POWIATOWY URZĄD PRACY w ŁAŃCUCIE
ul. Piłsudskiego 9
37-100 Łańcut
tel. 17 225 91 31
fax. 17 225 91 66
e-mail: rzla@praca.gov.pl

PI.244.3.2023

Łańcut, dnia 17 lipca 2023 r.

ZAPYTANIE OFERTOWE

w celu rozeznania rynku na usługę:
„Dostawa, uruchomienie i konfiguracja sprzętowego Firewalla - UTM"

Zgodnie z regulaminem Powiatowego Urzędu Pracy w Łańcucie z dnia 17 grudnia 2021r. o udzielaniu zamówień publicznych, których wartość jest mniejsza niż 130 000,00 zł zapraszamy zainteresowanych Wykonawców do przesłania oferty cenowej.

Zainteresowanych Wykonawców prosimy o przesłanie oferty cenowej.

1. Przedmiot zamówienia:

- **Przedmiotem zamówienia jest dostawa sprzętowego urządzenia Firewall / UTM dla Powiatowego Urzędu Pracy w Łańcucie, która obejmuje:**

a) Dostawa urządzenia.
b) Prace instalacyjno-konfiguracyjne dla dostarczonego rozwiązania.
c) Montaż i fizyczne uruchomienie systemu.
d) Konfiguracja dostarczonego urządzenia.
e) Przeprowadzenie testów funkcjonalnych urządzenia.
f) Oddanie systemu do eksploatacji.
g) Opracowanie dokumentacji powykonawczej.
h) Przeszkolenie 2 pracowników.
i) Opiekę serwisową przez 12 miesięcy od dnia protokolarnego odbioru przedmiotu umowy przez okres 12 miesięcy

- **Wymagania ogólne dla urządzeń i oprogramowania:**

a) Całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski.
b) Całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nieużywana we wcześniejszych projektach.
c) Całość sprzętu musi być objęta gwarancją opartą o **świadczenia gwarancyjne producenta sprzętu**, niezależnie od statusu partnerskiego Wykonawcy przez okres 12 miesięcy (chyba, że zapisy szczegółowe stanowią inaczej).

- **Warunki gwarancji i wsparcia technicznego dla sprzętu i oprogramowania sieciowego:**

O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. 12 miesięczna gwarancja (chyba, ze zapisy szczegółowe stanowią inaczej) oparta na gwarancji producenta rozwiązania; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań
W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;

- **Oprogramowanie:**

Oprogramowanie powinno posiadać min. 1-roczne wsparcie (chyba, że zapisy szczegółowe stanowią inaczej) – dostarczanie aktualizacji, zdalne (telefon lub e-mail, www) wsparcie techniczne w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem oprogramowania.

- **Miejsce instalacji:**

Dostawa, montaż i instalacja w ramach niniejszego postępowania odbędzie w siedzibie Zamawiającego.

- **Montaż i uruchomienie:**

Zamawiający wymaga, aby wraz z dostawą sprzętu przeprowadzić jego instalację, konfigurację oraz uruchomienie. Wszelkiego typu elementy połączeniowe np.: kable, zakończenia itp. powinny zostać ujęte w wycenie.
Przekazanie elementów systemu nastąpi w drodze protokołu przekazania do użytkowania, który będzie potwierdzał jego prawidłową instalację i działanie.

- **Jeżeli zapisy szczegółowe nie specyfikują inaczej Zamawiający oczekuje prac w zakresie:**

Wniesienia, ustawienia i fizycznego montażu wszystkich dostarczonych urządzeń w szafie rack w pomieszczeniu (miejscach) wskazanych przez zamawiającego.
Urządzenia, które nie są montowane w szafach teleinformatycznych powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego.
Usunięcia opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
Podłączenia całości rozwiązania do infrastruktury Zamawiającego.
Wykonania procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
Wykonania połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).

Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).

Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji zamówienia, **w ramach jednego weekendu (Piątek godz. 16:00 - Sobota godz. 22:00)** po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym.

UWAGA. Powyższe zapisy gwarancyjne, oraz czas wykonania obowiązują jedynie w przypadku braku szczegółowych zapisów w poniższym opisie przedmiotu zamówienia.

W celu potwierdzenia ważności oferty i spełniania wymaganych warunków, Wykonawca załączy na etapie składania oferty następujące dokumenty i oświadczenia według poniższych zasad:

a) Certyfikaty osób przewidzianych do wykonania prac konfiguracyjnych.
b) VMware Certified Professional - Data Center Virtualization 2019 (VCP-DCV 2019) (lub nowszym).
c) Veeam Certified Engineer (VMCE).

2. Wymagania szczegółowe:

Zamawiający wymaga dostarczenia 1 szt. Urządzenia FIrewall spełniającego **łącznie** poniższe warunki:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

- System musi wspierać IPv4 oraz IPv6 w zakresie:
    a. Firewall.
    b. Ochrony w warstwie aplikacji.
    c. Protokołów routingu dynamicznego.
- Redundancja, monitoring i wykrywanie awarii

W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
Monitoring stanu realizowanych połączeń VPN.
System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

- Interfejsy, Dysk, Zasilanie:
    a. System realizujący funkcję Firewall musi dysponować minimum:
        i. 16 portami Gigabit Ethernet RJ-45.
        ii. 8 gniazdami SFP 1 Gbps.
        iii. 2 gniazdami SFP+ 10 Gbps.
    b. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
    c. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
    d. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
    e. System musi być wyposażony w zasilanie AC.
- Parametry wydajnościowe:
    a. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
    b. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
    c. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
    d. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
    e. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
    f. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
    g. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
- Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
b. Kontrola Aplikacji.
c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
d. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
e. Ochrona przed atakami - Intrusion Prevention System.
f. Kontrola stron WWW.
g. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
h. Zarządzanie pasmem (QoS, Traffic shaping).
i. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
j. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
k. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
l. Analiza ruchu szyfrowanego protokołem SSH.

m. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system Polityki, Firewall
n. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
o. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    i. Translację jeden do jeden oraz jeden do wielu.
    ii. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
p. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
q. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
r. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    i. Amazon Web Services (AWS).
    ii. Microsoft Azure
    iii. Google Cloud Platform (GCP).
    iv. OpenStack.
    v. VMware NSX.

- Połączenia VPN
    a. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
        i. Wsparcie dla IKE v1 oraz v2.
        ii. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
        iii. Obsługa protokołu Diffie-Hellman grup 19 i 20.
        iv. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
        v. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
        vi. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
        vii. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
        viii. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
        ix. Mechanizm „Split tunneling" dla połączeń Client-to-Site.
    b. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
        i. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
        ii. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
        iii. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

YS.

- Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

  a. Routingu statycznego.
  b. Policy Based Routingu.
  c. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

- Funkcje SD-WAN
  a. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
  b. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
- Zarządzanie pasmem
  a. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
  b. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
  c. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
- Ochrona przed malware
  a. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
  b. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
  c. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
  d. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
  e. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
  f. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
- Ochrona przed atakami
  a. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
  b. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
  c. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
  d. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
  e. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
  f. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
- Kontrola aplikacji
  a. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

15.

b. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
c. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
d. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

- Kontrola WWW
  a. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
  b. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
  c. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
  d. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
  e. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
  f. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
  g. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
- Uwierzytelnianie użytkowników w ramach sesji
  a. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
     i. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
     ii. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
     iii. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
  b. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
  c. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
  d. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
- Zarządzanie
  a. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
  b. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
  c. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
  d. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

e. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
f. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
g. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

- Logowanie
  a. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
  b. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
  c. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
  d. Musi istnieć możliwość logowania do serwera SYSLOG.
- Serwisy i licencje
  a. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
  b. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
- Gwarancja oraz wsparcie
  a. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

3. Prace instalacyjno–konfiguracyjne dla dostarczonego rozwiązania:

- **Wymagania wstępne**

Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa.

Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.

W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową. Zamawiający w tym celu wyznaczy ze swojej strony Szefa Projektu z odpowiednimi kompetencjami.

Zamawiający wymaga następującego zakresu usług w ramach prowadzonego projektu realizowanego w porozumieniu z Zamawiającym:

a) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia.
b) Sporządzenia Dokumentacji Wykonawczej, według której nastąpi realizacja. Dokumentacja Wykonawcza musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności:
   - testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności
   - sposób odbioru uzgodniony z Zamawiającym
   - listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu
   - opis przypadków, w których projekt dopuszcza niedziałanie systemu
c) Realizacja wdrożenia nastąpi według Planu Wdrożenia, po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą.
d) Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą.

- **Montaż i fizyczne uruchomienie systemu – wymagania ogólne**

a) Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w miejscach wskazanych przez zamawiającego z uwzględnieniem wszystkich lokalizacji.
b) Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
c) Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
d) Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
e) Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
f) Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
g) Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
h) Wykonania projektu rozmieszczenia i połączenia lokalnych i odległych urządzeń sieciowych.
i) Wykonania projektu struktury adresacji urządzeń sieciowych.
j) Wykonania projektu architektury sieci VLAN.
k) Wykonania projektu podłączenia i wykorzystania systemu macierzowego oraz backupowego do systemu serwerowego.
l) Określenie wymagań związanych z polityką bezpieczeństwa.
m) Opracowanie dokumentacji wykonawczej i powykonawczej.

- **Konfiguracja dostarczonych urządzeń UTM**

Zamawiający wymaga zaplanowania, przeprowadzenia procedury konfiguracji urządzeń bezpieczeństwa oraz przeprowadzenie testów funkcjonalnych co najmniej w zakresie:

a) Przeprowadzenie audytu obecnej konfiguracji
b) Wykonanie kopii zapasowej obecnej konfiguracji
c) Przeprowadzenie aktualizacji do najnowszej stabilnej wersji zalecanej przez producenta oprogramowania
d) Konfiguracja interfejsów, adresacji, polityk bezpieczeństwa, reguł NAT
e) Konfiguracja tuneli VPN
f) Rekonfiguracja urządzeń Firewall w celu zapewnienia bezpiecznej komunikacji dla systemu zunifikowanej komunikacji (w tym inspekcja dla protokołów wykorzystywanych przez system, terminale – SIP / H.323)
g) Zapewnienie mechanizmów QoS dla systemu telefonii IP oraz aplikacji Syriusz
h) Podłączenie oraz skonfigurowanie dodatkowego łącza WAN

- **Termin Wykonania Prac Instalacyjno-Wdrożeniowych. Oddanie Systemu Do Eksploatacji.**
  Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia, w ramach jednego weekendu (piątek godz. 16:00 - sobota godz. 22:00) po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym. Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci dwóch osób w siedzibie Zamawiającego w ciągu 7 dni następujących po pracach wdrożeniowo – instalacyjnych w godzinach od 7.30 do 16.00.
  W tym czasie przedstawiciele Wykonawcy zobowiązani są do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. W tym czasie przedstawiciele Wykonawcy dokonają także przeszkolenia dwóch pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań.

- **Opracowanie Dokumentacji Powykonawczej**
  Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Zamawiający jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.

- **Opieka Serwisowa**
  Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych.

4. Miejsce i termin złożenia oferty:

Uzupełniony i podpisany **Formularz ofertowy**, stanowiący **(Załącznik nr 1 -Formularz ofertowy)** do zapytania, należy przesłać na adres w formie pisemnej **do dnia 25.07.2023 r. do godz. 12:00** na adres:
Powiatowy Urząd Pracy w Łańcucie, 37-100 Łańcut ul. Piłsudskiego 9.

Wykonawca składa ofertę w niniejszym postępowaniu w nieprzejrzystej, zabezpieczonej przed dostępem (zaklejonej) kopercie z adnotacją: **„Oferta na dostawę sprzętowego Firewalla - UTM, nie otwierać do dnia składania ofert do godziny 12.00."**
Znaczenie dla oceny zachowania powyższego terminu ma data i godzina wpływu oferty pod wskazany adres, a nie data jej wysłania. Oferty złożone po terminie nie biorą udziału w postępowaniu.

Przy wyborze oferty Zamawiający będzie się kierował kryterium: CENA – 100%

Punktacja w tym kryterium zostanie obliczona wg wzoru: C=(Cn:Co)x100 gdzie:
Cn - cena najniższa wśród ofert
Co – cena danego Wykonawcy
Obliczenia zostaną dokonane z dokładnością do dwóch miejsc po przecinku.
Ocenie podlegają wyłącznie oferty spełniające wymagania określone przez Zamawiającego w niniejszym zaproszeniu.
O wyborze najkorzystniejszej oferty zadecyduje największa ilość punktów uzyskanych przez Wykonawcę w kryterium cena.

Minimalny termin związania z ofertą: 14 dni od dnia wyboru najkorzystniejszej oferty.

Warunki płatności: zapłata za wykonane zamówienie nastąpi w terminie do 14 dni – licząc od dnia, w którym Zamawiający otrzyma prawidłowo wystawioną fakturę VAT. Podstawą do wystawienia faktury VAT jest protokół odbioru bez zastrzeżeń, o którym mowa w umowie, podpisany przez Zamawiającego.

Osobami uprawnionymi do kontaktu są:
a) Tomasz Sochacki e-mail: **admin@pup-lancut.pl**
b) Marcin Cużytek e-mail: **m.cuzytek@pup-lancut.pl**

Opis sposobu przygotowania i złożenia oferty:
a) Zaleca się złożenie oferty na formularzu ofertowym przygotowanym przez Zamawiającego – wg wzoru stanowiącego: **(Załącznik 1-Formularz ofertowy)**.
b) Treść oferty musi odpowiadać treści zapytania.
c) Wykonawca może złożyć tylko jedną ofertę.
d) Wszelkie koszty związane z przygotowaniem i złożeniem oferty ponosi Wykonawca.
e) Wykonawca ma prawo przed terminem wycofać ofertę składając stosowne oświadczenie.
f) Wykonawca może, przed upływem terminu do składania ofert zmienić ofertę.
g) Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty wyłącznie przed upływem terminu składania ofert. Powiadomienie o wprowadzeniu zmian przez Wykonawcę musi być złożone wg takich samych wymagań jak składana oferta, z dopiskiem „ZMIANA OFERTY"
h) Oferta powinna być czytelna i złożona w języku polskim.
i) Ofertę podpisuje osoba lub osoby uprawnione do reprezentowania i składania oświadczeń woli w imieniu Wykonawcy. Jeżeli ofertę w imieniu Wykonawcy podpisuje pełnomocnik Wykonawcy, do oferty należy dołączyć pełnomocnictwo.

Załączniki:

1. Załącznik 1 - Formularz ofertowy (wzór)
2. Załącznik 2 - Umowa (wzór)
3. Załącznik 3 – Protokół odbioru

DYREKTOR
Powiatowego Urzędu Pracy

Wojciech Wydrzyński
.....
(podpis Dyrektora)