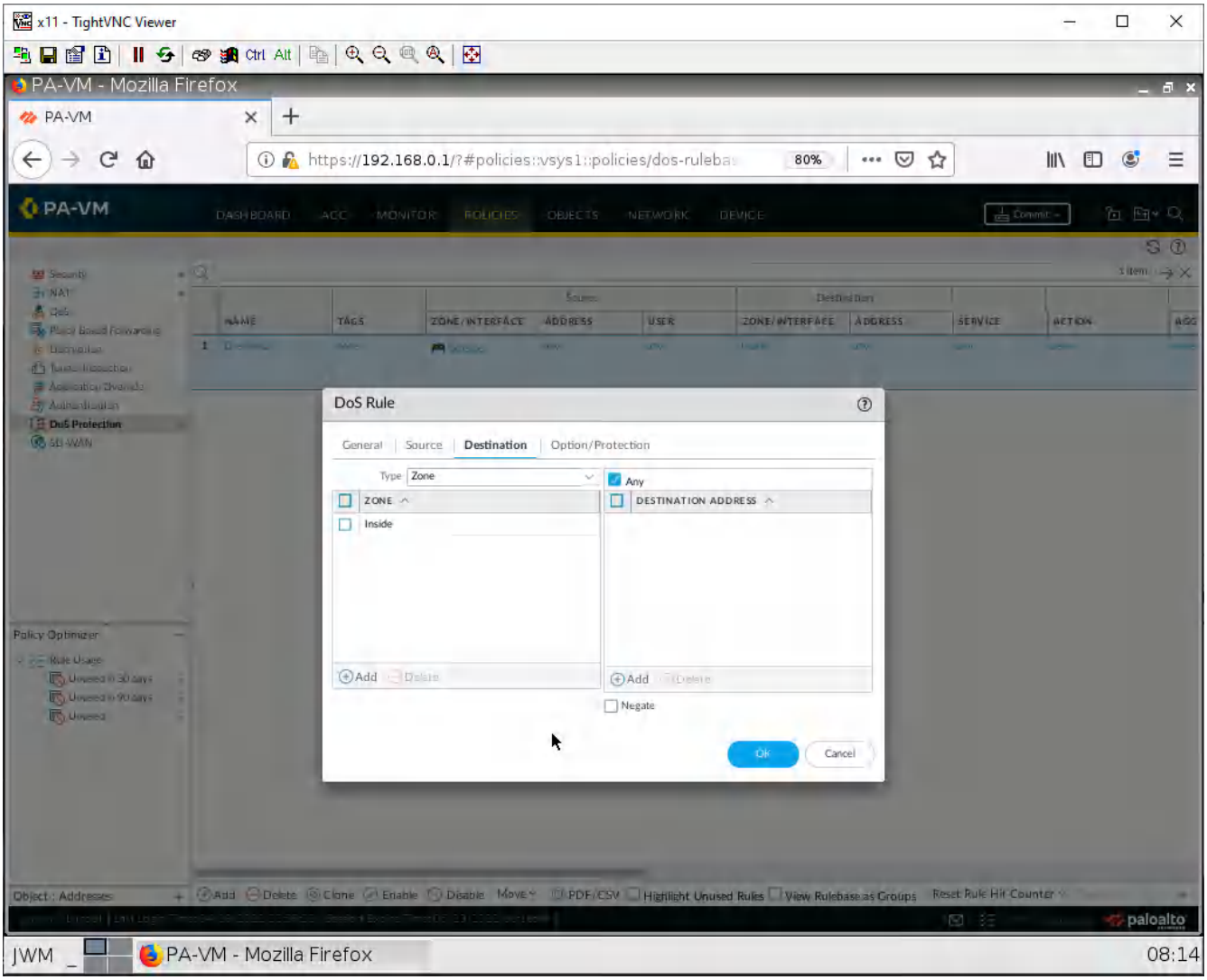


Figure 2.29: Add the Destination Zone

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	*Tick this box*
Profile	*The name of the one you created*
Address	source-IP-only

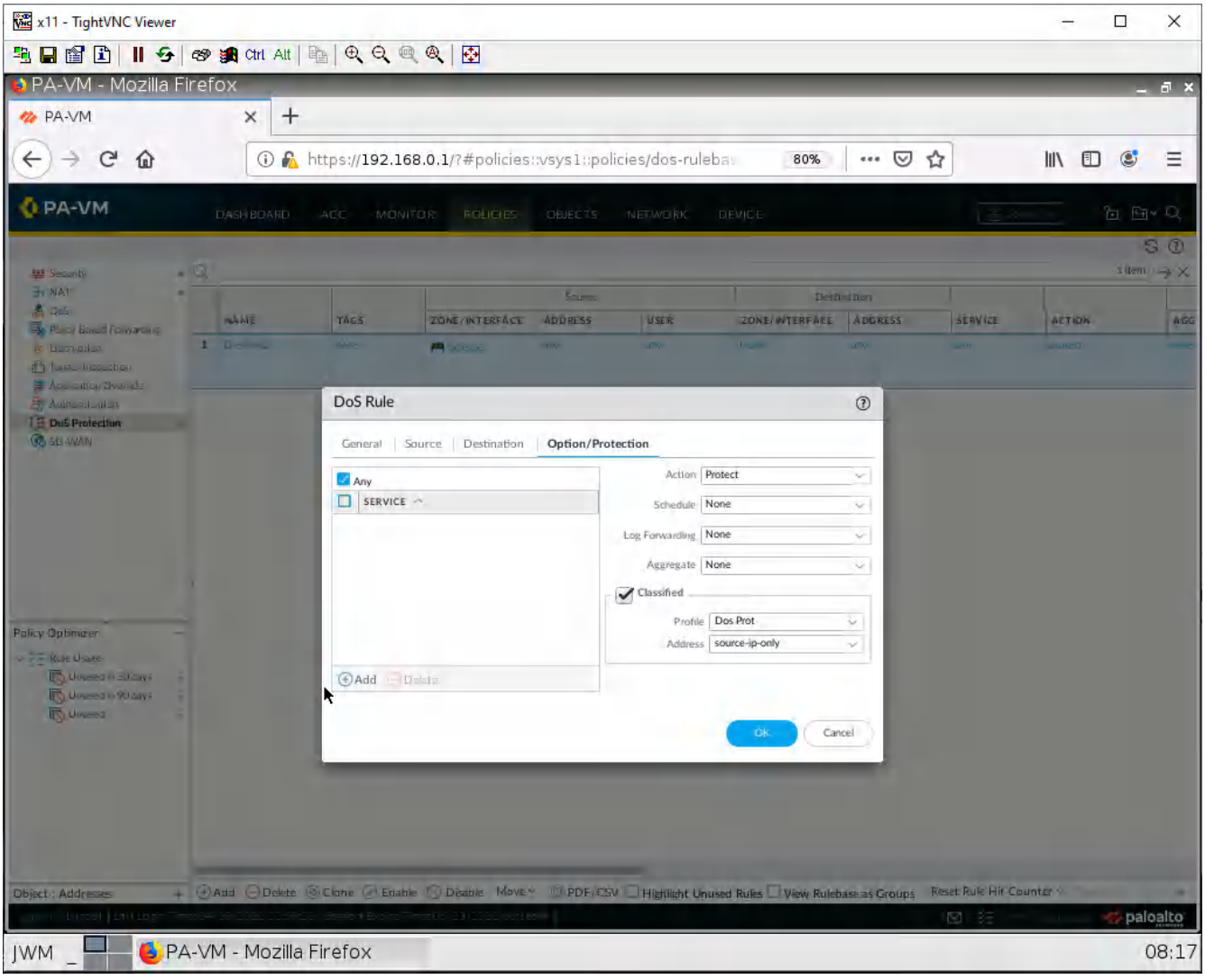


Figure 2.30: DoS Rule – Option/Policies

Then click **OK**.

Create a Zone Protection Profile

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

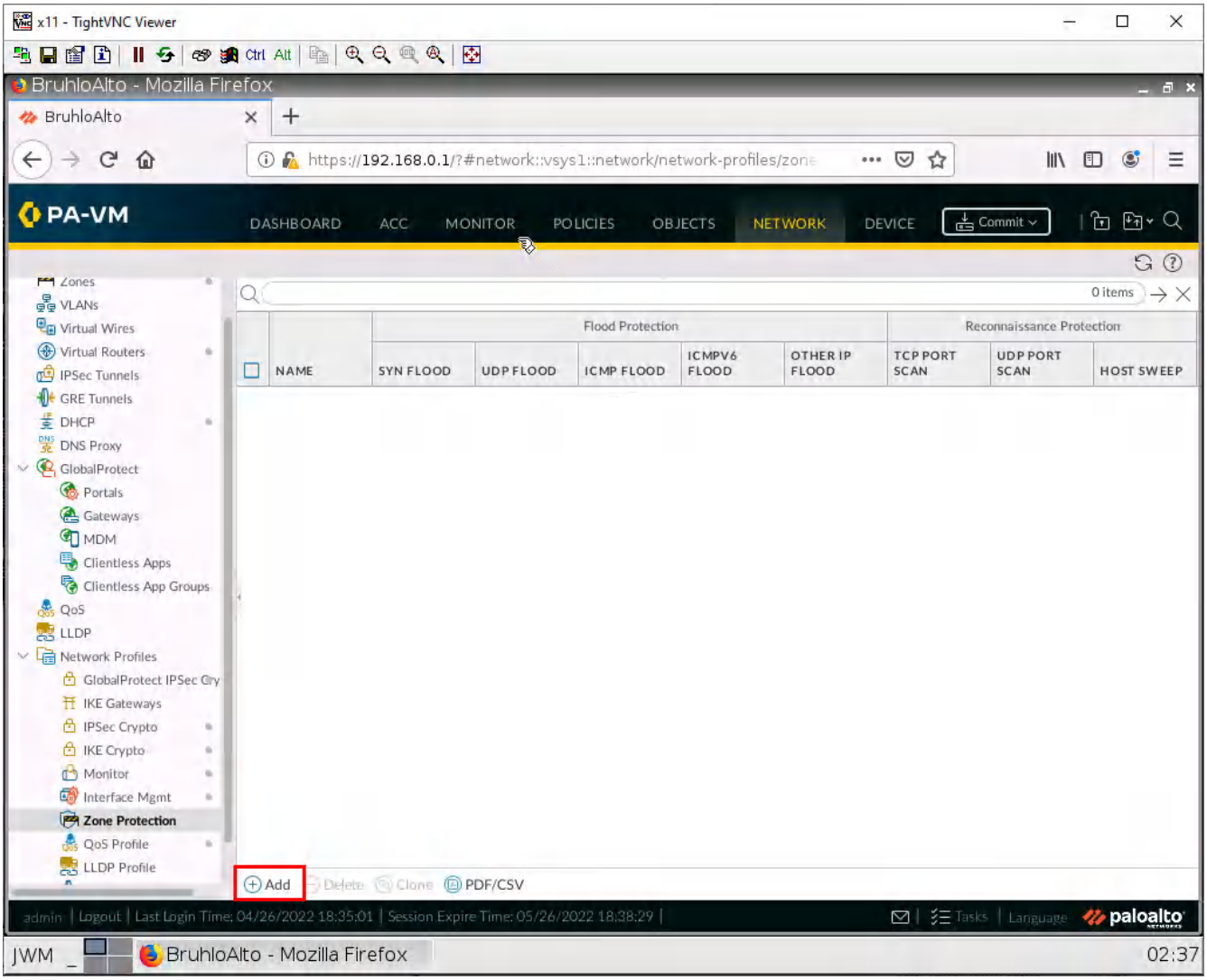


Figure 2.31: Add a Zone Protection

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

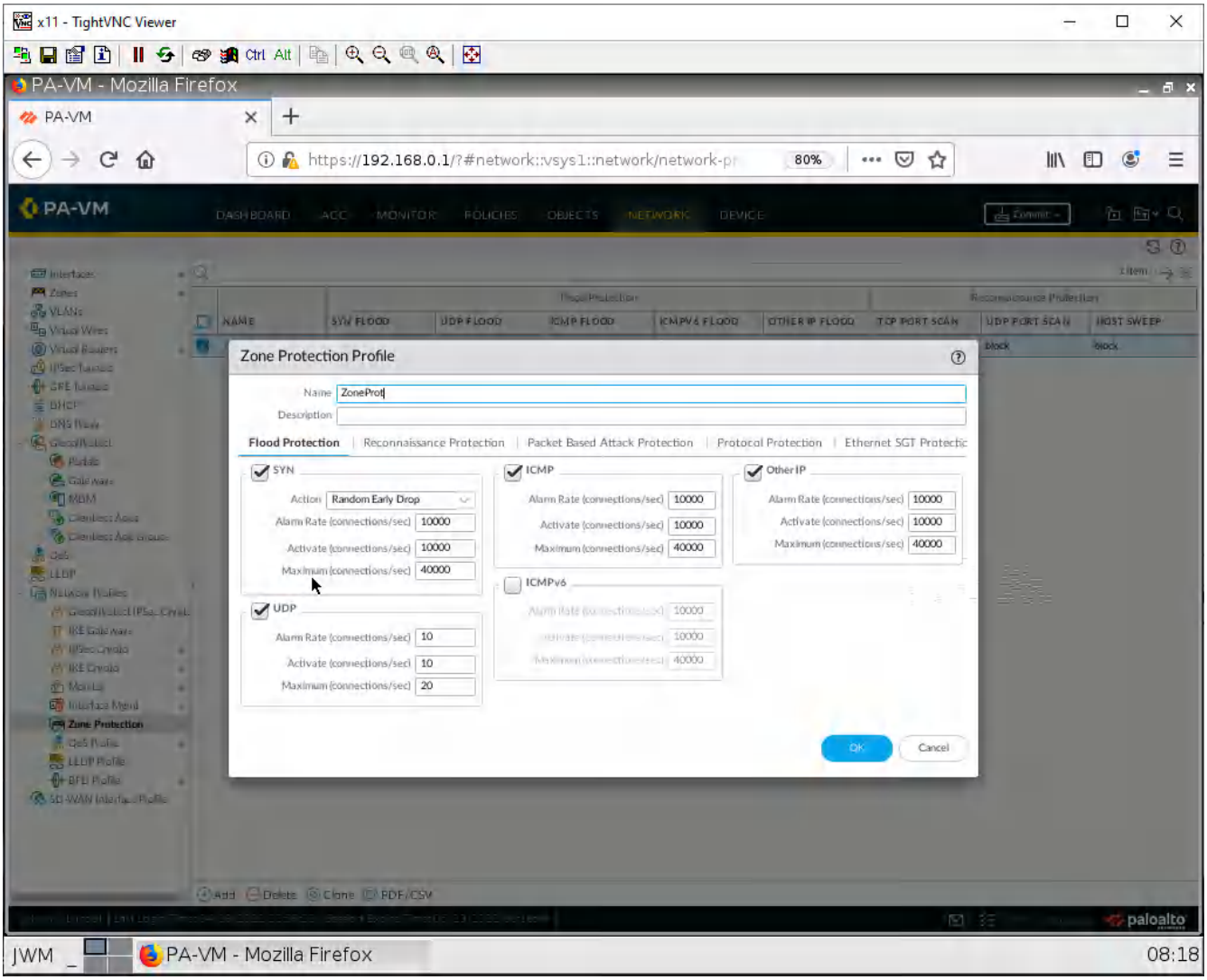


Figure 2.32: Add a Flood Protection

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

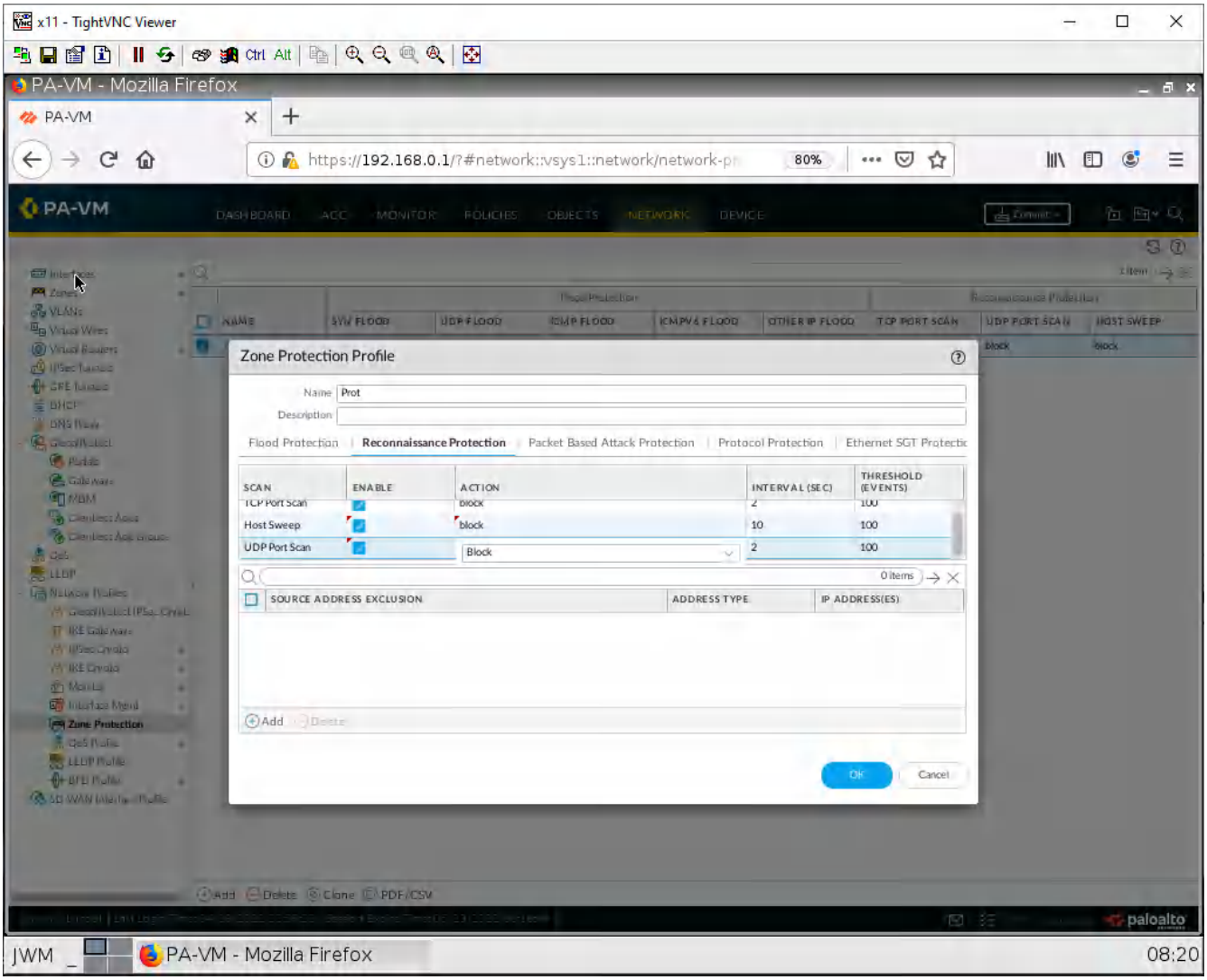


Figure 2.33: Set UDP Port Scan

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

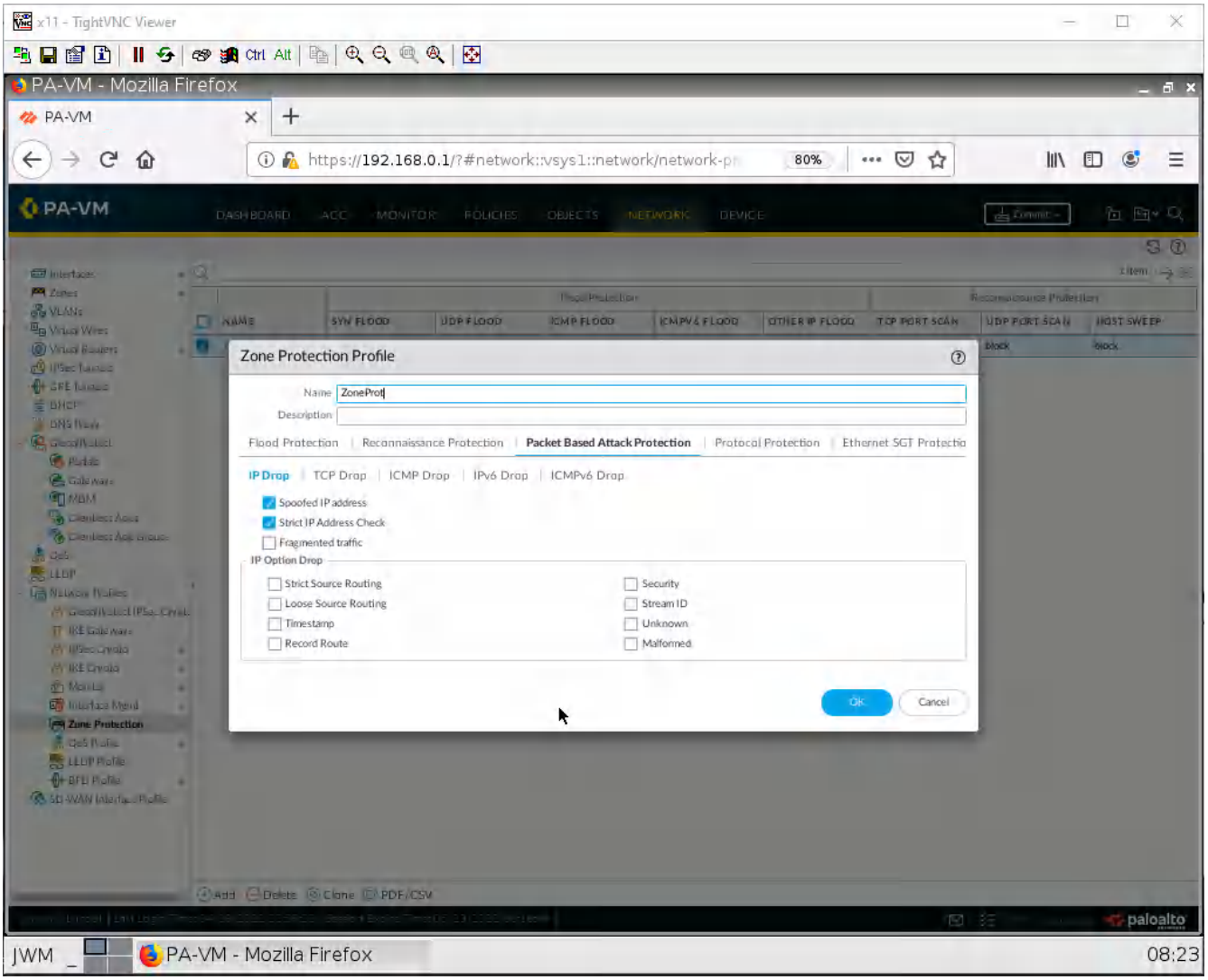


Figure 2.34: Enable Spoof IP address and Strict Address Check

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

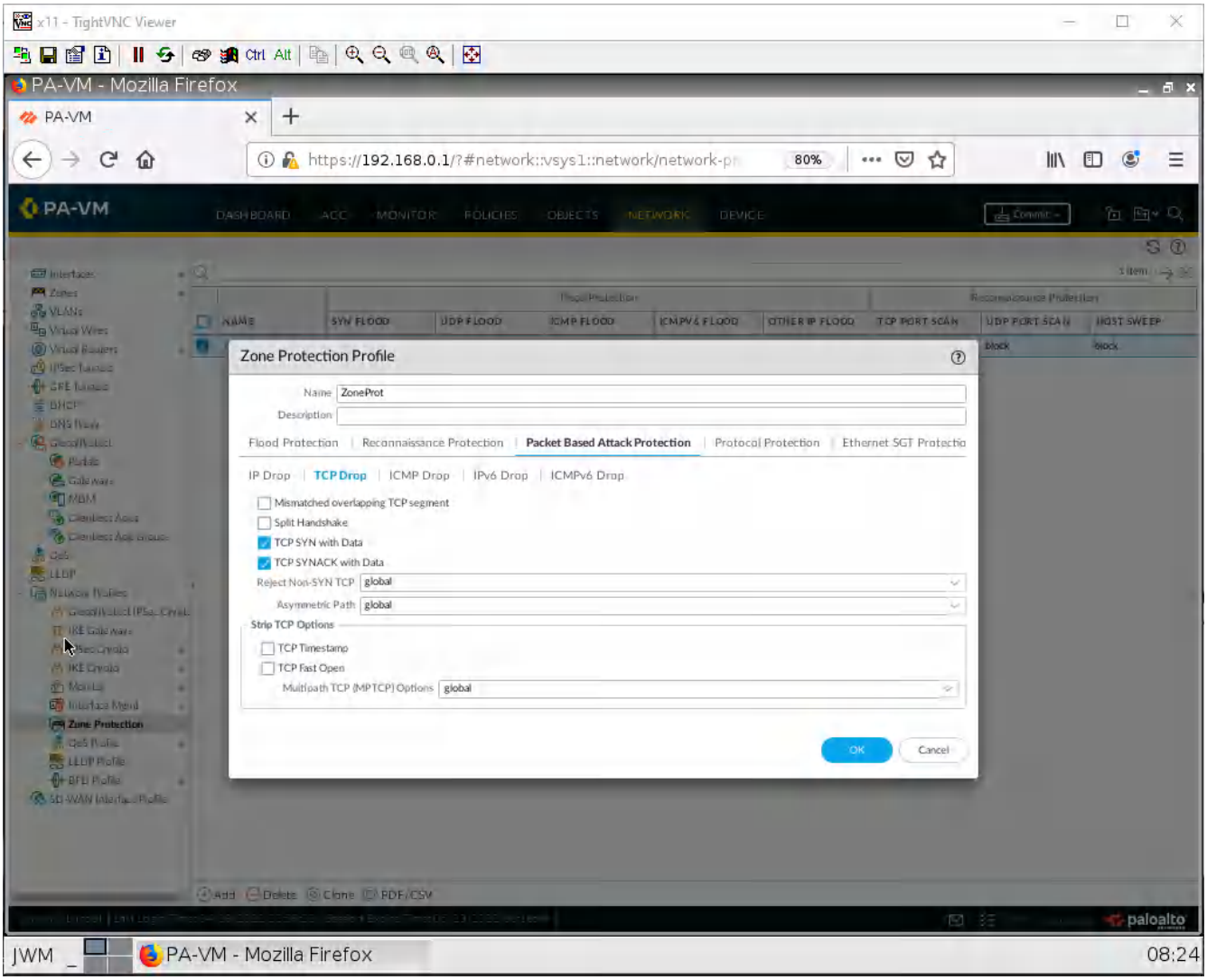


Figure 2.35: Enable TCP SYN with Data

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).**

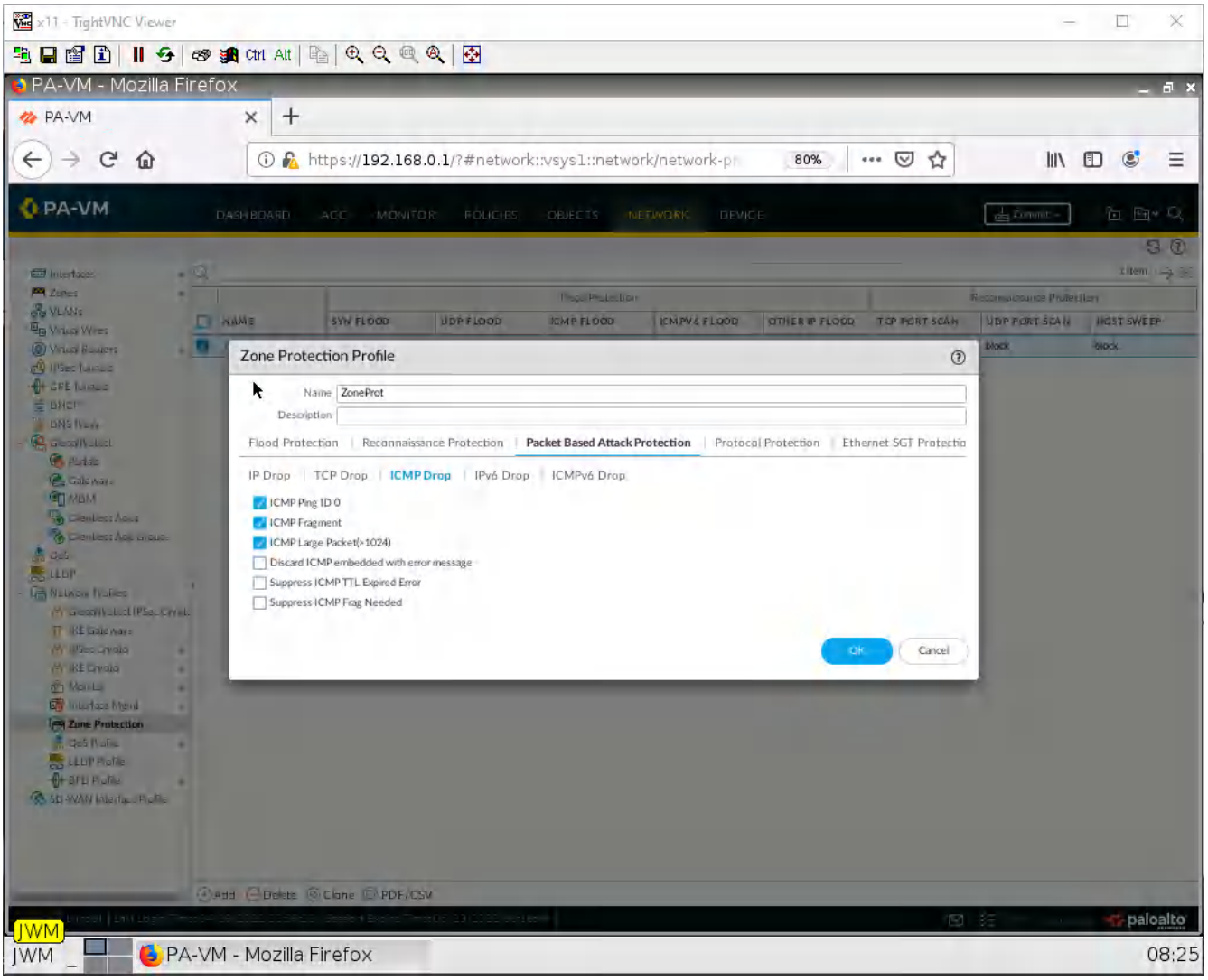


Figure 2.36: Enable ICMP Ping ID 0, ICMP Fragment

Then click **OK**.

Apply a Zone Protection Profile

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

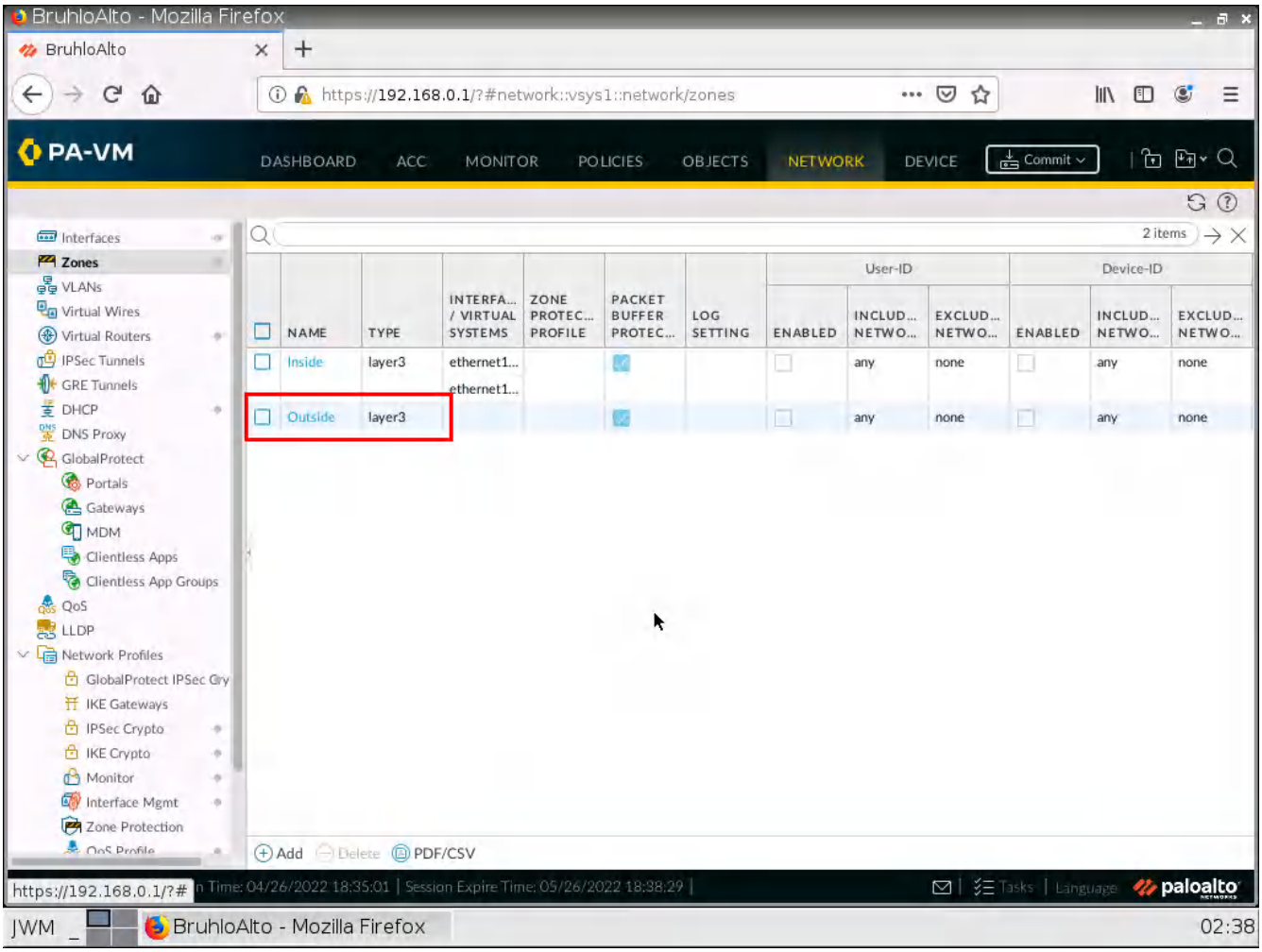


Figure 2.37: Create an Outside zone

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

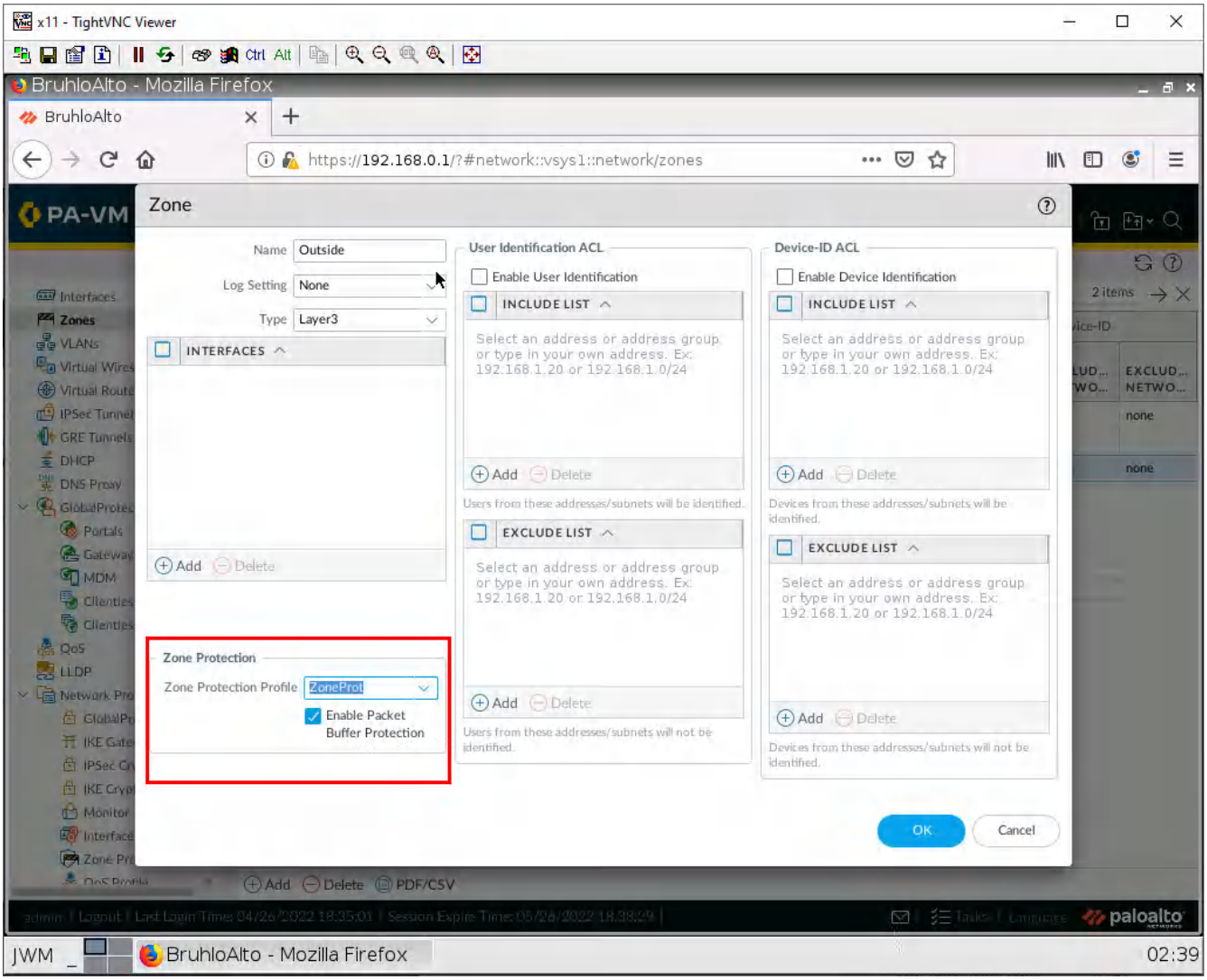


Figure 2.38: Enable Zone Protection under Outside Zone

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.

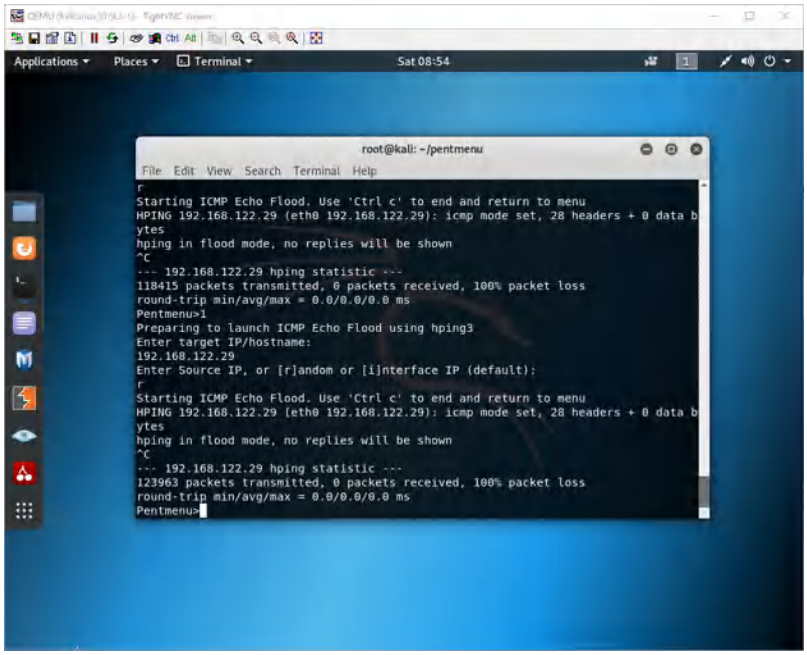


Figure 2.39: Running PentMenu

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

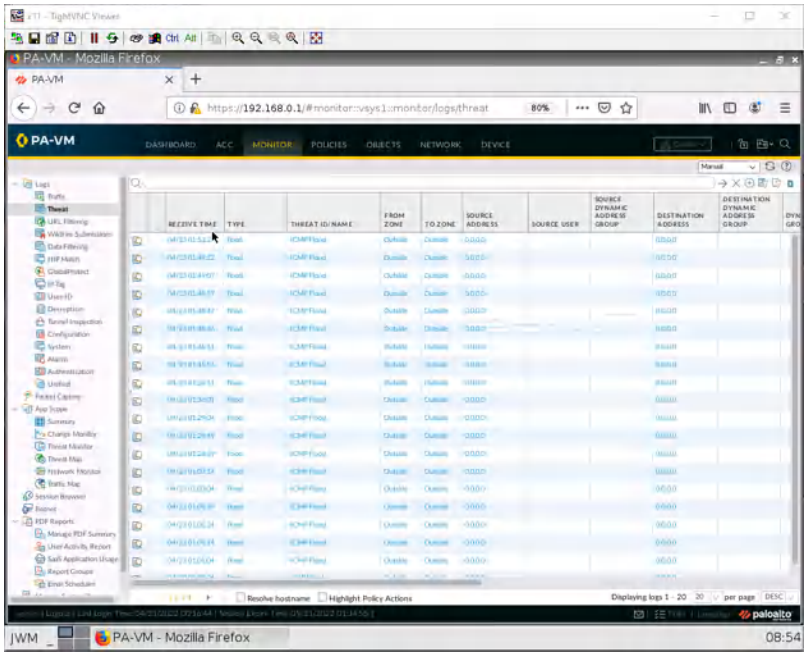


Figure 2.40: Verify logs

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

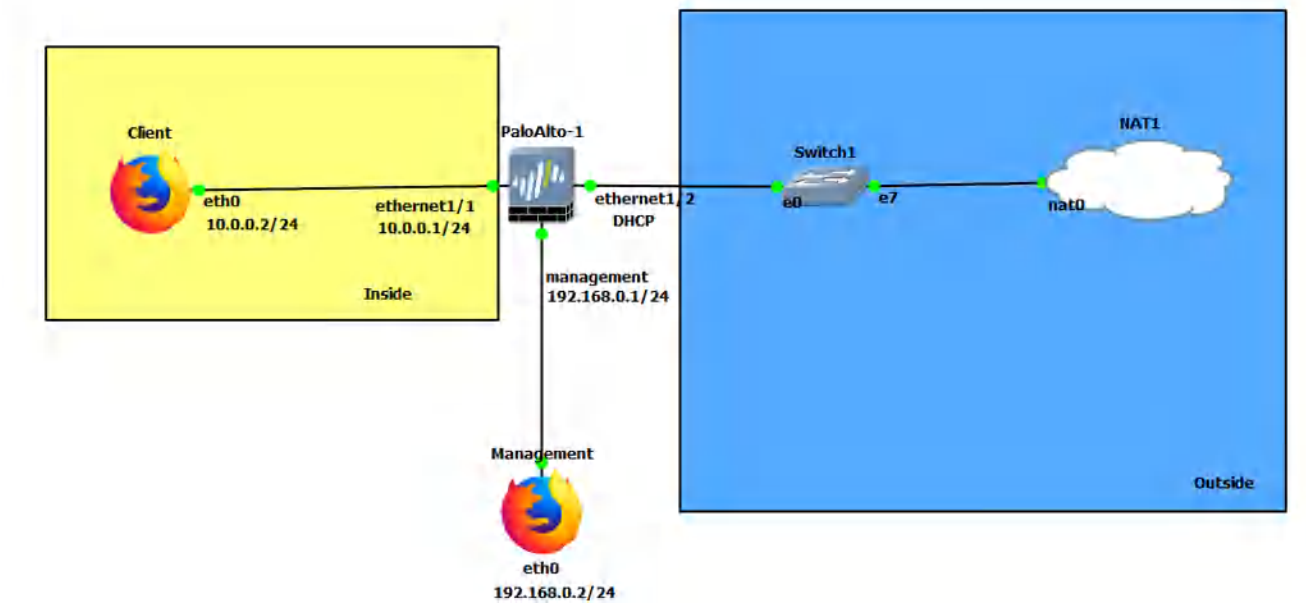


Figure 2.41: Main scenario

Table 2.6: Addressing Table

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

Table 2.7: Zone Configuration

Zone	**Interface**
Inside	Ethernet1/1
Outside	Ethernet1/2

Create an Antivirus Profile

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

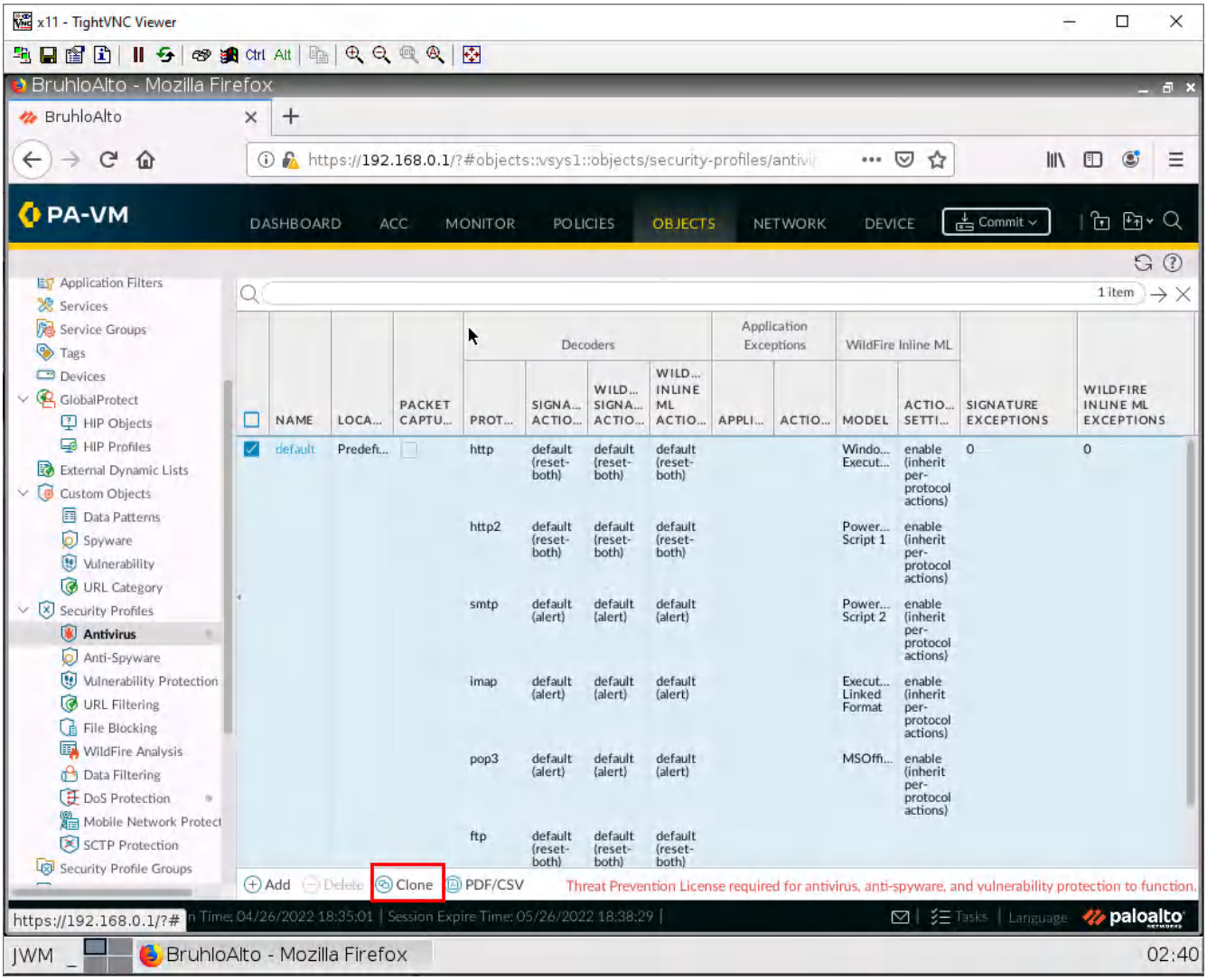


Figure 2.42: Creating an Antivirus Profile

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

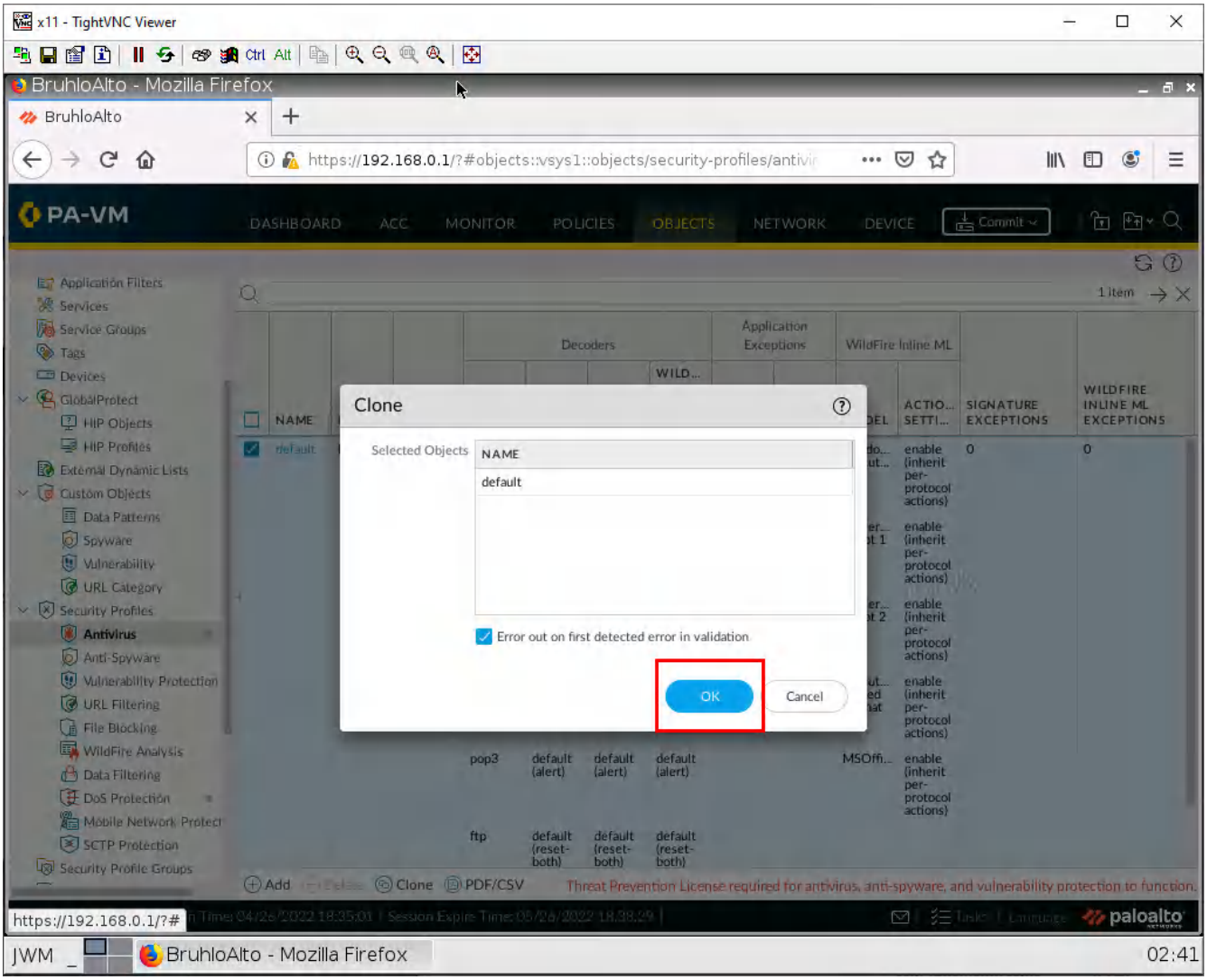


Figure 2.43: Cloning the Antivirus profile

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

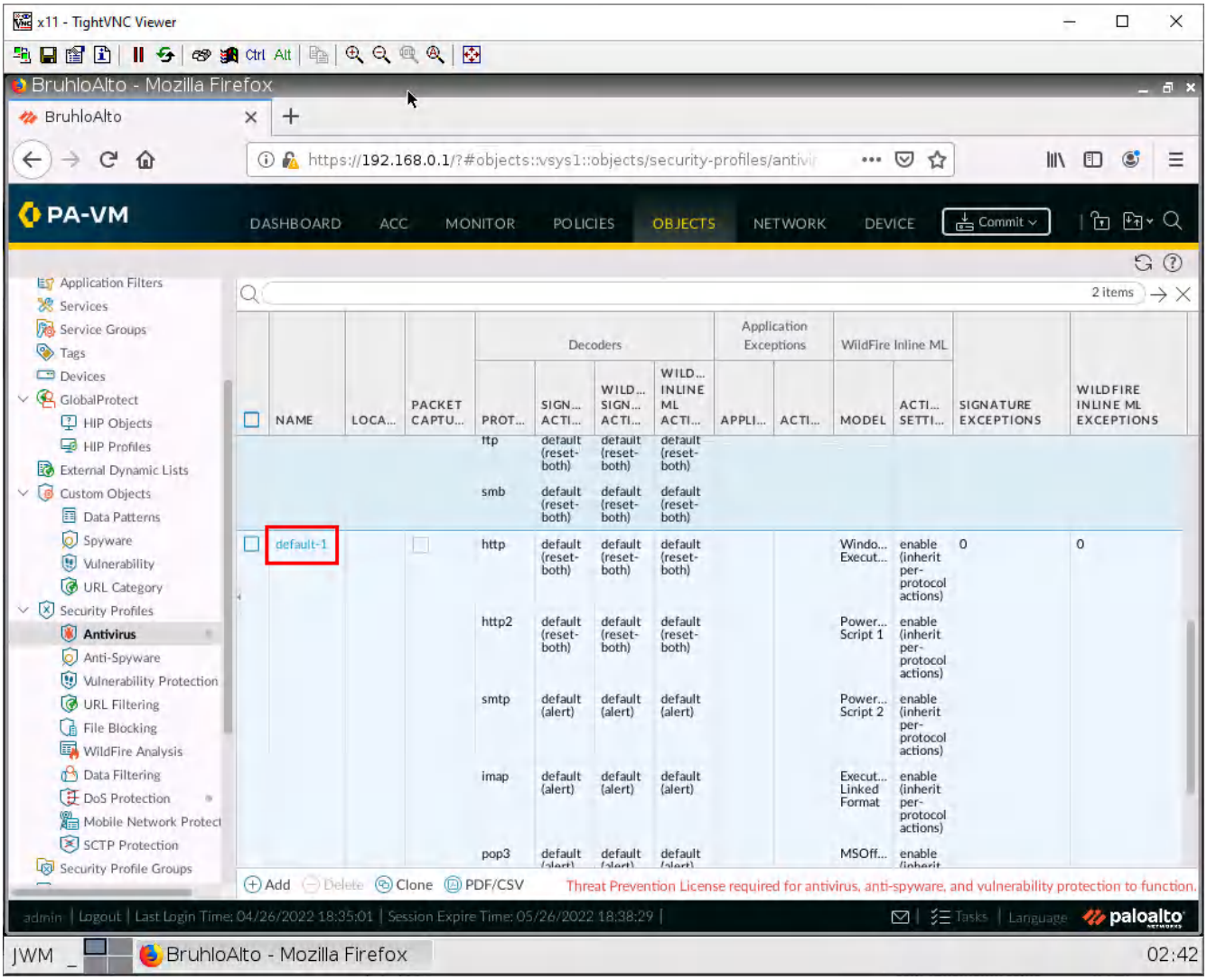


Figure 2.44: Verify the Antivirus profile

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

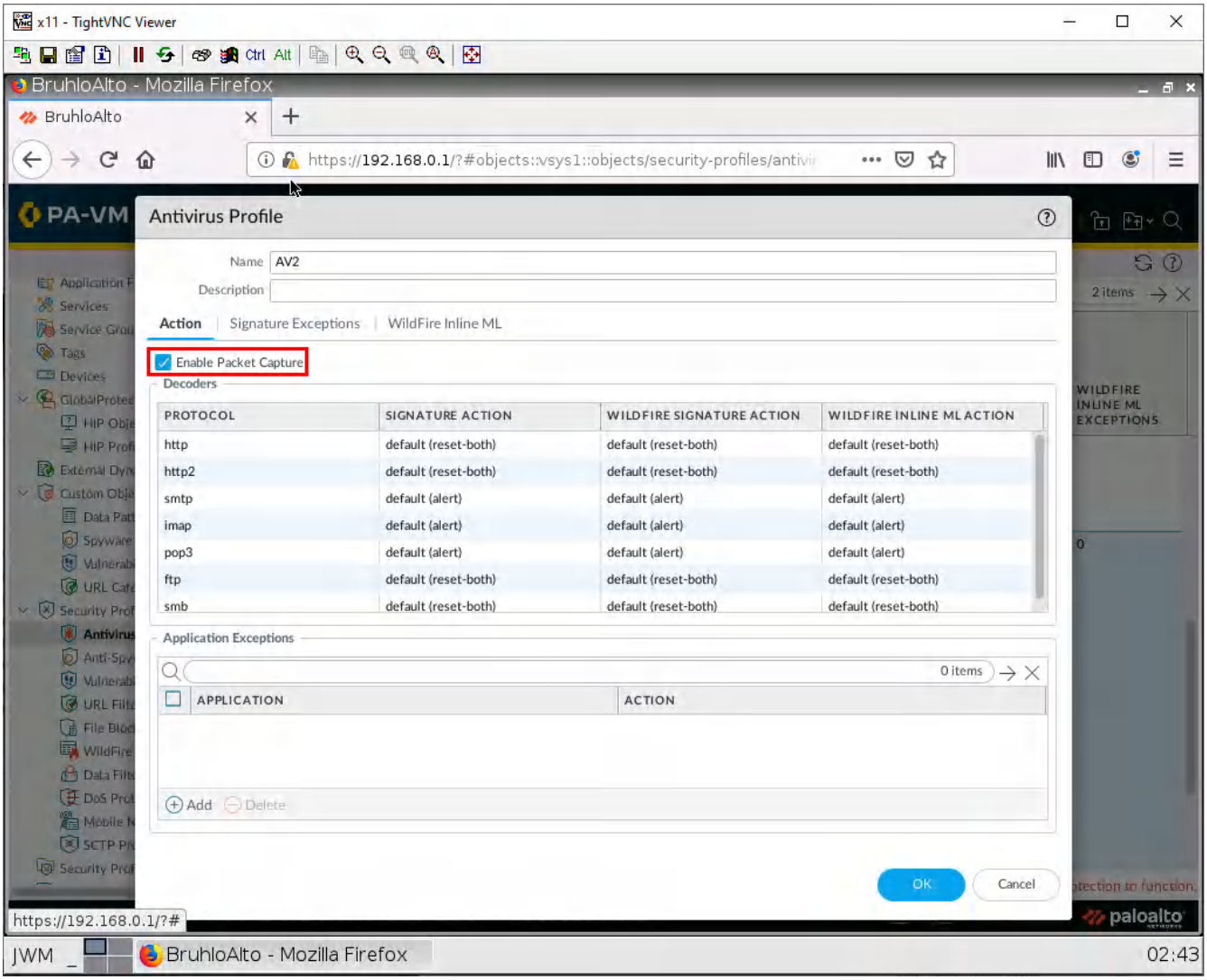


Figure 2.45: Enable Packet Captures under Antivirus Profile

Then press **OK**.

Create an Anti-Spyware Profile

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

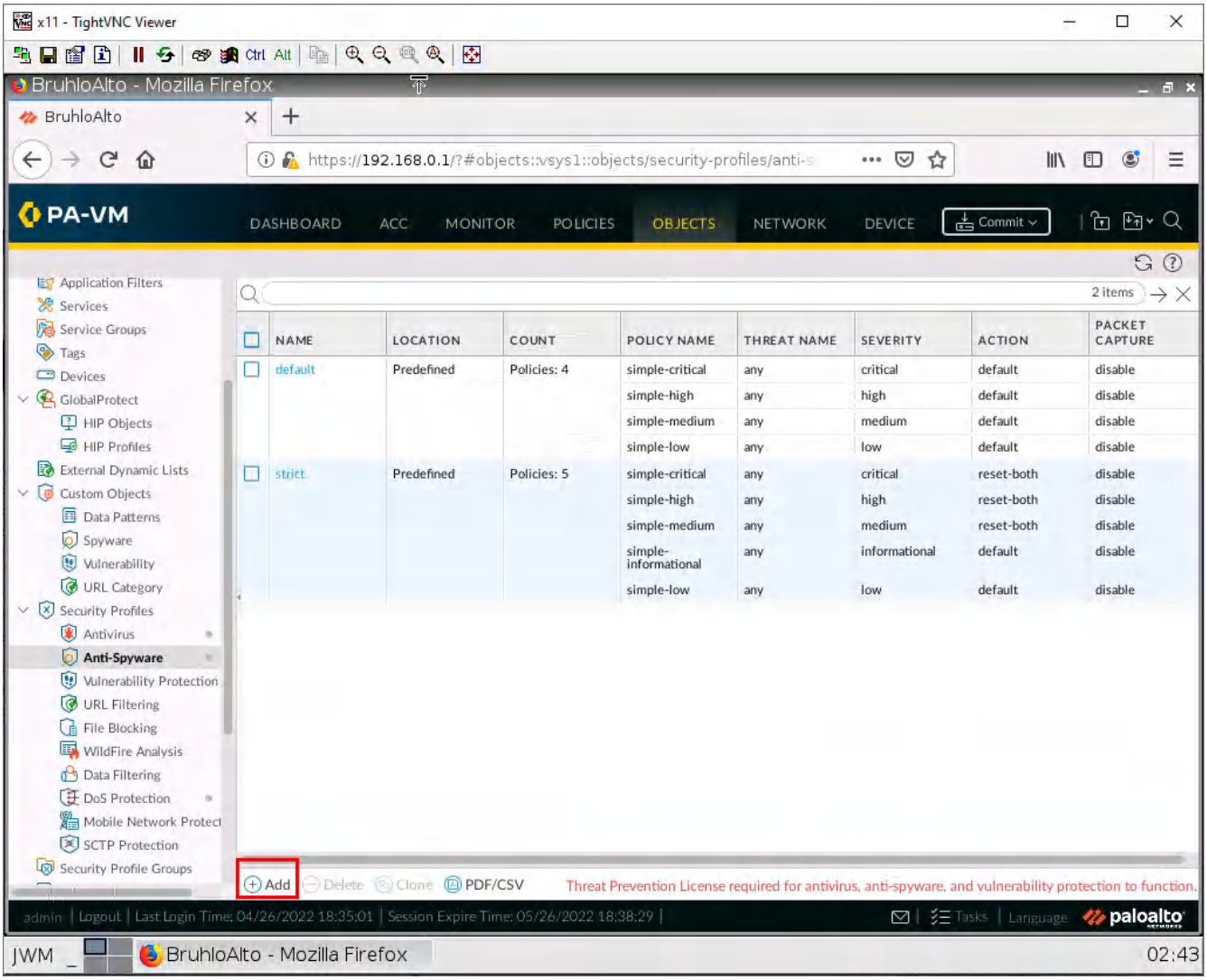


Figure 2.46: Add an Anti-Spyware Profile

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

Table 2.8: Anti-Spyware Configuration

Rule	Configuration
Medium	Action: *Alert* Severity: *Medium, Low, Informational*
HighAlert	Action: *Drop* *Severity: Critical, High*

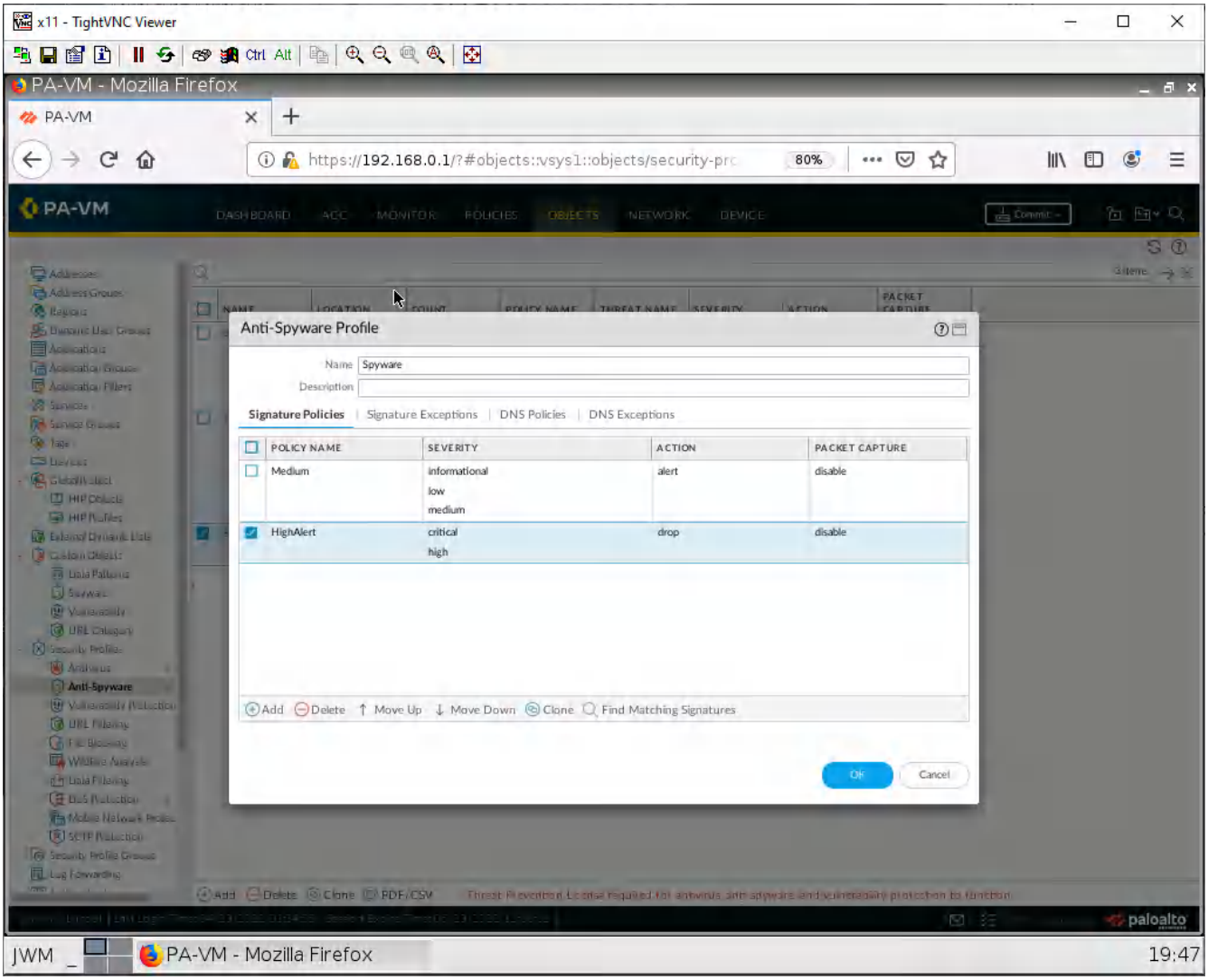


Figure 2.47: Verify an Anti-Spyware Profile

Then press **OK**.

Create a File Blocking Profile

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

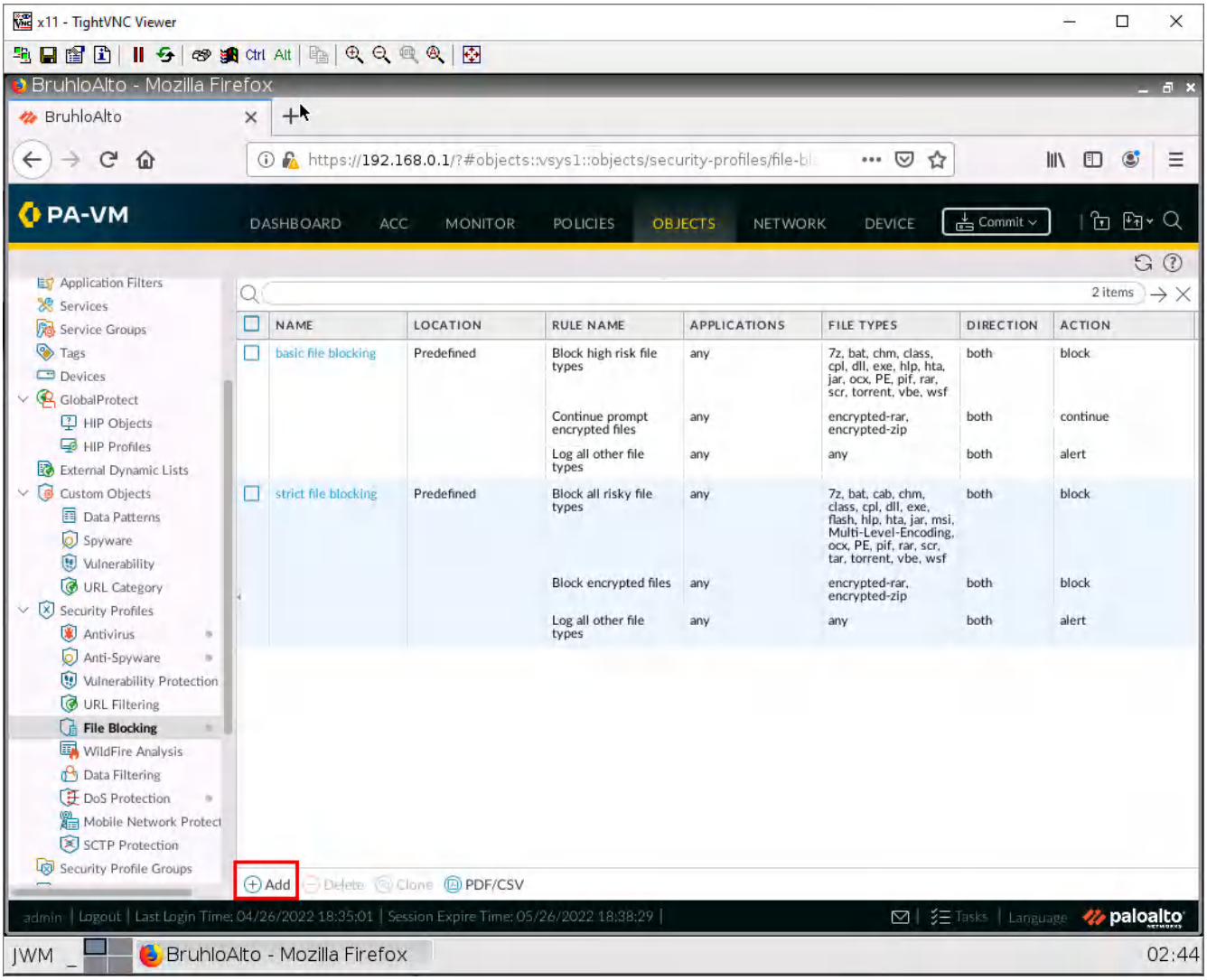


Figure 2.48: Add File blocking Profile

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

Table 2.9: File Blocking Configuration

Name	Properties
PDF	Applications: *any* File Types*: pdf, encrypted-pdf* Action: *Block*
EXE	Applications: *any* File Types: *exe, com* *Action: Block*

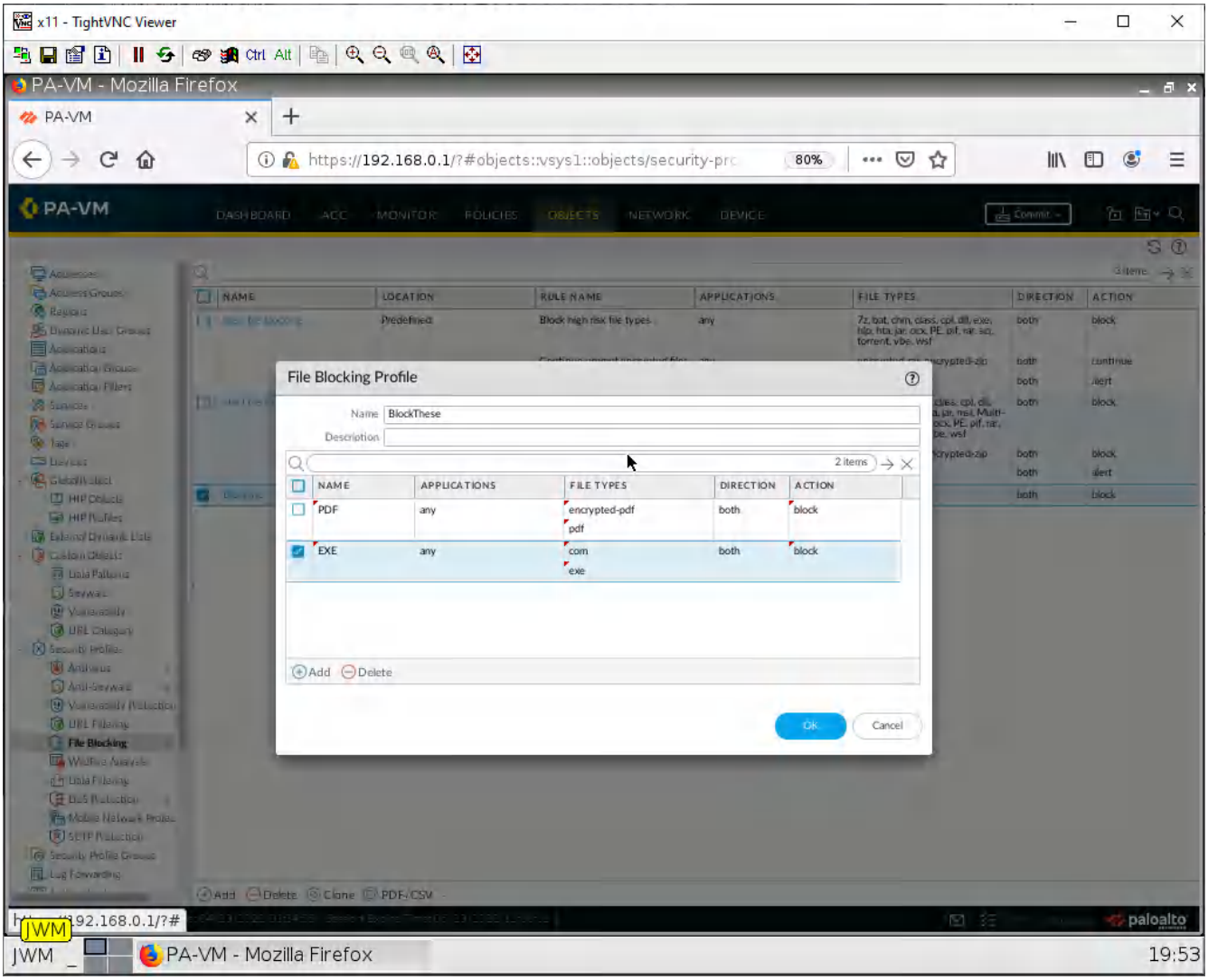


Figure 2.49: Configure the File blocking profile

Then click **OK**.

Create a WildFire Profile

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

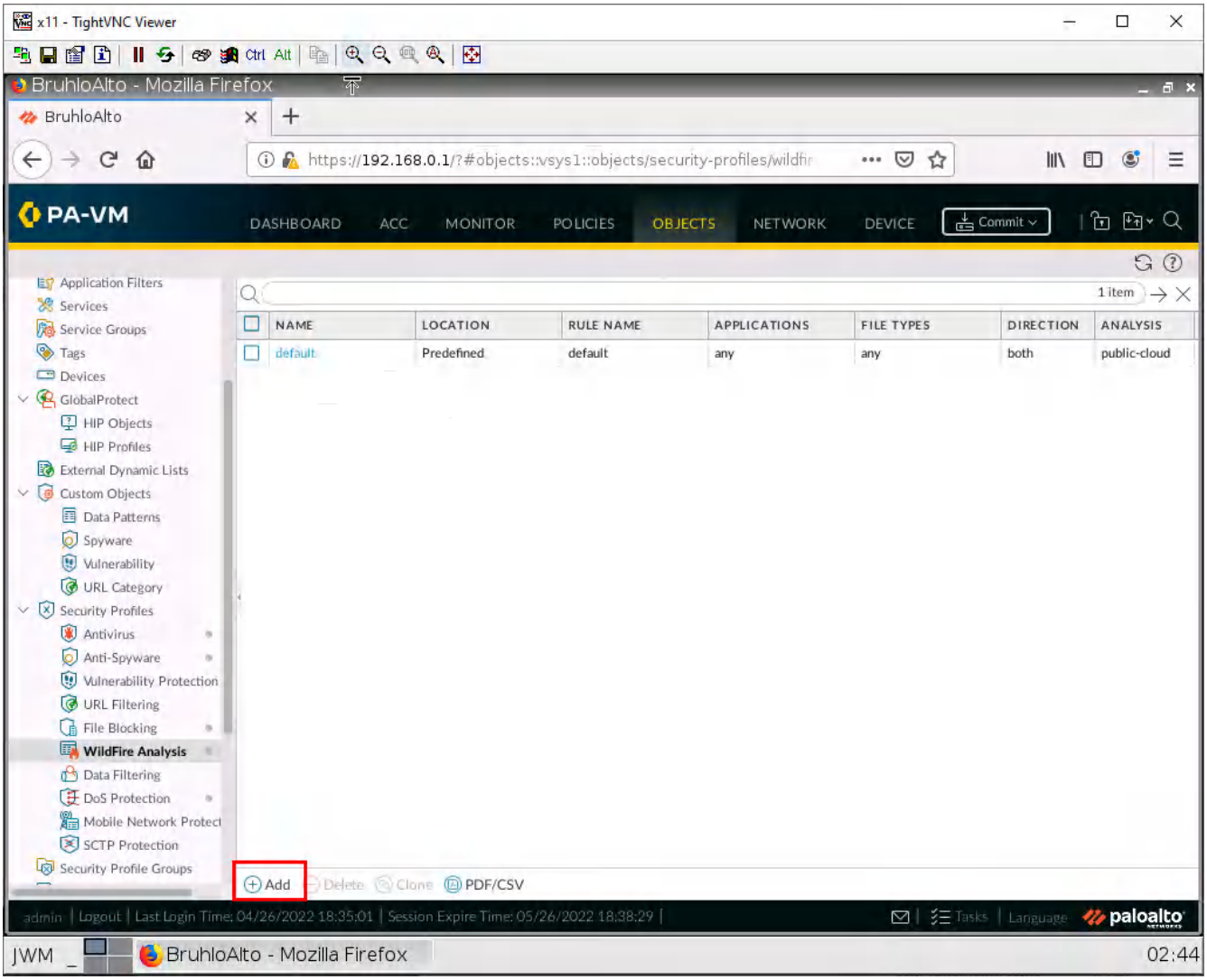


Figure 2.50: Add a WildFire Profile

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

Table 2.10: WildFire Configuration

Name	Properties
Detect	Applications: *any* File Types: *archive, jar, ms-office*

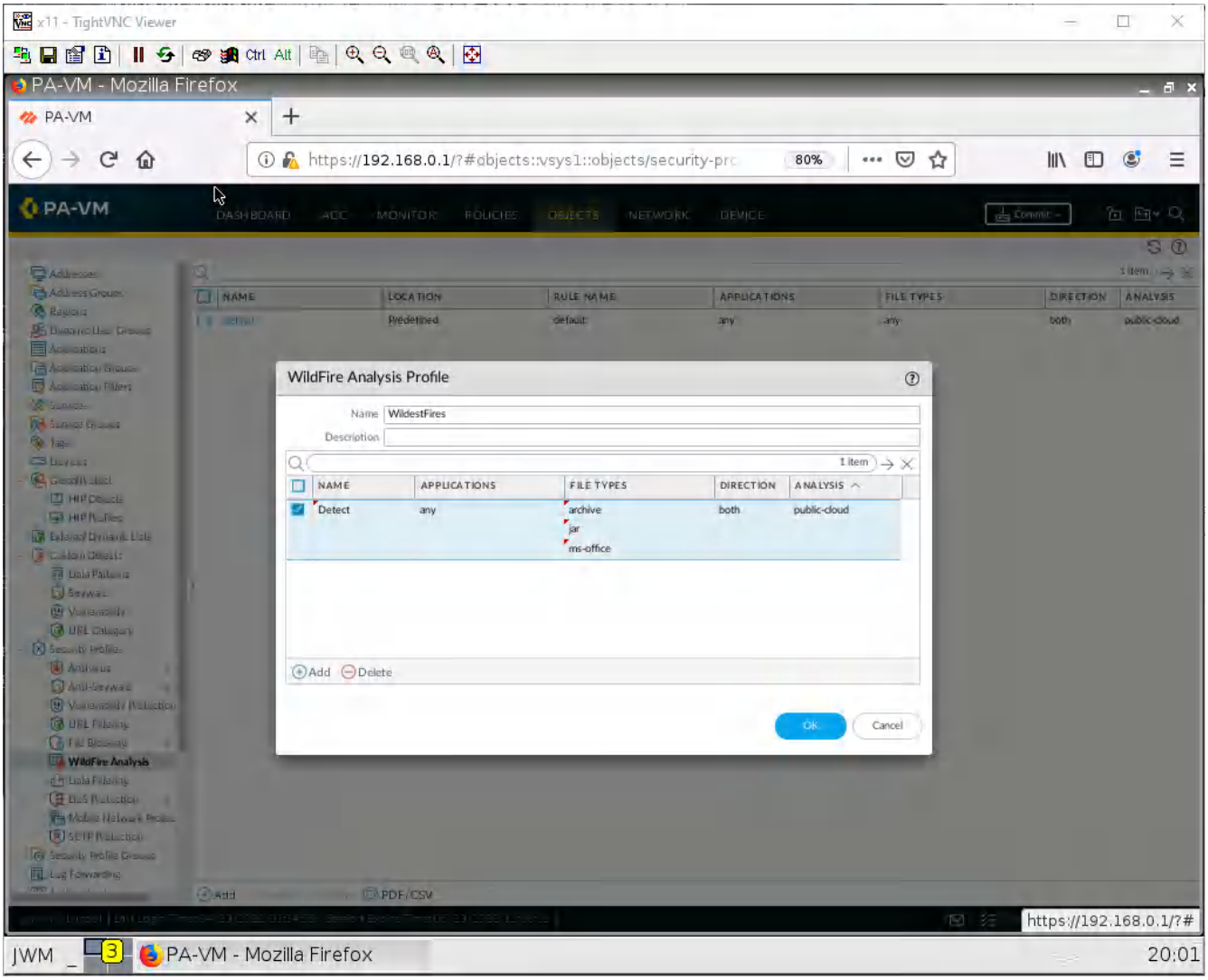


Figure 2.51: Add a WildFire Profile

Then press **OK**.

Apply Security Profiles to a Security Policy

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

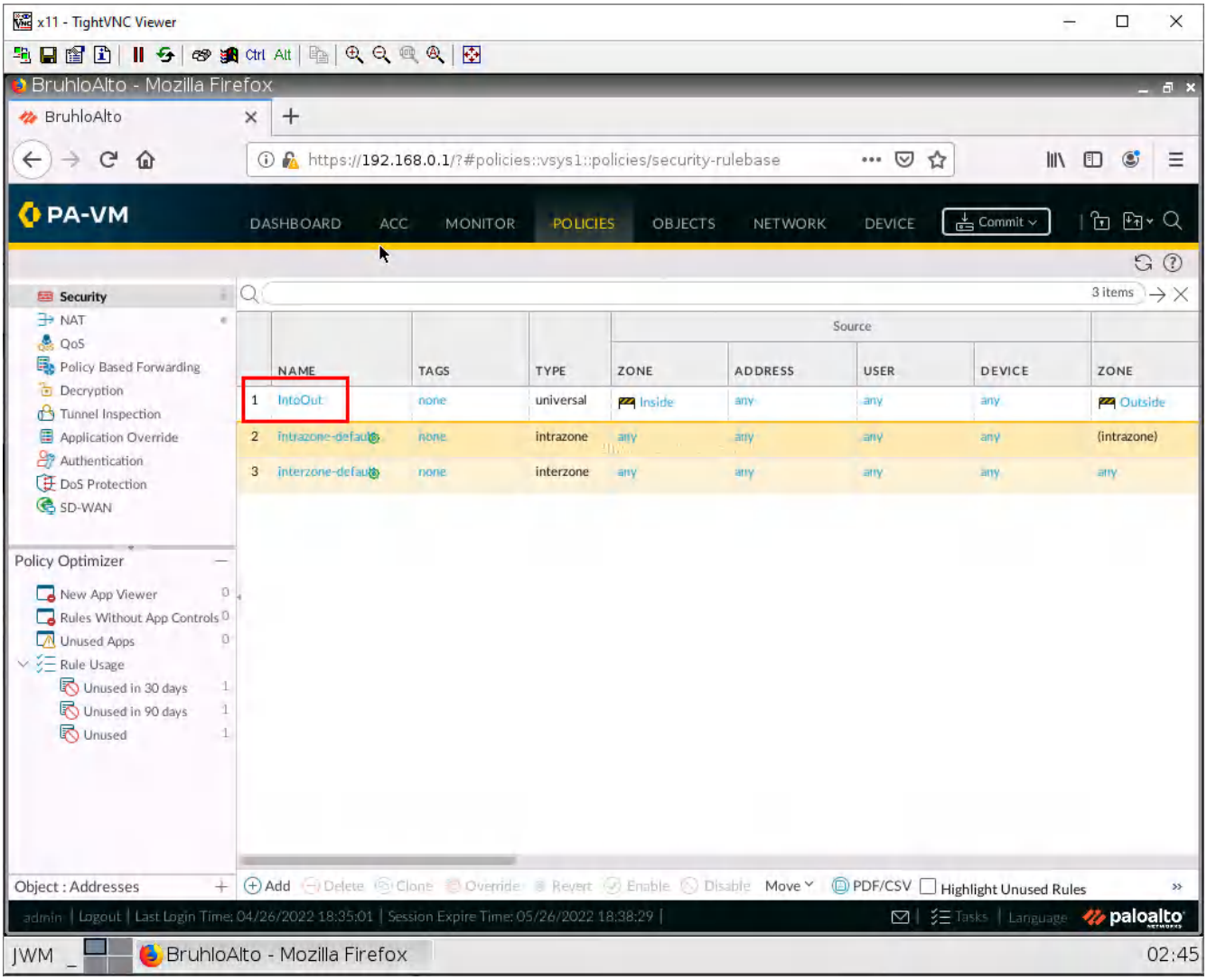


Figure 2.52: Add a Security Policy

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

Table 2.11: Security Policy Actions Configuration

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

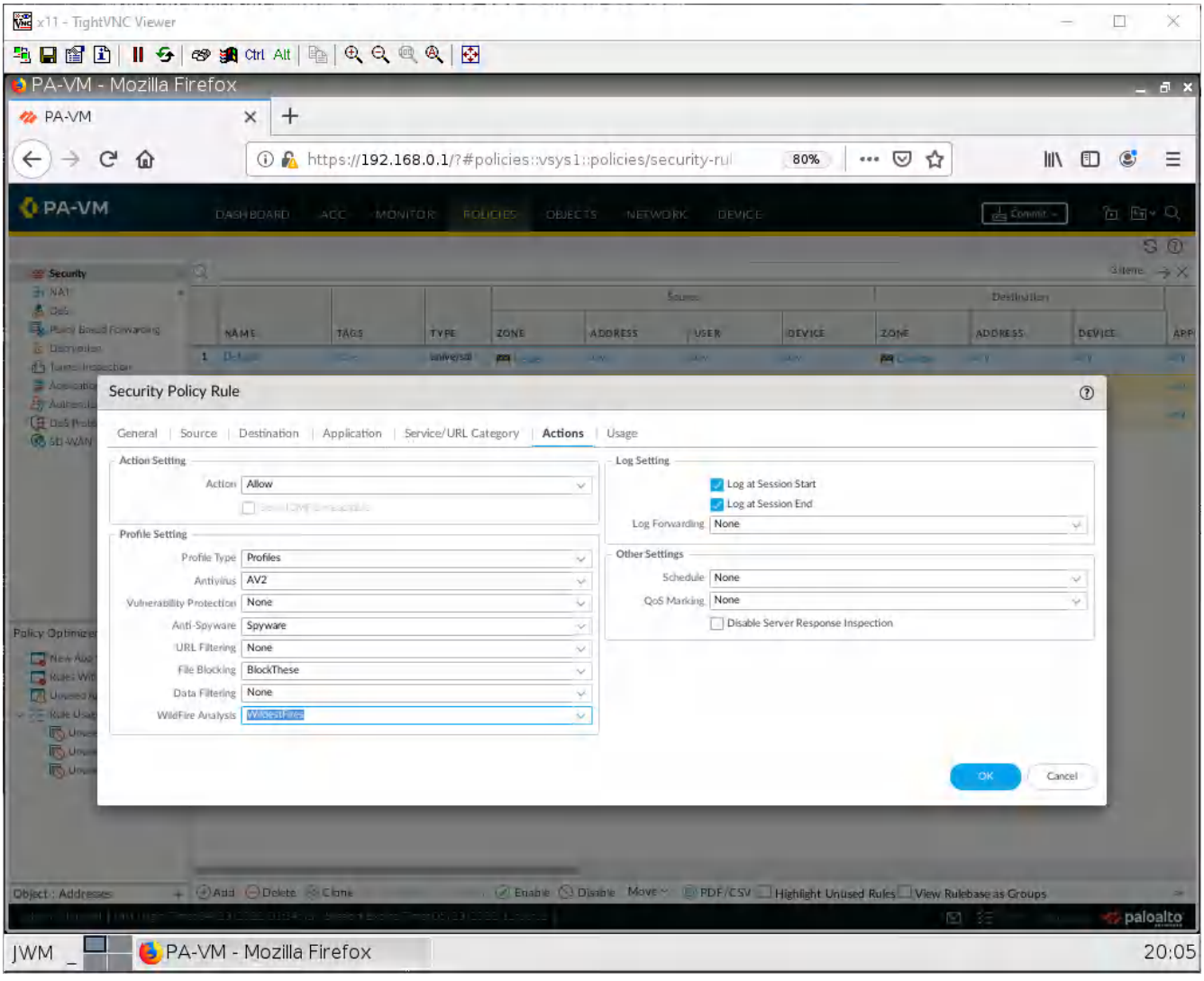


Figure 2.53: Assigning security profiles

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.

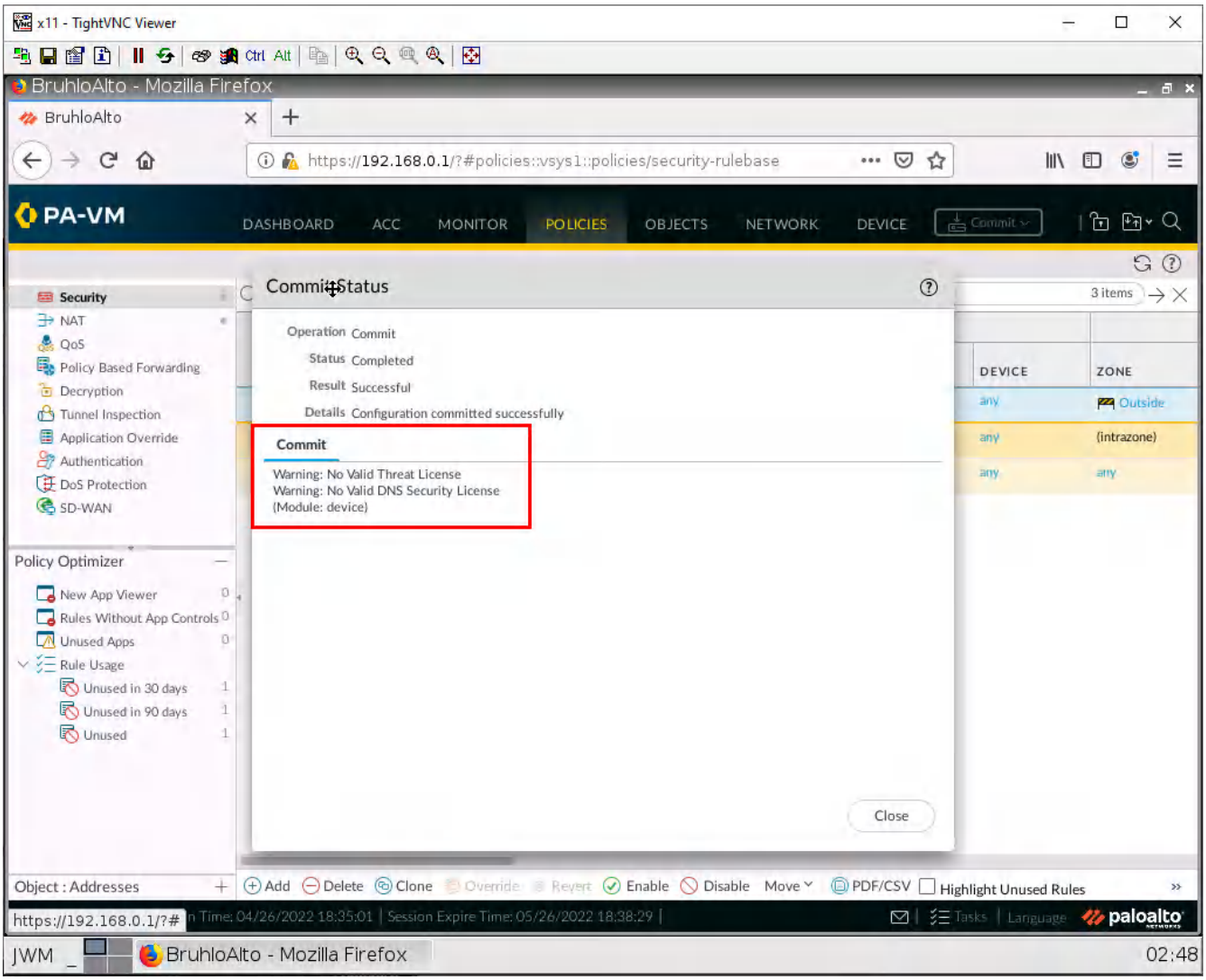


Figure 2.54: Commit the configuration

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).

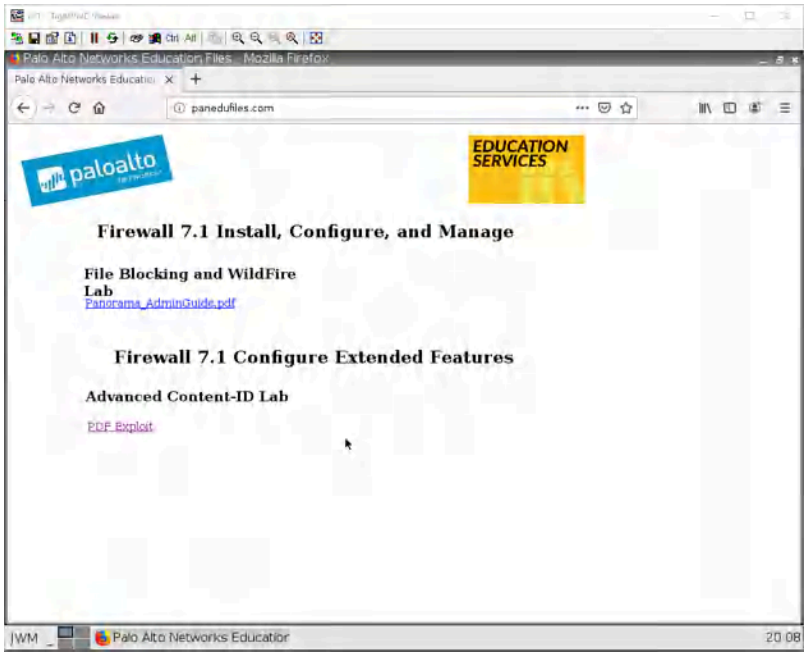


Figure 2.55: Verify the configuration

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

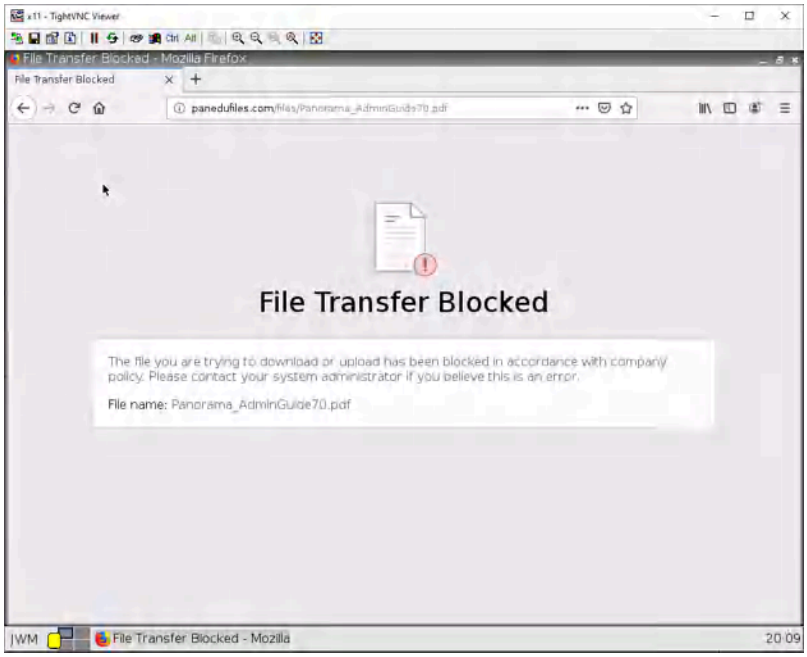


Figure 2.56: File Transfer Blocked

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.

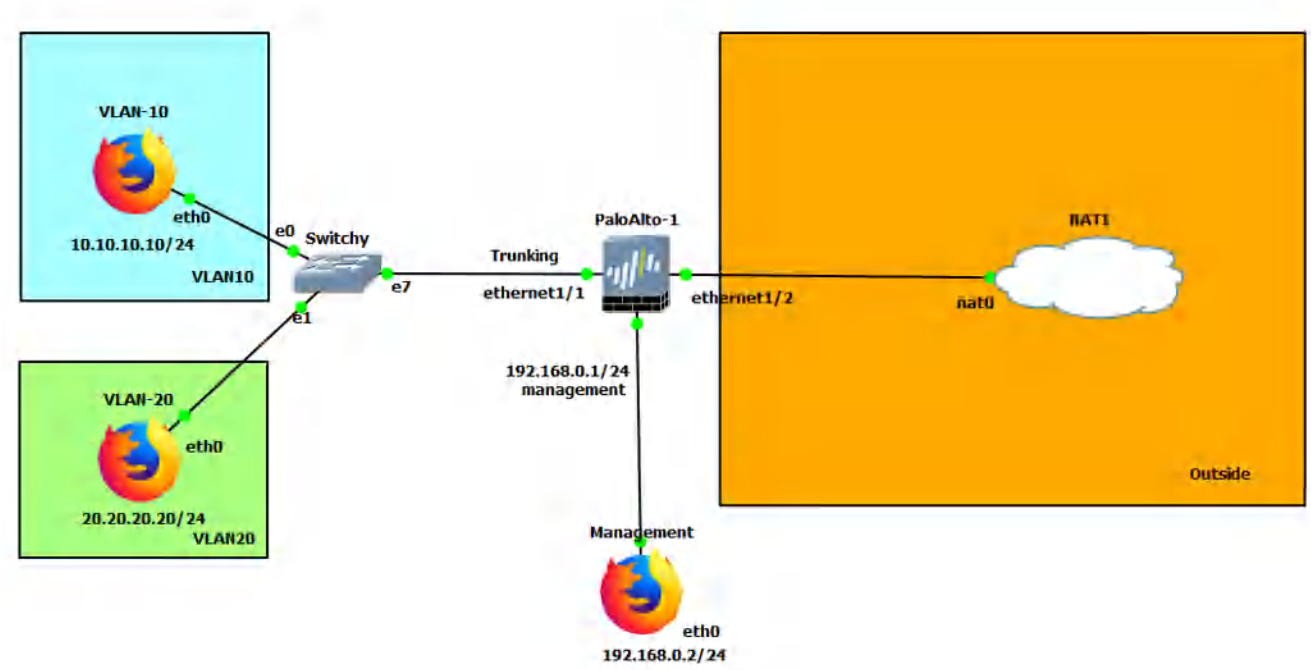


Figure 3.1: Main scenario

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.**

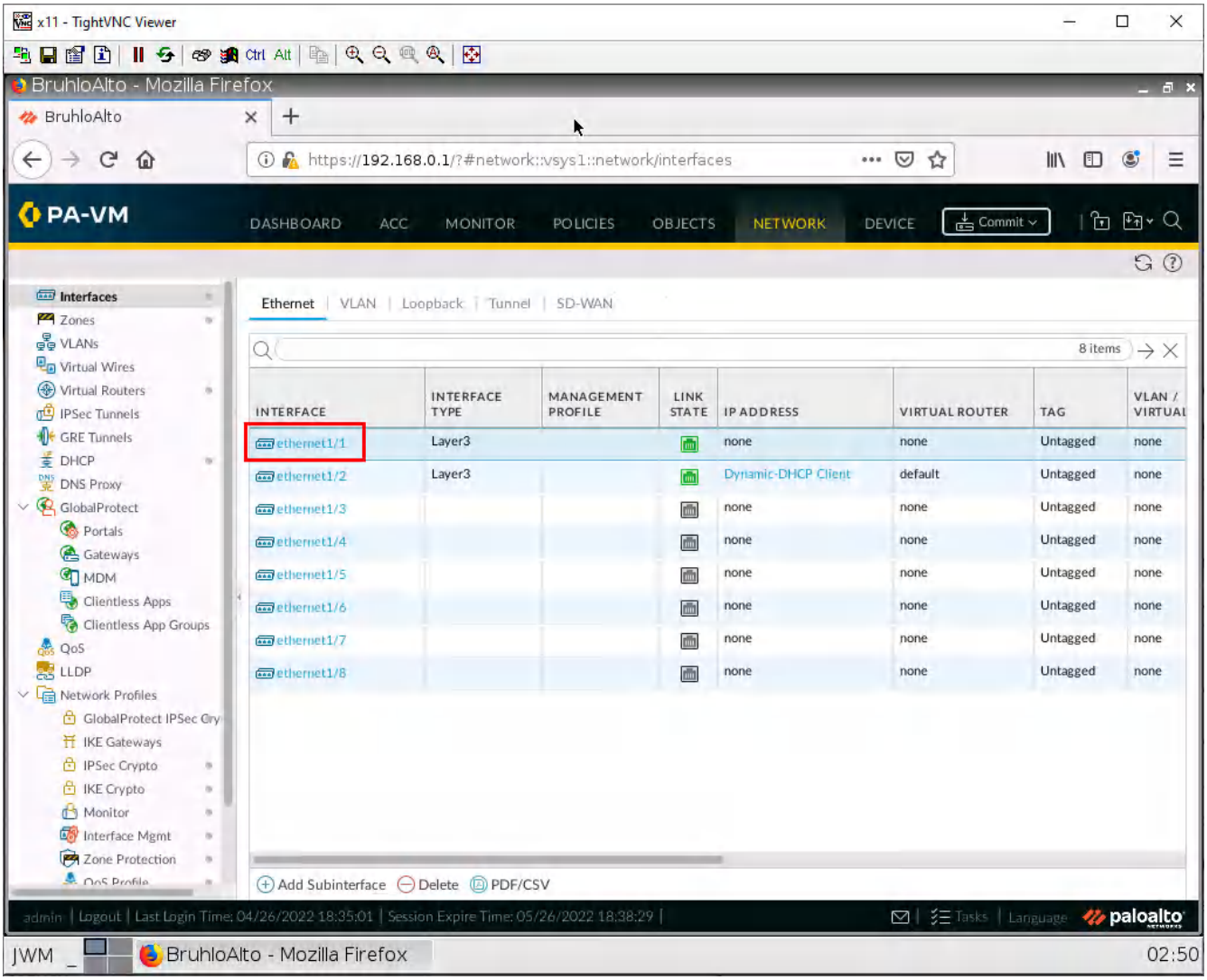


Figure 3.2: Ethernet 1/1 configuration

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

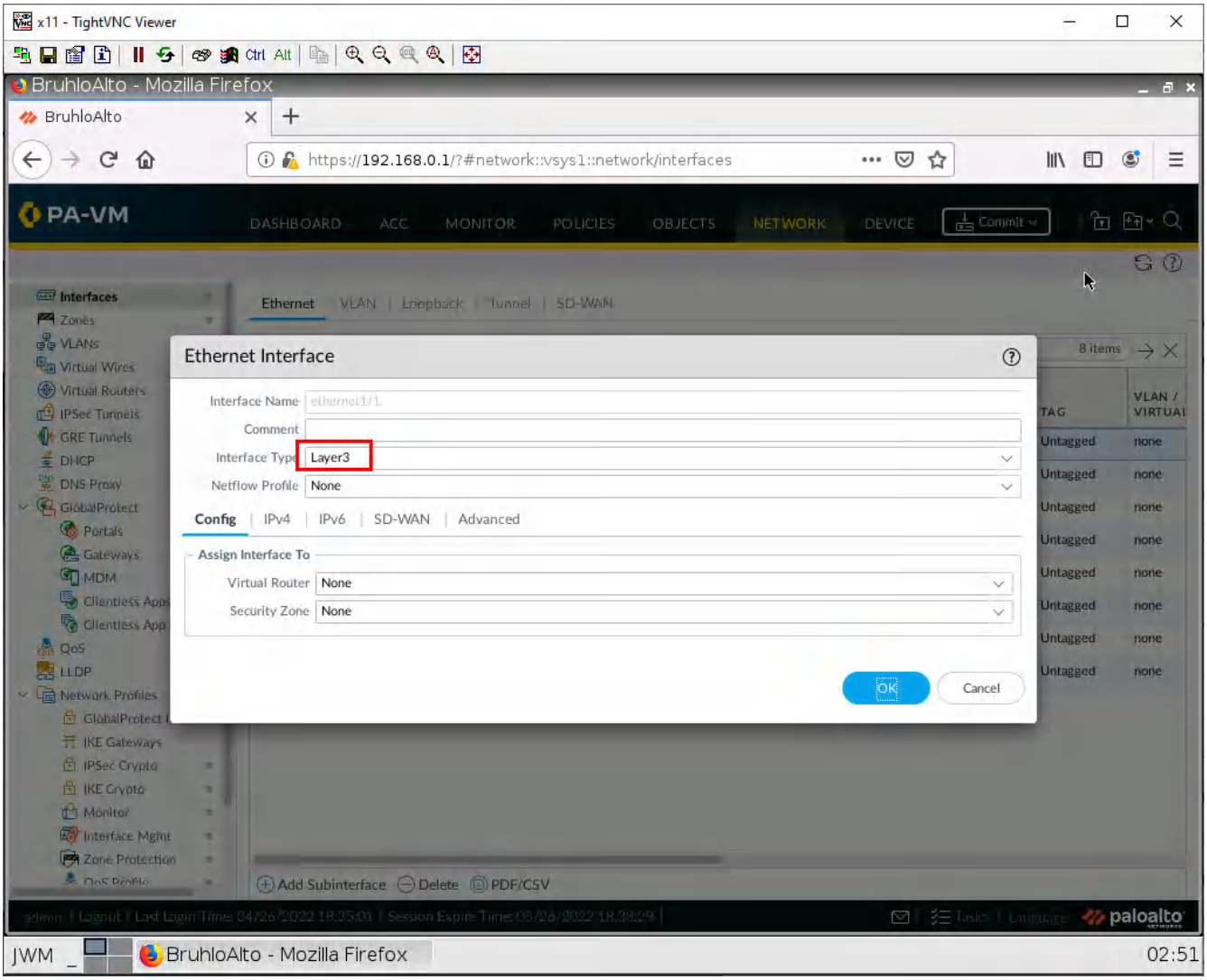


Figure 3.3: Set Interface type to Layer3

Then press **OK**.

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

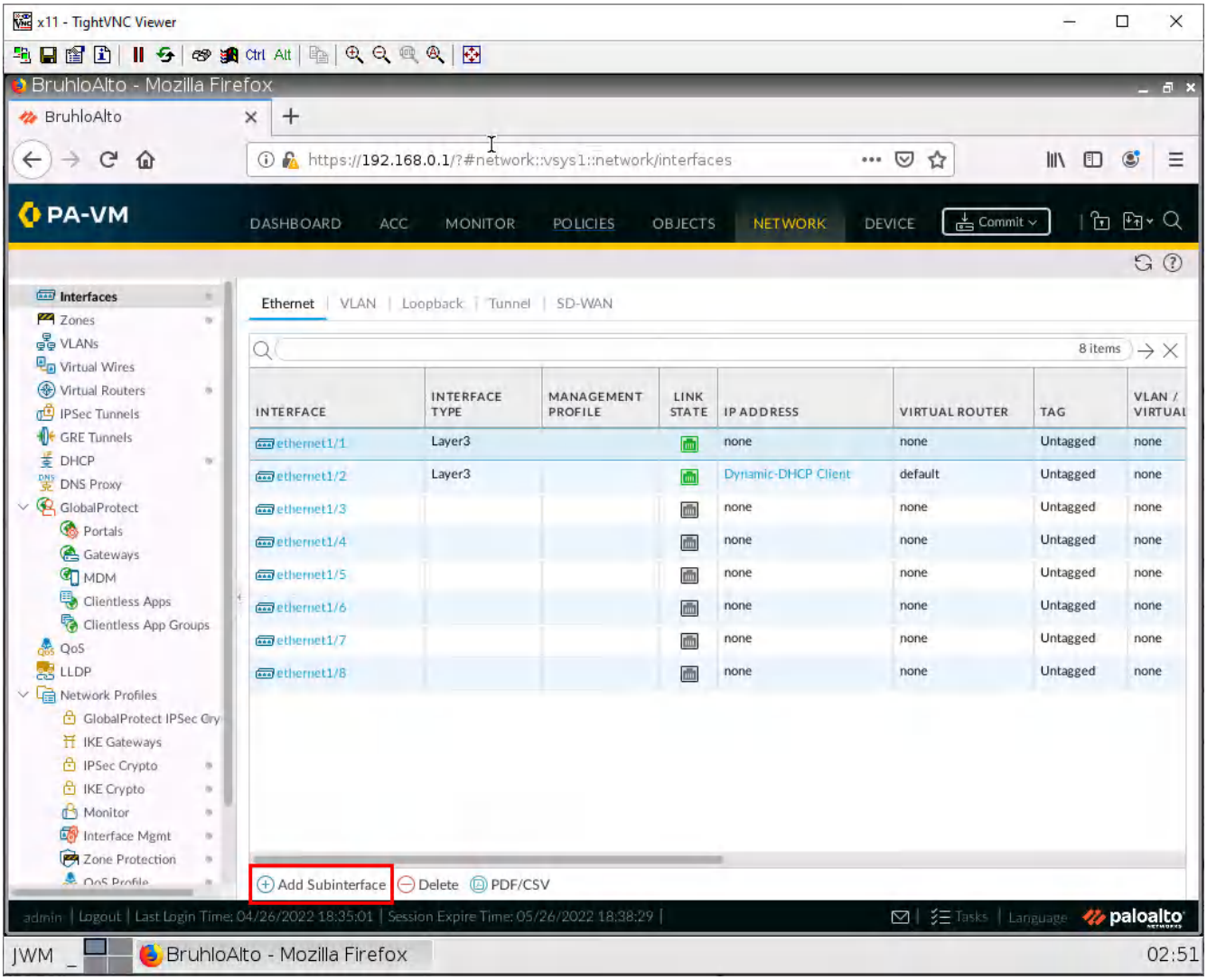


Figure 3.4: Add Sub interfaces

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: *default* – Security Zone: *VLAN10* IPv4: – Type: *Static* – *IP: 10.10.10.1/24*
Ethernet1/1.20	Interface Name: 20 Tag: 20 Config tab: – Virtual Router: *default* – Security Zone: *VLAN20* IPv4: – Type: *Static* – *IP: 20.20.20.1/24*

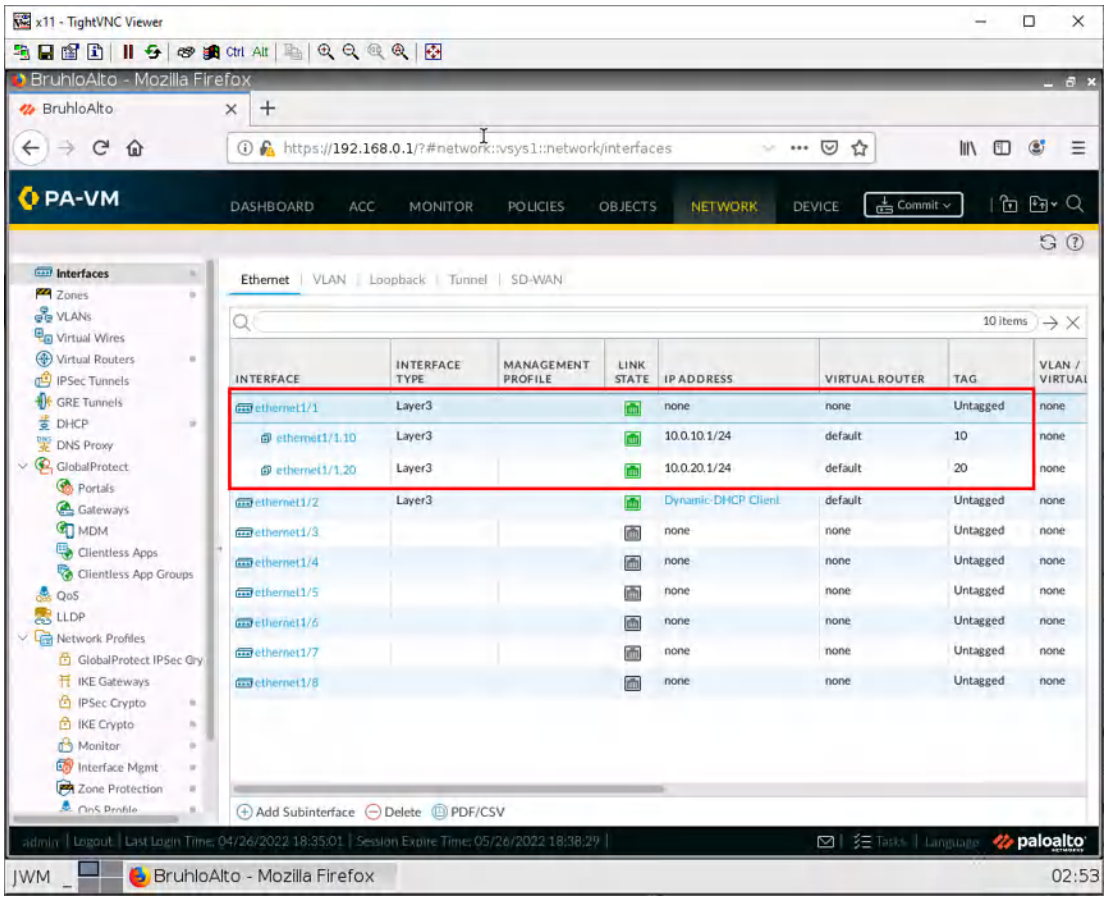


Figure 3.5: Verify Sub interfaces

Semi-Advanced Security Policies

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

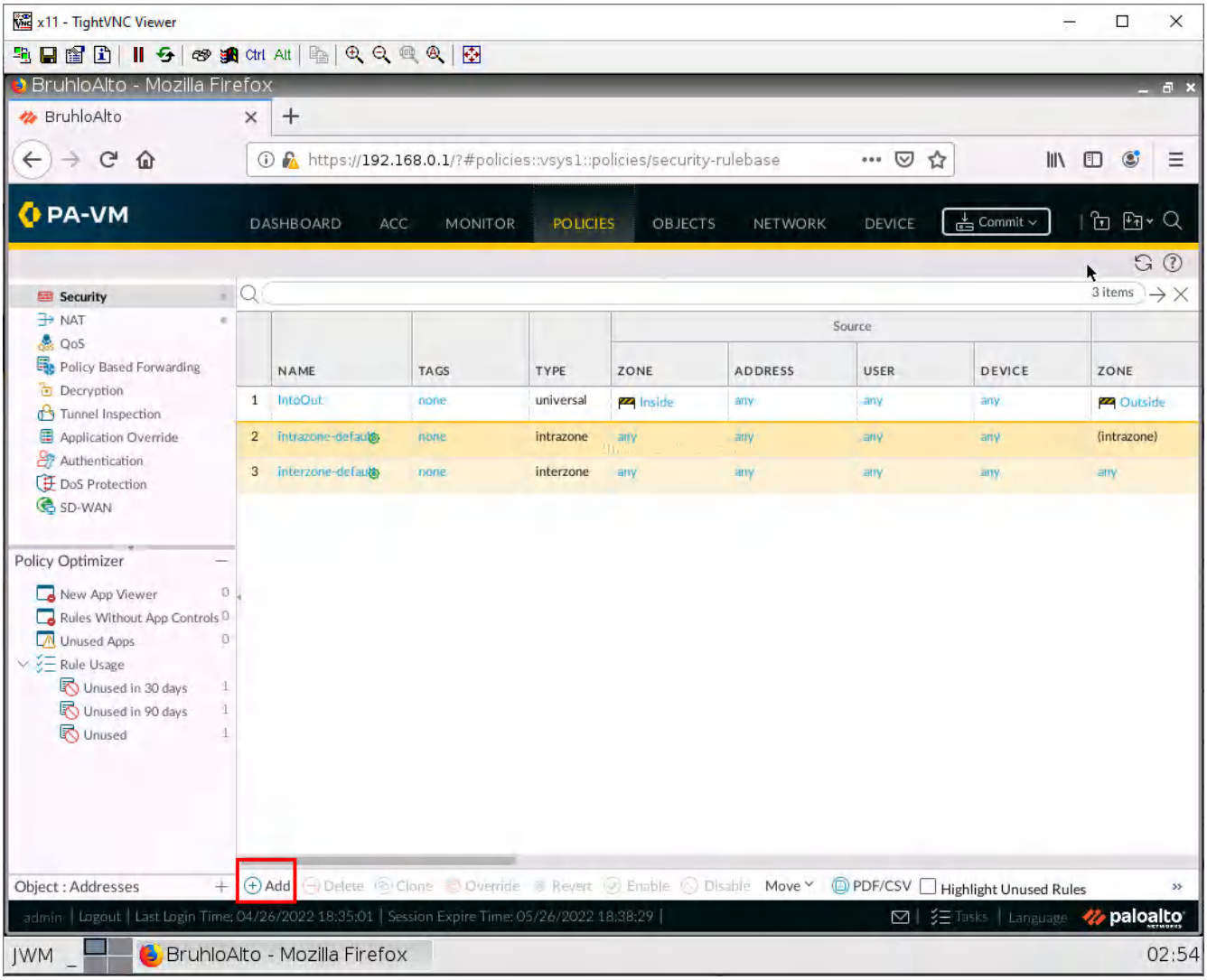


Figure 3.6: Add a Security Policy

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

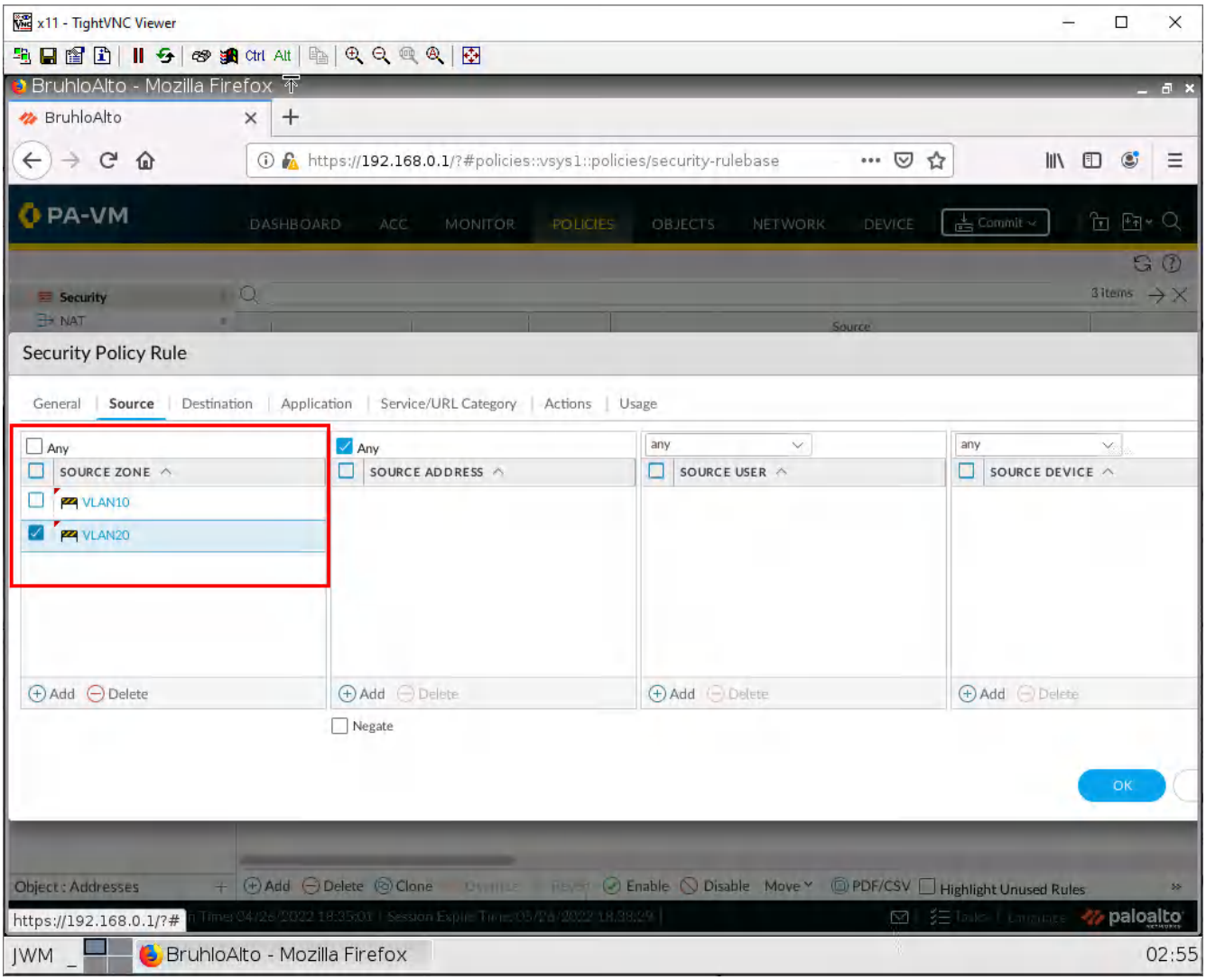


Figure 3.7: Security Policy Rule – Source Zone

Then click **OK**.

Semi-Advanced NAT Policies

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

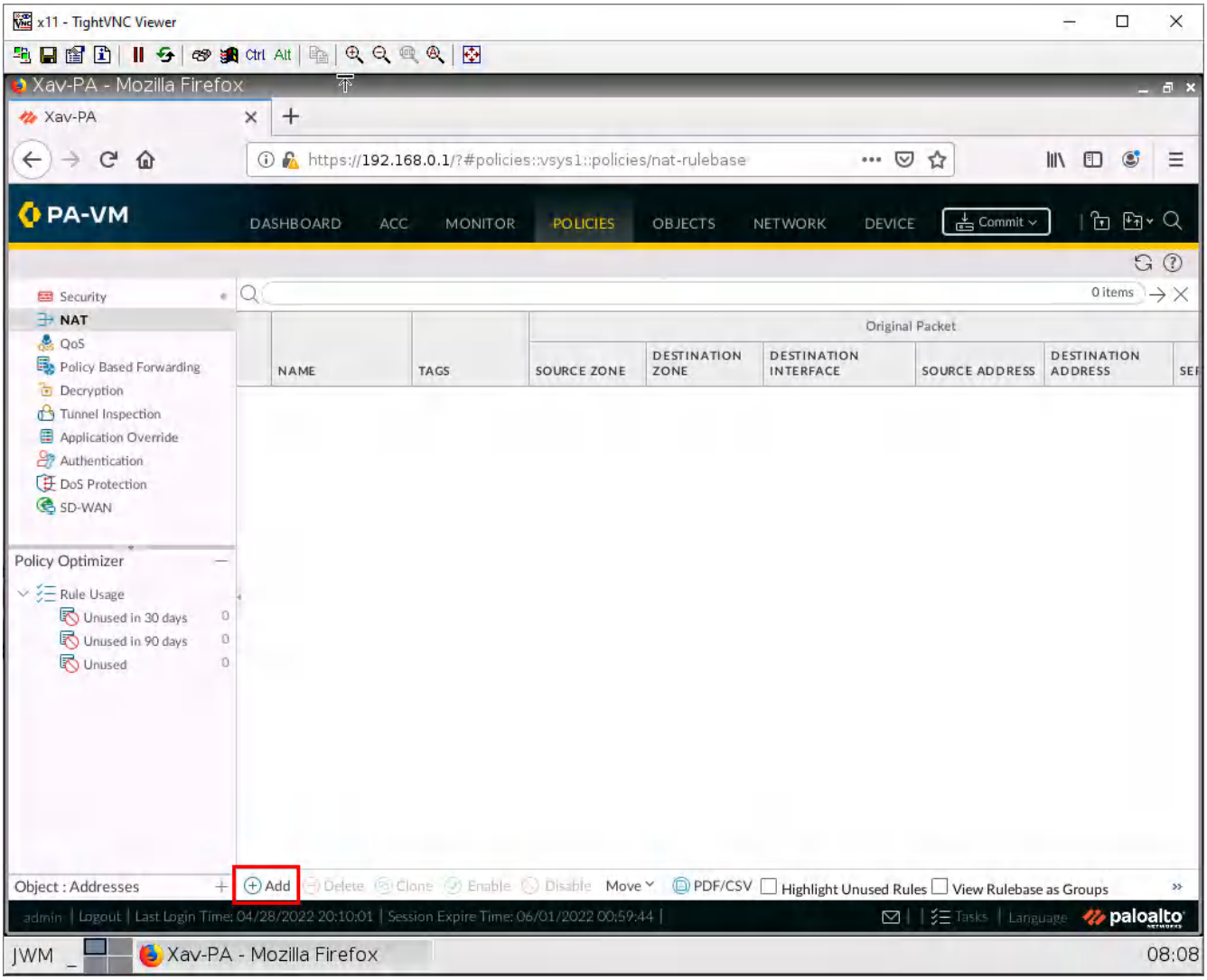


Figure 3.8: Add a NAT Policy

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

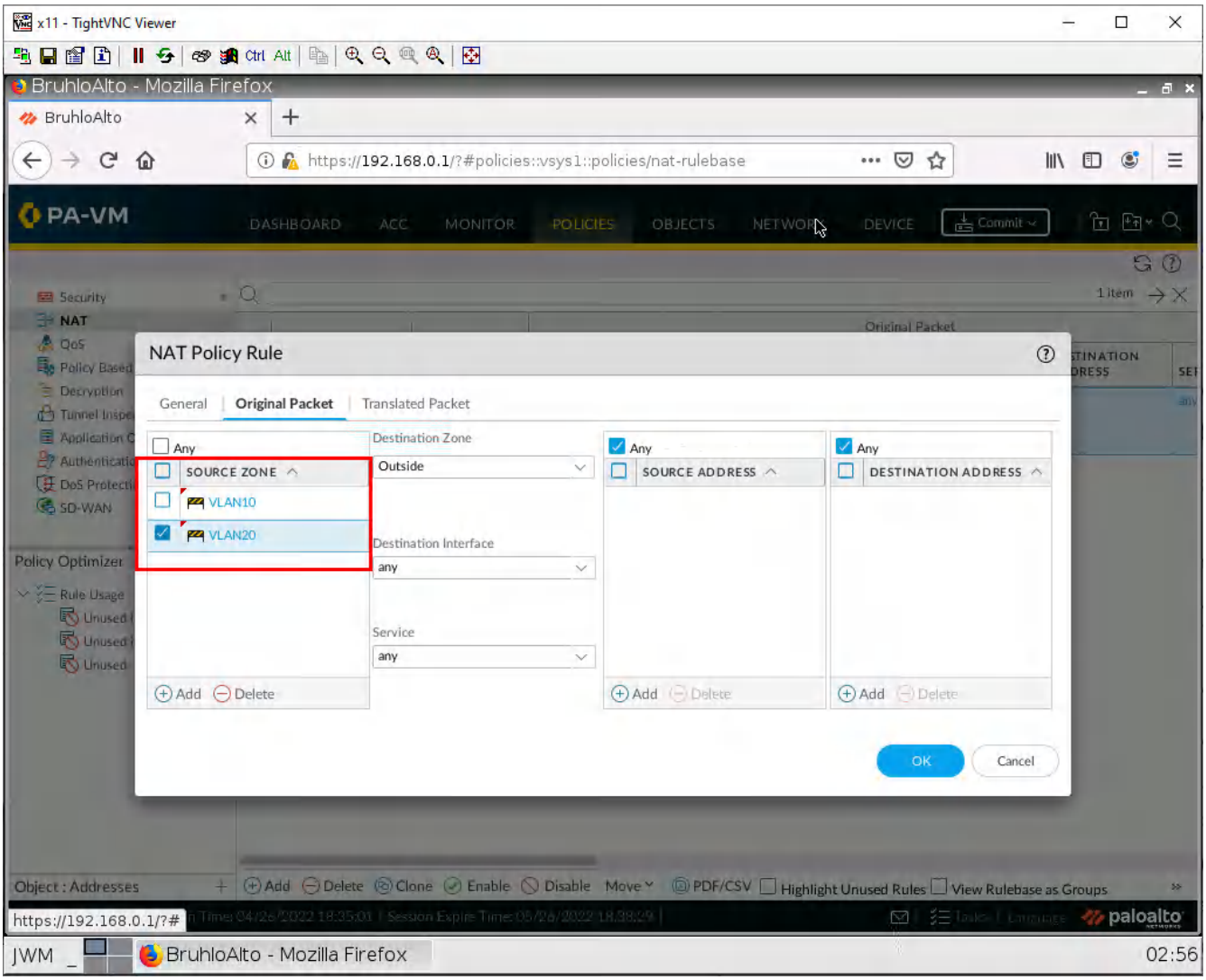


Figure 3.9: Select the Source Zone

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

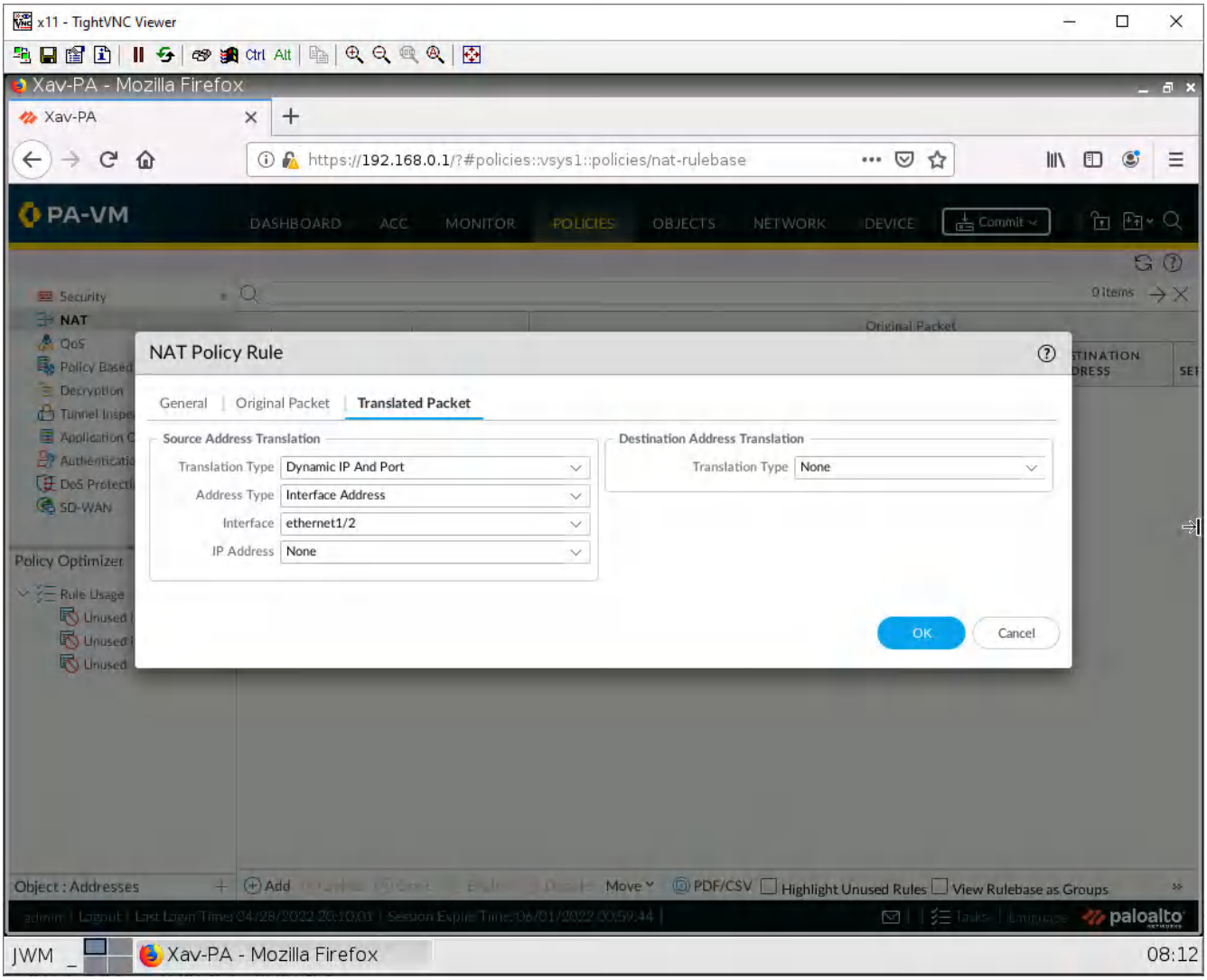


Figure 3.10: SNAT Translated Packet Tab

Add a User

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

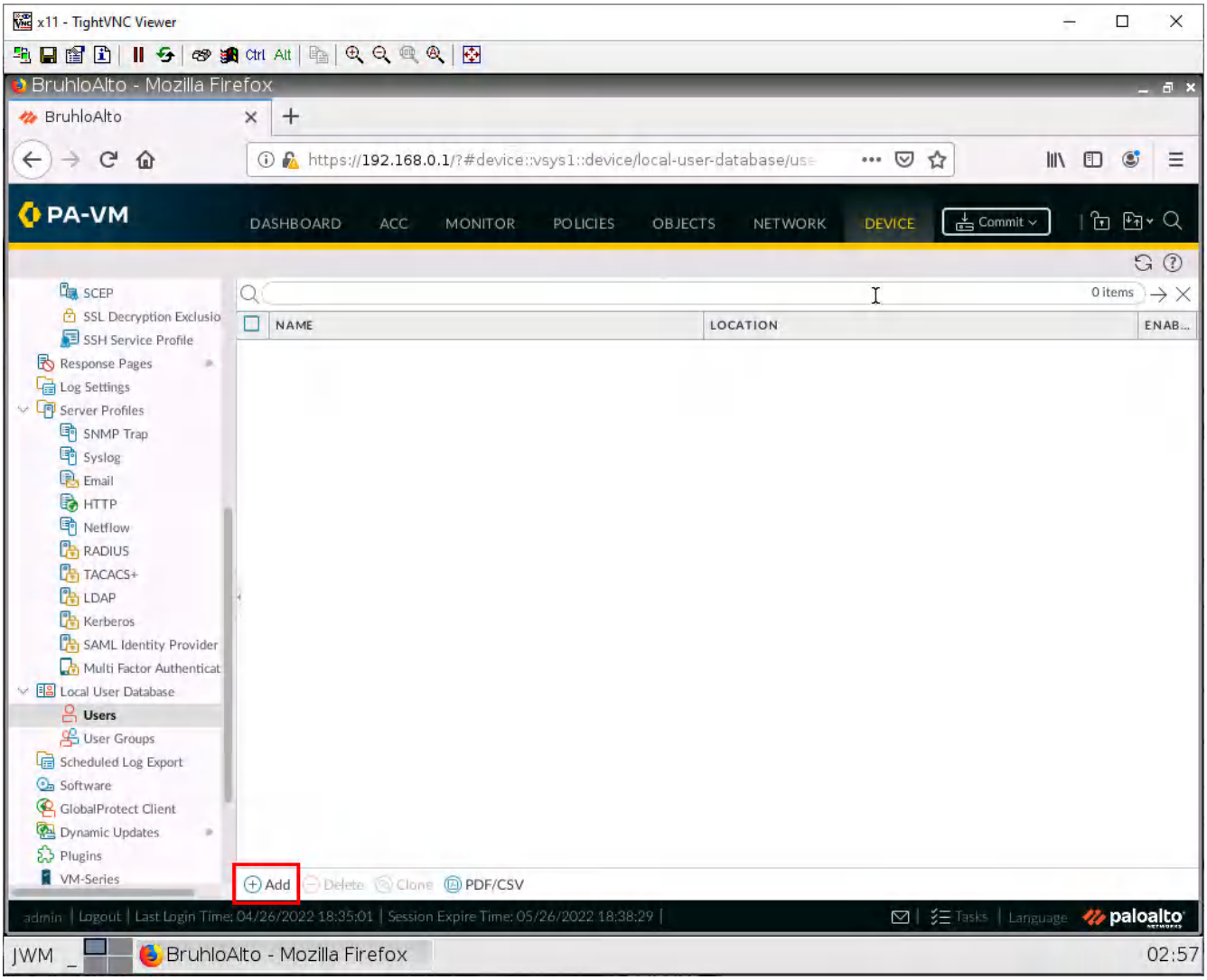


Figure 3.11: Add Users

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

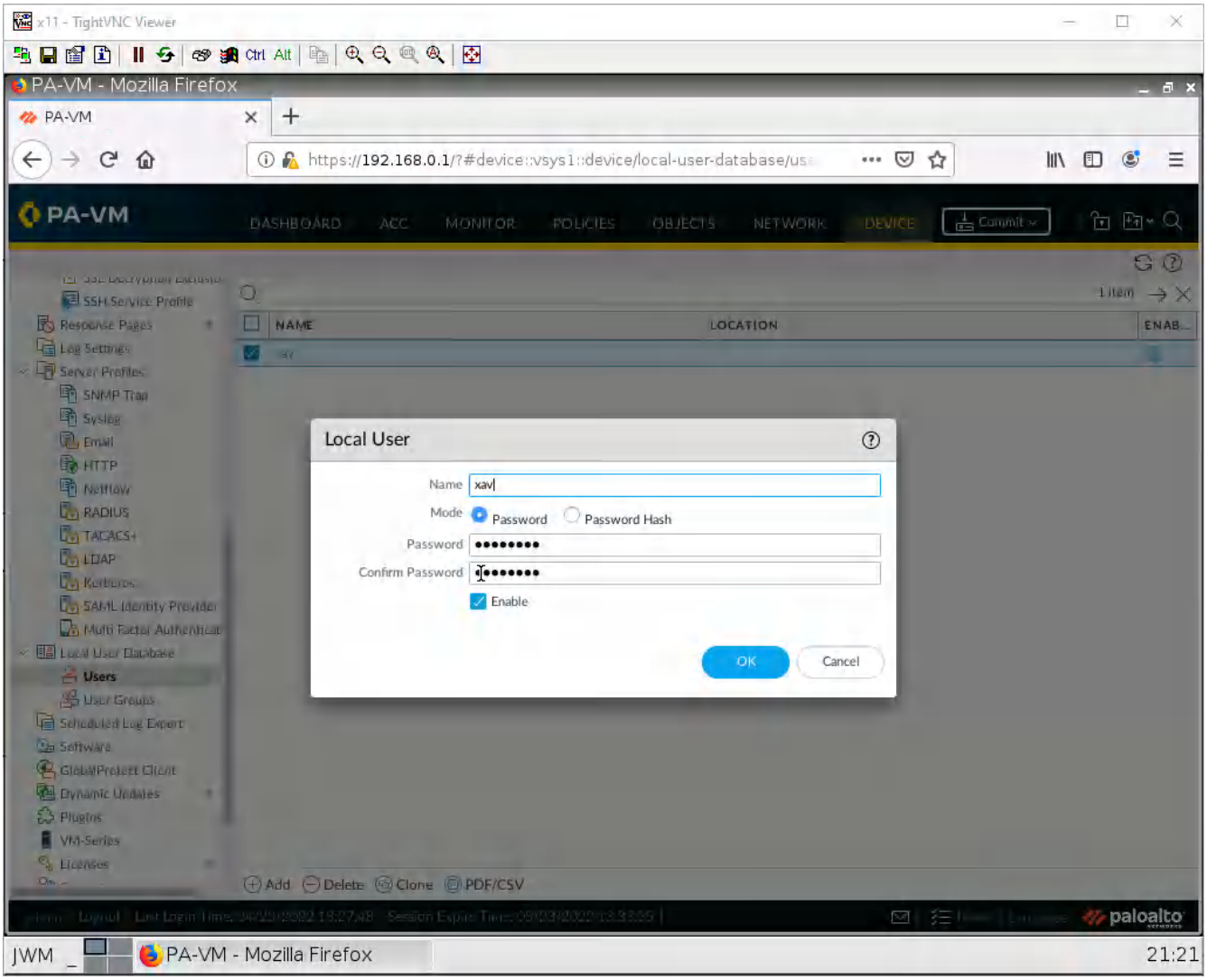


Figure 3.12: Add a user xav

Then click **OK**.

Create an Authentication Profile

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

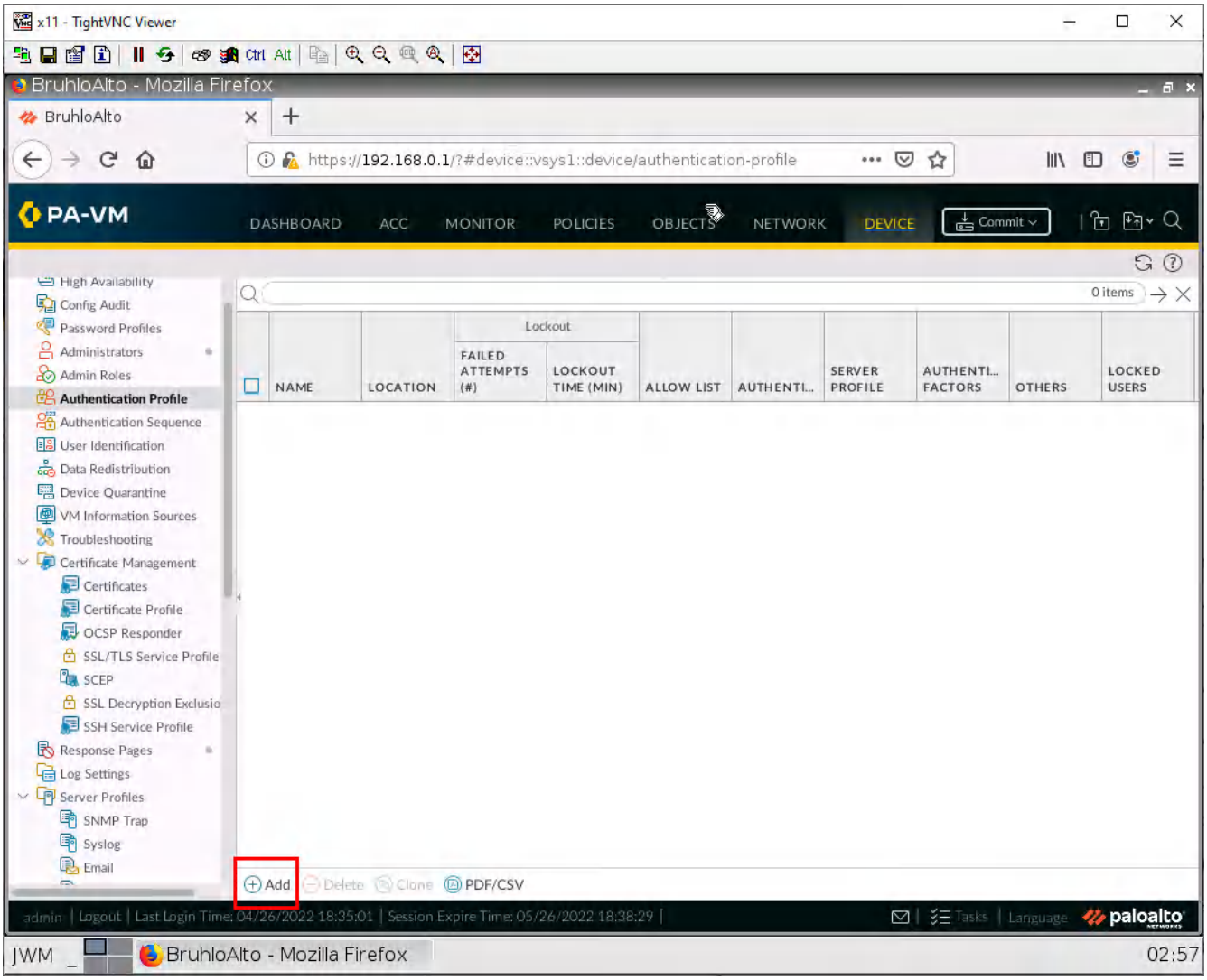


Figure 3.13: Add an Authentication Profile

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

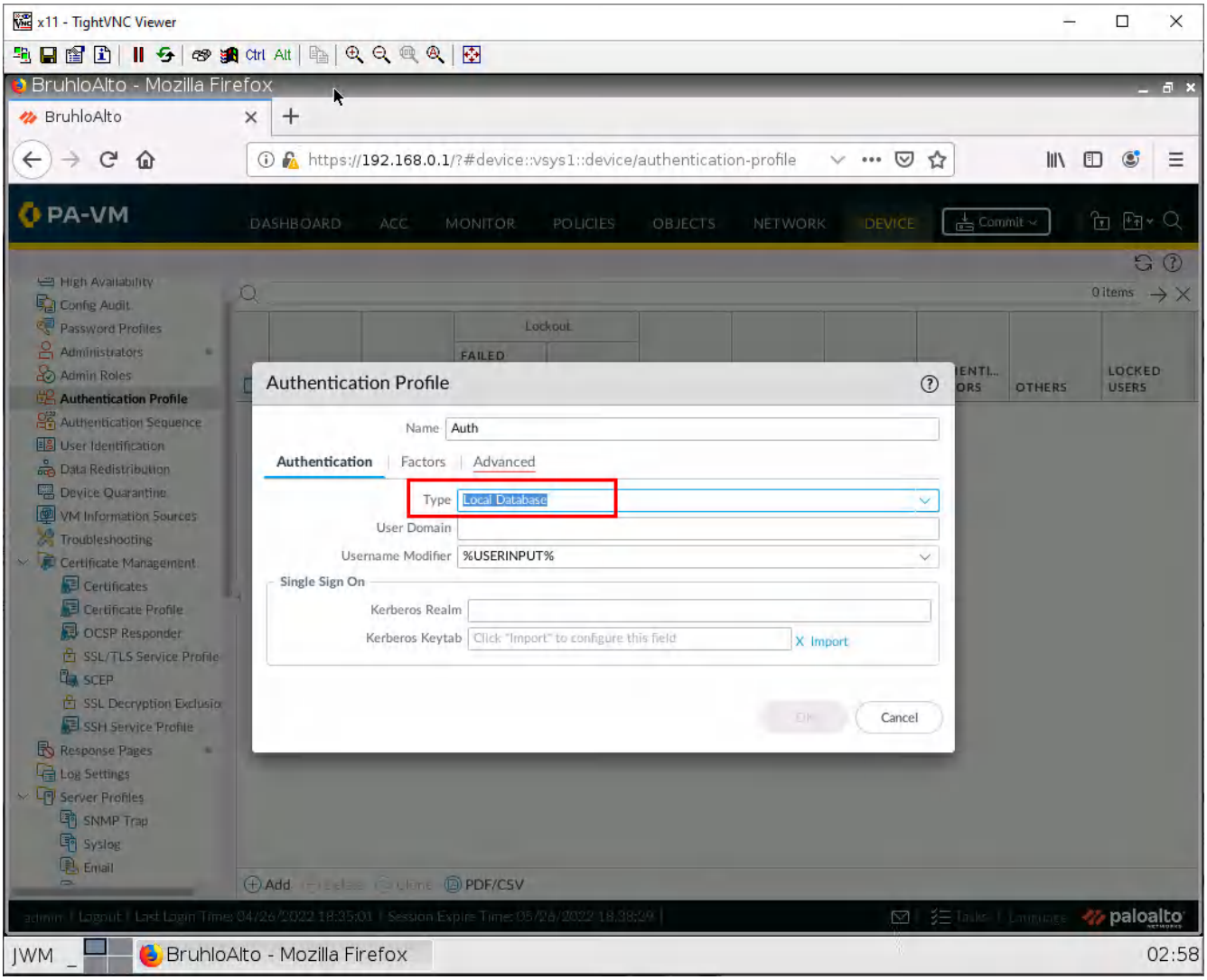


Figure 3.14: Select Local Database

Under the Advanced tab, add your user.

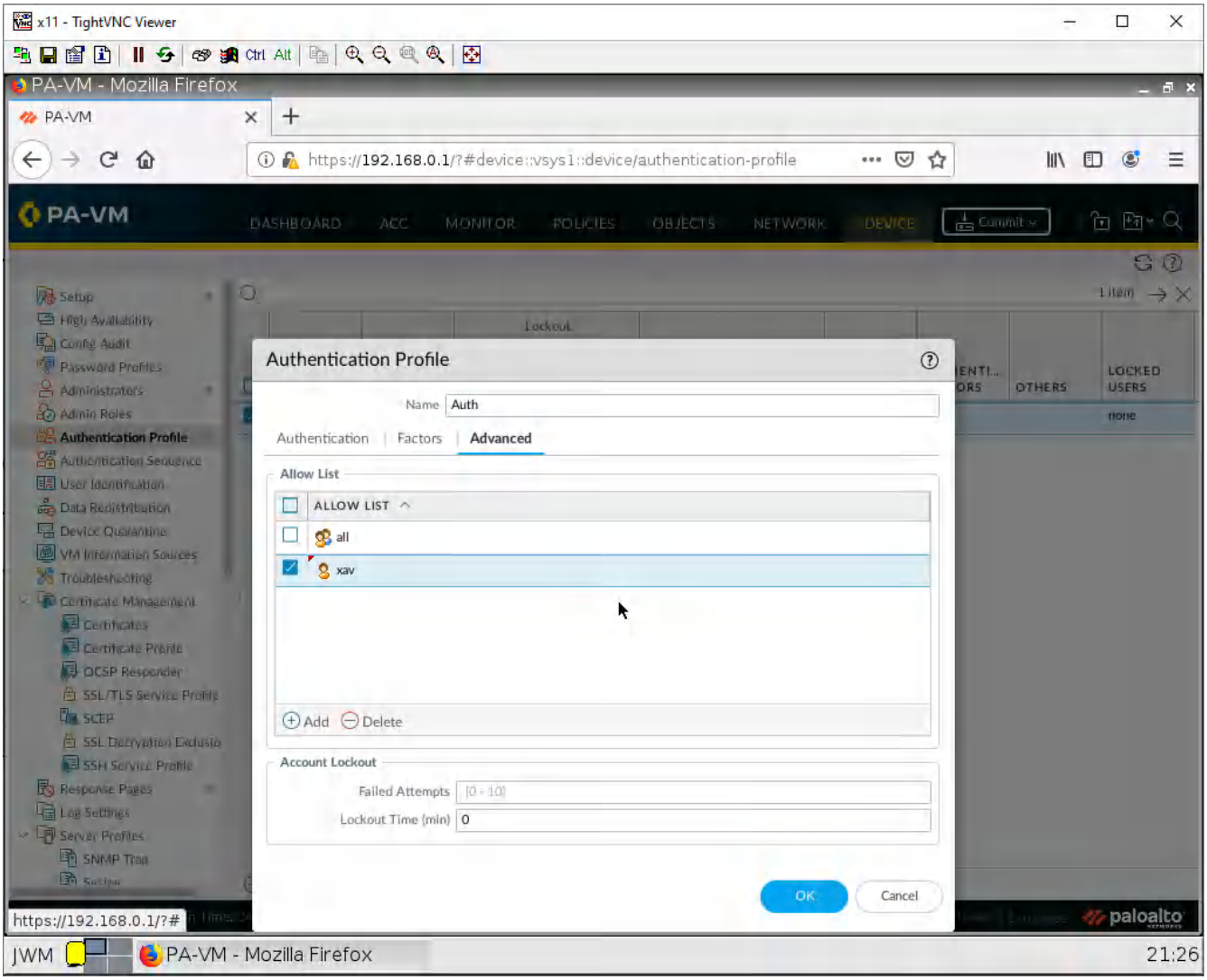


Figure 3.15: Add user xav as Allow List

Then press **OK**.

Configure the Captive Portal

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

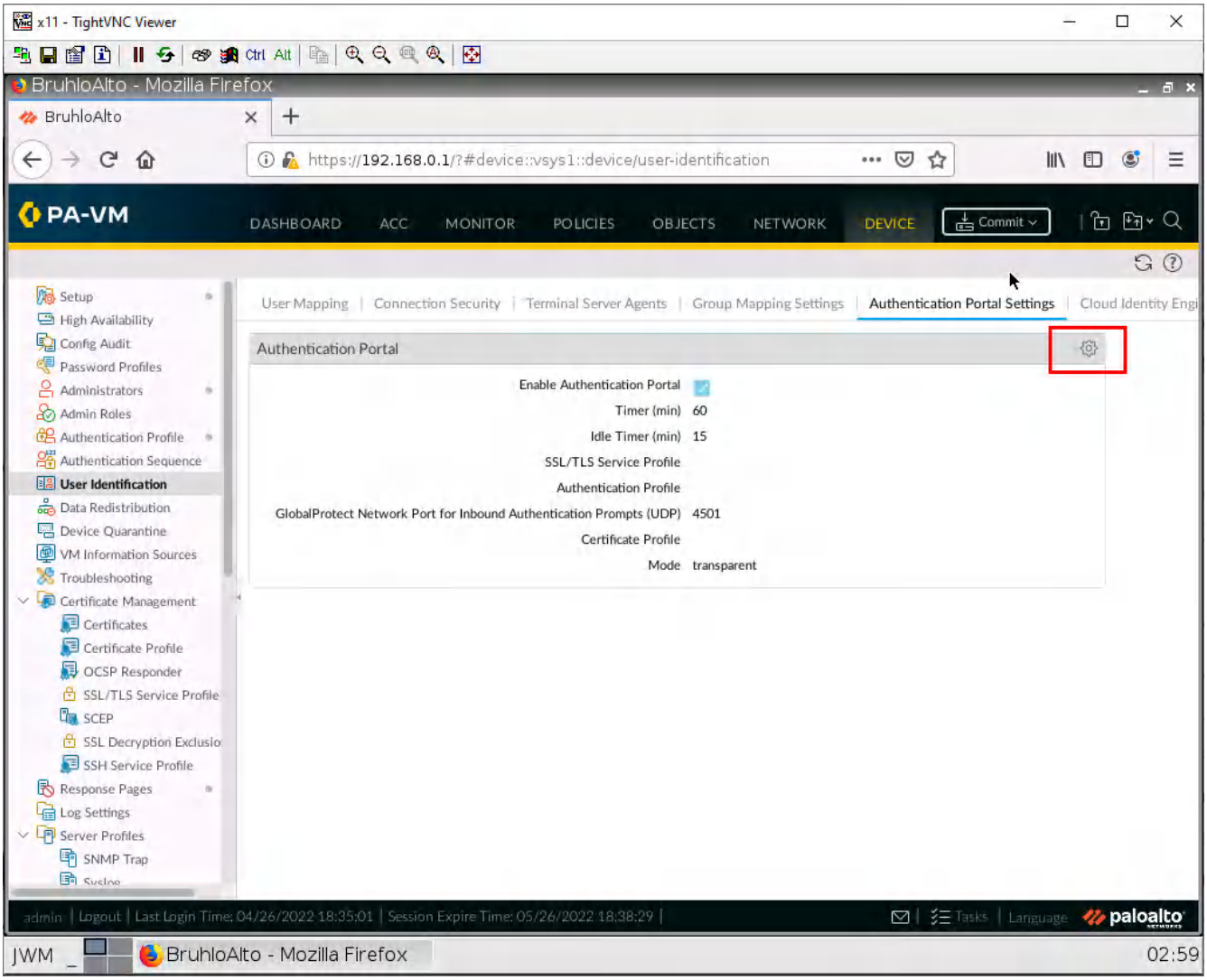


Figure 3.16: Authentication Portal Settings

Configure these settings:

Table 3.4: Authentication Portal Configuration

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

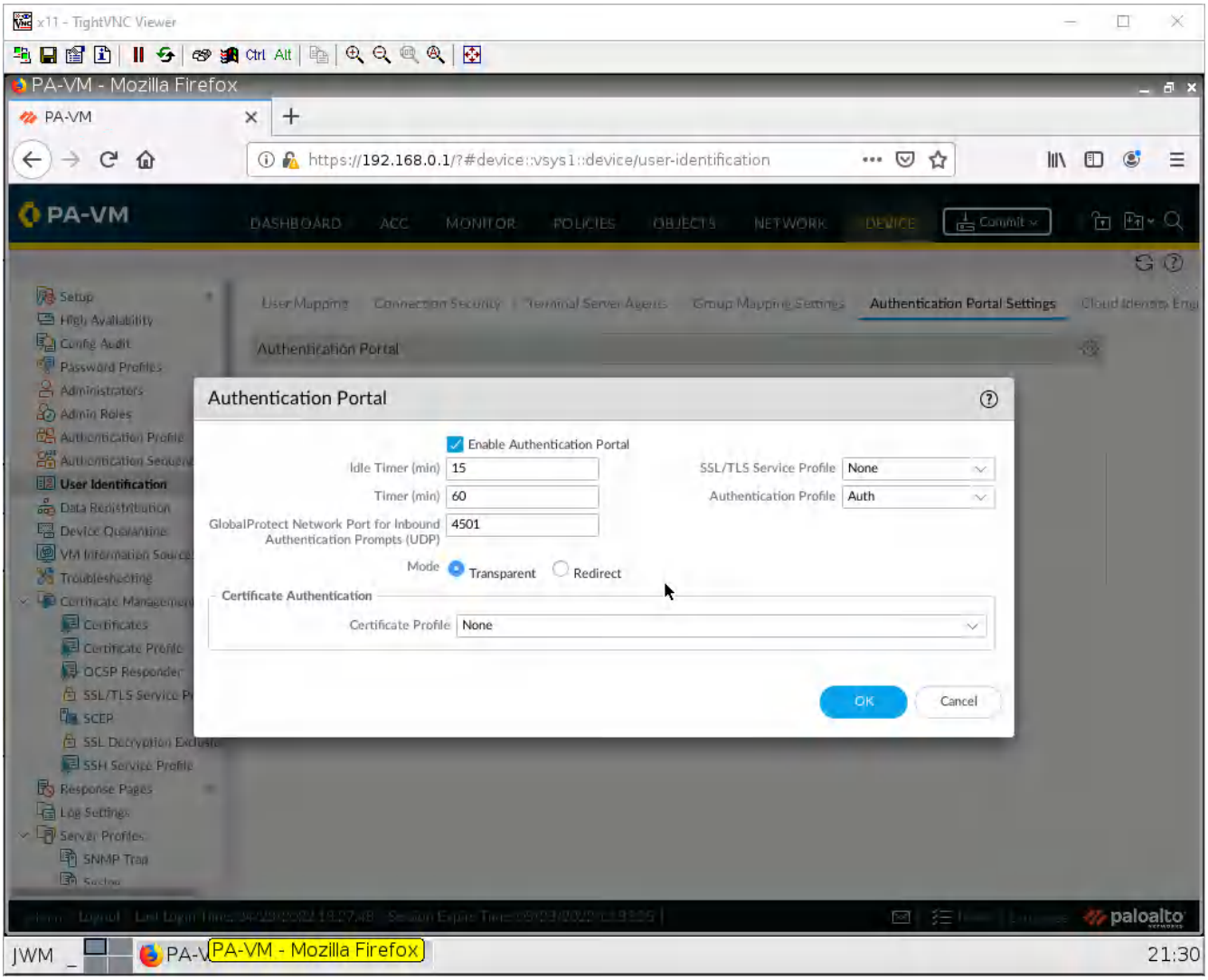


Figure 3.17: Authentication Portal Settings – Select Transparent

Then press **OK**.

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

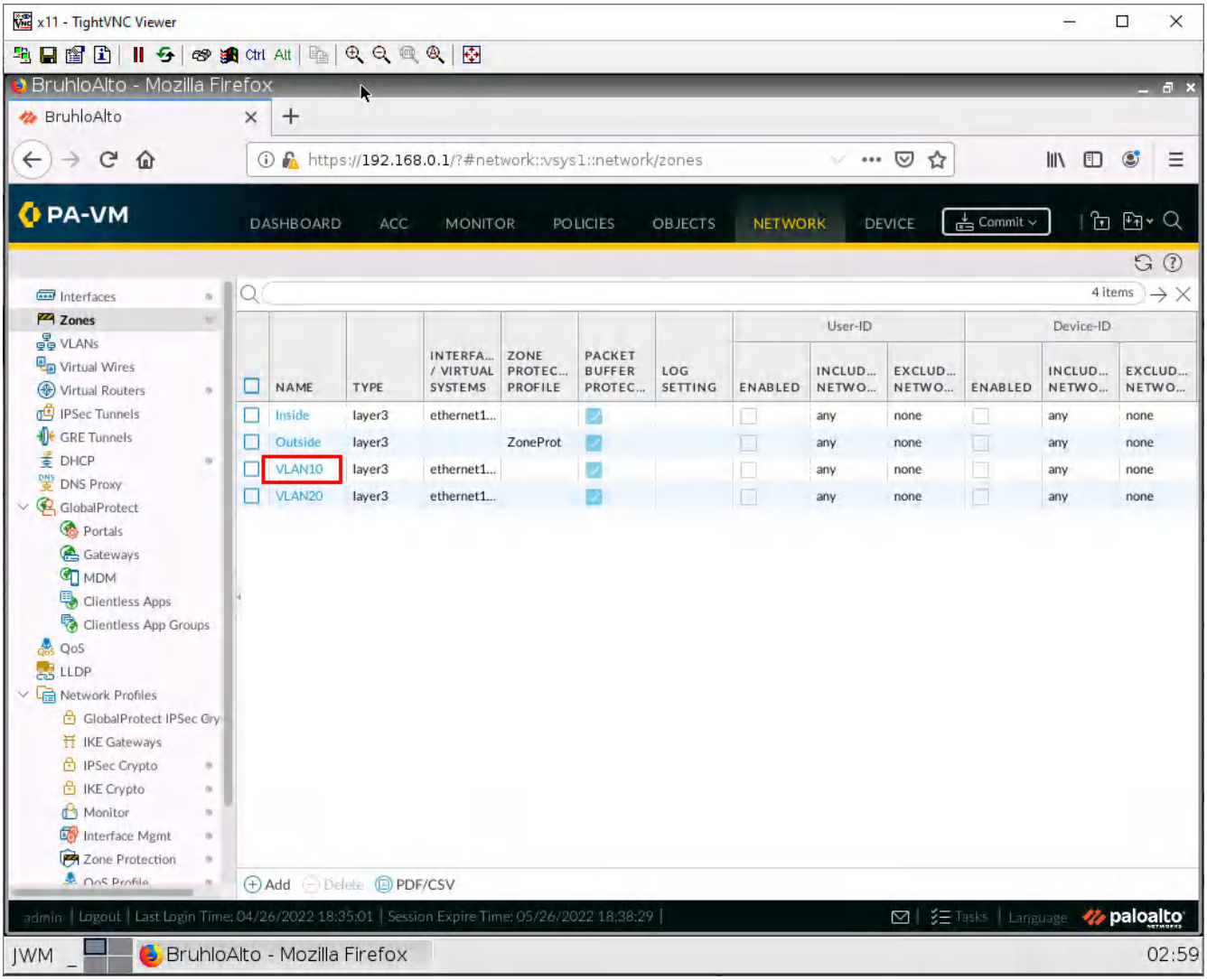


Figure 3.18: Select Vlan 10

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

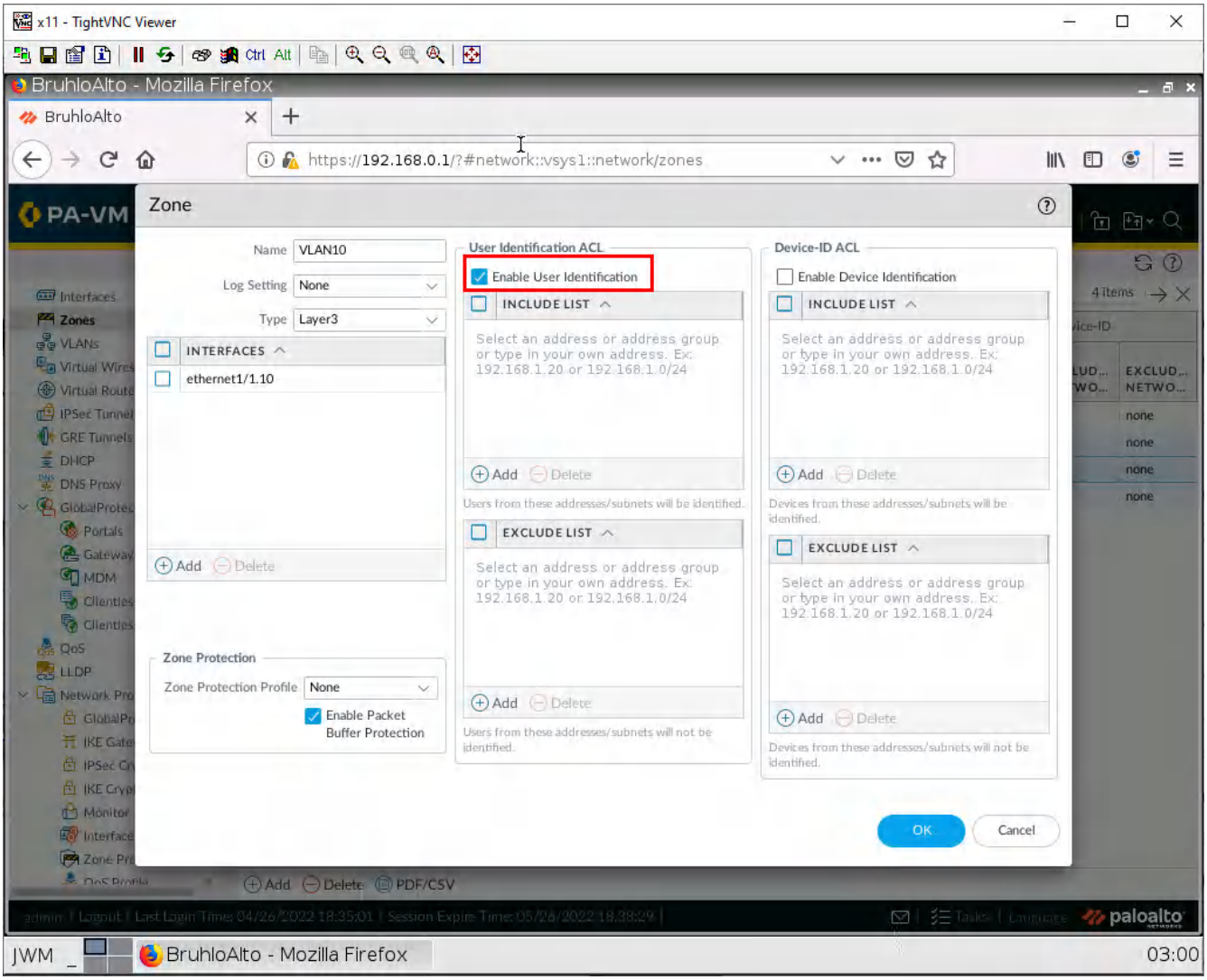


Figure 3.19: Enable User Identification

Then press **OK**.

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

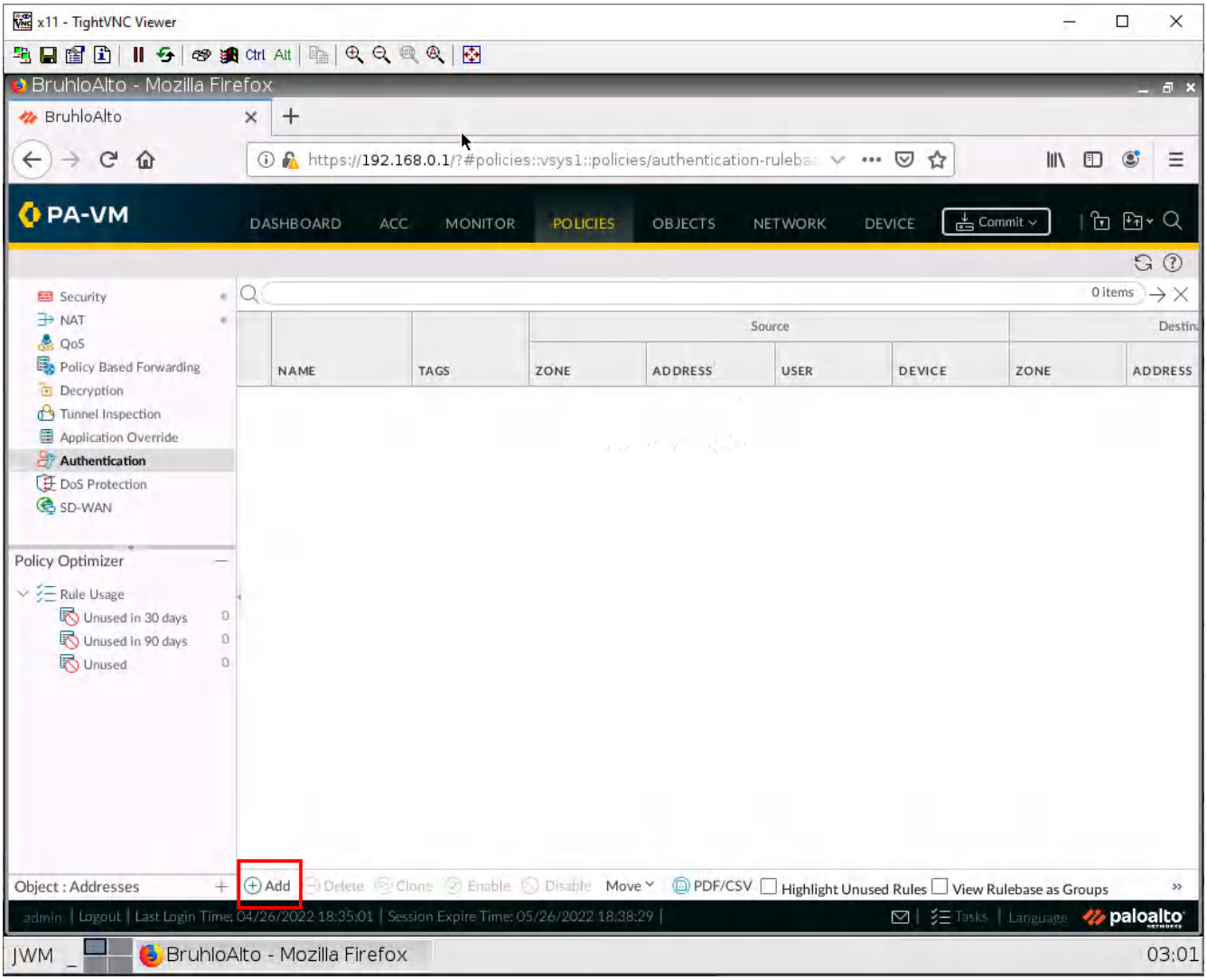


Figure 3.20: Add an authentication Policy

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

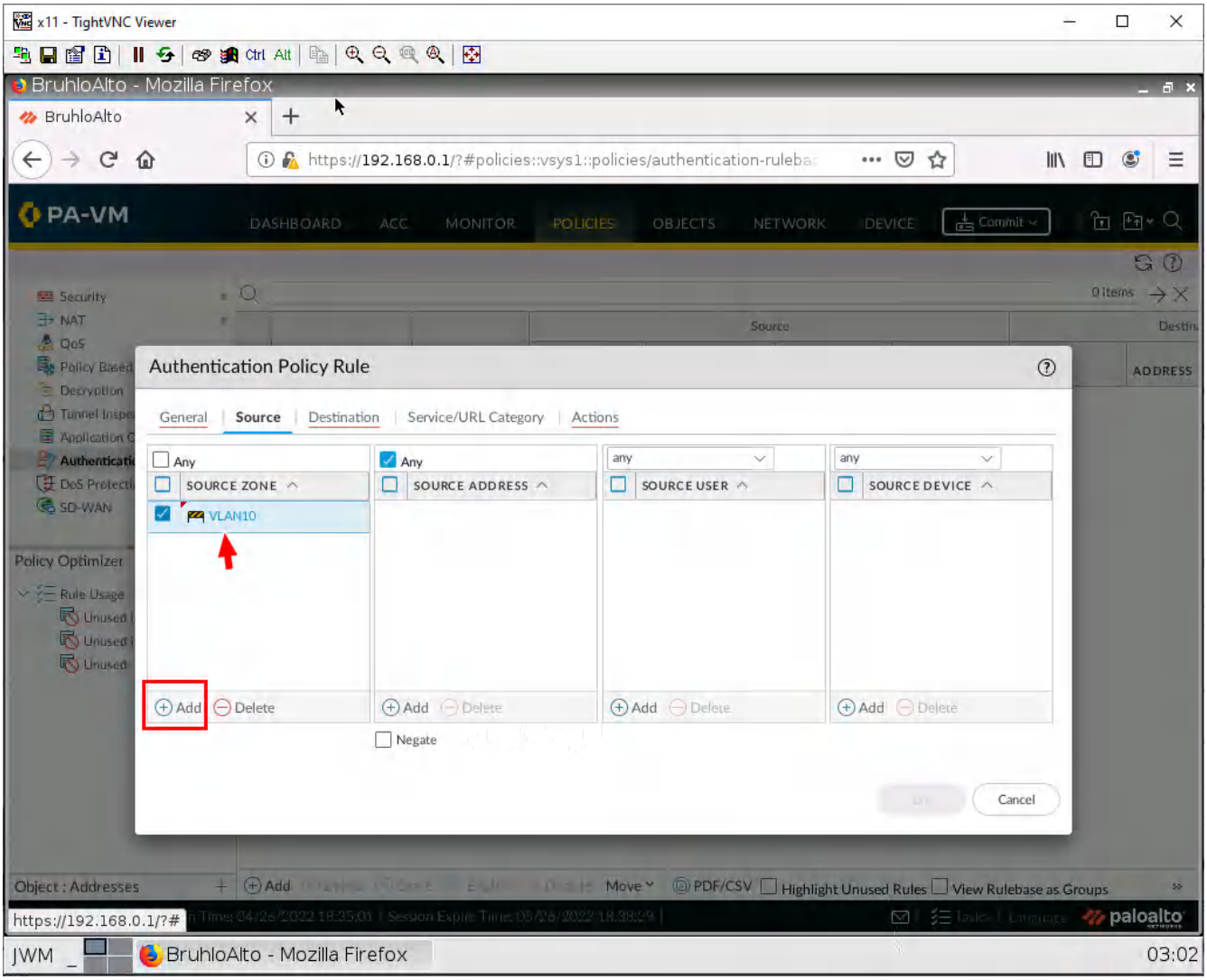


Figure 3.21: Add the Source Zone

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

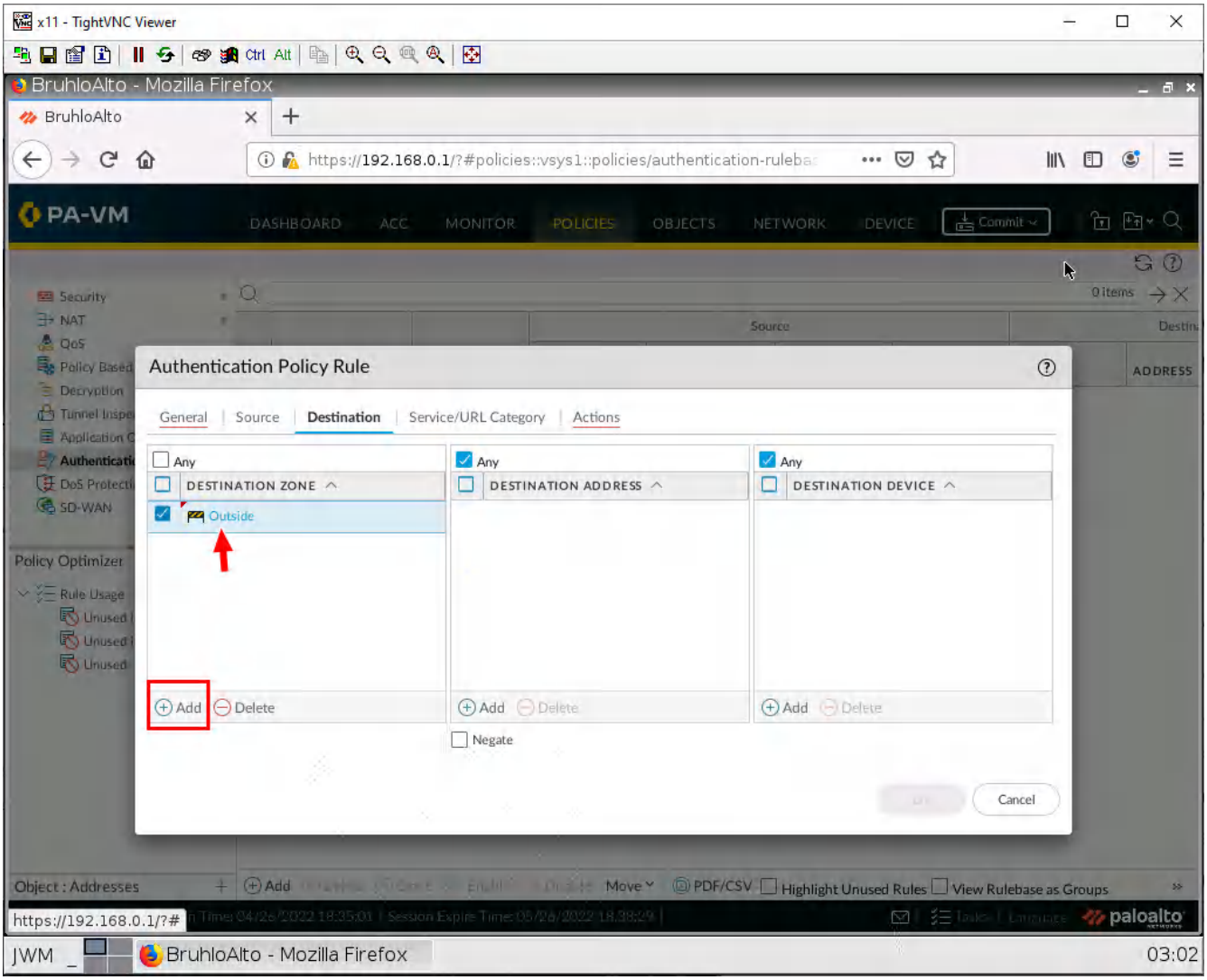


Figure 3.22: Add the Destination Zone

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

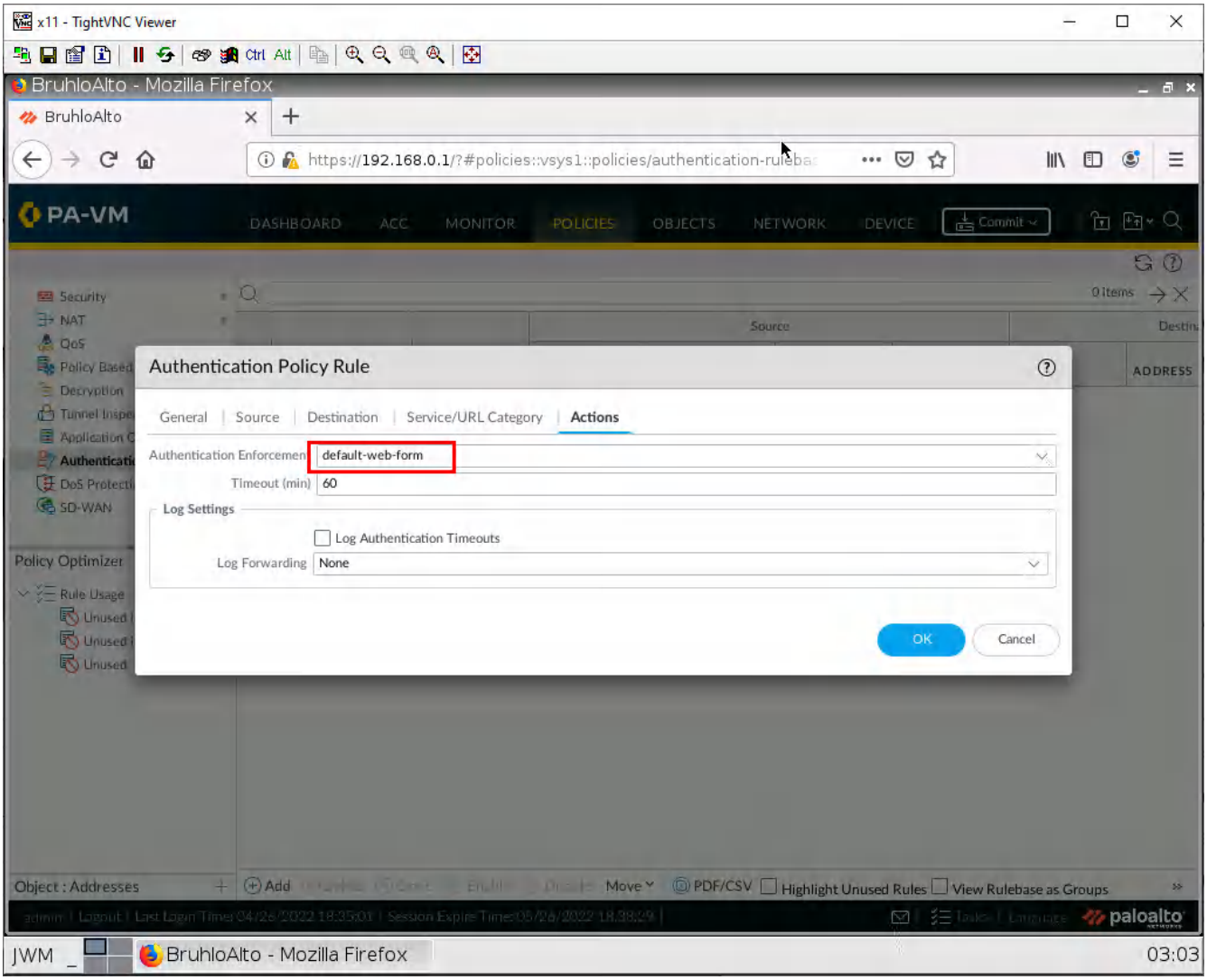


Figure 3.23: Select default-web-form

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.

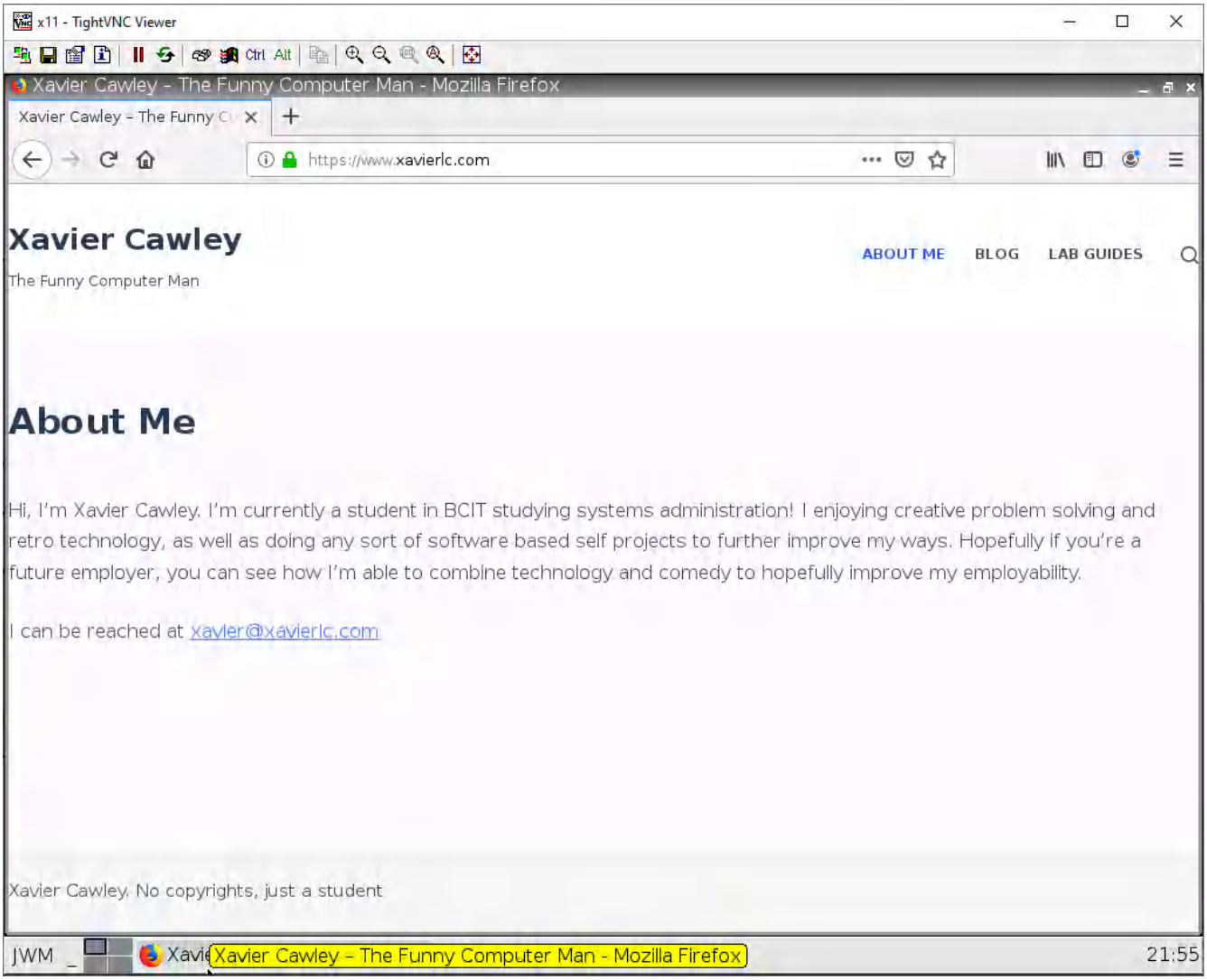


Figure 3.24: Verify your configuration

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.

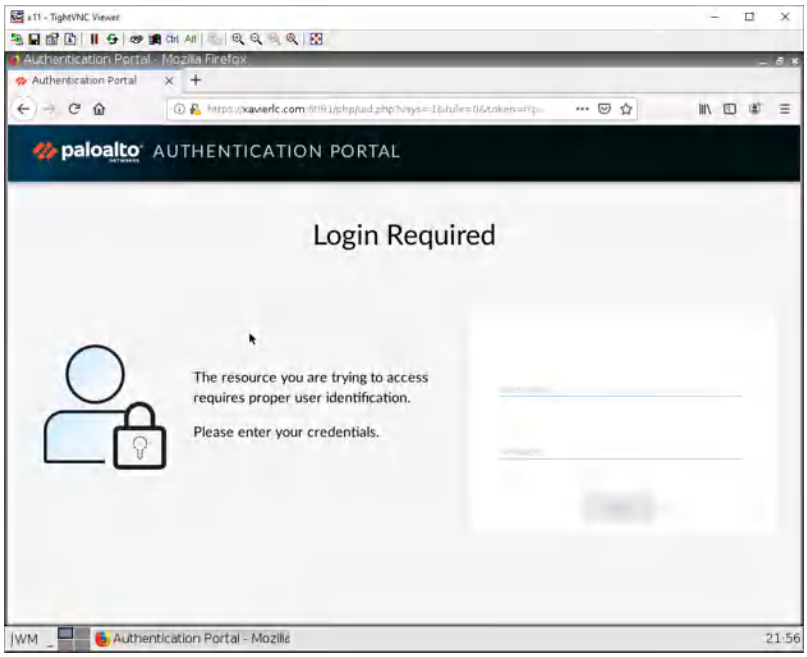


Figure 3.25: Login Page

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

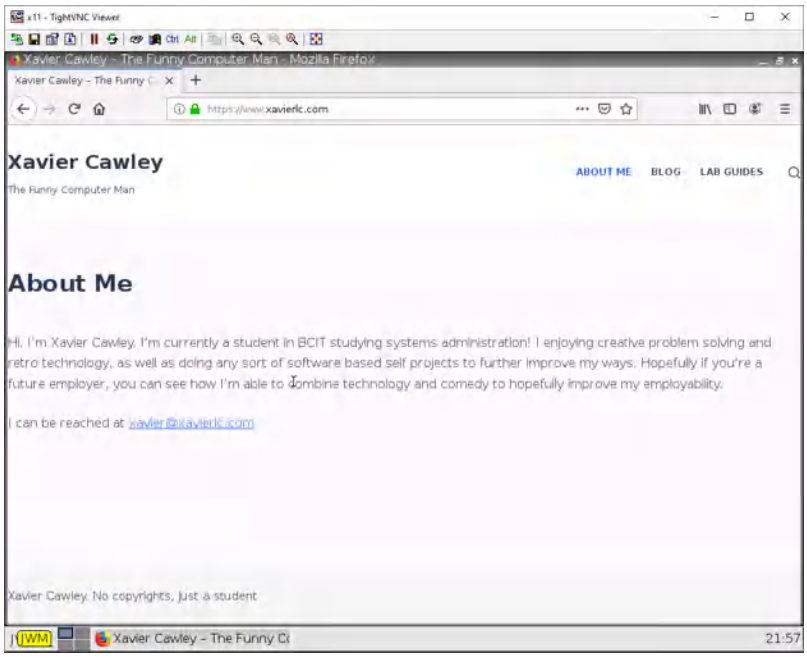


Figure 3.26: Verify your configuration

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.

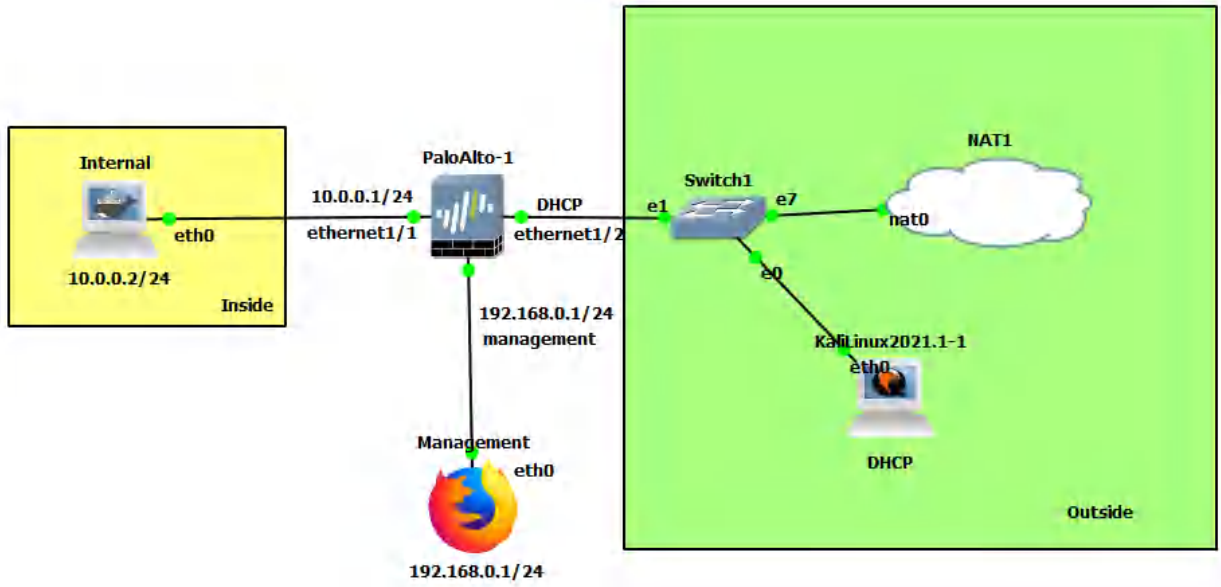


Figure 3.27: Main scenario

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**.

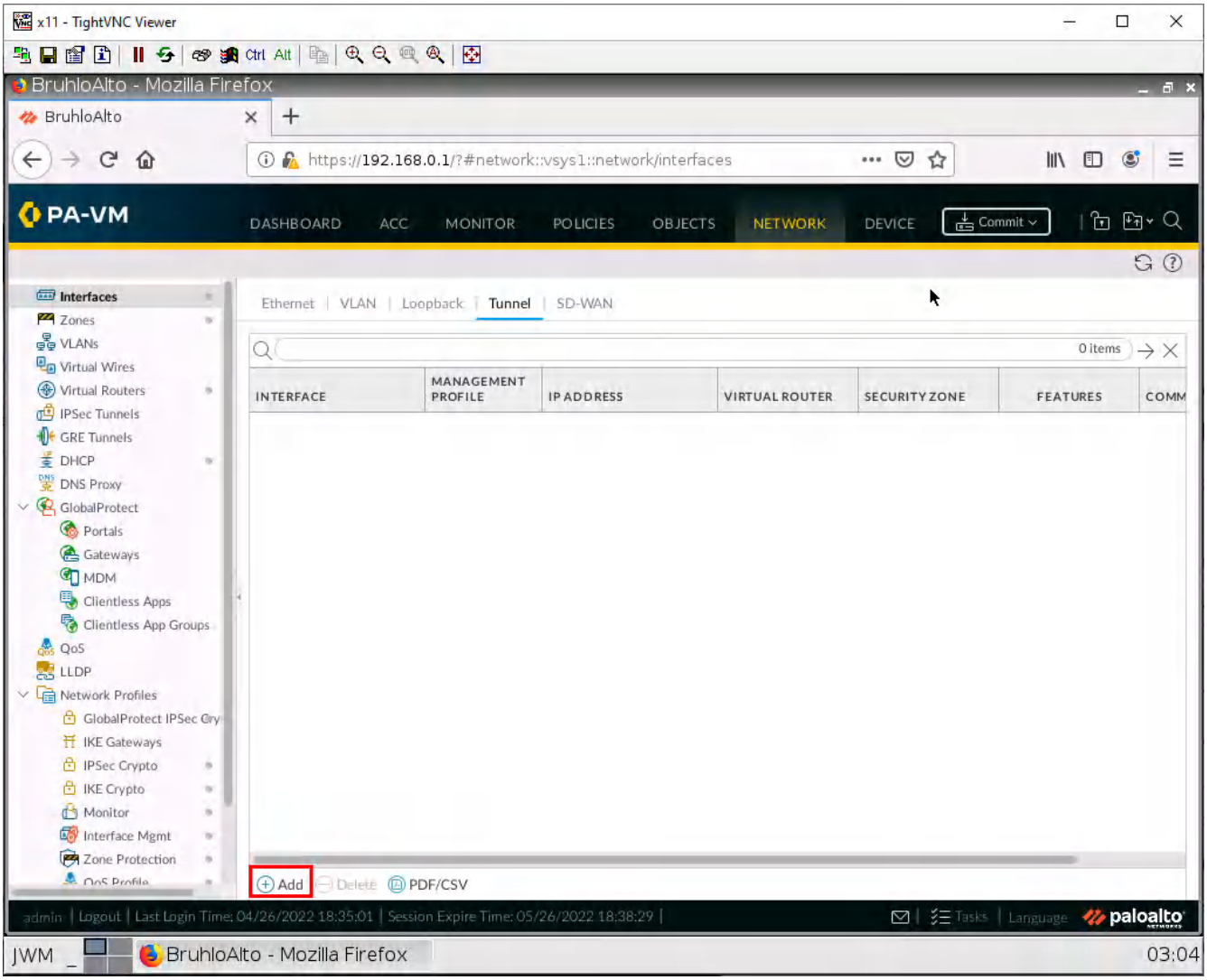


Figure 3.28: Creating a Tunnel

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

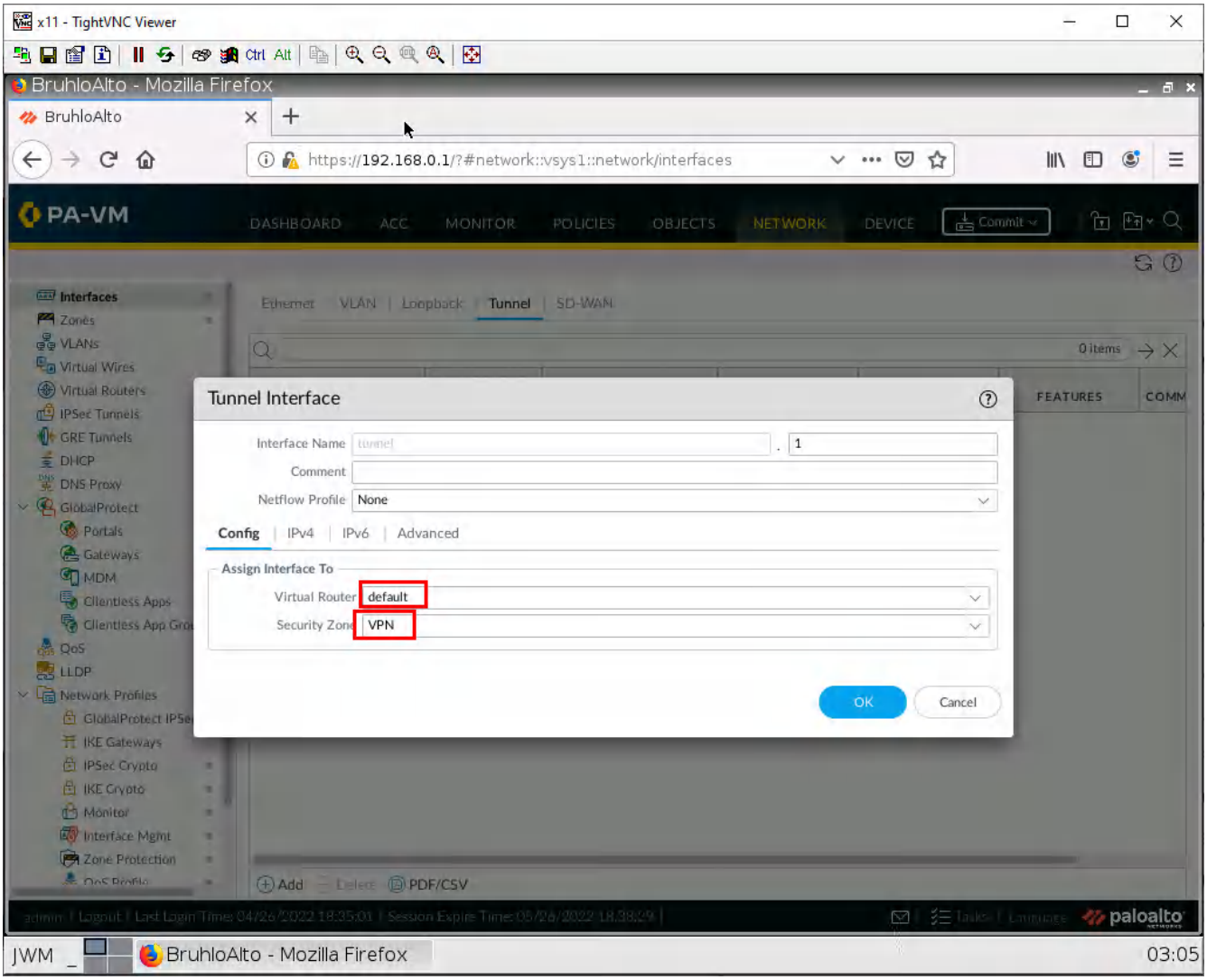


Figure 3.29: Tunnel Interface

Then click **OK**.

Enable User ACL for a Zone

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

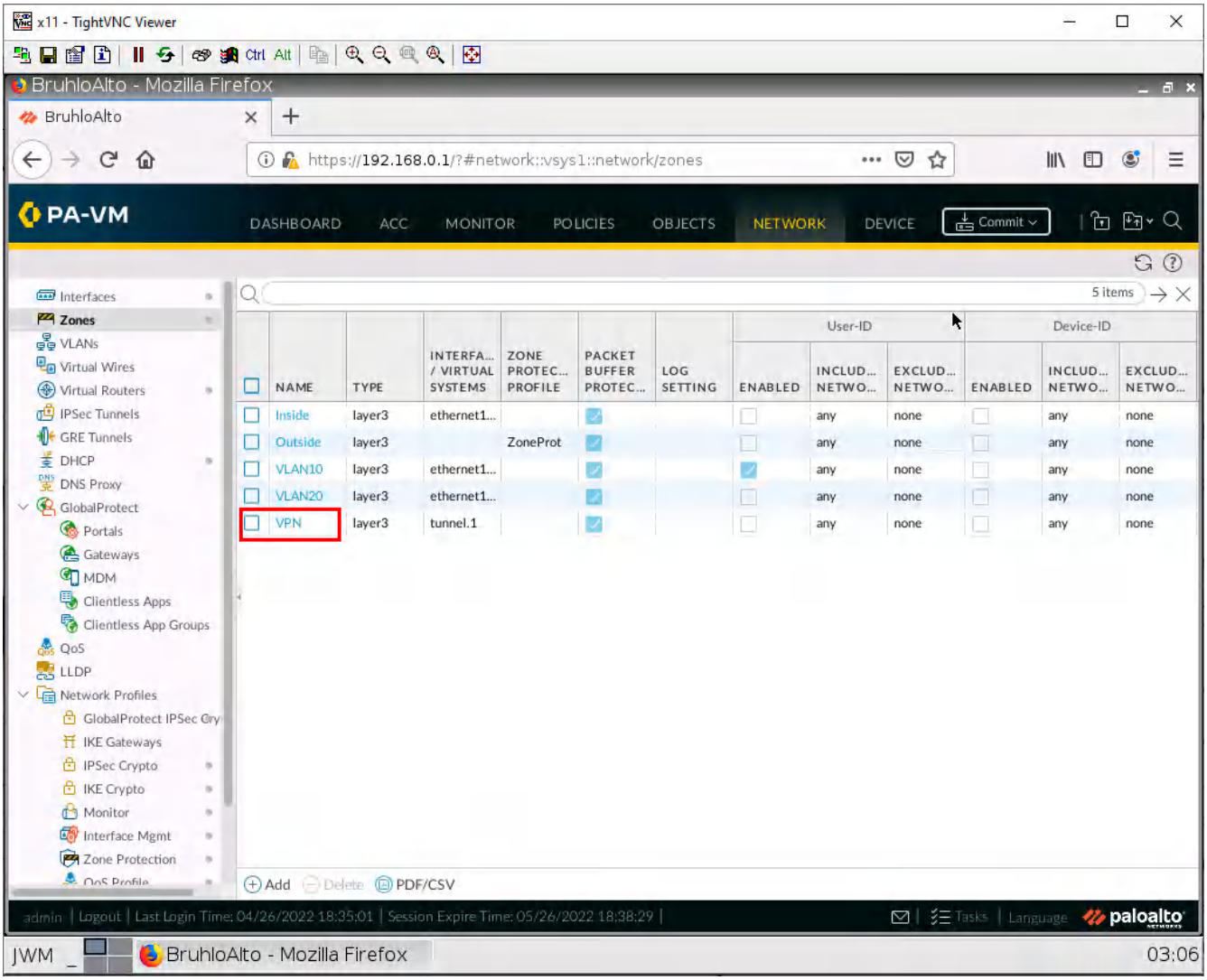


Figure 3.30: Create a VPN Zone

Tick the **Enable user identification** box.

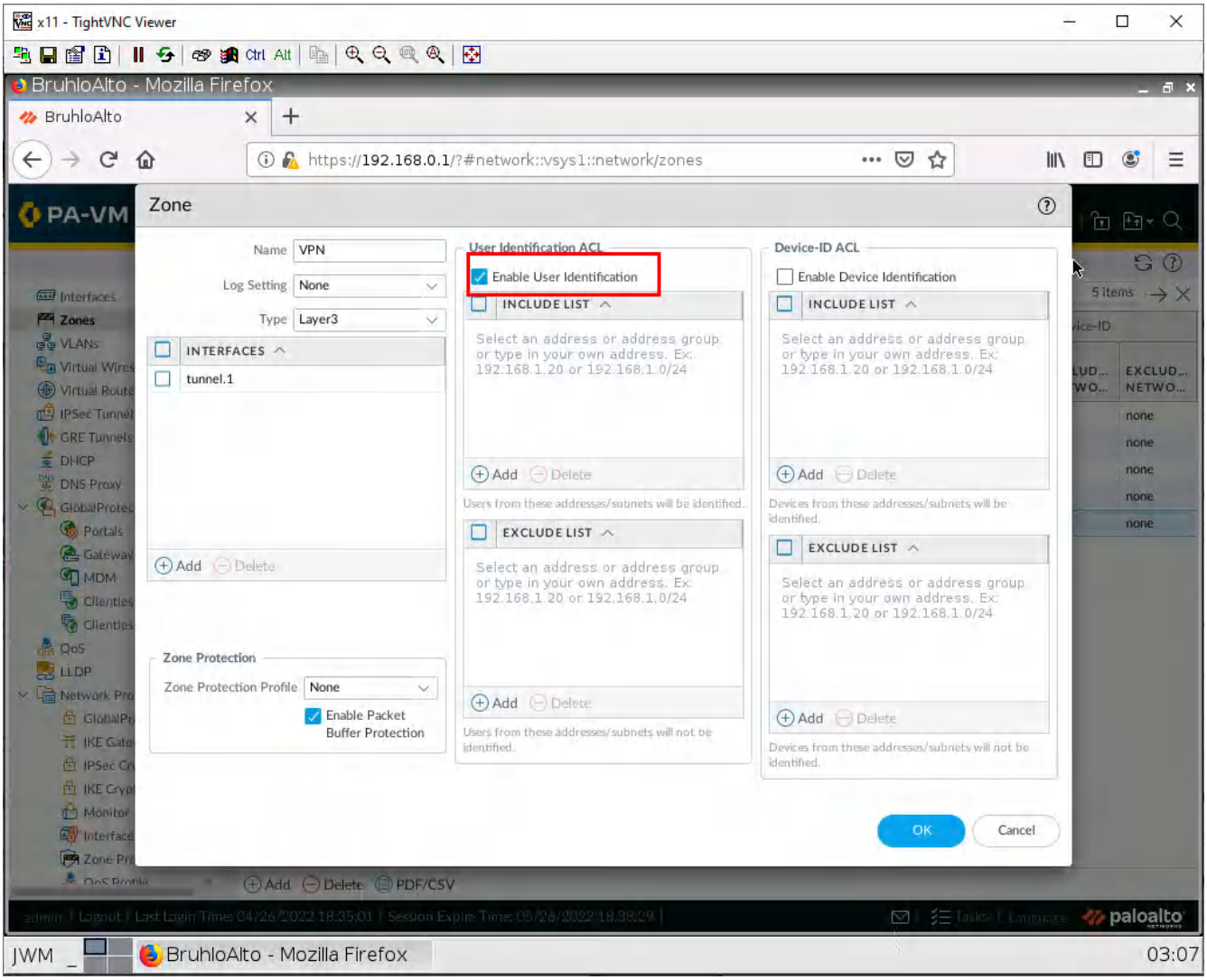


Figure 3.31: Enable User Identification under VPN Zone

Then press **OK**.

Generate Certs

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

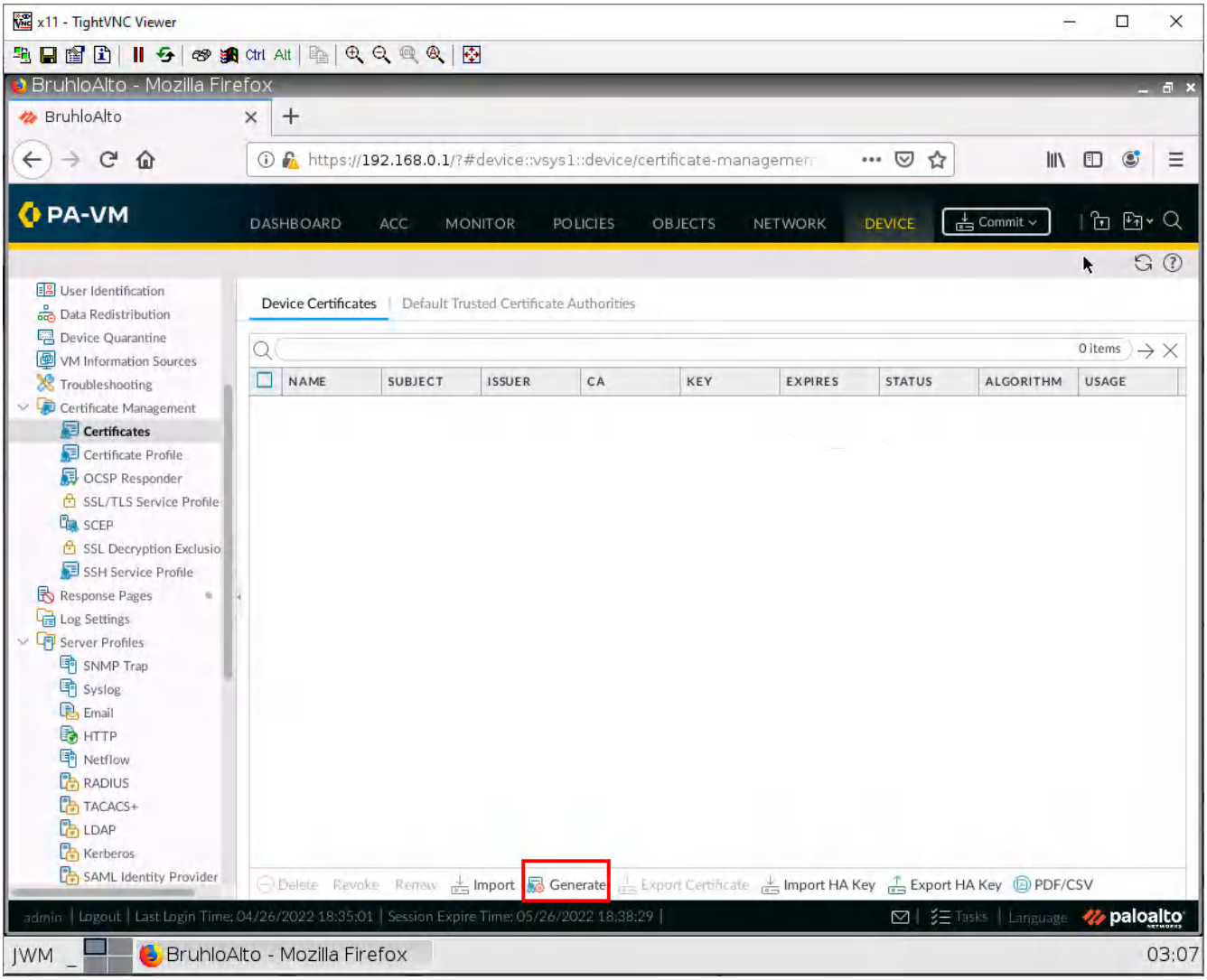


Figure 3.32: Generate a certificate

Configure these settings in the new window:

Table 3.7: Certificate Generation

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

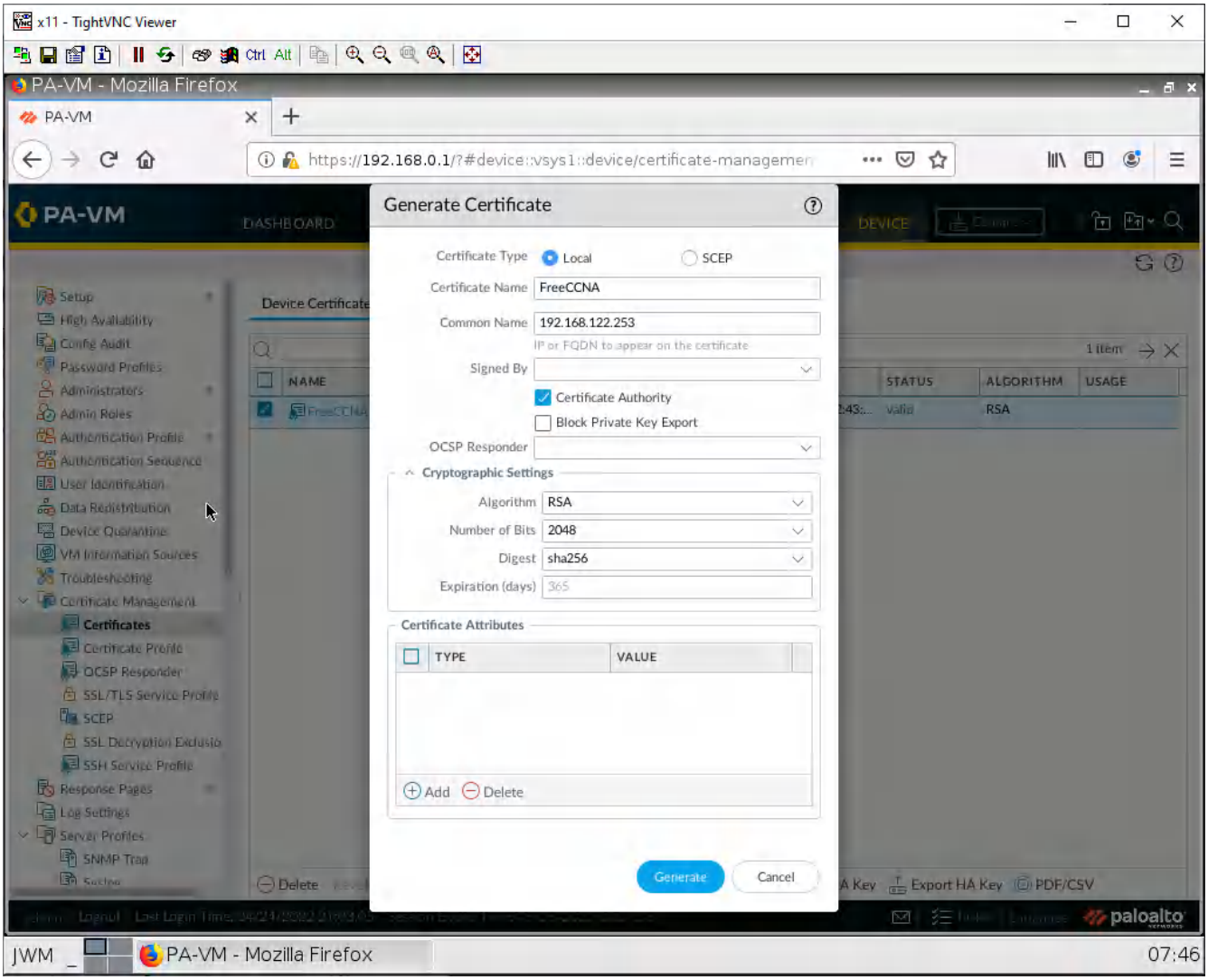


Figure 3.33: Generate a certificate

Then click **Generate**.

Create an SSL/TLS Service Profile

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

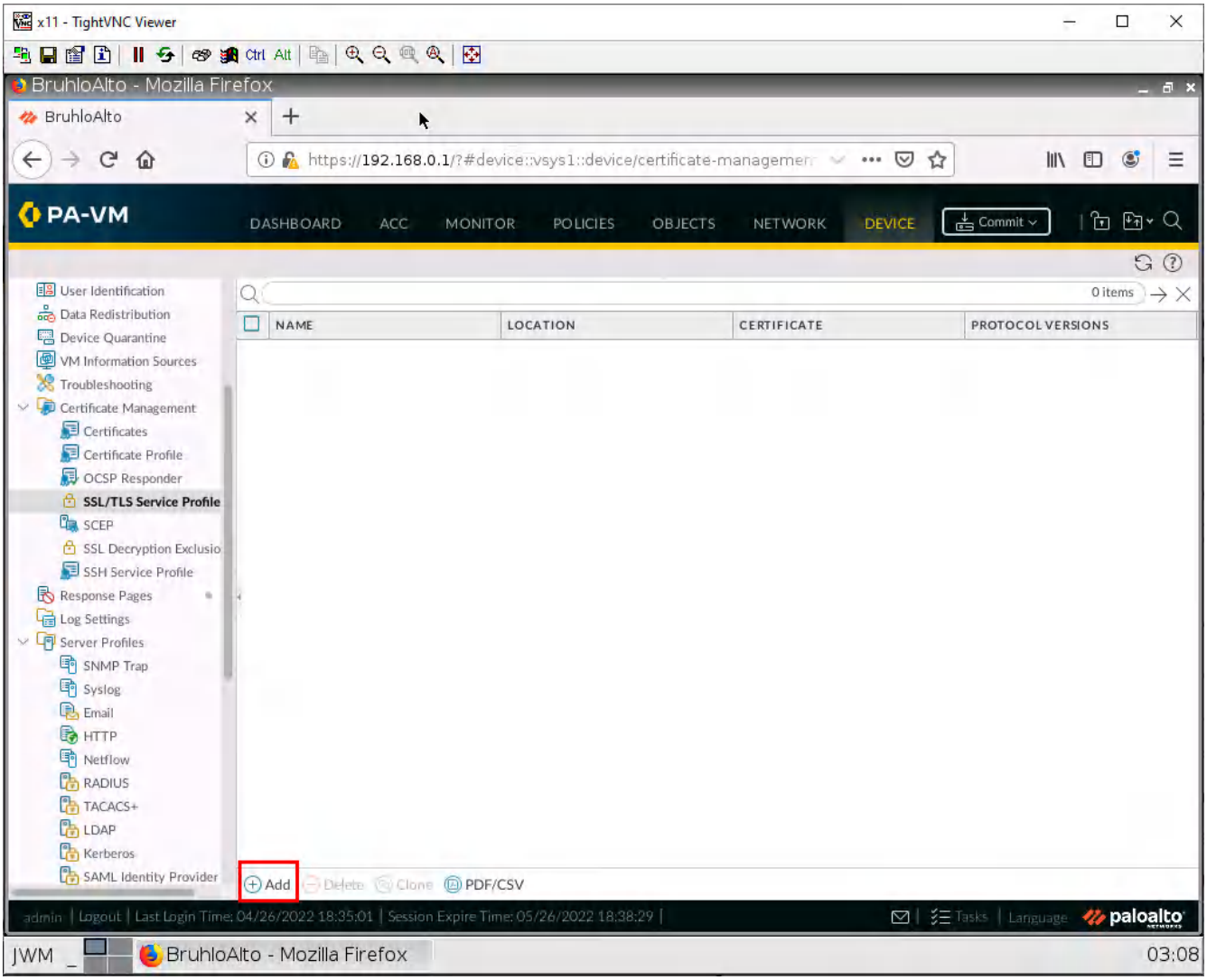


Figure 3.34: Add SSL/TLS Service Profile

In the new window, add the certificate you generated.

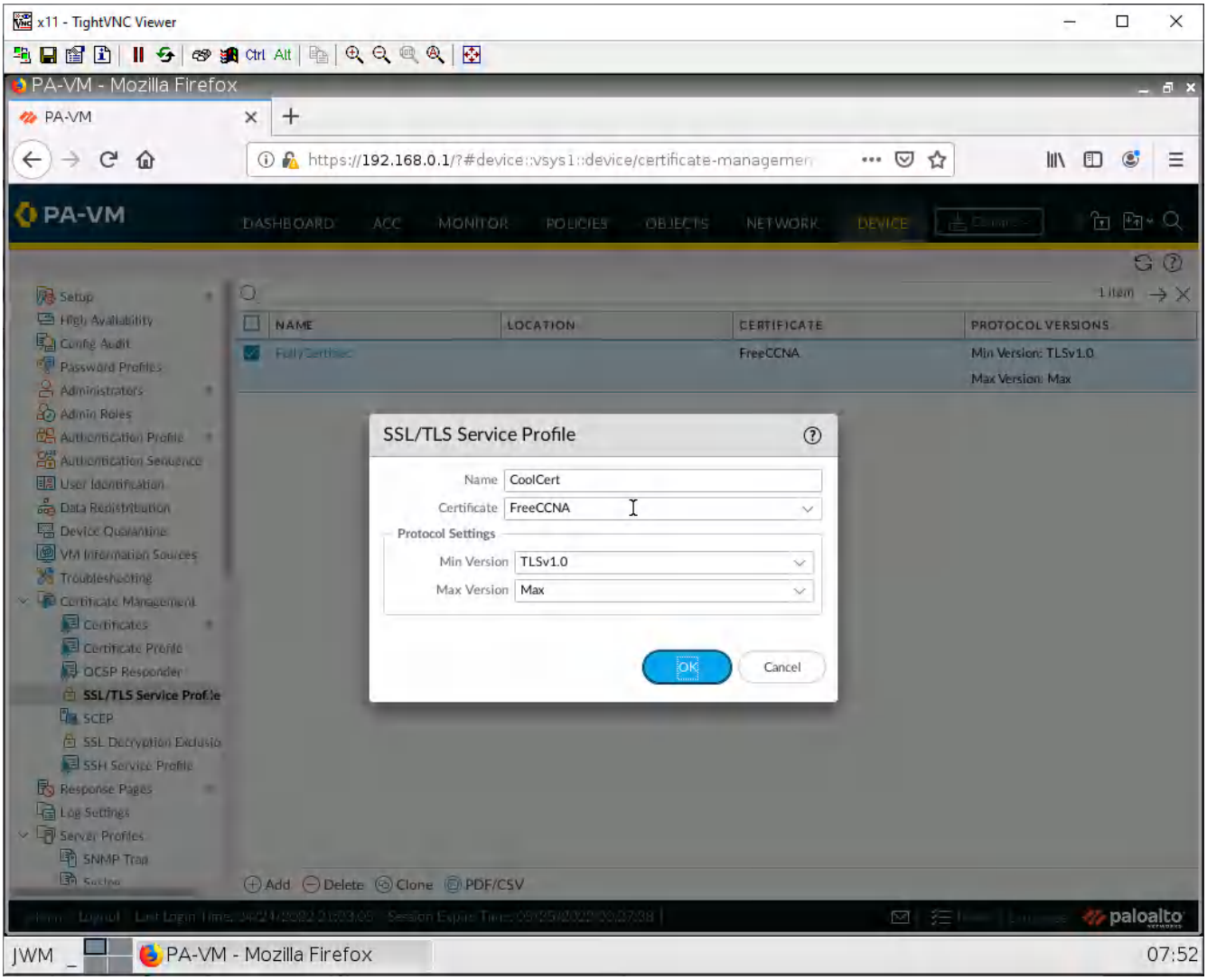


Figure 3.35: Configure SSL/TLS Service Profile

Then click **OK**.

Create a GlobalProtect Portal

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

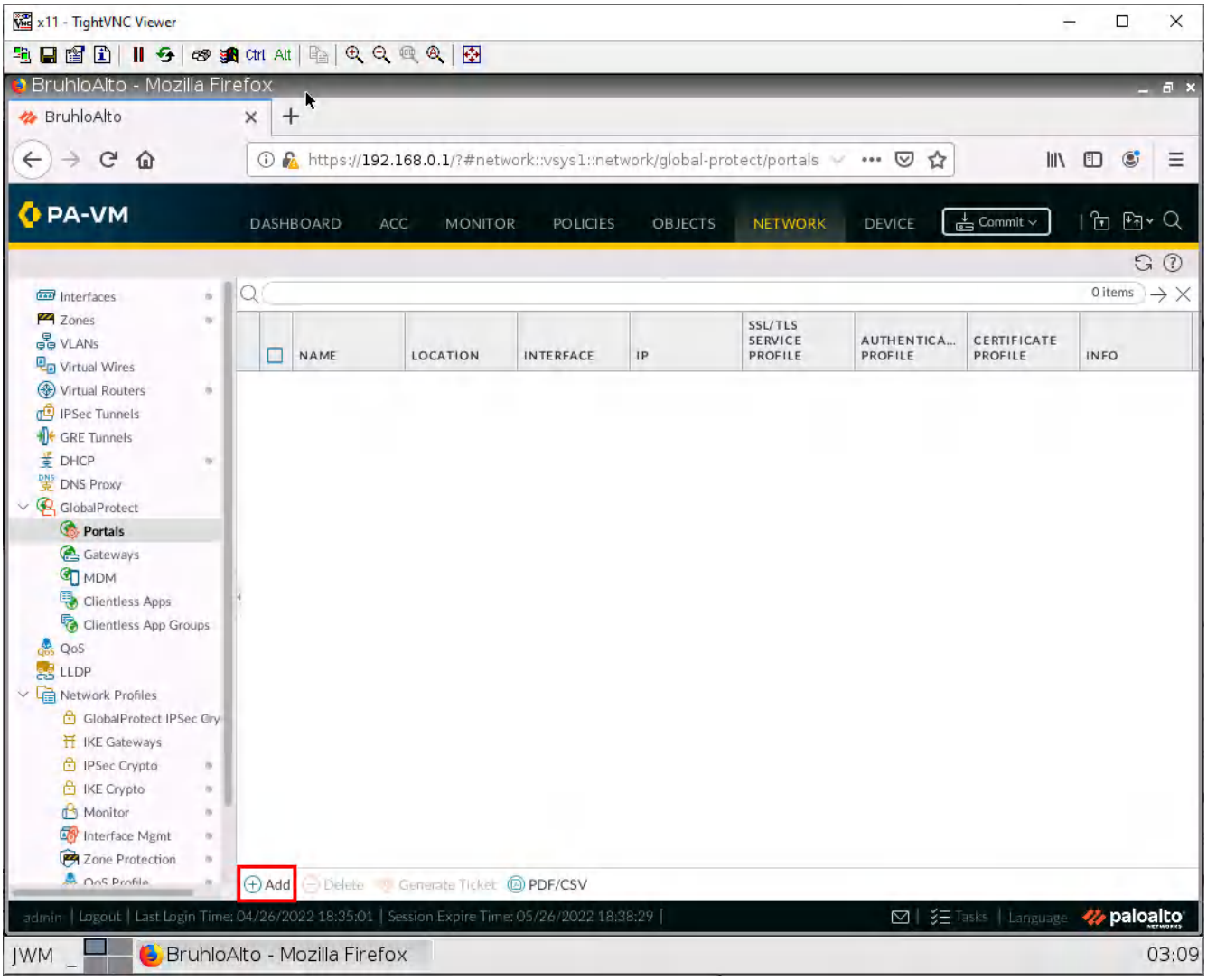


Figure 3.36: Add a Portal

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

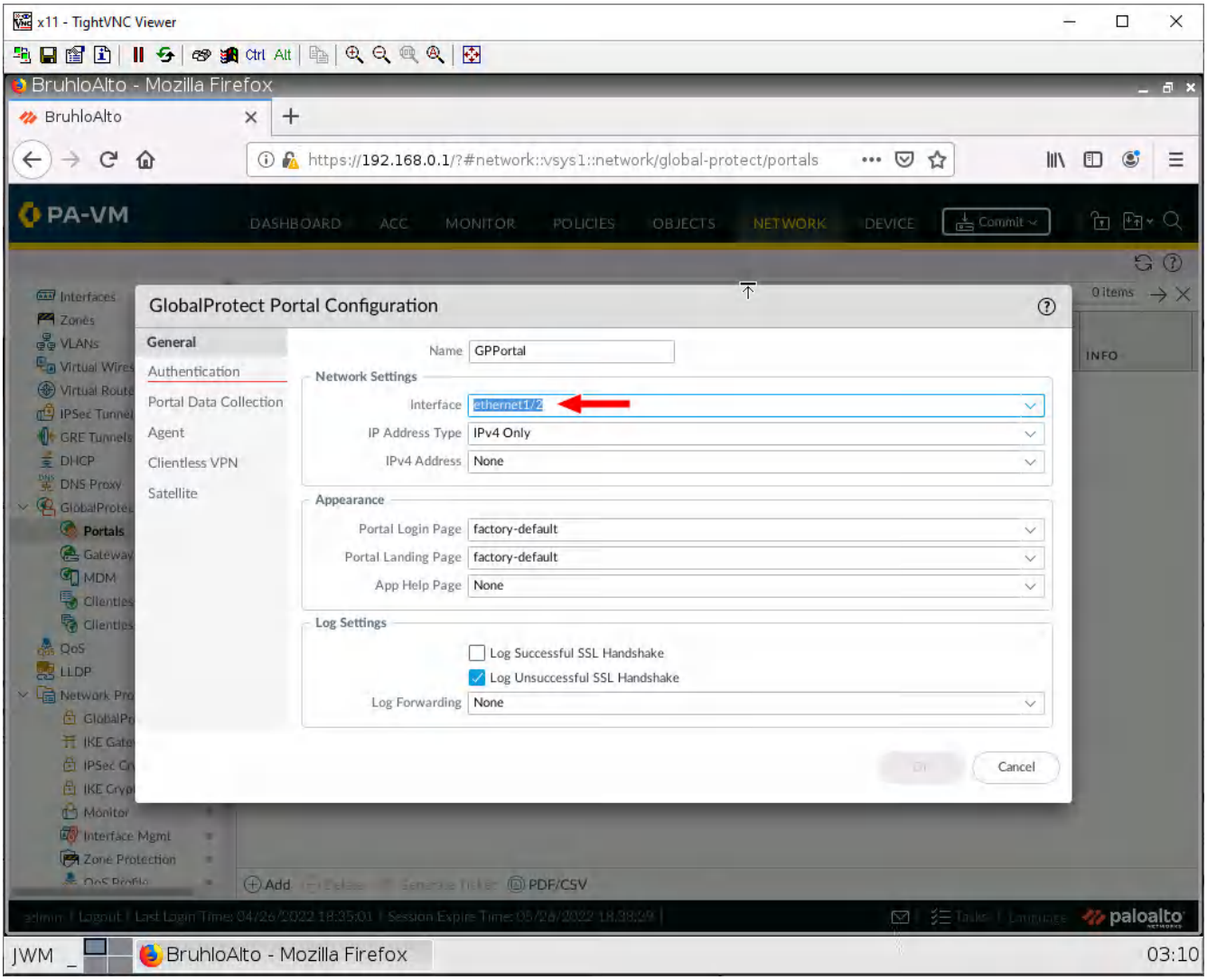


Figure 3.37: GlobalProtect Portal Configuration

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

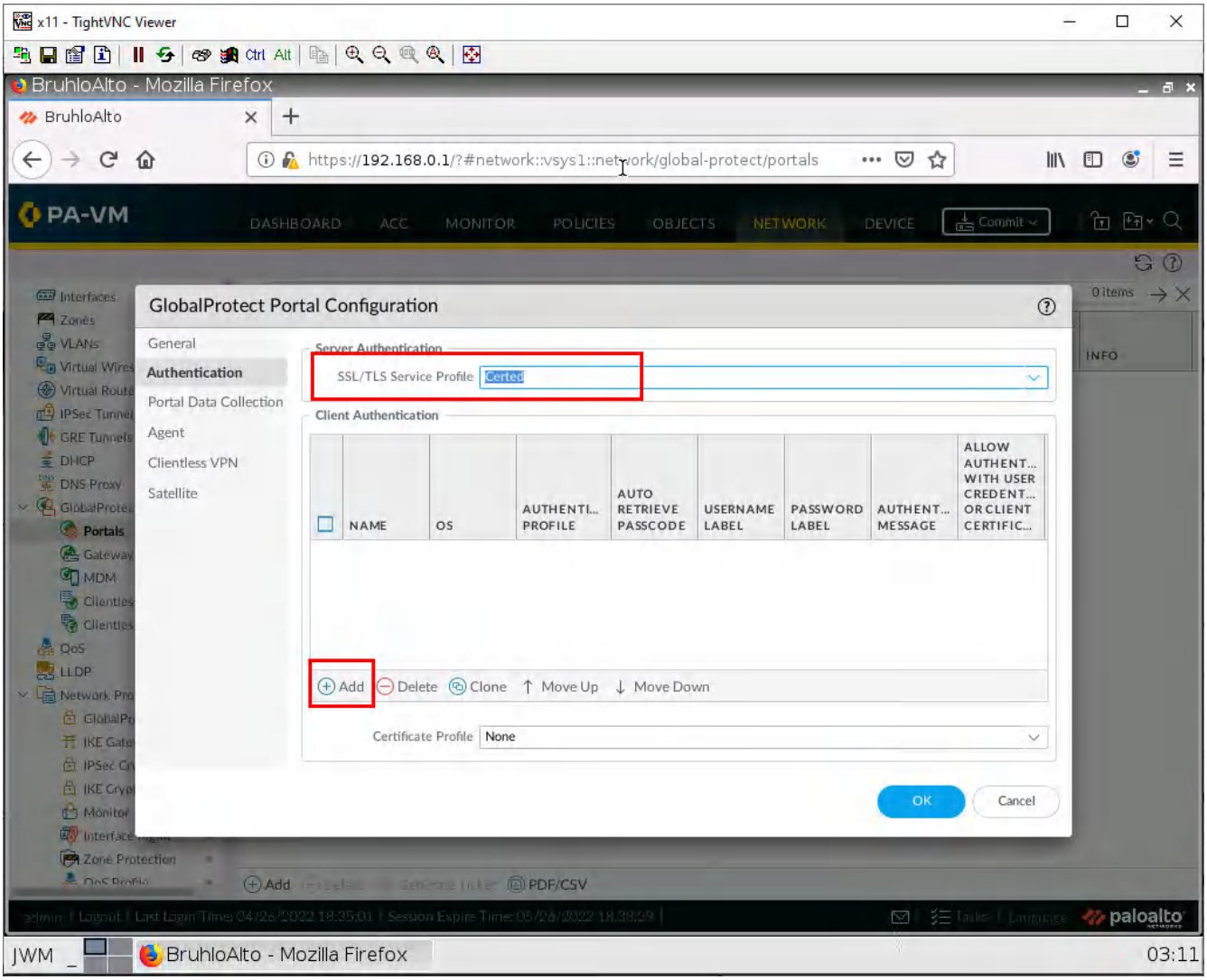


Figure 3.38: Adding SSL/TLS Profile

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

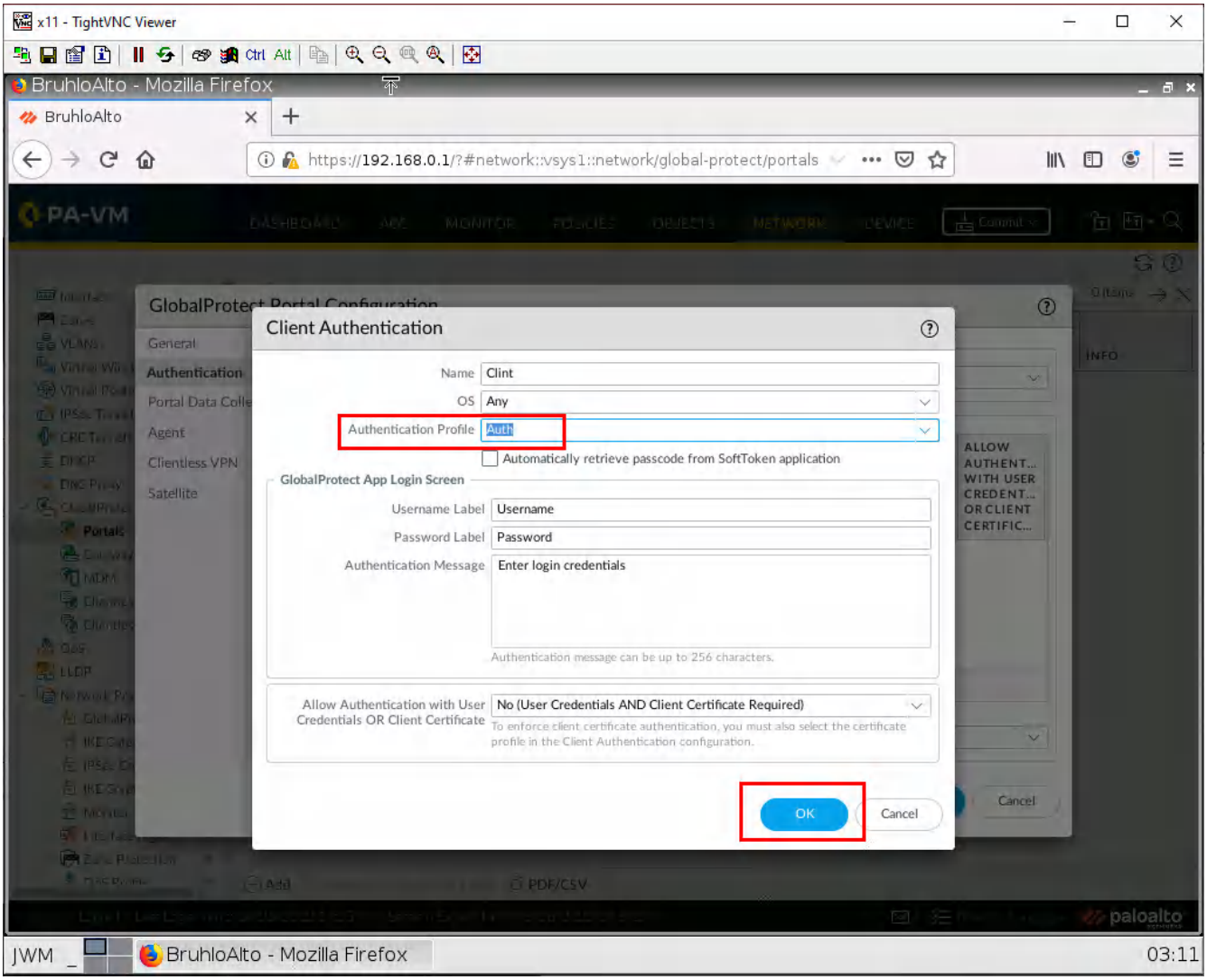


Figure 3.39: Adding Authentication Profile

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

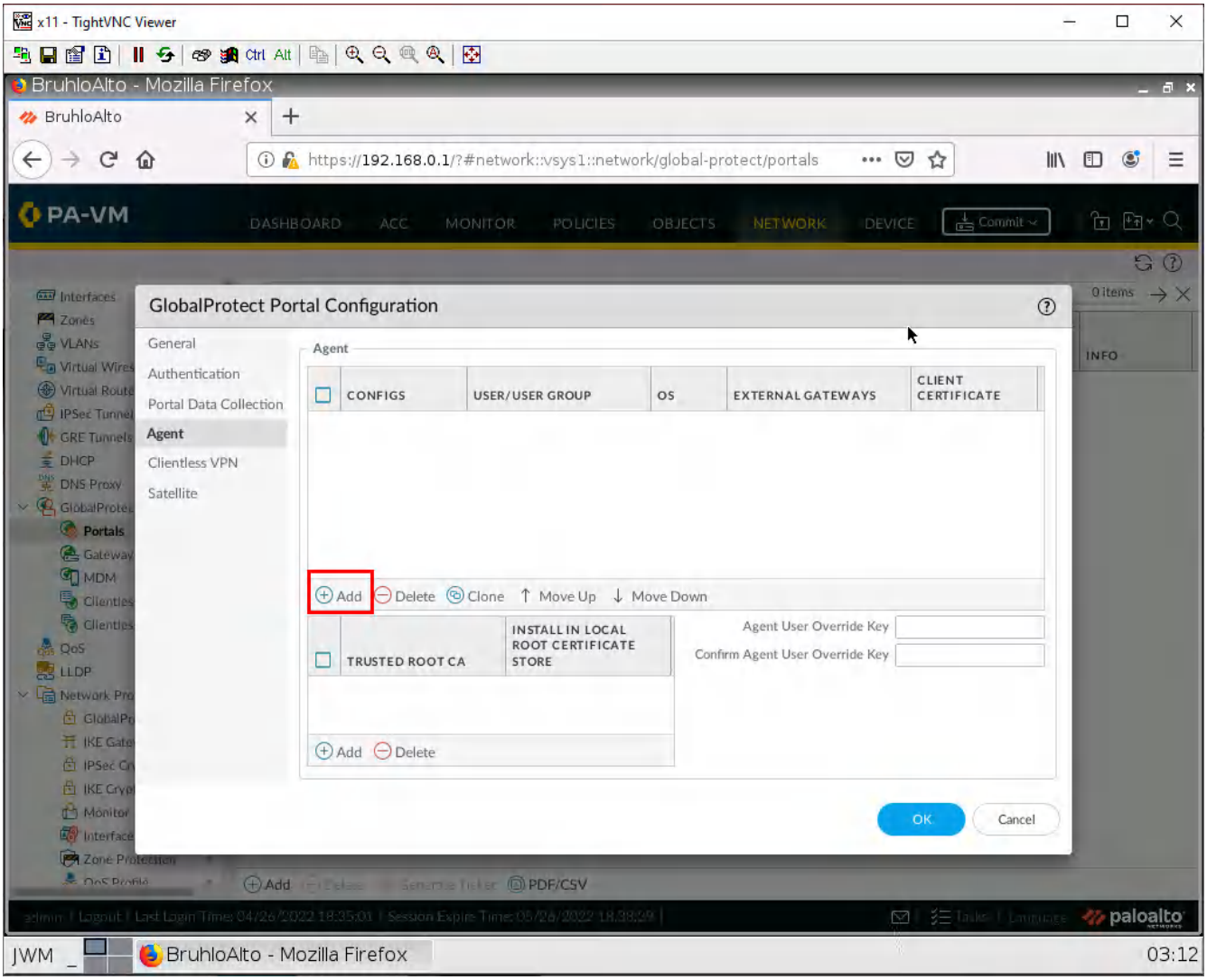


Figure 3.40: Adding the agent

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

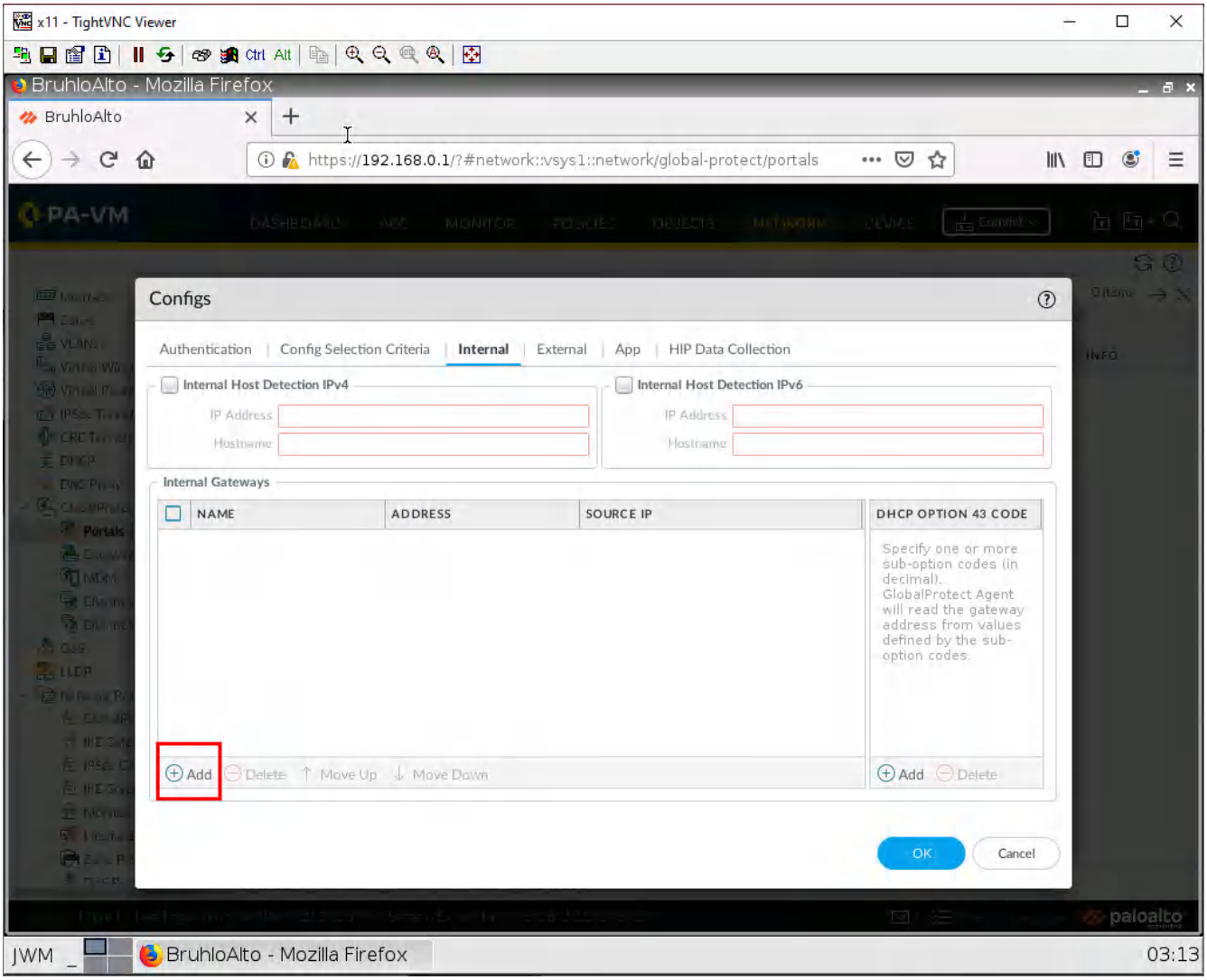


Figure 3.41: Configure Internal Gateway

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

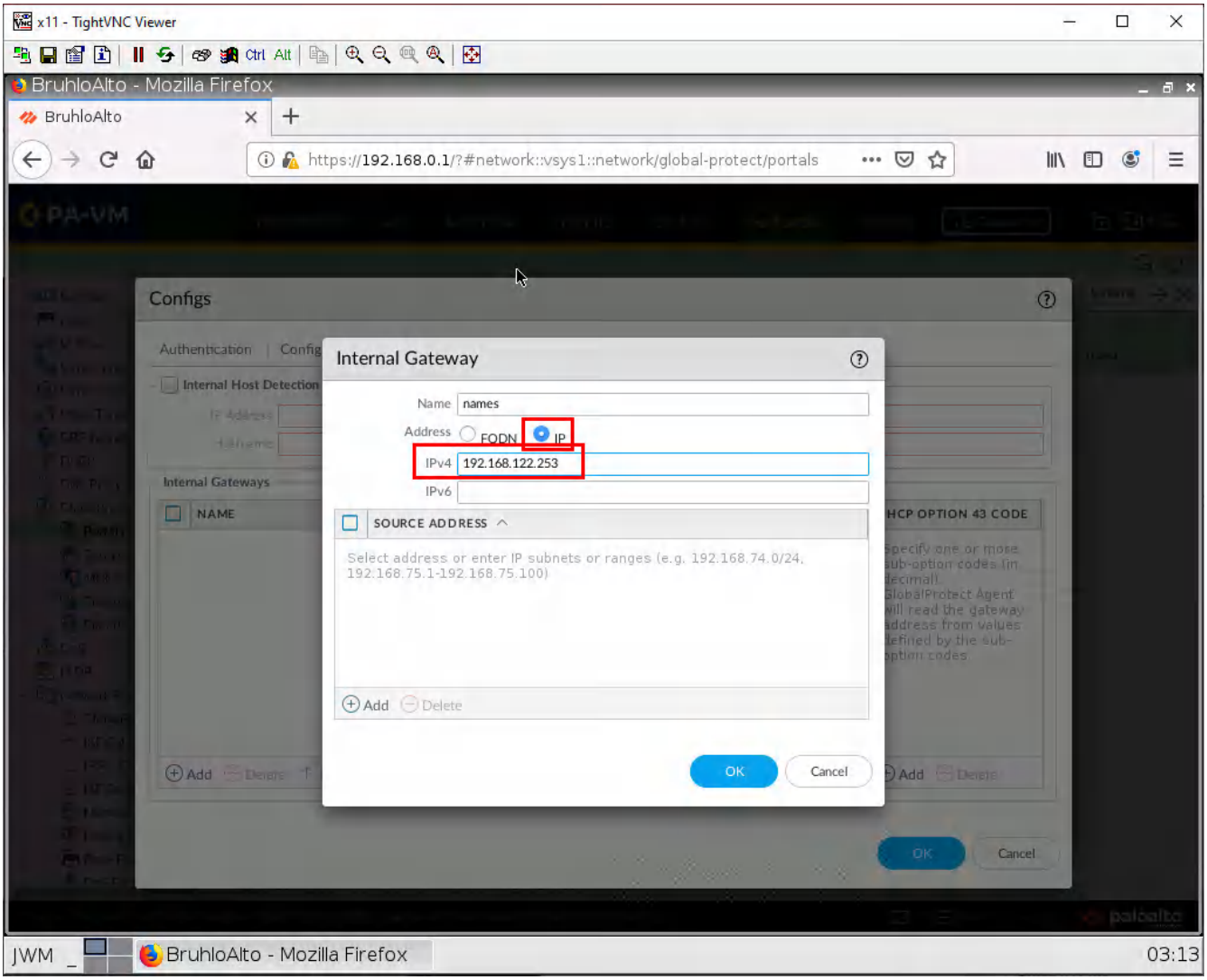


Figure 3.42: Set the IP address for Internal Gateway

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.

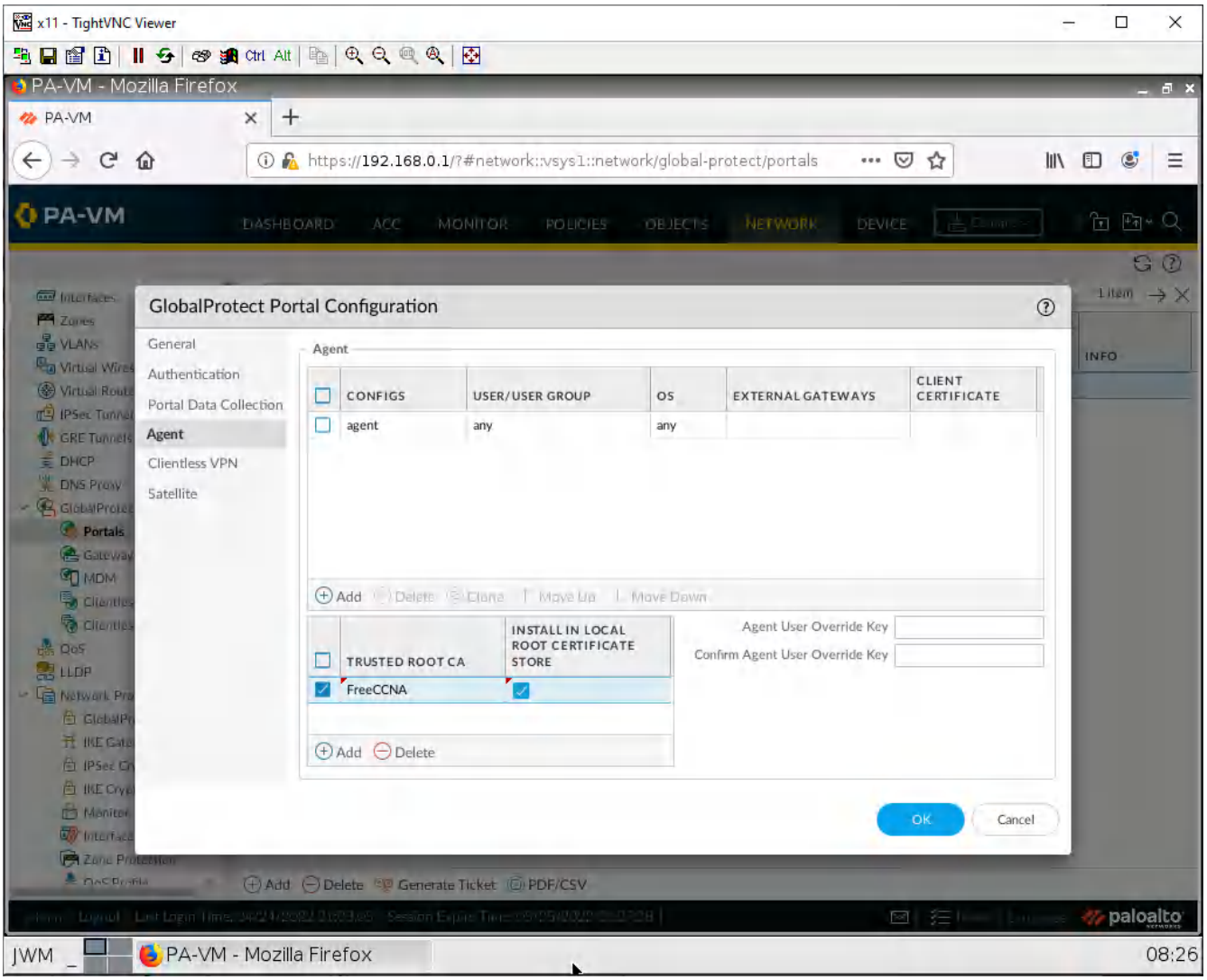


Figure 3.43: Add the Root CA certificate

Then press **OK**.

Create a GlobalProtect Gateway

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

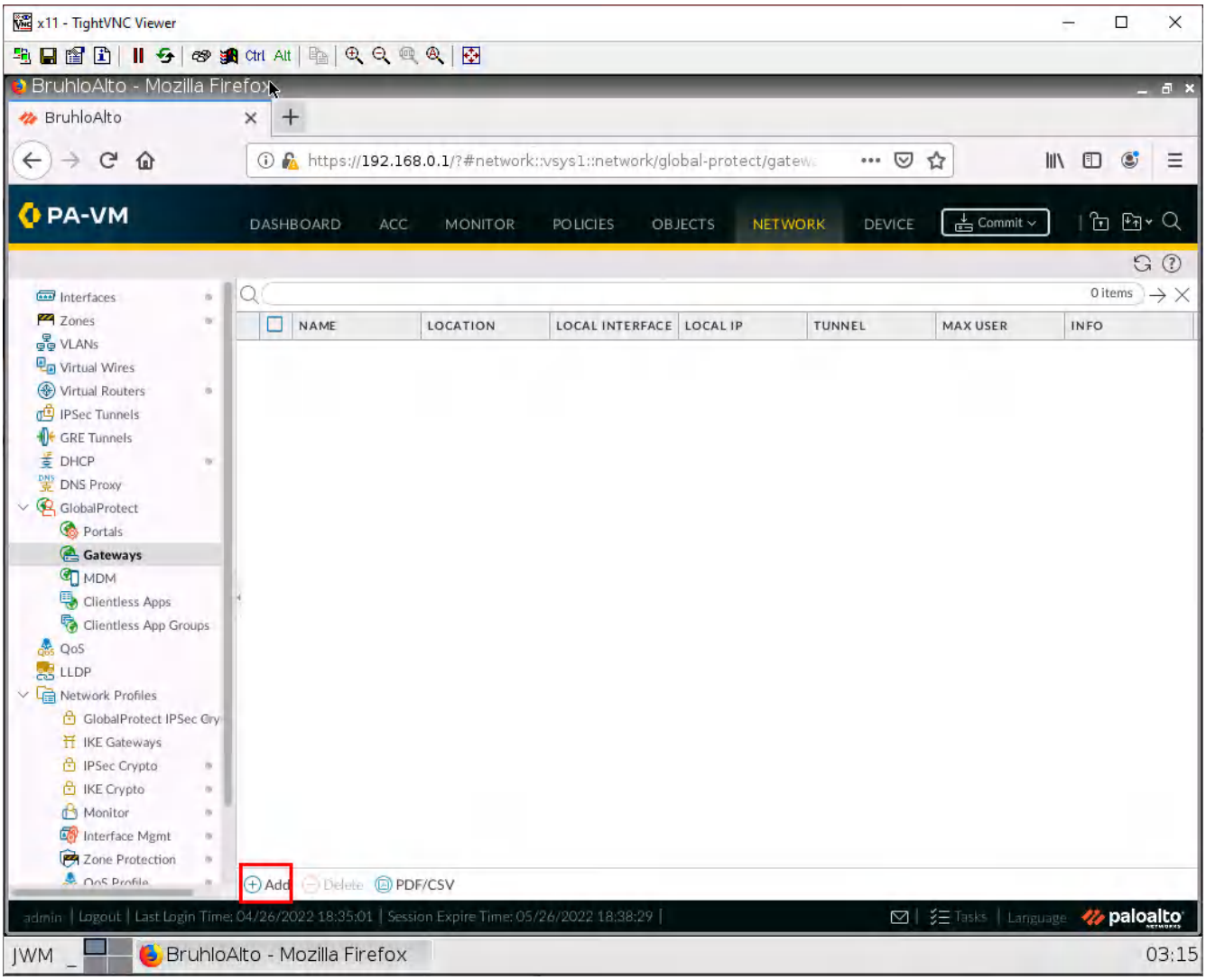


Figure 3.44: Add a Gateway

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

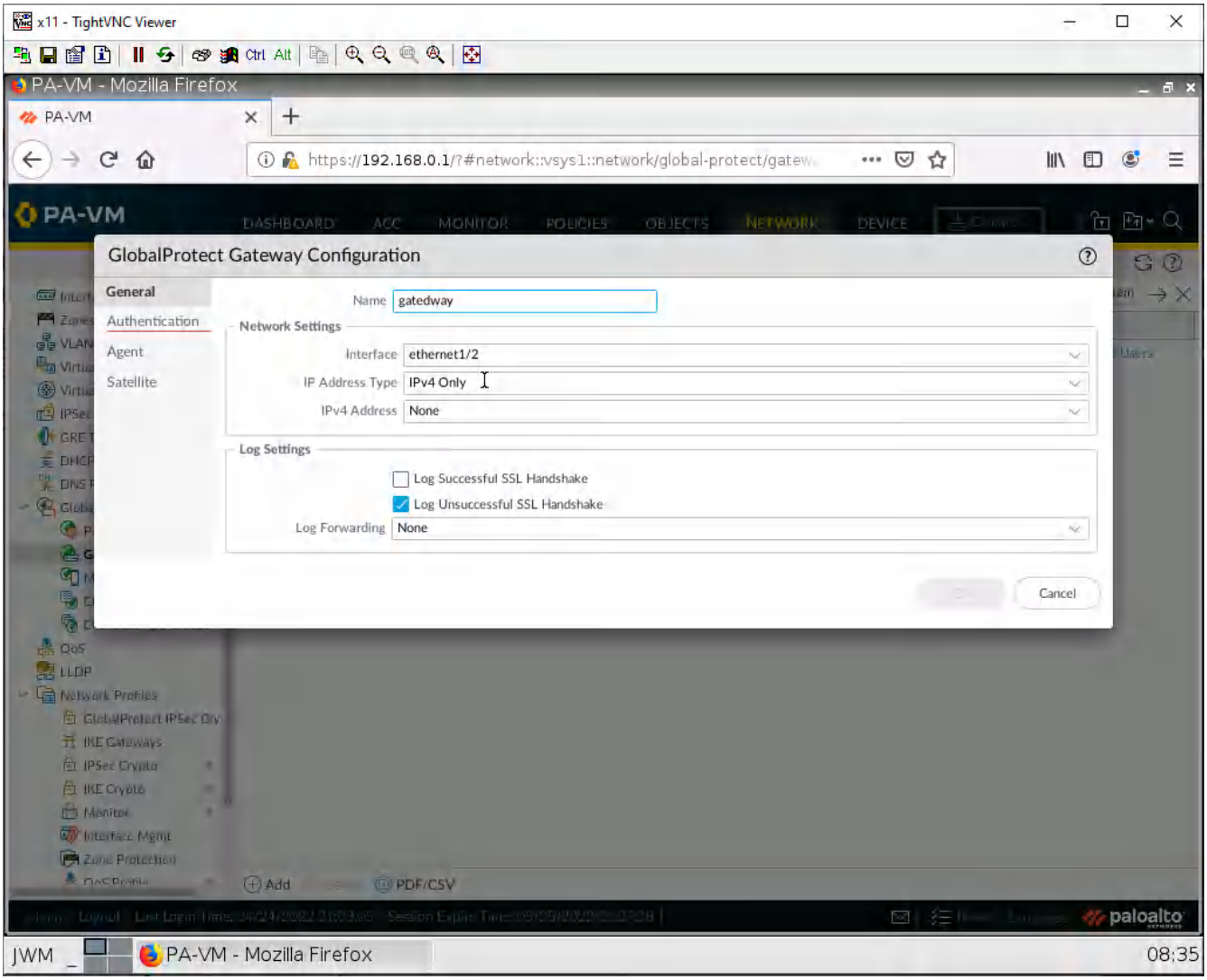


Figure 3.45: GlobalProtect Gateway Configuration

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

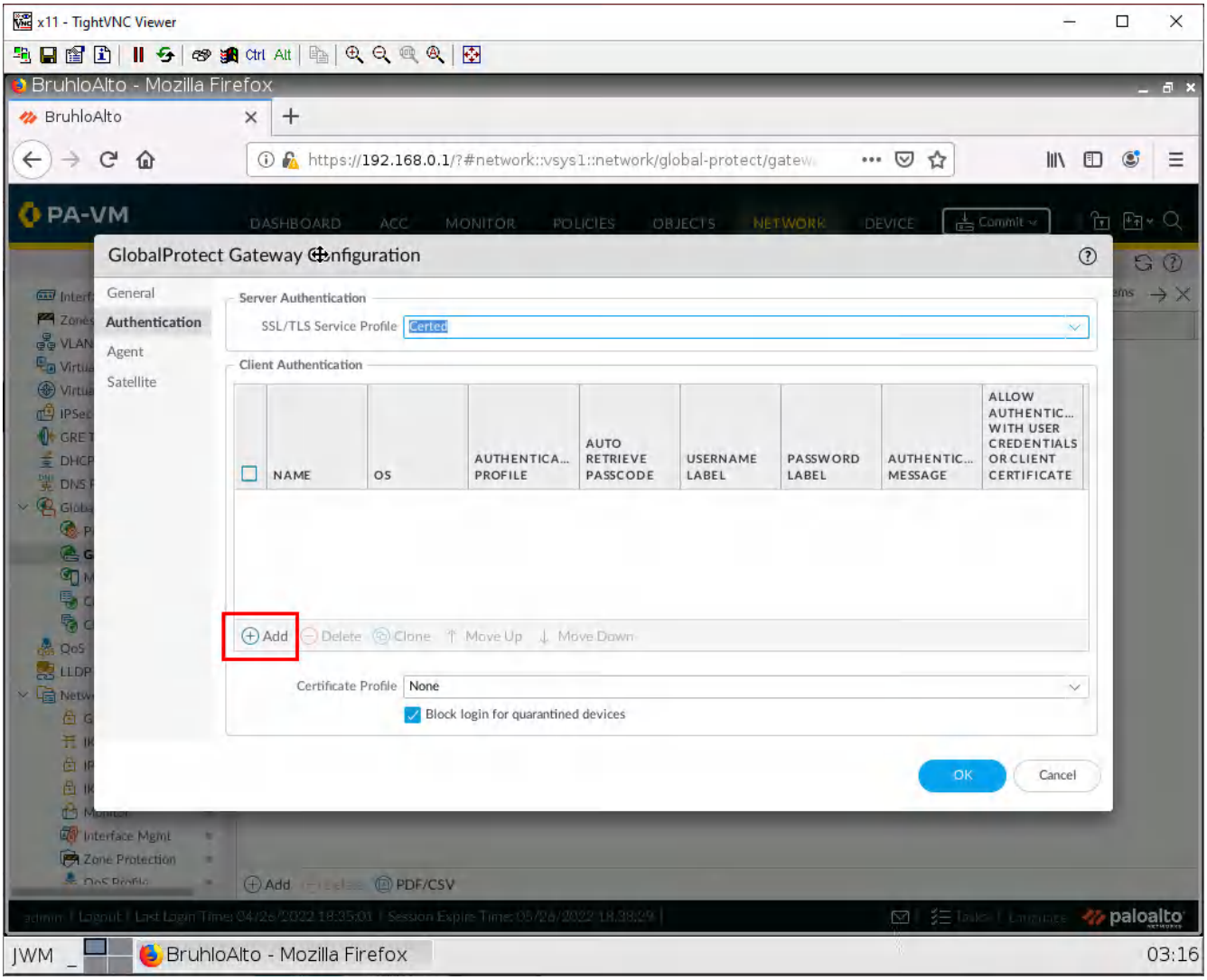


Figure 3.46: SSL/TLS Service Profile

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

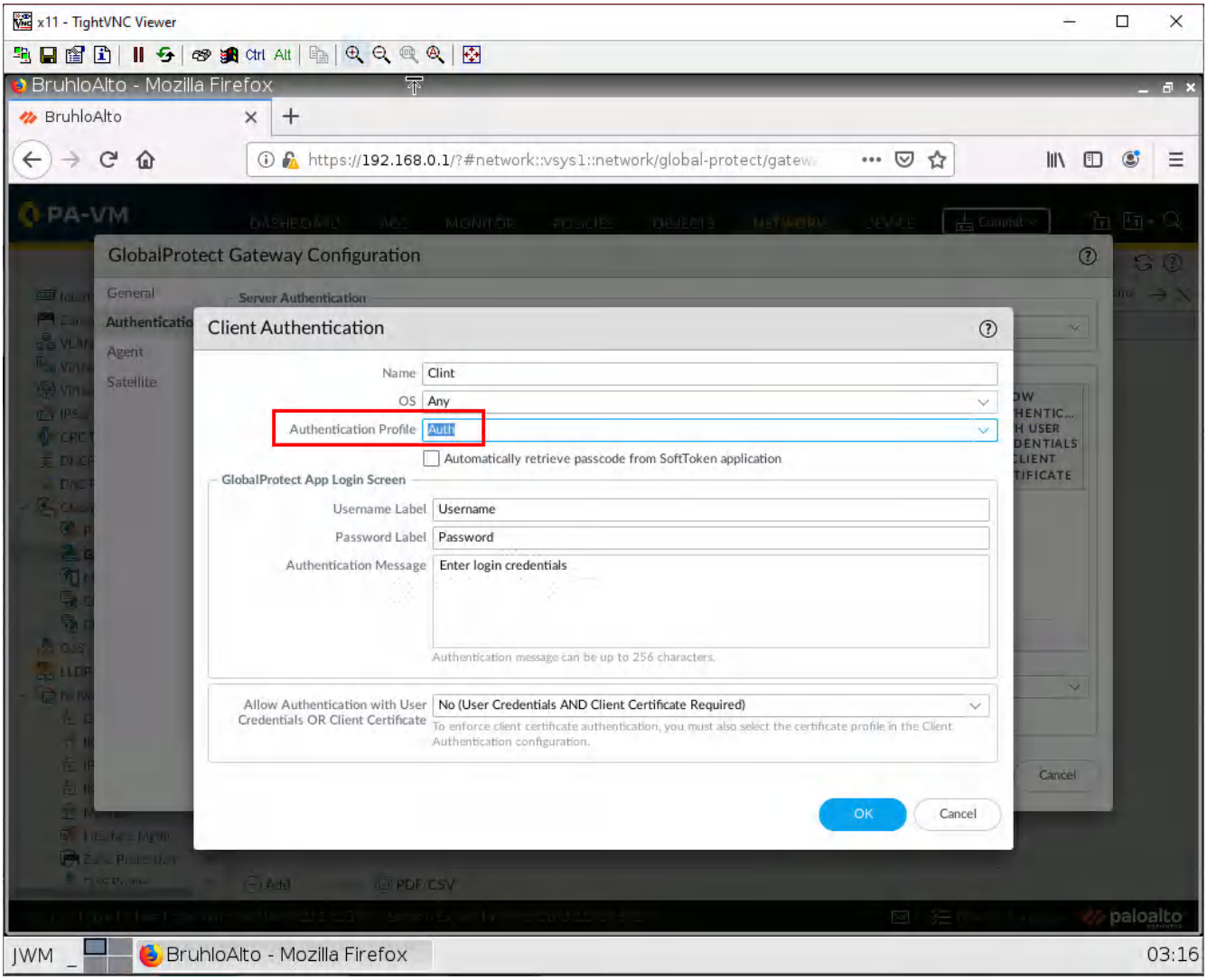


Figure 3.47: Authentication Profile

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

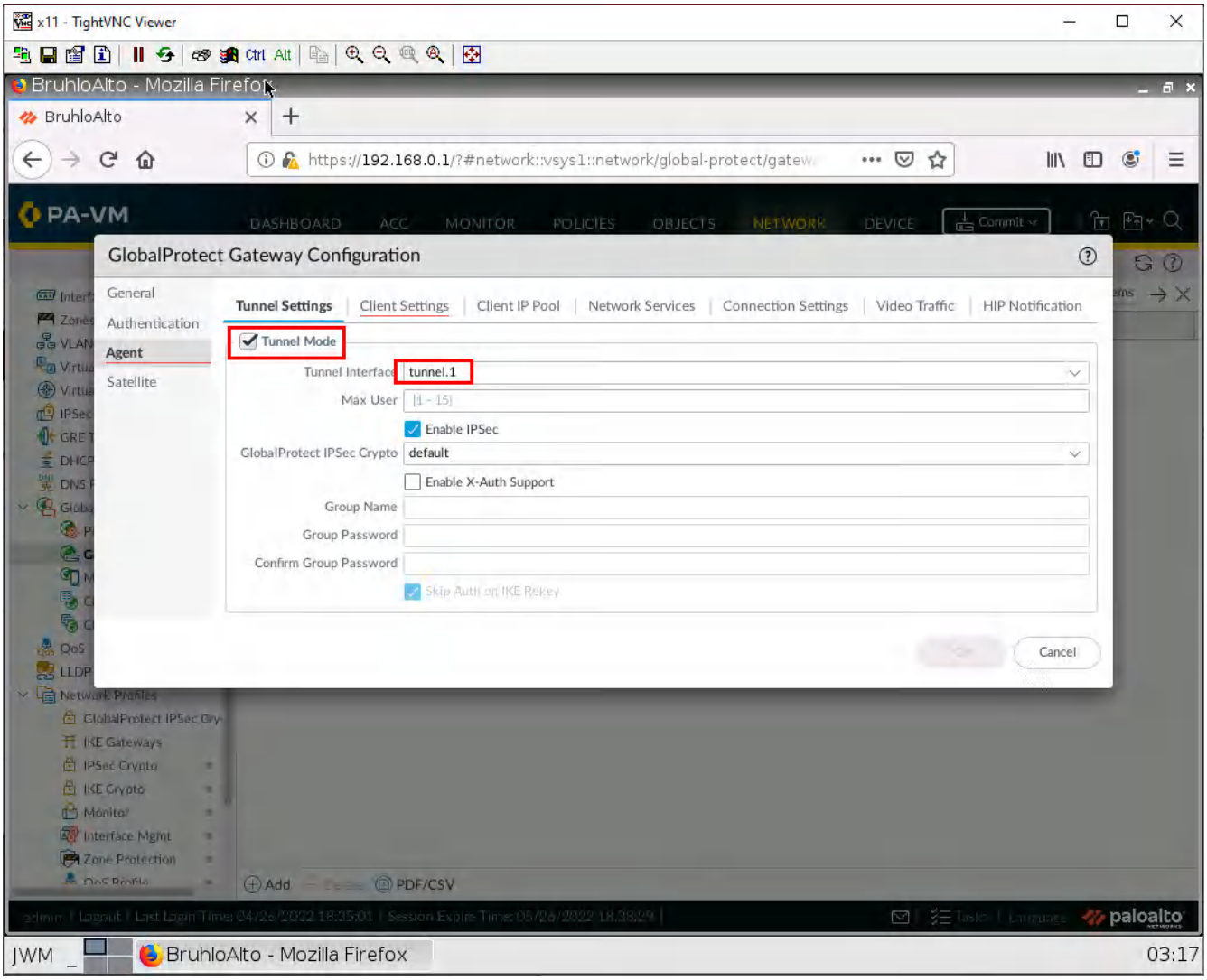


Figure 3.48: Tunnel Mode and Interface

In client settings, click **Add**.

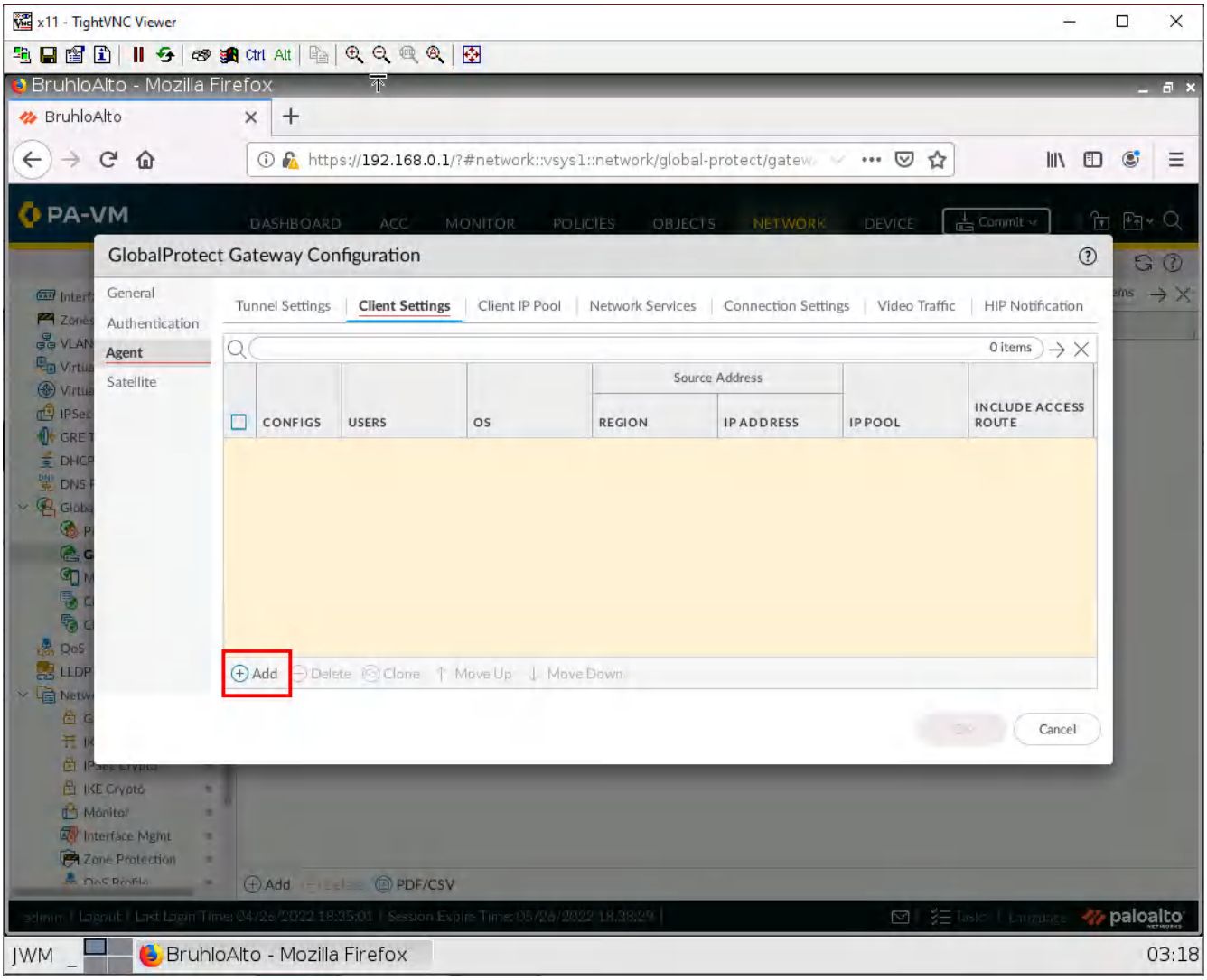


Figure 3.49: Client Settings

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

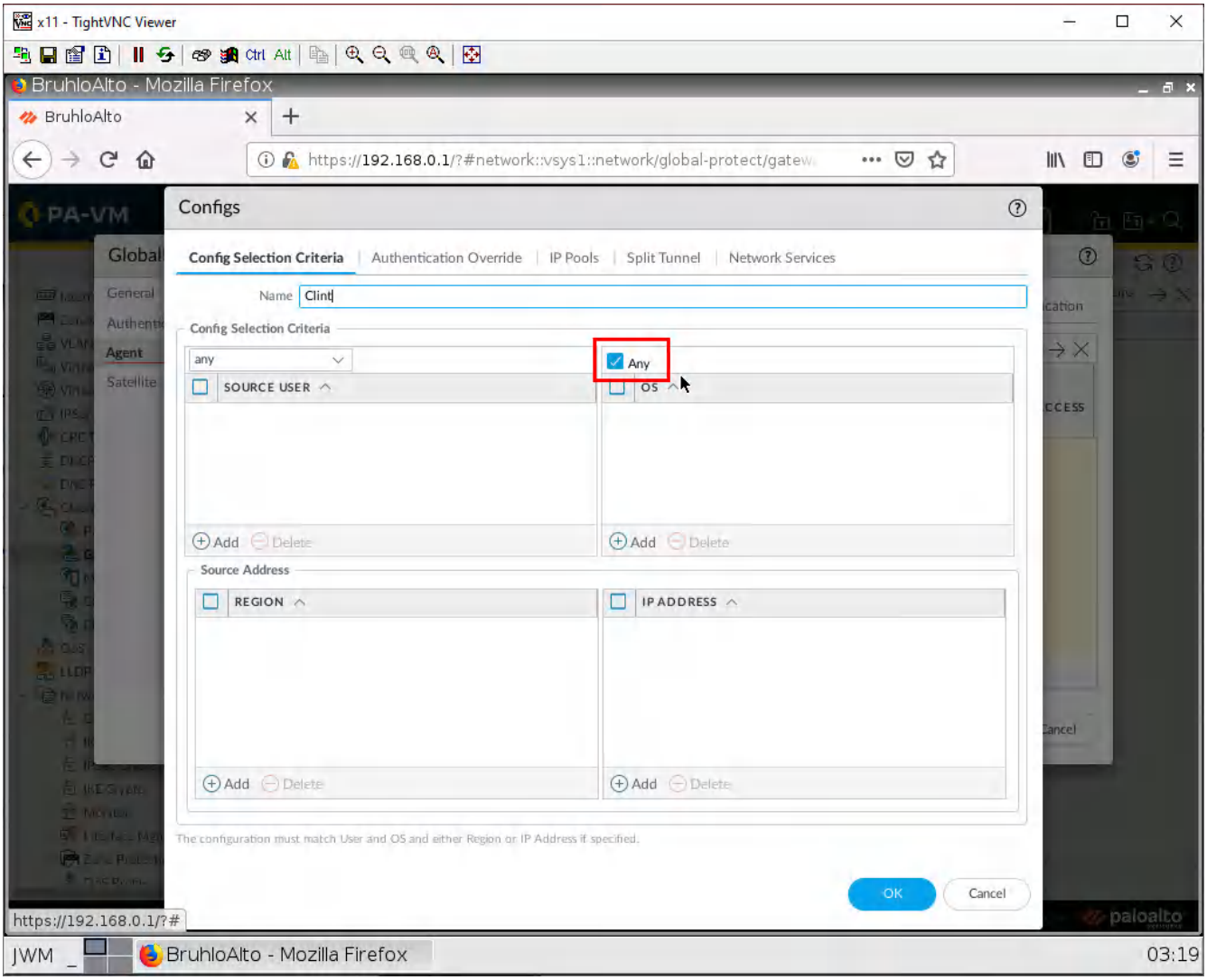


Figure 3.50: Select Client as Any

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

```
172.16.10.1-172.16.10.10
```

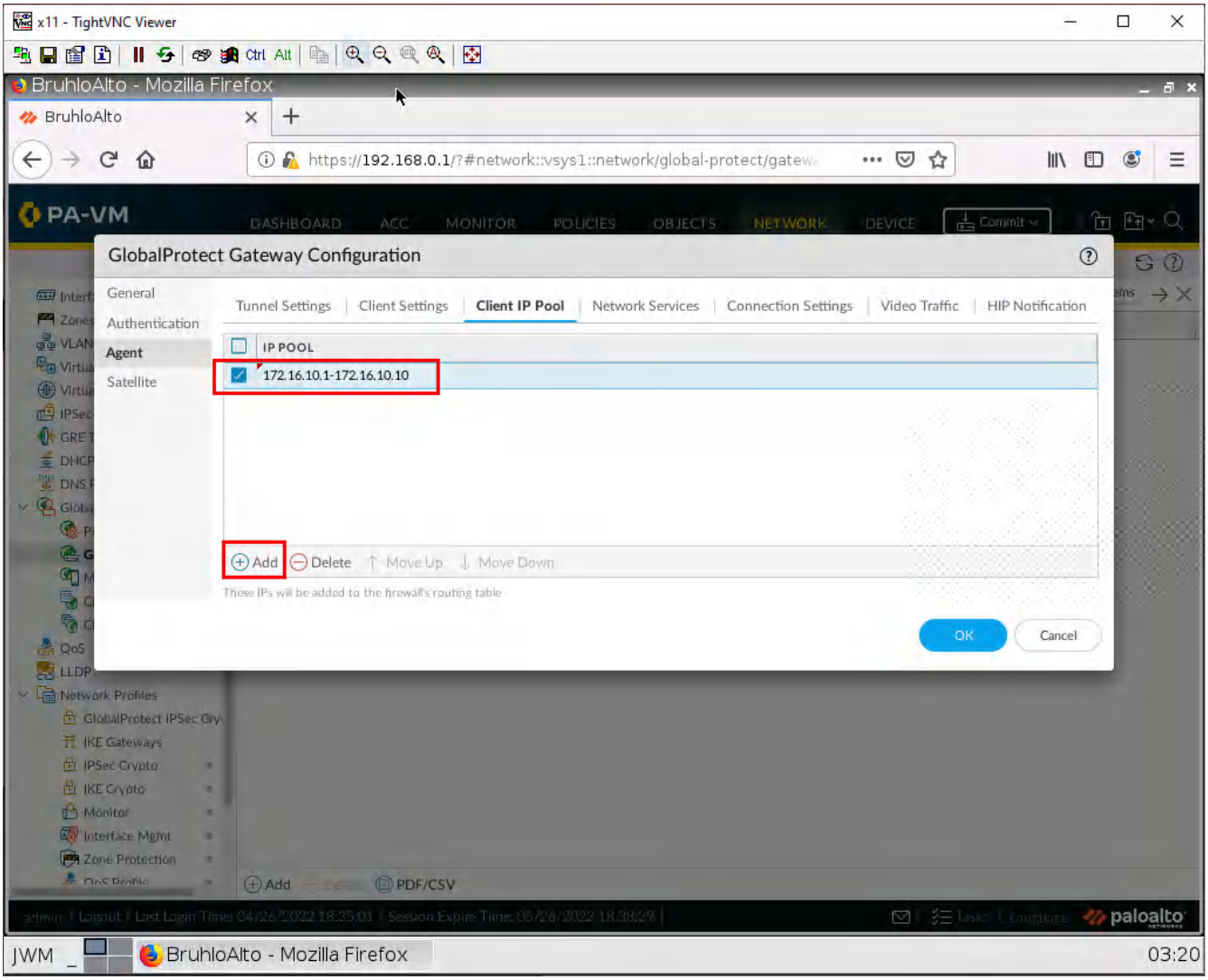


Figure 3.51: IP Pool Configuration

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.

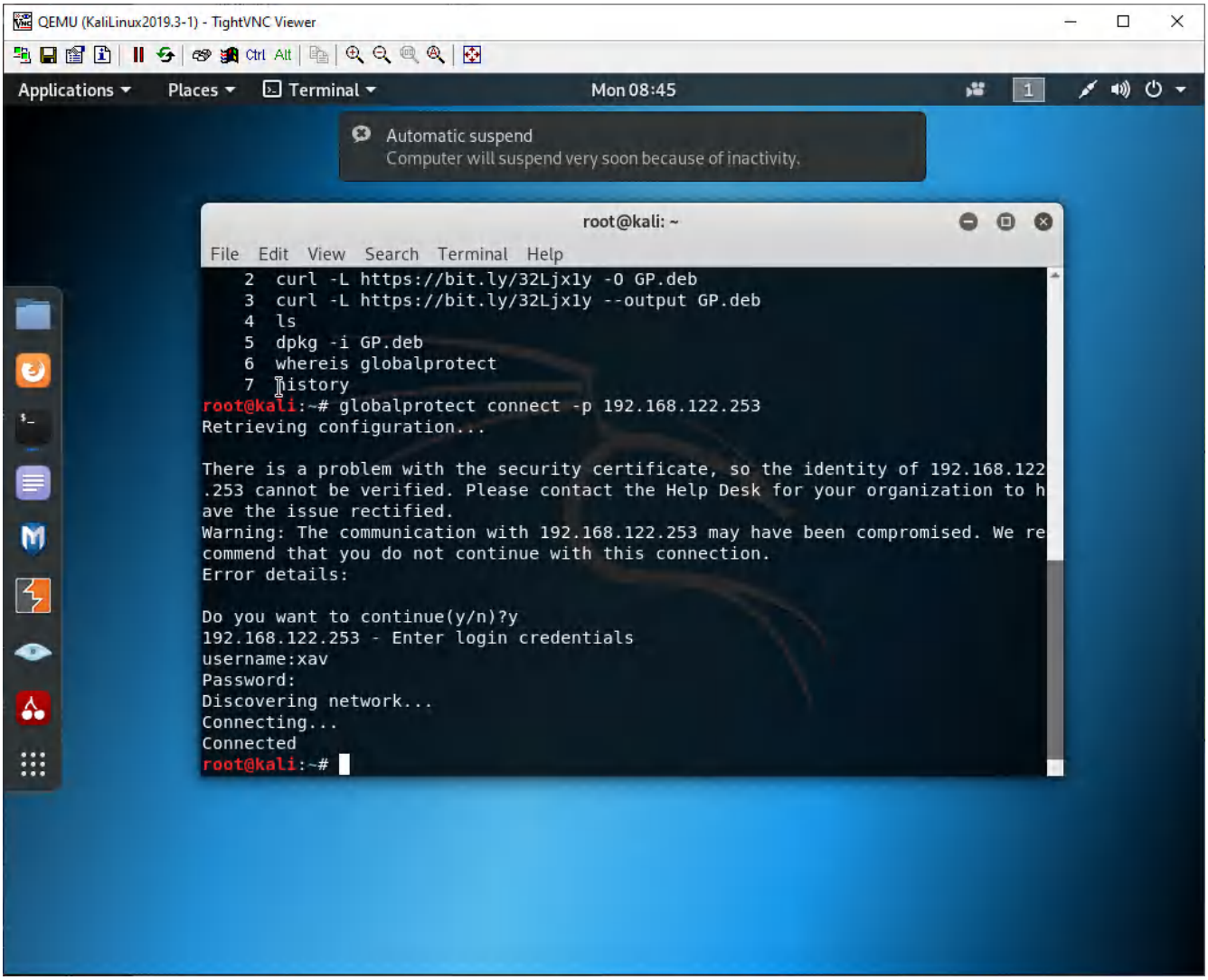


Figure 3.52: Installing GlobalProtect on Kali Linux

Test Remote Access VPN

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

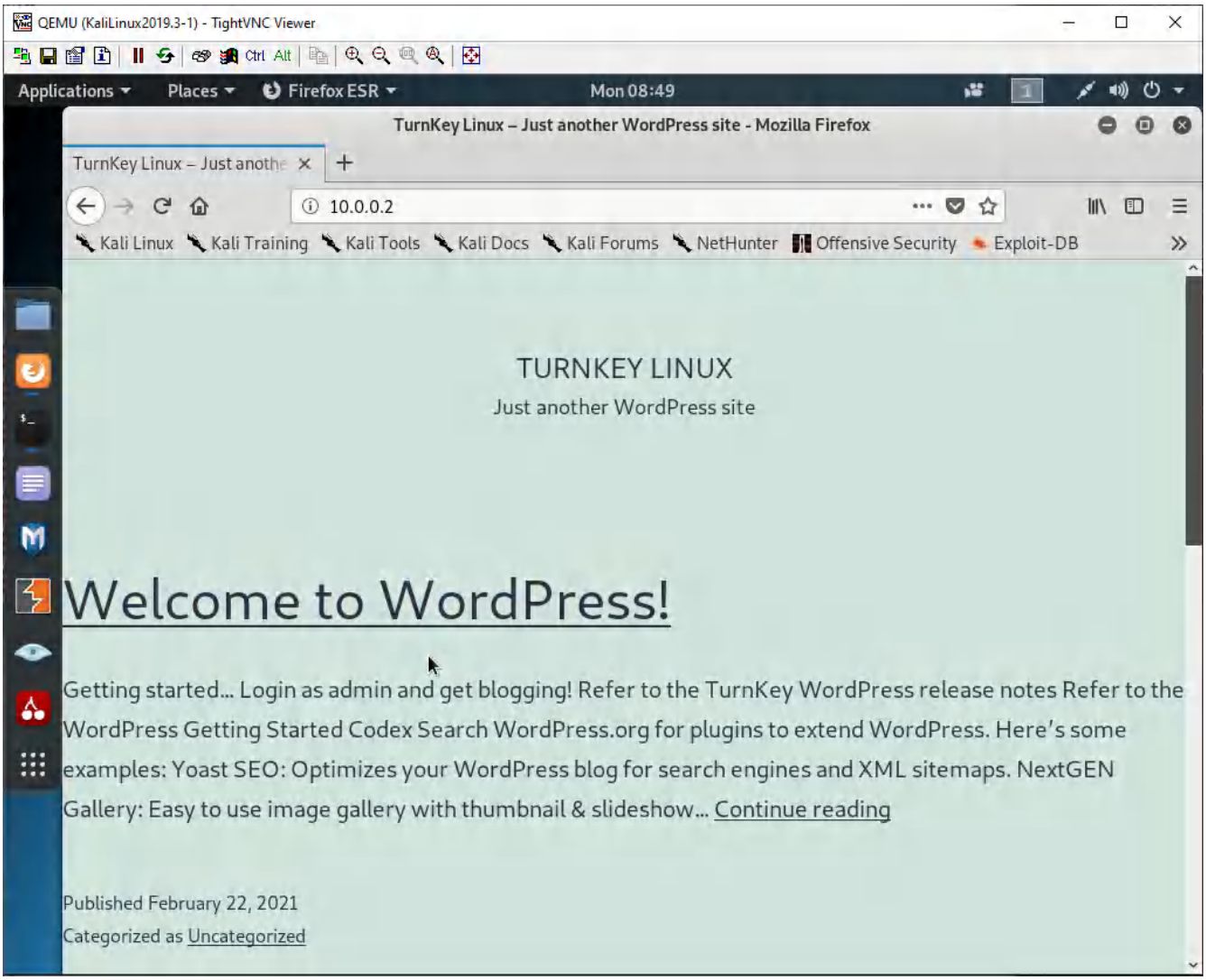


Figure 3.53: Verify your configuration

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.

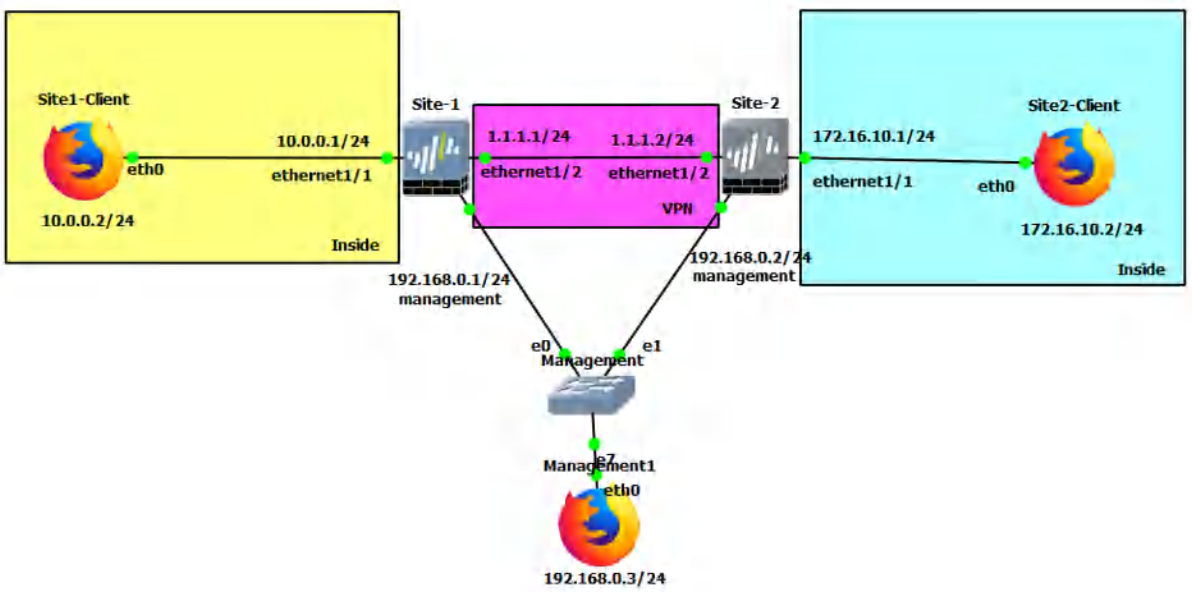


Figure 3.54: Main scenario

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**.

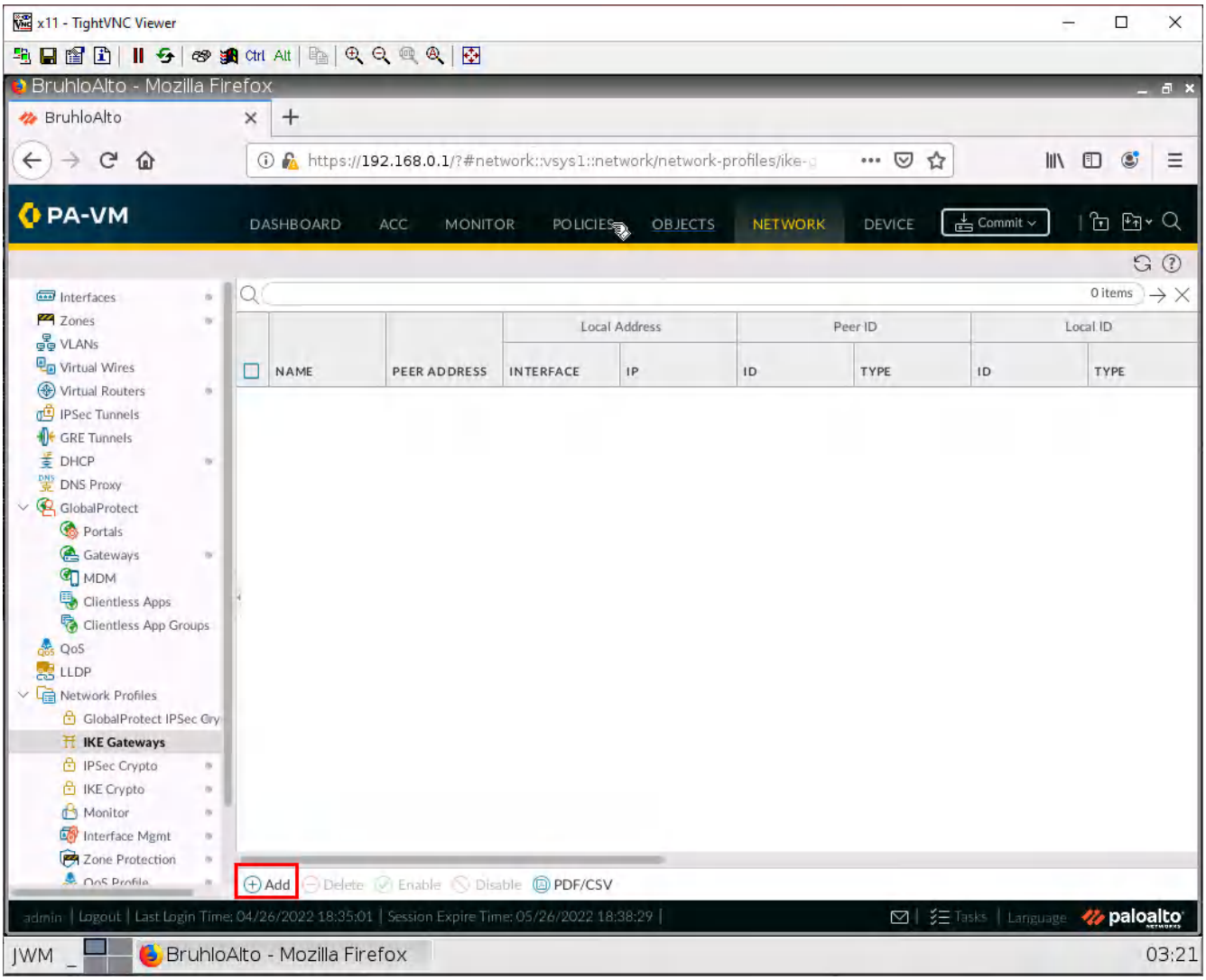


Figure 3.55: Add an IKE Gateway

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	*Password Here*
Confirm Pre-shared key	*Confirm Password Here*

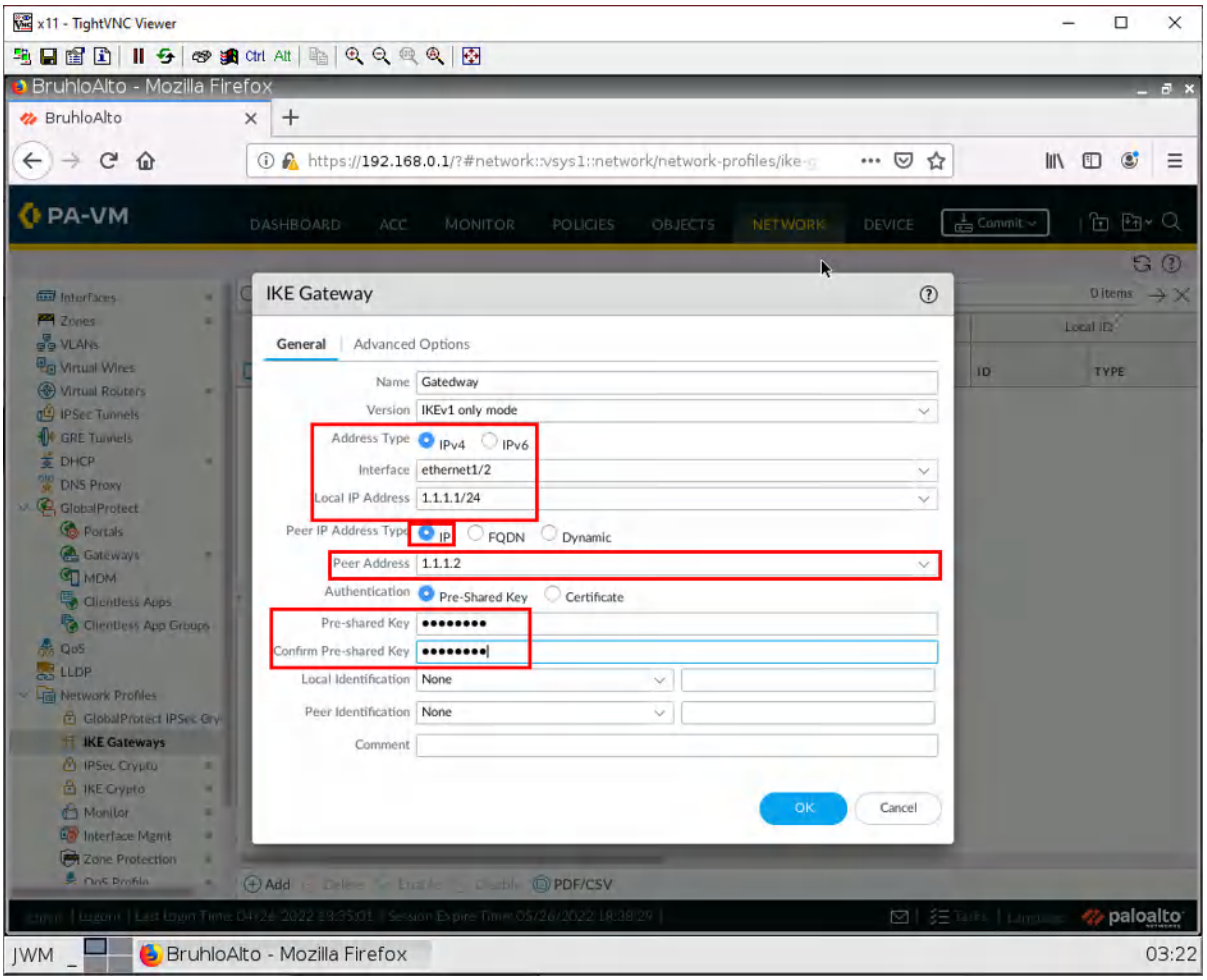


Figure 3.56: Site1 Firewall: IKE Gateway Configuration

Then press **OK**.

On the Site2 firewall, configure these settings:

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	*Same Password as before here*
Confirm Pre-shared key	*Confirm same password as before here*

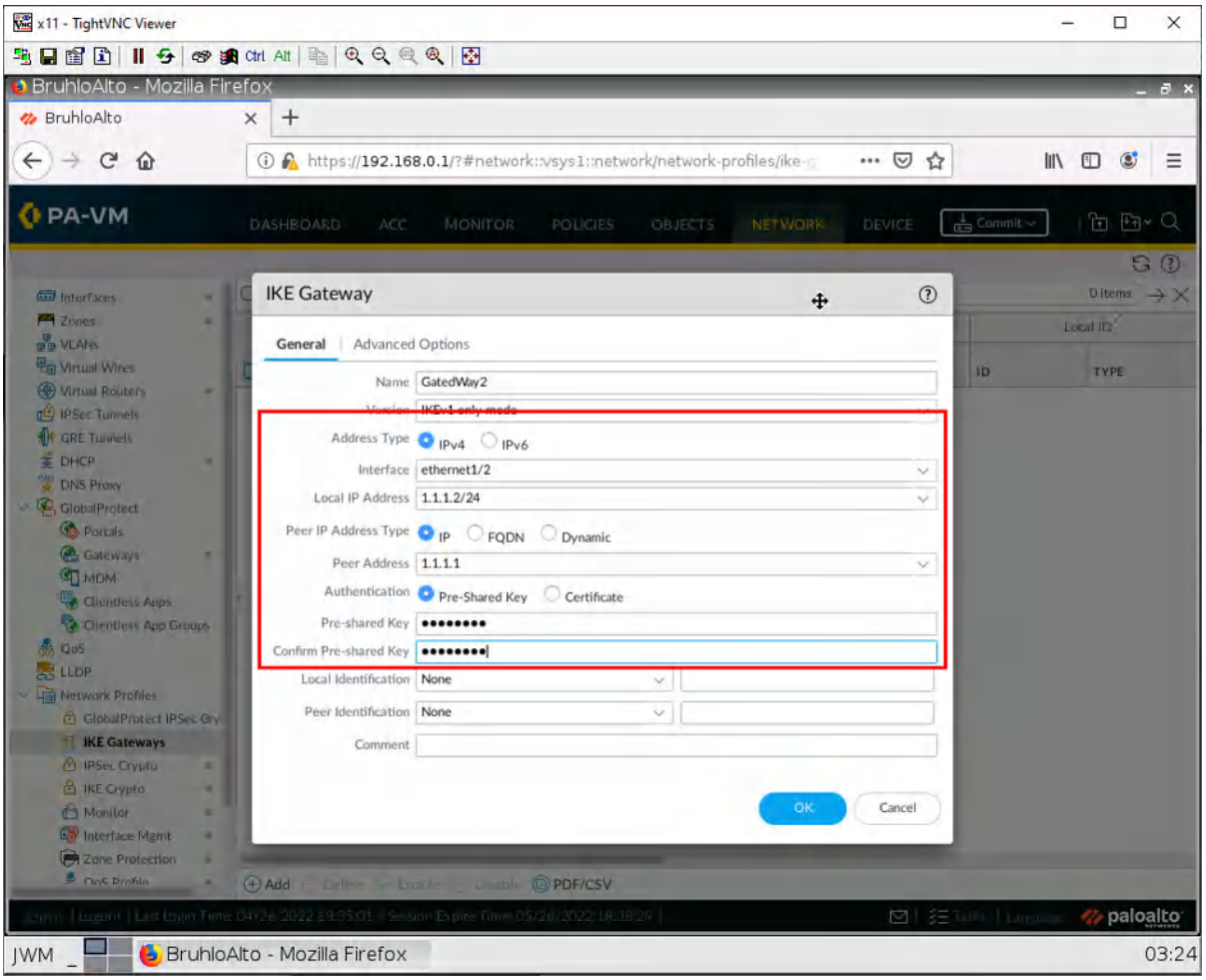


Figure 3.57: Site2 Firewall: IKE Gateway Configuration

Then press **OK**.

Create an IPsec Tunnel

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

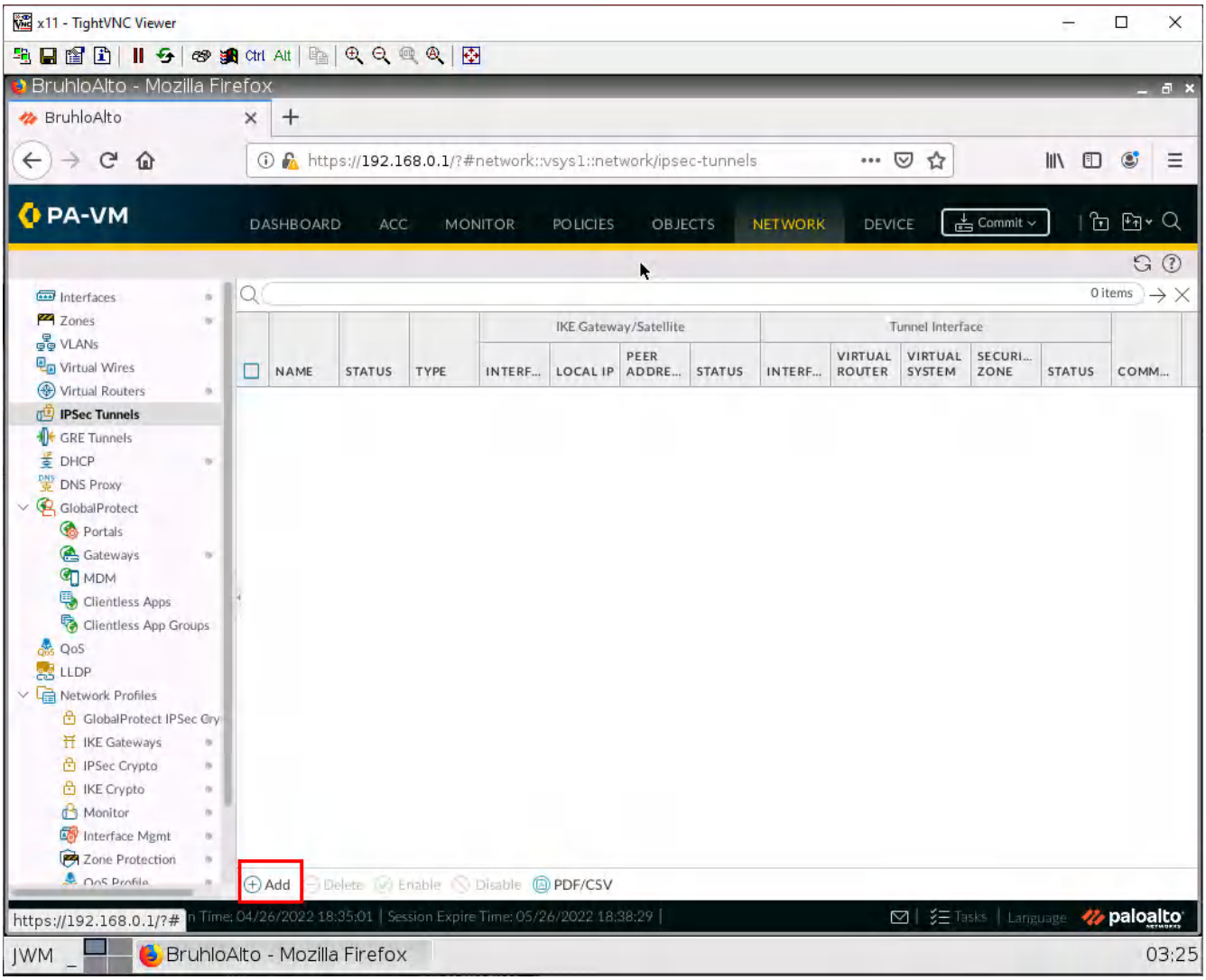


Figure 3.58: Site1 Firewall: Add an IPsec Tunnel

On both firewalls, configure these settings:

Table 3.13: IPsec Tunnel Configuration

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

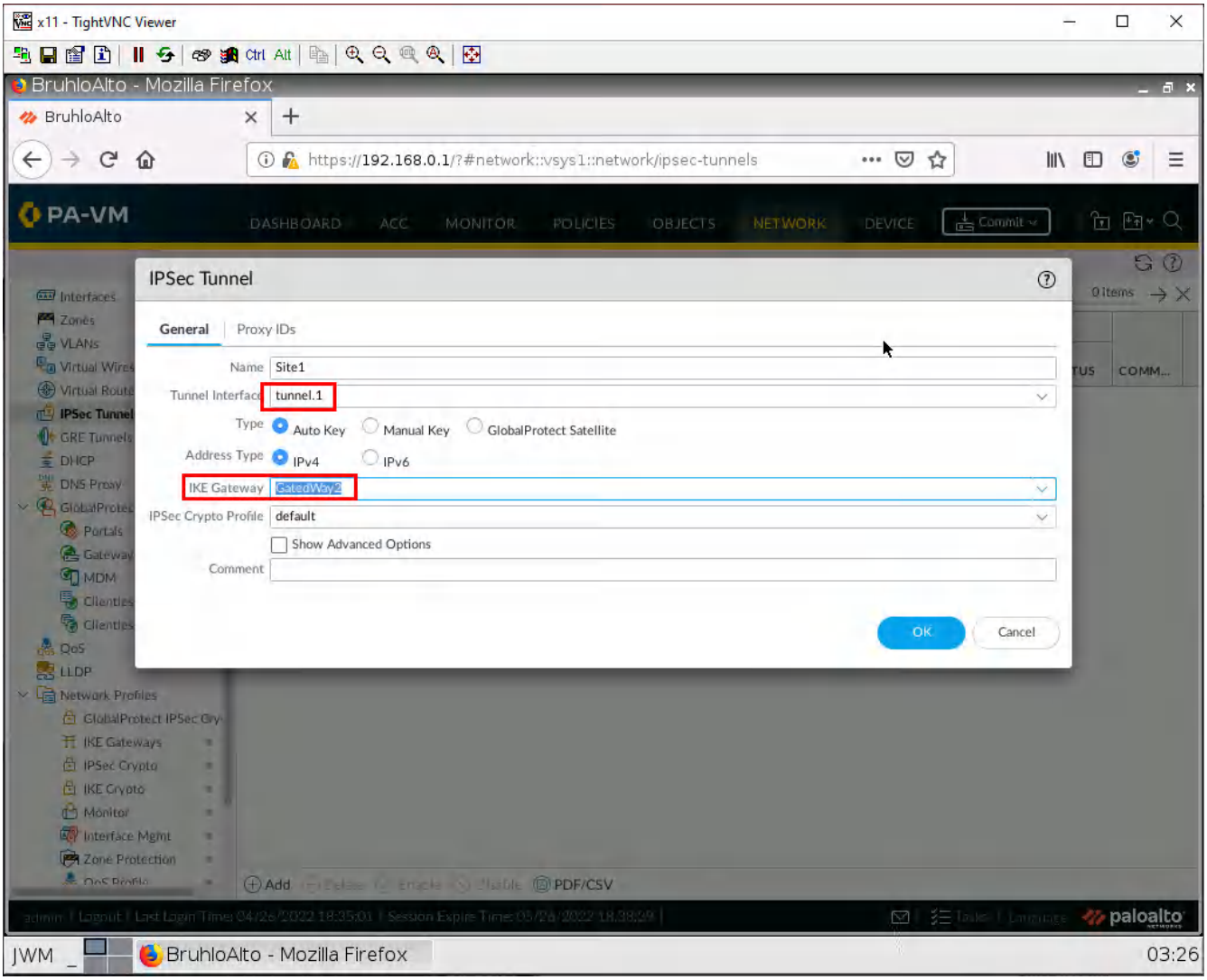


Figure 3.59: Site1 and Site2 Firewall: IPsec Tunnel Configuration

Create Static Routes

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

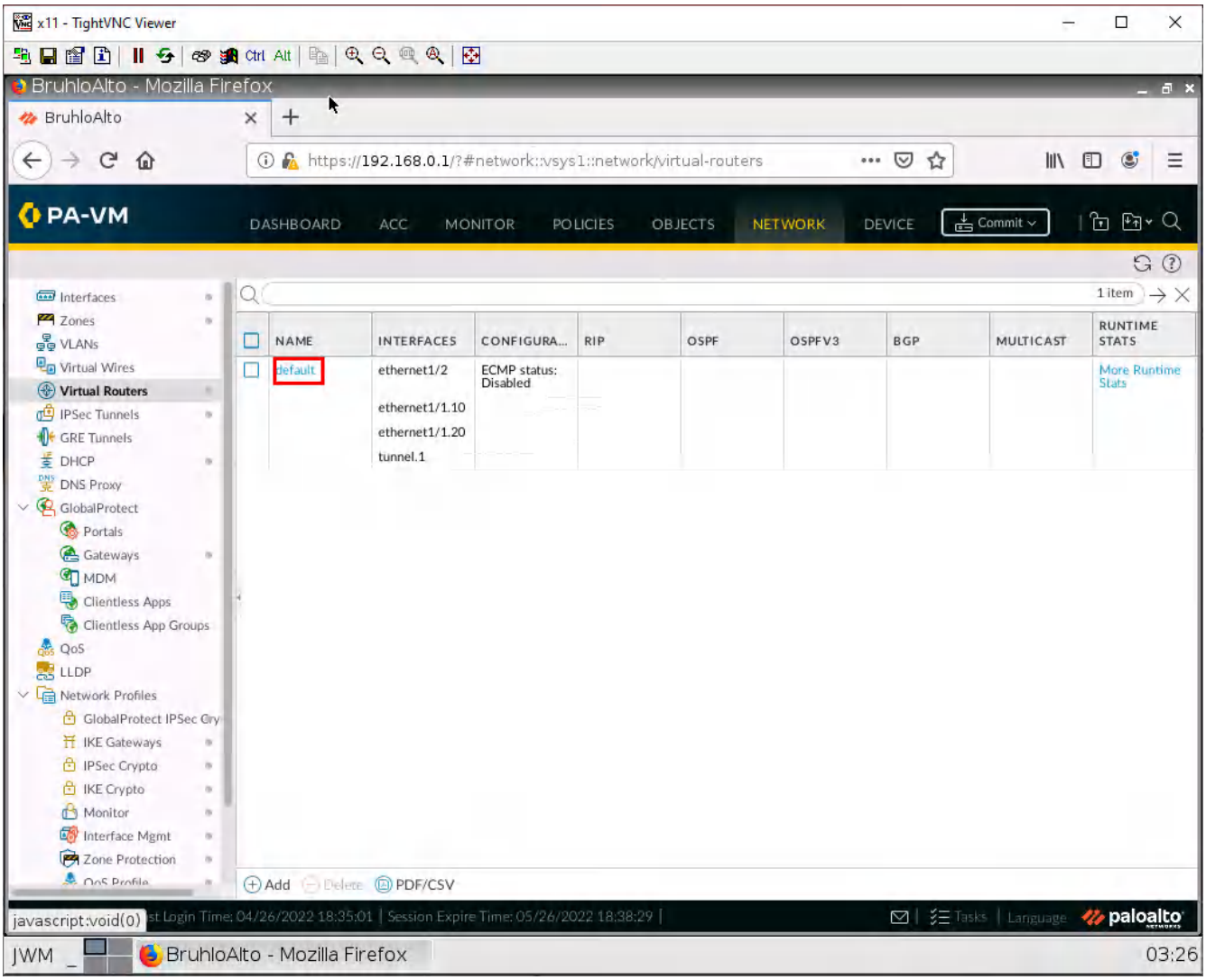


Figure 3.60: Virtual Routers Configuration

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

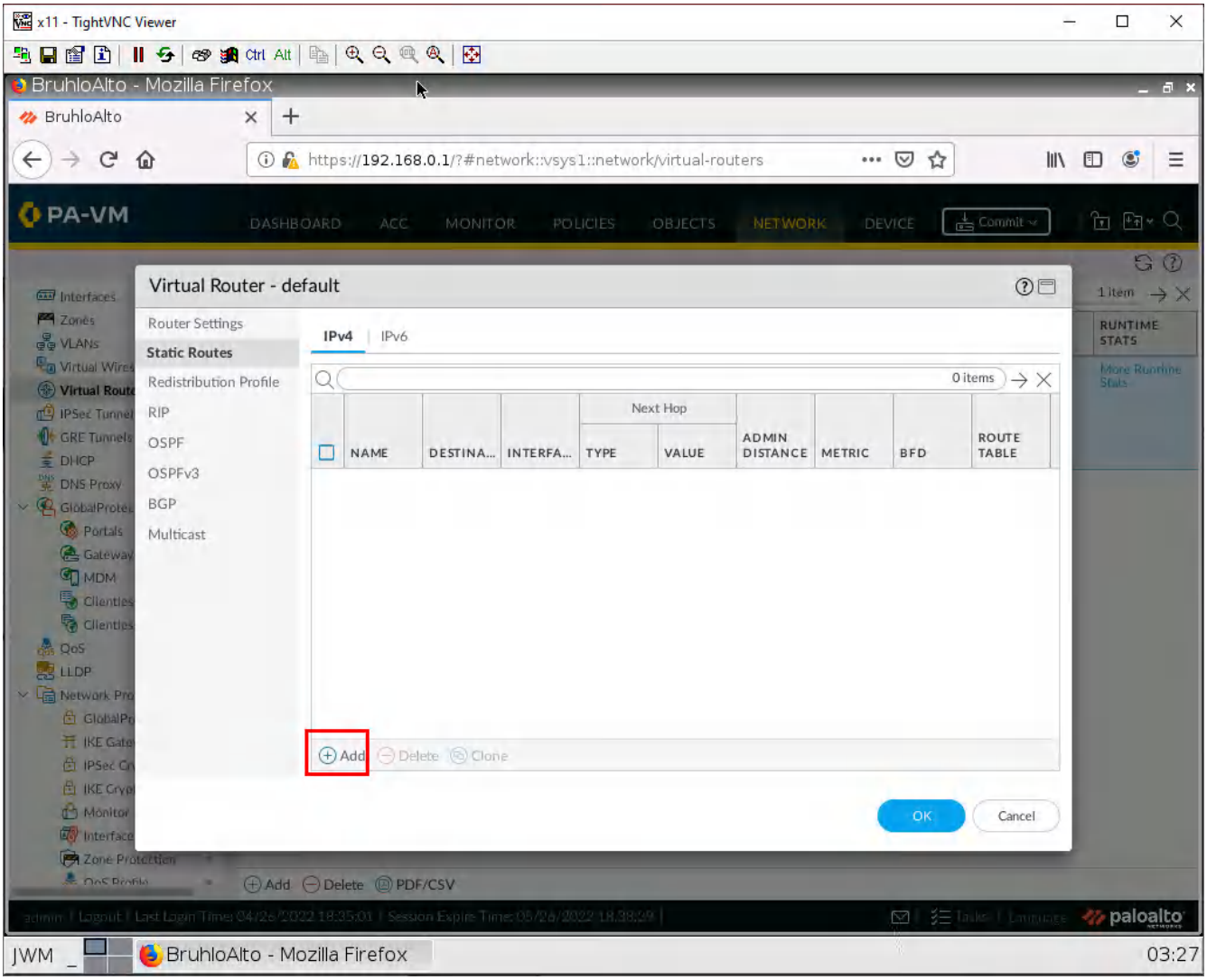


Figure 3.61: Add a Static Route in the Site1

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

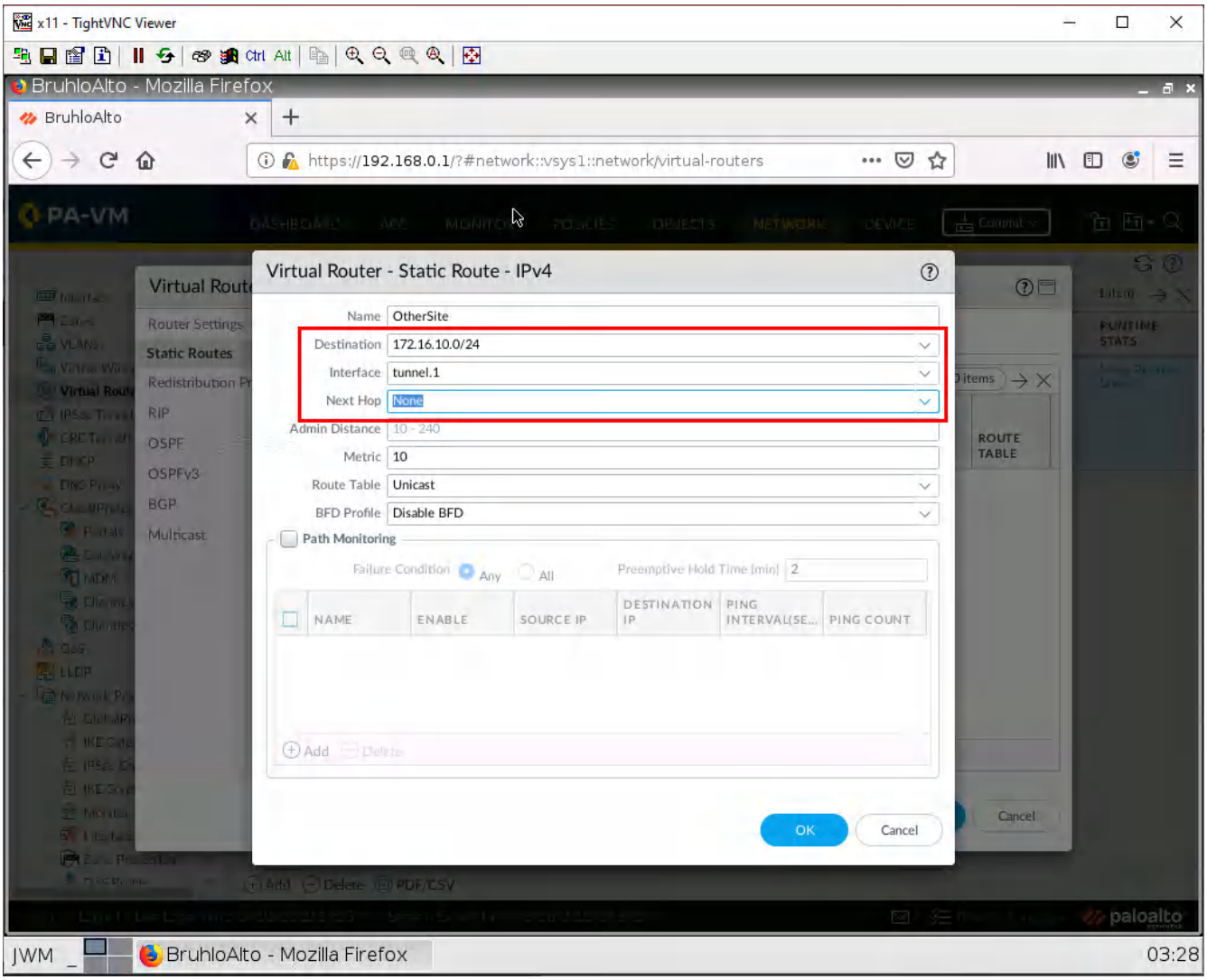


Figure 3.62: Static Route Configuration in the Site1

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

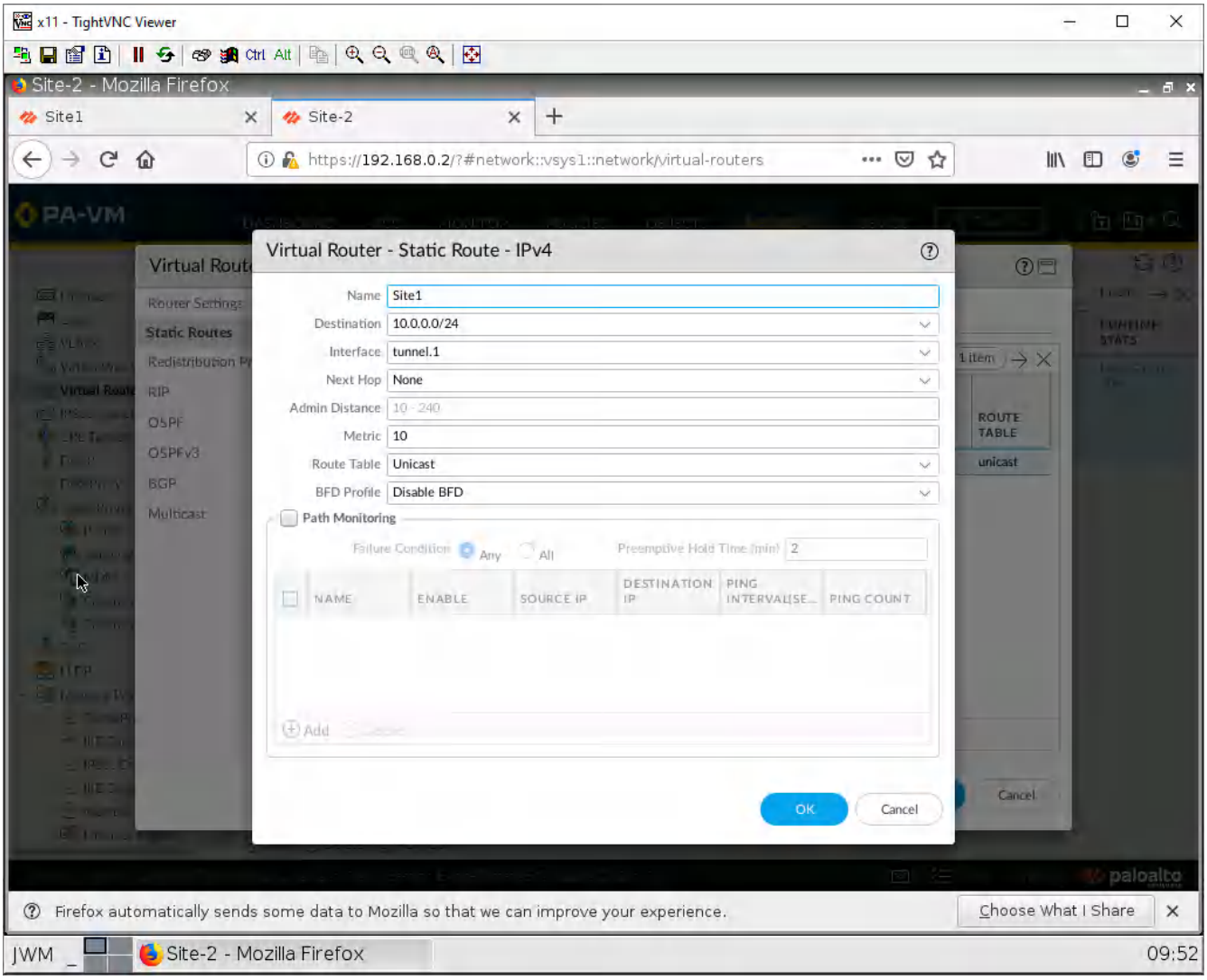


Figure 3.63: Static Route Configuration in the Site 2

Then press **OK**.

Test the Site-to-Site

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

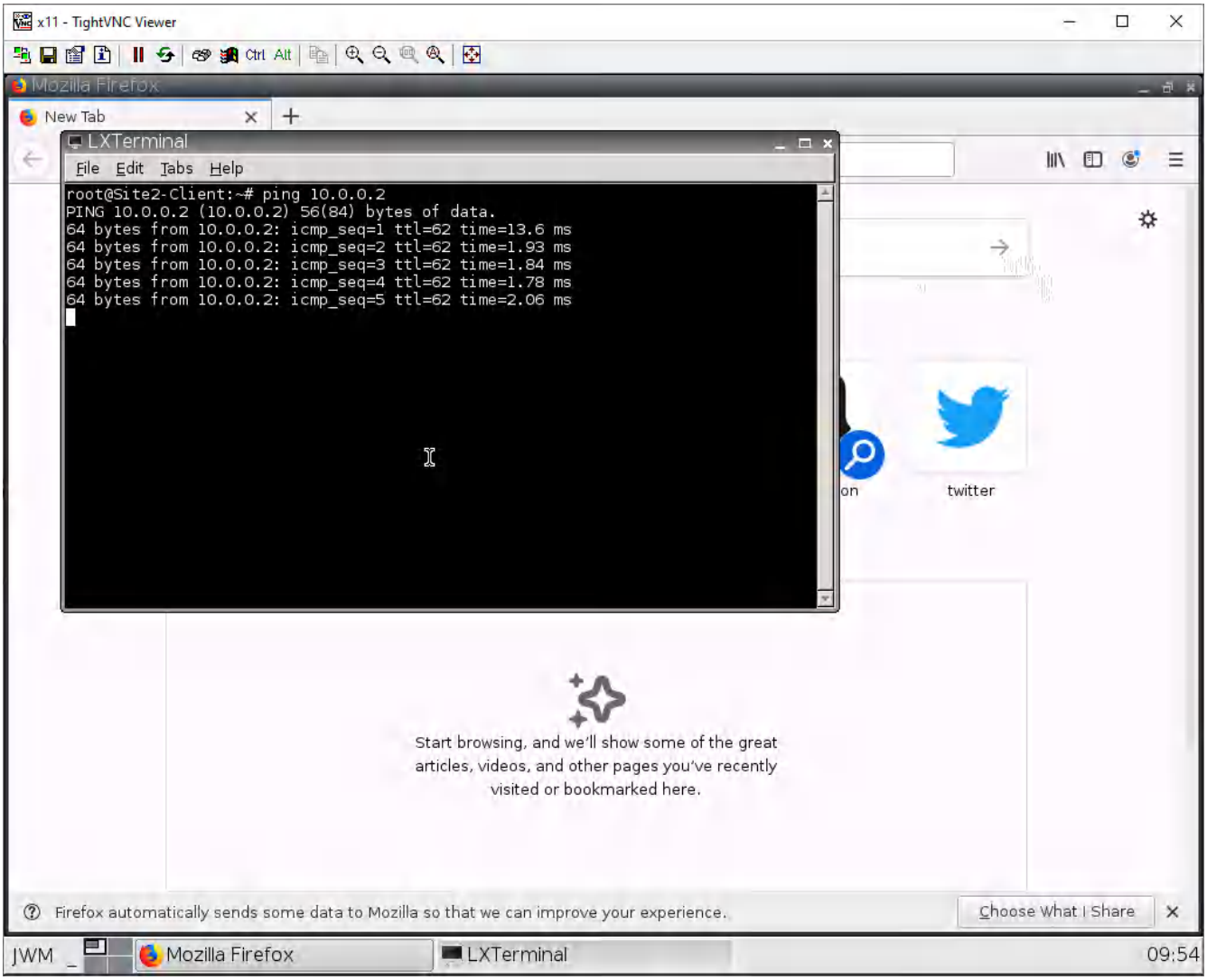


Figure 3.64: Verify your configuration

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.

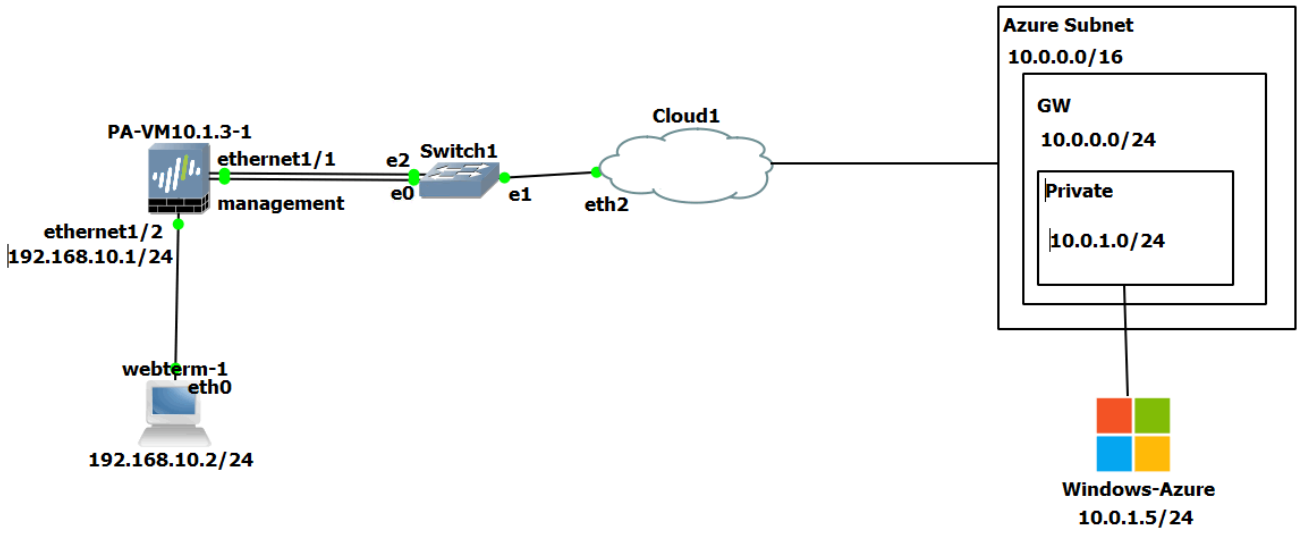


Figure 4.1: Main scenario

Azure Configuration

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

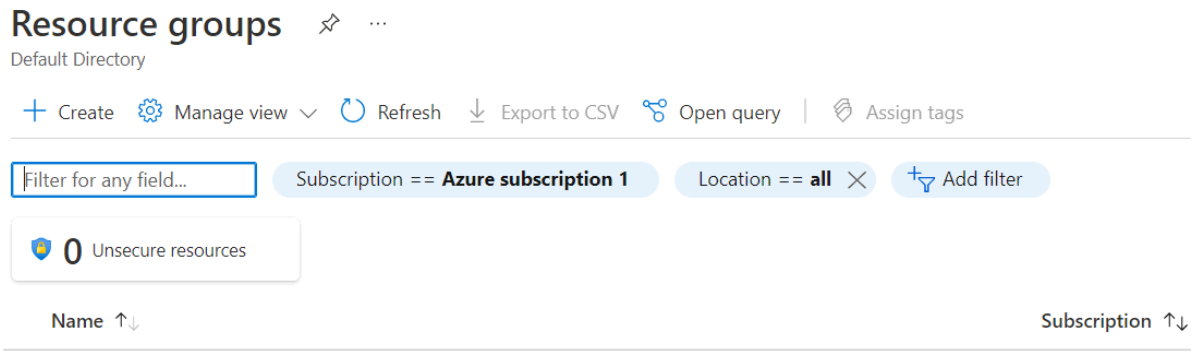


Figure 4.2: Create a resource group

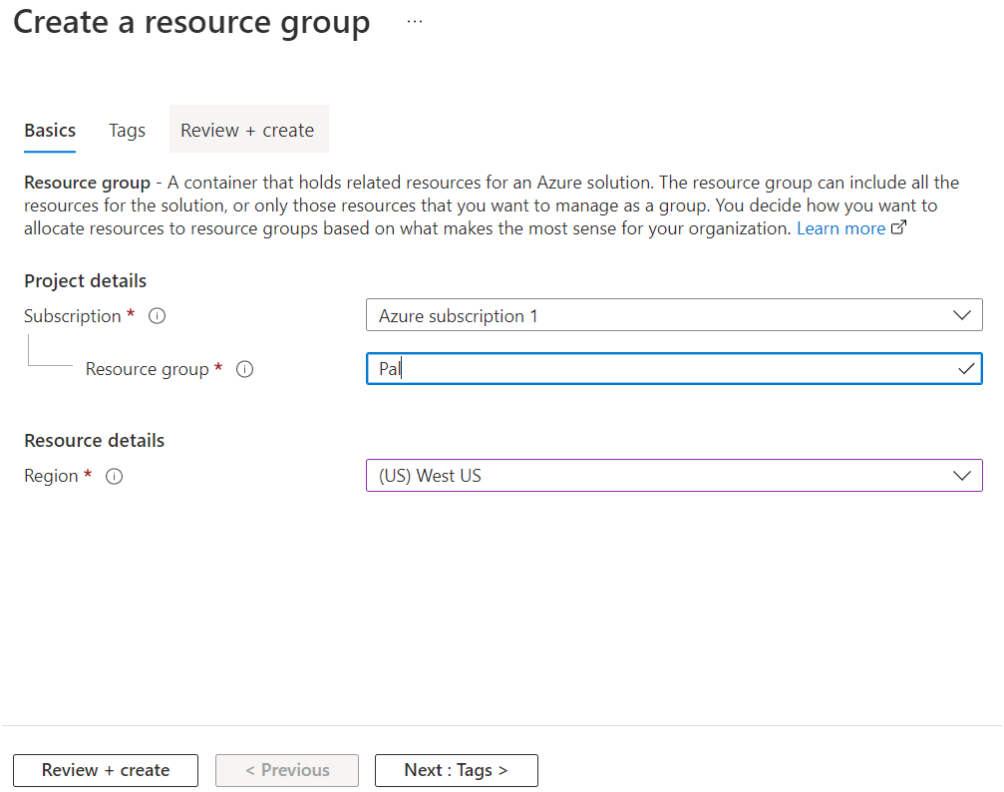


Figure 4.3: Create a resource group

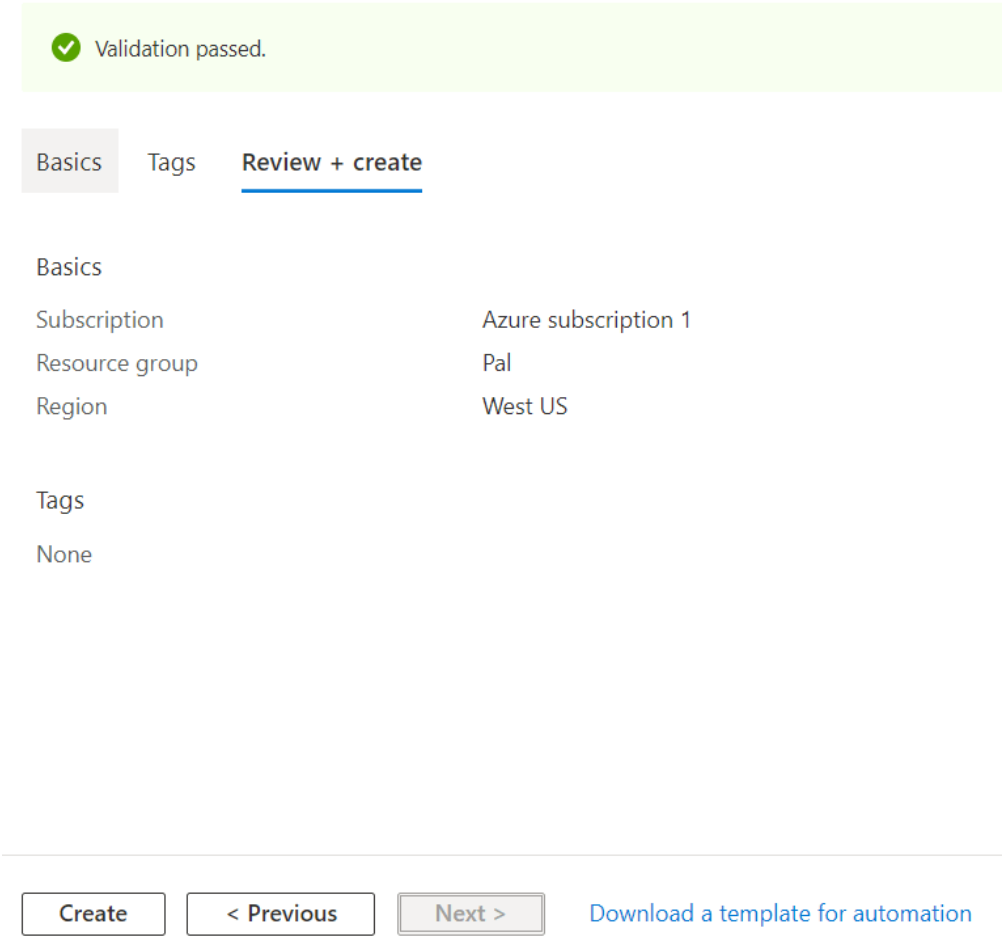


Figure 4.4: Create a resource group

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

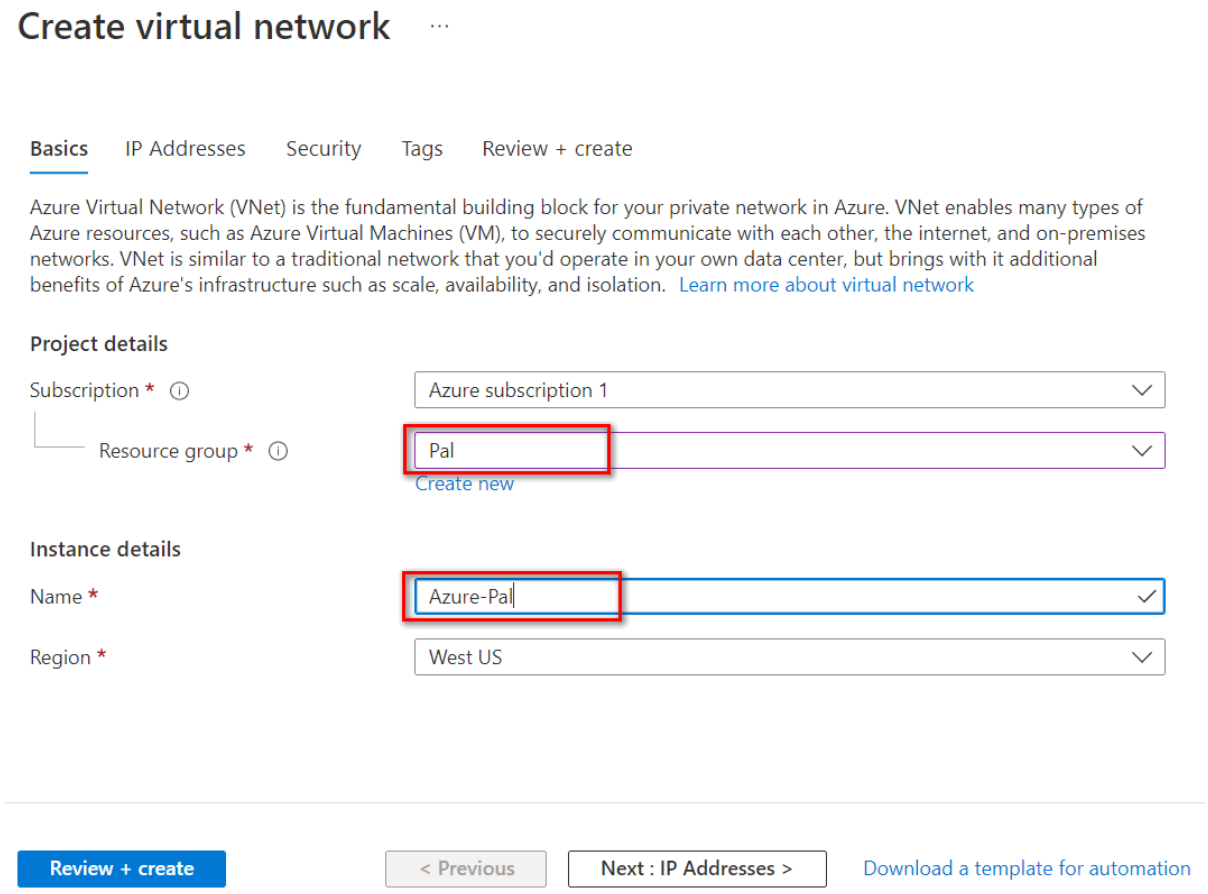


Figure 4.5: Create a virtual network

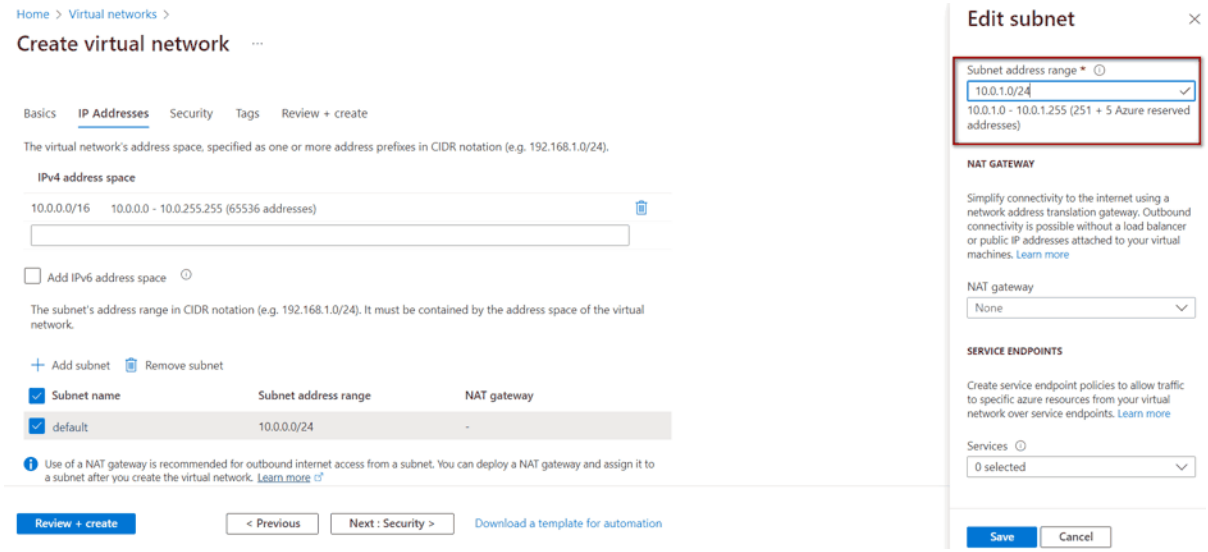


Figure 4.6: Create a virtual network (Change default subnet)

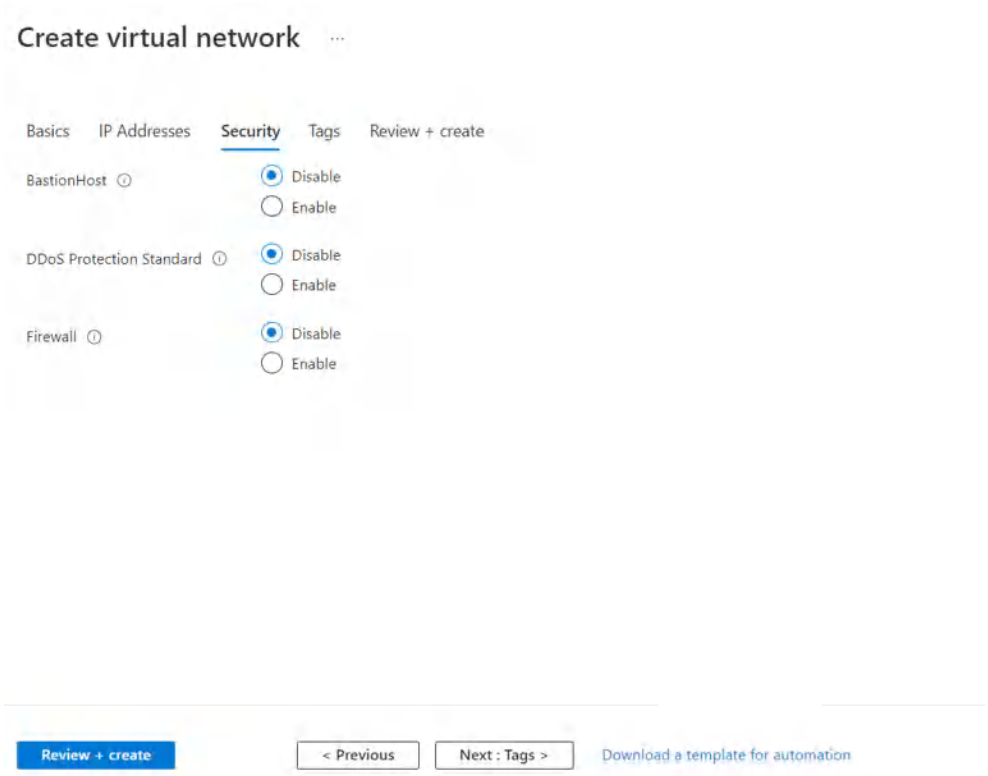


Figure 4.7: Create a virtual network

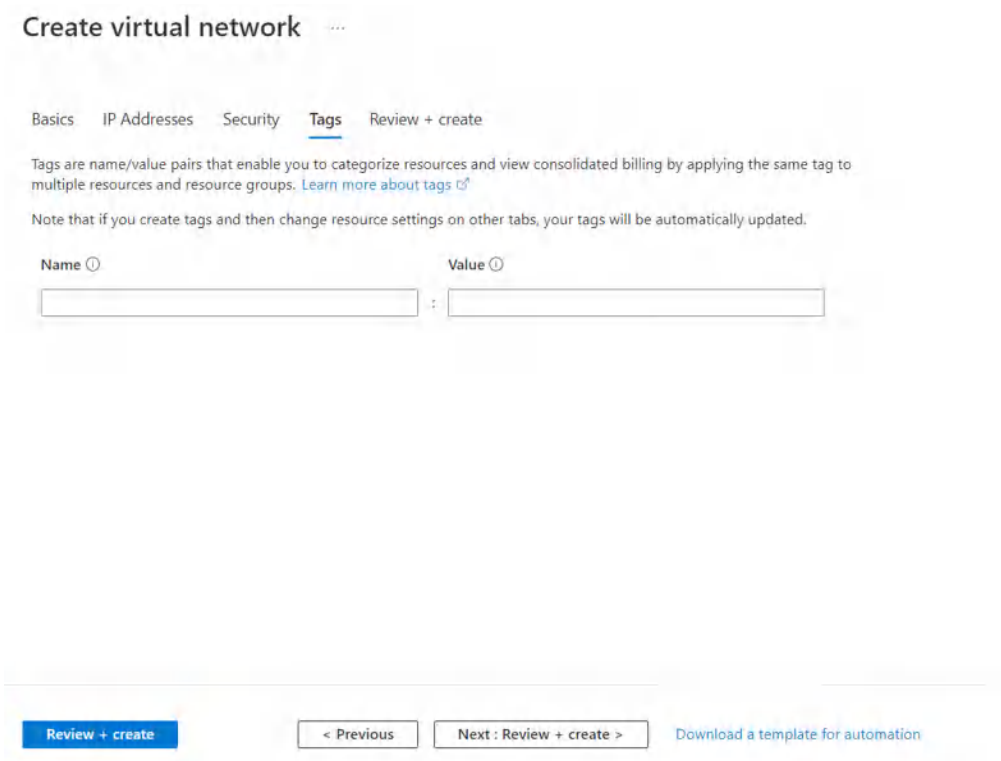


Figure 4.8: Create a virtual network

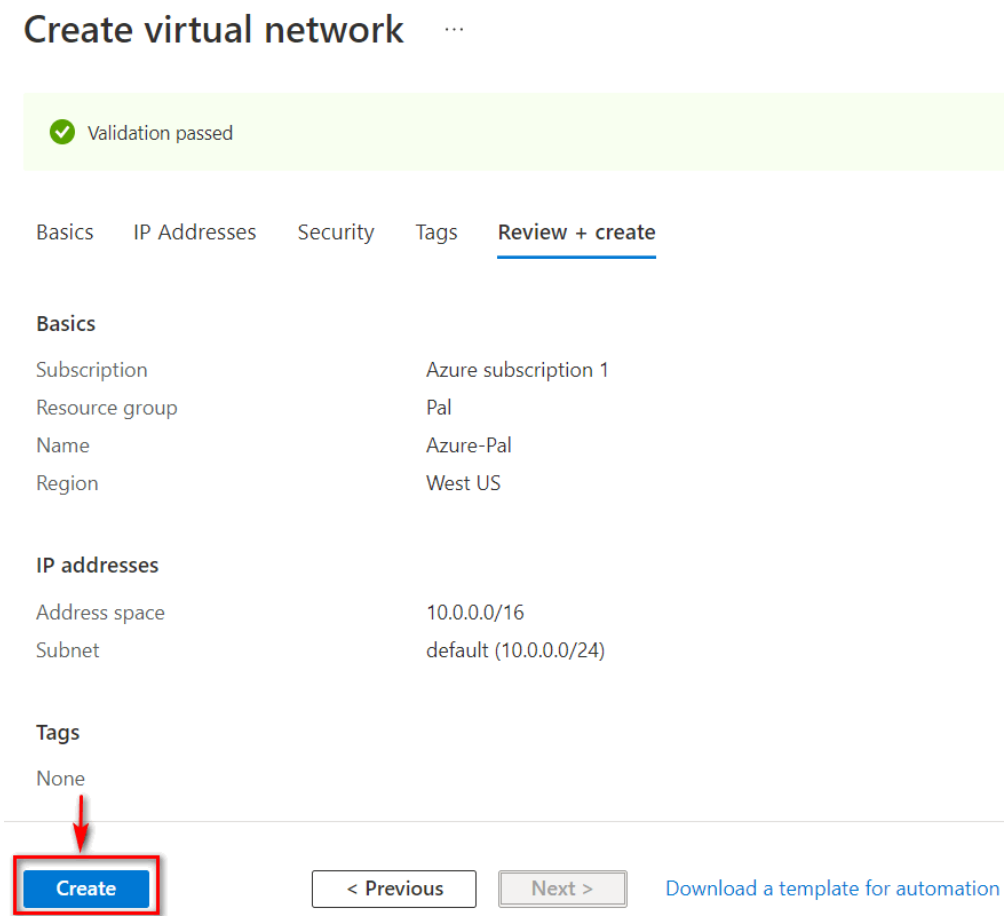


Figure 4.9: Create a virtual network

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.

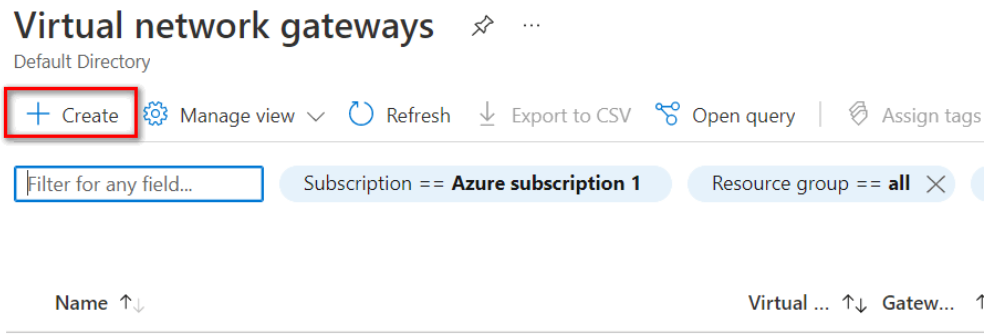


Figure 4.10: Create a virtual network gateway

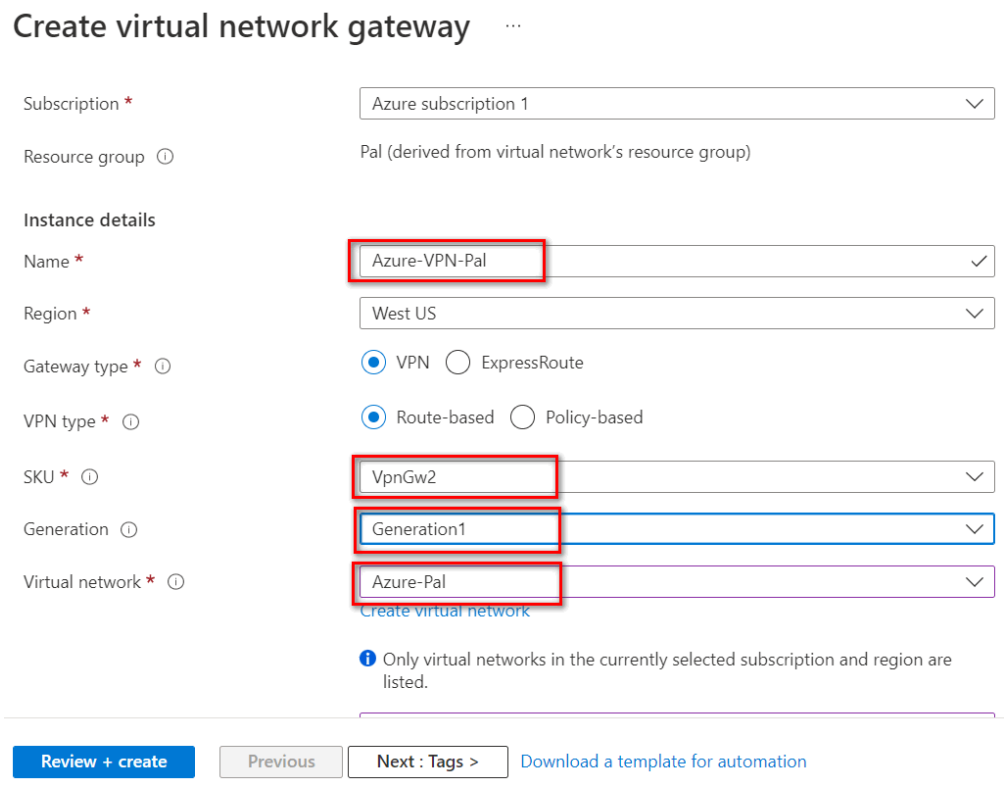


Figure 4.11: Create a virtual network gateway

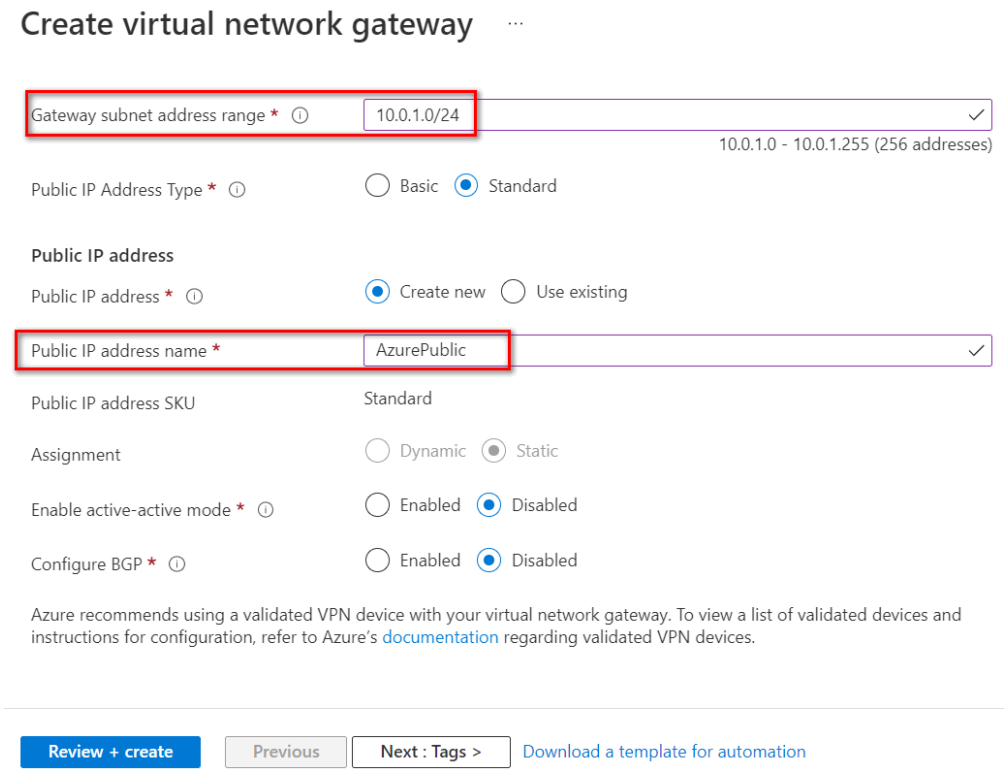


Figure 4.12: Create a virtual network gateway

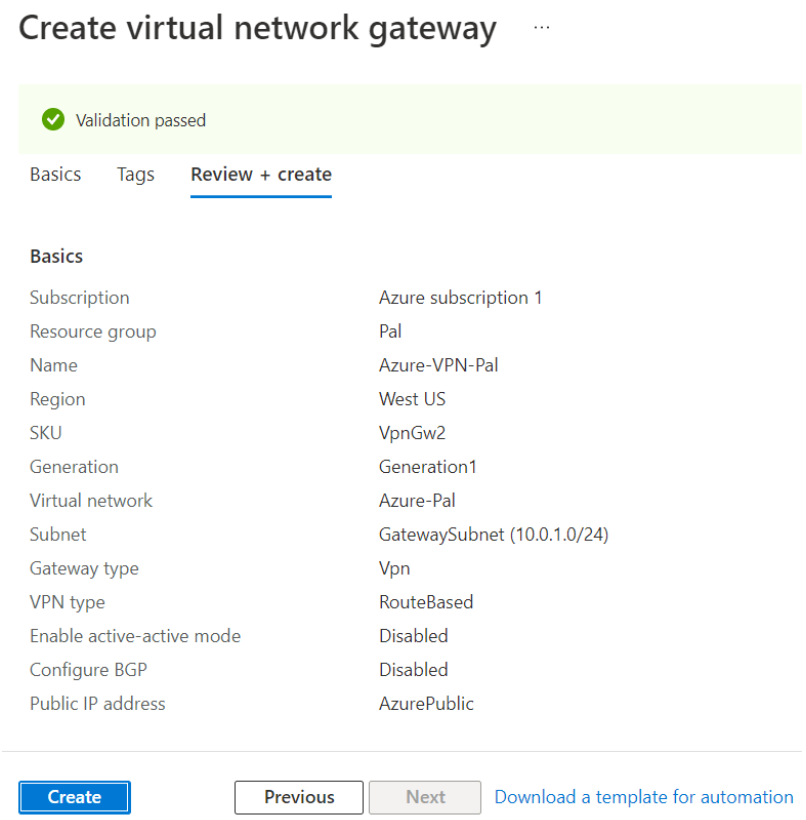


Figure 4.13: Create a virtual network gateway

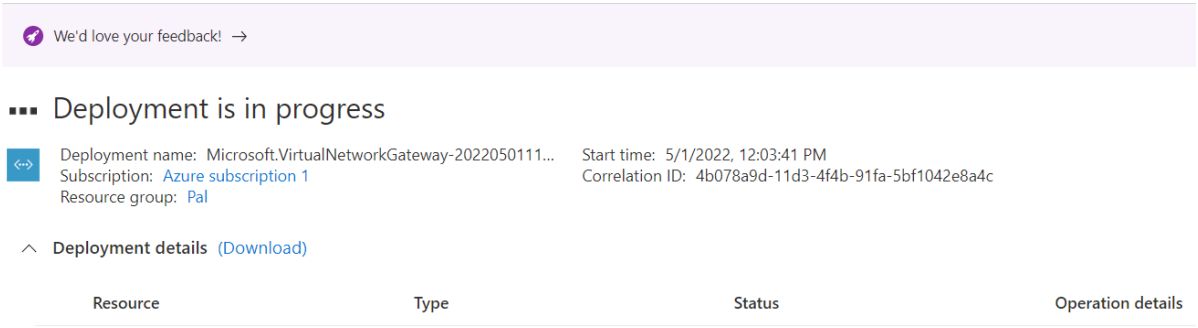


Figure 4.14: Create a virtual network gateway (deployment)

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

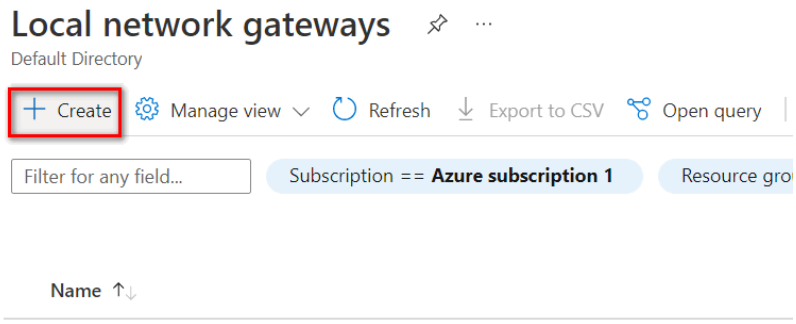


Figure 4.16: Create a local network gateway

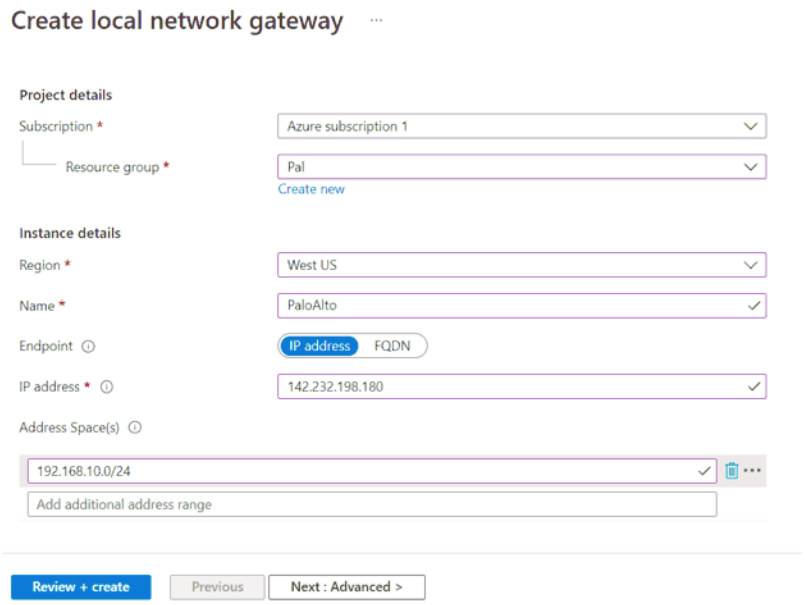


Figure 4.17: Create a local network gateway

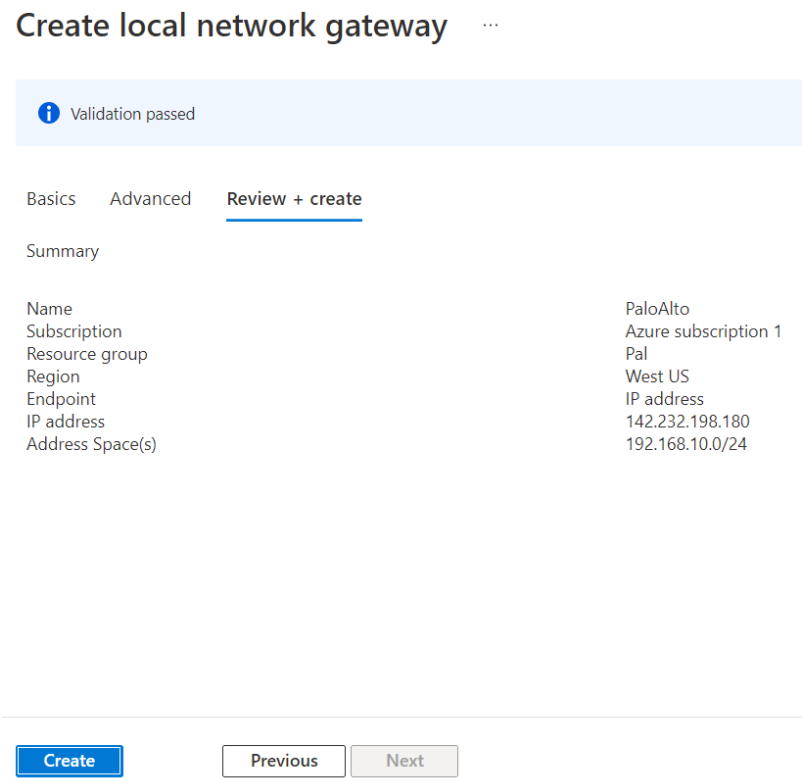


Figure 4.18: Create a local network gateway (review + create)

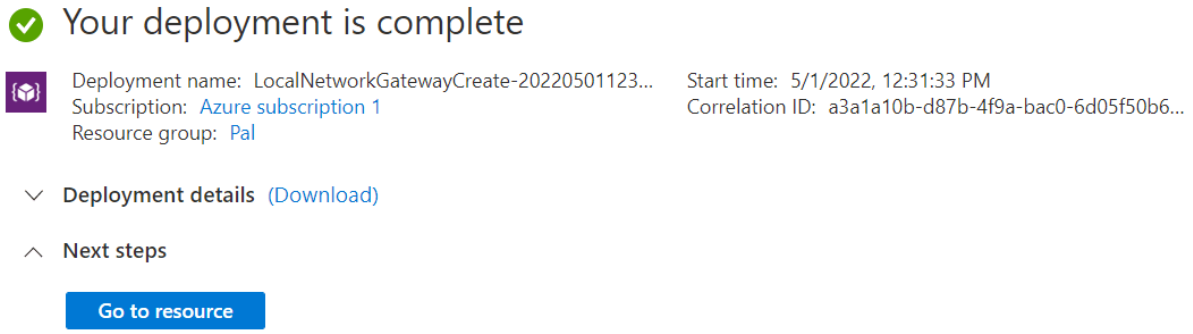


Figure 4.19: Verify local network gateway deployment

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

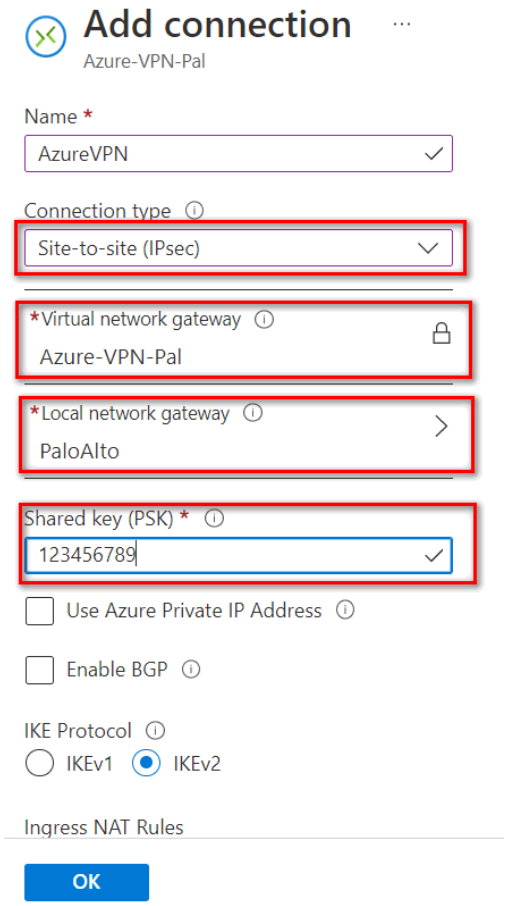


Figure 4.20: Connection configuration

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.

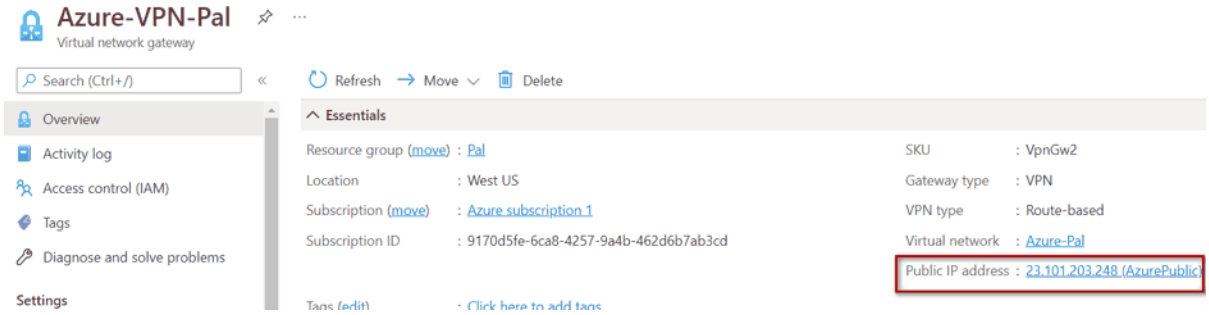


Figure 4.21: Verify the public IP address

Palo Alto Configuration

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

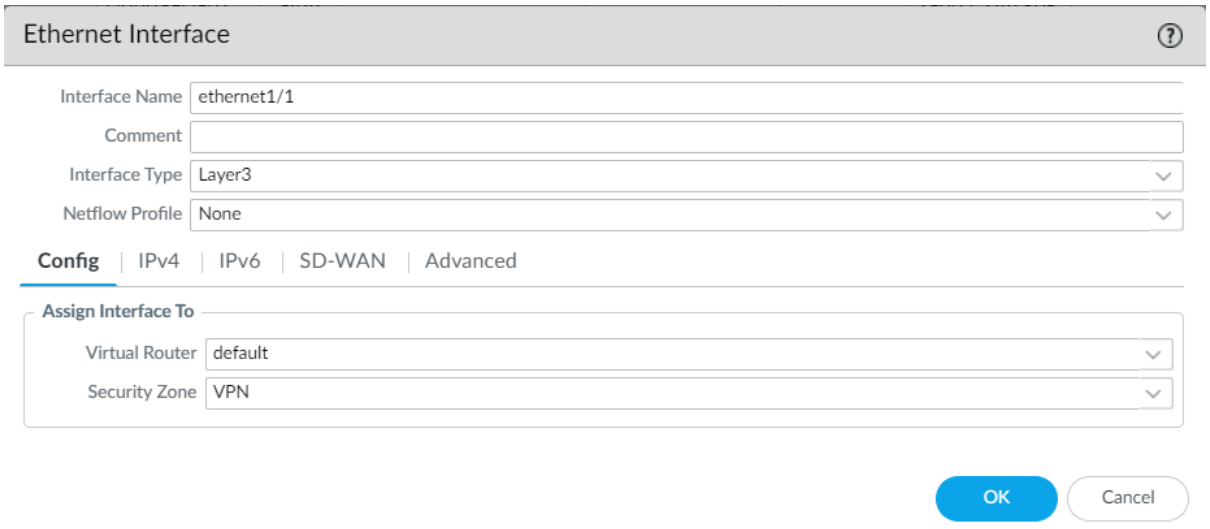


Figure 4.22: Ethernet 1/1 Config

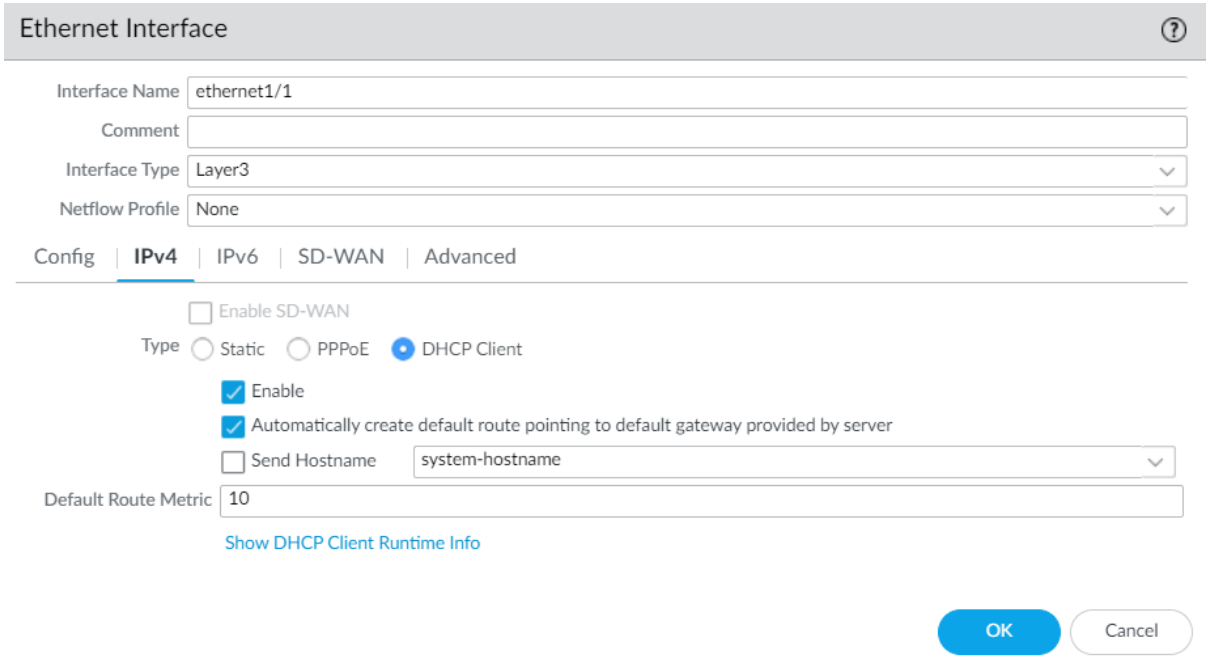


Figure 4.23: Ethernet 1/1 IPV4

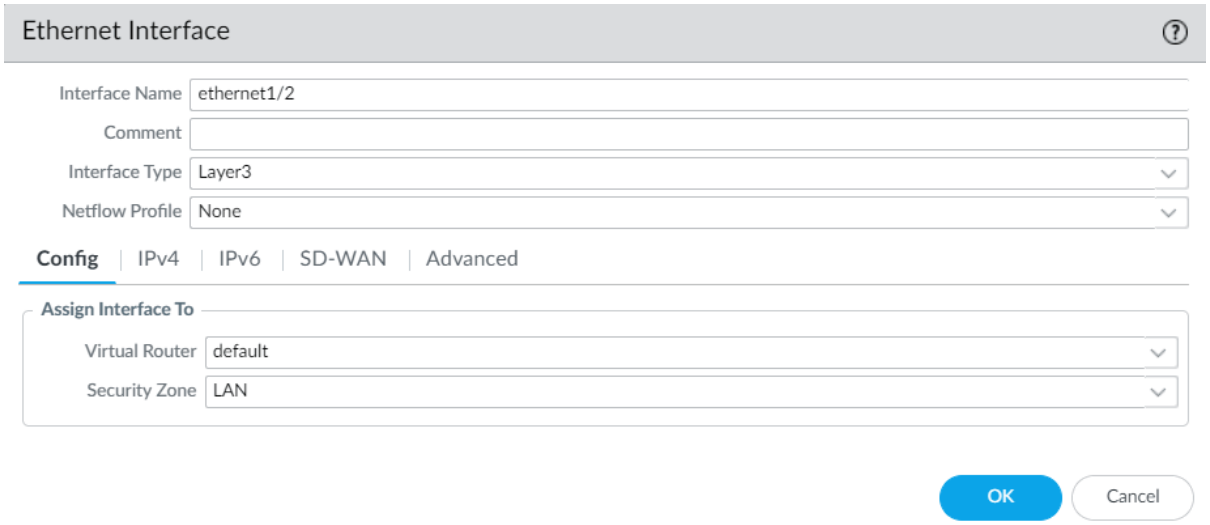


Figure 4.24: Ethernet 1/2 Config

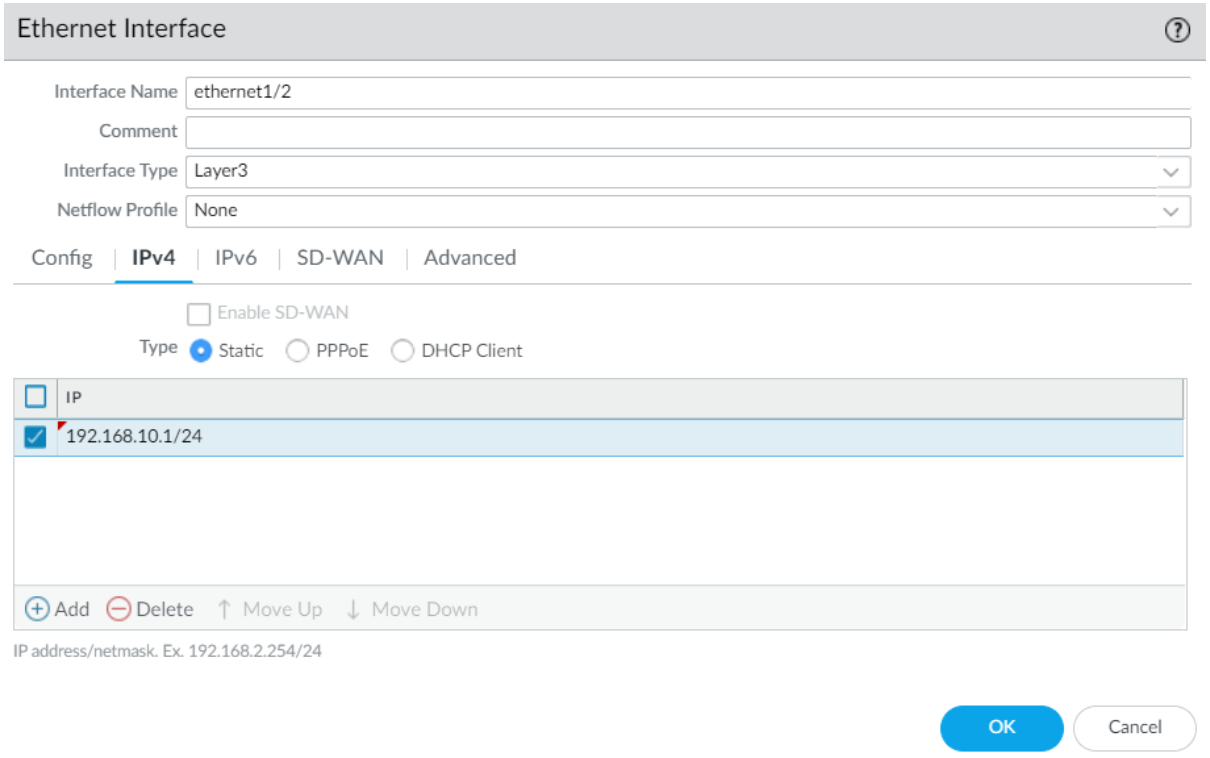


Figure 4.25: Ethernet 1/2 IPv4

Then, create a tunnel.

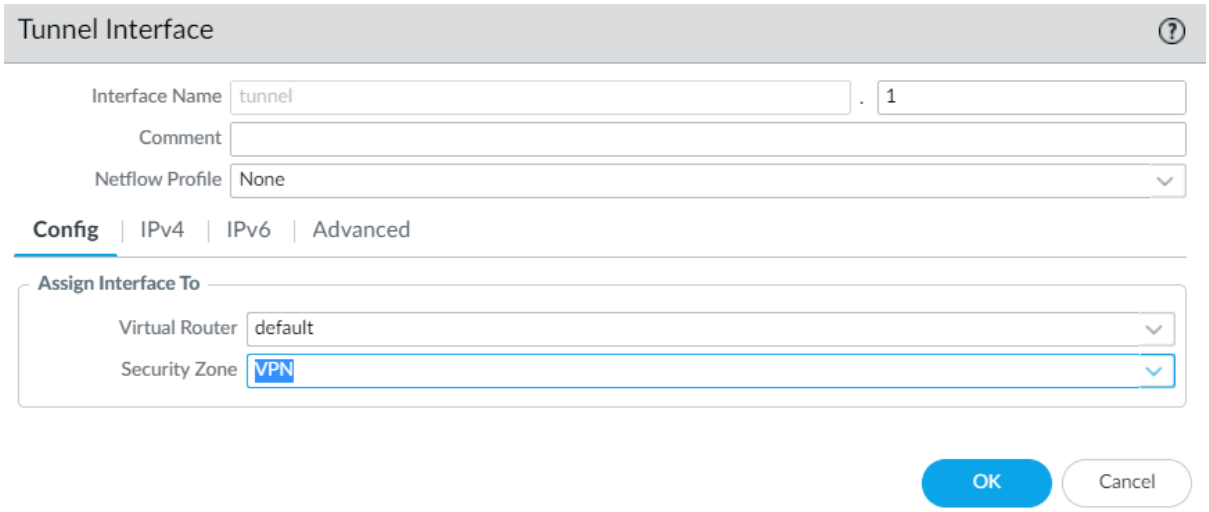


Figure 4.26: Create a tunnel 1

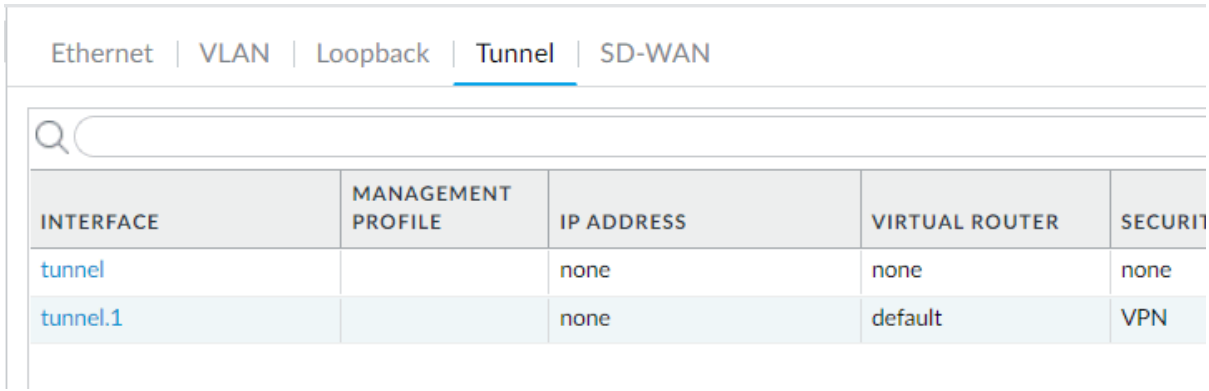


Figure 4.27: Verify Tunnel1

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.

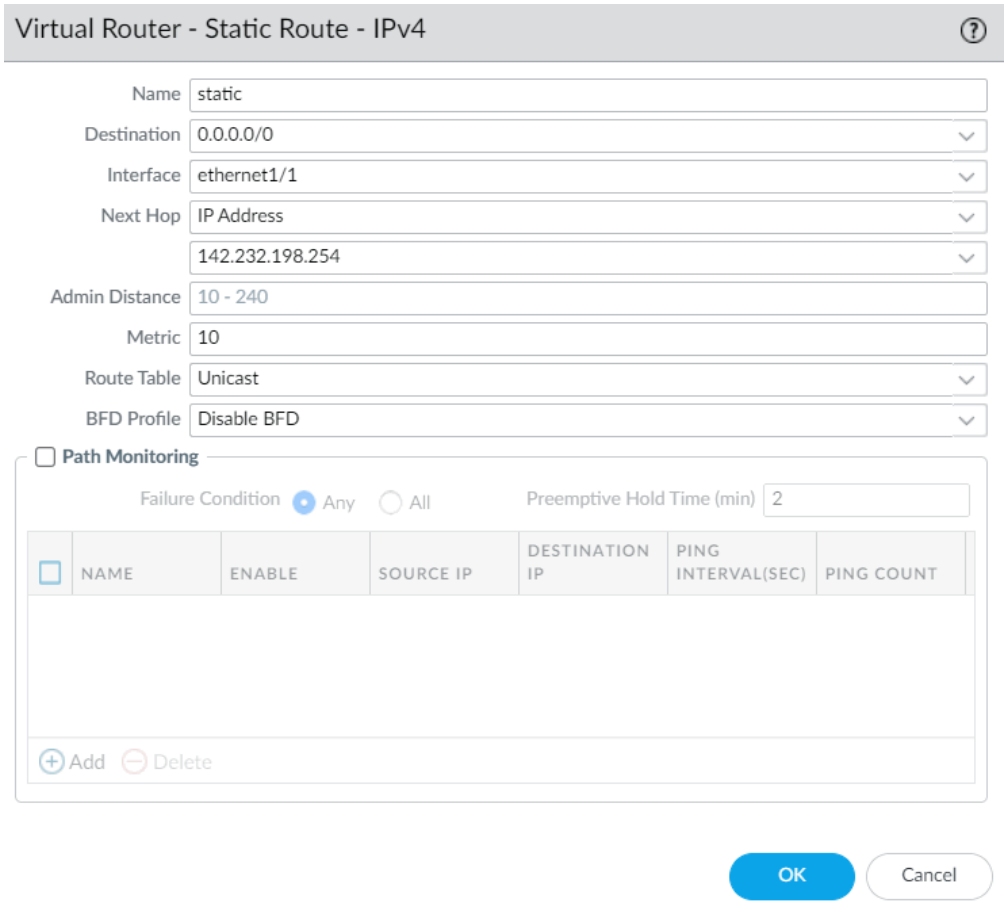


Figure 4.28: Create a static route to ethernet 1/1

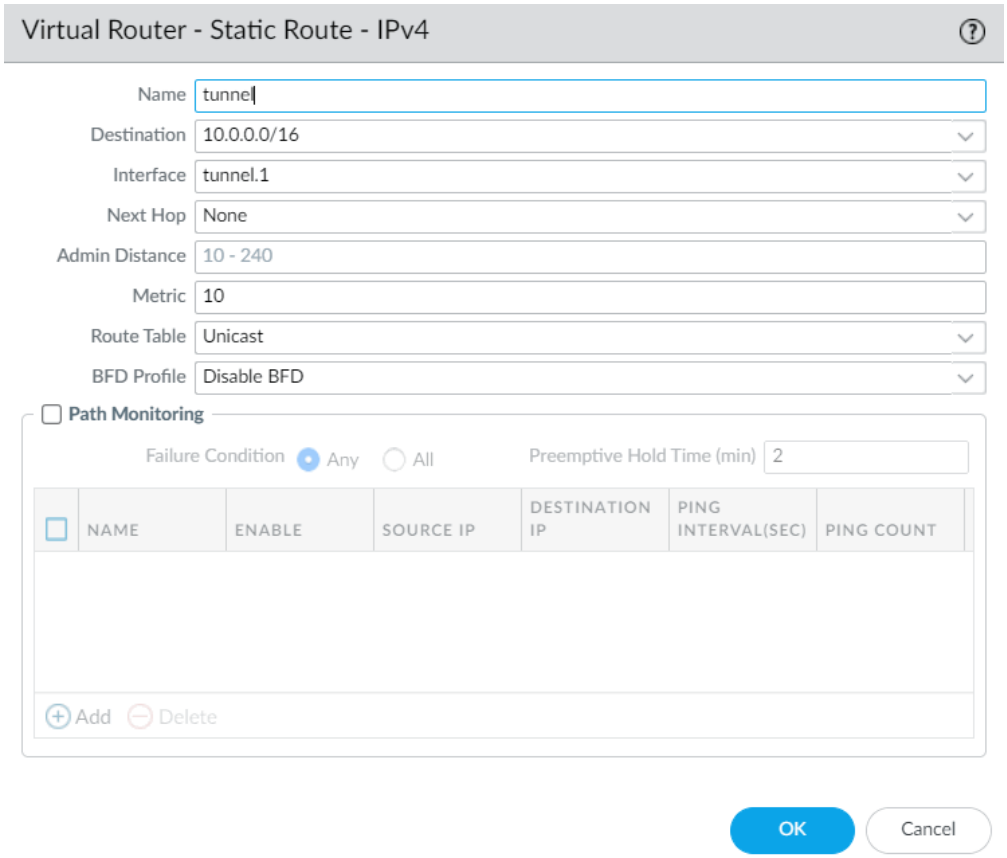


Figure 4.29: Create a static route to tunnel.1

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

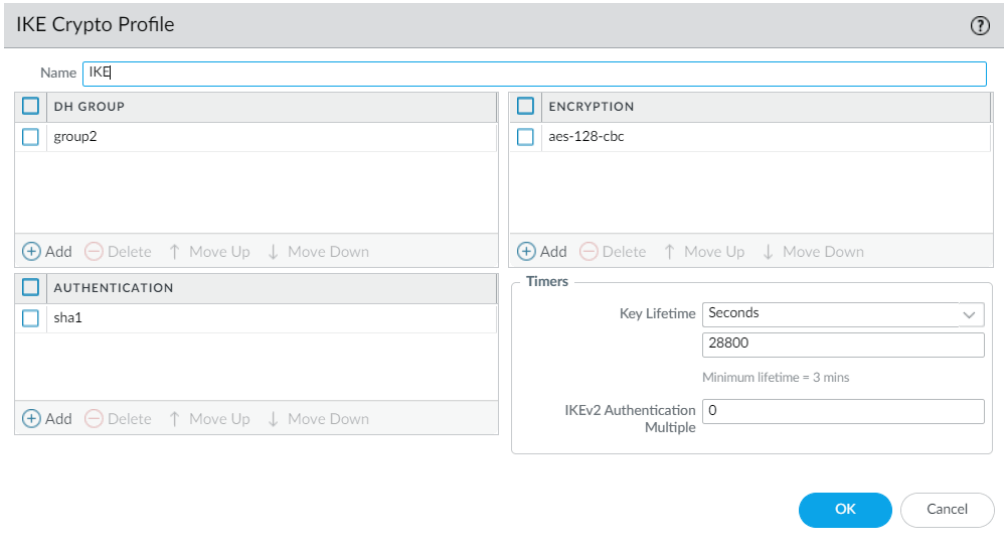


Figure 4.30: Create an IKE Crypto Profile

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

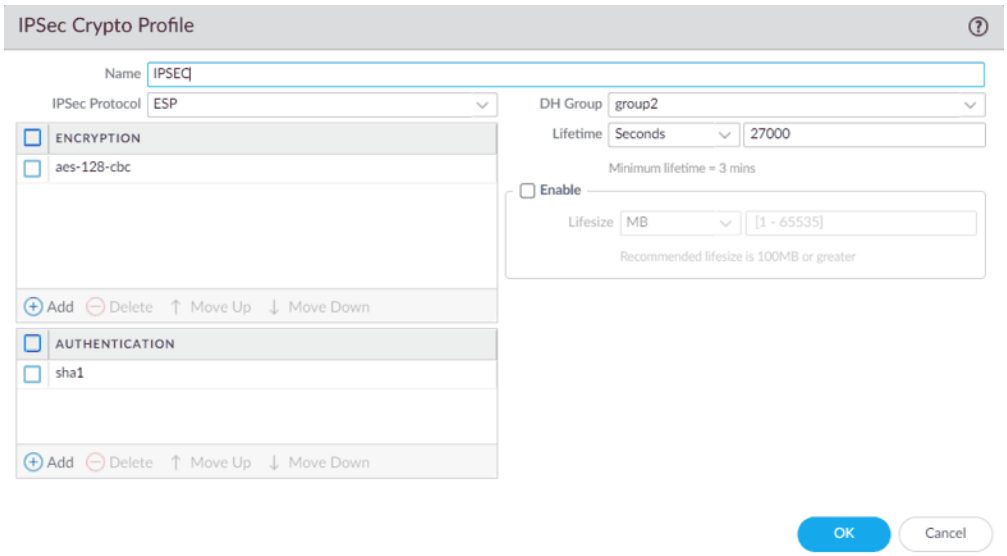


Figure 4.31: Create an IPsec Crypto Profile

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

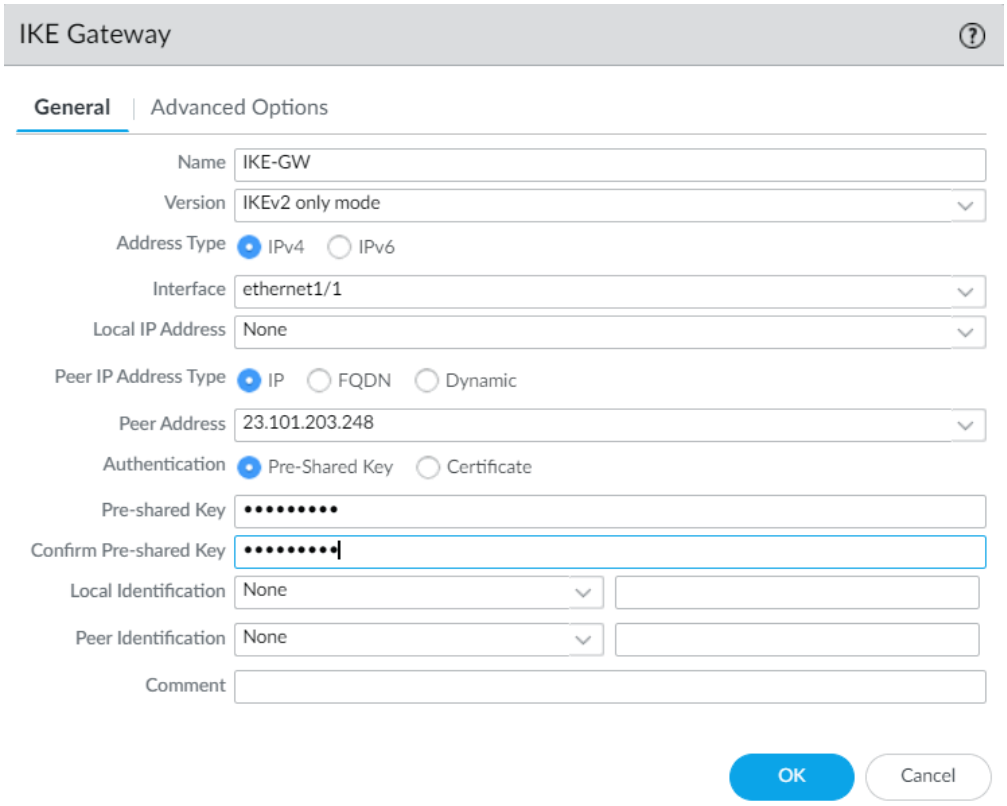


Figure 4.32: Create an IKE Gateway

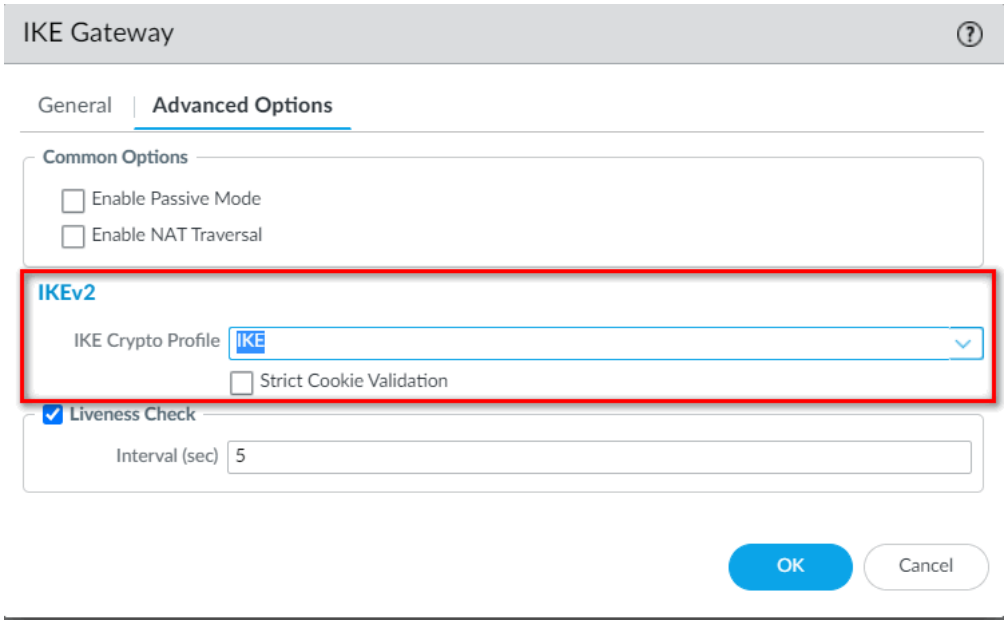


Figure 4.33: Select IKE Crypto Profile

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

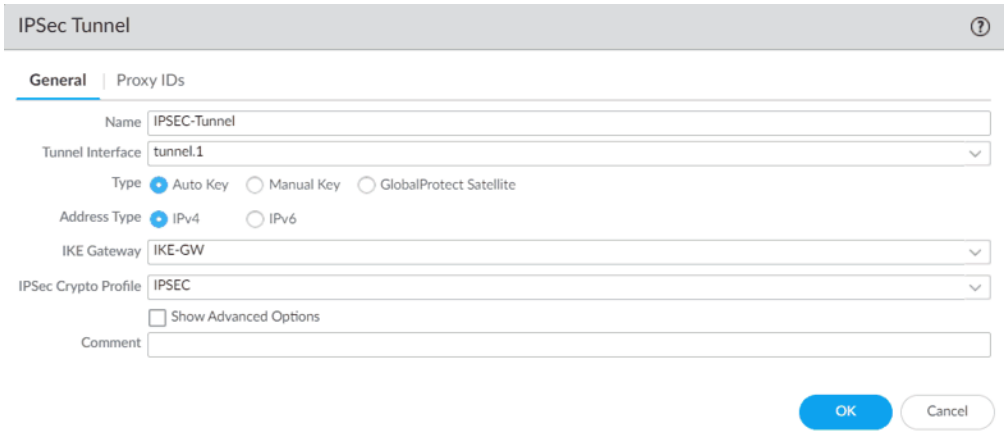


Figure 4.34: Create an IPsec Tunnel

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

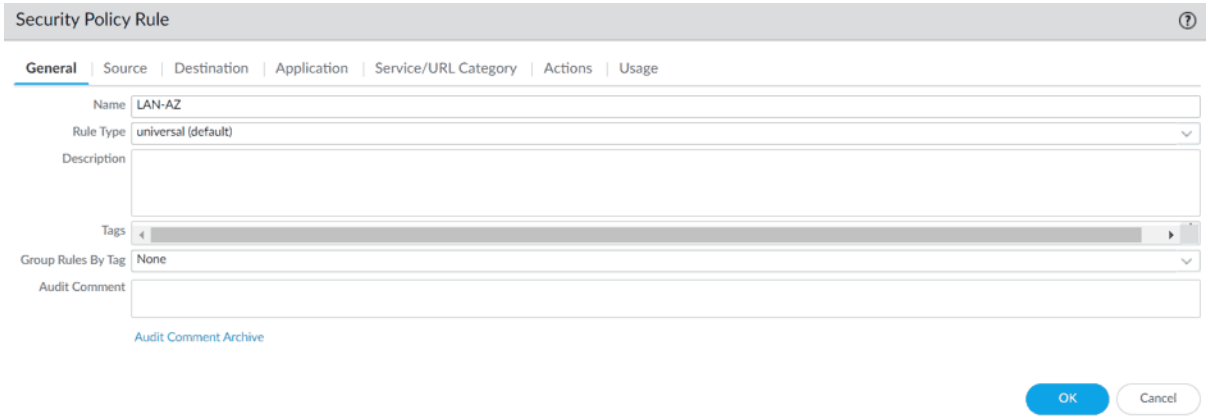


Figure 4.35: Create a security policy "LAN-AZ"

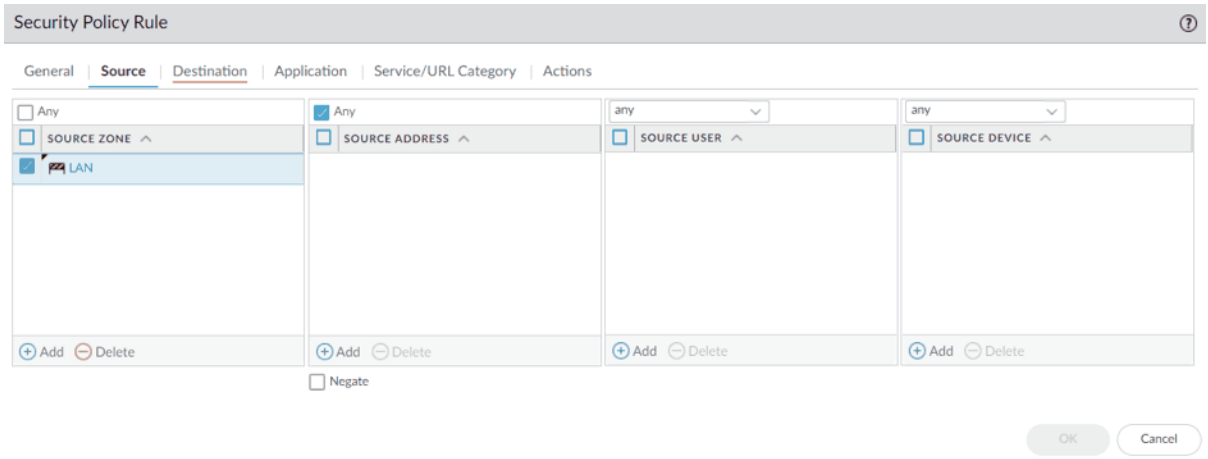


Figure 4.36: Create a security policy "LAN-AZ." Select the source zone as LAN.

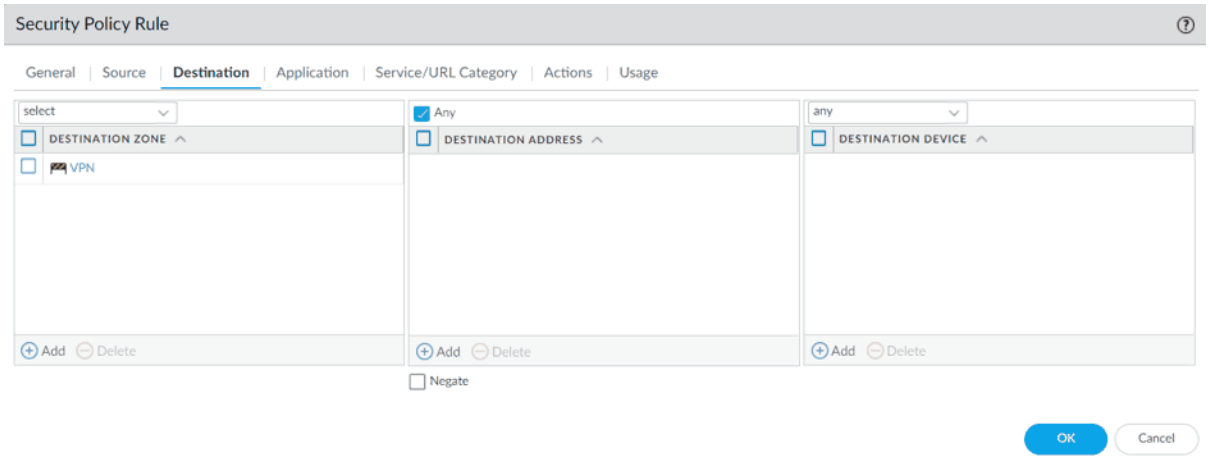


Figure 4.37: Create a security policy "LAN-AZ." Select destination zone as VPN.

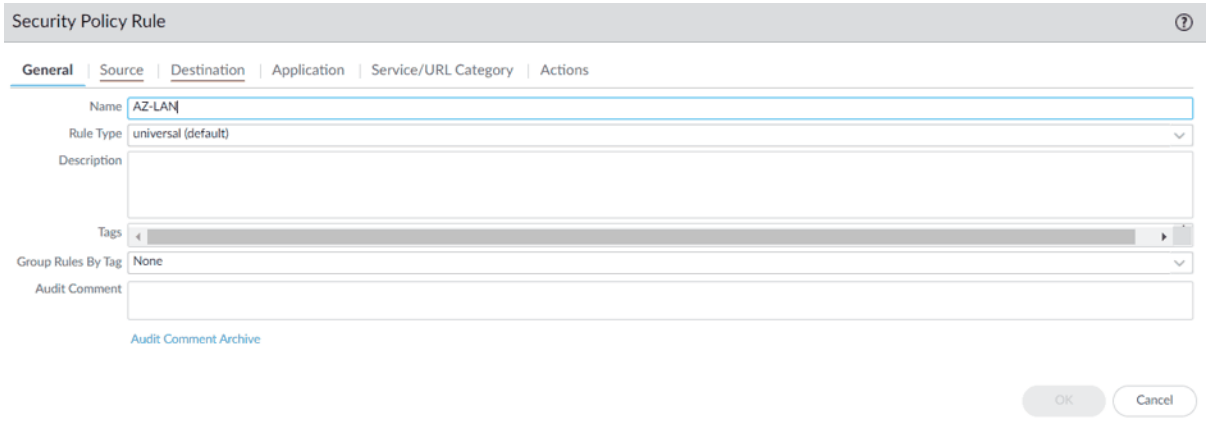


Figure 4.38: Create a security policy "AZ-LAN"

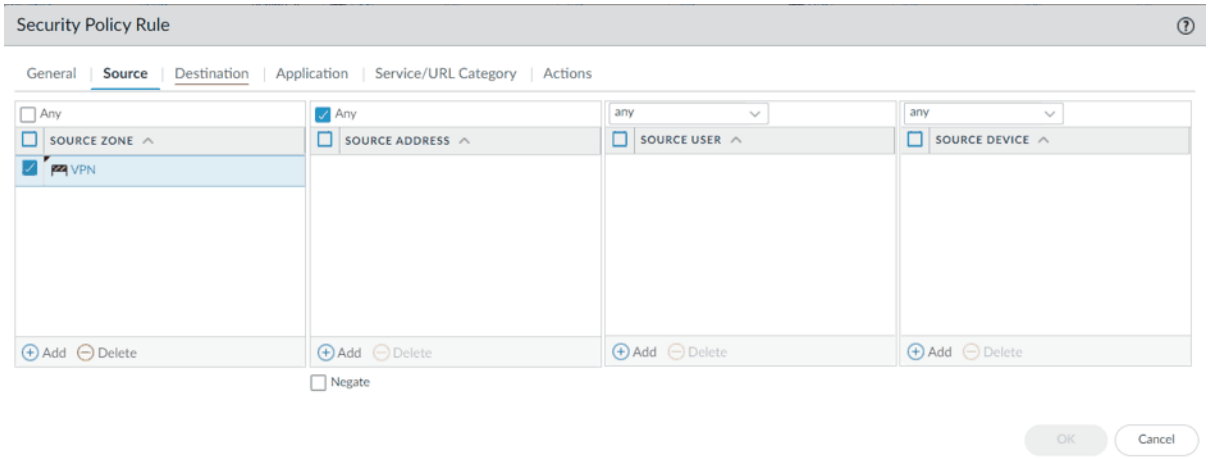


Figure 4.39: Create a security policy "AZ-LAN." Select source zone as VPN.

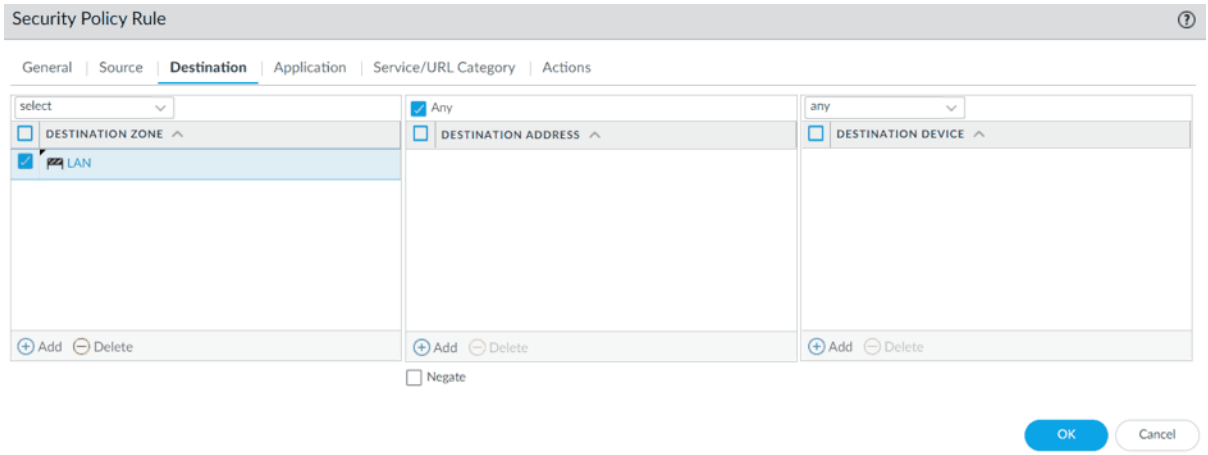


Figure 4.40: Create a security policy "AZ-LAN." Select destination zone as LAN.

Don't forget to commit the configuration!

Verify Connections

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

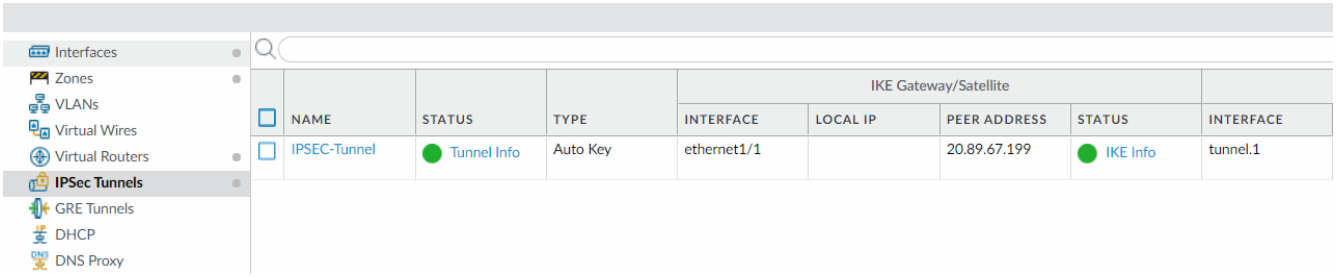


Figure 4.41: Verify IPsec Tunnel

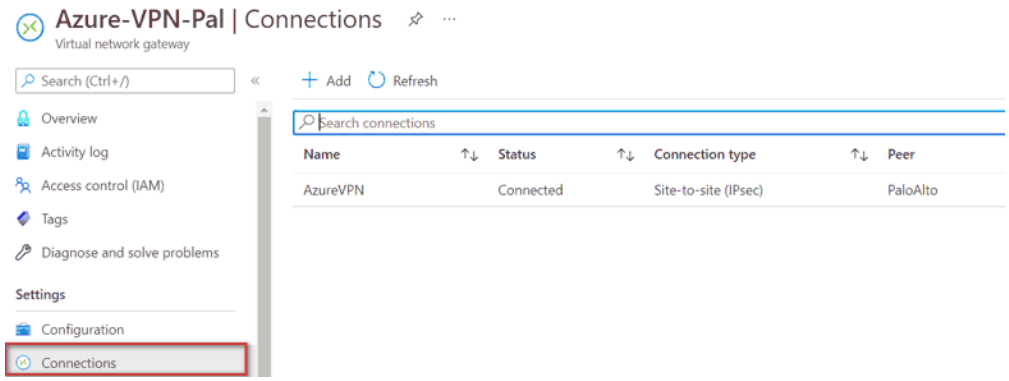


Figure 4.42: Verify connections in Azure

```
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

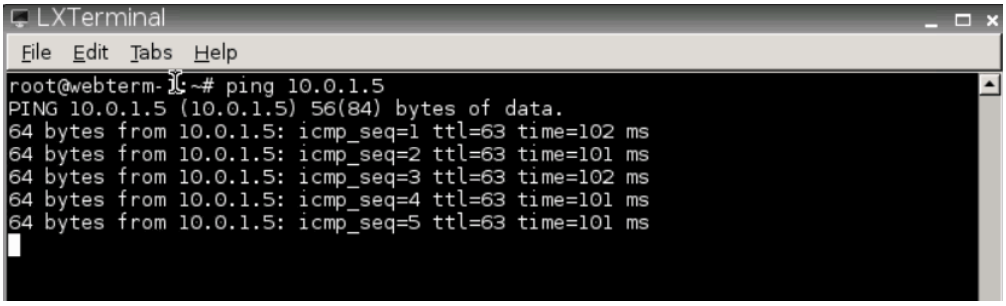


Figure 4.44: Verify ping from webterm to Windows in Azure

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.

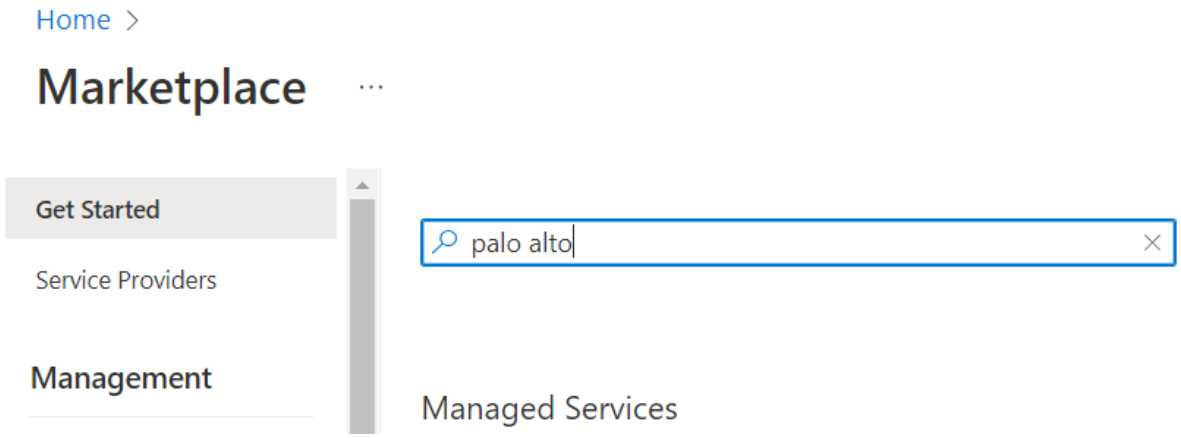


Figure 4.45: Search for Palo Alto

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

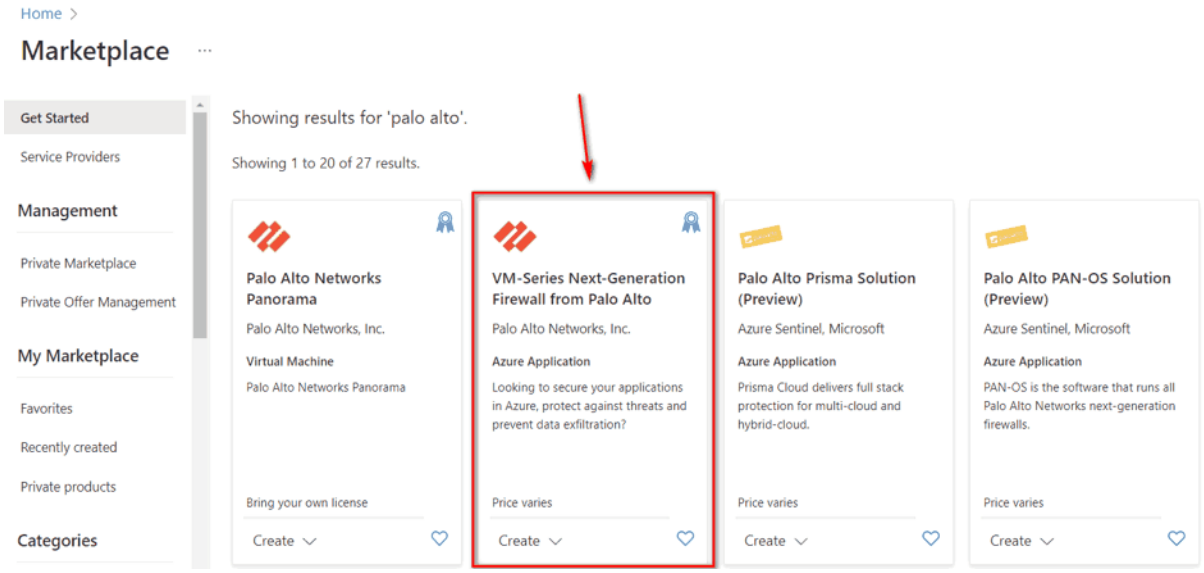


Figure 4.46: Select VM Series Next-Generation Firewall

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.

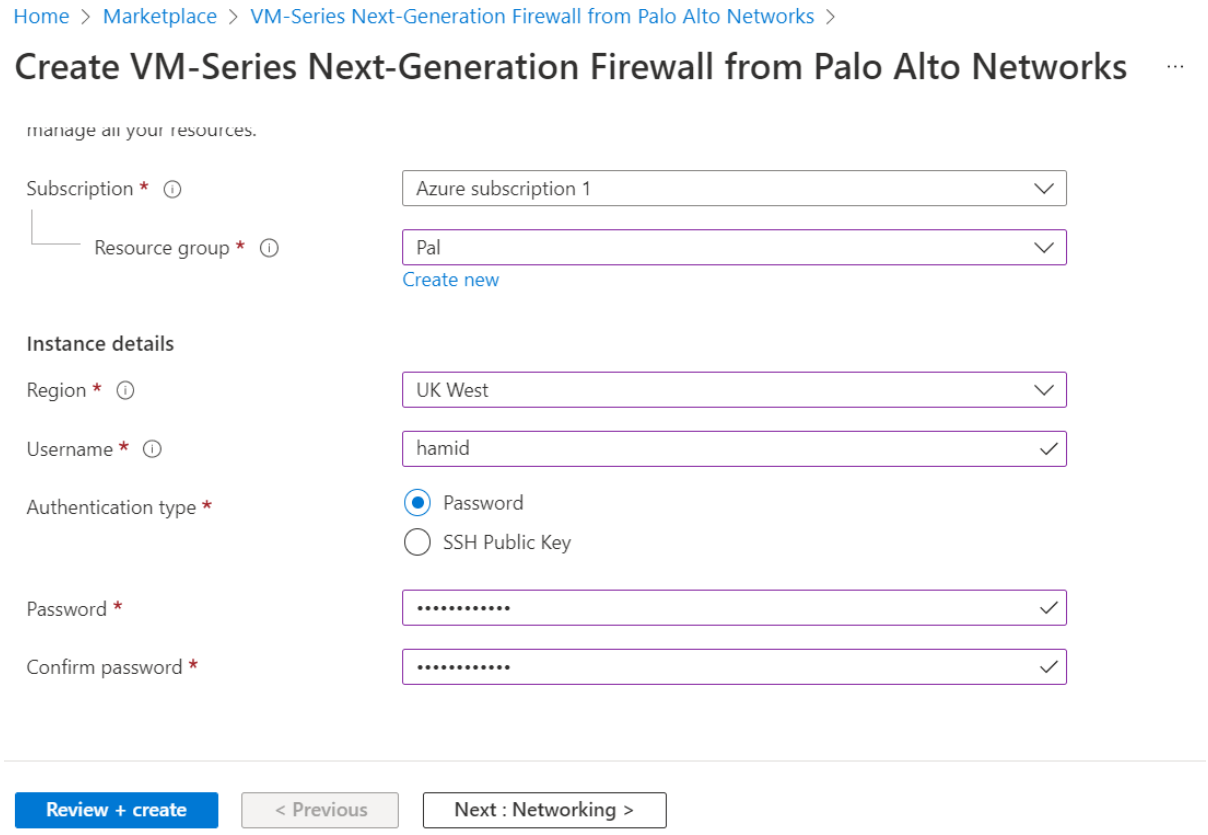


Figure 4.48: Create a VM-Series Palo Alto

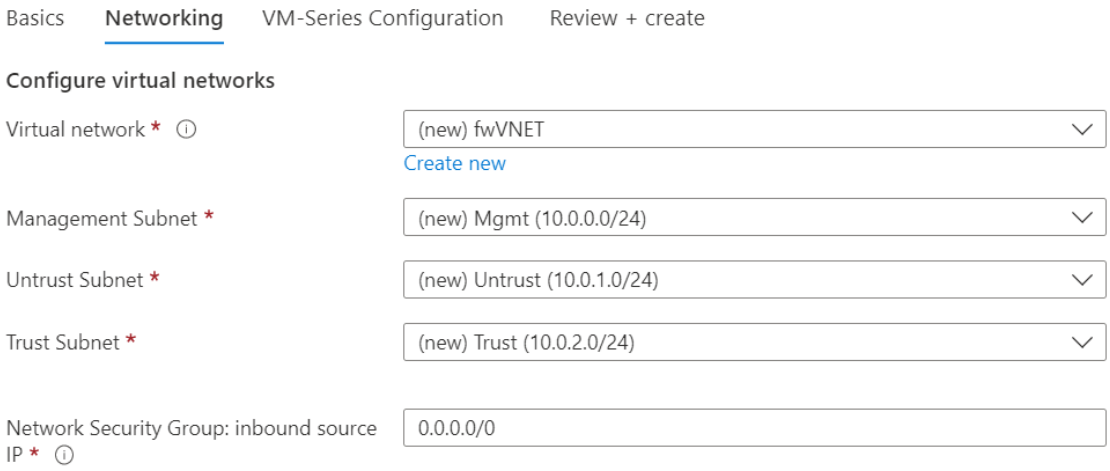


Figure 4.49: Networking configuration

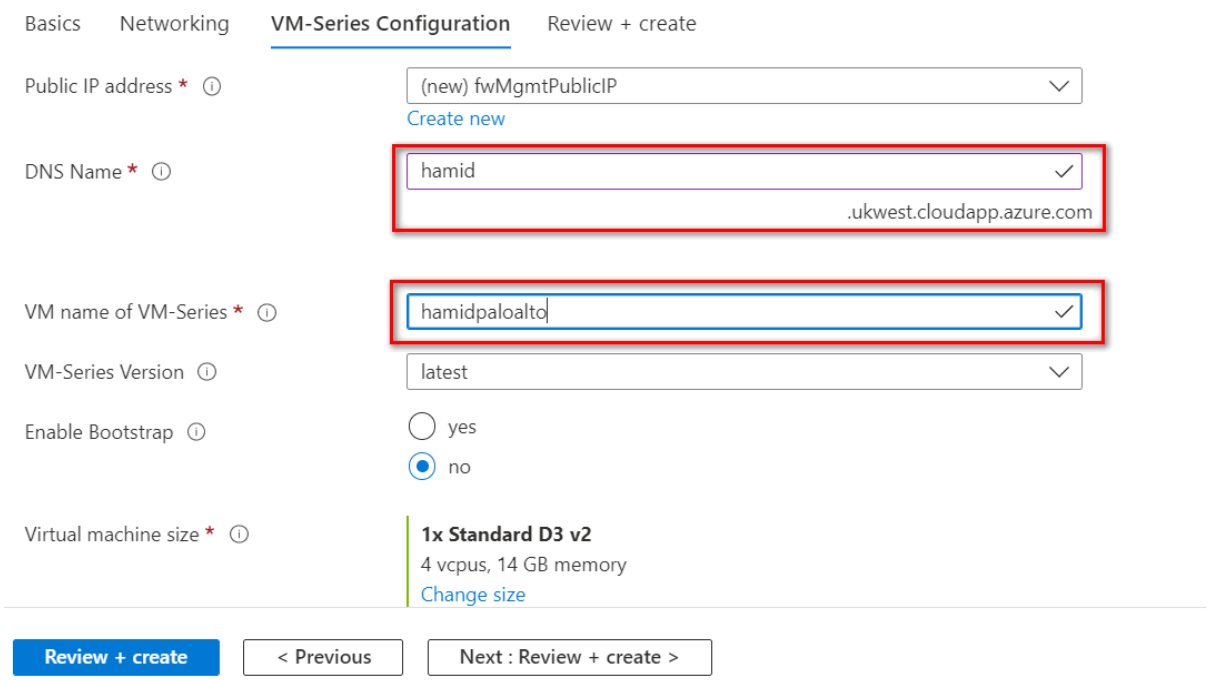


Figure 4.50: VM Configuration (DNS-VM Name)

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.

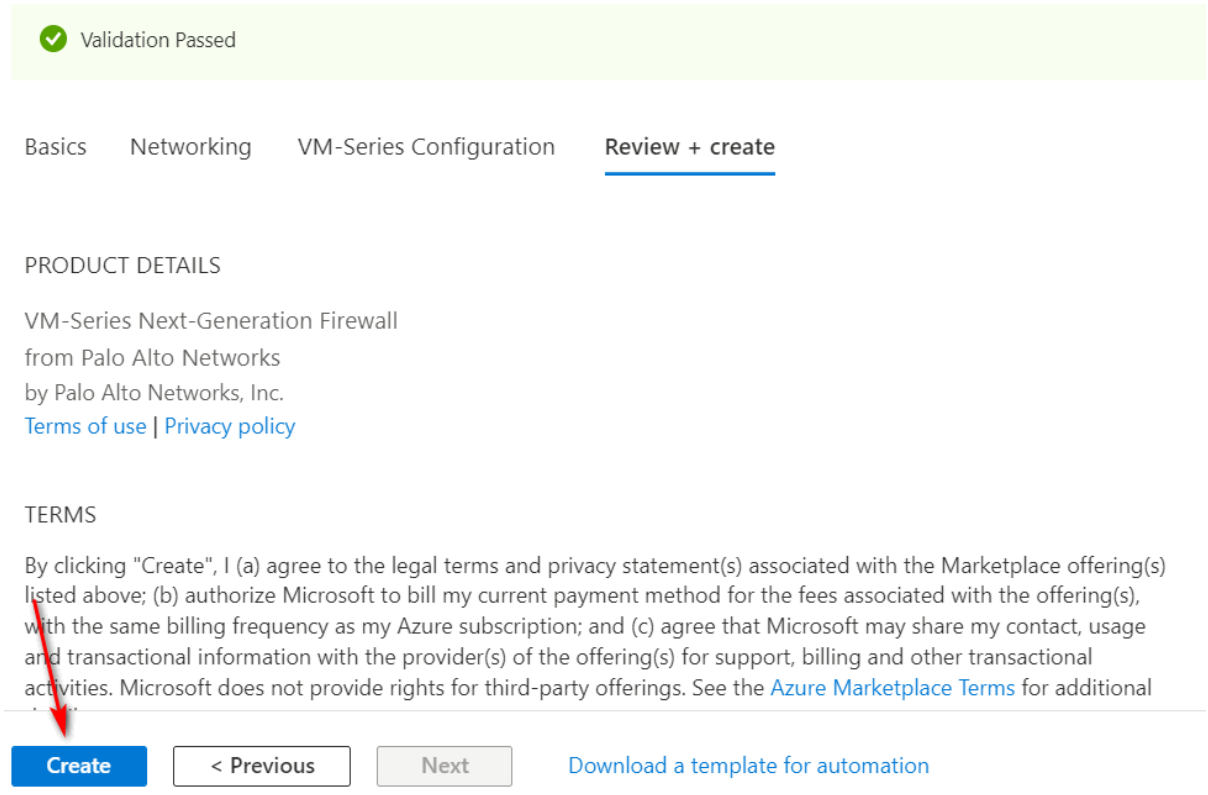


Figure 4.51: Create a firewall

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

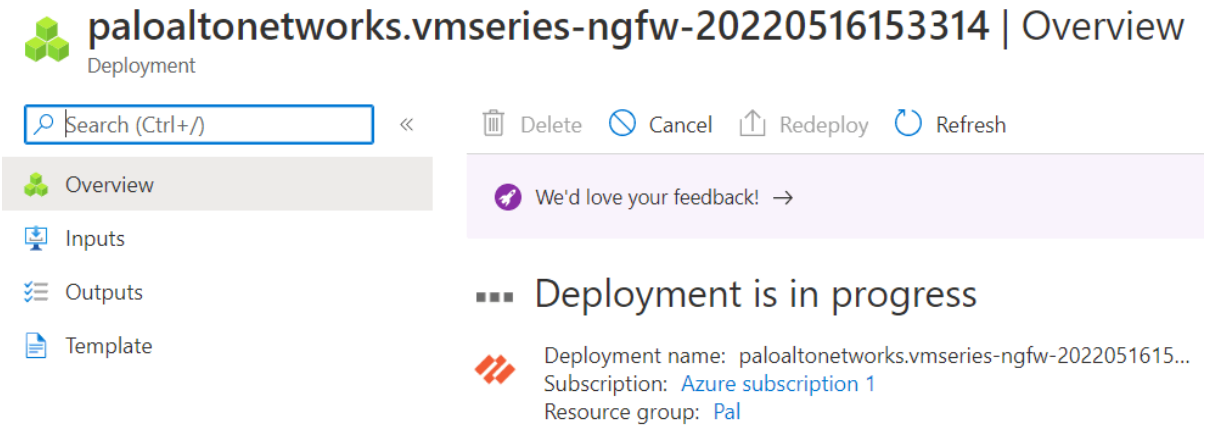


Figure 4.52: Deployment is in progress

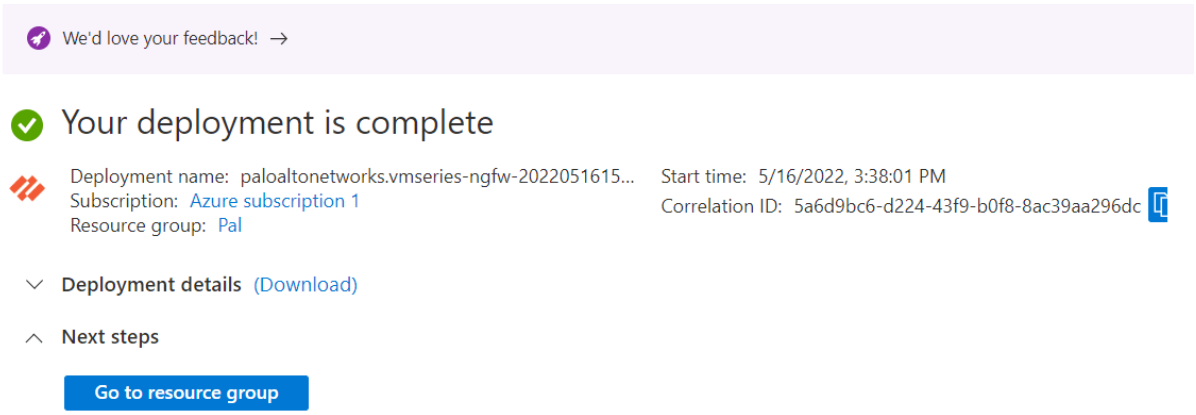


Figure 4.53: Deployment is complete

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

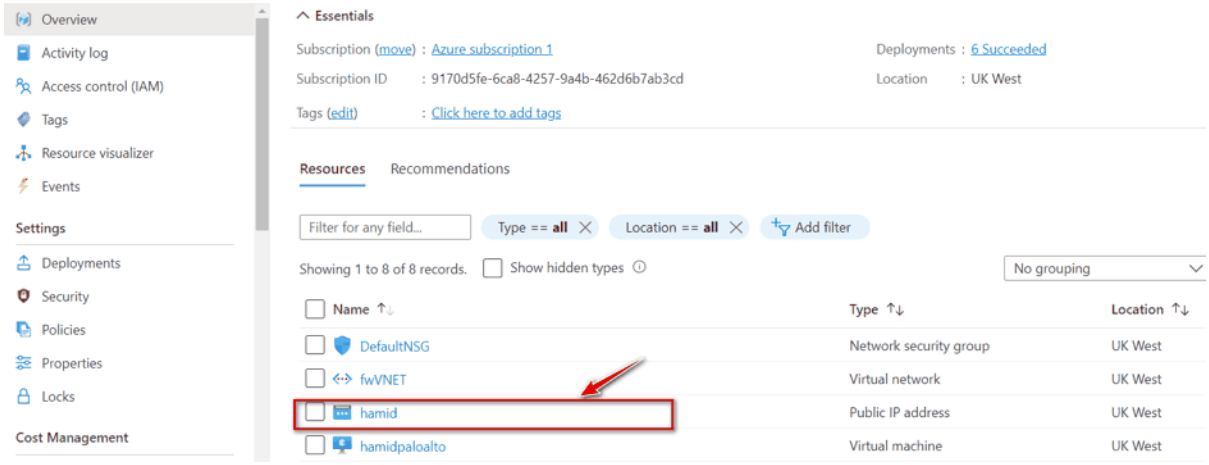


Figure 4.54: Palo Alto Public IP Address

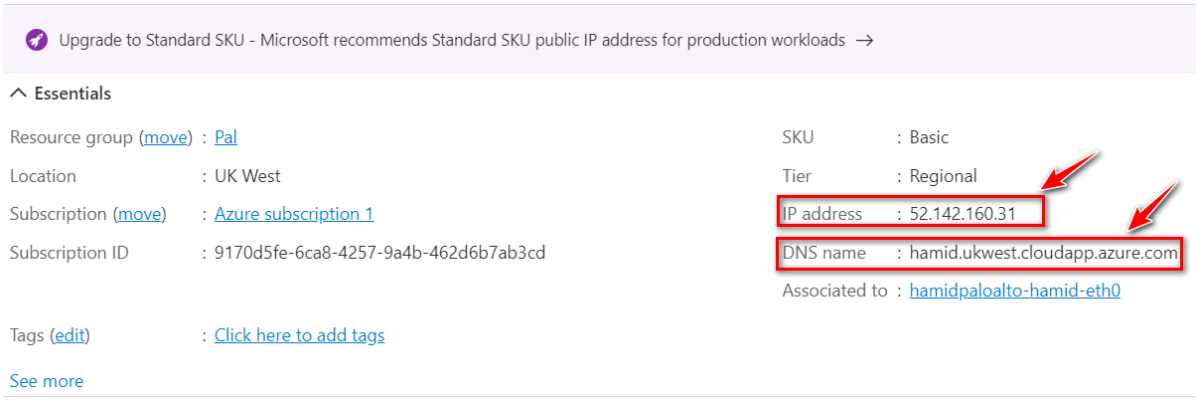


Figure 4.55: Palo Alto Public IP Address

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

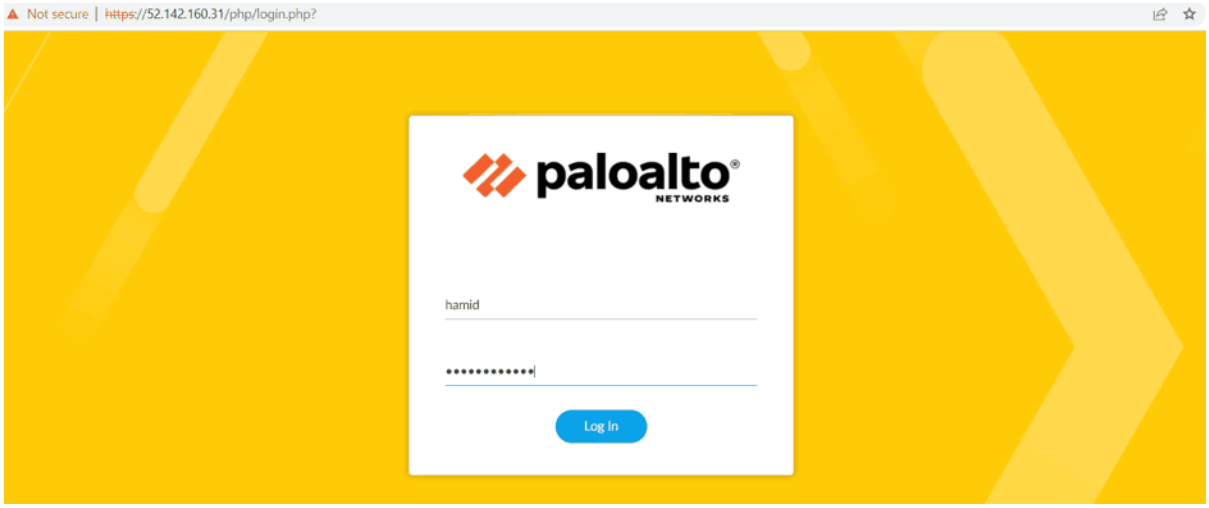


Figure 4.56: Palo Alto Firewall Credential Page

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

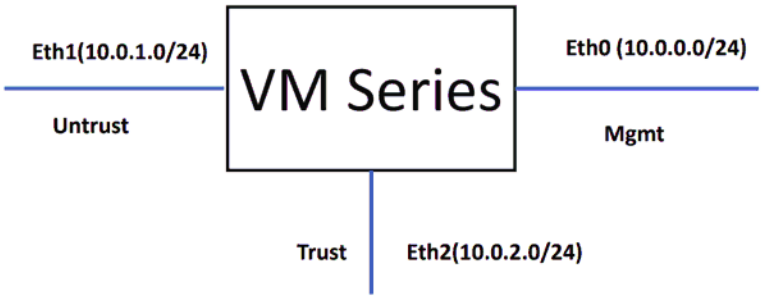


Figure 4.57: Palo Alto Firewall Interfaces by default

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

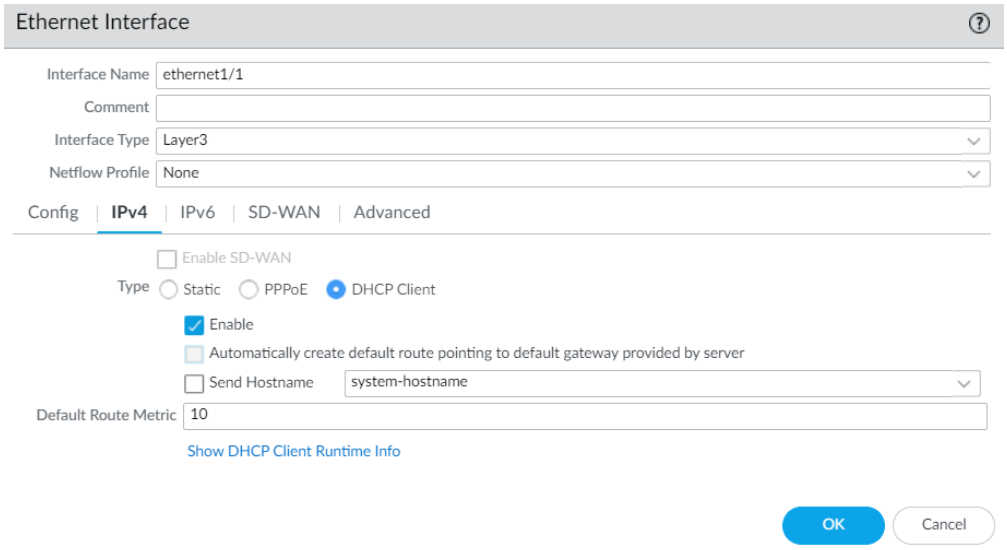


Figure 4.58: Ethernet1/1 configuration

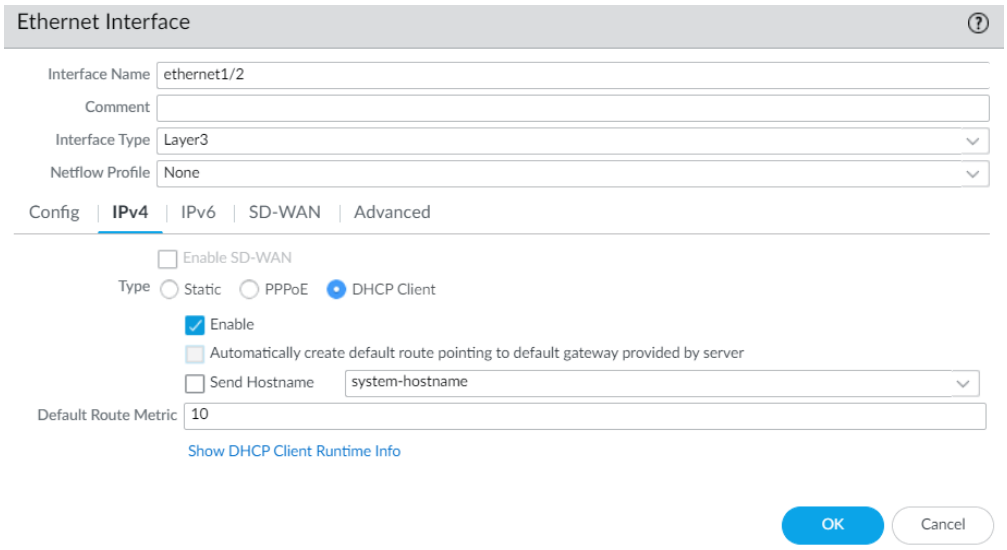


Figure 4.59: Ethernet1/2 configuration

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

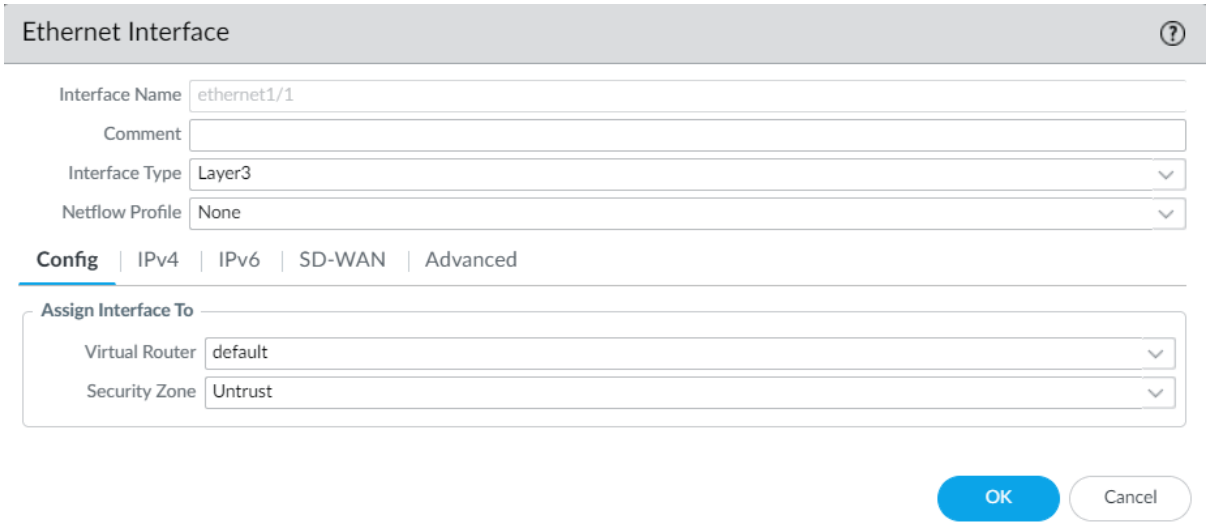


Figure 4.60: Ethernet1/1 zone and virtual router

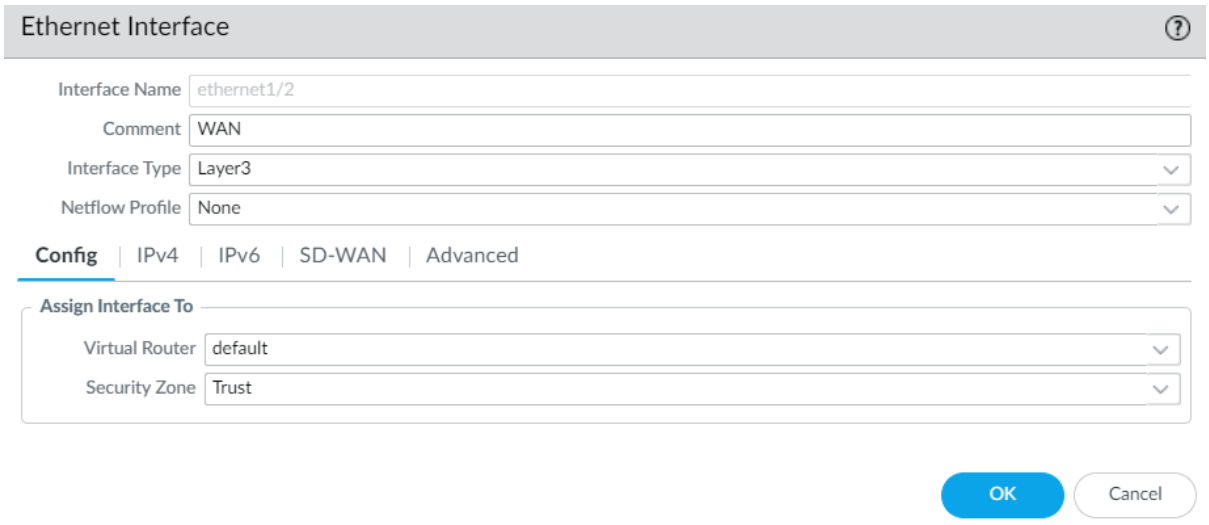


Figure 4.61: Ethernet1/2 zone and virtual router

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

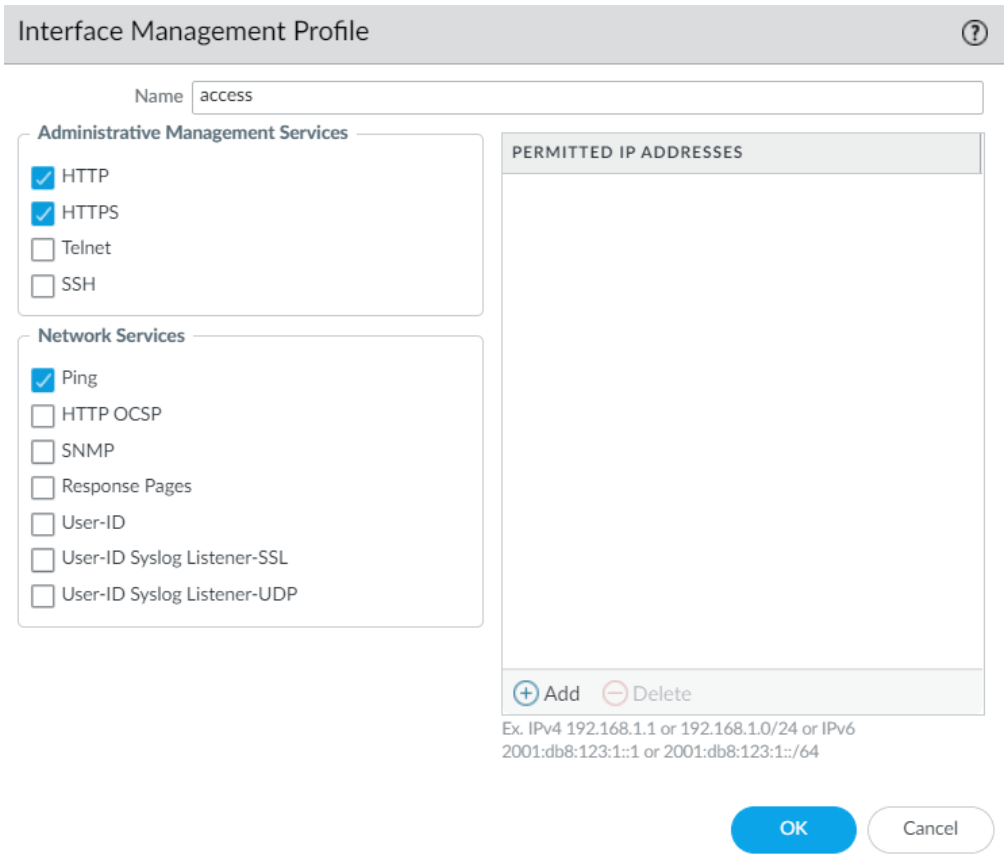


Figure 4.62: Ethernet1/1 Management Profile

12. Create a static route to 10.0.1.1.

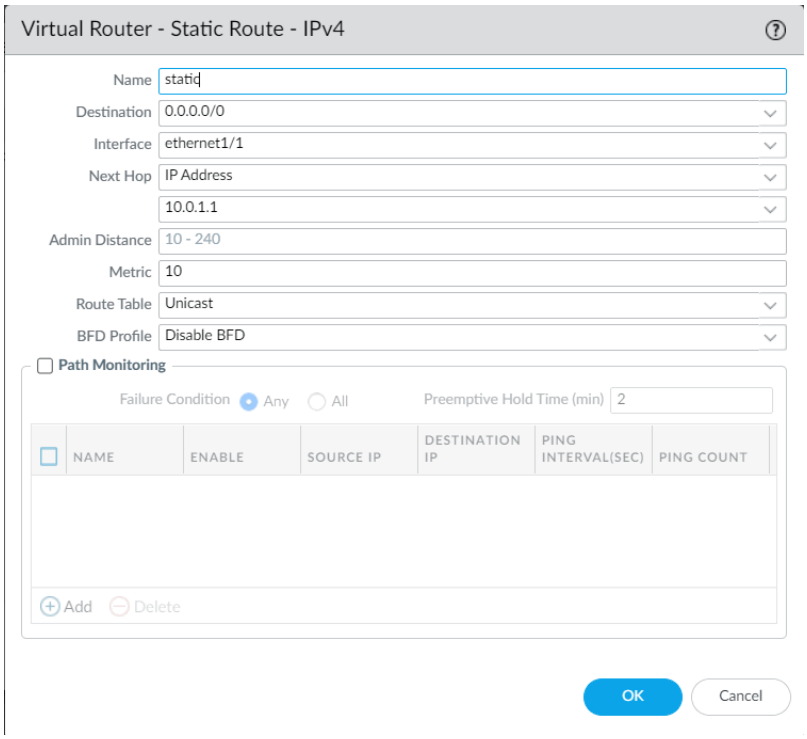


Figure 4.63: Create a static route to 10.0.1.1

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

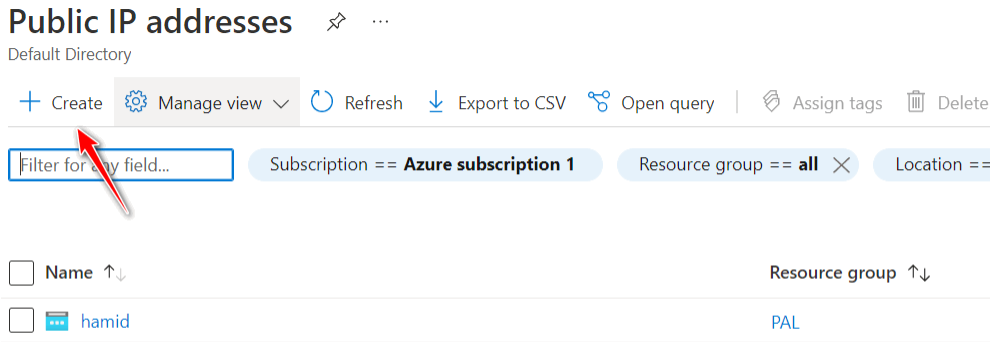


Figure 4.64: Create a public IP address

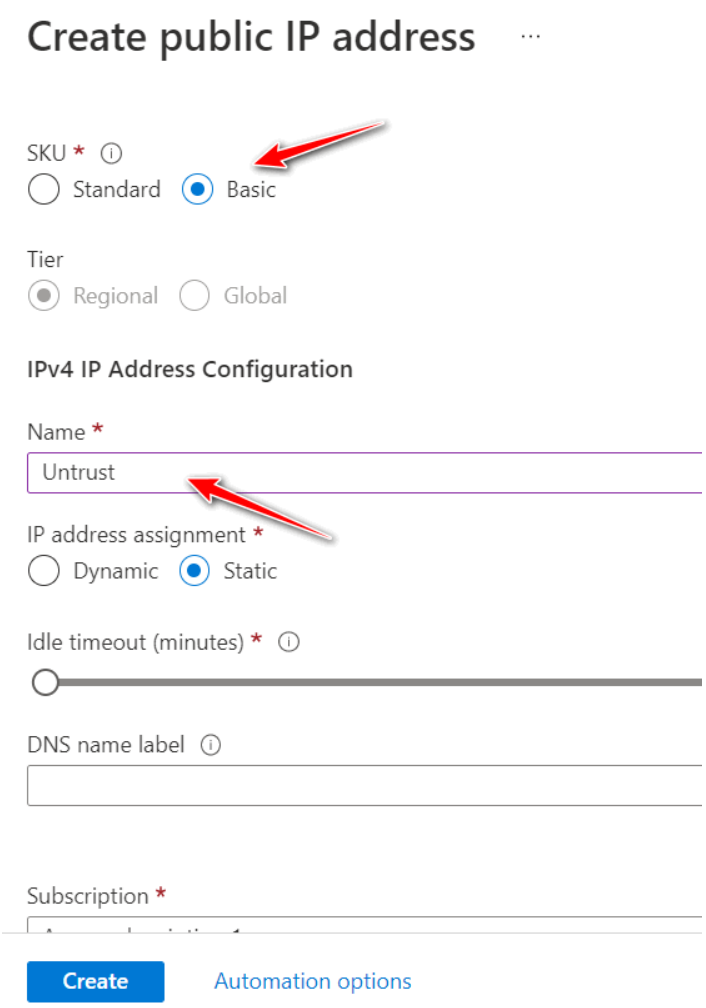


Figure 4.65: Create a public IP address (set SKU and name)

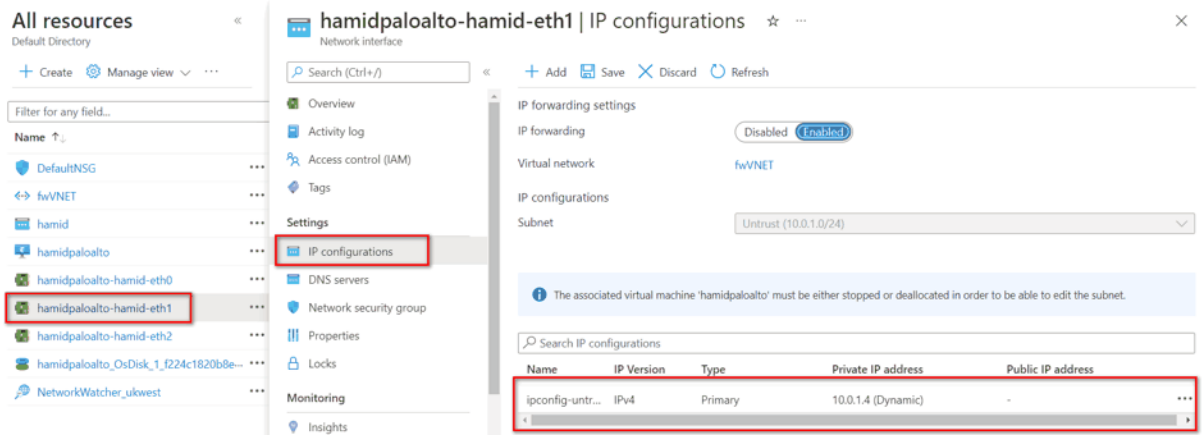


Figure 4.66: Select Interface eth1

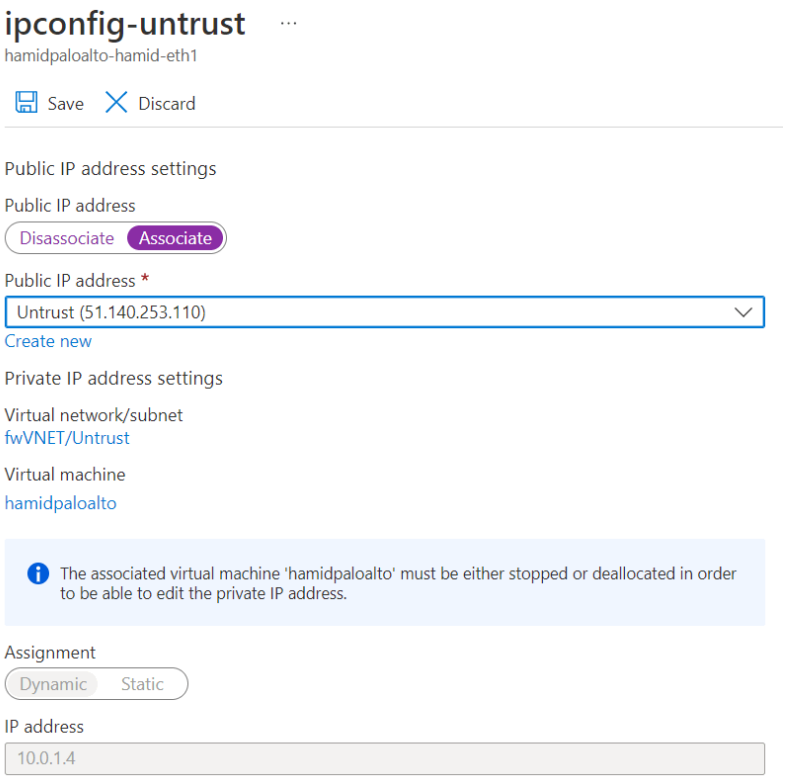


Figure 4.67: Assign public IP address to Eth1

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.

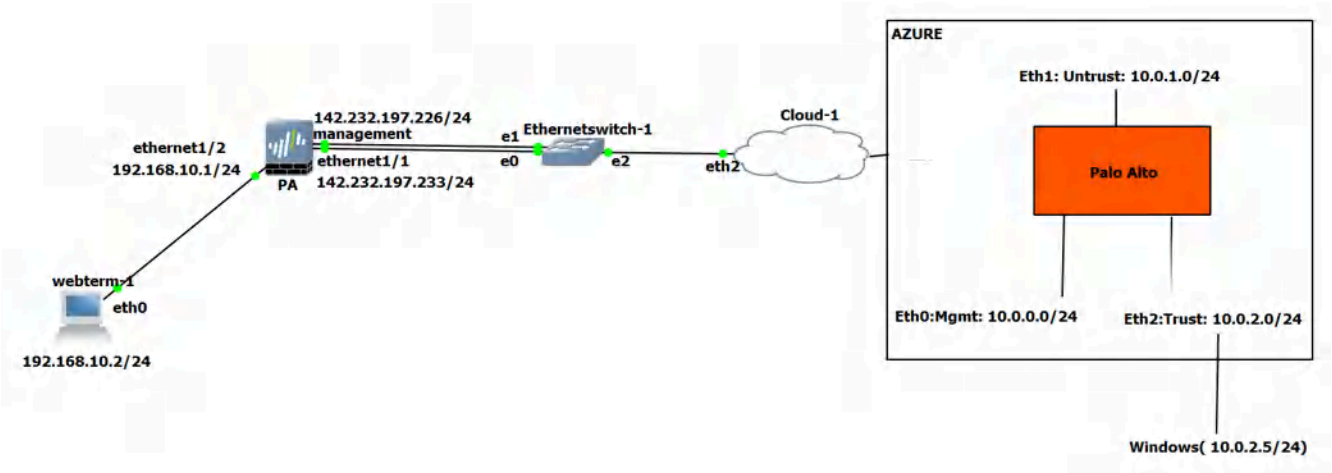


Figure 4.68: Main scenario

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.

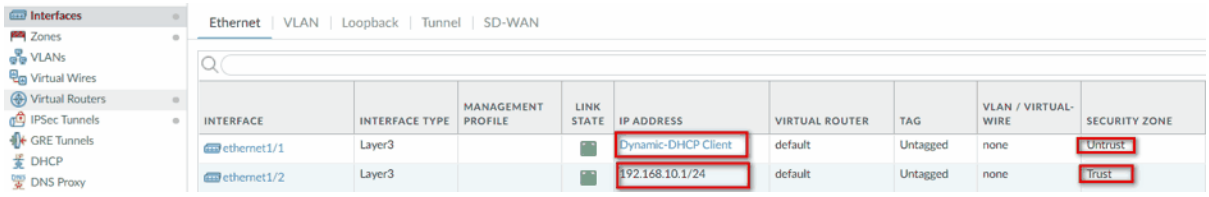


Figure 4.69: Firewall Interfaces

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

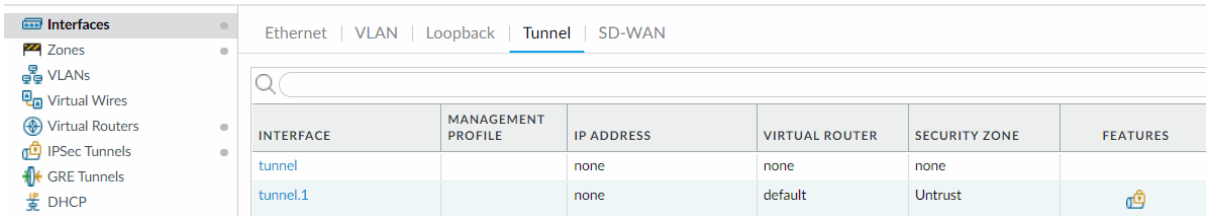


Figure 4.70: Create a tunnel

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.

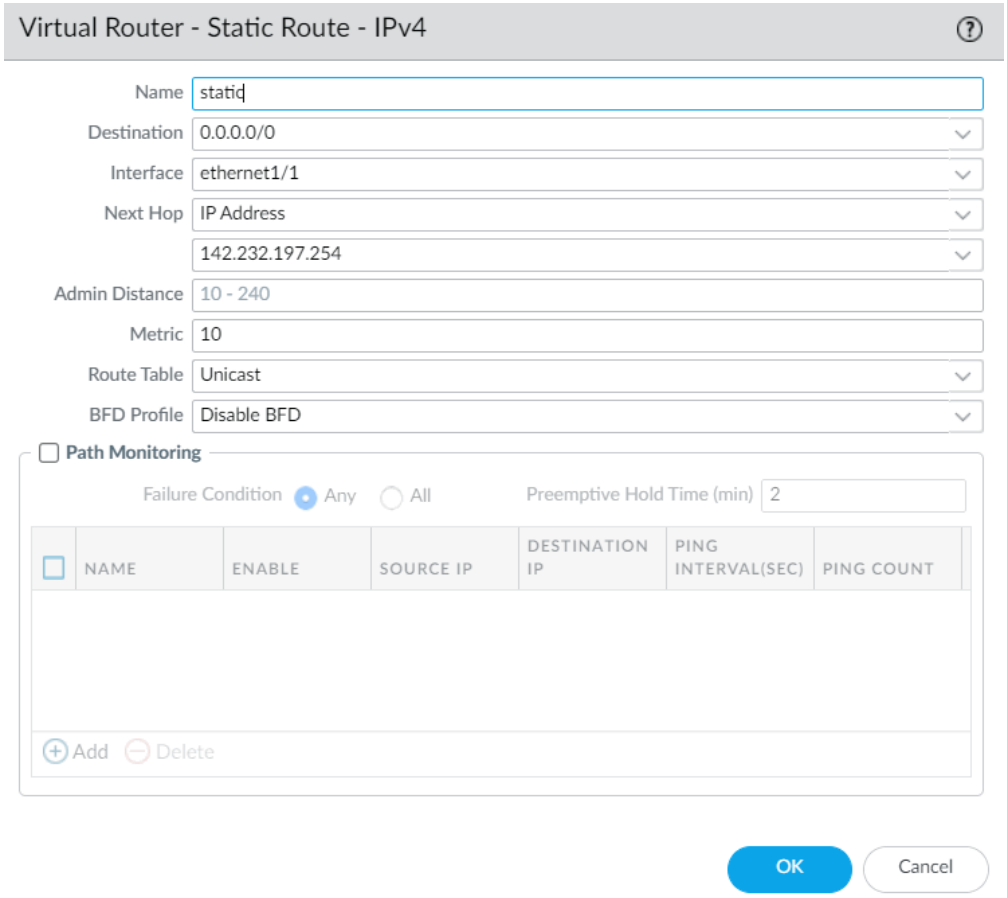


Figure 4.71: Create a static route to default gateway

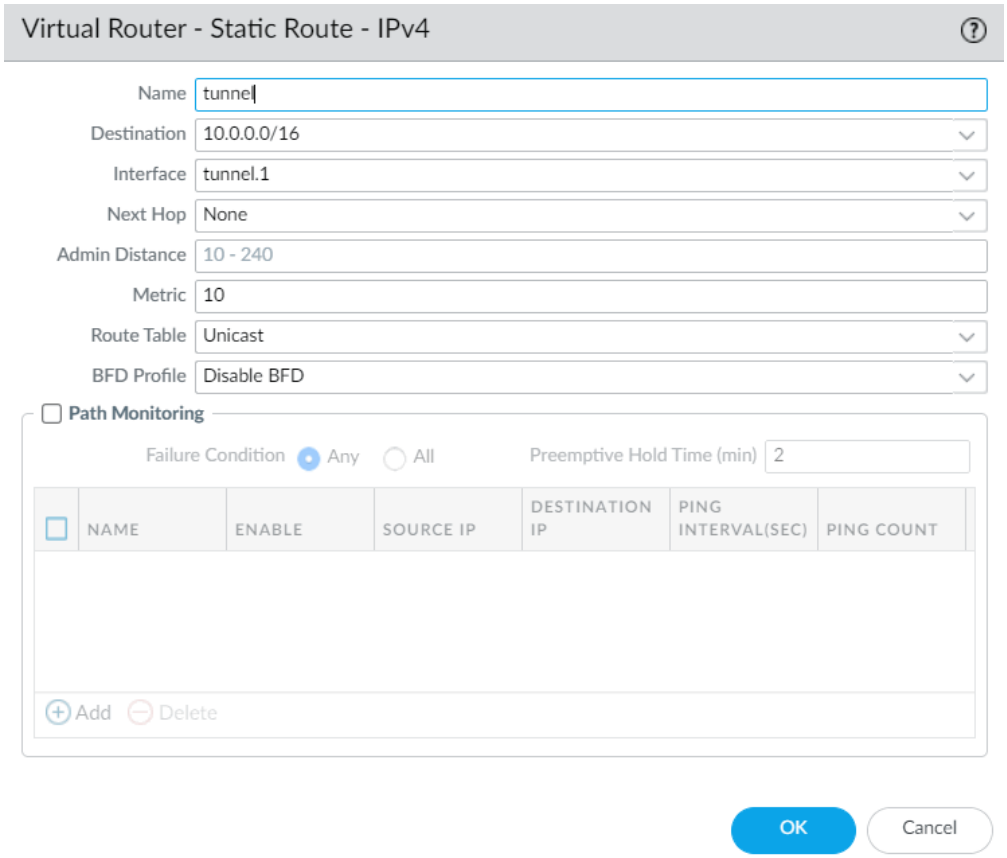


Figure 4.72: Create a static route to Azure

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.

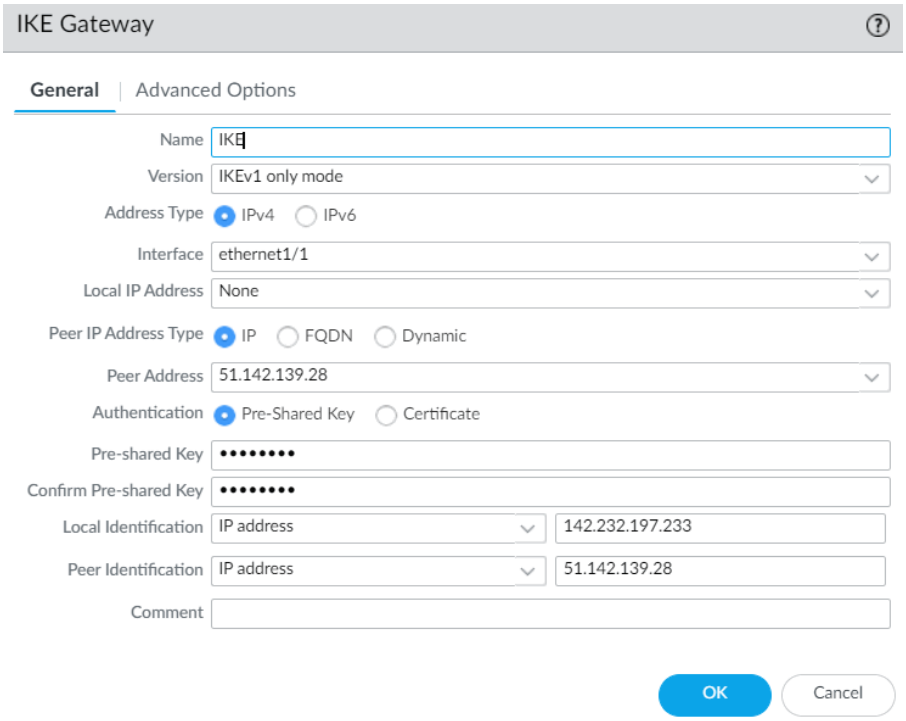


Figure 4.73: Create an IKE Gateway

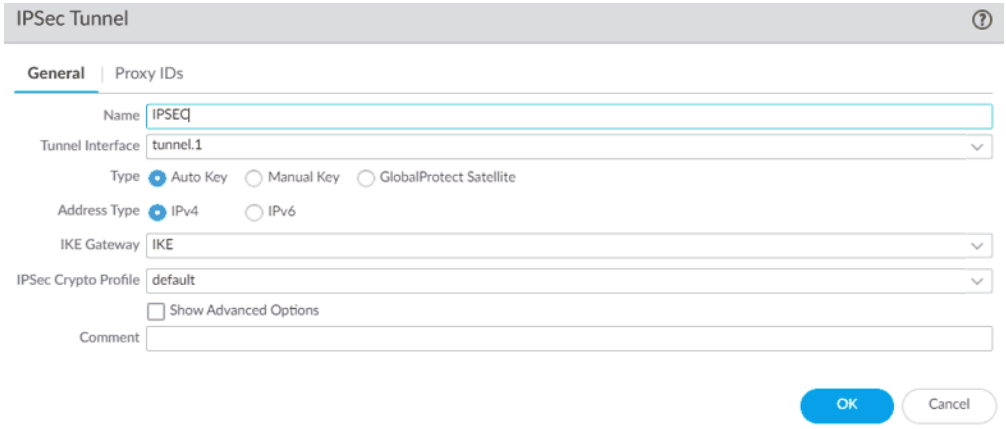


Figure 4.74: Create an IPsec Tunnel

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

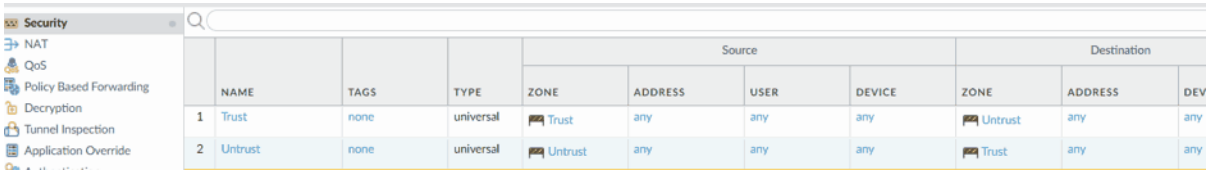


Figure 4.75: Create two security policies

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.

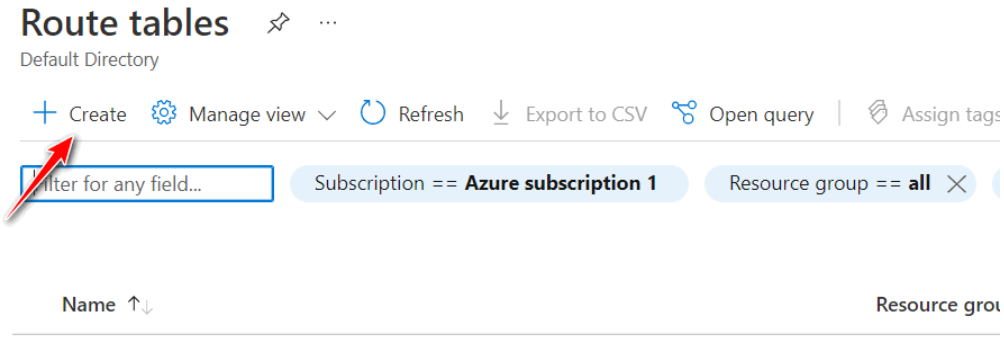


Figure 4.76: Create a route table

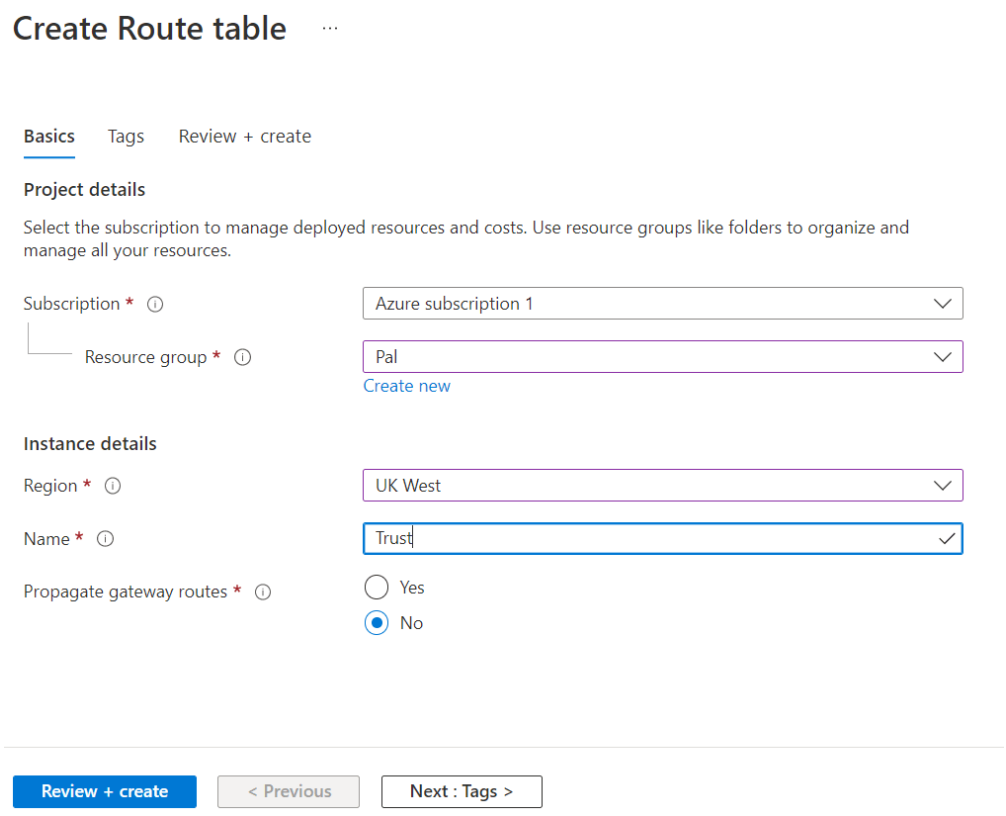


Figure 4.77: Create a route table

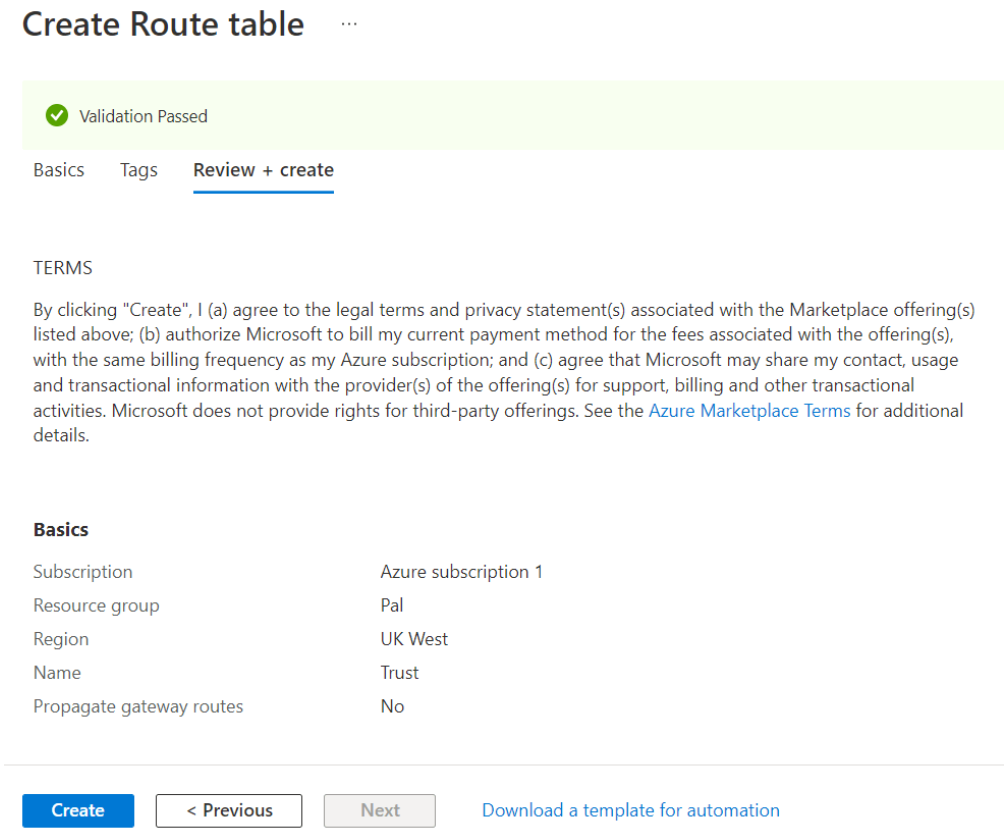


Figure 4.78: Create a route table (verify and create)

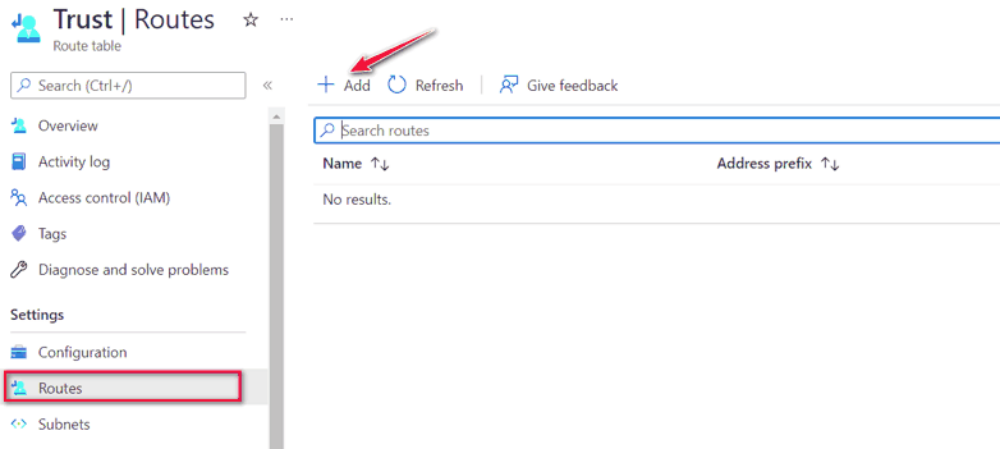


Figure 4.79: Add a Route

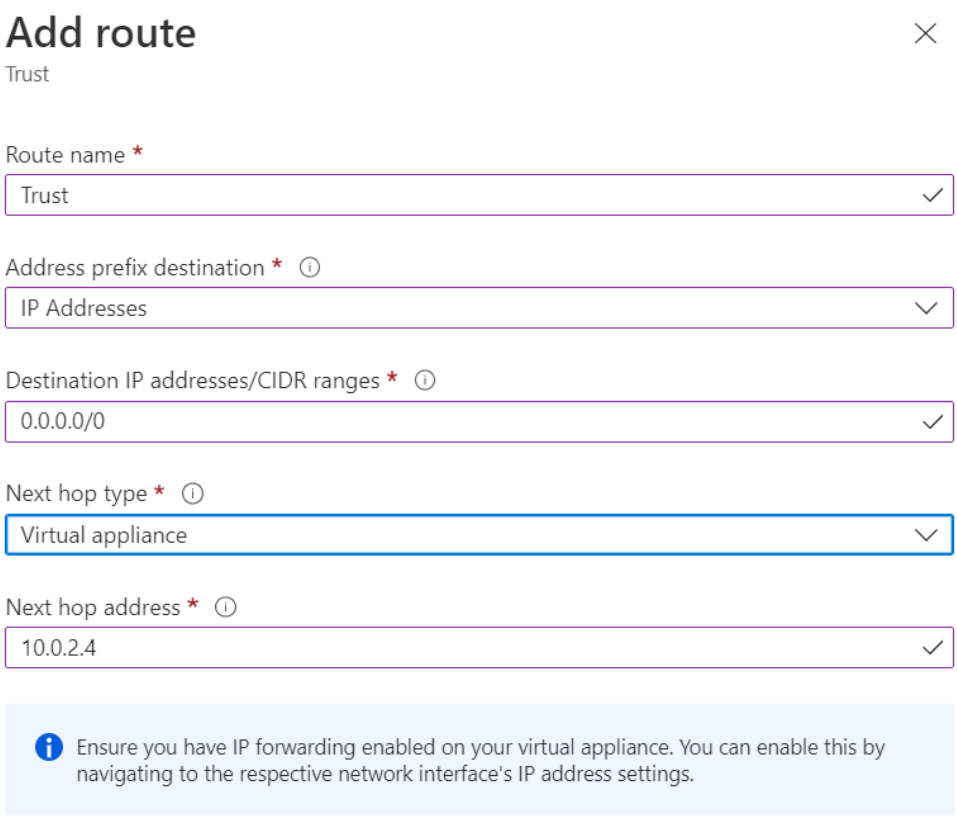


Figure 4.80: Add a default route pointing to 10.0.2.4 (Trust Interface)

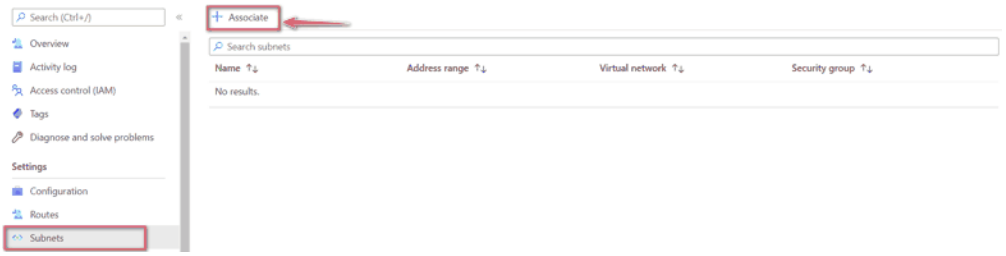


Figure 4.81: Associate Trust route to Trust Subnet

Figure 4.82: Associate fwVNET to Trust Subnet

3. Set static routes as figures 4.83 and 4.84.

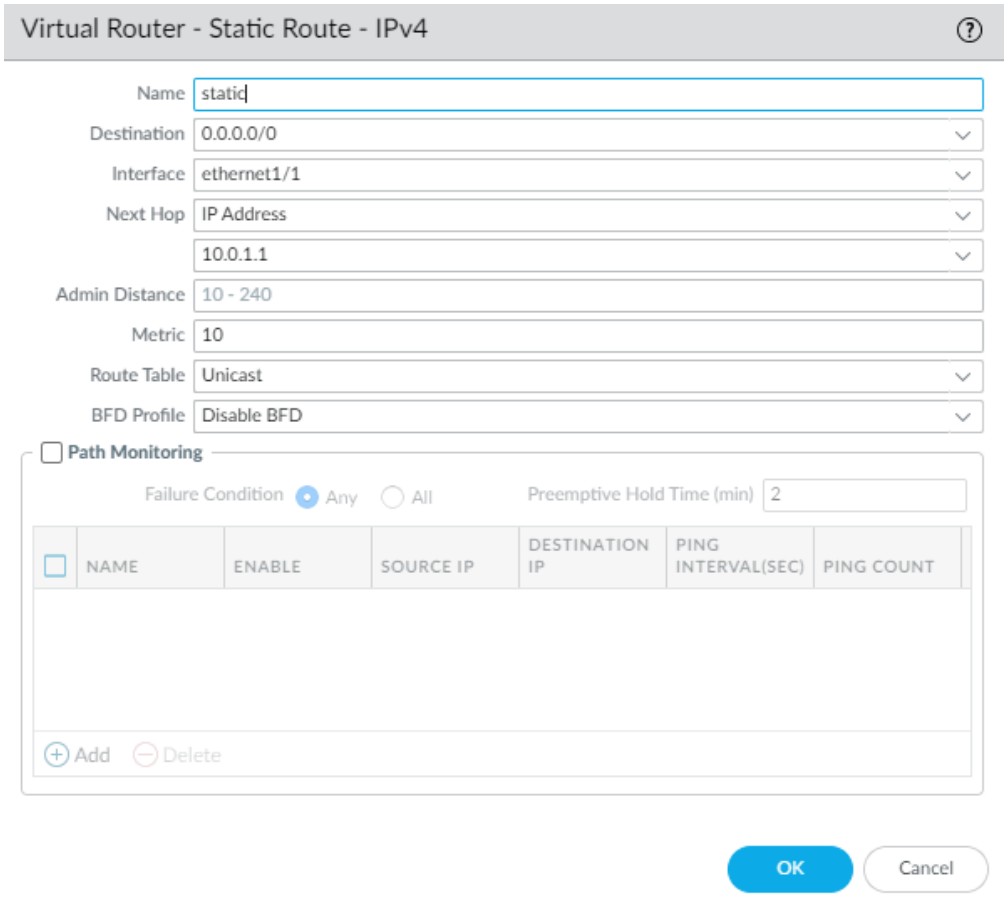


Figure 4.83: Static route pointing to default gateway

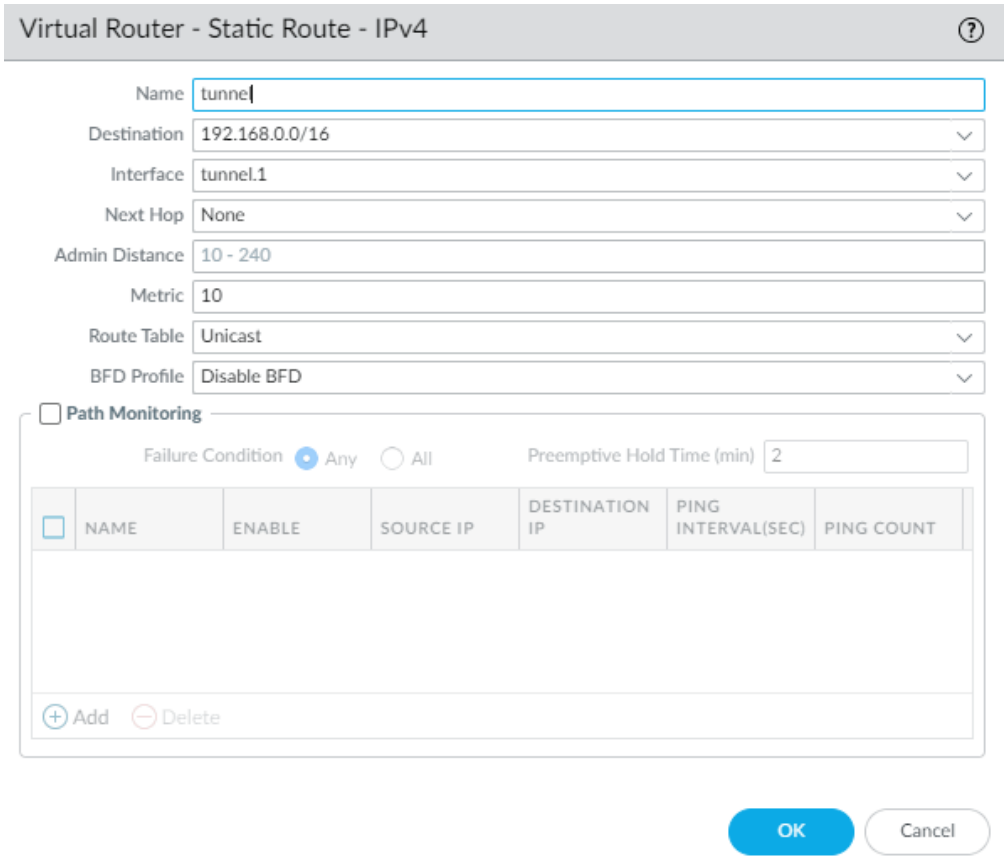


Figure 4.84: Static route pointing to tunnel

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.

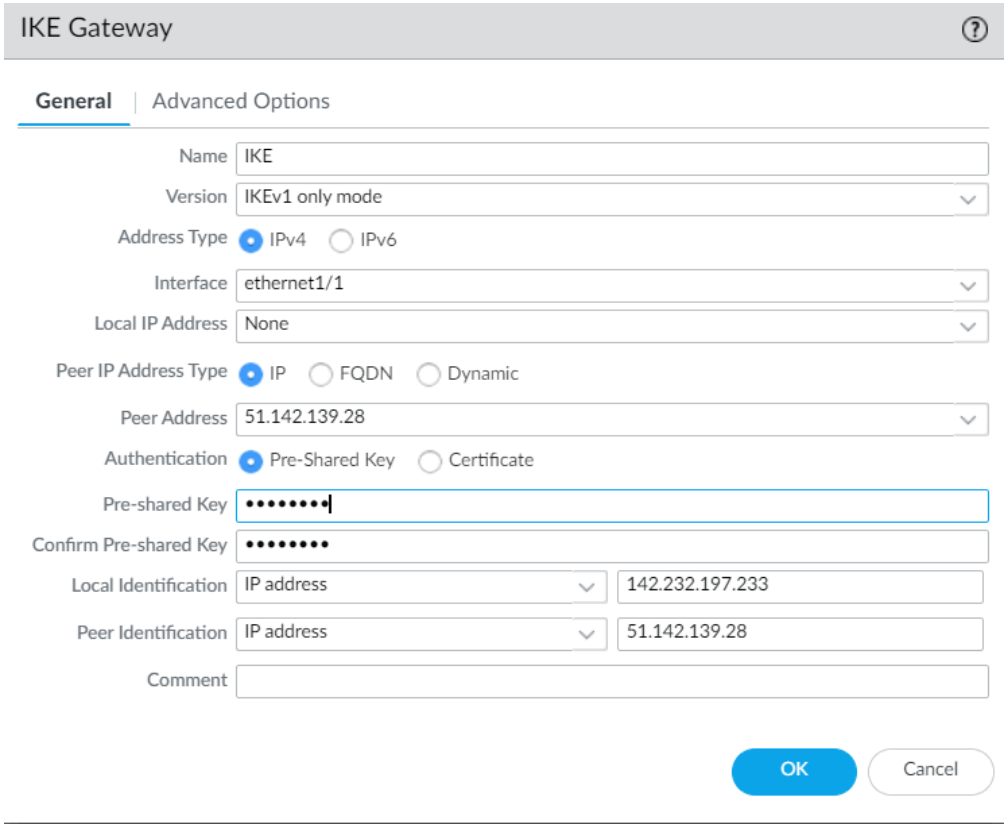


Figure 4.85: Create an IKE Gateway

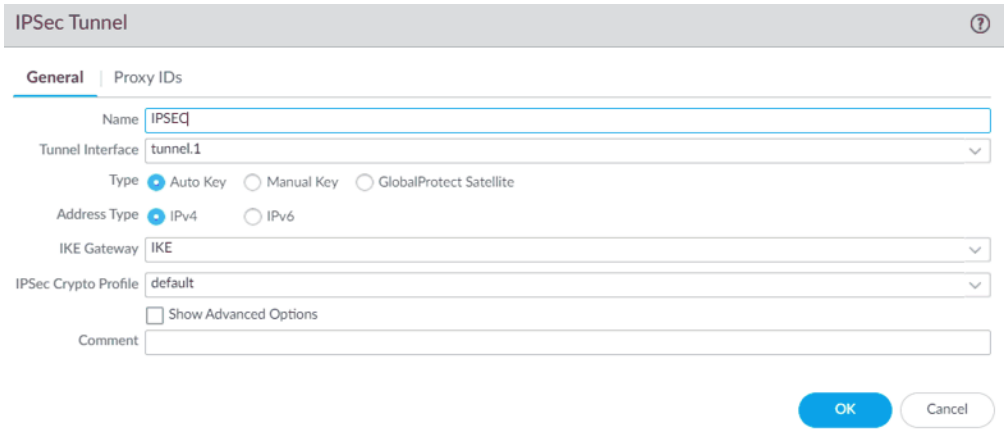


Figure 4.86: Create an IPsec Tunnel

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

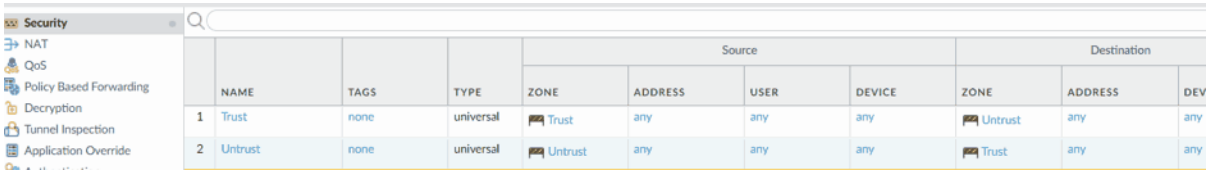


Figure 4.87: Create two security policies

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

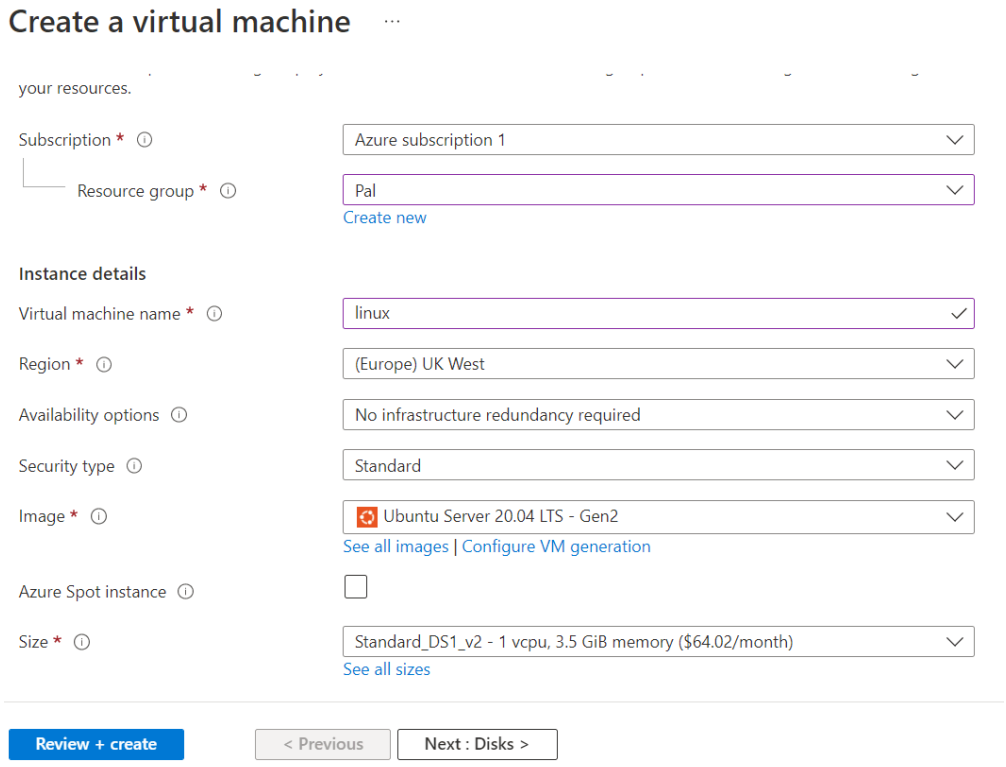


Figure 4.88: Create a VM

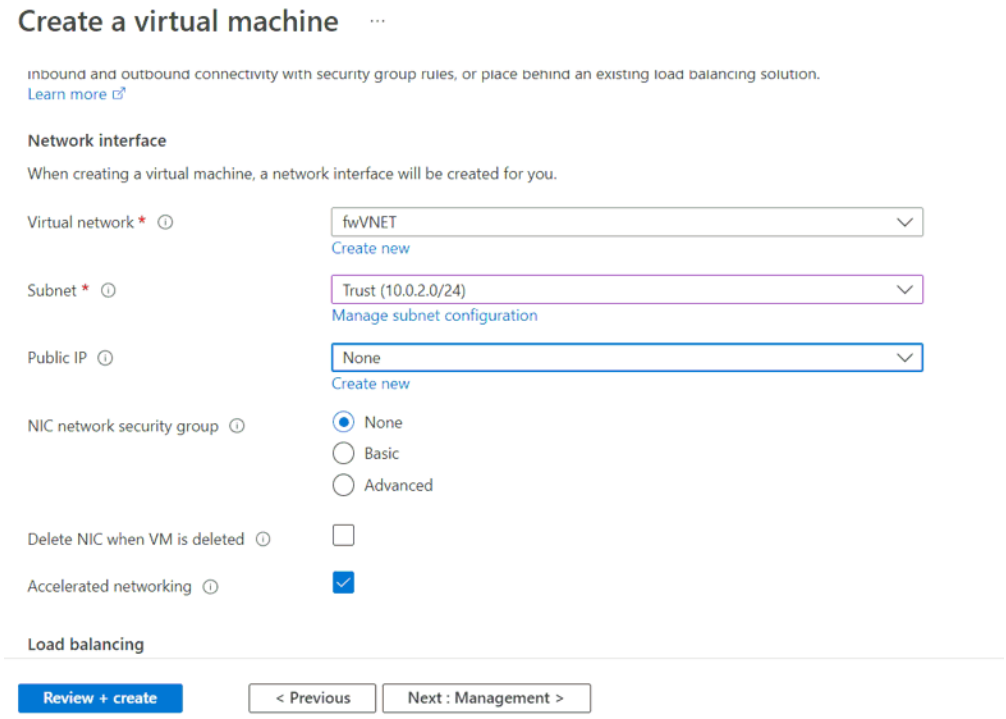


Figure 4.89: Assign Trust subnet with no public IP

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

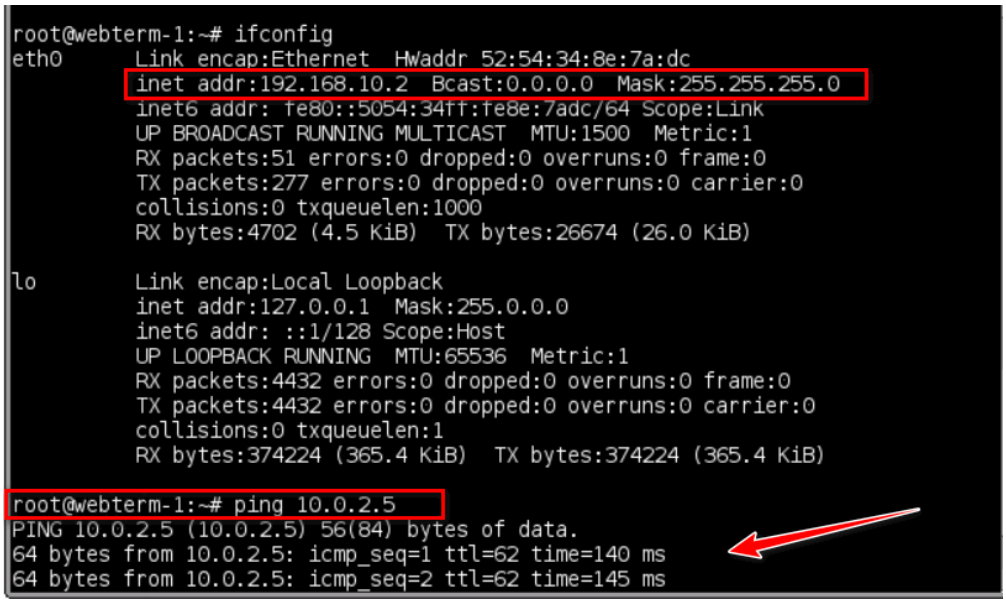


Figure 4.90: Ping from WebTerm to Azure

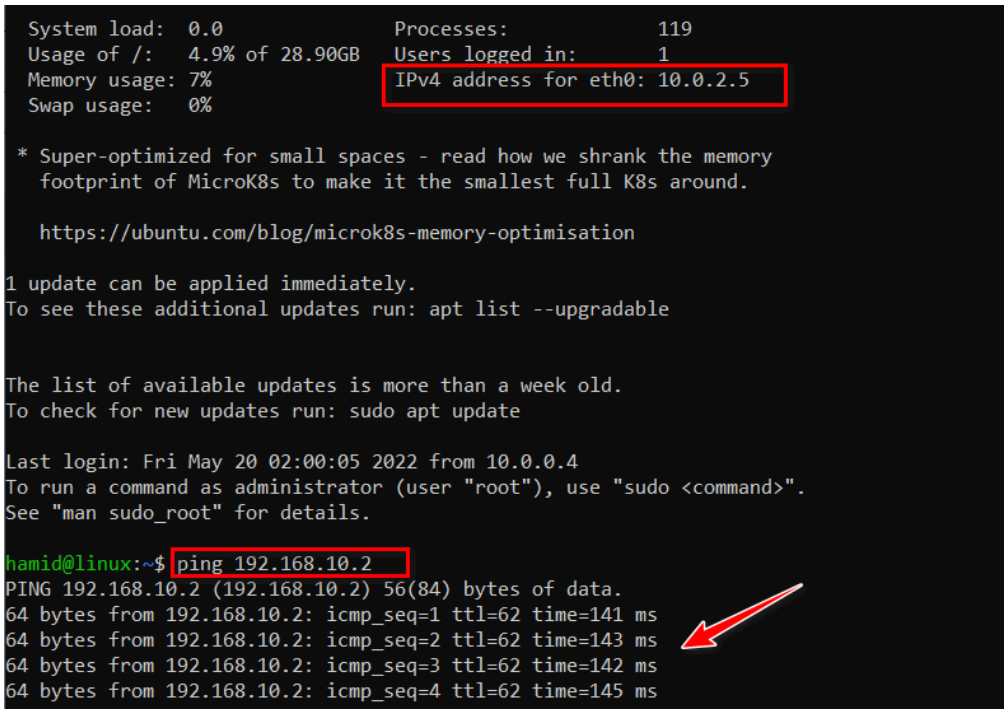


Figure 4.91: Ping from Azure to WebTerm

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

Figure 4.92: Tunnel Status

Capstone Project

Capstone Project

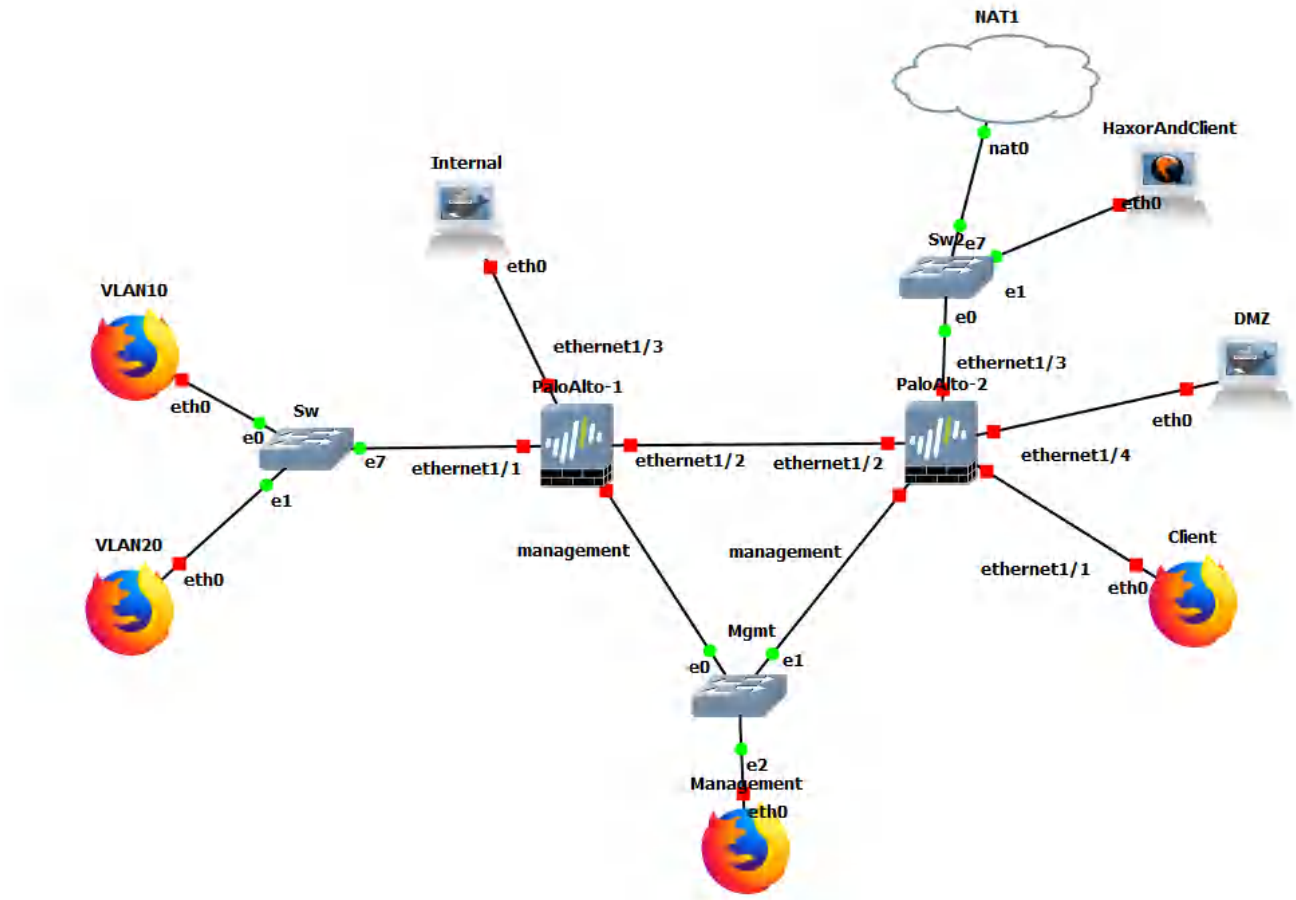


Figure C.1: Capstone Topology

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".

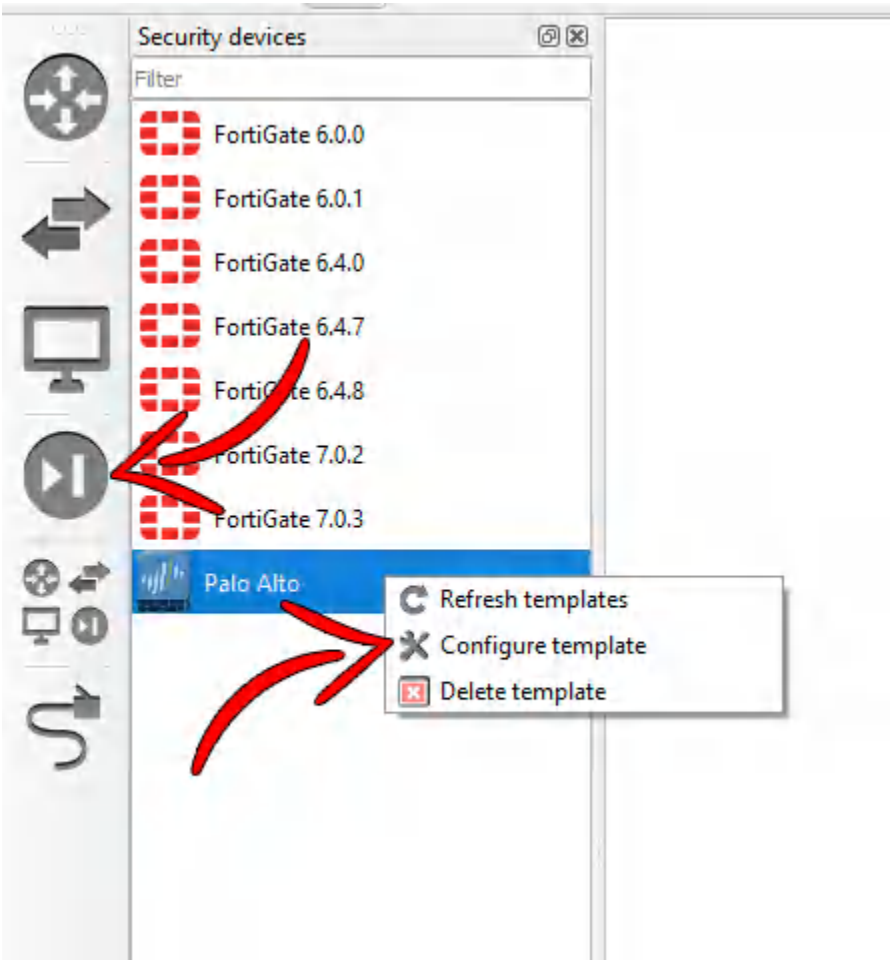


Figure A.1: Configure template

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

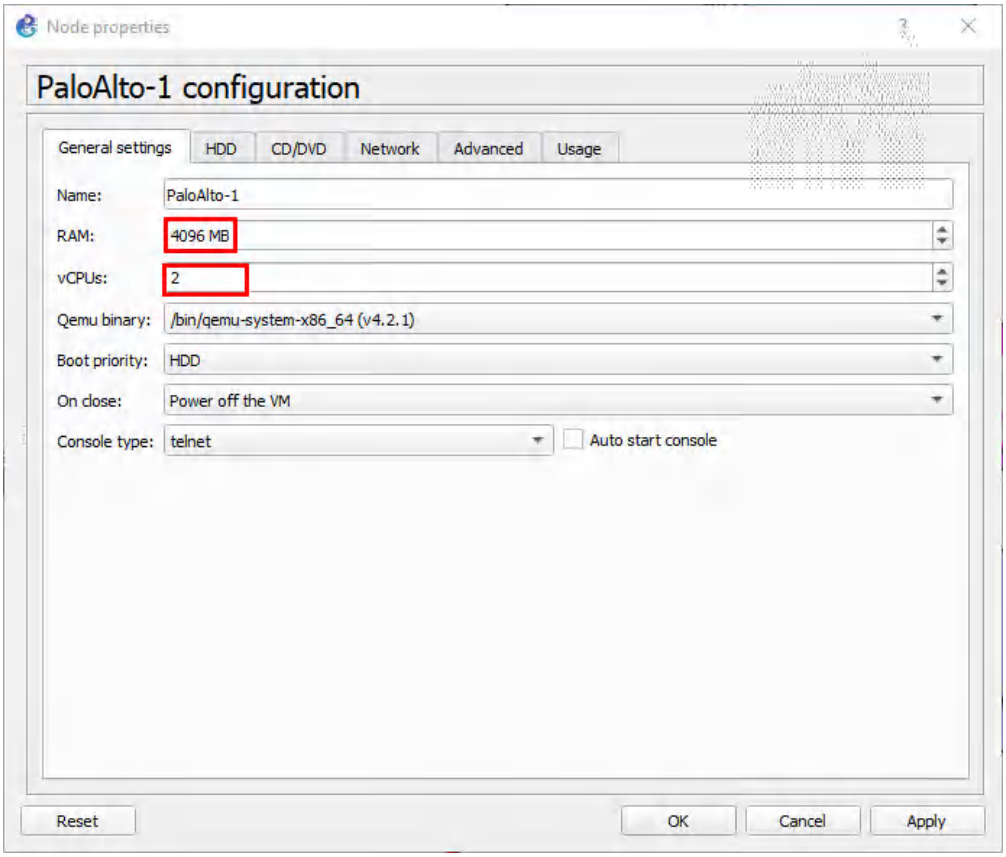


Figure A.2: Configure RAM and vCPUs

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

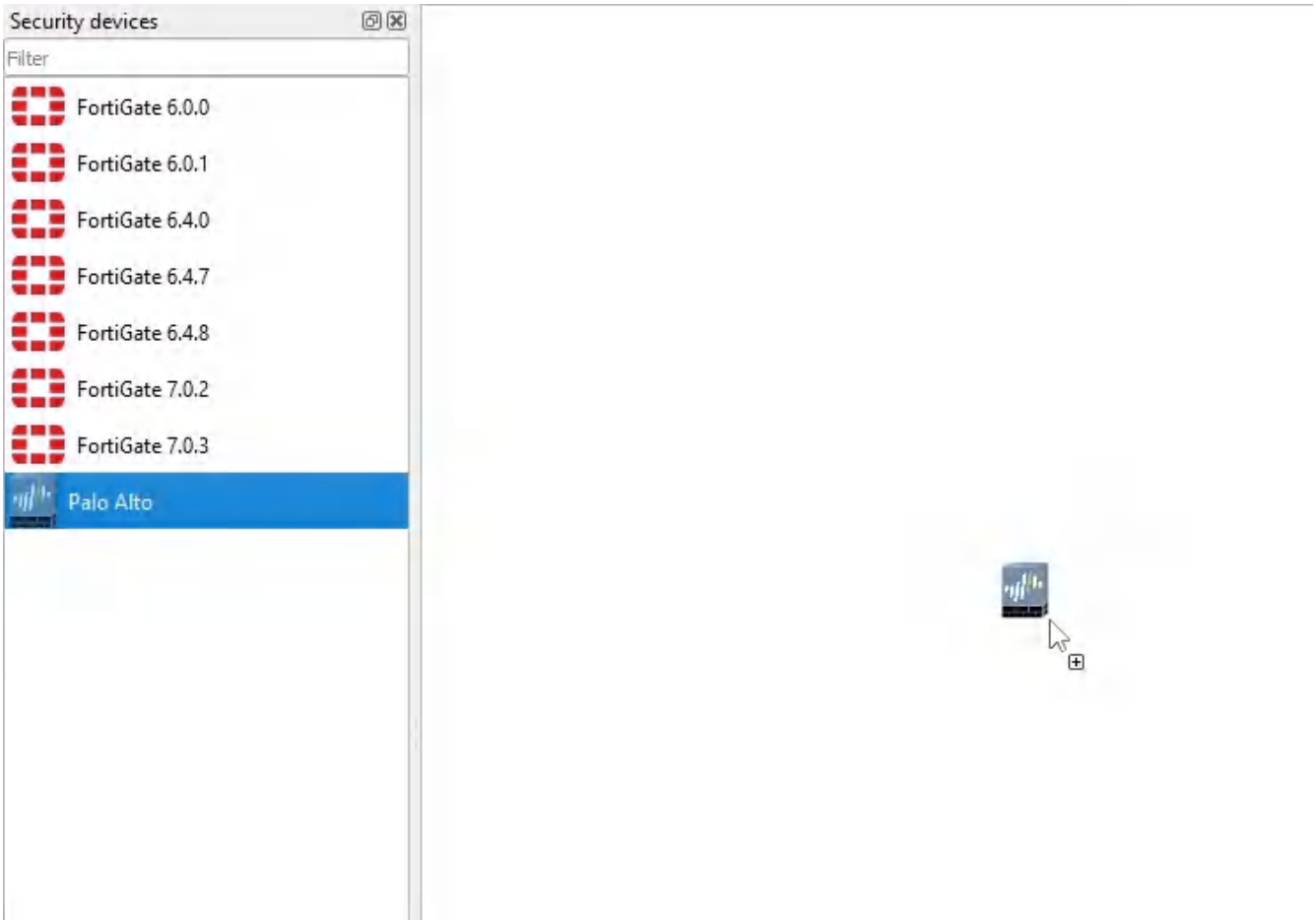


Figure A.3: Dragging the Palo Alto

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

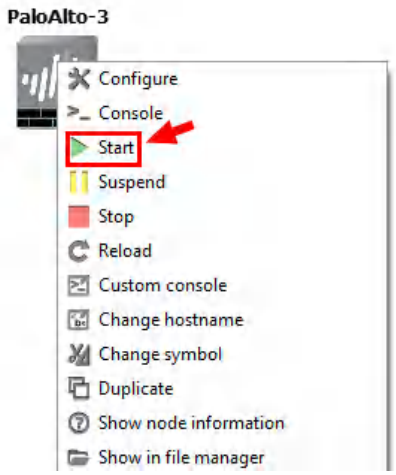


Figure A.4: Starting the Palo Alto

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.

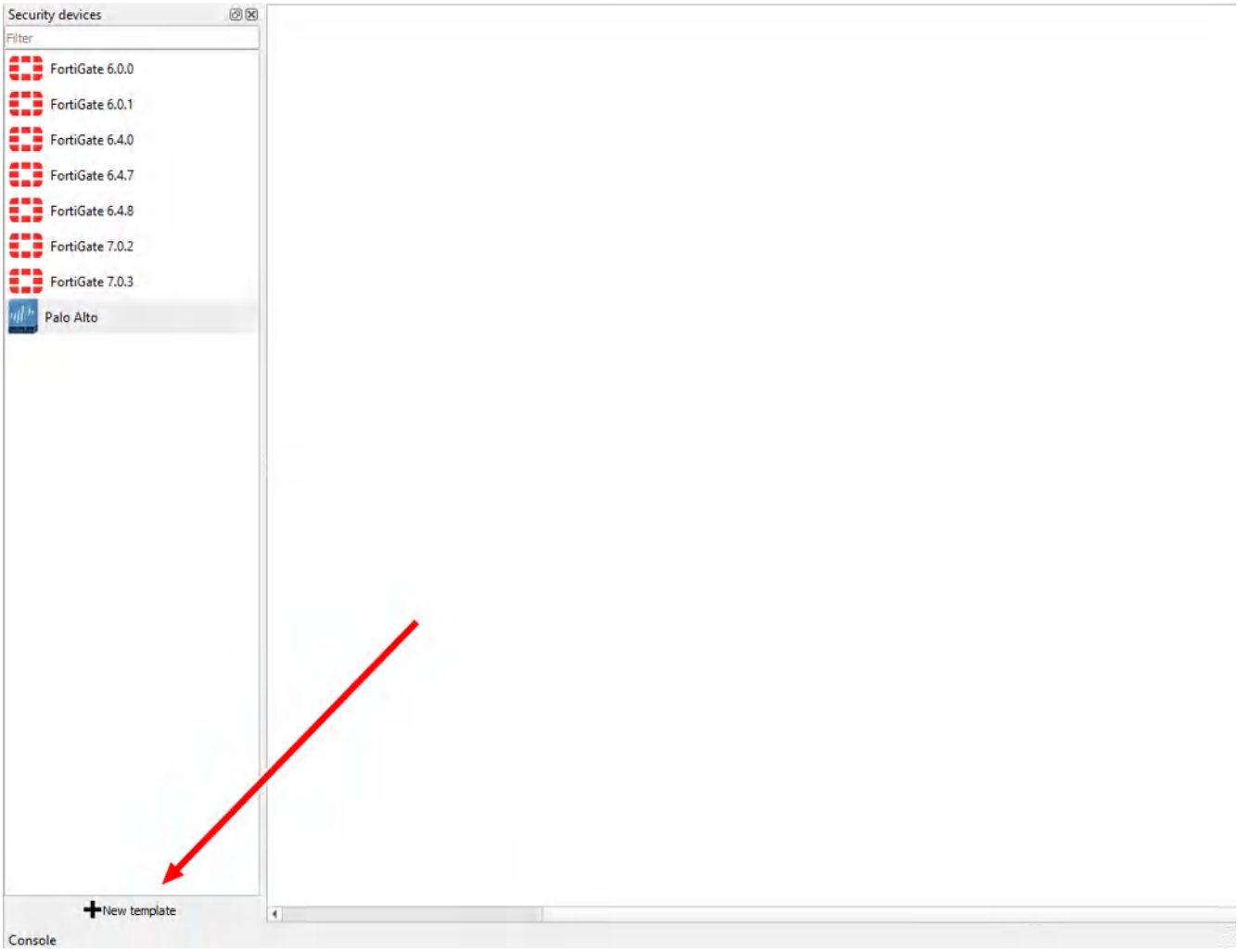


Figure A.5: Add a new template

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

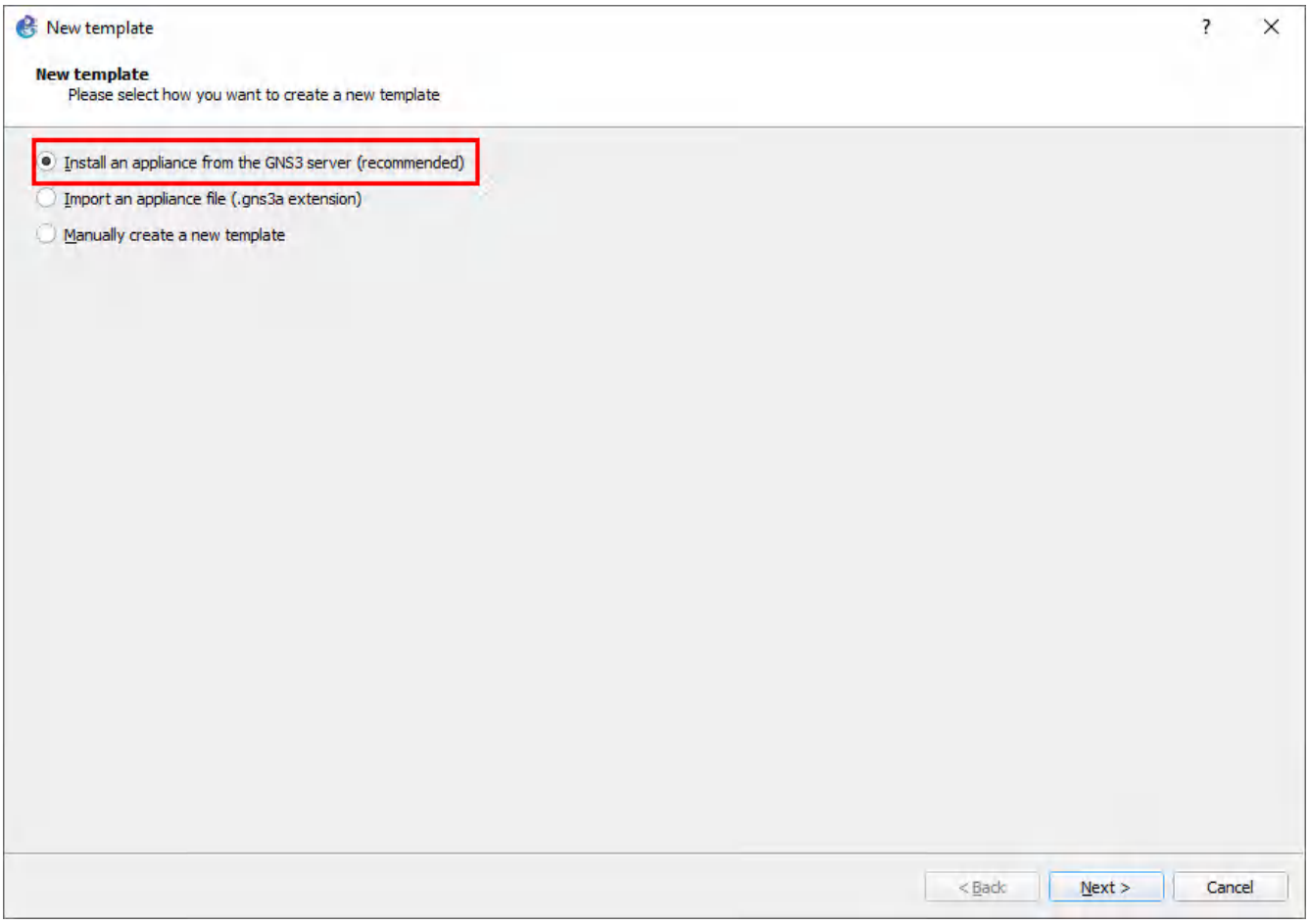


Figure A.6: Select “Install an appliance from the GNS3 server”

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

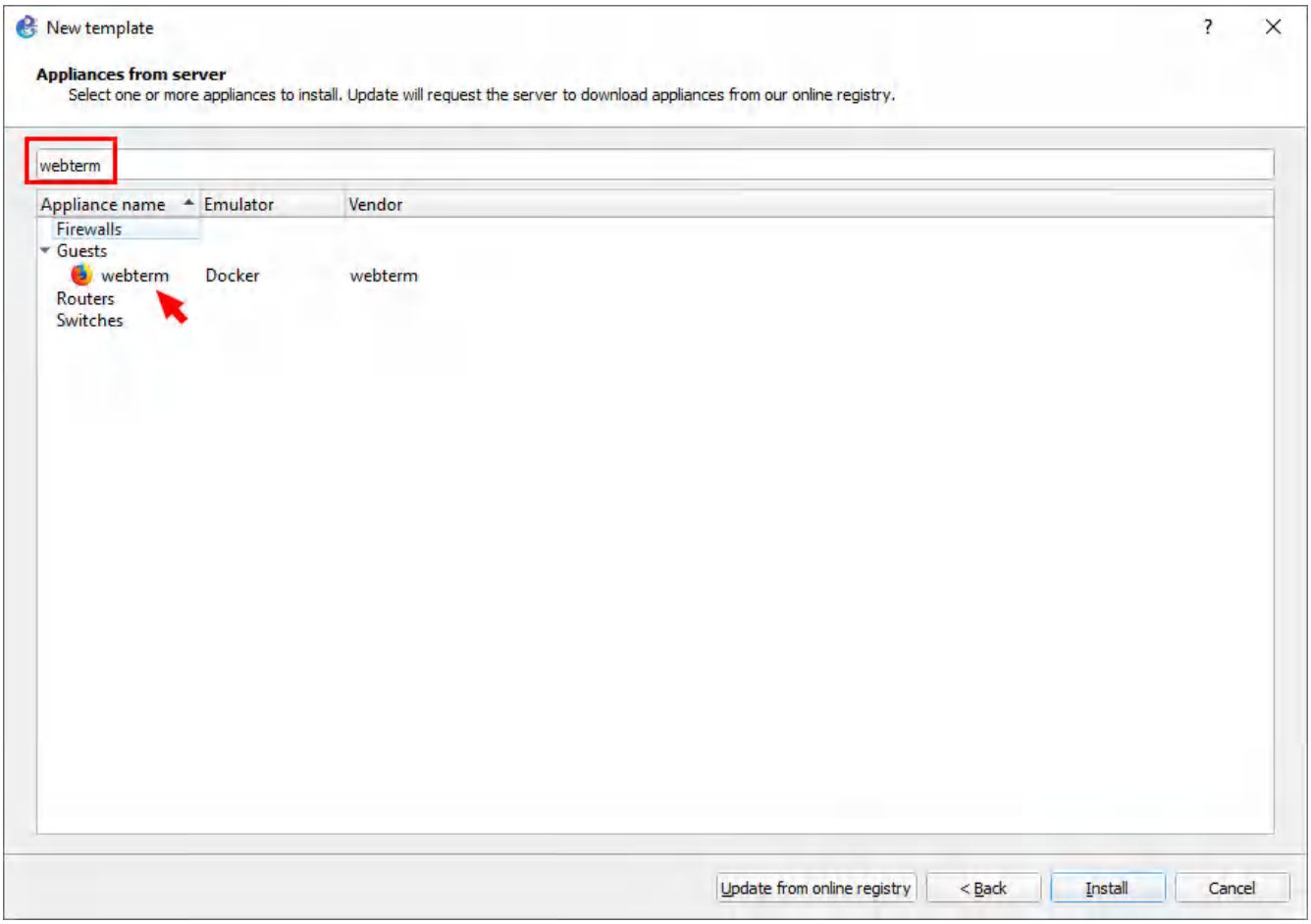


Figure A.7: Search for “webterm”

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

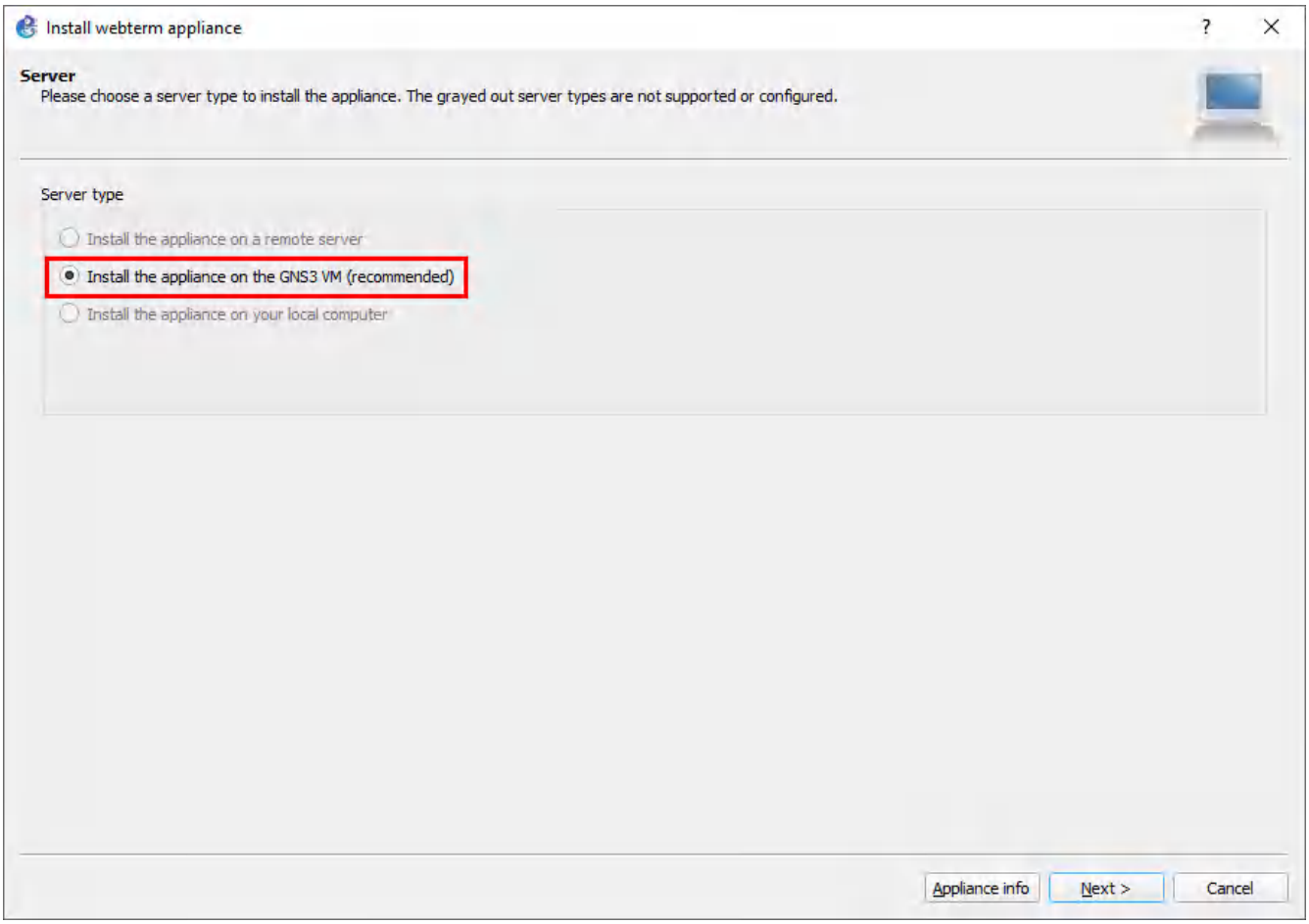


Figure A.8: Select “Install the appliance on the GNS3 VM”

On the next screen, click Finish.

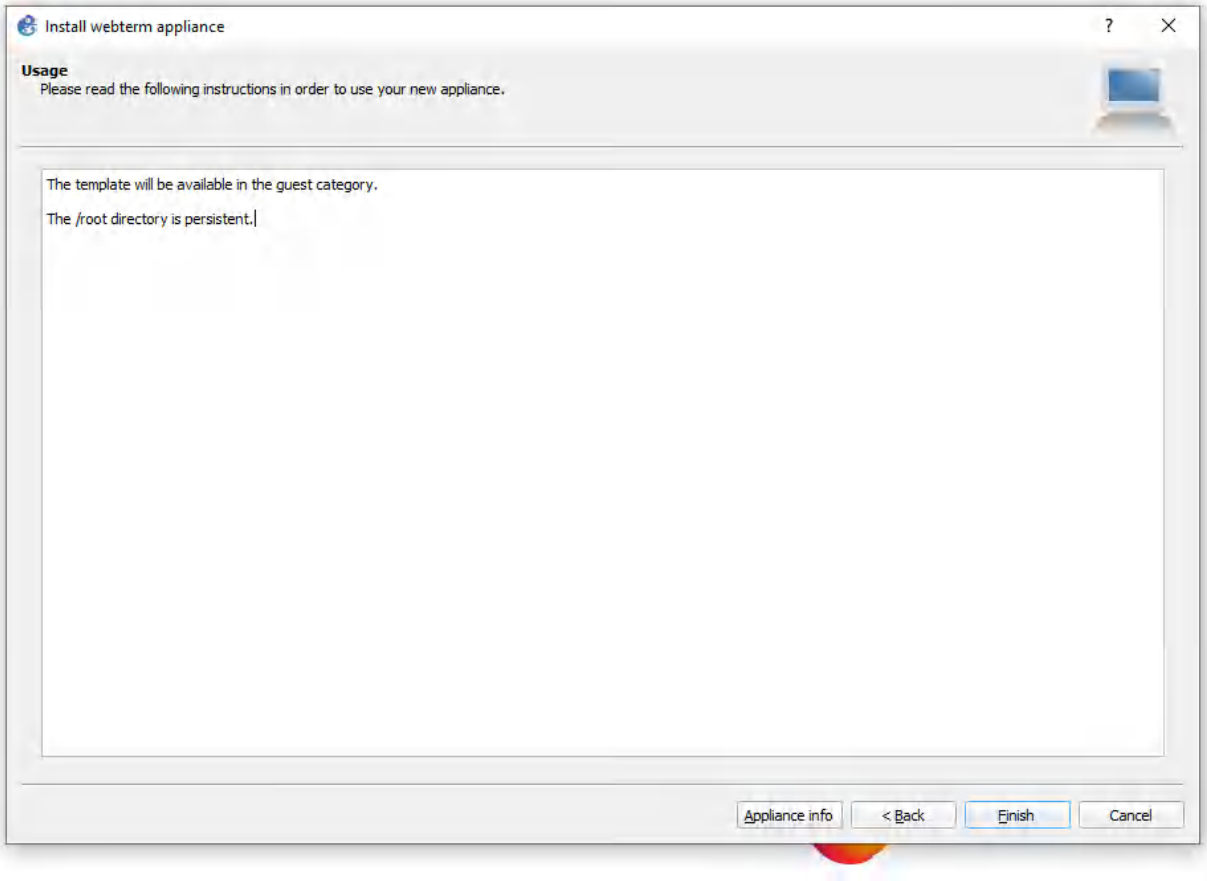


Figure A.9: Final step of Installation of webterm

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”.

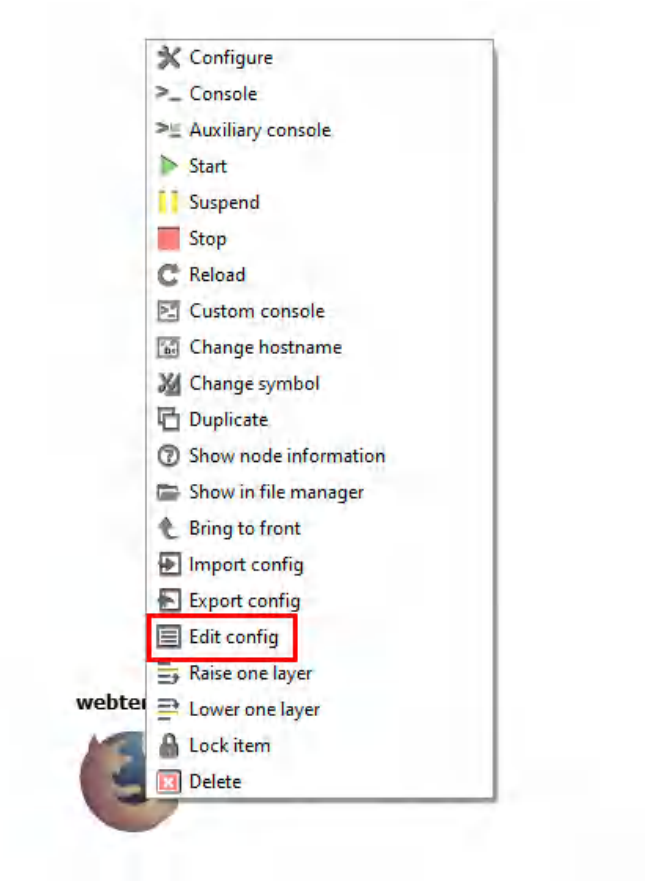


Figure A.10: Edit config

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:

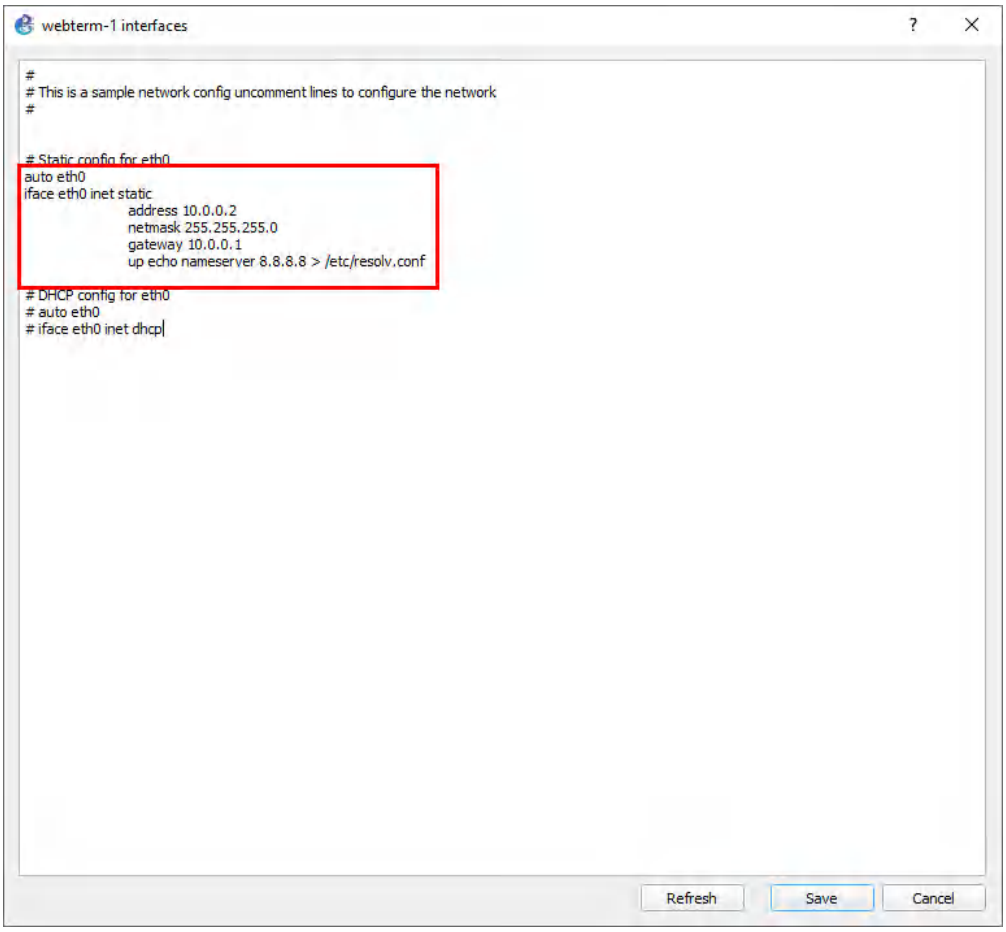


Figure A.11: Configure the static IP address

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.

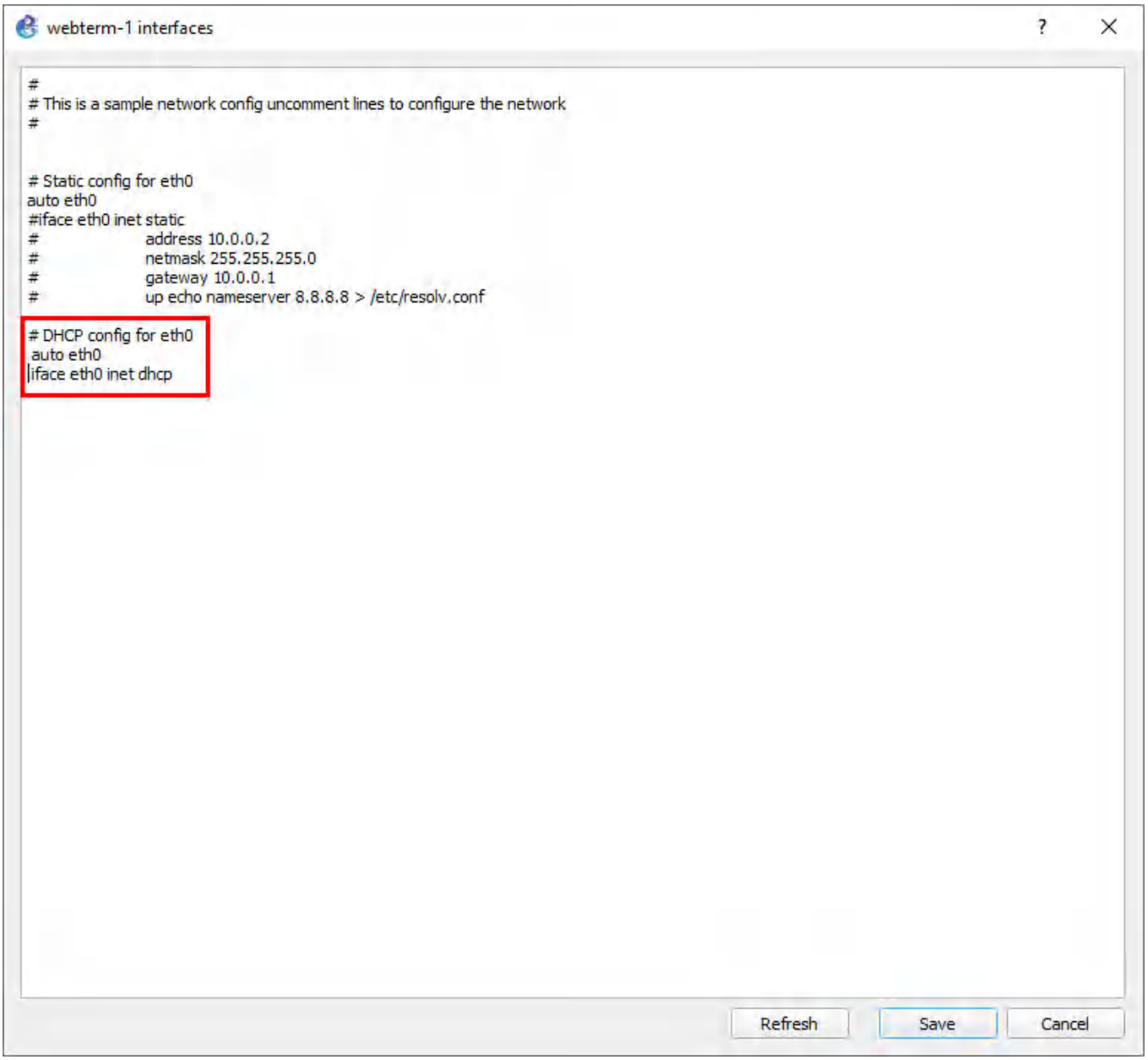


Figure A.12: Configure the DHCP IP address

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.

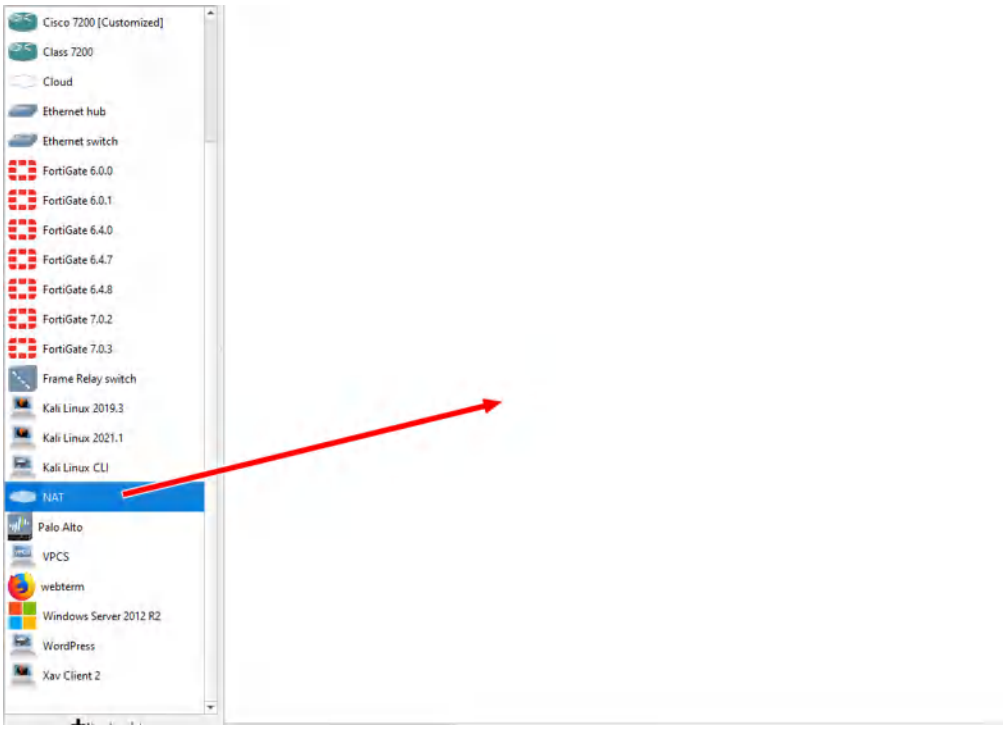


Figure A.14: Using NAT

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

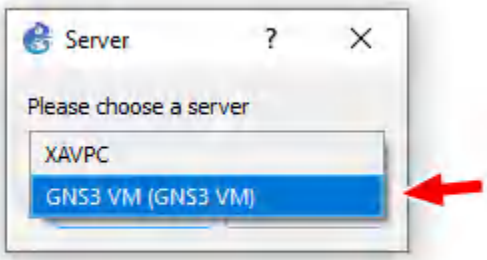


Figure A.15: Select GNS3 VM

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.

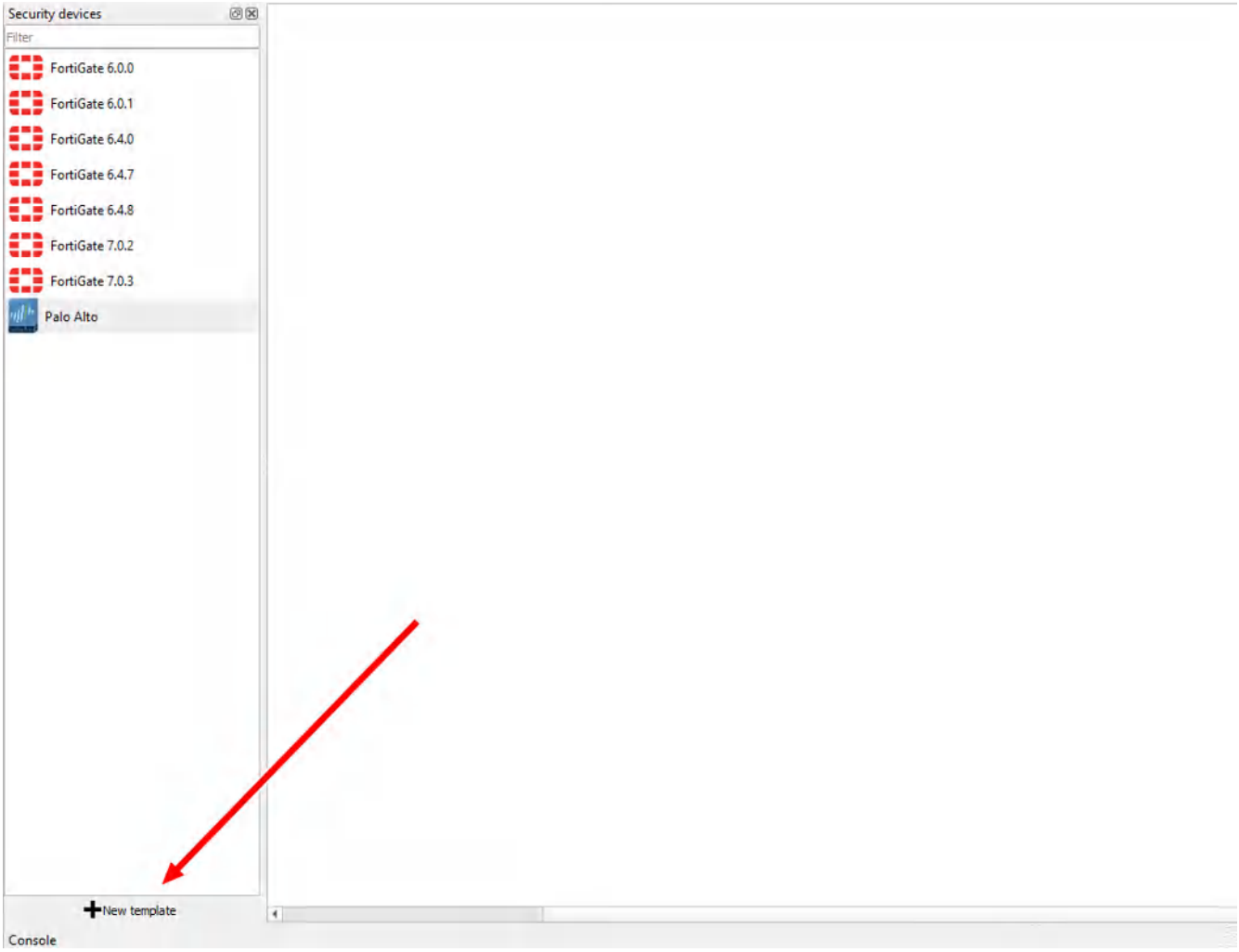


Figure A.16: Create a new template

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

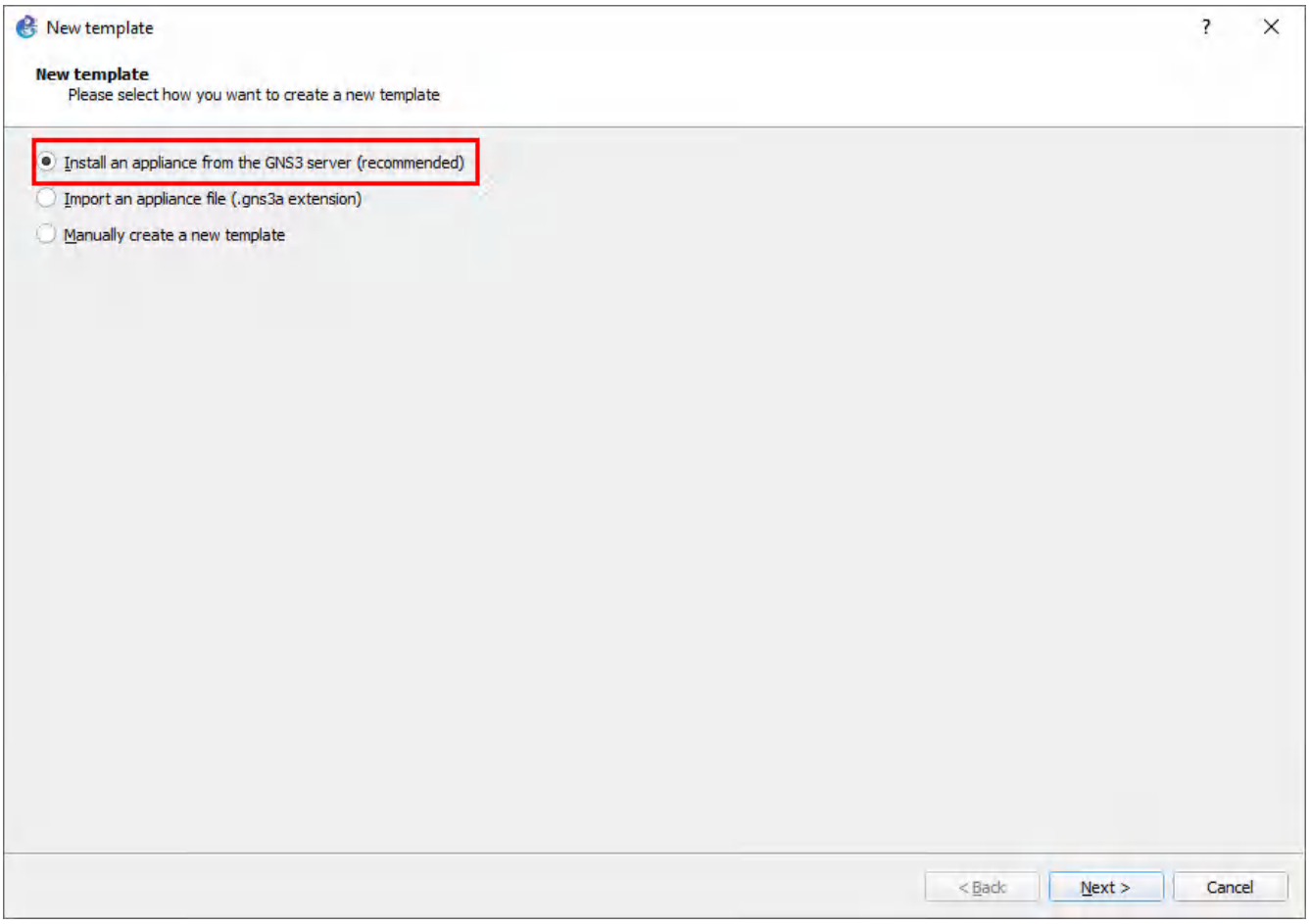


Figure A.17: Select “Install an appliance from the GNS3 server”

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

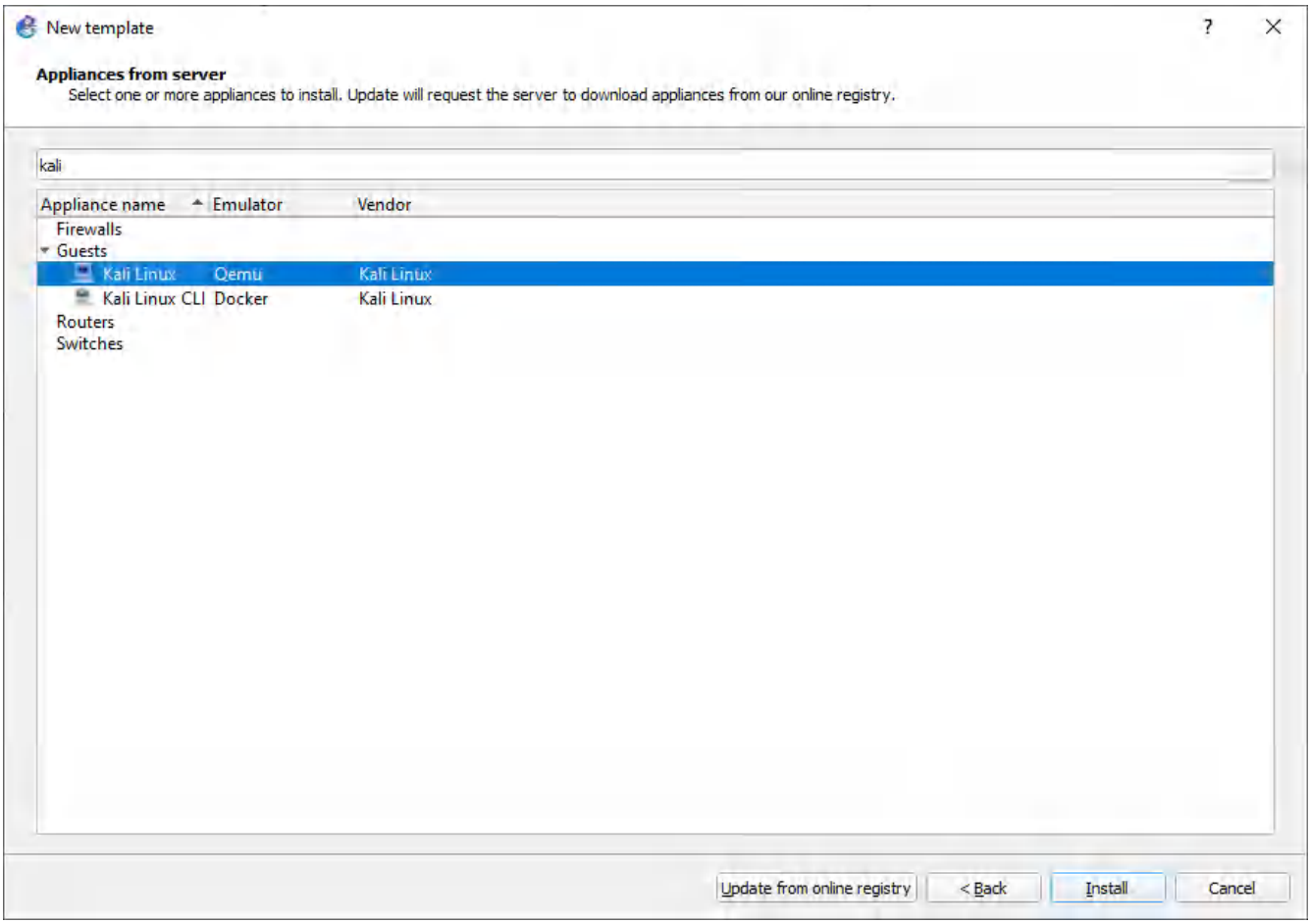


Figure A.18: Search for “kali”

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

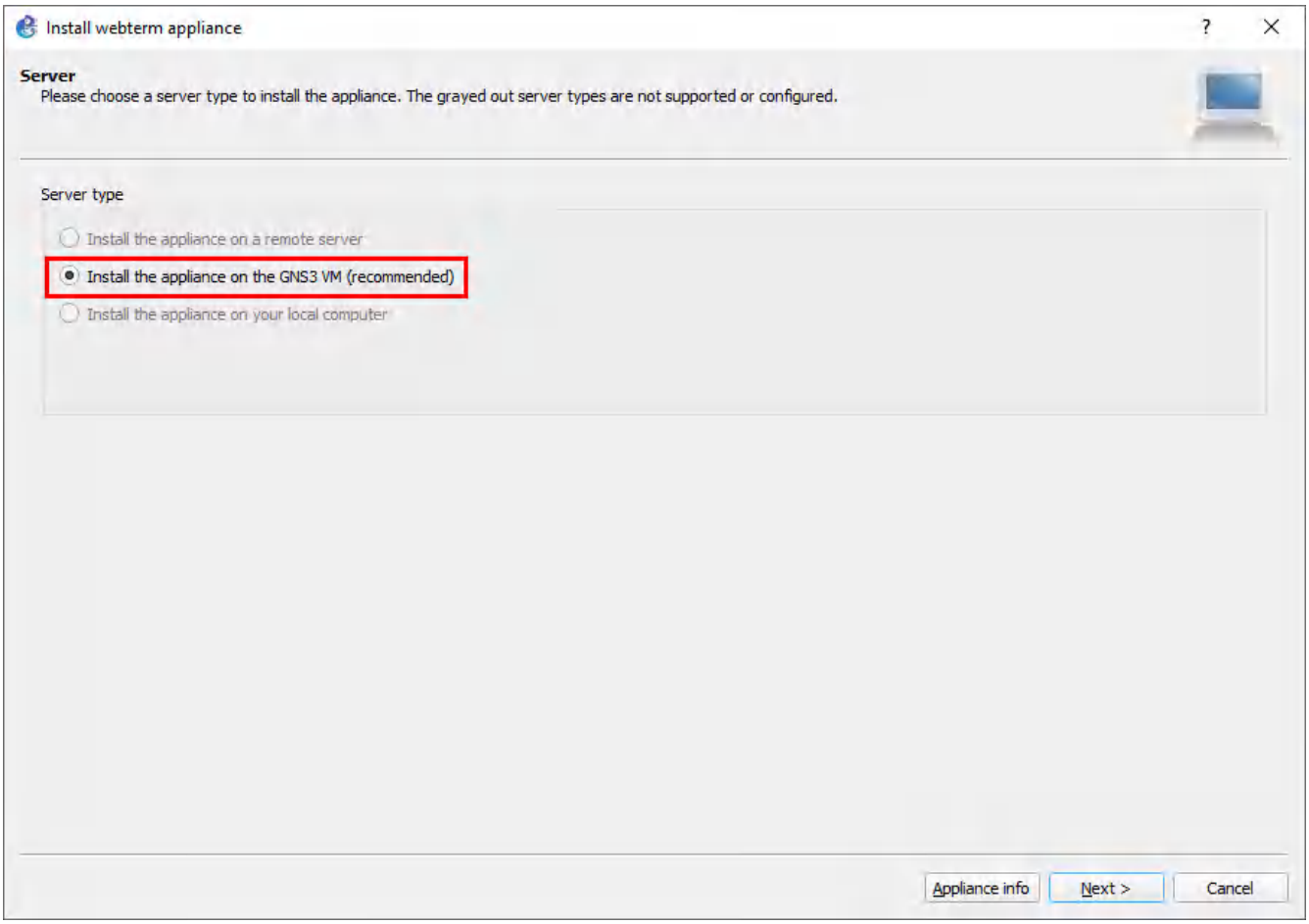


Figure A.19: Select “Install the appliance on the GNS3 VM”

Next again.

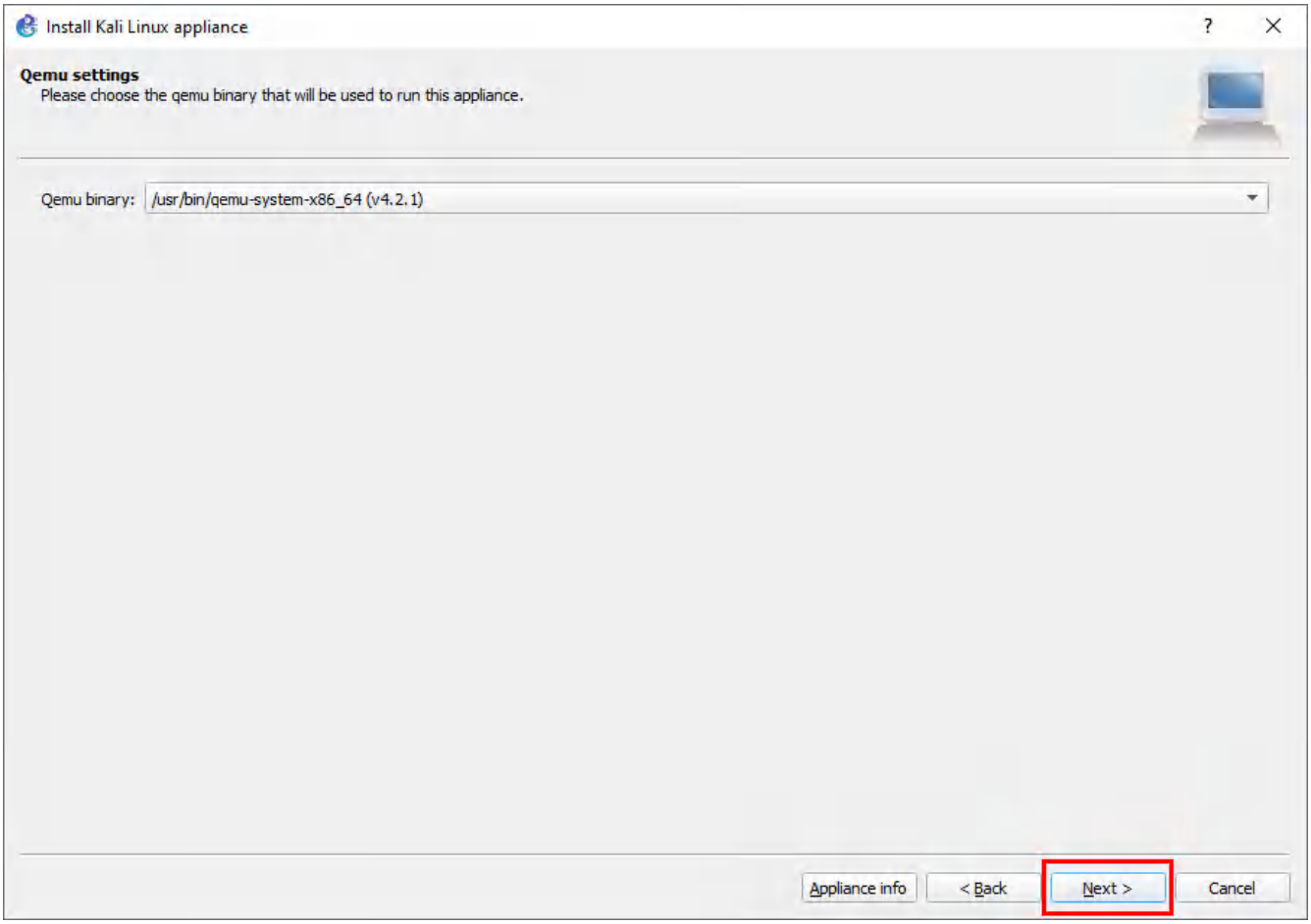
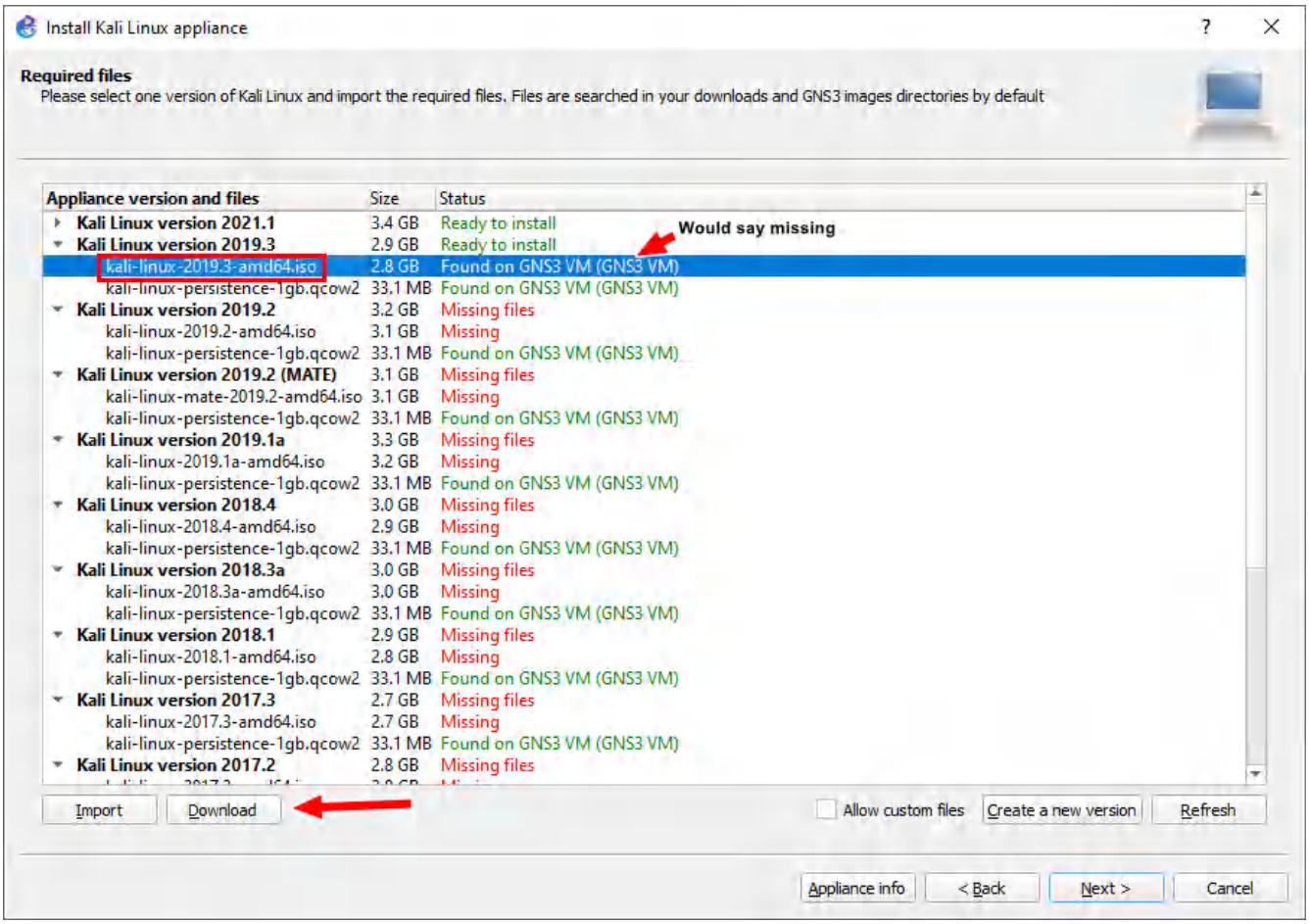


Figure A.20: Select Qemu binary

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



Appliance version and files	Size	Status
Kali Linux version 2021.1	3.4 GB	Ready to install
Kali Linux version 2019.3	2.9 GB	Ready to install
kali-linux-2019.3-amd64.iso	2.8 GB	Found on GNS3 VM (GNS3 VM)
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)
Kali Linux version 2019.2	3.2 GB	Missing files
kali-linux-2019.2-amd64.iso	3.1 GB	Missing
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)
Kali Linux version 2019.2 (MATE)	3.1 GB	Missing files
kali-linux-mate-2019.2-amd64.iso	3.1 GB	Missing
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)
Kali Linux version 2019.1a	3.3 GB	Missing files
kali-linux-2019.1a-amd64.iso	3.2 GB	Missing
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)
Kali Linux version 2018.4	3.0 GB	Missing files
kali-linux-2018.4-amd64.iso	2.9 GB	Missing
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)
Kali Linux version 2018.3a	3.0 GB	Missing files
kali-linux-2018.3a-amd64.iso	3.0 GB	Missing
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)
Kali Linux version 2018.1	2.9 GB	Missing files
kali-linux-2018.1-amd64.iso	2.8 GB	Missing
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)
Kali Linux version 2017.3	2.7 GB	Missing files
kali-linux-2017.3-amd64.iso	2.7 GB	Missing
kali-linux-persistence-1gb.qcow2	33.1 MB	Found on GNS3 VM (GNS3 VM)
Kali Linux version 2017.2	2.8 GB	Missing files

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

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

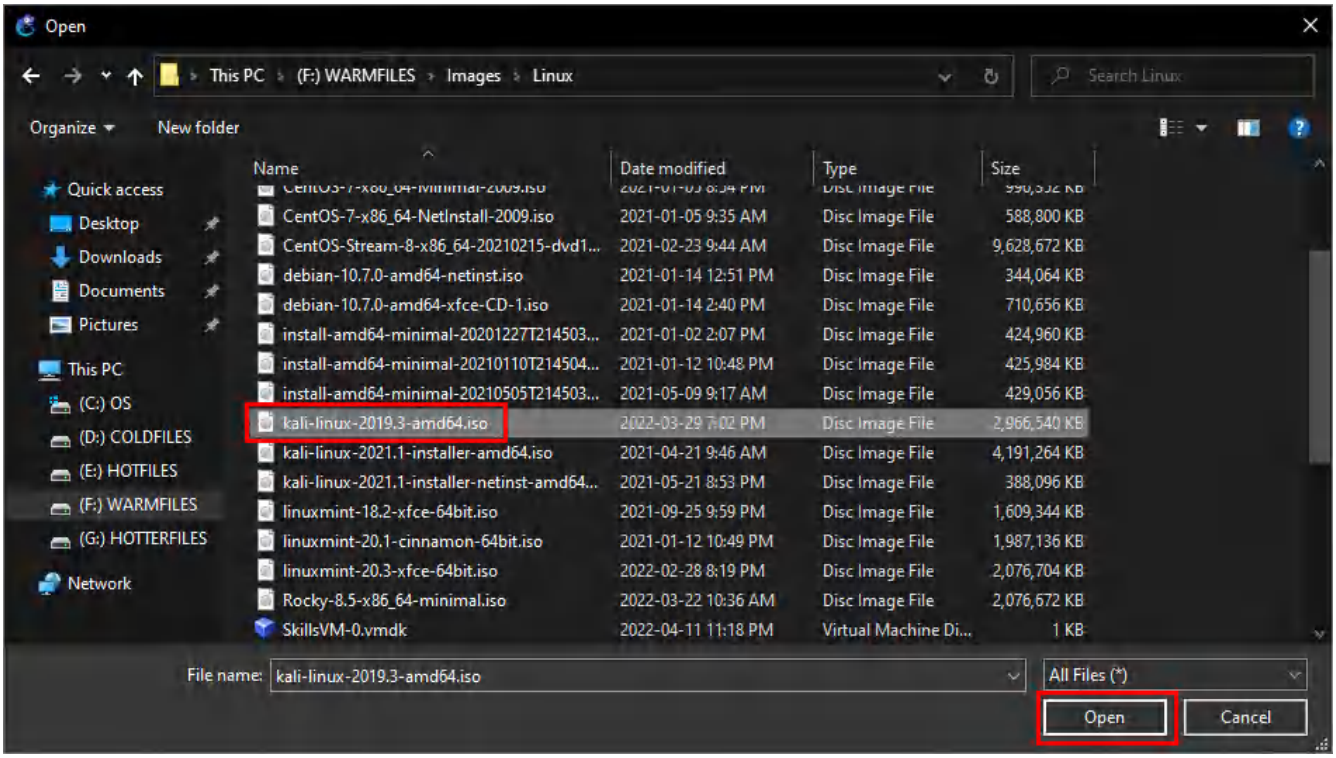


Figure A.22: Select “kali-linux-2019.3-amd64.iso”

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

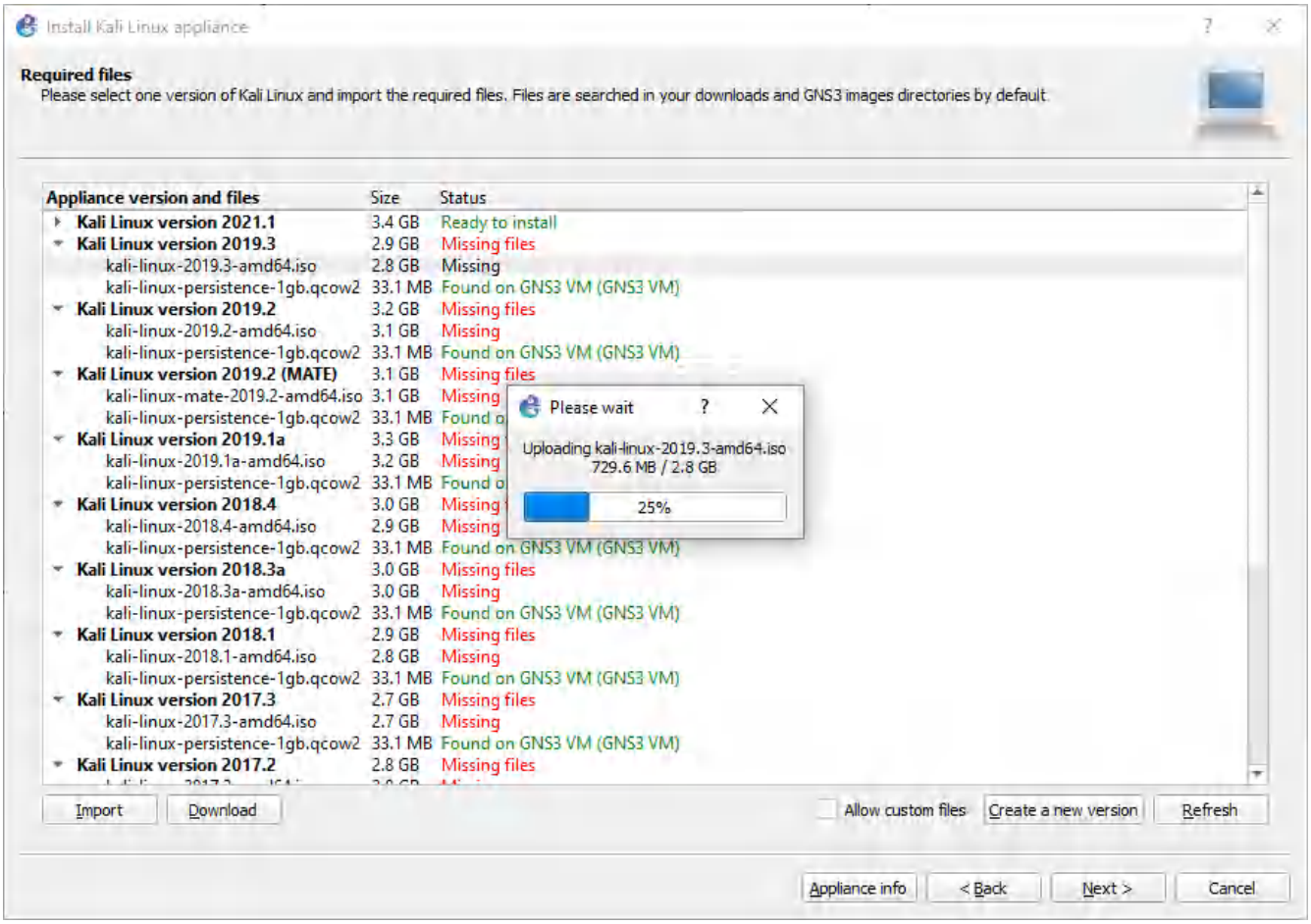


Figure A.23: Loading the ISO image

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

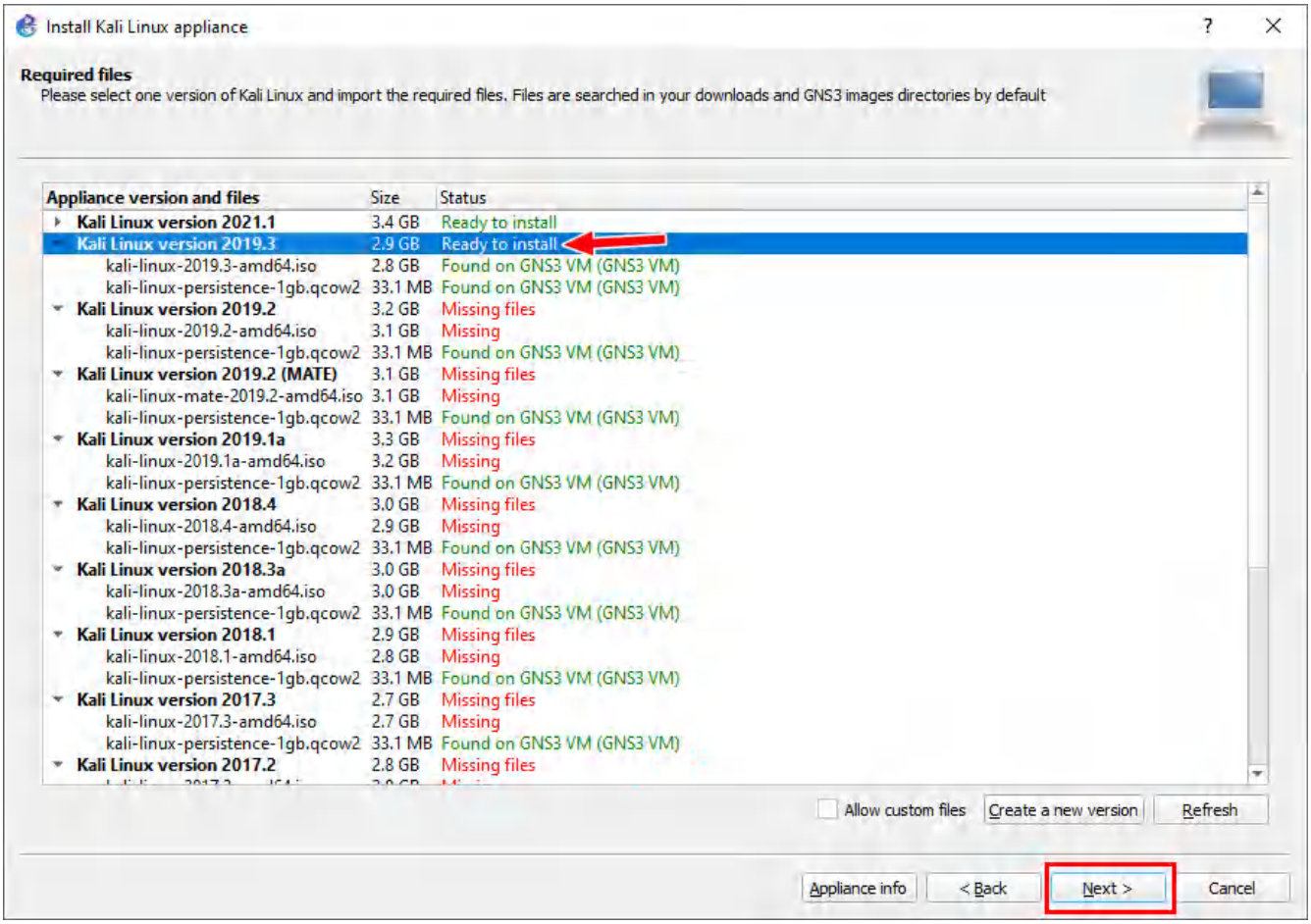


Figure A.24: Ready to install

Then click Finish.

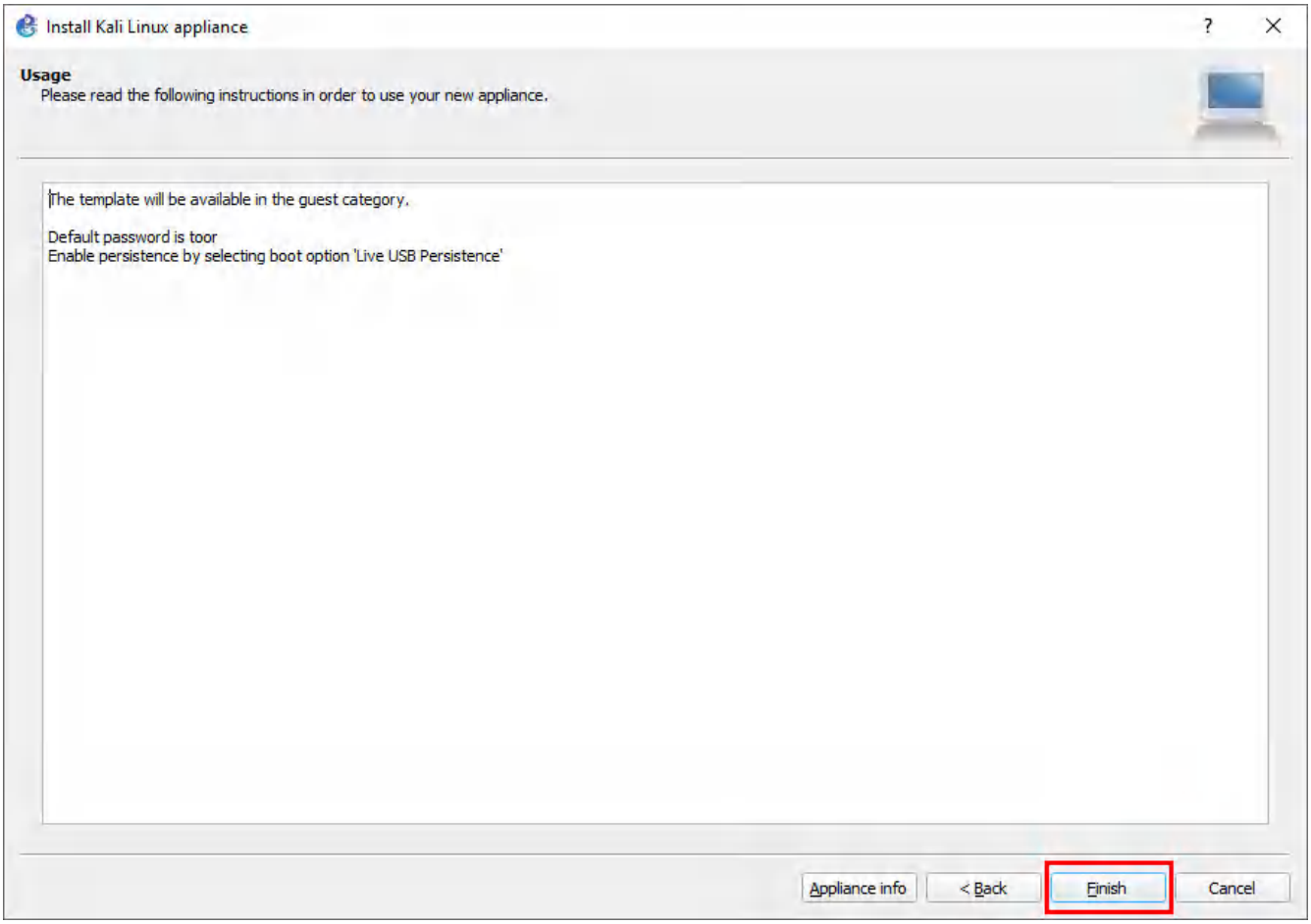


Figure A.25: Final step of configuration

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.

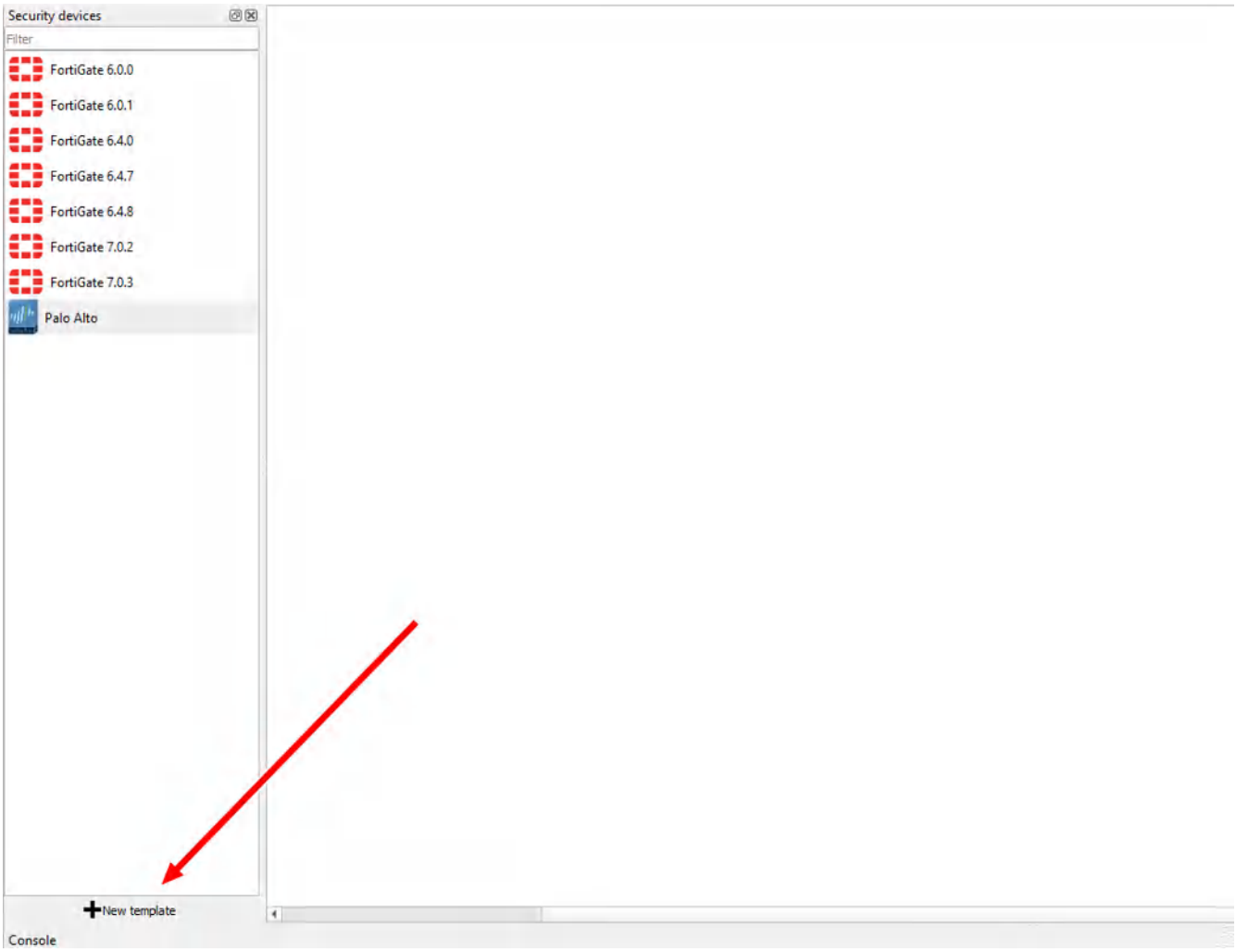


Figure A.26: Create a new template

We want to install an appliance from the GNS3 server.

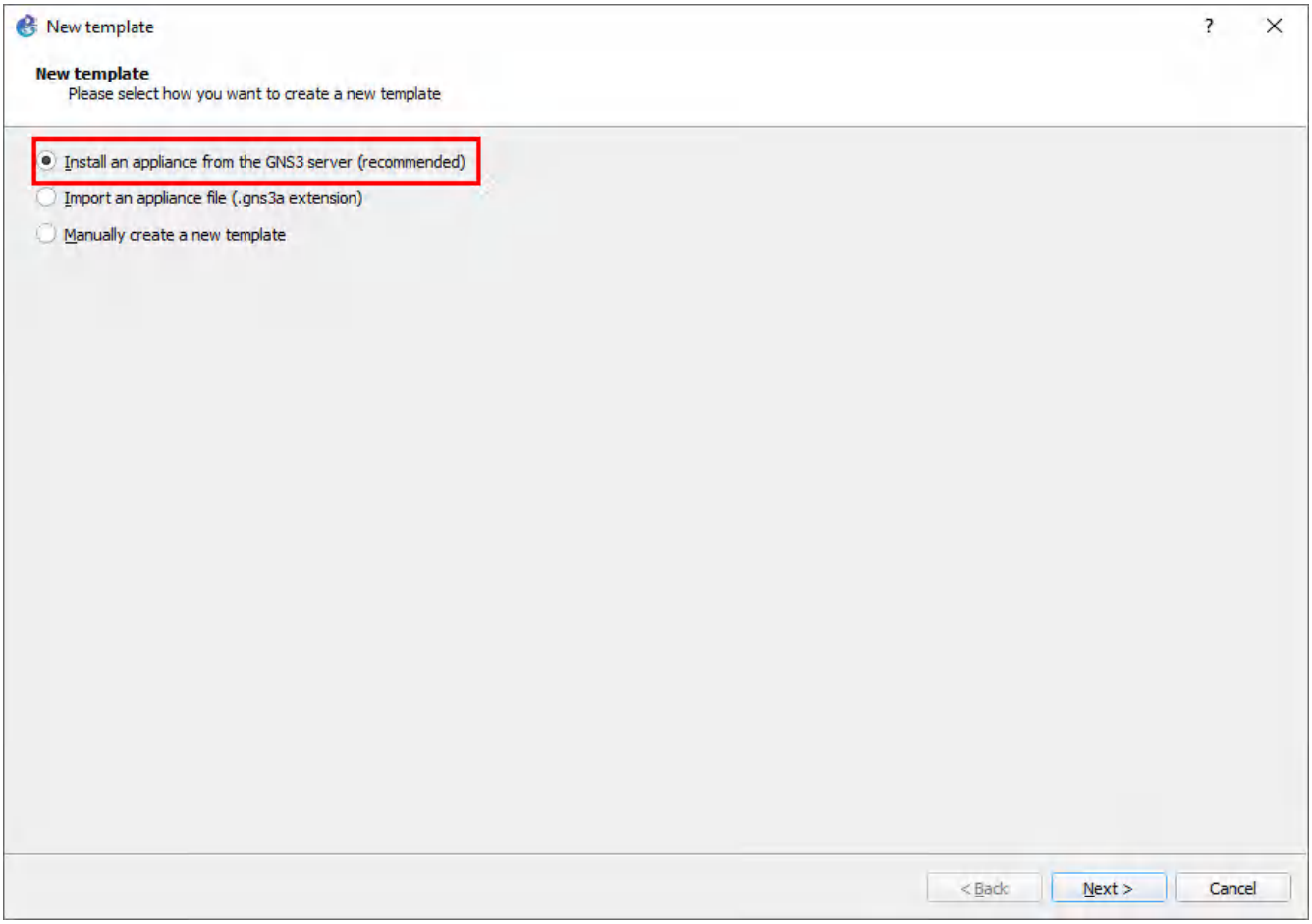


Figure A.27: Select "Install an appliance from the GNS3 server"

Lookup “WordPress”, then click Install.

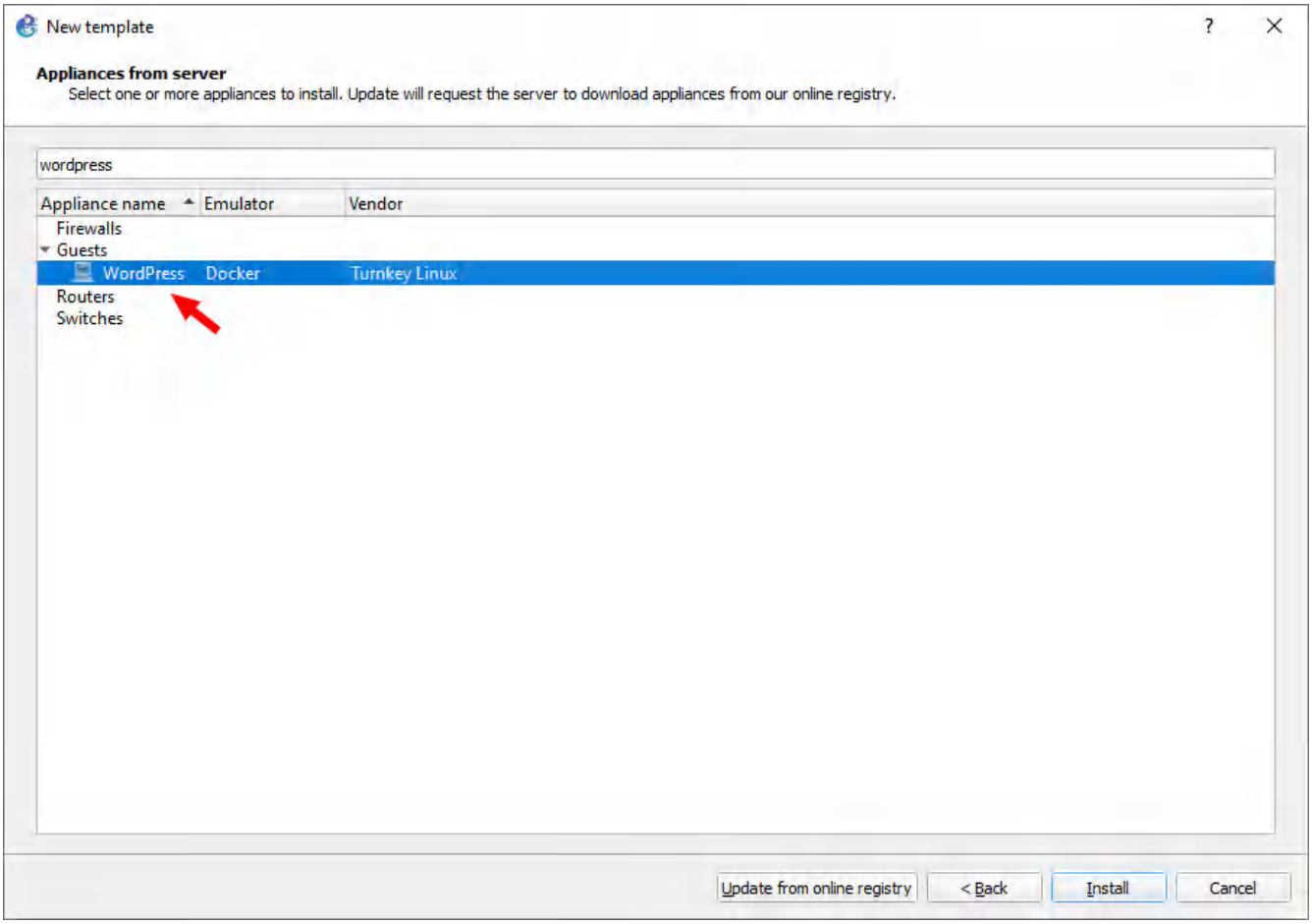


Figure A.28: Search for “WordPress”

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

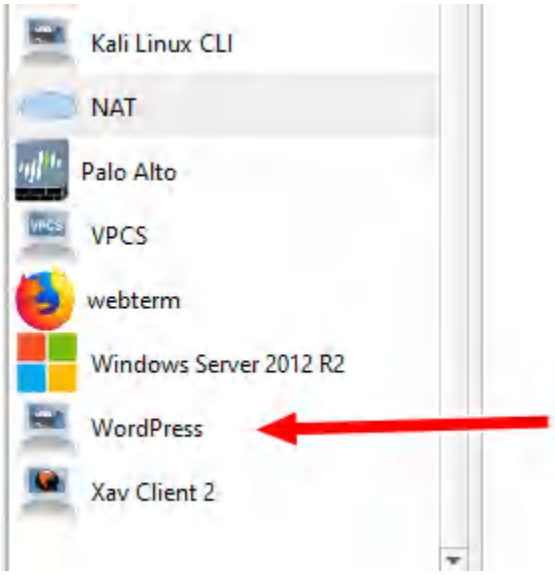


Figure A.29: Verify WordPress Installation

Configure WordPress

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

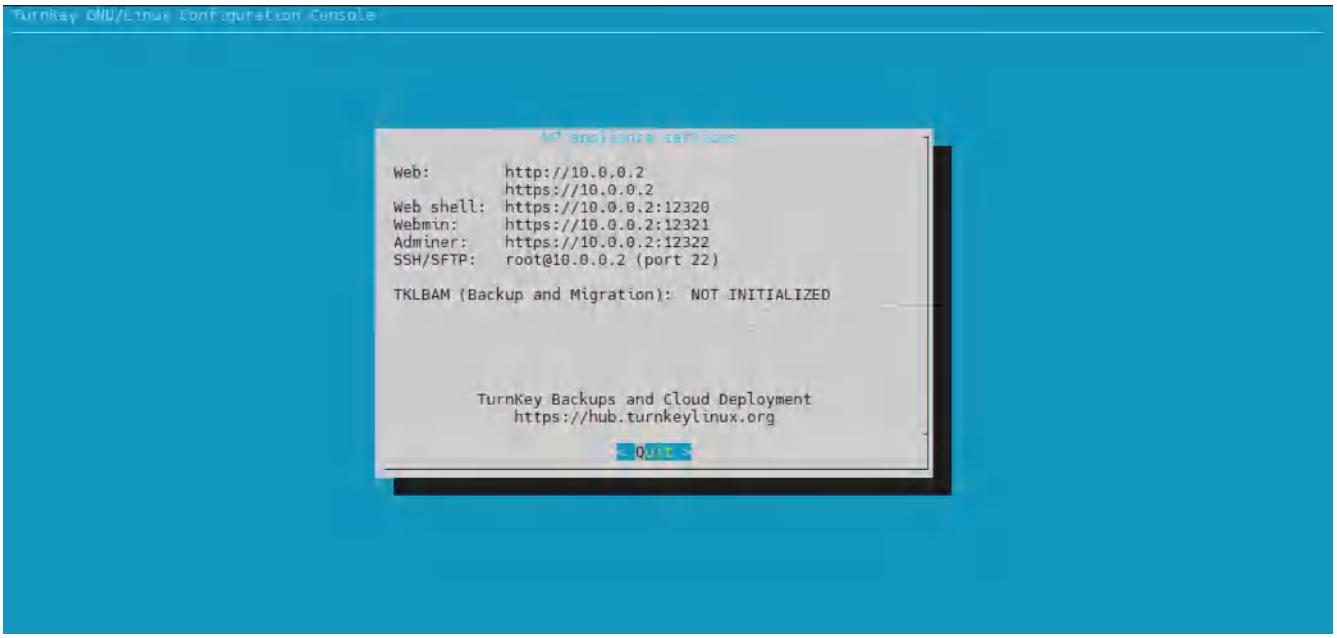


Figure A.30: Running WordPress

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!

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

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

TKLBAM (Backup and Migration):  NOT INITIALIZED

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

      https://www.turnkeylinux.org/tklbam


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

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

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

Figure A.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.

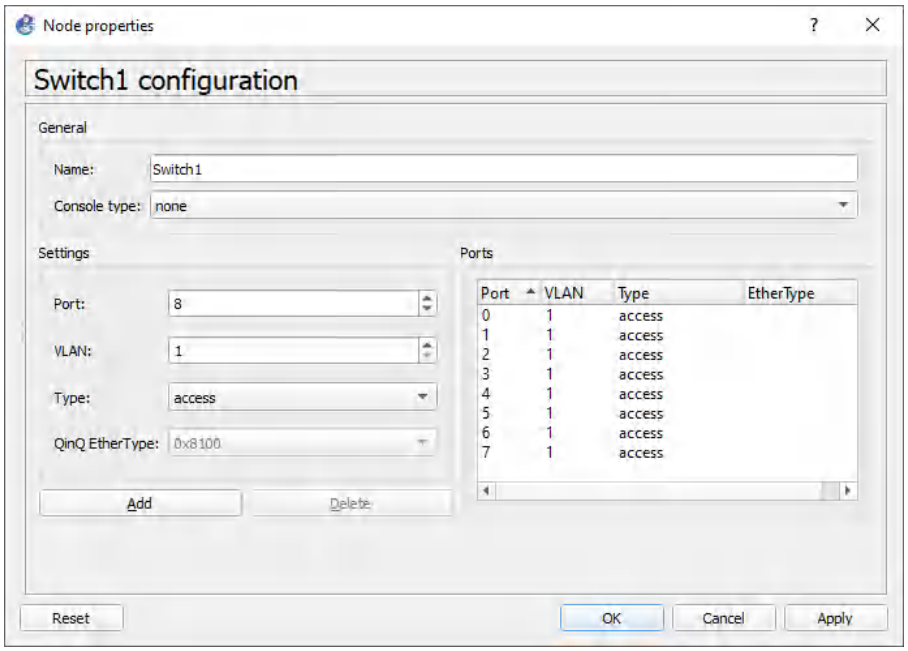


Figure A.32: Switch Configuration

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

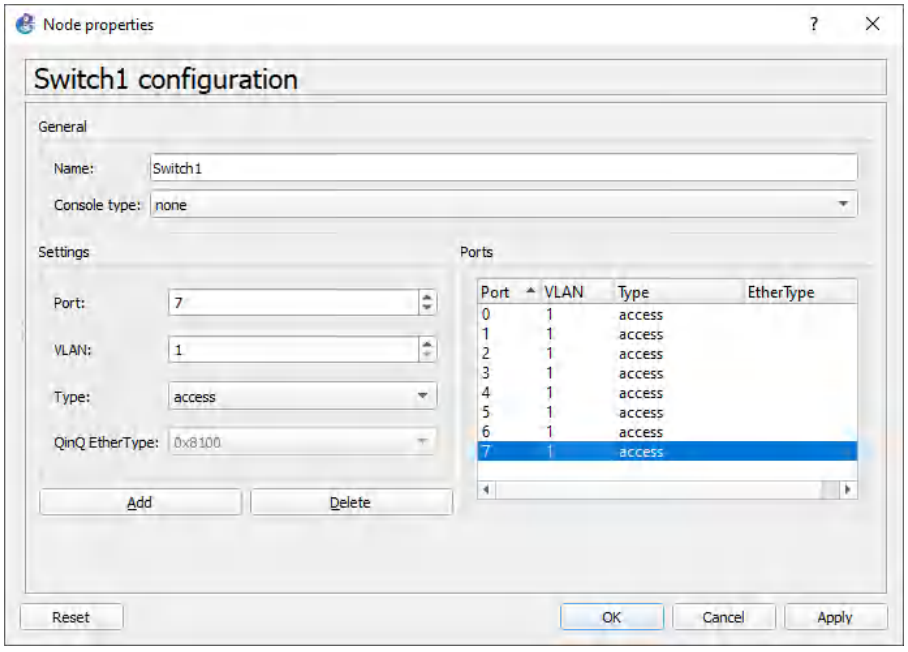


Figure A.33: Double click on port7

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

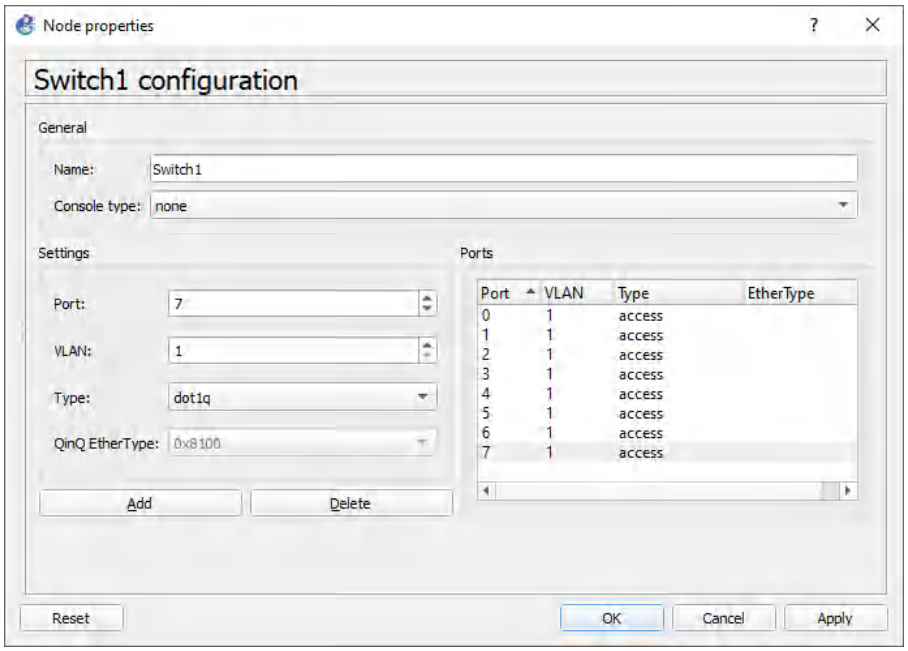


Figure A.34: Select port7 as dot1q

Click on add to apply the changes.

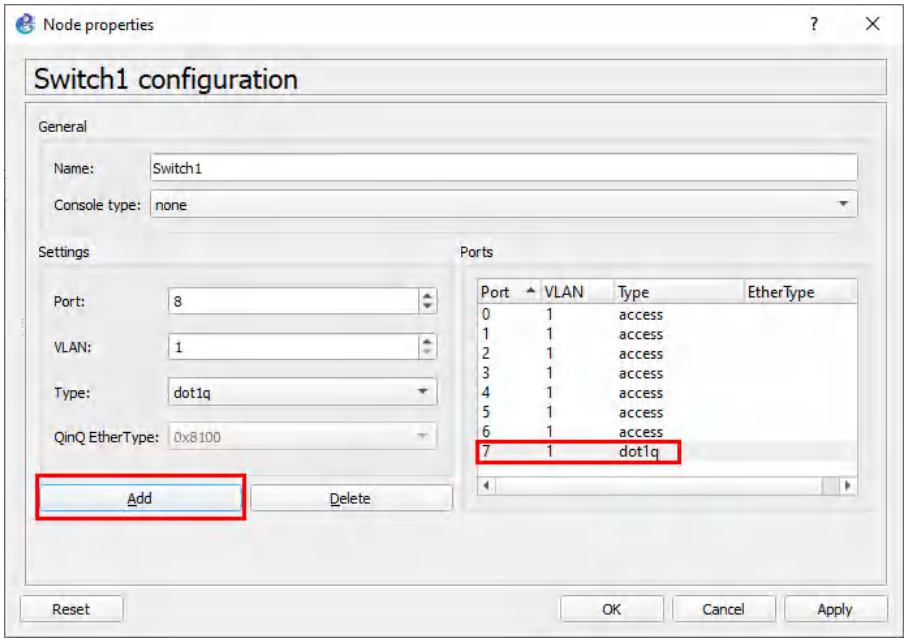


Figure A.35: Click on Add to apply the changes

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.