

CEPiK 2 – dostęp VPN

Metryka dokumentu

Tytuł	CEPIK 2 – dostęp VPN			
Autor	Centralny Ośrodek Informatyki			
Zatwierdzający				
Historia zmian	Wersja	Data	Kto	Opis zmian
	1.0	30.10.2015 r.	Marcin Buława	Utworzenie dokumentu

Spis treści

Metryka dokumentu.....	2
1. Wstęp	4
2. Zestawienie połączenia VPN.....	5
2.1. Połączenie typu LAN-TO-LAN	5
2.2. Połączenie typu Remote Access	5

1. Wstęp

W dokumencie opisano realizację połączeń VPN do systemu CEPiK 2.

2. Zestawienie połączenia VPN

Do poprawnego zestawienia tunelu VPN wymagane jest posiadanie certyfikatu wydanego przez MSW. Certyfikat jest dostarczony w postaci pliku .p12.

2.1. Połączenie typu LAN-TO-LAN

W przypadku połączeń VPN typu LAN-to-LAN urządzenie sieciowe (np. router) należy odpowiednio skonfigurować, aby do połączenia VPN wykorzystywało otrzymany certyfikat wraz z kluczem prywatnym.

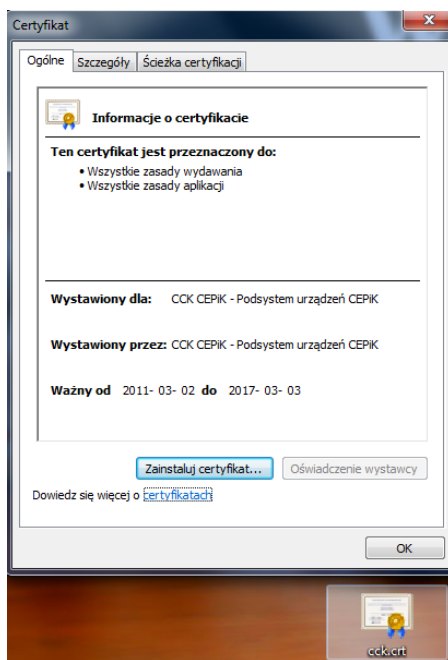
Parametry połączenia IPsec i host do ŚTI zostaną podane po potwierdzeniu połączenia do środowiska bez użycia VPN. W celu weryfikacji, czy podmiot posiada zestawione połączenie VPN L2L należy skontaktować się z lokalnym administratorem sieci lub osobą odpowiedzialną w podmiocie za lokalne administrowanie systemem.

2.2. Połączenie typu Remote Access

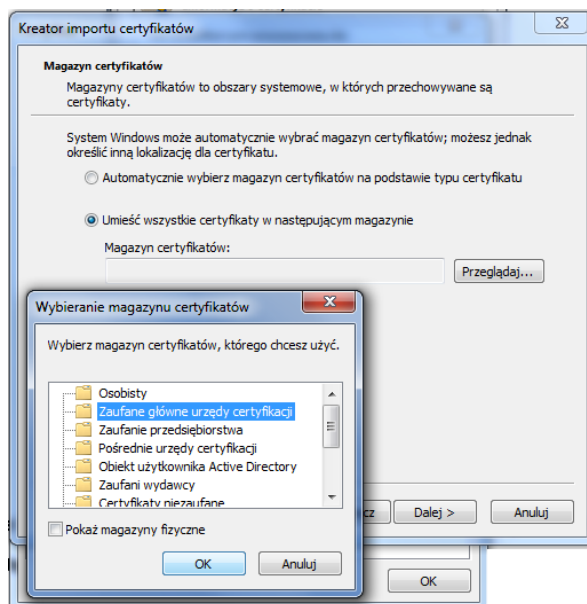
Kanał VPN typu remote access ma na celu umożliwienie zdalnej pracy z aplikacją jednej stacji roboczej z wykorzystaniem transmisji poprzez szyfrowany kanał VPN. Jest to połączenie oparte o architekturę klient – serwer i do zestawienia kanału szyfrowanego niezbędne jest oprogramowanie klienckie, które musi zostać zainstalowane na stacji roboczej. Do poprawnego skonfigurowania zdalnego dostępu należy pobrać i zainstalować oprogramowanie Cisco VPN Client lub skorzystać z innego alternatywnego rozwiązania.

Po poprawnej instalacji Cisco VPN Client w systemie operacyjnym, przystępujemy do instalacji wymaganych certyfikatów.

W pierwszym kroku instalujemy otrzymany certyfikat urzędu **CA**. W tym celu dwukrotnie klikamy na certyfikat (w tym przypadku **cck.crt**):



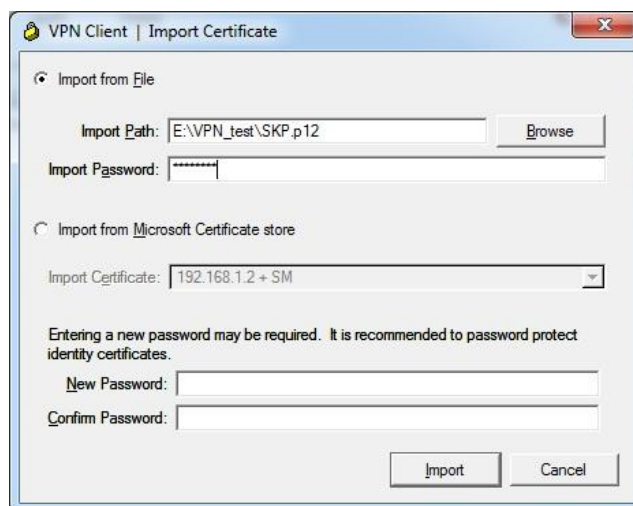
Wybieramy „Zainstaluj certyfikat”, następnie klikamy „Dalej”, wybieramy „Umieść wszystkie certyfikaty w następującym miejscu” i klikamy w opcję „Przeglądaj”



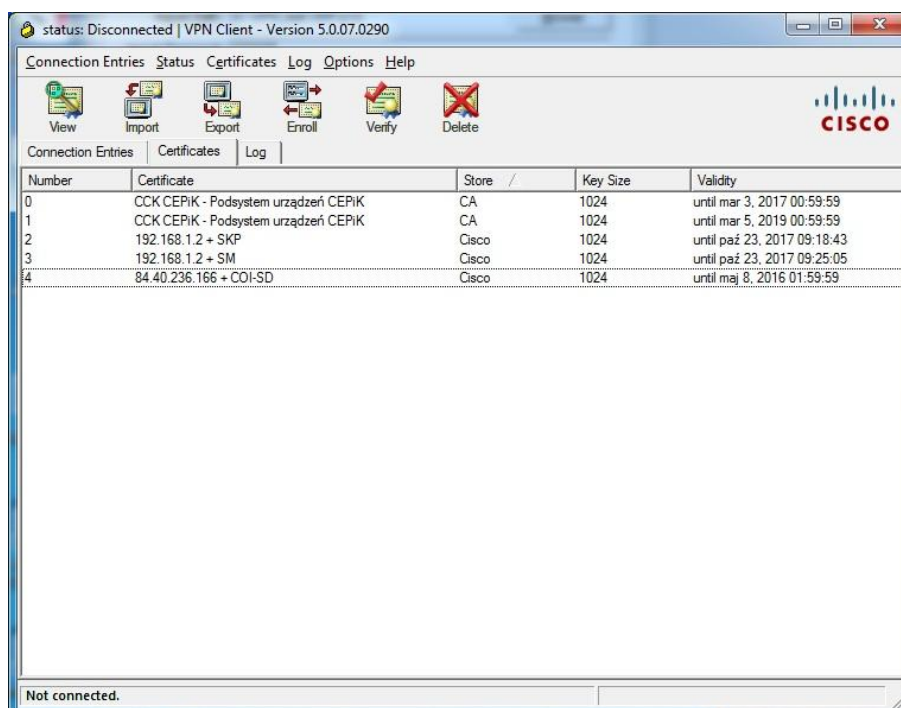
W okienku „Wybieranie magazynu certyfikatów” zaznaczamy „Zaufane główne urzędy certyfikacji” i klikamy „OK”. Następnie klikamy „Dalej”, w razie wystąpienia komunikatu z ostrzeżeniem o imporcie nieznanego klucza, wybieramy opcję zezwalającą na import i klucz został zaimportowany.

W drugim kroku uruchamiamy program **Cisco VPN Client** i definiujemy połączenie VPN.

Instalujemy otrzymany certyfikat „p.12”. Z wybieramy zakładkę **Certificates** i opcję **Import Certificate**. Wskazujemy plik z certyfikatem (**Import Path**) i wpisujemy otrzymane hasło do pliku (**Import Password**), a następnie klikamy przycisk **Import**.

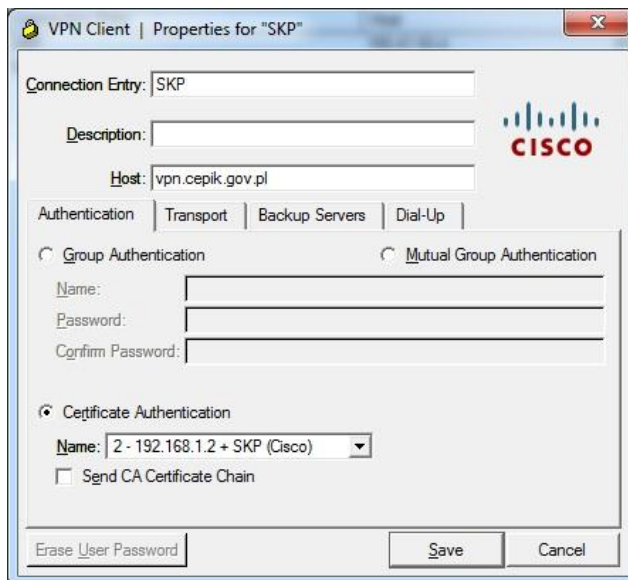


Certyfikat powinien się pojawić na liście (zakładka **Certificates**).



Następnie w zakładce **Connection Entries** definiujemy nowe połączenie. Wybieramy opcję **New**. Wypełniamy lub wybieramy następujące pola:
Connection Entry

- **Host** – podajemy adres **vpn.cepik.gov.pl**;
- **Authentication** -> **Certificate Authentication** - wskazujemy zainstalowany przez nas certyfikat jako parametr uwierzytelniania;
- **Transport** -> **Enable Transparent Tunneling** – wybieramy opcję **IPSec over UDP**.



VPN Client | Properties for "SKP"

Connection Entry: SKP

Description:

Host: vpn.cepik.gov.pl

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name:

Password:

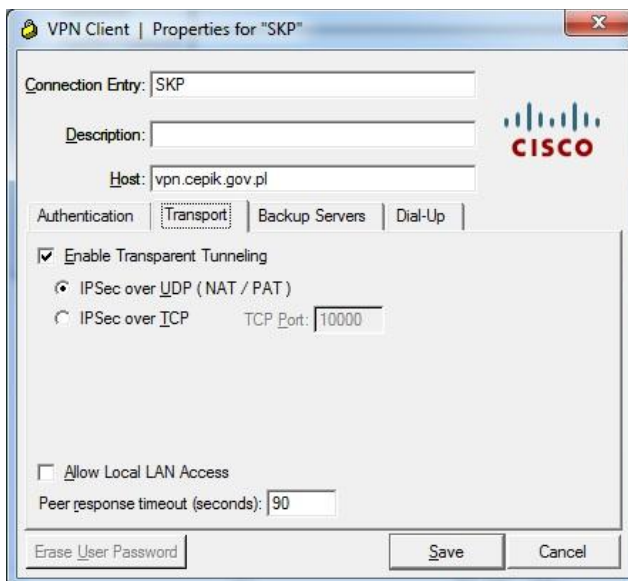
Confirm Password:

Certificate Authentication

Name: 2 - 192.168.1.2 + SKP (Cisco)

Send CA Certificate Chain

Erase User Password Save Cancel



VPN Client | Properties for "SKP"

Connection Entry: SKP

Description:

Host: vpn.cepik.gov.pl

Authentication | Transport | Backup Servers | Dial-Up

Enable Transparent Tunneling

IPSec over UDP (NAT / PAT)

IPSec over ICP TCP Port: 10000

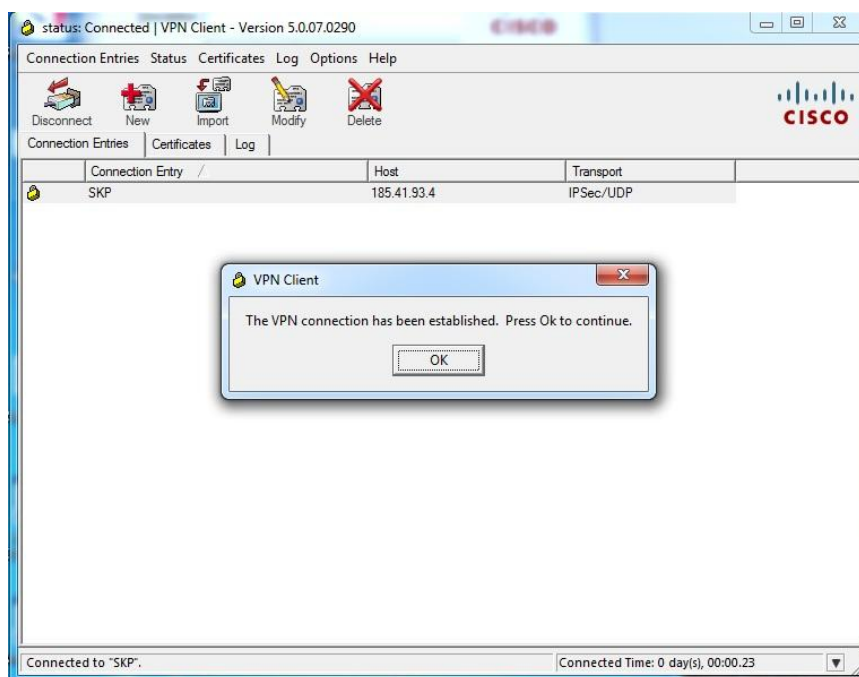
Allow Local LAN Access

Peer response timeout (seconds): 90

Erase User Password Save Cancel

Pozostałe parametry pozostawiamy bez zmian i zapisujemy konfigurację przyciskiem **Save**.

W celu zestawienia połączenia należy wybrać zdefiniowany uprzednio profil i dwukrotnie kliknąć lub wybrać opcję **Connect** z paska narzędziowego. Poprawne zestawienie połączenia zostanie zasygnalizowane przez aplikację komunikatem i ikoną zamkniętej kłódki przy nazwie profilu.



Po zakończeniu pracy rozłączamy połączenie VPN wybierając opcję **Disconnect**.