245545

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest: **dostawa oraz wdrożenie wysokodostępnej bramki wirtualnej sieci prywatnej (VPN).**

1. **Termin realizacji zamówienia:**

   Zgodnie ze złożoną ofertą nie później niż w terminie do 60 dni kalendarzowych od dnia zawarcia Umowy, nie później niż do 31.05.2026.

2. **Zamówienie obejmuje:**

   2.1. Dostawę czterech fizycznych bramek wirtualnej sieci prywatnej, urządzenia wraz z wymaganymi licencjami (dalej bramki VPN) dla środowiska produkcyjnego,
   2.2. Dostawę centralnego systemu zarządzania w formie maszyn wirtualnych wraz z wymaganymi licencjami (wirtualny appliance) dla środowiska produkcyjnego,
   2.3. Dostawę jednej maszyny wirtualnej bramki VPN dla środowiska testowego wraz z wymaganymi licencjami (dalej wirtualny appliance),
   2.4. Dostawę centralnego systemu zarządzania w formie maszyn wirtualnych wraz z wymaganymi licencjami (wirtualny appliance) dla środowiska testowego,
   2.5. Wdrożenie rozwiązania w sieci Zamawiającego we współpracy z Administratorami Zamawiającego
   2.6. zapewnienie, na wniosek Zamawiającego, realizacji czynności eksperckich w łącznym wymiarze do 500 godzin, zgodnie z wymaganiami opisanymi w pkt 3.7,
   2.7. Przeprowadzenie instruktażu dla Administratorów Zamawiającego.

   Dostawa urządzeń na własny koszt, do dwóch lokalizacji Zamawiającego na terenie m.st. Warszawy.

3. **Wymagania**

   3.1. Opis funkcjonalny rozwiązania

   Dostarczony sprzęt oraz oprogramowanie muszą pozwolić na zbudowanie wysokodostępnej, rozłożonej geograficznie (pomiędzy dwa Centra Przetwarzania Danych Zamawiającego, zwane dalej CPD) bramki VPN obsługującej pracowników oraz firmy współpracujące z Zamawiającym w zakresie zestawiania szyfrowanych połączeń VPN.

   Całość ma składać się z 2 środowisk:

   1. Testowego – służącego do testowania zmian w konfiguracji, testów aktualizacji oprogramowania oraz testów polityk konfiguracji – zbudowanego w całości z maszyn wirtualnych uruchomionych w środowisku VMware vShpere 8u3 lub nowszym (minimum jedna wirtualna bramka oraz wirtualny serwer zarządzający),

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

2. Produkcyjnego – służącego do obsługi połączeń zdalnych, zbudowane w architekturze wysokiej dostępności. Rozwiązanie ma składać się z 4 urządzeń (bramka VPN) zlokalizowanych po 2 w każdym CPD. Urządzenia w ramach każdego CPD muszą tworzyć klaster wysokiej dostępności (ang. High Availability, zwany dalej klaster HA). Każdy klaster musi posiadać własny publiczny adres IP wskazany przez Zamawiającego (łącznie 2 adresy IP – po jednym per każde CPD).

   Zarządzanie całością rozwiązania musi być centralne, z centralnego serwera zarządzającego dostarczonego w postaci maszyny lub maszyn wirtualnych.

Dostarczone licencje muszą uprawniać do korzystania z rozwiązania VPN przez pracowników Zamawiającego oraz osoby trzecie działające na jego rzecz, w tym w szczególności współpracowników, podmioty współpracujące oraz organizacje współpracujące z Zamawiającym.

Niżej opisano wymagania dla środowiska produkcyjnego, środowisko testowe nie musi spełniać wymagań w zakresie wydajności oraz wysokiej dostępności. Dla środowiska testowego wymagane jest zaoferowanie wirtualnych urządzeń posiadających takie samo oprogramowanie, ten sam system operacyjny oraz taką samą funkcjonalność umożliwiające przeprowadzanie testów dla min 10 Użytkowników.

Całość rozwiązania ma być posadowiona w infrastrukturze Zamawiającego (bramki VPN oraz zarządzanie) i nie może być zależne/zarządzanie z chmury producenta. Zamawiający dopuszcza, aby tylko listy reputacyjne pobierane były okresowo z chmury Producenta.

Całość rozwiązania musi pochodzić z oficjalnego kanału dystrybucji producenta na rynek polski.

3.2. <u>Architektura i wysoka dostępność</u>

3.2.1. Rozwiązanie ma składać się z 4 urządzeń (bramka VPN) zlokalizowanych po 2 w każdym CPD. Urządzenia w ramach każdego CPD muszą tworzyć klaster wysokiej dostępności (ang. High Availability, zwany dalej klaster HA) tj. 2 klastry zbudowane z 2 urządzeń. Każdy klaster musi posiadać własny publiczny adres IP wskazany przez Zamawiającego (łącznie 2 adresy IP – po jednym per każde CPD).

3.2.2. Skalowanie: wszystkie dostarczone urządzenia muszą mieć możliwość działania w ramach pojedynczego klastra Active-Active oraz Active-Passive zbudowanego z 4 urządzeń oraz posiadać możliwość min. 2-krotnego skalowania tj. rozbudowy do klastra Active-Active oraz Active-Passive składającego się z min. 8 urządzeń tego samego producenta.

3.2.3. Każda z bramek VPN musi posiadać wydajność umożliwiającą obsłużenie min. 1 tys. jednoczesnych połączeń Użytkowników.

3.2.4. Całość rozwiązania musi być zarządzana z centralnego serwera zarządzającego.

3.2.5. Całość rozwiązania tj. sprzęt i dostarczone oprogramowanie muszą pochodzić od jednego producenta.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.3. Wymagania dla bramki VPN

Niżej opisano wymagania dla pojedynczej bramki VPN.

3.3.1. Obudowa maksymalnie 2U RACK 19 cali dostarczona wraz z szynami montażowymi.

3.3.2. Min. 2 redundantne zasilacze (1+1) typu HotPlug o mocy umożliwiającej poprawną pracę urządzenia z pełną wydajnością w przypadku awarii jednego z nich, 240V AC.

3.3.3. Minimum 4 porty Ethernet SFP28 każdy 10/25 Gb/s. Wszystkie porty wraz z wkładkami SFP-25G-SR.

3.3.4. Karta/moduł zarządzający niezależna od systemu operacyjnego, posiadająca minimalną funkcjonalność:

- dostęp do karty zarządzającej poprzez dedykowany port RJ45, dostępny z poziomu obudowy urządzenia,
- karta posiada własny adres IP, działa niezależnie od systemu operacyjnego bramki VPN,
- dostęp do konsoli karty/modułu zarządzającej z poziomu przeglądarki webowej (GUI), wsparcie dla HTML 5, obsługa połączeń szyfrowanych SSL/TLS,
- zapewnia możliwość zdalnego włączenia, wyłączenia oraz restartu urządzenia,
- zapewnia możliwość wirtualnej, zdalnej konsoli.

3.3.5. Wydajność pozwalająca na obsługę min. 1300 Użytkowników VPN jednocześnie oraz przepustowość zaszyfrowanego ruchu VPN dla AES-GCM min. 10 Gbps.

3.3.6. Skalowanie tj. możliwość rozbudowy pozwalająca na 4-krotne zwiększenie wydajności oraz liczby obsługiwanych Użytkowników bez konieczności wymiany całego urządzenia, a jedynie dokupienie licencji lub rozbudowę pamięci RAM lub dodanie kart akceleracji operacji kryptograficznych.

3.3.7. Urządzenie musi pracować pod kontrolą dedykowanego, utwardzonego systemu operacyjnego producenta, zaprojektowanego do realizacji funkcji bezpieczeństwa sieciowego (Firewall/VPN). Nie jest dopuszczalne stosowanie ogólnych systemów operacyjnych (np. Linux, Windows).

3.3.8. Obsługa IPv4 i IPv6.

3.3.9. Obsługa routingu dynamicznego BGP i OSPFv2 i v3, obsługa routingu statycznego oraz policy based routing.

3.3.10. Obsługa połączeń VPN klienckich za pomocą IPSec oraz SSL/TLS oraz obsługa połączeń VPN Site-2Site, w tym routing dynamiczny w tunelu.

3.3.11. Obsługa statefull firewall w warstwach L3/L4, wraz z politykami aplikacyjnymi w L7 (rozpoznawanie aplikacji).

3.3.12. Obsługa NAT (SNAT/DNAT).

3.3.13. Obsługa QOS.

3.3.14. Obsługa VLAN oraz Bonding (802.3ad link agregation).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.3.15. Obsługa klastra HA, minimum Active/Standby wraz z synchronizacją stanu sesji (stateful failover) dla ruchu VPN oraz Firewall. Automatyczny failover, bez ręcznej interwencji z możliwości monitorowania interface, „helth checks" (usługi/procesy), definiowania priorytetów nodów klastra oraz możliwością ręcznego przełączania nodów klastra przez Administratra z podtrzymaniem sesji. Patchowanie bez żadnej przerwy i zrywania sesji VPN użytkowników.

3.3.16. Certyfikacje: CE oraz ROHS.

3.4. Klient VPN

3.4.1. Obsługa VPN: tunele site-2-site oraz połączenia klienckie.

3.4.2. Dostępny dedykowany przez producenta klient VPN na platformy Windows 11, macOS 15, macOS 26 oraz platformy mobilne: iOS 18 i nowszych, Android 13 i nowszych. Klient na platformy mobilne musi być dostępny w sklepach odpowiednio: AppStore i Google Play.

3.4.3. Wsparcia dla Linux - dostępny dedykowany przez producenta klient VPN lub możliwość zestawienia połączenia VPN z użyciem standardowych mechanizmów w tych systemach operacyjnych.

3.4.4. Obsługa IKEv2 oraz SSL/TLS VPN.

3.4.5. Obsługa min: AES-GCM, AES-CBC, SHA2, ECDH.

3.4.6. Możliwość konfiguracji obsługiwanych protokołów i algorytmów, możliwość wyłączenia po stronie bramki VPN obsługi słabych protokołów i algorytmów.

3.4.7. Obsługa split oraz full tunnel.

3.4.8. Obsługiwana autoryzacja za pomocą:

- certyfikatów X.509 wydanych przez CA Zamawiającego, z mapowaniem na konta i grupy Active Directory Zamawiającego,
- mechanizmów MFA,
- integracja z RADIUS.

3.4.9. Integracja z usługami Active Directory Zamawiającego:

- musi być możliwa integracja z usługami Active Directory Zamawiającego w zakresie mapowania kont użytkowników VPN na konta AD oraz budowanie reguł dostępu VPN i Firewall w oparciu o grupy Active Directory.
- musi istnieć możliwość budowania wielu reguł dostępu VPN/Firewall w oparciu o grupy kont Użytkowników oraz komputerów Active Directory.

3.4.10. Zintegrowany mechanizm bezpiecznego dostarczania certyfikatów X.509 dla klientów na platformach Windows, macOS, iOS i Android za pomocą jednorazowych kodów lub kodu QR. Certyfikaty powinny być wystawiane z CA Zamawiającego na platformie Windows Server lub za pomocą CA wbudowanego w dostarczone rozwiązanie. Dla każdego z Użytkownika powinien być możliwy do wygenerowania unikalny kod jednorazowy lub QR służący do wygenerowania przez klienta VPN certyfikatu do autoryzacji.

3.4.11. Możliwość budowania polityk dostępu VPN/Firewall z ograniczeniem per grupa, aplikacja, port (model ZtNA-like).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.4.12. Klient VPN na platformę Windows musi korzystać z protokołu IPSec oraz automatycznie przełączać się na tunel SSL/TLS w przypadku blokowanie tego protokołu w sieci.

3.4.13. Producent musi udostępniać mechanizm przygotowania paczki instalacyjnej klienta VPN na platformę Windows do instalacji nienadzorowanej z zaszytą konfiguracją połączenia oraz autoryzacji do VPN Zamawiającego (Zero-touch onboarding).

3.4.14. Producent musi udostępniać mechanizm konfiguracji klienta na platformy mobilne za pomocą kodu QR (skan kodu QR) lub za pomocą MDM Microsoft Intune. Kod QR oraz konfiguracja za pomocą MDM musi pozwolić skonfigurować połączenie do VPN Zamawiającego.

3.4.15. Obsługa 2 CPD:

- Klient VPN na platformę Windows musi obsługiwać połączenia do obu klastrów w obu CPD (w konfiguracji musi posiadać oba adresy IP), a w przypadku awarii (braku dostępności) jednego z klastrów (CPD) – automatycznie połączyć się do drugiego CPD w czasie mniejszym niż 60 sekund,
- rozwiązanie musi posiadać konfigurowalnym mechanizm preferencji danego CPD do połączeń VPN oraz rozkładania obciążenia na 2 CPD.

3.4.16. Obsługa tunelu VPN per komputer dla systemu Windows:

- musi być obsługiwane automatyczne zestawienie tunelu VPN per komputer, przed zalogowaniem Użytkownika do systemu operacyjnego z autoryzacją za pomocą certyfikatu X.509,
- po autoryzacji za pomocą certyfikatu musi być możliwość mapowania na grupy Active Directory komputerów oraz budowanie reguł zdalnego dostępu w oparciu o grupy AD kont komputerów,
- po zalogowaniu musi być możliwość automatycznego przełączenia tunelu VPN w kontekst zalogowane Użytkownika oraz ponowna autoryzacja za pomocą certyfikatu wraz z przypisaniem reguł dostępu per konta i grupy Użytkownika.

3.4.17. Dla systemu Windows musi być możliwość konfiguracji automatycznego zestawiania połączenia VPN po zalogowaniu Użytkownika (Auto Connect) – zarówno w trybie wymuszony przez Administratora jak i konfigurowalnym przez Użytkownika oraz mechanizmu automatycznego podtrzymywania sesji VPN (Always Up, Always Connect).

3.4.18. Dla systemu Windows musi być możliwość badania (wykrywania) przez klienta, że jest połączony w sieci wewnętrznej (LAN) – z konfigurowalną możliwością zestawiania lub rozłączania połączenia VPN.

3.4.19. Dla systemu Windows musi być możliwość badania zgodności konfiguracji urządzenia.

3.4.20. Dla systemu Windows, macOS oraz mobilnych iOS i Android musi być możliwość przydzielenia wirtualnego adresu IP dla klienta z puli konfigurowalnej przez

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Zamawiającego (np. z wykorzystaniem DHCP) oraz integracja z wewnętrznym serwerem DNS.

3.5. Centralne zarządzanie

3.5.1. Centralny serwer zarządzający w postaci maszyny wirtualnej.
3.5.2. Centralna konsola do zarządzania politykami, obiektami, konfiguracją VPN.
3.5.3. Możliwość jednoczesnej pracy w konsoli min. 3 Administratorów.
3.5.4. Konsola zarządzająca w postaci aplikacji dla systemu Windows lub aplikacji WEB oraz API do automatyzacji.
3.5.5. Możliwość budowania wspólnej polityki/konfiguracji dla wszystkich urządzeń.
3.5.6. Monitoring: dashboard (użytkownicy, przepustowość, opóźnienia), alerty oraz logi z połączeń VPN oraz reguł firewall oraz raportowanie.
3.5.7. Raportowanie w logach połączeń VPN geolokalizacji adresów IP klientów VPN.
3.5.8. Logowanie i audyt: integracja z SIEM (np. za pomocą syslog), konfigurowalna retencja logów.
3.5.9. Centralne aktualizacje, monitorowanie dostępności aktualizacji.
3.5.10. RBAC: definiowane role, śledzenie zmian, audyt działań Administratorów.
3.5.11. Mechanizm 2-poziomego weryfikowania i zatwierdzania zmian dokonanych w polityce bezpieczeństwa przez Administratorów tj. musi istnieć możliwość weryfikowania zmian w polityce dokonanej przez jednego Administratora i ich zatwierdzania przez innego Administratora przed instalacją polityki bezpieczeństwa na bramkach VPN. Mechanizm musi posiadać możliwość definiowania poziomów uprawnień w ramach kont Administratorów oraz mechanizm notyfikacji Administratorów, że są zmiany wymagające weryfikacji i akceptacji.

3.6. Wdrożenie oraz instruktaż

3.6.1. Wykonawca we współpracy z Administratorami Zamawiającego zaprojektuje (przygotuje projekt techniczny) oraz wdroży rozwiązanie w sieci Zamawiającego:
3.6.2. Spotkania wdrożeniowe oraz instruktaż będą prowadzone w języku polskim.
3.6.3. Instruktaż oraz wdrożenie możliwe są w formie stacjonarnej, hybrydowej oraz sesji zdalnych (MS Teams) – do uzgodnienia na etapie wdrożenia pomiędzy koordynatorami Umowy.
3.6.4. Instruktaż dla Administratorów Zamawiającego musi pozwolić na samodzielnie zarządzenie rozwiązaniem, strojenie konfiguracji i polityk, budowanie polityk, aktualizację oraz rozwiazywanie typowych problemów.
3.6.5. Instruktaż musi zostać przeprowadzony dla min 8 pracowników Zamawiającego i musi trwać min 10 dni roboczych, każdy po 8h.

3.7. Usługi eksperckie realizowane w ramach puli godzin:

3.7.1. Wykonawca zapewni realizację usług eksperckich w łącznym wymiarze do 500 godzin, wykonywanych na wniosek Zamawiającego, obejmujących czynności doradcze, konsultacyjne, administracyjne oraz konfiguracyjne związane z dostarczonym rozwiązaniem VPN.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.7.2. Osoby realizujące czynności w ramach puli godzin muszą posiadać:

a) minimum 3 lata doświadczenia w pracy z rozwiązaniami klasy Firewall/VPN w środowiskach enterprise,

b) praktyczną znajomość protokołów IKEv2, IPSec, SSL/TLS, mechanizmów HA, routingu dynamicznego (OSPF/BGP),

c) doświadczenie w integracji systemów z usługami Active Directory oraz certyfikatami X.509,

d) kompetencje adekwatne do zakresu realizowanych czynności, potwierdzone certyfikatem producenta ofertowanego rozwiązania.

3.7.3. Na żądanie Zamawiającego Wykonawca przedstawi wykaz osób wraz z ich kwalifikacjami.

3.7.4. Czynności będą realizowane w dni robocze w godzinach 08:00–16:00, chyba że Zamawiający, dla konkretnego zlecenia, wskaże inne wymagania.

3.7.5. Zgłoszenia prac będą przekazywane przez osoby upoważnione przez Zamawiającego.

3.7.6. Czas reakcji Wykonawcy na zgłoszenie nie może przekraczać 24 godzin.

3.7.7. Czynności mogą być wykonywane zdalnie lub na miejscu w siedzibie Zamawiającego — zgodnie z ustaleniami dotyczącymi danego zadania.

3.7.8. Każde wykonane zadanie musi być rejestrowane wraz z zakresem czynności, czasem trwania i osobą realizującą.

3.7.9. Rozliczenie godzin będzie następowało miesięcznie na podstawie protokołów odbioru zawierających:

a) opis wykonanych czynności,

b) daty i przedziały czasowe ich realizacji,

c) liczbę przepracowanych godzin,

d) dane osoby wykonującej czynności.

3.7.10. Minimalna jednostka rozliczeniowa wynosi 0,5 godziny.

3.7.11. Do czasu realizacji czynności nie wlicza się czasu dojazdu, oczekiwania ani aktywności niezwiązanych bezpośrednio z wykonaniem zadania.

3.8. Gwarancja

3.8.1. Sprzęt oraz oprogramowanie muszą być objęte serwisem gwarancyjnym przez okres 60 miesięcy od daty odbioru polegającym na naprawie lub wymianie urządzenia w przypadku jego uszkodzenia lub wadliwości.

3.8.2. W ramach serwisu musi być zapewniony dostęp do aktualizacji i nowych wersji oprogramowania oraz wsparcie techniczne w trybie 24x7, bez dodatkowych opłat

3.8.3. SLA 24x7, czas reakcji do 2h, czas naprawy/wymiany do 24 godzin.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.8.4. Gwarancja musi być świadczona przez Producenta lub jego autoryzowany serwis.

3.8.5. Oprogramowanie musi pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi dokumentami i danymi niezbędnymi do potwierdzenia legalności jego pochodzenia, do jego uruchomienia lub korzystania z niego (np.: dane dostępowe, certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji, itp.).

3.8.6. Oprogramowanie oraz aktualizacje będą wolne od mechanizmów celowo blokujących jego funkcje, wirusów, koni trojańskich, robaków i innych szkodliwych programów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706