

Lab#2
NetGate pfSense

NACT-261 Network Security
2024-2025 Spring Semester

Submitted by Jibreal Id-deen

Due by February 16
Professor Mark Jeremy

TABLE OF CONTENTS

Table of Figures.....	3
Objective	5
Procedure	6
Network Diagram.....	7
Questions and Answers.....	38
Observations	40

TABLE OF FIGURES

Figure 1 - Check the router's IP address from CMD	8
Figure 2 - Use that IP address on the website to look.....	8
Figure 3 - Seeing the account on the website	8
Figure 4 - Logging the account on the website.....	9
Figure 5 - Looking at the GUI of the pfSense Router.....	10
Figure 6 - Open the system then click General Setup.....	11
Figure 7 - Looking around the gernal setup.....	12
Figure 8 - Open the system and click package manager.....	13
Figure 9 - Looking around the package manager	14
Figure 10 - Open the system again and click routing	15
Figure 11 - Looking around routing.....	16
Figure 12 Click the pfSense to go back	16
Figure 13 - Update the version of pfSense Router.....	17
Figure 14 - Confirm the update.....	17
Figure 15 - Updating.....	18
Figure 16 - Rebooting.....	18
Figure 17 - Logging the account again	19
Figure 18 - Update completed.....	19
Figure 19 - Open the system and click package manager.....	20
Figure 20 - Click the available packages	20
Figure 21 - type "pfBlockerNG" on available package	21
Figure 22 - Install the pfBlockerNG	21
Figure 23 - Confirm the pfBlockerNG.....	22
Figure 24 - Installing.....	22
Figure 25 - Installation successfully	23
Figure 26 - Open firewall then click pfBlockerNG	23
Figure 27 - Set the pfBlockerNG up	24
Figure 28 - Proceeding.....	24
Figure 29 - Processing....	25

Figure 30 - Looking around the step 3 of 4	25
Figure 31 - Finish the pfBloceNG finalize	26
Figure 32 - Open firewall then pfBlockerNG	26
Figure 33 - Enable pfBlockerNG then click IP.....	27
Figure 34 - Click IPv4.....	27
Figure 35 - Click "Add"	27
Figure 36 - TYPE the blockwebsite and describe what it is for	28
Figure 37 - Typing...	28
Figure 38 - Scrolling down.....	28
Figure 39 - Click IPv4 Custom_List.....	29
Figure 40 - Before that, open the cmd	29
Figure 41 - Using nslookup to ask the router to get IP from it	30
Figure 42 - Asking the router to send me IP address from the lollupop.org website	30
Figure 43 - Putting the IP address on the custom list	31
Figure 44 - Saved IPv4 Setting to confirm	31
Figure 45 - Using nslookup to ask the router to get IP address from call of duty website	32
Figure 46 - Enable Domain/AS and put the name of website on it	33
Figure 47 - Confirm the IPv4 Setting	33
Figure 48 - Checking the websites before it get blocked.....	34
Figure 49 - Saved the IPv4 configuration	35
Figure 50 - Click Update.....	35
Figure 51 - Run the update status	35
Figure 52 - Complete the update log.....	36
Figure 53 - Lollypop is blocked now	36
Figure 54 - type the call of duty url on google	37
Figure 55 - Call of Duty website is now blocked	37

OBJECTIVE

To be able to understand how does the pfSense Router SG-3100 works and learn how to install pfBlockerNG. So, with that, I can learn how to block the website as whatever I want on this router and understand what the features appear on this.

PROCEDURE

- Walked to the ICS Equipment room
- Got the SG-3100 model Router, MAC.
- Got WAN and LAN cable to connect with the router and Internet
- Learned how to reset the Router
- Opened the GUI on the website
- Learned how to install pfBlockerNG on it
- Block the website
- Take the items what I took from ICS Equipment to give it back

NETWORK DIAGRAM

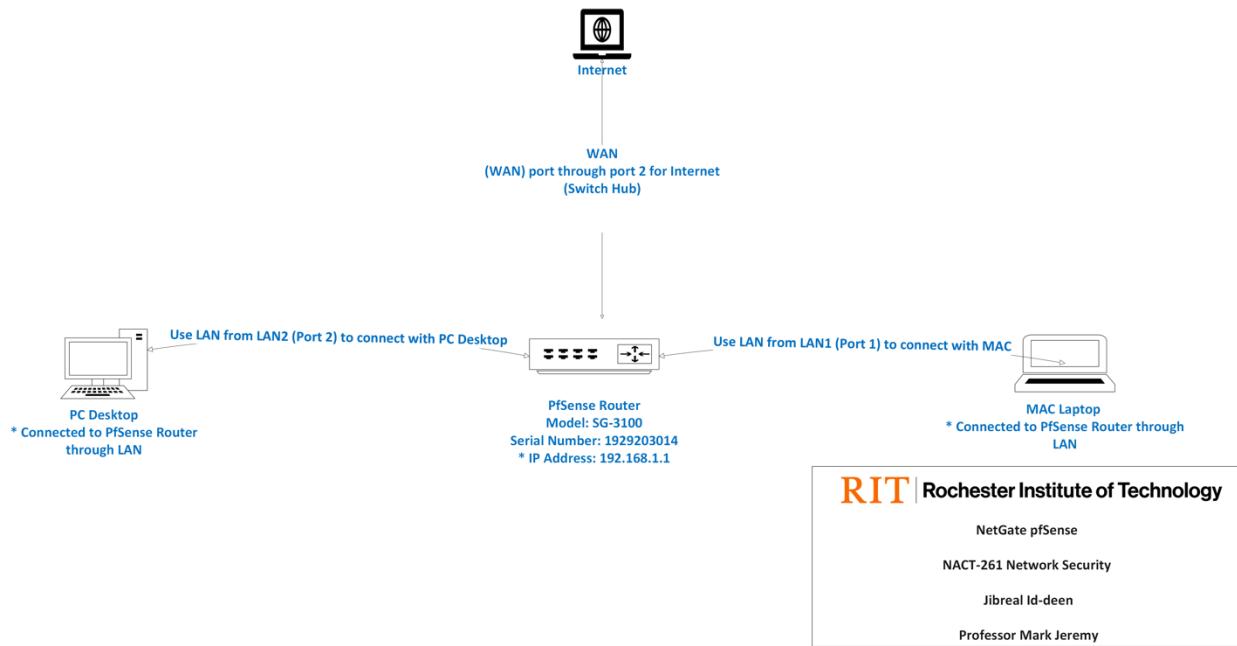


FIGURE 1 - NETWORK DIAGRAM

```
C:\Users\Student04>ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . : home.arpa
Link-local IPv6 Address : fe80::99e3:267:8025:5dbb%12
IPv4 Address : 192.168.1.134
Subnet Mask : 255.255.255.0
Default Gateway : fe80::208:a2ff:fe11:8c12%12
192.168.1.1 2

FIGURE 2 - CHECK THE ROUTER'S IP ADDRESS FROM CMD

Not secure https://192.168.1.1/index.php

FIGURE 3 - USE THAT IP ADDRESS ON THE WEBSITE TO LOOK



FIGURE 4 - SEEING THE ACCOUNT ON THE WEBSITE

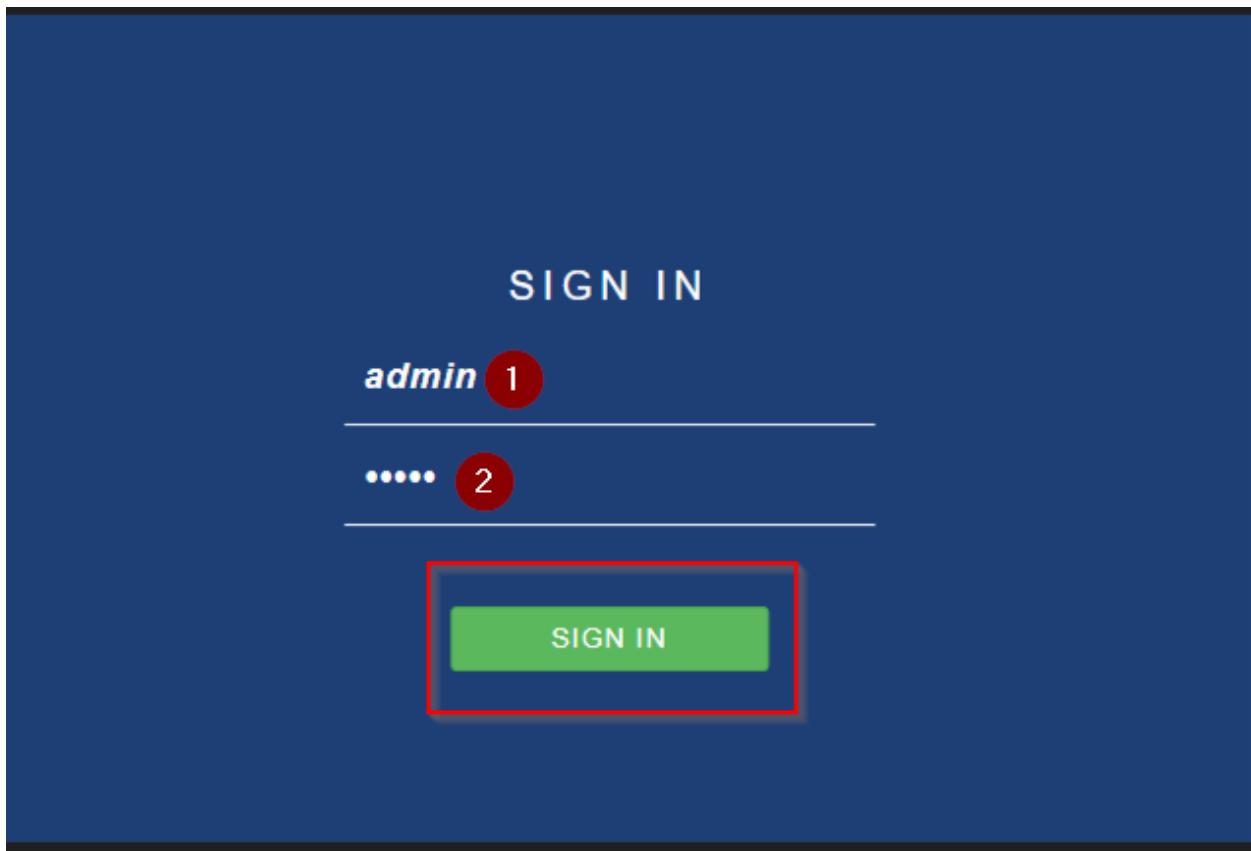


FIGURE 5 - LOGGING THE ACCOUNT ON THE WEBSITE

System Information

Name	pfSense.home.arpa
User	admin@192.168.1.134 (Local Database)
System	Netgate 3100 Serial: 1929203014 Netgate Device ID: 524cc036772cb963e3d6
Version	23.05.1-RELEASE (arm) built on Wed Jun 28 03:58:46 UTC 2023 FreeBSD 14.0-CURRENT
Version 23.09.1 is available.	
Version information updated at Wed Feb 5 20:34:02 UTC 2025	
CPU Type	ARM Cortex-A9 r4p1 (ECO: 0x00000000) 2 CPUs Crypto: Marvell Cryptographic Engine and Security Accelerator
Hardware crypto	AES-CBC,SHA1,SHA256
Uptime	01 Hour 13 Minutes 59 Seconds
Current date/time	Wed Feb 5 20:35:33 UTC 2025
DNS server(s)	• 127.0.0.1 • 10.1.40.1
Last config change	Tue Apr 30 20:05:34 UTC 2024
State table size	0% (47/202000) Show states
MBUF Usage	15% (1518/10035)
Temperature	57°C
Load average	0.41, 0.26, 0.22
CPU usage	12%
Memory usage	10% of 2027 MiB

Disks

Mount	Used	Size	Usage
/	1.8G	6.9G	28% of 6.9G (ufs)

Netgate Services And Support

Contract type	Community Support Community Support Only
---------------	---

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your [Netgate Device ID \(NDI\)](#) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces

WAN	↑ 1000baseT <full-duplex>	10.1.40.120
LAN	↑ 2500Base-KX <full-duplex>	192.168.1.1
ADMIN	↑ Other <full-duplex>	192.168.10.1
SYSTEMADMIN	↑ Other <full-duplex>	192.168.20.1
LAN 1	↑ 1000baseT <full-duplex> Switch Port	n/a
LAN 2	✗ none Switch Port	n/a
LAN 3	✗ none Switch Port	n/a
LAN 4	✗ none Switch Port	n/a
LAN Uplink	↑ Ethernet 2500Base-KX <full-duplex> Switch Uplink	n/a

FIGURE 6 - LOOKING AT THE GUI OF THE PFSENSE ROUTER

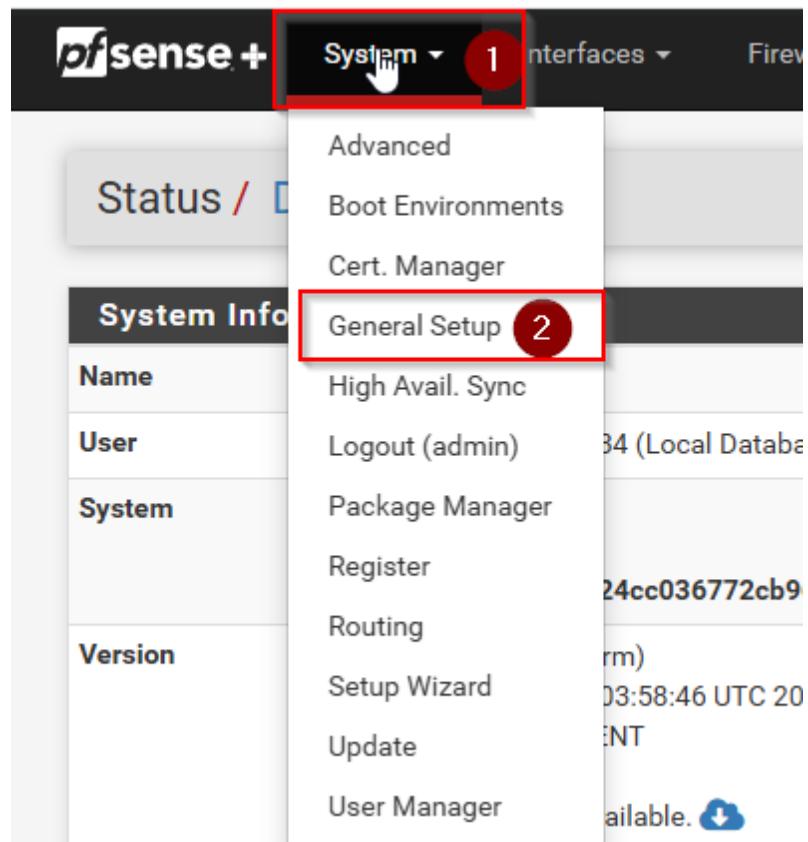


FIGURE 7 - OPEN THE SYSTEM THEN CLICK GENERAL SETUP

The screenshot shows the pfSense General Setup configuration page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is "System / General Setup".

System

- Hostname:** pfSense 1
Name of the firewall host, without domain part.
- Domain:** home.arpa 2
Domain name for the firewall.

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

DNS Server Settings

- DNS Servers:** 3 DNS Server Address: Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.
- Add DNS Server:** 4 [+ Add DNS Server](#)
- DNS Server Override:** 5 Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server
If this option is set, Netgate pfSense Plus will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS options is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.
- DNS Resolution Behavior:** 6 Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)
By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

FIGURE 8 - LOOKING AROUND THE GERNAL SETUP

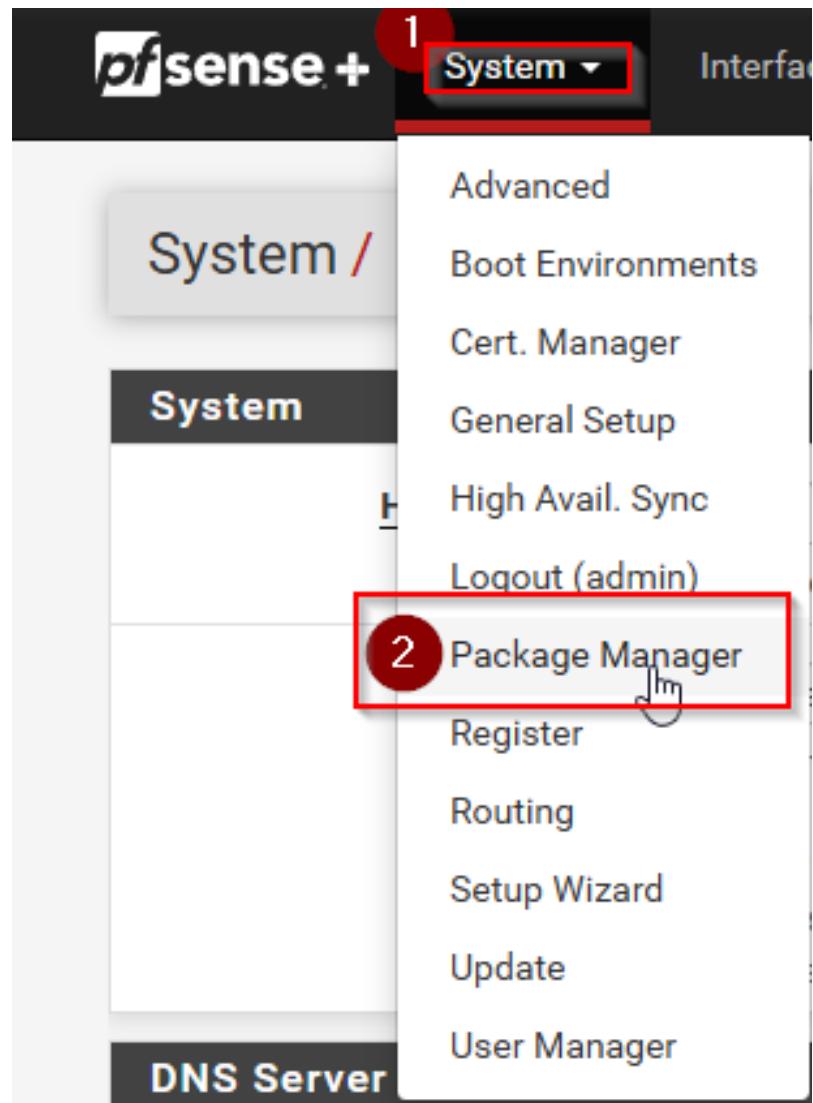


FIGURE 9 - OPEN THE SYSTEM AND CLICK PACKAGE MANAGER

The screenshot shows the pfSense Package Manager interface. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the path 'System / Package Manager / Installed Packages' is displayed. A red box highlights this path. A red circle with the number '1' is positioned at the top right of the main content area. The main content area has two tabs: 'Installed Packages' (which is selected) and 'Available Packages'. A red box highlights the 'Installed Packages' tab. A red circle with the number '2' is positioned to the left of the table header. The table lists two packages:

Name	Category	Version	Description	Actions
✓ aws-wizard	net	0.10	pfSense AWS VPC VPN Connection Wizard Package Dependencies: 🔗 php82-8.2.11 🔗 aws-sdk-php-3.273.3	💻 🔄 ⓘ
⟳ ipsec-profile-wizard	net	1.1_1	pfSense Mobile IPsec Client Profile Generator for Apple and Windows devices Package Dependencies: 🔗 zip-3.0_1	💻 ⓘ

Below the table, there are several status indicators and messages:

- 🕒 = Update ✓ = Current
- trash = Remove ⓘ = Information 🔖 = Reinstall
- Newer version available
- Package is configured but not (fully) installed or deprecated

FIGURE 10 - LOOKING AROUND THE PACKAGE MANAGER

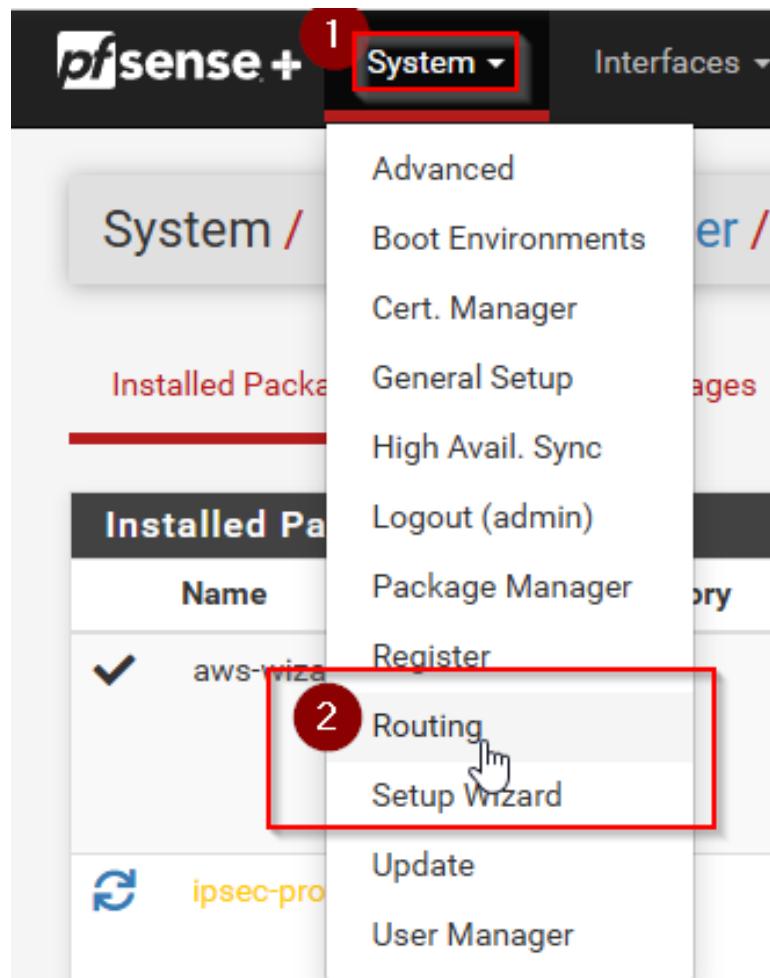


FIGURE 11 - OPEN THE SYSTEM AGAIN AND CLICK ROUTING

1

2

3

FIGURE 12 - LOOKING AROUND ROUTING

FIGURE 13 CLICK THE PFSENSE TO GO BACK

The screenshot shows the pfSense Status / Dashboard interface. At the top, there's a red box around the title "Status / Dashboard" with a red circle labeled "1" to its right. Below it is a "System Information" section with the following details:

Name	pfSense.home.arpa
User	admin@192.168.1.134 (Local Database)
System	Netgate 3100 Serial: 1929203014 Netgate Device ID: 524cc036772cb963e3d6
Version	23.05.1-RELEASE (arm) built on Wed Jun 28 03:58:46 UTC 2023 FreeBSD 14.0-CURRENT

At the bottom of the "System Information" section, there's a red box around a message: "Version 23.09.1 is available." with a download icon, and "Version information updated ~Wed Feb 5 20:34:02 UTC 2025" with a refresh icon. A red circle labeled "2" points to the "23.09.1" text.

FIGURE 14 - UPDATE THE VERSION OF PFSENSE ROUTER

The screenshot shows the pfSense System / Update / System Update interface. At the top, there's a red box around the title "System / Update / System Update" with a red circle labeled "1" to its right. Below it is a "Confirmation Required to update Netgate pfSense Plus system." section. The "Branch" dropdown is set to "Previous Stable Version (23.09.1)". The "Messages" section contains the message: "Your Netgate device has pfSense+ as part of your device purchase." Below that, two boxes show the current and latest base system versions: "Current Base System" is 23.05.1 (labeled "2") and "Latest Base System" is 23.09.1 (labeled "3"). At the bottom, there's a "Confirm Update" button with a green checkmark icon (labeled "4").

FIGURE 15 - CONFIRM THE UPDATE

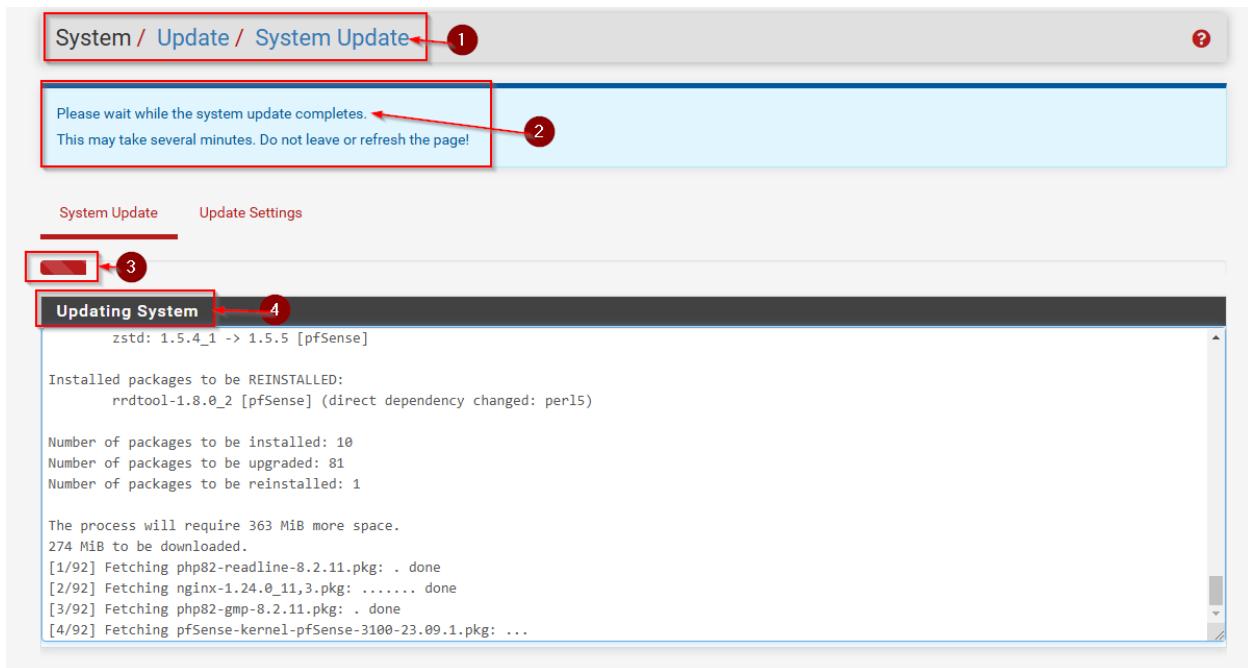


FIGURE 16 - UPDATING...

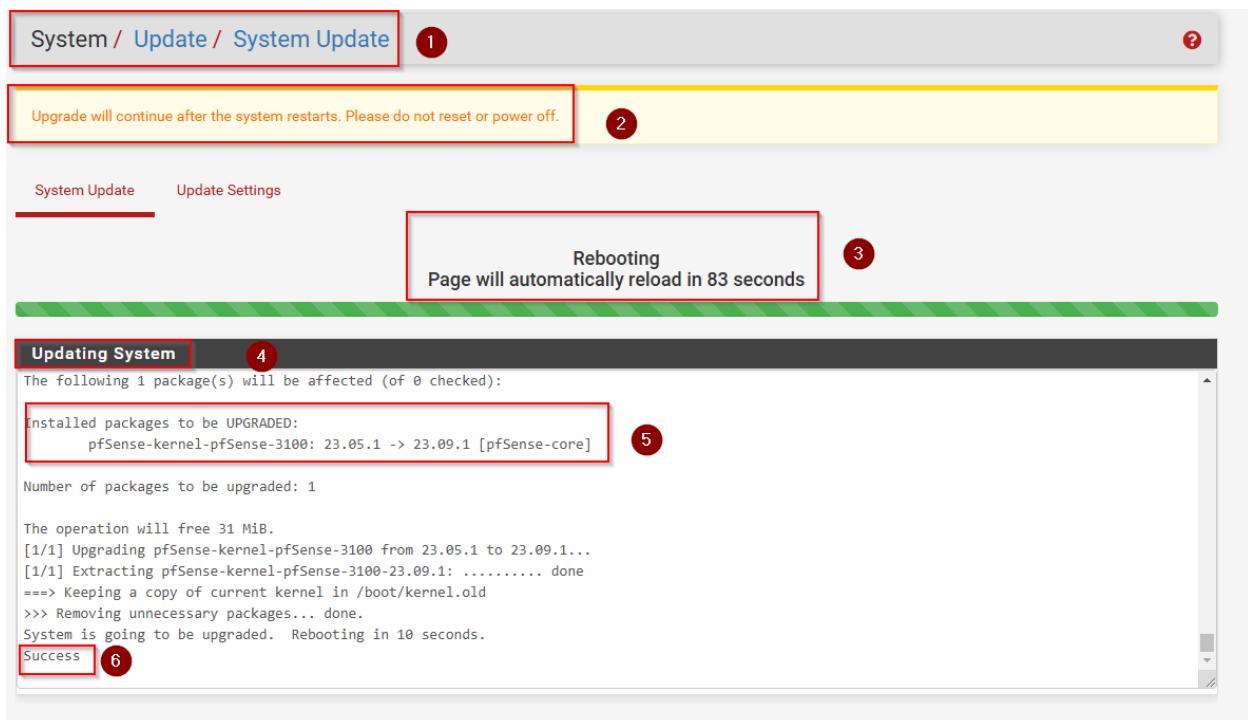


FIGURE 17 - REBOOTING....



FIGURE 18 - LOGGING THE ACCOUNT AGAIN

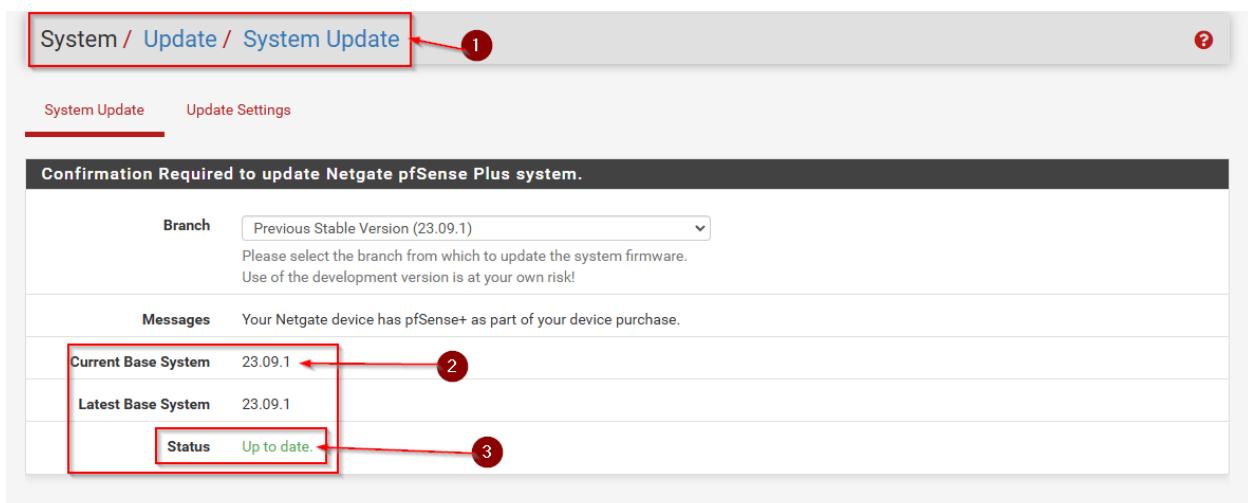


FIGURE 19 - UPDATE COMPLETED

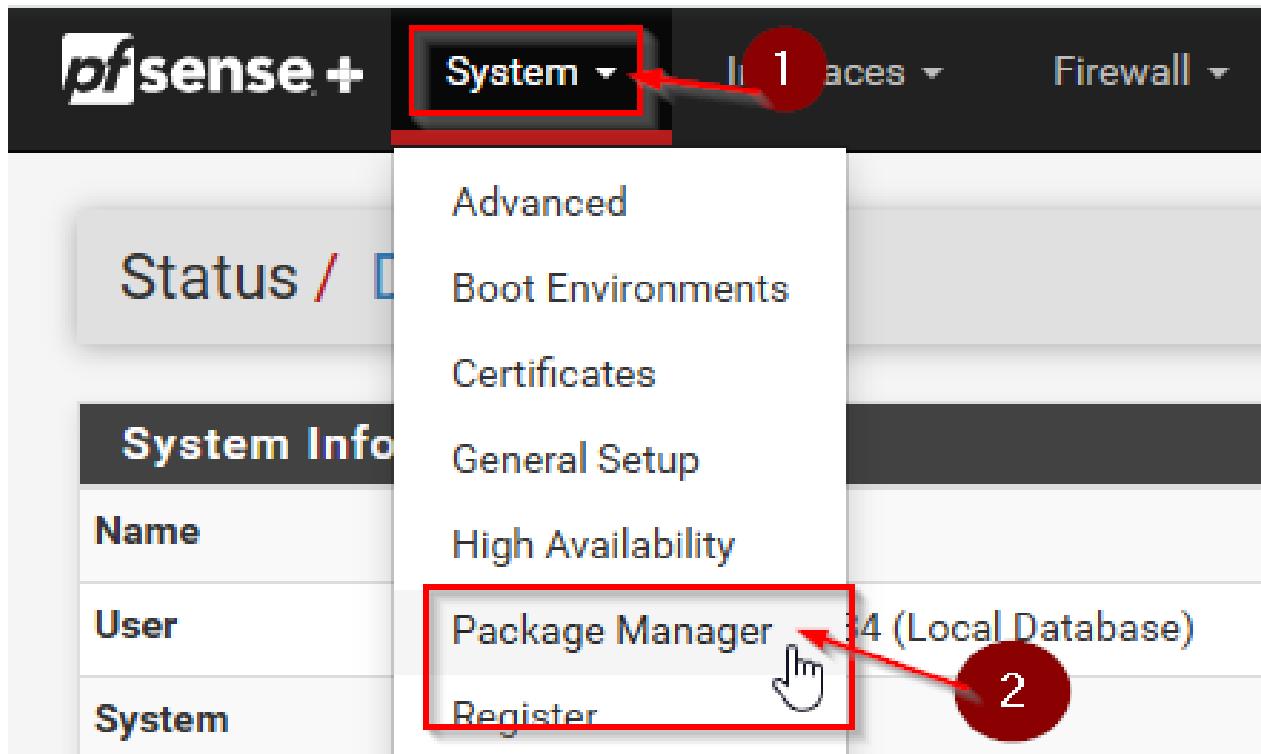


FIGURE 20 - OPEN THE SYSTEM AND CLICK PACKAGE MANAGER

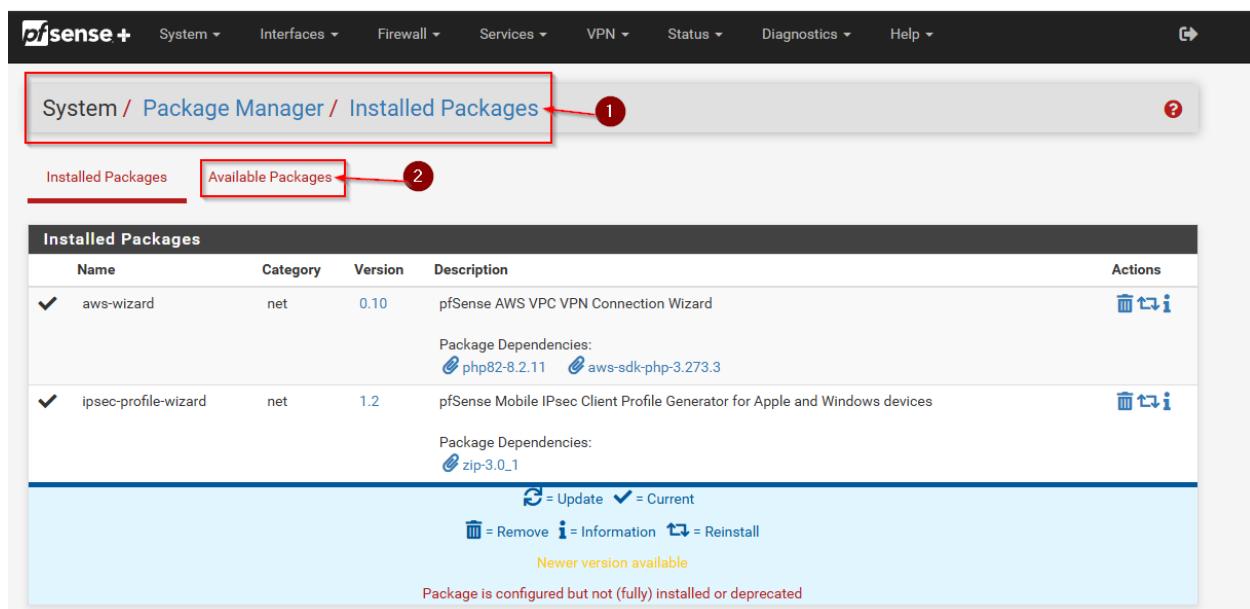


FIGURE 21 - CLICK THE AVAILABLE PACKAGES

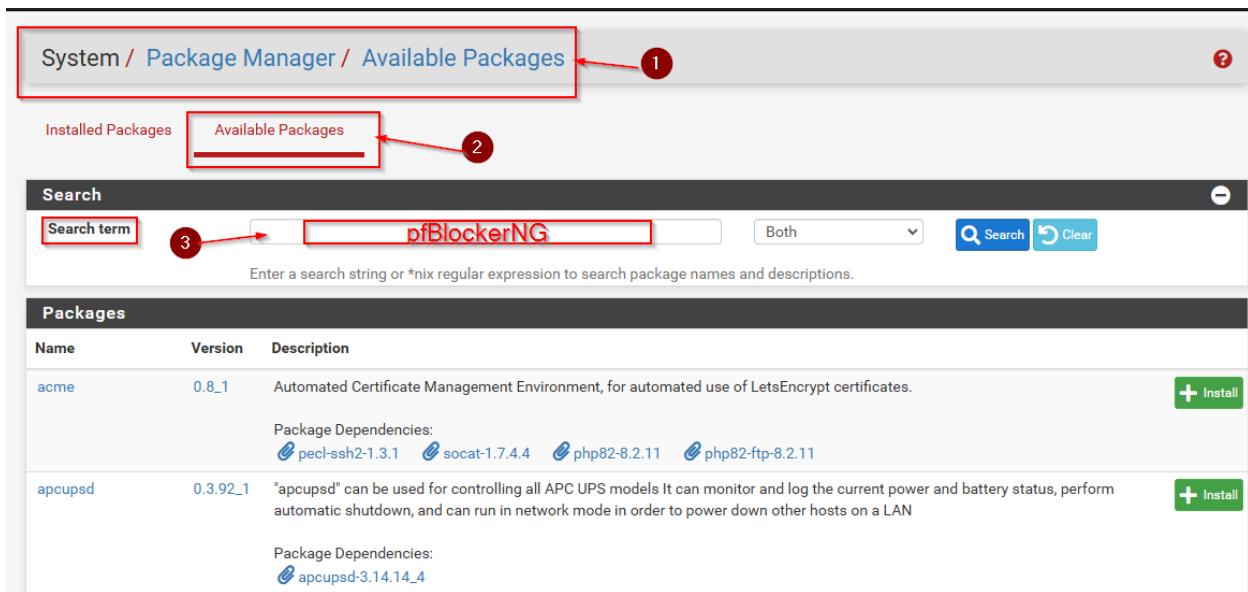


FIGURE 22 - TYPE "PFBLOCKERNG" ON AVAILABLE PACKAGE

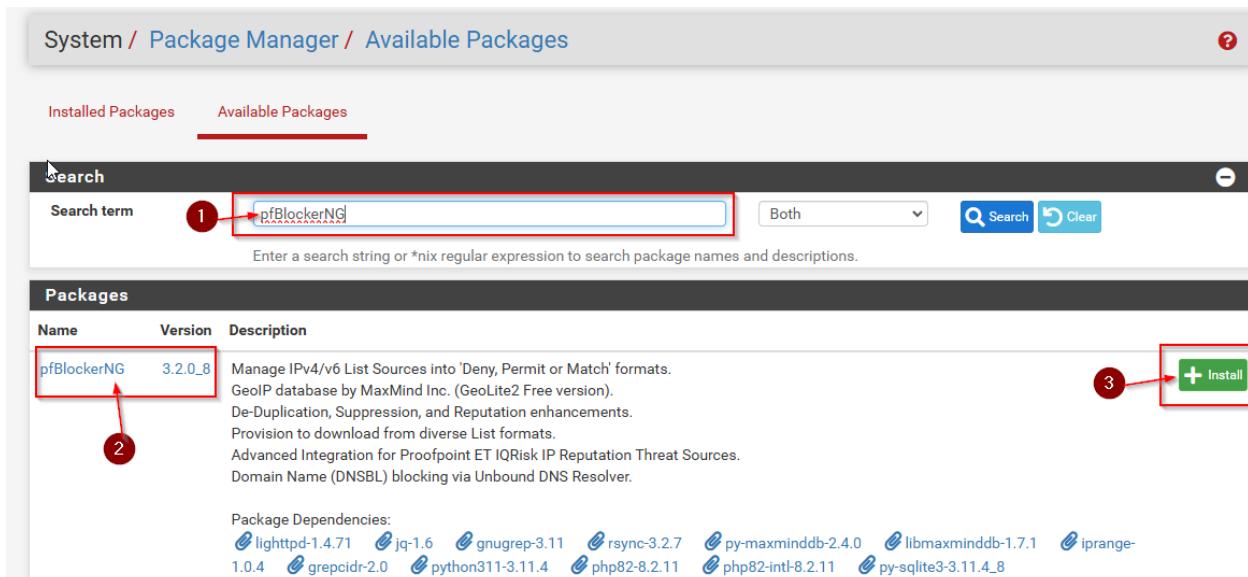


FIGURE 23 - INSTALL THE PFBLOCKERNG



FIGURE 24 - CONFIRM THE PFBLOCKERNG

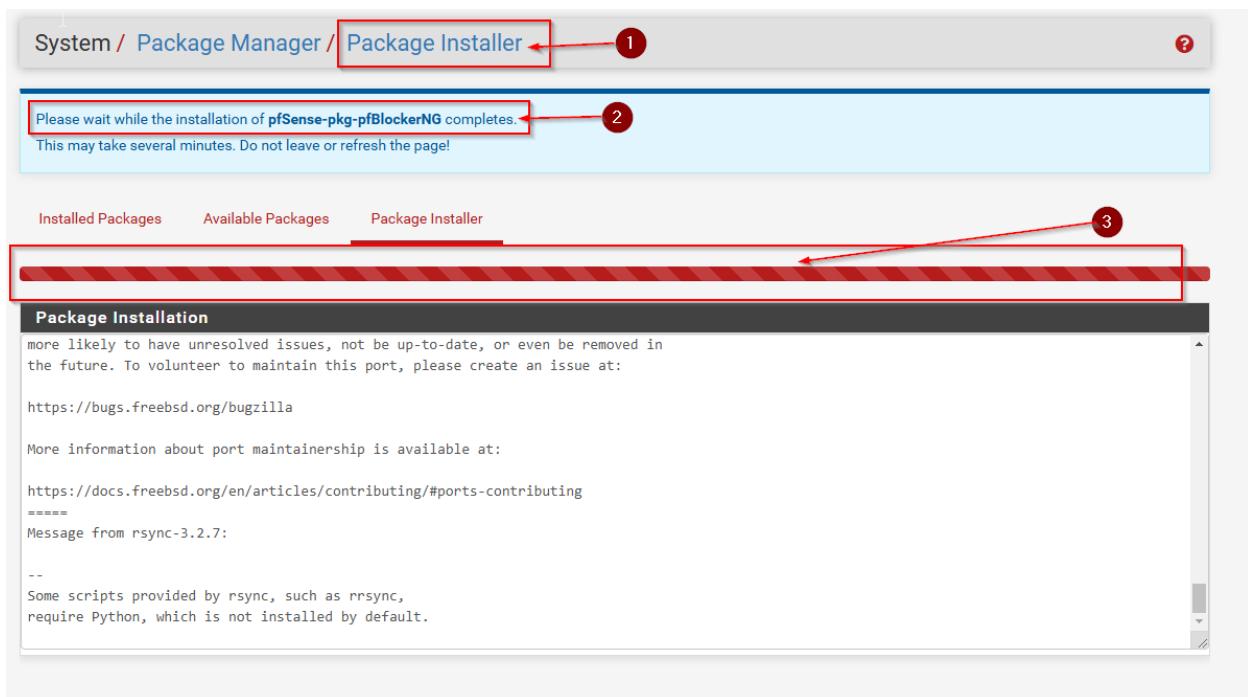


FIGURE 25 - INSTALLING....

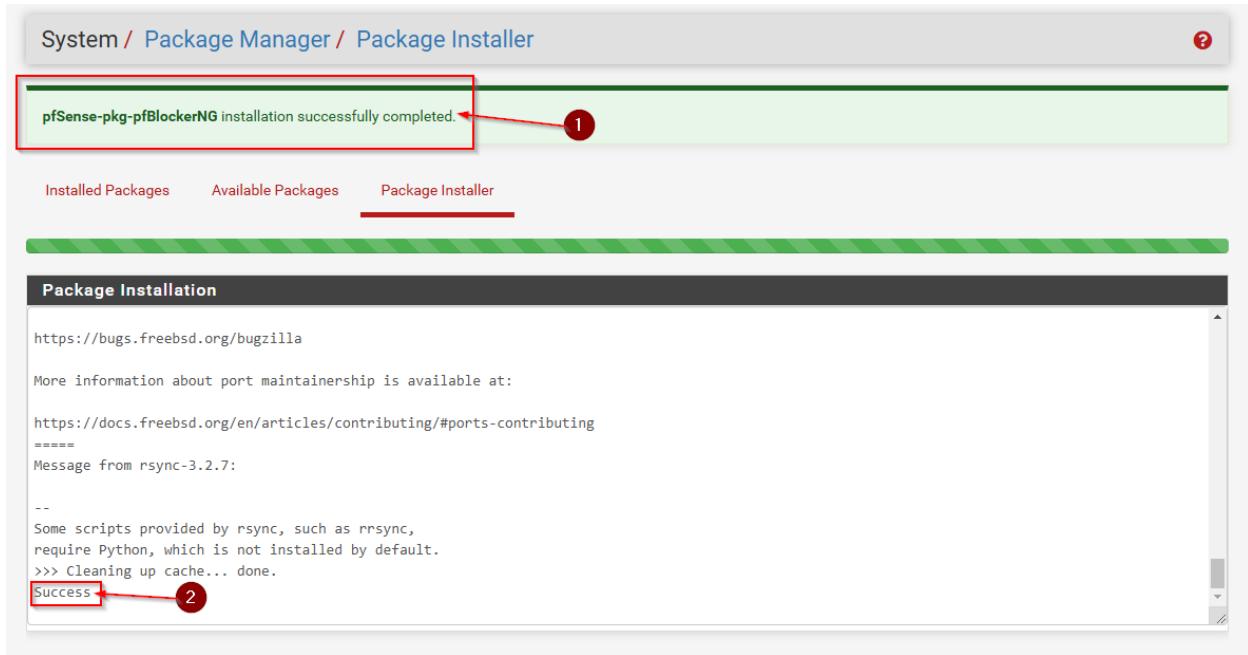


FIGURE 26 - INSTALLATION SUCCESSFULLY

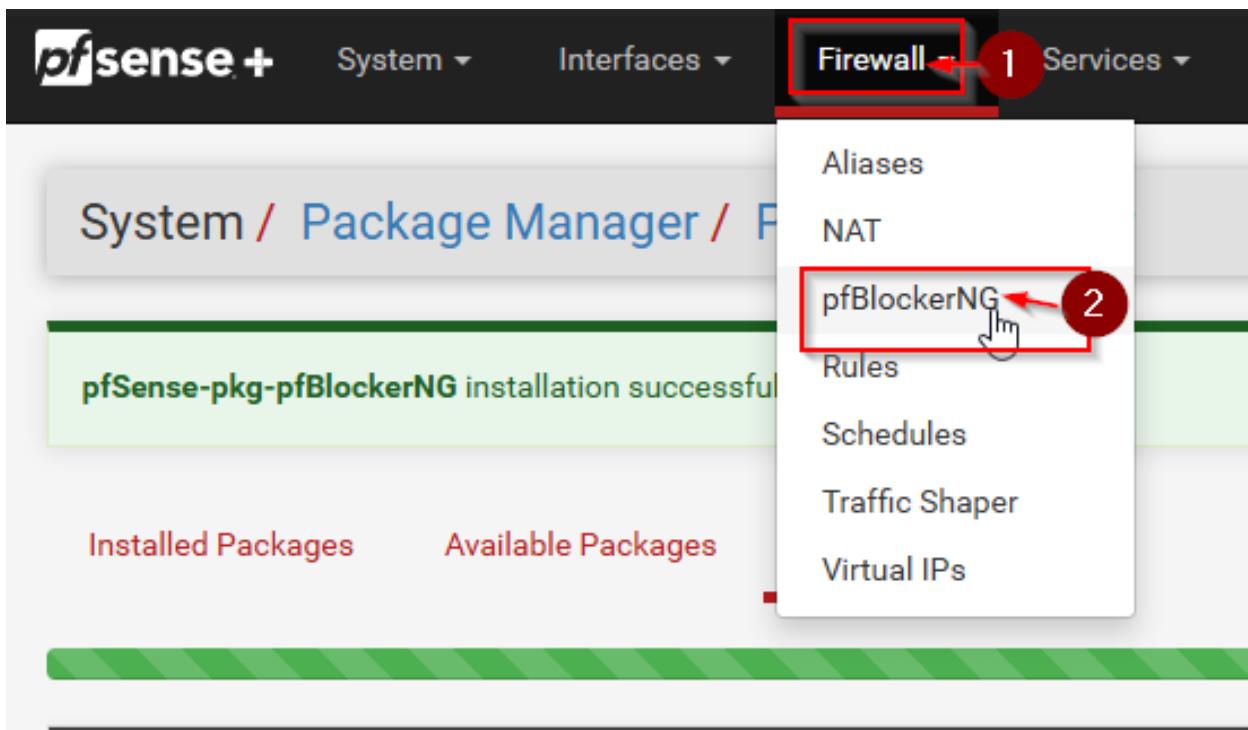


FIGURE 27 - OPEN FIREWALL THEN CLICK PFBLOCKERNG

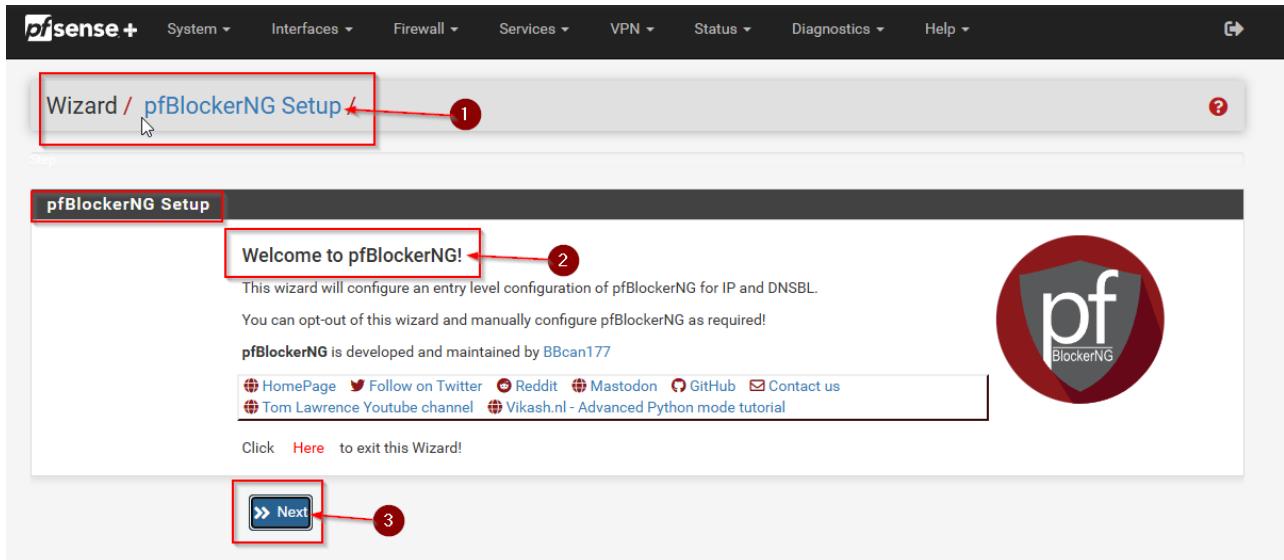


FIGURE 28 - SET THE PFBLOCKERNG UP

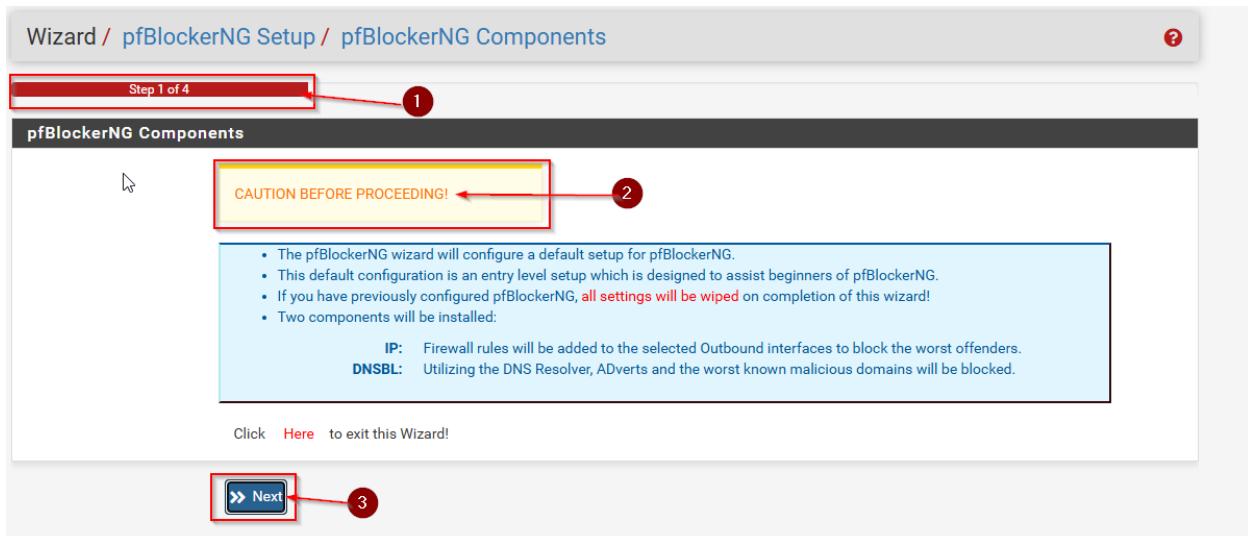


FIGURE 29 - PROCEEDING...

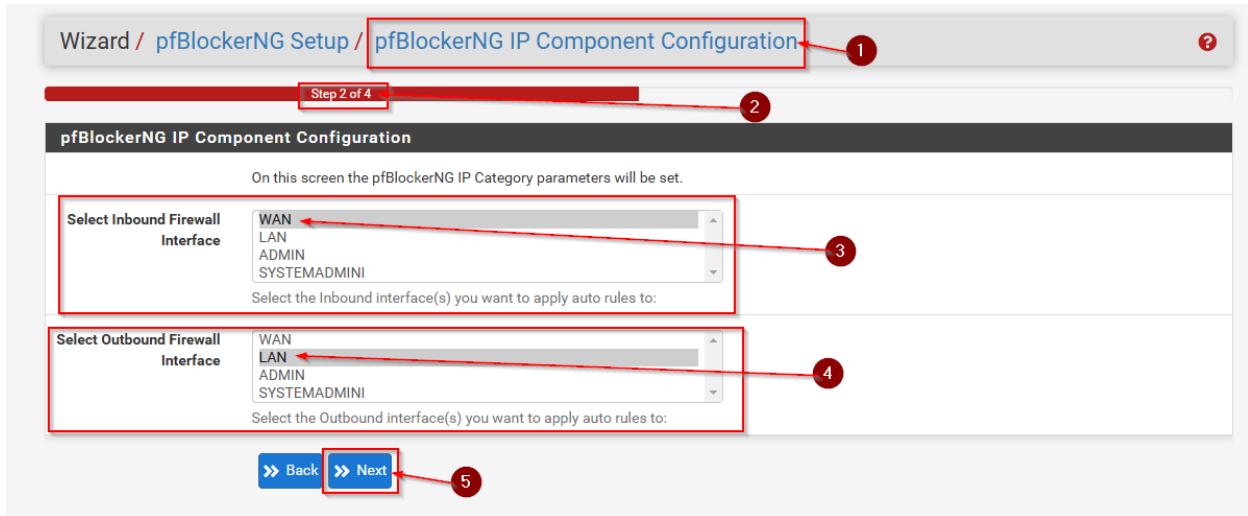


FIGURE 30 - PROCESSING....

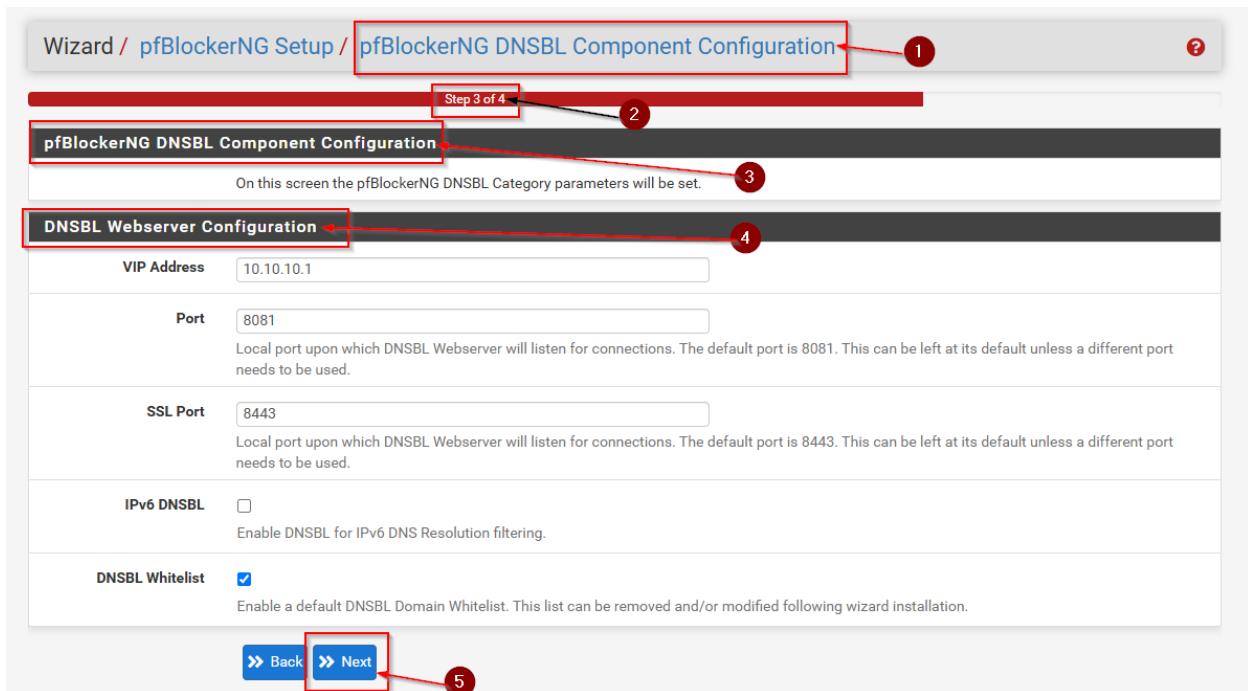


FIGURE 31 - LOOKING AROUND THE STEP 3 OF 4

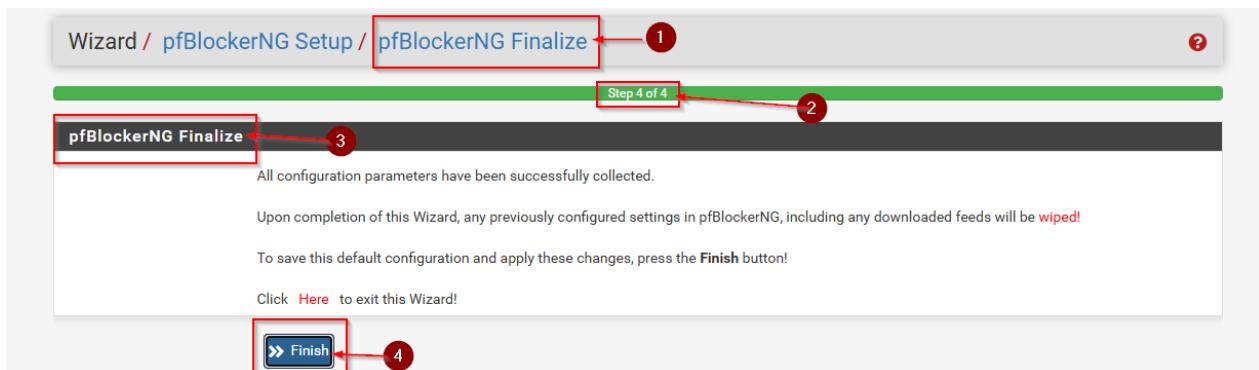


FIGURE 32 - FINISH THE PFBLOCKERNG FINALIZE

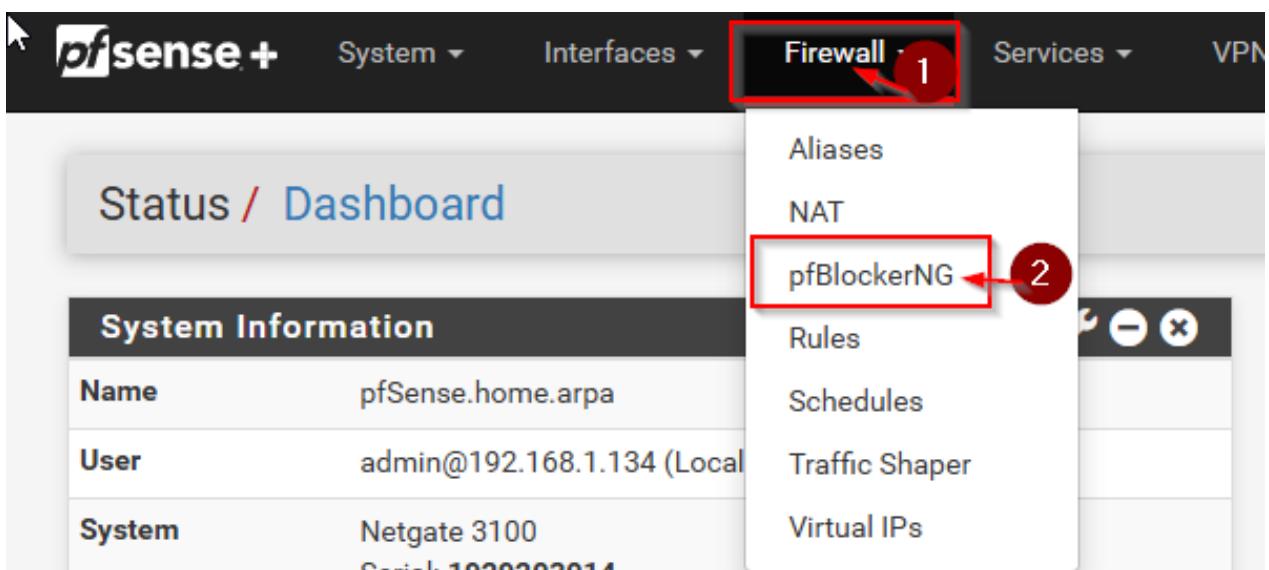


FIGURE 33 - OPEN FIREWALL THEN PFBLOCKERNG

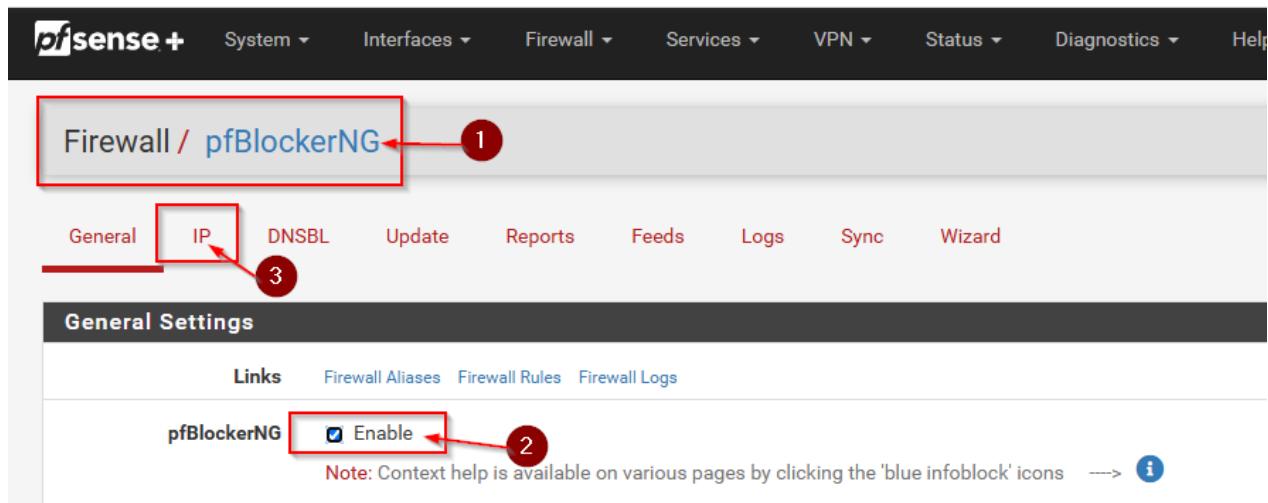


FIGURE 34 - ENABLE PFBLOCKERNG THEN CLICK IP

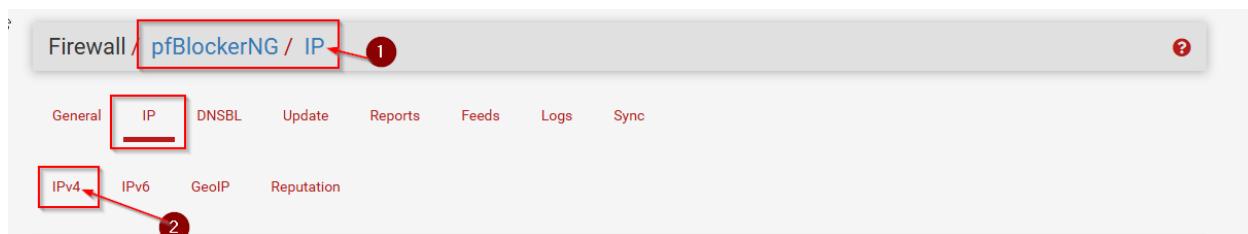


FIGURE 35 - CLICK IPv4

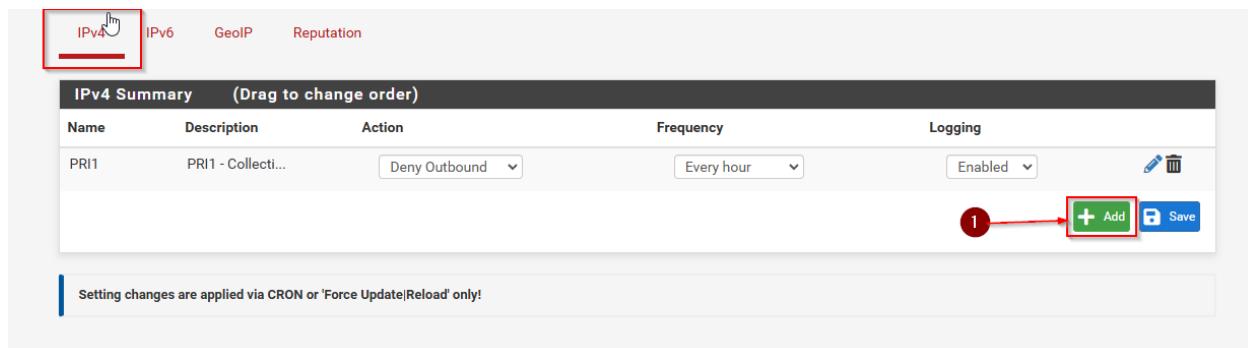


FIGURE 36 - CLICK "ADD"

IPv4 IPv6 GeoIP Reputation

Info

Links Firewall Aliases Firewall Rules Firewall Logs

Name / Description: **BlockWebsite**

Description: **Block any website**

Enter Name (Max 24 characters) and Description. i

FIGURE 37 - TYPE THE BLOCKWEBSITE AND DESCRIBE WHAT IT IS FOR

IPv4 IPv6 GeoIP Reputation

Info

Links Firewall Aliases Firewall Rules Firewall Logs

Name / Description: **BlockWebsite**

Description: **Block any website**

Enter Name (Max 24 characters) and Description. i

FIGURE 38 - TYPING...

IPv4 IPv6 GeoIP Reputation

Info

Links Firewall Aliases Firewall Rules Firewall Logs

Name / Description: **BlockWebsite**

Description: **Block any website**

Enter Name (Max 24 characters) and Description. i

Scroll down

FIGURE 39 - SCROLLING DOWN...

Settings

Action: Disabled

Default: Disabled
For Non-Alias type rules you must define the appropriate Firewall 'Auto' Rule Order option.
Click here for more info → [i](#)

Update Frequency: Never

Default: Never
Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.

Weekly (Day of Week): Monday

Default: Monday
Select the 'Weekly' (Day of the Week) to Update
This is only required for the 'Weekly' Frequency Selection. The 24 Hour Download 'Time' will be used.

Auto-Sort Header field: Enable auto-sort

Automatic sorting of the Header/Label field grouped by the Enabled/Disabled State field setting.

Enable Logging: Enabled

Default: Enable
Select - Logging to Status: System Logs: FIREWALL (Log)
This can be overridden by the 'Global Logging' Option in the General Tab.

States Removal: Enabled

With the 'Kill States' option (General Tab), you can disable States removal for this Alias.

Advanced Inbound Firewall Rule Settings

Advanced Outbound Firewall Rule Settings

Advanced Tuneables

IPv4 Custom_List 1

FIGURE 40 - CLICK IPv4 CUSTOM_LIST

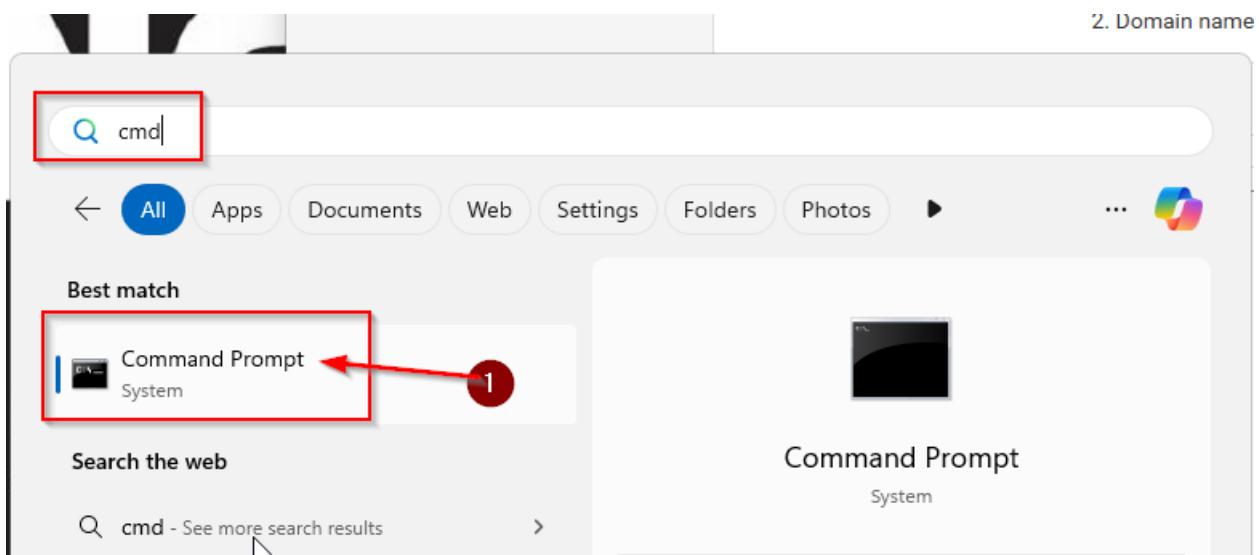


FIGURE 41 - BEFORE THAT, OPEN THE CMD

```
C:\ Command Prompt - nslookup X + ▾  
Microsoft Windows [Version 10.0.22631.4751]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\Student04>nslookup  
Default Server: pfSense.home.arpa  
Address: 192.168.1.1  
  
> |
```

FIGURE 42 - USING NSLOOKUP TO ASK THE ROUTER TO GET IP FROM IT

```
C:\Users\Student04>nslookup  
Default Server: pfSense.home.arpa  
Address: 192.168.1.1  
  
> lollipop.org 1  
Server: pfSense.home.arpa  
Address: 192.168.1.1  
  
Name: lollipop.org 2  
Address: 10.10.10.1  
  
> |
```

FIGURE 43 - ASKING THE ROUTER TO SEND ME IP ADDRESS FROM THE LOLLUPOP.ORG WEBSITE

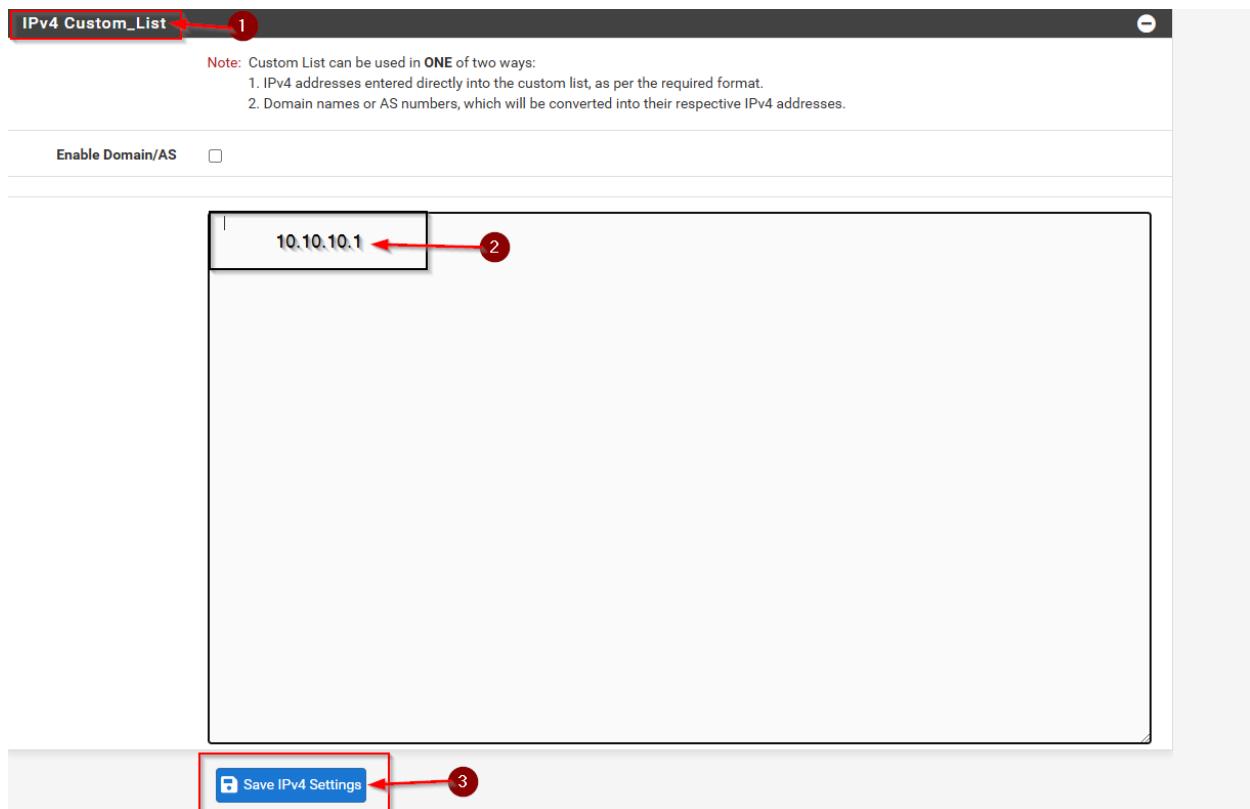


FIGURE 44 - PUTTING THE IP ADDRESS ON THE CUSTOM LIST

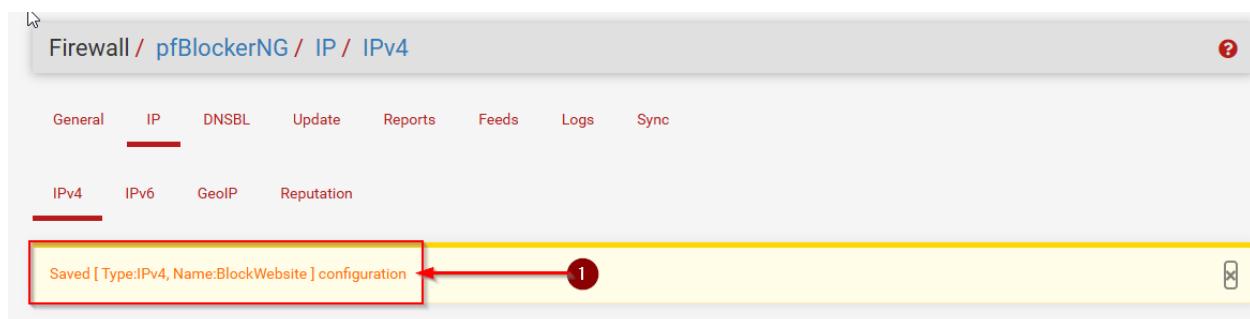


FIGURE 45 - SAVED IPV4 SETTING TO CONFIRM

```
C:\Users\Student06>nslookup  
Default Server: pfSense.home.arpa  
Address: 10.15.15.8  
  
> callofduty.com  
Server: pfSense.home.arpa  
Address: 10.15.15.8  
  
Non-authoritative answer:  
Name: callofduty.com  
Address: 23.45.193.225  
  
>
```

FIGURE 46 - USING NSLOOKUP TO ASK THE ROUTER TO GET IP ADDRESS FROM CALL OF DUTY WEBSITE

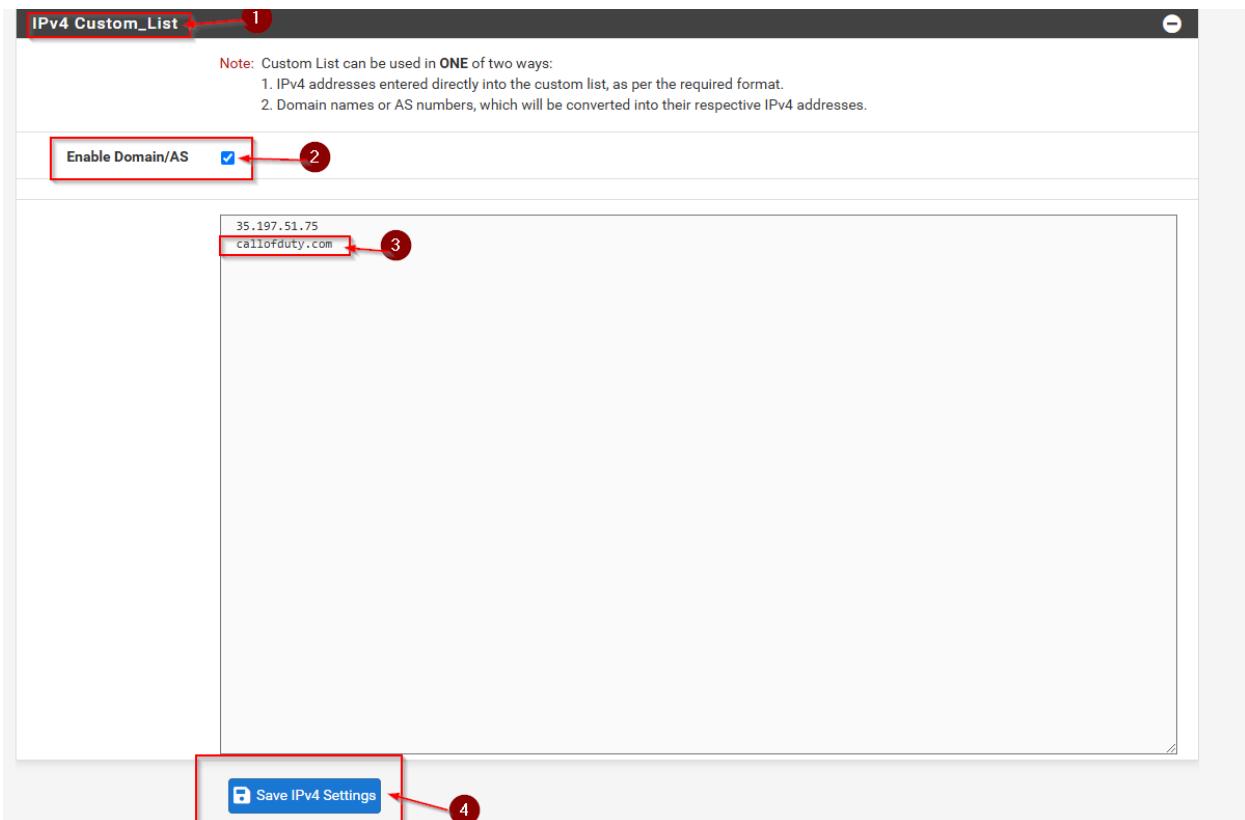


FIGURE 47 - ENABLE DOMAIN/AS AND PUT THE NAME OF WEBSITE ON IT



FIGURE 48 - CONFIRM THE IPv4 SETTING

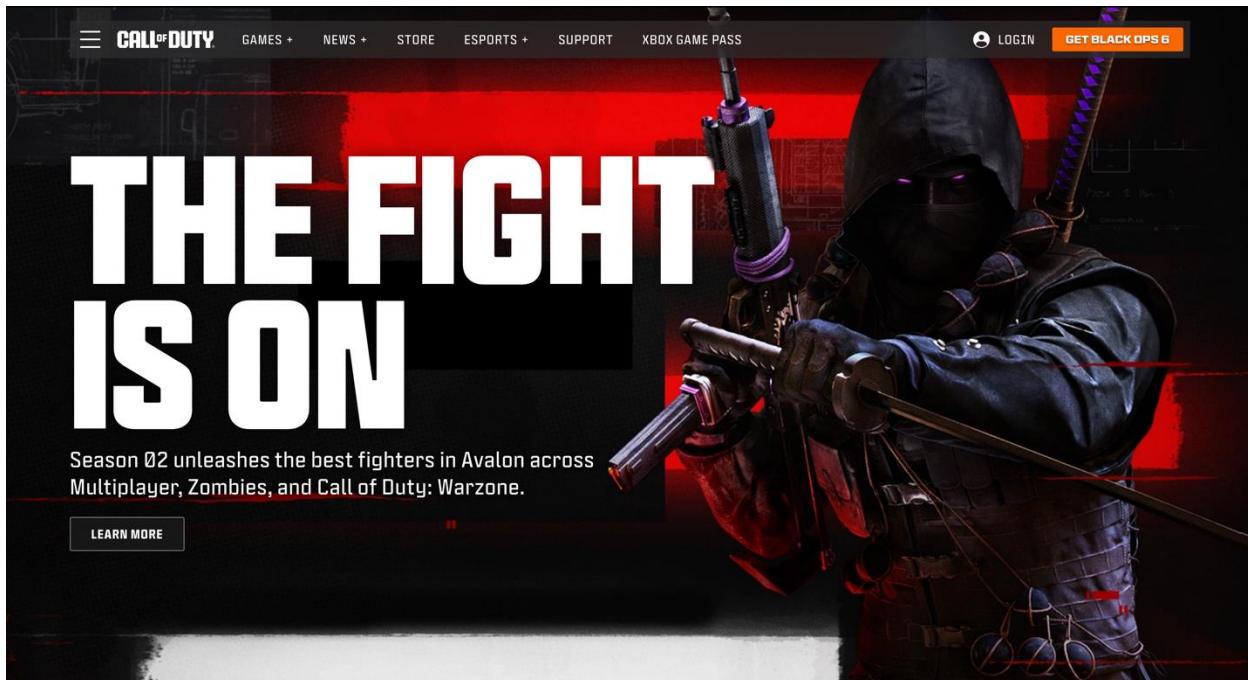


FIGURE 49 - CHECKING THE WEBSITES BEFORE IT GET BLOCKED

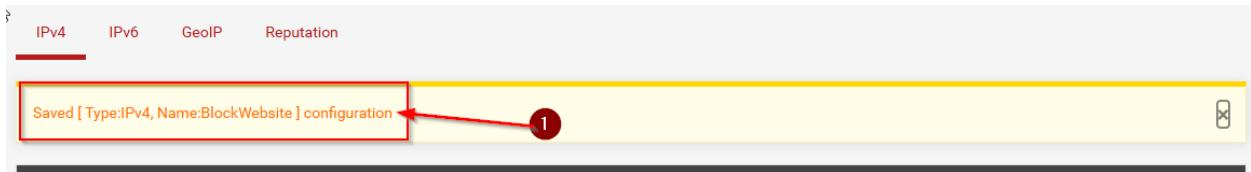


FIGURE 50 - SAVED THE IPv4 CONFIGURATION

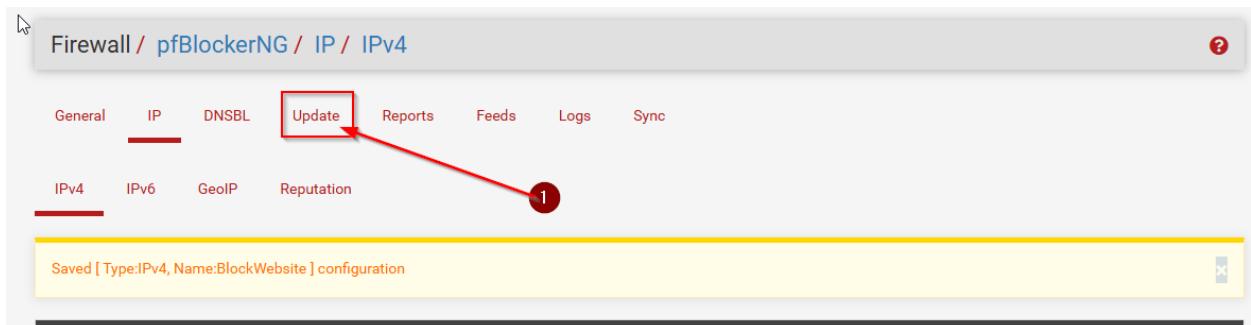


FIGURE 51 - CLICK UPDATE

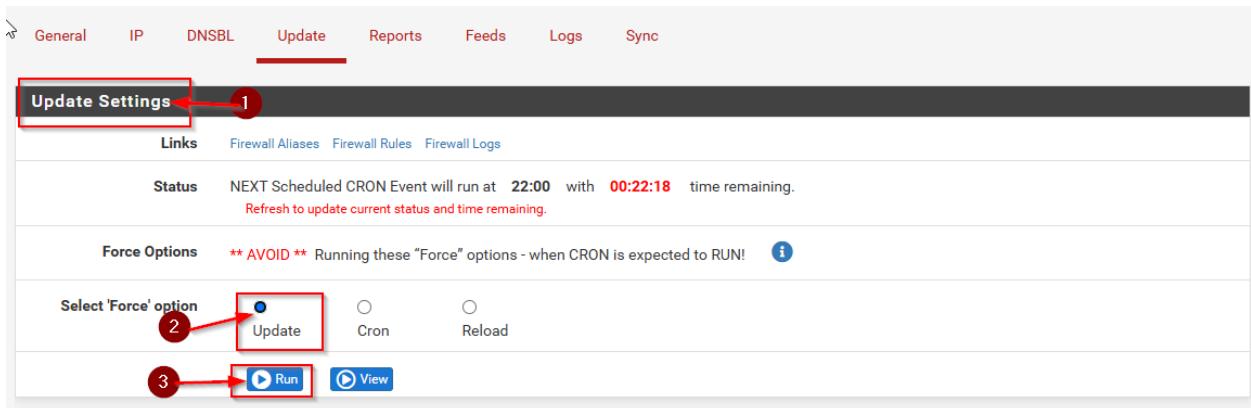


FIGURE 52 - RUN THE UPDATE STATUS

```

Log 1
Running Force Update Task

Feb 12 19:00 ISC_Block_v4
Feb 12 19:54 CINS_army_v4
Feb 12 20:55 Abuse_Feodo_C2_v4
Feb 12 21:07 Spamhaus_eDrop_v4

===== [ DNSBL Last Updated List Summary ] =====

Feb 5 22:00 StevenBlack_Abuse
Feb 5 23:55 BlockedSites_custom
=====

Database Sanity check [ PASSED ]
-----
Masterfile/Deny folder uniq check
Deny folder/Masterfile uniq check

Sync check (Pass=No IPs reported)
-----

Alias table IP Counts
-----
15899 /var/db/aliasables/pfB_PRI1_v4.txt

pfSense Table Stats
-----
table-entries hard limit 400000
Table Usage Count 15917
-----[2]
UPDATE PROCESS ENDED [ 02/12/25 21:38:27 ]

```

FIGURE 53 - COMPLETE THE UPDATE LOG

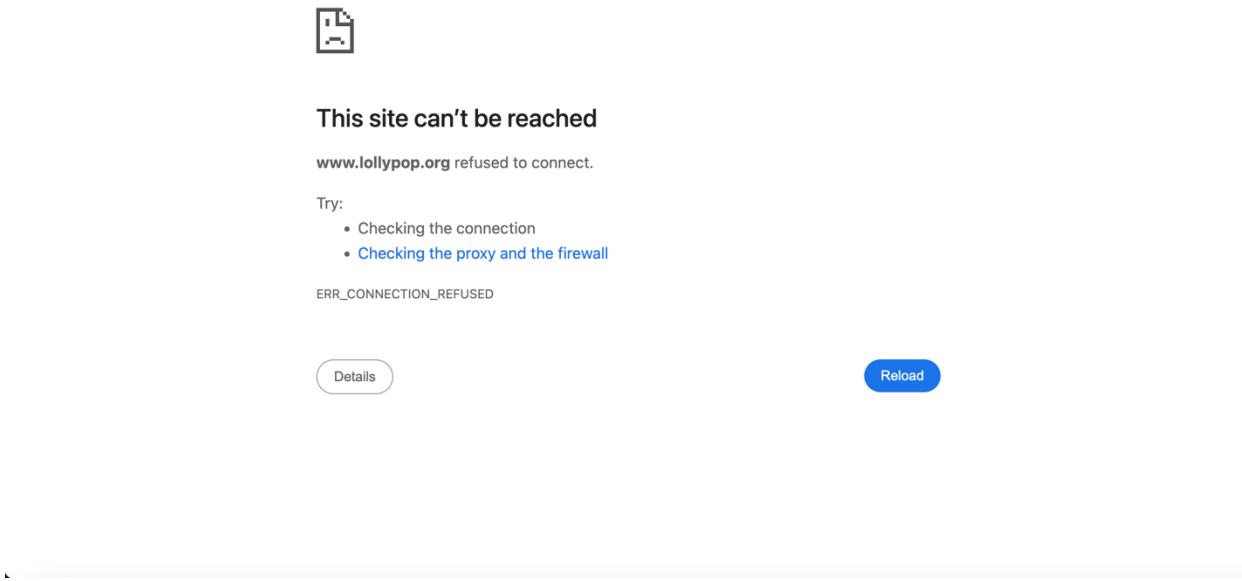


FIGURE 54 - LOLLYPOP IS BLOCKED NOW

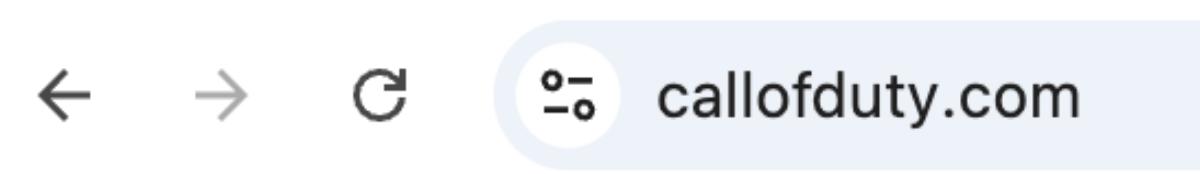


FIGURE 55 - TYPE THE CALL OF DUTY URL ON GOOGLE

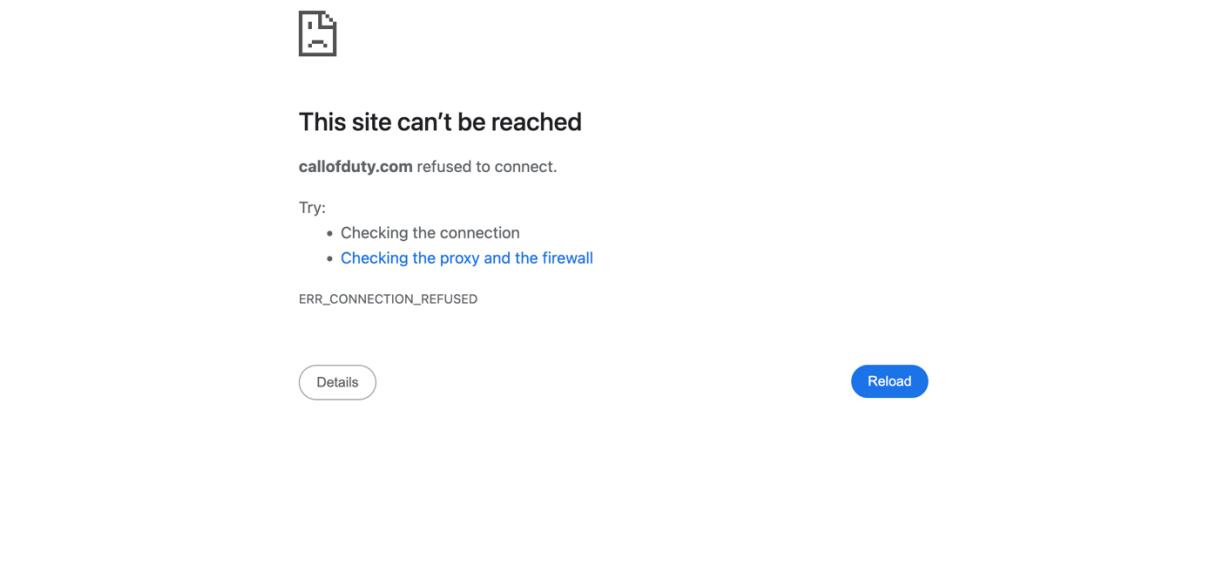


FIGURE 56 - CALL OF DUTY WEBSITE IS NOW BLOCKED

QUESTIONS AND ANSWERS

PART 2 –

1. Pick three different features that I like and describe each three features.
 - Please have look at #6 to #12 for the three features.
- General Setup
 - This feature is for configuring it as firewall and router for securing and managing network traffic.
- Package Manager
 - It allows you to easily install and manage additional software packages to extend its functionality.
- Routing
 - It involves setting up rules to determine how data packets are directed between different networks or subnets, ensuring proper communication across your network infrastructure.
2. Does the NetGate device have the firmware version? If not, what version do you have and what is the most recent version? Also, how do you upgrade?
 - Please have look at #13 to #18 for the upgrade.
 - For the old version before it became new, it was 23.05.1 old version. Now is the 23.09.1 new recent version of pfSense Router.
 - Yes, it has the firmware version.

PART 4 –

Please have look at #19 to #26 for installing pfBlockerNG.

PART 5 –

- In terms of product support, what do "End of Sales" (EOS) and "End-of-Life" (EOL) mean?

- End of Sales" (EOS) means the product is no longer available for purchase from the manufacturer, while "End-of-Life" (EOL) means the product will no longer receive updates, support, or maintenance from the manufacturer.
- Is there any EOS and/or EOL scheduled for your NetGate model?
- The Netgate SG-3100 has reached its End of Sale (EOS) and is approaching its End of Life (EOL). While the exact dates for these milestones are not publicly specified, but here is the reference link;

[The Netgate SG-3100](#)

OBSERVATIONS

At first of all, it was difficult to understand the concept of using WAN and LAN through the pfSense Router. But as time passed, I started to understand how it works. The Network diagram really helped me out.