**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.

**II Termin i sposób złożenia odpowiedzi:**

Odpowiedzi należy przesłać w terminie do 29.08.2017 ., na adresy e-mail: [wycenyDEI@zus.pl](mailto:wycenyDEI@zus.pl)

**III Sposób przygotowania oferty cenowej**

Oferta powinna zawierać:

1. informację o wykonawcy,
2. wycenę dostarczonego rozwiązania z 36 miesięczną gwarancją………….zł brutto, w tym:
   * + 1. Wartość sprzętu…………zł brutto;
          - W tym 12 miesięczna gwarancja…..zł brutto;
       2. Wartość oprogramowania……..zł brutto;
          - W tym 12 miesięczna gwarancja ……..zł brutto;
       3. Wartość usług wdrożeniowych…..zł brutto;
       4. Wartość praw autorskich do projektu……..zł brutto (o ile występują);
       5. Wartość usług 24 miesięcznego serwisu pogwarancyjnego;
          - W tym serwis pogwarancyjny dla sprzętu……..zł brutto;
          - W tym serwis pogwarancyjny dla oprogramowania……..zł brutto

# RZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest zakupu infrastruktury na potrzeby zapewnienia bezpieczeństwa brzegowego na punkcie styku Internetu z siecią KSI (zwanej „Systemem”).

Na przedmiot zamówienia składa się:

1. zakup czterech urządzeń proxy wraz z licencjami na 45.000 użytkowników,
2. wdrożenie zakupionego Systemu, przygotowanie dokumentacji wdrożeniowej, powdrożeniowej wraz z procedurami eksploatacyjnymi ,
3. udzieleniu 12 miesięcznej gwarancji na oferowany System a następnie świadczenie 24 miesięcznej pogwarancyjnej opieki serwisowej Systemu.

Termin realizacji zamówienia:

1. wdrożenie Systemu – do 14 dni od podpisania umowy;
2. dokumentacja powdrożeniowa wraz z procedurami eksploatacyjnymi– do 14 dni od wdrożenia.
3. Funkcjonalność Systemu:
4. System powinien posiadać dedykowany appliance sprzętowy pełniący funkcję proxy. Nie dopuszcza się standardowych serwerów, systemów wielofunkcyjnych, maszyn wirtualnych ani rozwiązań chmurowych;
5. Appliance musi pracować pod kontrolą utwardzonego systemu operacyjnego;
6. System musi pracować, jako forward proxy dla protokołów http, https. Pozostałe protokoły powinny być obsługiwane w trybie tunelowania;
7. System musi zapewnić możliwości działania, jako:
8. proxy dedykowane (explicit proxy),
9. proxy transparentne (transparent proxy),
10. explicit i transparent jednocześnie;
11. System musi zapewniać cachowanie, w tym cachowanie video;
12. w przypadku treści video oglądanych jednocześnie przez wielu użytkowników System musi ściągać treść tylko raz i dzielić ją na wszystkich użytkowników (split streaming);
13. dla treści video System musi implementować dedykowane proxy dla Quick Time, Windows Media i Flash;
14. 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;
15. 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;
16. dla użytkownika końcowego System forward proxy musi być widoczny pod jednym adresem IP;
17. 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;
18. Zamawiający dopuszcza balansowanie ruchem z wykorzystywaniem posiadanych przez Zamawiającego rozwiązań F5 LTM. Konfiguracja rozwiązania F5 LTM leży po stronie Wykonawcy;
19. System musi wspierać przekierowanie ruchu z wykorzystaniem routingu opartego o polityki (PBR – policy based routing) lub przekierowania z wykorzystaniem protokołu WCCP;
20. System musi umożliwiać inspekcję ruchu HTTPS;
21. 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:
22. strony rządowe,
23. finanse,
24. biznes,
25. sport,
26. pornografia,
27. przemoc,
28. hazard,
29. gry komputerowe,
30. portale społecznościowe,
31. zakupy i aukcje,
32. hacking,
33. blogi,
34. poczta internetowa,
35. chaty internetowe,
36. strony obciążające pasmo:
    * internetowe radio i telewizja
    * telefonia internetowa
    * media streamingowe
    * udostępniania plików w technologii per-to-peer
    * strony do indywidualnego backupu.
37. System musi wspierać kategoryzację z serwisu YouTube via klucz API;
38. System musi umożliwiać wyłączenie ruchu HTTPS dla konkretnych kategorii stron www, użytkowników, adresów źródłowych lub docelowych;
39. 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;
40. 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;
41. System powinien być wyposażony w moduł lub moduły raportujące, umożliwiające:

* 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;
* System musi umożliwiać raportowanie zarówno informacji o odwiedzanych stronach www, jak i o zablokowanych przez System próbach odwiedzenia stron www, które zostały zablokowane polityką;
* raporty powinny być dostępne „od ręki” co najmniej z okresu 6 ostatnich miesięcy (bez konieczności oczekiwania na import danych lub ich przebudowę (rebuilding));
* 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);
* archiwizację logów systemu za okres co najmniej 3 lat.

1. kategoryzacja adresów URL musi być oparta zarówno o statyczną, aktualizowaną przynajmniej raz dziennie bazę bezpośrednio na urządzeniu jak i rozproszony serwis w chmurze analizujący w czasie rzeczywistym nieznane adresy URL (analiza dynamiczna);
2. 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;
3. 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;
4. System musi posiadać możliwość rozszerzenia listy wspieranych web aplikacji, do co najmniej 10 tysięcy aplikacji;
5. System musi umożliwiać wysyłanie informacji do zewnętrznego systemu poprzez protokół ICAP w trybie request mode i responde mode;
6. System musi umożliwiać integrację z systemami typu DLP, przeciwdziałającymi wyciekowi informacji;
7. w przypadku blokady dostępu do strony system musi pokazywać w pełni konfigurowalną stronę html;
8. System będzie umożliwiał wyświetlanie captchy dla stron, których nie ma w bazie i nie zostały skategoryzowane przez mechanizm dynamicznej klasyfikacji;
9. System musi wspierać transparentne uwierzytelnienie użytkowników z wykorzystaniem protokołu Kerberos;
10. System musi wspierać mechanizm Kerberos Constrained Delegation;
11. System musi wspierać transparentną identyfikację użytkownika z wykorzystaniem dedykowanego agenta odpytującego się bezpośrednio kontrolera domeny o zalogowanych użytkowników;
12. System musi mieć możliwość komunikowania się z posiadanymi przez Zamawiającego serwerami Active Directory bez potrzeby instalowania dedykowanego agenta;
13. System musi zapewniać możliwość lokalnego uwierzytelniania użytkownika w przypadku braku informacji go identyfikujących;
14. System musi mieć możliwość identyfikacji stacji roboczej na podstawie revers DNS;
15. System musi mieć graficzny interfejs do budowanie polityk dostępowych, umożliwiający budowanie nieograniczonych rozgałęzień;
16. zarządzanie urządzeniem musi być możliwe zarówno przez interfejs graficzny(lokalna lub centralna konsola) jak i via command-line;
17. System nie powinien mieć żadnych ograniczeń interfejsu command-line w stosunku do interfejsu graficznego;
18. System powinien mieć możliwość tworzenia polityk dostępowych do Internetu w zależności od dni oraz godzin;
19. dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony serwerów;
20. inspekcja ruchu HTTPS musi być możliwa dla RSA / DHE i ECDHE;
21. 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;
22. System musi umożliwiać wyłączenie ruchu HTTPS dla konkretnych kategorii stron www, użytkowników, adresów źródłowych lub docelowych;
23. System musi dawać możliwość blokowania stron szyfrowanych nawet, jeśli mechanizm rozszywania SSLa jest wyłączony np. blokowanie Facebooka;
24. 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;
25. System musi posiadać funkcję Safe Search – przeciwdziałającą pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo;
26. System musi umożliwiać analizę odpowiedzi przesyłanych zwrotnie do łączących się do Internetu użytkowników. Analiza ta polegać ma na:
27. klasyfikacji w czasie rzeczywistym czy odpowiedź nie zawiera zaciemnionych skryptów; kodu, który mógłby spowodować wykorzystanie podatności na łączącym się komputerze,
28. sprawdzenie czy odpowiedź nie zawiera w sobie znanych (system antywirusowy) i specjalizowanych zagrożeń,
29. analizie reputacji stron www, wspierają wykrywanie nowych stron www,
30. wykrywaniu stron pishingowych;
31. powyższa analiza musi odbywać się na jednym i tym samym urządzeniu, na którym uruchomiona jest usługa forward proxy;
32. System musi umożliwiać w przyszłości rozbudowę o drugi silnik antywirusowy na istniejącym sprzęcie;
33. Silnik antywirusowy pracujący na Systemie musi skanować pliki z wszystkich kategorii URL;
34. Silnik antywirusowy musi skanować pliki o rozmiarze, co najmniej 5GB;
35. Silnik antywirusowy musi skanować pliki, o co najmniej 30 poziomach zagnieżdżenia kompresji;
36. System musi wykrywać i blokować pliki skompresowane z hasłem dla wszystkich użytkowników z możliwością wyłączenia uprzywilejowanych użytkowników;
37. System musi blokować nieznane typy plików na podstawie analizy treści;
38. System musi blokować pliki o złej reputacji na podstawie bazy hashy plików;
39. System musi dawać możliwość blokowania w oparciu o własną listę hashy plików;
40. 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;
41. sygnatury do analizy odpowiedzi powinny być na bieżąco aktualizowane w czasie nie dłuższym niż 5 minut;
42. System musi umożliwiać przesyłanie powyższych informacji z urządzenia do zewnętrznych systemów typu SIEM;
43. Oferowany System musi być rozwiązaniem docelowym, umożliwiającym w przyszłości rozbudowę zasobów dyskowych, pamięci RAM i interfejsów sieciowych;
44. 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 |

1. System objęty będzie 12 miesięczną gwarancją producenta a następnie 24 miesięczną opieka serwisu pogwarancyjnego. W obrębie gwarancji i opieki serwisowej zawarte musi być:
2. dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta,
3. sposób obsługi zgłoszeń w trybie 24 godziny na dobę, 7 dni w tygodniu, 365/366 dni w roku,
4. wymiana sprzętu następnego dnia roboczego po identyfikacji usterki,
5. subskrypcja dla serwisu kategoryzacji stron www oraz sygnatur wykorzystywanych do analizy odpowiedzi,
6. 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.
7. Sposób zgłaszania awarii
8. 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.
9. 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.