This step-by-step process started with this article:

DUO Implementation for pfSense Based OpenVPN Server with RADIUS (AD) Integration - Step by Step | Netgate Forum

Cmkrs: Thanks for the great start.

A few items I had to add and validate to make it all work.

Start with following the beginning section of this document: https://duo.com/docs/radius to get your application registered with DUO - you'll need the 3 keys they give you.

Install the DUO Authentication/Proxy Server using this article: https://duo.com/docs/radius#install-the-duo-authentication-proxy

a) The [radius_client] in DUO Authenticator/Proxy language is actually your Radius Server (NPS). Example IP address: 192.168.11.100
- To start: access your NPS server and create a new Radius_Client entry under NPS-Radius Clients and Servers-Radius Clients: These instructions are for Windows 2022 NPS
- Give it a friendly name such as DUO Proxy
- Set the IP address or FQDN of the machine hosting the DUO Authentication/Proxy server: example: 192.168.11.150
  - Click <Verify> then <Resolve> then <OK>

- Generate or enter a Shared Secret - make sure you keep this somewhere - you can always 'see' it by clicking the 'Generate' button (example: Th3r3!$N03y3!nT3@mButTh3r3!$M3)
- Click on the 'Advanced' tab and choose 'Radius Standard' as the Vendor Name.
- Click OK.

- there are more settings to completely create a Radius server under Windows/NPS/Radius Server
- here is a great link I used: https://thesolving.com/server-room/configure-radius-server-windows-authenticate-cisco-vpn-users/

b) in the DUO Proxy authproxy.cfg file -Noted in the DUO Authentication/Proxy setup is how to navigate to this section: https://duo.com/docs/radius

- Create a [radius_client] if it does not exits - I edited the default [ad_client] and changed the name to [radius_client]
- You only need these two sections - well documented here: https://duo.com/docs/radius - remove the ones you don't need and add the ones you do need

  - host=<IP address of your NPS server from (a) above> Example: 192.168.11.100
  - secret=<The secret you created or generated on the NPS server for the DUO Proxy server:192.168.11.150 (from above: the example secret is: Th3r3!$N03y3!nT3@mButTh3r3!$M3)

- Edit the [radius_server_auto] (Create if necessary - but the default layout has one)
  -ikey=DUO_Identification_Key_From_DUO_App_Protection_Settings_Page

-skey= DUO_Secret_Key_From_DUO_App_Protection_Settings_Page
-api_host= DUO_API_Host_From_DUO_App_Protection_Settings_Page
-radius_ip_1=LAN_IP_Address_Of_pfSense device: Example: 192.168.11.200
-radius_secret_1= This is a shared secret between the DUO Proxy and the pfSense device - you can create it or use a prior secret, but it must be same here and in the pfSense Radius configuration below. (Example: Th3C0wJump0v3rTh3M00n@tN!ght)
-failmode=safe
-client=radius_client (MUST match the section above - and is case sensitive)
-port=1812
Click <Validate>

- you will get an error if you are using a Windows NPS Radius server
- this can be found under the Event Viewer on the NPS Radius Server - <System>
- Event ID 16, Error, Source:NPS, Message: A RADIUS message with the Code field set to 12, which is not valid, was received on port 1812 from RADIUS client DuoProxy. Valid values of the RADIUS Code field are documented in RFC 2865.
- Windows Radius does not support Code 12 - has been an issue for over 10+ years - google it to see the thread
- here is a good summary: https://social.technet.microsoft.com/Forums/windowsserver/en-US/2c2b59ee-fc02-4fe4-bc5e-b3f0ab54ca72/when-will-the-ms-server-support-radius-code-field-12-statusserver?forum=winserverNIS

Click <Start Service> or <Restart Service>

c) On your pfSense device set up a new Radius authentication server (pfSense device IP example being used: 192.168.11.200 - same as in the DUO Authentication/Proxy config)
- navigate to <System><User Manager>
- click on the Authentication Server group (far Right in pfSense 23.05)
- Click <Add>
- Give it a friendly name: DuoProxy (example)
- Type: Radius
- Protocol: MS-CHAPv2
-IP address of the DUO Proxy Server - same one you put into the NPS configuration: example being used is 192.168.11.150 above
- Share secret: this is the secret you created for the [radius_server_auto] section above when configuring the DUO Authentication/Proxy application (from above: Th3C0wJump0v3rTh3M00n@tN!ght)
- Services Offered: Authentication and Accounting
- Authentication Port: 1812
- Authentication timeout: 5
- Radius NAS IP Attribute (WAN port hosting the dial in OpenVPN)
- Click Save

- Navigate to <VPN><OpenVPN>
- Click on Pencil icon (far right) for your <Remote Access (User Auth) server

- if you don't have this server then you need to set it up - pfSense/Netgate has a great article on the process: https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/authenticating-openvpn-users-with-radius-via-active-directory.html

- Scroll down to <Backend for authentication> and change the selection to your Radius Authentication Friendly Name (ex: DUOProxy)
- Scroll down and click <Save>

d) Log into your DUO account online
- Select a user: (example: Administrator) by clicking on the name
- Ensure the <Status> is set to <Active> - this means the user must use MFA (Dual Factor Authentication)
- Ensure there is a phone attached to this user - Navigate down to PHONES
- Verify the phone is <Activated> This is very important as you cannot use SMS with the DUO Proxy server - only the DUO Authenticator (well this is the only method that worked for me)
  - what does this mean? It means the phone has the DUO authenticator installed and activated.
  - if not click the <Activate DUO Mobile> and it will send you a link to install app and activate the phone.

Test by having a computer with the OpenVPN Client installed + necessary certificates, etc.
- I tested by going directly to the Radius Server (NPS) in my pfSense configuration (created a separate Authentication Server) to verify it was working then I switched <Backend for Authentication> on my pfSense device to DUOProxy for the MFA test.

My test activated a PUSH notification from DUO to my phone where I clicked <Ok> and I was logged into the OpenVPN server.

Credits: This is a compilation of several articles on the WEB, but it started here with this article as it had the most information. Thanks.