OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA

Dostawa sprzętu komputerowego, sprzętu sieciowego, akcesoriów komputerowych, serwerów, oprogramowania oraz licencji

1. POSTANOWIENIA OGÓLNE.

Przedmiotem niniejszego zamówienia jest rozbudowa istniejącej infrastruktury sieciowej i serwerowej Zamawiającego oraz posiadanej platformy kontroli dostępu do sieci NAC, znajdujących się w obecnej siedzibie Starostwa Powiatowego w Kielcach (budynek przy Al. IX Wieków Kielc 3), pod kątem potrzeb wyposażenia nowej siedziby Starostwa przy ul. Popiełuszki w Kielcach.

Celem niniejszego zamówienia jest zapewnienie wysokiej klasy rozwiązań z zakresu bezpiecznego dostępu użytkowników do repozytorium danych, sieci Internet oraz usług uruchamianych w ramach wewnętrznej sieci LAN oraz WLAN Przy wykorzystaniu posiadanej przez Zamawiającego platformy zarządzania infrastrukturą sieciową oraz siecią WLAN. Kluczowym elementem jest bezpieczna i wysokowydajna infrastruktura telekomunikacyjna pozwalająca na uruchomienie wielu usług jednocześnie, z zachowaniem wysokich parametrów pracy dla każdej z nich.

Postępowanie prowadzone jest w formie zadania, którym jest dostawa, montaż oraz instalacja i konfiguracja wszystkich wymaganych przez Zamawiającego komponentów infrastruktury serwerowej i sieciowej.

2. OPIS DOCELOWEJ INFRASTRUKTURY PASYWNEJ.

Budynek składający się z 5 kondygnacji obsługiwany będzie przez 10 Piętrowych Punktów Dystrybucyjnych PPD1-PPD10 oraz jeden Główny Punkt Dystrybucyjny GPD. W budynku zaprojektowano system okablowania światłowodowego o wydajność klasy OF 300 wg. PN-EN 50173-1:2009. Zastosowane przełącznice (panele krosowe) dla części światłowodowej zakończono interfejsem LC w konfiguracji wtyk-adapter-wtyk. Okablowanie szkieletowe wewnętrzne pomiędzy szafami GPD a PPD wykorzystuje kabel światłowodowy XG/OM3 uniwersalny 12x50/125/250µm z osłoną trudnopalną (ULSZH). Okablowanie miedziane - łączące punkty dystrybucyjne jest zrealizowane kablem podwójnie ekranowany typu S/FTP (PiMF) o paśmie przenoszenia 1200 MHz w osłonie niepalnej LSZH.

Instalacja okablowania strukturalnego obsługuje:

- Główny Punkt Dystrybucyjny GPD
- 10 Piętrowych Punktów Dystrybucyjnych PPD1 – PPD10

Główny Punkt Dystrybucyjny (GPD) stanowi sześć szaf typu 42U 19” 800x1000, ustawionych na cokole o wysokości 100mm oraz połączonych bokami. W Głównym Punkcie Dystrybucyjnym zlokalizowane zostaną następujące urządzenia sieciowe:

- serwery typu blade
- serwery typu host
- serwerowe przełączniki agregacyjne Top of Rack
- serwerowe przełączniki rdzeniowe
- system pamięci masowej

Piętrowy Punkt Dystrybucyjny (PPD) stanowi jedna lub dwie szafy typu 42U 19” 800x800, ustawione na cokole o wysokości 100mm.

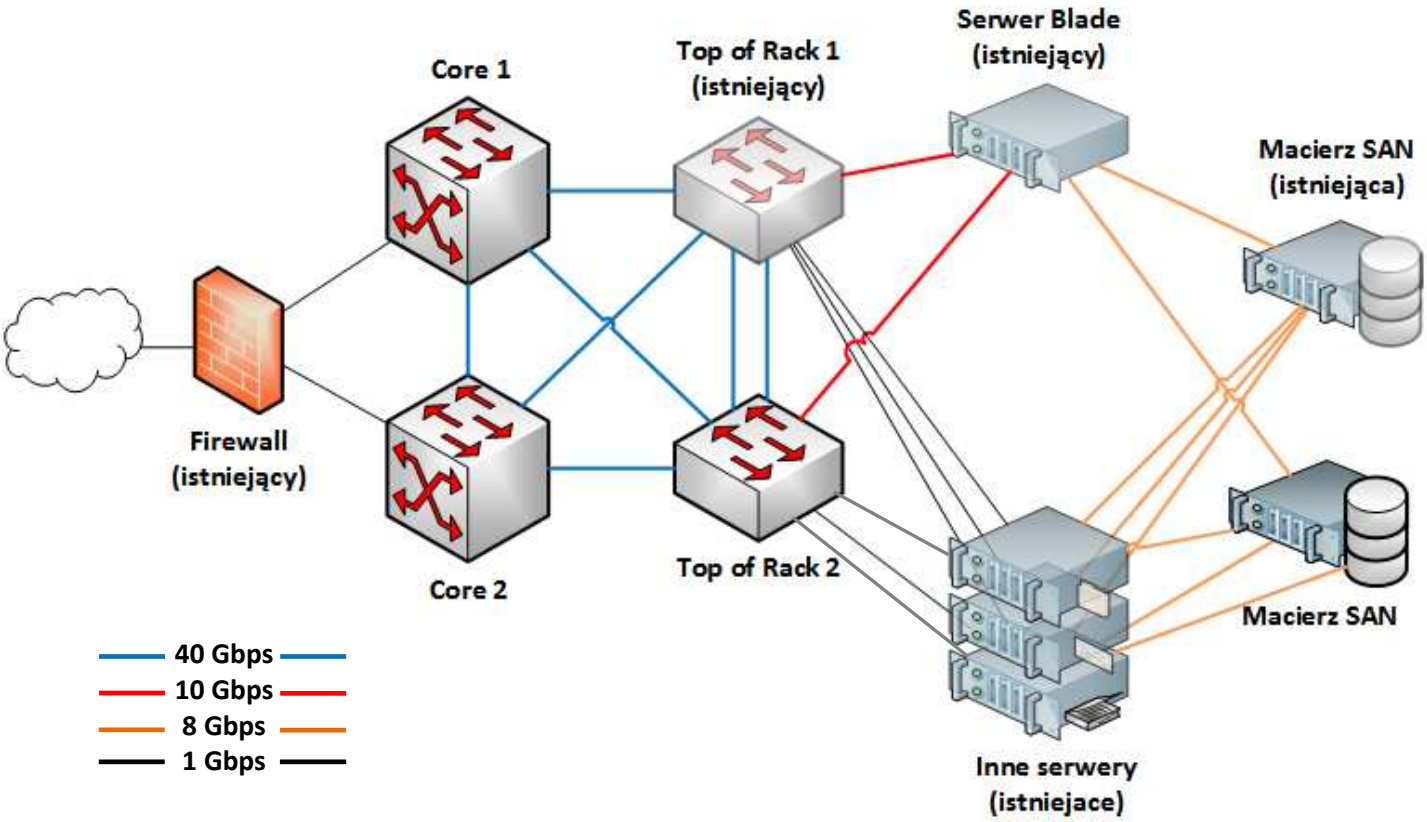
3. ROZBUDOWA GŁÓWNEGO PUNKTU DYSTRYBUCYJNEGO.

Jednym z przedmiotów niniejszego zamówienia jest rozbudowa Głównego Punktu Dystrybucyjnego stanowiącego punkt centralny infrastruktury sieciowej w obecnej lokalizacji Starostwa Powiatowego w Kielcach w oparciu o posiadane przez Zamawiającego rozwiązania sprzętowe oraz programowe. GPD jako centrum danych pełni rolę centralnego zarządzania (siecią fizyczną, sieciami wirtualnymi i pamięciami masowymi), wirtualizacji, łączności i systemu pamięci masowej.

W ramach postępowania Zamawiający wymaga dostarczenia następujących komponentów:

- ✓ dodatkowy (redundantny) serwerowy przełącznik agregacyjny Top of Rack - 1 sztuka
- ✓ sieciowy przełącznik rdzeniowy - 2 sztuki
- ✓ komplet niezbędnych interfejsów/modułów oraz okablowania
- ✓ dodatkowe serwery blade – 3 sztuki
- ✓ moduły pamięci RAM do rozbudowy posiadanych serwerów blade – 18 sztuk
- ✓ dodatkowy zasilacz do obudowy serwerów blade – 1 sztuka
- ✓ dodatkowe licencje do rozbudowy obudowy serwerów blade – 2 sztuki
- ✓ dodatkowa (redundantna) macierz dyskowa wraz z licencją replikacji zdalnej dla posiadanej przez Zamawiającego macierzy dyskowej Fujitsu ETERNUS DX90 S2

Strukturę docelową (wraz z już istniejącymi elementami) Głównego Punktu Dystrybucyjnego oraz wymagania odnośnie przepustowości pomiędzy poszczególnymi punktami przedstawia poniższych schemat:



Rys.1. Poglądowy schemat urządzeń Głównego Punktu Dystrybucyjnego.

3.1. Serwerowy przełącznik agregacyjny Top Of Rack

W związku z rozbudową posiadanej przez Zamawiającego infrastruktury sieciowej i serwerowej oraz aktualnie wykorzystywanymi urządzeniami i oprogramowaniem zarządzającym, a także w celu zapewnienia dowolności rekonfiguracji sprzętu oraz możliwości centralnego zarządzania Zamawiający wymaga aby serwerowy przełącznik agregacyjny:

1) umożliwiał połączenie z aktualnie zainstalowanym drugim przełącznikiem Top of Rack poprzez minimum dwa łącza 40 Gb QSFP+;
2) posiadał możliwość zbudowania jednego wirtualnego przełącznika z aktualnie zainstalowanym przełącznikiem Top of Rack. Przełącznik wirtualny powinien być widziany przez inne urządzenia sieciowe jako pojedyncze urządzenie zarówno pod kątem mechanizmów warstwy L2, L3 oraz L4. Technologia wirtualnego przełączania powinna automatycznie tworzyć agregację łączy, na których została ona uruchomiona;
3) wpierał technologię Data Center Bridging (DCB) – wsparcie konwergencji ruchu LAN i storage w strukturze zainstalowanego centrum danych. Rekomendowanym protokołem wymiany informacji jest Data Center Bridging Exchange (DCBX);
4) zapewniał pełną widoczność podłączonych do niego serwerów, pamięci masowych oraz środowisk wirtualnych z poziomu posiadanej i zainstalowanej w infrastrukturze aplikacji Data Center Manager firmy Enterasys;
5) przekazywał informacje na temat sprecyzowanych wcześniej odrębnych ról i profili przypisanych do poszczególnych serwerów, maszyn wirtualnych oraz aplikacji;
6) miał możliwość ustanowienia ról dla przepływów ruchu dedykowanych dla Data Center. Funkcja ta musi umożliwiać przypisanie minimum 100 ról i obsługiwać minimum 100 maszyn wirtualnych.

Ponadto w celu pełnej redundancji posiadanego sprzętu, oferowany przełącznik musi spełniać poniższe wymagania minimalne:

Serwerowy przełącznik agregacyjny Top Of Rack		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Interfejsy fizyczne	• Minimum 24 porty 1Gb/10 Gb SFP+, • Minimum 4 porty uplink 10Gb/40Gb QSFP+, • Minimum 1 port szeregowy konsoli do zarządzania.
2.	Montaż	• Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
3.	Pamięć i procesor	• Minimalna wielkość bufora pakietów 9 MB, • Ochrona CPU przed atakami typu Denial of Service (DoS).
4.	Wydajność	• Minimalna przepustowość: 575 Mpps, • Minimalna przepustowość przełączania: 800 Gbps.
5.	Zasilanie	• Przełącznik musi być zasilany z dwóch niezależnych źródeł zasilania. Moduły zasilające muszą zostać dostarczone wraz z przełącznikiem, • Przełącznik musi mieć możliwość doposażenia w minimum jeden dodatkowy moduł zasilania, • W przypadku awarii jednego ze źródeł zasilania drugie musi zapewniać możliwość wymiany w sposób zapewniający ciągłość pracy przełącznika, • Musi realizować chłodzenie w trybie „Exhaust” i „Intake” w zależności od dobranego modułu wentylatora i zasilacza.

6.	Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 128 tys.
7.	Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3, • Interfejs zarządzania sieci Web, • Standardowy interfejs wiersza poleceń CLI, • Zarządzanie IPv4/IPv6, • Zarządzanie wieloma kontami użytkowników lokalnych, • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie edytowalnej (Boot Prom) oraz pobieranie oprogramowania firmware przez port szeregowy, • Telnet Server/Client, • Secure Shell (SSHv2) Server/Client, • Syslog, • Audit Trail Logging, • Obsługa FTP/TFTP Client, • Simple Network Time Protocol (SNTP) lub NTP, • Management VLAN, • RMON – wsparcie dla 9 różnych grup, • Port Mirroring.
8.	Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły: • Generic VLAN Registration Protocol (GVRP), • 802.1Q VLANs, • 802.1D MAC Bridges, • 802.1s Multiple Spanning Tree, • 802.1t – Path Cost Amendment to 802.1D, • 802.3ad Link Aggregation z 64 grupami na 8 portach, • IP Multicast (IGMPv1,v2, v3), • Jumbo Packet ze wsparciem MTU Discovery Support dla interfejsu Gigabitowego (9216 bajtów) • Link Flap Detection, • Dynamic Egress (Automatyczna konfiguracja portu VLAN) • 802.1ab LLDP-MED • Data Center Bridging: o 802.1Qaz o ETS (Enhanced Transmission Selection) o DCBx (Data Center Bridge Exchange Protocol) o 802.1Qbb PFC (Priority Flow Control) o 802,1Qau Congestion Notification • 802.3-2008 Clause 57 (Ethernet OAM – Link Layer OAM) • IGMP v1/v2/v3 Snooping oraz Querier • MLD IPv6 Snooping oraz Querier • RFC 3580 IEEE 802.1 RADIUS Usage Guidelines, z VLAN to Policy Mapping • ARP Storm Prevention • MAC-to-Port Locking • Span Guard (Spanning Tree Protection) • RFC 2865 RADIUS • FC 2866 RADIUS Accounting • TACACS+ • Standard MIB

9.	QoS	• Algorytmy kolejkowania Strict Priority/ Weighted Round Robin • Ingress rate limiting • Obsługa min. 8 kolejek transmisyjnych na port • ToS/DSCP Marking/Remarking • 802.1p – Class of Service • 802.1D Priority-to-Transmit Queue Mapping
10.	Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o przez protokół 802.1X na porcie o przez sieć Web o wykorzystujące adres MAC • Obsługa wielu metod uwierzytelniania na jednym porcie, w dowolnie konfigurowalnej kolejności: o Uwierzytelnianie wielu użytkowników/maszyn na jednym porcie, wraz z przypisaniem specyficznych zasad użytkownikowi/urządzeniu/maszynie wirtualnej o Jednoczesne uwierzytelnianie, co najmniej 100 użytkowników/maszyn końcowych (sesji uwierzytelniających) na port o Zależne od wyników uwierzytelniania przypisywanie sieci VLAN dla co najmniej 100 sieci VLAN 802.1Q (untagged egress) na port. o Zależne od wyników uwierzytelniania przypisywanie sieci VLAN dla co najmniej 100 sieci VLAN 802.1Q (ingress) na port.
11.	Dodatkowe	• Wraz z przełącznikiem należy dostarczyć wymagane moduły/kable/przewody tego samego producenta, co dostarczane urządzenie do połączenia przełącznika z aktualnie zainstalowanym drugim przełącznikiem Top Of Rack poprzez dwa łącza 40 Gb QSFP+, • Wraz z przełącznikiem należy dostarczyć wymagane moduły/kable/przewody tego samego producenta, co dostarczane urządzenie do połączenia urządzenia z siecią LAN poprzez dwa łącza 40 Gb QSFP+, • Wraz z przełącznikiem należy dostarczyć minimum 20 modułów SFP+, do połączenia z posiadaną przez Zamawiającego infrastrukturą centrum danych, o parametrach: o Standard 10GBASE-USR lub 10GBASE-SR, o Współpraca ze standardem IEEE 802.3 MM, o Długość fali: 850 nm, o Minimalny zasięg: 100 m o Styk LC, o Moduły muszą pochodzić od tego samego producenta, co dostarczane urządzenie.
12.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.

3.3. Sieciowy przełącznik rdzeniowy

W związku z rozbudową posiadanej przez Zamawiającego infrastruktury sieciowej i serwerowej oraz konieczności uruchomienia pełnej funkcjonalności aktualnie wykorzystywanych urządzeń i oprogramowania zarządzającego infrastrukturą sieciową oraz dostępem do zasobów, a także w celu zapewnienia dowolności rekonfiguracji sprzętu i możliwości centralnego nim zarządzania Zamawiający wymaga aby sieciowe przełączniki rdzeniowe:

1) były połączone ze sobą przy użyciu łącza o przepustowości 40 Gbps. Zamawiający dopuszcza zastosowanie technologii agregacji łączy w celu osiągnięcia wymaganej przepustowości;
2) posiadały możliwość pracy jako jeden wirtualny przełącznik. Przełącznik wirtualny powinien być widziany przez inne urządzenia sieciowe jako pojedyncze urządzenie zarówno pod kątem mechanizmów warstwy L2, L3 oraz L4. Technologia wirtualnego przełączania powinna automatycznie tworzyć agregację łączy, na których została ona uruchomiona;
3) wspierały technologię równoważenia obciążenia pomiędzy znajdującymi się w infrastrukturze serwerami poprzez zastosowanie protokołu Load Sharing Network Address Translation (LSNAT). Zamawiający nie dopuszcza konieczności zakupu zewnętrznego oprogramowania lub urządzeń do równoważenia obciążenia ani modyfikacji konfiguracji stacji roboczych i serwerów;
4) wspierały technologię Shortest Path Bridging (SPB) opisaną standardem IEEE 802.1aq w celu dynamicznego routingu ścieżek w obrębie domeny uruchomionego centrum danych;
5) wpierały technologię Data Center Bridging (DCB) – wsparcie konwergencji ruchu LAN i SAN w strukturze posiadanego przez Zamawiającego centrum danych. Rekomendowanym protokołem wymiany informacji jest Data Center Bridging Exchange (DCBX);
6) implementowały architekturę opartą na przepływie strumieni danych poprzez technologię NetFlow lub równoważną. Monitorowanie sieci musi odbywać się bez użycia mechanizmów próbkowania danych, w czasie rzeczywistym oraz na każdym porcie sieciowych przełączników rdzeniowych. Zamawiający nie dopuszcza rozwiązań opartych na statystycznych metodach próbkowania lub rozwiązaniach bazujących na dodatkowych urządzeniach. Rekordy z informacją o przepływie, generowane przez sieciowe przełączniki rdzeniowe, będą analizowane przez posiadany przez Zamawiającego pakiet aplikacji do zarządzania siecią (Network Management Suite) NetSight firmy Enterasys;
7) umożliwiały zarządzane oraz implementację dowolnej funkcjonalności, wynikającej z karty katalogowej przełącznika, z poziomu posiadanego przez Zamawiającego pakietu aplikacji do zarządzania siecią (Network Management Suite) NetSight Advance firmy Enterasys.

Ponadto w celu pełnej integracji z posiadaną platformą zarządzającą oferowane przełączniki muszą spełniać poniższe wymagania minimalne:

Sieciowy przełącznik rdzeniowy		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Architektura	• Przełącznik musi posiadać budowę modularną umożliwiającą rozbudowę poprzez dodatkowe moduły zarządzająco-przełączające. • Przełącznik musi posiadać możliwość zainstalowania redundantnych modułów zarządzających lub modułów zarządzająco-przełączających w przypadku połączenia funkcji zarządzania i przełączania moduły te muszą działać w jednym czasie (Active–Active). • Wszystkie moduły muszą zapewniać możliwość wymiany w czasie pracy urządzania. Dotyczy to modułów zasilania, kart liniowych,

		modułów zarządzających oraz modułów przełączających, wentylatorów oraz wszelkich modułów dedykowanych. • Po wypełnieniu urządzenia wymaganymi modułami przełącznik musi posiadać przynajmniej dwa wolne gniazda rozszerzeń na dalszą rozbudowę systemu.
2.	Interfejsy fizyczne	• Minimum 24 porty 10 Gb SFP+ • Minimum 4 porty 10 Gb SFP+ mogące pracować w dwóch trybach: o tryb pozwalający na realizację wirtualnego przełącznika o tryb pozwalający na realizację połączeń pomiędzy przełącznikami z prędkością 10Gbps
3.	Montaż	• Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 9 U
4.	Pamięć i procesor	• Minimalna wielkość pamięci operacyjnej: 1GB na każdy moduł • Minimalna wielkość pamięci FLASH: 512 MB na każdy moduł • Minimalna wielkość bufora pakietów: 512 MB na każdy moduł
5.	Wydajność	• Każde gniazdo (przeznaczone do montażu kart zarządzających lub zarządzająco-przełączających) musi być podłączone do matrycy przełączającej/routującej szyną o przepustowości co najmniej 320Gb. • Maksymalne obłożenie modułami musi umożliwiać osiągniecie wydajności przełącznika na minimalnym poziomie 1280Gb.
6.	Zasilanie	• Przełącznik musi być zasilany z dwóch niezależnych źródeł zasilania. Moduły zasilające muszą zostać dostarczone wraz z przełącznikiem. • Przełącznik musi mieć możliwość doposażenia w minimum jeden dodatkowy moduł zasilania. • W przypadku awarii jednego ze źródeł zasilania drugie musi zapewniać możliwość wymiany w sposób zapewniający ciągłość pracy przełącznika.
7.	Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 128 tys.
8.	Sieci VLAN	• Wsparcie dla min. 4000 działających sieci wirtualnych (VLANs) • Wsparcie dla GVRP lub równoważne
9.	Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3 • Interfejs zarządzania sieci Web • Standardowy interfejs wiersza poleceń CLI • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania • Obsługa wielu plików konfiguracyjnych • Plik konfiguracyjny w formie edytowalnej (Boot Prom) oraz pobieranie oprogramowania firmware przez port szeregowy • Telnet Server/Client • Secure Shell (SSHv2) Server/Client • Syslog • Obsługa FTP/TFTP Client • Simple Network Time Protocol (SNTP) lub NTP • RFC 2865 RADIUS • RFC 2866 RADIUS Accounting • Management VLAN • TACACS+ • RMON – wsparcie dla 9 różnych grup • Port/VLAN mirroring (jeden do jednego, jeden do wielu)

10.	Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • Generic VLAN Registration Protocol (GVRP) • 802.1ab LLDP-MED • 802.1ad Provider Bridges • 802.1ag Connectivity Fault Management (CFM) • 802.1ak Multiple VLAN Registration Protocol (MVRP) • 802.1aq (SPB) Shortest Path Bridging (Ready) • 802.1ax-2008 / 802.3ad Link Aggregation - do 64 group po 8 portów na grupę • 802.1d MAC Bridges • 802.1q VLANs • 802.1s Multiple Spanning Tree • 802.1t Path Cost Amendment to 802.1D • 802.1w Rapid re-convergence of Spanning Tree • 802.3-2008 Clause 57 (Ethernet OAM – Link Layer OAM) • 802.3x Flow Control • IP Multicast (IGMPv1,v2,v 3) • IGMP v1/v2/v3 Snooping and Querier • Jumbo Packet ze wsparciem MTU Discovery Support dla interfejsu Gigabitowego (9216 bajtów) Link Flap Detection • Link Flap Detection • Dynamic Egress (Automated VLAN Port Configuration) • Data Center Bridging: o 802.1Qaz o ETS (Enhanced Transmission Selection) o DCBx (Data Center Bridge Exchange Protocol) o 802.1Qbb PFC (Priority Flow Control) o 802,1Qau Congestion Notification • MLD IPv6 Snooping and Querier • Pakiet Anty Spoofing: o DHCP Snooping o Dynamic Arp Inspection (DAI) o IP Source Guard • Standardowe listy ACL • Rozszerzone listy ACL • Sprzętowa realizacja NAT (Network Address Translation) • LSNAT (Load Sharing Network Address Translation) • TWCB (Transparent Web Cache Redirect) • Sprzętową obsługa nie próbkowanego mechanizmu NetFlow, lub równoważnego na każdym porcie bez straty wydajności urządzenia. • Funkcjonalność VPN dla BGP oraz MPLS
11.	Routing	Przełącznik musi obsługiwać następujące protokoły i technologie: • Sprzętowa obsługa routingu IPv4 i IPv6 • Trasy statyczne • RIPv2 • OSPF v1/v2/v3 • BGPv4 • Funkcjonalność IS-IS • Shortest Path Bridging (SPB) • Routing Multicast (IGMP v1/v2/v3, PIM-SM) • Policy-based Routing

		• Route Maps • VRRP, • VRF (Virtual Routing and Forwarding)
12.	Bezpieczeństwo	• Urządzenie musi wspierać profile bezpieczeństwa, profil bezpieczeństwa oznacza połączenie: o definicji sieci VLAN, o reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6, o realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6, o realizację zasad dublowania operacji dla ruchu IPv4 i IPv6 w warstwach L2-L4, o realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4. • Urządzenie musi obsługiwać możliwość zastosowania profilu bezpieczeństwa: o statycznie dla portu, o statycznie dla adresów MAC, o statycznie dla adresów IP, o statycznie dla VLAN-ów, o dynamicznie zgodnie z uwierzytelnieniem przez RADIUS. • Urządzenie musi umożliwiać wdrożenie profilu domyślnego do czasu dokonania poprawnej autentykacji i przydzielenia profilu docelowego.
13.	QoS	• Obsługa priorytetów zgodna z IEEE 802.1p. • Możliwość klasyfikacji pakietów w warstwach L2-L4 według: o źródłowego adresu MAC, o docelowego adresu MAC, o źródłowego adresu IP, o docelowego adresu IP, o UDP/TCP źródłowy port, o UDP/TCP docelowy port, o IP TOS, o IP Fragmentacja – klasyfikacja. • Sprzętowo realizowana obsługa minimum 16 kolejek priorytetów na każdym porcie. • Obsługa wielu mechanizmów kolejkowania (SPQ, WRR oraz ich kombinacji). • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego. • Możliwość przypisania ruchu do różnych sieci VLAN zgodnie z kryteriami L2-L4, nawet jeśli nie jest skonfigurowany protokół 802.1Q VLAN Tagging,
14.	Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o przez protokół 802.1X na porcie o przez sieć Web o wykorzystujące adres MAC
15.	Dodatkowe	• Wraz z przełącznikami należy dostarczyć wymagane moduły/kable/przewody tego samego producenta, co dostarczane urządzenia do połączenia obu przełączników rdzeniowych poprzez minimum 1 łącze 40 Gb QSFP+ lub 4 łącza 10 Gb SFP+, • Wraz z każdym przełącznikiem należy dostarczyć minimum 10

		modułów SFP+, do połączenia z przełącznikami dostępowymi, o parametrach: o Standard 10GBASE-SR, o Współpraca ze standardem IEEE 802.3 MM, o Długość fali: 850 nm, o Minimalny zasięg: 400 m o Styk LC, o Moduły muszą pochodzić od tego samego producenta, co dostarczane urządzenie.
16.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.

3.4. Serwer typu blade

W związku z rozbudową posiadanego przez Zamawiającego serwera typu blade o kolejne moduły serwerowe oraz rozszerzeniem pamięci operacyjnej posiadanych serwerów blade Zamawiający wymaga dostarczenia dodatkowych licencji dla posiadanych przez Zamawiającego przełączników FC poszerzających ilość obsługiwanych portów o kolejne 12 portów. Ponadto Zamawiający wymaga aby dostarczone komponenty spełniały poniższe parametry techniczne:

Serwer typu blade kompatybilny z obudową typu blade Fujitsu PRIMERGY BX900 S2		
Lp	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne urządzeń**
1.	Obudowa	• Typu blade, zgodna z posiadaną przez zamawiającego obudową Fujitsu BX900 S2; • możliwość instalacji 2 dysków SATA/SAS 2.0/ SSD, hotplug w obudowie serwera; • dioda pozwalająca na wizualną identyfikację serwera w obudowie; • diodowa sygnalizacja: pracy, usterki, aktywności połączeń LAN;
2.	Procesory	• Zainstalowane dwa procesory 8-rdzeniowe taktowane zegarem min. 2,10GHz, 20MB Cache, osiągające co najmniej 550 punktów w teście SPECint_rate2006; • Wymagane dostarczenie pełnego protokołu z testów SPEC poświadczonego przez producenta serwera lub wymagana obecność certyfikatu potwierdzającego osiągnięty wynik na stronie: www.spec.org
3.	Płyta główna	• Obsługa minimum dwóch procesorów ośmiordzeniowych; • Obsługa minimum 384 GB pamięci operacyjnej typu DDR3 z technologiami Advanced ECC, Chipkill (SDDC), wsparcie dla trybu aktywnej rezerwy i zapisu lustrzanego pamięci RAM; • Zaprojektowana i wyprodukowana przez producenta serwera; • Dwa złącza dla kart nakładkowych FC/Ethernet 10Gbit/IB typu mezzanine PCI Express gen. 3.0 x8 i dodatkowe złącze PCI Express gen.3 x8 na kontroler RAID; • wsparcie dla TPM 1.2 (możliwość integracji); • możliwość instalacji modułu flash do obsługi wirtualizatora (wewnętrzne złącze typu USB, niedostępne z zewnątrz serwera);
4.	Pamięć RAM	• Wyposażony w minimum 128 GB DDR3-1600

5.	Zintegrowane dyski / pamięć	• Zintegrowana pamięć wewnętrzna serwera typu flash min. 2GB • Pamięć typu flash min. 32GB w standardzie min. USB 2.0 przeznaczona do zainstalowania wewnątrz obudowy serwera blade w dedykowanym złączu USB.
6.	Interfejsy I/O , złącza	• Minimum 2 interfejsy LAN typu 10 Gbit/s ze wsparciem technologii Intel VT-c lub równoważnej podłączone poprzez backplane do switchy zainstalowanych w obudowie blade; • Dedykowany interfejs serwisowy typu LAN 100Mbit/s do obsługi i konfiguracji sprzętowej karty zarządzającej, możliwość przejęcia funkcji dedykowanego interfejsu serwisowego przez jeden z podstawowych interfejsów LAN 10 Gbit/s; • min. 2 interfejsy FC 8Gbit podłączone poprzez backplane do switchy zainstalowanych w obudowie blade;
7.	Oprogramowanie	• Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
8.	Zarządzanie	• Zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym; • Dedykowana karta LAN 10/100 Mb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera; • Umieszczona z przodu chowana karta identyfikacyjna serwera zawierająca nazwę serwera, numer seryjny, adresy MAC wbudowanych kart sieciowych;
9.	Gwarancja	• Na okres co najmniej 60 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. • Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego • Dostępność części zamiennych przez 5 lat od momentu zakończenia produkcji. • Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, • Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. • Oferent musi posiadać oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
10.	Inne	• 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; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.

3.5. Rozbudowa obudowy blade oraz poszerzenie pamięci operacyjnej RAM posiadanych serwerów.

Lp	Rozbudowa posiadanej przez Zamawiającego obudowy blade oraz serwerów typu blade	
1.	Rozbudowa serwerów blade	• Należy dostarczyć 18 kości pamięci 16GB RAM 1600MHz przeznaczonych dla posiadanych przez zamawiającego serwerów Fujitsu BX920 S3 (kości dostarczone przez producenta serwerów i przeznaczone dla serwerów posiadanych przez zamawiającego).
2.	Rozbudowa obudowy blade	• Należy dostarczyć licencję dla posiadanych przez zamawiającego przełączników FC przeznaczonych do obudowy Fujitsu BX900 S2 (model Brocade 5450) na rozbudowę o kolejne 12 aktywnych portów (dwie takie licencje, po jednej dla każdego z dwóch posiadanych przez zamawiającego przełączników). • Należy również dostarczyć dodatkowy zasilacz przeznaczony dla posiadanej przez zamawiającego obudowy Fujitsu BX900 S2 2880W klasy platinum wraz z przewodem zasilającym 16A C20->C19 1m

3.6. Macierz dyskowa SAN

Macierz dyskowa wraz z rozbudową posiadanej macierzy Fujitsu ETERNUS DX90 S2		
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne urządzenia**
1.	Obudowa	• Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych lub SSD kontrolowanych przez pojedynczą parę kontrolerów macierzowych (bez dodatkowych kontrolerów zewnętrznych, serwerów wirtualizujących, etc). Dostęp do macierzy realizowany jest poprzez redundantną sieć Storage Area Network (SAN) opartą o technologię FibreChannel 8Gb/s. • System musi być dostarczony ze wszystkimi komponentami do instalacji

		w standardowej szafie rack 19” z zajętością maks. 4U w tej szafie. • Obudowa musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy. • Obudowa powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy. • Obudowa nie może zawierać elementów typu bateria/akumulator wymagających jakiegokolwiek reżimu obsługowego: wymiana, przełączanie, ładowanie. • Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy - moduły dla rozbudowy musza posiadać obudowy o zajętości nie większej niż 2U w wyposażone w nadmiarowy układ zasilania i chłodzenia .
2.	Pojemność	• Dostarczony system musi umożliwiać instalację minimum 24 dysków formatu 2,5” oraz 12 dysków formatu 3,5” wykonanych jako dyski SAS lub NearLine-SAS lub SolidStateDrive. • System musi posiadać możliwość dołączania półek rozszerzeń umożliwiających uzyskanie sumarycznej przestrzeni dyskowej w trybie surowym (tzw. Raw) 480TB. • System musi mieć możliwość rozbudowy o redundantny kontroler RAID bez utraty wcześniej zapisanych danych. • Macierz musi umożliwiać instalacje dysków 2,5” oraz 3,5” w obrębie pojedynczego rozwiązania, wymagana jest możliwość instalacji maksymalnie 240 dysków w pojedynczym rozwiązaniu. • Macierz powinna posiadać możliwość późniejszej rozbudowy jak w pkt.2 wyłącznie poprzez zakup elementów sprzętowych. • Oferowana macierz musi zawierać 36 szt. Dysków w tym: ✓ maksymalnie 12 dysków NL-SAS 3.5” o prędkości obr. 7200 obr/min. ✓ 24 dyski 900GB SAS 2.5’’ o prędkości obrotowej 10 000 obr/min.
3.	Kontrolery	• System musi posiadać 2 kontrolery pracujące w układzie nadmiarowym typu active-active, z minimum 4GB pamięci podręcznej każdy. • W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik nie wymagający stosowania zasilania zewnętrznego lub bateryjnego. • Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia – dotyczy konfiguracji z dwoma kontrolerami RAID. • Macierz powinna pozwalać na wymianę kontrolera RAID bez utraty danych zapisanych na dyskach nawet w przypadku konfiguracji z jednym kontrolerem RAID. • W układzie z zainstalowanymi dwoma kontrolerami RAID zawartości pamięci podręcznej obydwu kontrolerów musi być identyczna tzw. cache mirror. • Każdy z kontrolerów RAID powinien posiadać dedykowany min. 1 interfejs RJ-45 Ethernet obsługujący połączenia z prędkościami : 1000Mb/s, 100Mb/s, 10Mb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.

4.	Interfejsy	• Oferowana macierz musi posiadać minimum 8 portów FC 8 Gb/s, do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, wyprowadzone po 4 porty na każdy kontroler RAID. • Macierz musi umożliwiać wymianę interfejsów każdego z kontrolerów RAID umożliwiając obsługę protokołów transmisji: FC 16Gb/s, iSCSI 1 Gb/s, iSCSI 10Gb/s FCoE 10Gb/s, SAS 2.0 6 Gb/s. • Wymiana portów j.w. nie może wymagać zmiany modelu kontrolerów RAID w oferowanym rozwiązaniu, w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych. • Interfejsy wspierane w rozwiązaniu nie mogą być wykorzystywane do innych pomocniczych rodzajów transmisji danych jak zarządzanie, konfiguracja zasobów macierzy. Zamawiający nie dopuszcza w tym wymaganiu zwielokrotniania interfejsów FC poprzez stosowanie zewnętrznych urządzeń aktywnych FC lub zarządzanych przez inne niż wbudowane w macierzy oprogramowanie kodowe.
5.	Poziomy RAID	Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1 ,1+0, 5, 6.
6.	Wspierane dyski	• Oferowana macierz musi wspierać: ✓ dyski technologii SAS 2.0 (6Gb/s), wspierające operacje hot-plug, o pojemnościach min. 300GB i prędkości obrotowej 15000 obrotów na minutę. ✓ dyski NL-SAS (NearLine SAS) z interfejsem SAS 2.0 6Gb/s, wspierające operacje hot-plug, o pojemnościach min. 1TB i prędkości obrotowej 7200 obrotów na minutę. ✓ dyski elektroniczne SolidStateDrive wykonane w technologii hot-plug o pojemnościach min. 100GB – macierz musi zapewniać obsługę min. 30 szt. dysków SSD w całym rozwiązaniu. • Interfejsy obsługiwanych dysków muszą być wyposażone w min. 2 porty SAS 2.0 6Gb/s, pracujące w reżimie full-duplex (jednoczesną transmisję danych przez dwa porty). • Macierz musi wspierać mieszaną konfigurację dysków SAS, NearLine-SAS i SSD w obrębie każdego pojedynczego modułu obudowy. • Macierz musi wspierać dla min. jednej z obsługiwanych technologii dyskowych mechanizm automatycznej przed awaryjnej migracji zapisów i składowanych danych na dysk zapasowy. • Macierz musi wspierać technologię energooszczędne typu Drive Spin Down lub wyłączanie dysków nieaktywnych w trybie ręcznym i automatycznym z wykorzystaniem mechanizmu typu ‘timescheduler’ czyli w zadanym i/lub powtarzalnym oknie czasowym. • Macierz musi umożliwiać definiowanie i obsługę dysków zapasowych tzw. hot-spare w trybach: ✓ hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID ✓ hot-spare dla zabezpieczania dowolnej grypy dyskowej RAID. • Macierz musi pozwalać na skonfigurowanie dowolnego dysku hot-plug w rozwiązaniu jako dysku zapasowego, niezależnie od miejsca jego fizycznej instalacji w dostarczonym rozwiązaniu.
7.	Opcje programowe	• Macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na min. 2048 kopii migawkowych.

		• Macierz musi wspierać Microsoft Volume ShadowCopy Services (VSS). • Macierz musi umożliwiać zdefiniowanie min. 4096 woluminów (LUN). • Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC lub iSCSI. • Dostarczone rozwiązanie musi umożliwiać szyfrowanie danych. Jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji należy dostarczyć je wraz z rozwiązaniem. • Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy lub bez konieczności wyłączania ścieżek logicznych FC/iSCSI/FCoE dla podłączonych stacji/serwerów. • Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji: ✓ zmiany rozmiaru woluminu, ✓ zmiany poziomu RAID, ✓ zmiany technologii dysków dla danej grupy RAID, ✓ dodawania nowych dysków do istniejącej grupy dyskowej. • Macierz musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server, SuSE Linux, RedHat Linux, HP-UNIX, IBM AIX, SUN Solaris, VMWare, Citrix XEN Server. • Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC/ iSCSI dla maksymalnej liczby podłączonych hostów. • Macierz musi obsługiwać woluminy logiczne o pojemności min. 128TB. • Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, z macierzą posiadaną przez zamawiającego (Fujitsu ETERNUS DX90 S2) z wykorzystaniem transmisji danych po protokołach FC oraz iSCSI, bez konieczności stosowania zewn. urządzeń konwersji wymienionych protokołów transmisji . Funkcjonalność replikacji danych musi być obsługiwana jako tzw. storage-based-replication, t.j. z poziomu oprogramowania wewnętrznego macierz. Jeżeli ta funkcjonalność wymaga licencjonowania należy w raz z macierzą dostarczyć taką licencję. • Macierz musi obsługiwać QoS (Quality of Services) czyli nadawanie priorytetów obsługi transmisji I/O dla skonfigurowanych hostów, LUN-ów, portów do hostów. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą w wariancie dla maksymalnej pojemności dyskowej danej macierzy • Macierz musi obsługiwać mechanizmy ograniczania wielkości pamięci podręcznej cache do obsługi wybranych woluminów LUN – tzw. cache partitioning. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą w wariancie dla maksymalnej pojemności • Macierz musi umożliwiać rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD • Macierz musi umożliwiać wirtualizację przydziału zasobów LUN dla hostów poprzez mechanizm ThinProvisioning, zamawiający wymaga dostarczenia stosownych licencji jeśli oferowane rozwiązanie tego wymaga.

8.	Konfiguracja, zarządzanie	• Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej bez konieczności dedykowania oddzielnego serwera do obsługi tego oprogramowania. • Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. • Pełne zdalne zarządzanie macierzą powinno być możliwe bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora. • Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.
9.	Gwarancja i serwis	• Całe rozwiązanie musi być objęte minimum 36 miesięcznym okresem gwarancji z naprawą w miejscu instalacji urządzenia w następnym dniu roboczym od zgłoszenia. Uszkodzone dyski pozostają u zamawiającego. • Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia w ciągu 36 miesięcy od daty zakupu. • System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez protokół SNMP (wersja: 1 ,2c, 3) lub SMTP. • Macierz musi pochodzić z legalnego kanału sprzedaży producenta w Polsce i musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych. • Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia • Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta sprzętu. • Oferent musi posiadać oświadczenie producenta , że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. • Serwis gwarancyjny macierzy oraz rozwiązania do wirtualizacji świadczony będzie w języku polskim**.** • W przypadku awarii dysku twardego, dysk pozostaje u Zamawiającego.
10.	Wsparcie techniczne producenta	Wsparcie techniczne musi być realizowane poprzez: • dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej, dającej możliwość weryfikacji konfiguracji fabrycznej zakupionego sprzętu, a także weryfikacji posiadanej/wykupionej gwarancji oraz statusu napraw urządzenia po podaniu unikalnego numeru seryjnego. • Dedykowany numer oraz email dla zgłoszeń awarii sprzętu objętego gwarancją typu OnSite, czynny 24h na dobę przez 365 dni w roku. • Wymagane są, przeglądy konserwacyjne, ocena stanu macierzy oraz rozwiązania do wirtualizacji i środowiska ich pracy oraz nanoszenie poprawek mikrokodu i oprogramowania. • Opiekę dedykowanego dla danej instalacji inżyniera serwisowego oraz co

		najmniej 60 godzin konsultacji technicznych rocznie w trakcie obowiązywania gwarancji.
11.	Rozbudowa posiadanej macierzy	• Należy dostarczyć licencję dla posiadanej przez zamawiającego macierzy Fujitsu ETERNUS DX90 S2 która pozwoli na wykonywanie replikacji pomiędzy macierzą posiadaną przez zamawiającego, a macierzą objętą niniejszym postępowaniem przetargowym

3.7. Zestawienie ilościowe.

Lp.	Element	Ilość
1.	Serwerowy przełącznik agregacyjny Top Of Rack	1 szt.
1a.	Moduł światłowodowy SR lub USR LC SFP+	20 szt.
2.	Sieciowy przełącznik rdzeniowy	2 szt.
2a.	Moduł światłowodowy SR LC SFP+	20 szt.
3.	Serwer typu blade	3 szt.
3a.	Moduły pamięci RAM do serwerów	18 szt.
3b.	Licencja rozszerzająca dla przełączników Brocade 5450	2 szt.
3c.	Zasilacz do obudowy blade	1 szt.
4.	Macierz dyskowa SAN	1 szt.
4a.	Licencja replikacji zdalnej „Remote copy” danych (jedna dla macierzy posiadanej przez Zamawiającego, druga dla macierzy dostarczanej)	2 szt.
4b.	Licencja „Local copy” (dla macierzy dostarczanej)	1 szt.
4c.	Licencja „Thin Provisioning” (dla macierzy dostarczanej)	1 szt.

4. WYPOSAŻENIE PIĘTROWYCH PUNKTÓW DYSTRYBUCYJNYCH.

Wyposażenie Piętrowych Punktów Dystrybucyjnych (PPD) w aktywne urządzenia sieciowe, stanowiące część dostępową infrastruktury, obejmuje dostarczenie urządzeń w pełni integrujących się z posiadanym przez Zamawiającego systemem zarządzania dostępem do sieci (NAC).

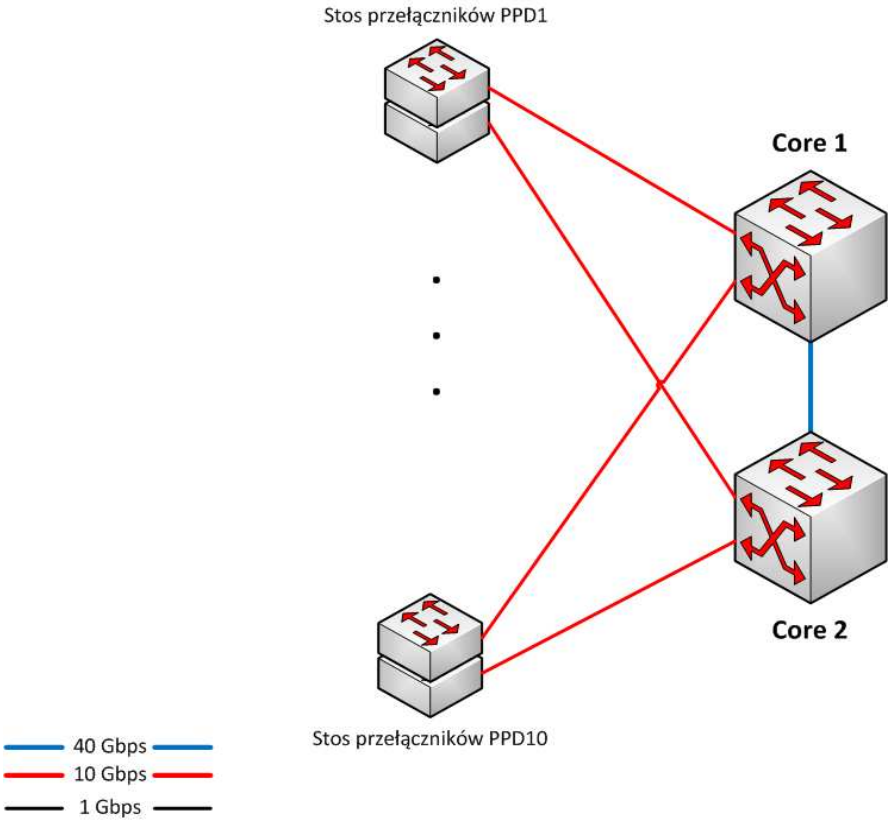
W ramach okablowania strukturalnego w poszczególnych PPD Zamawiający posiada następującą liczbę linii:

Piętrowy Punkt Dystrybucyjny	Liczba linii okablowania strukturalnego
PPD1	200
PPD2	92
PPD3	211
PPD4	233
PPD5	268
PPD6	237
PPD7	285
PPD8	281
PPD9	276
PPD10	257

Okablowanie szkieletowe pomiędzy szafami GPD a PPD zaprojektowano w oparciu o kabel światłowodowy XG/OM3 uniwersalny 12x50/125/250µm oraz interfejs LC.

4.1. Sieciowe przełączniki dostępowe.

Zamawiający przewiduje podłączenie każdego PPD z GPD za pomocą dwóch łączy o przepustowości 10 Gbps przy zachowaniu redundancji połączeń – po jednym do każdego z dwóch sieciowych przełączników rdzeniowych znajdujących się w GPD. W ramach każdego z PPD zainstalowana zostanie odpowiadająca mu liczba przełączników tworzących stos/wieżę, widziana przez inne urządzenia sieciowe jako pojedyncze urządzenie logiczne. Opisaną topologię przedstawia poniższy schemat:



W związku z rozbudową posiadanej przez Zamawiającego infrastruktury sieciowej i serwerowej oraz koniecznością uruchomienia pełnej funkcjonalności aktualnie wykorzystywanych urządzeń i oprogramowania zarządzającego infrastrukturą sieciową i dostępem do zasobów, a także w celu zapewnienia dowolności rekonfiguracji sprzętu oraz możliwości centralnego nim zarządzania Zamawiający wymaga aby sieciowe przełączniki dostępowe:

1) w ramach pojedynczego PPD posiadały możliwość pracy jako jeden wirtualny przełącznik. Przełącznik wirtualny powinien być widziany przez inne urządzenia sieciowe jako pojedyncze urządzenie zarówno pod kątem mechanizmów warstwy L2, L3 oraz L4. Technologia połączenia przełączników w stos/wieżę musi być wykonana przy użyciu dedykowanych portów bez konieczności ograniczania liczby portów dostępowych;
2) posiadały możliwości klasyfikowania pakietów warstw L2,L3 oraz L4, które mogą opierać się na ID portu fizycznego, adresie MAC, podsieci IP, adresie IP, typie protokołu IP, IP ToS (Type of Service), DSCP (Differentiated Services Code Point) oraz porcie TCP/UDP;
3) zapewniały wykrywanie lokalizacji systemów końcowych w czasie rzeczywistym i przechowywanie tych informacji w centralnej bazie danych;
4) umożliwiały zarządzane oraz implementację dowolnej funkcjonalności, wynikającej z karty katalogowej przełącznika, z poziomu posiadanego przez Zamawiającego pakietu aplikacji do zarządzania siecią (Network Management Suite) NetSight Advance firmy Enterasys;
5) obsługiwały uwierzytelnianie wielu systemów końcowych poprzez IEEE 802.1X, portal internetowy oraz adresie MAC jednocześnie na każdym porcie;
6) posiadały możliwość egzekwowania ról oraz profili systemów końcowych zgodnie z regułami zdefiniowanymi przy użyciu posiadanego przez Zamawiającego pakietu aplikacji do zarządzania siecią (Network Management Suite) NetSight Advance firmy Enterasys;
7) zapewniały ciągłe zarządzanie tożsamością użytkowników/urządzeń wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma przy użyciu

posiadanego przez Zamawiającego rozwiązania Network Access Control (NAC) firmy Enterasys.

Ponadto w celu pełnej integracji z posiadana platformą zarządzającą oferowane przełączniki muszą spełniać poniższe wymagania minimalne:

Sieciowy przełącznik dostępowy typu A		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Architektura	• Przełączniki muszą mieć możliwość łączenia w stosy/wieże do 8 przełączników lub budowę modularną, zapewniając możliwość rozbudowy liczby portów w poszczególnych punktach dystrybucyjnych, • Połączenie urządzeń w stos/wieżę powinno zapewniać redundancję - połączenie przełączników w pętlę zwrotną, • Zarządzanie stosem/wieżą poprzez 1 adres IP.
2.	Interfejsy fizyczne	• Minimum 48 portów 10/100/1000 BASE-T RJ45 PoE (zgodnych ze standardami 802.3.af oraz 802.3.at), z technologią auto-sensing, auto-negotiating MDI/MDI-X • Minimum 2 porty uplink 10 GBase-X SFP+, • Minimum 2 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania (COMBO), • Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych, • Minimum 1 port konsolowy do zarządzania przełącznikiem.
3.	Montaż	• Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
4.	Pamięć i procesor	• Minimalna wielkość pamięci SDRAM: 512 MB, • Minimalna wielkość pamięci FLASH: 32 MB.
5.	Wydajność	• Minimalna przepustowość: 100 Mpps, • Minimalna przepustowość przełączania: 128 Gbps na przełącznik, • Minimalna wydajność połączenia w stosie: 48 Gbps, a w urządzeniach modularnych minimum 48 Gbps pomiędzy modułami, • Przełącznik musi zapewniać przełączanie z pełną prędkością łącza w obie strony.
6.	Zasilanie	• Przełączniki muszą być wyposażone w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3at oraz 802.3af, • Przełączniki dodawane do stosu/wieży muszą zapewniać moc do 375W dla funkcjonalności PoE, • Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania zapewniając zasilanie dla wszystkich portów PoE zgodnie ze standardami 802.3af oraz 802.3at.
7.	Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 32 000.
8.	Sieci VLAN	• Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP, • Obsługa minimum 4 000 ID sieci VLAN oraz minimum 1 000 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
9.	Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3,

		• Standardowy interfejs wiersza poleceń CLI, • Secure Shell (SSHv2), • Secured Socket Layer (SSL), • RFC 2865 RADIUS, • RFC 2866 RADIUS Accounting, • TACACS+, przy czym TACACS+ musi zapewniać obsługę zarządzania AAA (uwierzytelniania, autoryzacja i audytowanie). • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie tekstowej, • Telnet, • Syslog, • Secure Copy oraz Secure FTP, • Simple Network Time Protocol (SNTP) lub NTP, • RMON – wsparcie dla 6 różnych grup, • Port mirroring (jeden do jednego, wiele do jednego), • Monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP, • Redundantne zarządzanie stosem.
10.	Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • LLDP/LLDP-MED • 802.3ad Link Aggregation • 802.1D MAC Bridges • 802.1s Multiple Spanning Tree • 802.1t Path Cost Amendment to 802.1D • 802.1w Rapid re-convergence of Spanning Tree • 802.3x Flow Control • IP Multicast (IGMPv1,v2,v 3) • IGMP v1/v2/v3 Snooping • Ramki Jumbo Frames (minimum 9 kB) • Standardowe listy ACL • Rozszerzone listy ACL • RIPv1 i RIPv2, • Trasy statyczne • DHCP/BootP Relay
11.	Bezpieczeństwo	Przełącznik musi obsługiwać następujące funkcjonalności: • Musi mieć możliwość pracy w architekturze bezpieczeństwa opartej na rolach. Zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, • Ochrona przed atakami typu DHCP/ARP Spoof Protection • Obsługa MAC Port Locking (dynamiczne i statyczne).
12.	QoS	Przełącznik musi obsługiwać następujące funkcjonalności: • Obsługa priorytetów zgodna z IEEE 802.1p, • Możliwość klasyfikacji pakietów w warstwach L2-L4 według: o ID portu fizycznego, o Adresie MAC, o Podsieci IP, o Adresie IP, o Typie protokołu IP, o IP ToS (Type of Service), o DSCP (Differentiated Services Code Point),

		○ Porcie TCP/UDP, • Sprzętowo realizowana obsługa minimum 8 kolejek priorytetów na każdym porcie, • Obsługa wielu mechanizmów kolejkowania (SPQ, WRR oraz ich kombinacji), • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego, • Możliwość przypisania ruchu do różnych sieci VLAN zgodnie z kryteriami L2-L4, nawet jeśli nie jest skonfigurowany protokół 802.1Q VLAN Tagging.
13.	Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: ○ poprzez IEEE 802.1x, ○ wykorzystujące adres MAC, ○ wykorzystujące przeglądarkę internetową, • Uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla minimalnie 4 użytkowników/urządzeń na port, • Obsługa Dynamic VLAN Assignment (RFC 3580), • Obsługa wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (minimum 4).
14.	Dodatkowe	• Wraz z każdym przełącznikiem należy dostarczyć 1 moduł SFP+, do połączenia z przełącznikiem rdzeniowym, o parametrach: ○ Standard 10GBASE-SR, ○ Współpraca ze standardem IEEE 802.3 MM, ○ Długość fali: 850 nm, ○ Minimalny zasięg: 400 m ○ Styk LC, ○ Moduł musi pochodzić od tego samego producenta, co dostarczane urządzenie.
15.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.
	Sieciowy przełącznik dostępowy typu B	
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Architektura	• Przełączniki muszą mieć możliwość łączenia w stosy/wieże do 8 przełączników lub budowę modularną, zapewniając możliwość rozbudowy liczby portów w poszczególnych punktach dystrybucyjnych, • Połączenie urządzeń w stos/wieżę powinno zapewniać redundancję - połączenie przełączników w pętlę zwrotną, • Zarządzanie stosem/wieżą poprzez 1 adres IP.
2.	Interfejsy fizyczne	• Minimum 24 porty 10/100/1000 BASE-T RJ45 PoE (zgodnych ze standardami 802.3.af oraz 802.3.at), z technologią auto-sensing, auto-negotiating MDI/MDI-X • Minimum 2 porty uplink 10 GBase-X SFP+, • Minimum 2 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania (COMBO), • Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych,

		• Minimum 1 port konsolowy do zarządzania przełącznikiem.
3.	Montaż	• Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
4.	Pamięć i procesor	• Minimalna wielkość pamięci SDRAM: 512 MB, • Minimalna wielkość pamięci FLASH: 32 MB.
5.	Wydajność	• Minimalna przepustowość: 64 Mpps, • Minimalna przepustowość przełączania: 82 Gbps na przełącznik, • Minimalna wydajność połączenia w stosie: 48 Gbps, a w urządzeniach modularnych minimum 48 Gbps pomiędzy modułami, • Przełącznik musi zapewniać przełączanie z pełną prędkością łącza w obie strony.
6.	Zasilanie	• Przełączniki muszą być wyposażone w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3at oraz 802.3af, • Przełączniki dodawane do stosu/wieży muszą zapewniać moc do 375W dla funkcjonalności PoE, • Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania zapewniając zasilanie dla wszystkich portów PoE zgodnie ze standardami 802.3af oraz 802.3at.
7.	Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 32 000.
8.	Sieci VLAN	• Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP, • Obsługa minimum 4 000 ID sieci VLAN oraz minimum 1 000 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
9.	Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3, • Standardowy interfejs wiersza poleceń CLI, • Secure Shell (SSHv2), • Secured Socket Layer (SSL), • RFC 2865 RADIUS, • RFC 2866 RADIUS Accounting, • TACACS+, przy czym TACACS+ musi zapewniać obsługę zarządzania AAA (uwierzytelniania, autoryzacja i audytowanie). • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie tekstowej, • Telnet, • Syslog, • Secure Copy oraz Secure FTP, • Simple Network Time Protocol (SNTP) lub NTP, • RMON – wsparcie dla 6 różnych grup, • Port mirroring (jeden do jednego, wiele do jednego), • Monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP, • Redundantne zarządzanie stosem.
10.	Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • LLDP/LLDP-MED • 802.3ad Link Aggregation • 802.1D MAC Bridges • 802.1s Multiple Spanning Tree

		• 802.1t Path Cost Amendment to 802.1D • 802.1w Rapid re-convergence of Spanning Tree • 802.3x Flow Control • IP Multicast (IGMPv1,v2,v 3) • IGMP v1/v2/v3 Snooping • Ramki Jumbo Frames (minimum 9 kB) • Standardowe listy ACL • Rozszerzone listy ACL • RIPv1 i RIPv2, • Trasy statyczne • DHCP/BootP Relay
11.	Bezpieczeństwo	Przełącznik musi obsługiwać następujące funkcjonalności: • Musi mieć możliwość pracy w architekturze bezpieczeństwa opartej na rolach. Zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, • Ochrona przed atakami typu DHCP/ARP Spoof Protection • Obsługa MAC Port Locking (dynamiczne i statyczne).
12.	QoS	Przełącznik musi obsługiwać następujące funkcjonalności: • Obsługa priorytetów zgodna z IEEE 802.1p, • Możliwość klasyfikacji pakietów w warstwach L2-L4 według: o ID portu fizycznego, o Adresie MAC, o Podsieci IP, o Adresie IP, o Typie protokołu IP, o IP ToS (Type of Service), o DSCP (Differentiated Services Code Point), o Porcie TCP/UDP, • Sprzętowo realizowana obsługa minimum 8 kolejek priorytetów na każdym porcie, • Obsługa wielu mechanizmów kolejkowania (SPQ, WRR oraz ich kombinacji), • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego, • Możliwość przypisania ruchu do różnych sieci VLAN zgodnie z kryteriami L2-L4, nawet jeśli nie jest skonfigurowany protokół 802.1Q VLAN Tagging.
13.	Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o poprzez IEEE 802.1x, o wykorzystujące adres MAC, o wykorzystujące przeglądarkę internetową, • Uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla minimalnie 4 użytkowników/urządzeń na port, • Obsługa Dynamic VLAN Assignment (RFC 3580), • Obsługa wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (minimum 4).
14.	Dodatkowe	• Wraz z każdym przełącznikiem należy dostarczyć 1 moduł SFP+, do połączenia z przełącznikiem rdzeniowym, o parametrach:

		o Standard 10GBASE-SR, o Współpraca ze standardem IEEE 802.3 MM, o Długość fali: 850 nm, o Minimalny zasięg: 400 m o Styk LC, o Moduł musi pochodzić od tego samego producenta, co dostarczane urządzenie.
15.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.
Sieciowy przełącznik dostępowy typu C		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Architektura	• Przełączniki muszą mieć możliwość łączenia w stosy/wieże do 8 przełączników lub budowę modularną, zapewniając możliwość rozbudowy liczby portów w poszczególnych punktach dystrybucyjnych, • Połączenie urządzeń w stos/wieżę powinno zapewniać redundancję - połączenie przełączników w pętlę zwrotną, • Zarządzanie stosem/wieżą poprzez 1 adres IP.
2.	Interfejsy fizyczne	• Minimum 48 portów 10/100/1000 BASE-T RJ45 PoE (zgodnych ze standardami 802.3.af oraz 802.3.at), z technologią auto-sensing, auto-negotiating MDI/MDI-X • Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania (COMBO), • Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych, • Minimum 1 port konsolowy do zarządzania przełącznikiem.
3.	Montaż	• Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
4.	Pamięć i procesor	• Minimalna wielkość pamięci SDRAM: 512 MB, • Minimalna wielkość pamięci FLASH: 32 MB.
5.	Wydajność	• Minimalna przepustowość: 70 Mpps, • Minimalna przepustowość przełączania: 90 Gbps na przełącznik, • Minimalna wydajność połączenia w stosie: 48 Gbps, a w urządzeniach modularnych minimum 48 Gbps pomiędzy modułami, • Przełącznik musi zapewniać przełączanie z pełną prędkością łącza w obie strony.
6.	Zasilanie	• Przełączniki muszą być wyposażone w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3at oraz 802.3af, • Przełączniki dodawane do stosu/wieży muszą zapewniać moc do 375W dla funkcjonalności PoE, • Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania zapewniając zasilanie dla wszystkich portów PoE zgodnie ze standardami 802.3af oraz 802.3at.
7.	Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 32 000.
8.	Sieci VLAN	• Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP,

		• Obsługa minimum 4 000 ID sieci VLAN oraz minimum 1 000 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
9.	Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3, • Standardowy interfejs wiersza poleceń CLI, • Secure Shell (SSHv2), • Secured Socket Layer (SSL), • RFC 2865 RADIUS, • RFC 2866 RADIUS Accounting, • TACACS+, przy czym TACACS+ musi zapewniać obsługę zarządzania AAA (uwierzytelniania, autoryzacja i audytowanie). • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie tekstowej, • Telnet, • Syslog, • Secure Copy oraz Secure FTP, • Simple Network Time Protocol (SNTP) lub NTP, • RMON – wsparcie dla 6 różnych grup, • Port mirroring (jeden do jednego, wiele do jednego), • Monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP, • Redundantne zarządzanie stosem.
10.	Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • LLDP/LLDP-MED, • 802.3ad Link Aggregation, • 802.1D MAC Bridges, • 802.1s Multiple Spanning Tree, • 802.1t Path Cost Amendment to 802.1D, • 802.1w Rapid re-convergence of Spanning Tree, • 802.3x Flow Control, • IP Multicast (IGMPv1,v2,v 3), • IGMP v1/v2/v3 Snooping, • Ramki Jumbo Frames (minimum 9 kB), • Standardowe listy ACL, • Rozszerzone listy ACL, • RIPv1 i RIPv2, • Trasy statyczne, • DHCP/BootP Relay.
11.	Bezpieczeństwo	Przełącznik musi obsługiwać następujące funkcjonalności: • Musi mieć możliwość pracy w architekturze bezpieczeństwa opartej na rolach. Zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, • Ochrona przed atakami typu DHCP/ARP Spoof Protection • Obsługa MAC Port Locking (dynamiczne i statyczne).
12.	QoS	Przełącznik musi obsługiwać następujące funkcjonalności: • Obsługa priorytetów zgodna z IEEE 802.1p, • Możliwość klasyfikacji pakietów w warstwach L2-L4 według: o ID portu fizycznego, o Adresie MAC, o Podsieci IP,

		o Adresie IP, o Typie protokołu IP, o IP ToS (Type of Service), o DSCP (Differentiated Services Code Point), o Porcie TCP/UDP, • Sprzętowo realizowana obsługa minimum 8 kolejek priorytetów na każdym porcie, • Obsługa wielu mechanizmów kolejkowania (SPQ, WRR oraz ich kombinacji), • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego, • Możliwość przypisania ruchu do różnych sieci VLAN zgodnie z kryteriami L2-L4, nawet jeśli nie jest skonfigurowany protokół 802.1Q VLAN Tagging.
13.	Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o poprzez IEEE 802.1x, o wykorzystujące adres MAC, o wykorzystujące przeglądarkę internetową, • Uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla minimalnie 4 użytkowników/urządzeń na port, • Obsługa Dynamic VLAN Assignment (RFC 3580), • Obsługa wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (minimum 4).
14.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.
Sieciowy przełącznik dostępowy typu D		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
2	Architektura	• Przełączniki muszą mieć możliwość łączenia w stosy/wieże do 8 przełączników lub budowę modularną, zapewniając możliwość rozbudowy liczby portów w poszczególnych punktach dystrybucyjnych, • Połączenie urządzeń w stos/wieżę powinno zapewniać redundancję - połączenie przełączników w pętlę zwrotną, • Zarządzanie stosem/wieżą poprzez 1 adres IP.
2.	Interfejsy fizyczne	• Minimum 24 porty 10/100/1000 BASE-T RJ45 PoE (zgodnych ze standardami 802.3.af oraz 802.3.at), z technologią auto-sensing, auto-negotiating MDI/MDI-X • Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania (COMBO), • Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych, • Minimum 1 port konsolowy do zarządzania przełącznikiem.
3.	Montaż	• Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
4.	Pamięć i procesor	• Minimalna wielkość pamięci SDRAM: 512 MB, • Minimalna wielkość pamięci FLASH: 32 MB.

5.	Wydajność	• Minimalna przepustowość: 35 Mpps, • Minimalna przepustowość przełączania: 48 Gbps na przełącznik, • Minimalna wydajność po łączenia w stosie: 48 Gbps, a w urządzeniach modularnych minimum 48 Gbps pomiędzy modułami, • Przełącznik musi zapewniać przełączanie z pełną prędkością łącza w obie strony.
6.	Zasilanie	• Przełączniki muszą być wyposażone w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3at oraz 802.3af, • Przełączniki dodawane do stosu/wieży muszą zapewniać moc do 375W dla funkcjonalności PoE, • Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania zapewniając zasilanie dla wszystkich portów PoE zgodnie ze standardami 802.3af oraz 802.3at.
7.	Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 32 000.
8.	Sieci VLAN	• Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP, • Obsługa minimum 4 000 ID sieci VLAN oraz minimum 1 000 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
9.	Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3, • Standardowy interfejs wiersza poleceń CLI, • Secure Shell (SSHv2), • Secured Socket Layer (SSL), • RFC 2865 RADIUS, • RFC 2866 RADIUS Accounting, • TACACS+, przy czym TACACS+ musi zapewniać obsługę zarządzania AAA (uwierzytelniania, autoryzacja i audytowanie). • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie tekstowej, • Telnet, • Syslog, • Secure Copy oraz Secure FTP, • Simple Network Time Protocol (SNTP) lub NTP, • RMON – wsparcie dla 6 różnych grup, • Port mirroring (jeden do jednego, wiele do jednego), • Monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP, • Redundantne zarządzanie stosem.
10.	Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • LLDP/LLDP-MED, • 802.3ad Link Aggregation, • 802.1D MAC Bridges, • 802.1s Multiple Spanning Tree, • 802.1t Path Cost Amendment to 802.1D, • 802.1w Rapid re-convergence of Spanning Tree, • 802.3x Flow Control, • IP Multicast (IGMPv1,v2,v 3), • IGMP v1/v2/v3 Snooping, • Ramki Jumbo Frames (minimum 9 kB),

		• Standardowe listy ACL, • Rozszerzone listy ACL, • RIPv1 i RIPv2, • Trasy statyczne, • DHCP/BootP Relay.
11.	Bezpieczeństwo	Przełącznik musi obsługiwać następujące funkcjonalności: • Musi mieć możliwość pracy w architekturze bezpieczeństwa opartej na rolach. Zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, • Ochrona przed atakami typu DHCP/ARP Spoof Protection, • Obsługa MAC Port Locking (dynamiczne i statyczne).
12.	QoS	Przełącznik musi obsługiwać następujące funkcjonalności: • Obsługa priorytetów zgodna z IEEE 802.1p, • Możliwość klasyfikacji pakietów w warstwach L2-L4 według: o ID portu fizycznego, o Adresie MAC, o Podsieci IP, o Adresie IP, o Typie protokołu IP, o IP ToS (Type of Service), o DSCP (Differentiated Services Code Point), o Porcie TCP/UDP, • Sprzętowo realizowana obsługa minimum 8 kolejek priorytetów na każdym porcie, • Obsługa wielu mechanizmów kolejkowania (SPQ, WRR oraz ich kombinacji), • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego, • Możliwość przypisania ruchu do różnych sieci VLAN zgodnie z kryteriami L2-L4, nawet jeśli nie jest skonfigurowany protokół 802.1Q VLAN Tagging.
13.	Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o poprzez IEEE 802.1x, o wykorzystujące adres MAC, o wykorzystujące przeglądarkę internetową, • Uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla minimalnie 4 użytkowników/urządzeń na port, • Obsługa Dynamic VLAN Assignment (RFC 3580), • Obsługa wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (minimum 4).
14.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.
Przewód do łączenia urządzeń w stos/wieżę - krótki		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Parametry	• Przeznaczony do łączenia w stos/wieżę przełączników dostępowych

		typu A, B, C, D opisanych w poprzedzających tabelach, • Przewód o długości nie krótszej niż 30 cm, • Przewód musi pochodzić od tego samego producenta, co dostarczane urządzenia, tworzące stos/wieżę.
Przewód do łączenia urządzeń w stos/wieżę - długi		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Parametry	• Przeznaczony do łączenia w stos/wieżę przełączników dostępowych typu A, B, C, D opisanych w poprzedzających tabelach, • Przewód o długości nie krótszej niż 90 cm, • Przewód musi pochodzić od tego samego producenta, co dostarczane urządzenia, tworzące stos/wieżę.

4.2. Rozbudowa dostępowej sieci WLAN.

Zamawiający przewiduje rozbudowę istniejącej infrastruktury sieci bezprzewodowej o dodatkowe punkty dostępowe, które podłączone zostaną do opisanych wcześniej sieciowych przełączników dostępowych.

W związku z rozbudową posiadanej przez Zamawiającego infrastruktury sieciowej i serwerowej oraz konieczności uruchomienia pełnej funkcjonalności aktualnie wykorzystywanych urządzeń i oprogramowania zarządzającego infrastrukturą sieciową i dostępem do zasobów, a także w celu zapewnienia dowolności rekonfiguracji sprzętu oraz możliwości centralnego nim zarządzania Zamawiający wymaga aby punkty dostępowe sieci WLAN:

1) były zarządzane w sposób scentralizowany przez posiadany przez Zamawiającego wirtualny kontroler sieci bezprzewodowej V2110 firmy Enterasys;
2) posiadały możliwość egzekwowania ról oraz profili użytkowników logujących się do sieci WLAN zgodnie z regułami zdefiniowanymi przy użyciu posiadanego przez Zamawiającego pakietu aplikacji do zarządzania siecią (Network Management Suite) NetSight Advance firmy Enterasys,
3) zapewniały ciągłe zarządzanie tożsamością użytkowników logujących się do sieci WLAN wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma przy użyciu posiadanego przez Zamawiającego rozwiązania Network Access Control (NAC) firmy Enterasys,

Ponadto oferowane punkty dostępowe muszą spełniać poniższe wymagania minimalne:

Punkt dostępowy sieci WLAN:		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Pasma robocze	• Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości • 802.11a/n (5 GHz) i 802.11b/g/n (2.4 GHz).
2.	Interfejsy fizyczne	• 1 port 10/100/1000 BASE-T RJ-45 z technologią autosensing • Dedykowany port konsoli zarządzającej typu RJ-45,
3.	Standardy sieciowe	Punkt dostępowy musi obsługiwać następujące funkcjonalności: • Zgodność z DFS2 (Dynamic Frequency Selection) by dopuścić

		dodatkowe kanały w paśmie 5 GHz, • Punkty dostępowe muszą obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence, • Obsługa protokołu 802.11e, w tym WMM, TSPEC oraz U-APSD, • Szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC), • Obsługa do 16 SSID (8 na częstotliwość radiową), • RADIUS Authentication & Accounting, • Płynny roaming pomiędzy podsieciami IP, • Płynny roaming pomiędzy wieloma kontrolerami, • Wsparcie dla protokołu IEEE 802.1p prioritization, • Możliwość wykonania minimum 12 jednoczesnych połączeń VoIP w ramach protokołu IEEE 802.11 a/b/g/n, • Wsparcie dla protokołu: IEEE 802.1X z wykorzystaniem metod: EAP-SIM, EAPFAST, EAP-TLS, EAP-TTLS, and PEAP, • Wsparcie dla protokołu: MAC address authentication przy wykorzystaniu lokalnych access-list lub przesyłanych z serwera RADIUS, • Mechanizmy: RADIUS AAA, przy wykorzystaniu EAP-MD5, PAP, CHAP oraz MS-CHAPv2, • RADIUS Client, • Mechanizm izolacji klientów na poziomie warstwy L2, • Mechanizmy IEEE 802.11i, WPA2 oraz WPA, przy zastosowaniu algorytmów szyfracji: Advanced Encryption Standard (AES) oraz Temporal Key Integrity Protocol (TKIP), • Obsługa technologii 802.11n pracując w konfiguracji 2x2 MIMO • Punkt dostępowy musi posiadać certyfikat 802.11n WiFi gwarantujący kompatybilność w sieciach WLAN, • Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g oraz 802.11n.
4.	Anteny	• Min. 4 anteny wewnętrzne.
5.	Tryby pracy	• Tryb działania radia WLAN: Client access, Local mesh, Packet capture, WDS, • Możliwość pracy punktu dostępowego bez kontrolera WLAN na wypadek awarii łącza, • Obsługa technologii 802.11n i praca w technice transmisji wieloantenowej MIMO 2x2 przy zasilaniu przez jedno źródło zgodne ze standardem IEEE 802.3af, bez wpływu na działanie kluczowych funkcji i wydajność, • Wsparcie dla mechanizmu minimum „Two spatial stream MIMO" dla wszystkich nadajników, • WDS (Wireless Distribution System) z możliwością tworzenia łączy typu backhaul na dowolnym łączu radiowym lub wykorzystania jednego łącza radiowego zarówno na potrzeby backhaul, jak i świadczenia usług klientom, • Instalacja typu plug & play, • Jednoczesna obsługa ruchu tunelowanego i mostowanego, • Wszystkie punkty dostępowe muszą mieć możliwość pracy w formie

		sensorów sieci – pracujących w pełnym lub niepełnym wymiarze czasu. • W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie i bez interwencji użytkownika.
6.	Funkcje zarządzania	• Punkt dostępowy musi zapewniać rozproszone zarządzanie łącznością radiową RF (Radio Frequency) Management niezależne od kontrolera - poza tylko wstępną konfiguracją. Po utracie połączenia z kontrolerem, punkt dostępowy musi być zdolny do zapewnienia ciągłości operacji związanych z szyfrowaniem, tworzeniem czarnych list, filtrowaniem, QoS oraz zarządzaniem łącznością radiową, zarówno dla swoich potrzeb, jak i lokalnie mostowanego ruchu. • Zarządzanie łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika. • Możliwość konfiguracji zapewniającej równoważenie obciążenia i sterowanie pasmem w celu pozwolenia punktom dostępowym na równoważenie/sterowanie ruchem klientów pomiędzy obiema częstotliwościami na jednym punkcie dostępowym i/lub pomiędzy wieloma punktami dostępowymi w ramach domeny łączności radiowej, • Punkty dostępowe muszą mieć możliwość wdrożenia w konfiguracji kratowej, tworzącej bezprzewodowe, wzajemne połączenia pomiędzy poszczególnymi punktami dostępowymi, • Możliwość stworzenia i jednoczesnego uruchomienia minimum 16 profili sieci bezprzewodowych WLAN, • Każdy profil wirtualny sieci bezprzewodowej powinien posiadać możliwość przypisania do sieci VLAN,
7.	Bezpieczeństwo	• Połączenie pomiędzy AP, a kontrolerem musi być szyfrowane przy pomocy technologii AES minimum 128 bit, • Punkty dostępowe muszą obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń, • Obsługa standardów uwierzytelniania i szyfrowania, w tym: WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x, • Punkt dostępowy musi wspierać szyfrowanie, tworzenie czarnych list, filtrowanie oraz QoS, niezależnie od kontrolera, • Możliwość pracy w architekturze bezpieczeństwa opartej na rolach, zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, aplikowane względem użytkownika i aplikacji, • Funkcje egzekwowania przypisanych ról i ograniczania przepustowości muszą być osiągalne na poziomie punktu dostępowego, • Przypisywanie ról klientom musi odbywać się bez konieczności segmentacji przez dedykowane SSID.
8.	WIPS	• Wymagane jest scentralizowane raportowanie i konfiguracja WIPS/WIDS, • Punkt dostępowy musi oferować funkcje WIPS/WIDS, działające bez

		wpływu na poziom świadczonych usług sieciowych, muszą być dostępne zarówno funkcje wykrywania, jak i zmniejszania zagrożeń, gdy punkt dostępowy świadczy innym klientom Wi-FI usługi transmisji danych, • Kategorie zagrożeń WIDS/WIPS, które należy wykrywać i raportować: o Analizy widma – zakłócenia pochodzące ze źródeł innych niż WiFi, o Aktywna obserwacja – wykorzystanie narzędzi takich jak NetStumbler i Wellenreiter, o Ataki typu chaff lub obfuskacja (tzw. zaciemnianie kodu) – ataki typu chaff mają za zadanie ukrywać obecności sieci, lub innych ataków na sieci, o Atak Packet Injection (wtryskiwanie pakietów) – atakujący wprowadza swoje pakiety w transmisję danych pomiędzy dwoma urządzeniami, dzięki temu urządzenia traktują te złośliwe pakiety, tak jakby pochodziły z autoryzowanego urządzenia, o Atak Denial of Service (skierowany na stację końcową) – zalewanie stacji końcowej komunikatami uwierzytelniania lub anulowania uwierzytelniania Fałszywy klient (ang. Spoofing client) – urządzenie, które wykorzystuje adres MAC innej, zazwyczaj autoryzowanej stacji roboczej. • Kategorie zagrożeń WIDS/WIPS, które należy wykrywać, raportować i zmniejszać: o Wewnętrzny Honeypot – punkt dostępowy rozgłaszający SSID, do którego nie ma upoważnienia, o Zewnętrzny Honeypot – punkt dostępowy rozgłaszający SSID, którego nie oferuje dla danej usługi, o Wrogi punkt dostępu (ang. Rogue AP) – punkt dostępowy podłączony do autoryzowanej sieci, pomimo braku upoważnienia do tego, o Fałszywy punkt dostępu (ang. Spoofing AP) – urządzenie posługujące się BSSID (adres MAC) w rzeczywistości należącym do innego, autoryzowanego punktu dostępowego, o Aktywne łamanie szyfrowania (ang. Active Encryption Cracking) – atak typu chop-chop i fragmentaryczny, o Nieautoryzowane przekazywanie danych lub routing – urządzenie przekazuje pakiety pomiędzy sieciami, pomimo braku autoryzacji do tego procesu, o Atak Denial of Service (skierowany na punkt dostępu) – zalewanie punktu dostępowego komunikatami autoryzacji i asocjacji.
9.	Dodatkowe	• Oprogramowanie działające na punktach dostępowych powinno umożliwiać oddzielną specyfikację częstotliwości dla każdego z modułów radia, • Punkty dostępowe powinny posiadać certyfikację Wi-Fi Alliance, zapewniającą kompatybilną pracę z urządzeniami klienckimi w ramach standardu 802.11a/b/g/n, • Wraz z punktem dostępowym należy dostarczyć, pochodzący od tego samego producenta, co dostarczane urządzenia, uchwyt umożliwiający montaż punktu dostępowego pod sufitem.
10.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon

		i zdalną sesję.

4.1. Zestawienie ilościowe.

Lp.	Element	Ilość
1.	Sieciowy przełącznik dostępowy typu A	15 szt.
2.	Sieciowy przełącznik dostępowy typu B	5 szt.
3.	Sieciowy przełącznik dostępowy typu C	32 szt.
4.	Sieciowy przełącznik dostępowy typu D	2 szt.
5.	Przewód do łączenia urządzeń w stos/wieżę - krótki	44 szt.
6.	Przewód do łączenia urządzeń w stos/wieżę - długi	10 szt.
7.	Moduł światłowodowy SR LC SFP+	20 szt.
8.	Punkt dostępowy sieci WLAN	30 szt.

5. ROZBUDOWA APLIKACJI CENTRUM DANYCH.

Kolejnym przedmiotem zamówienia jest rozbudowa posiadanego przez Zamawiającego centrum danych poprzez rozwiązania aplikacyjne, które jako rozwiązania wirtualne zostaną zainstalowane na posiadanych przez Zamawiającego serwerach znajdujących się w GPD.

5.1. System kontroli dostępu do sieci.

W związku z rozbudową posiadanej przez Zamawiającego infrastruktury serwerowej i aplikacyjnej oraz aktualnie wykorzystywanymi urządzeniami i oprogramowaniem zarządzającym, a także w celu zapewnienia dowolności rekonfiguracji sprzętu oraz możliwości centralnego zarządzania Zamawiający wymaga aby system kontroli dostępu:

1) stanowił rozbudowę posiadanego przez Zamawiającego systemu Network Access Control (NAC) firmy Enterasys do minimum 3000 sesji autentykacyjnych,
2) posiadał możliwość egzekwowania ról oraz profili użytkowników/urządzeń zgodnie z regułami zdefiniowanymi przy użyciu posiadanego przez Zamawiającego pakietu aplikacji do zarządzania siecią (Network Management Suite) NetSight Advance firmy Enterasys.

Ponadto oferowane rozwiązanie musi spełniać poniższe wymagania minimalne:

System kontroli dostępu do sieci – Network Access Control (NAC)		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Funkcjonalność	Rozwiązanie musi posiadać następujące funkcjonalności: • Aktywne zapobieganie przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów, • Współpraca z rozwiązaniem Microsoft NAP, • Przypisanie na stałe adresu MAC do określonego przełącznika lub portu przełącznika. Jeżeli system końcowy będzie próbował się uwierzytelnić na innym porcie lub przełączniku, zostanie odrzucony lub przypisana mu zostanie polityka w oparciu o akcje określoną podczas przypisywania mu portu MAC, • Funkcja *IP-to-ID Mapping*, która łączy razem nazwę użytkownika, adres IP, adres MAC oraz port fizyczny każdego punktu końcowego. Ta funkcjonalność jest kluczowa dla potrzeb audytów bezpieczeństwa i analiz dochodzeniowych, • Funkcja portalu rejestracyjnego dla kontroli dostępu gości, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT, • Zaawansowane możliwości sponsorowania dostępu takie jak sponsorowanie email oraz prosty portal dla sponsorów służący do zatwierdzania rejestracji gości.
2.	Architektura	Rozwiązanie musi posiadać następujące funkcjonalności: • Musi zapewniać rozwiązanie NAC typu *inline* oraz *out-of-band*, które możebyć zarządzane przez jedną centralną aplikację, • Musi być dostarczone jako maszyna wirtualna pozwalając na wykorzystanie istniejącego sprzętu, • Musi mieć możliwość pracy jako redundantne urządzenia wirtualne w trybie wysokiej dostępności.

3.	Raportowanie	Rozwiązanie musi posiadać następujące funkcjonalności: • Informacje o typie urządzeń działających w sieci oraz określonych potrzebach i zagrożeniach, które są z nimi związane, • Monitorowanie zdarzeń systemów końcowych i przedstawianie wyników o stanie zabezpieczeń systemu w oparciu o najbardziej aktualne skanowania przeprowadzane podczas oceniania, • Możliwość szybkiego podglądu historycznych i ostatnich znanych stanów połączeń dla każdego systemu końcowego i uzyskiwać informacje o znalezionych podczas skanowania zagrożeniach bezpieczeństwa systemu końcowego, • Kompleksowe raportowanie zgodności w oparciu o aktualne i historyczne informacje, • Powiadamianie poprzez syslog, pocztę elektroniczną lub usługi webowe o zmianach stanu systemów końcowych, rejestracji gości oraz wynikach skanowania stanu zabezpieczeń systemów końcowych.
4.	Narzędzia administracyjne	Rozwiązanie musi posiadać następujące funkcjonalności: • Musi zapewnić rozwiązanie oferujące jednolity, centralny obraz wszystkich niechronionych elementów związanych z użytkownikami i urządzeniami, który pozwoli później zredukować złożoność procesu zarządzania, • Musi posiadać intuicyjny panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych, • Musi posiadać funkcję portalu rejestracyjnego dla kontroli dostępu gości, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
5.	Bezpieczeństwo	Rozwiązanie musi posiadać następujące funkcjonalności: • Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania i autoryzacji podłączanych systemów końcowych, • Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP, • Musi umożliwiać ciągłe mechanizmy analizowania zagrożeń, zapobiegania im i przechowywania ich, • Rozwiązanie musi obsługiwać lokalną autoryzację MAC.
6.	Kontrola	Rozwiązanie musi posiadać następujące funkcjonalności: • Zdolność ciągłego przypisywania polityk określonemu użytkownikowi, adresowi MAC lub OUI *(Organizationally Unique Identifier)* adresu MAC, tak aby użytkownik, urządzenie lub grupa urządzeń miały przydzielony ten sam zestaw zasobów sieci, niezależnie od swojej lokalizacji lub konfiguracji serwera RADIUS, • Musi obsługiwać mechanizmy w oparciu o role umożliwiające przepuszczanie lub odrzucanie ruchu sieciowego, nadawanie mu priorytetów, ograniczanie jego szybkości, tagowanie, przekierowywanie i kontrolowanie go w oparciu o tożsamość użytkownika, czas i położenie, typ urządzenia i inne zmienne środowiskowe.

7.	Wsparcie dla środowiska wirtualnego	• Możliwość objęcia mechanizmem NAC maszyn wirtualnych oraz VDI.
8.	Automatyzacja	• Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych.
9.	Zgodność	Rozwiązanie musi posiadać następujące funkcjonalności: • Możliwość oceniania w oparciu o agentów lub sieć (skanowania sieci), • Musi dostarczyć rozwiązanie, które zapewni ciągłość działania organizacji poprzez oferowanie użytkownikom alternatywnych metod dostępu podczas procesu skanowania, • Musi przeprowadzać przed- i po-połączeniowe ocenianie stanu zabezpieczeń systemów końcowych.
10.	Skalowalność	Rozwiązanie musi posiadać następujące funkcjonalności: • Elastyczna obsługa wielu metod uwierzytelniania wielu użytkowników i urządzeń różnych dostawców, • Kontrola dla minimum 3000 sesji autentykacyjnych, • System musi umożliwiać przyszłą rozbudowę dla minimum 100 000 sesji autentykacyjnych.
11.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.

5.2. System korelacji informacji

W związku z rozbudową posiadanej przez Zamawiającego infrastruktury sieciowej oraz aktualnie wykorzystywanymi urządzeniami i oprogramowaniem zarządzającym, a także w celu zapewnienia dowolności rekonfiguracji sprzętu oraz możliwości centralnego zarządzania Zamawiający wymaga aby system korelacji informacji rejestrował dane o przepływie i zdarzeniach z urządzeń sieciowych, w tym serwerów aplikacji, serwerów Web, stacji roboczych, przełączników, firewalli oraz wylistowanych poniżej urządzeń posiadanych przez Zamawiającego:

1) przełączników sieciowych
   - dostarczanych w ramach niniejszego zamówienia sieciowych przełączników dostępowych,
   - dostarczanych w ramach niniejszego zamówienia sieciowych przełączników rdzeniowych,
   - dostarczanego w ramach niniejszego zamówienia serwerowego przełącznika agregacyjnego,
   - posiadanego przez Zamawiającego serwerowego przełącznika agregacyjnego Enterasys 7124,
2) systemu zarządzania siecią bezprzewodową
   - posiadanego przez Zamawiającego wirtualnego kontrolera sieci WLAN Enterasys V2110
3) serwera baz danych

- posiadanego przez Zamawiającego serwera Microsoft SQL Server

4) serwera poczty e-mail
   - posiadanego przez Zamawiającego serwera Microsoft Exchange 2007
5) serwera wirtualizacji
   - posiadanego przez Zamawiającego serwera VMware ESXi Enterprise Plus 5.x
6) serwera Web
   - posiadanego przez Zamawiającego serwera Apache, HTTP Server
7) serwerów usług sieciowych Microsoft:
   - posiadanego przez Zamawiającego serwera Microsoft DNS
   - posiadanego przez Zamawiającego serwera Microsoft IAS
   - posiadanego przez Zamawiającego serwera Microsoft DHCP Server
8) serwera antywirusowego
   - posiadanego przez Zamawiającego serwera Symantec Endpoint Protection
9) systemu firewall, UTM
   - posiadanego przez Zamawiającego systemu Fortinet (Fortigate 300C)
10) serwera zarządzania platformami Microsoft Windows
   - posiadanego przez Zamawiającego serwera Microsoft SCOM 2007
11) systemu zarządzania siecią
   - posiadanego przez Zamawiającego pakietu aplikacji do zarządzania siecią (Network Management Suite) Enterasys NetSight Advance,
12) systemu kontroli dostępu
   - posiadanego przez Zamawiającego systemy kontroli dostępu Enterasys NAC,
   - dostarczanego w ramach niniejszego zamówienia systemu kontroli dostępu,

Ponadto oferowane rozwiązanie musi spełniać poniższe wymagania minimalne:

System korelacji informacji - Security Information Management (SIM)		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Funkcjonalność	Rozwiązanie musi posiadać następujące funkcjonalności: • Musi zapewniać centralne zarządzanie wszystkimi komponentami infrastruktury sieciowej, • System musi identyfikować aplikacje wykorzystujące porty nie tylko te najczęściej spotykane, oraz aplikacje tunelujące swój ruch na inne porty (np. protokół HTTP wykorzystywany jako transport przez komunikator MS Instant Messenger powinien być wykrywany jako komunikator, a nie HTTP), • Obsługa źródeł danych takich jak: NetFlow, IPFIX, JFlow, SFlow, • Wykrywanie zdarzeń typu „zero-day”. Musi obsługiwać monitorowanie i wykrywanie aplikacji dla potrzeb rozpoznawania ruchu niezgodnego z politykami, w tym aplikacji P2P i strony portali społecznościowych.

2.	Architektura	Rozwiązanie musi posiadać następujące funkcjonalności: • Możliwość podłączania sensorów przepływu analizujących zachowania sieci, obsługujące przepustowość do 1Gbps, • Możliwość podłączenia wirtualnego urządzenia zbierającego przepływy, które w ramach wirtualnej infrastruktury pozwala analizować zachowania sieci i zapewnia widoczność warstwy 7, • Możliwość wdrożenia w rozproszonym środowisku, • System musi zostać dostarczony w postaci maszyny wirtualnej zapewniającej pełną funkcjonalność rozwiązania.
3.	Raportowanie	Rozwiązanie musi posiadać następujące funkcjonalności: • Zbieranie zdarzeń bezpieczeństwa i logów z wielu różnego typu urządzeń, pochodzących od różnych dostawców, • Zbieranie informacji o sieci i zabezpieczeniach bez konieczności umieszczania agentów lub innych opartych na hoście mechanizmów w istniejących klientach lub serwerach, • Przechwytywanie danych dla potrzeb analiz dochodzeniowych. Ilość przechwytywanych danych musi być konfigurowalna dla każdego przepływu, • Funkcja powiadamiania, bazującą na zaobserwowanych zagrożeniach bezpieczeństwa, anomaliach i zmianach w zachowaniu monitorowanych urządzeń, • Tworzenie przez użytkownika własnych profili i widoków, przy wykorzystaniu dowolnej cechy przepływu, zewnętrznego źródła danych lub już sprofilowanego ruchu, • Nadawanie odpowiedniej wagi powiadomieniom umożliwiając w ten sposób ich priorytetyzację. Wagi muszą być przypisywane w oparciu o wiele parametrów, takich jak typ zasobu, protokół, aplikacja, itp., • Szablony raportów dla COBIT, GLB, HIPAA, PCI i Sarbanes Oxley • Konfigurowalny mechanizm raportowania dla potrzeb tworzenia własnych raportów, • Możliwość planowania raportów.
4.	Narzędzia administracyjne	Rozwiązanie musi posiadać następujące funkcjonalności: • Tworzenie wielu użytkowników i przypisywanie każdemu użytkownikowi możliwości dostępu tylko do wybranej części monitorowanego zakresu adresów IP, • Oparty na sieci web graficzny interfejs użytkownika dla potrzeb zarządzania, analiz i raportowania, • Panel sterowania umożliwiający szybką wizualizację informacji o sieci i zabezpieczeniach. Powinna być udostępniona możliwość stosowania wielu paneli sterowania pozwalająca użytkownikom na dowolną organizację i dostosowanie widoków do swoich potrzeb.
5.	Bezpieczeństwo	Rozwiązanie musi posiadać następujące funkcjonalności: • Szyfrowanie transmisji danych pomiędzy poszczególnymi komponentami, • Wykrywanie ataków DoS (Denial-of-Service) i DDoS (Distributed Denial-of-Service)

8.	Automatyzacja	Rozwiązanie musi posiadać następujące funkcjonalności: • Automatyczne aktualizowanie informacji konfiguracyjnych, przy minimalnym udziale użytkownika, • Możliwość automatycznej oceny poziomu zagrożenia zgłoszonych zdarzeń bezpieczeństwa, zależnej od stanu zabezpieczeń zaatakowanych zasobów
10.	Skalowalność	Rozwiązanie musi posiadać następujące funkcjonalności: • System musi umożliwiać analizę minimum 1 000 zdarzeń na sekundę i minimum 50 000 przepływów na minutę.
11.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.

5.3. Aktualizacja posiadanych licencji.

W związku z rozbudową obecnej infrastruktury teleinformatycznej budynku Starostwa Powiatowego w Kielcach Zamawiający oczekuje aby wraz z pozostałymi wymienionymi w niniejszym dokumencie przedmiotami dostarczone zostały licencje rozszerzające funkcjonalność aktualnie posiadanych przez Zamawiającego rozwiązań zarządzania infrastrukturą sieci LAN, WLAN, posiadanych systemów operacyjnych oraz środowiska wirtualizacji.

Aktualizacja licencji			
Lp.	Nazwa komponentu	Obecna licencja	Wymagane minimalne parametry techniczne
1.	Enterasys NetSight Advance	NMS-ADV-5	• Licencja rozszerzająca liczbę wspieranych urządzeń z 5 do 100, z zastrzeżeniem zachowania i przeniesienia pełnej funkcjonalności obecnej licencji. • Roczne wsparcie producenta, z dostępem do nowych funkcjonalności, wsparcia przez email,
2.	Enterasys WLAN Controller	V2110 (8 AP)	• Licencja rozszerzająca liczbę wspieranych punktów dostępowych z 8 do minimum 34 urządzeń. • Roczne wsparcie producenta, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.
3.	VMware vSphere with Operations Management Enterprise Plus for 6 processors	VMware vSphere with Operations Management Enterprise Plus for 6 processors	• Licencja rozszerzająca liczbę wspieranych serwerów wirtualizacji ESXi o kolejne 6 procesorów z zastrzeżeniem zachowania i przeniesienia pełnej funkcjonalności obecnej licencji. • Roczne wsparcie producenta „Basic Support/Subscription VMware vSphere with Operations Management Enterprise Plus for 1 year” dla rozszerzanych 6 procesorów.

Pozostałe licencje i oprogramowanie		
Rozszerzenie posiadanej Licencji Open, Program nadrzędny: OPEN 90804130ZZG1408. Licencja jest aktywna do 31.08.2014, wystawiona na: Organizacja: Starostwo Powiatowe w Kielcach, Lokalizacja: Al. IX Wieków Kielc 3.		
1.	Windows Server Standard 2012 Government OPEN 1 License No Level 2 PROC	15 szt.
2.	Windows Server 2012 Open License Program-No Level Government, User CAL	300 szt.
3.	Windows Server 2012 Open License Program-No Level Government, Device CAL	70 szt.
4.	Windows 8 Pro Open License Program-No Level Government	20 szt.
5.	Office Standard 2013 Open License Program-No Level Government	15 szt.
6.	Office Professional Plus Open License Program-No Level Government	5 szt.
7.	VisioPro 2013 Open License Program-No Level Government	2 szt.
Pozostałe oprogramowanie		
1.	AVG PC TuneUp® Business Edition 2014 2 letnia subskrypcja na 3 komputery	1 szt.

Zamawiający dopuszcza dostarczenie rozwiązania innych producentów niż Enterasys spełniającego wymagania minimalne ujęte w pliku „Załącznik nr 1 do OPZ – Enterasys NetSight Advance" oraz „Załącznik nr 2 do OPZ – Enterasys WLAN Controller".

6. POZOSTAŁY SPRZĘT KOMPUTEROWY I AKCESORIA

W zakresie rozbudowy posiadanej bazy sprzętowej Zamawiający wymaga dostarczenia w ramach zamówienia komputerów typu desktop, workstation oraz urządzeń mobilnych o minimum równoważnych parametrach technicznych, wyspecyfikowanych w poniższych tabelach.

6.1. Komputer typu desktop

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputera
1.	Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych
3.	Procesor	Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 6600 punktów Passmark CPU Mark
4.	Pamięć operacyjna RAM	Pamięć operacyjna: min. 4GB możliwość rozbudowy do min 32GB.
5.	Parametry pamięci masowej	Min. 500 GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników..
6.	Grafika	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem dla DirectX 10.1, OpenGL 3.0, Shader 4.1 –

		z możliwością dynamicznego przydzielenia do 1,5GB pamięci.
7.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
8.	Obudowa	Typu SFF z obsługą kart PCI 32bit oraz PCI Express wyłącznie o niskim profilu, wyposażona w min. 3 kieszenie: 1 szt 5,25" zewnętrzna, 1 szt 3,5" wewnętrzna i 1 szt 3,5" zewnętrzna. Zasilacz o mocy minimum 280W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 86%, przy 50% obciążeniu. W celu szybkiej weryfikacji usterki w obudowę komputera musi być wbudowany akustyczny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami;
9.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 7 32bit i 64bit (dopuszcza się wydruk ze strony Microsoft WHCL)
10.	Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.
11.	BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, ilości i sposobu obłożenia slotów pamięciami RAM, typie procesora wraz z informacją o ilości rdzeni, wielkości pamięci cache L1, L2 i L3, pojemności zainstalowanego dysku twardego rodzajach napędów optycznych MAC adresie zintegrowanej karty sieciowej kontrolerze audio Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty

		sieciowej, modułu TPM, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przedzie obudowy, tylko tylnych portów.
12.	Dodatkowe oprogramowanie	Oprogramowanie dostarczone przez producenta komputera pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej: Zdalne wyłączanie i restart komputera w sieci, Monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS, Tworzenie indywidualnych numerów dla poszczególnych użytkowników, Włączenie lub wyłączanie BOOTowania portów USB Zdalne zarządzanie energią urządzeń. W pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu
13.	Certyfikaty i standardy	Komputery mają spełniać normy i posiadać deklaracje zgodności (lub inne dokumenty potwierdzające spełnienie norm) w zakresie: Deklaracja zgodności CE normy Energy Star 5.0 Certyfikat EPEAT na poziomie GOLD Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov – dopuszcza się wydruk ze strony internetowej Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.epeat.net - dopuszcza się wydruk ze strony internetowej Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 Dla potwierdzenia, że oferowany sprzęt odpowiada postawionym wymaganiom i był wykonany przez Wykonawcę (a jeżeli Wykonawca nie jest producentem to przez producenta) w systemie zapewnienia jakości wg normy ISO 9001 aby Wykonawca posiadał :Certyfikat ISO 9001 lub inne zaświadczenie/dokument wydane przez niezależny podmiot zajmujący się poświadczaniem zgodności działań wykonawcy z normami jakościowymi - odpowiadającej normie ISO 9001. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy.
14.	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 23 dB Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia

		narzędzi (wyklucza się użycia wkrętów, śrub motylkowych); Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki).
15.	Warunki gwarancji	• Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. • Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego • W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony komputer zastępczy • Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, • W przypadku awarii dysku twardego, dysk pozostaje u Zamawiającego • Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. • Oferent musi posiadać oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
16.	Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera –
17.	Wymagania dodatkowe	Zainstalowany system operacyjny Microsoft Windows 7 Professional (64-bit), nie wymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft wraz z nośnikiem. Wbudowane porty: Wbudowane porty minimalnie: 1 x VGA 1 x DVI 1 x RS-232 1 x LPT 1 x eSATA 2 x PS/2 1 x RJ-45 1 x Audio: line-in 1 x Audio: line-in/mikrofon 1 x Audio: line-out 1 x Audio: mikrofon z przodu obudowy 1 x Audio: słuchawki z przodu obudowy 12 szt USB w tym: minimum 2 porty z przodu obudowy, minimum 6 portów

		z tyłu obudowy (w tym min. 2 x USB 3.0), minimum 4 porty wewnątrz obudowy. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika) Płyta główna z wbudowanymi minimum: 1 złącze PCI (32-bit/33 MHz) 2 złącza PCI-Express x1 1 złącze PCI-Express 3.0 x16 Obsługa kart wyłącznie o niskim profilu – nie dopuszcza się kart o profilu pełnym, minimum 4 złącza DIMM z obsługą do 32GB DDR3 pamięci RAM, min. 4 złącz SATA NCQ w tym min 1 złącze SATA 3.0, Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll) Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt Dołączony nośnik ze sterownikami

6.2. Komputer typu workstation

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputera
1.	Płyta główna	• wyposażona w min. 2 złącza PCI Express 3.0 x16, 2 złącza PCI Express 3.0 x8, 1 złącze PCI Express 2.0 x16, 2 złącza PCI(32 bit/33MHz) 8 złącz DIMM DDR3 1600MHz ECC/non-ECC pracujące w systemie dwukanałowym, obsługa do 128GB pamięci RAM, zintegrowany z płytą główną moduł TPM 1.2, możliwość dezaktywacji w BIOS, zintegrowany kontroler 6xSATA II z obsługą macierzy RAID 0/1/10/5.
2.	Chipset	• Dostosowany do oferowanego procesora
3.	Procesor	• Procesor dedykowany do pracy w komputerach osobistych, wydajnościowo osiągający wynik co najmniej 11600 pkt w teście SysMark2007 w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net Osiągający w teście SPECintÒ_rate2006 min 280 pkt, raport z testu potwierdzony przez producenta i dostępny na stronach http://www.spec.org.
4.	Pamięć RAM	• Min 16 GB z możliwością rozbudowy do 128 GB
5.	Dysk twardy	• Min. 4 dyski: 1x SSD 256GB, szybkośc interfejsu min 500 MB/s, szybkość odczytu min 500 MB/s szybkoośc zpisu min 500 MB/s ,1x HDD o pojemności min 2000GB 7,2 k , zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników, fabrycznie przystosowany do pracy ciągłej..
6.	Karta graficzna	• Niezintegrowana osiągająca w teście Average G3D Mark min 2800 pkt obsługująca równoległą architekturę obliczeniowa

7.	Karta dźwiękowa	• Karta dźwiękowa zintegrowana z płytą główną, w standardzie High Definition obudowa wyposażona w głośnik
8.	Karta sieciowa	• 10/100/1000 Ethernet RJ 45 (zintegrowana) • Wspierająca funkcję Wake on LAN (funkcja włączana przez użytkownika) i PXE
9.	Porty	• Audio: line-in / microphone 1szt. • Audio: line-out 2szt. • Przód obudowy audio: mikrofon 1szt. • Przód obudowy audio: słuchawki 1szt. Minimum 13 portów USB, rozmieszczonych następująco: • Z przodu obudowy min. 2szt. USB 2.0 i min. 2szt. USB 3.0 • Z tyłu obudowy min. 6 szt. USB 2.0 • Wewnątrz obudowy min. 3szt. USB 2.0 • RS232 1 szt. • Mouse / Keyboard (PS/2) 2szt. • Ethernet (RJ-45) 1szt.
10.	Klawiatura	Klawiatura USB w układzie polski programisty.
11.	Mysz	Mysz optyczna USB z pięcioma klawiszami oraz rolką (scroll).
12.	Napęd optyczny	Nagrywarka Blu-ray DVD +/-RW wraz z oprogramowaniem do nagrywania płyt.
13.	Obudowa, zasilacz	• Typu Tower, fabrycznie przystosowana do pracy w układzie pionowym i poziomym (2 x 5,25” zewnętrzne, 2 x 3,5” zewnętrzne, 4 x 2,5” wewnętrzne, 4 x 2,5” wewnętrzne LUB 4 x 3,5” wewnętrzne) • Zintegrowany w obudowie, wyposażony w diody sygnalizacyjne (praca, obecność karty, odczyt) , obsługa kart CF I, CF II, Micro Drive, Memory Stick, MS Magic Gate,SD, HI-SPEED SD, SDHC, MMC • Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń i napędów optycznych i dysków twardych bez konieczności użycia narzędzi (wyklucza się użycia wkrętów i śrub oraz śrub motylkowych); • Możliwość montażu w szafie RACK • Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) • Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensington) oraz kłódki (oczko w obudowie do założenia kłódki) • Zasilacz o mocy max. 500W Active PFC i sprawności co najmniej 87 % • Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie więcej niż 1100mm w tym całkowita szerokość obudowy nie większa niż 190mm • wbudowany czujnik otwarcia obudowy
14.	System operacyjny	• Microsoft Windows 8 Professional PL, zainstalowany System operacyjny Microsoft Windows 7 Professional niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dołączony nośnik z oprogramowaniem, sterownikami dla systemów Windows 7 oraz XP, Płyty Recovery umożliwiające instalacje systemu zarówno w wersji 32 bitowej jak i 64 bitowej. W raz z systemem operacyjnym zainstalowany pakiet Office 2010 Starter.

15.	BIOS	• Możliwość odczytania z BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych , informacji na temat: zainstalowanego procesora, pamięci operacyjnej RAM wraz z informacją o obsadzeniu slotów pamięci, MAC adres karty sieciowej, • rozwiązanie sprzętowe zintegrowane w płycie głównej komputera zapewniające możliwość przywrócenia BIOS w przypadku jego uszkodzenia (ataki wirusów itp.) lub nieudanej aktualizacji bez pośrednictwa jakichkolwiek urządzeń zewnętrznych i w sytuacji, gdy obraz na monitorze nie jest wyświetlany i/lub nie ma możliwości wprowadzania znaków za pomocą konsoli tekstowej • W pamięci Flash, funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie usera, administratora oraz dysku twardego. • Możliwość włączenia/wyłączenia z zintegrowanej karty dźwiękowej z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. • Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przodzie obudowy, tylko tylnich portów, tylko zewnętrznych, tylko nieużywanych • Możliwość zmiany trybu pracy dysku twardego: na pracę zapewniającą największą wydajność, na pracę zmniejszającą poziom hałasu generowanego przez dysk twardy. • Zintegrowana z BIOS możliwość trwałego i bezpiecznego usunięcia danych z dysku realizowana według algorytmu Guttmana umożliwiająca wykorzystanie do 35 cyklów kasowania
16.	Bezpieczeństwo i zarządzanie	• Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. • Funkcje bezpieczeństwa w obudowie: ✓ czujnik otwarcia obudowy (sposób montażu czujnika nie może ograniczać lub uniemożliwiać instalacji kart rozszerzeń) ✓ slot Kensington ✓ fabrycznie zintegrowany zamek obudowy nie wystający poza obrys obudowy (nie dopuszcza się kłódek itp.) • Funkcje bezpieczeństwa w BIOS: ✓ hasło użytkownika i administratora ✓ blokada portów USB (w tym tylko zewnętrznych przed urządzeniami typu PenDrive) i pozostałych zewnętrznych interfejsów, blokada bootowania z FDD/ODD • Oprogramowanie wyprodukowane i wspierane przez producenta komputera wraz z licencją do zarządzania w sieci, pozwalające minimum na:

		✓ pracę w architekturze serwer-klient - licencja musi pozwalać na pełne wykorzystanie aplikacji w wymaganym zakresie ✓ możliwość zdalnego przypisania dla jednego, lub grupy komputerów unikalnego numeru inwentarzowego widocznego zdalnie dla administratora jak i bezpośrednio w BIOS maszyny ✓ monitoring systemu i przekazywanie informacji o zdarzeniach na stację administratorską (konsola graficzna na stacji zarządzającej, konsola tekstowa, email, sms) ✓ możliwość zdalnej konfiguracji sposobu zarządzania energią dla pojedynczego komputera jak i grupy komputerów w sieci (zarządzanie energią podłączonego do zestawu monitora, parametrów pracy zestawu – czas przejścia w tryb standby, hibernację, automatyczne wyłączenie monitora) ✓ możliwość konfiguracji i weryfikacji zakresu i stopnia szczegółowości alertów przekazywanych na stację administratorską oraz wybór sposobu informacji o zdarzeniu ✓ monitoring i przesyłanie alertów o stanie komponentów takich jak: dysk twardy (SMART), procesor, płyta główna, pamięci, wentylatorów, stanu czujnika otwarcia obudowy, monitoring temperatury wewnętrznej komputera ✓ zdalna aktualizacja sterowników dla pojedynczych komputerów i ich grup (aplikacja musi rozpoznawać typ maszyny i aktualizować sterowniki selektywnie) ✓ zdalną kontrolę urządzeń USB ✓ zdalne zarządzanie BIOS: wprowadzanie i zmiana haseł BIOS, archiwizacja i aktualizacja BIOSu dla pojedynczego komputera i grupy komputerów jednocześnie; modyfikacja sekwencji bootowania, aplikacja musi posiadać zabezpieczenie przed nadpisaniem nieodpowiednim rodzajem BIOS na podłączonych komputerach ✓ generowanie raportów dot. pojedynczych komputerów lub grup komputerów, w zakresie zainstalowanych komponentów, systemu operacyjnego oraz aplikacji • inwentaryzacja szczegółowa komputera: ✓ odczyt modelu, numeru seryjnego i numer inwentarzowego komputera ✓ wersja i model płyty głównej, wersja BIOS; ✓ model, wersja firmware i numer seryjny dysku twardego, ✓ model, wersja firmware i numer seryjny napędu optycznego ✓ sposób obsadzenia modułów pamięci wraz z informacją o modułach (pojemność, oznaczenie, numer seryjny kości)
17.	Oprogramowanie dodatkowe	• Dodatkowe w pełni funkcjonalne oraz nieodpłatne licencyjnie oprogramowanie producenta sprzętu pozwalające na:

		✓ Diagnostykę usterek typu hardware z poziomu DOS, ✓ W pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu ✓ Zarządzanie sprzętem IT oraz inwentaryzację posiadanego sprzętu wraz z zainstalowanymi podzespołami czy oprogramowaniem
18.	Certyfikaty i standardy	• Certyfikat ISO9001 dla producenta sprzętu. • Certyfikat EPEAT na poziomie co najmniej SILVER dla Polski. Certyfikat ważny w dniu składania oferty i potwierdzony wydrukiem ze strony WWW.epeat.net • ENERGY STAR 5.0 • Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z ww. systemem operacyjnym. • Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 20 dB. • Deklaracja zgodności CE • Certyfikat GS dla oferowanego modelu komputera • Oświadczenie producenta zapewniające poprawną pracę jednostki centralnej zarówno w pionie jak i poziomie. • Zgodność ze standardem WMI 1.5. • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.
19.	Gwarancja	• Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. • Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego • W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony komputer zastępczy • Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, • W przypadku awarii dysku twardego, dysk pozostaje u Zamawiającego • Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. • Oferent musi posiadać oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.

	Wsparcie techniczne producenta	• Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej, możliwość weryfikacji konfiguracji fabrycznej zakupionego sprzętu, a także weryfikacji posiadanej/wykupionej gwarancji oraz statusu napraw urządzenia po podaniu unikalnego numeru seryjnego.

6.3. Monitor 24" LCD

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	Typ ekranu	• Ciekłokrystaliczny z aktywną matrycą TN 24"
2.	Rozmiar plamki	• Maks. 0.270 mm
3.	Jasność	• min. 250 cd/m2
4.	Kontrast	• Min. 1000:1
5.	Kąty widzenia (pion/poziom)	• Min. 170°/170 stopni
6.	Czas reakcji matrycy	• Maks. 5ms
7.	Rozdzielczość natywna	• Min. 1920x1200
8.	Powłoka powierzchni ekranu	• Przeciwodblaskowa
9.	Częstotliwość odświeżania poziomego	• Częstotliwość odświeżania poziomego min. 30-82 kHz • Częstotliwość odświeżania pionowego min. 56-76 Hz
10.	Odwzorowanie kolorów	• Min 16,7 milionów kolorów
11.	Menu OSD	• Polskie menu OSD, Regulacja palety barw z menu OSD – co najmniej regulacja 6500K, 9300K, możliwość zapisu ustawień użytkownika (R,G,B); wyświetlanie modelu, numeru seryjnego monitora oraz parametrów pracy (rozdzielczość, używane złącze sygnałowe) poprzez menu OSD
12.	Podświetlenie	• System podświetlenia LED
13.	Zakres pochylenia monitora	• Co najmniej od -5° do +35°
14.	Zakres regulacji wysokości	• Min. 100 mm
15.	Kąt obrotu	• Min 340°
16.	Bezpieczeństwo	• Monitor musi być wyposażony w tzw. Kensington Slot
17.	Waga z podstawką	• Maksymalnie 6,5 kg

18.	Złącza	Co najmniej: • 15-stykowe D-Sub, • DVI-D (z HDCP) • DisplayPort • 1 x wejście audio (stereo mini-jack) • 4 x USB 2.0 • 1 x USB 2.0 (typ B)
19.	Dodatkowe	• Monitor musi posiadać usuwalną podstawę montażową, • Zintegrowany zasilacz • Wbudowane 2 głośniki min. 1,5W; • Kompatybilność z VESA 100mm • Fabrycznie dostarczone w zestawie: ✓ kabel VGA o długości minimum 1,8m ✓ kabel DVI-D o długości minimum 1,8m ✓ kabel USB (USB-A do USB-B) ✓ kabel zasilający ✓ Kabel audio stereo, analogowy o długości min 1,8m
20.	Gwarancja	• Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. • Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego • W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony monitor zastępczy • Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, • Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta sprzętu. • Oferent musi posiadać oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
21.	Certyfikaty	• Monitory muszą być wykonane zgodnie normami i posiadać Certyfikaty: TCO 5.2, ENERGY STAR 5.0, EPEAT Gold, ISO 9241-307, CE, EN 60950, RoHS, WEEE, IT ECO – lub inne dokumenty wdane przez niezależny podmiot uprawniony do kontroli jakości, potwierdzające, że dostarczone monitory odpowiadają wskazanym normom.
22.	Zużycie energii	• Max 26W • Mniej niż 1W – tryb uśpienia

6.4. Komputer przenośny typu laptop

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Ekran	• Matryca TFT Full HD WUXGA 15,6" z podświetleniem LED, zalecana rozdzielczość 1920 x 1080, anti-glare, matowa. o podwyższonej trwałości wykonana ze stopów magnezu. Metalowe, wzmacniane zawiasy
2.	Kamera	• Zintegrowana z obudową kamera HD wraz z oprogramowaniem.
3.	Procesor	• Procesor dla urządzeń mobilnych. Wydajność obliczeniowa: Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 4200 punktów Passmark CPU Mark.
4.	Pamięć RAM	• Min. 4 GB. Możliwa rozbudowa do 16GB.
5.	Dysk twardy	• Min. 500 GB.
6.	Karta graficzna	• Grafika powinna umożliwiać pracę trzymonitorową ze wsparciem dla DirectX 10.1, OpenGL 3.0, Shader 4.1 – z możliwością dynamicznego przydzielenia do 1,5GB pamięci
7.	Karta dźwiękowa	• Karta dźwiękowa Hight Definition.
8.	Karta sieciowa	• Ethernet 10/100/1000, WiFi (802.11 b/g/n), Bluetooth
9.	Porty/złącza	• 4 x USB 3.0 (w tym min. 2 typu USB 3.0 oraz 1 z możliwością ładowania zewnętrznych urządzeń bezpośrednio z portu USB komputera) • 1x RJ45 • 1x HDMI • 1x Display Port • 1 x VGA (D-Sub) • 1 x ExpressCard/34 • 1 x Wejście mikrofonu • 1 x combo audio (mikrofon/słuchawki) • czytnik kart multimedialnych 4 w 1
10.	Napęd optyczny	• Napęd optyczny DVD +/- RW SuperMulti DL), zamawiający nie dopuszcza rozwiązania typu „slot", wnęka na napęd optyczny powinna umożliwiać instalacje wymiennie dodatkowego dysku twardego pracującego w oparciu o interfejs S-ATA II, napędu Blu-Ray lub dodatkowej baterii nie wystającej poza obrys notebooka
11.	Bateria	• Bateria litowo-jonowa, co najmniej 6 celowa.
12.	Zasilacz	• Zasilacz zewnętrzny 110-240 V.
13.	Klawiatura	• Podświetlana pełnowymiarowa klawiatura - układ US –QWERTY. Klawiatura odporna na zalania, układ US -QWERTY, min 104 klawisze, z wydzielonym blokiem klawiatury numerycznej oraz z dwustopniowym podświetleniem
14.	Urządzenia	• TouchPad z obsługą sterowania dotykowego,

	wskazujące	
15.	System operacyjny	• Min. Windows® 7 Professional 32/64bit PL niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dołączony nośnik z oprogramowaniem, sterownikami dla systemów Windows 7, płyty Recovery umożliwiające instalacje systemu zarówno w wersji 32 bitowej jak i 64 bitowej
16.	Oprogramowanie dodatkowe	• Oprogramowanie producenta komputera do wykonania kopii bezpieczeństwa systemu operacyjnego i danych użytkownika na dysku twardym i dyskach zewnętrznych np. CD-ROM oraz ich odtworzenie po ewentualnej awarii systemu operacyjnego bez potrzeby jego reinstalacji, • Oprogramowanie diagnostyczne umożliwiające wykrywanie usterek z wyprzedzeniem. • Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). • Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz PIv6, a także zapewniająca: ✓ Monitorowanie konfiguracji komponentów komputera – CPU, Pamięć, HDD, wersja BIOS płyty głównej; ✓ Zdalną konfigurację ustawień BIOS; ✓ Zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; ✓ Zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keybord, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie; ✓ Zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej; ✓ Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/); ✓ Nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia

		z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS; ✓ Wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego; ✓ Sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji. ✓ Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O i zintegrowany układ graficzny
17.	Bezpieczeństwo	• Czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy, • Złącze typu Kensington Lock lub równoważne, • Kompatybilność z technologią Anti Theft Protection lub równoważną, • Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. • Czytnik linii papilarnych wraz z oprogramowaniem
18.	BIOS	• Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: ✓ modelu komputera, ✓ nr seryjnego komputera ✓ wersji BIOS (z datą), ✓ modelu procesora wraz z informacjami o prędkościach ✓ Informacji o ilości i typie pamięci RAM ✓ Informacji o dysku twardym: model oraz pojemność ✓ MAC adresie zintegrowanej karty sieciowej ✓ Numerze rodzaju matrycy • Możliwość wyłączenia/włączenia bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych min.: ✓ karty sieciowej RJ45 ✓ karty sieciowej WLAN ✓ karty sieciowej WWAN ✓ kamery ✓ portów USB ✓ czytnika kart multimedialnych

		✓ czytnika kart mikroprocesorowych ✓ czytnika linii papilarnych • Funkcja blokowania/odblokowania BOOT-owania z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. ✓ Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB ✓ Możliwość włączenia/wyłączenia hasła dla dysku twardego, ✓ Możliwość - bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie systemu, administratora i dysku twardego, • Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe
19.	Certyfikaty i standardy	• Deklaracja CE, EnergyStar®, • Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym Windows 32/64 bit. • Certyfikat EPEAT na poziomie GOLD Certyfikat ważny w dniu składania oferty. • Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 i ISO 14001
20.	Gwarancja	• Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. • Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego • W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony komputer zastępczy • Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, • W przypadku awarii dysku twardego, dysk pozostaje u Zamawiającego • Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. • Oferent musi posiadać oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane

		z serwisem.
21.	Waga	• Nie większa niż 3 kg z baterią.
22.	Dodatkowe	• Głośniki stereo wbudowane, wbudowany mikrofon, Torba dedykowana do rozmiaru oferowanego laptopa, jednokomorowa, • Przewodowa mysz optyczna USB.

6.5. Urządzenie mobilne typu tablet

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne urządzenia
1.	System operacyjny	• Min. Android 4.1.2 Jelly Bean lub równoważny.
2.	Wyświetlacz	• Przekątna Min. 10” • Ekran TFT Color LCD - dotykowy • Typ rozdzielczości: WUXGA • Rozdzielczość max.: 1920 x 1200 • Kolory: min. 16,7 mln. • Typ powierzchni: Nie pozostawiająca odcisków palców • Podświetlenie: LED
3.	Obudowa:	• Wodoodporna -IPX55/57 • Odporna na kurz- IP5X
4.	Układ graficzny:	• Adreno 320 lub równoważny
5.	Procesor	• Procesor dedykowany do urządzeń przenośnych np. Qualcomm Snapdragon S4 Pro APQ8064 + MDM9215M min. 1,5 GHz lub równoważny
6.	Pamięć	• Min. 2GB
7.	Pamięć wbudowana:	• Min. 16 GB
8.	Bezprzewodowa sieć danych	• LAN - IEEE 802.11 a/b/g/n • Bluetooth v4.0 • WiFi Miracast • GPS, NFC, DLNA • LTE 4G
9.	Przetwornik obrazu:	• 3-osiowy Akcelerometr • Żyroskop • Cyfrowy kompas • Pole magnetyczne • Czujnik oświetlenia otoczenia
10.	Kamera Tylna	• Przetwornik CMOS Exmor R dla urządzeń mobilnych • Rozdzielczość min. 3288 × 2472 • Efektywne piksele min.: 8,1 megapiksela • AF/Makro
11.	Kamera przednia	• Przetwornik CMOS Exmor R dla urządzeń mobilnych • Rozdzielczość min. 1920 x 1080 • Efektywne piksele min.: 2,2 megapiksela

12.	Podczerwień:	• Wspierana multifunkcja, funkcja uczenia (sterowania urządzeniami poprzez IR)
13.	Dźwięk/obraz	• Wbudowany głośnik • Wbudowany mikrofon • Kodeki audio: AAC, HE-AAC v1, HE-AAC v2, mp3, MIDI • Kodeki video: H.263, H.264, MPEG-4, VP8 • Obsługiwane formaty: JPEG, GIF, PNG, BMP, WEBP
14.	Interfejsy	• 1 x Audio (słuchawki) • 1 x czytnik kart Micro SD – obsługiwany format: microSD, microSDHC, microSDXC • 1 x SIM Card Slot • 1 x port microUSB-AB, wersja - 2.0 High Speed (480 MB/s) • HDMI – przez obsługę MHL
15.	Bateria	• Typ akumulatora Litowo-polimerowy, Czas ładowania mak. do ok. 6,5 godziny • Czas czuwania do ok. 800 godzin
16.	Wymiary	• Tablet: maks. wysokość: 175 mm x szerokość 270 mm x głębokość 8 mm • Stacja dokująca maks: 290 x 65 x 35 mm
17.	dominujący kolor obudowy	• Ciemny kolor (czarny)
18.	Akcesoria	• Ładowarka stacjonarna • Stacja dokująca: ✓ Port ze złączem do ładowania x1 ✓ Port microUSB (do ładowania) x1 ✓ Swobodna regulacja konta podstawy
19.	Osłona:	• Wymiary dopasowane do rozmiaru tabletu, bez wystających elementów, materiał zewnętrzny- skóra, materiał wewnętrzny: poliester, funkcja – ochronna – lub funkcja podstawki, dwa sposoby składania i regulacji funkcji nachylenia tabletu, automatyczne włączanie/wyłączanie ekranu tabletu po otwarciu/zamknięciu osłony, kolor: czarny.
20.	Gwarancja	• Min. 24 miesiące. • Wykonawca wraz ze sprzętem dostarczy dokument potwierdzający udzielenie gwarancji przez producenta sprzętu (karta gwarancyjna producenta).

6.6. Pozostałe akcesoria komputerowe

Lp.	Nazwa komponentu
1.	• Pamięć RAM DIMM DDR2 2GB 800MHz 1,8V np. Kingston KVR800D2N6/2GB lub równoważna o nie gorszych parametrach. Pamięć dedykowana do komputerów HP DC 7800 CMT. Preferowane chipsety: Elpida, Kingston, Hynix.

6.7. Zestawienie ilościowe

Lp.	Element	Ilość
1.	Komputer typu desktop	10 szt.
2.	Komputer typu workstation	1 szt.
3.	Monitor 24” LCD	11 szt.
4.	Komputer przenośny typu laptop	3 szt.
5.	Urządzenie mobilne typu tablet	4 szt.
6.	Moduły pamięci RAM DIMM DDR2 2GB 800MHz	30 szt.

Załącznik nr 1 do OPZ – Enterasys NetSight Advance

Rozwiązanie do zarządzania siecią spełniające poniższe wymagania minimalne:		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
	Funkcjonalność	• Musi zapewniać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia • Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji • Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci • Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN • Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II • Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent • Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania *firmware*, typ CPU i pamięć
	Architektura	• Musi zapewniać scentralizowane zarządzanie urządzeniami sieci przewodowej i bezprzewodowej dla minimum 100 urządzeń aktywnych oraz minimum 100 punktów dostępowych. • Musi zawierać zintegrowane aplikacje typu *plug-in*, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania. • Musi mieć możliwość instalacji, jako maszyna wirtualna • Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej • Rozwiązanie musi integrować się ze środowiskiem wirtualnym: o Musi posiadać wsparcie dla VMware ESX i ESXi o Musi posiadać wsparcie dla Citrix XEN o Musi posiadać wsparcie dla Microsoft HyperV • Obsługa funkcji wysokiej dostępności (High Availability)
	Raportowanie	• Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci • Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (*OID*) • Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń) • Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia • Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu

		• Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu *firmware* urządzenia • Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń • Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych • Musi zapewniać możliwości analiz na poziomie portu • Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów • Możliwość raportowania do elementu zarządzającego maszynami wirtualnymi (vSphere oraz XenCenter), informacji o rzeczywistym położeniu maszyny wirtualnej w sieci- fizyczny port i przełącznik
	Narzędzia administracyjne	• Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń • i zadań oraz planowanie terminu ich wykonania • Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB *(Management Information Base)* z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB • Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby • Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania *firmware* i wielkość pliku konfiguracyjnego • Musi posiadać możliwość pobierania oprogramowania *firmware* do jednego urządzenia lub do wielu urządzeń jednocześnie • Musi mieć możliwość pobierania obrazów *boot PROM* do jednego urządzenia lub do wielu urządzeń jednocześnie • Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń • Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń • Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania • Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury • Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym
	Bezpieczeństwo	• Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji • Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https. Musi mieć możliwość definiowania polityk: o ograniczających poziom pasma, o ograniczających liczbę nowych połączeń sieciowych, o ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3, o nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania

		• Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej aplikacji, poprzez wykonanie jednej czynności, dzięki której polityki zostaną rozesłane do wszystkich urządzeń • Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci • Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC • Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p • Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania • Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku • Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 *Trap* (*Inform*) • Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS
	Kontrola	• Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia • Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci • W przypadku spełnienia wcześniej określonych kryteriów musi mieć możliwość przypisania „roli kwarantanny” użytkownikowi podłączonemu do portu. • Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji • W przypadku spełnienia wcześniej określonych kryteriów musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci Możliwość przypisywania sieci VLAN, reguł filtrowania warstw L2-L4 oraz QoS na warstwach L2-L4 (DSCP i 802.1p) dla każdej maszyny wirtualnej opartej na przełączniku wirtualnym i wirtualnej grupie portów. Reguły filtrowania na warstwach L3-L4 i reguły QoS muszą obsługiwać zarówno IPv4, jak i IPv6.
	Wsparcie dla środowiska wirtualnego	• Możliwość konfiguracji vSwitch i PortGroups w ramach zarządzania maszynami wirtualnymi (vSphere i XenCenter), bez uruchamiania aplikacji do zarządzania maszynami wirtualnymi • Zdolność do ograniczania komunikacji pomiędzy maszynami wirtualnymi Dostarczanie danych historycznych o obecności maszyny wirtualnej (na jakim rzeczywistym porcie oraz przełączniku, i w jakim czasie, dana maszyna wirtualna była obecna).

		• Dostarczanie informacji o systemie operacyjnym maszyny wirtualnej. Możliwość dostarczenia informacji o stanie zabezpieczeń maszyny wirtualnej, po instalacji specjalnego modułu lub rozszerzeniu licencji. • Możliwość ograniczenia dostępu do określonych zasobów sieci, zgodnie z mechanizmem NAC, tylko dla zatwierdzonych maszyn wirtualnych. W przypadku przyłączenia maszyny wirtualnej do wirtualnej grupy portów lub wirtualnego przełącznika, ruch pochodzący z tej maszyny wirtualnej musi być blokowany, aż do momentu uzyskania odpowiednich praw dostępu dla tej maszyny wirtualnej. • Możliwość ograniczenia dostępu do określonych zasobów sieci zgodnie z mechanizmem NAC, także dla VDI (Virtual Desktop Infrastructure)
	Skalowalność	• Obsługa minimum 100 VM (Virtual Machine) jednocześnie, możliwość rozbudowy do obsługi 500 VM jednocześnie • Aplikacja musi umożliwiać przyszłą rozbudowę do minimum 500 urządzeń sieciowych oraz minimum 5000 punktów dostępowych
	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.

Załącznik nr 2 do OPZ – Enterasys WLAN Controller

Kontroler sieci WLAN		
	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Parametry	• Kontroler sieci bezprzewodowej w momencie dostawy musi obsługiwać minimum 34 punkty dostępowe w normalnym trybie pracy. Kontroler musi umożliwiać rozbudowę do minimum 248 punktów dostępowych w trybie normalnej pracy oraz do minimum 496 punktów w trybie wysokiej dostępności.
2.	Mech. przekazywana danych	• Kontroler musi obsługiwać jednocześnie różne mechanizmy przekazywania danych, w tym routing, tunelowanie ruchu z AP (Bridge@Controller) i zamykanie ruchu w AP (Bridge@AP). • Różne mechanizmy przekazywania danych muszą być dostępne do skonfigurowania w podziale na wirtualne grupy sieciowe.
3.	Captive portal	• Musi posiadać zintegrowany (w kontrolerze), logicznie wydzielony portal dostępowy (Captive Portal), dowolnie konfigurowany przez administratora, z wykorzystaniem wbudowanych narzędzi edycyjnych, wykorzystujących mechanizmy HTML i PHP. • Dostęp gościnny poprzez Captive Portal musi umożliwiać logowanie do sieci WLAN z wykorzystaniem autentykacji 802.1x • Dostęp gościnny poprzez Captive Portal musi umożliwiać logowanie do sieci WLAN poprzez otrzymanie zezwolenia od uprawnionych użytkowników lub administratora • Captive Portal będzie dawał dostęp Gościom do zasobów internetu w dedykowanym VLAN-nie (Sieć Gości), nie dopuszczając Gości do zasobów wewnętrznych Zamawiającego (Intranet) • Administrator lub uprawiony użytkownik przydzielając dostęp do Sieci Gości ma mieć wybór przydzielenia dostępu w interwałach czasu.
4.	QoS	• Musi zapewniać możliwość zmiany parametrów QoS (802.1p, ToS/DSCP i rate-limit) i zmianę list ACL dla dowolnego użytkownika bez zrywania istniejących sesji. • Musi obsługiwać przypisywanie indywidualnych parametrów obsługi ruchu poszczególnym użytkownikom (QoS, ACL), bez konieczności segmentacji przez dedykowane SSID. • Musi obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence.
5.	Bezpieczeństwo	• Musi obsługiwać szyfrowanie połączeń do punktów dostępowych sieci WLAN (AP) na poziomie minimum AES 128bit. • System musi obsługiwać przypisywanie polityk klientom, bez konieczności segmentacji przez dedykowane SSID. • System musi obsługiwać ujednoliconą, opartą na rolach kontrolę

		dostępu do sieci przewodowej i bezprzewodowej. • System musi zapewniać automatyczną ochronę typu Over The Air Intrusion Prevention przed zagrożeniami takimi jak fałszywe punkty dostępowe, źle skonfigurowane punkty dostępowe, sieci typu ad hoc, spoofing MAC, punkty dostępowe typu Evil Twin lub Honeypot, itp. • System musi zapewniać ochronę przed atakami typu Denial of Service, w tym takimi jak wysyłanie tysięcy fałszywych uwierzytelnień lub asocjacji, „zalewanie" poleceniami unieważnienia uwierzytelnienia lub dysasocjacji, „zalewanie" wiadomościami protokołu EAPOL (EAP over LAN) . • System musi zapewniać możliwość lokalizacji zagrożeń, bez względu na to czy są one aktualnie aktywne czy też nie. • System musi umożliwiać administratorom sieci zmianę przeznaczenia punktów dostępowych realizujących usługi WLAN na sensory, na stałe lub tymczasowo przez prostą operację zarządzania polegającą na naciśnięciu odpowiedniego przycisku. • System powinien umożliwiać wykrywanie access-pointów typu rouge (IEEE 802.11a/g/n),
6.	Zarządzanie	• Musi umożliwiać zarządzanie poprzez telnet, ssh, https, snmpv3 oraz dedykowaną aplikację do zarządzania • System musi obsługiwać wiele typów kontrolerów (wirtualnych i sprzętowych) dla różnych typów wdrożeń sieci. • Wymagane jest scentralizowane raportowanie i konfiguracja WIPS/WIDS • W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie, bez interwencji użytkownika • System zarządzania łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika • Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g oraz 802.11n • System zarządzania łącznością radiową RF Management musi wspierać funkcje automatycznego wyboru kanału i automatycznej kontroli mocy emitowanego sygnału TPC (Transmit Power Control) • Kontroler musi zapewniać zarządzanie oparte o graficzny interfejs użytkownika • Musi pozwalać nietechnicznym pracownikom na tworzenie tymczasowych kont gości i dystrybuowanie zezwoleń poprzez łatwy w użyciu graficzny interfejs użytkownika
7.	Certyfikaty	• System musi posiadać certyfikat 802.11n WiFi dla kompatybilności w sieciach WLAN.

8.	Integracja	• Musi w pełni współpracować z punktami AP, systemem zarządzania oraz Rozwiązaniem kontroli dostępu do sieci NAC.
9.	Gwarancja	• Roczna gwarancja producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.