**Specyfikacja Istotnych Warunków Zamówienia**

**- przetarg nieograniczony –**

o wartości szacunkowej zamówienia mniejszej niż wyrażona w złotych
równowartości kwoty określonej dla dostaw i usług w przepisach wydanych na podstawie
art. 11 ust. 8 pzp

**na dostawę, instalację, wdrożenie wraz ze wsparciem technicznym platformy sprzętowej firewall z pełnym zdalnym zarządzaniem oraz szkoleniem z zakresu zarządzania
w ramach dostarczonego rozwiązania**

Kody CPV:

 **32420000-3 – Urządzenia sieciowe**

 **48200000-0 - Pakiety oprogramowania dla sieci, internetu i intranetu**

 **72265000-0 - Usługi konfiguracji oprogramowania**

 **80510000-2 - Usługi szkolenia specjalistycznego**

###

### Nr sprawy: PS.ZZZP.343-26(1)/13

## Gdańsk – lipiec 2013 r.

# ZAMAWIAJĄCY

**Miejski Ośrodek Pomocy Rodzinie w Gdańsku,** 80-432 Gdańsk, ul. Konrada Leczkowa 1A. NIP 583 20 94 853, REGON 002837021, tel. (058) 342-31-50; faks (058) 342-31-51, [www.mopr.gda.pl](http://www.mopr.gda.pl) .

# TRYB UDZIELENIA ZAMÓWIENIA

Postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie przepisów ustawy z dnia 29 stycznia 2004 r.- Prawo zamówień publicznych
(t.j. Dz. U. z 2010 r. Nr 113 poz. 759 z późn. zm.).

# OPIS PRZEDMIOTU ZAMÓWIENIA

1. **INFORMACJE OGÓLNE**
2. Przedmiotem zamówienia jest:
* Dostawa, instalacja, konfiguracja i uruchomienie platformy sprzętowej firewall
z pełnym zdalnym zarządzaniem, serwerem VPN oraz pozostałymi serwisami
z jednej graficznej konsoli administracyjnej pracującej pod systemami MS Windows.
* Serwis platformy sprzętowej i aktualizacja licencji w ciągu 48 miesięcy w trybie SLA 24x7.
* Szkolenie pracowników z zakresu administracji, konfiguracji urządzeń zawartych w platformie.
1. Oferowany sprzęt musi być fabrycznie nowy, tj. nieużywany przed dniem dostawy.
2. Wykonawca zobowiązuje się do instalacji i konfiguracji 4 urządzeń wskazanych przez Zamawiającego.
3. Wykonawca zobowiązuje się do wymiany urządzeń po 4 latach od momentu uruchomienia usługi.
4. Dostawa musi być realizowana na koszt Wykonawcy. Miejscem realizacji przedmiotu Zamówienia jest siedziba Zamawiającego w Gdańsku ul. Leczkowa 1A wraz
z jednostkami organizacyjnymi, zgodnie z tabelą:

|  |  |
| --- | --- |
| Lp. | lokalizacja |
| 1 | Oddział ul. Dyrekcyjna 5 |
| 2 | Oddział ul. Elbląska 66 |
| 3 | Oddział ul. Plac Ks. Prałata Jana Gustkowicza 13 |
| 4 | Oddział ul. Lecha 1 |
| 5 | Oddział ul. Marynarki Polskiej 134A |
| 6 | Oddział ul. Modrzewskiego 2A |
| 7 | Oddział ul. Powstańców Warszawskich 25 |
| 8 | Oddział ul. Spadzista 5 |
| 9 | Oddział ul. Sternicza 2 |
| 10 | Oddział ul. Wolności 16A |

1. Wymaga się aby dostawy sprzętu realizowane były jedynie w obecności przedstawiciela Wykonawcy, który odpowiada za stan dostawy i potwierdzi jej kompletność.
2. Termin realizacji: Realizacji zamówienia w terminie 30 dni od daty zawarcia umowy.
3. Płatność za sprzęt, wdrożenie oraz szkolenie nastąpi 21 dni po wykonaniu przedmiotu zamówienia i wystawieniu faktury. Natomiast płatność za 4 lata asysty technicznej nastąpi do 16 stycznia 2014 r.
4. **INFORMACJE TECHNICZNE OGÓLNE**
5. Rozwiązanie musi być dostępne jako platforma sprzętowa jak i maszyna wirtualna kompatybilna z rozwiązaniem VMware vSphere oraz Citrix XenServer.
6. Rozwiązanie ma umożliwiać scentralizowane zarządzanie wieloma różnymi urządzeniami typu firewall.
7. Rozwiązanie musi posiadać zintegrowany system operacyjny, tzn. nie może wymagać
od użytkownika instalacji osobnego systemu operacyjnego.
8. Rozwiązanie musi działać w dwóch instancjach:
	1. systemu operacyjnego, na którym uruchamiane są usługi centralnego zarządzania,
	2. serwera centralnego zarządzania, na którym istnieje możliwość konfigurowania poszczególnych usług.
9. Rozwiązanie musi posiadać personal firewall, który będzie filtrować wszystkie połączenia przychodzące/wychodzące do/z usług uruchomionych na urządzeniu.
10. Rozwiązanie ma mieć modułową budowę, pozwalającą na odinstalowanie/ /zainstalowanie, wyłączenie/włączenie każdego z modułów rozwiązania
bez restartowania rozwiązania.
11. Wymagana możliwość obsługi klastra High Availability z możliwością pracy w trybach Active-Passive.
12. Urządzenie ma zezwalać na stworzenie dedykowanego linku, służącego tylko
do monitorowania stanu partnera w klastrze High Availability.
13. Rozwiązanie ma posiadać możliwość uruchamiania własnych skryptów z poziomu CLI.
14. Rozwiązanie ma posiadać bazę predefiniowanych skryptów, do dyspozycji administratora, dostępnych z poziomu CLI.
15. Rozwiązanie ma pozwalać na uruchamiania skryptów zgodnie z przyjętym harmonogramem lub w chwili pojawienia się odpowiedniego zdarzenia na urządzeniu.
16. Rozwiązanie ma posiadać wbudowany serwer syslog.
17. Rozwiązanie ma dawać możliwość zarządzania systemem przez większą liczbę administratorów o określonych uprawnieniach.
18. Dostęp do urządzenia ma być możliwy za pomocą dedykowanego przez producenta narzędzia do centralnego zarządzania w trybie graficznym.
19. Administrator ma mieć możliwość dokonywania zdalnej konfiguracji i kontrolowania urządzenia za pomocą pojedynczego interfejsu. Ustawień związanych m.in.
z: bezpieczeństwem, ustawieniami reguł na firewallu, zarządzaniem ruchem, politykami dostępu, parametrami systemów operacyjnych, parametrami routingu.
	1. **SYSTEM CENTRALNEGO ZARZĄDZANIA:**
20. Rozwiązanie musi mieć możliwość hierarchicznego zarządzania urządzeniami
w środowisku, pozwalające na stworzenie co najmniej struktury: Kraj > Województwo > Miasto (miastem jest fizyczne urządzenie).
21. Uwierzytelnianie administratorów ma odbywać się w oparciu o silne szyfrowanie
oraz szyfrowanie AES.
22. Rozwiązanie musi posiadać moduł zarządzania uprawnieniami administratorów, pozwalający na zdefiniowanie uprawnień dla każdego z administratorów z osobna.
23. Rozwiązanie ma mieć możliwość definiowania różnych uprawnień administracyjnych
i delegowania ich na poszczególne jednostki lub lokalizacje.
24. Rozwiązanie musi dawać możliwość ukrywania wybranych opcji konfiguracyjnych, wybranym administratorom.
25. Rozwiązanie ma posiadać możliwość integracji z usługami katalogowymi Active Directory, LDAP, Radius, domeną NT 4, oraz obsługą: RSA SecureID,
do uwierzytelniania administratorów.
26. Rozwiązanie musi mieć możliwość tworzenia szablonów konfiguracyjnych
dla poszczególnych modułów.
27. Rozwiązanie musi posiadać dedykowany moduł pozwalający na dystrybucję aktualizacji do zarządzanych urządzeń. Moduł aktualizacji musi posiadać swój odrębny interfejs dostępny z programu do zarządzania.
28. Rozwiązaniem ma mieć możliwość zdalnego kontrolowania wersji i aktualizacji silników: antyspamu, antywirusa, filtra zawartości, NACa.
29. Rozwiązanie ma mieć możliwość centralnego zarządzania oraz przeglądania statystyk
z podległych mu urządzeń.
30. Rozwiązanie musi pozwalać na przesyłanie logów z podległych urządzeń na serwer centralnego zarządzania.
31. Rozwiązania ma posiadać system wersjonowania konfiguracji, pozwalający
na porównanie zmian dokonanych w konfiguracji oraz na przywrócenie konfiguracji historycznej dla pojedynczej jednostki konfiguracyjnej (np.: właściwości usługi VPN, właściwości usługi firewalla, zestaw reguł itp).
32. Rozwiązanie ma archiwizować konfigurację podległych mu urządzeń.
33. Rozwiązanie ma umożliwiać tworzenie tuneli VPN metodą drag&drop.
34. Rozwiązanie ma mieć wbudowany graficzny edytor konfiguracji tuneli VPN.
35. Graficzny edytor tuneli VPN musi mieć możliwość swobodnego układania serwerów VPN w interfejsie.
36. Interfejs graficznego edytora tuneli VPN musi mieć możliwość pracy w trybie pełnoekranowym, oraz mieć możliwość swobodnego oddalania i przybliżania mapy
z serwerami VPN.
37. Rozwiązanie ma mieć możliwość tworzenia wizualizacji w czasie rzeczywistym,
statusów tuneli VPN.
38. Rozwiązanie ma mieć możliwość zarządzania strukturą składającą się z urządzeń podległych pracujących pod kontrolą różnych wersji produktu.
39. Rozwiązanie ma posiadać dedykowane konsole do:
	1. sprawdzania ogólnego statusu urządzeń podległych,
	2. wizualizacji podległych urządzeń na mapach świata,
	3. sprawdzania statusu ostatniej wysłanej aktualizacji konfiguracji,
	4. wizualizacji aktualnie aktywnych sesji administracyjnych,
	5. wizualizacji statusu aktywacji urządzeń,
	6. wysyłania aktualizacji oprogramowania do podległych urządzeń,
	7. uruchamiania aktualizacji oprogramowania na podległych urządzeniach.
40. Rozwiązanie ma umożliwiać zarządzanie licencjami, oraz podgląd ich stanu
z poziomu systemu centralnego zarządzania.
41. Rozwiązanie ma zapewnić możliwość przeglądania zdarzeń, które wystąpiły
na zarządzanych urządzeniach.
42. Rozwiązanie ma przesyłać informacje o zdarzenia za pomocą protokołów SMTP
lub SNMP.
43. Rozwiązanie ma umożliwiać scentralizowane zarządzanie certyfikatami i kluczami podległych urządzeń.
44. Rozwiązanie ma budować dedykowany tunel VPN do komunikacji i zarządzania, pomiędzy systemem centralnego zarządzania a urządzeniem końcowym.
45. Rozwiązanie ma umożliwiać definiowania wirtualnych adresów IP w obrębie specjalnego tunelu VPN służącego do komunikacji pomiędzy systemem centralnego zarządzania
a klientem końcowym.
46. Urządzenie ma umożliwiać bezpieczne zdalne zarządzanie plikami wykonywalnymi, szyfrowanymi za pomocą SSHV2.
47. Rozwiązanie ma mieć możliwość dostosowania widoku drzewa konfiguracyjnego
i stworzenia własnych widoków.
48. Rozwiązanie ma posiadać serwer czasu NTP.
49. Wszystkie funkcjonalności mają być dostępne za pomocą interfejsu graficznego producenta urządzenia.
	1. **SERWIS:**
50. Oferowane urządzenie musi posiadać minimum czteroletnią gwarancję i wsparcie techniczne obejmującą wszystkie elementy urządzenia.
51. W czasie trwania gwarancji zamawiający ma prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade).
52. W czasie trwania gwarancji zamawiający ma dostęp do wsparcia technicznego świadczonego w dni robocze od poniedziałku do piątku w godzinach 8:00-18:00.
53. Wykonawca zapewni wymianę uszkodzonego urządzenia na sprawne. Wysyłka następnego dnia roboczego po stwierdzeniu uszkodzenia.
54. Wykonawca musi zatrudniać co najmniej 3 certyfikowanych przez producenta inżynierów świadczących wsparcia dla powyższego rozwiązania.
55. Wsparcie techniczne oraz szkolenie z produktu prowadzone są w języku polskim przez certyfikowanego przez producenta trenera.
56. **OPIS TECHNICZNY URZĄDZEŃ**
	1. **FIREWALL – szt. 1**

**OGÓLNE:**

1. Rozwiązanie musi być dostępne jako platforma sprzętowa.
2. Rozwiązanie musi posiadać zintegrowany system operacyjny, tzn. nie może wymagać
od użytkownika instalacji osobnego systemu operacyjnego.
3. Rozwiązanie posiada nielimitowaną licencję dla użytkowników Firewalla.
4. Minimalna przepustowość firewalla to co najmniej 300 Mbps.
5. Rozwiązanie musi obsługiwać do 2000 sesji równoległych.
6. Rozwiązanie łączy w sobie:
	1. zaporę sieciową z inspekcją stanu pakietów (stateful inspection firewall),
	2. system IPS/IDS,
	3. filtr warstwy 7,
	4. serwer VPN.
7. Rozwiązanie ma mieć modułową budowę, pozwalającą na odinstalowanie/ zainstalowanie, wyłączenie/włączenie każdego z modułów rozwiązania bez restartowania rozwiązania.
8. Rozwiązanie ma zapewniać ochronę przed atakami typu DoS/DDoS: IP spoofing. SYN flooding, flood ping i innymi, oraz przed skanowaniem portów i adresów.
9. Rozwiązanie ma usługiwać:
	1. NAT, PAT, proxy arp, VLAN,
	2. Protokoły VoIP – H.323, SIP, SCCP,
	3. Protokoły OSPF, RIP zarówno przy połączeniach IP jak i VPN.
10. Rozwiązanie ma umożliwiać pełne zdalne zarządzania firewallem, serwerem VPN
oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej
pod systemami MS Windows.
11. Rozwiązanie musi posiadać możliwość przeglądania zmian nanoszonych przez automatyczne aktualizacje systemu z graficznej konsoli administracyjnej.
12. Rozwiązanie ma umożliwiać zarządzanie urządzeniem poprzez zdalne kody SMS.
13. Rozwiązanie musi umożliwiać generowanie statystyk w czasie rzeczywistym – opóźnienie statystyk ma być nie większe niż 10 sekund.
14. Aktywne powiadomienia o zdarzeniach przez SMTP i SNMP.
15. Możliwość ustawienia żądania potwierdzenia przez administratora odczytania powiadomienia o krytycznym zdarzeniu (w systemie pozostaje informacja, który administrator odczytał i skasował ostrzeżenie o zdarzeniu krytycznym).
16. Rozwiązanie musi umożliwiać przesyłanie statystyk i/lub logów na serwer centralnego zarządzania.
17. Rozwiązanie ma mieć możliwość zarządzania systemem przez wielu administratorów
w jednym czasie.
18. Rozwiązanie ma zapewniać integrację z usługami katalogowymi Active Directory, LDAP, Radius, domena NT 4.
19. Ponadto, rozwiązanie ma zapewniać obsługę: RSA SecureID, TACACS+ przez usługi firewall, serwer VPN oraz uwierzytelnianie administratorów.
20. Rozwiązanie ma zapewnić obsługa uwierzytelniania administratorów przy pomocy hasła (lokalnego lub synchronizowanego z usługą katalogową), klucza zapisanego na tokenie lub karcie kryptograficznej albo równocześnie przy pomocy i hasła, i klucza.
21. Rozwiązanie musi umożliwiać obsługę wybranych kart UMTS/EDGE/HSDPA.
22. Czas pełnej instalacji lub odtworzenia systemu zapory sieciowej po awarii jest nie większy niż 30 minut.
23. Rozwiązanie ma zapewniać możliwość uruchamiania własnych skryptów z poziomu CLI.
24. Urządzenie ma posiadać bazę predefiniowanych skryptów, do dyspozycji administratora, dostępnych z poziomu CLI.
25. Rozwiązanie ma zezwalać na uruchamianie skryptów zgodnie z przyjętym harmonogramem lub w chwili pojawienia się odpowiedniego zdarzenia na urządzeniu.
26. Możliwość zarządzania systemem przez większą liczbę administratorów o określonych uprawnieniach.

**FIREWALL:**

1. Urządzenie musi posiadać personal firewall, obsługujący wszystkie połączenia wychodzące i przychodzące do usług zainstalowanych na urządzeniu.
2. Rozwiązanie musi umożliwiać tworzenie obiektów dynamicznych, zależnych od miejsca,
w którym zostało zainstalowane urządzenie.
3. Rozwiązanie ma umożliwiać tworzenie reguł firewalla z mechanizmem TCP Proxy.
4. Rozwiązanie ma pracować w trybie bridge (transparentnym), routera, oraz mieszanym (równocześnie jako bridge i router).
5. Rozwiązanie musi umożliwiać tworzenie reguł NAT wewnątrz reguły tworzonej
na firewallu.
6. Urządzenie ma umożliwiać podzielenie reguł firewalla na logiczne grupy, pomiędzy którymi występują kaskadowe połączenia.
7. Urządzenie ma umożliwiać definiowanie reguł dynamicznych na firewallu, automatycznie wyłączających się po ustalonym czasie.
8. Wbudowany analizator pakietów (sniffer) uruchamiany z graficznej konsoli użytkownika
i z CLI.
9. Wbudowany tester reguł pozwalający na sprawdzenie poprawności i wyników działania tworzonych reguł przed ich aktywacją na firewallu.
10. Wbudowany filtr aplikacji typu P2P, komunikatorów internetowych oraz gier.

**VPN:**

1. Rozwiązanie musi posiadać własny protokół dla tuneli VPN site-2-site i client-2-site.
2. Rozwiązanie musi posiadać możliwość tworzenia specjalnych tuneli VPN, służących
do zarządzania urządzeniami, niezależnie od głównego tunelu VPN.
3. Rozwiązanie ma zapewnić możliwość budowy kanałów VPN w strukturze gwiaździstej
z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami – minimalna liczba kanałów VPN zapewniających pełną komunikację pomiędzy wszystkimi lokalizacjami nie powinna być większa niż liczba lokalizacji.
4. Rozwiązanie ma obsługiwać multitransport VPN – tworzenie do 24 transportów
w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień.
5. Rozwiązanie ma zapewnić możliwość łączenia transportów VPN (agregacja łączy
na poziomie pakietów lub sesji) i wyznaczania transportów zapasowych.
6. Rozwiązanie ma umożliwiać przypisywanie ruchu do wybranego transportu VPN
w zależności od adresu źródłowego, adresu docelowego, portu, protokołu, nazwy uwierzytelnionego użytkownika lub grupy, do której należy oraz dnia tygodnia i godziny nawiązania połączenia.
7. Rozwiązanie ma zapewniać budowanie tuneli VPN w oparciu o protokoły: TCP, UDP, ESP, TCP i UDP.
8. Rozwiązanie ma zezwalać na nawiązywanie połączeń VPN przechodzących przez serwer proxy HTTPS.
9. Rozwiązanie musi posiadać w standardzie darmowego klienta NAC integrującego
się z centrum akcji w systemach Windows Vista/7.
10. Dostępne centrum autoryzacji na lokalnym serwerze VPN.
11. Rozwiązanie ma umożliwiać uwierzytelnianie użytkowników VPN za pomocą certyfikatów cyfrowych i/lub logowania.
12. Obsługa urządzeń kryptograficznych (tokenów, kart) współpracujących z mechanizmem Microsoft Strong Credential Provider dla systemu Windows.
13. Klient VPN musi mieć możliwość wyświetlania tekstu powitalnego przy połączeniu
do sieci korporacyjnej (tzw. MOTD).
14. Klient VPN musi mieć możliwość sprawdzania jak i modyfikowania rejestru systemu Windows komputera, na którym jest zainstalowany.
15. Klient VPN musi być stworzony przez tą samą firmę co dostarczone rozwiązanie.
16. Obsługa uwierzytelniania wieloskładnikowego w kliencie VPN.
17. Rozwiązanie ma umożliwiać przydzielanie ustawień tunelu VPN client-to-site
na podstawie przynależności użytkownika do grupy zabezpieczeń w usłudze katalogowej Active Directory lub LDAP.
18. Możliwość uwierzytelniania certyfikatem X.509 przy integracji z zewnętrzną infrastrukturą PKI i przydzielanie ustawień tunelu VPN client-to-site w zależności
od atrybutów certyfikatu.
19. Klient VPN ma być dedykowany na platformy: Windows, Linux.
20. Klient VPN musi posiadać graficzny interfejs użytkownika.
21. Możliwość zdefiniowania na platformach Windows skrótu do połączenia VPN
z ukrytymi wszystkimi opcjami konfiguracyjnymi.
22. Obsługa uwierzytelniania stron przy tworzeniu tuneli VPN typu site-to-site oraz client-to-site za pomocą certyfikatów X.509 ze struktury PKI zarządzanej przez dowolny serwer PKI z obsługą list CRL.
23. Rozwiązanie ma zapewniać możliwość zarządzania pasmem w ramach tunelu VPN
i na każdym tunelu VPN z osobna.
24. Rozwiązanie ma automatycznie zmieniać polityki podziału pasma w tunelach VPN
po awarii jednego z transportów VPN i przełączenia ruchu na transport zapasowy.
25. Rozwiązanie ma zapewniać kompresję danych przesyłanych w tunelach VPN.
26. Rozwiązanie ma mieć możliwość buforowania danych przesyłanych w tunelach VPN
dla protokołów zdefiniowanych przez administratora.
27. Rozwiązanie ma automatycznie zmieniać trasowanie ruchu VPN w przypadku awarii tunelu VPN.

**SIEĆ:**

1. Rozwiązanie ma mieć mechanizm pozwalający na aktywację nowej konfiguracji sieci
na co najmniej trzy sposoby z czego jeden z nich nie może zrywać aktywnych sesji
na urządzeniu.
2. Rozwiązanie ma automatycznie przywracać ostatnią działającą konfigurację sieci
po zdefiniowanym czasie od momentu utracenia połączenia administracyjnego.
3. Rozwiązanie ma obsługiwać:
	1. kilka łączy internetowych równocześnie, w tym multipath routing,
	2. łączy z dynamicznie przypisywanymi adresami IP,
	3. DynDNS.
4. Rozwiązaniu musi umożliwiać automatyczne przekierowanie ruchu na łącze zapasowe
w przypadku awarii łącza głównego.
5. Możliwość podziału łącza w oparciu o wirtualne drzewa decyzyjne dla każdego z użytkowników z osobna lub dla grup użytkowników oraz możliwość ustawiania priorytetów (traffic shaping).
6. Obsługa dynamicznego (priorytety ruchu) i statycznego (ograniczenie maksymalnej przepustowości) podziału pasm.

**SPRZĘT:**

1. Urządzenie musi posiadać co najmniej 4 interfejsy sieciowe (10/100/1000 MBit RJ45).
2. Urządzenie musi posiadać co najmniej 2 złącza USB 2.0.
3. Urządzenie musi posiadać procesor o prędkości co najmniej 500 MHz.
4. Urządzenie musi posiadać co najmniej 512 MB pamięci operacyjnej RAM.
5. Urządzenie musi posiadać dysk flash o pojemności co najmniej 4 GB.

**SERWIS:**

1. Oferowane urządzenie musi posiadać minimum czteroletnią gwarancję i wsparcie techniczne obejmującą wszystkie elementy urządzenia.
2. W czasie trwania gwarancji zamawiający ma prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade).
3. W czasie trwania gwarancji zamawiający ma dostęp do wsparcia technicznego świadczonego w dni robocze od poniedziałku do piątku w godzinach 8:00-18:00.
4. Wykonawca zapewni wymianę uszkodzonego urządzenia na sprawne. Wysyłka następnego dnia roboczego po stwierdzeniu uszkodzenia.
5. Wsparcie techniczne oraz szkolenie z produktu, prowadzone są w języku polskim przez certyfikowanego przez producenta trenera.
6. Wykonawca musi zatrudniać co najmniej 3 certyfikowanych przez producenta inżynierów, świadczących wsparcie dla powyższego urządzenia.
	1. **FIREWALL – szt. 8**

**OGÓLNE:**

1. Rozwiązanie musi być dostępne jako platforma sprzętowa.
2. Rozwiązanie musi posiadać zintegrowany system operacyjny, tzn. nie może wymagać
od użytkownika instalacji osobnego systemu operacyjnego.
3. Rozwiązanie posiada nielimitowaną licencję dla użytkowników Firewalla.
4. Minimalna przepustowość firewalla to co najmniej 300 Mbps.
5. Rozwiązanie musi obsługiwać do 2000 sesji równoległych.
6. Rozwiązanie łączy w sobie:
	1. zaporę sieciową z inspekcją stanu pakietów (stateful inspection firewall),
	2. system IPS/IDS pozwalający całkowite wyładowanie z systemu,
	3. filtr warstwy 7,
	4. serwer VPN,
	5. HTTP Proxy wraz z co najmniej 50 kategoriami tematycznymi,
	6. filtr antyspamowy.
7. Rozwiązanie ma mieć modułową budowę, pozwalającą na odinstalowanie/ zainstalowanie, wyłączenie/włączenie każdego z modułów rozwiązania bez restartowania rozwiązania.
8. Rozwiązanie ma zapewniać ochronę przed atakami typu DoS/DDoS: IP spoofing. SYN flooding, flood ping i innymi oraz przed skanowaniem portów i adresów.
9. Rozwiązanie ma usługiwać:
	1. NAT, PAT, proxy arp, VLAN,
	2. Protokoły VoIP – H.323, SIP, SCCP,
	3. Protokoły OSPF, RIP zarówno przy połączeniach IP jak i VPN.
10. Rozwiązanie ma umożliwiać pełne zdalne zarządzania firewallem, serwerem VPN
oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej
pod systemami MS Windows.
11. Rozwiązanie musi posiadać możliwość przeglądania zmian nanoszonych przez automatyczne aktualizacje systemu z graficznej konsoli administracyjnej.
12. Rozwiązanie ma umożliwiać zarządzanie urządzeniem poprzez zdalne kody SMS.
13. Rozwiązanie musi umożliwiać generowanie statystyk w czasie rzeczywistym – opóźnienie statystyk ma być nie większe niż 10 sekund.
14. Aktywne powiadomienia o zdarzeniach przez SMTP i SNMP.
15. Możliwość ustawienia żądania potwierdzenia przez administratora odczytania powiadomienia o krytycznym zdarzeniu (w systemie pozostaje informacja, który administrator odczytał i skasował ostrzeżenie o zdarzeniu krytycznym).
16. Rozwiązanie musi umożliwiać przesyłanie statystyk i/lub logów na serwer centralnego zarządzania.
17. Urządzenie musi umożliwiać sprawdzanie w czasie rzeczywistym statusu: działających usług, łącz internetowych, czy statusu switchy, za pomocą wbudowanego mechanizmu.
18. Rozwiązanie ma mieć możliwość zarządzania systemem przez wielu administratorów
w jednym czasie.
19. Rozwiązanie ma zapewniać integrację z usługami katalogowymi Active Directory, LDAP, Radius, domena NT 4.
20. Ponadto, rozwiązanie ma zapewniać obsługę: RSA SecureID, TACACS+ przez usługi firewall, serwer VPN, proxy HTTP (działające na wielu procesorach), proxy FTP, proxy SSH oraz uwierzytelnianie administratorów.
21. Rozwiązanie ma zapewnić obsługa uwierzytelniania administratorów przy pomocy hasła (lokalnego lub synchronizowanego z usługą katalogową), klucza zapisanego na tokenie lub karcie kryptograficznej albo równocześnie przy pomocy i hasła, i klucza.
22. Wymagana możliwość obsługi klastra High Availability z możliwością pracy w trybach Active-Passive i Active-Active.
23. Urządzenie ma pozwalać na stworzenie dedykowanego linku, służącego tylko
do monitorowania stanu partnera w klastrze High Availability.
24. Rozwiązanie musi umożliwiać obsługę wybranych kart UMTS/EDGE/HSDPA.
25. Czas pełnej instalacji lub odtworzenia systemu zapory sieciowej po awarii jest
nie większy niż 30 minut.
26. Rozwiązanie ma zapewniać możliwość uruchamiania własnych skryptów z poziomu CLI.
27. Urządzenie ma posiadać bazę predefiniowanych skryptów, do dyspozycji administratora, dostępnych z poziomu CLI.
28. Rozwiązanie ma zezwalać na uruchamianie skryptów zgodnie z przyjętym harmonogramem lub w chwili pojawienia się odpowiedniego zdarzenia na urządzeniu.
29. Możliwość zarządzania systemem przez większą liczbę administratorów o określonych uprawnieniach.

**FIREWALL:**

1. Urządzenie musi posiadać personal firewall obsługujący wszystkie połączenia wychodzące i przychodzące do usług zainstalowanych na urządzeniu.
2. Rozwiązanie musi umożliwiać tworzenie obiektów dynamicznych, zależnych od miejsca,
w którym zostało zainstalowane urządzenie.
3. Rozwiązanie ma umożliwiać tworzenie reguł firewalla z mechanizmem TCP Proxy.
4. Rozwiązanie ma pracować w trybie bridge (transparentnym), routera, oraz mieszanym (równocześnie jako bridge i router).
5. Rozwiązanie musi umożliwiać tworzenie reguł NAT wewnątrz reguły tworzonej
na firewallu.
6. Urządzenie ma umożliwiać podzielenie reguł firewalla na logiczne grupy, pomiędzy którymi występują kaskadowe połączenia.
7. Urządzenie ma umożliwiać definiowanie reguł dynamicznych na firewallu, automatycznie wyłączających się po ustalonym czasie.
8. Wbudowany analizator pakietów (sniffer) uruchamiany z graficznej konsoli użytkownika
i z CLI.
9. Wbudowany tester reguł pozwalający na sprawdzenie poprawności i wyników działania tworzonych reguł przed ich aktywacją na firewallu.
10. Wbudowany filtr aplikacji typu P2P, komunikatorów internetowych oraz gier.

**VPN:**

1. Rozwiązanie musi posiadać własny protokół dla tuneli VPN site-2-site i client-2-site.
2. Rozwiązanie musi posiadać możliwość tworzenia specjalnych tuneli VPN opartych
o autorski protokół, służących do zarządzania urządzeniami, niezależnie od głównego tunelu VPN.
3. Rozwiązanie ma zapewnić możliwość budowy kanałów VPN w strukturze gwiaździstej
z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami – minimalna liczba kanałów VPN zapewniających pełną komunikację pomiędzy wszystkimi lokalizacjami nie powinna być większa niż liczba lokalizacji.
4. Rozwiązanie ma obsługiwać multitransport VPN – tworzenie do 24 transportów
w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień.
5. Rozwiązanie ma zapewnić możliwość łączenia transportów VPN (agregacja łączy
na poziomie pakietów lub sesji) i wyznaczania transportów zapasowych.
6. Rozwiązanie ma umożliwiać przypisywanie ruchu do wybranego transportu VPN
w zależności od adresu źródłowego, adresu docelowego, portu, protokołu, nazwy uwierzytelnionego użytkownika lub grupy, do której należy oraz dnia tygodnia i godziny nawiązania połączenia.
7. Rozwiązanie ma zapewniać budowanie tuneli VPN w oparciu o protokoły: TCP, UDP, ESP, TCP i UDP.
8. Rozwiązanie ma zezwalać na nawiązywanie połączeń VPN przechodzących przez serwer proxy HTTPS.
9. Rozwiązanie musi posiadać w standardzie darmowego klienta NAC integrującego
się z centrum akcji w systemach Windows Vista/7.
10. Dostępne centrum autoryzacji na lokalnym serwerze VPN.
11. Rozwiązanie ma umożliwiać uwierzytelnianie użytkowników VPN za pomocą certyfikatów cyfrowych i/lub logowania.
12. Obsługa urządzeń kryptograficznych (tokenów, kart) współpracujących z mechanizmem Microsoft Strong Credential Provider dla systemu Windows.
13. Klient VPN musi mieć możliwość wyświetlania tekstu powitalnego przy połączeniu
do sieci korporacyjnej (tzw. MOTD).
14. Klient VPN musi mieć możliwość sprawdzania jak i modyfikowania rejestru systemu Windows komputera, na którym jest zainstalowany.
15. Klient VPN musi być stworzony przez tą samą firmę co dostarczone rozwiązanie.
16. Obsługa uwierzytelniania wieloskładnikowego w kliencie VPN.
17. Rozwiązanie ma umożliwiać przydzielanie ustawień tunelu VPN client-to-site
na podstawie przynależności użytkownika do grupy zabezpieczeń w usłudze katalogowej Active Directory lub LDAP.
18. Możliwość uwierzytelniania certyfikatem X.509 przy integracji z zewnętrzną infrastrukturą PKI i przydzielanie ustawień tunelu VPN client-to-site w zależności
od atrybutów certyfikatu.
19. Klient VPN ma być dedykowany na platformy: Windows, Linux.
20. Klient VPN musi posiadać graficzny interfejs użytkownika.
21. Możliwość zdefiniowania na platformach Windows skrótu do połączenia VPN
z ukrytymi wszystkimi opcjami konfiguracyjnymi.
22. Obsługa uwierzytelniania stron przy tworzeniu tuneli VPN typu site-to-site oraz client-to-site za pomocą certyfikatów X.509 ze struktury PKI zarządzanej przez dowolny serwer PKI z obsługą list CRL.
23. Rozwiązanie ma zapewniać możliwość zarządzania pasmem w ramach tunelu VPN
i na każdym tunelu VPN z osobna.
24. Rozwiązanie ma automatycznie zmieniać polityki podziału pasma w tunelach VPN
po awarii jednego z transportów VPN i przełączenia ruchu na transport zapasowy.
25. Rozwiązanie ma zapewniać kompresję danych przesyłanych w tunelach VPN.
26. Rozwiązanie ma mieć możliwość buforowania danych przesyłanych w tunelach VPN
dla protokołów zdefiniowanych przez administratora.
27. Rozwiązanie ma automatycznie zmieniać trasowanie ruchu VPN w przypadku awarii tunelu VPN.

**SIEĆ:**

1. Rozwiązanie ma mieć mechanizm pozwalający na aktywacje nowej konfiguracji sieci
na co najmniej trzy sposoby z czego jeden z nich nie może zrywać aktywnych sesji
na urządzeniu.
2. Rozwiązanie ma automatycznie przywracać ostatnią działającą konfigurację sieci
po zdefiniowanym czasie od momentu utracenia połączenia administracyjnego.
3. Rozwiązanie ma obsługiwać:
	1. kilka łączy internetowych równocześnie, w tym multipath routing,
	2. łączy z dynamicznie przypisywanymi adresami IP,
	3. DynDNS.
4. Rozwiązaniu musi umożliwiać automatyczne przekierowanie ruchu na łącze zapasowe
w przypadku awarii łącza głównego.
5. Możliwość podziału łącza w oparciu o wirtualne drzewa decyzyjne dla każdego z użytkowników z osobna lub dla grup użytkowników oraz możliwość ustawiania priorytetów (traffic shaping).
6. Obsługa dynamicznego (priorytety ruchu) i statycznego (ograniczenie maksymalnej przepustowości) podziału pasm.

**SPRZĘT:**

1. Urządzenie musi posiadać co najmniej 4 interfejsy sieciowe (10/100/1000 MBit RJ45).
2. Rozwiązanie musi dawać możliwość wyboru wersji urządzenia z modułem wifi lub bez modułu.
3. Urządzenie musi posiadać co najmniej 2 złącza USB 2.0.
4. Urządzenie musi posiadać procesor o prędkości co najmniej 500 MHz,
5. Urządzenie musi posiadać co najmniej 2 GB pamięci operacyjnej RAM,
6. Urządzenie musi posiadać dysk flash o pojemności co najmniej 4 GB.

**SERWIS:**

1. Oferowane urządzenie musi posiadać minimum czteroletnią gwarancję i wsparcie techniczne obejmującą wszystkie elementy urządzenia.
2. W czasie trwania gwarancji zamawiający ma prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade).
3. W czasie trwania gwarancji zamawiający ma dostęp do wsparcia technicznego świadczonego w dni robocze od poniedziałku do piątku w godzinach 8:00-18:00.
4. Wykonawca zapewni wymianę uszkodzonego urządzenia na sprawne. Wysyłka następnego dnia roboczego po stwierdzeniu uszkodzenia.
5. Wsparcie techniczne oraz szkolenie z produktu, prowadzone są w języku polskim przez certyfikowanego przez producenta trenera.
6. Wykonawca musi zatrudniać co najmniej 3 certyfikowanych przez producenta inżynierów, świadczących wsparcie dla powyższego urządzenia.
	1. **FIREWALL – szt. 1**

**OGÓLNE:**

1. Rozwiązanie musi być dostępne jako platforma sprzętowa.
2. Rozwiązanie musi posiadać zintegrowany system operacyjny, tzn. nie może wymagać
od użytkownika instalacji osobnego systemu operacyjnego.
3. Rozwiązanie posiada nielimitowaną licencję dla użytkowników Firewalla.
4. Minimalna przepustowość firewalla to co najmniej 400 Mbps.
5. Rozwiązanie musi obsługiwać do 35000 sesji równoległych.
6. Rozwiązanie łączy w sobie:
	1. zaporę sieciową z inspekcją stanu pakietów (stateful inspection firewall),
	2. system IPS/IDS pozwalający całkowite wyładowane z systemu,
	3. filtr warstwy 7,
	4. serwer VPN,
	5. HTTP Proxy, wraz z co najmniej 50 kategoriami tematycznymi,
	6. filtr antyspamowy.
7. Rozwiązanie ma mieć modułową budowę, pozwalającą na odinstalowanie/ zainstalowanie, wyłączenie/włączenie każdego z modułów rozwiązania bez restartowania rozwiązania.
8. Rozwiązanie ma zapewniać ochronę przed atakami typu DoS/DDoS: IP spoofing. SYN flooding, flood ping i innymi, oraz przed skanowaniem portów i adresów.
9. Rozwiązanie ma usługiwać:
	1. NAT, PAT, proxy arp, VLAN,
	2. Protokoły VoIP – H.323, SIP, SCCP,
	3. Protokoły OSPF, RIP zarówno przy połączeniach IP jak i VPN.
10. Rozwiązanie ma umożliwiać pełne zdalne zarządzania firewallem, serwerem VPN
oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej
pod systemami MS Windows.
11. Rozwiązanie musi posiadać możliwość przeglądania zmian nanoszonych przez automatyczne aktualizacje systemu z graficznej konsoli administracyjnej.
12. Rozwiązanie ma umożliwiać zarządzanie urządzeniem poprzez zdalne kody SMS.
13. Rozwiązanie musi umożliwiać generowanie statystyk w czasie rzeczywistym – opóźnienie statystyk ma być nie większe niż 10 sekund.
14. Aktywne powiadomienia o zdarzeniach przez SMTP i SNMP.
15. Możliwość ustawienia żądania potwierdzenia przez administratora odczytania powiadomienia o krytycznym zdarzeniu (w systemie pozostaje informacja, który administrator odczytał i skasował ostrzeżenie o zdarzeniu krytycznym).
16. Rozwiązanie musi umożliwiać przesyłanie statystyk i/lub logów na serwer centralnego zarządzania.
17. Urządzenie musi umożliwiać sprawdzanie w czasie rzeczywistym statusu: działających usług, łącz internetowych czy statusu switchy za pomocą wbudowanego mechanizmu.
18. Rozwiązanie ma mieć możliwość zarządzania systemem przez wielu administratorów
w jednym czasie.
19. Rozwiązanie ma zapewniać integrację z usługami katalogowymi Active Directory, LDAP, Radius, domena NT 4.
20. Ponadto, rozwiązanie ma zapewniać obsługę: RSA SecureID, TACACS+ przez usługi firewall, serwer VPN, proxy HTTP (działające na wielu procesorach), proxy FTP, proxy SSH oraz uwierzytelnianie administratorów.
21. Rozwiązanie ma zapewnić obsługa uwierzytelniania administratorów przy pomocy hasła (lokalnego lub synchronizowanego z usługą katalogową), klucza zapisanego na tokenie lub karcie kryptograficznej albo równocześnie przy pomocy i hasła, i klucza.
22. Wymagana możliwość obsługi klastra High Availability z możliwością pracy w trybach Active-Passive i Active-Active.
23. Urządzenie ma pozwalać na stworzenie dedykowanego linku służącego tylko
do monitorowania stanu partnera w klastrze High Availability.
24. Rozwiązanie musi umożliwiać obsługę wybranych kart UMTS/EDGE/HSDPA.
25. Czas pełnej instalacji lub odtworzenia systemu zapory sieciowej po awarii jest nie większy niż 15 minut.
26. Rozwiązanie ma zapewniać możliwość uruchamiania własnych skryptów z poziomu CLI.
27. Urządzenie ma posiadać bazę predefiniowanych skryptów, do dyspozycji administratora, dostępnych z poziomu CLI.
28. Rozwiązanie ma zezwalać na uruchamianie skryptów zgodnie z przyjętym harmonogramem lub w chwili pojawienia się odpowiedniego zdarzenia na urządzeniu.
29. Możliwość zarządzania systemem przez większą liczbę administratorów o określonych uprawnieniach.

**FIREWALL:**

1. Urządzenie musi posiadać personal firewall, obsługujący wszystkie połączenia wychodzące i przychodzące do usług zainstalowanych na urządzeniu.
2. Rozwiązanie musi umożliwiać tworzenie obiektów dynamicznych, zależnych od miejsca,
w którym zostało zainstalowane urządzenie.
3. Rozwiązanie ma umożliwiać tworzenie reguł firewalla z mechanizmem TCP Proxy.
4. Rozwiązanie ma pracować w trybie bridge (transparentnym), routera, oraz mieszanym (równocześnie jako bridge i router).
5. Rozwiązanie musi umożliwiać tworzenie reguł NAT wewnątrz reguły tworzonej
na firewallu.
6. Urządzenie ma umożliwiać podzielenie reguł firewalla na logiczne grupy, pomiędzy którymi występują kaskadowe połączenia.
7. Urządzenie ma umożliwiać definiowanie reguł dynamicznych na firewallu, automatycznie wyłączających się po ustalonym czasie.
8. Urządzenie ma umożliwiać tworzenie dynamicznych reguł firewalla uruchamianych
z interfejsu SSL VPN.
9. Wbudowany analizator pakietów (sniffer) uruchamiany z graficznej konsoli użytkownika
i z CLI.
10. Wbudowany tester reguł pozwalający na sprawdzenie poprawności i wyników działania tworzonych reguł przed ich aktywacją na firewallu.
11. Rozwiązanie musi posiadać zintegrowany filtr warstwy 7.
12. Rozwiązanie musi pozwalać na blokowanie pojedynczych funkcji konkretnych aplikacji (np. blokowanie tylko transfery plików w Gadu-Gadu, lub przepuszczania tylko
i wyłącznie aktualizacji programów pracujących w sieci.
13. Rozwiązanie musi mieć możliwość transparentnego skanowania ruchu zaszyfrowanego (MITM).

**VPN:**

1. Rozwiązanie musi posiadać własny protokół dla tuneli VPN site-2-site i client-2-site.
2. Rozwiązanie musi posiadać możliwość tworzenia specjalnych tuneli VPN opartych
o autorski protokół, służących do zarządzania urządzeniami, niezależnie od głównego tunelu VPN.
3. Rozwiązanie ma zapewnić możliwość budowy kanałów VPN w strukturze gwiaździstej
z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami – minimalna liczba kanałów VPN zapewniających pełną komunikację pomiędzy wszystkimi lokalizacjami nie powinna być większa niż liczba lokalizacji.
4. Rozwiązanie ma obsługiwać multitransport VPN – tworzenie do 24 transportów
w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień.
5. Rozwiązanie ma zapewnić możliwość łączenia transportów VPN (agregacja łączy
na poziomie pakietów, lub sesji) i wyznaczania transportów zapasowych.
6. Rozwiązanie ma umożliwiać przypisywanie ruchu do wybranego transportu VPN
w zależności od adresu źródłowego, adresu docelowego, portu, protokołu, nazwy uwierzytelnionego użytkownika lub grupy, do której należy oraz dnia tygodnia i godziny nawiązania połączenia.
7. Rozwiązanie ma zapewniać budowanie tuneli VPN w oparciu o protokoły: TCP, UDP, ESP, TCP i UDP.
8. Rozwiązanie ma zezwalać na nawiązywanie połączeń VPN przechodzących przez serwer proxy HTTPS.
9. Rozwiązanie musi posiadać w standardzie, darmowego klienta NAC integrującego
się z centrum akcji w systemach Windows Vista/7.
10. Dostępne centrum autoryzacji na lokalnym serwerze VPN.
11. Rozwiązanie ma umożliwiać uwierzytelnianie użytkowników VPN za pomocą certyfikatów cyfrowych i/lub logowania.
12. Obsługa urządzeń kryptograficznych (tokenów, kart) współpracujących z mechanizmem Microsoft Strong Credential Provider dla systemu Windows.
13. Klient VPN musi mieć możliwość wyświetlania tekstu powitalnego przy połączeniu
do sieci korporacyjnej (tzw. MOTD).
14. Klient VPN musi mieć możliwość sprawdzania jak i modyfikowania rejestru systemu Windows komputera, na którym jest zainstalowany.
15. Klient VPN musi być stworzony przez tą samą firmę co dostarczone rozwiązanie.
16. Obsługa uwierzytelniania wieloskładnikowego w kliencie VPN.
17. Rozwiązanie ma umożliwiać przydzielanie ustawień tunelu VPN client-to-site
na podstawie przynależności użytkownika do grupy zabezpieczeń w usłudze katalogowej Active Directory lub LDAP.
18. Możliwość uwierzytelniania certyfikatem X.509 przy integracji z zewnętrzną infrastrukturą PKI i przydzielanie ustawień tunelu VPN client-to-site w zależności
od atrybutów certyfikatu.
19. Klient VPN ma być dedykowany na platformy: Windows, Linux.
20. Klient VPN musi posiadać graficzny interfejs użytkownika.
21. Możliwość zdefiniowania na platformach Windows skrótu do połączenia VPN
z ukrytymi wszystkimi opcjami konfiguracyjnymi.
22. Obsługa uwierzytelniania stron przy tworzeniu tuneli VPN typu site-to-site oraz client-to-site za pomocą certyfikatów X.509 ze struktury PKI zarządzanej przez dowolny serwer PKI z obsługą list CRL.
23. Rozwiązanie ma zapewniać możliwość zarządzania pasmem w ramach tunelu VPN
i na każdym tunelu VPN z osobna.
24. Rozwiązanie ma automatycznie zmieniać polityki podziału pasma w tunelach VPN
po awarii jednego z transportów VPN i przełączenia ruchu na transport zapasowy.
25. Rozwiązanie ma zapewniać kompresję i deduplikację danych przesyłanych w tunelach VPN.
26. Rozwiązanie ma mieć możliwość buforowania danych przesyłanych w tunelach VPN
dla protokołów zdefiniowanych przez administratora.
27. Rozwiązanie ma automatycznie zmieniać trasowanie ruchu VPN w przypadku awarii tunelu VPN.

**SIEĆ:**

1. Rozwiązanie ma mieć mechanizm pozwalający na aktywacje nowej konfiguracji sieci
na co najmniej trzy sposoby z czego jeden z nich nie może zrywać aktywnych sesji
na urządzeniu.
2. Rozwiązanie ma automatycznie przywracać ostatnią działającą konfigurację sieci
po zdefiniowanym czasie od momentu utracenia połączenia administracyjnego.
3. Rozwiązanie ma obsługiwać:
	1. kilka łączy internetowych równocześnie, w tym multipath routing,
	2. łączy z dynamicznie przypisywanymi adresami IP,
	3. DynDNS.
4. Rozwiązaniu musi umożliwiać automatyczne przekierowanie ruchu na łącze zapasowe
w przypadku awarii łącza głównego.
5. Możliwość podziału łącza w oparciu o wirtualne drzewa decyzyjne dla każdego z użytkowników
z osobna lub dla grup użytkowników oraz możliwość ustawiania priorytetów (traffic shaping).
6. Obsługa dynamicznego (priorytety ruchu) i statycznego (ograniczenie maksymalnej przepustowości) podziału pasm.

**SPRZĘT:**

1. Urządzenie musi posiadać co najmniej 4 interfejsy sieciowe (10/100/1000 MBit RJ45).
2. Rozwiązanie musi dawać możliwość wyboru wersji urządzenia z modułem wifi, lub bez modułu.
3. Urządzenie musi posiadać procesor o prędkości co najmniej 1,5 GHz.
4. Urządzenie musi posiadać co najmniej 2 GB pamięci operacyjnej RAM.
5. Urządzenie musi posiadać dysk SSD o pojemności co najmniej 40 GB.
6. Urządzenie musi posiadać dysk flash o pojemności co najmniej 128 MB.
7. Urządzenie musi posiadać co najmniej 2 złącza USB 2.0.
8. Urządzenie musi posiadać zasilacz o mocy co najmniej 60W.

**SERWIS:**

1. Oferowane urządzenie musi posiadać minimum czteroletnią gwarancję i wsparcie techniczne obejmującą wszystkie elementy urządzenia.
2. W czasie trwania gwarancji zamawiający ma prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade).
3. W czasie trwania gwarancji zamawiający ma dostęp do wsparcia technicznego świadczonego w dni robocze od poniedziałku do piątku w godzinach 8:00-18:00.
4. Wykonawca zapewni wymianę uszkodzonego urządzenia na sprawne. Wysyłka następnego dnia roboczego po stwierdzeniu uszkodzenia.
5. Wsparcie techniczne oraz szkolenie z produktu, prowadzone są w języku polskim przez certyfikowanego przez producenta trenera.
6. Wykonawca musi zatrudniać co najmniej 3 certyfikowanych przez producenta inżynierów, świadczących wsparcie dla powyższego urządzenia
	1. **FIREWALL – szt. 1**

**OGÓLNE:**

1. Rozwiązanie musi być dostępne jako platforma sprzętowa.
2. Rozwiązanie musi posiadać zintegrowany system operacyjny, tzn. nie może wymagać
od użytkownika instalacji osobnego systemu operacyjnego.
3. Rozwiązanie posiada nielimitowaną licencję dla użytkowników Firewalla.
4. Minimalna przepustowość firewalla to co najmniej 3,9 Gbps.
5. Rozwiązanie musi obsługiwać do 300000 sesji równoległych.
6. Rozwiązanie łączy w sobie:
	1. zaporę sieciową z inspekcją stanu pakietów (stateful inspection firewall),
	2. system IPS/IDS pozwalający całkowite wyładowane z systemu,
	3. filtr warstwy 7,
	4. serwer VPN,
	5. HTTP Proxy, wraz z co najmniej 50 kategoriami tematycznymi,
	6. filtr antyspamowy.
7. Rozwiązanie ma mieć modułową budowę, pozwalającą na odinstalowanie/ zainstalowanie, wyłączenie/włączenie każdego z modułów rozwiązania bez restartowania rozwiązania.
8. Rozwiązanie ma zapewniać ochronę przed atakami typu DoS/DDoS: IP spoofing. SYN flooding, flood ping i innymi, oraz przed skanowaniem portów i adresów.
9. Rozwiązanie ma usługiwać:
	1. NAT, PAT, proxy arp, VLAN,
	2. Protokoły VoIP – H.323, SIP, SCCP,
	3. Protokoły OSPF, RIP zarówno przy połączeniach IP jak i VPN.
10. Rozwiązanie ma umożliwiać pełne zdalne zarządzania firewallem, serwerem VPN
oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej
pod systemami MS Windows.
11. Rozwiązanie musi posiadać możliwość przeglądania zmian nanoszonych przez automatyczne aktualizacje systemu, z graficznej konsoli administracyjnej.
12. Rozwiązanie ma umożliwiać zarządzanie urządzeniem poprzez zdalne kody SMS.
13. Rozwiązanie musi umożliwiać generowanie statystyk w czasie rzeczywistym – opóźnienie statystyk ma być nie większe niż 10 sekund.
14. Aktywne powiadomienia o zdarzeniach przez SMTP i SNMP.
15. Możliwość ustawienia żądania potwierdzenia przez administratora odczytania powiadomienia o krytycznym zdarzeniu (w systemie pozostaje informacja, który administrator odczytał i skasował ostrzeżenie o zdarzeniu krytycznym).
16. Rozwiązanie musi umożliwiać przesyłanie statystyk i/lub logów na serwer centralnego zarządzania.
17. Urządzenie musi umożliwiać sprawdzanie w czasie rzeczywistym statusu: działających usług, łącz internetowych, czy statusu switchy, za pomocą wbudowanego mechanizmu.
18. Rozwiązanie ma mieć możliwość zarządzania systemem przez wielu administratorów
w jednym czasie.
19. Rozwiązanie ma zapewniać integrację z usługami katalogowymi Active Directory, LDAP, Radius, domena NT 4.
20. Ponadto, rozwiązanie ma zapewniać obsługę: RSA SecureID, TACACS+ przez usługi firewall, serwer VPN, proxy HTTP (działające na wielu procesorach), proxy FTP, proxy SSH oraz uwierzytelnianie administratorów.
21. Rozwiązanie ma zapewnić obsługa uwierzytelniania administratorów przy pomocy hasła (lokalnego lub synchronizowanego z usługą katalogową), klucza zapisanego na tokenie lub karcie kryptograficznej albo równocześnie przy pomocy i hasła, i klucza.
22. Wymagana możliwość obsługi klastra High Availability z możliwością pracy
w trybach Active-Passive i Active-Active.
23. Urządzenie ma pozwalać na stworzenie dedykowanego linku, służącego tylko
do monitorowania stanu partnera w klastrze High Availability.
24. Urządzenie musi mieć możliwość łączenia wielu kart sieciowych w jedną logiczną kartę sieciową w celu zwiększenia przepustowości.
25. Rozwiązanie musi umożliwiać obsługę wybranych kart UMTS/EDGE/HSDPA.
26. Czas pełnej instalacji lub odtworzenia systemu zapory sieciowej po awarii jest
nie większy niż 10 minut.
27. Rozwiązanie ma zapewniać możliwość uruchamiania własnych skryptów z poziomu CLI.
28. Urządzenie ma posiadać bazę predefiniowanych skryptów, do dyspozycji administratora, dostępnych z poziomu CLI.
29. Rozwiązanie ma zezwalać na uruchamianie skryptów zgodnie z przyjętym harmonogramem lub w chwili pojawienia się odpowiedniego zdarzenia na urządzeniu.
30. Możliwość zarządzania systemem przez większą liczbę administratorów
o określonych uprawnieniach.

**FIREWALL:**

1. Urządzenie musi posiadać personal firewall, obsługujący wszystkie połączenia wychodzące i przychodzące do usług zainstalowanych na urządzeniu.
2. Rozwiązanie musi umożliwiać tworzenie obiektów dynamicznych, zależnych od miejsca,
w którym zostało zainstalowane urządzenie.
3. Rozwiązanie ma umożliwiać tworzenie reguł firewalla z mechanizmem TCP Proxy.
4. Rozwiązanie ma pracować w trybie bridge (transparentnym), routera, oraz mieszanym (równocześnie jako bridge i router).
5. Rozwiązanie musi umożliwiać tworzenie reguł NAT wewnątrz reguły tworzonej
na firewallu.
6. Urządzenie ma umożliwiać podzielenie reguł firewalla na logiczne grupy, pomiędzy którymi występują kaskadowe połączenia.
7. Urządzenie ma umożliwiać definiowanie reguł dynamicznych na firewallu, automatycznie wyłączających się po ustalonym czasie.
8. Urządzenie ma umożliwiać tworzenie dynamicznych reguł firewalla uruchamianych
z interfejsu SSL VPN.
9. Wbudowany analizator pakietów (sniffer) uruchamiany z graficznej konsoli użytkownika i z CLI.
10. Wbudowany tester reguł pozwalający na sprawdzenie poprawności i wyników działania tworzonych reguł przed ich aktywacją na firewallu.
11. Rozwiązanie musi posiadać zintegrowany filtr warstwy 7.
12. Rozwiązanie musi pozwalać na blokowanie pojedynczych funkcji konkretnych aplikacji (np. blokowanie tylko transfery plików w Gadu-Gadu, lub przepuszczania tylko
i wyłącznie aktualizacji programów pracujących w sieci.
13. Rozwiązanie musi mieć możliwość transparentnego skanowania ruchu zaszyfrowanego (MITM).

**VPN:**

1. Rozwiązanie musi posiadać własny protokół dla tuneli VPN site-2-site i client-2-site.
2. Rozwiązanie musi posiadać możliwość tworzenia specjalnych tuneli VPN opartych
o autorski protokół, służących do zarządzania urządzeniami, niezależnie od głównego tunelu VPN.
3. Rozwiązanie ma zapewnić możliwość budowy kanałów VPN w strukturze gwiaździstej
z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami – minimalna liczba kanałów VPN zapewniających pełną komunikację pomiędzy wszystkimi lokalizacjami nie powinna być większa niż liczba lokalizacji.
4. Rozwiązanie ma obsługiwać multitransport VPN – tworzenie do 24 transportów
w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień.
5. Rozwiązanie ma zapewnić możliwość łączenia transportów VPN (agregacja łączy
na poziomie pakietów lub sesji) i wyznaczania transportów zapasowych.
6. Rozwiązanie ma umożliwiać przypisywanie ruchu do wybranego transportu VPN
w zależności od adresu źródłowego, adresu docelowego, portu, protokołu, nazwy uwierzytelnionego użytkownika lub grupy, do której należy oraz dnia tygodnia
i godziny nawiązania połączenia.
7. Rozwiązanie ma zapewniać budowanie tuneli VPN w oparciu o protokoły: TCP, UDP, ESP, TCP i UDP.
8. Rozwiązanie ma zezwalać na nawiązywanie połączeń VPN przechodzących przez serwer proxy HTTPS.
9. Rozwiązanie musi posiadać w standardzie, darmowego klienta NAC integrującego
się z centrum akcji w systemach Windows Vista/7.
10. Dostępne centrum autoryzacji na lokalnym serwerze VPN.
11. Rozwiązanie ma umożliwiać uwierzytelnianie użytkowników VPN za pomocą certyfikatów cyfrowych i/lub logowania.
12. Obsługa urządzeń kryptograficznych (tokenów, kart) współpracujących
z mechanizmem Microsoft Strong Credential Provider dla systemu Windows.
13. Klient VPN musi mieć możliwość wyświetlania tekstu powitalnego przy połączeniu
do sieci korporacyjnej (tzw. MOTD).
14. Klient VPN musi mieć możliwość sprawdzania jak i modyfikowania rejestru systemu Windows komputera, na którym jest zainstalowany.
15. Klient VPN musi być stworzony przez tą samą firmę co dostarczone rozwiązanie.
16. Obsługa uwierzytelniania wieloskładnikowego w kliencie VPN.
17. Rozwiązanie ma umożliwiać przydzielanie ustawień tunelu VPN client-to-site
na podstawie przynależności użytkownika do grupy zabezpieczeń w usłudze katalogowej Active Directory lub LDAP.
18. Możliwość uwierzytelniania certyfikatem X.509 przy integracji z zewnętrzną infrastrukturą PKI i przydzielanie ustawień tunelu VPN client-to-site w zależności
od atrybutów certyfikatu.
19. Klient VPN ma być dedykowany na platformy: Windows, Linux.
20. Klient VPN musi posiadać graficzny interfejs użytkownika.
21. Możliwość zdefiniowania na platformach Windows skrótu do połączenia VPN
z ukrytymi wszystkimi opcjami konfiguracyjnymi.
22. Obsługa uwierzytelniania stron przy tworzeniu tuneli VPN typu site-to-site oraz client-to-site za pomocą certyfikatów X.509 ze struktury PKI zarządzanej przez dowolny serwer PKI z obsługą list CRL.
23. Rozwiązanie ma zapewniać możliwość zarządzania pasmem w ramach tunelu VPN
i na każdym tunelu VPN z osobna.
24. Rozwiązanie ma automatycznie zmieniać polityki podziału pasma w tunelach VPN
po awarii jednego z transportów VPN i przełączenia ruchu na transport zapasowy.
25. Rozwiązanie ma zapewniać kompresję i deduplikację danych przesyłanych w tunelach VPN.
26. Rozwiązanie ma mieć możliwość buforowania danych przesyłanych w tunelach VPN
dla protokołów zdefiniowanych przez administratora.
27. Rozwiązanie ma automatycznie zmieniać trasowanie ruchu VPN w przypadku awarii tunelu VPN.

**SIEĆ:**

1. Rozwiązanie ma mieć mechanizm pozwalający na aktywacje nowej konfiguracji sieci na co najmniej trzy sposoby z czego jeden z nich nie może zrywać aktywnych sesji na urządzeniu.
2. Rozwiązanie ma automatycznie przywracać ostatnią działającą konfigurację sieci po zdefiniowanym czasie od momentu utracenia połączenia administracyjnego.
3. Rozwiązanie ma obsługiwać:
	1. kilka łączy internetowych równocześnie, w tym multipath routing,
	2. łączy z dynamicznie przypisywanymi adresami IP,
	3. DynDNS.
4. Rozwiązaniu musi umożliwiać automatyczne przekierowanie ruchu na łącze zapasowe w przypadku awarii łącza głównego.
5. Możliwość podziału łącza w oparciu o wirtualne drzewa decyzyjne dla każdego z użytkowników z osobna lub dla grup użytkowników oraz możliwość ustawiania priorytetów (traffic shaping).
6. Obsługa dynamicznego (priorytety ruchu) i statycznego (ograniczenie maksymalnej przepustowości) podziału pasm.

**SPRZĘT :**

1. Urządzenie musi posiadać co najmniej 8 interfejsów sieciowych (10/100/1000 MBit RJ45).
2. Urządzenie musi posiadać 1 gniazdo pozwalające na uzupełnienie ich o moduły rozszerzeń.
3. Urządzenie musi posiadać możliwość montażu następujących modułów rozszerzeń
w gniazda:
	1. moduł zawierający co najmniej 8 portów 10/100/1000 MBit RJ45,
	2. moduł zawierający co najmniej 4 porty 1 GbE Fibre SFP,
	3. moduł zawierający co najmniej 2 porty 10 GbE Fibre SFP.
4. Urządzenie musi posiadać co najmniej 2 rdzeniowy procesor.
5. Urządzenie musi posiadać co najmniej 4 GB pamięci operacyjnej RAM.
6. Urządzenie musi posiadać dysk SSD o pojemności co najmniej 80 GB.
7. Urządzenie musi posiadać dysk flash o pojemności co najmniej 128 MB.
8. Urządzenie musi posiadać wyświetlacz LCD umożliwiający wyświetlanie co najmniej
2 linii tekstu po 20 znaków każda.
9. Urządzenie musi posiadać co najmniej 2 złącza USB 2.0.
10. Wielkość urządzenie nie może przekraczać 1U.

**SERWIS:**

1. Oferowane urządzenie musi posiadać minimum czteroletnią gwarancję i wsparcie techniczne obejmującą wszystkie elementy urządzenia.
2. W czasie trwania gwarancji zamawiający ma prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade).
3. Wykonawca zapewni wymianę uszkodzonego urządzenia na sprawne. Wysyłka następnego dnia roboczego po stwierdzeniu uszkodzenia.
4. W czasie trwania gwarancji zamawiający ma dostęp do wsparcia technicznego świadczonego w dni robocze od poniedziałku do piątku w godzinach 8:00-18:00.
5. Wsparcie techniczne oraz szkolenie z produktu, prowadzone są w języku polskim przez certyfikowanego przez producenta trenera.
6. Wykonawca musi zatrudniać co najmniej 3 certyfikowanych przez producenta inżynierów, świadczących wsparcie dla powyższego urządzenia
	1. **CENTRALNE ZARZĄDZANIE- szt. 1**

**OGÓLNE:**

1. Rozwiązanie musi być dostępne jako platforma sprzętowa, jak i maszyna wirtualna kompatybilna z rozwiązaniem VMware vSphere oraz Citrix XenServer.
2. Rozwiązanie ma umożliwiać scentralizowane zarządzanie wieloma różnymi urządzeniami typu firewall.
3. Rozwiązanie musi posiadać zintegrowany system operacyjny, tzn. nie może wymagać
od użytkownika instalacji osobnego systemu operacyjnego.
4. Rozwiązanie musi działać w dwóch instancjach:
	1. systemu operacyjnego, na którym uruchamiane są usługi centralnego zarządzania,
	2. serwera centralnego zarządzania, na którym istnieje możliwość konfigurowania poszczególnych usług.
5. Rozwiązanie musi posiadać personal firewall, który będzie filtrować wszystkie połączenia przychodzące/wychodzące do/z usług uruchomionych na urządzeniu.
6. Rozwiązanie ma mieć modułową budowę, pozwalającą na odinstalowanie/ zainstalowanie, wyłączenie/włączenie każdego z modułów rozwiązania bez restartowania rozwiązania.
7. Wymagana możliwość obsługi klastra High Availability z możliwością pracy
w trybach Active-Passive.
8. Urządzenie ma zezwalać na stworzenie dedykowanego linku służącego tylko
do monitorowania stanu partnera w klastrze High Availability.
9. Czas pełnej instalacji lub odtworzenia systemu zapory sieciowej po awarii sprzętu wynosi do 10 minut.
10. Rozwiązanie ma posiadać możliwość uruchamiania własnych skryptów z poziomu CLI.
11. Rozwiązanie ma posiadać bazę predefiniowanych skryptów, do dyspozycji administratora, dostępnych z poziomu CLI.
12. Rozwiązanie ma pozwalać na uruchamiania skryptów zgodnie z przyjętym harmonogramem lub w chwili pojawienia się, odpowiedniego zdarzenia na urządzeniu.
13. Rozwiązanie ma posiadać wbudowany serwer syslog.
14. Rozwiązanie ma dawać możliwość zarządzania systemem przez większą liczbę administratorów o określonych uprawnieniach.
15. Dostęp do urządzenia ma być możliwy za pomocą dedykowanego przez producenta narzędzia do centralnego zarządzania w trybie graficznym.
16. Administrator ma mieć możliwość dokonywania zdalnej konfiguracji i kontrolowania urządzenia za pomocą pojedynczego interfejsu. Ustawień związanych m.in.
z: bezpieczeństwem, ustawieniami reguł na firewallu, zarządzaniem ruchem, politykami dostępu, parametrami systemów operacyjnych, parametrami routingu.

**SYSTEM CENTRALNEGO ZARZĄDZANIA:**

1. Rozwiązanie musi mieć możliwość hierarchicznego zarządzania urządzeniami
w środowisku, pozwalające na stworzenie co najmniej struktury: Kraj > Województwo > Miasto (miastem jest fizyczne urządzenie).
2. Uwierzytelnianie administratorów ma odbywać się w oparciu o silne szyfrowanie
oraz szyfrowanie AES.
3. Rozwiązanie musi posiadać moduł zarządzania uprawnieniami administratorów, pozwalający na zdefiniowanie uprawnień dla każdego z administratorów z osobna.
4. Rozwiązanie ma mieć możliwość definiowania różnych uprawnień administracyjnych
i delegowania ich na poszczególne jednostki lub lokalizacje.
5. Rozwiązanie musi dawać możliwość ukrywania wybranych opcji konfiguracyjnych, wybranym administratorom.
6. Rozwiązanie ma posiadać możliwość integracji z usługami katalogowymi Active Directory, LDAP, Radius, domeną NT 4, oraz obsługą: RSA SecureID,
do uwierzytelniania administratorów.
7. Rozwiązanie musi mieć możliwość tworzenia szablonów konfiguracyjnych
dla poszczególnych modułów.
8. Rozwiązanie musi posiadać dedykowany moduł pozwalający na dystrybucję aktualizacji do zarządzanych urządzeń. Moduł aktualizacji musi posiadać swój odrębny interfejs dostępny z programu do zarządzania.
9. Rozwiązaniem ma mieć możliwość zdalnego kontrolowania wersji i aktualizacji silników: antyspamu, antywirusa, filtra zawartości, NACa.
10. Rozwiązanie ma mieć możliwość centralnego zarządzania oraz przeglądania statystyk
z podległych mu urządzeń.
11. Rozwiązanie musi pozwalać na przesyłanie logów z podległych urządzeń na serwer centralnego zarządzania.
12. Rozwiązania ma posiadać system wersjonowania konfiguracji, pozwalający na porównanie zmian dokonanych w konfiguracji oraz na przywrócenie konfiguracji historycznej, dla pojedynczej jednostki konfiguracyjnej (np.: właściwości usługi VPN, właściwości usługi firewalla, zestaw reguł itp).
13. Rozwiązanie ma archiwizować konfigurację podległych mu urządzeń.
14. Rozwiązanie ma umożliwiać tworzenie tuneli VPN metodą drag&drop.
15. Rozwiązanie ma mieć wbudowany graficzny edytor konfiguracji tuneli VPN.
16. Graficzny edytor tuneli VPN musi mieć możliwość swobodnego układania serwerów VPN w interfejsie.
17. Interfejs graficznego edytora tuneli VPN musi mieć możliwość pracy w trybie pełnoekranowym, oraz mieć możliwość swobodnego oddalania i przybliżania mapy
z serwerami VPN.
18. Rozwiązanie ma mieć możliwość tworzenia wizualizacji w czasie rzeczywistym,
statusów tuneli VPN.
19. Rozwiązanie ma mieć możliwość zarządzania strukturą składającą się z urządzeń podległych pracujących pod kontrolą różnych wersji produktu.
20. Rozwiązanie ma posiadać dedykowane konsole do:
	1. sprawdzania ogólnego statusu urządzeń podległych,
	2. wizualizacji podległych urządzeń na mapach świata,
	3. sprawdzania statusu ostatniej wysłanej aktualizacji konfiguracji,
	4. wizualizacji aktualnie aktywnych sesji administracyjnych,
	5. wizualizacji statusu aktywacji urządzeń,
	6. wysyłania aktualizacji oprogramowania do podległych urządzeń,
	7. uruchamiania aktualizacji oprogramowania na podległych urządzeniach.
21. Rozwiązanie ma umożliwiać zarządzanie licencjami oraz podgląd ich stanu
z poziomu systemu centralnego zarządzania.
22. Rozwiązanie ma zapewnić możliwość przeglądania zdarzeń, które wystąpiły
na zarządzanych urządzeniach.
23. Rozwiązanie ma przesyłać zdarzeń za pomocą SMTP lub SNMP.
24. Rozwiązanie ma umożliwiać scentralizowane zarządzanie certyfikatami i kluczami podległych urządzeń.
25. Rozwiązanie ma budować dedykowany tunel VPN do komunikacji i zarządzania, pomiędzy systemem centralnego zarządzania, a urządzeniem końcowym. Nawiązywane połączenie odbywa się przy użyciu tunelu opracowanego przez producenta sprzętu.
26. Rozwiązanie ma umożliwiać definiowania wirtualnych adresów IP w obrębie specjalnego tunelu VPN służącego do komunikacji pomiędzy systemem centralnego zarządzania
a klientem końcowym.
27. Urządzenie ma umożliwiać bezpieczne zdalne zarządzanie plikami wykonywalnymi, szyfrowanymi za pomocą SSHV2.
28. Rozwiązanie ma mieć możliwość dostosowania widoku drzewa konfiguracyjnego
i stworzenia własnych widoków.
29. Rozwiązanie ma posiadać serwer czasu NTP.
30. Wszystkie funkcjonalności mają być dostępne za pomocą autorskiego interfejsu graficznego producenta urządzenia.

**SERWIS:**

1. Oferowane urządzenie musi posiadać minimum czteroletnią gwarancję i wsparcie techniczne obejmującą wszystkie elementy urządzenia.
2. W czasie trwania gwarancji zamawiający ma prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade).
3. Wykonawca zapewni wymianę uszkodzonego urządzenia na sprawne. Wysyłka następnego dnia roboczego po stwierdzeniu uszkodzenia.
4. W czasie trwania gwarancji zamawiający ma dostęp do wsparcia technicznego świadczonego w dni robocze od poniedziałku do piątku w godzinach 8:00-18:00.
5. Wsparcie techniczne oraz szkolenie z produktu, prowadzone są w języku polskim przez certyfikowanego przez producenta trenera.
6. Wykonawca musi zatrudniać co najmniej 3 certyfikowanych przez producenta inżynierów, świadczących wsparcie dla powyższego urządzenia.
7. **ZAKRES WDROŻENIA PLATFORMY**
	1. **Konfiguracja urządzeń i usług:**
8. Konfiguracja usługi DHCP Relay, w sposób umożliwiający na otrzymywanie adresów IP z jednego centralnego serwera DHCP. Usługa DHCP Relay musi być skonfigurowana
w taki sposób, aby centralny serwer DHCP rozdawał adresy IP
w lokalizacjach. Nie jest dopuszczalne konfigurowanie osobnego serwera DHCP
w każdej z lokalizacji. Konfiguracja usługi umożliwiającej WebFiltering oraz kontrolę przeglądanych przez użytkowników stron WWW zgodnie z zaleceniami zamawiającego.
9. Konfiguracja tuneli VPN pomiędzy lokalizacjami a centralą. Tunele VPN mają zapewniać możliwie jak najwyższą dostępność usług. Wymagana jest konfiguracja
co najmniej dwóch, równocześnie pracujących tuneli pomiędzy lokalizacją a centralą.
W niektórych lokalizacjach wymagana jest agregacja tuneli VPN.
10. **Konfiguracja i wdrożenie na miejscu u klienta.**
11. 1 szt. urządzenia zarządzającego w Centrali Zamawiającego w budynku
przy ul. Leczkowa 1A w Gdańsku.
12. 1 szt. urządzenia firewall w Centrali Zamawiającego w budynku
przy ul. Leczkowa 1A w Gdańsku.
13. 2 szt. urządzeń w dwóch lokalizacjach wybranych przez Zamawiającego.
14. **Szkolenie techniczne**
15. Zamawiający oczekuje szkolenia zamkniętego dla grupy pracowników w siedzibie Zamawiającego.
16. Szkolenie musi być zorganizowane przez Autoryzowane Centrum Szkoleniowe producenta oferowanego sprzętu.
17. Czas szkolenia: 5 dni x 7h.
18. Termin zostanie ustalony w harmonogramie realizacji.
19. Szkolenie : maksymalnie dla 5 osób.
20. Szkolenie musi zapewnić wiedzę pozwalającą na pełne wykorzystanie wdrożonego rozwiązania.
21. Szkolenie musi zakończyć się egzaminem i otrzymaniem certyfikatu producenta.
22. Trener zapewnia niezbędne materiały szkoleniowe oraz wirtualne środowisko
do przeprowadzenia szkolenia.
23. **ZAMÓWIENIA CZĘŚCIOWE:**

Zamawiający nie dopuszcza składania ofert częściowych.

1. **OPIS CZĘŚCI ZAMÓWIENIA**

Zamówienie nie zostało podzielone na części.

1. **TERMIN WYKONANIA ZAMÓWIENIA**

Termin wykonania zamówienia – od 27 września 2013 r. – 26 września 2017 r.

1. **WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW:**
2. W postępowaniu mogą wziąć udział wykonawcy, którzy spełniają warunki udziału
w postępowaniu, o których mowa w art. 22 ust. 1 ustawy Prawo zamówień publicznych:
	1. posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania:
* Warunek ten zostanie spełniony /w przypadku istnienia takiego wymogu
w stosunku do technologii objętej przedmiotem niniejszego postępowania
(tzw. produkty podwójnego zastosowania)/ jeżeli wykonawca wykaże, że przy wprowadzeniu na terytorium Polski przedmiotowej technologii 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 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.
	1. posiadają wiedzę i doświadczenie do wykonania zamówienia;
	2. dysponują odpowiednim potencjałem technicznym oraz osobami zdolnymi
	do wykonania zamówienia:
* Warunek ten zostanie spełniony, jeżeli wykonawca wykaże, że dysponuje aktywnym kontem poczty elektronicznej e-mail;
* Warunek ten zostanie spełniony, jeżeli wykonawca wykaże, że dysponuje osobami zapewniającymi wsparcie techniczne, posiadającymi certyfikat producenta urządzenia.
	1. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 ustawy.

W postępowaniu mogą wziąć udział wykonawcy, którzy spełniają warunek udziału
w postępowaniu dotyczący braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego w okolicznościach, o których mowa w art. 24 ust. 2 pkt 5 ustawy.

W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, każdy
z warunków określonych w pkt 1.1) - 1.4) winien spełniać co najmniej jeden z tych wykonawców albo wszyscy ci wykonawcy wspólnie.

Warunki określone w pkt 2 i 3 powinien spełniać każdy z wykonawców samodzielnie.

Wykonawca powołujący się przy wykazywaniu spełnienia warunków udziału
w postępowaniu na potencjał innych podmiotów, które będą brały udział w realizacji części zamówienia, przedkłada pisemne zobowiązanie innych podmiotów do oddania mu
do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia.

1. **WYKAZ OŚWIADCZEŃ I DOKUMENTÓW, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU**
	* 1. W celu potwierdzenia spełniania warunków udziału w postępowaniu, o których mowa
		w art. 22 ust. 1 ustawy Pzp, do oferty należy załączyć następujące dokumenty w formie oryginału lub kopii poświadczonych za zgodność z oryginałem przez Wykonawcę
		lub osobę upoważnioną, z zachowaniem sposobu reprezentacji:
	1. Oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu określonych art. 22 ust.1 Pzp według wzoru stanowiącego załącznik nr 2 do SIWZ (oryginał);
	2. Wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia (Wykaz Certyfikatowanych Inżynierów) według wzoru stanowiącego załącznik nr 4
	do SIWZ;
	3. Oświadczenie o posiadaniu aktywne konta poczty elektronicznej (e-mail) poprzez podanie adresu w ofercie.
	4. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), wykonawca winien jest przedłożyć:
	5. 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.);
	6. 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.
	7. W przypadku, gdy technologia objęta przedmiotem niniejszego postępowania
	nie wyczerpuje definicji tzw. produktu podwójnego zastosowania wykonawca winien jest złożyć oświadczenie, z którego treści jednoznacznie będzie wynikał brak obowiązku posiadania dokumentów, o których mowa w ust. 4.

W przypadku oferty składanej przez wykonawców ubiegających się wspólnie
o udzielenie zamówienia publicznego, oświadczenie o spełnianiu każdego z warunków,
o których mowa w art. 22 ust. 1 ustawy składa co najmniej jeden z tych wykonawców albo wszyscy ci wykonawcy wspólnie.

* + 1. W celu wykazania spełnienia warunku udziału w postępowaniu dotyczącego braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego wykonawcy w okolicznościach, o których mowa w art. 24 ust. 1 ustawy Pzp należy złożyć następujące dokumenty w formie oryginału lub kopii poświadczonych
		za zgodność z oryginałem przez wykonawcę lub osobę upoważnioną, z zachowaniem sposobu reprezentacji:
1. Oświadczenie o braku podstaw do wykluczenia z postępowania z powodu niespełnienia warunków, o których mowa w art. 24 ust.1 ustawy Pzp, według wzoru stanowiącego załącznik nr 3 do SIWZ;
2. Aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji
o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert.

Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, przedkłada dokument wystawiony w kraju, w którym
ma siedzibę lub miejsce zamieszkania potwierdzający, że nie otwarto jego likwidacji ani nie ogłoszono upadłości - wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert.

W przypadku oferty składanej przez wykonawców ubiegających się wspólnie
o udzielenie zamówienia publicznego, dokumenty potwierdzające, że Wykonawca
nie podlega wykluczeniu składa każdy z wykonawców oddzielnie.

* + 1. W celu wykazania spełnienia warunku udziału w postępowaniu dotyczącego braku podstaw do wykluczenia z postępowania o udzielenie zamówienia wykonawcy
		w okolicznościach, o których mowa w art. 24 ust. 2 pkt 5 ustawy należy złożyć następujące dokumenty w formie oryginału lub kserokopii poświadczonej za zgodność
		z oryginałem przez Wykonawcę lub osobę upoważnioną z zachowaniem sposobu reprezentacji:
1. Listę podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy Pzp w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów albo informacji o tym, że nie należy do grupy kapitałowej według wzoru stanowiącego załącznik nr 5 do SIWZ.
	* 1. **Inne wymagane dokumenty:**

Dokument, z którego wynika upoważnienie wykonawcy do podpisania oferty (oryginał lub poświadczona zgodnie z zasadą reprezentacji „za zgodność
z oryginałem” kopia) lub pełnomocnictwo do reprezentowania wykonawcy, o ile ofertę składa pełnomocnik (oryginał lub poświadczona notarialnie „za zgodność
 z oryginałem” kopia).

**Zamawiający przypomina, że z treści oferty i załączonych do niej dokumentów powinno wynikać jednoznacznie, że osoba/y, która/e ją podpisała/y jest/są do tego upoważniona/e, pod rygorem nieważności oferty.**

# INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI.

1. Postępowanie o udzielenie zamówienia prowadzone jest w języku polskim,
z zachowaniem formy pisemnej.
2. Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują pisemnie.
3. Zamawiający dopuszcza składanie oświadczeń, wniosków i zawiadomień za pomocą poczty elektronicznej, pod warunkiem niezwłocznego potwierdzenia treści korespondencji na piśmie z własnoręcznym podpisem. W przypadku przesyłania korespondencji pocztą elektroniczną, każda ze stron zobowiązana jest na żądanie drugiej niezwłocznie potwierdzić fakt ich otrzymania. W przypadku braku potwierdzenia otrzymania pisma przez Wykonawcę Zamawiający domniema, iż pismo wysłane przez Zamawiającego
na adres poczty elektronicznej podany przez Wykonawcę zostało mu doręczone w sposób umożliwiający zapoznanie się Wykonawcy z treścią pisma.
4. Forma pisemna jest zastrzeżona do złożenia oferty wraz załącznikami, w tym oświadczeń
i dokumentów potwierdzających spełnienie warunków udziału w postępowaniu, oświadczeń o braku podstaw do wykluczenia, listy podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy/informacji o tym, że wykonawca nie należy do grupy kapitałowej oraz pełnomocnictw.
5. Wykonawca może zwrócić się na piśmie do Zamawiającego o wyjaśnienie SIWZ. Zamawiający udzieli wyjaśnień, jeżeli wniosek wpłynie do niego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Zamawiający udzieli wyjaśnień wszystkim Wykonawcom, którym doręczono SIWZ.
6. W szczególnie uzasadnionych przypadkach zamawiający może w każdym czasie, przed upływem terminu do składania ofert, zmodyfikować treść niniejszej specyfikacji. Dokonaną w ten sposób modyfikację przekaże niezwłocznie wszystkim wykonawcom, którym przekazano SIWZ.
7. Zamawiający przedłuży termin składania ofert z uwzględnieniem czasu niezbędnego
do wprowadzenia w ofertach zmian wynikających z modyfikacji treści SIWZ.
O przedłużeniu terminu składania ofert zamawiający niezwłocznie zawiadomi wykonawców. W tym przypadku wszelkie prawa i zobowiązania Zamawiającego
i Wykonawcy odnośnie wcześniej ustalonego terminu będą podlegały nowemu terminowi.
8. Osobą uprawnioną do porozumiewania się z Wykonawcami jest: **Marcin Zawisza -
 tel. 58 342-31-58.**
9. Korespondencję wysyłaną pocztą elektroniczną prosimy kierować na adres: **dyrekcja@mopr.gda.pl**.

Korespondencja będzie wysyłana z adresu m.zawisza@mops.gda.pl, który nie służy
do przesyłania korespondencji przez Wykonawców. Korespondencja przesłana na ten adres nie będzie rejestrowana i rozpatrywana.

# WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie wymaga wniesienia wadium.

# TERMIN ZWIĄZANIA OFERTĄ

Wykonawca jest związany ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Wykonawca samodzielnie lub na wniosek zamawiającego może przedłużyć termin związania ofertą, z tym że zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą zwrócić się do wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

# OPIS SPOSOBU PRZYGOTOWYWANIA OFERTY

Zamawiający wymaga, aby Wykonawca sporządził ofertę zgodnie z poniższym opisem.

* + - 1. Zamawiający wymaga, aby:
1. Wykonawca zapoznał się ze wszystkimi rozdziałami składającymi się na SIWZ;
2. Każdy Wykonawca złożył tylko jedną ofertę;
3. Oferta była sporządzona w języku polskim (dokumenty sporządzone w języku obcym powinny być złożone wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę);
4. Oferta obejmowała całość przedmiotu zamówienia;
5. Wykonawca poniósł wszelkie koszty związane z przygotowaniem i złożeniem oferty;
6. Oferta była napisana na maszynie lub komputerze, ewentualnie odręcznie;
7. Formularz oferty był wypełniony przez Wykonawcę bez dokonywania w nim zmian. Załączniki dołączone do SIWZ przedstawione są w formie wzoru graficznego. Wykonawca może przedstawić je wg własnego układu graficznego, lecz muszą one zawierać wszystkie zapisy i informacje ujęte we wzorach;
8. Wszystkie strony oferty, a także wszelkie miejsca, w których naniesiono zmiany (poprawki) były podpisane przez upoważnionego/nych przedstawiciela/li Wykonawcy. Osobą/ami upoważnioną/ymi do reprezentowania Wykonawcy będą osoby wskazane odpowiednio: w odpisie z właściwego rejestru, aktualnym zaświadczeniu o wpisie do ewidencji działalności gospodarczej lub które upoważniono do reprezentowania w niniejszym postępowaniu w zakresie udzielonego pełnomocnictwa;
9. Wykonawca wskazał, którą część zamówienia zamierza powierzyć podwykonawcom.
10. Jeżeli oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, Wykonawca winien w sposób
nie budzący wątpliwości zastrzec, które spośród zawartych w ofercie informacji stanowią tajemnicę przedsiębiorstwa. Informacje te będą umieszczone w osobnej wewnętrznej kopercie, odrębnie od pozostałych informacji zawartych w ofercie
i oznaczone klauzulą „Tajemnica przedsiębiorstwa”.

Poprzez „tajemnicę przedsiębiorstwa” rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa
lub inne informacje posiadające wartość gospodarczą, co do których Przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności – art. 11 ust. 4 ustawy
z dnia 16 kwietnia 1993 r.- o zwalczaniu nieuczciwej konkurencji (tekst jednolity
Dz. U. z 2003 r. Nr 153, poz. 1503).

1. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Pzp.
2. Wszystkie strony oferty były ze sobą połączone w sposób trwały, uniemożliwiający jej naruszenie (z uwzględnieniem sytuacji opisanej w pkt. 10).
3. Wykonawca musi umieścić ofertę wraz ze wszystkimi załącznikami w prawidłowym, zamkniętym opakowaniu, w sposób gwarantujący zachowanie w poufności jej treści
oraz zabezpieczający jej nienaruszalność do terminu otwarcia ofert. Poprzez prawidłowe opakowanie oferty, w tym także zamknięcie, należy rozumieć taki sposób zabezpieczenia treści oferty, który uniemożliwia osobom postronnym, czyli jakiejkolwiek osobie, zapoznanie się przed upływem terminu otwarcia ofert – zgodnie z art. 86 ust. 1 i 2 ustawy, z jakimkolwiek elementem treści oświadczeń złożonych przez Wykonawcę.
4. Wykonawca zamieścił ofertę w kopercie (opakowaniu), która będzie posiadać następujące oznaczenie:

Miejski Ośrodek Pomocy Rodzinie w Gdańsku,

**ul. Konrada Leczkowa 1A, 80-432 Gdańsk,**

**Oferta na:**

#### na dostawę, instalację, wdrożenie wraz ze wsparciem technicznym platformy

#### sprzętowej firewall z pełnym zdalnym zarządzaniem oraz szkoleniem z zakresu zarządzania w ramach dostarczonego rozwiązania

#### Nie otwierać przed 19.08.2013 r. godzina 10:10

Poza oznaczeniem podanym powyżej, koperta (opakowanie) musi posiadać nazwę i adres wykonawcy, aby ofertę złożoną po terminie można było zwrócić bez otwierania.

1. Wykonawca prawidłowo oznaczył ofertę. Niewłaściwe oznaczenie opakowania zawierającego ofertę spowoduje odrzucenie oferty, jeżeli braki lub błędy w tym zakresie uniemożliwią prawidłowe otwarcie oferty, (np. z powodu braku oznaczenia „Oferta na ...” lub „nie otwierać przed ...” w przypadku przekazania oferty
np. poprzez pocztę, Kancelaria MOPR w Gdańsku może dokonać jej otwarcia przed wyznaczonym terminem, zgodnie z zasadami obowiązującymi w Ośrodku dotyczącymi korespondencji, - co spowoduje odrzucenie oferty).
2. Wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę przed terminem składania ofert, pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmian lub wycofaniu. Powiadomienie
o wprowadzeniu zmian lub wycofaniu zostanie przygotowane i oznaczone zgodnie
z postanowieniami pkt 14), a koperta będzie dodatkowo oznaczona „ZMIANA”
lub „WYCOFANIE”.

Na ofertę składają się:

* 1. Wypełniony Formularz ofertowy stanowiący załącznik nr 1 do niniejszej SIWZ;
	2. Dokumenty wymienione w rozdziale VII niniejszej SIWZ;
	3. Pełnomocnictwo do reprezentowania Wykonawcy w postępowaniu dla osoby podpisującej ofertę, o ile ofertę składa pełnomocnik.

# MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1. Termin składania ofert upływa **w dniu 19.08.2013 r. o godzinie 1000**.
2. Otwarcie ofert nastąpi **w dniu 19.08.2013 r. o godzinie 1010**
w siedzibie Zamawiającego w **pok. 13**. **(parter przy ul. Konrada Leczkowa 1A)**
3. Ofertę należy złożyć w:

**Miejskim Ośrodku Pomocy Rodzinie w Gdańsku**

**ul. Konrada Leczkowa 1A, 80-432 Gdańsk,**

**Kancelaria ogólna - pok. nr 4**

1. Złożenie oferty w miejscu innym, niż wyżej podane może skutkować nie dotarciem oferty do komisji przetargowej w terminie wyznaczonym na składanie ofert z winy Wykonawcy. Oferta taka, jako złożona po terminie nie będzie brała udziału w postępowaniu.

# OPIS SPOSOBU OBLICZENIA CENY

1. Wykonawca zobowiązany jest skalkulować cenę oferty tak, aby obejmowała wszystkie koszty, jakie Wykonawca może ponieść przy realizacji zamówienia.
2. Ceny należy podać w złotych polskich. Wszystkie wartości należy zaokrąglić do dwóch miejsc po przecinku, zgodnie z obowiązującymi przepisami.
3. Cena oferty określona przez Wykonawcę pozostanie stała w okresie realizacji umowy
i nie będzie podlegała zmianom.

# OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW ORAZ SPOSOBU OCENY OFERT

1. Jedynym kryterium oceny ofert jest łączna cena brutto oferty – cena 100%.
2. Kryterium ceny będzie rozpatrywane na podstawie całkowitej wartości usługi podanej przez Wykonawcę w formularzu oferty.
3. Za najkorzystniejszą zostanie uznana oferta, która będzie odpowiadać zasadom określonym w ustawie Pzp, spełni warunki określone w niniejszej SIWZ oraz będzie miała najniższą cenę.
4. Zamawiający poprawia w tekście oferty oczywiste omyłki pisarskie oraz oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek oraz inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujące istotnych zmian w treści oferty, niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.
5. Jeżeli w terminie 3 dni od dnia otrzymania zawiadomienia wykonawca nie zgodzi się
na poprawienie omyłki o której mowa w art. 87 ust. 2 pkt 3 uPzp, jego oferta zostanie odrzucona.

# INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY, W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.

1. W przypadku udzielenia zamówienia konsorcjum (tzn. wykonawcy określonemu
w art. 23 ust. 1 ustawy Pzp) - zamawiający przed podpisaniem umowy zażąda złożenia umowy regulującej współpracę tych wykonawców.
2. Przed podpisaniem umowy zamawiający zażąda niezwłocznego złożenia załączników
do umowy, których sporządzenie zależy od wybranego wykonawcy.

#  WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY.

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

# ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TRESCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, OGÓLNE WARUNKI UMOWY ALBO WZÓR UMOWY, JEŻELI ZAMAWIAJĄCY WYMAGA OD WYKONAWCY, ABY ZAWARŁ Z NIM UMOWĘ W SPRAWIE ZAMÓWIENIA PUBLICZNEGO NA TAKICH WARUNKACH.

Wzór umowy stanowi załącznik nr 6 do niniejszej specyfikacji.

# PRZEWIDYWANE ISTOTNE ZMIANY POSTANOWIEŃ UMOWY.

Nie przewiduje się istotnych zmian postanowień zawartej umowy.

#  INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH UZUPEŁNIAJĄCYCH, O KTÓRYCH MOWA W ART. 67 UST. 1 PKT 6 I 7 USTAWY.

Zamawiający nie przewiduje udzielenie zamówień uzupełniających na podstawie art. 67 ust. 1 pkt 6 ustawy.

# POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA.

Wykonawcom przysługują środki ochrony prawnej zgodnie z przepisami Działu VI ustawy – Prawo zamówień publicznych.

#### Wykaz załączników:

Załącznik nr 1– Formularz ofertowy;

Załącznik nr 2 – Oświadczenie o spełnianiu warunków art. 22 ust. 1 ustawy Pzp;

Załącznik nr 3 – Oświadczenie o braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego
na podstawie art. 24 ust. 1 ustawy Pzp;

Załącznik nr 4 – Wykaz osób;

Załącznik nr 5 – Wzór wykazu/informacji;

Załącznik nr 6 – Wzór umowy.

 **ZATWIERDZAM**

*Wzór formularza oferty*

załącznik nr 1 do specyfikacji istotnych warunków zamówienia

**OFERTA WYKONAWCY**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(pieczęć adresowa Wykonawcy)

Nazwa wykonawcy:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Wykonawców w przypadku oferty wspólnej)

REGON: **|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_| ,** NIP  **|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|\_\_\_|**

Siedziba: (kod, miejscowość, ulica, nr domu, nr lokalu):

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_ , \_\_\_\_\_\_\_\_\_\_\_\_\_\_** ,
Internet: http:// \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

tel.**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ,**

e-mail, na który ma przesyłać korespondencję zamawiający: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*w przypadku oferty wspólnej należy podać dane dotyczące podmiotów występujących wspólnie oraz Pełnomocnika Wykonawcy*

 **Miejski Ośrodek Pomocy Rodzinie
w Gdańsku,**

 **ul. Konrada Leczkowa 1A,**

 **80 – 865 Gdańsk**

W odpowiedzi na ogłoszenie o przetargu nieograniczonym na:

**na dostawę, instalację, wdrożenie wraz ze wsparciem technicznym platformy sprzętowej firewall z pełnym zdalnym zarządzaniem oraz szkoleniem z zakresu zarządzania
w ramach dostarczonego rozwiązania**

oświadczamy, że akceptujemy w całości wszystkie warunki zawarte w Specyfikacji Istotnych Warunków Zamówienia.

1. **SKŁADAMY OFERTĘ** na wykonanieprzedmiotu zamówienia w zakresie określonym w Specyfikacji Istotnych Warunków Zamówienia, zgodnie z opisem przedmiotu zamówienia i wzorem umowy, na następujących warunkach:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Rodzaj** | Jednostka miary | Ilość  | Oferowany typ/model oraz producent | Cena jednostka netto | Stawka Vat | Cena jednostkowa brutto | **Wartość łączna brutto** |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I**(D x H) |
| 1 | **Koszt urządzenia III. cz. 3.1** | szt. | 1 |  |  |  |  |  |
| 2 | **Koszt urządzeń III. cz. 3.2** | szt. | 8 |  |  |  |  |  |
| 3 | **Koszt urządzenia III. cz. 3.3** | szt. | 1 |  |  |  |  |  |
| 4 | **Koszt urządzenia III. cz. 3.4** | szt. | 1 |  |  |  |  |  |
| 5 | **Koszt urządzenia III. cz. 3.5** | szt.  | 1 |  |  |  |  |  |
| 6 | **Koszt wdrożenia i szkolenia pracowników** | szt. | 1 | X |  |  |  |  |
| 7. | **Asysta techniczna rozwiązania na okres 4 lat** | szt. | 1 | X |  |  |  |  |
| **Wartość netto oferty** |  |
| **Wartość VAT (………)** |  |
| **Wartość brutto oferty** |  |

1. Oświadczamy, że powyższa cena brutto zawiera wszystkie koszty, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.
2. Oświadczamy, że akceptujemy warunki płatności określone przez Zamawiającego
w Specyfikacji Istotnych Warunków Zamówienia przedmiotowego postępowania.
3. Oświadczamy, że będziemy realizować przedmiot zamówienia w okresie opisanym
w SIWZ.
4. Oświadczamy, iż przewidujemy/nie przewidujemy\* powierzenie podwykonawcom realizacji zamówienia w części ………………………………………………………….. .
5. Oświadczamy, że jesteśmy związani niniejszą ofertą przez okres 30 dni od dnia upływu terminu składania ofert.
6. Oświadczamy, że niniejsza oferta zawiera na stronach nr od \_\_\_\_ do \_\_\_\_ informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.
7. Oświadczamy, że zapoznaliśmy się z postanowieniami umowy, określonymi
w  Specyfikacji Istotnych Warunków Zamówienia i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach określonych w Specyfikacji Istotnych Warunków Zamówienia, w miejscu i terminie wyznaczonym przez Zamawiającego.
8. Ofertę niniejszą składam na \_\_\_\_\_\_\_\_\_ kolejno ponumerowanych stronach.
9. Wraz z ofertą składamy następujące oświadczenia i dokumenty:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Informacja dla Wykonawcy:*

*Formularz oferty musi być podpisany przez osobę lub osoby upełnomocnione do reprezentowania firmy.*

***\* niepotrzebne skreślić***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_2013 r.

 \_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 podpis osoby(osób) uprawnionej(ych)

 *do reprezentowania Wykonawcy*

*Wzór oświadczenia*

*załącznik nr 2 do specyfikacji istotnych warunków zamówienia*

# Oświadczenie

My, niżej podpisani

.................................................................................................................................................

.................................................................................................................................................

działając w imieniu i na rzecz (nazwa /firma/ i adres Wykonawcy)

.................................................................................................................................................

.................................................................................................................................................

.................................................................................................................................................

oświadczamy, iż spełniamy warunki udziału w postępowaniu, o których mowa w pkt. 7 Specyfikacji Istotnych Warunków Zamówienia, w tym:

1. posiadamy uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
2. posiadamy wiedzę i doświadczenie niezbędne do wykonanie zamówienia;
3. dysponujemy odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia;
4. znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_2013 r.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 podpis osoby(osób) uprawnionej(ych)

 *do reprezentowania Wykonawcy*

Wzór oświadczenia

załącznik nr 3 do specyfikacji istotnych warunków zamówienia

# Oświadczenie

My, niżej podpisani

.................................................................................................................................................

.................................................................................................................................................

działając w imieniu i na rzecz (nazwa /firma/ i adres Wykonawcy)

.................................................................................................................................................

.................................................................................................................................................

.................................................................................................................................................

oświadczamy, iż nie podlegamy wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ust. 1 ustawy Prawo zamówień publicznych.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_2013 r.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 podpis osoby(osób) uprawnionej(ych)

 *do reprezentowania Wykonawcy*

Wzór wykazu osób

Załącznik nr 4 do specyfikacji istotnych warunków zamówienia

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (pieczęć adresowa Wykonawcy)

**Wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia, odpowiedzialnych za wsparcie techniczne, posiadających certyfikat producenta urządzenia wraz z informacją na temat ich podstawie do dysponowania tymi osobami**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Imię i nazwisko | Kwalifikacje / Certyfikaty | Podstawa dysponowania |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| 5. |  |  |  |
| 6. |  |  |  |
| 7. |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_2013 r.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 podpis osoby(osób) uprawnionej(ych)

 *do reprezentowania Wykonawcy*

Wzór listy/informacji

Załącznik nr 6 do specyfikacji istotnych warunków zamówienia

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (pieczęć adresowa Wykonawcy)

**Lista podmiotów należących do tej samej grupy kapitałowej/
informacja o tym, że wykonawca nie należy do grupy kapitałowej\*.**

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego na:

**Świadczenie usługi szkoleniowej na terenie miasta Gdańska dla beneficjentów projektu na dostawę, instalację, wdrożenie wraz ze wsparciem technicznym platformy sprzętowej firewall z pełnym zdalnym zarządzaniem oraz szkoleniem z zakresu zarządzania
w ramach dostarczonego rozwiązania**

zgodnie z art. 26 ust. 2 pkt. 2d ustawy z dnia 29 stycznia 2004 roku - Prawo zamówień publicznych (Dz. U. z 2010 r. Nr 113, poz. 759 z późn. zm.)

1. **składamy listę podmiotów**, razem z którymi należymy do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. Nr 50 poz. 331 z późn. zm.).

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa podmiotu** | **Adres podmiotu** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_2013 r.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 podpis osoby(osób) uprawnionej(ych)

 *do reprezentowania Wykonawcy*

1. **informujemy, że nie należymy do grupy kapitałowej**, o której mowa w art. 24 ust. 2 pkt. 5 ustawy Prawo zamówień publicznych.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_2013 r.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 podpis osoby(osób) uprawnionej(ych)

 *do reprezentowania Wykonawcy*

**\* - należy wypełnić pkt. 1 albo pkt. 2**

*Wzór umowy*

*Załącznik nr 6 do specyfikacji istotnych warunków zamówienia*

**WZÓR**

**Umowa Nr PS.ZZZP.346-26( )/13**

zawarta w dniu ................................ 2013r. pomiędzy:

**Miejskim Ośrodkiem Pomocy Rodzinie w Gdańsku**

**ul. Konrada Leczkowa 1a, 80-432 Gdańsk**

**NIP: 853-20-94-583, Regon: 002837021**

reprezentowanym przez:

**Ewa Wołczak – z-cę Dyrektora Miejskiego Ośrodka Pomocy Rodzinie w Gdańsku**

zwanym dalej **„Zamawiającym”**

a

**…………………………………………**

reprezentowanym przez:

**…………………………………………**

zwanym w dalszej części umowy **,, Wykonawcą"**

Umowę zawarto z Wykonawcą wybranym w wyniku przeprowadzonego postępowania w ramach ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (*Dz. U. Nr 113, poz. 759 z 2010r. ze zm.*) zwanej dalej ustawą, w trybie przetargu nieograniczonego na:  **dostawę, instalację, wdrożenie wraz ze wsparciem technicznym, platformy sprzętowej firewall z pełnym zdalnym zarządzaniem oraz szkoleniem z zakresu zarządzania
w ramach dostarczonego rozwiązania.**

**§ 1**

* + - 1. Przedmiotem Umowy, zwanym dalej „Zamówieniem”, jest realizacja zadań:

1) dostawa, wdrożenie i szkolenia z obsługi platformy sprzętowej firewall, zwanego dalej „Systemem”;

 2) świadczenie usługi wsparcia technicznego Systemu;

zgodnie ze Szczegółowym Opisem Przedmiotu Zamówienia, stanowiącym Załącznik nr 1
do Umowy.

* + - 1. Wykonawca zrealizuje dostawę, wdrożenie oraz szkolenie z obsługi Systemu, o których mowa
			w ust. 1 pkt 1, w terminie 30 dni od dnia zawarcia Umowy.
			2. Usługi wsparcia technicznego Systemu, o których mowa w ust. 1 pkt 2, Wykonawca będzie świadczył przez okres 48 miesięcy od dnia dostawy i wdrożenia Systemu,
			o którym mowa w ust. 2.

**§ 2**

* + - 1. Z tytułu dostarczenia, wdrożenia oraz szkolenia z obsługi Systemu, o których mowa
			w § 1 ust. 1 pkt 1, Wykonawcy przysługuje wynagrodzenie w wysokości ………. zł netto (słownie: ……………… 00/100), co powiększone o należny podatek VAT w wysokości ………….. zł, stanowi kwotę…….. zł (słownie: …..… złotych …./100) brutto.
			2. Za świadczenia usług wsparcia technicznego Systemu, o których mowa w § 1 ust. 1 pkt 2, Wykonawca otrzyma wynagrodzenie w wysokości ……..zł netto (słownie: …..… złotych …./100), ), co powiększone o należny podatek VAT w wysokości ………, stanowi kwotę…….. zł (słownie: …..… złotych …./100) brutto.
			3. Zapłatę wynagrodzenia z tytułu dostarczenia, wdrożenia i szkolenia z obsługi Systemu,
			o którym mowa w ust. 1, Wykonawca otrzyma 21 dni po wykonaniu przedmiotu zamówienia
			i wystawieniu prawidłowo faktury.
			4. Zapłatę wynagrodzenia z tytułu 4 letniego wsparcia technicznego Systemu, o którym mowa
			w ust. 2, Wykonawca otrzyma do dnia 16 stycznia 2014 r.
			5. Wykonawca wystawi fakturę za usługę wsparcia technicznego z 14 dniowym terminem płatności.
			6. Zamawiający zastrzega sobie prawo do zapłaty całości lub części wynagrodzenia
			za usługę wsparcia technicznego w terminie wcześniejszym niż określony w ust. 4,
			po wcześniejszym poinformowaniu Wykonawcy o takim zamiarze. W tym przypadku Wykonawca zobowiązany jest w ciągu 10 dni wystawić prawidłową fakturę.
			7. Wykonawca oświadcza, że wynagrodzenie zaspokaja wszelkie jego roszczenia wobec Zamawiającego z tytułu wykonania Zamówienia.
			8. Podstawą wystawienia faktury jest podpisanie przez Zamawiającego bez zastrzeżeń protokołu odbioru.
			9. Za każdy dzień opóźnienia w zapłacie Wynagrodzenia Wykonawca może żądać
			od Zamawiającego odsetek ustawowych.

**§ 3**

1. W terminie 7 dni od dnia dostarczenia, wdrożenia i szkolenia z obsługi Systemu,
o których mowa w § 2 ust. 1 pkt 1, Strony sporządzą protokół odbioru Systemu, zwany dalej „Protokołem”.
2. Protokół powinien zawierać co najmniej:
3. datę i miejsce jego sporządzenia;
4. oświadczenie Zamawiającego o braku albo o istnieniu zastrzeżeń do realizacji zadania,o którym mowa w § 2 ust. 1 pkt 1, w tym o braku albo o istnieniu wad.
5. Zastrzeżenia, o których mowa w ust. 2 pkt 2, Zamawiający zgłosi w protokole, jeżeli stwierdzi, że zadanie, o którym mowa w § 1 ust. 1 pkt 1, nie odpowiada warunkom uzgodnionym przez Strony, wskazanym w szczególności w Załączniku nr 1 do Umowy.
6. W razie zgłoszenia zastrzeżeń w protokole Zamawiający pisemnie wyznaczy Wykonawcy stosowny termin, nie dłuższy jednak niż 10 dni w celu usunięcia stwierdzonych protokołem wad. Na taki wypadek, Wykonawca zobowiązuje się usunąć wady w wyznaczonym przez Zamawiającego terminie, bez osobnego wynagrodzenia
z tego tytułu.
7. Wraz z bezskutecznym upływem terminu wyznaczonego na podstawie ust. 4, Zamawiający może od Umowy odstąpić i żądać od Wykonawcy zapłaty kary umownej określonej w§ 6 ust. 1.

**§ 4**

1. Zgłoszenia błędnego działania lub awarii Systemu przyjmowane będą przez Wykonawcę telefonicznie pod numerem tel. ………… lub faksem na numer …………… lub poprzez pocztę elektroniczną na adres …….. .
2. Oferowany System posiada ………. gwarancję obejmującą wszystkie elementy Systemu.
3. W czasie trwania gwarancji zamawiający ma dostęp do wsparcia technicznego świadczonego
w dni robocze od poniedziałku do piątku w godzinach 8:00-18:00.
4. Wsparcie techniczne prowadzone będzie w języku polskim.
5. Wykonawca zapewni wymianę uszkodzonego urządzenia na sprawne. Wysyłka następnego dnia roboczego po stwierdzeniu uszkodzenia.
6. W przypadku konieczności wymiany lub naprawy sprzętu będącego elementem Systemu, dyski twarde urządzeń pozostają u Zamawiającego.
7. Wykonawca zobowiązuje się do darmowej wymiany dostarczonego Systemu na nowy
po czterech latach od uruchomienia Systemu. Parametry elementów Systemu nie mogę być gorsze niż tych elementów przedstawionych w ofercie Wykonawcy.

**§ 5**

1. Wykonawca może powierzyć wykonanie Zamówienia podwykonawcom.
2. Za działania lub zaniechania podwykonawców Wykonawca odpowiada jak za własne.

**§ 6**

1. W razie niewykonania lub nienależytego dostarczenia, wdrożenia oraz szkolenia
z obsługi Systemu, o których mowa w § 1 ust. 1 pkt 1, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20 % kwoty brutto wskazanej w § 2 ust. 1.
2. Za każdy dzień opóźnienia w realizacji dostarczenia, wdrożenia oraz szkolenia z obsługi Systemu, o których mowa w § 1 ust. 1 pkt 1, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 2% kwoty brutto wskazanej w § 2 ust. 1, licząc od upływu terminu określonego w § 1 ust. 2.
3. Wykonawca wyraża zgodę na potrącenie kary umownej określonej w ust. 1–2
z przysługującego mu Wynagrodzenia.

**§ 7**

1. Do współpracy w sprawach związanych z wykonaniem Umowy upoważnia się:

1) ze strony Zamawiającego: …………………;

2) ze strony Wykonawcy: ……………………….

1. Zmiana osób, o których mowa w ust. 1, następuje poprzez pisemne powiadomienie drugiej Strony i nie stanowi zmiany treści Umowy.

**§ 8**

Wszelkie spory, które mogą wyniknąć w związku z interpretacją lub wykonywaniem Umowy, Strony będą rozstrzygać na drodze polubownej. W przypadku braku możliwości osiągnięcia porozumienia Strony poddają spory pod rozstrzygnięcie sądu powszechnego właściwego miejscowo dla siedziby Zamawiającego.

**§ 9**

W sprawach nieuregulowanych Umową stosuje się przepisy Ustawy – Prawo Zamówień Publicznych i Kodeksu cywilnego.

**§ 10**

Integralną częścią Umowy są następujące załączniki:

1) Załącznik nr 1: Szczegółowy Opis Przedmiotu Zamówienia;

2) Załącznik nr 2: kopia oferty Wykonawcy.

ZAMAWIAJĄCY WYKONAWCA