



NullSec

YOUR SHIELD IN THE DIGITAL BATTLE

A new horizon to SunToWater.

Project Report to SunToWater co.

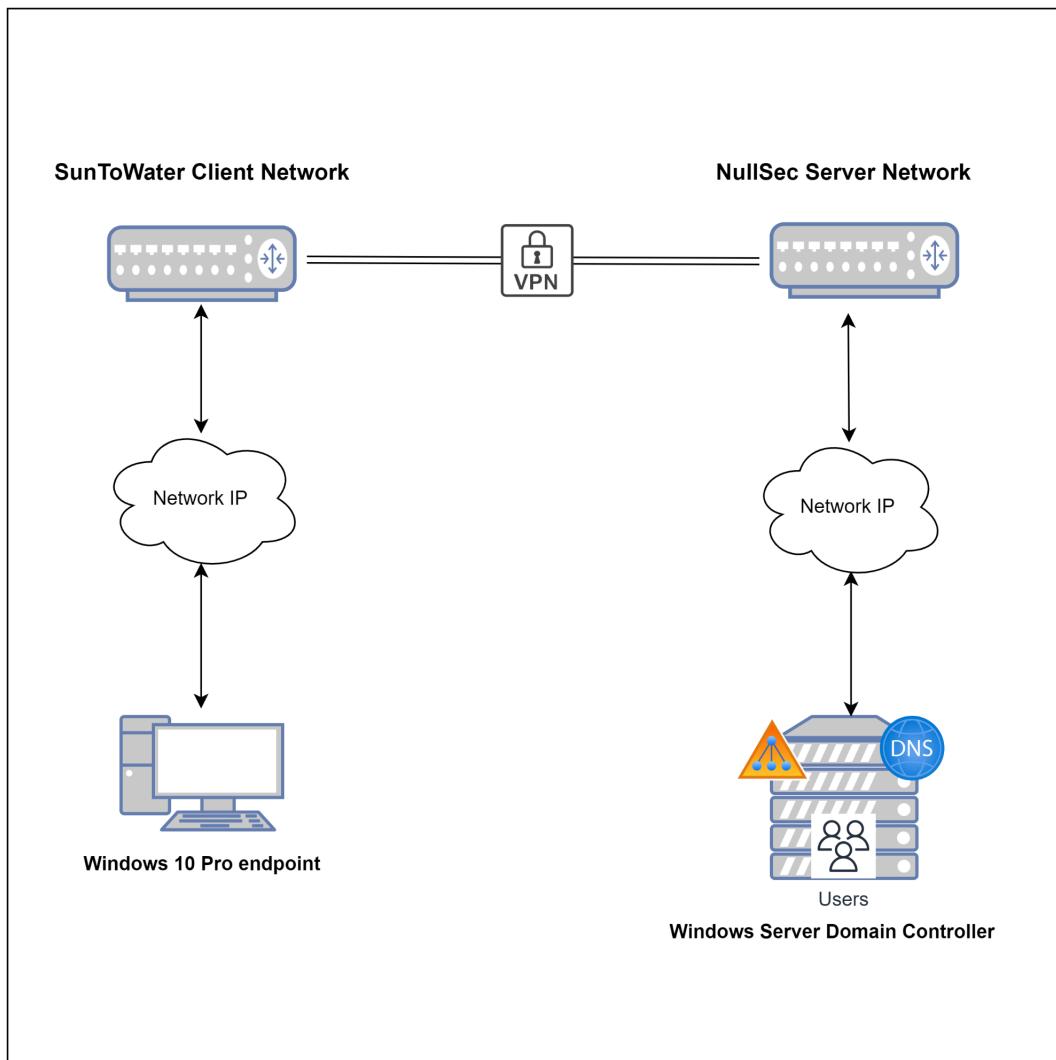
Abstract

In this project, the NullSec team successfully implemented a site-to-site VPN tunnel connecting the SunToWater company network to our own infrastructure. Additionally, we deployed a RADIUS authentication server to enhance network security. Furthermore, we developed a PowerShell script capable of automating the setup process for a new installation of Windows Server, enabling the server to function as a domain controller with all requisite services operational.

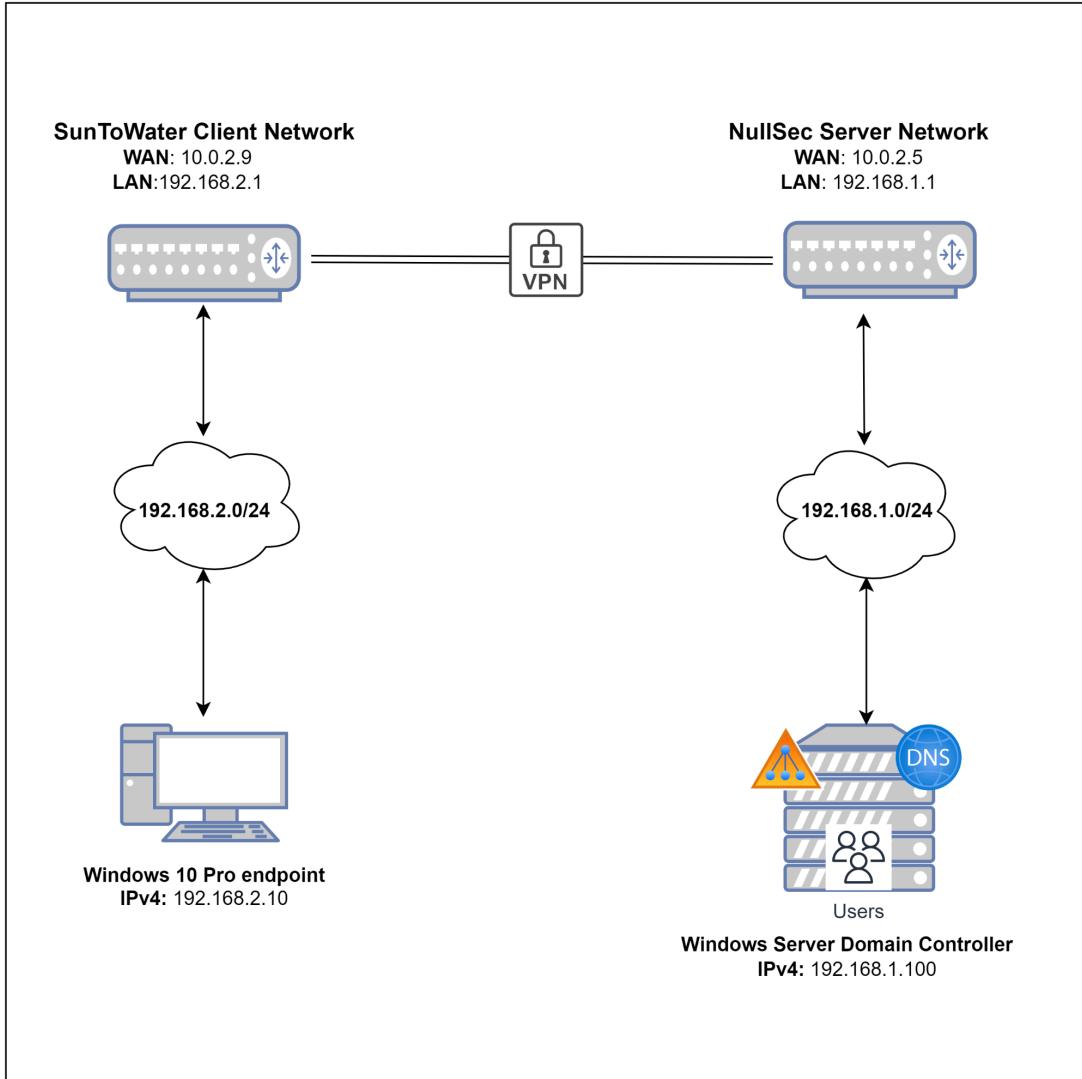
<https://www.securew2.com/blog/configure-windows-server-2019>

Network Topology diagram

- Before



- After



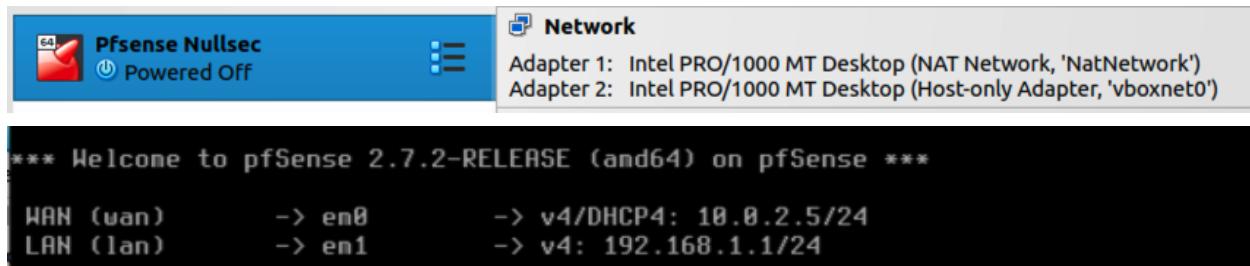
Implementation of Virtual Private Networking (VPN)

We have set up two environments in VirtualBox to simulate the **Nullsec** server and the **Sun To Water** client.

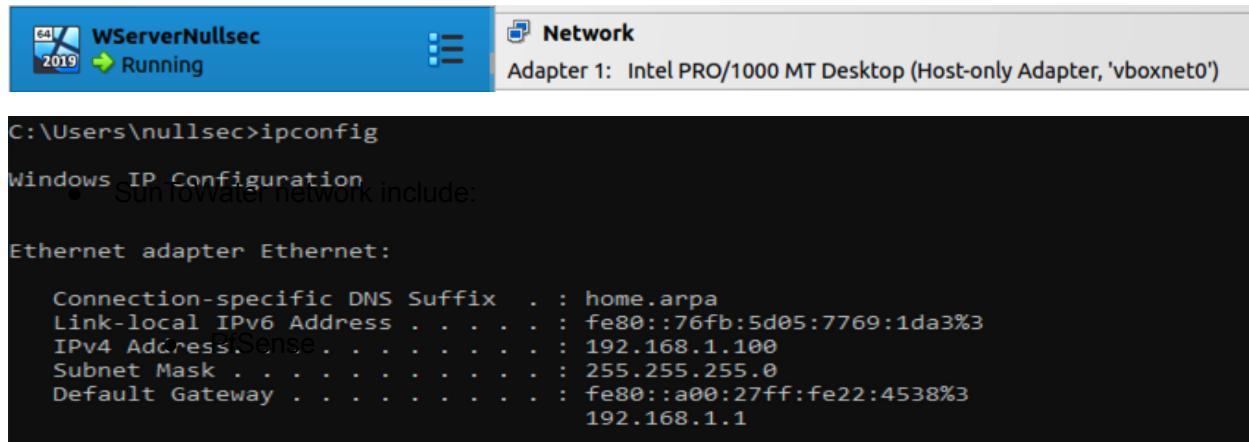
The **Nullsec** environment consists of a PfSense and a Windows Server, while the **Sun to Water** client contains a PfSense and a Windows 10. We modified the WAN of the PfSense on the client to place them on different networks.

Below, we provide screenshots of each VM and their respective networks and IPs.

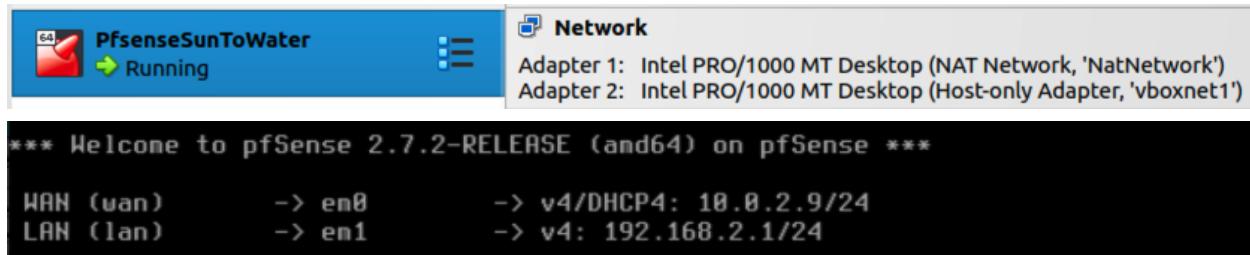
- **Nullsec** network include:
 - pfSense



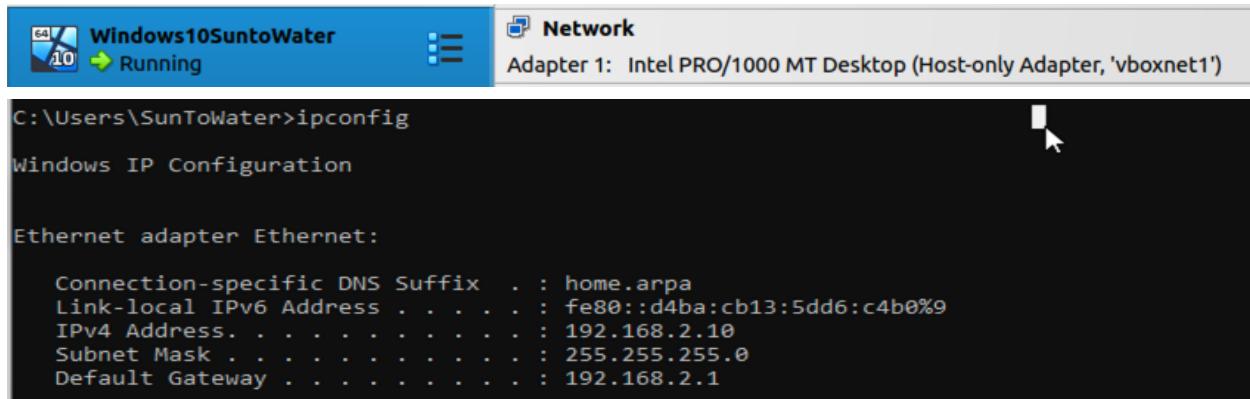
- Windows Server Domain Controller



- **Sun To Water** network include:
 - pfSense



- Windows 10 Endpoint



Configuring pfSense

Preliminary note: The Client's pfSense will have a white background, while the **Nullsec** will have a dark background.

Now, let's prepare the two pfSense devices to handle the VPN connection. We are enabling default blocking of private networks and Bogon networks to give the green light to pfSense routers to respond to pings on the WAN.

Pfsense Sun To Water

Reserved Networks	
Block private networks and loopback addresses	<input type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/> Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Pfsense Nullsec

Reserved Networks	
Block private networks and loopback addresses	<input checked="" type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input checked="" type="checkbox"/> Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

At this stage, we configured the tunnel negotiations on both pfSense devices following these steps:

Navigate to VPN > IPsec and select the Advanced Settings tab.

Set IKE SA, IKE Child SA, and Configuration Backend to Diag.

PfSense Sun To Water

IPsec Logging Controls	
Daemon	Control
SA Manager	Control
IKE SA	Diag
IKE Child SA	Diag
Job Processing	Control
Configuration backend	Diag

Pfsense Nullsec

IPsec Logging Controls	
Daemon	Control
SA Manager	Control
IKE SA	Diag
IKE Child SA	Diag
Job Processing	Control
Configuration backend	Diag

We configured the following specifications on each pfSense for Phase 1

Phase 1

- Protocol: IKEv2
- Interface: WAN
- Remote Gateway: the WAN IPv4 address of the other router
- Method: Mutual PSK (Pre-Shared Key 1234)
- Encryption: AES 256-bit
- Lifetime: 28800 sec

For better visualization, prints on the page below.

Pfsense Sun to Water - Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Description	<input type="text" value="Phase1SunToWater"/>
A description may be entered here for administrative reference (not parsed).	
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE ID	1

IKE Endpoint Configuration

<u>Key Exchange</u>	<input type="text" value="IKEv2"/>
<u>version</u> Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.	
<u>Internet Protocol</u>	<input type="text" value="IPv4"/>
Select the Internet Protocol family.	
<u>Interface</u>	<input type="text" value="WAN"/>
Select the interface for the local endpoint of this phase1 entry.	
<u>Remote Gateway</u>	<input type="text" value="10.0.2.5"/>
Enter the public IP address or host name of the remote gateway. i	

Phase 1 Proposal (Authentication)

<u>Authentication Method</u>	<input type="text" value="Mutual PSK"/>
Must match the setting chosen on the remote side.	
<u>My identifier</u>	<input type="text" value="My IP address"/>
<u>Peer identifier</u>	<input type="text" value="Peer IP address"/>
<u>Pre-Shared Key</u>	<input type="text" value="1234"/>
Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.	
Generate new Pre-Shared Key	

Phase 1 Proposal (Encryption Algorithm)

<u>Encryption Algorithm</u>	<input type="text" value="AES"/>	<input type="text" value="256 bits"/>	<input type="text" value="SHA256"/>	<input type="text" value="14 (2048 bit)"/>	Delete
Algorithm	Key length	Hash	DH Group		

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm [+ Add Algorithm](#)

Pfsense Nullsec - Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Description Phase1nullsec

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 ID 1

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. (i)

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

Pre-Shared Key 1234

Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

 Generate new Pre-Shared Key

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm	AES	Algorithm	256 bits	Key length	SHA256	Hash	14 (2048 bit)	DH Group	 Delete
-----------------------------	-----	-----------	----------	------------	--------	------	---------------	----------	--

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm  + Add Algorithm

Expiration and Replacement

Life Time 28800

For Phase 2, we followed the following steps on both pfSense devices:

Phase 2

- Mode: Tunnel IPv4
- Local Network: LAN subnet
- Remote Network: the the *subnet address* of the LAN on the other router
This is a subnet address address, e.g. 10.0.2.0/24, which is different from a gateway address such as 10.0.2.1
- Protocol: ESP
- Encryption: AES 256-bit
- PFS Key Group: 14 (2048 bit)
- Lifetime: 3600 sec

For better visualization, prints on the page below.

Pfsense Sun to Water - Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Description: Phase2SunToWater
A description may be entered here for administrative reference (not parsed).

Disabled: Disable this phase 2 entry without removing it from the list.

Mode: Tunnel IPv4

Phase 1: Phase1SunToWater (IKE ID 1)

Networks

Local Network: LAN subnet / 0
Type: Address
Local network component of this IPsec security association.

NAT/BINAT translation: None / 0
Type: Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Network / 24
Type: Address
Remote network component of this IPsec security association.

Phase 2 Proposal (SA/Key Exchange)

Protocol: ESP
Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Encryption Algorithms:
 AES (256 bits)
 AES128-GCM (128 bits)
 AES192-GCM (Auto)
 AES256-GCM (Auto)
 CHACHA20-POLY1305

Hash Algorithms:
 SHA1 SHA256 SHA384 SHA512 AES-XCBC
Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group: 14 (2048 bit)
Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Expiration and Replacement

Life Time: 3600

IPsec Tunnels											
	Remote Gateway		Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions			
	ID	IKE									
<input type="checkbox"/>	Disable	1	V2	WAN 10.0.2.5	Mutual PSK -	AES (256 bits)	SHA256	14 (2048 bit)	Phase1SunToWater	  	
	<input type="checkbox"/>	Disable	1	tunnel	LAN	192.168.1.0/24	ESP	AES (256 bits), AES128-GCM (128 bits)	SHA256	Phase2SunToWater	  
		Add P2									
		Add P1								 Delete P1s	

Pfsense Nullsec - Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Description: Phase2nullsec
A description may be entered here for administrative reference (not parsed).

Disabled: Disable this phase 2 entry without removing it from the list.

Mode: Tunnel IPv4

Phase 1: Phase1nullsec (IKE ID 1)

Networks

Local Network: LAN subnet / 0
Type: Address
Local network component of this IPsec security association.

NAT/BINAT translation: None / 0
Type: Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Network 192.168.2.0 / 24
Type: Address
Remote network component of this IPsec security association.

Phase 2 Proposal (SA/Key Exchange)

Protocol: ESP
Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Encryption Algorithms:
 AES 256 bits
 AES128-GCM 128 bits
 AES192-GCM Auto
 AES256-GCM Auto
 CHACHA20-POLY1305

Hash Algorithms:
 SHA1 SHA256 SHA384 SHA512 AES-XCBC
Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group: 14 (2048 bit)
Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Expiration and Replacement

Life Time: 3600

We created matching rules on WAN and IPsec interfaces.

Firewall Rule specification:

- Action: Allow
- Protocol: Any
- Source: Any
- Destination: Any

Pfsense Sun to Water - Firewall Rules WAN/IPsec

Edit Firewall Rule

Action	<input type="button" value="Pass"/>	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	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="WAN"/>	Choose the interface from which packets must come to match this rule.
Address Family	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.
Protocol	<input type="button" value="Any"/>	Choose which IP protocol this rule should match.
Source		
Source	<input type="checkbox"/> Invert match	<input type="button" value="Any"/> <input type="button" value="Source Address"/> / <input type="button" value=""/>
Destination		
Destination	<input type="checkbox"/> Invert match	<input type="button" value="Any"/> <input type="button" value="Destination Address"/> / <input type="button" value=""/>

Pfsense Nullsec - Firewall Rules WAN/IPsec

Edit Firewall Rule

Action	Pass				
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	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.				
Interface	WAN				
Choose the interface from which packets must come to match this rule.					
Address Family	IPv4				
Select the Internet Protocol version this rule applies to.					
Protocol	Any				
Choose which IP protocol this rule should match.					
Source					
Source	<input type="checkbox"/> Invert match	Any	Source Address	/	v
Destination					
Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	v

Attempt to verify connectivity

IPsec Status								
ID	Description	Local		Remote	Role	Timers	Algo	Status
con1 #2	Phase1SunToWater	ID: 10.0.2.9 Host: 10.0.2.9:500		ID: 10.0.2.5 Host: 10.0.2.5:500	IKEv2 Initiator	Rekey: 24012s (06:40:12) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256	Established 115 seconds (00:01:55) ago
		SPI: 526b1f991433bc22		SPI: b708dad9f05ea044			MODP_2048	Disconnect P1

ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #3	Phase2SunToWater	192.168.2.0/24	Local: c4162687	192.168.1.0/24	Rekey: 3087s (00:51:27) Life: 3485s (00:58:05) Install: 115s (00:01:55)	AES_GCM_16 (128) IPComp: None	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0

IPsec Status								
ID	Description	Local		Remote	Role	Timers	Algo	Status
con1 #1	Phase1nullsec	ID: 10.0.2.5 Host: 10.0.2.5:500		ID: 10.0.2.9 Host: 10.0.2.9:500	IKEv2 Responder	Rekey: 23775s (06:36:15) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256	Established 165 seconds (00:02:45) ago
		SPI: b708dad9f05ea044		SPI: 526b1f991433bc22			MODP_2048	Disconnect P1

ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #3	Phase2nullsec	192.168.1.0/24	Local: c0a86917	192.168.2.0/24	Rekey: 2778s (00:46:18) Life: 3435s (00:57:15) Install: 165s (00:02:45)	AES_GCM_16 (128) IPComp: None	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0

Success in establishing the VPN tunnel connection. We will now attempt to ping between the machines.

Sun To Water machine to Nullsec Server - Testing connectivity (ping)

Ping

<u>Hostname</u>	192.168.1.100
<u>IP Protocol</u>	IPv4
<u>Source address</u>	LAN
Select source address for the ping.	
<u>Maximum number of pings</u>	3
Select the maximum number of pings.	
<u>Seconds between pings</u>	1
Select the number of seconds to wait between pings.	

 Ping

Results

```
PING 192.168.1.100 (192.168.1.100) from 192.168.2.1: 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=127 time=0.959 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=127 time=2.207 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=127 time=2.347 ms

--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.959/1.838/2.347/0.624 ms
```

Activate Windows

Nullsec Server to Sun To Water Machine - Testing connectivity (ping)

Ping

<u>Hostname</u>	192.168.2.10
<u>IP Protocol</u>	IPv4
<u>Source address</u>	LAN
Select source address for the ping.	
<u>Maximum number of pings</u>	3
Select the maximum number of pings.	
<u>Seconds between pings</u>	1
Select the number of seconds to wait between pings.	

 Ping

Results

```
PING 192.168.2.10 (192.168.2.10) from 192.168.1.1: 56 data bytes
64 bytes from 192.168.2.10: icmp_seq=0 ttl=127 time=0.000 ms
64 bytes from 192.168.2.10: icmp_seq=1 ttl=127 time=3.175 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=127 time=3.521 ms

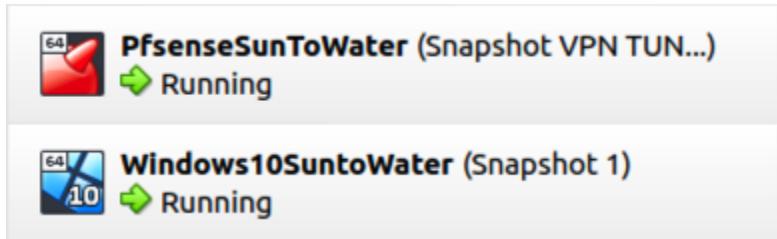
--- 192.168.2.10 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.000/2.232/3.521/1.585 ms
```

We've confirmed successful VPN tunnel connectivity by analyzing pfSense status indicators and system logs.

```
Apr 22 13:09:15  charon    10185  10[NET] <con1|11> sending packet: from 10.0.2.5[500] to 10.0.2.9[500] (80 bytes)
Apr 22 13:09:15  charon    10185  10[NET] <con1|11> received packet: from 10.0.2.9[500] to 10.0.2.5[500] (80 bytes)
Apr 22 13:09:15  charon    10185  10[ENC] <con1|11> parsed INFORMATIONAL request 6 []
Apr 22 13:09:15  charon    10185  10[ENC] <con1|11> generating INFORMATIONAL response 6 []
Apr 22 13:09:15  charon    10185  10[NET] <con1|11> sending packet: from 10.0.2.5[500] to 10.0.2.9[500] (80 bytes)
Apr 22 13:09:15  charon    10185  10[NET] <con1|11> received packet: from 10.0.2.9[500] to 10.0.2.5[500] (80 bytes)
Apr 22 13:09:15  charon    10185  10[ENC] <con1|11> parsed INFORMATIONAL response 8 []
Apr 22 13:09:15  charon    10185  10[IKE] <con1|11> activating new tasks
Apr 22 13:09:15  charon    10185  10[IKE] <con1|11> nothing to initiate
```

Captive Portal configuration

After successfully creating the VPN tunnel, we will use the client's machine to create access to the network with an AAA security configuration level (Authentication, Authorization and Accounting), for this we will implement a RADIUS system that creates a captive portal for network users and authenticates them using AD credentials.



The Snapshots you can see in the image were created after the VPN Tunnel was completed for security reasons so that if something goes wrong during the RADIUS implementation, we can go back.

Configuration chosen

It will condition navigation and traffic transmitted on the user's local network, until the user authenticates the portal's login page.

The screenshot shows the pfSense web interface. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services (which is currently selected), VPN, and Status. A red warning box is displayed, stating: "WARNING: The 'admin' account password is set to the default value 'admin'. Please change it immediately!" Below the warning, the main content area has a title "Status / Dashboard". Under "System Information", there is a table with the following data:

Name	pfSenseSunToWater.home.arpa
User	admin@192.168.2.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: dfcc03d4eba2424d9

On the right side, a vertical sidebar lists various services: Auto Config Backup, Captive Portal (with a cursor icon pointing to it), DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server, DNS Forwarder, DNS Resolver, Dynamic DNS, and IGMP Proxy.

Defining zone name.

This feature will allow us to divide the network used into different areas with different access levels.

The screenshot shows the "Add Captive Portal Zone" configuration page. The top navigation bar includes links for Services, Captive Portal, and Add Zone. The main form has a title "Add Captive Portal Zone". It contains two fields: "Zone name" (set to "SunToWater") and "Zone description" (set to "Captive Portal"). Below the "Zone name" field is a note: "Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit." Below the "Zone description" field is a note: "A description may be entered here for administrative reference (not parsed)."

Configuring Captive Portal to do Authentication Server from SunToWater Data

Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
SunToWater	LAN	1	Captive project prep	 

Services / Captive Portal / SunToWater / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

Captive Portal Configuration

Enable Enable Captive Portal

Description Captive project prep
A description may be entered here for administrative reference (not parsed).

Interfaces WAN LAN
Select the interface(s) to enable for captive portal.

Authentication

Authentication Method Use an Authentication backend
Select an Authentication Method to use for this zone. One method must be selected.
- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server SunToWater Local Database
You can add a remote authentication server in the [User Manager](#).
Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

Secondary authentication Server SunToWater Local Database
You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs.
This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

Captive Portal Login Page

Display custom logo image	<input checked="" type="checkbox"/> Enable to use a custom uploaded logo
Logo Image	<input type="button" value="Choose File"/> SunToWater logo.png
Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, It can be of any image type: .png, .jpg, .svg This image will not be stored in the config. The default logo will be used if no custom image is present.	

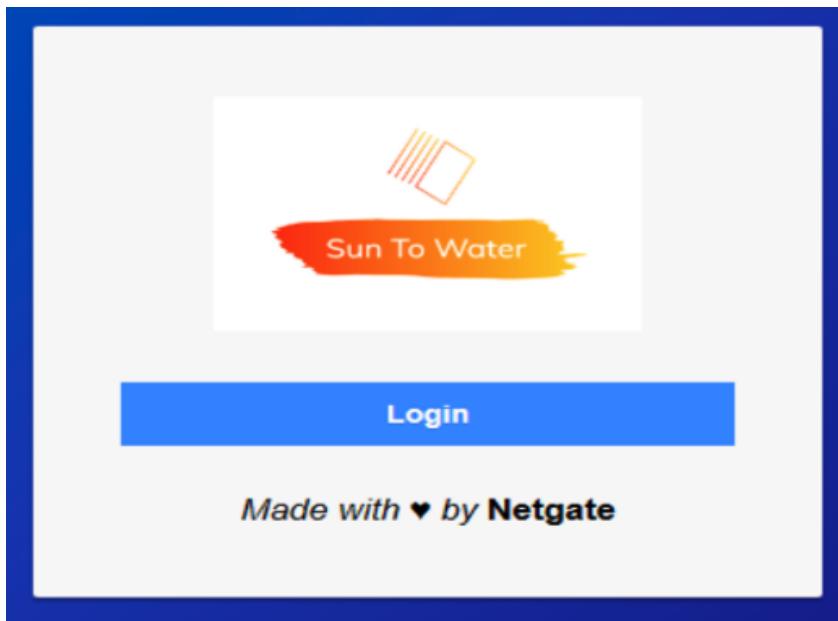
Authentication to anyone who want to access to network

This type of authentication will force users to use a login and a password.

Authentication

<u>Authentication Method</u>	<input type="button" value="Use an Authentication backend"/> Select an Authentication Method to use for this zone. One method must be selected. - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
------------------------------	---

Local Authentication Privileges	<input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set
HTTPS Options	
Login	<input type="checkbox"/> Enable HTTPS login When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.
<input type="button" value="Save"/>	



Users add, that should be access.

It is necessary to create users so that we can later define who can authenticate and have authorization to access the network and with what type of permissions.
password test: Benfica2024!

WARNING: The password is set to the default value. Change the password in the User Manager.

System /

Users Groups

Users

Username

User Manager

Logout (admin)

Users

name Status Groups Actions

System Administrator ✓ admins Edit Delete

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by USER

Disabled This user cannot login

Username michaelscott

Password

Full name Michael Scott, COO

User's full name, for administrative information only

Custom Settings Use individual customized GUI options and dashboard layout for this user.

Group membership

admins

Not member of Member of

» Move to "Member of" list < Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.

Save

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

Username	Full name	Status	Groups	Actions
<input type="checkbox"/> admin	System Administrator	✓	admins	
<input type="checkbox"/> michaelscott	Michael Scott, Chief operations Officer (COO)	✓		

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

Username	Full name	Status	Groups	Actions
<input type="checkbox"/> admin	System Administrator	✓	admins	
<input type="checkbox"/> badehabib	Bade Habib, CIO	✓	IT	
<input type="checkbox"/> bobslydell	Bob Slydell, CFO	✓	Financial	
<input type="checkbox"/> courtneyhans	Courtney Hans, CISO	✓	Security	
<input type="checkbox"/> michaelscott	Michael Scott, COO	✓	OperationGroup	
<input type="checkbox"/> minervamcgongall	Minerva McGonagall	✓	HR	
<input type="checkbox"/> petergibbons	Peter Gibbons, CMO	✓	Marketing	

Creating a group of user's

Creating groups allows you to define the structure and framework of the company's various departments to define the corresponding users.

WARNING: The password is set to the default value. Change the password in the User Manager.

System /

Users **Groups**

Users

User Manager Logout (admin)

Users

name	Status	Groups	Actions
System Administrator	✓	admins	

Add Delete

System / User Manager / Groups

Users Groups Settings Authentication Servers

Groups

Group name	Description	Member Count	Actions
all	All Users	2	
admins	System Administrators	1	

Add

Group Properties

Group name SunToWater

Scope Local

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description operation group

Group description, for administrative information only

Group membership

Not members	admin	michaelscott
Members		

Move to "Members" Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Save

In this field when the user tries to access the internet for the first time after connecting to the network, he is automatically redirected to the captive portal login page.

Users Groups Settings Authentication Servers

Group Privileges

Group SunToWater

Assigned privileges

- User - Services: Captive Portal login
- WebCfg - Services: Captive Portal
- WebCfg - Services: Captive Portal HA
- WebCfg - Services: Captive Portal Voucher Rolls
- WebCfg - Services: Captive Portal Vouchers
- WebCfg - Services: Captive Portal Zones
- WebCfg - Services: Captive Portal: Allowed Hostnames
- WebCfg - Services: Captive Portal: Allowed IPs
- WebCfg - Services: Captive Portal: Edit Allowed Hostnames
- WebCfg - Services: Captive Portal: Edit Allowed IPs
- WebCfg - Services: Captive Portal: Edit MAC Addresses
- WebCfg - Services: Captive Portal: Edit Zones
- WebCfg - Services: Captive Portal: File Manager
- WebCfg - Services: Captive Portal: Mac Addresses
- WebCfg - Status: Captive Portal
- WebCfg - Status: Captive Portal Voucher Rolls
- WebCfg - Status: Captive Portal Vouchers
- WebCfg - Status: Captive Portal: Expire Vouchers
- WebCfg - Status: Captive Portal: Test Vouchers
- WebCfg - Status: System Logs: Portal Auth

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter Show only the choices containing this term

Save Filter Clear

Indicates whether the user is able to login on the captive portal.

Assigned Privileges

Name	Description	Action
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	

+ Add

Save

Users Groups Settings Authentication Servers

Groups

Group name	Description	Member Count	Actions
SunToWater	operation group	1	
admins	System Administrators	1	
all	All Users	2	

Verification of authentication.

Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
SunToWater	LAN	1	Captive project prep	

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

ARP Table

Authentication

Diagnostics / Authentication

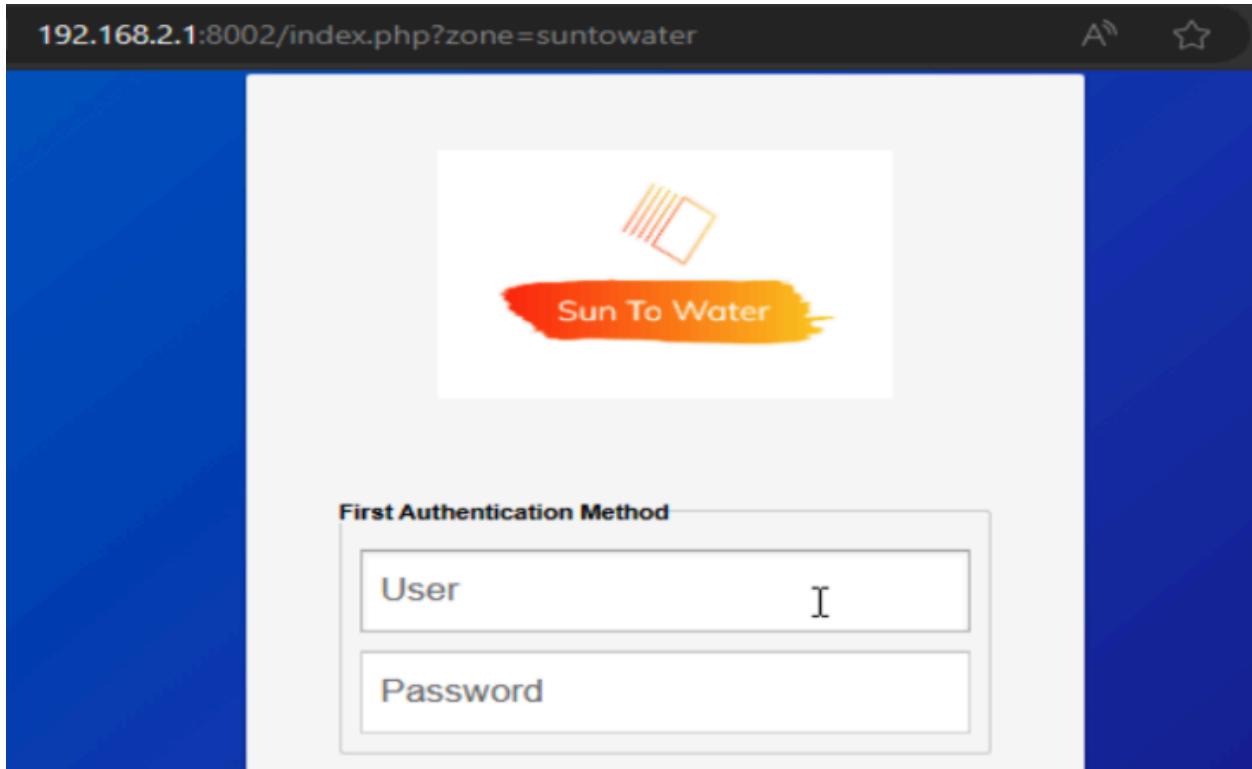
Authentication Test

Authentication Server	Local Database
Select the authentication server to test against.	
Username	michaelscott
Password	Benfica2024!
Debug	<input type="checkbox"/> Set debug flag Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

User michaelscott authenticated successfully. This user is a member of groups:

- SunToWater
- all

Requesting username and password access to authenticate the login page of the portal you intend to access.

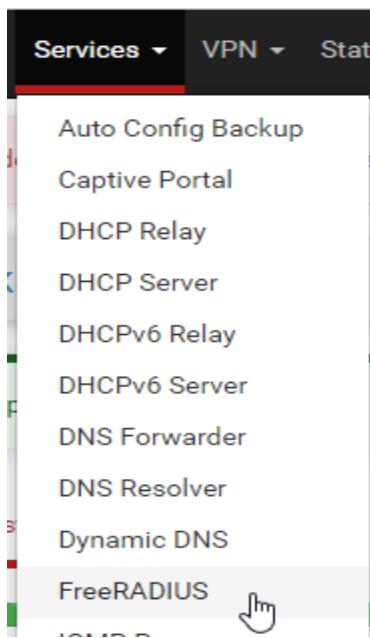


Deployment of RADIUS Authentication Server

- Deploying a RADIUS system that raises a captive portal for new network users and authenticates them using Active Directory (AD) credentials, thus centralizing management to control who can access the network infrastructure.

Installing and configuring Radius (It is a client-server protocol and software that enables remote access servers to communicate with a central server to authenticate and authorize their access to the request system or service).

The screenshot shows the pfSense web interface. At the top, there's a navigation bar with the pfSense logo and tabs for 'System' and 'Interfaces'. A dropdown menu from 'System' includes options like 'Advanced', 'Certificates', 'General Setup', 'High Availability', 'Package Manager' (which is highlighted with a cursor icon), and 'Register'. Below this, a 'Status / D' section is visible. On the left, a 'System Info' panel shows a 'WARNING: The' message. The main content area is titled 'Packages'. It lists the package 'freeradius3' with version '0.15.10_1'. The description states it's a free implementation of the RADIUS protocol supporting MySQL, PostgreSQL, LDAP, Kerberos, etc. An 'Install' button is present. Underneath, it shows package dependencies: 'bash-5.2.15', 'freeradius3-3.2.3', and 'python311-3.11.6'. At the bottom, a success message says 'pfSense-pkg-freeradius3 installation successfully completed.' There are tabs for 'Installed Packages', 'Available Packages', and 'Package Installer'.



Creating a user.

Users MACs NAS / Clients Interfaces Settings EAP SQL LDAP View Config XMLRPC Sync

Filter by: A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Filter field: Username Filter text:

Username	Password	Use One Time Password	Simult. Connections	IP Address	Expiration Date	Session Timeout	Possible Login Times	VLAN ID	Description

General Configuration

Username	michaelscott
Enter the username. Whitespace is allowed. Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP.	
Password	Benfica2024!
Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password.	
Password Encryption	Cleartext-Password
Select the password encryption for this user. If the (pre-hashed) options are used, the password should already be hashed by the expected hash function. Note that not all authentication protocols are compatible with all types of hashed passwords. Default: Cleartext-Password	

Configure the NAS / client of radius. IP 127.0.0.1/24, password: Benfica2024!

NAS (Network Attached Storage)

Define the ipV4 of the client from which the RADIUS server should accept packets.

Services / FreeRADIUS / Edit / NAS / Clients

?

Users MACs **NAS / Clients** Interfaces Settings EAP SQL LDAP View Config XMLRPC Sync

General Configuration

Client IP Address Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).

Client IP Version

Client Shortname Enter a short name for the client. This is generally the hostname of the NAS.

Client Shared Secret Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, access point, etc.) needs to communicate with the RADIUS server. **FreeRADIUS is limited to 31 characters for the shared secret.**
Warning: Single quotes in shared secret must be escaped with a backslash (\'). Backslash must be escaped by using two backslashes (\\\).

 Save

Services / FreeRADIUS / NAS / Clients								?	
Users	MACs	NAS / Clients	Interfaces	Settings	EAP	SQL	LDAP	View Config	XMLRPC Sync
Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description		
192.168.2.0/24	ipaddr	Windows10SuntoW	udp	other	no	16		 	

Configure listen interfaces, the IPv4 in this case authentication. We choose (*) because it means all interfaces, and use Port 1812.

Services / FreeRADIUS / Interfaces

Users MACs NAS / Clients **Interfaces** Settings EAP SQL LDAP View Config XMLRPC Sync

Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	

General Configuration

Interface IP Address * Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)

Port 1812 Enter the port number of the listening interface. Different interface types need different ports. Click Info for details. i

Interface Type Authentication Enter the type of the listening interface. (Default: Authentication)

IP Version IPv4 Enter the IP version of the listening interface. (Default: IPv4)

Description Optionally enter a description here for your reference.

Save

Users MACs NAS / Clients **Interfaces** Settings EAP SQL LDAP View Config XMLRPC Sync

Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	

Add

Save

Add radius database. IP server 127.0.0.1, Wan 10.0.2.14, password: benfica

A screenshot of the pfSense User Manager interface showing the 'Authentication Servers' list. The top navigation bar includes 'Users', 'Groups', 'Settings', and 'Authentication Servers'. A red cursor arrow points to the 'Authentication Servers' tab. Below it is a table with columns: 'Server Name', 'Type', 'Host Name', and 'Actions'. One entry is listed: 'Local Database' under 'Type' and 'pfSense' under 'Host Name'. A green 'Add' button with a plus sign is located at the bottom right.

Server Name	Type	Host Name	Actions
Local Database		pfSense	

+ Add

A screenshot of the pfSense User Manager interface showing the 'Edit' screen for an authentication server. The top navigation bar shows 'System / User Manager / Authentication Servers / Edit'. The 'Authentication Servers' tab is selected. The main area is titled 'Server Settings'.

Server Settings

<u>Descriptive name</u>	SunToWater
<u>Type</u>	RADIUS

RADIUS Server Settings

<u>Protocol</u>	MS-CHAPv2
<u>Hostname or IP address</u>	127.0.0.1
<u>Shared Secret</u>
<u>Services offered</u>	Authentication and Accounting
<u>Authentication port</u>	1812
<u>Accounting port</u>	1813
<u>Authentication Timeout</u>	5

Users	Groups	Settings	Authentication Servers
Authentication Servers			
Server Name	Type	Host Name	Actions
SunToWater	RADIUS	127.0.0.1	
Local Database		pfSenseSunToWater	

Testing Authentication user's

Diagnostics / Authentication

User michaelscott authenticated successfully. This user is a member of groups:

Authentication Test

<u>Authentication</u>	<input type="button" value="SunToWater"/>
<u>Server</u>	Select the authentication server to test against.
<u>Username</u>	michaelscott
<u>Password</u>

User bobslydell authenticated successfully. This user is a member of groups:

Authentication Test

<u>Authentication</u>	<input type="button" value="SunToWater"/>
<u>Server</u>	Select the authentication server to test against.
<u>Username</u>	bobslydell
<u>Password</u>
<u>Debug</u>	<input type="checkbox"/> Set debug flag Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).
Test	

User badehabib authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server	SunToWater
Select the authentication server to test against.	
Username	badehabib
Password
Debug	<input type="checkbox"/> Set debug flag Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

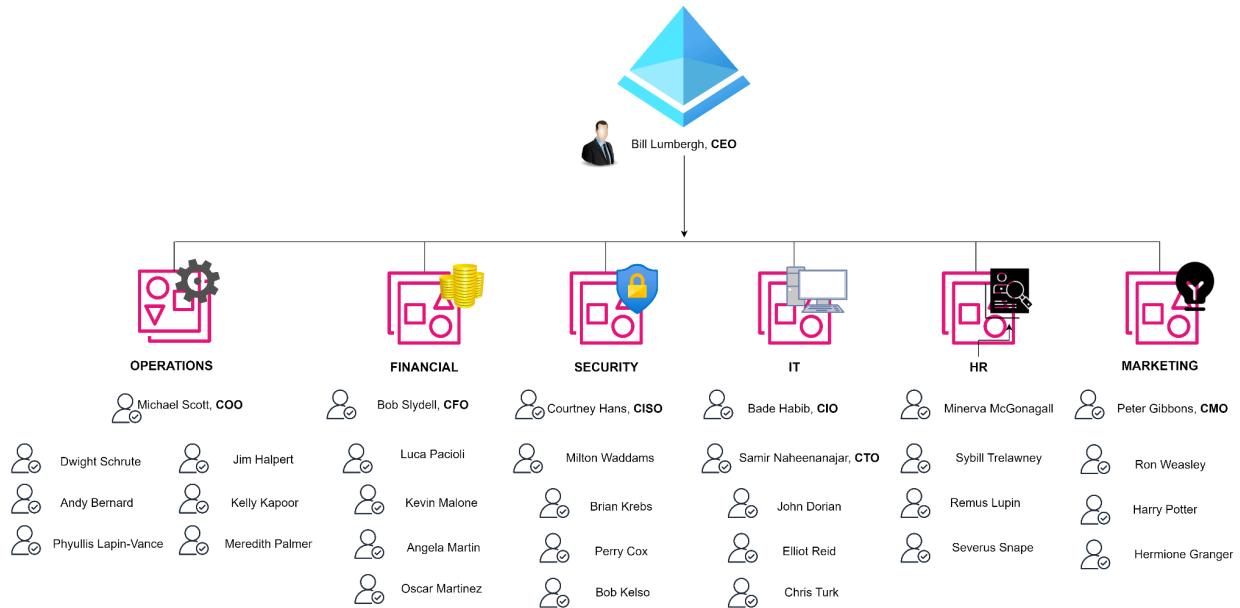
Logs authentication report.

- Status / System Logs / Authentication / Captive Portal Auth

General	Captive Portal Auth	PPPoE Logins	L2TP Logins	OS User Events	OS Account Changes
Last 10 Captive Portal Auth Log Entries. (Maximum 500)					
Time	Process	PID	Message		
Apr 19 08:32:12	logportalauth	397	Zone: suntowater - Reconfiguring captive portal(SunToWater).		
Apr 19 08:35:00	logportalauth	396	Zone: suntowater - ACCEPT: unauthenticated, 08:00:27:28:17:23, 192.168.1.100		
Apr 19 09:06:32	logportalauth	396	Zone: suntowater - Reconfiguring captive portal(SunToWater).		
Apr 19 09:14:12	logportalauth	397	Zone: suntowater - DISCONNECT: unauthenticated, 08:00:27:28:17:23, 192.168.1.100		
Apr 19 09:21:44	logportalauth	397	Zone: suntowater - Reconfiguring captive portal(SunToWater).		
Apr 19 09:33:50	logportalauth	397	Zone: suntowater - ACCEPT: michaelscott, 08:00:27:28:17:23, 192.168.1.100		
Apr 19 10:47:22	logportalauth	1111	Zone: suntowater - Reconfiguring captive portal(SunToWater).		
Apr 19 11:48:36	logportalauth	1111	Zone: suntowater - DISCONNECT: michaelscott, 08:00:27:28:17:23, 192.168.1.100		
Apr 19 11:52:46	logportalauth	396	Zone: suntowater - ACCEPT: michaelscott, 08:00:27:28:17:23, 192.168.1.100		
Apr 19 11:53:35	logportalauth	1111	Zone: suntowater - DISCONNECT: michaelscott, 08:00:27:28:17:23, 192.168.1.100		

PowerShell Script for automatic DC Deployment

Present the scenario org chart



Script should demonstrably perform:

- Assigns the Windows Server VM a static IPv4 address
- Assigns the Windows Server VM a DNS

```
1 # Static IP, default Gateway and DNS variables
2
3 $IP = "192.168.1.100"
4 $MaskBits = 24 # This means /24 CIDR block, or subnet mask 255.255.255.0
5 $Gateway = "192.168.1.1"
6 $DNS = "1.1.1.1"
7 $IPType = "IPv4"
8
9 # Retrieve the network adapter that you want to configure
10
11 $adapter = Get-NetAdapter | ? {$_.Status -eq "up"}
12
13 # Remove any existing IP, gateway from our ipv4 adapter
14
15 If (($adapter | Get-NetIPConfiguration).IPv4Address.IPAddress) {
16     $adapter | Remove-NetIPAddress -AddressFamily $IPType -Confirm:$false
17 }
18 If (($adapter | Get-NetIPConfiguration).Ipv4DefaultGateway) {
19     $adapter | Remove-NetRoute -AddressFamily $IPType -Confirm:$false
20 }
21
22 # Configure the IP address and default gateway
23
24 $adapter | New-NetIPAddress ` 
25     -AddressFamily $IPType ` 
26     -IPAddress $IP ` 
27     -PrefixLength $MaskBits ` 
28     -DefaultGateway $Gateway
29
30 # Configure the DNS client server IP addresses
31
32 $adapter | Set-DnsClientServerAddress -ServerAddresses $DNS
```

Variables were used for this part of the project, for ease of configuration. Part of the excerpt to find the current active network adapter was taken from [this website \(Source\)](#).

Lines 30-32 show what commandlets and variables I used to set up a manual DNS provider for the machine for optimal functionality. In this case, I used Cloudflare's DNS service, at 1.1.1.1.

- Renames the Windows Server VM

```

34  # Rename the machine
35
36  Rename-Computer -NewName "STWServer"

```

Renaming the computer is done with the Rename-Computer commandlet, adding the -NewName and the desired name after quotes. Note that the system name cannot exceed 15 characters.

A restart is not required for this part of the set up, but a restart is necessary in the next step before and after.

- Installs AD-Domain-Services

```

38  # Install AD-Domain-Services
39
40  Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

```

Install-WindowsFeatures -Name AD-Domain-Services, with the extra parameter -IncludeManagementTools, ensures that all of the necessary and extra features required for Active Directory to run are installed.

This part requires a restart to accept the previous Rename-Computer commandlet before installing AD features into the system. Just run the script again after the restart.

- Creates an AD Forest

```

42  # Elevate to Domain Controller and create AD Forest
43
44  $domainAdmin = "Administrator"
45  $domainPassword = ConvertTo-SecureString "Benfica2024!" -AsPlainText -Force
46  $domainAdminCredential = New-Object System.Management.Automation.PSCredential ($domainAdmin, $domainPassword)
47
48  Install-ADDSForest ` 
49    -DomainName "suntowater.site" ` 
50    -DomainNetbiosName "SUNTOWATER" ` 
51    -DomainMode "WinThreshold" ` 
52    -ForestMode "WinThreshold" ` 
53    -InstallDNS ` 
54    -SafeModeAdministratorPassword (ConvertTo-SecureString "Benfica2024!" -AsPlainText -Force) ` 
55    -Force ` 
56

```

I attempted to use a few variables to automate the setup process, or else PowerShell would prompt the user to add their own password. I believe not all of these variables ended up being used, such as \$domainAdminCredential, but I will keep those there since that is what I ended up uploading to GitHub. It did not contribute to any errors or strange behavior.

This part requires another system restart once complete. Let the system reboot and finish configuring DC and AD, then log back in as the Domain administrator, not as a local user, before running the script again.

- Creates Organizational Units (OU)

```
57 # Create Organizational Units
58
59 New-ADOrganizationalUnit -Name "CEO" -Path "DC=suntowater,DC=site"
60 New-ADOrganizationalUnit -Name "CSO" -Path "DC=suntowater,DC=site"
61 New-ADOrganizationalUnit -Name "HR" -Path "DC=suntowater,DC=site"
62 New-ADOrganizationalUnit -Name "IT" -Path "DC=suntowater,DC=site"
63 New-ADOrganizationalUnit -Name "Security" -Path "DC=suntowater,DC=site"
64 New-ADOrganizationalUnit -Name "Finances" -Path "DC=suntowater,DC=site"
65 New-ADOrganizationalUnit -Name "Marketing" -Path "DC=suntowater,DC=site"
66 New-ADOrganizationalUnit -Name "Management" -Path "DC=suntowater,DC=site"
```

To add a new organization unit, the New-ADOrganizationalUnit commandlet is used, with the -Name and -Path parameters, defining them clearly for the Active Directory's database. Note that, since the Domain is suntowater.site, it is required to separate the path as shown above. Using DC=suntowater or DC=suntowater.site is not recognized as an acceptable path, and it will produce errors and prevent these commands and the next ones from working.

- Creates users

```

68  # Define the CSV file location and import the data
69  $Csvfile = "C:\temp\ImportADUsers.csv"
70  $Users = Import-Csv $Csvfile
71
72  # The password for the new user
73  $Password = "P@ssw0rd1234"
74
75  # Import the Active Directory module
76  Import-Module ActiveDirectory
77
78  # Loop through each user
79  foreach ($User in $Users) {
80      try {
81          # Retrieve the Manager distinguished name
82          $managerDN = if ($User.'Manager') {
83              Get-ADUser -Filter "DisplayName -eq '$($User.'Manager')'" -Properties DisplayName |
84              Select-Object -ExpandProperty DistinguishedName
85          }
86
87          # Define the parameters using a hashtable
88          $NewUserParams = @{
89              Name             = "$($User.'First name') $($User.'Last name')"
90              GivenName        = $User.'First name'
91              Surname          = $User.'Last name'
92              DisplayName      = $User.'Display name'
93              SamAccountName   = $User.'User logon name'
94              UserPrincipalName = $User.'User principal name'
95              StreetAddress    = $User.'Street'
96              City             = $User.'City'
97              State            = $User.'State/province'
98              PostalCode       = $User.'Zip/Postal Code'
99              Country          = $User.'Country/region'
100             Title           = $User.'Job Title'
101             Department       = $User.'Department'
102             Company          = $User.'Company'
103             Manager          = $managerDN
104             Path             = $User.'OU'
105             Description      = $User.'Description'
106             Office           = $User.'Office'
107             OfficePhone      = $User.'Telephone number'
108             EmailAddress     = $User.'E-mail'
109             MobilePhone      = $User.'Mobile'
110             AccountPassword  = (ConvertTo-SecureString "$Password" -AsPlainText -Force)
111             Enabled          = if ($User.'Account status' -eq "Enabled") { $true } else { $false }
112
113             ChangePasswordAtLogon = $true # Set the "User must change password at next logon"
114         }
115
116         # Add the info attribute to OtherAttributes only if Notes field contains a value
117         if (![[string]::IsNullOrEmpty($User.Notes)) {
118             $NewUserParams.OtherAttributes = @{Info = $User.Notes }
119         }
120
121         # Check to see if the user already exists in AD
122         if (Get-ADUser -Filter "SamAccountName -eq '$($User.'User logon name')'" ) {
123
124             # Give a warning if user exists
125             Write-Host "A user with username $($User.'User logon name') already exists in Active Directory." -ForegroundColor Yellow
126         }
127         else {
128
129             # User does not exist then proceed to create the new user account
130             # Account will be created in the OU provided by the $User.OU variable read from the CSV file
131             New-ADUser @NewUserParams
132             Write-Host "The user $($User.'User logon name') is created successfully." -ForegroundColor Green
133         }
134     }
135     catch {
136
137         # Handle any errors that occur during account creation
138         Write-Host "Failed to create user $($User.'User logon name') - $($_.Exception.Message)" -ForegroundColor Red
139     }
}

```

This part of the script was more complex and required some specific target directories, file names, and a specific .CSV file with all the user information required for it to be successfully added to Active Directory. Note that this portion of the script can be run standalone once DC is set up, for future changes in the users database of Active Directory.

This script was taken in large part from [this source](#), as it streamlined the process and made it very easy to understand.

The .CSV was made by our team, using the company hierarchy picture provided by the project assignment. After many iterations that could not be successfully imported, this is the final version:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	First name	Last name	Display na	User logon	User princ	Street	City	State/prov	Zip/Postal	Country/n	Job Title	Departme	Company	Manager	OU	Description	Office	Telephone	Other Tele	E-mail	Mobile	Notes	Account status
2	Bill	Lumbergh	Bill	Lumbergh	Bill	Lumbergh	Lumbergh@suntowater.site				CEO	CEO	SunToWater		OU=CEO,DC=suntowater,DC=site								Enabled
3	Minerva	McGonagall	Minerva	A. Minerva	McGonagall@suntowater.site						Executive HR	SunToWater		OU=HR,DC=suntowater,DC=site								Enabled	
4	Sybill	Trelawney	Sybill	Trelawney	Sybill.Trelawney@suntowater.site						Director T+HR	SunToWater		OU=HR,DC=suntowater,DC=site								Enabled	
5	Remus	Lupin	Remus	Lupin	Remus.Lupin@suntowater.site						Manager THR	SunToWater		OU=HR,DC=suntowater,DC=site								Enabled	
6	Severus	Snape	Severus	S. Severus	Severus.Snape@suntowater.site						Human Re HR	SunToWater		OU=HR,DC=suntowater,DC=site								Enabled	
7	Bade	Habibi	Habibi	Bade	Habibi.Bade@suntowater.site						Chief Infor IT	SunToWater		OU=IT,DC=suntowater,DC=site								Enabled	
8	Samir	Naheenah	Naheenah	Samir	Naheenah.Samir@suntowater.site						Chief Tech IT	SunToWater		OU=IT,DC=suntowater,DC=site								Enabled	
9	John	Dorian	John	Dorian	John.Dorian@suntowater.site						Senior Eng IT	SunToWater		OU=IT,DC=suntowater,DC=site								Enabled	
10	Elliot	Reid	Elliot	Reid	Elliot.Reid@suntowater.site						Frontend IT IT	SunToWater		OU=IT,DC=suntowater,DC=site								Enabled	
11	Chris	Turk	Chris	Turk	Chris.Turk@suntowater.site						Backend DIT	SunToWater		OU=IT,DC=suntowater,DC=site								Enabled	
12	Courtney	Hans	Courtney	Courtney	Courtney.Hans@suntowater.site						Chief Infor Security	SunToWater		OU=CSO,DC=suntowater,DC=site								Enabled	
13	Milton	Waddams	Milton	W.Milton	W.Milton.Waddams@suntowater.site						Facilities MSecurity	SunToWater		OU=Security,DC=suntowater,DC=site								Enabled	
14	Brian	Krebs	Brian	Krebs	Brian.Krebs@suntowater.site						Directory ISecurity	SunToWater		OU=Security,DC=suntowater,DC=site								Enabled	
15	Perry	Cox	Perry	Cox	Perry.Cox@suntowater.site						Defensive Security	SunToWater		OU=Security,DC=suntowater,DC=site								Enabled	
16	Bob	Kelso	Bob	Kelso	Bob.Kelso@suntowater.site						Offensive Security	SunToWater		OU=Security,DC=suntowater,DC=site								Enabled	
17	Bob	Slydell	Bob	Slydell	Bob.Slydell@suntowater.site						Chief Finan Finances	SunToWater		OU=Finances,DC=suntowater,DC=site								Enabled	
18	Luca	Pacioli	Luca	Pacioli	Luca.Pacioli@suntowater.site						Senior Auc Finances	SunToWater		OU=Finances,DC=suntowater,DC=site								Enabled	
19	Kevin	Malone	Kevin	Mal Kevin	Mal Kevin.Malone@suntowater.site						Jr Account Finances	SunToWater		OU=Finances,DC=suntowater,DC=site								Enabled	
20	Angela	Martin	Angela	Ma Angela	Ma Angela.Martin@suntowater.site						Sr Account Finances	SunToWater		OU=Finances,DC=suntowater,DC=site								Enabled	
21	Oscar	Martinez	Oscar	Mar.Oscar	Mar.Oscar.Martinez@suntowater.site						Ap Admin Finances	SunToWater		OU=Finances,DC=suntowater,DC=site								Enabled	
22	Peter	Gibbons	Peter	Gibb Peter	Gibb Peter.Gibbons@suntowater.site						Chief MarMarketing	SunToWater		OU=Marketing,DC=suntowater,DC=site								Enabled	
23	Ron	Weasley	Ron	Weas Ron	Weas Ron.Weasley@suntowater.site						Sr Manage Marketing	SunToWater		OU=Marketing,DC=suntowater,DC=site								Enabled	
24	Harry	Potter	Harry	Pott Harry	Pott Harry.Potter@suntowater.site						Sr Manage Marketing	SunToWater		OU=Marketing,DC=suntowater,DC=site								Enabled	
25	Hermione	Granger	Hermione	Hermione.Hermione	Hermione.Hermione.Granger@suntowater.site						Sr Manage Marketing	SunToWater		OU=Marketing,DC=suntowater,DC=site								Enabled	
26	Michael	Scott	Michael	Sc Michael	Sc Michael.Scott@suntowater.site						Chief Oper Manager	SunToWater		OU=Management,DC=suntowater,DC=site								Enabled	
27	Dwight	Schrute	Dwight	Sd Dwight	Sd Dwight.Schrute@suntowater.site						Divisional Manager	SunToWater		OU=Management,DC=suntowater,DC=site								Enabled	
28	Andy	Bernard	Andy	Bern Andy	Bern Andy.Bernard@suntowater.site						Regional N Manager	SunToWater		OU=Management,DC=suntowater,DC=site								Enabled	
29	Phyllis	Lapin-VanPhyllis	Phyllis	La Phyllis	La Phyllis.Lapin-Vance@suntowater.site						Regional N Manager	SunToWater		OU=Management,DC=suntowater,DC=site								Enabled	
30	Jim	Halpert	Jim	Halper Jim	Halper.Jim.Halpert@suntowater.site						Regional N Manager	SunToWater		OU=Management,DC=suntowater,DC=site								Enabled	
31	Kelly	Kapoor	Kelly	Kapo Kelly	Kapo Kelly.Kapoor@suntowater.site						Regional N Manager	SunToWater		OU=Management,DC=suntowater,DC=site								Enabled	
32	Meredith	Palmer	Meredith	Meredit	Meredit.Meredith.Meredith.Palmer@suntowater.site						Regional N Manager	SunToWater		OU=Management,DC=suntowater,DC=site								Enabled	

This .CSV was imported with no errors.

Script additions

- DNS

```

57 # Configure DNS service (with Google DNS and Cloudflare DNS as forwarders)
58
59 Install-WindowsFeature -Name DNS -IncludeManagementTools
60 Add-DnsServerPrimaryZone -Name "suntowater.site" -ZoneFile "suntowater.site.dns"
61 Set-DnsServerForwarder -IPAddress 1.1.1.1, 8.8.8.8
62 Add-DnsServerResourceRecordA -Name "www" -ZoneName "suntowater.site" -IPv4Address "192.168.1.100" -CreatePtr

```

I noticed that I did not configure a proper DNS service for the Windows Server above, and so it is now set with a basic configuration. All DNS traffic should be forwarded through the VPN tunnel, to the Server's DNS, and then forwarded to the listed providers.

- RADIUS

```
64 # Initial setup for Windows Server RADIUS (couldn't verify if it's working fully due to not having the same virtual environment as the project target)
65
66 Install-WindowsFeature -Name NPAS -IncludeManagementTools
67 New-NpsRadiusClient -Name "SunToWater" -Address "192.168.2.1" -SharedSecret "secretosdeporco"
68 Set-NpsRadiusServerSettings -AccountingOnOff $true -NpsDnsDomain "suntowater.site"
69 Set-NpsRadiusAuthentication -EapTls $true -EapTlsCipherSuite "TLS_RSA_WITH_AES_128_CBC_SHA256"
70 Start-Service "IAS"
71
72 # RADIUS check
73 Get-NpsRadiusClient
74 Get-NpsConnectionRequestPolicy
75 Get-NpsNetworkPolicy
```

This part of the script will set up the basic RADIUS server configuration and point it towards the pfSense to be used as the RADIUS client. Note that I believe some extra manual configuration is required with policies that were not included in the script because of the level of granularity required for a proper configuration.

Demonstration

Script part 1

The videos are long because the virtual machine was very slow, so feel free to skip ahead. In the first part, I changed the IP address settings and the basic DNS lookup provider. I also changed the system name, as shown. Since this is one single script that's meant to do everything, it aborted after it tried to install Active Directory because it still needed a name change. Those errors are there for that reason, but after a reboot the setup will continue.

Script part 2

Part 2 installs Active Directory and all necessary tools and features required to run it. Note that installing and the initial setup of Active Directory requires a reboot, so the rest of the script could not be completed in this part.

Script part 3

This final part skips the steps that were already implemented, verifies the installation of Active Directory, and finishes setting up the Forest and the Domain. It also imports all users to the AD database, to be used with RADIUS and for domain logins.