KOLUSZKI
zawsze w centrum

Koluszki, dnia 29.12.2017 r.

IN.270.102.5.2017

Zaproszenie do złożenia oferty / Zapytanie ofertowe

(postępowanie poniżej kwoty 30.000 EURO).

1. Przedmiot zamówienia

Przedmiotem niniejszego zamówienia jest dostawa sprzętu informatycznego – urządzenia UTM STORMSHIELD SN510 (sztuk 1) wraz z niezbędnym serwisem i licencjami - dla Urzędu Miejskiego w Koluszkach.

2. Wymagania dotyczące przedmiotu zamówienia - (UTM STORMSHIELD SN510 – 1 sztuka) i realizacji zamówienia:

OBSŁUGA SIECI

1) Wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA

2) Firewall klasy Stateful Inspection.
3) Obsługa translacji adresów NAT n:1, NAT 1:1 oraz PAT.
4) Możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (część jako router, a część jako bridge).
5) Interface (GUI) do konfiguracji firewalla umożliwia 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.
6) Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u.
7) Edytor reguł na firewallu posiada wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
8) Firewall umożliwia uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

IPS

9) System detekcji i prewencji włamań (IPS) ma 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.
10) Moduł IPS jest opracowany przez producenta urządzenia.
11) Moduł IPS zabezpiecza przed co najmniej 10 000 ataków i zagrożeń.
12) Moduł IPS wykrywa i jednocześnie usuwa szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.
13) Urządzenie ma możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.

14) Administrator urządzenia ma 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.

KSZTAŁTOWANIE PASMA

15) Urządzenie posiada możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
16) Ograniczenie pasma lub priorytetyzacja jest określane względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
17) Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
18) Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

19) Rozwiązanie zezwala na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie
20) Co najmniej jeden z dwóch skanerów antywirusowych jest dostarczany w ramach podstawowej licencji.
21) Administrator ma możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
22) Administrator ma 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 posiada możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

OCHRONA ANTYSPAM

23) Producent udostępnia mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
24) Ochrona antyspam działa w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. heurystyczny skaner.
25) 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.
26) Wpis w nagłówku wiadomości zaklasyfikowanej jako spam jest w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWANTE

27) Urządzenie posiada wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
28) Urządzenie pozwala budować kanały VPN w oparciu o:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN
29) SSL VPN działa w trybach Tunel i Portal.
30) Urządzenie posiada funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
31) Urządzenie posiada wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
32) Urządzenie pozwala na tworzenie tuneli w oparciu o technologię Route Based.

FILTR DOSTĘPU DO STRON WWW

33) Urządzenie posiada wbudowany filtr URL.
34) Filtr URL działa w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
35) Administrator ma możliwość dodawania własnych kategorii URL.
36) Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
37) Moduł filtra URL, wspierany przez HTTP PROXY, jest zgodny z protokołem ICAP co najmniej w trybie REQUEST.
38) Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
    a. blokowanie dostępu do adresu URL,

b. zezwolenie na dostęp do adresu URL,
c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

39) Administrator posiada możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
40) Strona blokady umożliwia wykorzystanie zmiennych środowiskowych.
41) Filtrowanie URL uwzględnia także komunikację po protokole HTTPS.
42) Urządzenie posiada możliwość identyfikacji oraz blokowanie przesyłanych danych z wykorzystaniem typu MIME.
43) Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.
44) Urządzenie posiada możliwość włączenia pamięci cache dla ruchu http.

UWIERZYTELNIANIE

45) Urządzenie zezwala na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory.
46) Rozwiązanie zezwala na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos.
47) Urządzenie posiada co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.
48) W urządzeniu co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
49) Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI OD DOSTAWCÓW USŁUG INTERNETOWYCH (ISP).

50) Urządzenie posiada wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
51) Mechanizm równoważenia obciążenia łącza internetowego działa w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem adresu źródłowego i docelowego (połączenia).
52) Mechanizm równoważenia łącza uwzględnia wagi przypisywane osobno dla każdego z łączy do Internetu.
53) Urządzenie posiada mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
54) Urządzenie posiada mechanizm statycznego trasowania pakietów.
55) Urządzenie oferuje możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
56) Urządzenie posiada możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
57) Rozwiązanie zapewnia obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIP, OSPF oraz BGP.
58) Rozwiązanie wspiera technologię Link Aggregation.

POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA

59) Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
60) Urządzenie pozwala na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
61) Konfiguracja serwera DHCP jest niezależna dla protokołu IPv4 i IPv6.
62) Urządzenie posiada określenia różnych bram, a także serwerów DNS
63) Urządzenie jest wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
64) Urządzenie posiada usługę DNS Proxy.

ADMINISTRACJA URZĄDZENIEM

65) Producent dostarcza w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.

66) Konfiguracja urządzenia jest możliwa z wykorzystaniem polskiego interfejsu graficznego.
67) Interfejs konfiguracyjny jest dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
68) Komunikacja może odbywać się na porcie innym niż https (443 TCP).
69) Urządzenie jest zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
70) Urządzenie daje możliwość eksportowania logów na zewnętrzny serwer (syslog).
71) Urządzenie pozwala na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
72) Urządzenie pozwala na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

RAPORTOWANIE

73) Urządzenie posiada wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
74) System raportowania i przeglądania logów wbudowany w system nie wymaga licencji do swojego działania.
75) System raportowania posiada predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
76) System raportujący umożliwia wygenerowanie co najmniej 25 różnych raportów.
77) System raportujący daje możliwość edycji konfiguracji z poziomu raportu.
78) W ramach podstawowej licencji zamawiający otrzymuje możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
79) Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy

PARAMETRY SPRZĘTOWE

80) Urządzenie jest wyposażone w dysk twardy o pojemności co najmniej 320 GB.
81) Liczba portów Ethernet 10/100/1000 – min. 12.
82) Urządzenie posiada funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G.
83) Przepustowość Firewalla – min. 5 Gbps
84) Przepustowość Firewalla wraz z włączonym systemem IPS – min. 3 Gbps.
85) Przepustowość filtrowania Antywirusowego – min. 850 Mbps
86) Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1 Gbps.
87) Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 500.
88) Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100
89) Obsługa min. 280 VLAN
90) Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 20 000 nowych sesji/sekundę.
91) Urządzenie daje możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
92) Urządzenie jest nielimitowane na użytkowników.

SERWIS I LICENCJONOWANIE

93) Premium UTM Security Pack na okres minimum 36 miesięcy
94) Next Business Day (wymiana urządzenia w przypadku awarii na następny dzień roboczy) na okres minimum 36 miesięcy
95) Pełne wsparcie i pomoc przy konfiguracji urządzenia w formie telefonicznej i połączenia zdalnego

3. Termin realizacji zamówienia i miejsce dostawy:

a) Termin realizacji zamówienia 14 dni od daty podpisania umowy dostawy.
b) Miejsce dostawy: sprzęt musi być dostarczony do siedziby Urzędu Miejskiego w Koluszkach, ul. 11 Listopada 65, na koszt Sprzedającego.

4. Opis kryteriów oceny oferty:

a) Cena oferty - 100 %
b) Wybrana zostanie oferta z najniższą ceną, która spełnia wszystkie wymagania zawarte w niniejszym zapytaniu.

5. **Opis sposobu przygotowania oferty:**
   a) Termin składania ofert do dnia 09.01.2018 r., godzina 12:00.
   b) Oferta powinna być sporządzona czytelnie w języku polskim. Wszystkie strony oferty powinny być spięte i podpisane przez osobę uprawnioną do występowania w imieniu Oferenta.
   c) Cena oferty powinna być wyrażona w walucie polskiej.
   d) Koperta powinna być zaadresowana do zamawiającego na adres:
   Urząd Miejski w Koluszkach
   ul. 11 Listopada 65
   95-040 Koluszki
   oraz opatrzona napisem: „Oferta na dostawę sprzętu informatycznego. Nie otwierać przed dniem 09.01.2018 r. do godz. 12:00"

6. **Oferta powinna zawierać następujące dokumenty :**
   a) Wypełniony formularz ofertowy,
   b) Aktualny wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej lub aktualny wpis do Krajowego Rejestru Sądowego.
   c) W/w dokumenty powinny być czytelnie podpisane przez osobę upoważnioną do występowania w imieniu Wykonawcy.

7. **Płatność:**
   a) Należność zostanie uregulowana ze środków budżetowych Gminy Koluszki.
   b) Należność będzie uregulowana przelewem w terminie do 21 dni od daty dostawy i otrzymania prawidłowo wypełnionej faktury VAT.
   c) Zakup sfinansowany zostanie z środków Gminy Koluszki dział 750, rozdział 75023 § 6050

8. **Postanowienia końcowe.**
   Do niniejszego zapytania ofertowego nie mają zastosowania przepisy Ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych (Dz. U. z 2017 poz. 1579 ze zmianami).

9. **Do kontaktów z oferentami upoważniony jest:**
   a) Pan Dariusz Sobieszek
   stanowisko ds. informatyki i bezpieczeństwa sieci komputerowej
   tel. 44 725-67-15,
   e-mail: it@koluszki.pl
   b) Informacje udzielane są w godzinach pracy Urzędu Miejskiego w Koluszkach.

10. **Załączniki do zaproszenia:**
   a) Załącznik nr 1 - Formularz ofertowy
   b) Załącznik nr 2 - Projekt umowy dostawy

Zatwierdził:
BURMISTRZ
mgr Waldemar Chałat

SEKRETARZ GMINY
mgr Beata Kusiak-Stanisławska

INFORMATYK
mgr inż. Dariusz Sobieszek

INSPEKTOR d/s zamówień publicznych
mgr Marek Gorowiński

Urząd Miejski w Koluszkach
ul. 11 Listopada 65
95-040 Koluszki
um@koluszki.pl
www.koluszki.pl
tel.: 44 725 67 00, 10
fax: 44 714 58 15
NIP- 728 - 24 - 71 - 753
REGON - 590648362

Załącznik nr 1

Zamawiający: Gmina Koluszki
ul. 11 Listopada 65
95-040 Koluszki

Wykonawca :
.....
.....
.....
.....
(nazwa, adres, tel/fax)

Formularz ofertowy

Przedmiot postępowania: dostawa sprzętu informatycznego (UTM) dla Gminy Koluszki.

Lp.	Wyszczególnienie asortymentu	J.m	Ilość	Wartość netto (zł)	Wartość brutto (zł)
1.	UTM STORMSHIELD SN510 wraz z odpowiednim serwisem i licencjami opisanymi w zaproszeniu ofertowym	szt.	1		

Ogółem cena brutto: ..... zł

słownie:.....

Oświadczamy, że zapoznaliśmy się z zaproszeniem do złożenia oferty i innymi dokumentami postępowania, i nie wnosimy do nich zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty.

....., dnia.....

.....
czytelny podpis osoby upoważnionej do występowania w imieniu Wykonawcy

Załącznik nr 2

UMOWA Nr .....
zawarta w Koluszkach dnia ..... r.

pomiędzy: ....., NIP .....,
reprezentowanym przez .....
zwanym w dalszej części umowy „Dostawcą",
a
GMINĄ KOLUSZKI z siedzibą w Koluszkach przy ul. 11 LISTOPADA 65, NIP 7282471753,
reprezentowaną przez:
Burmistrza Koluszek - Waldemara Chałata
przy kontrasygnacie Skarbnika Gminy - Bogusławy Kubicz
zwaną w dalszej części umowy „Zamawiającym".

Umowę zawiera się na podstawie art. 4 pkt 8 Ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych (tekst jednolity Dz. U. z 2017 poz. 1579 ze zmianami).

§ 1

Przedmiot umowy:

1. Dostawa UTM STORMSHIELD SN510 sztuk 1 - specyfikacja zgodnie z ogłoszeniem ofertowym na dostawę sprzętu komputerowego z dnia ..... r.

§ 2

1. Wartość umowy brutto: ..... PLN,
   słownie: .....
   Wartość umowy netto: ..... PLN,
   słownie: .....
2. Nie dopuszcza się możliwości waloryzacji ceny ofertowej.
3. Należność zostanie sfinansowana ze środków budżetowych Gminy Koluszki zabezpieczonych na 2018 rok:
   - dział ..... rozdział ..... § .....

§ 3

Termin dostawy nie później niż 14 dni od daty podpisania umowy dostawy.

§ 4

Warunki dostawy:

1. Miejsce dostawy: siedziba Urzędu Miejskiego w Koluszkach przy ul. 11 Listopada 65.
2. Miejsce dostawy jest jednocześnie miejscem spełnienia świadczenia.
3. Transport na koszt i zlecenie Dostawcy.

§ 5

1. Płatność: przelewem w terminie do 21 dni od daty otrzymania towaru, czego potwierdzeniem będzie protokół odbioru i złożenie prawidłowo wypełnionej faktury VAT.
2. Wynagrodzenie wypłacone będzie Dostawcy przelewem na rachunek bankowy wskazany na wystawionej fakturze VAT.

§ 6

1) Długość udzielonej gwarancji: 36 miesięcy - Next Business Day, 36 – miesięcy Premium UTM Security Pack

§ 7

Reklamacje:

1. W przypadku stwierdzenia niezgodności dostawy pod względem jakości, ilości lub przedmiotowości, Zamawiający wstrzyma zapłatę reklamowanych pozycji.
2. W razie stwierdzenia wad Zamawiający złoży stosowną reklamację Dostawcy, który udzieli odpowiedzi na nią w terminie 3 dni, a po bezskutecznym upływie tego terminu reklamacja uważana będzie za uznaną w całości zgodnie z żądaniem Zamawiającego.
3. Sposoby załatwiania reklamacji:
   - wymiana wadliwego lub uszkodzonego towaru
   - dostarczenie brakujących materiałów.
4. Wszelkie koszty związane z reklamacją ponosi Dostawca.

§ 8

1. Za nieterminowe wykonanie umowy Dostawca zapłaci Zamawiającemu kary umowne w wysokości 0,5 % wartości netto od niezrealizowanej umowy licząc za każdy dzień zwłoki jednak nie więcej niż 20 % wartości netto podpisanej umowy.
2. Zamawiający może na zasadach ogólnych dochodzić odszkodowania przewyższającego karę umowną zastrzeżoną w pkt 1 niniejszego paragrafu.
3. Dostawca wyraża zgodę na potrącenie kar umownych z wystawionych faktur.

§ 9

1. Wszelkie sprawy sporne wynikłe z realizacji niniejszej umowy rozpatrywane będą przez właściwy sąd powszechny właściwy dla siedziby Zamawiającego.
2. Sprawy nieuregulowane niniejszą umową rozpatrywane będą zgodnie z Kodeksem cywilnym.

§ 10

Każda zmiana treści umowy powinna być dokonana pisemnie w formie aneksu do umowy, pod rygorem nieważności.

§ 11

Umowę sporządzono w trzech jednobrzmiących egzemplarzach. Jeden egzemplarz dla Dostawcy i dwa egzemplarze dla Zamawiającego.

Zamawiający : Dostawca:

kontrasygnata Skarbnika Gminy