8.3.2 Remote user to a web server:

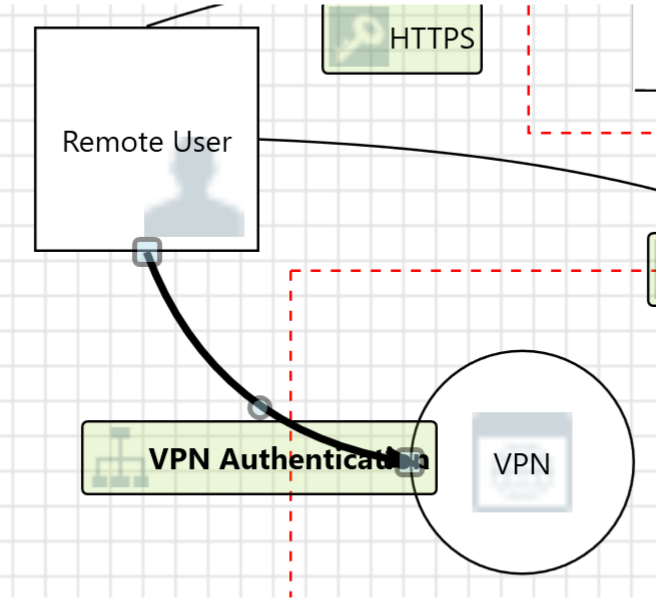

Figure 7: VPN Authentication

In Figure 7, VPN authentication by a remote user is depicted. Listed below are potential threats and corresponding measures to mitigate them.

Elevation Using Impersonation

Category:	Elevation Of Privilege
Description:	VPN may be able to impersonate the context of Remote User in order to gain additional privilege.
Mitigation:	User authentication will be done through Single Sign On (SSO) with MFA enabled for all external connections (Grassi et al., 2017).

VPN May be Subject to Elevation of Privilege Using Remote Code Execution

Category:	Elevation Of Privilege
Description:	Remote User may be able to remotely execute code for VPN.
Mitigation:	A key principle of Zero Trust Access is to grant the user only the necessary privileges, known as the least privilege approach.

Elevation by Changing the Execution Flow in VPN

Category:	Elevation Of Privilege

Description:	An attacker may pass data into VPN in order to change the flow of program execution within VPN to the attacker's choosing.
Mitigation:	ZTNA will be used to avoid VPN-related attacks. ZTNA solutions commonly use robust authentication methods to confirm the identity of users and devices seeking to access resources. These may involve multi-factor authentication (MFA), certificates, or other reliable forms of authentication. By guaranteeing that only authorised users with validated identities are granted access, ZTNA minimizes the likelihood of unauthorized privilege escalation.