SPECYFIKACJA TECHNICZNA WYKONANIA I ODBIORU ROBÓT

STADIUM: Dokumentacja techniczna systemu łączności dla potrzeb Portu Lotniczego Gdynia – Kosakowo

MIEJSCOWOŚĆ: Kosakowo

OBIEKT: Port Lotniczy Gdynia – Kosakowo

TEMAT: **Specyfikacja techniczna dla systemu łączności Portu Lotniczego Gdynia – Kosakowo**

DATA WYKOANIA: Wrzesień 2012

ZLECENIODAWCA: **Port Lotniczy Gdynia Kosakowo Sp. z o.o.**

ADRES: Al. Marszałka Piłsudskiego 52/54, 81-382 Gdynia

WYKONAŁ:

Imię Nazwisko	Firma	Podpis
mgr inż. Bogusz Danowski	TeleBAD Bogusz Danowski ul. Skalniakowa 5 81-198 Kosakowo	
inż. Tomasz Szymański	PIRET Tomasz Szymański Ul. Grabowa 6A/4 80-060 Gdańsk	

Spis treści

1 Część ogólna

1.1 Nazwa

Dostawa z montażem Systemu Łączności Portu Lotniczego Gdynia – Kosakowo.

1.2 Nazwy i kody

32412000-4 Sieci komunikacyjne

32422000-7 Elementy składowe sieci

32424000-1 Infrastruktura sieciowa

32581000-9 Sprzęt do przesyłu danych

1.3 Podstawowe definicje

Objaśnienia niektórych terminów wykorzystywanych w niniejszej dokumentacji:

LSP – Budynek Lotniskowej Straży Pożarnej

GA – Budynek Terminala GA

PLGK – Port Lotniczy Gdynia Kosakowo

MDF – Główny Punkt Dystrybucyjny

IDF – Pośredni Punkt Dystrybucyjny

PDC – Podstawowy kontroler domeny

BDC – Zapasowy kontroler domeny

Switch – przełącznik sieciowy

1.4 Przedmiot i zakres dostawy

Dostawa wraz z montażem, konfiguracją i uruchomieniem Systemu Łączności PLGK.

Zakres dostawy:

1. Wykonanie Dokumentacji Montażu
2. Dostawa urządzeń, oprogramowania, licencji i koniecznych kabli połączeniowych Systemu Łączności
3. Montaż elementów i urządzeń Systemu Łączności
4. Konfiguracja urządzeń zgodnie z wytycznymi Inwestora
5. Wykonanie Dokumentacji Powykonawczej

6. Uruchomienie i sprawdzenie działania systemu (w obecności przeszkolonego Administratora Inwestora)

Według wymogów Inwestora i wytycznych z „Koncepcji Systemu Łączności" w poniższych lokalizacjach, mają zostać zamontowane wyszczególnione urządzenia:

1. MDF L (pom. 4.1.05 lub 06):
    a. Switch rdzeniowy – 1szt
    b. Przełącznik dostępowy dla użytkowników 48 portowych (typ 1)
    c. Firewall tzw. Next Generation i IDS/IPS
    d. Kontroler sieci bezprzewodowej WLAN
    e. Serwer PDC (Kontrolera domeny)),
    f. Serwer wirtualizacyjny dla Aplikacji zarządzającej, NAC, Korelacji zdarzeń z macierzą dysków
    g. Centrala abonencka obsługująca PSTN, ISDN, VoIP
    h. System nagrywania współpracującego z systemem telefonicznym
2. IDF L1 - 2 piętro LSP (pom. 3.1.05):
    a. Przełącznik dostępowy dla użytkowników 48 portowych (typ 1)
    b. Przełącznik dostępowy dla użytkowników 24 portowych (typ 2)
3. IDF L2 – 1 piętro LSP (pom. 2.3.04):
    a. Przełącznik dostępowy dla użytkowników 48 portowych (typ 1)
    b. Przełącznik dostępowy dla użytkowników 24 portowych (typ 2)
4. IDF L3 – 1 piętro LSP (pom. 2.10.01):
    a. Przełącznik dostępowy dla użytkowników 24 portowych (typ 2)
    b. Przełącznik dostępowy dla użytkowników 24 portowych (typ 1)
5. MDF G – Terminal GA (pom. techniczne)
    a. Switch rdzeniowy – 1szt
    b. Firewall Next Generation i IDS/IPS
    c. Kontroler sieci bezprzewodowej WLAN
    d. Serwer BDC
    e. Serwer wirtualizacyjny dla Aplikacji zarządzającej, NAC, Korelacji zdarzeń
6. IDF G1 – Terminal GA (pom. TE-12):
    a. Przełącznik dostępowy dla użytkowników 48 portowych (typ 1) – 2 szt.
    b. Przełącznik dostępowy dla użytkowników 48 portowych (typ 2)
7. IDF G2 – Terminal GA (zaplecze pom. GA-09):
    a. Przełącznik dostępowy dla użytkowników 24 portowych (typ 2)

Lokalizacja pozostałych drobnych elementów zgodnie z wytycznymi Inwestora w trakcie realizacji zadania.

Budowana sieć musi zapewnić bezawaryjną obsługę użytkowników i systemów w budynkach Lotniskowej Straży Pożarnej (LSP) i budynku Terminala GA (GA):

- Systemu telefonii VoIP
- Systemu FIS

- Systemów Handlingowych (check-in)
- Pracowników biurowych PLGK
- Najemców (z możliwością określania parametrów łącza dostępowego do Internetu)

Połączenia pomiędzy budynkami realizowane będą za pomocą łączy światłowodowych jednomodowych (SM) i wewnątrz budynków za pomocą łączy światłowodowych wielomodowych (MM).

Połączenie pomiędzy switchami rdzeniowymi należy wykonać za pomocą łączy minimum 2x10GE.

Switche rdzeniowe podłączone zostaną do Internetu poprzez Firewall-e.

Firewall-e zostaną podłączone do Internetu, przez Routery/modemy operatora zlokalizowane w pomieszczeniu przyłączy. Połączenia z MDF-ów do Pomieszczenia przyłączy wykonane zostaną za pomocą jednomodowych łączy światłowodowych.

Serwery zarządzające, PDC, BDC i system bezpieczeństwa zostaną podłączone do switchy rdzeniowych.

Wszystkie switch-e dostępowe podłączone są do obu przełączników rdzeniowych w technologii 1Gb.

W trakcie normalnej pracy wszystkie połączenia pomiędzy switchami są aktywne.

Centrala telefoniczna zostanie podłączona do sieci LAN PLGK w MDF L. Porty centrali wewnętrzne i miejskie należy zakończyć na 50xRJ45 panelach telefonicznych 3 kat.

Centrala telefoniczna powinna dostarczyć otrzymane fax-y do dedykowanej skrzynki pocztowej na serwerze Exchange.

Terminale abonenckie (poza terminalami VoIP) zostaną podłączone do centrali poprzez sieć okablowania strukturalnego (wykonanego w ramach innych zadań)

Terminale VoIP zostaną podłączone do centrali telefonicznej w następujący sposób:

- Poprzez siec VLAN – terminale mobilne
- Poprzez switch-e dostępowe typu 1

W ramach dostawy, należy dostarczyć wszystkie kable przyłączeniowe dla połączeń pomiędzy urządzeniami aktywnymi, jak i dla podłączeń aparatów telefonicznych do centrali.

Switch-e rdzeniowe, firewall-e, kontrolery i serwery muszą zostać wyposażone w dodatkowe zasilacze „Hot-Swap”, pozwalające na wymianę bez konieczności wyłączenia urządzenia. Dodatkowo urządzenia, muszą zostać skonfigurowane w trybie Failover, w taki sposób, aby wykluczyć tzw. Punkt Pojedynczej Awarii.

Wszystkie systemy zarządzające należy zainstalować i skonfigurować zgodnie z zasadą „dobrej praktyki inżynierskiej” i zaleceniami producentów.

Inwestor wymaga nieodpłatnego zapewnienia aktualizacji reguł bezpieczeństwa, baz wirusów i innego oprogramowania wykorzystywanego do realizacji zadania na okres 36 m-cy.

Należy połączyć wyniesioną końcówkę sieci AFTN Gdańsk Rębiechowo z wydzielonym VLAN-em AFTN w budowanej sieci LAN.

Inwestor wymaga implementacji poniższych polityk bezpieczeństwa:

- Separacja podsieci najemców od siebie, dostęp tylko do Internetu
- Wydzielenie VLAN-u dla połączeń VoIP
- Przed uzyskaniem dostępu do sieci komputery próbujące uzyskać do niej dostęp zostaną umieszczone w odseparowanych segmentach sieci nazywanych kwarantanną.(wdrożone dla pracowników Inwestora, nie obejmuje pasażerów i najemców)
- Przypisanie komputerów Inwestora do VLAN-u – Users_x, po uprzedniej weryfikacji
- Dostęp gościnny do sieci bezprzewodowej i Internetu
- Szyfrowanego dostępu z zewnątrz sieci do sieci wewnętrznej poprzez Internet (VPN, IPSec)
- VLAN AFTN, nie ma połączenia z innymi VLAN-ami. Wymaga kontroli podłączenia innych niż zdefiniowane urządzenia, każde nieautoryzowane podłączenie jest blokowane

Systemy FIS, Handligowe i sieci najemców zostaną podłączone poprzez dedykowane VLAN-y zdefiniowane na switch-ach dostępowych.

Inwestor wymaga podziału sieci na VLAN-y, zgodnie z poniższą tabelą:

Nazwa VLAN-u	Numer VLAN-u	Opis
Users_x	101-199	Użytkownicy, zakłada się zastosowanie osobnego vlanu per punkt dystrybucyjny
Servers_x	201-299	Serwery
Management	301-399	Adresy zarządzające urządzeń aktywnych
FIS/Handling/AFTN	401-499	Systemy FIS, Handling, AFTN, inne
NAJM_[nazwa firmy]	501-599	Najemcy powierzchni handlowych, zakłada się zastosowanie osobnego vlanu per firmę

1.5 Ogólne wymagania dotyczące prac montażowych

Wykonawca robót jest odpowiedzialny za jakość ich wykonania oraz, za ich zgodność ze Specyfikacją Techniczną i poleceniami Inspektora Nadzoru.

1.5.1 Przekazanie terenu

Zamawiający, w terminie określonym w dokumentach umowy, przekaże Wykonawcy teren budowy wraz ze wszystkimi wymaganymi uzgodnieniami prawnymi i administracyjnymi, poda lokalizację obiektu, dwa egzemplarze Specyfikacji Technicznej.

1.5.2 Zgodność robót ze Specyfikacją Techniczną

Specyfikacja Techniczna, oraz dodatkowe dokumenty przekazane Wykonawcy przez Inspektora nadzoru stanowią załączniki do umowy, a wymagania wyszczególnione w choćby jednym z nich są obowiązujące dla Wykonawcy tak jakby zawarte były w całej dokumentacji. W przypadku rozbieżności w ustaleniach poszczególnych dokumentów decyzje, co do wyboru toku postępowania podejmuje Inspektor nadzoru. Wykonawca nie może wykorzystywać błędów lub niedoborów w dokumentacji, a o ich wykryciu winien natychmiast powiadomić Inspektora nadzoru, który dokona odpowiednich zmian i poprawek. W przypadku stwierdzenia ewentualnych rozbieżności podane na rysunku wielkości liczbowe wymiarów są ważniejsze od odczytu ze skali rysunków. Wszystkie wykonane roboty i dostarczone materiały mają być zgodne ze Specyfikacją Techniczną. Wielkości określone w dokumentacji projektowej i w ST będą uważane za wartości docelowe, od których dopuszczalne są odchylenia w ramach określonego przedziału tolerancji.

Cechy materiałów i elementów budowli muszą być jednorodne i wykazywać zgodność z określonymi wymaganiami, a rozrzuty tych cech nie mogą przekraczać dopuszczalnego przedziału tolerancji. W przypadku, gdy dostarczone materiały lub Wykonane roboty nie będą zgodne ze ST i mają wpływ na niezadowalającą, jakość elementu budowli, to takie materiały zostaną zastąpione innymi, a elementy budowli rozebrane i wykonane ponownie na koszt wykonawcy.

1.5.3 Zabezpieczenia terenu prac montażowych

Wykonawca jest zobowiązany do zabezpieczenia terenu prac w okresie trwania realizacji kontraktu aż do zakończenia i odbioru ostatecznego robót. Wykonawca dostarczy, zainstaluje i będzie utrzymywać tymczasowe urządzenia zabezpieczając, w tym: ogrodzenia, poręcze, oświetlenia, sygnały i znaki ostrzegawcze, dozorców; wszelkie inne niezbędne do ochrony robót.

1.5.4 Ochrona środowiska w czasie wykonania robót

Wykonawca ma obowiązek znać i stosować w czasie prowadzenia prac montażowych wszelkie przepisy dotyczące ochrony środowiska naturalnego. W okresie trwania prac montażowych i wykonywania robót wykończeniowych Wykonawca będzie:

a) utrzymywać teren prac montażowych w stanie bez wody stojącej

b) podejmować wszelkie konieczne kroki mające na celu stosowanie się do przepisów i norm dotyczących ochrony środowiska na terenie i wokół terenu prac montażowych oraz będzie unikać uszkodzeń lub uciążliwości dla osób lub własności społecznej, a wynikających ze skażenia, hałasu lub innych przyczyn powstałych w następstwie jego sposobu działania.

Stosując się do tych wymagań. Wykonawca będzie miał szczególny wzgląd na:

1. lokalizację baz, warsztatów; magazynów, składowisk, ukopów i dróg dojazdowych,
2. środki ostrożności i zabezpieczenia przed:
   - zanieczyszczeniem zbiorników i cieków wodnych pyłami lub substancjami toksycznymi,
   - zanieczyszczeniem powietrza pyłami i gazami.
   - możliwością powstania pożaru.

1.5.5 Ochrona przeciwpożarowa

Wykonawca będzie przestrzegać przepisy ochrony przeciwpożarowej. Wykonawca będzie utrzymywać sprawny sprzęt przeciwpożarowy, wymagany odpowiednimi przepisami, na terenie baz produkcyjnych, w pomieszczeniach biurowych, mieszkalnych i magazynowych oraz w maszynach i pojazdach. Materiały łatwopalne będą składowane w sposób zgodny z. odpowiednimi przepisami i zabezpieczone przed dostępem osób trzecich. Wykonawca będzie odpowiedzialny za wszelkie straty spowodowane pożarem wywołanym, jako rezultat realizacji robót albo przez personel wykonawcy.

1.5.6 Ochrona własności publicznej i prywatnej

Wykonawca odpowiada za ochronę instalacji i urządzeń zlokalizowanych na powierzchni terenu i pod jego poziomem, takie jak rurociągi, kable itp. Wykonawca zapewni właściwe oznaczenie i zabezpieczenie przed uszkodzeniem tych instalacji i urządzeń w czasie trwania budowy. O fakcie przypadkowego uszkodzenia tych instalacji Wykonawca bezzwłocznie powiadomi Inspektora nadzoru i zainteresowanych użytkowników oraz będzie z nimi współpracował, dostarczając wszelkiej pomocy potrzebnej przy dokonywaniu napraw. Wykonawca będzie odpowiadał za wszelkie spowodowane przez jego działania uszkodzenia instalacji na powierzchni ziemi i urządzeń podziemnych, wykazanych w dokumentach dostarczonych przez Zamawiającego.

1.5.7 Bezpieczeństwo i higiena pracy

Podczas realizacji robót wykonawca będzie przestrzegać przepisów dotyczących bezpieczeństwa i higieny pracy. W szczególności wykonawca ma obowiązek zadbać, aby personel nie wykonywał pracy w warunkach niebezpiecznych, szkodliwych dla zdrowia oraz niespełniających odpowiednich wymagań sanitarnych. Wykonawca zapewni i będzie utrzymywał wszelkie urządzenia zabezpieczające, socjalne oraz sprzęt i odpowiednią odzież dla ochrony życia i zdrowia osób zatrudnionych na obiekcie. Uznaje się , że wszelkie koszty związane z wypełnieniem wymagań określonych powyżej nie podlegają odrębnej zapłacie i są uwzględnione w cenie umownej.

1.5.8 Ochrona i utrzymanie robót

Wykonawca będzie odpowiedzialny za ochronę prac montażowych i za wszelkie materiały i urządzenia używane do robót od daty rozpoczęcia do daty odbioru ostatecznego.

1.5.9 Stosowanie się do prawa i innych przepisów

Wykonawca zobowiązany jest znać wszelkie przepisy wydane przez organy administracji państwowej i samorządowej, które są w jakikolwiek sposób związane z pracami montażowymi i będzie w pełni odpowiedzialny za przestrzeganie tych praw, przepisów i wytycznych podczas prowadzenia prac.

Wykonawca będzie przestrzegał praw patentowych i będzie w pełni odpowiedzialny za wypełnienie wszelkich wymagań prawnych odnośnie wykorzystania opatentowanych urządzeń lub metod i w sposób ciągły będzie informować Inspektora nadzoru o swoich działaniach, przedstawiając kopie zezwoleń i inne odnośne dokumenty

2 Materiały

Wszelkie nazwy własne produktów i materiałów przywołane w specyfikacji służą ustaleniu pożądanego standardu wykonania i określenia właściwości i wymogów technicznych.

2.1 Ogólne wymagania dotyczące właściwości materiałów

Do wykonania i montażu instalacji, urządzeń elektrycznych i odbiorników energii elektrycznej w obiektach budowlanych należy stosować przewody, kable, osprzęt oraz aparaturę i urządzenia elektryczne posiadające dopuszczenie do stosowania w budownictwie.

Za dopuszczone do obrotu i stosowania uznaje się wyroby, dla których producent lub jego upoważniony przedstawiciel:

- Dokonał oceny zgodności z wymaganiami dokumentu odniesienia według określonego systemu oceny zgodności,
- Wydał deklarację zgodności z dokumentami odniesienia, takimi jak: zharmonizowane specyfikacje techniczne, normy opracowane przez Międzynarodową Komisję Elektrotechniczną(IEC) i wprowadzone do zbioru Polskich Norm, normy krajowe opracowane z uwzględnieniem przepisów bezpieczeństwa Międzynarodowej Komisji ds. Przepisów Dotyczących Zatwierdzenia Sprzętu Elektrycznego (CEE), aprobaty techniczne,
- Oznakował wyroby znakiem CE lub znakiem budowlanym B zgodnie z obowiązującymi przepisami,
- Wydał deklarację zgodności z uznanymi regułami sztuki budowlanej, dla wyrobu umieszczonego w określonym przez Komisję Europejską wykazie wyrobów mających niewielkie znaczenie dla zdrowia i bezpieczeństwa,
- Wydał oświadczenie, że zapewniono zgodność wyrobu budowlanego, dopuszczonego do jednostkowego zastosowania w obiekcie budowlanym, z indywidualną dokumentacją projektową, sporządzoną przez projektanta obiektu lub z nim uzgodnioną.

Zastosowanie innych wyrobów, wyżej nie wymienionych, jest możliwe pod warunkiem posiadania przez nie dopuszczenia do stosowania w budownictwie i uwzględnienia ich w zatwierdzonym projekcie dotyczącym montażu urządzeń elektroenergetycznych w obiekcie budowlanym.

2.2 Zastosowane urządzenia

2.2.1 Przełącznik rdzeniowy (2 szt.)

Każdy z przełączników powinien charakteryzować się następującymi wymaganiami minimalnymi:

- Przełącznik modularny pozwalający na instalację do min. 64 portów 10Gb SFP+, z czego minimum 32 porty 10Gb muszą pracować z pełną prędkością lub do min. 288 portów Gigabit Ethernet 10/100/1000BASE-T lub światłowodowych wykorzystujących interfejsy typu SFP lub równoważne.
- Przełącznik musi być wyposażony w 48 portów 10/100/1000 1G RJ45, 12 portów 1G SFP oraz minimum 12 portów 10G SFP+.
- Każdy slot musi być podłączony do matrycy przełączającej/routującej szyną o przepustowości, co najmniej 160Gb. Maksymalne obłożenie modułami musi umożliwiać osiągniecie wydajności na minimalnym poziomie 640Gb oraz 480Mpps.
- Dostarczony przełącznik musi posiadać redundantne moduły zarządzające lub moduły zarządzająco-przełączające.W przypadku połączenia tych funkcji w moduły te muszą działać w równocześnie (Active – Active).
- Redundancja zasilania N+1.
- Wszystkie moduły muszą zapewniać możliwość wymiany w czasie pracy urządzania. Dotyczy to zasilania, kart liniowych, fabric, zarządzających oraz modułów przełączających, wentylatorów oraz wszelkich modułów dedykowanych
- Przełącznik powinien zapewniać możliwość rozbudowy o dodatkowe porty. Wymagane jest zapewnienie rozbudowy minimum 144 portów 1G SFP lub 32 porty 10G.
- Każdy moduł liniowy musi posiadać przynajmniej 1GB bufora pakietów.
- Pojemność tabeli MAC adresów min. 60 tys. wpisów.
- Wsparcie dla min. 4000 działających sieci wirtualnych (VLANs) jednocześnie, wsparcie dla GVRP lub równoważne.
- Możliwość klasyfikacji pakietów w L2-L4 według:
- źródłowego adresu MAC,
- docelowego adresu MAC,
- źródłowego adresu IP,
- docelowego adresu IP,
- UDP/TCP źródłowy port,
- UDP/TCP docelowy port,
- IP TOS,
- IP typ,
- IP Fragmentacja – klasyfikacja.
- Obsługa minimum 8 kolejek priorytetów na każdym porcie realizowana sprzętowo.
- Obsługa priorytetów zgodna z IEEE 802.1p.
- Obsługa Link Aggregation IEEE 802.3ad, co najmniej 127 grup.
- Musi obsługiwać SNMPv3, RFC 3826 – AES dla SNMP.
- Musi obsługiwać wiele mechanizmów kolejkowania (SPQ, WFQ, WRR, Hybrid).
- Musi obsługiwać kontrolę poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego.
- Musi obsługiwać opcje Port/VLAN mirroring (jeden do jednego, jeden do wielu, wielu do wielu).
- Musi obsługiwać następujące metody uwierzytelniania:

- IEEE 802.1X Port Based Access Network,
- MAC Autoryzacja,
- RADIUS Snooping,
- Port-Based Web Authentication,
- Musi wspierać profile bezpieczeństwa, profil bezpieczeństwa oznacza połączenie:
    - definicji sieci VLAN,
    - w warstwach L2-L4 reguły filtrowania zarówno IPv4 jak i IPv6,
    - w warstwach L2-L4 zasady jakości usług do obsługi IPv4 i IPv6,
    - w warstwach L2-L4 zasad dublowania operacji dla ruchu w IPv4 i IPv6,
    - w warstwach L2-L4 z zasady ograniczenia prędkości dla ruchu w IPv4 jak i Ipv6.
    - Musi obsługiwać co najmniej 1000 unikatowych profili bezpieczeństwa.
    - Dwa urządzenia rdzeniowe musza zachowywać się, jako jedno logiczne urządzenie we wszystkich kwestiach przełączania i routingu (wszystkie protokoły i mechanizmy w warstwie L2 i L3).
- Obsługiwać możliwość zastosowania profilu bezpieczeństwa:
    - statycznie dla portu,
    - statycznie dla adresów MAC,
    - statycznie dla adresów IP,
    - statycznie dla VLAN-ów,
    - dynamicznie zgodnie z uwierzytelnieniem przez RADIUS.
    - Musi umożliwiać wdrożenie profilu domyślnego do czasu dokonania poprawnej autentykacji i przydzielenia profilu docelowego.
- Funkcjonalności umożliwiające integrację z innymi systemami:
    - Musi obsługiwać zdolność do identyfikacji i autoryzacji telefonii VoIP i innych tego typu systemów oraz dla urządzeń różnych producentów - H.323, SIP, CDPv2, LLDP-MED lub równoważne.
    - Musi obsługiwać LLDP i LLDP-MED, CDP,
    - Musi umożliwiać przypisanie ruchu do różnych sieci VLAN zgodnie z L2-L4 kryteriów, nawet, jeśli nie jest skonfigurowany protokół 802.1Q tagging,
    - Musi obsługiwać technologię RADIUS Accounting.
    - Musi obsługiwać technologię TACACS+.
    - Sprzętowa obsługa nie samplowanego NetFlowm na każdym porcie bez straty wydajności urządzenia lub równoważne, ale nie samplowane i bez strat wydajności urządzenia.
    - Sprzętowa obsługa routingu IPv4 i IPv6.
    - Musi obsługiwać funkcje routingu, w tym: trasy statyczne, BGP, OSPF v1/v2/v3, RIPv2, IPv4, routing Multicast (IGMP v1/v2/v3, PIM-SM), Policy Based Routing, Route Maps, VRRP, VRF (Virtual Routing and Forwarding).
    - NAT realizowany sprzętowo.
    - Obsługa zewnętrznego systemu logowania zdarzeń SYSLOG, RMON (9 grup), SMON.
    - Obsługa synchronizacji czasu w oparciu o zewnętrzny serwer SNTP lub NTP.
    - Obsługa SSHv2 serwer i klient, Telnet, TFTP.
- Wraz z przełącznikami należy dostarczyć następujące moduły:

- 10GBASE-LR, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 Km, LC SFP+
- 10GBASE-LRM, IEEE 802.3 MM, 1310 nm Long Wave Length, 220 M, LC SFP+
- 8 x 1000Base-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550 M, LC SFP
- 8 x 1000Base-LX, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 Km, LC SFP

2.2.2 Przełącznik dostępowy dla użytkowników 48 portów (typ 1)

- Powinien posiadać 48 portów 10/100/1000 PoE 802.3at oraz 4 porty 1GbE SFP oraz 2 porty umożliwiające łączenie w stos (wieżę).
- Powinna być zapewniona moc do 375W dla PoE.
- Musi zapewniać przełączanie z pełną prędkością łącza w obie strony, wydajność szyny stakującej minimum 48Gbps.
- Musi obsługiwać IP Multicast
- Musi obsługiwać COS Inbound Rate Limiting
- Musi obsługiwać 802.1p Traffic Classification
- Musi posiadać możliwości klasyfikowania pakietów warstw 2/3/4, które mogą opierać się na ID portu fizycznego, adresie MAC, podsieci IP, adresie IP, typie protokołu IP, IP ToS (Type of Service), DSCP (Differentiated Services Code Point) oraz porcie TCP/UDP.
- Musi obsługiwać IP ToS Rewrite
- Musi obsługiwać Weighted Round Robin i Strict Priority Queuing
- Musi obsługiwać do 8 priorytetowych kolejek na port
- Musi obsługiwać IEEE 802.3ad Link Aggregation
- Musi zapewniać dystrybucję zagregowanych linków pomiędzy wieloma przełącznikami w obrębie stosu
- Musi umożliwiać tworzenie stosów w formie zamkniętej pętli.
- Musi zapewniać redundantne zarządzanie stosem.
- Musi umożliwiać zarządzanie stosem przy wykorzystaniu jednego adresu IP.
- Musi posiadać redundantne źródło zasilania.
- Musi obsługiwać uwierzytelnianie użytkownika poprzez IEEE 802.1x
- Musi obsługiwać uwierzytelnianie wykorzystujące adres MAC
- Musi obsługiwać uwierzytelnianie wykorzystujące przeglądarkę internetową
- Musi umożliwiać uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla maksymalnie 4 użytkowników/urządzeń na port.
- Musi obsługiwać MAC Port Locking (dynamiczne i statyczne)
- Musi obsługiwać Dynamic VLAN Assignment (RFC 3580)
- Musi obsługiwać wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (do 4)
- 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. Musi zapewniać bezpieczne zarządzanie przy wykorzystaniu: SSH, SSL, SNMPv3, RADIUS oraz TACACS+. Obsługa TACACS+ musi zapewniać wsparcie dla procesów uwierzytelniania, autoryzacji i audytowania.
- Musi obsługiwać opcje Secure Copy oraz Secure FTP
- Musi zapewniać ochronę przed atakami typu DHCP/ARP spoofing/snooping.

- Musi zapewnić monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP.
- Musi obsługiwać następujące grupy RMON: Statistics, History, Alarms, Events, Packet Capture/Filtering Sampling
- Musi obsługiwać sFlow lub równoważne
- Musi obsługiwać Port Mirroring
- Musi obsługiwać dynamiczne i statyczne polityki na danym porcie
- Musi obsługiwać IEEE 802.1s Multiple Spanning Tree
- Musi obsługiwać IEEE 802.1w Rapid Reconfiguration of Spanning Tree
- Musi obsługiwać IGMP Snooping (v1, v2, v3)
- Musi obsługiwać do 4,096 ID sieci VLAN oraz do 1,024 VLAN aktywnych jednocześnie w pojedynczym stosie
- Pojemność tablicy MAC minimum 30000 adresów
- Musi obsługiwać sieci VLAN IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP
- Musi obsługiwać LLDP / LLDP-MED Network-Policy TLV
- Musi obsługiwać Jumbo Ethernet Frames
- Musi zapewniać prosty routing IP bez stosowania dodatkowej licencji (trasy statyczne oraz RIP v1/v2)
- Musi umożliwiać wykrywanie lokalizacji systemów końcowych w czasie rzeczywistym i przechowywanie tych informacji w centralnej bazie danych
- Musi działać w temperaturze otoczenia do 50°C
- Należy dostarczyć niezbędne kable do łączenia w stos.

2.2.3 Przełącznik dostępowy dla użytkowników 48 portów (typ 2)

- Powinien posiadać 48 portów 10/100/1000 oraz 4 porty 1GbE SFP oraz 2 porty umożliwiające łączenie w stos (wieżę).
- Musi zapewniać przełączanie z pełną prędkością łącza w obie strony, wydajność szyny stakującej minimum 48Gbps.
- Musi obsługiwać IP Multicast
- Musi obsługiwać COS Inbound Rate Limiting per Policy User
- Musi obsługiwać 802.1p Traffic Classification
- Musi posiadać możliwości klasyfikowania pakietów warstw 2/3/4, które mogą opierać się na ID portu fizycznego, adresie MAC, podsieci IP, adresie IP, typie protokołu IP, IP ToS (Type of Service), DSCP (Differentiated Services Code Point) oraz porcie TCP/UDP.
- Musi obsługiwać IP ToS Rewrite
- Musi obsługiwać Weighted Round Robin i Strict Priority Queuing
- Musi obsługiwać do 8 priorytetowych kolejek na port
- Musi obsługiwać IEEE 802.3ad Link Aggregation
- Musi zapewniać dystrybucję zagregowanych linków pomiędzy wieloma przełącznikami w obrębie stosu
- Musi umożliwiać tworzenie stosów w formie zamkniętej pętli.
- Musi zapewniać redundantne zarządzanie stosem.
- Musi umożliwiać zarządzanie stosem przy wykorzystaniu jednego adresu IP.

- Musi posiadać redundantne źródło zasilania.
- Musi obsługiwać uwierzytelnianie użytkownika poprzez IEEE 802.1x
- Musi obsługiwać uwierzytelnianie wykorzystujące adres MAC
- Musi obsługiwać uwierzytelnianie wykorzystujące przeglądarkę internetową
- Musi umożliwiać uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla maksymalnie 4 użytkowników/urządzeń na port.
- Musi obsługiwać MAC Port Locking (dynamiczne i statyczne)
- Musi obsługiwać Dynamic VLAN Assignment (RFC 3580)
- Musi obsługiwać wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (do 4)
- 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.
- Musi zapewniać bezpieczne zarządzanie przy wykorzystaniu: SSH, SSL, SNMPv3, RADIUS oraz TACACS+. Obsługa TACACS+ musi zapewniać wsparcie dla procesów uwierzytelniania, autoryzacji i audytowania.
- Musi obsługiwać opcje Secure Copy oraz Secure FTP
- Musi zapewniać ochronę przed atakami typu DHCP/ARP spoofing/snooping.
- Musi dostarczać ostrzeżenia o wysokiej temperaturze przez komunikaty SNMP traps oraz zdarzenia syslog.
- Musi zapewnić monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP.
- Musi obsługiwać następujące grupy RMON: Statistics, History, Alarms, Events, Packet Capture/Filtering Sampling
- Musi obsługiwać sFlow lub równoważne.
- Musi obsługiwać Port Mirroring
- Musi obsługiwać dynamiczne i statyczne polityki na danym porcie
- Musi obsługiwać IEEE 802.1s Multiple Spanning Tree
- Musi obsługiwać IEEE 802.1w Rapid Reconfiguration of Spanning Tree
- Musi obsługiwać IGMP Snooping (v1, v2, v3)
- Musi obsługiwać do 4,096 ID sieci VLAN oraz do 1,024 VLAN aktywnych jednocześnie w pojedynczym stosie
- Pojemność tablicy MAC minimum 30000 adresów
- Musi obsługiwać sieci VLAN IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP
- Musi obsługiwać LLDP / LLDP-MED Network-Policy TLV
- Musi obsługiwać Jumbo Ethernet Frames
- Musi zapewniać prosty routing IP(trasy statyczne oraz RIP v1/v2)
- Musi umożliwiać wykrywanie lokalizacji systemów końcowych w czasie rzeczywistym i przechowywanie tych informacji w centralnej bazie danych
- Musi działać w temperaturze otoczenia do 50°C
- Należy dostarczyć niezbędne kable do łączenia w stos.

2.2.4 Przełącznik dostępowy dla użytkowników 24 portów (typ 1)

- Powinien posiadać 24 portów 10/100/1000 PoE 802.3at oraz 4 porty 1GbE SFP oraz 2 porty umożliwiające łączenie w stos (wieżę).
- Powinna być zapewniona moc do 375W dla PoE.
- Musi zapewniać przełączanie z pełną prędkością łącza w obie strony, wydajność szyny stakującej minimum 48Gbps.
- Musi obsługiwać IP Multicast
- Musi obsługiwać COS Inbound Rate Limiting
- Musi obsługiwać 802.1p Traffic Classification
- Musi posiadać możliwości klasyfikowania pakietów warstw 2/3/4, które mogą opierać się na ID portu fizycznego, adresie MAC, podsieci IP, adresie IP, typie protokołu IP, IP ToS (Type of Service), DSCP (Differentiated Services Code Point) oraz porcie TCP/UDP.
- Musi obsługiwać IP ToS Rewrite
- Musi obsługiwać Weighted Round Robin i Strict Priority Queuing
- Musi obsługiwać do 8 priorytetowych kolejek na port
- Musi obsługiwać IEEE 802.3ad Link Aggregation
- Musi zapewniać dystrybucję zagregowanych linków pomiędzy wieloma przełącznikami w obrębie stosu
- Musi umożliwiać tworzenie stosów w formie zamkniętej pętli.
- Musi zapewniać redundantne zarządzanie stosem.
- Musi umożliwiać zarządzanie stosem przy wykorzystaniu jednego adresu IP.
- Musi posiadać redundantne źródło zasilania.
- Musi obsługiwać uwierzytelnianie użytkownika poprzez IEEE 802.1x
- Musi obsługiwać uwierzytelnianie wykorzystujące adres MAC
- Musi obsługiwać uwierzytelnianie wykorzystujące przeglądarkę internetową
- Musi umożliwiać uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla maksymalnie 4 użytkowników/urządzeń na port.
- Musi obsługiwać MAC Port Locking (dynamiczne i statyczne)
- Musi obsługiwać Dynamic VLAN Assignment (RFC 3580)
- Musi obsługiwać wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (do 4)
- 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.
- Musi zapewniać bezpieczne zarządzanie przy wykorzystaniu: SSH, SSL, SNMPv3, RADIUS oraz TACACS+. Obsługa TACACS+ musi zapewniać wsparcie dla procesów uwierzytelniania, autoryzacji i audytowania.
- Musi obsługiwać opcje Secure Copy oraz Secure FTP
- Musi dostarczać ostrzeżenia o wysokiej temperaturze przez komunikaty SNMP traps oraz zdarzenia syslog.
- Musi zapewnić monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP.

- Musi obsługiwać następujące grupy RMON: Statistics, History, Alarms, Events, Packet Capture/Filtering Sampling
- Musi obsługiwać sFlow lub równoważne
- Musi obsługiwać Port Mirroring
- Musi obsługiwać dynamiczne i statyczne polityki na danym porcie
- Musi obsługiwać IEEE 802.1s Multiple Spanning Tree
- Musi obsługiwać IGMP Snooping (v1, v2, v3)
- Musi obsługiwać do 4,096 ID sieci VLAN oraz do 1,024 VLAN aktywnych jednocześnie w pojedynczym stosie
- Pojemność tablicy MAC minimum 30000 adresów
- Musi obsługiwać sieci VLAN IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP lub równoważne.
- Musi obsługiwać LLDP / LLDP-MED Network-Policy TLV
- Musi obsługiwać Jumbo Ethernet Frames
- Musi zapewniać prosty routing IP (trasy statyczne oraz RIP v1/v2)
- Musi umożliwiać wykrywanie lokalizacji systemów końcowych w czasie rzeczywistym i przechowywanie tych informacji w centralnej bazie danych
- Musi działać w temperaturze otoczenia do 50°C
- Należy dostarczyć niezbędne kable do łączenia w stos.

2.2.5 Przełącznik dostępowy dla użytkowników 24 portów (typ 2)

- Powinien posiadać 24 portów 10/100/1000 oraz 4 porty 1GbE SFP oraz 2 porty umożliwiające łączenie w stos (wieżę).
- Musi zapewniać przełączanie z pełną prędkością łącza w obie strony, wydajność szyny stakującej minimum 48Gbps.
- Musi obsługiwać IP Multicast
- Musi obsługiwać COS Inbound Rate Limiting
- Musi obsługiwać 802.1p Traffic Classification
- Musi posiadać możliwości klasyfikowania pakietów warstw 2/3/4, które mogą opierać się na ID portu fizycznego, adresie MAC, podsieci IP, adresie IP, typie protokołu IP, IP ToS (Type of Service), DSCP (Differentiated Services Code Point) oraz porcie TCP/UDP.
- Musi obsługiwać IP ToS Rewrite
- Musi obsługiwać Weighted Round Robin i Strict Priority Queuing
- Musi obsługiwać do 8 priorytetowych kolejek na port
- Musi obsługiwać IEEE 802.3ad Link Aggregation
- Musi zapewniać dystrybucję zagregowanych linków pomiędzy wieloma przełącznikami w obrębie stosu
- Musi umożliwiać tworzenie stosów w formie zamkniętej pętli.
- Musi zapewniać redundantne zarządzanie stosem.
- Musi umożliwiać zarządzanie stosem przy wykorzystaniu jednego adresu IP.
- Musi posiadać redundantne źródło zasilania.
- Musi obsługiwać uwierzytelnianie użytkownika poprzez IEEE 802.1x

- Musi obsługiwać uwierzytelnianie wykorzystujące adres MAC
- Musi obsługiwać uwierzytelnianie wykorzystujące przeglądarkę internetową
- Musi umożliwiać uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla maksymalnie 4 użytkowników/urządzeń na port.
- Musi obsługiwać MAC Port Locking (dynamiczne i statyczne)
- Musi obsługiwać Dynamic VLAN Assignment (RFC 3580)
- Musi obsługiwać wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (do 4)
- 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.
- Musi zapewniać bezpieczne zarządzanie przy wykorzystaniu: SSH, SSL, SNMPv3, RADIUS oraz TACACS+. Obsługa TACACS+ musi zapewniać wsparcie dla procesów uwierzytelniania, autoryzacji i audytowania.
- Musi obsługiwać opcje Secure Copy oraz Secure FTP
- Musi zapewniać ochronę przed atakami typu DHCP/ARP spoofing/snooping.
- Musi dostarczać ostrzeżenia o wysokiej temperaturze przez komunikaty SNMP traps oraz zdarzenia syslog.
- Musi zapewnić monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP.
- Musi obsługiwać następujące grupy RMON: Statistics, History, Alarms, Events, Packet Capture/Filtering Sampling
- Musi obsługiwać sFlow lub równoważne.
- Musi obsługiwać Port Mirroring
- Musi obsługiwać dynamiczne i statyczne polityki na danym porcie
- Musi obsługiwać IEEE 802.1s Multiple Spanning Tree
- Musi obsługiwać IGMP Snooping (v1, v2, v3)
- Musi obsługiwać do 4,096 ID sieci VLAN oraz do 1,024 VLAN aktywnych jednocześnie w pojedynczym stosie
- Pojemność tablicy MAC minimum 30000 adresów
- Musi obsługiwać sieci VLAN IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP
- Musi obsługiwać LLDP / LLDP-MED Network-Policy TLV
- Musi obsługiwać Jumbo Ethernet Frames
- Musi zapewniać prosty routing IP (trasy statyczne oraz RIP v1/v2)
- Musi umożliwiać wykrywanie lokalizacji systemów końcowych w czasie rzeczywistym i przechowywanie tych informacji w centralnej bazie danych
- Musi działać w temperaturze otoczenia do 50°C
- Należy dostarczyć niezbędne kable do łączenia w stos.

2.2.6 Aplikacja zarządzająca

- Aplikacja musi umożliwiać zarządzanie do minimum 25 urządzeń sieciowych oraz minimum 250 punktów dostępowych jak i umożliwiać przyszłą rozbudowę do minimum 100 urządzeń sieciowych oraz minimum 500 punktów dostępowych.

- Musi zapewniać scentralizowane zarządzanie urządzeniami sieci przewodowej i bezprzewodowej.
- Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji.
- 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 zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci po przez zadane kryteria: IP/MAC/User Name, Multicast address
- 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 z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB.
- 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.
- Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji.
- Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https.
- Powinno oferować możliwość instalacji na urządzeniu wirtualnym.
- Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na proponowanych urządzeniach sieci przewodowej i bezprzewodowej.
- Musi mieć możliwość definiowania polityk ograniczających poziom pasma, ograniczających liczbę nowych połączeń sieciowych, ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3, nadających tagi pakietom, izolujących/poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania.
- Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednego kliknięcia.
- Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci.
- Musi zapewniać łatwość wdrożenia, administracji oraz rozwiązywania problemów.
- Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).
- Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania.
- Musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC.
- Musi pozwalać administratorom IT na proste definiowanie liczby wcześniej skonfigurowanych polityk sieciowych oraz desygnowanie wybranego personelu do aktywowania/dezaktywowania tych polityk w razie potrzeby.
- Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p.

- Musi być łatwa do konfiguracji i wdrożenia, zapewniając uproszczoną, działającą w sieci Web aplikację zarządzania.
- Nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent.
- Musi dostarczyć szczegółowy wykaz produktów, zorganizowany według typu urządzenia.
- Musi umożliwiać śledzenie atrybutów urządzeń, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć.
- Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania firmware i wielkość pliku.
- 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 zapewniać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania spisem urządzeń.
- Musi umożliwiać generowanie wartościowych, szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych.
- 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 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/IPS/SIEM/Firewall .
- Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci.
- Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia.
- Musi nadawać „rolę kwarantanny” użytkownikowi podłączonemu do portu.
- Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji.
- Musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci.

- 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 diagnozowania problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym.
- Musi zapewniać możliwości analiz na poziomie portu.
- Musi oferować możliwość tworzenia niestandardowych raportów.

2.2.7 System korelacji informacji

- Rozwiązanie SIM musi zapewniać centralne zarządzanie wszystkimi komponentami.
- Rozwiązanie SIM musi pozwalać na tworzenie wielu użytkowników i przypisywanie każdemu użytkownikowi możliwości dostępu tylko do wybranej części monitorowanego zakresu adresów IP.
- Rozwiązanie SIM musi wspierać dostęp oparty na rolach.
- Rozwiązanie SIM musi oferować oparty na sieci web graficzny interfejs użytkownika dla potrzeb zarządzania, analiz i raportowania.
- System musi identyfikować aplikacje wykorzystujące porty nie tylko te najczęściej spotykane, oraz aplikacje tunelujące swój ruch na inne porty (np. protokół HTTP wykorzystywany jako transport przez komunikator MS Instant Messenger powinien być wykrywany jako komunikator a nie HTTP).
- Musi umożliwiać podłączanie sensorów przepływu analizujących zachowania sieci, obsługujące przepustowość do 1Gbps.
- Musi umożliwiać podłączenie wirtualnego urządzenia zbierającego przepływy, które w ramach wirtualnej infrastruktury pozwala analizować zachowania sieci i zapewnia widoczność warstwy 7.
- Musi zapewniać automatyczne aktualizowanie informacji konfiguracyjnych, przy minimalnym udziale użytkownika.
- System powinien szyfrować transmisję danych pomiędzy poszczególnymi komponentami.
- System powinien umożliwiać analizę minimum 100 zdarzeń na sekundę i minimum 15.000 przepływów na minutę oraz umożliwiać przyszłą rozbudowę do minimum 500 zdarzeń na sekundę oraz minimum 50.000 przepływów na minutę.
- Musi zapewniać zbieranie zdarzeń bezpieczeństwa i logów z wielu różnego typu urządzeń, pochodzących od różnych dostawców – minimum wyspecyfikowanych w załączonej dokumentacji.
- Musi identyfikować ruch sieciowy z wielu różnych aplikacji, pochodzących od różnych dostawców. Prosimy o załączenie listy wspieranych aplikacji i ich dostawców.
- Musi integrować dane z różnych aplikacji służących do wykrywania luk w zabezpieczeniach, przy tworzeniu profili zasobów.
- Powinno obsługiwać źródła danych takie jak: NetFlow, IPFIX, JFlow, SFlow.

- Musi umożliwiać zbieranie informacji o sieci i zabezpieczeniach bez konieczności umieszczania agentów lub innych opartych na hoście mechanizmów w istniejących klientach lub serwerach.
- Musi obsługiwać zewnętrzne mechanizmy przechowywania.
- Powinno umożliwiać przechwytywanie danych dla potrzeb analiz dochodzeniowych. Ilość przechwytywanych danych musi być konfigurowalna dla każdego przepływu.
- Musi wykrywać zdarzenia typu „zero-day". Musi obsługiwać monitorowanie i wykrywanie aplikacji dla potrzeb rozpoznawania ruchu niezgodnego z politykami, w tym aplikacji P2P i strony portali społecznościowych.
- Musi wykrywać ataki DoS (Denial-of-Service) i DDoS (Distributed Denial-of-Service).
- Musi wykrywać ruch należący do zaobserwowanych zagrożeń w sieci i prezentować jego formę.
- Musi pozwalać użytkownikowi na tworzenie własnych profili i widoków, przy wykorzystaniu dowolnej cechy przepływu, zewnętrznego źródła danych lub już sprofilowanego ruchu.
- Powinno zapewniać możliwość automatycznej oceny poziomu zagrożenia zgłoszonych zdarzeń bezpieczeństwa, zależnej od stanu zabezpieczeń zaatakowanych zasobów.
- Musi zapewniać możliwość przypisywania wskaźników wiarygodności do monitorowanych urządzeń bezpieczeństwa.
- Musi oferować funkcję powiadamiania, bazującą na zaobserwowanych zagrożeniach bezpieczeństwa, anomaliach i zmianach w zachowaniu monitorowanych urządzeń.
- Musi nadawać odpowiednią wagę powiadomieniom umożliwiając w ten sposób ich priorytetyzację. Wagi muszą być przypisywane w oparciu o wiele parametrów, takich jak typ zasobu, protokół, aplikacja, itp.
- Musi zapewniać szablony raportów dla COBIT, GLB, HIPAA, PCI i Sarbanes Oxley.
- Musi zapewniać konfigurowalny mechanizm raportowania dla potrzeb tworzenia własnych raportów.
- Musi posiadać możliwość planowania raportów.
- Musi udostępniać szablony w celu szybkiego tworzenia i dostarczania raportów obejmujących wiele zagadnień - od kwestii operacyjnych po biznesowe.
- Musi oferować panel sterowania umożliwiający szybką wizualizację informacji o sieci i zabezpieczeniach. Powinna być udostępniona możliwość stosowania wielu paneli sterowania pozwalająca użytkownikom na dowolną organizację i dostosowanie widoków do swoich potrzeb.
- Musi charakteryzować się łatwością użytkowania.
- Musi mieć możliwość wdrożenia w rozproszonym środowisku.
- Musi oferować funkcję wysokiej dostępności HA (High Availability), która zagwarantuje dostępność danych SIEM na wypadek awarii sprzętu lub sieci w formie dodatkowej licencji.
- Musi obsługiwać wszystkie systemy wymienione w specyfikacji oraz umożliwiać dodanie innych niewymienionych w specyfikacji.

2.2.8 System NAC

- Musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów
- Musi elastycznie obsługiwać wiele metod uwierzytelniania wielu użytkowników i urządzeń różnych dostawców.
- Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania I autoryzacji podłączanych systemów końcowych.
- Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych.
- Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP.
- Rozwiązanie musi posiadać wbudowany serwer RADIUS oraz serwer AAA.
- Musi współpracować z rozwiązaniem Microsoft NAP.
- Rozwiązanie musi obsługiwać lokalną autoryzację MAC.
- Musi przeprowadzać przed- i po-połączeniowe ocenianie stanu zabezpieczeń systemów końcowych.
- Powinien posiadać możliwość rozbudowy o dodatkową funkcjonalność oceniania w oparciu o agentów lub sieć (skanowania sieci).
- Musi umożliwiać ciągłe mechanizmy analizowania zagrożeń, zapobiegania im i przechowywania ich.
- Musi mieć zdolność ciągłego przypisywania polityk określonemu użytkownikowi, adresowi MAC lub OUI adresu MAC, tak, aby użytkownik, urządzenie lub grupa urządzeń miały przydzielony ten sam zestaw zasobów sieci, niezależnie od swojej lokalizacji lub konfiguracji serwera RADIUS.
- Rozwiązanie musi zapewniać informacje o typie urządzeń działających w sieci oraz określonych potrzebach i zagrożeniach, które są z nimi związane.
- Musi zapewnić rozwiązanie oferujące jednolity, centralny obraz wszystkich niechronionych elementów związanych z użytkownikami i urządzeniami, który pozwoli później zredukować złożoność procesu zarządzania.
- Musi dostarczyć rozwiązanie, które zapewni ciągłość działania organizacji poprzez oferowanie użytkownikom alternatywnych metod dostępu podczas procesu skanowania.
- Rozwiązanie musi umożliwiać przypisanie na stałe adresu MAC do określonego przełącznika lub portu przełącznika. Jeżeli system końcowy będzie próbował się uwierzytelnić na innym porcie lub przełączniku, zostanie odrzucony lub przypisana mu zostanie polityka w oparciu o akcje określoną podczas przypisywania mu portu MAC.
- Musi umożliwiać monitorowanie zdarzeń systemów końcowych i przedstawianie wyników o stanie zabezpieczeń systemu w oparciu o najbardziej aktualne skanowania przeprowadzane podczas oceniania.

- Musi posiadać możliwość szybkiego podglądu historycznych i ostatnich znanych stanów połączeń dla każdego systemu końcowego i uzyskiwać informacje o znalezionych podczas skanowania zagrożeniach bezpieczeństwa systemu końcowego.
- Musi zapewnić kompleksowe raportowanie zgodności w oparciu o aktualne i historyczne informacje.
- Musi obsługiwać powiadamianie poprzez syslog, pocztę elektroniczną lub usługi webowe o zmianach stanu systemów końcowych, rejestracji gości oraz wynikach skanowania stanu zabezpieczeń systemów końcowych.
- Musi zapewniać rozwiązanie NAC typu inline oraz out-of-band, które może być zarządzane przez jedną centralną aplikację.
- Musi obsługiwać polityki umożliwiające przepuszczanie lub odrzucanie ruchu sieciowego, nadawanie mu priorytetów, ograniczanie jego szybkości, tagowanie, przekierowywanie
- i kontrolowanie go w oparciu o tożsamość użytkownika, czas i położenie, typ urządzenia i inne zmienne środowiskowe.
- Musi posiadać funkcję IP-to-ID Mapping, która łączy razem nazwę użytkownika, adres IP, adres MAC oraz port fizyczny każdego punktu końcowego. Ta funkcjonalność jest kluczowa dla potrzeb audytów bezpieczeństwa i analiz dochodzeniowych.
- Musi posiadać łatwy w obsłudze panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych.
- Musi posiadać funkcję portalu rejestracyjnego dla kontroli dostępu gości, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT. Musi także oferować zaawansowane możliwości sponsorowania dostępu takie, jak sponsorowanie email oraz prosty portal dla sponsorów służący do zatwierdzania rejestracji gości.
- Musi być dostarczony, jako redundantne urządzenia wirtualne w trybie wysokiej dostępności.
- System musi umożliwiać kontrolę dostępu do sieci dla minimum 500 użytkowników i minimum 1500 urządzeń oraz umożliwiać przyszłą rozbudowę.

2.2.9 Firewall tzw. Next Generation i IPS

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa, Wykonawca zapewni wszystkie poniższe funkcjonalności:

- Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu. W ramach postępowania dostawca powinien dostarczyć system w formie redundantnej w postaci klastra urządzeń. –
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- Monitoring stanu realizowanych połączeń VPN.

- System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
- System realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/100 BaseTX
- Możliwość tworzenia min 254 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
- W zakresie Firewall'a obsługa nie mniej niż 1,5 miliona jednoczesnych połączeń oraz 40 tys. nowych połączeń na sekundę
- Przepustowość Firewall'a: nie mniej niż 6 Gbps
- Wydajność szyfrowania AES lub 3DES: nie mniej niż 3 Gbps
- System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 30 GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku do poszczególnych lokalizacji musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
- W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
  - kontrola dostępu - zapora ogniowa klasy Stateful Inspection
  - ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS).
  - poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
  - ochrona przed atakami - Intrusion Prevention System [IPS]
  - kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
  - kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
  - kontrola pasma oraz ruchu [QoS, Traffic shaping]
  - Kontrola aplikacji oraz rozpoznawanie ruchu P2P
  - Możliwość analizy ruchu szyfrowanego protokołem SSL
  - Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji
- Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 1 Gbps
- Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączoną funkcją: Antivirus min. 400 Mbps
- W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
  - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
  - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
  - Praca w topologii Hub and Spoke oraz Mesh
  - Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
  - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
- Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.

- Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
- Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
- Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
- Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
- Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
- Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
- Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
- Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
- System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
  - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
  - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
  - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
  - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.
- Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
  - ICSA dla funkcjonalności SSLVPN, IPS, Antywirus
  - ICSA lub EAL4 dla funkcjonalności Firewall
- Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- Systemy Firewall i kontroli dostępu do sieci „NAC" opisane w specyfikacji muszą być w stanie wymieniać w czasie rzeczywistym informacje o uwierzytelnianiu użytkownika i stanu autoryzacji użytkowników oraz mapowaniu ID.
- Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 36 miesięcy.

2.2.10 Kontroler sieci bezprzewodowej WLAN

- Musi integrować się bezproblemowo z infrastrukturą przewodową.
- Musi posiadać certyfikat 802.11n WiFi dla kompatybilności w sieciach WLAN.
- Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g oraz 802.11n.
- System musi umożliwiać centralne wdrażanie konfiguracji i aktualizacji.
- Kontrolery muszą obsługiwać elastyczne opcje wdrożenia, obsługując zarówno scentralizowaną, jak i rozproszoną architekturę.
- Kontroler sieci bezprzewodowej w momencie dostawy musi obsługiwać minimum 30 punktów dostępowych w normalnym trybie pracy. Kontroler musi umożliwiać rozbudowę do minimum 248 punktów dostępowych w trybie normalnej pracy oraz do minimum 496 punktów w trybie wysokiej dostępności.
- Musi obsługiwać standardy uwierzytelniania i szyfrowania, w tym: WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x.
- Musi posiadać portal dostępowy Captive Portal zintegrowany z kontrolerem, który można dowolnie dostosowywać do potrzeb.
- Musi pozwalać nietechnicznym pracownikom na tworzenie tymczasowych kont gości i dystrybuowanie zezwoleń poprzez łatwy w użyciu graficzny interfejs użytkownika.
- Musi obsługiwać funkcje egzekwowania polityk i ograniczania przepustowości w punkcie dostępowym.
- Zarządzanie łącznością radiową RF Management musi obsługiwać funkcje automatycznego wyboru kanału i automatycznej kontroli mocy emitowanego sygnału TPC (Transmit Power Control).
- 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.
- 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.
- Kontrolery i 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.
- Musi obsługiwać szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC).
- Musi obsługiwać RADIUS Authentication & Accounting.
- Kontrolery muszą obsługiwać różne mechanizmy przekazywania danych, w tym routing i mostowanie. Mechanizm przekazywania danych musi być skonfigurowany w podziale na wirtualne grupy sieciowe.
- Musi obsługiwać płynny roaming pomiędzy podsieciami IP.

- Musi obsługiwać płynny roaming pomiędzy wieloma kontrolerami.
- Musi obsługiwać przypisywanie polityk klientom, bez konieczności segmentacji przez dedykowane SSID.
- Musi oferować polityki oparte na rolach zapewniające bezpieczeństwo, kontrolę dostępu i priorytety QoS, aplikowane względem użytkownika i aplikacji,
- Musi obsługiwać ujednoliconą, opartą na rolach kontrolę dostępu do sieci przewodowej i bezprzewodowej.
- Wykonawca dostarczy 2 redundantne, wirtualne kontrolery sieci bezprzewodowej.
- Wsparcie dla protokołu SpectraLink voice priority (SVP) lub równoważne,
- Możliwość diagnostyki za pomocą logów systemowych, które zawierają minimum takie informacje jak: czas asosjacji i autentykacji klientów sieci WLAN, oraz logi wewnętrznego DHCP serwera zawierające parametry sieciowe i o której godzinie zostały udzielone klientom WLAN,
- Możliwość diagnostyki systemu przy pomocy wbudowanego narzędzia do zbierania w czasie rzeczywistym ruchu pakietów z interfejsów Ethernet oraz 802.11 (format PCAP),
- Możliwość diagnostyki systemu przy pomocy wbudowanego narzędzie prezentującego aktualne wykorzystanie pasma transmisji dla poszczególnych interfejsów,
- System powinien umożliwiać wykrywanie access-pointów typu rouge (IEEE 802.11a/b/g/n),

2.2.11 Punkt dostępowy do sieci bezprzewodowej WLAN

- Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości 802.11a/n (5 GHz) i 802.11b/g/n (2.4 GHz).
- Punkty dostępowe muszą obsługiwać technologię 802.11n i pracę w technice transmisji wieloantenowej MIMO 2x2 przy zasilaniu przez jedno źródło zgodne z 802.3af, bez wpływu na działanie kluczowych funkcji i wydajności.
- Wsparcie dla mechanizmu minimum Two spatial stream MIMO dla wszystkich nadajników
- Punkty dostępowe muszą być zgodne z DFS2 (Dynamic Frequency Selection) by dopuścić dodatkowe kanały w paśmie 5 GHz.
- Punkty dostępowe muszą obsługiwać 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.
- Punkt dostępowy musi obsługiwać instalację typu plug&play.
- Punkty dostępowe muszą jednocześnie obsługiwać ruch tunelowany i mostowany.
- Połączenie pomiędzy AP a kontrolerem musi być szyfrowane minimum AES 128 bit.
- Punkty dostępowe muszą obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń.
- Musi obsługiwać standardy 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.
- Punkt dostępowy musi zapewniać rozproszone zarządzanie łącznością radiową RF Management (Radio Frequency), niezależne 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.

- Punkty dostępowe muszą mieć możliwość wdrożenia w formie sensorów sieci – pracujących w pełnym lub niepełnym wymiarze czasu.
- Musi obsługiwać funkcje egzekwowania polityk i ograniczania przepustowości w punkcie dostępowym.
- 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.
- 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.
- Punkty dostępowe sieci WLAN muszą mieć możliwość konfiguracji zapewniającej równoważenie obciążenia i sterowanie pasmem. Ta funkcja pozwala 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.
- Kontrolery i 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.
- Punkty dostępowe muszą obsługiwać protokoły 802.11e, w tym WMM, TSPEC oraz U-APSD.
- Musi obsługiwać szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC).
- Musi obsługiwać do 16 SSID (8 na częstotliwość radiową).
- Musi obsługiwać RADIUS Authentication & Accounting.
- Musi obsługiwać płynny roaming pomiędzy podsieciami IP.
- Musi obsługiwać płynny roaming pomiędzy wieloma kontrolerami.
- Musi obsługiwać przypisywanie polityk klientom, bez konieczności segmentacji przez dedykowane SSID.
- Musi wspierać polityki oparte na rolach zapewniające bezpieczeństwo, kontrolę dostępu i priorytety QoS, aplikowane względem użytkownika i aplikacji,
- Wsparcie dla protokołu IEEE 802.1p prioritization,
- AP powinien umożliwiać wykonanie minimum 12 jednoczesnych połączeń VoIP w ramach protokołu IEEE 802.11 a/b/g/n,
- Punkty dostępowe powinny posiadać dwa radia zgodne z: IEEE 802.11/b/g/n oraz 802.11a/n,
- Oprogramowanie działające na punktach dostępowych powinno umożliwiać oddzielną specyfikację częstotliwości dla każdego z modułów radia,

- Punkty dostępowe powinny posiadać certyfikację Wi-Fi Alliance, zapewniającą kompatybilną pracę z urządzeniami klienckimi w ramach standardu 802.11a/b/g/n,
- Możliwość stworzenia i jednoczesnego uruchomienia minimum 16 profili sieci bezprzewodowych WLAN,
- Każdy profil wirtualny sieci bezprzewodowej powinien posiadać możliwość przypisania do VLANu,
- Wymagane jest wsparcie dla protokołu: IEEE 802.1X z wykorzystaniem metod: EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS, and PEAP,
- Wymagane jest wsparcie dla protokołu: MAC address authentication przy wykorzystaniu lokalnych access-list lub przesyłanych z serwera RADIUS,
- Wymagane jest wsparcie dla mechanizmów: RADIUS AAA, przy wykorzystaniu EAP-MD5, PAP, CHAP oraz MS-CHAPv2,
- Wymagane jest wsparcie dla mechanizmów: RADIUS Client
- Wymagane jest wsparcie dla mechanizmów izolacji klientów na poziomie L2,
- Wymagane jest wsparcie dla mechanizmów IEEE 802.11i, WPA2 oraz WPA, przy zastosowaniu algorytmów szyfracji: Advanced Encryption Standard (AES) oraz Temporal Key Integrity Protocol (TKIP),
- Wymagana minimalna ilość portów: 1 RJ-45 autosensing 10/100/1000 port (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex:10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only,
- Dedykowany port konsoli zarządzającej typu RJ-45,
- Radia: dwa radia (a/n + b/g/n),
- Tryb działania radia WLAN: Client access, Local mesh, Packet capture, WDS
- Możliwość pracy punktu dostępowego bez kontrolera WLAN na wypadek awarii łącza,
- Certyfikacja Wi-Fi Alliance Certification dla protokołów 802.11a/b/g/n,
- Liczba anten: 6 anten wewnętrznych,
- Musi umożliwiać administratorom sieci zmianę przeznaczenia punktów dostępowych realizujących usługi WLAN na sensory, na stałe lub tymczasowo przez prostą operację w systemie zarządzania.

2.2.12 Sensory sieci bezprzewodowej

- Sensor protokołów WiFi 802.11b, 802.11b/g, 802.11a, 802.11n
- Musi posiadać zdolność do wykrywania zagrożeń związanych z urządzeniami wykorzystującymi technologię 802.11n (draft 802.11, pre-802.11n, 802.11n).
- Musi wspierać wykorzystanie różnego typu sensorów (nie tylko dedykowanych).
- Musi być w pełni zintegrowany z systemem zarządzania opisanym w tej specyfikacji w celu minimalizacji interakcji użytkownika z systemem.
- Musi uwzględniać szczególną obsługę urządzeń gości, by zapewnić odpowiedni status uwierzytelnienia.
- Musi wspierać bezpieczne protokoły szyfrujące: WEP, TKIP, CCMP (AES).
- Musi obsługiwać automatyczne wykrywanie SSID.

- 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.
- 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) .
- Musi obsługiwać jednocześnie skanowanie i ochronę przed atakami.
- Musi umożliwiać tworzenie planu pomieszczeń z możliwością zaznaczenia lokalizacji każdego autoryzowanego laptopa Wi-Fi, PDA, tagu RFID, itp.
- Musi zapewniać możliwość lokalizacji zagrożeń, bez względu na to czy są one aktualnie aktywne czy też nie.
- Musi dostarczać raporty zgodności z wymaganiami, w tym: Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, DoD Directive 8100.2, PCIS (v1.1 & v1.2), MITS
- Musi obsługiwać raporty dostosowane do potrzeb użytkownika, opierające się na typie zdarzenia, klienta, itp.
- Musi zapewniać automatyczne generowanie raportów.
- Musi zapewniać dokładną klasyfikację urządzeń, by ograniczyć liczbę informacji fałszywie pozytywnych i fałszywie negatywnych.
- Należy dostarczyć 5 licencji dla punktów dostępowych umożliwiających działanie w trybie sensora.
- Musi umożliwiać administratorom sieci zmianę przeznaczenia punktów dostępowych realizujących usługi WLAN na sensory, na stałe lub tymczasowo przez prostą operację w systemie zarządzania.

2.2.13 Serwer PDC (Kontrolera domeny), Serwer BDC (Zapasowego kontrolera domeny) z obsługą serwera Exchange wraz z licencjami i macierzą dysków

Serwer o minimalnych parametrach nie gorszych niż:

- procesor Intel Xeon E5-2430 2.20GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W
- PCIE Riser for Chassis with 2 Proc
- Obudowa na minimum 4 dyski 3.5" lub 2.5" Hot Plug Hard Drives
- Bezel - 4/8 Drive Chassis
- Performance Optimized
- 1333 MHz RDIMMs
- minimum 32GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x4
- Intel Xeon E5-2430 2.20GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W
- trzy dyski 300GB SAS 6GB/s 15 000obr./min 3,5-calowy dysk twardy Hot Plug
- PERC H710 Integrated RAID Controller, 512MB NV Cache
- x Heat Sink,PowerEdge
- 1x No Optical Drive
- Power Distribution Board for Hot Plug Power Supplies
- dwie sztuki 2M Rack Power Cord C13/C14 12A

- Dual Hot Plug Power Supplies 550W
- SAS Cable for 3.5" in Hot Plug Chassis
- On Board Network Adapter
- ReadyRails Sliding Rack Rails without Cable Management Arm
- iDRAC7 Enterprise
- iDRAC Port Card
- Performance BIOS Setting
- Windows Server 2008 R2 SP1, Enterprise Edition, English, Incl. 10 CALs, No Media
- DVD Media for Windows Server 2008 R2 SP1, Enterprise Edition, English

Wymagana gwarancja

- 1 Base Warranty
- 1 3Yr Basic Warranty - Next Business Day - Minimum Warranty
- 1 3Yr ProSupport and 4hr Mission Critical
- 1 Declined Remote Advisory

Macierz o minimalnych parametrach nie gorszych niż:

- PV MD3220 ramka
- minimum sześć dysków 600GB SAS 6Gb/s 10tys.obr./min 2,5-calowy dysk twardy
- minimum sześć dysków 300GB SAS 6Gbps 15k 2.5" HD
- Nadmiarowy zasilacz (2 jednostki) 600W
- dwa zapasowe przewody zasilania 2m
- cztery sztuki 1m kabel zewnętrznego złącza SAS
- jedna sztuka szyny Rapid Rails do szaf serwerowych, z kwadratowymi otworami

Wymagana gwarancja

- 1 Remote Implementation of a Dell PowerVault MD3xxx Series Array
- 1 Base Warranty
- 1 3Yr Basic Warranty - Next Business Day - Minimum Warranty
- 3Yr ProSupport and 4hr Mission Critical

Wraz ze sprzętem należy dostarczyć poniższe licencje:

- 120 licencji ExchgStdCAL 2010 SNGL OLP NL UsrCAL
- 110 licencji WinSvrCAL 2008 SNGL Promo OLP NL UsrCAL

2.2.14 Serwer wirtualizacyjny dla Aplikacji zarządzającej, NAC, Korelacji zdarzeń

Serwery (2 szt.) o minimalnych parametrach nie gorszych niż:

- 1 Intel Xeon E5-2430 2.20GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W
- 1 PCIE Riser for Chassis with 2 Proc
- Bezel - 4/8 Drive Chassis
- obudowa dla 8 dysków, 2.5" Hot Plug Hard Drives
- Performance Optimized
- 1333 MHz RDIMMs

- 48GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x4
- Intel Xeon E5-2430 2.20GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W
- minimum dwa dyski146GB SAS 6Gb/s 15tys.obr./min 2,5-calowy dysk twardy Hot Plug
- SAS 6Gbps HBA External Controller
- PERC H710 Integrated RAID Controller, 512MB NV Cache
- xHeat Sink,PowerEdge
- No Internal Optical Drive
- Power Distribution Board for Hot Plug Power Supplies
- 2 x 2M Rack Power Cord C13/C14 12A
- Dual Hot Plug Power Supplies 550W
- On Board Network Adapter
- ReadyRails Sliding Rack Rails without Cable Management Arm
- C8 - RAID 1 for H310/H710, 2 SAS/SATA/SSD HDDs
- iDRAC7 Enterprise
- iDRAC Port Card
- Performance BIOS Setting
- No DVD Media

Wymagana gwarancja

- Base Warranty
- 3Yr Basic Warranty - Next Business Day - Minimum Warranty
- 3Yr ProSupport and 4hr Mission Critical
- Declined Remote Advisory

2.2.15 Wymagane kable do uruchomienia działającego systemu

- Kable przyłączeniowe RJ45/RJ45 kategorii 5e nieekranowane PVC,
- Kable przyłączeniowe RJ45/RJ45 kategorii 6 ekranowane LSZH,
- Kabel przyłączeniowy 2 G50/125 OM3 zakończenia dopasowane do zastosowanego sprzętu i przełącznic optycznych,
- Kabel przyłączeniowy 2 E9/125 zakończenia dopasowane do zastosowanego sprzętu i przełącznic optycznych

2.2.16 Centrala abonencka obsługująca PSTN, ISDN, VoIP

- Umożliwia realizację usług telekomunikacyjnych w technologii TDM i IP,
- Posiada możliwość obsługi sieci publicznej za pomocą traktów ISDN PRA, BRA, SIP Trunk,
- Posiada możliwość obsługi abonentów wewnętrznych za pomocą aparatów analogowych, systemowych, aparatów IP, aplikacji softphone, DECT, VoWLAN- wymagania odnośnie rodzajów portów i aparatów podane są w dalszej części specyfikacji,
- Musi umożliwiać rozbudowę jedynie poprzez dołożenie kart abonenckich do łącznej liczby 512 użytkowników w dostarczanej obudowie bez wymiany lub rozbudowy modułów sterujących.

- System musi być kompletny, tj. musi posiadać wszystkie niezbędne elementy sprzętowe (hardware konieczny do uruchomienia systemu zgodnie z wymaganiami), programowe oraz licencyjne.
- System musi posiadać minimum funkcje: prezentację numeru dzwoniącego (CLIP), blokade prezentacji numeru (CLIR), identyfikacje numeru dzwoniącego (COLP), blokade identyfikacji numeru dzwoniącego (COLR) na wszystkich aparatach (analogowych, systemowych TDM i IP).
- System musi wspierać połączenia automatyczne typu gorąca linia (HOT LINE) bezzwłocznie realizowane natychmiast po podniesieniu mikrotelefonu
- System musi wspierać połączenia automatyczne typu gorąca linia (HOT LINE) ze zwłoką, realizowane po upływie predefiniowanego czasu po podniesieniu mikrotelefonu jeżeli użytkownik nie rozpoczął wybierania w sposób konwencjonalny
- Centrakla musi posiadać funkcję identyfikacji złośliwych połączeń z publicznej sieci ISDN
- Telefony analogowe przewodowe z funkcją CLIP i współpracujące z oferowaną centralą telefoniczną muszą być obsługiwane przez minimum 3 karty abonenckie
- System telekomunikacyjny musi mieć zaimplementowane uniwersalne licencjonowanie portów abonenckich i miejskich – jeden wspólny typ licencji musi otwierać port abonencki (TDM, VoIP, cyforwy), port miejski analogowy, kanał B portu miejskiego ISDN.
- Centrala musi posiadać zintegrowany sprzętowo moduł abonentów Voice over IP wykorzystujący jako medium transportowe sieć LAN/WAN z zachowaniem pełnej funkcjonalności systemowego aparatu stacjonarnego.
- Posiada funkcję automatycznego wyboru najtańszej trasy połączenia (funkcja LeastCost Routing),
- Centrala musi posiadać funkcję „wejście na trzeciego” dla uprzywilejowanego abonenta - możliwość włączenia się w trwającą rozmowę, możliwość przerwania trwającej rozmowy i zestawienie rozmowy z wybranym numerem.
- System musi wspierać tworzenie uprawnień dla przerywania użytkownikowi aktualnie prowadzonej rozmowy i połączenie się z nim – w sytuacjach priorytetowych
- Musi posiadać funkcjonalność tworzenia centralnej i osobistej książki adresowej dostępnej dla wszystkich użytkowników systemu.
- System musi posiadać funkcję przypisania kilku różnych numerów wewnętrznych (co najmniej pięciu) do jednego aparatu systemowego. Musi istnieć możliwość wyboru przez przycisk na aparacie linii wewnętrznej, za pomocą której będzie realizowane połączenie wychodzące (właściwa i różna prezentacja numeru dla połączeń wychodzących w zależności od wybranej linii wewnętrznej: służbowej, prywatnej i pilnej).
- Musi umożlwiać tworzenia grup abonenckich i definiowanie ścieżki połączeń dla różnych abonentów w grupie (dzwonienie jednoczesne, kolejne, przechwytywanie połączeń w grupie, przekazywanie połączenia na inny numer przy określonej sytuacji np. po określonej liczbie sygnałów lub zajętości),
- Musi posiadać możliwość nadawania uprawnień jak i ograniczeń w zakresie realizowania połączeń i korzystania z funkcjonalności dla poszczególnych grup i poszczególnych abonentów wewnętrznych systemu,
- System musi być wyposażony w duplikację jednostki sterującej działającej w trybie „gorącej rezerwy” (zawierającej pełną replikę oprogramowania sterującego i aplikacyjnego) w

szczególności wymagane jest utrzymanie bez zmian i strat jakości wszystkich zestawionych połączeń w czasie i po przełączeniu na zapasową jednostkę sterującą.

- System musi posiadać redundantne zasilacze półek abonenckich i półki sterującej. Awaria jednego z prostowników nie może powodować wyłączenia poszczególnych półek
- System musi być wyposażony w interfejsy do sieciowania z systemem telekomunikacyjnym wieży kontroli lotów PAŻP Gdańsk Rębiechowo, gdzie znajduje zlokalizowany jest system HighPath 4000, za pomocą łącza 1 PRA (należy zapewnić odpowiedni hardware wraz z pracami instalacyjnymi dla oferowanej centrali oraz dla centrali po stronie PAŻP) z przeniesieniem co najmniej następujących funkcji :
  - Prezentacja numeru (CLIP)
  - Blokada prezentacji numeru (CLIR)
  - Identyfikacja numeru dzwoniącego (COLP)
  - Blokada identyfikacji numeru dzwoniącego (COLR)
  - Oddzwanianie przy zajętości – w przypadku zajętości stacji wywoływanej abonent może zażądać zasygnalizowania faktu, że stacja wywoływana przeszła w stan spoczynku, tzn. zakończyła dotychczasowe połączenie
  - „Wejście na trzeciego" dla uprzywilejowanego abonenta - możliwość włączenia się w trwającą rozmowę, możliwość przerwania trwającej rozmowy i zestawienie rozmowy z wybranym numerem
- System musi posiadać funkcjonalność obsługi zestawów sekretarsko-dyrektorskich. Praca zestawów w konfiguracji typu n-sekretarek obsługuje m dyrektorów, gdzie n=1-2 (minimum) m=1-4 (minimum)
  - Układ sekretarsko dyrektorski musi wspierać: filtrowanie połączeń zewnętrznych i wewnętrznych; natychmiastowe przekazywanie połączeń z telefonu dyrektora do telefonu sekretarki, aktywowane przez dyrektora lub sekretarkę.
- System musi umożliwiać tworzenia personalizowanych zapowiedzi głosowych.
- Musi posiadać funkcję automatycznego operatora dla minimum 4 opcji wyboru i minimum 4 poziomów
- Posiada funkcję poczty głosowej dla wszystkich użytkowników systemu. Funkcjonalność poczty głosowej musi być ograniczona tylko do umożliwienia nagrywania na żądanie rozmowy w czasie jej trwania zdefiniowanym klawiszem na aparacie telefonicznym. Minimalny czas przechowywania nagrania musi wynosić 30 dni.
- Zarządzanie uprawnieniami poczty głosowej musi być definiowane tylko przez administratora systemu lub osoby uprawomocnione.
- PIN kody dla realizacji połączeń zewnętrznych dla minimum 20 użytkowników systemu.
- System musi umożliwiać tworzenie min 10 konferencji trójstronnych oraz min 3 konferencje wielostronne (do 7 abonentów każda)
- Centrala musi posiadać możliwość stworzenia jednorodnego planu numeracji o następującej charakterystyce:
  - Dopasowany do zewnętrznej numeracji telefonicznej
  - Dopuszczający nieciągłość numeracji
  - Dopuszczający różną długość planu numeracji od 3 do 8 cyfr,
- System zapewni konwergencję systemu telefonii IP z telefonią GSM w szczególności:

- Możliwość przypisania do użytkownika systemu jego telefonu GSM.
- Możliwość jednoczesnego skierowania połączenia przychodzącego na dany numer wewnętrzny oraz przypisany do tego numeru, numer GSM (Użytkownik będzie miał wybór odebrania połączenia ta telefonie stacjonarnym lub komórkowym).

- Centrala musi dostarczać funkcjonalność powiadamiania alarmowego o następujących parametrach:
  - Możliwość powiadamiania wszystkich użytkowników centrali
  - Liczba jednocześnie odtwarzanych komunikatów nie mniejsza niż 4 (system powiadamiania alarmowego musi posiadać co najmniej 4 równoległe kanały głosowe).
- System musi umożliwiać dystrybucję wcześniej przygotowanych informacji słownych poprzez automatyczne wykonywanie połączeń na zdefiniowane numery telefonów, z kontrolą faktu odebrania połączenia. Musi istnieć możliwość zainicjowania rozgłoszenia przez użytkownika systemu z poziomu dowolnego aparatu w tym z konsoli dyspozytorskiej.
- Minimalne wymagania techniczne dla systemu telefonicznego
  - Interfejsy wewnętrzne:
    - 48 użytkowników terminali analogowych wraz z prezentacją CLIP
    - 16 użytkowników terminali cyfrowych
    - 64 użytkowników terminali IP w oparciu o protokół SIP/HFA
    - 3 konsole dyspozytorskie z ekranami dotykowymi wraz z współpracującymi aparatami cyfrowymi i słuchawkami nagłownymi.
    - Integracja dla 10 użytkowników GSM z systemem telefonicznym
  - Interfejsy do sieci publicznej:
    - 2 trakty PRA
  - Interfejsy do centrali PAŻP
    - 1 trakt PRA
  - Zasilanie awaryjne na elementy sterujące systemu na 2 godzin

2.2.17 Aparaty systemowe

- **Terminale cyfrowe typu A – 7 sztuk o minimalnej charakterystyce:**
  - Wyświetlacz w języku polskim
  - Przycisk dostępu do poczty głosowej
  - Kolorowy, podświetlany, ruchomy, wyświetlacz graficzny o rozdzielczości min. 320x240 pix
  - Przycisk dostępu do funkcji głośnomówiącej
  - Umożliwiać dołączenie przystawek z dodatkowymi klawiszami programowalnymi wyposażonych w wyświetlacz LCD zapewniający wyświetlanie opisów klawiszy
  - Przycisk ponownego wybierania
  - Przycisk regulacji głośności/ wyciszania mikrofony
  - Regulowany kąt nachylenia wyświetlacza
  - Możliwość podłączenia zewnętrznego zestawu nagłownego poprzez dedykowane złącze z funkcją automatycznego wykrywania obecności zestawu
  - Musi umożlwiać prowadzenie rozmowy za pomocą zestawu głośnomówiącego (full duplex).

- **Terminal cyfrowy typu B – 12 sztuk o minimalnej charakterystyce:**
  - Wyświetlacz w języku polskim
  - Wyświetlacz monochromatyczny 205x41 pix, dwuwierszowy min. 24-znakowy
  - 8 wbudowanych przycisków programowalnych
  - Przycisk regulacji głośności/ wyciszania mikrofony
  - Musi umożlwiać prowadzenie rozmowy za pomocą zestawu głośnomówiącego (full duplex).
- **Przystwka dodatkowych klawiszy – 1 sztuka o minimalnej charakterystyce:**
  - przystawka z 65 dodatkowymi klawiszami programowalnymi wyposażonymi w wyświetlacz LCD zapewniający wyświetlanie opisów klawiszy

2.2.18 Konsole operatorskie z obsługą gorących linii

- Konsola musi być zbudowana w postaci specjalizowanego terminala dedykowanego do równoległej obsługi ruchu o dużym natężeniu, zawierająca wyświetlacz dotykowy LCD min 10” wspomagany wbudowanymi przyciskami mechanicznymi.
- Konsola musi być zbudowana w oparciu o jednostkę centralną z użyciem Compact Flash (CF) zamiast dysku twardego oraz bez użycia wentylatorów
- Konsola musi zapewniać zmianę kąta manipulatora pochylenia umożliwiając pracę użytkownika stojącego oraz pracę w zmiennych warunkach oświetleniowych poprzez podświetlanie wyświetlacza
- Interfejs użytkownika konsol musi być dostępny w języku polskim
- Obowiązkowe wyposażenie stanowiska dyspozytorskiego to wbudowany zestaw głośnikowy oraz dwie standardowe słuchawki z podkładkami (klasyczne przewodowe w wbudowanym przyciskiem umożliwiającym funkcjonalność: „naciśnij aby wyciszyć” lub „naciśnij aby mówić”),
- Konsola musi zapewniać obsługę minimum 4 rozmów jednocześnie,
- Wymagana jest wbudowana funkcja monitorowania (podsłuchu) wszystkich lub wybranych linii głosowych na poszczególnych stanowiskach (możliwość miksowania 4 linii na jeden kanał głośnikowy),
- Wymagana jest regulacja poziomu głośności osobno dla każdego kanału audio,
- Konsola musi umożliwiać dowolną konfigurację rozmieszczenia kontrolek sterujących oraz przypisanych do nich funkcji,
- Konfiguracja ekranu konsoli wykonywana przez administratora poprzez aplikacje do zarządzania systemem
- Wymagany jest konfigurowalny dostęp do funkcji konsoli, poprzez mechanizm uprawnień, ustawianych tylko przez administratora, każdy profil użytkownika konsoli może być chroniony hasłem
- Wymagany jest szybki prosty dostęp do wpisów książki telefonicznej oraz do historii wywołań (łącznie ostatnie 40 wywołań)
- Wymagana jest zmiana dźwięków sygnalizacyjnych w konsolach poprzez wybór z listy dostępnych dzwonków,
- Konsola musi działać z zastosowaniem indywidualnej jej konfiguracji (profilu) dla każdego dyspozytora

- Wymagane jest wsparcie pracy na jednej konsoli wielu dyspozytorów (tryb zmianowy). Każdy dyspozytor pracuje na indywidualnych ustawieniach konsoli (profil). Indywidualne ustawienia są wczytywane poprzez zalogowanie się dyspozytora do konsoli przy użyciu indywidualnej nazwy użytkownika i hasła.
- Każda z konsol musi uwierzytelnić profil każdego dyspozytora i zaoferować dostęp do jego indywidualnego profilu.
- Interfejs graficzny użytkownika konsoli musi zapewniać:
- programowalne klawisze: liniowe, funkcyjne bądź dedykowane na min 10 poziomach z co najmniej 20-oma programowalnymi polami każde
- optyczną sygnalizację stanu klawiszy liniowych
- wizualizacja kolejki wywołań przychodzących i zawieszonych polegająca na prezentacji tych wywołań w kolejności zgodnie z czasem wywołania linii dyspozytorskiej oraz jej priorytetem
- Połączenia wychodzące muszą być realizowane przez:
- szybkie wybieranie automatyczne za pomocą elektronicznej książki telefonicznej
- przyciski automatycznego wybierania z automatyczną selekcją wolnej linii
- powtórne wybieranie numeru (numer ostatni bądź zapamiętany)
- wybranie numeru z historii połączeń wychodzących
- przycisków programowalne tzw. „gorące linie”, przyciski wybierania natychmiastowego lub specjalne
- możliwość wejścia „na trzeciego” w aktualnie prowadzoną rozmowę na innej konsoli
- Połączenia przychodzące muszą być realizowane za pomocą:
- automatycznego zgłoszenia się poprzez podniesienie mikrotelefonu do pierwszego abonenta z kolejki priorytetów wywołań skierowanych do stanowiska dyspozytora, lub selektywny wybór abonenta kursorem na wyświetlaczu lub monitorze
- przycisków liniowych
- przycisków bezpośredniego wyboru
- listy połączeń przychodzących tzw. Kolejki wywołań
- priorytetów w kolejkowaniu dla linii dyspozytorskich czekających na przyjęcie przez dyspozytora, według programowalnego menu wybieranego w zależności od istniejących sytuacji
- przyjmowania tych samych linii i numerów abonenckich na wskazanych konsolach
- Wymagana jest realizacja funkcji odbierania przez dyspozytora dowolnego połączenia bez zachowania kolejności lub pozostawienie go w stanie oczekiwania realizując inne połączenia wychodzące.
- System musi wspierać przejmowanie funkcji pomiędzy konsolami (np. w przypadku awaryjnego przeniesienia stanowiska dyspozytora do lokalizacji zapasowej).
- System musi integrować się z rejestratorem rozmów poprzez sieć LAN/WAN, rejestrator musi obierać audio rozmów z dedykowanego interfejsu serwera dyspozytorskiego oraz dane CTI z dedykowanego interfejsu.
- Wymagane jest przyjęcie i obsługa kolejki w zakresie od 2 do co najmniej 20 przywołań oczekujących z prezentacją numeru, nazwy abonenta lub linii i uszeregowaniem abonentów wg listy co najmniej 5-ciu priorytetów.

- Wymagana jest współpraca konsol z aparatami telefonicznymi systemu komunikacyjnego pracujących w grupach przejmowania rozmów – przejęcie rozmowy poprzez kod funkcji lub dedykowany klawisz konsoli
- System dyspozytorski musi mieć możliwość integracji z systemem TETRA poprzez łącza DSS1 lub SIP. Muszą być dostępne minimum usługi: CLIP, CLIR, COLP, COLR, HOLD, HOT LINE. Integracja nie może powodować wymiany dostarczonych urządzeń.
- Wymagane jest tworzenie kopi zapasowej ustawień systemu dyspozytorskiego – kompletna kopia całego systemu, eksport pojedynczych profili konsol dyspozytorskich, eksport ustawień książki telefonicznej

2.2.19 Aplikacja do Zarządzania systemem telefonii

Wraz z systemem dostarczone zostanie oprogramowanie do administracji dostępne poprzez sieć LAN/WAN. Minimalne wymagania oprogramowania to:

- Proponowane rozwiązanie musi posiadać możliwość konfiguracji z wykorzystaniem dedykowanej aplikacji lub za pośrednictwem przeglądarki WWW,
- Dostarczona Aplikacja do Zarządzania musi być tego samego producenta co dostarczony system telefoniczny
- Dostarczona Aplikacja musi umożliwiać łatwe tworzenie wszystkich użytkowników systemu (w tym użytkowników aplikacji UC).
- Dostarczona Aplikacja musi umożliwiać łatwe modyfikowanie dowolnych parametrów konfiguracyjnych wszystkich obiektów w systemie telefonicznym
- Aplikacja ma pracować na systemie operacyjnym Windows i umożliwia obsługę w języku polskim,
- Aplikacja ma gwarantować pracę w środowisku okienkowym (graficznym) umożliwiając realizację zadań administratora bez konieczności znajomości kodu programowania systemu telefonicznego,
- Aplikacja ma umożliwiać uwierzytelnianie użytkowników i możliwość przypisania ich do odpowiednich grup o ściśle określonych uprawnieniach (pełny dostęp / do odczytu),
- Aplikacja ma umożliwiać tworzenie profili dla użytkowników/grup użytkowników z podziałem na parametry, które mogą być zarządzane przez tych użytkowników/grupy użytkowników w systemie telefonicznym
- Aplikacja ma umożliwiać zarządzanie centralną książką telefoniczną,
- Centralna książka telefoniczna musi być dostępna z poziomu przeglądarki WWW i musi realizować funkcję click-to-call z poziomu przeglądarki
- Dane zawarte w centralnej książce telefonicznej dotyczące konkretnego użytkownika systemu telefonicznego, muszą być edytowalne z poziomu przeglądarki WWW przez tego użytkownika.
- Aplikacja ma umożliwiać administrowanie wszystkimi typami użytkowników (analogowi, systemowymi, IP)
- Aplikacja ma umożliwiać dostęp do rejestru zdarzeń systemu telefonicznego,

- Aplikacja musi posiadać mechanizm alarmowy, który w razie wystąpienia awarii lub dowolnych nieprawidłowości, będzie informował administratorów poprzez wysłanie wiadomości email.

2.2.20 Aplikacja Taryfikacyjna

Wraz z systemem dostarczone ma być oprogramowanie do administracji i taryfikacji dostępne poprzez sieć LAN/WAN. Minimalne wymagania oprogramowania to:

- Pracuje na systemie operacyjnym Windows i umożliwia obsługę w języku polskim,
- Umożliwia automatyczne tworzenie raportów z połączeń dla poszczególnych użytkowników/grup użytkowników i automatyczne wysyłanie raportów do wskazanych użytkowników/grup użytkowników poprzez e-mail.
- Wymagana jest zdolność do taryfikacji połączeń przychodzących i wychodzących, wewnętrznych
- Wymagany jest mechanizm kontroli kosztów z podziałem na osoby, grupy osób i typy połączeń
- Wymagany jest mechanizm szczegółowego raportowania z elastycznie definiowanymi kryteriami, tworzenie wielopoziomowej struktury raportu, eksport raportów do formatu xls, PDF, txt.
- Wymagany jest mechanizm symulacji kosztów w przypadku podłączenia innego operatora
- Archiwizacja i zabezpieczenie danych na nośnikach zewnętrznych (zapis na CD, DVD itp.).
- Umożliwia automatyczne tworzenie raportów z połączeń dla poszczególnych użytkowników/grup użytkowników i automatyczne wysyłanie raportów do wskazanych użytkowników/grup użytkowników poprzez e-mail.

2.2.21 Systemu nagrywania współpracującego z systemem telefonicznym

- System rejestracji rozmów musi umożliwiać rejestrację treści rozmów telefonicznych w postaci zapisu cyfrowego
- Wymagana jest rejestracja jednocześnie 16 abonentów analogowych, traktu ISDN PRA (30B+D) do operatora oraz 3 konsol dyspozytorskich.
- Rejestrator musi archiwizować nagrania na zewnętrznym nośniku danych (płyta DVD, dysk twardy) oraz na udostępnionym zasobie sieciowym. Wymaga się archiwizacji w trybie automatycznym i manualnym. Proces archiwizacji rozmów nie może usuwać nagrań na dysku twardym rejestratora.
- Łączny czas nagrań na wewnętrznym dysku rejestratora musi być nie mniejszy niż 25000 godzin.
- Rejestrator musi być wyposażony w ochronę usuwania nagrań przez administratorów i użytkowników systemu.
- Proces odsłuchu rozmowy musi być niezależny od procesu rejestracji rozmów w danym momencie. Nie dopuszcza się rozwiązań, w których odsłuch rozmowy może zakłócić, zatrzymać proces nagrywania rozmów oraz odsłuch rozmowy pogarsza jakość rejestrowanego audio.

- Wymagany jest dostęp do funkcji odsłuchu nagrań jednocześnie przez minimum trzech użytkowników oraz do funkcji administracyjnych jednocześnie przez minimum dwóch administratorów.
- Wymagane jest zapewnienie rozbudowy rejestratora o kolejnych użytkowników analogowych, cyfrowych i VoIP.
- Rejestrator rozmów musi natychmiast raportować o błędach lub awariach urządzeń wchodzących w skład rejestratora
- Rejestrator rozmów powinien opatrywać nagrania głosowe dodatkowymi informacjami tj.:
  - numer abonenta dzwoniącego (w ruchu przychodzącym),
  - numer wewnętrzny,
  - numer wybrany,
  - data i godzina połączenia,
  - czas trwania połączenia,
  - kierunek rozmowy,
- Rejestrator rozmów musi umożliwić wyszukiwanie nagrań co najmniej według następujących kryteriów:
  - data i czas nagrania,
  - numer linii (kanał),
  - numer dzwoniący,
  - numer wewnętrzny,
  - kierunek połączenia.
- Zarządzanie i administracja rejestratora oraz odsłuch nagrań musi się odbywać poprzez sieć LAN z zastosowaniem dedykowanego oprogramowania zainstalowanego na stacji roboczej. Dostęp do aplikacji musi być umożliwiony po autentykacji użytkownika/administratora - podanie loginu i hasła.
- Rejestrator musi być wyposażony w funkcję eksportu nagrań do pliku (np. pliku wav) na dedykowanej stacji użytkownika i administratora. Format pliku wyeksportowanego nagrania musi umożliwiać jego odsłuch z zastosowaniem dostępnego oprogramowania np. Windows Media Player bez konieczności komunikacji z rejestratorem, który daną rozmowę nagrał.

2.3 Montaż urządzeń aktywnych

Urządzenia aktywne montujemy w szafie dystrybucyjnej na stelażu 19” za pomocą zestawu elementów śrub mocujących (4x śruba, podkładka oraz nakrętka). Instalacja winna przebiegać zgodnie z kartą katalogową danego urządzenia.

2.4 Transport

Środki i urządzenia transportowe powinny być odpowiednio przystosowane do transportu materiałów, elementów, konstrukcji urządzeń itp. niezbędnych do wykonywania danego rodzaju robót elektrycznych. W czasie transportu należy zabezpieczyć przemieszczane przedmioty w sposób zapobiegający ich uszkodzeniu.

W czasie transportu, załadunku i wyładunku oraz składowania elementów urządzeń należy przestrzegać zaleceń wytwórców. Należy zastosować się do zaleceń producenta.

Zaleca się dostarczenie urządzeń bezpośrednio przed montażem, w celu uniknięcia dodatkowego transportu z magazynu budowy.

3 Odbiór prac montażowych

3.1 Ogólne zasady odbioru prac montażowych

Prace uznaje się za wykonane zgodnie z ST i wymaganiami Inspektora, jeżeli wszystkie pomiary i badania z zachowaniem tolerancji dały wyniki pozytywne.

Jako odbiór robót związanych z instalacją systemu zintegrowanego, traktuje się iż system pozytywnie przechodzi następujące testy:

1. Weryfikacja warstwy fizycznej instalacji urządzeń sieciowych i systemów zarządzania w poszczególnych MDF-ach i PDF-ach
2. Weryfikacja poprawności funkcjonowania warstwy sieci LAN, podziału na segmenty sieci, ich roli, elementów niezawodnościowych w sieci.
3. Testy niezawodności połączeń pomiędzy punktami dystrybucyjnymi a rdzeniem sieci LAN
4. Testy działania funkcjonalności port-security na przełącznikach dostępowych
5. Test poprawności działania dostępu administracyjnego
6. Test Sprawdzenie działania dostępu administracyjnego w oparciu o zewnętrzną bazę danych – Microsoft Active Directory
7. Weryfikacja poprawności konfiguracji warstwy zabezpieczeń sieciowych
8. Test działania funkcjonalności failover firewall
9. Warstwy detekcji i prewencji przed włamaniami, w oparciu o sondy IDP/IPS.
10. Weryfikacja poprawności funkcjonowania systemu klasy SIEM
11. Weryfikacja poprawności działania systemów kontroli dostępu do sieci: systemu NAC.
12. Test funkcjonalności systemu NAC – podłączenie klienta
13. Weryfikacja poprawności działania warstwy dostępu do sieci Internet.
14. Weryfikacja poprawności funkcjonowania warstwy systemu zarządzania
15. Weryfikacja poprawności działania sieci bezprzewodowej, z uwzględnieniem kontrolerów i systemu zarządzania
16. Test dostępu do bezprzewodowej sieci gościnnej
17. Test dostępu do bezprzewodowej sieci dla pracowników
18. Test generowania raportów z systemu zarządzającego
19. Test poprawności wykonania połączeń telefonicznych przychodzących i wychodzących ,wewnętrznych i zewnętrznych – aparatów analogowych
20. Test poprawności wykonania połączeń telefonicznych przychodzących i wychodzących, wewnętrznych i zewnętrznych – aparatów VoIP
21. Test poprawności wykonania połączeń telefonicznych przychodzących i wychodzących, wewnętrznych i zewnętrznych – aparatów systemowych

22. Weryfikacja nagrywania rozmów wewnętrznych
23. Weryfikacja nagrywania rozmów „na żądanie”
24. Test połączeń wykonywanych za pomocą konsoli operatorskiej
25. Test obsługi kolejek za pomocą konsoli operatorskiej
26. Test połączeń bezpośrednich z wykorzystaniem konsoli operatorskiej
27. Test odbierania fax-ów i dostarczania ich do dedykowanej skrzynki mail-owej na serwerze Exchange
28. Test generowania bilingów

3.2 Odbiór wstępny robót

Odbiór wstępny polega na finalnej ocenie rzeczywistego wykonania robót w odniesieniu do ich ilości, jakości i wartości. Całkowite zakończenie robót oraz gotowości do odbioru wstępnego będzie stwierdzona przez Wykonawcę powiadomieniem na piśmie o tym fakcie Inwestora. Odbiór wstępny robót nastąpi w terminie ustalonym w dokumentach kontraktowych licząc od dnia potwierdzenia przez Inwestora zakończenia robót i przyjęcia dokumentów, o których mowa w punkcie 3.3.

Odbioru wstępnego robót dokona komisja wyznaczona przez Inwestora w obecności Wykonawcy. Komisja odbierająca roboty dokona ich oceny jakościowej na podstawie przedłożonych dokumentów, wyników badań pomiarów, oceny wizualnej oraz zgodności wykonania robót z dokumentacją montażu i specyfikacjami technicznymi.

W toku odbioru wstępnego robót komisja zapozna się z realizacją ustaleń przyjętych w trakcie odbiorów robót zanikających i ulegających zakryciu, zwłaszcza w zakresie wykonania robót uzupełniających i robót poprawkowych. W przypadkach niewykonania wyznaczonych robót poprawkowych, robót uzupełniających lub robót wykończeniowych komisja przerwie swoje czynności i ustali nowy termin odbioru wstępnego.

3.3 Dokumenty do odbioru wstępnego

Podstawowym dokumentem do dokonania odbioru wstępnego robót jest protokół odbioru wstępnego robót sporządzony według wzoru ustalonego przez Inwestora. Do odbioru wstępnego wykonawca jest zobowiązany przygotować następujące dokumenty:

- Dokumentację powykonawczą
- Specyfikacje techniczne (podstawowe z kontraktu i ewentualnie uzupełniające lub zamienne).
- Ustalenia technologiczne.
- Dokumenty zainstalowanego wyposażenia.
- Rejestry obmiarów (oryginały).
- Deklaracje zgodności lub certyfikaty zgodności wbudowanych materiałów zgodnie z specyfikacjami technicznymi.
- Rysunki (dokumentacje) na wykonanie robót towarzyszących oraz protokoły odbioru i przekazania tych robót właścicielom urządzeń.
- Instrukcje eksploatacyjne.

W przypadku, gdy według komisji roboty pod względem przygotowania dokumentacyjnego nie będą gotowe do odbioru wstępnego, komisja, w porozumieniu z Wykonawcą, wyznaczy ponowny termin odbioru wstępnego robót.

Wszystkie zarządzone przez komisję roboty poprawkowe lub uzupełniające będą zestawione według wzoru ustalonego przez Zamawiającego.

Termin wykonania robót poprawkowych i robót uzupełniających wyznaczy komisja.

3.4 Odbiór końcowy

Odbiór końcowy - pogwarancyjny polega na ocenie wykonanych robót związanych z usunięciem wad stwierdzonych przy odbiorze wstępnym i zaistniałych w okresie gwarancyjnym.

Odbiór końcowy – pogwarancyjny będzie dokonany na podstawie oceny wizualnej obiektu z uwzględnieniem zasad opisanych w punkcie 3.2 „Odbiór wstępny robot"