# Bezpieczeństwo dostępu do usługi SaaS EZD RP.

## Rekomendacje dla podmiotów grupy rządowej

EZD RP

wersja 1.01 z dnia 21.02.2023 r.

Usługa SaaS EZD RP dostępna jest wyłącznie dla podmiotów grupy rządowej objętej bezpłatnymi usługami wsparcia w zakresie wdrażania i eksploatacji EZD RP świadczonymi przez Operatora EZD RP (https://www.gov.pl/web/ezd-rp/podmioty-grupy-rzadowej).

W celu aktywacji SaaS EZD RP konieczne jest wykonanie następujących czynności:

- złożenie wniosku o aktywację usługi SaaS EZD RP,
- akceptacja Regulaminu usługi SaaS EZD RP,
- zawarcie umowy powierzenia przetwarzania danych osobowych,
- wskazanie administratorów systemu EZD RP,
- wskazanie informacji technicznych niezbędnych do zestawienia łącza IPSec VPN.

## Bezpieczne łącze dostępowe IPSec VPN Site-2-Site

Dostęp do usługi SaaS EZD RP wymaga zestawienia bezpiecznego połączenia pomiędzy siecią komputerową instytucji a infrastrukturą serwerową Operatora EZD RP. Do tego celu wykorzystywane są:

- wirtualne sieci prywatne VPN (Virtual Private Network) – umożliwiające tworzenie wydzielonych tuneli, przez które realizowana jest wymiana informacji bezpośrednio pomiędzy nadawcą i odbiorcą, za pośrednictwem sieci publicznej. Rozróżnia się kilka rodzajów połączeń VPN, jednym z nich jest konfiguracja Site-to-Site.
- zbiór protokołów IPSec (Internet Protocol Security) – służących do implementacji bezpiecznych połączeń i wymiany kluczy szyfrowania pomiędzy komputerami.

VPN oparta na IPsec składa się z minimum dwóch kanałów komunikacyjnych pomiędzy połączonymi komputerami: kanału wymiany kluczy, za pośrednictwem którego przekazywane są dane związane z uwierzytelnianiem i szyfrowaniem (klucze) oraz kanału (jednego lub więcej), w którym transmitowane są dane poprzez sieć prywatną.

Usługa SaaS EZD RP do zestawiania bezpiecznych połączeń wykorzystuje rozwiązanie IPSec VPN Site-2-Site. Takie podejście pozwala instytucji korzystającej z SaaS EZD RP na zachowanie pełnej kontroli dostępu do systemu przez poszczególnych pracowników. Z chwilą zablokowania lub usunięcia użytkownika w infrastrukturze komputerowej instytucji, automatycznie traci on możliwość łączenia się i korzystania z usługi SaaS EZD RP.

**Wymagane parametry techniczne dla urządzeń i łącza dostępowego dla usługi SaaS EZD RP:**

- połączenie VPN IPSec Site-2-Site,
- protokół IKEv2 dla VPN,
- metoda uwierzytelniania wykorzystująca mocny klucz współdzielony (hasło),
- algorytmy szyfrujące dla fazy 1 i 2 (wartości minimalne): AES256-CBC, SHA-256, DH 14 (2048 bits).

**Informacje i zasoby niezbędne do konfiguracji łącza:**

1. Faza pierwsza konfiguracji:
   - kontakt do administratora urządzenia, na którym zostanie zestawiony tunel IPSec VPN,
   - stały publiczny adres IP (zdalna brama dla IPSec),
   - mocne hasło (minimum 21 znaków, litery, cyfry, znaki specjalne),
   - zastosowany algorytm szyfrowania: np.: AES256-CBC, SHA256, DH19 (rekomendacja),

2. Faza druga konfiguracji:
   - lokalny adres IP,
   - zastosowany algorytm szyfrowania np.: AES256-CBC, SHA256, DH19 (rekomendacja),
   - osiągalny adres IP do sprawdzania połączenia komendą ping.

Z uwagi na różnice w sposobie implementacji rozwiązań technicznych w różnych urządzeniach sieciowych i systemach operacyjnych proces zestawiania bezpiecznego łącza zazwyczaj wymaga kontaktu i komunikacji pomiędzy administratorami oraz testowania wdrażanych zmian i rozwiązań. Standardowo cały proces realizowany jest w terminie trzech dni roboczych. W przypadku ewentualnych problemów technicznych lub braku kompatybilności pomiędzy urządzeniami sieciowymi, okres ten może się wydłużyć (konieczność dodatkowych czynności konfiguracyjnych i testy).

## Dostęp do SaaS EZD RP z wielu lokalizacji

W przypadku instytucji posiadających placówki w różnych lokalizacjach, rekomendowanym rozwiązaniem jest połączenie poszczególnych lokalnych sieci komputerowych w jedną tzw. sieć korporacyjną (poprzez łącza VPN pomiędzy lokalizacjami). Pozwala to ujednolicić i uprościć infrastrukturę służącą do komunikacji z siecią internetową oraz innymi systemami publicznymi wykorzystywanymi przez instytucję. Po utworzeniu sieci korporacyjnej dostęp do usługi SaaS EZD RP wymaga zestawienia tylko jednego łącza IPSec Site-2-Site.

W przypadku braku sieci korporacyjnej, konieczne będzie zestawianie bezpiecznych połączeń do wszystkich lokalizacji danej jednostki. Wiązać się to może z koniecznością wyposażenia infrastruktury lokalnych sieci komputerowych w urządzenia umożliwiające zestawienie bezpiecznych połączeń IPSec VPN spełniających przedstawione powyżej wymagania techniczne.

## Użytkownicy mobilni oraz praca zdalna

W przypadku, gdy instytucja zatrudnia osoby pracujące zdalnie i przewiduje korzystane z usługi SaaS EZD RP na urządzeniach przenośnych (np. laptopach) nie podłączonych do lokalnej sieci komputerowej, konieczne jest zastosowanie konfiguracji VPN Point-2-Site. Tego typu VPN pozwala użytkownikom mobilnym łączyć się przez szyfrowany kanał z lokalną siecią komputerową.

Dalsza konfiguracja polega na utworzeniu odpowiednich reguł kierowania ruchem sieciowym i konfiguracji serwerów DNS (Directory Name Services), tak aby ruch z przenośnych urządzeń końcowych do serwerów SaaS EZD RP, przechodził przez tzw. bramę lokalnej sieci komputerowej instytucji (network gateway). Dzięki takiemu rozwiązaniu urządzenia przenośne uzyskają dostęp do usługi SaaS EZD RP.

## Bezpieczeństwo teleinformatyczne

Instytucja, która planuje korzystać z usługi SaaS EZD RP, powinna przygotować infrastrukturę i procedury organizacyjne, w taki sposób, aby umożliwiały one realizację obowiązków usługobiorcy określonych w Regulaminie usługi SaaS EZD RP oraz w przepisach i wytycznych obowiązujących dany podmiot. Dotyczy to przede wszystkim:

- zapewnienia ochrony lokalnej sieci komputerowej lub sieci korporacyjnej za pomocą urządzeń i systemów bezpieczeństwa realizujących funkcje: zapory sieciowej i kontroli dostępu, szyfrowania połączeń, ochrony przed wirusami i złośliwym oprogramowaniem,
- stosowania oprogramowania pochodzącego z zaufanych źródeł oraz wdrażania jego aktualnych wersji usuwających wykryte podatności i luki bezpieczeństwa,
- zapewnienia, aby dostęp do systemu posiadały wyłącznie osoby do tego upoważnione, które w wyznaczonym przedziale czasu, realizują zadania wymagające dostępu do systemu EZD RP.

## Wielofunkcyjne urządzenia ochrony sieci

W przypadkach, gdy konieczny jest zakup dodatkowych urządzeń umożliwiających podłączenie lokalnej sieci komputerowej do usługi SaaS EZD RP, rekomendowane jest użycie powszechnie dostępnych na rynku urządzeń wielofunkcyjnych, które oferują wszystkie wymagane funkcje sieciowe

(router brzegowy, VPN) i bezpieczeństwa (UTM, IPS/IDS, antymalware itp.). Przed zakupem zalecane jest przeprowadzenie inwentaryzacji stosowanych w organizacji rozwiązań IT (systemy bezpieczeństwa, sieciowe, operacyjne), aby przy okazji rozbudowy, zapełnić możliwie wiele luk w użytkowanej infrastrukturze.

## Parametry łącza dopasowane do liczby użytkowników

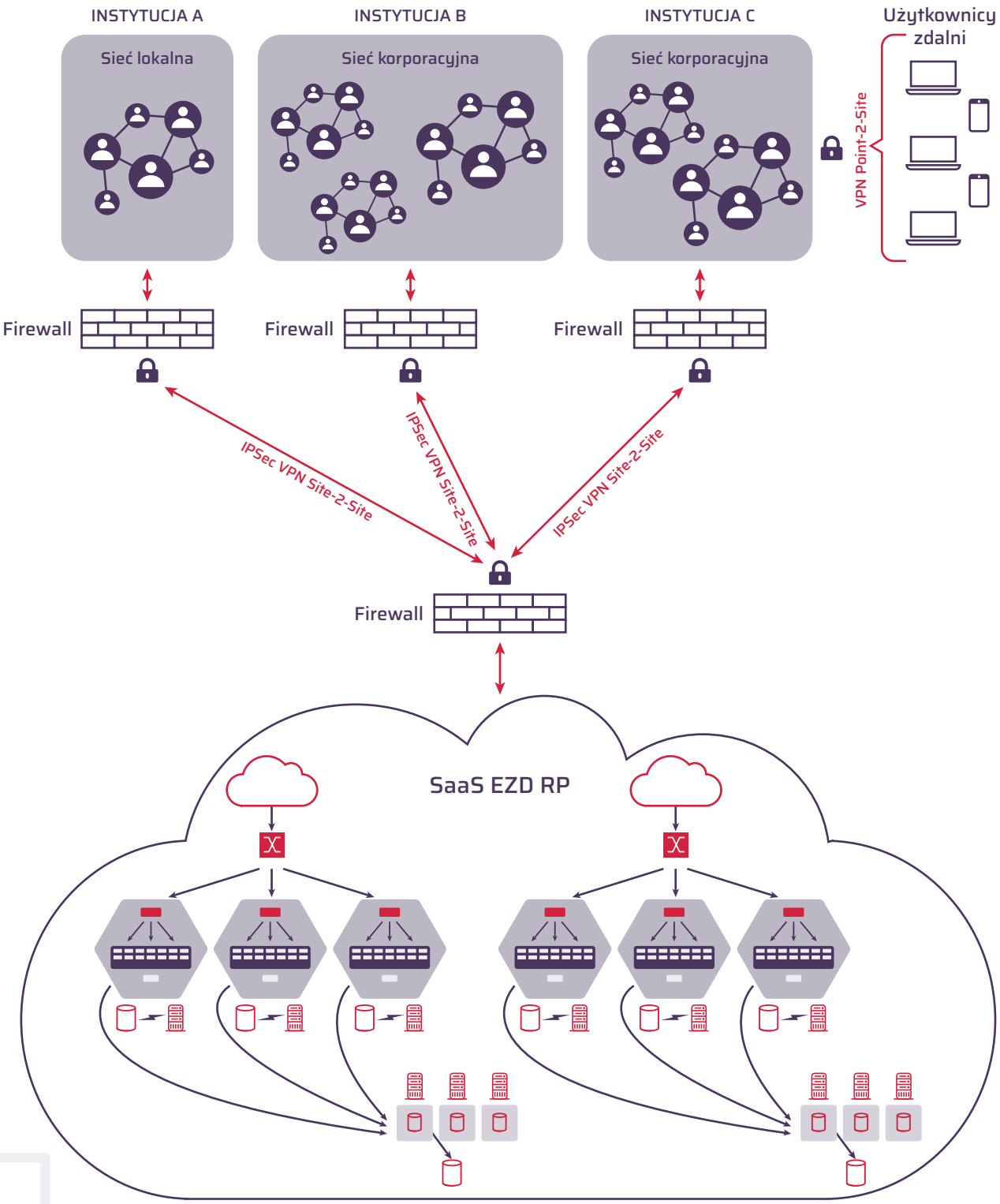
Przeprowadzone symulacje i szacunki pokazują, że dla uzyskania komfortowych warunków pracy dla 100 użytkowników aktywnie pracujących w systemie EZD RP (czasy odpowiedzi poniżej 1 sek.) należy zarezerwować symetryczne pasmo o przepustowości 20 Mbps / 20 Mbps (pobieranie/wysyłanie). Jeśli użytkownicy sporadycznie korzystają z systemu, wymagania te można obniżyć nawet o połowę.

Jeżeli charakter organizacji wymusza częstą pracę ze skanowanymi, wielostronicowymi dokumentami o wysokiej rozdzielczości (większej niż 150 DPI) lub o dużym rozmiarze (powyżej 2 MB), potrzebne mogą być wyższe parametry łącza dostępowego lub czasy odpowiedzi dla niektórych operacji mogą się zwiększyć (np. do 3–5 sek.).

Oprócz prędkości pobierania i wysyłania danych (tzw. przepływność łącza), na komfort pracy w systemie dostępnym w usłudze chmurowej, wpływają też parametry takie jak opóźnienie i tzw. jitter (krótkookresowe odchylenie od ustalonych parametrów sygnału). Przy zbyt wysokich wartościach – opóźnienie większe niż 50 ms lub jitter powyżej 10 ms, mogą występować dłuższe czasy oczekiwania. Poniższa tabela przedstawia szacowane przeciętne parametry dotyczące prędkości pobierania i wysyłania danych na potrzeby obsługi ruchu sieciowego dla systemu EZD RP, w zależności od liczby użytkowników korzystających z danego łącza (tunelu IPSec VPN).

| Liczba użytkowników | Minimalne | Rekomendowane | Komfortowe |
|---|---|---|---|
| do 50 | 3/3 Mbps | 5/5 Mbps | 10/10 Mbps |
| 51–300 | 10/10 Mbps | 20/20 Mbps | 50/50 Mbps |
| 301–2000 | 50/50 Mbps | 100/100 Mbps | 200/200 Mbps |
| powyżej 2000 | 200/200 Mbps | 500/500 Mbps | 1/1 Gbps |

# Sposób realizacji bezpiecznych łączy dostępowych do usługi SaaS EZD



NASK – Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa

Oddział NASK w Białymstoku
Łukowska 2, 15-373 Białystok

ezdrp@nask.pl
ezdrp.gov.pl

EZD RP NASK
Kancelaria Prezesa Rady Ministrów
PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTRA CYFRYZACJI