UMOWA

W dniu ..... w Lublinie pomiędzy:
Gminą Lublin, z siedzibą w Lublinie, Plac Władysława Łokietka 1,
reprezentowaną przez
.....
zwaną dalej „Zamawiającym”
a
.....,
z siedzibą w .....,
wpisanym do ..... pod numerem .....,
reprezentowanym przez .....,
zwanym dalej
„Wykonawcą”,
w wyniku przeprowadzenia przez Zamawiającego przetargu nieograniczonego, w którym oferta Wykonawcy uznana
została za najkorzystniejszą, zawarta została umowa o następującej treści.

§ 1

1. Przedmiotem umowy jest dostawa, montaż i uruchomienie zintegrowanego urządzenia bezpieczeństwa sieciowego (lub zespołu takich urządzeń) zapewniającego ochronę sieci w czasie rzeczywistym w zakresie i według wymagań określonych w załączniku nr 1 do niniejszej umowy - Szczegółowe wymagania, warunki techniczne i zakres rzeczowy zamówienia.
2. Materiały i urządzenia użyte do wykonania Zadania powinny odpowiadać co do jakości wymogom wyrobów dopuszczonych do obrotu i stosowania oraz wymaganiom zawartym w załączniku nr 1 do umowy.
3. Na każde żądanie Zamawiającego Wykonawca zobowiązany jest okazać w stosunku do wskazanych materiałów i urządzeń aprobatę techniczną, atest, certyfikat, świadectwo zgodności (homologacji), specyfikację techniczną,itp.
4. Wykonawca ponosi odpowiedzialność za dołączone do systemu identyfikatory i dokumenty określające producenta, legalność, jakość wykonania, standard, zgodność z polskimi i międzynarodowymi normami oraz innymi wymaganymi prawem regulacjami.

§ 2

1. Wykonawca wykona zadanie w terminie 30 dni od daty podpisania umowy.
2. Wykonawca ma prawo zwrócić się do Zamawiającego o przedłużenie terminu umownego, jeżeli jego niedotrzymanie wynika z okoliczności, których nie można było przewidzieć.

3. Okoliczności uzasadniające przedłużenie terminu wykonania umowy nie dają prawa do żądania zmiany wynagrodzenia określonego w § 6 ust. 1.
4. Wykonawca zobowiązany jest do natychmiastowego informowania Zamawiającego o przeszkodach w realizacji Zadania z winy Zamawiającego.

§ 3

Wykonawca zobowiązany jest do:
1. Wykonania schematu obejmującego sposób montażu urządzeń.
2. Wykonania Zadania zgodnie z przyjętym schematem.
3. Uzgodnienia warunków wejścia do obiektów, w których projektowany jest montaż urządzeń.
4. Dokonania komisyjnego przekazania zrealizowanego Zadania, a także przygotowania i przekazania Zamawiającemu trzech egzemplarzy dokumentacji powykonawczej, zawierające w szczególności schemat, określony w punkcie 1), protokoły z przeprowadzonych testów, wszystkie wymagane prawem lub niezbędne z innych przyczyn atesty, certyfikaty, licencje, świadectwa

jakości i homologacji, dokumenty gwarancyjne, specyfikacje technicznych sprzętu i urządzeń, instrukcje obsługi.
5. Przeprowadzenia przed odbiorem wymaganych właściwymi przepisami prób, badań, pomiarów, jak również uzyskania od właściwych organów odpowiednich zaświadczeń.
6. Niezwłocznego, pisemnego zgłoszenia gotowości do odbioru końcowego.
7. Usunięcia wad i niezgodności w terminie wyznaczonym przez Zamawiającego w przypadku stwierdzenia przy odbiorze Zadania, że prace wykonane zostały sprzecznie z umową lub wystąpiły wady.
8. Przeprowadzenia szkolenia dla 4 administratorów oferowanego systemu. Szkolenie odbędzie się w centrum szkoleniowym certyfikowanym przez producenta oferowanego rozwiązania i zostanie przeprowadzone przez osoby posiadające odpowiednie uprawnienia potwierdzone przez producenta oferowanego rozwiązania.

§ 4

1. Wykonawca obejmie przedmiot umowy 12-miesięczną gwarancją i w dniu odbioru przekaże Zamawiającemu dokument gwarancyjny.
2. Początkiem okresu gwarancyjnego jest data podpisania protokołu odbioru.
3. W ramach serwisu gwarancyjnego Wykonawca jest zobowiązany do:
a) dostarczenia subskrypcji na dostęp do aktualizacji baz danych wykorzystywanych przez usługi ochrony antywirusowej, kontroli zawartości (URL filtering), kontroli antyspamowej oraz ochrony przed atakami (Deep Inspection). Oferowane rozwiązanie musi umożliwiać rozszerzenie w/w subskrypcji na dłuższy okres czasu (np. poprzez odnowienie subskrypcji).,
b) przyjmowania zgłoszeń awarii przez całą dobę pod numerem telefonu, faxu .....
c) usunięcia w siedzibie Zamawiającego awarii każdego z elementów systemu i przyczyn jego niestabilnej pracy do końca pierwszego dnia roboczego następującego po dniu zgłoszenia awarii,
d) udzielenia w siedzibie Zamawiającego przez inżyniera wsparcia technicznego certyfikowanego przez producenta sprzętu 16 godzin konsultacji w zakresie sprzętu i oprogramowania,
e) udzielania drogą telefoniczną w godzinach pracy Urzędu przez upoważnionego przez Wykonawcę pracownika nielimitowanych konsultacji w zakresie sprzętu i oprogramowania pod numerem telefonu .....
f) bezpłatnego udostępnienia Zamawiającemu sprzętu zastępczego w przypadku niemożności usunięcia awarii
w siedzibie Zamawiającego.

§ 5

1. Wykonawca oświadcza, iż przedmiot zamówienia wykona siłami własnymi
lub
1. Wykonawca oświadcza, iż powierzy Podwykonawcom następujący zakres:
1) .....
2. Wykonawca zobowiązany jest zawrzeć z Podwykonawcą umowę, której zapisy nie będą naruszały postanowień niniejszej umowy.
3. Wykonawca jest odpowiedzialny za działania i zaniechania osób, z których pomocą wykonuje przedmiot umowy, w tym za jakość i terminowość prac, jak za własne działania.

§ 6

1. Za wykonanie przedmiotu umowy, zwanego dalej „Zadaniem” Wykonawcy będzie przysługiwać wynagrodzenie ryczałtowe określone w ofercie: netto ....., z należnym podatkiem VAT w wysokości ....., razem brutto ..... (słownie:..... złotych).
2. Podstawą wypłaty wynagrodzenia będzie faktura końcowa wystawiona w oparciu o protokół odbioru
końcowego.

3. Termin płatności faktury końcowej ustala się na 21 dni od daty jej otrzymania.
4. Zamawiający upoważnia do wystawiania faktur VAT bez swojego podpisu.

§ 7

1. Za opóźnienie w wykonaniu przedmiotu umowy Wykonawca zapłaci Zamawiającemu za każdy dzień opóźnienia karę umowną w wysokości 1% wynagrodzenia brutto określonego w § 6 ust. 1.
2. W przypadku odstąpienia przez Wykonawcę od umowy z przyczyn, za które ponosi on odpowiedzialność, zapłaci on Zamawiającemu karę umowną w wysokości 10 % wynagrodzenia brutto określonego w § 6 ust. 1.
3. W przypadku odstąpienia przez Zamawiającego od umowy z przyczyn, za które ponosi odpowiedzialność Wykonawca, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10 % wynagrodzenia brutto określonego w § 6 ust. 1.
4. W przypadku odstąpienia przez Zamawiającego od umowy z przyczyn, za które ponosi on odpowiedzialność z zastrzeżeniem § 8.ust. 1 zobowiązany jest on zapłacić Wykonawcy karę umowną w wysokości 10% wynagrodzenia brutto określonego w § 6 ust. 1.
5. Uchybienie przez Wykonawcę zobowiązaniom określonym w § 4 ust. 3 skutkuje naliczeniem przez Zamawiającego kary umownej w wysokości 500 zł za każdy dzień przekroczenia terminów w nim określonych.

§8

1. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
2. W przypadku odstąpienia od umowy, o którym mowa w ust. 1 Wykonawca ma prawo żądać jedynie wynagrodzenia należnego za prace wykonane do odstąpienia od umowy.

§ 9

1. Wykonawca wyznacza jako swojego przedstawiciela .....
2. Zamawiający wyznacza jako swojego przedstawiciela: Pan Andrzej Małecki, Główny Specjalista ds. Sieci w Wydziale Informatyki i Telekomunikacji.

§ 10

Strony mają prawo dochodzenia odszkodowania przewyższającego kary umowne na zasadach ogólnych.

§ 11

1. Zmiana postanowień zawartej umowy może nastąpić wyłącznie za zgodą obu stron wyrażoną w formie pisemnego aneksu pod rygorem nieważności.
2. Nie dopuszcza się zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, chyba że konieczność wprowadzenia takich zmian wynika z okoliczności, których nie można było przewidzieć w chwili zawarcia umowy, lub zmiany te są korzystne dla Zamawiającego.

§ 12

W sprawach nie uregulowanych w niniejszej umowie stosuje się przepisy obowiązującego prawa, w tym prawa
zamówień publicznych i kodeksu cywilnego.

§ 13

Ewentualne spory powstałe w związku z wykonywaniem przedmiotu umowy będą rozpatrywane

przez właściwe
rzeczowo sądy powszechne w Lublinie.

§ 14

Umowę sporządzono w czterech egzemplarzach, po dwa dla każdej strony.

ZAMAWIAJĄCY WYKONAWCA

zał. Nr 2 do SIWZ

FORMULARZ OFERTOWY	
PRZEDMIOT ZAMÓWIENIA	**Dostawa, montaż i uruchomienie zintegrowanego urządzenia bezpieczeństwa sieciowego (lub zespołu takich urządzeń) zapewniającego ochronę sieci w czasie rzeczywistym**
ZAMAWIAJĄCY	***Gmina Miasto Lublin***
NAZWA I ADRES WYKONAWCY	
Adres do korespondencji oraz telefon, fax i e-mail (o ile wykonawca takie posiada)	
CENA OFERTY NETTO (cyfrowo i słownie)	
Kwota podatku VAT (cyfrowo i słownie)	
CENA OFERTY BRUTTO (cyfrowo i słownie)	
Podpis (y)	

zał. Nr 3 do SIWZ

.....
wykonawca data

OŚWIADCZENIA

dotyczy przetargu nieograniczonego na dostawa, montaż i uruchomienie zintegrowanego urządzenia bezpieczeństwa sieciowego (lub zespołu takich urządzeń) zapewniającego ochronę sieci w czasie rzeczywistym

1. Oświadczenie o spełnieniu warunków udziału w postępowaniu.

Oświadczam, że spełniam warunki udziału w postępowaniu.

2. Oświadczenie o części zamówienia, której wykonanie, wykonawca zamierza powierzyć podwykonawcom.

Oświadczam, że: *
a) Całość zamówienia zostanie wykonana siłami własnymi wykonawcy
b) Część zamówienia będzie wykonywana przy pomocy Podwykonawców

1. .....

2. .....

3. .....

.....
podpis osoby/ osób upoważnionych do występowania w imieniu wykonawcy

* Niepotrzebne (a lub b) skreślić.

Załącznik nr 4 do SIWZ

Wykaz wykonanych w okresie ostatnich 3 lat przed dniem wszczęcia postępowania o udzielnie zamówienia a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 3 dostaw urządzeń sieciowych o wartości co najmniej 50 000 zł brutto każda

Lp.	Przedmiot	Data wykonania	Wartość realizowana przez wykonawcę	Odbiorca

.....
podpis osoby/ osób upoważnionych do
występowania w imieniu wykonawcy

Zał. Nr 5 do SIWZ
[Załącznik Nr 1 do umowy]

Szczegółowe wymagania, warunki techniczne i zakres rzeczowy zamówienia.

1. Urządzenie dostarczane jest jako dedykowane urządzenie sieciowe, przystosowane do montażu w szafie rack 19". Urządzenie musi być zasilane z sieci 230V prądu przemiennego.
2. Urządzenie musi być wyposażone w co najmniej cztery interfejsy Gigabit Ethernet 10/100/1000 TX (gotowe do użycia bez konieczności zakupu dodatkowych modułów i licencji). W urządzeniu musi istnieć możliwość uruchomienia co najmniej dziesięciu interfejsów sieciowych (dobieralnych spośród Fast Ethernet, Gigabit Ethernet, E1 i Serial).
3. Urządzenie musi obsługiwać protokoły dostępowe warstwy 2 OSI co najmniej: Frame Relay, Ethernet (z obsługą co najmniej 140 sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q) oraz Point-to-Point Protocol/High level Data Link Control (PPP/ Cisco HDLC).
4. Wraz z urządzeniem musi zostać dostarczony kabel RS-232 do podłączenia konsoli.
5. Urządzenie musi posiadać minimum 1 GB pamięci operacyjnej (DRAM).
6. System zabezpieczeń musi realizować zadania firewall, wykonując kontrolę na poziomie sieci oraz aplikacji w oparciu o technologię Deep Packet Inspection.
7. Aktualizacja bazy sygnatur ataków musi odbywać się automatycznie zgodnie z ustalonym harmonogramem (np. raz na dobę). Baza sygnatur ataków musi zawierać ponad 900 definicji.
8. Urządzenie zabezpieczeń musi posiadać wbudowany moduł filtrowania treści stron WWW wywoływanych przez użytkowników umożliwiający blokowanie adresów URL oraz adresów IP w oparciu o dostarczone przez producenta lub własne kategorie. Włączenie filtrowania treści stron WWW nie może wymagać dodatkowego serwera.
9. Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antywirusowej kontrolujący pocztę elektronicznej (SMTP, POP3, IMAP), FTP oraz HTTP z licencją na nieograniczoną liczbę użytkowników. Włączenie kontroli antywirusowej nie może wymagać dodatkowego serwera. Minimalna przepływność urządzenia przy włączonej funkcji ochrony antywirusowej musi wynosić 200 Mbps
10. Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist z licencją na nieograniczoną liczbę użytkowników. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera.
11. System zabezpieczeń musi wykrywać i blokować ataki intruzów (in-line IDS), posiadać mechanizmy zarządzania pasmem sieci (QoS) oraz zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site.
12. Wraz z urządzeniem musi być dostarczone dedykowane (tzn. pochodzące od producenta urządzenia) oprogramowanie typu client VPN pracujące w systemach operacyjnych: Windows XP, Vista (oraz licencje na to oprogramowanie jeżeli są wymagane w minimalnej ilości 20 sztuk).
13. Urządzenia zabezpieczeń muszą być sterowane przez opracowany przez producenta zabezpieczeń dedykowany system operacyjny czasu rzeczywistego (tzn. nie może być to zmodyfikowany system operacyjny ogólnego przeznaczenia jak Linux, czy FreeBSD).
14. Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż 1 Gbps dla firewall, nie mniej niż 500 Mbps dla VPN (3DES) i musi obsługiwać nie mniej niż 120,000 jednoczesnych połączeń.
15. System zabezpieczeń musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI) oraz w trybie transparentnym (tzn. w warstwie 2 modelu OSI). Funkcjonując w trybie transparentnym urządzenie nie posiada skonfigurowanych adresów IP na interfejsach sieciowych. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji.
16. Sieci VPN tworzone przez system zabezpieczeń muszą działać poprawnie w środowiskach sieciowych, gdzie na drodze VPN wykonywana jest translacja adresów NAT. System zabezpieczeń musi posiadać zaimplementowany mechanizm IPSec NAT Traversal dla konfiguracji VPN client-tosite oraz site-to-site i umożliwiać logowanie z wykorzystaniem certyfikatów, LDAP, RADIUS, user list.
17. Sieci VPN site-to-site muszą potrafić działać w konfiguracjach Meshed VPN oraz Hub&Spoke. System zabezpieczeń musi posiadać zaimplementowane mechanizmy monitorowania stanu tuneli VPN i stałego utrzymywania ich aktywności (tzn. po wykryciu nieaktywności tunelu automatycznie musi następować negocjacja IKE).
18. Konfiguracja VPN musi odbywać się w oparciu o reguły polityki bezpieczeństwa (Policy-based VPN) oraz ustawienia rutingu (Routing-based VPN).
19. W jednym urządzeniu musi istnieć możliwość definiowania wirtualnych ruterów, gdzie każdy z nich posiada swoje indywidualne tabele rutingu. Urządzenie musi obsługiwać ruting statyczny oraz protokoły dynamicznego rutingu jak OSPF i BGP. Urządzenie zabezpieczeń musi wykonywać ruting IP na bazie adresu miejsca przeznaczenia pakietów oraz adresu źródłowego (tzw. source-based routing).
20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i

maksymalne, priorytety, oznaczenia DiffServ).
21. System zabezpieczeń musi wykrywać i blokować techniki i ataki stosowane przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan), blokować adresy URL i niebezpieczne komponenty (m.in. Java/ActiveX/zip/exe), chronić sieci VPN przed atakami powtórzeniowymi (Replay Attack) oraz limitować maksymalną liczbę otwartych sesji z jednego adresu IP.
22. Zarządzanie mechanizmami zabezpieczeń w pełnym zakresie musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (tzn. wykonywane musi być szyfrowanie komunikacji). System zabezpieczeń musi udostępniać możliwość zdefiniowania wielu kont administratorów o różnych poziomach uprawnień. Administratorzy muszą być uwierzytelniani za pomocą haseł statycznych, haseł dynamicznych (RADIUS, RSA SecureID) oraz certyfikatów cyfrowych SSL.
23. Całość konfiguracji systemu operacyjnego (m.in. adresacja i ruting IP) i zabezpieczeń (m.in. obiekty, polityka bezpieczeństwa firewall i VPN) musi odbywać się z jednej, centralnej konsoli zarządzania GUI.
24. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą haseł statycznych i dynamicznych. Użytkownicy mogą być definiowani w bazie lokalnej (tzn. bazie utrzymywanej na urządzeniu) oraz na zewnętrznych serwerach LDAP, RADIUS lub SecurID (ACE/Server).
25. System zabezpieczeń musi współpracować z wiodącymi urzędami certyfikacji (m.in. Verisign, Entrust, Microsoft) i wspierać standardy PKI (PKCS 7, PKCS 10) oraz protokoły SCEP i OCSP.
26. System zabezpieczeń musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą realizować m.in. dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. Udostępnianie w Internecie usług wielu serwerów musi odbywać się z użyciem tylko jednego publicznego adresu IP.
27. System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Urządzenia zabezpieczeń w klastrze muszą mieć możliwość funkcjonowania w trybie Active-Active.
28. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.
29. Oferowane rozwiązanie musi zapewniać pełną redundancję sprzętową, tzn. musi składać się z 2 urządzeń zawierających identyczne wyposażenie sprzętowe, zgodne z wymaganiami Zamawiającego. W każdym urządzeniu musi być zainstalowany i uruchomiony odpowiedni system operacyjny.
30. Wymagane jest przeprowadzenie szkolenia dla 4 administratorów oferowanego systemu. Szkolenie musi odbywać się w centrum szkoleniowym certyfikowanym przez producenta oferowanego rozwiązania i musi być prowadzone przez osoby posiadające odpowiednie uprawnienia potwierdzone przez producenta oferowanego rozwiązania.
W przypadku prowadzenia szkolenia poza siedzibą Zamawiającego (miasto Lublin) Wykonawca musi uwzględnić w ofercie koszty utrzymania uczestników szkolenia (zakwaterowania i wyżywienia przez czas trwania szkolenia).Czas trwania szkolenia nie może być krótszy niż 2 dni.
31. Wykonawca musi:
1.Dostarczyć, zainstalować, skonfigurować i uruchomić kompletny system w serwerowni Plac Władysława Łokietka 1 w Lublinie.
2.Wykonać dokumentację techniczną dostarczonego systemu i dołączyć ją do protokołu odbioru.
3.Wykonać pomiary wydajności zainstalowanego systemu i dołączyć je do protokołu odbioru.
4.Dostarczyć wraz protokołem odbioru instrukcje obsługi na CD oraz wymagane licencje, dokumenty stwierdzające udział osób wskazanych przez Zamawiającego w szkoleniu.
32. Odbiór systemu nastąpi po:
1.Stwierdzeniu zgodności konfiguracji sprzętowej z zamówieniem.
2.Stwierdzeniu poprawności funkcjonowania systemu.
3. Zatwierdzeniu protokołu odbioru przez Zamawiającego.