Fundusze Europejskie Program Regionalny | Rzeczpospolita Polska | DOLNY ŚLĄSK | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

TOM III

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

NAZWA ZAMÓWIENIA

Dostawa serwerów wraz z niezbędną infrastrukturą

Zadanie jest realizowane w ramach projektu pn. : „Wdrożenie elektronicznych usług publicznych w zakresie gospodarki wodno-kanalizacyjnej oraz nekropolii na terenie Gminy Nowogrodziec" nr RPDS.02.01.01-02-0022/17

PREZES ZARZĄDU
Jacek Ruchała

Spis treści

1. Zamawiający

Nazwa (firma) i adres Zamawiającego (Beneficjenta)

Hydro - Tech Spółka z o.o.
ul. Młyńska 3a
59 - 730 Nowogrodziec

wpisana do Krajowego Rejestru Sądowego pod nr 0000218357 prowadzonego przez Sąd Rejonowy dla miasta Wrocławia

NIP: 612-16-31-843
REGON: 230914302

Tel.: (075) 734-96-00
Faks: (075) 734-96-15

E-mail: hydro@nowogrodziec.pl,
Strona internetowa: www.hydrotech.info.pl, www.bip.hydrotech.ig.pl

2. Projekt

2.1. Nazwa projektu

„Wdrożenie elektronicznych usług publicznych w zakresie gospodarki wodno-kanalizacyjnej oraz nekropolii na terenie Gminy Nowogrodziec"

2.2. Numer projektu

RPDS.02.01.01-02-0022

2.3. Umowa o dofinansowanie

Umowa nr RPDS.02.01.01-02-0022/17-00 z dnia 21.03.2019 r.

2.4. Cel projektu

Usprawnienie realizacji procesów biznesowych obsługi klienta w zakresie usług publicznych dotyczących gospodarki wodno-ściekowej oraz zarządzania cmentarzami.

2.5. Opis projektu

Projekt „Wdrożenie elektronicznych usług publicznych w zakresie gospodarki wodno-kanalizacyjnej oraz nekropolii na terenie Gminy Nowogrodziec" nr RPDS.02.01.01-02-0022 obejmuje następujące zadania:

Lp.	Nazwa Zadania / Podzadania	Źródło finansowania
1.	**Wykonanie i wdrożenie platformy e-cmentarze**	**RPO WD**
2.	**Wykonanie i wdrożenie platformy e-BOK**	**RPO WD**
3.	**Dostawa 1500 szt. nakładek na wodomierze i 2 szt. zestawów inkasenckich**	**RPO WD**
4.	**Dostawa serwerów wraz z niezbędną infrastrukturą**	**RPO WD**

Opis działań planowanych do realizacji w ramach przedsięwzięcia:

1) Wdrożenie platformy e-cmentarze umożliwiającej elektroniczne przeszukiwanie zasobów gminnych cmentarzy, wnoszenie opłaty za miejsce na cmentarzu, zlecenie dodatkowych płatnych usług.
2) Zaprojektowanie, wykonanie i wdrożenie systemu informatycznego realizującego e-usługi: eBOK składający się z modułów: e-wodkan, e-faktury, e-zgłoszenie.
3) Dostawa 1500 szt. nakładek na wodomierze oraz 2-ch zestawów inkasenckich do radiowego odczytu wraz z oprogramowaniem do zdalnego (radiowego) odczytu wodomierzy.
4) Dostawa serwerów wraz z niezbędną infrastrukturą oraz montaż i uruchomienie ich w miejscu wskazanym przez Zamawiającego (siedziba spółki).

3. Dostawa sprzętu IT

Wymagania dotyczące przedmiotu zamówienia:

1) Oferowany sprzęt musi być: fabryczne nowy, nie może być obciążony prawami na rzecz osób trzecich, sprzedawany przez legalny kanał dystrybucji na rynek polski lub rynki wielu krajów, w tym na rynek polski, kompletny (z pełnym okablowaniem, materiałami startowymi, niezbędnym wyposażeniem np.: baterie, złącza, zasilacze, wtyczki i itp.), gotowy do pracy, aktualne produkowany na rynku, o parametrach nie gorszych niż wymagane przez Zamawiającego,
2) Zamawiający nie dopuszcza jakiejkolwiek ingerencji poza producentem w dostarczony sprzęt przed dostawą do Zamawiającego,
3) Wykonawca wraz z dostawą sprzętu dostarczy instrukcje obsługi/użytkowania w języku polskim lub języku angielskim

4) Wykonawca wraz z dostawą sprzętu dostarczy certyfikaty CE(odrębne dla każdego urządzenia), zgodne z wymogami SIWZDostawa sprzętu obejmuje transport, wniesienie, uruchomienie i konfigurację, a także sprawdzenie poprawności działania urządzeń (czynności, które należy wykonać, aby oferowane urządzenia były podłączone, uruchomione i poprawnie działające),
5) Przedmiot zamówienia będzie dostarczony transportem Wykonawcy, na jego koszt i ryzyko,
6) Ewentualne szkody powstałe w związku z wnoszeniem i montażem sprzętu, zostaną usunięte na koszt Wykonawcy.
7) Dostarczone elementy oraz dostarczone wraz z nimi oprogramowanie muszą pochodzić z oficjalnych kanałów dystrybucyjnych producentów, zapewniających w szczególności realizację uprawnień gwarancyjnych.
8) Cały dostarczony sprzęt musi zostać wyprodukowany zmontowany nie dalej niż 12 miesięcy przed dniem dostarczenia.
9) Wykonawca zobowiązany jest do znakowania dostarczanych urządzeń i sprzętu plakietkami informującymi o dofinansowaniu projektu ze środków Regionalnego Programu Operacyjnego Województwa Dolnośląskiego na lata 2014-2020 zgodnie z obowiązującymi wytycznymi. Projekty plakietek informacyjnych muszą zostać zaakceptowane przez Zamawiającego.
10) Na infrastrukturze musi zostać zainstalowane odpowiednie wymagane do poprawnej pracy systemu oprogramowanie w tym oprogramowanie serwerowe oraz oprogramowanie zarządzające i monitorujące.

3.1. Zestaw komputerowy (2 sztuki)

Każdy z 2-ch zestawów komputerowych będzie zawierał następujące elementy:

1.1. Jednostka robocza o parametrach nie gorszych niż:

- CPU i7 najwyższa dostępna generacja, min 6 rdzeni
- ilość zainstalowanych dysków – 3 szt.
- 1 szt. dysk SSD minimum 500 GB (na system)
- 2 szt. dysk SATA 1TB z RAID0 (na dane)
- sprzętowy sterownik macierzy RAID0, RAID0 ma być na dodatkowe dyski 1TB, czyli 500 GB SSD plus 2x1TB z RAID0
- pamięć RAM – 16GB
- rodzaj pamięci – DDR4, RDIMM 2400MHz
- ilość portów sieciowych – 2 szt.
- typ kart sieciowych - 1Gigabit
- interfejs karty graficznej HDMI
- napęd DVD-RW – tak
- ilość interfejsów USB 2.0 – 2 szt.
- Ilość interfejsów USB 3.0 – 2 szt., zewnętrzne USB 2.0 - 4 szt.

- system operacyjny Windows 10 Pro PL 64-bit w języku polskim 64bit

1.2. UPS - minimalne wymagania::

- umożliwiający nieprzerwaną pracę urządzeń, o których mowa w pkt. 1.1 oraz 1.3 niniejszego rozdziału przez co najmniej 10 min
- co najmniej 3 gniazda
- moc co najmniej 390W
- wyposażony w port USB i oprogramowanie monitorujące zasilanie (zabezpieczenie przeciw przepięciowe i przeciw wyładowaniom atmosferycznym)

1.3. Monitor - minimalne wymagania:

- przekątna 24"
- rozdzielczość 1920x1080 (full HD)
- format obrazu 16:9
- technologia podświetlenia LED
- rodzaj interfejsu HDMI

1.4. Gwarancja, która będzie obejmować fazę realizacyjną przedsięwzięcia do jednego roku z podstawową gwarancją w reżimie NBD on-site (czas reakcji następny dzień roboczy) i trwać min. 5 lat. W przypadku awarii, dyski zostają u Zamawiającego

1.5. Oprogramowanie biurowe: pakiet MS Office Home and Business 2019 w skład którego wchodzą co najmniej programy biurowe Word, Excel, Outlook, OneNote, PowerPoint – lub równoważny pakiet biurowy

3.2. Szafa rack 19" (1 sztuka)

W ramach wdrożenia **szafę należy umieścić w klimatyzowanym pomieszczeniu technicznym Wykonawcy** w sposób umożliwiający swobodny dostęp do przednich i tylnych drzwi, a jeżeli boki szafy również będą demontowane to tak aby można było swobodnie dokonać demontażu w celach konserwacyjnych. Szafa musi zostać wypoziomowana, a zasilanie do wnętrza szafy ma zostać doprowadzone w odpowiednim oplocie/peszlu aby zminimalizować ryzyko uszkodzenia kabla. Szafa powinna zostać dostarczona wraz z przełącznikiem LAN, który w ramach dostawy ma zostać zainstalowany w szafie i podłączony kompletem przewodów

Lp.	Wymagane minimalne parametry techniczne
1.	Szafa wysokość wewnętrzna minimum 40U
2.	szafa przeznaczona do zastosowań wewnątrz pomieszczeń serwerowych
3.	Drzwi przednie perforowane otwierane na klamkę z zamkiem
4.	drzwi tylne stalowe perforowane dwuskrzydłowe uchylne z zamkiem
5.	drzwi boczne demontowane na zatrzaskach z możliwością montażu zamka
6.	Szafa musi zawierać co najmniej dwie półki do umieszczenia urządzeń typu Tower montowane jednocześnie do przednich i tylnych szyn rack.
7.	Wymiary szafy powinny uwzględniać najdłuższy z elementów w niej instalowany – nie dopuszcza się pozostawienia niezamkniętych lub zdemontowanych drzwi.
8.	Gwarancja na urządzenie minimum 3 lata - NDB Next Business Day - serwis u klienta następnego dnia roboczego po zgłoszeniu usterki.
9.	minimalne, niezbędne wyposażenie – min 2 listwy zasilające po 6 gniazd, panel wentylacyjny z min 2 wentylatorami
10.	48 x 10/100/1000, 2 x SFP
11.	Bufor co najmniej 1,5MB
12.	Obudowa RACK
13.	Liczba obsługiwanych sieci VLAN co najmniej 4000
14.	Chłodzenie pasywne
15.	Maksymalny pobór mocy – 30W

3.3. Serwery wirtualizacji (2 sztuki)

Serwery muszą zostać połączone i skonfigurowane do współpracy z macierzą z wykorzystaniem wirtualizatora aby zapewnić wysoką dostępność uruchomionych systemów. Wirtualizator w ramach dostawy musi zostać zainstalowany i skonfigurowany do pracy z systemami Zamawiającego, w tym również należy dokonać migracji obecnie wykorzystywanych systemów tj., TYTAN SQL firmy TYTAN odpowiadający za proces sprzedaży, SYMFONIA firmy SAGE zapewniające obsługę Zamawiającego w zakresie księgowości, kadr i płac oraz THB SEZaM korelujący czynsze i zasoby.

Lp.	Wymagane minimalne parametry techniczne
1.	Montaż w szafie RACK
2.	Minimalna ilość RAM: 32GB
3.	Półprzewodnikowy nośnik pamięci (w trybie dual) pozwalający na uruchomienie hypervisora systemu wirtualizacji o pojemności minimum 32GB (jeżeli hypervisor wymaga większej pojemności to ma zostać zastosowana adekwatna do pełnego uruchomienia

	środowiska wirtualizacji)
4.	Karta sieciowa dwuportowa, pozwalająca na połączenie iSCSI z macierzą dyskową (równoważnie dopuszcza się zastosowanie połączenia FC)
5.	Jeden fizyczny procesor zgodny z architekturą x86
6.	Procesor z min. 6 fizycznymi rdzeniami
7.	Gwarancja na urządzenie minimum 3 lata - NDB Next Business Day - serwis u klienta następnego dnia roboczego po zgłoszeniu usterki.
8.	Oprogramowanie MS Windows 2019 Standard z możliwością downgrade
9.	10 licencji dostępowych do w/w systemu operacyjnego na urządzenia
10.	1 licencja umożliwiająca dostęp do serwera, poprzez zdalne połączenie za pomocą protokołu RDP

3.4. Hypervisor systemu wirtualizacji (1 sztuka)

Hypervisor ma zostać uruchomiony na klastrze serwerów **(3.3 Serwery wirtualizacji (2 sztuki))** z zdefiniowanym miejscem przechowywania systemów zwirtualizowanych na macierzy dyskowej **(3.5 Macierz dyskowa (1 sztuka)).**

Lp.	**Wymagane minimalne parametry techniczne**
2.	W ramach wdrożenia należy zainstalować i skonfigurować na opisanych w pkt. **3.3 Serwerach wirtualizacji (2 sztuki)** instancję Hypervisora z automatycznym – w przypadku awarii – uruchomieniem systemów gości na działającym serwerze (klaster niezawodnościowy). A także uruchomić podstawową instancję systemu zwirtualizowanego zawierającego system operacyjny (wraz z licencją jeżeli wybrany system będzie tego wymagał) pełniący funkcję serwera SYSLOG zbierającego informacje z systemów Zamawiającego takich jak: UTM, WAF oraz jeżeli to możliwe z macierzy i UPS (np. poprzez połączenie USB, zbieranie zdarzeń do dziennika logów). Rejestry syslog powinny być replikowane/przesyłane na urządzenie backupowe, opisano w pkt. 3.7. Wdrożenie systemu uznaje się za zrealizowane gdy wszystkie systemy niezbędne do prezentacji treści na portalu e-BOK, zostaną uruchomione na odpowiedniej liczbie systemów gości w ramach Hypervisora, którego konfiguracja zapewni dostępność nawet w przypadku awarii jednego z serwerów klastra niezawodnościowego. W przypadku realizacji systemu e-BOK poza lokalizacją sieci wewnętrznej Zamawiającego powyższego zapisu nie stosuje się.

	Wykonawca zapewni Gwarancję na przeprowadzone prace wdrożeniowe minimum 3 lata - NDB Next Business Day - serwis następnego dnia roboczego po zgłoszeniu usterki.

3.5. Macierz dyskowa (1 sztuka)

Macierz zbudowana z 2 węzłów będzie stanowiła punkt wspólny lokalizacji danych i serwerów wirtualnych uruchamianych na serwerach. System wirtualizatora i backupu należy skonfigurować w taki sposób aby codziennie wykonywana była kopia zapasowa serwerów gości a pliki archiwizacyjne replikowane były również na urządzenie kopii zapasowej.. Retencja danych powinna zakładać przetrzymywanie przynajmniej jednej kopii tygodniowej oraz minimum 3 miesięcy wstecz (jedna pełna kopia na miesiąc).

Lp.	Wymagane minimalne parametry techniczne dla pojedynczego węzła
1.	Montaż w szafie RACK, obudowa 19" 1U. W zestawie szyny do montażu w szafie. Szyny powinny umożliwiać zainstalowanie urządzenia w stelażu szafy o głębokości 89cm.
2.	Pozwalająca na montaż minimum 4 dysków: - 3.5" SATA 3 HDD - 2.5" SATA 3 HDD - 2.5" SATA 3 SSD Obsługa pojemności min. 14TB jednego dysku. Możliwość wymiany podczas pracy – hot swap. Możliwość rozbudowy do 8 dysków poprzez dołożenie jednostki rozszerzającej. Dyski muszą być kompatybilne z wymaganym sprzętem NAS oraz ich model powinien

	znajdować się na liście kompatybilności zaoferowanego sprzętu NAS. Dedykowane do pracy w urządzeniach NAS. O parametrach nie gorszych: 2TB, SATA III 6Gb/s, 3,5", 7200 rpm, 128 MB cache. Dostarczone w ilości 2szt. Objęte 5 letnią gwarancją producenta dysku
3.	Procesor 64-bit, 4-rdzeniowy, taktowany zegarem co najmniej 2,1 GHz, pamięcią cache CPU co najmniej 8 MB osiągający średnią wydajność na poziomie minimum 2300 punktów w teście wydajnościowym PassMark CPU Benchmarks wg. kolumny Passmark CPU Mark, którego wyniki są publikowane na stronie http://cpubenchmark.net/cpu_list.php nie później niż na dzień 12-03-2020, 2GB RAM DDR3, jeden slot wolny, z możliwością rozszerzenia do min. 18GB
4.	Karta sieciowa 4x1GbE Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę Link Aggregation. Obsługa kart sieciowych 10GbE, - minimum 2szt USB 3.0 - minimum 1szt PCIe 2.0 x4, umożliwiające obsługę kart sieciowych lub karty rozszerzeń M.2 SATA SSD - port konsoli RS232 - port do podłączenia dodatkowej półki, dopuszcza się eSATA
5.	Możliwość pracy w trybie RAID 0, 1, 5, 6, 10 z funkcją rozbudowy i funkcją migracji poziomu RAID, RAID Hot Spare - obsługa iSCSI - liczba iSCSI Target: 128 - liczba jednostek iSCSI LUN: 256 - obsługa klonowania/migawek jednostek iSCSI LUN
6.	- szyfrowanie folderów współdzielonych - skanowanie złych sektorów, S.M.A.R.T., - szyfrowana replikacja, - automatyczne blokowanie adresów IP - powiadomienia przez e-mail - kopia zapasowa konfiguracji - kopia na nośnik zewnętrzny, - logi systemowe (użytkownicy, alarmy, błędy, połączenia do plików), - FTP przez SSL/TLS - zarządzenie przez przeglądarkę HTTPS - współpraca z zasilaczami awaryjnymi UPS

	- przypisanie usługi sieciowej do konkretnego portu - interfejs aplikacji www do zarządzania w języku polskim
7.	Zasilanie nadmiarowe – redundantne. 100 – 240V, 50/60 Hz moc pojedynczego zasilacza minimum 150W
8.	- obsługa iSCSI - liczba iSCSI Target: 128 - liczba jednostek iSCSI LUN: 256 - obsługa klonowania/migawek jednostek iSCSI LUN
9.	System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie , dostarczenie oraz instalację sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu od momentu potwierdzenia zasadności zgłoszenia w miejscu instalacji wykonana przez certyfikowanego inżyniera w zakresie oferowanego rozwiązania, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5 . Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. Oferent winien przedłożyć dokumenty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.

3.6. Zasilacz UPS (1 sztuka)

Zasilacz w ramach dostawy ma zostać zainstalowany w szafie i podłączony kompletem przewodów zapewniając zasilanie wszystkich urządzeń służących do dostarczania systemów i aplikacji sieciowych takich jak: serwery, macierz, UTM, WAF, Ochrona E-mail.

Lp.	Wymagane minimalne parametry techniczne
1.	Montaż w szafie RACK

2.	Wydajność urządzenia pozwala na utrzymanie zasilania przez czas minimum 10min przy założeniu obciążenia na poziomie 2700W
3.	Komplet okablowania umożliwiający podłączenie zasilania zarówno jednostki UPS jak i wszystkich urządzeń zainstalowanych w szafie rack
4.	Zapewnienie odpowiednich listew zasilających montowanych do szyn RACK 19" pozwalających na podłączenie wszystkich urządzeń zainstalowanych w szafie rack
5.	Gwarancja na urządzenie (z wyłączeniem baterii akumulatorów) minimum 3 lata - NDB Next Business Day - serwis u klienta następnego dnia roboczego po zgłoszeniu usterki.

3.7. Serwer Backup wraz z oprogramowaniem (1 sztuka)

Serwer backup w ramach dostawy ma zostać zainstalowany w szafie i podłączony kompletem przewodów zapewniając redundantne zasilanie i oprogramowanie wszystkich platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji

Lp.	**Wymagane minimalne parametry techniczne**
1.	Czterordzeniowy procesor o taktowaniu co najmniej 1,5 GHz (zwiększanym do 2,3 GHz)
2.	Pamięć systemowa 4GB / Maksymalnie 8GB
3.	Obudowa RACK na 4 dyski 3,5" SATA 6Gb/s
4.	4 x RJ45 10/100/1000Mbps
5.	1 x Gniazko PCIe Gen 2 x2
6.	4 x USB 3.2
7.	2 zasilacze redundantne co najmniej 250W
8.	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V, oraz AWS EC2
9.	Oprogramowanie musi pozwalać na wdrożenie w środowiskach na serwerze sprzętowym, obsługiwane systemy operacyjne w ramach: Windows Server 2008 R2 – 2019 (x64), Windows 7 – 10 Professional (x64), Ubuntu 12.04 – 18.04 Server (x64), Red Hat Enterprise Linux 6.3 – 7.4 (x64), SUSE Linux Enterprise Server 11 SP3 – 12 SP3 (x64) jako maszyna wirtualna Vmware jako maszyna wirtualna Amazon na serwerze NAS: QNAP, Synology
10	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS.

11	Oprogramowanie nie może wymagać instalacji jakiegokolwiek agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania.
12	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 10 maszyn wirtualnych (w środowisku Vmware lub Hyper-V lub AWS lub Nutanix) lub maszyn fizycznych przez okres 5 lat.
13	Gwarancja minimum 3 lata.

3.8. UTM nowej generacji zabezpieczający sieć i serwery usług wraz z subskrypcją sygnatur bezpieczeństwa (1 sztuka)

Wdrożenie ma obejmować skonfigurowanie urządzenia do pracy w zakładzie zarówno pod kątem dostarczanych systemów WAF jak i polityk bezpieczeństwa użytkowników komputerów osobistych, serwerów wewnętrznych, serwerów aplikacji oraz usług dostarczanych do klientów Zamawiającego w przestrzeni DMZ.

Lp.	**Wymagane minimalne parametry techniczne**
1.	System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
2.	Monitoring i wykrywanie awarii • Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. • Monitoring stanu realizowanych połączeń VPN.
3.	Interfejsy: • System realizujący funkcję Firewall musi dysponować minimum 8 portami Gigabit Ethernet RJ-45. • W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 64 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. • Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów.
4.	Parametry wydajnościowe: • W zakresie Firewall'a obsługa nie mniej niż 200 000. jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę. • Przepustowość Stateful Firewall: nie mniej niż 3 Gbps • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 500 Mbps • Wydajność szyfrowania IPSec VPN: nie mniej niż 350Mbps • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu

	http – minimum 135 Mbps.
5.	Funkcje Systemu Bezpieczeństwa: W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, SMTPS, POP3, POP3S, HTTP, FTP, FTPS, HTTPS. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, SMTPS, POP3, POP3S. • Zarządzanie pasmem (QoS, Traffic shaping). • Analiza ruchu szyfrowanego protokołem SSL. • Filtrowanie adresatów wysyłanych wiadomości przesyłanych plików według rozmiarów, zawartości czy rozszerzeń, ograniczeń dotyczących odbiorców wiadomości?
6.	Polityki, Firewall • Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. • System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: o Translację jeden do jeden oraz jeden do wielu. o Dedykowany plugin dla protokołu SIP. • W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
7.	Routing i obsługa łączy WAN • W zakresie routingu rozwiązanie powinno zapewniać obsługę: o Routingu statycznego. o Policy Based Routingu. o Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP • System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

8.	Kontrola Antywirusowa • Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. • System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • Urządzenie ma być dostarczone wraz z komercyjnym skanerem Antywirusowym, nie dopuszcza się stosowania skanera rozwijanego w ramach projektów OpenSource. • Urządzenie musi umożliwiać analizę typu sandbox przeprowadzaną w chmurze producenta. Nie dopuszcza się aby analiza była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza była przeprowadzana przez firmy trzecie..
9.	Ochrona przed atakami • Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków powinna zawierać minimum 4500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • System musi dysponować sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA. • Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. • Wykrywanie i blokowanie komunikacji C&C do sieci botnet. • Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. • Moduł skanujący musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. • Moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i

	informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.
10	Kontrola aplikacji • Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Baza Kontroli Aplikacji powinna zawierać minimum 350 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. • Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 65 kategorii tematycznych stron internetowy • W ramach filtra URL sklasyfikowanych jest co najmniej 100 milionów stron internetowych.Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
11	Zarządzanie • Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. • Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
12	Logowanie • Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. • W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku. Chmura musi znajdować się w Europejskim Obszarze Gospodarczym. • Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. • Musi istnieć możliwość logowania do serwera SYSLOG.
13	Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i

	serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen Sygnatury ochrony systemów przemysłowych SCADA a także Logowanie do usługi realizowanej w chmurze **na okres 5 lat**.
14	Urządzenie ma być objęte 5 letnią gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od stwierdzenia awarii. Wymaga się, aby dostawa obejmowała również minimum 5 letnią gwarancję producenta na dostarczone licencje dla wszystkich funkcji bezpieczeństwa. W przypadku wymiany urządzenie zamawiający musi mieć możliwość usunięcia i zachowania dysku twardego przed jego odesłaniem do dostawcy bez utraty gwarancji. Dla zapewnienia wysokiego poziomu usług podmiot realizujący serwis rozszerzony musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe muszą być przyjmowane w języku polskim w trybie co najmniej 8/5 [maksymalnie 24/7] przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim. *Wykonawca w ramach rozszerzonego wsparcia technicznego w Formularzu oferty:* *a) Oświadcza, że serwis rozszerzony na rzecz Zamawiającego świadczony będzie przez Producenta lub Autoryzowanego Dystrybutora oraz podaje* *- adres strony internetowej serwisu,* *- numer infolinii telefonicznej,* *b) oświadcza, iż podmiot serwisujący posiada Certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych.*

Wadliwość rozumie się jako uszkodzenie fizyczne, mechaniczne lub funkcjonalne powodujące iż produkt nie jest zdatny do użytku lub jego użytkowanie w zdefiniowanym obszarze funkcjonalnym jest nieprawidłowe lub znacznie odbiegające od normy przyjętej dla tego modelu urządzeń, które pojawiło się w procesie produkcyjnym i ujawniło w okresie gwarancyjnym. Zakres zobowiązań producenta musi być ujęty w ogólnej umowie licencyjnej produktu.

3.9. Web Application Firewall stanowiący zabezpieczenie portalu usług zlokalizowanego na serwerach wraz z subskrypcją sygnatur bezpieczeństwa na 5 lat (1 sztuka)

System ochrony aplikacji webowych oraz Firewall XML - którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System powinien umożliwiać lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów. Musi istnieć możliwość implementacji systemu in-line w trybach Reverse Proxy lub Transparentnym, jak również implementacji w trybie nasłuchu.

Wdrożenie obejmować będzie konfigurację systemu zapewniającą **objęcie ochroną strony głównej Zamawiającego wraz z e-BOK oraz projektowanymi e-usługami**. Jeżeli będzie to wymagane należy

przenieść stronę WWW do zasobów hypervisora wraz z uruchomieniem systemu operacyjnego i skonfigurowaniem odpowiednich usług serwera HTTP oraz skonfigurowaniem polityk na urządzeniu UTM.

Lp.	**Wymagane minimalne parametry techniczne**
1.	Tryb auto-uczenia – przyspieszający i ułatwiający implementację
2.	Podział obciążenia na kilkanaście serwerów (loadbalancing)
3.	Akceleracja SSL dla wybranych serwisów w centrum danych
4.	Możliwość analizy poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje)
5.	Firewall XML realizujący z możliwością routingu w oparciu o kontent, walidacją schematów XML oraz weryfikacją WDSL.
6.	Firewall aplikacji webowych chroniący przed takimi zagrożeniami jak: • SQL and OS Command Injection. • Cross Site Scripting (XSS). • Cross Site Request Forgery. • Outbound Data Leakage. • HTTP Request Smuggling. • Buffer Overflow. • Encoding Attacks. • Cookie Tampering / Poisoning. • Session Hijacking. • Broken Access Control. • Forceful Browsing /Directory Traversal. • Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP. • DoS w warstwie aplikacji. • Ochrona przed atakami typu Brute force.
7.	Rozwiązanie musi obsługiwać przepustowość dla ruchu http - min **25 Mbps**
8.	Aktualizacja baz sygnatur powinna być systematycznie aktualizowana zgodnie ze zdefiniowanych harmonogramem
9.	System realizujący funkcje podstawowe musi obsługiwać minimum 3 interfejsy sieciowe oraz 1 wirtualny procesor
10	Możliwość logowania do zewnętrznego serwera syslog
11	Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa e-mailem
12	Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować: Skanowanie aplikacji, Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres **5 lat.**
13	System musi być objęty serwisem gwarancyjnym producenta polegającym na naprawie w

	przypadku jego wadliwości oraz serwisem wsparcia technicznego w trybie 8/5 przez okres **5 lat**.

3.10. Prace konfiguracyjne oraz wdrożeniowe w zakresie uruchomienia systemów na platformach sprzętowych

W ramach niniejszego zamówienia zostanie wykonana usługa instalacji dostarczonego przez Wykonawcę Sprzętu komputerowego oraz konfiguracji środowiska obejmująca konfiguracje urządzeń sieciowych u Zamawiającego w tym:

1. przeniesienie aktualnego okablowania ze starej szafy RACK do nowej
2. fizyczna instalacja w zaoferowanej szafie RACK infrastruktury serwerowo-macierzowej i sieciowej,
3. instalacja, podłączenie, konfiguracja elementów sieciowych i serwerowych,
4. przygotowanie systemów i maszyn wirtualnych
5. testy poprawności działania systemów.

Konfiguracja urządzeń

Szczegółowe informacje dotyczące konfiguracji poszczególnych elementów systemu mogą być ograniczone prawem autorskim Wykonawców, a jednocześnie ich publiczne ujawnienie może wiązać się ze znacznym obniżeniem bezpieczeństwa systemu jako całości. Zamawiający, po podpisaniu umów z Wykonawcami systemów **e-BOK, e-cmentarze**, przekaże Wykonawcy **pełną informację związaną z fizycznym połączeniem poszczególnych urządzeń z dokładnością do poszczególnych portów**. Jednocześnie zakres ingerencji Wykonawcy wewnątrz poszczególnych systemów musi stać się przedmiotem odrębnych ustaleń pomiędzy nim a Zamawiającym lub Wykonawcą poszczególnych systemów.

3.11. Termin realizacji

Termin dostawy serwerów wraz z niezbędną infrastrukturą oraz montaż i uruchomienie ich w miejscu wskazanym przez Zamawiającego (siedziba spółki)- 30 dni od dnia podpisania umowy

PREZES ZARZĄDU
Jacek Ruchała