



Opis Przedmiotu Zamówienia

I. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest świadczenie usług kolokacyjnych dla posiadanych przez MJWPU serwerów.
2. Rozpoczęcie świadczenia usług kolokacyjnych powinno nastąpić 1.08.2024 i będzie świadczone przez 12 miesięcy.
3. Wykonawca w ramach usługi, przeniesie z obecnej do docelowej lokalizacji serwery MJWPU. Przeniesienie serwerów musi nastąpić przed rozpoczęciem świadczenia usług kolokacyjnych.

II. Wymagane parametry dla centrum danych Wykonawcy

1. Kolokacja w odległości nie przekraczającej 35 kilometrów od siedziby Zamawiającego (mierzona w linii prostej).
2. Dedykowana szafa minimum 19U przestrzeni dostępnej do użycia (wyłączając listwy zasilające / panele krosownicze / inne stałe elementy, jeżeli ich obecność uniemożliwia montaż standardowego serwera w danym miejscu), minimalne wymiary 1000 mm x 600 mm, zamknięcie co najmniej na zamek mechaniczny.
3. Gwarantowane redundantne zasilanie w obrębie szafy (przynajmniej 2 niezależne obwody zasilające, minimum 22 gniazdka zasilających ISO/IEC C14).
4. Serwerownia zasilana co najmniej z dwóch niezależnych linii energetycznych z podtrzymaniem zasilania przez urządzenia UPS oraz agregat prądotwórczy, zapewniający bezprzerwowe podtrzymanie zasilania w przypadku zaniku napięcia sieciowego.
5. Wartość mocy maksymalnej z tabliczek znamionowych wszystkich zasilanych urządzeń, przy uwzględnieniu redundancji zasilaczy, wynosi 12 kW.
6. Zamawiający wymaga aby energia elektryczna była rozliczana w formie ryczałtu i uwzględniona w miesięcznej opłacie.
7. Symetryczne łącze do sieci Internet o dostępnej przepustowości co najmniej 500 Mb/s. Łącze do sieci Internet musi być chronione poprzez aplikacyjny system anti-DDoS.
8. Przynajmniej 14 stałych adresów IPv4.
9. Możliwość utworzenia minimum 4 tuneli IPSec S2S oraz minimum 10 połączeń VPN dla użytkowników.
10. Możliwość tworzenia użytkowników VPN na urządzeniu Wykonawcy (maksymalnie 50 kont, baza lokalna).
11. Inter-VLAN (10 VLAN) dla sieci wewnętrznych z wydajnością nie mniejszą niż 1 Gb/s.
12. Wraz z dostępem do sieci Internet, Wykonawca świadczyć będzie usługi bezpieczeństwa teleinformatycznego, polegające na ochronie styku z siecią Internet realizowaną na

- poziomie warstwy 3, 4 i 7 modelu OSI. Wykonawca zapewni dostęp do panelu administracyjnego, umożliwiającego administrację fizycznym lub wirtualnym firewallem (współdzielonym z innymi klientami Wykonawcy, pod warunkiem zapewnienia pełnej separacji oraz wydajności od sieci innych klientów) oraz bieżący dostęp do logów firewala.
13. SLA na dostęp do sieci Internet, zasilanie i utrzymanie temperatury w serwerowni nie niższe niż 99,5% liczone w skali miesiąca. Na żądanie Zamawiającego, Wykonawca udostępni raport dostępności do sieci Internet.
 14. Fizyczna i techniczna ochrona obiektu serwerowni realizowana w trybie 24 / 7 / 365, w tym wyposażenie serwerowni w automatyczny system ochrony przeciwpożarowej, system kontroli dostępu oraz system monitoringu wizyjnego CCTV działający na zewnątrz oraz w środku serwerowni, zapewniający rejestrację obrazu wraz z datą i godziną oraz zapewniający przechowywanie i dostęp do zarejestrowanych zapisów przez minimum 30 dni.
 15. Dostęp w ramach serwerowni do klawiatura USB, mysz USB, monitor VGA / DVI / HDMI.

III. Wymagania związane z przeniesieniem urządzeń Zamawiającego do centrum danych Wykonawcy

1. Wykonawca w ramach usługi, przeniesie urządzenia Zamawiającego z obecnej lokalizacji do swojego centrum danych.
2. Obecnie urządzenia znajdują się pod adresem: ul. Grochowskiej 21a, 04-186 Warszawa.
3. Przeniesienie urządzeń powinno rozpocząć się w dniu 31.07.2024 i trwać nie dłużej niż 24 godziny. Wykonawca w tym czasie powinien rozłączyć wszystkie połączenia (fiber channel, LAN, zasilanie) i zdemontować urządzenia w obecnej lokalizacji, zabezpieczyć je na czas transportu, przewieźć do swojego centrum danych, zainstalować i odtworzyć połączenia w dedykowanej szafie.
4. Zamawiający informuje iż urządzenia nie są objęte ubezpieczeniem na wypadek uszkodzenia lub zaginięcia w transporcie. Wykonawca ubezpieczy sprzęt Zamawiającego na czas transportu. W przypadku wystąpienia usterki lub zaginięcia sprzętu, Zamawiający oczekuje, że Wykonawca doprowadzi urządzenia do stanu poprawnego działania, wymieniając uszkodzone lub zaginione komponenty na własny koszt.
5. Naprawa, o której mowa powyżej, powinna zostać wykonana w terminie maksymalnie do 5 dni kalendarzowych od chwili rozpoczęcia przeniesienia urządzeń. Jeżeli Wykonawca nie jest w stanie wykonać naprawy w powyższym terminie, Zamawiający dopuszcza użycie urządzeń zastępczych, o parametrach nie gorszych niż przenoszone urządzenia.
6. Do czasu potwierdzenia przez Zamawiającego poprawności uruchomienia urządzeń i wykonanych konfiguracji, Wykonawca zapewni niezbędne i natychmiastowe wsparcie.
7. Wykonawca przed przystąpieniem do relokacji sprzętu powinien okazać Zamawiającemu, posiadaną polisą o której mowa powyżej.

IV. Wymagania związane z konfiguracją firewalla

1. Wykonawca przeprowadzi konfigurację reguł i interfejsów na przydzielonym Zamawiającemu firewallu, która będzie odzwierciedlać aktualną konfigurację na firewallu udostępnionym Zamawiającemu. Zamawiający korzysta z urządzenia typu Next Generation Firewall Palo Alto PA-5220. Aktualne reguły firewall wykorzystują technologię IPSEC VPN, Threat-Prevention, URL Filtering oraz DNS Security. Firewall jest wykorzystywany do ochrony styku z internetem jak i inter-vlan wewnętrznych podsieci Zamawiającego. Firewall musi posiadać aktualne sygnatury i subskrypcje dla podanych funkcji.
2. Firewall wydajnościowo musi obsługiwać ruch wewnętrzny jaki i zewnętrzny uwzględniając nieplanowane incydenty takie jak ataki DDoS.
3. Wszelkie reguły firewall oraz interfejsy muszą być w osobnym kontekście (VSYS).
4. Na podstawie obecnej konfiguracji reguł, Wykonawca dostosuje je do przydzielonej publicznej adresacji IP. Wewnętrzna adresacja oraz nr VLAN, powinny zostać niezmienione.
5. Połączenia z infrastrukturą Zamawiającego dwoma interfejsami RJ45 1GB z agregacją LACP

V. Wymagania związane z audytem centrum danych

1. Wykonawca umożliwi Zamawiającemu przeprowadzenie audytu centrum danych, razy w ciągu trwania Umowy.
2. Wykonawca, ze swojej strony, wyznaczy osobę z którą będzie się porozumiewał Zamawiający w sprawach związanych z przeprowadzeniem audytu, przekazaniem niezbędnych dokumentów i wizyty w centrum danych.
3. Audyt będzie obejmował następujące obszary tematyczne:
 - a. certyfikaty bezpieczeństwa posiadane przez centrum danych,
 - b. procedury związane z kontrolą dostępu do centrum danych,
 - c. systemy klimatyzacji centrum danych,
 - d. zasilanie centrum danych w tym agregaty prądotwórcze, systemy UPS, dostawy energii,
 - e. systemy gaśnicze,
 - f. systemy monitorowania warunków środowiskowych,
 - g. zabezpieczenie łącza Internetowego,
 - h. dostawcy łącza internetowego,
 - i. procedury związane ze zgłaszaniem incydentów w centrum danych,
 - j. ochrona fizyczna centrum danych.
4. Audyt w centrum danych będzie przeprowadzany maksymalnie w czasie 2 godzin. Wykonawca powinien udostępnić zamawiającemu dokumenty związane z przeglądami systemów klimatyzacji, agregatów prądotwórczych, UPS, Systemów gaśniczych, monitorujących warunki środowiskowe.

VI. Wymagania zawiązane z optymalizacją obciążenia serwerów

1. Wykonawca będzie świadczył usługę optymalizacji obciążenia serwerów (load balancing) dla aplikacji webowej przy pomocy platformy sprzętowej składającej się z dwóch urządzeń działających w klastrze wysokiej dostępności HA lub przy pomocy rozwiązania softwarowego.
2. Ze względu na bezpieczeństwo oraz na niezawodność pracy, Wykonawca nie dopuszcza rozwiązań typu Open Source.
3. Zamawiający dopuszcza możliwość współdzielenia urządzenia z innymi klientami Wykonawcy, pod warunkiem zapewnienia pełnej separacji od sieci innych klientów.
4. Pojedyncze urządzenie wchodzące w skład klastra lub rozwiązanie softwarowe/chmurowe, powinno spełniać następujące wymagania:
 - a. musi mieć możliwość zapewnienia minimum 1 Gbps przepustowości dla ruchu SSL dla pakietów 100B.
 - b. musi pozwalać na minimum 25 000 jednoczesnych połączeń TCP
 - c. powinno posiadać wydajność szyfrowania na poziomie 10000 nowych połączeń CPS SSL dla klucza RSA 2024 oraz P256 ECC SSL.
 - d. musi zapewniać możliwość rozkładania obciążenia za pomocą algorytmów minimum: Fastest Connection, Inbound/Outbound Bandwith, Concurrent Connections.
 - e. musi zapewniać load balancing bazując na informacjach z warstw 4-7 modelu OSI ISO.
 - f. musi wspierać monitorowanie dostępności usług na serwerze za pomocą protokołów HTTP i HTTPS (aktywne próbkowanie).
 - g. powinno obsługiwać funkcje: sticky sessions, SSL Passthrough, terminację SSL, modyfikacje treści w warstwie ISO/OSI L7 (modyfikacja nagłówków HTTPS – np. X-Forwarded-For, X-Forwarded-Proto).

VII. Specyfikacja urządzeń objętych usługą kolokacji

Urządzenie	Wysokość U	Wartość początkowa
Macierz dyskowa IBM v5000	3	226 534,02 zł
Serwer Dell EMC PowerEdge R640	1	72 645,03 zł
Serwer Dell EMC PowerEdge R640	1	72 645,03 zł
Serwer Dell EMC PowerEdge R640	1	72 645,03 zł
Macierz dyskowa Dell EMC ME5024	2	132 000,00 zł
Switch FC IBM SAN24B-6	1	56 088,00 zł
Switch FC IBM SAN24B-6	1	56 088,00 zł
Switch LAN Brocade ICX7450	1	27 060,00 zł

Switch LAN Brocade ICX7450	1	27 060,00 zł
Serwer Dell EMC PowerEdge R330	1	13 286,46 zł

Łączna wartość	756 051,57 zł
-----------------------	----------------------