ZAŁĄCZNIK NR 1 do SIWZ

SPECYFIKACJA TECHNICZNA – opis przedmiotu zamówienia

Zamówienie obejmuje dostarczenie serwerów i systemu WLAN, instalację systemów oraz przeprowadzenie testu poprawności działania w siedzibie Zamawiającego. Wszystkie podane parametry techniczne są parametrami minimalnymi. Wykonawca może zaproponować sprzęt o parametrach technicznych wyższych, lecz nie gorszych od wskazanych przez Zamawiającego. W przypadkach, w których Zamawiający dokonał opisu przedmiotu zamówienia w SIWZ przez wskazanie znaków towarowych lub pochodzenia, wykonawcy zobowiązani są do oferowania urządzeń określonych w opisie przedmiotu zamówienia lub równoważnych o parametrach tego typu, lecz nie gorszych od wskazanych przez Zamawiającego. Do oceny parametrów technicznych będą brane pod uwagę wszystkie parametry techniczne danego sprzętu.

Wszystkie elementy przedmiotu zamówienia, muszą być fabrycznie nowe (nieużywane), nie mogą być prototypem, muszą pochodzić z bieżącej oferty, wyprodukowane nie wcześniej niż w 2014 r.

Wymagana gwarancja na całość przedmiotu zamówienia minimum 36 miesięcy.

W przypadku, gdy naprawa sprzętu jest dłuższa niż 2 dni robocze lub istnieje konieczność oddania części (np. dysku, płyty głównej itp.) do serwisu Wykonawca na żądanie Zamawiającego jest zobowiązany do podstawienia zastępczego sprzętu o takich samych parametrach i standardach lub uzgodniony sprzęt o podobnej funkcjonalności na okres naprawy gwarancyjnej. Sprzęt zastępczy powinien być dostarczony następnego dnia roboczego po dniu, w którym nastąpiło zgłoszenie.

Sprzedawca zapewnia serwis gwarancyjny w miejscu użytkowania W przypadku, gdy naprawa uszkodzonego sprzętu potrwa dłużej niż 3 tygodnie lub sprzęt był naprawiany 3 razy i nastąpi kolejna awaria, Zamawiającemu przysługuje wymiana sprzętu na nowy, taki sam lub uzgodniony, o co najmniej takich samych parametrach.

Okres gwarancji zostanie automatycznie wydłużony o czas trwania naprawy.

CZĘŚĆ 1

Serwer Rack – 5 sztuk

Komponent	Minimalne wymagania
Obudowa	Obudowa Rack o wysokości maks. 2U z możliwością instalacji min. 24 dysków 2.5" Hot Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli. Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Procesor	Dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 889 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej. Do oferty należy załączyć wynik testu dla serwera z oferowanymi procesorami.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Pamięć RAM	128 GB pamięci RAM typu LV RDIMM o częstotliwości pracy 1333MHz. Płyta powinna obsługiwać do 768GB pamięci RAM, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczonych dla pamięci. Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, SBEC, Lockstep
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum trzy sloty x16 generacji 3 o prędkosci x8 niskoprofilowe - minimum jeden slot x16 generacji 3 o prędkości x8 - minimum dwa sloty x16 generacji 3 o prędkości x16 pełnej długości i wysokości
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	min. 4 porty USB 2.0 , 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232
Interfejsy sieciowe	Minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT , interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI Express. Wsparcie dla protokołów iSCSI Boot oraz IPv6. Możliwość instalacji wymiennie modułów udostępniających: - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+ - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+
Kontroler dysków	Sprzętowy kontroler dyskowy, posiadający min. 1GB nieulotnej pamięci cache , możliwe konfiguracje poziomów RAID : 0, 1, 5, 6, 10, 50, 60
Wewnętrzna pamięć masowa	Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS, SSD oraz samoszyfrujących dostępnych w aktualnej ofercie producenta serwera. Zainstalowane 8 dysków twardych o pojemności min. 146GB SAS 15k RPM każdy, skonfigurowane fabrycznie przez producenta serwera w dwa osobne poziomy zabezpieczeń RAID 5. Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash z możliwoscią konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde.
Zasilacze	Redundantne zasilacze Hot Plug o mocy maks. 750W każdy
Wentylatory	Minimum 6 redundantnych wentylatorów Hot-Plug
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

Karta zarządzająca	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów - wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla IPv6 - wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer - integracja z Active Directory - możliwość obsługi przez dwóch administratorów jednocześnie - wsparcie dla dynamic DNS - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej - możliwość podłączenia lokalnego poprzez złącze RS-232 - w przypadku awarii karty sieciowej, kontrolera RAID dla dysków wewnętrznych lub płyty głównej, w przypadku wymiany serwisowej zostaną wczytane automatycznie te same ustawienia i wersje firmware, BIOS, specyficzne dla danych komponentów zapisane na wbudowanej w karte zarządzającą pamięci flash.. Jeśli funkcjonalność ta wymaga płatnych komponentów lub usługi dodatkowej to powinny zostać uwzględnione w wycenie.
Gwarancja	Trzy lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem– dokumenty potwierdzające załączyć do oferty
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2008 R2 x64, x86, Microsoft Windows Server 2012
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

CZĘŚĆ 2

Serwery aplikacyjne – 2szt.			
L.p.	**Parametr**	**Opis wymagań Zamawiającego**	
1.	Procesor	– zainstalowane min. cztery identyczne procesory 64-bitowe – procesory dedykowane do pracy w serwerach – liczba rdzeni/procesor: min. 16 – procesory muszą umożliwiać osiągnięcie wyniku min. 1050 pkt. w teście SPECint_rate2006 dla układu 4-procesorowego – procesory muszą umożliwiać osiągnięcie wyniku min. 810 pkt. w teście SPECfp_rate2006 dla układu 4-procesorowego – Wynik musi być opublikowany na stronie www.spec.org dla dowolnego modelu serwera z zainstalowanymi 4-ema oferowanymi procesorami.	
2.	Płyta główna	– min. 4 sloty na procesory – min. 32 sloty pamięci RAM – maksymalna wielkość pamięci RAM: 1TB – zintegrowane dwa porty RJ-45 10/100/1000 – zintegrowany port RS-232	

		– zintegrowany, dedykowany port RJ-45 zarządzający (BMC) – zintegrowane złącze VGA – min. 2 porty USB – min. 5 slotów PCI-e 2.0 x8 (w tym trzy ze złączami x16) – min. 1 slot PCI-e 2.0 x4 – min. 1 slot PCI-e 2.0 x4 ze złączem x8	
3.	Pamięć RAM	– zainstalowane min. 256GB – przepustowość pamięci min. 12800MB/s – wydajność min. 1600MT/s – korekcja błędów ECC oraz SDDC lub Advanced ECC – obsadzona tylko połowa slotów pamięci	
4.	LAN	– karty sieciowe muszą wspierać load balancing, failover i TCP/IP Offload lub TSO oraz posiadać funkcjonalność PXE (Preboot Execution Environment) - – zainstalowane dwie dodatkowe karty dual-port 10Gb/s DAC/SFP+ ze sprzętowym wsparciem dla iSCSI Offload	
5.	Kontroler RAID	– sprzętowy kontroler RAID SAS2 – obsługa dla min. 6 dysków SAS2 – kontroler współpracujący z systemem Linux bez potrzeby instalacji dodatkowych sterowników – wsparcie w jądrze systemu – dostępne poziomy RAID 0, 1, 5, 10, 50, 60 – min. 1GB pamięci cache	
6.	HDD	Obsługa min. 6-u dysków twardych 2,5”. Zainstalowane 6szt. jednakowych dysków twardych SAS2 o parametrach: – format: 2,5” Hot-Plug – interfejs zewnętrzny SAS2 (6Gbps) – prędkość obrotowa: min. 10kRPM – pojemność: min. 1.2TB – wsparcie dla NCQ Oferowane dyski twarde muszą być przeznaczone do pracy ciągłej 24h przez 365 dni w roku oraz muszą być podłączone do kontrolera RAID pkt. 5.	
7.	Zarządzanie	Serwery muszą umożliwiać zdalne zarządzanie poprzez dedykowane złącze RJ-45 charakteryzujące się następującymi funkcjonalnościami: zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, temperatury, konfiguracji serwera, o przekroczeniu zadanego dozwolonego prądu dla każdej z kart), szyfrowane połączenie (SSL) oraz autentykacje i autoryzację użytkownika, możliwość załączenia, wyłączenia i zresetowania serwera, możliwość podmontowania zdalnych wirtualnych napędów, wirtualną konsolę z dostępem do myszy, klawiatury, wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, zgodność z Intel Node Manager 2.0, VLAN tagging, SSH, możliwość obsługi przez trzech administratorów jednocześnie, wysyłanie do administratora maila z powiadomieniem o awarii. Rozwiązanie sprzętowe niezależne od	

		systemów operacyjnych. Zdalne zarządzanie musi posiadać wsparcie dla KVM-over-IP oraz Virtual-media.	
8.	Certyfikaty	Serwery muszą być wyprodukowane zgodnie z normami ISO 9001, ISO 14001 oraz posiadać deklaracje CE. Do oferty należy dołączyć powyższe certyfikaty wystawione dla Producenta serwera	
9.	Kompatybilność	Wszystkie komponenty serwerów muszą być kompatybilne (dostępność sterowników) z systemami operacyjnymi opartymi o jądro Linux 3.2.14 lub nowszej	
10.	Gwarancja	36 miesięcy gwarancja producenta serwerów. Czas reakcji serwisu - do końca następnego dnia roboczego. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta.	
11.	Zasilanie	Każdy serwer musi być wyposażony w redundantne hot-plugowe zasilacze o mocy max. 1100W (per zasilacz)	
12.	Inne	– obudowa: max 2U z możliwością wymiany zasilaczy, wentylatorów w trakcie pracy – obudowa musi posiadać szyny rack oraz organizer kabli – obudowa serwera musi zapewniać redundantne chłodzenie podzespołom – ze względu na ograniczenia miejsca w szafach rack obudowa nie może być głębsza niż: 72cm	

Macierze dyskowe – 2szt.			
L.p.	**Parametr**	**Opis wymagań Zamawiającego**	
1.	Obudowa	– obudowa w formacie max. 2U, montowana w szynach rack z organizerem przewodów – obudowa musi pozwalać na wymianę dysków, zasilaczy oraz modułów I/O podczas pracy – obudowa musi umożliwiać korzystanie z min. 12 dysków hot-plug w formacie 3,5” SAS2 (7,2K, 10K, 15K) oraz SSD – obudowa musi posiadać redundantne zasilacze (min. 2, o łącznej mocy max. 1400W) oraz redundantny system wentylatorów – ze względu na ograniczenia miejsca w szafach rack oferowane macierze nie mogą być głębsze niż 60cm.	
2.	Parametry macierzy	– min. dwa reduntantne moduły zarządzające – min. 1 port SAS SFF-8088 wejściowy per moduł zarządzający – min. 1 port SAS SFF-8088 wyjściowy per moduł zarządzający	
3.	Kontroler HBA	Do macierzy musi być dostarczony kontroler RAID o parametrach: – interfejs wewnętrzny: PCI-e x8 – interfejs zewnętrzny: SAS2 – ilość portów zewnętrznych: 2x SAS2 (6Gbps) – maksymalna ilość obsługiwanych dysków min. 192 – pamięć cache Non-Volatile: min. 1GB (taktowanie min.	

		800MHz DDR-2) – wspierane sprzętowo poziomy RAID: 0, 1, 5, 6, 10, 50, 60, JBOD – wsparcie dla migracji poziomu RAID – możliwość dodawania dysków do skonfigurowanego poziomu RAID – wsparcie dla redundant-path – wsparcie dla IO load balancingu – ilość macierzy możliwych do podłączenia do pojedyńczego kontrolera: min. 8 – bateria BBU (Batery Backup Unit) – wsparcie dla systemów Linux (RHEL/CentOS) – kontroler musi współpracować z oferowaną macierzą dyskową	
4.	Dyski	Zainstalowane min. 5 jednakowych dysków o parametrach: – pojemność: min. 4TB – interfejs zewnętrzny: SAS2 (6Gbps) – prędkość obrotowa: min. 7.2kRPM – wsparcie dla NCQ, hot-swap – oferowane dyski muszą być przetestowane przez producenta macierzy dyskowej Oferowane dyski twarde muszą być przeznaczone do pracy ciągłej 24h przez 365 dni w roku oraz muszą być podłączone do kontrolera RAID pkt. 5.	
5.	Certyfikaty	Macierz musi być wyprodukowana zgodnie z normami ISO 9001, ISO 14001 oraz posiadać deklaracje CE. Do oferty należy dołączyć powyższe certyfikaty wystawione dla Producenta serwera	
6.	Gwarancja	36 miesięcy gwarancja producenta macierzy. Czas reakcji serwisu - do końca następnego dnia roboczego. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta.	

Wymagania dodatkowe			
L.p.	**Parametr**	**Opis wymagań Zamawiającego**	
1.	Okablowanie	– w momencie dostawy wymagane jest dostarczenie pełnego okablowania (wszystkie połączenia sieciowe, zasilanie, monitoring)	
2.	Ograniczenia licencyjne	w momencie dostawy serwery i macierze dyskowe nie mogą podlegać ograniczeniom licencyjnym nie pozwalającym na	

		wykorzystanie wszystkich oferowanych przez producenta funkcjonalności	
3.	Współpraca urządzeń	Ze względu na planowaną konfigurację wymagane jest by serwery (w tym ich podzespoły) oraz macierze zostały ze sobą przetestowane.	

CZĘŚĆ 3

Serwer – 2 sztuki

Nazwa parametru	Wymagania minimalne
Przeznaczenie	Serwer aplikacyjny i bazodanowy ogólnego zastosowania
Obudowa	Obudowa o wysokości maksymalnie 1U, dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, wyposażona w panel diagnostyczny LCD.
Typ procesora	Procesor wielordzeniowy dedykowany do pracy w serwerach wieloprocesorowych, pozwalający na uruchomienie systemu Linux 64-bit, nie więcej niż 65W TDP.
Wydajność systemu	Oferowany model serwera musi osiągać w teście SPECint_2006 rate Baseline minimum 217 pkt. w konfiguracji 2 procesory / 12 rdzeni (tj. 6 rdzeni na procesor). Wyniki testu dla oferowanego modelu serwera muszą być opublikowane i powszechnie dostępne na stronie www.spec.org. Zainstalowane procesory muszą pozwalać na uruchomienie co najmniej 12 równoległych wątków.
Ilość procesorów	Zainstalowane 2
Pamięć RAM	Minimum 64 GB DDR3, Dual Rank LV, RDIMM lub równoważna, możliwość rozszerzenia pamięci do minimum 256 GB.
Płyta główna	Dwuprocesorowa, dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera.
Sloty PCIe	minimum 1 slot x16 G2
Dyski HDD	3 x 600GB, SAS 6Gbps, 3.5-in, 15K RPM Hard Drive (Hot Plug). Możliwość zainstalowania do 4 dysków SAS, SATA lub SSD, 3.5-in w obudowie (Hot Plug).
Kontroler macierzowy	Kontroler macierzowy SAS/SATA/SSD, umożliwiający konfigurację dysków w RAID 0, 1, 5, 6, 10, 50, 60
Karty rozszerzeń	Zintegrowane z płytą główną 2 porty GigabitEthernet. Zintegrowane porty sieciowe muszą wspierać load balancing, failover i TCP/IP Offload Engine.
Karta graficzna	Zintegrowana karta graficzna
Zasilanie	Redundantne zasilacze typu Hot-Plug. Min. 500 W na zasilacz.
Zarządzanie	Możliwość wyposażenia serwera w kartę zdalnego zarządzania (konsoli) pozwalającej na:

	włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu i restartu OS). Serwer musi posiadać możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Baseboard Management Controller, zgodność z normą IPMI 2.0.
Inne wymagania dotyczące sprzętu:	1. Urządzenia muszą być fabrycznie nowe. 2. Wszystkie oferowane komponenty serwera muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2008 lub normą równoważną. 3. W momencie oferowana wszystkie elementy oferowanej architektury muszą być dostępne (dostarczane) przez producenta. 4. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. 5. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych. 6. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej. 7. Do każdego urządzenia musi być dostarczony komplet sterowników pozwalających na uruchomienie systemu Ubuntu/Debian Linux, jeśli bez nich nie jest to możliwe. 8. Wszystkie serwery muszą posiadać Certyfikat CE produktu albo spełniać normy równoważne. 9. Oferowane serwery muszą być przygotowane do współpracy z systemami operacyjnymi takimi jak: Microsoft Windows Server 2008, Microsoft Windows Server 2008, LINUX Red Hat, SLES 10. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz. 11. Zamawiający wymaga, aby całość oferowanego sprzętu pochodziła z oficjalnego kanału sprzedaży na terytorium Rzeczypospolitej Polskiej. 12. Zamawiający zastrzega sobie możliwość zgłaszania awarii bezpośrednio w lokalnej (polskiej) organizacji serwisowej producenta sprzętu. W przypadku uzasadnionych wątpliwości Zamawiający może żądać po dostawie sprzętu dokumentów potwierdzających fakt świadczenia serwisu gwarancyjnego przez lokalną organizację serwisową producenta.

CZĘŚĆ 4

Specyfikacja techniczna do przetargu.

Projekt sieci WLAN dla Wydziału Biologii UW zakłada zintegrowanie bezprzewodowej sieci LAN z istniejącą infrastrukturą budynku Wydziału Biologii przy ul. Miecznikowa 1. Rozwiązanie ma zostać oparte na kontrolerze WLAN sterującym roamingiem, mocą sygnału urządzeń acces-point (AP), dostępem do sieci w oparciu o polityki bezpieczeństwa oraz punktami dostępowymi obsługującymi standard 802.11n.
Na tym etapie inwestycji projekt obejmuje sieć WLAN w części A i B (parter i piętro pierwsze) oparty na 9 AP wraz z instalacją okablowania i montażem oraz skonfigurowanie urządzeń. Projekt zakłada wykorzystanie następujących urządzeń:

Wymagania sprzętowe i programowe.

Kontroler sieci WLAN **1 sztuka**

Kontroler sieci WLAN		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne

1.	Parametry	• Kontroler sieci bezprzewodowej w momencie dostawy musi obsługiwać minimum 9 punktów dostępowych w normalnym trybie pracy. Kontroler musi umożliwiać rozbudowę do minimum 50 punktów dostępowych w trybie normalnej pracy oraz do minimum 100 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	• Musi posiadać 5 letnią gwarancje producenta, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.

Sieciowy przełącznik dostępowy 2 sztuki

Sieciowy przełącznik dostępowy		
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	1. 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 2. Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania (COMBO), 3. Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych, 4. 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	5. Minimalna wielkość pamięci SDRAM: 512 MB, 6. 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, • 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	• Gwarancja producenta obejmująca wysyłkę następnego dnia roboczego, z dostępem do nowych funkcjonalności, wsparcia technicznego przez email, telefon w wymiarze 8x5 oraz aktualizację oprogramowania, na okres nie krótszy niż 5 lat.

Punkty dostępowe (AP) 9 sztuk

Punkt dostępowy AP		
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 B A S E - T RJ-45 z technologią autosensing • Dedykowany port konsoli zarządzającej typu RJ-45

3.	Standardy sieciowe	Punkt dostępowy musi obsługiwać następujące funkcjonalności: • Zgodnść 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 • 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 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 3x3 MIMO • 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. 6 gniazd SMA RP umożliwiających podłączenie zewnętrznych anten
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 3x3 przy zasilaniu przez jedno źródło zgodne ze standardem IEEE 802.3af, bez wpływu na działanie kluczowych funkcji i wydajność • Wsparcie dla mechanizmu minimum „3x3:3 ” dla wszystkich nadajników - 3 anteny nadawcze, 3 anteny odbiorcze, 3 strumienie przestrzenne z dwoma modułami radiowymi • 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	Wydajność transmisji	• Przepustowość transmisji min. 900Mbps • Minimalna moc transmisji na radio: 25 dBm • Minimalne wzmocnienie anteny na radio: 3 dBi
10.	Dodatkowe	• Oprogramowanie działające na punktach dostępowych powinno umożliwiać oddzielną specyfikację częstotliwości dla każdego z modułów radia • Wraz z punktem dostępowym należy dostarczyć, najlepiej od tego samego producenta, elementy do montażu punktu dostępowego do sufitu podwieszanego
11.	Gwarancja	• Gwarancja obejmująca wysyłkę następnego dnia roboczego po zgłoszeniu awarii, aktualizację oprogramowania, wsparcia technicznego przez email, telefon w wymiarze 8x5, na okres nie krótszy niż 5 lat