**Rozeznanie rynku – „Wdrożenie systemu VPN do zarządzania zdalnym dostępem do sieci ZUS”**

**I. Ogólne informacje:**

1. Szczegółowe wymagania dotyczące oferty są przedstawione w dalszej części niniejszego zapytania.
2. Oferta cenowa będzie podstawą do oszacowania wartości zamówienia.
3. Niniejsze zapytanie nie stanowi oferty zawarcia umowy w rozumieniu przepisów Kodeksu Cywilnego.
4. Potencjalni składający nie będą uprawnieni do występowania z jakimikolwiek roszczeniami pieniężnymi lub niepieniężnymi w związku z przygotowaniem odpowiedzi na niniejsze zapytanie.
5. Treść dokumentu, wszelkie informacje, do których się odwołuje oraz prowadzona korespondencja i rozmowy muszą zostać zachowane w tajemnicy. Przesyłający ofertę jest zobowiązany do nie udostępniania osobom trzecim informacji uzyskanych w związku z zapytaniem bez pisemnej zgodny i upoważnienia ze strony ZUS.
6. Wycena powinna być podana w PLN, z podatkiem VAT.
7. Okres obowiązywania oferty powinien wynosić co najmniej 3 miesiące.
8. Z wyceny ma jasno wynikać jaki producent i model urządzenia zostały wycenione.

**II. Termin i sposób złożenia odpowiedzi:**

Odpowiedzi należy przesłać w terminie do **13.06.2018** r., na adres e-mail:

[wojciech.kudla@zus.pl](mailto:wojciech.kudla@zus.pl)

[dariusz.skibinski@zus.pl](mailto:dariusz.skibinski@zus.pl)

[tomasz.wojcik02@zus.pl](mailto:tomasz.wojcik02@zus.pl)

**III. Sposób przygotowania oferty cenowej**

Oferta powinna zawierać wycenę systemu VPN zgodnie z poniższą tabelą:

|  |  |  |
| --- | --- | --- |
| **Formularz cenowy** | | |
| **Produkt** | **Ilość** | **Koszt jednostkowy (PLN brutto)** |
| 1. Koncentrator VPN (Appliance) |  |  |
| 2. System kontroli zdalnego dostępu (Appliance) z możliwością przechowywania danych logowań przez okres co najmniej 1 roku |  |  |
| 3. System kontroli zdalnego dostępu (Appliance) z możliwością przechowywania danych logowań przez okres co najmniej 3 lat |  |  |
| 4. Licencje dla 6000 użytkowników |  |  |
| 5. Licencje dla 10000 użytkowników |  |  |
| 6. Zwiększenie licencji o 1000 użytkowników\* |  |  |
| 7. Zwiększenie licencji o 2000 użytkowników\*\* |  |  |
| 8. Serwis 36 miesięcy - 8 godzinny czas naprawy wraz ze wsparciem producenta |  |  |
| 9. Serwis 36 miesięcy - 24 godzinny czas naprawy wraz ze wsparciem producenta |  |  |
| 10. Przeszkolenie\*\*\* |  |  |
| 11. Wdrożenie |  |  |
| 12. Prawa autorskie\*\*\*\* |  |  |

\* Ad. 6. Prosimy o wycenę ewentualnego zwiększenia ilości licencji (w trakcie trwania umowy) o kolejne 1000 licencji.

\*\* Ad. 7. Prosimy o wycenę ewentualnego zwiększenia ilości licencji (w trakcie trwania umowy) o kolejne 2000 licencji.

\*\*\* Ad. 10. Prosimy o wycenę dwudniowego (8 godzin dziennie) przeszkolenia z zakresu przeprowadzonego wdrożenia dla maksymalnie 10 pracowników Zamawiającego (jednorazowo przeszkolenie może być przeprowadzone dla maksymalnie 5 osób) na terenie Warszawy. Przeszkolenie musi być przeprowadzone w języku polskim.

\*\*\*\* Ad. 12. Prosimy o wycenę kosztów przeniesienia praw autorskich z tytułu opracowania projektu wdrożenia i migracji systemu VPN oraz dokumentacji powdrożeniowej systemu VPN.

Koncentrator VPN (wpisać producenta i model): ………………………………………………………………..

System kontroli zdalnego dostępu (wpisać producenta i model): ………………………………………………..

### IV. Opis przedmiotu zamówienia

Przedmiotem wyceny jest zakup systemu VPN do zarządzania zdalnym dostępem do sieci ZUS. W ramach zakupu dostarczone mają być koncentratory VPN oraz system kontroli zdalnego dostępu.

**Wymagania dla koncentratorów VPN:**

1. Rozwiązanie musi być dostarczone jako dedykowane urządzenia sieciowe (Appliance).

2. System musi posiadać licencje niezbędne do obsługi ilości użytkowników podanych   
w tabeli z pkt. IV oraz obsługiwać minimum 500 jednoczesnych, szyfrowanych połączeń SSL VPN (Remote Access).

3. System musi posiadać licencje niezbędne do obsługi minimum 100 jednoczesnych, szyfrowanych tuneli IPSEC (Site-to-Site).

4. Zestawienie szyfrowanego tunelu VPN do zasobów ZUS musi skutkować brakiem możliwości jednoczesnego korzystania z lokalnego dostępu do sieci Internet (tzw. split-tunneling).

5. Wymagane jest wykorzystanie certyfikatów cyfrowych podczas zestawiania połączeń poprzez sieć VPN.

6. Urządzenia terminujące tunele VPN muszą wykorzystywać mechanizmy wysokiej dostępności (tryb Failover Active/Standby).

**Wymagania dla systemu kontroli zdalnego dostępu:**

1. Rozwiązanie musi być dostarczone jako dedykowane urządzenia sieciowe (Appliance).

2. Uwierzytelnianie użytkowników musi opierać się na wykorzystaniu protokołu TACACS/RADIUS.

3. Uwierzytelnianie użytkowników zdalnych musi zostać zrealizowane przy użyciu „silnych” haseł, tzn. minimum 8 znaków, zawierających małe i duże litery, cyfry oraz znaki specjalne.

4. System musi integrować się z usługami LDAP i RADIUS oraz umożliwiać tworzenie, modernizację oraz utrzymywanie lokalnych baz danych (w tym bazy użytkowników).

5. Rozwiązanie musi integrować się z Active Directory 2008 R2 lub nowszym za pośrednictwem RADIUS lub Kerberos.

6. System musi umożliwiać zdalny dostęp do zasobów sieci korporacyjnej dla użytkowników VPN w tym samym czasie oraz umożliwiać filtrowanie i ograniczanie ruchu zgodnie z polityką bezpieczeństwa firmy.

7. Zdalny dostęp będzie realizowany za pośrednictwem sieci Internet z wykorzystaniem urządzeń użytkowników (notebooki i inne typowe urządzenia mobilne).

8. Uwierzytelnianie tożsamości użytkownika ma się odbywać za pomocą certyfikatów cyfrowych oraz wymiany kluczy publicznych i prywatnych pomiędzy hostem, a serwerem CA (ang. Certification Authority).

9. System musi umożliwiać kontrolę i weryfikację urządzeń użytkowników pod kątem zgodności z obowiązującymi regułami dostępu do sieci korporacyjnej (sprawdzanie wersji OS, aktualizacji oprogramowania antywirusowego, stosowanych wpisów w rejestrze OS).

10. System musi umożliwiać uruchomienie w trybie wysokiej dostępności geograficznej, tj. tak, aby serwery lub farma serwerów zlokalizowane w dwóch ośrodkach obliczeniowych Zamawiającego) miały zaimplementowane mechanizmy wysokiej dostępności (tryb Failover Active/Standby).

11. System musi pozwalać na przechowywanie danych z logowania się użytkowników do systemu VPN przez okres co najmniej 1 roku.

**Istotniejsze warunki usługi:**

Wykonawca zobowiązany jest do przeprowadzenia wdrożenia oraz przeniesienia obecnej funkcjonalności, polityk i baz danych z obecnego rozwiązania (koncentratory VPN Cisco ASA, system Cisco NAC oraz system Cisco ACS).

Wykonawca zapewni w ramach całodobowej usługi gwarancyjnej dostęp telefoniczny oraz e-mail do serwisu Wykonawcy w trybie ciągłym, tzn. 7 dni w tygodniu, 24 godziny na dobę, 365 dni w roku. Usługi serwisu gwarancyjnego będą świadczone w lokalizacjach Zamawiającego w Warszawie ul. Szamocka 3, 5 oraz ul. Czerniakowska 16. Maksymalny czas reakcji na zgłoszenie serwisowe to 1 godzina.

Wycena serwisu ze wsparciem producenta musi zapewnić Zamawiającemu dostęp do najnowszych wersji oprogramowania (przez cały okres obowiązywania umowy).

Okres obowiązywania serwisu gwarancyjnego – 36 miesięcy.