MIASTO ŁOWICZ
99-400 Łowicz
Pl. Stary Rynek 1
REGON 750148621, NIP 834-188-25-02

Łowicz, dnia 05 marca 2018 r.

ZAPYTANIE OFERTOWE

I. Znak Sprawy: I.271.4.6.2018.DF

II. Zamawiający
Gmina Miasto Łowicz
Stary Rynek 1
99-400 Łowicz
NIP 834-18-82-502
REGON 750148621

III. Tryb udzielania zamówienia publicznego
Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie zapytania ofertowego na podstawie art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. 2017, poz. 1579 z późn. zm.), zgodnie z Zarządzeniem nr 255a/14 Burmistrza Miasta Łowicza z dnia 8 lipca 2014 r. w sprawie regulaminu udzielania zamówień publicznych o wartości poniżej 30.000 euro, zmienionego Zarządzeniem Nr 237/16 Burmistrza Miasta Łowicza z dnia 12 lipca 2016 r. w sprawie regulaminu udzielenia zamówień publicznych o wartości poniżej 30.000 euro.
Zamówienie powyżej 50 tys. PLN netto udzielone jest zgodnie z zasadą konkurencyjności, wysłane jest do potencjalnych Oferentów w celu wyboru najkorzystniejszej oferty oraz jest również dostępne na stronie internetowej Zamawiającego http://www.lowicz.eu/bip/

Informacje ogólne

Zamawiający:
Urząd Miejski w Łowiczu
Pl. Stary Rynek 1
99-400 Łowicz
telefon: 46 830 91 51-52
internet: http://www.lowicz.eu/bip/

Adres do korespondencji:
Urząd Miejski w Łowiczu
Pl. Stary Rynek 1
99-400 Łowicz
telefon: (46) 830 91 23 (osoby wyznaczone do kontaktu)

Data publikacji: 2018-03-05

Termin składania oferty: 2018-03-26

Opis przedmiotu zamówienia publicznego

Nazwa zamówienia:

Zapytanie ofertowe na **dostawę, instalację, uruchomienie i konfigurację sieciowego urządzenia zabezpieczającego UTM**

Rodzaj i przedmiot zamówienia zgodnie ze Wspólnym Słownikiem Zamówień CPV

Główny CPV
32420000-3 Urządzenia sieciowe
Dodatkowe kody CPV
48000000-8 Pakiety oprogramowania i systemy informatyczne.
80511000-9 Usługi szkolenia personelu

Opis przedmiotu zamówienia

Wymagania Ogólne

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.
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.
Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
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. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Dostarczone urządzenie musi być fabrycznie nowe, wyprodukowane nie później niż pół roku od daty złożenia ofert, nie być wycofane z produkcji lub sprzedaży przez producenta.
Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.

Redundancja, monitoring i wykrywanie awarii

1. 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.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 8 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 32 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 14 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 20 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 11 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4.7 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 6.8 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:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. 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.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - 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.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.

· Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. 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.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. 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 avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - 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.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. 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.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi 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, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów w przestrzeni o pojemności co najmniej 200 GB.
3. W ramach logowania system 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.
4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
5. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

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 IPSec VPN.
- ICSA dla funkcji SSL VPN.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy.
b) Logowanie do usługi realizowanej w chmurze na okres 12 miesięcy.
c) Kontrola Sandbox realizowana w chmurze na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 8x5.

Opis usługi

1. Inwentaryzacja sieci miejskiej oraz zaprojektowanie wdrożenia rozwiązania
2. Wstępna konfiguracja urządzenia (upgrade firmware, tworzenie obiektów adresowych, tworzenie obiektów serwisowych, konfiguracja filtrowania stron Internetowych, AV, AntySpam, IPS/IDS). Urządzenie musi posiadać najnowszy rekomendowany system operacyjny wolny od podatności kategorii wysokiej, potwierdzony raportem skanera podatności.
3. Dostosowanie protokołu routingu do wewnętrznej infrastruktury.
4. Zintegrowanie komputerów podłączonych do domeny UM Łowicz za pomocą protokołu LDAP z nową zaporą sieciową.
5. Zestawienie tuneli do usługodawców zewnętrznych oraz tuneli serwisowych.
6. Przepięcie urządzenia – eliminacja starego rozwiązania Cisco ASA.
7. Docelowa konfiguracja urządzenia - filtrowanie stron Internetowych bazując na grupach użytkowników. Konfiguracja polityk kontroli dostępu, tasowania, polityk antyspamowych, polityk IDS/ IPS. Redystrybucja certyfikatów służących do rozszywania sesji SSL na wszystkie wyznaczone przez UM komputery.
8. Wyeliminowanie wszystkich problemów podczas pierwszych trzech dni od momentu przełączenia urządzeń.
9. Doubezpieczenie urządzenia- hardening. Logowanie do urządzenia musi być skonfigurowane z konkretnych urządzeń w sieci. Utworzenie niestandardowych profili administracyjnych, zarówno dla osób odpowiedzialnych za IT oraz serwisantów. Zintegrowanie UTM z usługami chmurowymi.
10. Weryfikacja poprawności działania polityk oraz profili NGF
11. Utworzenie powykonawczej dokumentacji technicznej
12. Jednodniowe szkolenie techniczne z zakresu działania UTM (min. 7 godz.).

Wszystkie prace powodujące przerwy w łączności z internetem muszą odbywać się poza godzinami pracy Urzędu Miejskiego w Łowiczu.

Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny ich spełniania

1) Z możliwości składania ofert wyklucza się Oferentów, którzy:
   Są podmiotem powiązanym z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:
   a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
   b) posiadaniu co najmniej 10 % udziałów lub akcji,
   c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
   d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.
2) Zamawiający zastrzega możliwość sprawdzenia informacji zawartych w dokumentach.
3) Dokumenty wymagane od wykonawcy
   a) formularz ofertowy – zał. 1,
   b) zestawienie parametrów technicznych – zał. 2
   c) dokument stwierdzający prawo osoby (osób) podpisującej ofertę do reprezentowania wykonawcy w postępowaniu o uzyskanie przedmiotowego zamówienia publicznego, w szczególności aktualny odpis z Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, pełnomocnictwo,
   d) na żądanie Zamawiającego, Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu zamieszcza informacje o podwykonawcach w oświadczeniach.

Kryteria oceny oferty
Informacja o wagach punktowych lub procentowych przypisanych do poszczególnych kryteriów oceny oferty

Zamawiający oceni i porówna jedynie te oferty, które nie zostaną odrzucone przez Zamawiającego. Oferty zostaną ocenione przez Zamawiającego w oparciu o następujące kryteria i ich znaczenie:

Kryterium	Znaczenie procentowe kryterium	Maksymalna liczba punktów, jakie może otrzymać oferta za dane kryterium
Cena brutto	100 %	100 pkt

Termin składania ofert
Sposób przygotowania i złożenia oferty

1. Ofertę należy sporządzić w języku polskim.

BURMISTRZ
Kaliński
Krzysztof Jan Kaliński

2. Oferta musi zawierać:
   - Wypełniony formularz ofertowy wraz z oświadczeniem o braku powiązań kapitałowych i osobowych z Zamawiającym zgodny ze wzorem określonym w **Załączniku nr 1** do zapytania ofertowego;
   - zestawienie parametrów technicznych zgodny ze wzorem określonym w **Załączniku nr 2**
   - dokument stwierdzający prawo osoby (osób) podpisującej ofertę do reprezentowania wykonawcy w postępowaniu o uzyskanie przedmiotowego zamówienia publicznego, w szczególności aktualny odpis z Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, pełnomocnictwo,
3. Podpisaną ofertę wraz z ww. załącznikami **(od 1 - do 2)** należy dostarczyć do siedziby Zamawiającego osobiście lub listem poleconym/kurierem do dnia **26.03.2018 r. do godziny 10:00**. Decyduje data faktycznego wpływu oferty do Zamawiającego (nie np. data nadania, data stempla pocztowego). Oferty, które wpłyną po terminie zostaną odrzucone. Opis na kopercie z ofertą:
   Oferta na dostawę, instalację, uruchomienie i konfigurację sieciowego urządzenia zabezpieczającego UTM dla Urzędu Miejskiego w Łowiczu.
4. Oferty niekompletne lub niezgodne z warunkami udziału w postępowaniu, będą odrzucone.
5. Pytania do niniejszego zapytania należy kierować na adres e-mail: dariusz.fabijanski@um.lowicz.pl

Postanowienia dodatkowe i końcowe

1. Zamawiający zapłaci za faktycznie wykonaną usługę na podstawie faktury wystawionej przez Wykonawcę.
2. Zapłata zostanie dokonana w terminie do 14 dni po otrzymaniu poprawnie wystawionej faktury.
3. Wykonawca ponosi wszelkie koszty własne związane z przygotowaniem i złożeniem oferty, niezależnie od wyniku postępowania. Zamawiający nie odpowiada za koszty poniesione przez Wykonawcę w związku z przygotowaniem i złożeniem oferty.
4. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert.
5. Termin związania ofertą: 30 dni kalendarzowych.
6. Złożenie oferty jest jednoznaczne z zaakceptowaniem powyższych zasad.

W załączeniu:
1. Załącznik nr 1 - formularz ofertowy
2. Załącznik nr 2 - zestawienie parametrów technicznych
3. Załącznik nr 3 - wzór umowy

Sporządził:

Dariusz Fabijański

Zatwierdzam:
BURMISTRZ
Krzysztof Jan Kaliński
Krzysztof Jan Kaliński