# 2023/08/31: TunnelCrack protection implemented in SoftEther VPN Client

Daiyuu Nobori, August 31, 2023

TunnelCrack protection has been implemented in SoftEther VPN Client.

TunnelCrack is a security attack technique pointed out in the paper "Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables" presented at the international conference USENIX Security '23 on August 11, 2023.

The TunnelCrack attack technique is problematic when using malicious and untrusted public wireless LANs. Various popular VPN client software can be affected by the TunnelCrack attack method, which requires countermeasures on the part of the VPN client software.

We have added TunnelCrack protection in **SoftEther VPN Client Ver 4.43 Build 9799 Beta (8/31/2023)**. TunnelCrack protection can be easily enabled from the settings screen and prohibits TCP and UDP connections for physical local network communication during the VPN connection. This provides additional protection when using untrusted public wireless LANs.

SoftEther VPN Client's TunnelCrack protection function addresses both LocalNet Attack and ServerIP Attack.

Below is the TunnelCrack protection configuration screen in SoftEther VPN Client.




Note that when TunnelCrack Protection is enabled, TCP and UDP connections over the physical local LAN are prohibited while the VPN connection is established. This protection is beneficial when using unreliable public Wi-Fi. On the other hand, enabling TunnelCrack protection will also prevent you from accessing servers on trusted LANs, such as the company LAN, and simultaneously accessing servers to which you have a VPN connection. Please be aware of this.

When TunnelCrack protection is activated, TCP connections already established prior to activation will be maintained without being disconnected. New TCP and UDP connections established after activation will be blocked.