5.3.2 Przełączniki szkieletowe 24 porty 10/100/1000 - (3 szt.)

Wymagania ogólne

- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem nowym, nie używanym (dostarczanym) wcześniej w innych projektach.
- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji świadczonej przez producenta sprzętu.
- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży producenta. Co zgodnie z opisem wyżej, będzie on sprzętem nowym i posiadającym stosowny pakiet usług gwarancyjnych kierowanych również do użytkowników z obszaru Rzeczpospolitej Polskiej.

Element	Wymagane minimalne parametry techniczne urządzenia
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.
Interfejsy fizyczne	• Minimum 24 porty 10/100/1000 BASE-T RJ45 z technologią auto-sensing, auto-negotiating MDI/MDI-X • Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania, • Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych, • Minimum 1 port konsolowy do zarządzania przełącznikiem.
Montaż	• Standardowy stelaż teletechniczny 19" typu Rack o wysokości nie większej niż 1 U.
Wydajność	• Minimalna przepustowość: 35 Mpps, • Minimalna wydajność przełącznika: 48 Gbps • Minimalna wydajność po łączenia w stosie: 20 Gbps, a w urządzeniach modularnych minimum 20 Gbps pomiędzy modułami.
Zasilanie	• Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania.
Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 8 000.
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 255 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.

Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3, • Standardowy interfejs wiersza poleceń CLI, • Secure Shell (SSH), • RADIUS, • TACACS+, • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie tekstowej, • Telnet, • Secure Copy oraz Secure FTP, • Simple Network Time Protocol (SNTP) lub NTP, • RMON – wsparcie dla minimum 4 grup (history, statistics, alarms, events) • Port mirroring w oparciu o protokół SPAN lub równoważny
Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • LLDP • 802.3ad Link Aggregation, • 802.1D, • 802.1s Multiple Spanning Tree, • 802.1w Rapid re-convergence of Spanning Tree, • 802.3x Flow Control, • IGMPv1,v2,v 3, • IGMP Snooping, • Ramki Jumbo Frames (minimum 9 kB), • Standardowe listy ACL, • Rozszerzone listy ACL, • RIPv1 i RIPv2, • Trasy statyczne, • DHCP/BootP Relay.
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,
QoS	Przełącznik musi obsługiwać następujące funkcjonalności: • Obsługa priorytetów zgodna z IEEE 802.1p, • Obsługa minimum 4 kolejek priorytetów na każdym porcie, • Obsługa wielu mechanizmów kolejkowania - minimum SPQ • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego, • Możliwość przypisania ruchu do różnych sieci VLAN
Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o poprzez IEEE 802.1x, o wykorzystujące adres MAC, • Obsługa Dynamic VLAN Assignment (RFC 3580),
Gwarancja	• Gwarancja 36 miesięcy 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.

5.4 Budowa Stacji Bazowych

Zamawiający zakłada, budowę 4 Stacji Bazowych (ich lokalizacje zostały określone wyżej) w których zostaną zainstalowane urządzenia stanowiące ich wyposażenie.

W warstwie dostępowej sieci wykonawca musi zapewnić urządzenia radiowe, pracujące w paśmie licencjonowanym.

Budowane Stacje Bazowe, powinny być wyposażone w następujący zestaw elementów i urządzeń:

a) w zakresie infrastruktury pasywnej) :

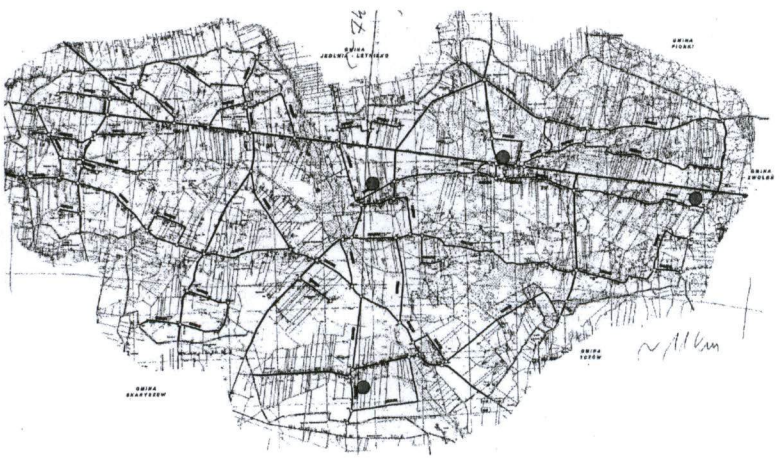
- maszty i/lub konstrukcje wsporcze pod anteny
- szafka dystrybucyjna 19"
- okablowanie zasilające do szaf
- okablowanie sygnałowe/logiczne

b) w zakresie infrastruktury aktywnej

- stacje bazowe systemu Punkt-Wielopunkt
- anteny sektorowe stacji bazowych o azymutach 0, 120, 240 stopni
- urządzenia synchronizacji czasowej
- zarządzalny przełącznik dystrybucyjny (określony wyżej)
- zasilacz awaryjny UPS

Lokalizacja szaf dystrybucyjnych, sposób prowadzenia instalacji zasilającej i sygnałowej powinien być wcześniej uzgodniony z właścicielem obiektu.

Poniżej przedstawiono schemat lokalizacji węzłów sieci oraz minimalne wymagania techniczne, funkcjonalne i gwarancyjno- serwisowe poszczególnych elementów i urządzeń do budowy stacji bazowych sieci.



Rys. 1 Schemat lokalizacji węzłów (Stacji Bazowych)

5.4.1 Stacje Bazowe (min. 4 kpl.)

Wymagania techniczne:

1. Wykorzystanie technik OFDM MIMO 2x2 oraz Diversity;
2. Obsługiwane modulacje BPSK/QPSK/16QAM/64QAM;
3. Korekcja błędów FEC k= 1/2, 2/3, 3/4, 5/6;
4. Obsługiwane szerokości kanałów 10, 20 oraz 40MHz;
5. Automatyczny wybór kanałów ACS i żądanie retransmisji ARQ;
6. Adaptacyjna modulacja i kodowanie;
7. Symetryczny przydział ruchu co najmniej 80% w kierunku Downlink;
8. Obsługiwana szerokość ramki 2048 bajtów;
9. Wydajność sprzętowa co najmniej 360.000PPS;
10. Synchronizacja za pomocą GPS;
11. Obsługa Multicast i Broadcast;
12. Możliwość konfiguracji CIR;
13. Obsługa QoS poziom 4 zgodnie z 802.1p i Diffserv;
14. Obsługa VLAN 802.1Q, 802.1P, QinQ;
15. Wbudowany analizator widma;
16. Dostępne interfejsy IDU 1000BaseT oraz SFP;
17. Dostępne złącza antenowe typu N dla anteny sektorowej;
18. Możliwość lokalnej i zdalnej aktualizacji oprogramowania;
19. Zarządzanie za pomocą dedykowanego oprogramowania, przeglądarki internetowej oraz przy pomocy protokołów SNMP v3 oraz Telnet;
20. Zasilanie stacji bazowej poprzez PoE;
21. Pobór mocy urządzeń radiowych <25W;
22. Klasa szczelności urządzeń radiowych IP67;
23. Temperaturowy zakres pracy od -35^{0}C do 60^{0}C;
24. Certyfikat CE;

Wymagania gwarancyjne i serwisowe

Wymagany jest 36 miesięczny serwis gwarancyjny na wszystkie urządzenia, świadczony w następującym zakresie:

- przyjmowanie zgłoszeń bezpośrednio w godzinach od 8:00-16:00 w dni robocze
- naprawa lub wymiana w następny dzień roboczy od pisemnego zgłoszenia lub mailem
- prawo do aktualizacji oprogramowania systemowego

5.4.2 UPS 1000VA RACK - (4 szt.)

Wymagania techniczne

1. Moc pozorna 1000VA
2. Moc rzeczywista 900 Wat
3. Architektura UPS'a line-interactive
4. Minimalny czas podtrzymywania dla obciążenia 100% - 4 min
5. Minimalny czas podtrzymywania dla obciążenia 50% - 12 min
6. Urządzenie musi posiadać układ automatycznej regulacji napięcia AVR
7. Urządzenie musi być wyposażone w port komunikacyjny RS232, port USB, ochronę linii RJ45
8. Urządzenie musi posiadać oprogramowanie do monitorowania parametrów pracy UPSa
9. Urządzenia musi posiadać obudowę typu Rack 19"
10. Maksymalna wysokość urządzenia 2U

Wymagania gwarancyjne i serwisowe

- urządzenia typu UPS muszą być objęte 36-miesięczną gwarancją producenta

5.5 Wyposażenie Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią szerokopasmową.

5.5.1 Przełącznik szkieletowy L3 (1 szt.)

Wymagania techniczne

Element	Wymagane minimalne parametry techniczne urządzenia
Architektura	• Przełącznik musi 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.
Interfejsy fizyczne	• Minimum 24 porty 10/100/1000 BASE-T RJ45 PoE (zgodnych ze standardem 802.3.af, z technologią auto-sensing, auto-negotiating MDI/MDI-X • Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania, • Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych, • Minimum 1 port konsolowy do zarządzania przełącznikiem.
Montaż	• Standardowy stelaż teletechniczny 19" typu Rack o wysokości nie większej niż 1 U.

Wydajność	• Minimalna przepustowość: 35 Mpps, • Minimalna wydajność przełącznika: 48 Gbps • Minimalna wydajność połączenia w stosie: 32 Gbps
Zasilanie	• Przełączniki muszą być wyposażone w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3af, • Przełączniki dodawane do stosu/wieży muszą zapewniać moc do 540 W dla funkcjonalności PoE, • Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania zapewniając zasilanie dla wszystkich portów PoE zgodnie ze standardami 802.3af
Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 12 000.
Sieci VLAN	• Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q, • Obsługa minimum 4 000 ID sieci VLAN oraz minimum 1 000 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3, • Standardowy interfejs wiersza poleceń CLI, • Secure Shell (SSH), • RADIUS, • TACACS+, • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie tekstowej, • Telnet, • Secure Copy oraz Secure FTP, • Simple Network Time Protocol (SNTP) lub NTP, • RMON – wsparcie dla minimum 4 grup (history, statistics, alarms, events) • Port mirroring w oparciu o protokół SPAN lub równoważny
Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • LLDP • 802.3ad Link Aggregation, • 802.1D, • 802.1s Multiple Spanning Tree, • 802.1w Rapid re-convergence of Spanning Tree, • 802.3x Flow Control, • IGMPv1,v2,v 3, • IGMP Snooping, • Ramki Jumbo Frames (minimum 9 kB), • Standardowe listy ACL, • Rozszerzone listy ACL, • DHCP/BootP Relay.
Protokoły routingu	Przełącznik musi obsługiwać następujące protokoły routingu: • RIPv1 i RIPv2, • Trasy statyczne, • OSPF, • PIM-SM,

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
QoS	Przełącznik musi obsługiwać następujące funkcjonalności: • Obsługa priorytetów zgodna z IEEE 802.1p, • Obsługa minimum 4 kolejek priorytetów na każdym porcie, • Obsługa wielu mechanizmów kolejkowania - minimum SPQ • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego, • Możliwość przypisania ruchu do różnych sieci VLAN
Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o poprzez IEEE 802.1x, o wykorzystujące adres MAC, • Obsługa Dynamic VLAN Assignment (RFC 3580),
Gwarancja	• Gwarancja 36 miesięcy 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

5.5.2 Urządzenie bezpieczeństwa sieciowego (1 szt.)

Wymagania techniczne

Element	Wymagane minimalne parametry techniczne urządzenia
Architektura	• System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować sprzętowa separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. • System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej. • System zabezpieczeń musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych. Musi istnieć możliwość jednoczesnej konfiguracji poszczególnych interfejsów w różnych trybach. • System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive oraz w trybie Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

Interfejsy fizyczne	• Minimum 8 porów 10/100/1000 BASE-T RJ45, • Minimum 8 portów 1000Base-X SFP, • Minimum 1 port konsolowy do zarządzania urządzeniem
Montaż	• Standardowy stelaż teletechniczny 19" typu Rack o wysokości nie większej niż 1 U.
Funkcjonalność	• System zabezpieczeń musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji. • System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa. • Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). • System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. • System zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. • System zabezpieczeń musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS) bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. • System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej, kontrolującego przynajmniej pocztę elektronicznej (SMTP, POP3, IMAP), FTP oraz HTTP i HTTPS bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza AV musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny. • System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza WF musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny • System zabezpieczeń transparentnie ustala tożsamość użytkowników sieci (integracja z Active Directory, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

Sieci VLAN	• Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. • Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
Wydajność	• Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż: o 2 Gb/s dla kontroli firewall (w tym kontrola aplikacji), o 1 Gb/s dla kontroli zawartości (w tym kontrola AV, IPS i WF) o 500 Mb/s dla połączeń IPSec VPN • Urządzenie zabezpieczeń musi obsługiwać nie mniej niż 250 000 jednoczesnych połączeń. • Urządzenie zabezpieczeń musi wspierać minimum 2 000 jednocześnie obsługiwanych tuneli IPSec VPN.
Funkcje zarządzania	• Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI), graficznej konsoli Web GUI oraz scentralizowanego systemu zarządzania. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
Funkcje routingu	• Urządzenie musi obsługiwać protokoły rutingu dynamicznego, nie mniej niż: o RIP, o BGP, o OSPF. • System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
Funkcje raportowania	• Urządzenie zabezpieczeń musi posiadać wbudowany twardy dysk (minimum 120 GB) do przechowywania logów i raportów. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń.
Bezpieczeństwo	• System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów. • System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama. • System zabezpieczeń musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

QoS	• System zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego.
Gwarancja i serwis	• 36 miesięcy gwarancji • Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. • Wraz z produktem wymagane jest dostarczenie opieki technicznej ważnej przez okres 36 miesięcy. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów oraz bazy kategorii stron WWW, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

5.5.3 Zasilacz awaryjny UPS 3000 VA (wraz bateriami) (1 szt.)

Wymagania techniczne:

1. Moc pozorna 3000VA
2. Moc rzeczywista 2600 Wat
3. Architektura UPS'a line-interactive
4. Minimalny czas podtrzymywania dla obciążenia 100% - 5 min
5. Minimalny czas podtrzymywania dla obciążenia 50% - 13 min
6. Urządzenie musi posiadać układ automatycznej regulacji napięcia AVR
7. Urządzenie musi być wyposażone w port komunikacyjny RS232, Port USB, ochronę linii RJ45
8. Urządzenie musi posiadać oprogramowanie do monitorowania parametrów pracy UPSa i być wyposażone w kartę RJ45 umożliwiającą wyłączenie serwerów w przypadku braku zasilania
9. Urządzenie musi posiadać możliwość rozbudowy poprzez dołożenie dodatkowego modułu bateryjnego
10. Urządzenia musi posiadać obudowę typu Rack 19''

Wymagania gwarancyjne i serwisowe

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją producenta.

5.5.4 Szafa rack

Wymagania techniczne:

1. Szafa serwerowa 42U szer:800 głeb:1000
2. Drzwi tylne i przednie perforowane z blachy, boki z blachy pełnej

3. Cokół 100 mm z możliwością poziomowania

Wyposażenie

1. Panel wentylacyjny dachowy z termostatem i 4 wentylatorami
2. Zaślepka filtracyjna w otworach podstawy szafy
3. Półka 2U 400 mm na urządzenia desktop
4. Półka ruchoma pod klawiaturę
5. Listwa zasilająca 19" z filtrem 2 szt

5.5.5 Serwery i urządzenia dodatkowe

5.5.5.1 Platforma do wirtualizacji środowisk serwerowych –serwer (1 szt.)

Wymagania techniczne (sprzętowe oraz systemowe):

Serwer sieciowy przeznaczony do zapewnienia usług dostępowych dla Beneficjentów sieci	
Płyta główna	- Wieloprocesorowa; - Minimum 7 złącz PCI Express 3 generacji (złącza mogą być uzyskane za pomocą dodatkowych kart) - Zintegrowany układ TPM 1.2.
Procesory	- Zainstalowane procesory osiągające w oferowanym serwerze w testach wydajności SPECint_rate2006 wynik min. 427 pkt;
Pamięć RAM	- Zainstalowane minimum 32 GB pamięci RAM DDR3 LV Registered - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing; - Minimum 24 gniazda pamięci RAM na płycie głównej, obsługa do minimum 1,5 TB pamięci RAM.
Obudowa	- Typ stelażowy, o maksymalnej wysokości 2U; - Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy
Kontrolery dyskowe	- Zainstalowany kontroler SAS 6G RAID 0,1 z portami wewnątrz obudowy
Dyski twarde	- Zainstalowane 4 dyski SAS 6G o pojemności minimum 900 GB każdy, 10 tys. obr./min., hotplug; - Minimum 8 wnęk dla dysków twardych hotplug 2,5"; - Obsługa dysków SAS, SATA, SSD.
Inne napędy zintegrowane	- Zintegrowany napęd DVD-RW

Kontrolery LAN	- zintegrowana dwuportowa 1Gb/s ze wsparciem iSCSI, RJ-45; - dodatkowa 4 portowa karta sieciowa 1Gb/s, RJ45
Porty	- zintegrowana karta graficzna ze złączem VGA (z przodu oraz z tyłu obudowy); - minimum 4x USB 2.0, w tym minimum 2 na panelu przednim, minimum 2 z tyłu obudowy; - 1x RS-232.
Zasilanie, chłodzenie	- Redundantne zasilacze hotplug o sprawności minimum 94% - Redundantne wentylatory hotplug;
Zarządzanie	- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta 1 Gb/s (dedykowane złącze RJ-45) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Oprogramowanie zarządzające i diagnostyczne 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 (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
Wspierane systemy	-Windows, VMware, Red Hat Linux, SUSE Linux
Gwarancja	- 3 lata gwarancji producenta serwera, realizowanej w miejscu instalacji sprzętu z gwarantowanym czasem usunięcia awarii następnego dnia roboczego od chwili zgłoszenia. - W przypadku uszkodzenia dysków w okresie gwarancji pozostają one u Zamawiającego.
Inne wymagania	- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801) 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;

Wymagania ogólne dotyczące instalacji oprogramowania na serwerach:

Na dostarczonych serwerach należy zainstalować oraz skonfigurować następujące oprogramowanie:

- instalacja oraz konfiguracja środowiska wirtualizacji serwerów w oparciu o dowolne dostarczone rozwiązanie do wirtualizacji.
- utworzenie oraz konfiguracja maszyny wirtualnej dla Systemu zarządzania siecią,
- dostawa, instalacja oraz konfiguracja Systemu zarządzania siecią na maszynie wirtualnej,
- utworzenie oraz konfiguracja maszyny wirtualnej dla Systemu zarządzania kontrolą dostępu do sieci,
- dostawa, instalacja oraz konfiguracja System zarządzania kontrolą dostępu do sieci na maszynie wirtualnej,

5.5.5.2 System zarządzania siecią (1 kpl.)

Element	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 wszystkimi urządzeniami sieci przewodowej. • 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	• Aplikacja w momencie dostawy musi obsługiwać minimum 10 urządzeń sieciowych oraz 10 punktów dostępowych • Aplikacja musi umożliwiać przyszłą rozbudowę do minimum 50 urządzeń sieciowych oraz minimum 100 punktów dostępowych
Gwarancja	• 3 letni bezpłatny dostęp do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.