Złotoryja, dnia 13 października 2015r.

L.dz/ZP/214/1224/2015

…..….....
…..….....
…..….....

Dyrektor Wojewódzkiego Szpitala Psychiatrycznego w Złotoryi
Samodzielny Publiczny Zakład Opieki Zdrowotnej
59-500 Złotoryja, ul. Szpitalna 9

Z A P R A S Z A

do złożenia „oferty cenowej" na zadanie pod nazwą:

„Dostawa urządzeń typu UTM do Wojewódzkiego Szpitala Psychiatrycznego w Złotoryi"

1. **Przedmiot zamówienia:**
   a) Dostawa 2 urządzeń typu UTM (United Thread Menagement) przeznaczonych do sieci komputerowych obsługujących 45 – 70 stacji roboczych Wojewódzkiego Szpitala Psychiatrycznego w Złotoryi i Ośrodka Psychiatrycznej i Odwykowej Opieki Zdrowotnej w Legnicy.
   b) Oferta może obejmować wymianę aktualnie posiadanego rozwiązania i powinna uwzględniać wszystkie możliwe rabaty z tego wynikające.
   c) Posiadane rozwiązania: Netasq U30, Netasq U70
   d) **Wykonawca** zapewnia konfigurację i uruchomienie urządzeń w siedzibie Zamawiającego w Wojewódzkim Szpitalu Psychiatrycznym w Złotoryi przy ul. Szpitalnej 9, oraz jego filii - Ośrodku Psychiatrycznej i Odwykowej Opieki Zdrowotnej w Legnicy przy ul. Chojnowskiej 81 w obecności personelem informatycznego Zamawiającego. Konfiguracja winna nastąpić w uzgodnionym przez strony terminie, jednak nie później niż 10 dni od daty otrzymania sprzętu.
   e) **Zamawiający** oczekuje wykonania zamówienia w terminie do 10 dni, od dnia udzielenia zamówienia.

2. **Urządzenie musi bezwzględnie zapewniać funkcjonalności:**
   a) Firewall, IPS, VPN, filtr URL, Antywirus
   b) audyt podatności
   c) obsługa kart SD
   d) 8 portów Ethernet w tym min. 2 konfigurowalne interfejsy jako WAN
   e) zarządzenie przez przeglądarkę internetową
   f) serwis urządzenia – 1 rok
   g) serwis typu NBD (24 x7)

3. Przykładowe orientacyjne parametry techniczne:

1) Zapora korporacyjna (Firewall):
   a) Firewall klasy Stateful Inspection.
   b) Urządzenie powinno obsługiwać translacje adresów NAT, PAT, 1-PAT
   c) Urządzenie powinno dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (część jako router, a część jako bridge).
   d) Narzędzie do konfiguracji firewalla powinno umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów.
   Przy zastosowaniu takiej technologii osoba administrująca ma możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
   e) Edytor reguł na firewallu powinien posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
   f) Firewall powinien umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows NT4.0 (NTLM) i Windows 2k (Kerberos).

2) Intrusion Prevention System (IPS):
   a) System detekcji i prewencji włamań (IPS) powinien być zaimplementowany w jądrze systemu i wykrywa włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
   b) Moduł IPS powinien nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.
   c) Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
   d) Urządzenie powinno mieć możliwość inspekcji dowolnego ruchu tunelowanego wewnątrz protokołu SSL.
   e) Administrator urządzenia powinien mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

3) Kształtowanie pasma (Traffic Shapping):
   a) Urządzenie powinno mieć możliwość kształtowania pasma w oparciu o priorytezację ruchu oraz minimalną i maksymalną wartość pasma.
   b) Ograniczenie pasma lub priorytezacja powinna być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
   c) Rozwiązanie powinno umożliwiać tworzenie tzw. kolejki nie mającej wpływ na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
   d) Urządzenie powinno mieć możliwość zdefiniowania priorytetu kolejki, która obsłuży cały ruch nie ujęty przez kolejki użytkownika.

4) Ochrona antywirusowa:
   a) Rozwiązanie powinno pozwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
   b) Co najmniej jeden z dwóch skanerów antywirusowych powinien być dostarczany w ramach podstawowej licencji.
   c) Administrator powinien mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto powinna być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

5) Ochrona antyspam:
   a) Producent powinien udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
   b) Ochrona antyspam powinna działać w oparciu o:
      - Białe/czarne listy
      - DNS RBL
      - Heurystyczny skaner
   c) W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
   d) Wpis w nagłówku wiadomości powinien być w formacie zgodnym z formatem programu Spamassassin**.**

6) Wirtualne sieci prywatne (VPN):
   a) Urządzenie powinno posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
   b) Odpowiednio kanały VPN można budować w oparciu o:
      - PPTP VPN
      - IPSec VPN
      - SSL VPN
   c) Urządzenie powinno posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
   d) Urządzenie powinno posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.

7) Filtr adresów URL:
   a) Urządzenie powinno posiadać wbudowany filtr URL.
   b) Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP zarówno w trybie RESPOND jak i REQUEST.
   c) Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
      - blokowanie dostępu do adresu URL,
      - zezwolenie na dostęp do adresu URL,
      - blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

d) Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
e) Możliwość identyfikacji oraz blokowanie przesyłanych danych z wykorzystaniem typu MIME.
f) Możliwość stworzenia białej listy stron wyłączonych z filtrowania URL oraz białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.

8) Uwierzytelnianie:
   a) Urządzenie powinno pozwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
      - lokalną bazę użytkowników (wewnętrzny LDAP),
      - zewnętrzną bazę użytkowników (zewnętrzny LDAP),
      - integracje z serwerem Microsoft Active Directory.
   b) Rozwiązanie powinno pozwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:
      - SSL
      - Radius
      - NTLM
      - Kerberos
   c) Autoryzacja użytkowników z wykorzystaniem użytkowników Microsoft Active Directory nie wymaga instalacji agenta na serwerze AD ani modyfikacji schematu.

9) Administracja łączami od dostawców usług internetowych (ISP):
   a) Urządzenie powinno posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
   b) Mechanizm równoważenia obciążenia łącza internetowego powinien działać w oparciu o następujące dwa mechanizmy:
      - równoważenie względem adresu źródłowego,
      - równoważenie względem adresu docelowego.
   c) Urządzenie powinno posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

10) Administracja urządzeniem:
   a) Producent powinien dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.
   b) Konfiguracja urządzenia powinna być możliwa z wykorzystaniem polskiego interfejsu graficznego.
   c) Komunikacja pomiędzy aplikacją do zarządzania, a urządzeniem musi odbywać się przez przeglądarkę www z wykorzystaniem bezpiecznego protokołu https.
   d) Urządzenie może być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
   e) Urządzenie powinno być dostępne wraz z konsolą do centralnej administracji pozwalającą na zarządzanie przynajmniej 5 urządzeniami w różnych lokalizacjach w podstawowej cenie urządzenia.
   f) Urządzenie powinno mieć możliwość eksportowania logów na zewnętrzny serwer (syslog).

11) Parametry sprzętowe:
    a) Urządzenie powinno być pozbawione dysku twardego, a oprogramowanie wewnętrznego działa z wbudowanej pamięci flash.
    b) Liczba portów Ethernet 10/100/1000 – min. 6
    c) Przepustowość Firewalla wraz z włączonym systemem IPS wynosi min. 600 Mbps.
    d) Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi 120 Mbps.
    e) Maksymalna liczba tuneli VPN IPSec nie powinna być mniejsza niż 100.
    f) Obsługa min. 32 VLAN-ów.
    g) Maksymalna liczba równoczesnych sesji wynosi min. 100 000.
    h) Urządzenie jest nielimitowane na użytkowników.

12) Pasywny skaner wnętrza sieci:
    Urządzenie winno zawierać tzw. pasywny skaner wnętrza sieci umożliwiający wykrywanie nieaktualnych aplikacji oraz innych zagrożeń mogących zaistnieć na stacjach roboczych w sieci komputerowej. Licencja na to oprogramowanie może być udzielana oddzielnie i nie może być krótsza niż trzy lata.

13) Przykładowe rozwiązania:
    - Stormshield SN 300 + opcjonalne wymagania wynikające ze specyfikacji
    - Fortigate 60D + opcjonalne wymagania wynikające ze specyfikacji

4. Kryterium oceny ofert:

- cena 100%

5. Warunki płatności:

Zamawiający zobowiązuje się zapłacić **Wykonawcy** w/w kwotę w czterech równych ratach, przelewem na podane konto w terminie:

- pierwsza rata: do 30 dni, po realizacji zamówienia oraz otrzymaniu prawidłowo sporządzonej faktury VAT;
- druga rata: do 30 dni od spłacenia pierwszej raty;
- trzecia rata: do 60 dni od spłacenia pierwszej raty;
- czwarta rata: do 90 dni od spłacenia pierwszej raty.

6. Wykonawca do „propozycji cenowej" winien złożyć:

- ofertę cenową (netto + VAT = brutto) uwzględniającą wszystkie koszty realizacji zamówienia (formularz w załączeniu);
- kserokopię wpisu do właściwego rejestru, potwierdzoną za zgodność z oryginałem;
- oświadczenie **Wykonawcy** o spełnianiu warunków określonych w art. 22 ust. 1 Pzp. oraz niepodleganiu wykluczeniu - art. 24 ust. 1, 2 (zał. nr 1);
- oświadczenie **Wykonawcy** o związaniu ofertą (zał. nr 2);
- wzór umowy na dostawę urządzeń typu UTM (zał. nr 3).

7. **Termin, forma, miejsce złożenia „oferty cenowej”:**

   - termin: do dnia 19 października 2015r, godz. 10:00
   - forma:
     a) pisemnie: Złotoryja, ul. Szpitalna 9, Sekretariat Szpitala
     b) e-mailem: sekretariat.wszp@gmail.com

     Uwaga

     W temacie e-maila należy wpisać **Oferta na dostawę urządzeń typu UTM**, a w treści umieścić zwrot **„Proszę o potwierdzenie otrzymania niniejszej oferty”.**
     Otrzymanie oferty, zostanie niezwłocznie potwierdzone przez Zamawiającego e-mailem zwrotnym.
     W przypadku nieotrzymania potwierdzenia prosimy o kontakt tel. pod nr 76 8779 330 - przed upływem terminu składania ofert.

8. **Zamawiający** zastrzega sobie prawo do odrzucenia oferty jeżeli jej cena będzie znacząco odbiegała od cen rynkowych urządzeń tej samej klasy.

9. Zastrzega się prawo unieważnienia postępowania, w przypadku otrzymania ofert niespełniających oczekiwań **Zamawiającego**.

10. Osoby uprawnione do kontaktów z **Wykonawcami:**

    a) Sebastian Filipiak nr tel. 76 8779 300 wew. 323

11. **UWAGA:**

    Szacunkowa wartość zamówienia jest niższa od kwoty 30.000 euro - nie stosuje się przepisów ustawy Prawo zamówień publicznych art. 4 pkt 8 ustawy z dnia 29 stycznia 2004r. Pzp, (Dz.U. z dnia 2013r, poz. 907 z późniejszymi zmianami).

Złotoryja, dnia 13 października 2015r. ….....