CONESTOGA

Connect Life and Learning

OpenVPN Host-to-Network VPN with Two-Factor Authentication (2FA) – Project Report

Onyeka Ofojetu Mmesooma

Course: INFO8581 – Secure Network Administration

Project Title: Configuring OpenVPN on pfSense with FreeRADIUS and Google Authenticator (2FA)

Date: 2025-07-25

CONTENTS

1.0 INTRODUCTION

Virtual Private Networks (VPNs) are essential in modern cybersecurity infrastructures for enabling secure remote access to internal organizational resources. A host-to-network VPN setup, often called a "Road Warrior" configuration, allows remote users to connect securely from any location, functioning as if they were within the local network. This configuration is particularly valuable for remote employees, IT administrators, and third-party contractors.

The purpose of this project is to demonstrate the practical implementation of a secure host-to-network VPN using OpenVPN on pfSense. To enhance authentication security, the project integrates Two-Factor Authentication (2FA) powered by FreeRADIUS and Google Authenticator, leveraging the Time-Based One-Time Password (TOTP) protocol. The result is a robust, encrypted communication tunnel that ensures both confidentiality and strong access control for remote users.

This documentation outlines the complete setup process, configuration steps, testing methodology, challenges encountered, and key takeaways from the deployment.

2.0 PROJECT OBJECTIVES

This project was designed to simulate a realistic network security deployment using industry-standard open-source tools. The aim was to ensure a strong authentication mechanism while offering seamless remote access. It also allowed for hands-on experience in configuring and troubleshooting VPN systems in a secure environment.

- Deploy and configure OpenVPN server on pfSense
- Install and configure FreeRADIUS for authentication
- Integrate TOTP-based 2FA using Google Authenticator
- Establish secure client connectivity and validate encrypted communication
- Troubleshoot and resolve challenges related to authentication and routing

3.0 ENVIRONMENT AND TOOLS

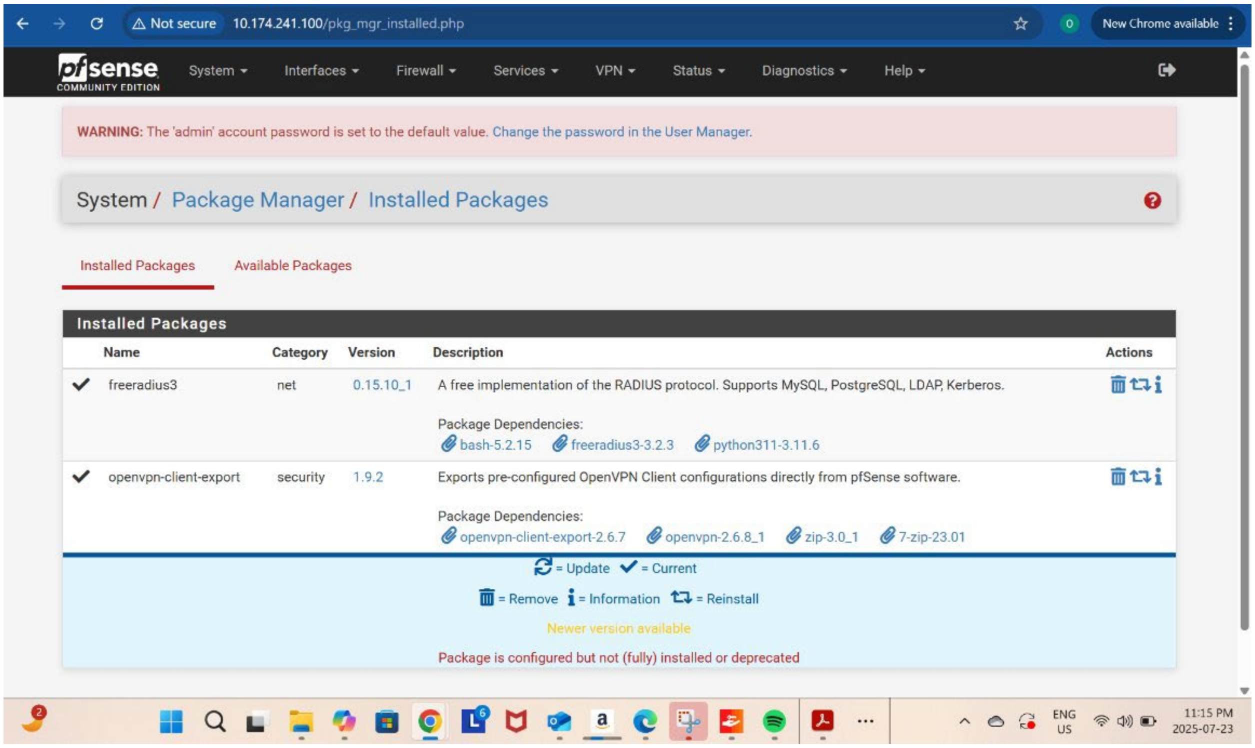
- **Virtual Environment:** VMware vSphere (pfSense and test clients)
- **Firewall:** pfSense 2.7.2
- **Authentication:** FreeRADIUS (installed via pfSense package manager)

- **VPN Protocol:** OpenVPN (UDP 1194)
- **Client:** Windows 10 with OpenVPN GUI
- **2FA Tool:** Google Authenticator (TOTP)

4.0 STEP-BY-STEP CONFIGURATION

4.1 INSTALLING PACKAGES

- Installed **FreeRADIUS** and **OpenVPN Client Export Utility** via pfSense Package Manager.
- Confirmed installation via Diagnostics > Installed Packages.



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

System / Package Manager / Installed Packages

Installed Packages

	Name	Category	Version	Description	Actions
✓	freeradius3	net	0.15.10_1	A free implementation of the RADIUS protocol. Supports MySQL, PostgreSQL, LDAP, Kerberos. Package Dependencies: bash-5.2.15 freeradius3-3.2.3 python311-3.11.6	🗑 ⟲ ℹ
✓	openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software. Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01	🗑 ⟲ ℹ

⟳ = Update ✓ = Current

🗑 = Remove ℹ = Information ⟲ = Reinstall

Newer version available

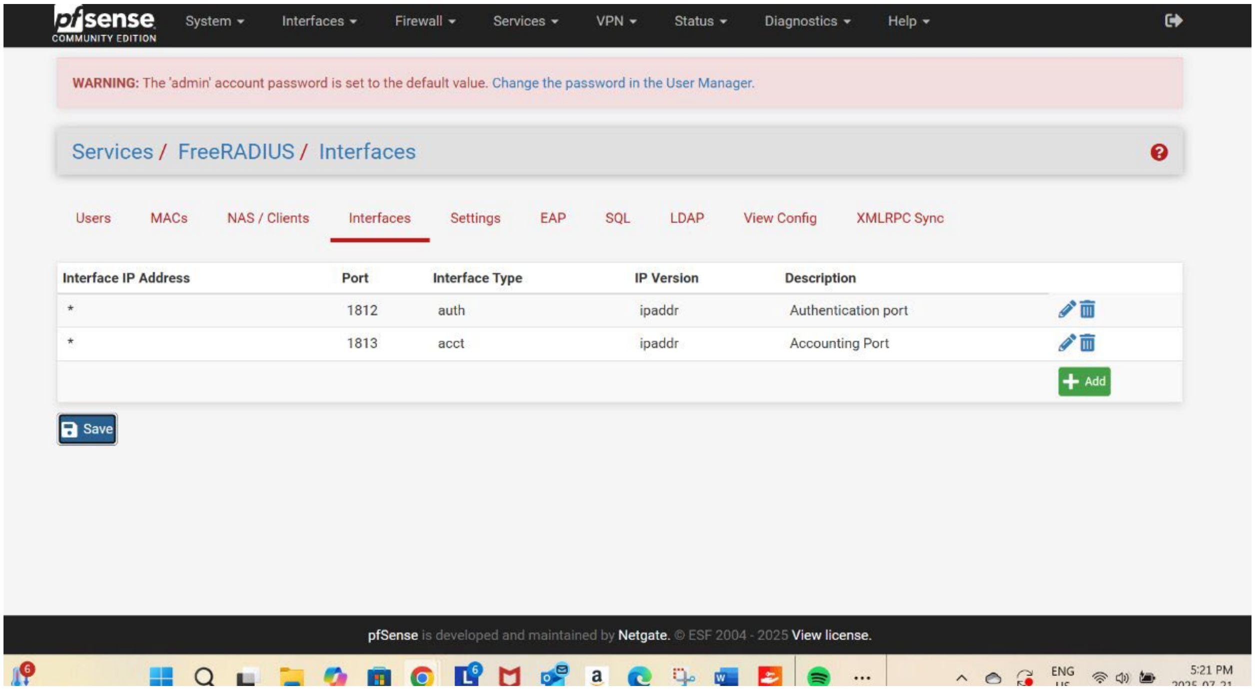
Package is configured but not (fully) installed or deprecated

Figure 4.1: Installed Packages.

4.2 FREERADIUS CONFIGURATION

Interfaces Tab:

- Authentication Port: 1812
- Accounting Port: 1813



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

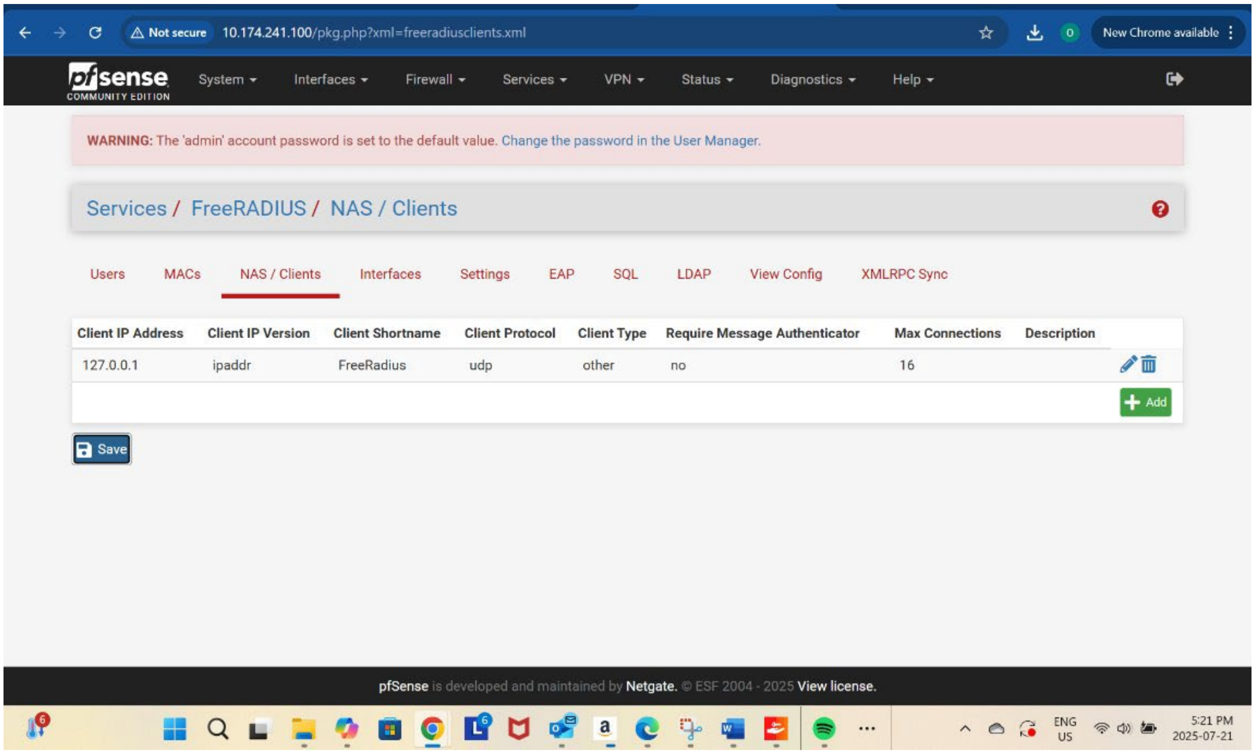
Services / FreeRADIUS / Interfaces

Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	Authentication port
*	1813	acct	ipaddr	Accounting Port

Figure 4.2: Interfaces of FreeRADIUS

NAS / Clients Tab:

- NAS IP: 127.0.0.1 (pfSense itself)
- Shared Secret: configured securely for RADIUS communication



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

Services / FreeRADIUS / NAS / Clients

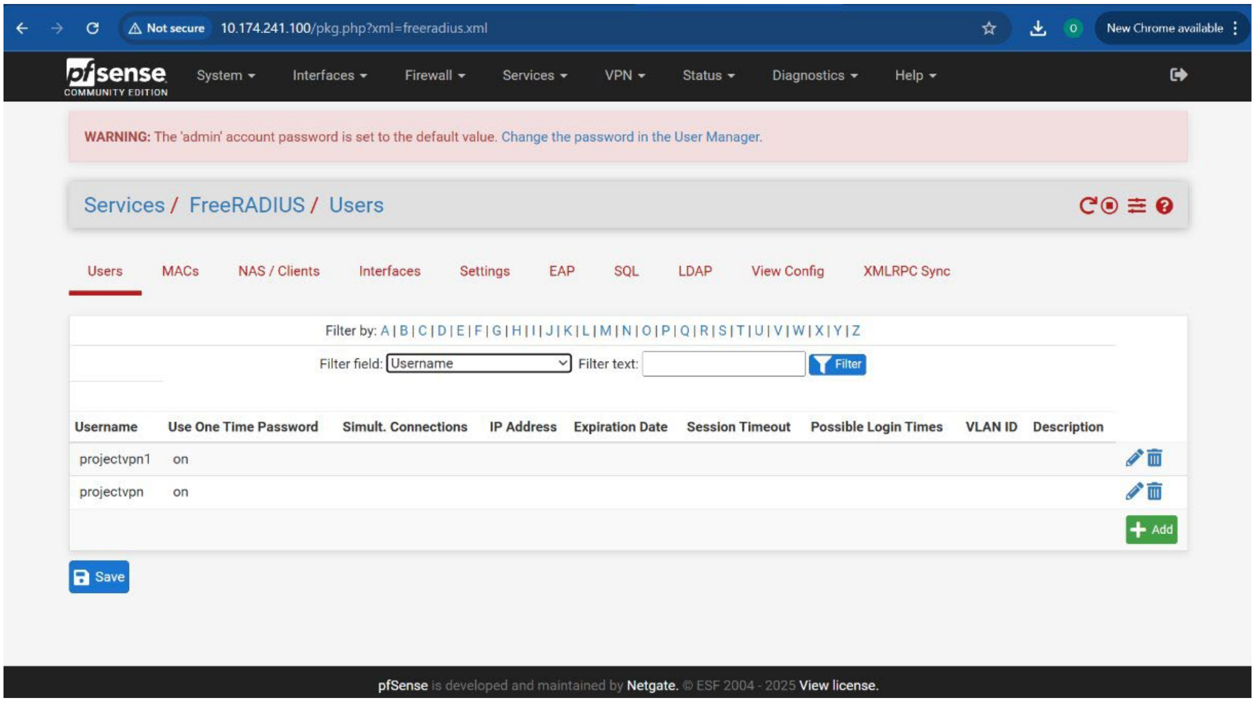
Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description
127.0.0.1	ipaddr	FreeRadius	udp	other	no	16	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Figure 4.3: NAS/Clients of FreeRADIUS

Users Tab:

- Created two VPN test accounts: projectvpn and projectvpn1
- Enabled One-Time Password (OTP) per user



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

Services / FreeRADIUS / Users

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:

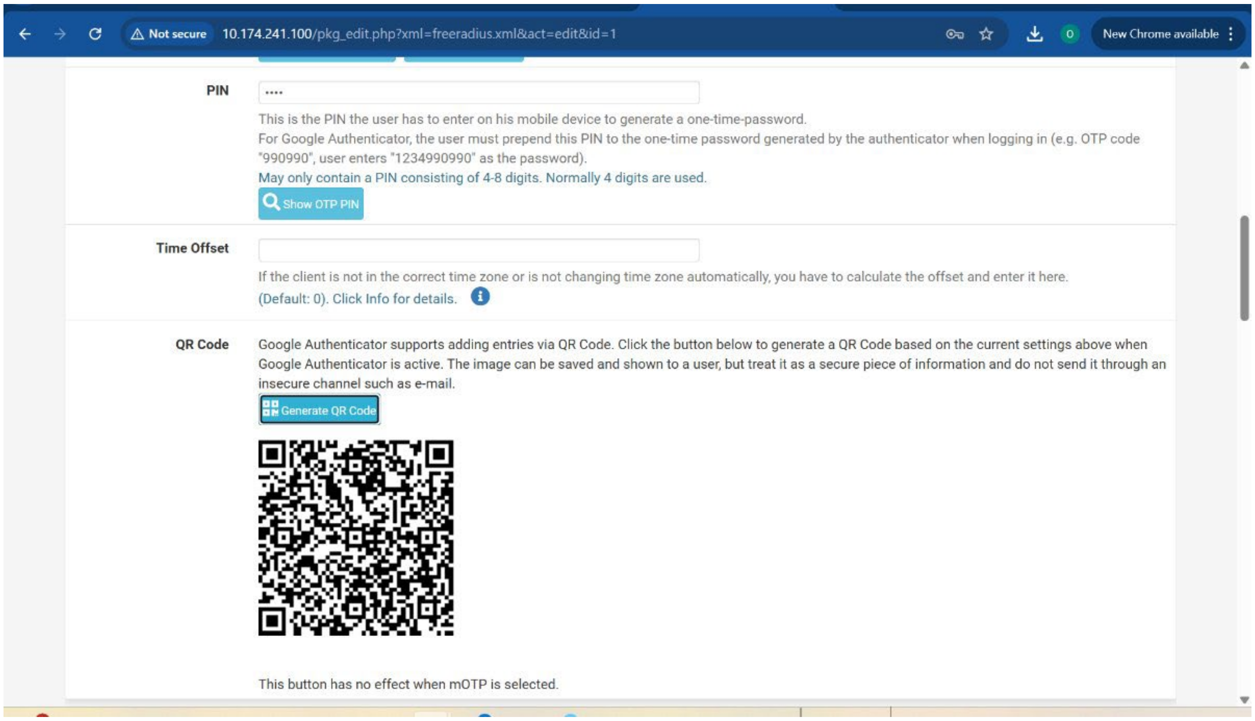
Username	Use One Time Password	Simult. Connections	IP Address	Expiration Date	Session Timeout	Possible Login Times	VLAN ID	Description
projectvpn1	on							
projectvpn	on							

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Figure 4.4: Users of FreeRADIUS

4.3 TOTP CONFIGURATION (2FA)

- Each user was assigned a unique TOTP secret and QR code
- Scanned QR code using the Google Authenticator app on mobile
- Verified code generation and sync with system time (NTP enabled)



Not secure
10.174.241.100/pkg_edit.php?xml=freeradius.xml&act=edit&id=1
New Chrome available

PIN ••••

This is the PIN the user has to enter on his mobile device to generate a one-time-password.
For Google Authenticator, the user must prepend this PIN to the one-time password generated by the authenticator when logging in (e.g. OTP code "990990", user enters "1234990990" as the password).
May only contain a PIN consisting of 4-8 digits. Normally 4 digits are used.

Time Offset

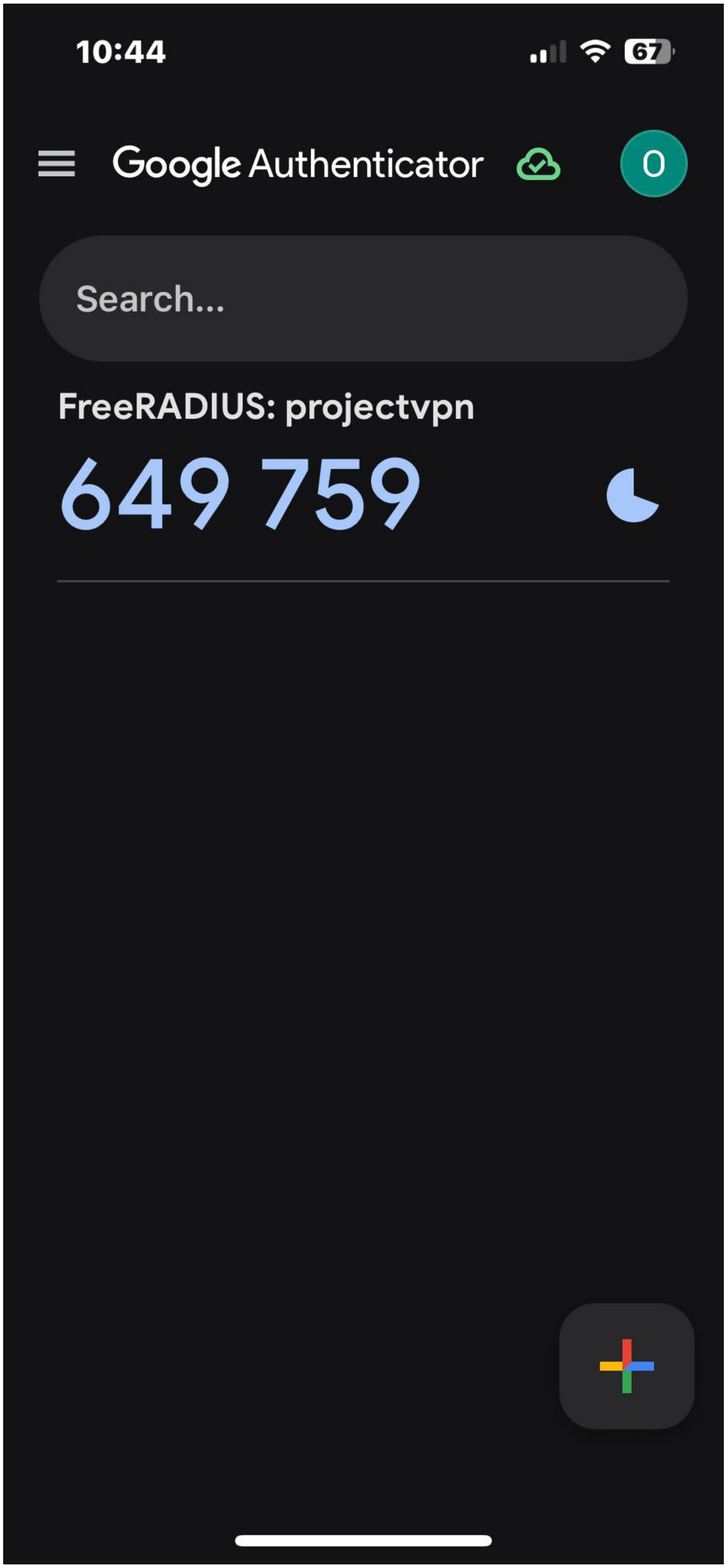
If the client is not in the correct time zone or is not changing time zone automatically, you have to calculate the offset and enter it here.
(Default: 0). Click Info for details.

QR Code

Google Authenticator supports adding entries via QR Code. Click the button below to generate a QR Code based on the current settings above when Google Authenticator is active. The image can be saved and shown to a user, but treat it as a secure piece of information and do not send it through an insecure channel such as e-mail.

This button has no effect when mOTP is selected.

Figure 4.5: TOTP QR Code.



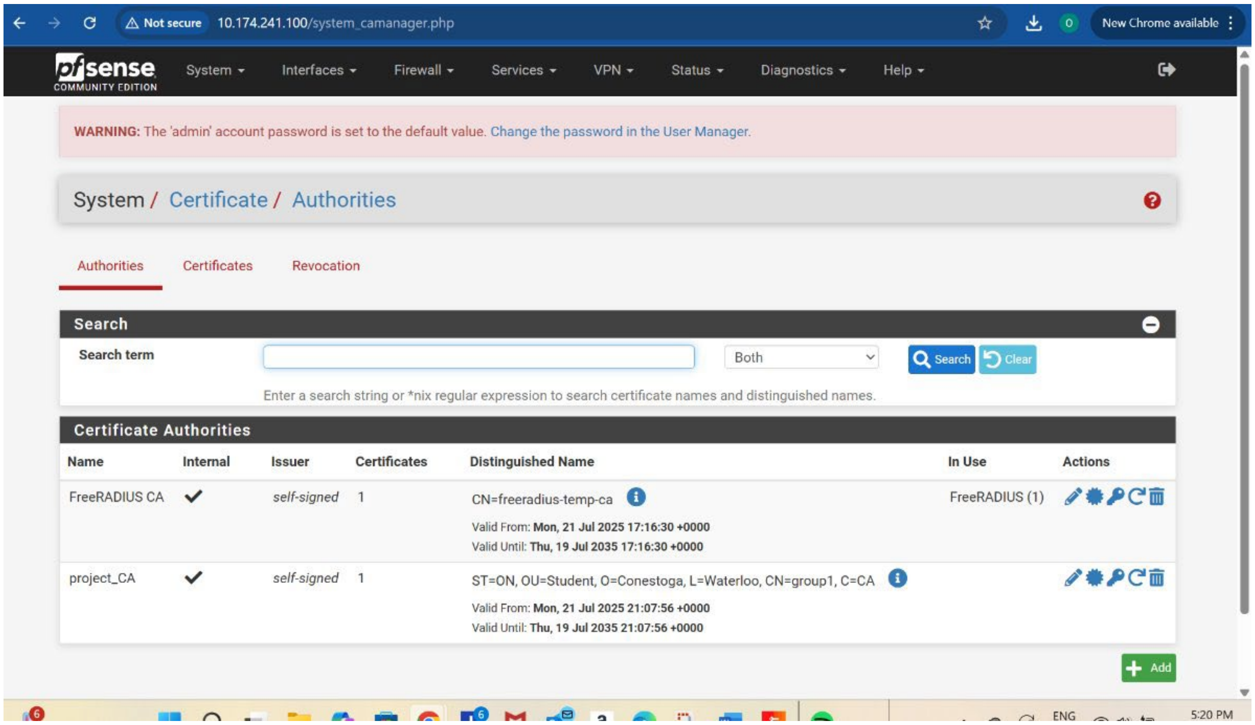
FreeRADIUS: projectvpn

649 759

Figure 4.6: Google Authentication Page.

4.4 CERTIFICATE SETUP

- Created a Certificate Authority named project_CA
- Issued Project OpenVPN Server Certificate from project_CA
- This cert was bound to the OpenVPN server for encryption



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

System / Certificate / Authorities

Authorities Certificates Revocation

Search

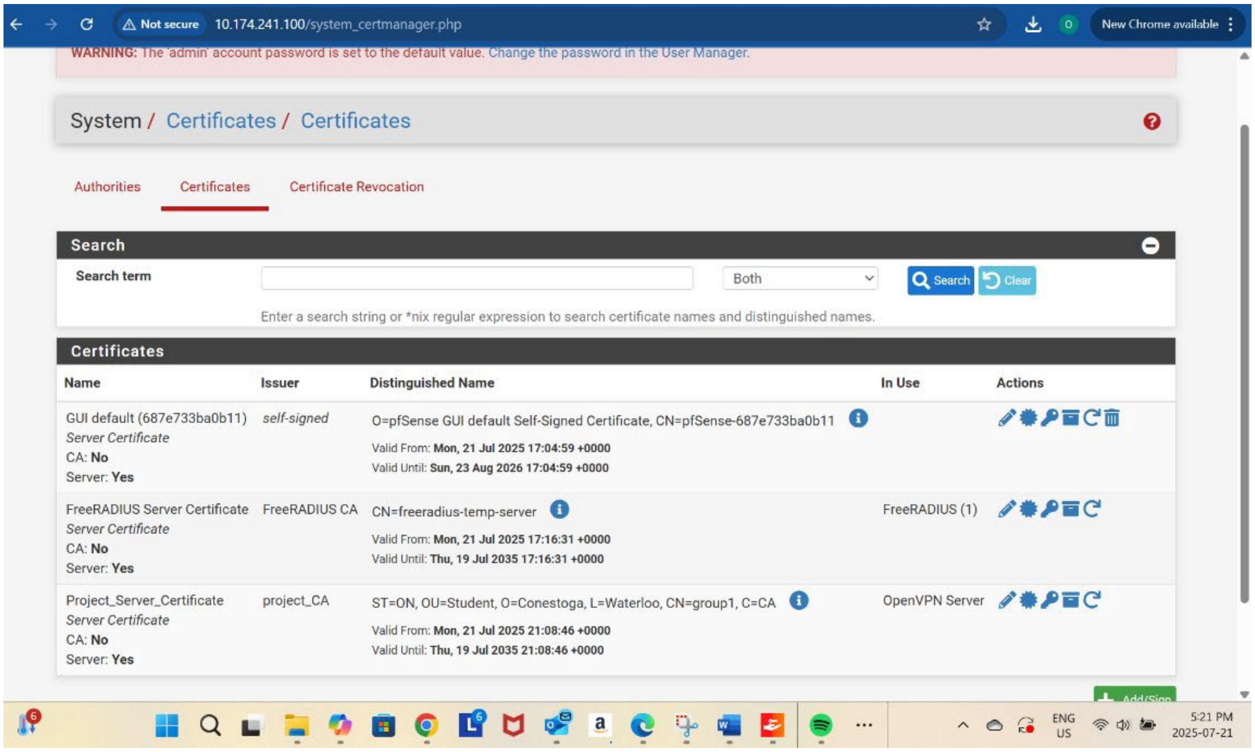
Search term: [ ] Both [Search] [Clear]

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
FreeRADIUS CA	✓	*self-signed*	1	CN=freeradius-temp-ca Valid From: **Mon, 21 Jul 2025 17:16:30 +0000** Valid Until: **Thu, 19 Jul 2035 17:16:30 +0000**	FreeRADIUS (1)	
project_CA	✓	*self-signed*	1	ST=ON, OU=Student, O=Conestoga, L=Waterloo, CN=group1, C=CA Valid From: **Mon, 21 Jul 2025 21:07:56 +0000** Valid Until: **Thu, 19 Jul 2035 21:07:56 +0000**		

Figure 4.7: Certificate Authority.



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

System / Certificates / Certificates

Search

Search term

Enter a search string or *nix regular expression to search certificate names and distinguished names.

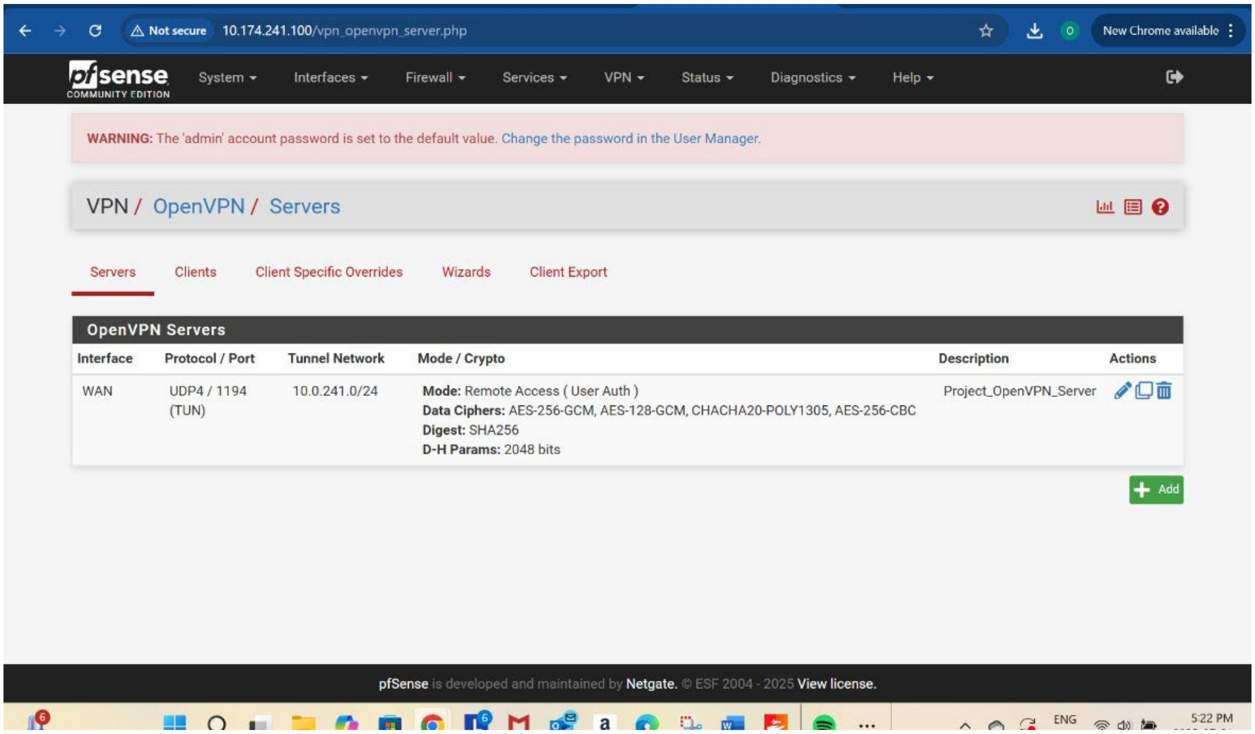
Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (687e733ba0b11) *Server Certificate* CA: **No** Server: **Yes**	*self-signed*	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-687e733ba0b11 Valid From: **Mon, 21 Jul 2025 17:04:59 +0000** Valid Until: **Sun, 23 Aug 2026 17:04:59 +0000**		
FreeRADIUS Server Certificate *Server Certificate* CA: **No** Server: **Yes**	FreeRADIUS CA	CN=freeradius-temp-server Valid From: **Mon, 21 Jul 2025 17:16:31 +0000** Valid Until: **Thu, 19 Jul 2035 17:16:31 +0000**	FreeRADIUS (1)	
Project_Server_Certificate *Server Certificate* CA: **No** Server: **Yes**	project_CA	ST=ON, OU=Student, O=Conestoga, L=Waterloo, CN=group1, C=CA Valid From: **Mon, 21 Jul 2025 21:08:46 +0000** Valid Until: **Thu, 19 Jul 2035 21:08:46 +0000**	OpenVPN Server	

Figure 4.8: Certificate Setup.

4.5 OPENVPN SERVER SETUP

- Protocol: UDP | Port: 1194
- Tunnel Network: 10.0.241.0/24
- Local Network: 10.0.0.0/24 (internal LAN)
- Authentication Backend: FreeRADIUS
- Encryption: AES-256-GCM



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

VPN / OpenVPN / Servers

OpenVPN Servers

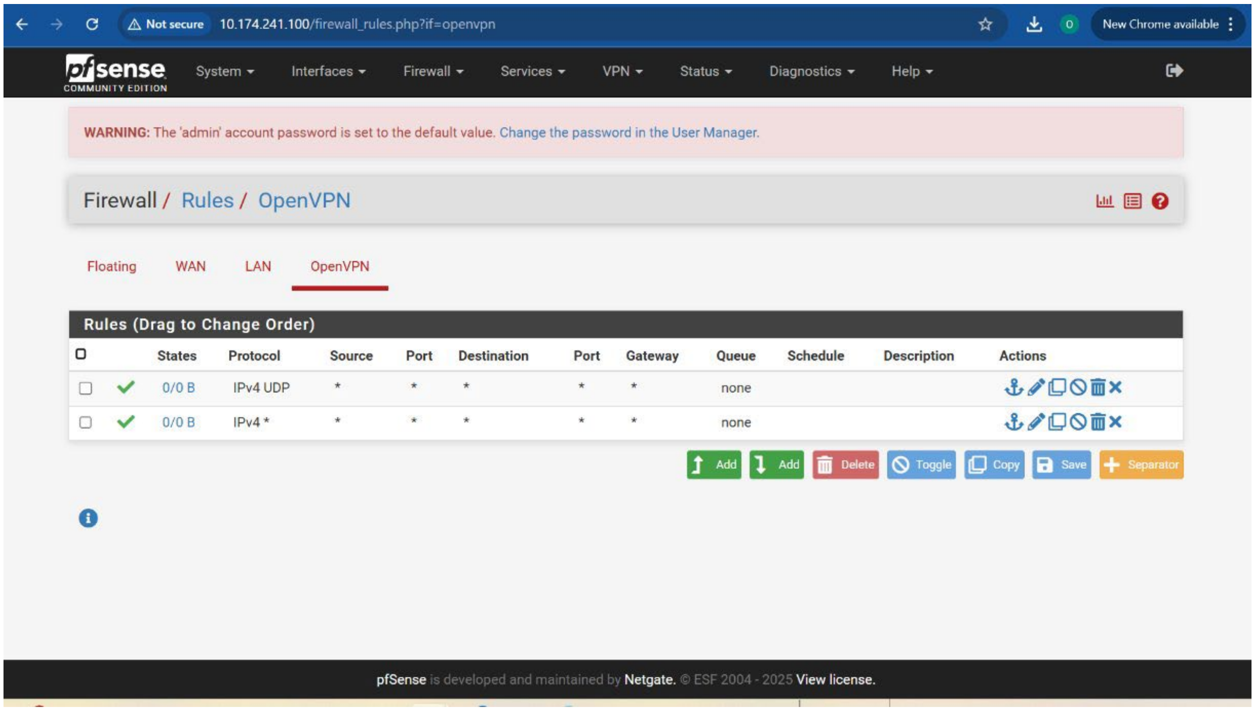
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.241.0/24	**Mode:** Remote Access (User Auth) **Data Ciphers:** AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC **Digest:** SHA256 **D-H Params:** 2048 bits	Project_OpenVPN_Server	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Figure 4.9: OpenVPN Servers setup.

4.6 FIREWALL RULES

- **WAN Rule:** Allow UDP 1194 (OpenVPN)
- **OpenVPN Rule:** Allow all traffic from tunnel



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

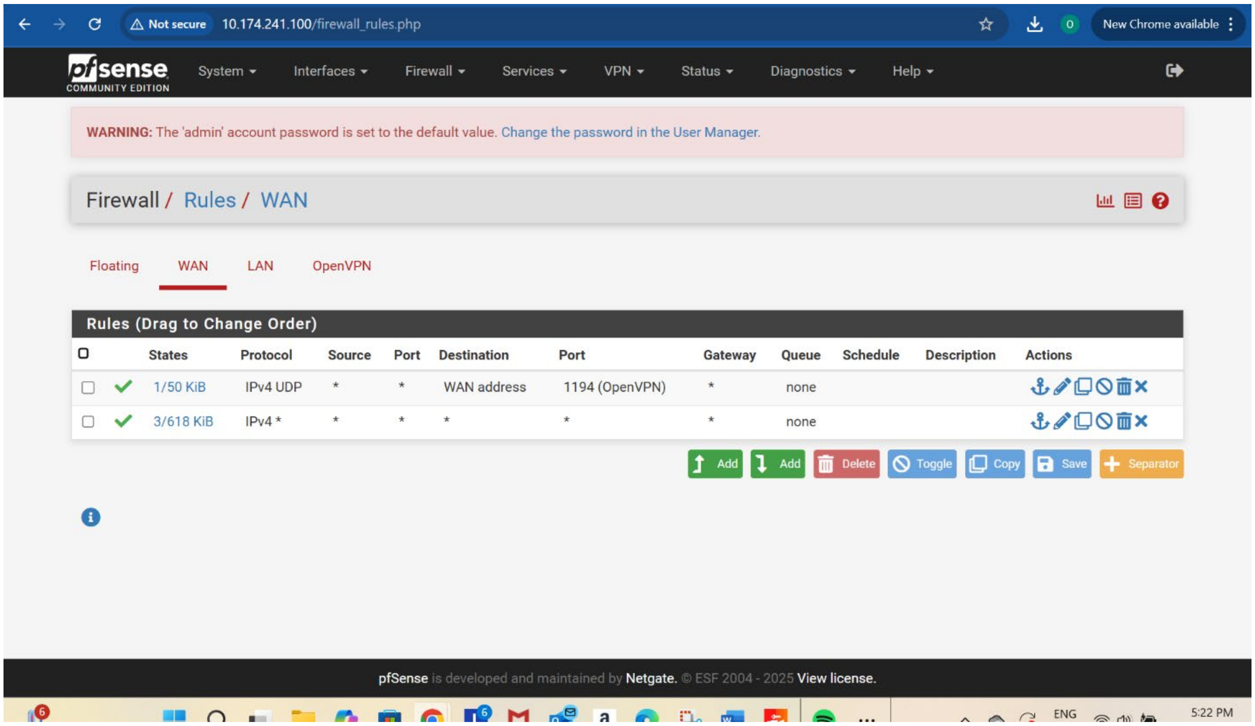
Firewall / Rules / OpenVPN

Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 UDP	*	*	*	*	*	none			
☐	✓	0/0 B	IPv4 *	*	*	*	*	*	none			

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Figure 4.10: Firewall Rules OpenVPN.



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

Firewall / Rules / WAN

Rules (Drag to Change Order)

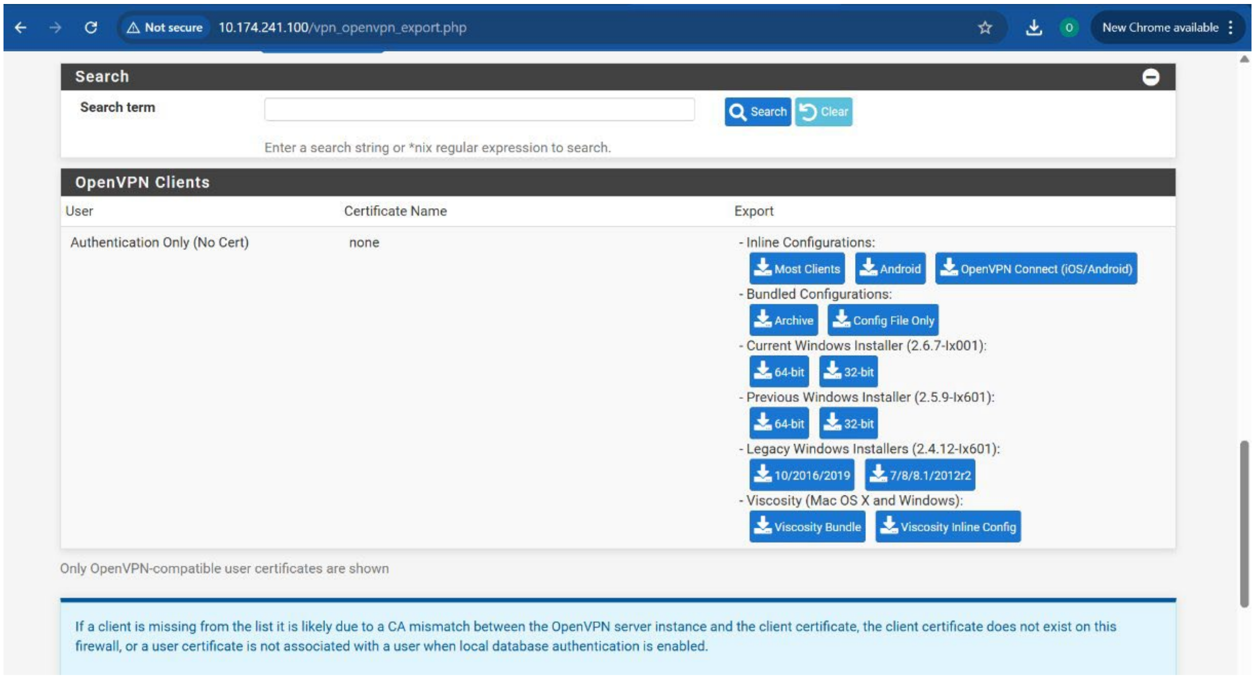
☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	1/50 KiB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none			
☐	✓	3/618 KiB	IPv4 *	*	*	*	*	*	none			

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Figure 4.11: Firewall Rules WAN.

4.7 CLIENT EXPORT AND CONNECTION

- Used the **OpenVPN Client Export** package to generate inline. ovpn config
- Imported into OpenVPN GUI on Windows client
- Upon connection, user was prompted for:
    - **Username**
    - **Password**
    - **TOTP code from Google Authenticator**
- Successful connection confirmed by OpenVPN logs and pfSense status



Search

Search term

Search | Clear

Enter a search string or *nix regular expression to search.

OpenVPN Clients

User	Certificate Name	Export
Authentication Only (No Cert)	none	- Inline Configurations: Most Clients · Android · OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive · Config File Only - Current Windows Installer (2.6.7-Ix001): 64-bit · 32-bit - Previous Windows Installer (2.5.9-Ix601): 64-bit · 32-bit - Legacy Windows Installers (2.4.12-Ix601): 10/2016/2019 · 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle · Viscosity Inline Config

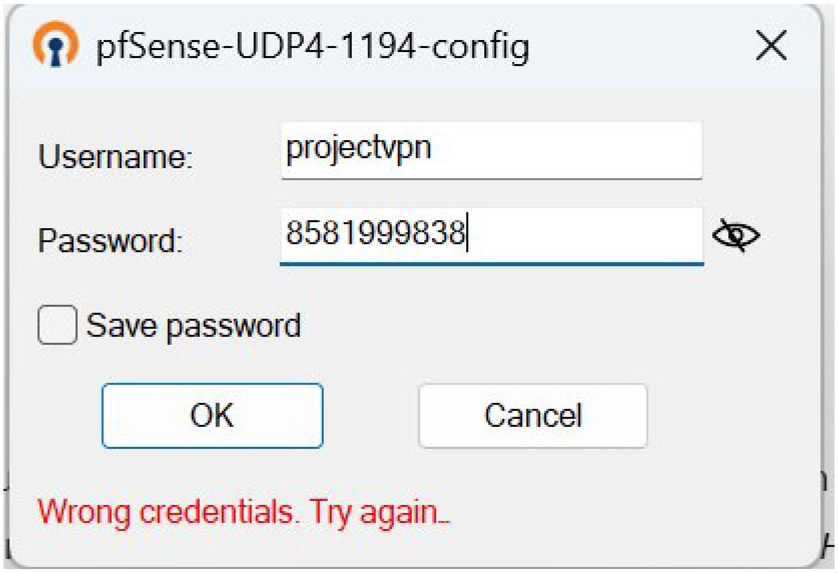
Only OpenVPN-compatible user certificates are shown

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

Figure 4.12: Export Ovpn.

4.8 VPN CONNECTION STATUS

- VPN client was successfully assigned the virtual IP: 10.0.241.6
- OpenVPN logs confirmed successful authentication and tunnel establishment
- pfSense OpenVPN status page displayed active session for user projectvpn



pfSense-UDP4-1194-config

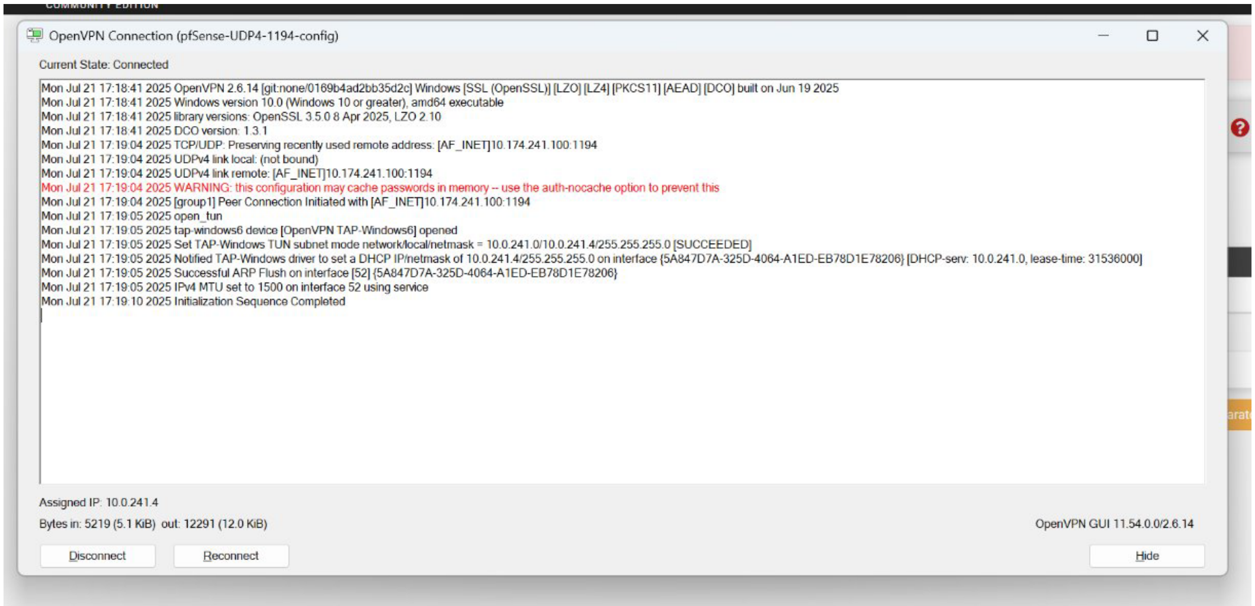
Username: projectvpn

Password: 8581999838

□ Save password

Wrong credentials. Try again..

Figure 4.13: Login Prompt.



OpenVPN Connection (pfSense-UDP4-1194-config)

Current State: Connected

```
Mon Jul 21 17:18:41 2025 OpenVPN 2.6.14 [git:none/0169b4ad2bb35d2c] Windows [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [AEAD] [DCO] built on Jun 19 2025
Mon Jul 21 17:18:41 2025 Windows version 10.0 (Windows 10 or greater), amd64 executable
Mon Jul 21 17:18:41 2025 library versions: OpenSSL 3.5.0 8 Apr 2025, LZO 2.10
Mon Jul 21 17:18:41 2025 DCO version: 1.3.1
Mon Jul 21 17:19:04 2025 TCP/UDP: Preserving recently used remote address: [AF_INET]10.174.241.100:1194
Mon Jul 21 17:19:04 2025 UDPv4 link local: (not bound)
Mon Jul 21 17:19:04 2025 UDPv4 link remote: [AF_INET]10.174.241.100:1194
Mon Jul 21 17:19:04 2025 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Mon Jul 21 17:19:04 2025 [group1] Peer Connection Initiated with [AF_INET]10.174.241.100:1194
Mon Jul 21 17:19:05 2025 open_tun
Mon Jul 21 17:19:05 2025 tap-windows6 device [OpenVPN TAP-Windows6] opened
Mon Jul 21 17:19:05 2025 Set TAP-Windows TUN subnet mode network/local/netmask = 10.0.241.0/10.0.241.4/255.255.255.0 [SUCCEEDED]
Mon Jul 21 17:19:05 2025 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.0.241.4/255.255.255.0 on interface {5A847D7A-325D-4064-A1ED-EB78D1E78206} [DHCP-serv: 10.0.241.0, lease-time: 31536000]
Mon Jul 21 17:19:05 2025 Successful ARP Flush on interface [52] {5A847D7A-325D-4064-A1ED-EB78D1E78206}
Mon Jul 21 17:19:05 2025 IPv4 MTU set to 1500 on interface 52 using service
Mon Jul 21 17:19:10 2025 Initialization Sequence Completed
```

Assigned IP: 10.0.241.4

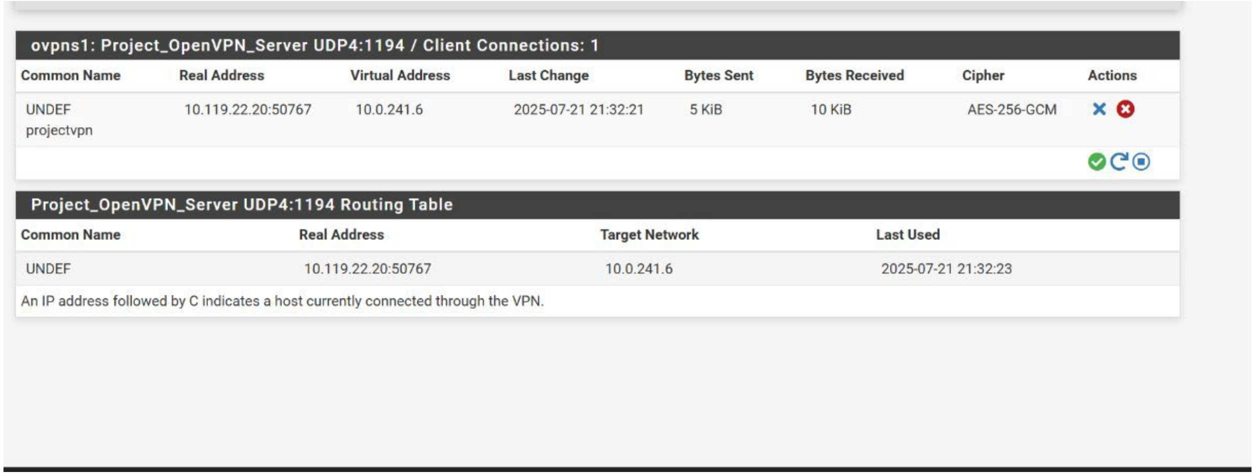
Bytes in: 5219 (5.1 KiB) out: 12291 (12.0 KiB)

OpenVPN GUI 11.54.0.0/2.6.14

Figure 4.14: Login Successful.

4.9 TUNNEL TESTING

- From the client device, executed ping 10.0.241.1 to test tunnel reachability
- Received successful replies from the pfSense OpenVPN interface, proving tunnel routing
- tracert 10.0.241.1 confirmed that traffic was directed through the VPN tunnel and not the default WAN



ovpns1: Project_OpenVPN_Server UDP4:1194 / Client Connections: 1

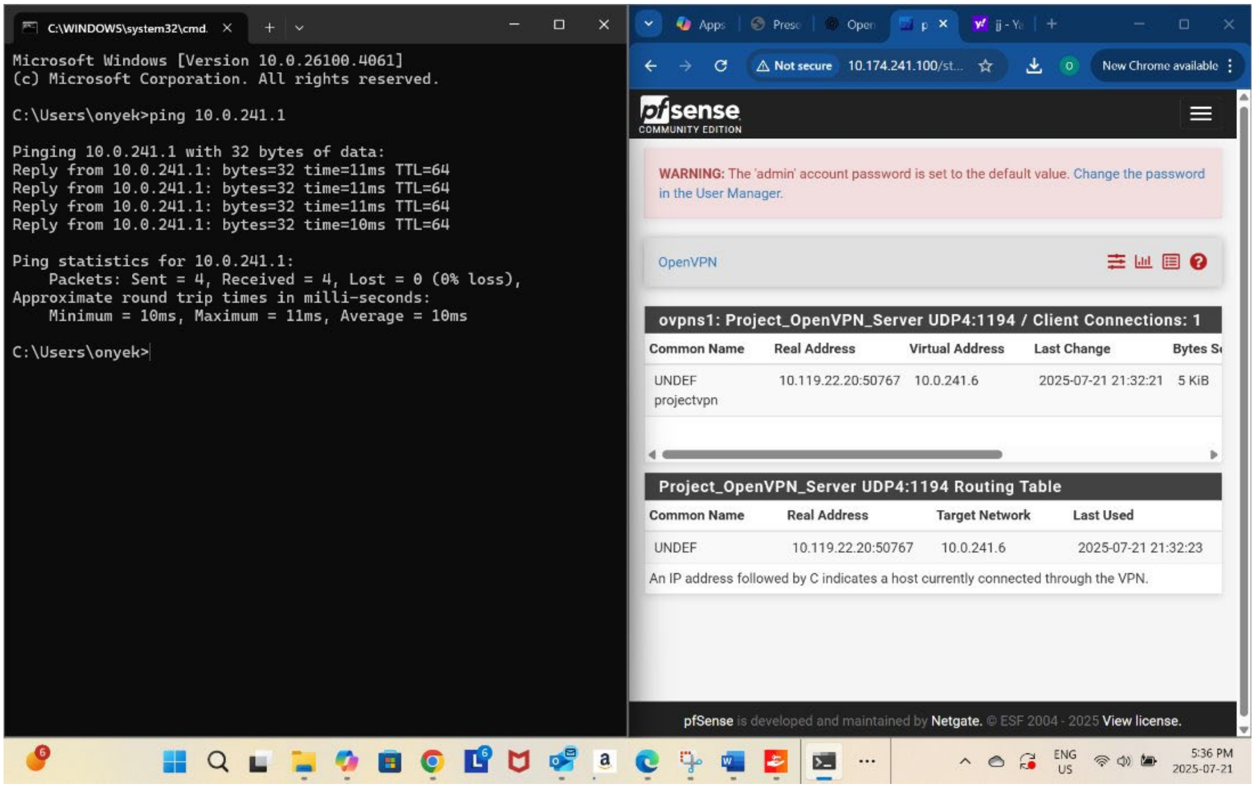
Common Name	Real Address	Virtual Address	Last Change	Bytes Sent	Bytes Received	Cipher	Actions
UNDEF projectvpn	10.119.22.20:50767	10.0.241.6	2025-07-21 21:32:21	5 KiB	10 KiB	AES-256-GCM	✕ ⊗

Project_OpenVPN_Server UDP4:1194 Routing Table

Common Name	Real Address	Target Network	Last Used
UNDEF	10.119.22.20:50767	10.0.241.6	2025-07-21 21:32:23

An IP address followed by C indicates a host currently connected through the VPN.

Figure 4.15: Status Configuration.



```
Microsoft Windows [Version 10.0.26100.4061]
(c) Microsoft Corporation. All rights reserved.

C:\Users\onyek>ping 10.0.241.1

Pinging 10.0.241.1 with 32 bytes of data:
Reply from 10.0.241.1: bytes=32 time=11ms TTL=64
Reply from 10.0.241.1: bytes=32 time=11ms TTL=64
Reply from 10.0.241.1: bytes=32 time=11ms TTL=64
Reply from 10.0.241.1: bytes=32 time=10ms TTL=64

Ping statistics for 10.0.241.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 11ms, Average = 10ms

C:\Users\onyek>
```

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

ovpns1: Project_OpenVPN_Server UDP4:1194 / Client Connections: 1

Common Name	Real Address	Virtual Address	Last Change	Bytes Se
UNDEF projectvpn	10.119.22.20:50767	10.0.241.6	2025-07-21 21:32:21	5 KiB

Project_OpenVPN_Server UDP4:1194 Routing Table

Common Name	Real Address	Target Network	Last Used
UNDEF	10.119.22.20:50767	10.0.241.6	2025-07-21 21:32:23

An IP address followed by C indicates a host currently connected through the VPN.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Figure 4.16: Ping Connection Successful.

5.0 CHALLENGES FACED

Challenge 1: TOTP Time Sync Failure

- The TOTP codes initially failed during authentication.
- Root cause: time drift between the pfSense firewall and the client device.
- Resolution: Enabled Network Time Protocol (NTP) on pfSense to maintain accurate time sync.

Challenge 2: FreeRADIUS Port Mismatch

- Authentication was rejected due to incorrect port configuration.
- Port 1812 (authentication) and 1813 (accounting) needed to match between pfSense and FreeRADIUS settings.
- Resolution: Verified and corrected ports in FreeRADIUS Interfaces tab and pfSense Authentication Servers.

Challenge 3: Firewall Rule Restrictions

- OpenVPN tunnel was established, but no traffic could pass.
- Resolution: Created correct firewall rules under both WAN and OpenVPN tab to allow necessary UDP and internal routing traffic.

6.0 LESSONS LEARNED

- FreeRADIUS and pfSense integration requires careful coordination across NAS clients, shared secrets, and authentication server setup.
- Two-Factor Authentication using TOTP is straightforward yet highly effective when system clocks are in sync.
- Firewall rules are critical in allowing or restricting tunnel traffic. Even a working tunnel can be functionally useless without them.
- Testing and debugging using logs, ping, and traceroute is a valuable methodical approach to troubleshooting network access issues.
- Exporting client profiles with the OpenVPN utility simplifies client-side configuration.

7.0 KEY TAKEAWAYS

- pfSense combined with FreeRADIUS and OpenVPN creates a flexible and secure enterprise-ready VPN infrastructure.
- TOTP-based 2FA strengthens authentication and is well-supported by mobile apps like Google Authenticator.
- Certificate management ensures encrypted tunnels, protecting data in transit.
- RADIUS allows centralized user authentication which scales better than managing local users.
- Consistent testing (e.g., ping, traceroute, log review) is necessary to ensure not just tunnel creation, but full operational routing.
- System time accuracy is non-negotiable for 2FA and must be enforced through NTP.

8.0 CONCLUSION

This project demonstrated the practical implementation of a secure OpenVPN host-to-network tunnel using pfSense with FreeRADIUS and TOTP-based 2FA. By combining encryption, multi-factor authentication, and access controls, the deployment emulates real-world enterprise VPN scenarios, equipping the student with valuable hands-on cybersecurity and network administration skills.

Beyond the technical configuration, the project provided key experience in managing service dependencies, ensuring time synchronization for TOTP reliability, and systematically resolving network and authentication issues. These are crucial competencies for any cybersecurity professional working in environments where secure remote access is required.

The layered security approach of using centralized FreeRADIUS authentication along with Google Authenticator for time-based codes significantly increases protection against unauthorized access, especially in scenarios involving credential compromise. Moreover, integrating these tools into a virtualized pfSense environment highlights the practicality and flexibility of open-source solutions in a professional setting.

Overall, this implementation aligns with industry best practices for VPN security and demonstrates the importance of combining technical accuracy, user training, and network policy enforcement to maintain strong, scalable, and resilient remote access infrastructures.

9.0 REFERENCES

National Institute of Standards and Technology (NIST). (2020). *Digital Identity Guidelines – SP 800-63-3*. Retrieved from NIST.gov: https://pages.nist.gov/800-63-3/

Netgate. (2024). *pfSense Documentation*. Retrieved from Netgate Documentation Portal: https://docs.netgate.com/pfsense/en/latest/

OpenVPN. (2023). *Community Wiki*. Retrieved from OpenVPN: https://community.openvpn.net