Zapytanie o informację

(RFI)

Warszawa, wrzesień 2018

I. *Przedmiot i cel Zapytania o informację*

1. Zakład Ubezpieczeń Społecznych rozważa dokonania zakupu polegającego na **dostawie, wdrożeniu i świadczeniu usług opieki serwisowej systemu dostępu do Internetu** w lokalizacji Zamawiającego w Warszawie.
2. Celem niniejszego zapytania o informację jest pozyskanie przez Zakład Ubezpieczeń Społecznych od podmiotów zajmujących się profesjonalnie określonym zakresem, danych dotyczących szacunkowego kosztu realizacji.

II. Ogólne informacje o charakterze formalnym

1. Niniejsze Zapytanie o informację nie stanowi oferty zawarcia umowy w rozumieniu przepisów *ustawy z dnia 23 kwietnia 1964 r.- Kodeks cywilny*. Udzielenie odpowiedzi na niniejsze Zapytanie o informację nie będzie uprawniało do występowania z jakimikolwiek roszczeniami w stosunku do Zakładu Ubezpieczeń Społecznych.
2. Niniejsze Zapytanie o informację nie jest elementem jakiegokolwiek postępowania o udzielenie zamówienia, w rozumieniu *ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych*, jak również nie jest elementem jakiegokolwiek procesu zakupowego prowadzonego w oparciu o wewnętrzne regulacje Zakładu Ubezpieczeń Społecznych.
3. Złożenie odpowiedzi na niniejsze Zapytanie o informację jest jednoznaczne z wyrażeniem zgody przez podmiot składający taką odpowiedź na nieodpłatne wykorzystanie przez Zakład Ubezpieczeń Społecznych wszystkich lub części przekazanych informacji.

III. Termin i sposób złożenia odpowiedzi na Zapytanie o informację

1. Odpowiedź na Zapytanie o informację należy przygotować w oparciu o formularz stanowiący **Załącznik nr 2** do Zapytania o informację.
2. W przypadku, gdy informacje zawarte w odpowiedzi na Zapytanie o informację stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, podmiot składający taką odpowiedź winien to wyraźnie zastrzec w odpowiedzi. Brak przedmiotowego zastrzeżenia, Zakład Ubezpieczeń Społecznych będzie traktował przekazane informacje jako informacje, które nie stanowią tajemnicy przedsiębiorstwa.
3. Odpowiedź na Zapytanie o informację należy przesłać w terminie do **21 września 2018 r.** na adres e-mail: **rfi-urzadzenia-windows@zus.pl**

Załącznik nr 1 do Zapytania o informację

Opis przedmiotu Zapytania o informację

I. W ramach realizacji przedmiotu zamówienia Wykonawca:

1. Dostarczy i wdroży oferowany system dostępu do Internetu (dalej System) z uwzględnieniem sprzętu i licencji;
2. Dostarczy Zamawiającemu dokumentację powdrożeniową proponowanego Systemu wraz z procedurami eksploatacyjnymi;
3. Obejmie 36-miesięczną usługą opieki serwisowej oferowane rozwiązanie.

II. Wymagania funkcjonalne oferowanego rozwiązania:

1. Funkcjonalność Systemu:
   1) System powinien posiadać dedykowany appliance sprzętowy pełniący funkcję proxy. Nie dopuszcza się standardowych serwerów, systemów wielofunkcyjnych, maszyn wirtualnych ani rozwiązań chmurowych;
   2) Appliance musi pracować pod kontrolą utwardzonego systemu operacyjnego;
   3) System musi pracować, jako forward proxy dla protokołów http, https. Pozostałe protokoły powinny być obsługiwane w trybie tunelowania;
   4) System musi zapewnić możliwości działania, jako:
      a. proxy dedykowane (explicit proxy),
      b. proxy transparentne (transparent proxy),
      c. explicit i transparent jednocześnie;
   5) System musi zapewniać cachowanie, w tym cachowanie video;
   6) w przypadku treści video oglądanych jednocześnie przez wielu użytkowników System musi ściągać treść tylko raz i dzielić ją na wszystkich użytkowników (split streaming);
   7) dla treści video System musi implementować dedykowane proxy dla Quick Time, Windows Media i Flash;
   8) System musi być dostarczony w postaci klastra typu aktywny – aktywny, N+1 (awaria jednego węzła nie wpływa na wydajność całości), zapewniającego obsługę 45 tysięcy użytkowników;
   9) System będzie działać w dwóch centrach przetwarzania danych i w każdym centrum przetwarzania danych muszą znajdować się przynajmniej po dwa urządzenia, ale nie więcej niż cztery;
   10) dla użytkownika końcowego System forward proxy musi być widoczny pod jednym adresem IP;
   11) dopuszczalne jest zaproponowanie systemu składającego się z kilku niezależnych forward proxy z centralnym systemem zarządzania politykami lub synchronizacją polityk(zmiana konfiguracji na serwerze centralnej polityki lub na jednym węźle automatycznie dystrybuuje konfigurację na pozostałe węzły). Balansowanie ruchu za pomocą plików PAC, WPAD lub innych statycznych metod jest niedopuszczalne;
   12) Zamawiający dopuszcza balansowanie ruchem z wykorzystywaniem posiadanych przez Zamawiającego rozwiązań F5 LTM. W tym przypadku wykonawca dostarczy pełną dokumentację opisującą konfigurację posiadanych przez Zamawiającego rozwiązań F5 LTM do współpracy z Systemem. Konfiguracja fizyczna rozwiązania F5 LTM leży po stronie Zamawiającego;
   13) System musi wspierać przekierowanie ruchu z wykorzystaniem routingu opartego o polityki (PBR – policy based routing) lub przekierowania z wykorzystaniem protokołu

WCCP;

14) System musi umożliwiać inspekcję ruchu HTTPS;
15) System musi filtrować dostęp do stron WWW porównując odwołania z bazą danych dostarczaną i aktualizowaną on-line przez producenta. Baza powinna zawierać nie mniej niż 30 milionów skategoryzowanych stron internetowych. Domeny zawarte w bazie powinny być podzielone na kategorie. Wśród zdefiniowanych przez producenta kategorii muszą znaleźć się kategorię takie jak:
    a. strony rządowe,
    b. finanse,
    c. biznes,
    d. sport,
    e. pornografia,
    f. przemoc,
    g. hazard,
    h. gry komputerowe,
    i. portale społecznościowe,
    j. zakupy i aukcje,
    k. hacking,
    l. blogi,
    m. poczta internetowa,
    n. chaty internetowe,
    o. strony obciążające pasmo:
        - internetowe radio i telewizja
        - telefonia internetowa
        - media streamingowe
        - udostępniania plików w technologii per-to-peer
        - strony do indywidualnego backupu.
16) System musi wspierać kategoryzację z serwisu YouTube via klucz API lub przez ustawienie odpowiedniego predefiniowanego poziomu ustawień;
17) System musi umożliwiać wyłączenie ruchu HTTPS dla konkretnych kategorii stron www, użytkowników, adresów źródłowych lub docelowych;
18) System musi umożliwiać tworzenie grup użytkowników o odrębnych przywilejach - takich jak dostępność i wykluczenie: stron i kategorii stron, protokołów (np. ftp), rodzaju strumienia danych (Streaming Media, Peer 2 Peer, VOIP), typu pobieranych plików, zakresów czasowych;
19) System musi posiadać możliwość tworzenia polityk per adres IP, zakresów adresów IP, nazwy użytkownika, przynależności do grupy Active Directory/LDAP/lokalnej bazy/RADIUS/certyfikat użytkownika;
20) System powinien być wyposażony w moduł lub moduły raportujące, umożliwiające:
    a. generowanie raportów zawierających szczegółowe informacje na temat, pojedynczych użytkowników i grup, (nazwa użytkownika, adres IP), kiedy (dokładna data i godzina) i które strony odwiedzał (dokładne adresy URL) , wielkość pobranych i wysłanych danych, ilość odwołań z możliwością podziału na odpowiednie kategorie stron. Raporty te powinny być dostępne przez przeglądarkę www;
    b. System musi umożliwiać raportowanie zarówno informacji o odwiedzanych stronach www, jak i o zablokowanych przez System próbach odwiedzenia stron www, które

zostały zablokowane polityką;
c. raportowanie musi dotyczyć każdego z urządzeń Systemu osobno, jak również wszystkich urządzeń łącznie;
d. raporty muszą być dostępne „od ręki" co najmniej z okresu 6 ostatnich miesięcy (bez konieczności oczekiwania na import danych lub ich przebudowę (rebuilding));
e. dane z okresu wcześniejszego niż dostępne „od ręki" muszą mieć możliwość składowania, z możliwością przywrócenia ich do wglądu;
f. w plikach logów muszą znajdować się informacje m.in. o: nazwie użytkownika, adresie IP stacji, odwiedzanym hoście, wielkości danych, dokładnym czasie (data, godzina, minuta, sekunda);
g. archiwizację logów systemu za okres co najmniej 3 lat.

21) kategoryzacja adresów URL musi być oparta o statyczną, aktualizowaną przynajmniej raz dziennie bazę bezpośrednio na urządzeniu lub rozproszony serwis w chmurze analizujący w czasie rzeczywistym nieznane adresy URL (analiza dynamiczna);
22) System musi pozwalać na konstruowanie polityki w oparciu o reputację danej strony w połączeniu z bazą kategorii i geolokalizacji np. blokuj strony skategoryzowane, jako dynamiczny DNS o średnim lub wysokim poziomie ryzyka znajdujące się w Chinach;
23) System musi dawać możliwości kontroli popularnych webaplikacji z akcjami typu upload, download, post czy send. Minimalny zestaw webaplikacji: facebook, twitter, linkedin, youtube, box, sugarsync, Flickr, istagram, webex;
24) System musi posiadać możliwość rozszerzenia listy wspieranych web aplikacji, do co najmniej 3 tysięcy aplikacji;
25) System musi umożliwiać wysyłanie informacji do zewnętrznego systemu poprzez protokół ICAP w trybie request mode i responde mode;
26) System musi umożliwiać integrację z systemami typu DLP, przeciwdziałającymi wyciekowi informacji;
27) w przypadku blokady dostępu do strony system musi pokazywać w pełni konfigurowalną stronę html;
28) System wspiera transparentne uwierzytelnienia użytkowników z wykorzystaniem protokołu NTLM;
29) System musi wspierać transparentną identyfikację użytkownika z wykorzystaniem dedykowanego agenta odpytującego się bezpośrednio kontrolera domeny o zalogowanych użytkowników;
30) System musi mieć możliwość komunikowania się z posiadanymi przez Zamawiającego serwerami Active Directory bez potrzeby instalowania dedykowanego agenta;
31) System musi zapewniać możliwość lokalnego uwierzytelniania użytkownika w przypadku braku informacji go identyfikujących;
32) System musi mieć możliwość identyfikacji stacji roboczej na podstawie revers DNS;
33) System musi mieć graficzny interfejs do budowanie polityk dostępowych, umożliwiający budowanie nieograniczonych rozgałęzień;
34) zarządzanie urządzeniem musi być możliwe zarówno przez interfejs graficzny(lokalna lub centralna konsola) jak i poprzez command-line;
35) System nie powinien mieć żadnych ograniczeń interfejsu command-line w stosunku do interfejsu graficznego;
36) System powinien mieć możliwość tworzenia polityk dostępowych do Internetu w zależności od dni oraz godzin;
37) dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od

strony serwerów;

38) inspekcja ruchu HTTPS musi być możliwa dla RSA / DHE i ECDHE;
39) System musi umożliwiać przesłanie rozszytego ruchu HTTPS do dodatkowej analizy do systemów typu IPS (pracujący w warstwie L2), typu sandbox (pracujących w warstwie L2 lub L3), czy też DLP;
40) System musi umożliwiać wyłączenie ruchu HTTPS dla konkretnych kategorii stron www, użytkowników, adresów źródłowych lub docelowych;
41) System musi dawać możliwość blokowania stron szyfrowanych nawet, jeśli mechanizm rozszywania SSL jest wyłączony np. blokowanie Facebooka;
42) w trybie rozszywania ruchu SSL system musi dawać możliwość kontroli certyfikatu serwera, do którego łączy się użytkownik tj. minimum sprawdzenia daty ważności i łańcucha certyfikacji;
43) System musi posiadać funkcję Safe Search – przeciwdziałającą pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo;
44) System musi umożliwiać analizę odpowiedzi przesyłanych zwrotnie do łączących się do Internetu użytkowników. Analiza ta polegać ma na:
    a. klasyfikacji w czasie rzeczywistym czy odpowiedź nie zawiera zaciemnionych skryptów; kodu, który mógłby spowodować wykorzystanie podatności na łączącym się komputerze,
    b. sprawdzenie czy odpowiedź nie zawiera w sobie znanych i specjalizowanych zagrożeń,
    c. analizie reputacji stron www, wspierają wykrywanie nowych stron www,
    d. wykrywaniu stron pishingowych;
45) powyższa analiza musi odbywać się na jednym i tym samym urządzeniu, na którym uruchomiona jest usługa forward proxy;
46) Silnik antywirusowy pracujący na Systemie musi skanować pliki z wszystkich kategorii URL;
47) Silnik antywirusowy musi skanować pliki o rozmiarze, co najmniej 5GB;
48) Silnik antywirusowy musi skanować pliki, o co najmniej 30 poziomach zagnieżdżenia kompresji;
49) System musi wykrywać i blokować pliki skompresowane z hasłem dla wszystkich użytkowników z możliwością wyłączenia uprzywilejowanych użytkowników;
50) System musi blokować nieznane typy plików na podstawie analizy treści;
51) System musi blokować pliki o złej reputacji na podstawie bazy hashy plików;
52) System musi dawać możliwość blokowania w oparciu o własną listę hashy plików;
53) System musi umożliwiać w przyszłości rozszerzenie funkcjonalności antymalware o rozwiązanie typu sandbox pracujące lokalnie i umożliwiające detonację plików w czasie rzeczywistym tj. bez infekcji pacjenta zdrowego;
54) sygnatury do analizy odpowiedzi powinny być na bieżąco aktualizowane w czasie nie dłuższym niż 5 minut;
55) System musi umożliwiać przesyłanie powyższych informacji z urządzenia do zewnętrznych systemów typu SIEM;
56) System musi wspierać protokół Socks do bezpiecznej komunikacji dla aplikacji TCP/IP;
57) Oferowany System musi być rozwiązaniem docelowym, umożliwiającym w przyszłości rozbudowę zasobów dyskowych, pamięci RAM i interfejsów sieciowych;

58) Każde z poszczególnych urządzeń Systemu urządzenia musi spełniać wymogi przedstawione w poniższej tabeli:

Lp.	Parametr	Wymagania
1	Pamięć RAM urządzenia	Nie mniej niż 64GB
2	Maksymalna przepustowość do Internetu	2 Gbps
3	Gęstość interfejsów	Nie mniej niż dwa interfejsy z możliwością obsadzenia wkładkami 1000 Base-T, nie mniej niż dwa interfejsy z możliwością obsadzenia wkładkami SFP+, oddzielny interfejs zarządzania, port konsolowy. Należy zapewnić przynajmniej 2 porty 1000 Base-T oraz 2 porty 10 Gigabit Ethernet SR

2. Korzystanie przez Zamawiającego z dostarczonego rozwiązania nie może naruszać majątkowych praw autorskich osób trzecich.

3. Wszystkie dostarczane urządzenia, moduły i podzespoły muszą być:

1) oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
2) przeznaczone do sprzedaży i serwisu na rynku polskim.

III. Warunki serwisu i płatności

1. System objęty będzie 36 miesięczną usługą opieki serwisowej na następujących warunkach:
   1) dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta,
   2) sposób obsługi zgłoszeń w trybie 24 godziny na dobę, 7 dni w tygodniu, 365/366 dni w roku,
   3) wymiana sprzętu następnego dnia roboczego po identyfikacji usterki. Dniem roboczym Zamawiającego są dni od poniedziałku do piątku (z wyłączeniem dni ustawowo wolnych od pracy) w godzinach 8:00 – 16:00.
   4) subskrypcja dla serwisu kategoryzacji stron www oraz sygnatur wykorzystywanych do analizy odpowiedzi,
   5) gwarantowany czas rozwiązania zgłoszonego problemu - 24 godziny od momentu zgłoszenia awarii do jej usunięcia. W uzasadnionych przypadkach (np. termin mieszczący się w ciągu 24 godzin byłby dla Zamawiającego niedogodny z uwagi na funkcjonujące przetwarzanie lub inne uwarunkowania) Zamawiający ma prawo do wydłużenia czasu naprawy.
2. Sposób zgłaszania awarii
   1) zgłoszenia będą dokonywane w trybie 24 godziny na dobę, 7 dni w tygodniu, 365/366 dni w roku za pomocą HP Service Manager lub w przypadku jego awarii pocztą elektroniczną lub telefonicznie,
   2) czas reakcji (potwierdzenie przyjęcia zgłoszenia) nie dłuższy niż 1 godzina od momentu zgłoszenia awarii. Potwierdzenia należy dokonać w systemie HP Service Manager lub w przypadku jego awarii za pomocą e-maila zwrotnego,
   3) zgłoszenie awarii musi odbywać się w języku polskim,

4) reakcja serwisu Wykonawcy na zgłoszenie serwisowe nie powinna przekraczać 2 godzin.

Załącznik nr 2 do Zapytania o informację

Dane podmiotu	
Adres Wykonawcy: kod, miejscowość, ulica, nr lokalu	
Nr telefonu	
E-mail	

Zakład Ubezpieczeń Społecznych

ul. Szamocka 3, 5

01-748 Warszawa

FORMULARZ ODPOWIEDZI NA ZAPYTANIE O INFORMACJĘ

1. W odpowiedzi na Zapytanie o informację dotyczące ***Zakupu systemu dostępu do Internetu*** przedstawiam poniższe informacje.
2. Poniższe informacje (**wybrać właściwe**):
   - *zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i nie mogą być ujawniane innym podmiotom.
   - *nie zawierają informacji stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i mogą być ujawniane innym podmiotom.
3. Przedstawione informacje dotyczące szacunkowych kosztów (**wybrać właściwe*):
   - *zawierają upusty na poziome ….% od „cen katalogowych”.
   - *nie zawierają upustów od „cen katalogowych” i ZUS może uzyskać upust na poziome ….% od poniżej przedstawionych kosztów.
4. Wszelką korespondencję dotyczącą przedmiotowej odpowiedzi na zapytanie o informację należy kierować na:

Imię i Nazwisko	
Nazwa podmiotu	
Adres	
Nr telefonu	
Nr faksu	
Adres e-mail	

Specyfikacja proponowanego rozwiązania

	Szczegółowa specyfikacja (m.in. producent, nazwa, model, wersja)
Urządzenia proxy	*<Szczegółowa informacja o proponowanych urządzeniach>*
Oprogramowanie	*<Szczegółowa informacja o proponowanych oprogramowanie>*

Formularz cenowy

	1	2	3	4	5	6	7	8
Lp.	**Zakres**	**Jednostka**	**Cena jednostkowa w PLN (bez VAT)**	**Stawka podatku VAT w %**	**Cena jednostkowa w PLN (z VAT) [kol. 3 + kol. 4]**	**Całkowita Liczba**	**Razem w PLN (bez VAT) [kol. 3 * kol. 6]**	**Razem w PLN (z VAT) [kol. 5 * kol. 6]**
1	**Urządzenia proxy**	**Sztuka**	**……***	**……***	**……***	**12**	**……***	**……***
2	**Oprogramowanie**	**Liczba użytkowników**	**……***	**……***	**……***	**45.000**	**……***	**……***
3	**Usługa wdrożeniowa**		**……***	**……***	**……***	**1**	**……***	**……***
4	**Usługa opieki serwisowej**		**……***	**……***	**……***	**36**	**……***	**……***
5	**Prawa autorskie do projektu**		**……***	**……***	**……***	**1**	**……***	**……***
……*								

* Wypełnia oferent.

Wskazane w powyższym formularzu ceny obejmują wszystkie koszty związane z realizacją przedmiotu zamówienia.

Nazwisko i imię osoby (osób) uprawnionej(-ych)	Podpis(-y) osoby(osób) uprawnionej(-ych)	Miejscowość i data