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

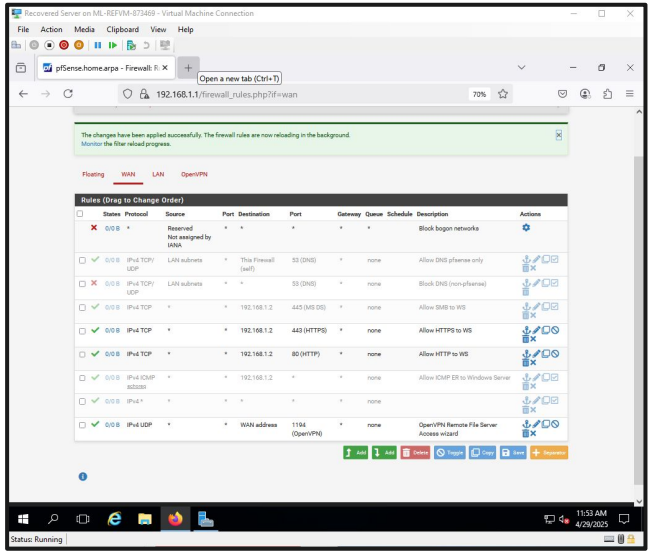
Once OpenVPN is installed, pfSense displays:

- 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:

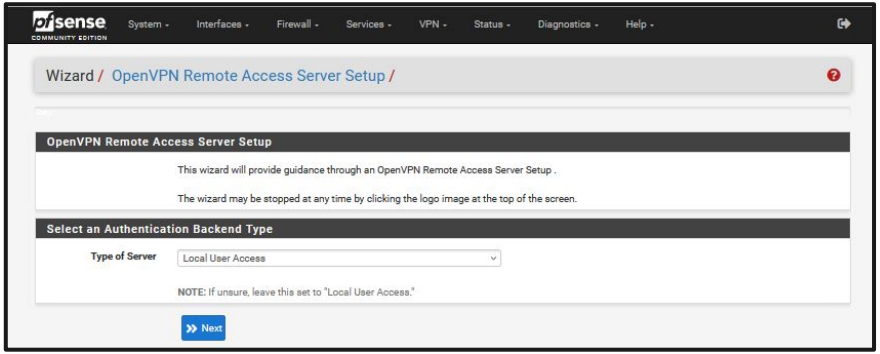
- New rules allow secure VPN traffic on port 1194
- Existing rules remain active (e.g., 80/443)
- VPN can override stricter LAN/WAN restrictions for authorized users



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

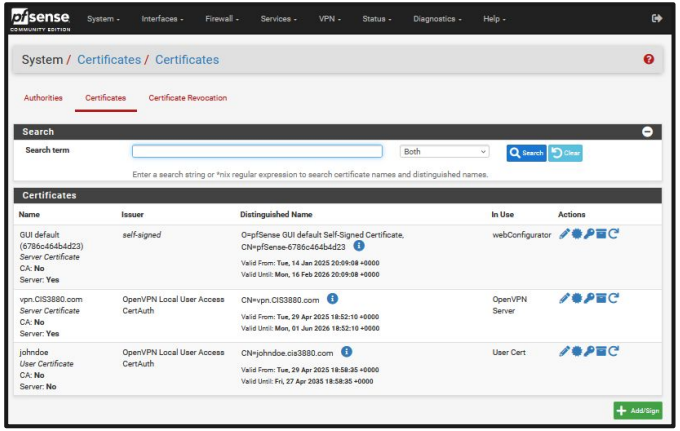


Why Certificate Authorities Matter

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



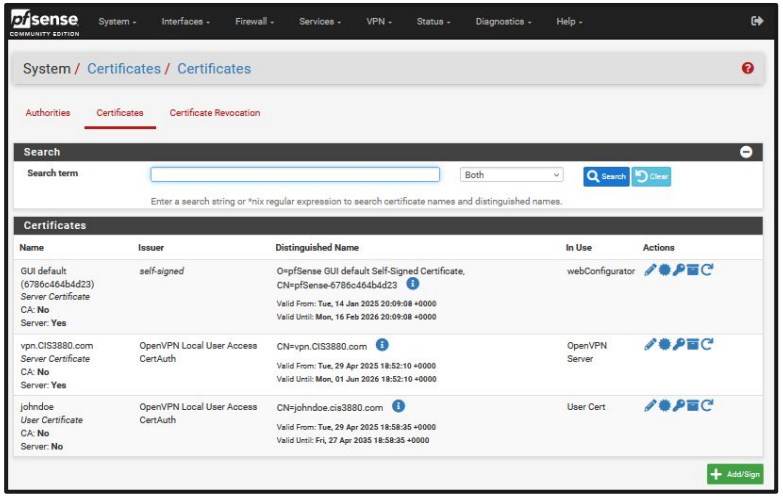
Subnet and Network Design

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

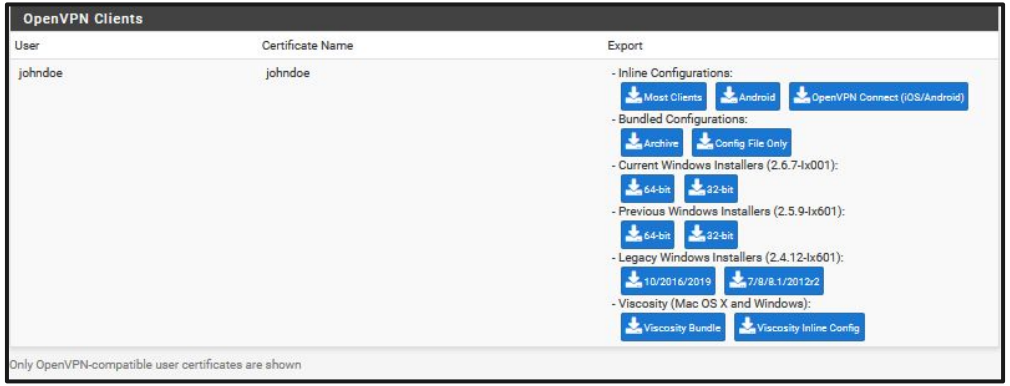


Client Export and Configuration

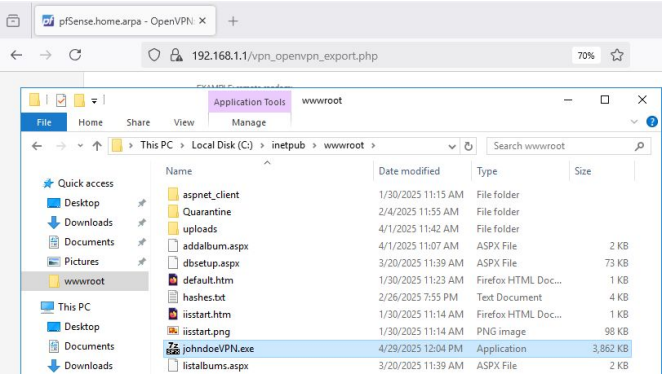
VPN client installed on remote machine (e.g., Azure host)

Tray icon allows connection toggle

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



Client Export and Configuration

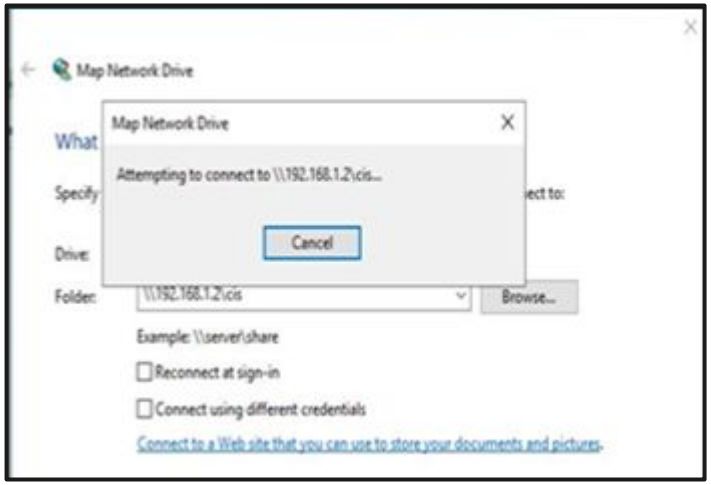


Shared Folder Access Without VPN

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

VPN & Network Defense

Enhancing Network Defense with Remote Access VPN

Brian F. Smith | Ethical Hacking & Countermeasures