Załącznik nr 6b do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA – Część 1

Dostawa sieci bezprzewodowej. Zadanie obejmuje dostawę I instalację urządzeń objetych przemiotem zamówienia, w tym doprowadzenie instalacji okablowania do każdego punktu dostepowego. W ramach zadania należy skonfigurować dwie sieci bezprzewodowe (SSID):

- Jedną dla urządzeń i pracowników Zamawiającego – z zaimplementowanymi mechanizmami uwierzytelniania w oparciu o posiadaną przez Zamawiającego usługę Active Directory
- Jedną sieć gościnną, do której dostęp wymaga zaakceptowania regulaminu wykorzystania sieci opracowanego przez Zamawiającego

Należy wykonać okablowanie skrętkowe dla 33 access pointów. Zamawiający nie przewiduje budowy nowych punktów dystrybucyjnych. Okablowanie skrętkowe dla access piontów ma być zakończone na patch panelach krosowych w istniejących punktach dystrybucyjnych. Szczegółowy zakres wdrożenia zostanie spisany i zaakceptowany przez Zamawiającego i Wykonawcę na etapie podpisania umowy.

Opis:

- Punkt dostępowy z antenami wewnętrznymi – 31 sztuk
- Punkt dostępowy z antenami zewnętrznymi – 2 sztuki
- Kontroler sieci WLAN – 1 sztuka
- System do zarządzania – 1 sztuka
- Okablowanie

Punkt dostępowy z antenami wewnętrznymi – 31 sztuk

Punkt dostępowy sieci WLAN z antenami wewnętrznymi		
Lp.	Nazwa parametru	Wymagania minimalne
1.	Pasma robocze	• Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości 802.11ac/a/n (5 GHz) i 802.11b/g/n (2.4 GHz)
2.	Interfejsy fizyczne	• 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 oraz U-APSD, • Szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC), • Obsługa do 16 SSID (8 na częstotliwość radiową), • Obsługa minimum 254 użytkowników jednocześnie, • 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,
4.	Anteny	• Min. 4 anteny wewnętrzne.
5.	Tryby pracy	• Tryb działania radio WLAN: Client access, Local mesh, Packet capture, WDS, • Obsługa technologii 802.11ac 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, • Instalacja typu plug & play, • Jednoczesna obsługa ruchu tunelowanego i mostowanego, • 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. • 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.	Dodatkowe	• Oprogramowanie działające na punktach dostępowych powinno umożliwiać oddzielną specyfikację częstotliwości dla każdego z modułów radia, • Wraz z punktem dostępowym należy dostarczyć, pochodzący od tego samego producenta, co dostarczane urządzenia, uchwyt umożliwiający montaż punktu dostępowego pod sufitem.
9.	Gwarancja	• Gwarancja producenta obejmująca wysyłkę następnego dnia roboczego, wsparcia technicznego przez email, telefon w wymiarze 8x5, na okres nie krótszy niż 5 lat.

Punkt dostępowy z antenami zewnętrznymi – 2 sztuki

Punkt dostępowy sieci WLAN z antenami zewnętrznymi		
Lp.	Nazwa parametru	Wymagania minimalne
1.	Pasma robocze	• Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości 802.11ac/a/n (5 GHz) i 802.11b/g/n (2.4 GHz)
2.	Interfejsy fizyczne	• 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 oraz U-APSD, • Szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC), • Obsługa do 16 SSID (8 na częstotliwość radiową), • Obsługa minimum 254 użytkowników jednocześnie, • 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,
4.	Anteny	• Min. 4 gniazda pozwalające na przyłączenie anten zewnętrznych • Wraz z punktem dostępowym wymagane jest dostarczenie anten sektorowych 120°, działających w paśmie 2.4 i 5GHz oraz kabli
5.	Tryby pracy	• Tryb działania radio WLAN: Client access, Local mesh, Packet capture, WDS, • Obsługa technologii 802.11ac 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, • Instalacja typu plug & play, • Jednoczesna obsługa ruchu tunelowanego i mostowanego, • 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. • 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.	Dodatkowe	• Oprogramowanie działające na punktach dostępowych powinno umożliwiać oddzielną specyfikację częstotliwości dla każdego z modułów radia, • Wraz z punktem dostępowym należy dostarczyć, pochodzący od tego samego producenta, co dostarczane urządzenia, uchwyt umożliwiający

		montaż punktu dostępowego pod sufitem.
9.	Gwarancja	• Gwarancja producenta obejmująca wysyłkę następnego dnia roboczego, wsparcia technicznego przez email, telefon w wymiarze 8x5, na okres nie krótszy niż 5 lat.

Kontroler sieci WLAN – 1 sztuka

Kontroler sieci WLAN		
Lp.	Nazwa parametru	Wymagania minimalne
1.	Parametry	• Kontroler sieci bezprzewodowej w momencie dostawy musi obsługiwać minimum 32 punkty dostępowe. Kontroler musi umożliwiać rozbudowę do minimum 250 punktów dostępowych. • Kontroler powinien zostać dostarczony w formie maszyny wirtualnej instalowanej na posiadanym przez Zamawiającego środowisku wirtualizacyjnycm.
2.	Mech. przekazywana danych	• Kontroler musi obsługiwać jednocześnie różne mechanizmy przekazywania danych, w tym routing, tunelowanie ruchu z punktu dostępowego do kontrolera i zamykanie ruchu lokalnie w punkcie dostępowym, • 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, dowolnie konfigurowany przez administratora, z wykorzystaniem wbudowanych narzędzi edycyjnych, wykorzystujących mechanizmy HTML i PHP, • Dostęp gościnny poprzez portal gościnny musi umożliwiać logowanie do sieci WLAN z wykorzystaniem autentykacji 802.1x, • Dostęp gościnny poprzez portal gościnny musi umożliwiać logowanie do sieci WLAN poprzez otrzymanie zezwolenia od uprawnionych użytkowników lub administratora, • Administrator lub uprawiony użytkownik przydzielając dostęp do Sieci Gości ma mieć wybór przydzielenia dostępu w interwałach czasowych.
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.

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	Integracja	• Musi w pełni współpracować z punktami AP, systemem zarządzania oraz rozwiązaniem kontroli dostępu do sieci.
8	Gwarancja	• 5-letnia gwarancja producenta, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.

System zarządzania siecią oraz uwierzytelniania użytkowników – 1 sztuka

System zarządzania siecią oraz uwierzytelniania użytkowników		
Lp.	Nazwa parametru	Wymagania minimalne
1.	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
2.	Architektura	• Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami wchodzącymi w skład proponowanego systemu oraz dawać możliwość zarządzania urządzeniami sieci przewodowej w przyszłości. • Musi zawierać zintegrowane aplikacje typu *plug-in*, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania. • Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej • Rozwiązanie musi integrować się ze środowiskiem wirtualnym VMware ESX i ESXi • Rozwiązanie musi zostać dostarczone w formie maszyn wirtualnych kompatybilnych z posiadanym przez Zamawiającego środowiskiem wirtualizacyjnym. Wymagane jest rozdzielenie funkcjonalności zarządzania

3.	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
4.	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

5.	Bezpieczeństwo	• Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji. • System powinien pełnić funkcję RADIUS Proxy i mieć możliwość korzystania zarówno z lokalnej bazy użytkowników jak i innych repozytoriów, tj. Active Directory i serwery LDAP bądź RADIUS. • 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 • Polityki muszą być przydzielane użytkownikom na podstawie spełnianych kryteriów, tj. przynależność do grupy użytkowników, rodzaj wykorzystywanego urządzenia, system operacyjny, lokalizacja, pora dnia, itd. • 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 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

6.	Kontrola	• 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.
8.	Skalowalność	• System w momencie dostawy musi obsługiwać wszystkie urządzenia wchodzące w skład dostarczanego systemu obsługi sieci bezprzewodowej. • Aplikacja musi umożliwiać przyszłą rozbudowę do minimum 100 urządzeń sieciowych oraz minimum 500 punktów dostępowych. • Wymagana jest możliwość uwierzytelniania co najmniej 1 500 urządzeń końcowych dziennie, z opcją późniejszej rozbudowy do co najmniej 5 000
9.	Gwarancja	• 5-letnia gwarancja producenta, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.

Okablowanie skrętkowe dla 33 punktów dostępowych

Okablowanie skrętkowe		
Lp.	Nazwa parametru	Wymagania minimalne
1.	Trasy kablowe	• Kable skrętkowe będą prowadzone w istniejących korytach kablowych.
2.	Kategoria okablowania	• Wymagane jest ułożenie kabla kategorii 5e lub wyższej
3.	Punkty dystrybucyjne	• Od strony access pointa kabel musi być zakończony wtykiem RJ45 a od strony punktu dystrybucyjnego na module umieszczonym w panelu krosowym. Okablowanie skrętkowe dla access piontów ma być zakończone na patch panelach krosowych w istniejących punktach dystrybucyjnych. Należy
3.	Wymagane certyfikacje	• Wszystkie elementy toru transmisyjnego mają być zgodne z wymaganiami obowiązujących norm elementów, na Kategorię 5e: Skrętka teleinformatyczna musi posiadać certyfikaty niezależnych instytutów badawczych (GHMT, 3P, DELTA, IŁ) w zgodności z normami {ISO/IEC 11801 ED.2.2((2011-06)), EN 50173-1((2011-09)), ANSI/TIA-568-C.2 ((2009-08))} dla potwierdzenia spełniania parametrów. • Moduł RJ45 Keystone JACK musi posiadać certyfikaty niezależnych instytutów badawczych (GHMT, 3P, DELTA, IŁ) w zgodności z normami {ISO/IEC 11801 ED.2.2((2011-06)), EN 50173-1((2011-09)), ANSI/TIA-568-C.2 ((2009-08))} dla potwierdzenia spełniania parametrów
4.	Pomiary wykonanej instalacji	Po wykonaniu należy wykonać pomiary 100% połączeń miedzianych zgodnie z odpowiednimi normami dla danej klasy okablowania. Do tego celu należy wykorzystać mierniki o odpowiednim poziomie dokładności pomiarów. Urządzenie/a którym będą wykonywane pomiary muszą być skalibrowane i posiadać ważny certyfikat wydany przez producenta. Wyniki pomiarów wszystkich torów (optycznych i miedzianych) muszą zostać umieszczone w dokumentacji powykonawczej. Wykonawcę obowiązuje w tym zakresie m.in.. norma PN-EN 50346:2004/A1:2009 „Technika informatyczna. Instalacja okablowania. Badanie zainstalowanego okablowania. Pomiar każdego toru transmisyjnego poziomego (miedzianego) powinien zawierać minimum: Wire Map mapa połączeń , Length długość poszczególnych par, Resistance rezystancja pary Capacitance pojemność pary Impedance impedancja charakterystyczna Propagation Delay czas propagacji, Delay Skew opóźnienie skrośne, Attenuation tłumienność, NEXT przesłuch, ACR stosunek tłumienia do przesłuchu, Return Loss tłumienność odbicia, ELFEXT ujednolicony przesłuch zdalny,

5.	Wymagane certyfikaty producenta	• Producent systemu okablowania musi posiadać certyfikat jakości EN ISO 9001:2008 w zakresie działalności handlowej i produkcyjnej.
6.	Gwarancja na system okablowania	• System okablowania strukturalnego powinien być objęty 25 letnią gwarancją systemową wystawianą przez producenta.

Przełączniki sieciowe – 2 sztuki
Jako rozbudowa system posiadanego przez Zamawiającego wymagane jest dostarczenie 2 sztuk przełączników sieciowych D-Link DGS-1510-28P lub równoważnych.