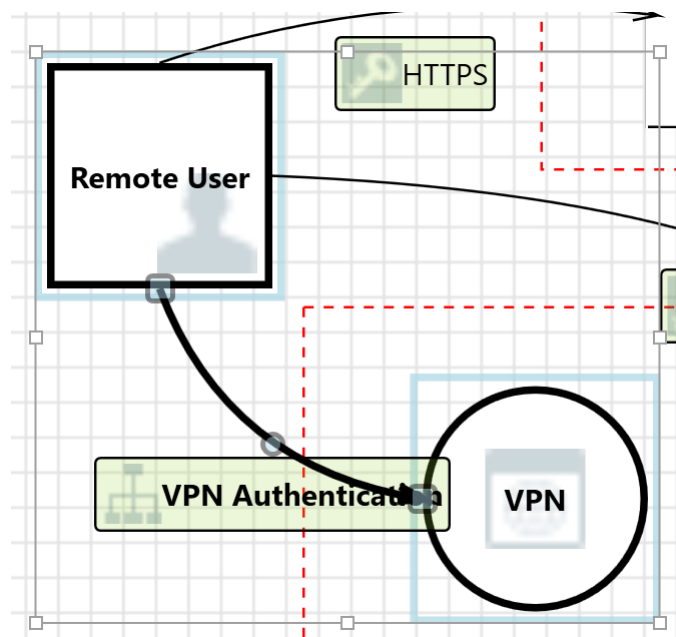### 8.3.8 Remote User to VPN:

Figure 13: Remote user to VPN

In Figure 13, the remote user to VPN is depicted. Listed below are potential threats and corresponding measures to mitigate them.

1.1.1.1 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).

1.1.1.2 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:	Zero Trust Network Access will be used to avoid issues related to on-prem VPN

1.1.1.3 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:	Zero Trust Network Access will be used to avoid issues related to on-prem VPN.