SITK RP Oddział w Krośnie & SUNRISE P.H.U. Grzegorz Krzemieniecki

www.klubdiagnosty.pl www.dlid.pl

VPN dla CEPIK 2.0

(wirtualna sieć prywatna dla CEPIK 2.0)

Józef Gawron

Radom, 2 lipiec 2016 r.

SITK RP Oddział w Krośnie & SUNRISE P.H.U. Grzegorz Krzemieniecki

www.klubdiagnosty.pl www.dlid.pl

CEPIK 2.0

(co się zmieni w SKP)

Dostosowanie sprzętu do komunikacji z systemem CEPiK 2.0

Data publikacji 17.06.2016 Wer.1.1 MC/COI

aidc

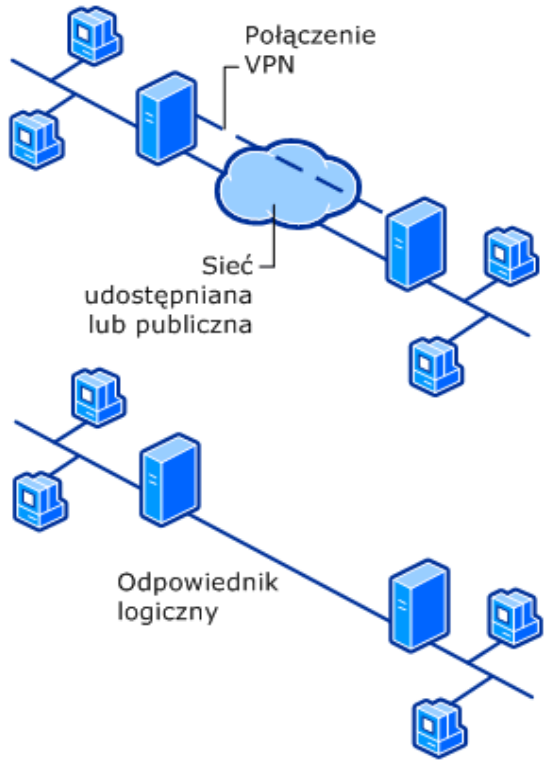
Radom, 2 lipiec 2016 r.

Co to jest VPN?

VPN (ang. Virtual Private Network) – Wirtualna sieć prywatna, to połączenie typu punkt-punkt (np. Klient – Serwer) po przez Internet. Klient sieci VPN używa specjalnych protokołów TCP/IP tworząc bezpośredni tunel do wirtualnego portu na Serwerze sieci VPN.

Połączenie typu VPN w oparciu o sięć publiczną typu Internet umożliwia emulację łącza prywatnego i wysyłanie między Klientem a Serwerem danych szyfrowanych i hermetyzowanych w celu zachowania poufności.

Istnieją dwa typy połączeń VPN:
•Połączenie VPN dostępu zdalnego
•Połączenie VPN typu lokacja-lokacja



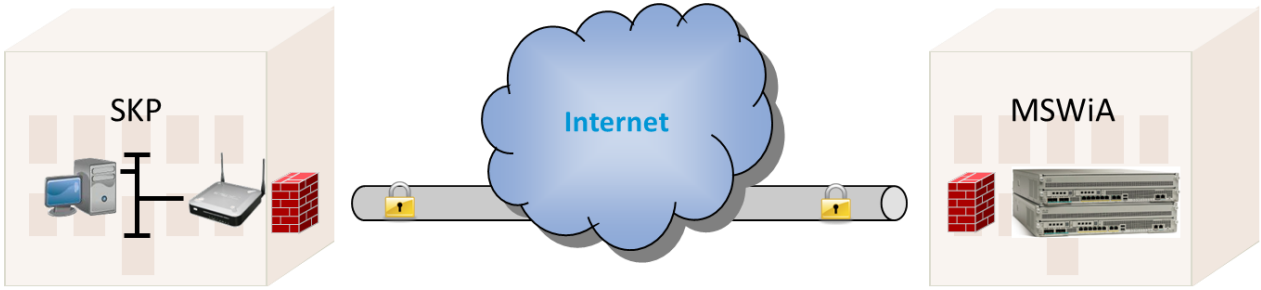
Połączenie VPN

Właściwości połączeń VPN
- Hermetyzacja
- Uwierzytelnianie
- Szyfrowanie danych

Hermetyzacja – Protokoły tunelowania sieci VPN

Uwierzytelnianie – 1) użytkownik PPP, 2) usługa Internet Key Exchenge, 3) pochodzenie danych

Szyfrowanie danych – oparte o klucz szyfrowania używany oraz znany tylko przez nadawcę i odbiorcę



Połączenie VPN

•MC/COI zaleca używanie klienta VPN instalowanego na stacji klienckiej

•Rekomenduje wykorzystanie rozwiązań CISCO VPN

•CISCO największy dostawca produktów i usług sieciowych na świecie

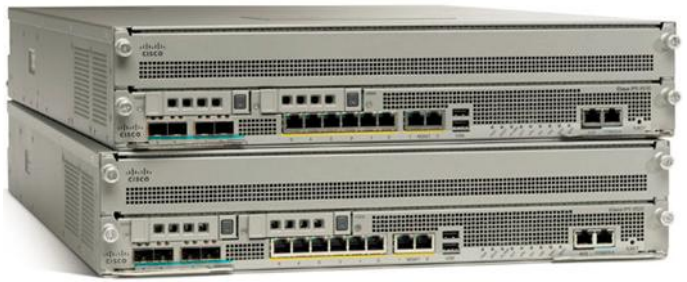
•CEPIK 2.0 bazować będzie na połączeniu VPN Remote Access (klient) lub na połączeniu typu LAN to LAN (VPN Router RA)

•Bezpieczeństwo sieci w SKP musi integracją osób nieuprawnionych oraz przed atakami z sieci publicznej

•Do zestawienia tunelu VPN (połączenia) wymagane jest posiadanie certyfikatu wydanego przez Centrum Certyfikacji dla CEPIK w postaci pliku w formacie PKCS#12 (.p12)

Połączenie VPN

Po stronie MSWiA Cisco ASA 55xx firewall Next Generation



Funkcjonalność

- Cisco® ASA firewalling połączony z Sourcefire® NG IPS
- Ochrona przed zagrożeniami w całego ataku
- Najlepszy IPS, widoczność i kontrola aplikacji (AVC) oraz URL filtering według NSS Labs

Zalety

- Wielowarstwowa ochrona przed zagrożeniami
- Znakomita widoczność zdarzeń i zasobów sieciowych
- Advanced malware protection
- Zmniejszenie kosztu i złożoności sieci

Po stronie SKP

- **Połączenie typu LAN-TO-LAN w trybie RA (Router)**

Parametry połączenia Ipsec :

ikev1 AES256 HMAC-SHA1,
host: vpn.cepik.gov.pl lub 185.41.93.4

Parametry IPSEC

Faza 1
Authentication — Certyfikat
Encryption — AES-256 & SHA
SA Lifetime — 86400
Key Group — 5
Faza 2
ESP-AES-256-SHA

Po stronie SKP

•Połączenie typu Remote Access – Cisco VPN Client

- Stację komputerową AIDC C-Station™ (DELL)
- Parametryzację systemu operacyjnego
- Konfigurację oprogramowania sieciowego dla Klienta VPN pod CEPIK 2.0
- Kartę kryptograficzną mini
- Czytnik karty kryptograficznej USB (SSL)

Instalacja certyfikatu VPN PKCS #12 i test połączenia oraz certyfikatu do karty kryptograficznej SSL

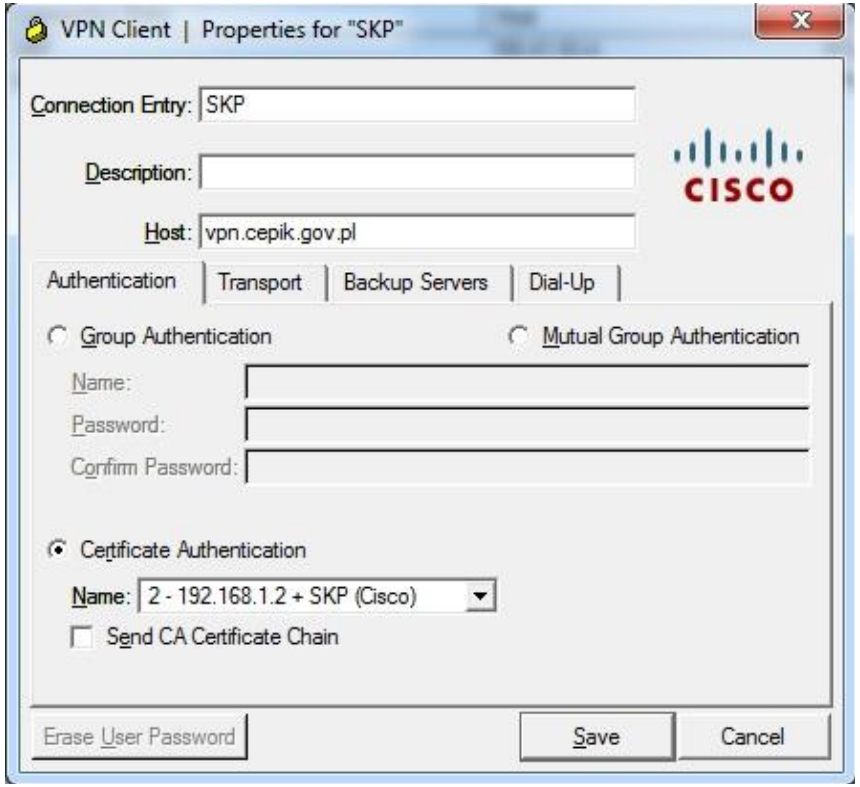
CEPKI 2.0 – Dostęp VPN

CISCO VPN Remote Access

Ma na celu umożliwienie połączenia z CEPIK 2.0 jednej stacji roboczej z wykorzystaniem transmisji poprzez szyfrowany kanał VPN w oparciu o architekturę Klient-Serwer na bazie oprogramowania klienckiego CISCO VPN Clinet zainstalowanego na stacji roboczej.

CISCO VPN Router

Urządzenie sieciowe (Router) odpowiednio skonfigurowane do połączenia VPN wykorzystującego otrzymany certyfikat wraz z kluczem prywatnym. CEPIK 2.0 przerzuca odpowiedzialność za prawidłową konfigurację połączenia typu L2L na SKP.



Dostosowanie sprzętu do komunikacji z systemem CEPiK 2.0 (MC/COI)

Zalecenia

-zaleca się używanie oprogramowania do zestawiania połączeń VPN instalowanego na stacji klienckiej (komputer) klienta „Cisco VPN Client" lub klienta „Cisco AnyConnect".

-usługa VPN jest realizowana w trybie Remote Access, client – server ,rekomendowany sposób zestawiania połączeń VPN z systemem CEPiK 2.0.

-MC/COI: nie przewiduje się zestawiania połączeń VPN typu LAN to LAN z SKP,
-MC/COI: LAN to LAN może być realizowane wyłącznie dla dużych podmiotów w trybie oddzielnych ustaleń.

-SKP musi przede wszystkim zabezpieczyć połączenie VPN przed ingerencją osób nieuprawnionych oraz przed atakami z sieci publicznej Internet.

-Service Desk CEPiK będzie udzielał wsparcia w konfiguracji połączeń VPN typu Remote Access.
-Service Desk CEPiK nie będzie udzielał wsparcia w realizacji połączeń VPN typu L2L

Dostosowanie sprzętu do komunikacji z systemem CEPiK 2.0 (MC/COI)

Wymagania dla stacji

• łącze internetowe o minimalnej przepustowości co najmniej 512 KB/s,

• oprogramowanie do obsługi VPN „Cisco AnyConnect" lub „Cisco VPN Client",

• certyfikat VPN do zestawienia bezpiecznego połączenia IPSec z systemem CEPiK 2.0,

• certyfikat SSL użytkownika , każde stanowisko komputerowe do przeprowadzania badań technicznych musi mieć swój zestaw kryptograficzny (czytnik oraz kartę z certyfikatem), obecnie wydane certyfikaty SSL będą mogły zostać wykorzystane również w CEPiK 2.0 – jeżeli ważność certyfikatu będącego w posiadaniu SKP upływa w najbliższym okresie, SKP musi wystąpić o odnowienie tego certyfikatu,

• oprogramowanie do komunikacji z systemem CEPiK 2.0 – SKP PRO pełna integracja oprogramowania z systemem CEPiK 2.0.

Józef Gawron / AIDC Solutions

Dziękuję za uwagę!

AIDC Solutions – BP Group

Józef Gawron
E-mail: gawron@aidc.pl / cepik@aidc.pl
Tel.: +48 600 969 555

www.aidc.pl