Instrukcja obsługi OpenVPN dla pracowników UMK

Na podstawie informacji z Uniwersyteckiego Centrum Informatycznego

Informacje i uwagi:

1. Usługa OpenVPN jest dostępna dla pracowników, którzy mają zainstalowany indywidualny profil VPN wydany na te potrzeby. Usługa ta umożliwia autoryzowany dostęp do:
   - serwerów pocztowych, w przypadku, gdy provider internetowy uniemożliwia wysyłanie maili lub gdy wysyłanie maili przez serwer dostawcy stwarza problemy (np. klasyfikuje wysyłane maile jako spamy),
   - wybranych systemów zarządzania, np. USOSadm.
2. Uwagi przy uzyskiwaniu dostępu do konkretnych usług:
   - W celu dostępu do usług USOSadm lub XPrimer nie jest potrzebne przekazywanie adresu IP do Działu Usług Sieciowych.

Zdalny pulpit

Pracownicy administracji

- Regulacje i sposób postępowania w sprawie dostępu pracowników administracji do lokalnych stacji roboczych za pośrednictwem usługi pulpitu zdalnego (RDP) reguluje ZARZĄDZENIE Nr 42 Kanclerza Uniwersytetu Mikołaja Kopernika w Toruniu z dnia 31 grudnia 2021 r. dostępne pod adresem: https://dokumenty.umk.pl/423-lista/d/7183/5/.
- Pracownikiem administracji jest osoba zatrudniona na stanowisku (nie funkcji) wymienionym w par. 10 punkt 1. 1) Regulaminu Organizacyjnego UMK

Pozostali pracownicy

- Aby uzyskać dostęp do zdalnego pulpitu swojego komputera w pracy, należy przekazać do Działu Sieci Lokalnych i Monitoringu adres IP tego komputera.
- Jeżeli na komputerze zainstalowany jest ESET (...) Security i blokuje połączenie, to należy skonfigurować zaporę sieciową ESET-a pod zdalny pulpit. Ewentualnej pomocy w zakresie konfiguracji ESET-a udziela Dział Sieci Lokalnych (pomoc@uci.umk.pl lub 56-611-2727).

Adres IP

- Adres IP swojego komputera w pracy można uzyskać po wejściu na stronę https://ip.uci.umk.pl/, na stronę należy wejść z komputera w sieci UMK, nie z komputera domowego.

3. OpenVPN – instalacja:

Profil konfiguracyjny należy pobrać z serwera profili VPN. Gdy mamy już profil VPN, wykonujemy następujące kroki:

System Windows

- Instalujemy klienta usługi OpenVPN, którego możemy pobrać pod adresem strony pobrań producenta: https://openvpn.net/community-downloads/, zalecamy korzystanie z najnowszej wersji.
- Pobrany wcześniej profil VPN zapisujemy w podkatalogu OpenVPN\config głównego katalogu użytkownika.
- Uruchamiamy OpenVPN GUI, na przykład przy pomocy ikony na pulpicie (w przyszłości program będzie się uruchamiał automatycznie przy starcie systemu Windows).
- Klikamy prawym przyciskiem myszy na ikonę OpenVPN GUI w pasku zadań (uwaga może być ukryta i wymagać rozwinięcia menu po prowej stronie dolnego paska menu) i wybieramy Połącz.
- Przy pierwszym połączeniu pojawi się pytanie o hasło - proszę podać hasło pobrane ze strony serwera profili VPN i zaznaczyć opcję "Save password", by nie było potrzebne podawanie hasła przy kolejnych uruchomieniach.

System MacOS

- Pobieramy aplikację Tunnelblick https://tunnelblick.net/downloads.html, zalecamy korzystanie z wersji stable, obecnie 3.8.2 wersja stable.
- Instalujemy aplikację klikając na pobrany plik dmg, a następnie na ikonę Tunnelblick:
  - potwierdzamy żądanie otwarcia pliku pobranego z Internetu klikając "Otwórz"
  - klikamy "Kontynuuj" w oknie "Witamy w Tunnelblick"
  - podajemy hasło użytkownika komputera w celu instalacji programu
- Na koniec instalacji pojawia się okno "Witamy w Tunnelblick" z informacją Żadna konfiguracja VPN nie jest zainstalowana, klikamy na przycisk "Mam pliki konfiguracyjne".
- W oknie "Dodaj konfiguracje" klikamy przycisk "OK". Uwaga! UCI nie odpowiada za błędy ortograficzne w tłumaczeniu.
- Przeciągamy pobrany wcześniej plik konfiguracyjny .ovpn do ikony programu Tunnelblick w górnym pasku menu, pojawia się okno z pytaniem "Zainstalować konfigurację dla wszystkich użytkowników", można kliknąć domyślne ustawienie "Tylko ja".
- Podajemy hasło użytkownika, by zainstalować konfigurację.
- W górnym menu, klikamy na ikonie Tunnelblick i wybieramy "Połącz vpn"
- Przy pierwszym połączeniu pojawi się pytanie o hasło - proszę podać hasło pobrane ze strony serwera profili VPN i zaznaczyć opcję "Zapisz w programie Keychain", by nie było potrzebne podawanie hasła przy kolejnych uruchomieniach Tunnelblick.
- Wszelkie ostrzeżenia pojawiające się w czasie startu Tunnelblick można zignorować.