

Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

Student:

Vidhi Kadakia

Email:

jinsukrishna108@gmail.com

Time on Task:

6 hours, 7 minutes

Progress:

100%

Report Generated: Sunday, November 23, 2025 at 6:37 PM

Section 1: Hands-On Demonstration

Part 1: Configure an IPsec VPN Server

18. Make a screen capture showing the updated Certificate Authorities table.

The screenshot shows the pfSense web interface for managing certificates. The title bar indicates "Configuring a VPN Server with pfSense (3e) v1Workstation". The main window is titled "System / Certificate Manager / CAs". A red warning message at the top says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, there are tabs for "CAs", "Certificates", and "Certificate Revocation". The "CAs" tab is selected. A search bar is present. The table lists one certificate authority:

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
IPsecVPN_VidhiKadakia	✓	self-signed	0	ST=Kentucky OU=Cybersecurity, O=Northern Kentucky University, L=Highland Heights, CN=internal-ca, C=US Valid From: Sat, 22 Nov 2025 20:59:01 +0000 Valid Until: Tue, 20 Nov 2038 20:59:01 +0000		Edit Delete Details

At the bottom of the page, it says "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license." and shows the date "11/22/2025" and time "12:59 PM".

Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

32. Make a screen capture showing the updated Certificates table.

The screenshot shows the pfSense Certificate Manager interface. The title bar reads "Configuring a VPN Server with pfSense (3e) vWorkstation". The main content area is titled "Certificates" and shows two entries:

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense-93559202000000000000000000000000	No	edit, delete, details
IPsecVPN_dhchallenge	ST=Kentucky, O=OpenWrt, CN=Northern Kentucky University, L=Highland Heights, OH-902-2011, C=US	Valid From: Sat, 22 Mar 2023 21:28:49 +0000 Valid Until: Tue, 29 Nov 2022 16:07:43 +0000	Yes	edit, delete, details

At the bottom right of the table, there is a green "+ Add New" button.

56. Make a screen capture showing the updated IPsec Tunnels table.

The screenshot shows the pfSense IPsec Tunnels table. The title bar reads "Configuring a VPN Server with pfSense (3e) vWorkstation". The main content area is titled "IPsec Tunnels" and shows one entry:

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transform	P1 DH Group	P1 Description	Actions
V2	WAN	AES (128 bit)	SHA256	14 (2048 bit)	MobilePass		edit, delete, details

At the bottom right of the table, there is a green "+ Add New" button.

Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

74. Make a screen capture showing the updated Pre-Shared Keys table.

The screenshot shows the pfSense configuration interface for a VPN server. The title bar reads "Configuring a VPN Server with pfSense (3e) v1Workstation". The top navigation bar includes "System", "Interfaces", "Firewall", "Diagnostics", and "Help". The Firewall dropdown shows "2025-11-22 16:20:53". The User Manager dropdown shows "Vidhi Kadakia". A red warning message at the top states: "WARNING: The admin account password is set to the default value. Change the password in the User Manager." Below this, a green message says "The changes have been applied successfully." The main content area has tabs for "Tunnels", "Mobile Clients", "Pre-Shared Keys" (which is selected), and "Advanced Settings". The "Pre-Shared Keys" table lists one entry:

Identifier	Type	Pre-Shared Key	Actions
remoteworker01	EAP	password1	

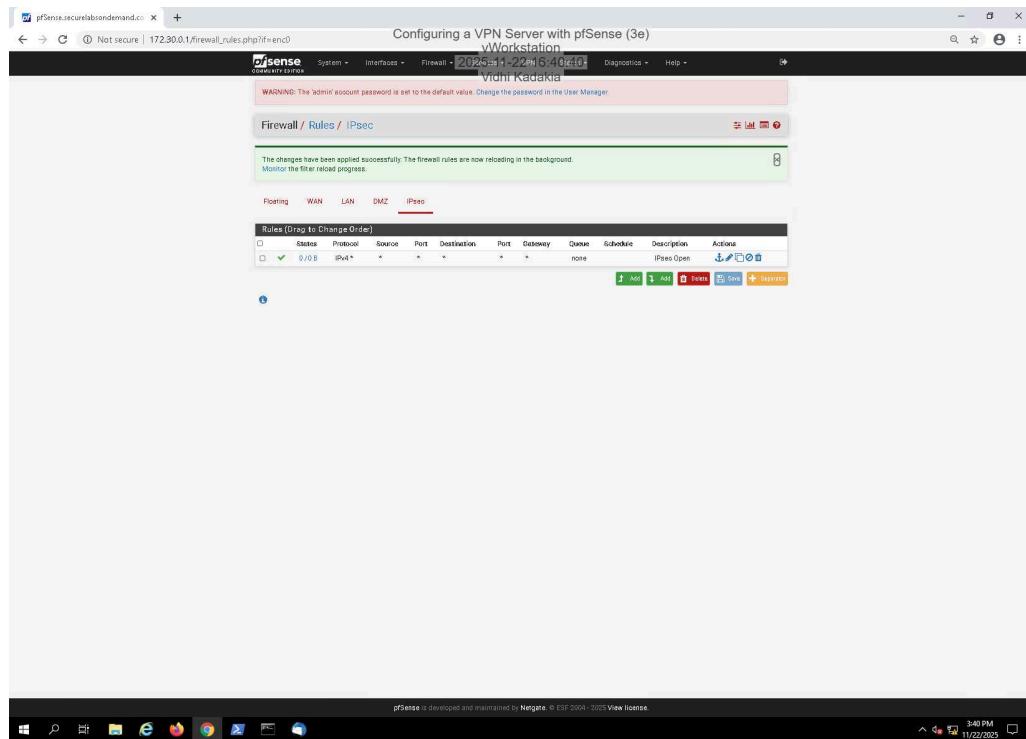
A green "+ Add" button is located at the bottom right of the table. The pfSense footer indicates it is developed and maintained by Netgate © EST 2004 - 2023 View License. The system status bar at the bottom right shows "3:20 PM" and "11/22/2025".

Part 2: Configure a Firewall Rule for VPN Traffic

Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

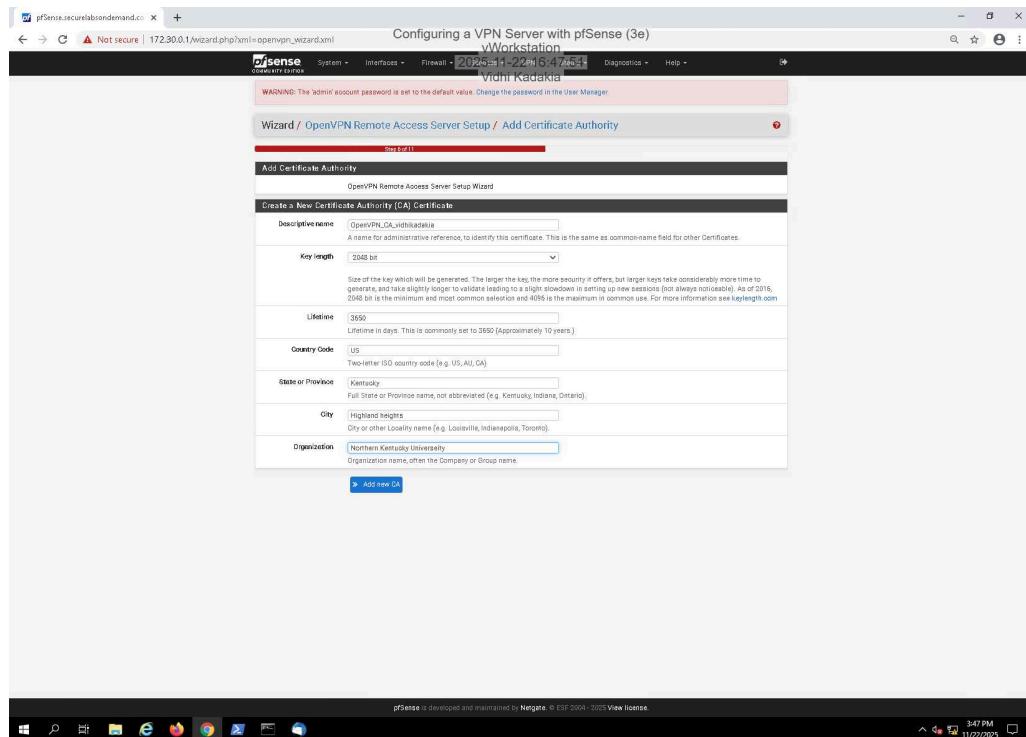
9. Make a screen capture showing the updated IPsec Rules table.



Section 2: Applied Learning

Part 1: Configure an OpenVPN VPN Server

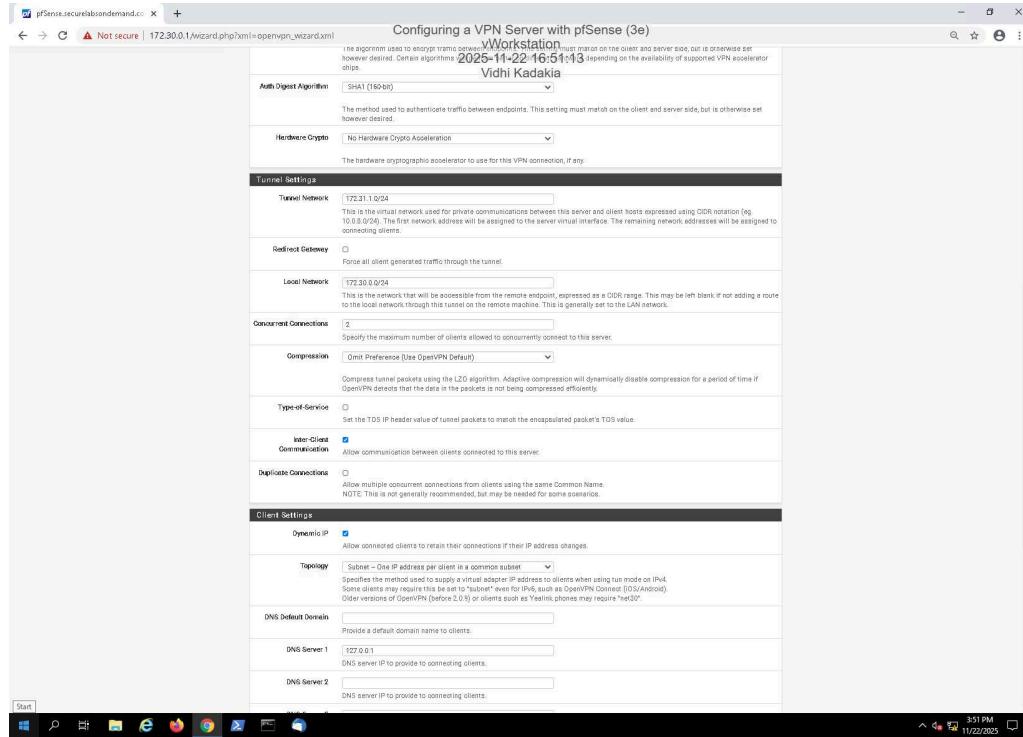
13. Make a screen capture showing the CA configuration form.



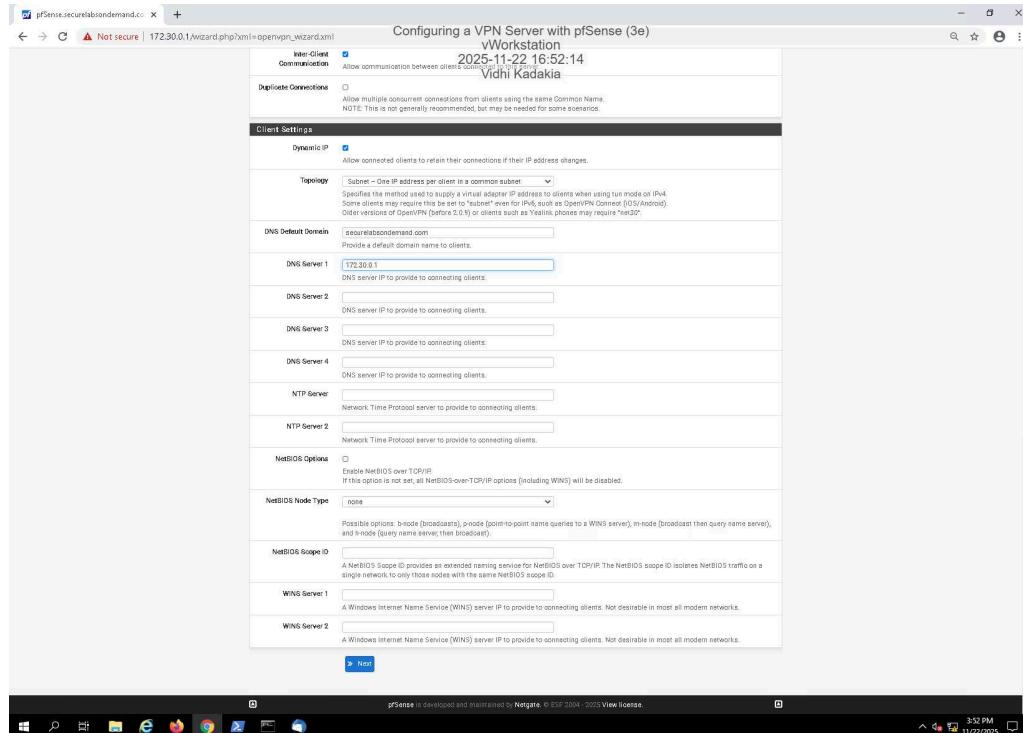
Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

27. Make a screen capture showing the Tunnel Settings section.

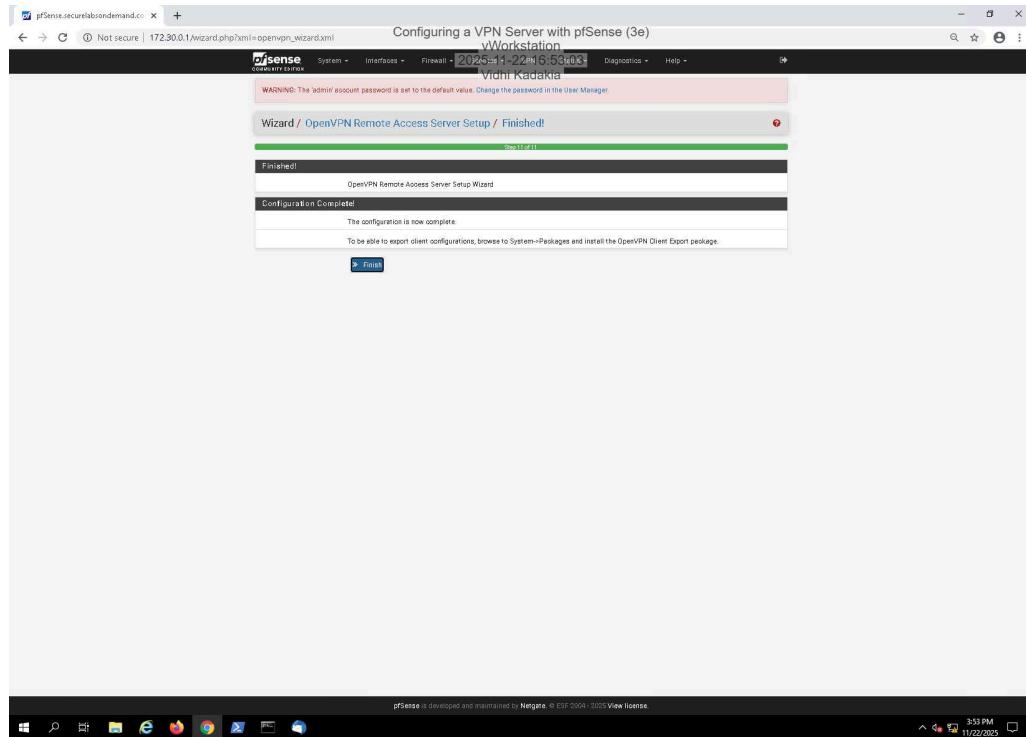


30. Make a screen capture showing the Client Settings section.



Part 2: Configure a Firewall Rule for VPN Traffic

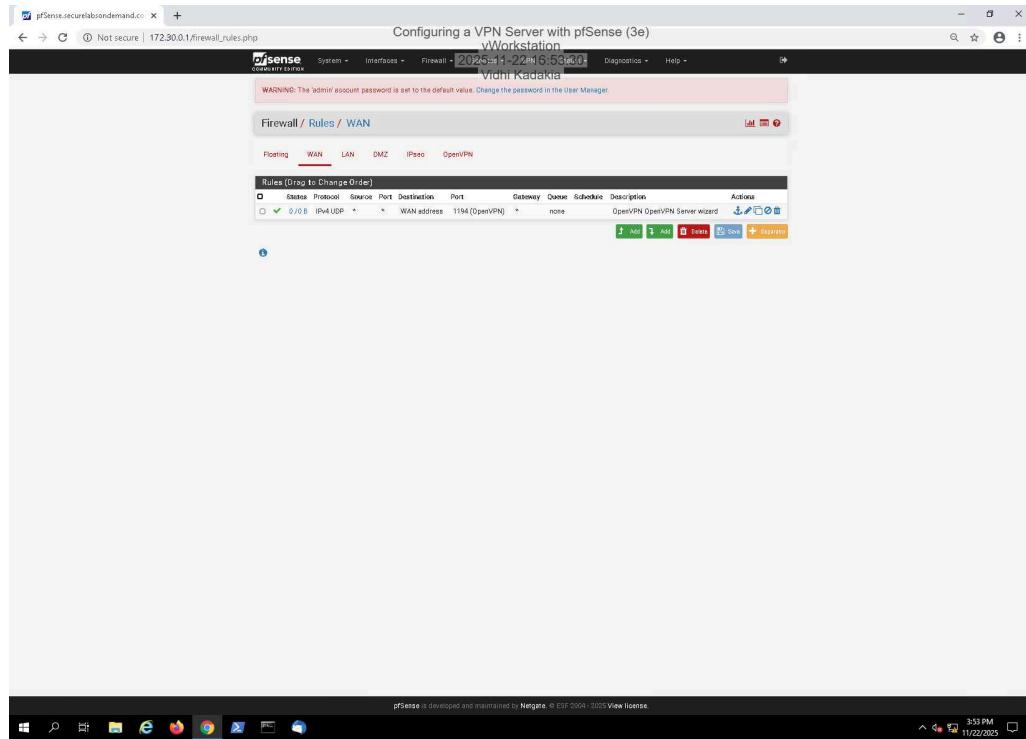
2. Make a screen capture showing the completed OpenVPN configuration.



Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

5. Make a screen capture showing the OpenVPN rule on the WAN Rules table.

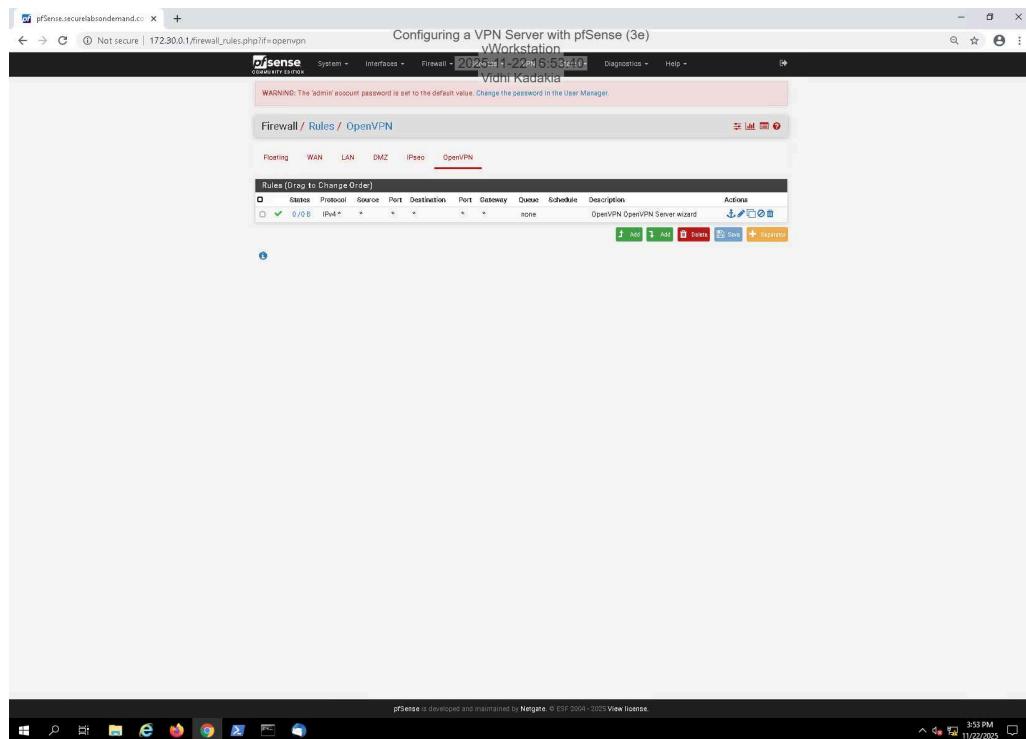


The screenshot shows the pfSense Firewall Rules table for the WAN interface. There is one rule listed:

Status	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action			
✓	0/0 B	IPv4:UDP	*	*	1194 [OpenVPN]	*	none		OpenVPN OpenVPN Server wizard				

Below the table are buttons for Add, Edit, Delete, Save, and Log.

7. Make a screen capture showing the OpenVPN rule on the OpenVPN Rules table.



The screenshot shows the pfSense Firewall Rules table for the OpenVPN interface. There is one rule listed:

Status	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action			
✓	0/0 B	IPv4*	*	*	*	*	none		OpenVPN OpenVPN Server wizard				

Below the table are buttons for Add, Edit, Delete, Save, and Log.

Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

Section 3: Challenge and Analysis

Part 1: Enable IP Roaming for Remote VPN Clients

Make a screen capture showing the enabled MOBIKE option in the IPsec tunnel configuration.

The screenshot shows the pfSense IPsec tunnel configuration page for a connection named 'VWorkstation'. The 'Phase 1 Proposal (Encryption Algorithm)' section has 'AES' selected as the encryption algorithm, '128 bits' as the key length, and 'SHA256' as the hash function. The 'MOBIKE' option is set to 'Enable'. The 'Save' button is visible at the bottom left of the configuration form. The pfSense footer at the bottom indicates it is developed and maintained by Netgate, with a license link and copyright information from 2004-2025.

Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

Part 2: Create Explicit Firewall Rules for an IPsec VPN

Make a screen capture showing the disabled automatic IPsec rule creation option.

The screenshot shows the pfSense web interface under the 'System / Advanced / Firewall & NAT' section. A green message bar at the top states 'The changes have been applied successfully.' Below it, the 'Firewall Advanced' tab is selected. In the 'Disable Auto-added VPN rules' section, there is a checked checkbox labeled 'Disable all auto-added VPN rules.' A note below it says 'Note: This disables automatically added rules for IPsec.' The rest of the page contains various configuration options for firewall timeouts, maximum states, and fragment entries, all of which appear to be standard settings without specific modifications.

Configuring a VPN Server with pfSense (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 08

Make a screen capture showing your firewall rules that permit IPsec traffic.

The screenshot shows the pfSense Firewall Rules configuration interface for the WAN tab. A message at the top states: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." A green "Apply Changes" button is visible. The main table lists four IPsec rules:

Index	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
1	0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN OpenVPN Server wizard		
2	0 / 0 B	IPv4 UDP	*	*	This Firewall	500 (ISAKMP)	*	none		allow IKE (UDP 500) for IPsec VPN		
3	0 / 0 B	IPv4 UDP	*	*	This Firewall	4500 (IPsec NAT-T)	*	none				
4	0 / 0 B	IPv4 ESP	*	*	This Firewall	*	*	*	none			

At the bottom, there are buttons for Add, Save, and Separator. The pfSense footer includes the license information: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license."