

WÓJT GMINY
Wieczfnia Kościelna
.....woj. mazowieckie.....

ZIP" 26.11.2016
SEKRETARZ GMINY
inż. Krzysztof Kowalczyk

Wieczfnia Kościelna, dnia 24 listopada 2016 roku

(pieczęćka zamawiającego)

ZAPYTANIE OFERTOWE

1. Zamawiający: **Gmina Wieczfnia Kościelna, 06-513 Wieczfnia Kościelna.**

Zaprasza do złożenia oferty na:

2. Przedmiot zamówienia: **Dostawa urządzenia UTM dla Gminy Wieczfnia Kościelna.**
3. Wymagania dotyczące urządzenia:

Urządzenie klasy UTM według wymagań Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa obsługujących Urząd Gminy Wieczfnia Kościelna, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

- 1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
- 2) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączu sieciowych.
- 3) Monitoring stanu realizowanych połączeń VPN.
- 4) System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
- 5) System realizujący funkcję Firewall powinien dysponować minimum 7 portami Ethernet 10/100/1000 Base-TX
- 6) System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- 7) W zakresie Firewall'a obsługa nie mniej niż 1,5 mln. jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę
- 8) Przepustowość Firewall'a: nie mniej niż 2 Gbps
- 9) Wydajność szyfrowania VPN IPSec: nie mniej niż 180 Mbps
- 10) System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony

komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.

- 11) System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
- 12) W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
 - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
 - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
 - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
 - Ochrona przed atakami - Intrusion Prevention System
 - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
 - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
 - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
 - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
 - Możliwość analizy ruchu szyfrowanego protokołem SSL
 - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
 - Możliwość późniejszego zastosowania dwu-składnikowego uwierzytelniania z wykorzystaniem tokenów sprzętowych lub programowych.
- 13) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 700 Mbps
- 14) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 160 Mbps
- 15) W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
 - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
 - Praca w topologii Hub and Spoke oraz Mesh
 - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF

- Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
- 16) W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
 - 17) Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
 - 18) Translacja adresów NAT adresu źródłowego i docelowego.
 - 19) Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
 - 20) Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
 - 21) Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
 - 22) Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
 - 23) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
 - 24) Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
 - 25) Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
 - 26) System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
 - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
 - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
 - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

27) Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall
- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPsec VPN

28) Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

29) Serwisy i licencje

- W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 1 rok.

30) Gwarancja oraz wsparcie

a) Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczypospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej.

b) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

c) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

4. Instalacja i wdrożenie urządzenia w siedzibie zamawiającego.

5. Termin wykonania zamówienia: **do 20 grudnia 2016 roku.**

6. Termin płatności: **14 dni po wykonaniu zamówienia i dostarczeniu faktury VAT do siedziby zamawiającego.**

7. Warunki gwarancji: **12 miesięcy,**

8. Miejsce i termin złożenia oferty: **Urząd Gminy Wieczfnia Kościelna 48, 06-513 Wieczfnia Kościelna, w terminie do dnia 01 grudnia 2016 roku, (treść oferty stanowi załącznik Nr 1).**

W O J T
mgr J. Wójcik
.....
(podpis osoby upoważnionej)

TREŚĆ OFERTY

Nazwa wykonawcy

.....

Adres/siedziba wykonawcy

.....

NIP

REGON

Nr rachunku bankowego

.....

Oferuję wykonanie przedmiotu zamówienia

zamawiający wpisuje nazwę zamówienia

za:

Cenę netto zł

Podatek VAT zł

Cenę brutto zł

Oferuję wykonanie zamówienia na następujących warunkach:

- termin wykonania zamówienia.....

- parametry techniczne

.....

.....

- termin płatności

- warunki gwarancji

- inne warunki realizacji zamówienia

Oświadczam, że zapoznałam się z opisem przedmiotu zamówienia i zobowiązuje się go wykonać na wyżej wskazanych warunkach.

Oświadczam, że dysponuję potencjałem technicznym i osobami zdolnymi do wykonania zamówienia:

data

.....
podpis i pieczęć wykonawcy lub osoby upoważnionej