

## Warunki techniczne zamawianego sprzętu i oprogramowania oraz wykaz usług do wykonania.

### 1. Przełącznik zarządzany warstwy trzeciej – 2 sztuki – o parametrach minimalnych:

1	Ilość portów: przełącznik musi posiadać min. 2 karty liniowe, z których: 1 karta liniowa posiadająca co najmniej: - 24 porty 10/100/1000 BASE-T PoE+. 1 karta liniowa posiadająca co najmniej: - 20 portów 10/100/1000 BASE-T PoE+, 2 porty 1000 BASE-T (RJ45), 2 porty SFP+ z modułami miniGIBIC typu LC.
2	Obudowa: Obudowa modułarna z min. 6 slotami na karty liniowe
3	Pamięć : 4 MB flash, 128 MB compact flash, 256 MB DDR SDRAM
4	Rozmiar tablicy adresów MAC: min 10 000 pozycji
5	Zarządzanie: CLI, WWW, telnet, pozapasmowe (port szeregowy RS-232C)
6	Warstwa przełączania: 2,3,4
7	Funkcje warstwy 3: static IP routing, RIP, RIPv2 , routing OSPF, routing multicastów PIM Sparse/Dense mode, oraz o wsparcie dla VRRP
8	Prędkość magistrali: min. 288 Gbps
9	Przepustowość: min 214 Mpps
10	Ilość obsługiwanych VLAN-ów: min. 2048 (802.1q) w tym możliwość rozbudowy poprzez licencję o QinQ
11	Funkcje wysokiej dostępności: Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), Multiple Spanning Tree (802.1s),
12	Bezpieczeństwo: Radius, TACACS+, SNMPv3, SSL, SSHv2, 802.1x (możliwość jednoczesnej autentykacji dwoma sposobami np. 802.1x oraz MAC, lub 802.1x lub WWW, obsługa do 32 autentykowanych stacji na jednym porcie, wsparcie dla voice vlanów), Access control lists (ACLs), Identity-driven ACL, DHCP Snooping, Dynamic ARP Protection, BPDU filtering oraz BPDU Protection, STP RootGuard, Access control lists (ACLs)
13	QoS: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ
14	Monitorowanie: RMON 4 grupy statistics, history, alarm, events, SFLOW, zdalny port mirroring poprzez tunel UDP (możliwość śledzenia całego portu, w oparciu o vlan bądź ACL)
16	autonegocjacja prędkości, duplex-u oraz połączenia (MDI/MDIX)
17	Oprogramowanie: Aktualizacje dostępne na stronie producenta
18	Urządzenie musi posiadać minimum 24 miesiące gwarancji. Wymagane jest, aby w okresie gwarancji urządzenie zostało objęte wsparciem technicznym producenta.
19	Serwis: Czas naprawy urządzenia nie może przekroczyć 12 h od chwili zgłoszenia awarii. W przypadku, kiedy Wykonawca nie zdoła dokonać naprawy przełącznika w ciągu 12h, musi podstawić urządzenie zastępcze o nie gorszych parametrach od przełącznika Zamawiającego.
20	Pozostałe funkcje: LLDP,LLDP-MED, dual flash images, CPU protection, Virus Throttling, ICMP throttling, obsługa ramek typu Jumbo, iSCSI
21	Zasilanie: urządzenie musi posiadać dwa niezależne zasilacze 230VAC,, 1500W PoE+.
24	Wykonawca do każdego przełącznika dostarczy kable patchcord kategorii 6 klasy E w ilości równej liczbie portów 10/100/1000 BASE-T, o długości 2metry każdy oraz po 2 patchcordsy światłowodowe kategorii OM3 wg normy PN-EN 50173-1:2009 zakończone złączami typu LC o długości minimum 5 metrów, umożliwiające transmisję danych z prędkością 10 Gbit/s.
25	Wykonawca musi dostarczyć Zamawiającemu licencje na oprogramowanie systemowe – system operacyjny dla każdego przełącznika, które umożliwi wykorzystanie wszystkich portów bez ograniczeń w pełnej funkcjonalności..
26	Urządzenie musi posiadać możliwość łączenia w stos.
27	Urządzenie musi posiadać możliwości instalacji w szafie rack 19. Wykonawca wraz z urządzeniem dostarczy wszystkie elementy montażowe.

## 2. Zapora sieciowa, ochrona styku z Internetem - 2 sztuki - o parametrach minimalnych:

- 1) Typ urządzenia
  - a) Dwa urządzenia typu UTM, zapewniające funkcjonalności: zapewniające funkcjonalności: firewall, koncentrator IPsec VPN, ochrona przed wirusami, spyware, sonda IPS, filtrowanie poczty, kontrolę aplikacji
- 2) Specyfikacja fizyczna urządzenia
  - a) Dedykowane rozwiązanie sprzętowe
  - b) Obudowa 1U przeznaczona do montażu w szafie RACK
  - c) Pamięć RAM: minimum 512 GB
  - d) Pamięć FLASH: minimum 512 MB Compact Flash
  - e) Ilość interfejsów
    - nie mniej niż 6 interfejsów GigabitEthernet
    - nie mniej niż 2 interfejsy USB
    - 1 interfejs konsoli
- 3) Wydajność urządzenia
  - a) Obsługa nielimitowanej ilości hostów w sieci chronionej
  - b) Przepustowość zapory sieciowej przy pracy w trybie Statefull Packet Inspection, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 1,5 Gbps
  - c) Przepustowość zapory sieciowej pracującej jako sonda IPS, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 0,75 Gbps
  - d) Przepustowość zapory sieciowej przy pracy w trybie Deep Packet Inspection, przy włączonych wszystkich usługach filtrowania i skanowania: nie mniejsza niż 240 Mbps
  - e) Przepustowość zintegrowanego z zaporą sieciową koncentratora połączeń IPsec VPN AES/3DES mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 625 Mbps
  - f) Minimalna ilość jednocześnie obsługiwanych sesji w trybie UTM: nie mniej niż 175000
  - g) Minimalna ilość jednocześnie obsługiwanych sesji: nie mniej niż 325000
  - h) Obsługa nie mniej niż 7000 nowych sesji na sekundę
  - i) Ochrona przed atakami DoS i DDoS
- 4) Oferowane rozwiązanie musi wspierać funkcjonalność Active / Passive z możliwością synchronizowania sesji.
- 5) Funkcjonalności urządzeń w zakresie konfiguracji połączeń IPsec VPN
  - a) Minimalna ilość jednocześnie obsługiwanych połączeń IPsec VPN: 800
  - b) Minimalna ilość klientów IPsec VPN w cenie urządzenia: 50
  - c) Wspierane mechanizmy uwierzytelniania i szyfrowania: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1
  - d) Wspierane mechanizmy wymiany kluczy: IKE, IKEv2, Manual Key, PKI (X.509)
  - e) Wsparcie certyfikatów: Verisign, Thawte, Cybertrust, RSA Keon, Entrust, Microsoft CA dla połączeń site-to-site pomiędzy urządzeniami oferowanymi.
  - f) Obsługa funkcjonalności: L2TP IPsec, DHCP over VPN, redundantna brama zdalna w przypadku połączeń site-site VPN
- 6) Sieciowe funkcjonalności urządzeń
  - a) Możliwość pracy jako Router, Bridge L2 lub w trybie transparentnym
  - b) Obsługa nie mniej niż 200 sieci VLAN działających zgodnie ze standardem 802.1Q
  - c) Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP
  - d) Możliwość przesyłania komunikatów DHCP pomiędzy różnymi strefami
  - e) Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many, PAT
  - f) Możliwość scentralizowanego zarządzania nie mniej niż 128 punktami dostępowymi, wsparcie dla standardów 802.11 b/g, WEP, WPA, TKIP, 802.1x, EAP-PEAP,

EAP-TTLS, IPSec over WLAN

- g) Możliwość kreowania reguł routingu statycznego
  - h) Wsparcie dynamicznych protokołów routingu: RIP v1/v2, OSPF i wsparcie dla routowania transmisji multicast
  - i) Wsparcie funkcjonalności QoS: tagowanie/mapowanie 802.1p, DSCP, możliwość ustawienia przynajmniej 100 reguł określających maksymalne i gwarantowane pasmo
  - j) Możliwość skonfigurowania przynajmniej 2 łączy WAN, działających w trybie redundantnym lub umożliwiających równoważenie obciążeń dla ruchu wychodzącego.
  - k) Możliwość konfiguracji monitorowania pracy łączy WAN w oparciu o połączenia TCP i ICMP i reguł przełączenia ruchu z łączy podstawowego na łączy redundantne
  - l) Możliwość konfiguracji reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej
  - ł) Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, pełna kompatybilność z większością urządzeń i serwerów VoIP
  - m) Funkcjonalności urządzeń w zakresie uwierzytelniania użytkowników
    - Lokalna baza użytkowników umożliwiająca wykreowanie nie mniej niż 2500 kont
    - Uwierzytelnianie użytkowników w oparciu o: XAUTH/RADIUS, Active Directory, SSO, LDAP, lokalna baza użytkowników
- 7) Funkcjonalności urządzeń w zakresie zarządzania i wysokiej dostępności
- a) Możliwość zarządzania urządzeniem poprzez: HTTP, HTTPS, CLI (SSH, konsola), SNMP v2
  - b) Możliwość dokupienia dedykowanego oprogramowania producenta do scentralizowanego zarządzania większą ilością urządzeń
  - c) Praca w klastrze wysokiej dostępności w trybie Active – Passive z synchronizacją sesji
- 8) Funkcjonalności urządzeń w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection
- a) Możliwość kreowania stref bezpieczeństwa przydzielanych do danych interfejsów zarówno fizycznych, jak i wirtualnych (możliwość przypisania więcej niż jednego interfejsu do pojedynczej strefy bezpieczeństwa)
  - b) Możliwość indywidualnej konfiguracji usług bezpieczeństwa dla każdej ze stref
  - c) Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do zadanej strefy, w określonych przedziałach czasu, z uwzględnieniem użytkowników, dla których reguła ma być aktywna
  - d) Możliwość włączania i wyłączania reguł Firewall i NAT bez konieczności ich usuwania
  - e) Wymagane jest, aby na urządzeniach uruchomione były następujące usługi w subskrypcji na okres jednego roku:
    - Sieciowa ochrona antywirusowa zapewniająca skanowanie ruchu na protokołach HTTP, FTP, POP3, SMTP, IMAP, ruch TCP oraz NetBios.  
Filtr antywirusowy powinien zapewniać skanowanie załączników poczty elektronicznej, plików skompresowanych ZIP i GZIP. Wymagane jest, aby możliwe było włączenie lub wyłączenie usługi antywirus w poszczególnych strefach bezpieczeństwa, oraz możliwość włączenia lub wyłączenia reagowania na określone sygnatury.
    - Sonda IDP/IPS (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. Sygnatury powinny umożliwiać wykrywanie i blokowanie zdarzeń takich jak: korzystanie z programów do wymiany plików P2P (np. Limewire, BitTorrent, eMule, etc.), korzystanie z komunikatorów internetowych (np. Yahoo Messenger, Gadu-Gadu, Skype, etc.), ataki typu backdoor, exploit, SQL-Injection, etc. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych.
    - Sieciowa ochrona antyspyware, zapewniająca skanowanie ruchu HTTP, FTP, SMTP, POP3, IMAP. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych.
    - Usługa filtrowania treści stron WWW, zapewniająca blokowanie apletów Java, aplikacji Active-X, plików cookie, definiowanie białych i czarnych list stron www, definiowanie słów

kluczowych umożliwiających zablokowanie strony w przypadku ich wystąpienia. Dodatkowo wymagane jest tworzenie reguł filtrowania treści dla poszczególnych grup użytkowników umożliwiających filtrowanie treści w oparciu o informacje z zewnętrznych serwerów zawierających bazę stron zestawionych w co najmniej 56 kategoriach. Wymagane jest, aby mechanizm filtrowania treści uwzględniał także filtrowanie stron HTTPS oraz możliwość włączenia lub wyłączenia mechanizmu filtrowania treści w poszczególnych strefach bezpieczeństwa i zdefiniowanie domyślnej reguły dla każdej ze stref działającej niezależnie od uprawnień poszczególnych użytkowników.

- Usługa Firewall aplikacji umożliwiająca definiowanie własnych sygnatur oraz reakcji urządzenia w przypadku wykrycia ruchu zgodnego z wprowadzonymi sygnaturami.
  - Ochrona poczty elektronicznej w oparciu o białe/czarne listy nadawców oraz serwery RBL.
- f) Wymagana jest taka możliwość skonfigurowania połączeń IPSec VPN client-site, aby cały ruch z połączonych do urządzeń klientów przesyłany był poprzez urządzenia i możliwe było jego skanowanie przez mechanizmy antywirus, antyspyware, IDP, filtrowania treści.
- g) Wymaga się, aby na urządzeniach możliwe było włączenie blokowania ruchu przesyłanego pomiędzy strefami w przypadku, kiedy na stacjach roboczych lub serwerach nie będzie zainstalowanego odpowiedniego oprogramowania antywirusowego, lub oprogramowanie to będzie miało nieaktualne sygnatury.
- h) Wymaga się, aby mechanizmy antywirus, antyspyware i sonda IDP nie posiadały ograniczeń co do wielkości skanowanych plików
- 9) Monitorowanie i raportowanie zdarzeń
- a) Wymagane jest dostarczenie dedykowanego oprogramowania (instalowanego na zewnętrznym serwerze) zapewniającego monitorowanie, rejestrację i graficzną (w postaci tabel i wykresów) prezentację danych przesłanych z urządzenia firewall dotyczących ruchu, oraz zagrożeń sieciowych. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, wykorzystanie pasma przez każdego z użytkowników, informacje dotyczące przeglądanych witryn przez każdego z użytkowników sieci informatycznej, informacje dotyczące użytkowników łamiących zasady przeglądania witryn, informacje dot. ataków, detekcji intruzów, zagrożeń antywirusowych. Dane muszą mieć możliwość wydruku.
- 10) Wsparcie techniczne i gwarancja
- a) Urządzenie musi zostać objęte gwarancją na okres nie krótszy niż 24 miesiące. Naprawa urządzenia nie może przekroczyć 12h od chwili zgłoszenia awarii. W przypadku kiedy Wykonawca nie zdoła naprawić urządzenia w ciągu 12h, musi podstawić urządzenie zastępcze nie gorszych parametrach od urządzenia Zamawiającego.
- b) Wymagane jest, aby w okresie gwarancji urządzenie objęte było wsparciem technicznym 24x7.

### 3. Zasilacz awaryjny (UPS) – 1 szt. - o parametrach minimalnych:

- 1) Moc wyjściowa UPS-a 15 kVA / 13,5 kW
- 2) Urządzenie ma być przystosowane do przyszłej rozbudowy w układzie pracy równoległej do maksymalnie czterech jednostek. Układ połączeń logicznych pomiędzy jednostkami układu równoległego nie może stanowić pojedynczego punktu awarii, to znaczy przerwanie połączenia logicznego między urządzeniami pracującymi równoległe nie może spowodować utraty funkcjonalności systemu zasilania gwarantowanego. Nawet w przypadku braku komunikacji logicznej urządzenia zapewnią podtrzymanie zasilania przy zaniku napięcia z sieci (praca z falownika) z równomiernym obciążeniem wszystkich jednostek układu. Do oferty należy dołączyć opis technologii synchronizacji napięć wyjściowych jednostek równoległych stosowanej w oferowanych urządzeniach. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
- 3) Ilość faz 3/3 trzy fazy wejściowe i trzy fazy wyjściowe
- 4) Napięcie wejściowe – wyjściowe toru obejściowego 3x400 V zgodne z wartościami zapisanymi w Polskiej Normie PN-IEC 60038, z tolerancją minimum 340V do 440V przy 100% obciążeniu.
- 5) Napięcie wejściowe toru prostownika 3x400 V z tolerancją -20% / +20% przy obciążeniu 100%.
- 6) Urządzenie powinno posiadać:
  - Wejście trójfazowe 5-cio przewodowe (TN-S), zasilanie dwutorowe: oddzielne wejścia zasilania prostownika i bypassu wewnętrznego.
  - Wyjście trójfazowe 5-cio przewodowe (TN-S)
- 7) Częstotliwość wejściowa 50 Hz zgodna z wartościami zapisanymi w Polskiej Normie PN-IEC 60038 z tolerancją min. 45Hz do 65Hz
- 8) Urządzenie powinno zapewnić ciągłe bezprzerwowe zasilanie w trybie TRUE ONLINE z podwójną konwersją przy zupełnych lub chwilowych zanikach napięcia i wahaniami częstotliwości w sieci elektrycznej przez cały czas pracy urządzenia. Zgodnie z normą PN-EN 62040-3, urządzenie klasy VFI-SS-111
- 9) Czas pracy autonomicznej urządzenia przy obciążeniu znamionowym o współczynniku  $\cos \varphi = 0,7$  musi wynosić, co najmniej, 15 minut. Baterie powinny być umieszczone w obudowie UPS. Wymagane są baterie o żywotności, wg EUROBAT, min. 5 lat.
- 10) Urządzenie powinno być wyposażone w komunikacyjny wyświetlacz LCD z odczytem parametrów elektrycznych wejścia/wyjścia i komunikatów o stanie pracy UPS w języku polskim.
- 11) Masa urządzenia z bateriami i bypasse mechanicznym nie może przekraczać 300 kg.
- 12) Kolor obudowy UPS: czarny.
- 13) Poziom hałasu urządzenia w trybie podwójnego przetwarzania przy obciążeniu znamionowym nie może przekraczać 55dBA z odl. 1m.
- 14) Urządzenie powinno być wyposażone w system nieciągłego ładowania baterii. Do oferty należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
- 15) Dla normalnego i autonomicznego trybu pracy zakres zmian napięcia wyjściowego maks. +/- 3V, stabilizacja napięcia wyjściowego  $\leq 5\%$  Un przy obciążeniu dynamicznym zmieniającym się od 10% do 90% i odwrotnie z czasem odbudowy 1 ms.
- 16) Sprawność > 90 % w trybie TRUE ONLINE przy dla 100% obciążenia znamionowego.
- 17) Wejściowy współczynnik mocy  $\cos \varphi$  min. 0,99, THDi nie wyższe niż 5%.
- 18) Możliwość pracy z niesymetrycznym obciążeniem poszczególnych faz, w zakresie 0-100% obciążenia.
- 19) Zdolność zwarciowa zasilacza musi być nie mniejsza niż 55 A w czasie 300 ms.
- 20) Urządzenie powinno zapewnić spełnienie wymogów Certyfikatu Bezpieczeństwa: Spełnienie norm kompatybilności elektromagnetycznej EN 55022, EN 55011, EN 50091 (IEC 62040)
- 21) Wymagana deklaracja producenta zgodności produktu z normami: EN 62040-1-1, EN 62040-2 oraz spełnienia dyrektyw: 2006/95/EC (LVD), 2004/108/EC (EMC) wraz z określeniem roku przyznania znaku bezpieczeństwa CE.
- 22) Zasilacz musi być wyposażony w wewnętrzny elektroniczny i mechaniczny układ obejściowy.
- 23) Dostawa musi zawierać wyłącznik awaryjny ppoż. EPO oraz zdalny panel LCD możliwy do wyniesienia na odległość min. 100m.
- 24) Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:
  - Gniazdo komunikacji RS-232,
  - Karta sieciowa 10/100 Base-T RJ-45 (Web/SNMP).

- 25) W wyposażeniu musi znajdować się oprogramowanie umożliwiające monitorowanie UPS i zamykanie systemów operacyjnych pracujących pod min nast. Systemami:
- Windows: 2000, 98, Me, NT 4.0, XP, Vista, Server 2003 i 2008
  - UNIX: HP-UX wer.11, IBM AIX wer. 5.3
  - Linux: SuSE Linux 10.0, SuSE Enterprise Linux Server 10
  - Sun Solaris wer.10
  - VMware ESX Serwer 3.5
  - Novell NetWare wer. 6.0 i 6.5 .
- 26) Zamawiający po dostawie wykona pomiary i testy funkcjonalne potwierdzające spełnianie przez urządzenie zadeklarowanych parametrów. Jeżeli którykolwiek parametr nie zostanie spełniony Zamawiający rozwiąże umowę z Dostawcą zaś Dostawca zobowiązany będzie do wykonania demontażu i odebrania urządzenia na własny koszt.
- 27) Oferowane urządzenie do bezprzerwowego zasilania urządzeń komputerowych, zwane dalej urządzeniem, ma być fabrycznie nowe i ma pochodzić z seryjnej produkcji. Data jego wyprodukowania nie może być wcześniejsza niż 6 miesięcy przed terminem złożenia ofert. Producent oferowanego urządzenia powinien spełniać wymagania międzynarodowego standardu jakości ISO 9001, co powinno być potwierdzone ważnym certyfikatem. Dostawca urządzenia ma zapewnić dostawę części zamiennych przez okres, co najmniej, 7 lat od daty zakończenia produkcji oferowanego modelu urządzenia.
- 28) Gwarancja na dostarczony zasilacz UPS oraz baterie musi zostać udzielona na okres minimum 24 miesiące.
- 29) Wraz z zasilaczem należy dostarczyć zewnętrzny czujnik środowiskowy do pomiaru temperatury i wilgotności powietrza. Komunikacja musi odbywać się poprzez kartę SNMP. Odczyt wartości pomiarowych czujnika musi być dostępny za pośrednictwem dowolnej przeglądarki internetowej.

#### 4. Serwer o następujących parametrach minimalnych – 1 szt

Nazwa parametru	minimalne
Obudowa	Obudowa o wysokości maksymalnie 1U, dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Typ procesora	Procesor czterordzeniowy dedykowany do pracy w serwerach wieloprocesorowych.
Wydajność systemu	Minimum Quad-Core Intel® Xeon® Processor E5620 (2.40 GHz 80Watt )
Ilość procesorów	Możliwość instalacji 2 CPU, zainstalowany 1 procesor,
Pamięć RAM	Minimum 24 GB DDR3, z technologią ECC, możliwość rozszerzenia pamięci do minimum 192 GB.
Płyta główna	Dwuprocesorowa, dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera,
Słoty PCI	Minimum 2 sloty PCI-Express 2.0 x16 Serwer musi mieć możliwość adaptacji do uzyskania min 2 slotów PCI-X lub posiadać takie sloty w standardzie.
Dyski HDD	2 x 300 GB SAS 10000 obrotów na minutę 6Gbs, Hot-Plug 2,5", możliwość zainstalowania minimalnie 8 dysków (SAS/SATA) w wewnętrznych zatokach serwera. Możliwość instalacji dysków w technologii SSD.
Kontroler macierzowy	Kontroler macierzowy SAS/SATA umożliwiający konfigurację dysków w RAID 0/1/10 z opcjonalną możliwością rozbudowy do RAID 6/60 oraz szyfrowania SED.
Karta rozszerzeń	Zintegrowane z płytą główną 2x GigabitEthernet. Karty sieciowe muszą wspierać load balancing, failover i TCP/IP Offload Engine. Możliwość instalacji dodatkowych dwóch interfejsów GigabitEthernet nie zajmujących slotu PCI-E.
Karta graficzna	Zintegrowana karta graficzna min. 16 MB
Porty	2 porty RJ-45 Gigabit Ethernet. 1 port RJ-45 dla interfejsu zdalnego zarządzania. 3 porty USB z czego przynajmniej 1 port umiejscowiony na panelu czołowym serwera. 1 port VGA. 1 port szeregowy.
Napęd dysków optycznych	DVD-ROM.
Zasilanie	Redundantne zasilacze typu Hot-Plug. Maksymalnie 460 W na zasilacz.
Chłodzenie	Redundantne wiatraki typu Hot-swap.
Zarządzanie	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.
Bezpieczeństwo	Wbudowany moduł TPM 1,2 do przechowywania kluczy kryptograficznych. Dodatkowo wbudowany panel diagnostyczny umożliwiający identyfikację uszkodzonego elementu serwera, wyposażony także w system przewidywania awarii poszczególnych elementów serwera takich ja: dysków twardych, pamięci RAM, zasilaczy, wiatraków, wraz oprogramowaniem pozwalającym na wysłanie komunikatów alarmowy do administratora.
Gwarancja i serwis	Urządzenie musi zostać objęte gwarancją oraz wsparciem technicznym producenta na okres minimum 36 miesięcy w trybie 24h/7 dni w tygodniu/365 dni w roku. Maksymalny czas usunięcia awarii – 12h od chwili zgłoszenia awarii. W przypadku, kiedy Wykonawca nie zdoła naprawić serwera w ciągu 12h, musi podstawić serwer zastępczy o parametrach nie gorszych od serwera Zamawiającego. Naprawa serwera musi być realizowana w siedzibie Zamawiającego. W przypadku uszkodzenia dysku twardego, uszkodzony dysk pozostaje u Zamawiającego.
System operacyjny	MS Windows Serwer 2008 R2 Standard PL 64bit(1-4 CPU, 5 CAL) lub równoważny.

## 5. Serwer o następujących parametrach minimalnych – 1 szt.

Nazwa elementu, parametru lub cechy	Opis wymagań
Obudowa	Obudowa o wysokości max. 2U, dedykowana do zamontowania w szafie rack 19" z zestawem szyn do montażu w szafie i wysuwania do celów serwisowych.
Procesor	Procesor czterordzeniowy dedykowany do pracy w serwerach wieloprocessorowych. Minimum Quad-Core Intel® Xeon® Processor E5620 (2,4 GHz, 1066 MHz, 12MB).
Liczba procesorów zainstalowanych	2 procesory
Płyta główna	Umożliwiająca instalację 2 procesorów, wykonana i zaprojektowana przez producenta serwera
Pamięć RAM	24GB PC3-10600 CL9 ECC DDR3 1333MHz LP RDIMM, z technologią ECC, ChipKill, memory mirroring, wymagane min. 12 slotów na kości pamięci. Oryginalna pamięć producenta serwera, przy czym każdy moduł pamięci musi posiadać tzw. part number producenta serwera.
Rozbudowa pamięci RAM	Możliwość rozbudowy pamięci RAM do min. 48GB na procesor. Łącznie do min. 96GB
Kontroler dysków twarde	Kontroler SAS/SATA RAID, min. 8 portów , pozwalający na zbudowanie poziomu RAID 0, 1, 10
Dyski twarde	6 x 300GB 3.5in HS 15K 6Gbps SAS HDD i 2 x 500GB 3.5in HS 7.2K SATA HDD, z możliwością wyciągnięcia podczas pracy serwera (hot swap)
Liczba wszystkich wnęk na dyski twarde	Minimum 8 wnęk typu hot swap 3.5". Możliwość instalacji dysków SATA/SAS.
Gniazda rozszerzeń	Minimum 2 gniazda PCI-Express x8
Napęd DVD	DVD- RW wewnętrzny
Interfejsy sieciowe	Minimum 2 porty 10/100/1000 wbudowane na płycie głównej.
Procedura przewidywania awarii	Obejmująca dyski, pamięć, procesory, zasilacze, wentylatory, VRM.
Zarządzanie	Zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera.
Grafika	Zintegrowana z płytą główną, pamięć minimum 16MB
Zasilacze	2 zasilacze Hot-Plug o mocy maksymalnie 460W
Wentylatory	Zestaw redundantnych wentylatorów.
Porty dodatkowe	Serwer musi być wyposażony minimum w następujące porty zewnętrzne: 2 porty RJ45 Gigabit Ethernet 1 port RJ45 dla interfejsu zdalnego zarządzania 3 porty USB, z czego przynajmniej 1 port umiejscowiony na panelu czołowym serwera 1 port VGA 1 port szeregowy.
Systemy operacyjne	Wspierane systemy: Microsoft Windows Server2008, Microsoft Windows Server 2003, Red Hat Enterprise Linux 5, SUSE Linux Enterprise Server 11.
Karty rozszerzeń	Serwer musi być wyposażony w kartę rozszerzeń umożliwiającą podłączenie zewnętrznego napędu LTO za pośrednictwem interfejsu danych SAS, jeśli w konfiguracji standardowej serwer nie posiada takiego interfejsu wyprowadzonego w postaci zewnętrznego portu w tylnej części obudowy.
Gwarancja i serwis	Urządzenie musi zostać objęte gwarancją oraz wsparciem technicznym producenta na okres minimum 36 miesięcy w trybie 24h/7dni w tygodniu/365 dni w roku. Maksymalny czas usunięcia awarii – 12h od chwili zgłoszenia awarii. W przypadku kiedy Wykonawca nie zdoła dokonać naprawy serwera w ciągu 12h, musi podstawić serwer zastępczy o nie gorszych parametrach od serwera Zamawiającego.



	Naprawa serwera musi być realizowana w siedzibie Zamawiającego. W przypadku uszkodzenia dysku twardego, uszkodzony dysk pozostaje u Zamawiającego.
Pochodzenie	Dostarczony sprzęt musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Wymagane oświadczenie producenta że oferowany do przetargu sprzęt spełnia ten wymóg. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne. Oferent zobowiązany jest dostarczyć wraz z ofertą, szczegółową specyfikację techniczną oferowanego sprzętu.
System operacyjny	MS Windows Serwer 2008 R2 Standard PL 64 bit(1-4 CPU, 5 CAL) lub równoważny. MS Windows Serwer 2008 CAL(100 users)

## 6. Szafa serwerowa – 1 szt. - o parametrach minimalnych:

- 1) szkielet sześć belek nośnych,
- 2) wysokość 42U, szerokość 800 mm, głębokość 1000mm
- 3) dwie osłony boczne z blachy pełnej,
- 4) drzwi przednie i tylne z blachy perforowanej o zwiększonej przewodności
- 5) dach pełny, przystosowany do montażu panela wentylacyjnego
- 6) cokół o wysokości 200 mm z wysuwaną ramą wsporczą,
- 7) listwę uziemienia oraz linki uziemienia drzwi, osłon i dachu,
- 8) zaślepki z włókniną do otworów płyty dolnej i górnej (komplet dla wszystkich otworów)
- 9) panel wentylacyjny z minimum 4-ema wentylatorami z możliwością sterowania termostatem
- 10) termostat do sterowania wentylatorami
- 11) dwie listwy zasilające po minimum 8 gniazd każda
- 12) gwarancja: 24 m-ce
- 13) deklaracje zgodności:
  - deklaracja informująca o tym, że oferowana szafa (wyrób) jest zgodna z postanowieniami następujących dyrektyw WE - dyrektywa o ogólnym bezpieczeństwie, wytyczne dotyczące maszyn, dyrektywa niskonapięciowa LVD, dyrektywa EMC – pod warunkiem wykorzystywania ich zgodnie z przeznaczeniem i z obowiązującymi normami i zaleceniami technicznymi
  - deklaracja informująca o tym, że oferowana szafa (wyrób) jest zgodne z postanowieniami dyrektyw RoHS 2002/95/WE (łącznie z jej wszystkimi zmianami i uzupełnieniami).

## 7. Streamer – urządzenie archiwizacji danych:

- 1) Streamer zewnętrzny LTO-4
- 2) Pojemność natywna: 800 GB
- 3) Pojemność z kompresją: 1600 GB
- 4) interfejs danych: SAS

Streamer musi współpracować z serwerem wyszczególnionym w pkt. 5.

Wraz ze streamerem Wykonawca dostarczy:

- taśma czyszcząca LTO – 3 szt
- taśma LTO4 800/1600 GB – 10 szt.

## 8. Usługi związane z montażem i konfiguracją zamawianych urządzeń:

W ramach realizacji przedmiotowego zamówienia wykonawca jest zobowiązany wykonać poniższe usługi.

1. Instalacja urządzeń sieciowych,
2. Instalacja urządzeń na styku z Internetem
3. Rekonfiguracja obecnej sieci LAN, w skład, której wejdzie:
  - a. Konfiguracja urządzeń do komunikacji z centralnym systemem zarządzania oraz rekonfiguracja obecnych ustawień
  - b. Konfiguracja dostarczonych przełączników oraz rekonfiguracja obecnych przełączników
  - c. Dokonanie aktualizacji oprogramowania
  - d. Konfiguracja STP na przełącznikach
  - e. Konfiguracja poziomu uprawnień do przełączników dla określonej grupy użytkowników
  - f. Konfiguracja routingu
  - g. Rekonfiguracja sieci w skład, której będzie wchodziła nowa adresacja dla urządzeń sieciowych, użytkowników
  - h. Wykreowanie sieci VLAN
  - i. Zdefiniowanie ACL na przełącznikach
  - j. Konfiguracja wybranych portów na urządzeniu do agregacji łączy protokołem 802.3ad LACP
4. Konfiguracja urządzeń na styku z Internetem:
  - a. Konfiguracja IPS do działania w trybie in-line,
  - b. Wydzielenie oraz rekonfiguracja strefy DMZ,
  - c. Wydzielenie puli adresów IP dla urządzeń w strefie DMZ,
  - d. Konfiguracja IPS do kontroli ruchu oraz zapobiegania włamaniom do strefy DMZ
  - e. Konfiguracja translacji adresów (statyczny NAT oraz PAT),
  - f. Konfiguracja firewalla mechanizmami ACL, QoS,
  - g. Konfiguracja urządzenia do inspekcji oraz blokowania ruchu P2P,
  - h. Konfiguracja urządzenia przed atakami typu DoS, DDoS,
  - i. Konfiguracja tunelu IPSec/VPN typu remote-access,
  - j. Konfiguracja urządzenia umożliwiająca dostęp poprzez SSH i HTTPS,
  - k. Aktualizacja oprogramowania
  - l. Konfiguracja urządzenia umożliwiająca przechowywanie zdarzeń lokalnie na urządzeniu oraz wyznaczonym do tego serwerze.
  - m. Konfiguracja High-availability
5. Testy weryfikujące poprawność działania i konfiguracji dostarczonych urządzeń
6. Wykonanie dokumentacji powykonawczej:
7. Instalacja zasilacza awaryjnego UPS:
  - przystosowanie istniejącej instalacji zasilającej do wymagań technicznych wynikających z parametrów techniczno-eksploatacyjnych dostarczonego UPS-a,
  - montaż i prace podłączeniowe nowego UPS-a wraz z osprzętem (wyłącznik awaryjny, bypass, adapter SNMP, detektor środowiskowy temperatury i wilgotności),
  - uruchomienie UPS-a i przeprowadzenie testów,
  - podłączenie, skonfigurowanie i uruchomienie adaptera SNMP,
  - skonfigurowanie UPS-a do współpracy z oprogramowaniem zarządzającym i uruchomienie monitorowania oraz zdalnego awaryjnego zamykania systemu na stacji roboczej wskazanej przez Zamawiającego,
  - wykonanie dokumentacji powykonawczej podłączenia urządzenia UPS oraz zasilania

urządzeń techniki informatycznej (dokumentację papierową należy dostarczyć w formie papierowej w ilości 2 egzemplarze oraz w formie elektronicznej na nośniku CD lub DVD w oparciu o program typu CAD tj \*dwg lub \*dxf w ilości 2 szt.

Dokumentacja powykonawcza musi zawierać m.in. :

- 1) zalecenia instalacyjne i eksploatacyjne producenta zawierające:
  - wartości zabezpieczeń elektrycznych
  - przekroje kabli zasilających
  - minimalną wytrzymałość stropu konieczną do zainstalowania urządzenia
  - sposób ustawienia urządzenia, w tym zachowanie minimalnych odległości od ścian
  - rodzaje i długości kabli połączeniowych
  - maksymalne i minimalne wartości temperatury i wilgotności, w których może być eksploatowane urządzenie (ze wskazaniem wartości optymalnych)
  - listę możliwych opcji sprzętowych i programowych oraz akcesoriów współpracujących z urządzeniem.
- 2) instrukcję obsługi i eksploatacji urządzenia zawierającą:
  - zasady obsługi i eksploatacji
  - wykaz i zasady wykonywania czynności konserwacyjnych i okresowych pomiarów kontrolnych parametrów techniczno-eksploatacyjnych urządzenia
  - opis podstawowych zasad diagnostyki w sytuacjach awaryjnych
  - podstawowe zasady BHP przy obsłudze urządzenia
  - opis instalacji oprogramowania zarządzającego pracą sieci komputerowej.