

Project SunToWater Technologies

In this document we are going to explain how to create and configure a site-to-site VPN.

We begin by deploying two PfSense and two windows 10 machines, in this case a machine from SunToWater and other from GlobeX, two machines separated by many miles away.

```
Pfsense 1 (BaseLine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a96694f1c6b8b678996b

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.17/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

Enter an option:

9) pfTop

Pfsense 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 833848aff3e2e5723962

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

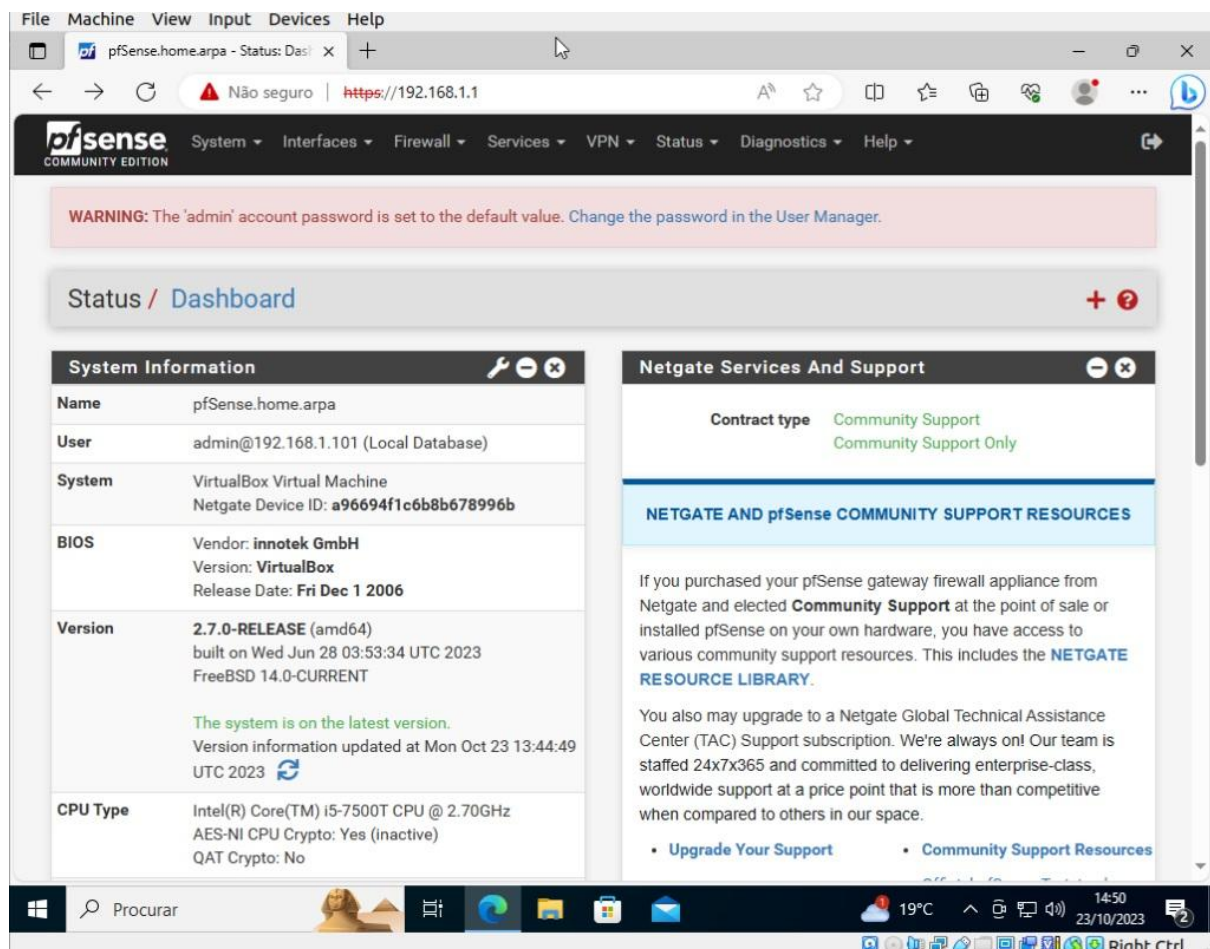
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.9/24
LAN (lan)      -> em1      -> v4: 192.168.2.1/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

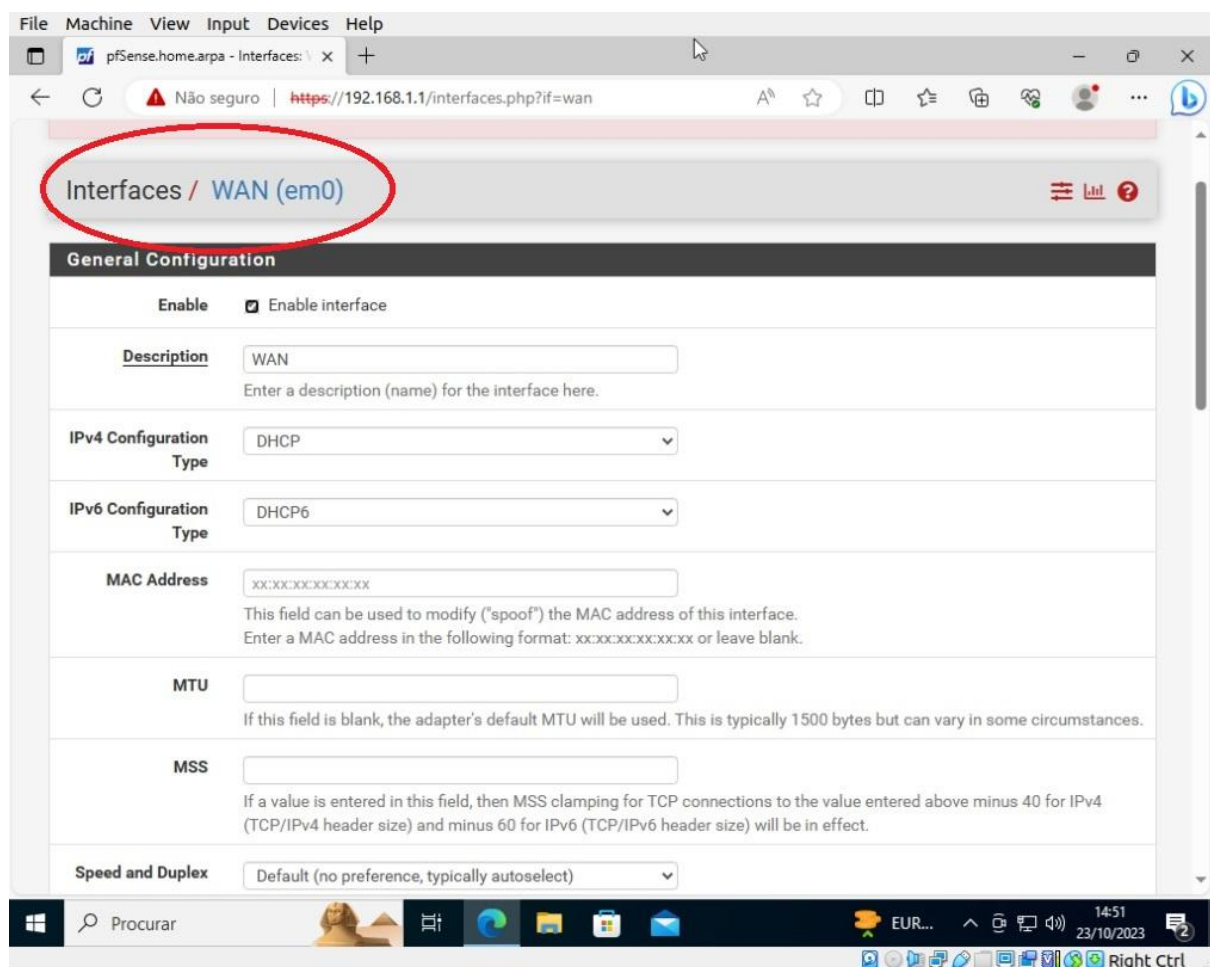
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option:
```

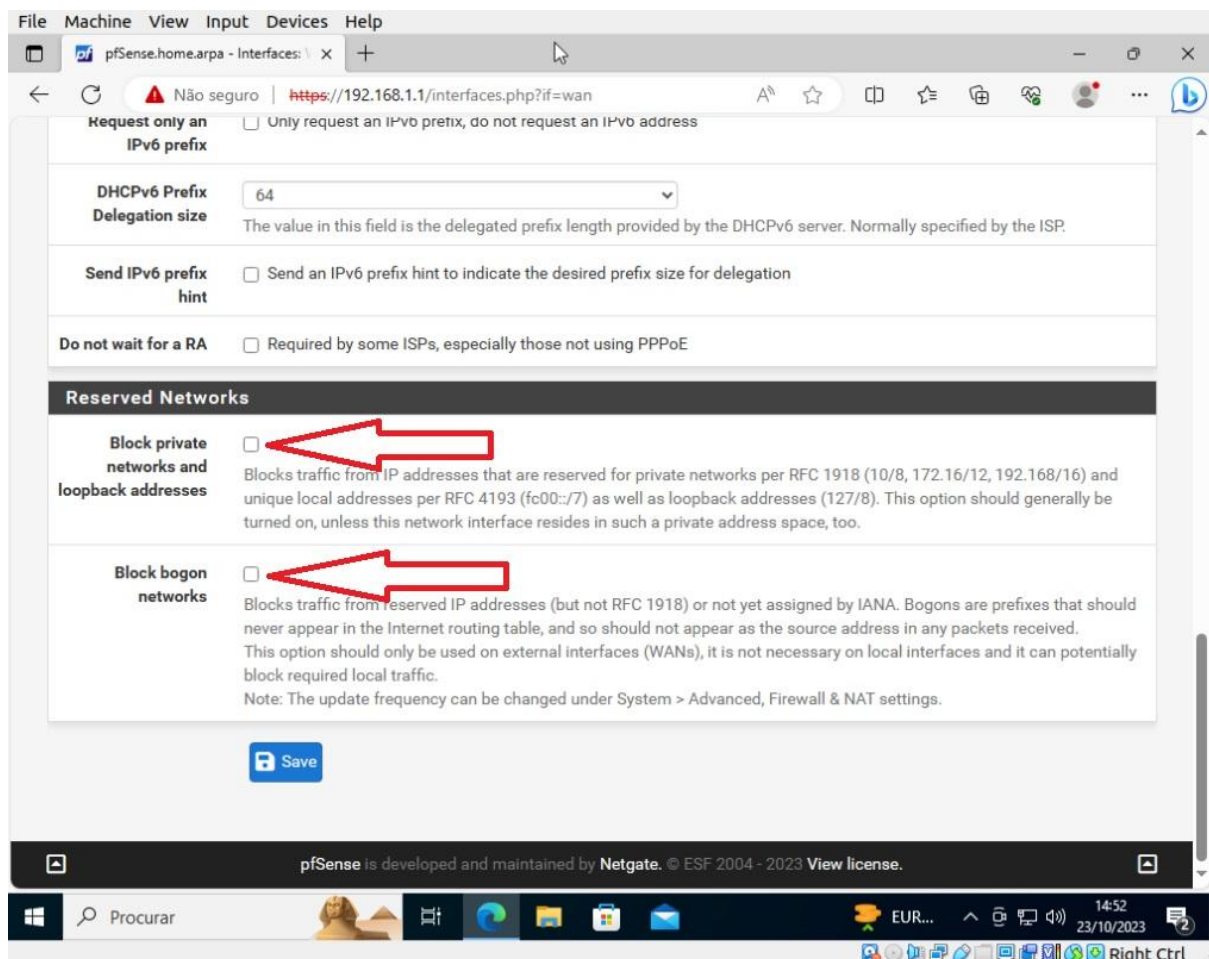
Next step is to configure each PfSense in order to accomplished the Site to site vpn. Open the PfSense Web configuration by using the Lan IP. **These steps must be made in both PfSenses (the ip address of the web configurator will be different)**



Next we need to enter “Interfaces” and choose “WAN”

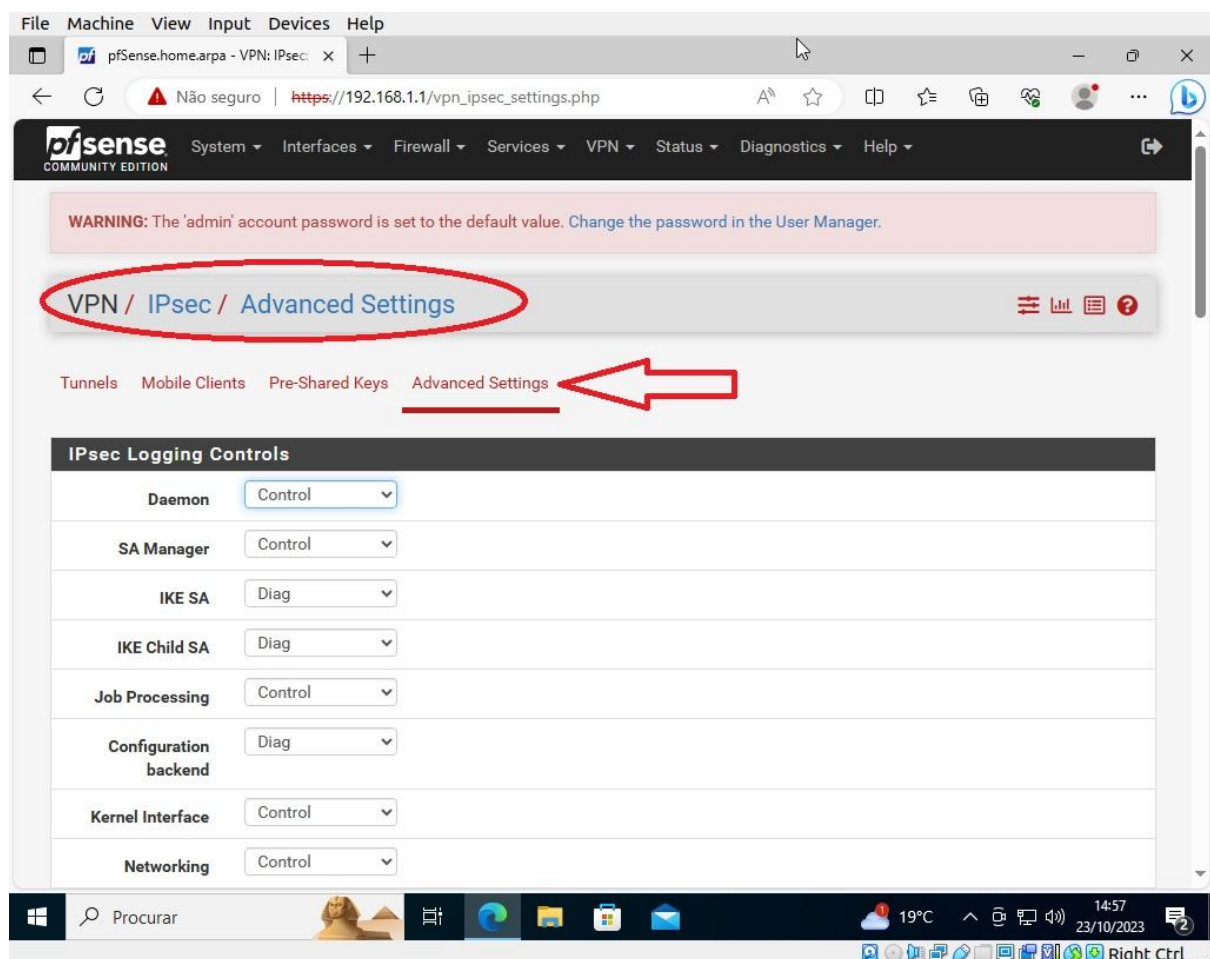


And in the same page uncheck “Block private networks and loopback addresses” and “Block bogon networks”

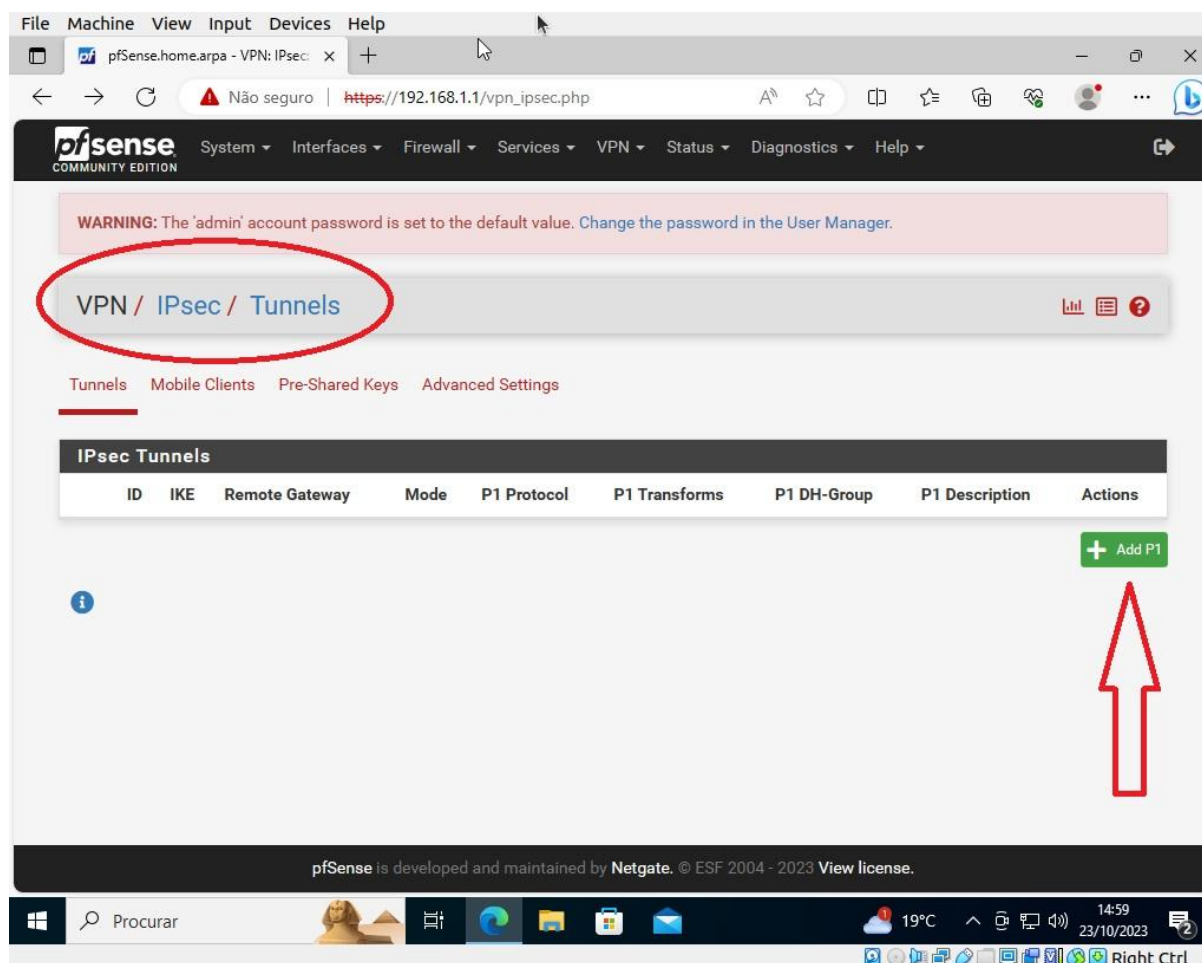


Next we are going to “VPN” in the top menu, next “IPsec” and choose “Advanced Settings”.

In these settings IKE SA should be “Diag”, IKE Child SA should be “Diag” and configuration backend should be “Diag”, everything else must be “Control”.



Next we are going to choose “Tunnels” option and click on the green button “+ Add P1”. In this phase we are going to create a tunnel.



In these steps we have to make sure that every option is ok.

Make a Description.

Set the Remote Gateway to the other PfSense WAN IP.

TIP: While configuring the other Pfsense the WAN Ip will be the other way around.

Authentication Method: "Mutual PSK"

File Machine View Input Devices Help

pfSense.home.arpa - VPN: IPsec: x

Não seguro | https://192.168.1.1/vpn_ipsec_phase1.php

Description Sun1 Phase1
A description may be entered here for administrative reference (not parsed).

Disabled ☐ Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration

Key Exchange version IKEv2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol IPv4
Select the Internet Protocol family.

Interface WAN
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway 10.0.2.9
Enter the public IP address or host name of the remote gateway. ⓘ

Phase 1 Proposal (Authentication)

Authentication Method Mutual PSK
Must match the setting chosen on the remote side.

My identifier My IP address

Peer identifier Peer IP address

Procurar

19°C 15:02 23/10/2023

Right Ctrl

In the same page we will encounter more configurations.

After the Authentication Method, we have to Generate a new pre-shared Key, this key will be the same in both PfSenses.

Encryption Algorithm will be “AES” with “256 bits” and “SHA256”

Life Time: “28800”

The screenshot displays the pfSense web interface for configuring a VPN Phase 1 Proposal. The browser address bar shows the URL `https://192.168.1.1/vpn_ipsec_phase1.php`. The page is divided into three main sections: Authentication, Encryption Algorithm, and Expiration and Replacement. Red circles and an arrow highlight specific configuration fields.

Phase 1 Proposal (Authentication)

- Authentication Method:** Mutual PSK (circled in red)
- My identifier:** My IP address
- Peer identifier:** Peer IP address
- Pre-Shared Key:** ee04f64ce09e00cb154b99c9b29286b3b7b52323c77bd9 (circled in red, with a red arrow pointing to it)

Phase 1 Proposal (Encryption Algorithm)

- Encryption Algorithm:** AES (circled in red)
- Key length:** 256 bits (circled in red)
- Hash:** SHA256 (circled in red)
- DH Group:** 14 (2048 bit)

Expiration and Replacement

- Life Time:** 28800 (circled in red)

The Windows taskbar at the bottom shows the system time as 15:05 on 23/10/2023, with a temperature of 19°C.

Then we must Save configurations and enter “Phase 2”

File Machine View Input Devices Help

pfSense.home.arpa - VPN: IPsec

Não seguro | https://192.168.1.1/vpn_ipsec.php

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The changes have been applied successfully.

IPsec Tunnels

	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 10.0.2.9		AES (256 bits)	SHA256	14 (2048 bit)	Sun1 Phase1	

[+ Show Phase 2 Entries \(0\)](#)

[+ Add P1](#) [Delete P1s](#)

Windows taskbar: Procurar, 19°C, 15:08, 23/10/2023, Right Ctrl

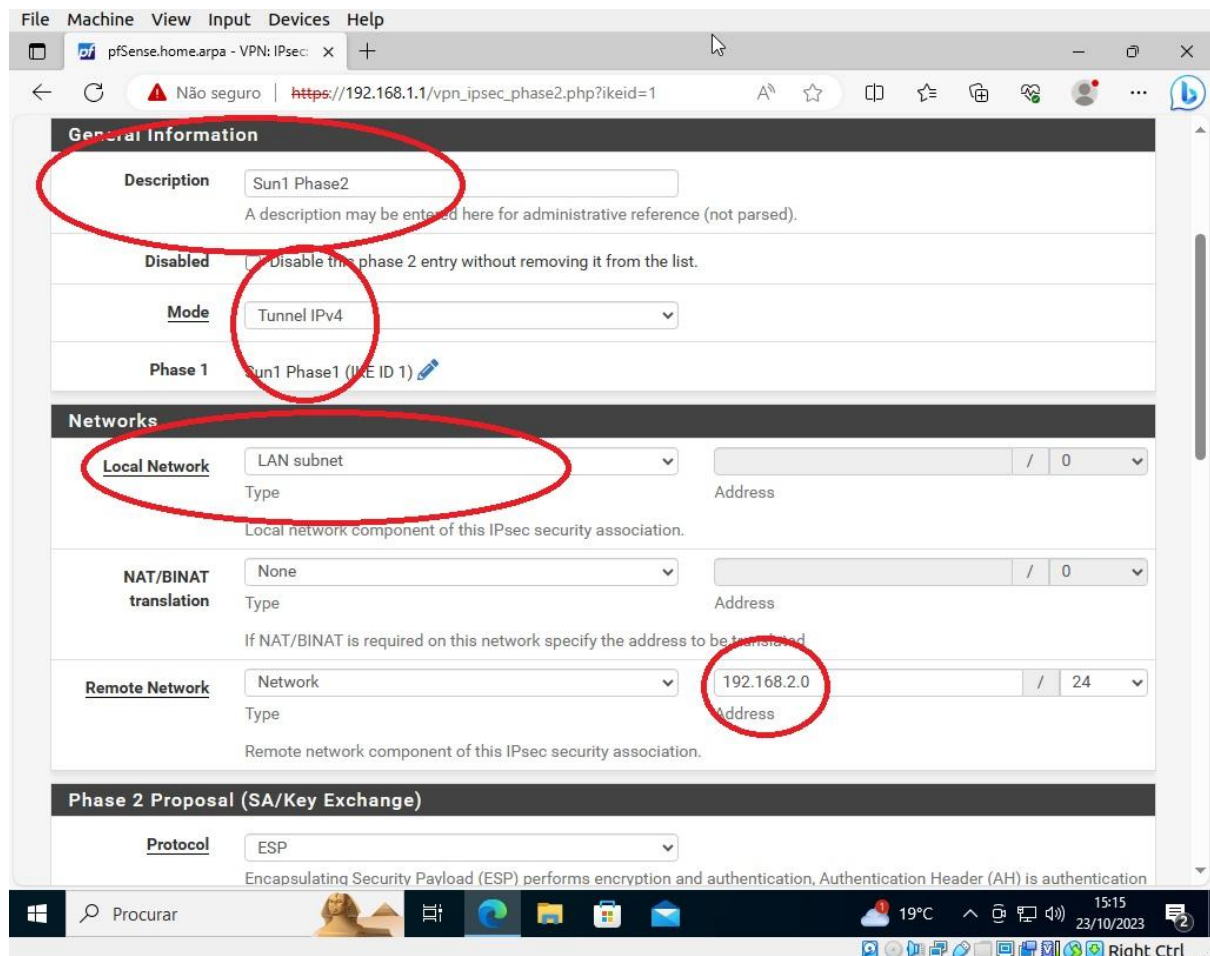
In this configuration we are going to:

Make a “Description”, then:

Verify if “Mode” is on Tunnel IPv4, check:

If “Local Network” is on Lan subnet and:

Remote Network: Network - (the IP address must be the network of the Lan of the other Pfsense).



The screenshot shows the pfSense web interface for configuring an IPsec Phase 2 proposal. The browser address bar indicates the URL is https://192.168.1.1/vpn_ipsec_phase2.php?ikeid=1. The configuration is for a VPN named "Sun1 Phase2".

General Information

- Description:** Sun1 Phase2
- Disabled:** ☐ Disable this phase 2 entry without removing it from the list.
- Mode:** Tunnel IPv4
- Phase 1:** Sun1 Phase1 (IKE ID 1)

Networks

- Local Network:** LAN subnet
- NAT/BINAT translation:** None
- Remote Network:** Network, Address: 192.168.2.0 / 24

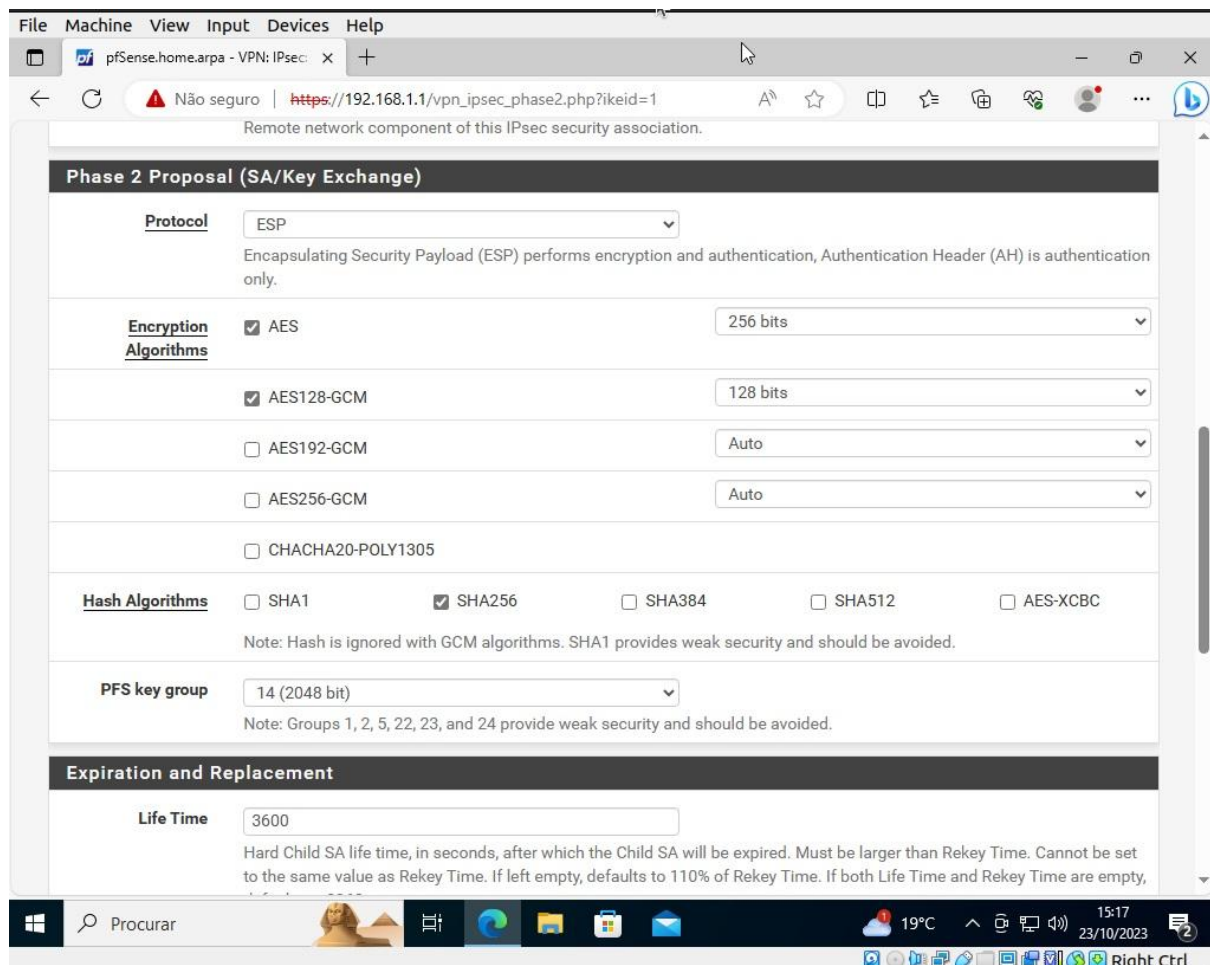
Phase 2 Proposal (SA/Key Exchange)

- Protocol:** ESP

The Windows taskbar at the bottom shows the date and time as 15:15 on 23/10/2023, and the system temperature as 19°C.

In the same page we need to check if:

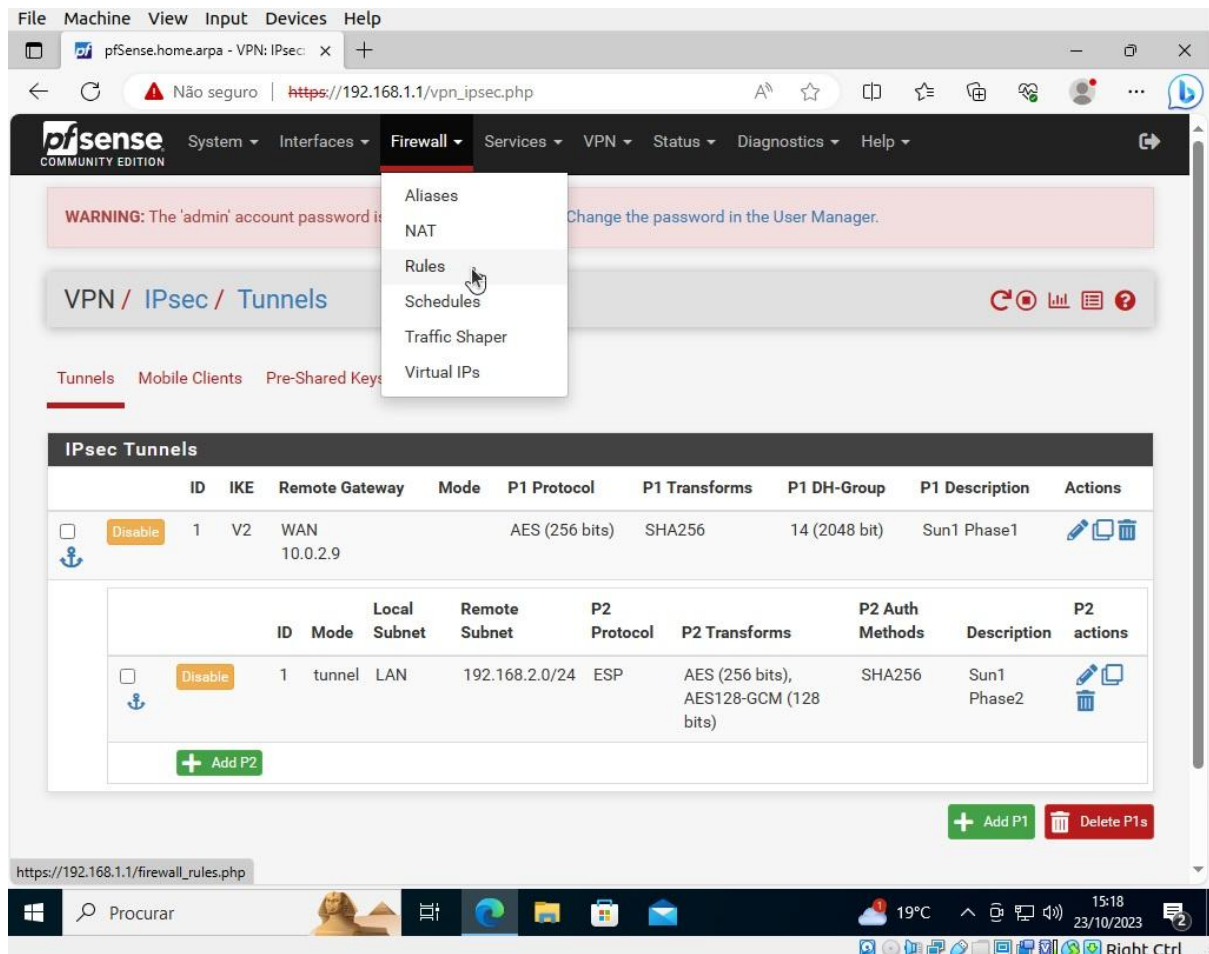
Protocol is on “ESP”, the on Encryption Algorithms “AES” is on 256 bits, the “PFS Key Group” is on 14 (2048 bit), and finally the “Life Time” on 3600.



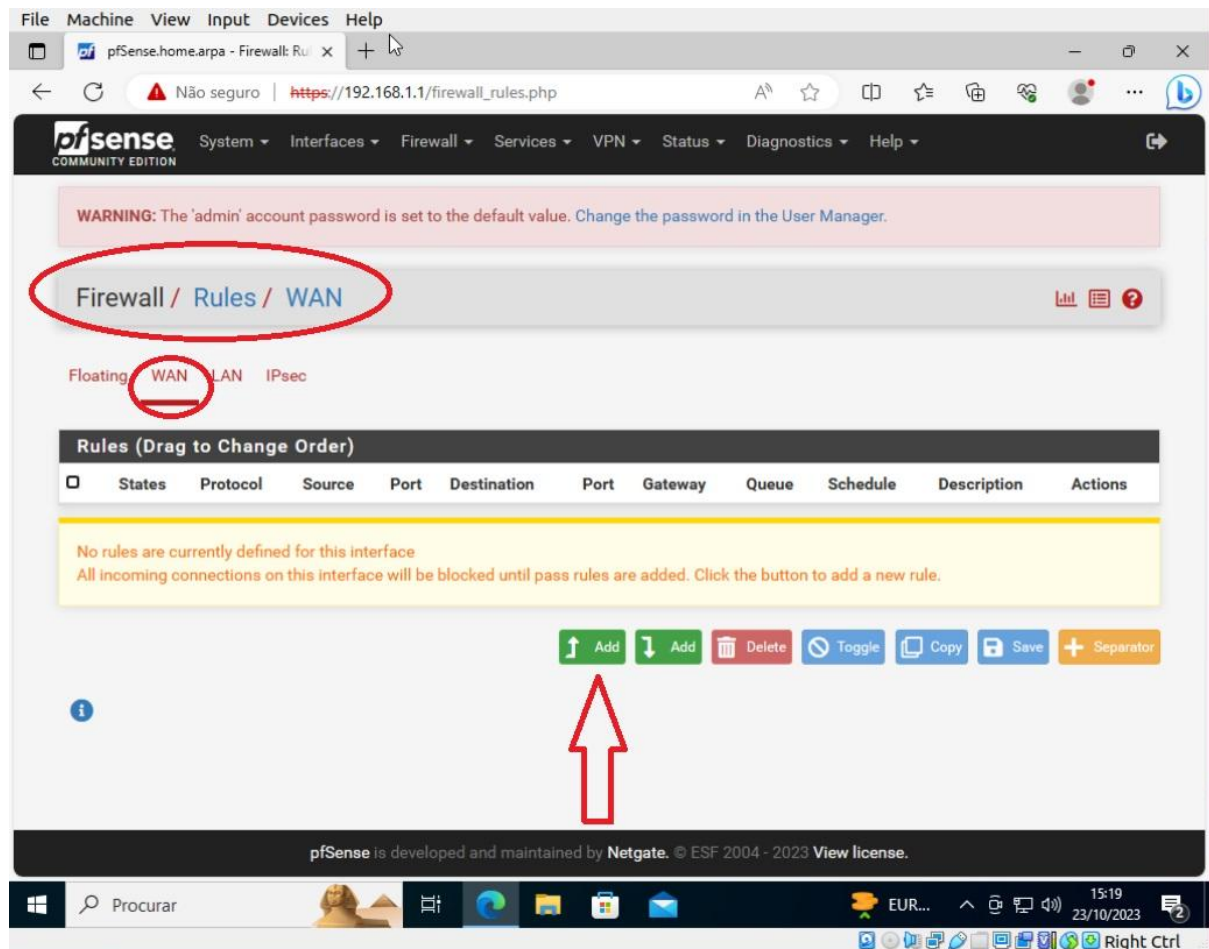
In the next step we must save these configurations and verify that were really saved.

After saving previously configurations we need to:

In top menu choose “Firewall”, then choose “Rules”.



In Rules menu we need to choose “WAN” and add a “rule”.



In this rule we have to make sure the following firewall rules are correct.

Action must be on “Pass”

Interface must be “Wan”

Protocol we have to choose “Any”

Source must be “Any”

Destination must be “Any”

The screenshot shows the 'Edit Firewall Rule' page in a web browser. The browser's address bar shows the URL `https://192.168.1.1/firewall_rules_edit.php?if=wan&after=-1`. The page has a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. The main content area is titled 'Edit Firewall Rule' and contains several sections:

- Action:** A dropdown menu set to 'Pass'. Below it is a hint: 'Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.'
- Disabled:** A checkbox labeled 'Disable this rule' is unchecked. Below it is the text: 'Set this option to disable this rule without removing it from the list.'
- Interface:** A dropdown menu set to 'WAN'. Below it is the text: 'Choose the interface from which packets must come to match this rule.'
- Address Family:** A dropdown menu set to 'IPv4'. Below it is the text: 'Select the Internet Protocol version this rule applies to.'
- Protocol:** A dropdown menu set to 'Any'. Below it is the text: 'Choose which IP protocol this rule should match.'
- Source:** A section with a checkbox 'Invert match' (unchecked) and a dropdown menu set to 'any'. To the right is a 'Source Address' field with a slash and a dropdown arrow.
- Destination:** A section with a checkbox 'Invert match' (unchecked) and a dropdown menu set to 'any'. To the right is a 'Destination Address' field with a slash and a dropdown arrow.
- Extra Options:** A section at the bottom, currently empty.

The Windows taskbar at the bottom shows the search bar with 'Procurar', several application icons, and system tray information including '19°C', '15:21', and '23/10/2023'.

In Rules menu we need to choose **“IPSEC”** and add a “rule”.

In this rule we have to make sure the following firewall rules are correct.

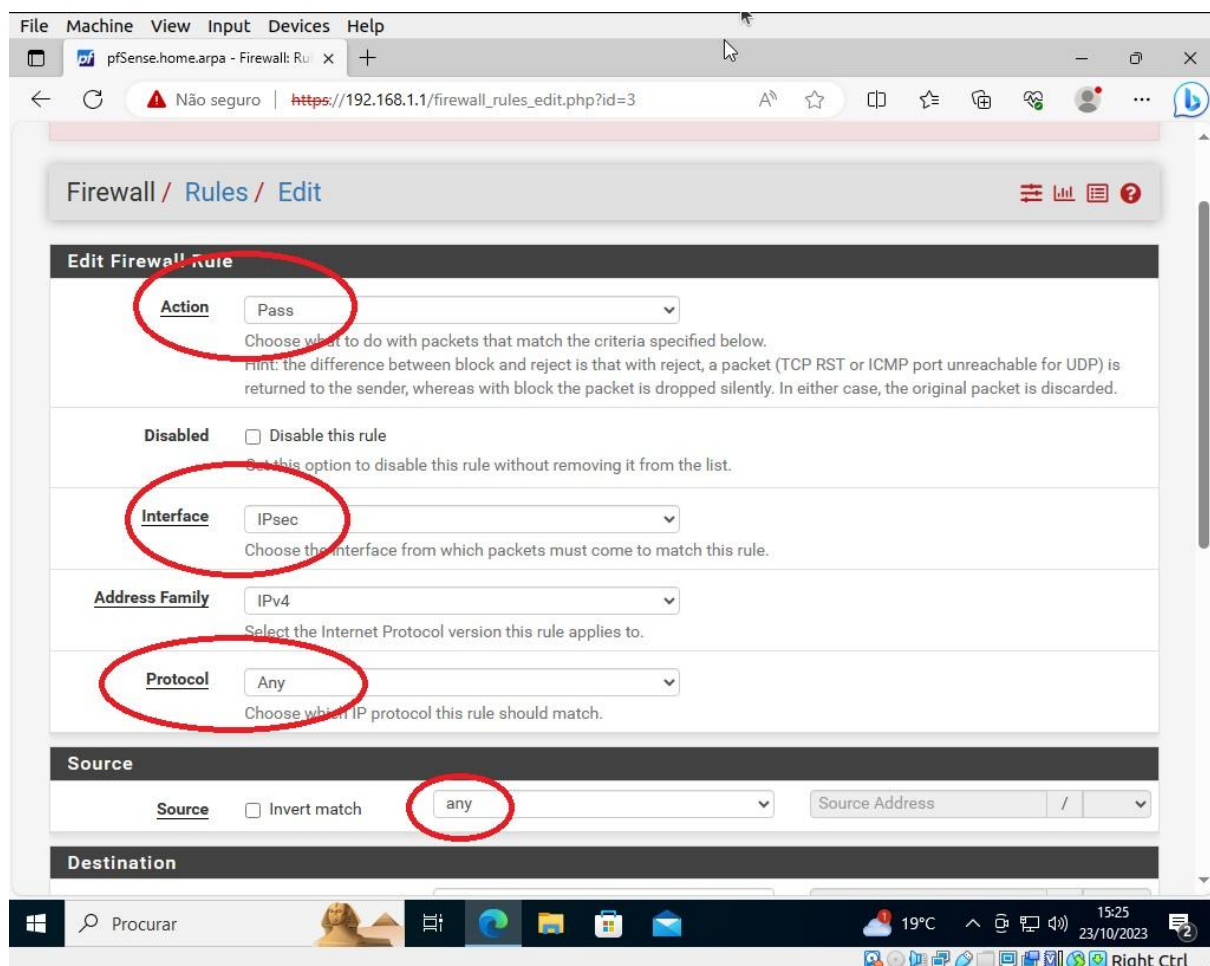
Action must be on “Pass”

Interface must be “IPsec”

Protocol we have to choose “Any”

Source must be “Any”

Destination must be “Any”

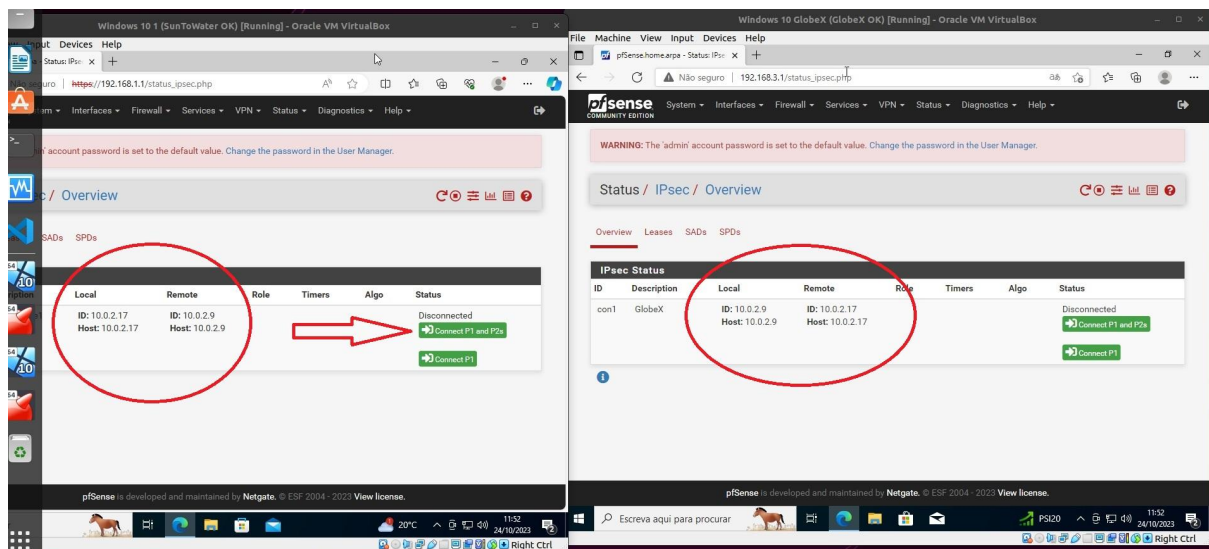


After saving these configurations we are ready to make the Tunnel work.

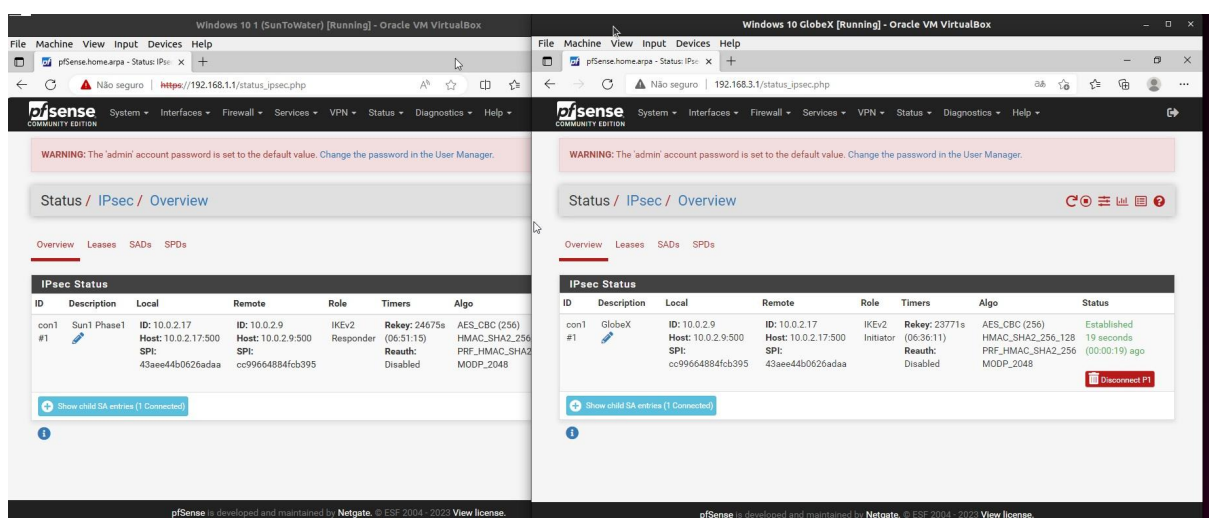
Next step we have to connect the VPN Tunnel by:

On top menu choose “Status”, then “IPsec”.

Make sure the IP addresses are OK and click “Connect P1 and P2s”, you only need to press this button only in one machine. If the Tunnel is well configured it will connect automatically.

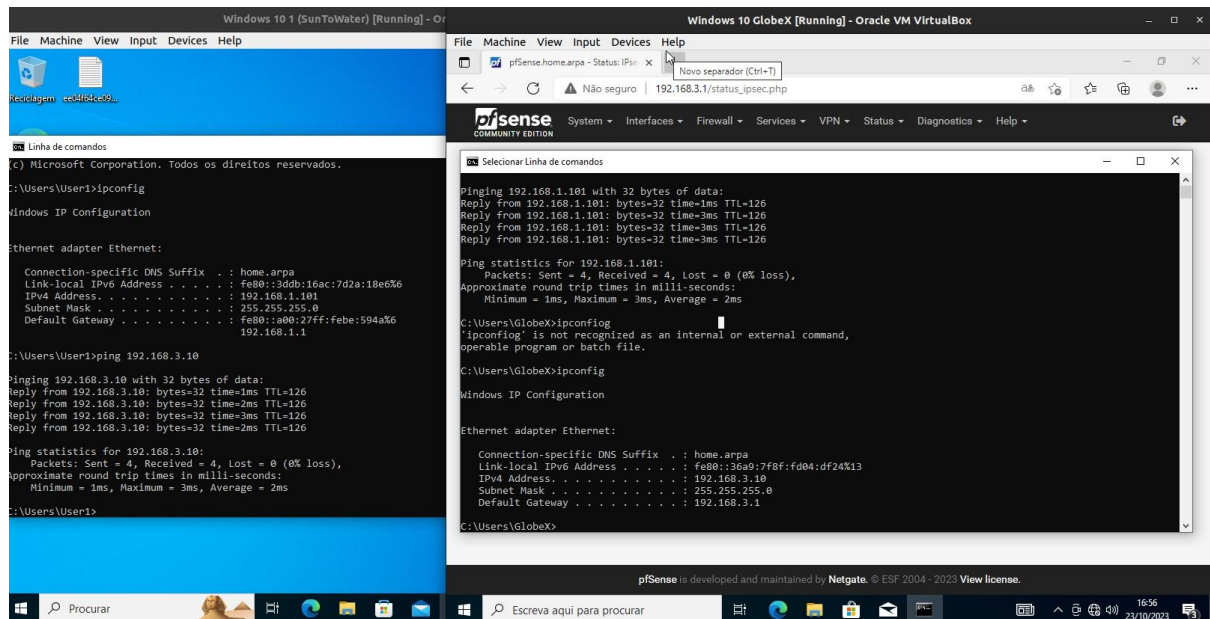


If everything was correct, congratulations we have a tunnel.

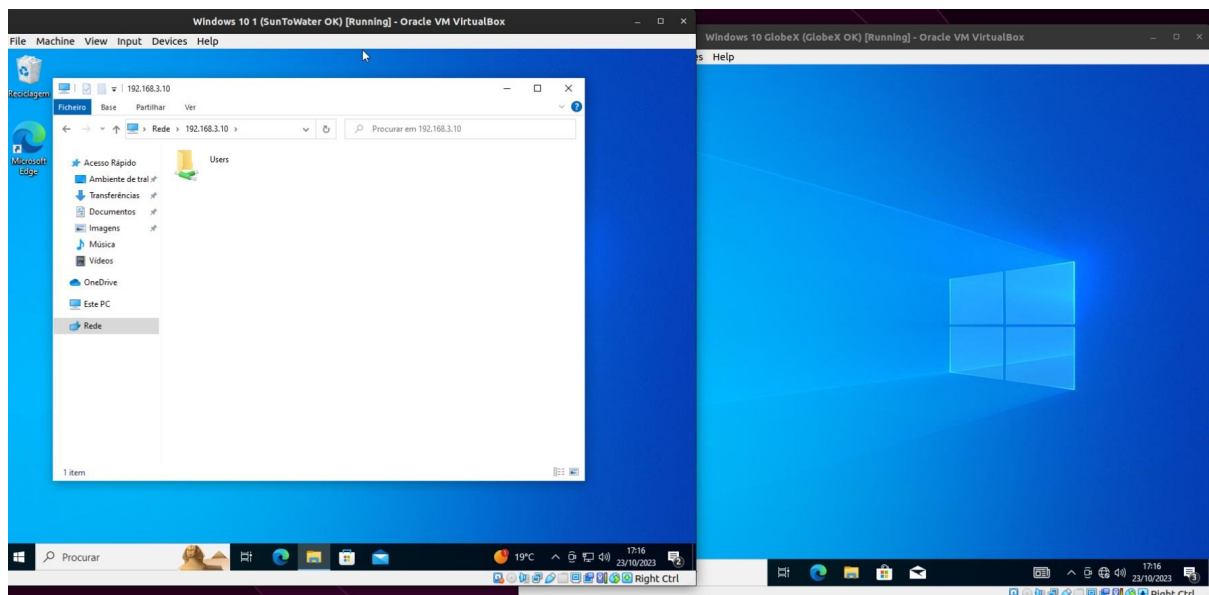


With the tunnel working we have to verify if two machines can communicate with each other. We can check this by a command in “cmd”, ping each other IP’s.

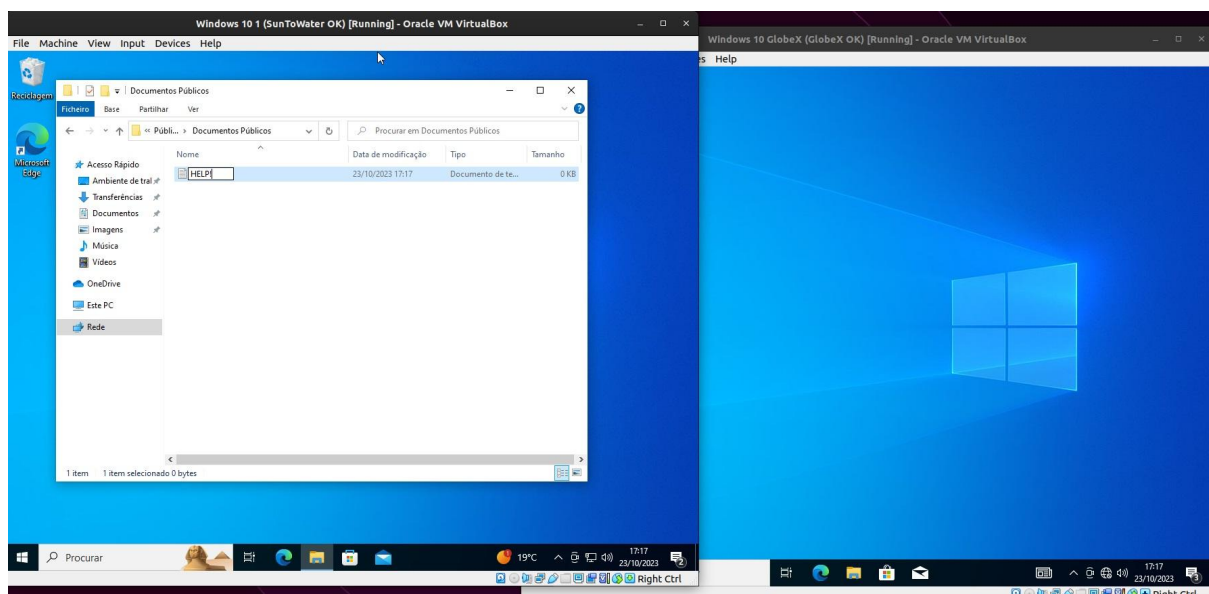
If everything is ok we should get a reply from the other machine.



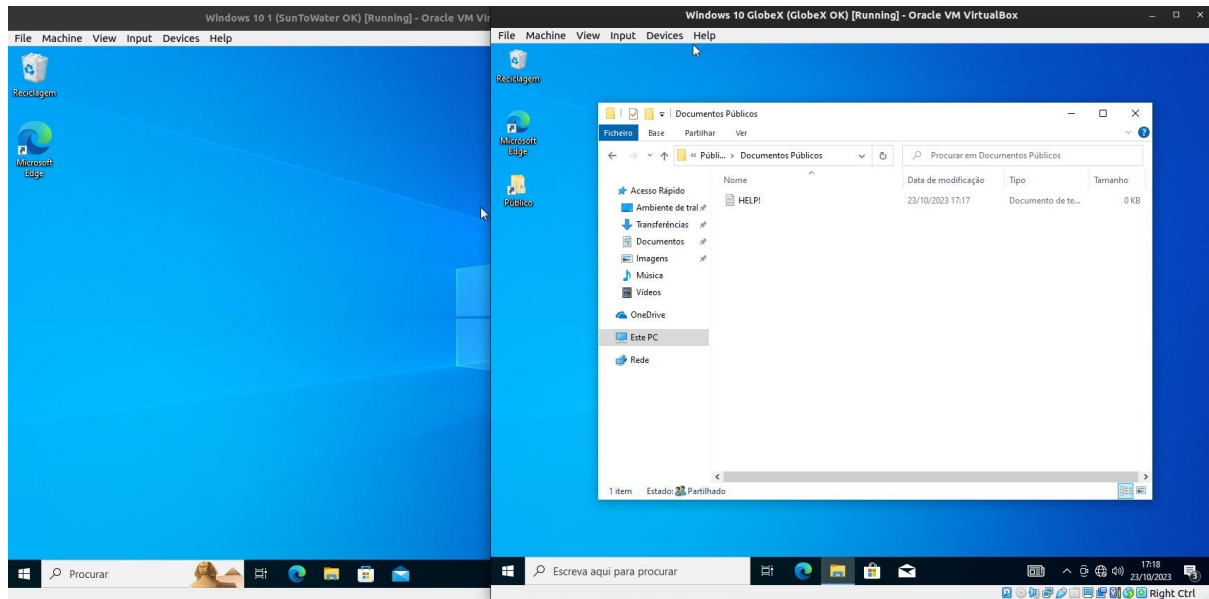
With the two machines working we must access each other folders.



With this done we can create, modify, and copy shared data.



And in the other end, check if it was really created and simply verify the files.



The End!