

CEPiK 2 – dostęp VPN

ul. Suwak 3 | 02-676 Warszawa | tel.: +48 22 250 28 83 | fax: +48 22 250 29 87 | e-mail: coi@coi.gov.pl | www.coi.gov.pl



Metryka dokumentu

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



Spis treści

Me	trvka	dokumentu	2
1.	Wst		4
2.	Zest	tawienie 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**):



Certyfikat
Ogólne Szczegóły Ścieżka certyfikacji
Informacje o certyfikacie
Ten certyfikat jest przeznaczony do: • Wszystbie zasady wydawania • Wszystbie zasady aplikacji
Wystawiony dla: CCK CEPIK - Podsystem urządzeń CEPIK Wystawiony przez: CCK CEPIK - Podsystem urządzeń CEPIK
Ważny od 2011-03-02 do 2017-03-03
Zainstaluj certyfikat Oświadczenie wystawcy Dowiedz się więcej o <u>certyfikatach</u>
ОК

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

Kreator importu certyfikatów	X
Magazyn certyfikatów	
Magazyny certyfikatów to obszary systemowe, w certyfikaty.	których przechowywane są
System Windows może automatycznie wybrać maj określić inną lokalizację dla certyfikatu.	jazyn certyfikatów; możesz jednak
Automatycznie wybierz magazyn certyfikati	ów na podstawie typu certyfikatu
Omieść wszystkie certyfikaty w następujący	m magazynie
Magazyn certyfikatów:	
	Przeglądaj
Wybieranie magazynu certyfikatów Wybierz magazyn certyfikatów, którego chcesz użyć.	
Osobisty Zaufane główne urzędy certyfikacji Zaufanie przedsiębiorstwa Pośrednie urzędy certyfikacji Obiekt użytkownika Active Directory Zaufani wydawcy	
Certyfikaty niezaufane Pokaż magazyny fizyczne	cz Dalej > Anuluj
OK Anuluj	ОК

W okienku "**Wybieranie magazynu certyfikatów**" zaznaczamy "**Zaufane główne urzędy certyfikacji**" i klikamy "**OK**". Następnie klikamy 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**.

Import from File		
Import <u>P</u> ath:	E:\VPN_test\SKP.p12	Browse
Import Password:		
Import from Mich	sooft Certificate store	<u>.</u>
Import Certificate:	sooft Certificate store 192.168.1.2 + SM assword may be required. It is recommend	ed to password protect
Import rom Mich Import Certificate: Entering a new pa identity certificate:	sooft Certificate store 192.168.1.2 + SM assword may be required. It is recommend s.	ed to password protect
Import Certificate: Entering a new pa identity certificate: <u>N</u> ew Password	soft Certificate store 192.168.1.2 + SM assword may be required. It is recommend s. :	ed to password protect

Certyfikat powinien się pojawić na liście (zakładka Certificates).

👌 status: Disconnected VPN Client - Version 5.0.07.0290						
<u>C</u> onnection Entries <u>S</u> tatus C <u>e</u> rtificates <u>L</u> og <u>O</u> ptions <u>H</u> elp						
View Connection Ent	View Import Export Erroll Verify Delete CISCO					
Number	Certificate	Store /	Key Size	Validity		
U 1 2 3 4	CUK VEMK - Podsystem urządzeń CEPIK CCK CEPIK - Podsystem urządzeń CEPIK 192.168.1.2 + SKP 192.168.1.2 + SM 84.40.236.166 + COI-SD	CA CA Cisco Cisco Cisco	1024 1024 1024 1024 1024	until mar 3, 2017 00:59:59 until mar 5, 2019 00:59:59 until paź 23, 2017 09:18:43 until paź 23, 2017 09:25:05 until maj 8, 2016 01:59:59		
)	a					

Następnie w zakładce **Connection Entries** definiujemy nowe połaczenie. 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.

onnection Entry:	SKP			
Description:				ahaha
Host	von cenik ar	ov ol		cisco
Authentication	Tranenort	Backup Server	Dial-Un	
	manapoir	backup Server		A di an an
Group Autne	ntication		(<u>M</u> utual Grou	up Authentication
Name:				
Confirm Passy	word:			
<u>-</u> <u>e</u> min + daav				
Certificate Au	uthentication			
Name: 2 - 19	92.168.1.2 + 9	SKP (Cisco)	-1	
Send CA	Certificate Cha	ain		
France loar Paper	word		Save	Cancel
Trase User Pass	word		Save	Cancel
Trase User Passi VPN Client onnection Entry:	Properties f	for "SKP"	Save	Cancel
VPN Client onnection Entry:	Properties f	for "SKP"	Save	Cancel
VPN Client onnection Entry: Description:	Properties f	for "SKP"	Save	Cancel
VPN Client vnnection Entry: Description: Host:	Properties f SKP vpn.cepik.go	for "SKP"	Save	Cancel
VPN Client vpn client nnection Entry: Description: Host: Authentication	Properties f SKP vpn.cepik.go Transpot	for "SKP" ov.pl Backup Server	Save	Cancel
VPN Client vrnection Entry: Description: Host: Authentication ✓ Enable Trans	Properties f SKP vpn.cepik.go Transport sparent Tunne	for "SKP" ov.pl Backup Server eling	Save	Cancel
VPN Client unnection Entry: Description: Host: Authentication G IPSec over	Properties f SKP vpn.cepik.go Transpot sparent Tunne er UDP (NAT	for "SKP" ov.pl Backup Server eling / PAT)	Save	Cancel
VPN Client UPN Client Description: <u>Host</u> : Authentication ✓ Enable Trans (• IPSec ove (• IPSec ove (• IPSec ove	Properties f SKP vpn.cepik.gc Transpot sparent Tunne er UDP (NAT ar ICP	for "SKP" ov.pl Backup Server eling / PAT) TCP <u>P</u> ort: 10000	Save	Cancel
VPN Client Protection Entry: Description: Host: Authentication ✓ Enable Trans ← IPSec ove ← IPSec ove	Properties f SKP vpn.cepik.go Transport sparent Tunne er UDP (NAT ar TCP	for "SKP" pv.pl Backup Server eling / PAT) TCP <u>P</u> ort: 10000	Save	Cancel
VPN Client onnection Entry: Description: Host: Authentication ✓ Enable Trans (* IPSec ove (* IPSec ove	Properties f SKP vpn.cepik.go Transpot sparent Tunne ar UDP (NAT er ICP	for "SKP" pv.pl Backup Server eling / PAT) TCP Port: 10000	Save	Cancel
VPN Client onnection Entry: Description: Host: Authentication ✓ Enable Trans () IPSec ove () IPSec ove	Properties f SKP [vpn.cepik.go [Transport] sparent Tunne er UDP (NAT ar ICP	for "SKP" ov.pl Backup Server eling / PAT) TCP <u>P</u> ort: 10000	Save	Cancel
VPN Client prinection Entry: Description: Host: Authentication ✓ Enable Trans (* IPSec ove (* IPSec ove	Properties f SKP vpn.cepik.go [Transport] sparent Tunno er UDP (NAT ar ICP	for "SKP" ov.pl Backup Server eling / PAT) TCP <u>P</u> ort: 10000	Save	Cancel
VPN Client Protection Entry: Description: Host: Authentication ✓ Enable Trans ← IPSec ove ← IPSec ove ← Allow Local I Protection	Properties f SKP vpn.cepik.go Transport sparent Tunne er UDP (NAT er ICP	for "SKP" pv.pl Backup Server eling / PAT) TCP Port: 10000 do): 190	Save	Cancel
VPN Client prinection Entry: Description: Host: Authentication ✓ Enable Tran: (* IPSec ove (* IPSec ove)	Properties f SKP vpn.cepik.go Transpot sparent Tunne er UDP (NAT er TCP LAN Access meout (secon	for "SKP" by.pl Backup Server eling / PAT) TCP Port: 10000 ds): 90	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.



Status: Connected VPN Clier	nt - Version 5.0.07.0290	01500	
Connection Entries Status Cer	tificates Log Options Help		alaha
Disconnect New Impo Connection Entries Certificates	ort Modify Delete		CISCO
Connection Entry /	Host	Tra	ansport
SKP	185.41.93	.4 IPS	ec/UDP
	The VPN connection has been	OK	ontinue.
Connected to "SKP".		Conr	nected Time: 0 day(s), 00:00.23

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