



# VPN & Network Defense

*Enhancing Network Defense with Remote Access VPN*

Brian F. Smith | Ethical Hacking & Countermeasures



## Project Objective

*To implement secure remote access through a VPN while applying robust access control methods to restrict unauthorized lateral movement within the network.*



# Internal Access Control Overview

**Primary Goal:** Prevent internal misuse or movement across systems.

**Techniques:**

- **VLANs & ACLs:** Enforce segmentation between network zones
- **802.1X:** Port-based device authentication
- **MAC Filtering:** Whitelist/blacklist devices
- **RBAC:** Access permissions based on roles
- **Device Posture Validation:** Ensure compliance before connection

# External Access Control Overview

**Primary Goal:** Block threats at the network perimeter.

**Mechanisms:**

- **Next-Gen Firewalls:** Traffic filtering with DPI
- **IDS/IPS:** Detect and respond to malicious activity
- **VPN Gateways:** Enable secure remote access
- **Web Proxies:** URL filtering, outbound content control
- **DDoS Mitigation:** Throttle malicious external traffic





# Benefits of Enforcing Access Control

- Shrinks the overall attack surface
- Stops lateral movement by compromised users/devices
- Helps enforce compliance with internal security policies
- Guards internal assets from internet-based threats
- Provides safe, authenticated remote access



# OpenVPN Integration in pfSense

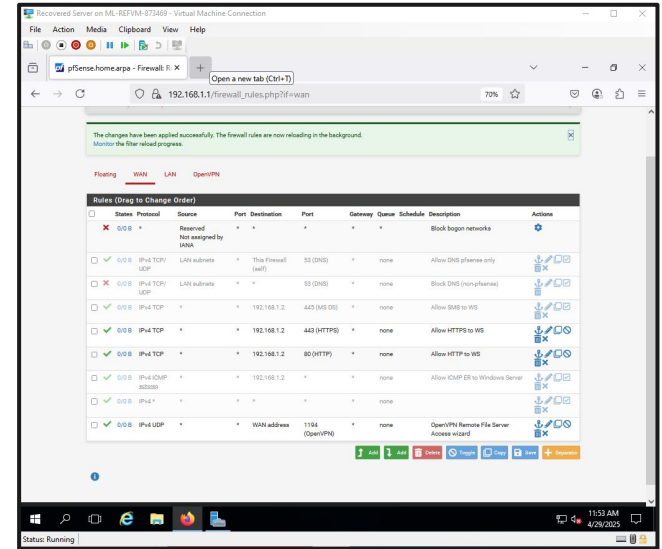
Once OpenVPN is installed, pfSense displays:

- Server/client configuration sections
- Tunnel network information (e.g., /24 over UDP 1194)
- Export tools and user/client management

# Firewall Rule Creation

Upon OpenVPN setup completion:

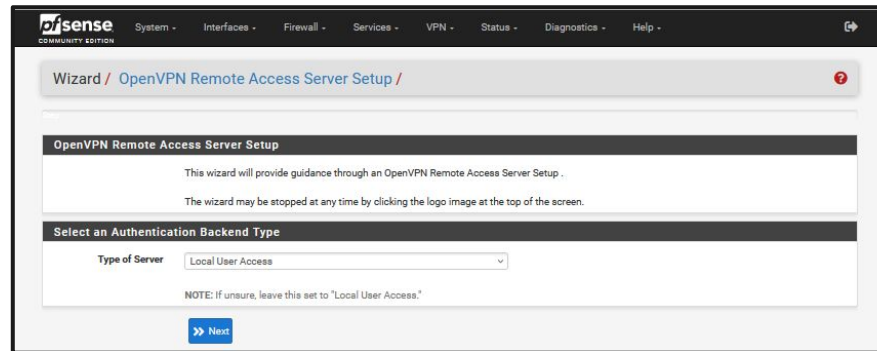
- New rules allow secure VPN traffic on port 1194
- Existing rules remain active (e.g., 80/443)
- VPN can override stricter LAN/WAN restrictions for authorized users



# Server Certificate Creation

Self-signed CA created for internal trust

- Each client assigned a user-specific certificate
- Example: user **johndoe** linked to OpenVPN Local User Access CA



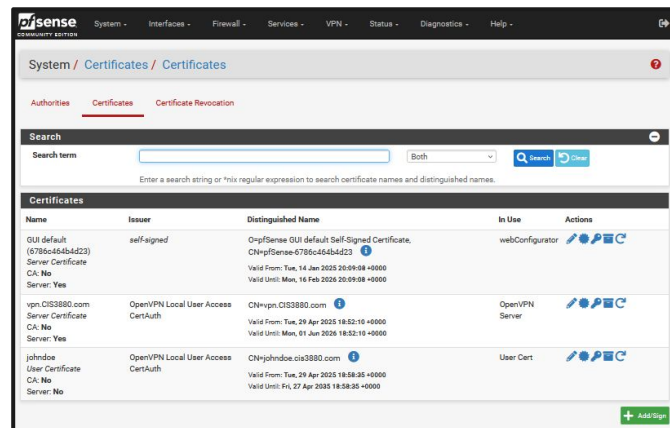


# Why Certificate Authorities Matter

A Certificate Authority (CA) confirms trust between the VPN server and its users.

## Key Functions:

- Verifies identity with signed certs
- Enables TLS encryption
- Prevents spoofed access
- Centralized control for issuing/revoking credentials





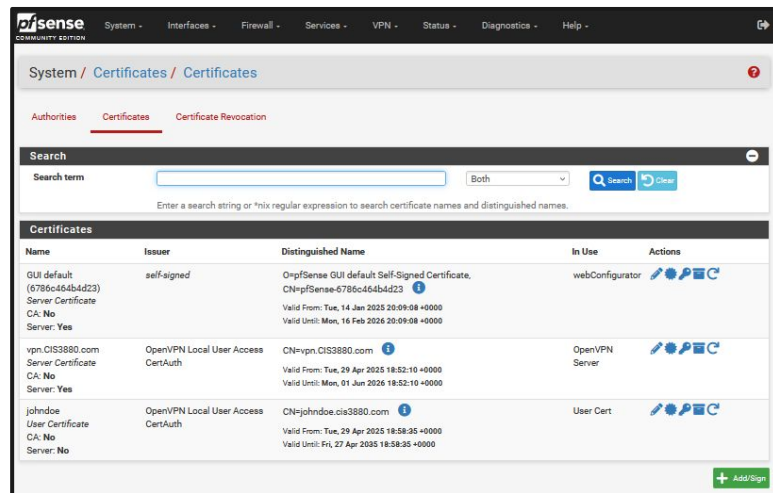
# Subnet and Network Design

## Purpose of Subnetting:

- Isolate zones for policy enforcement
- Reduce broadcast domains and improve performance
- Simplify routing and address management
- Map access policies cleanly across devices

# User and Certificate Setup

- Screenshot of user creation with cert
- Describe:
  - Importance of user-specific certificates
  - Binding credentials to identity

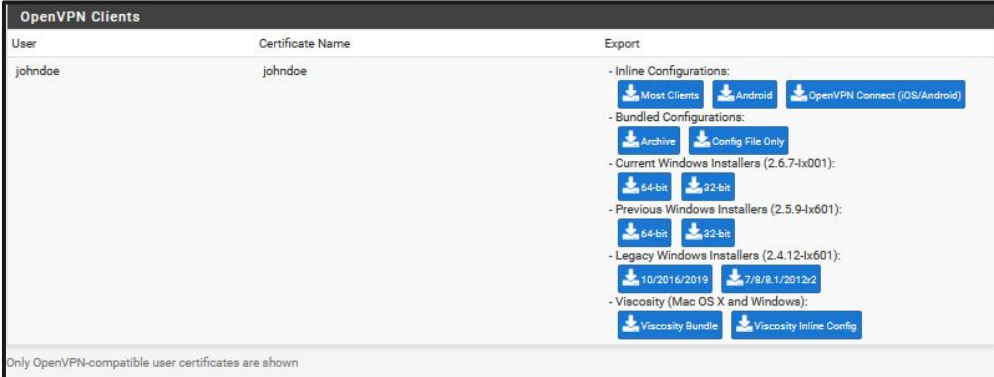


# Client Export and Configuration

VPN client installed on remote machine (e.g., Azure host)

Tray icon allows connection toggle

User logs in using credentials + certificate (e.g., johndoe)

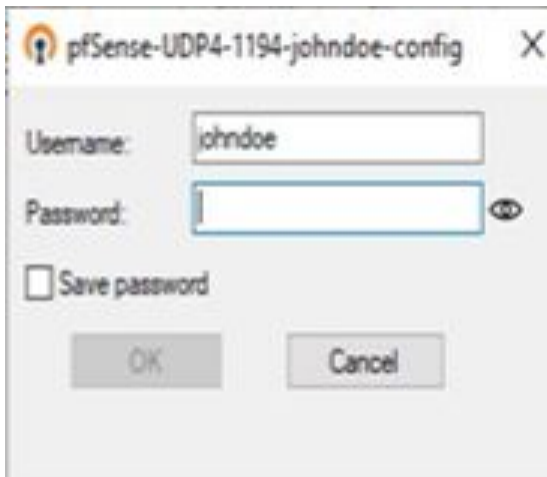
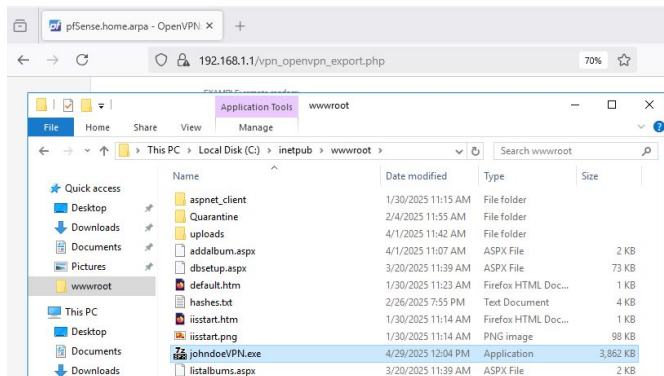


The screenshot displays the 'OpenVPN Clients' interface. It features a table with two columns: 'User' and 'Certificate Name'. A single entry for 'johndoe' is visible. To the right of the table is an 'Export' section with various download links categorized by platform and configuration type. At the bottom, a note states: 'Only OpenVPN-compatible user certificates are shown'.

User	Certificate Name	Export
johndoe	johndoe	<div><div><div>Inline Configurations:</div><div><a href="#">Most Clients</a> <a href="#">Android</a> <a href="#">OpenVPN Connect (iOS/Android)</a></div></div><div><div>Bundled Configurations:</div><div><a href="#">Archive</a> <a href="#">Config File Only</a></div></div><div><div>Current Windows Installers (2.6.7-ix001):</div><div><a href="#">64-bit</a> <a href="#">32-bit</a></div></div><div><div>Previous Windows Installers (2.5.9-ix601):</div><div><a href="#">64-bit</a> <a href="#">32-bit</a></div></div><div><div>Legacy Windows Installers (2.4.12-ix601):</div><div><a href="#">10/2016/2019</a> <a href="#">7/8/8.1/2012/2</a></div></div><div><div>Viscosity (Mac OS X and Windows):</div><div><a href="#">Viscosity Bundle</a> <a href="#">Viscosity Inline Config</a></div></div></div>

Only OpenVPN-compatible user certificates are shown

# Client Export and Configuration



# Shared Folder Access Without VPN

Without VPN active, port 445 blocks access to internal shares

Connection attempts to network drives stall or fail

Access is only permitted once connected through VPN





# Shared Folder Access With VPN

With VPN enabled, user can access internal drives

File share (e.g., `\\192.168.1.10\cis`) is reachable

Encrypted communication secures data in transit



# Network Policy and Enforcement

**Purpose:** Enforce how devices/users interact with network assets.

**Policy Elements:**

- Access restrictions by role/device
- Baseline configs for secure operations
- Continuous monitoring/auditing
- Dynamic enforcement via NAC/firewalls





# How VPN Enhances Security

**Encryption:** Protects data from interception

**Authentication:** MFA/certificates confirm identity

**Granular Access:** Policies apply even offsite

**Split Tunneling:** Custom routing of user traffic

**Endpoint Validation:** Check compliance before access

11

User and Certificate Setup

12

Client Export and Configuration

13

Client Export and Configuration

14

General Server Access Without VPN

15

General Server Access With VPN

16

Network Policy and Enforcement

# VPN & Network Defense

*Enhancing Network Defense with Remote Access VPN*

Brian F. Smith | Ethical Hacking & Countermeasures

Version history

All versions

Last week

▶ April 29, 11:49 PM

Current version

Brian

▶ April 29, 3:06 PM

Brian

▶ April 29, 12:20 PM

Brian

April 29, 11:56 AM

Brian