Załącznik nr 2

Znak sprawy: ***DWOMP.V.221.01.2020.ZP***

OPIS PRZEDMIOTU ZAMÓWIENIA

na modernizację sieci teleinformatycznych w ramach projektu pn. „Rozbudowa istniejącej infrastruktury informatycznej oraz wdrożenie e-usług w Dolnośląskim Wojewódzkim Ośrodku Medycyny Pracy DWOMP i u Partnerów”

1. Modernizacja sieci teleinformatycznych w zakresie infrastruktury LAN

Przedmiot i zakres prac.
Wykonawca wykona projekt przebudowy instalacji teleinformatycznej w budynkach DWOMP i u Partnerów

A. Wymagania dla lokalizacji WROCŁAW (kat.6a)

Podstawą do opracowania zagadnień związanych z okablowaniem strukturalnym są normy okablowania strukturalnego.

Normy europejskie dotyczące okablowania strukturalnego – wymagań ogólnych i specyficznych dla danego środowiska:

- *ISO/IEC11801:2011 - Information technology - Generic cabling for customer premises*
- *PN-EN 50173-1:2011 Technika Informatyczna – Systemy okablowania strukturalnego - Część 1: Wymagania ogólne*
- *PN-EN 50173-2:2008/A1:2011E Technika Informatyczna – Systemy okablowania strukturalnego - Część 2: Budynki biurowe;*

Normy europejskie pomocnicze - w zakresie instalacji:

- *PN-EN 50174-1:2010/A1:2011E Technika informatyczna. Instalacja okablowania - Część 1 - Specyfikacja i zapewnienie jakości;*
- *PN-EN 50174-2:2010/A1:2011E Technika informatyczna. Instalacja okablowania -Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków;*
- *PN-EN 50174-3:2014-02 Technika informatyczna. Instalacja okablowania -Część 3 - Planowanie i wykonawstwo instalacji na zewnątrz budynków;*
- *PN-EN 50346:2004/A2:2010P Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania*
- *PN-EN 50310:2016-09 Sieci połączeń wyrównawczych w budynkach i innych obiektach budowlanych z instalacjami telekomunikacyjnymi*

W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy.

Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami norm obowiązujących w czasie realizacji zadania, przy uwzględnieniu wszystkich wymagań opisanych w dokumentacji projektowej a zdefiniowane przez dokumenty wskazane powyżej.

System okablowania oraz wydajność komponentów na etapie oddania instalacji do użytku musi pozostać w zgodzie z wymaganiami norm PN-EN50173-1:2011 i ISO/IEC11801:2011.

1. ZAŁOŻENIA OGÓLNE DLA OKABLOWANIA STRUKTURALNEGO

1.1 Struktura okablowania

System okablowania strukturalnego składać się będzie z trzech sektorów zgodnych z normą europejską EN50173-1:
1. Okablowanie szkieletowe (pionowe),
2. Okablowanie poziome,
3. Okablowanie obszaru roboczego.

Na potrzeby niniejszego opracowania, przyjęto oznaczenia:

- GPD – Główny punkt dystrybucyjny, szafa 19” wyposażona w elementy pasywne i aktywne systemu okablowania strukturalnego, będąca centralnym punktem sieci okablowania strukturalnego.
- PPD – Pośredni punkt dystrybucyjny, szafa 19” obsługująca dany obszar roboczy, w której znajdują się elementy aktywne i pasywne systemu okablowania strukturalnego. Od PPD rozchodzi się instalacja okablowania poziomego do punktów logicznych.
- PL3 – Punkt logiczny, zakończenie okablowania poziomego w postaci 3 złączy RJ45, będące punktem przyłączeniowym dla urządzeń końcowych.
- PL2 - Punkt logiczny, zakończenie okablowania poziomego w postaci 2 złączy RJ45, będące punktem przyłączeniowym dla urządzeń końcowych.
- T, - Punkt logiczny, zakończenie okablowania poziomego w postaci 1 złącza RJ45, będące punktem przyłączeniowym dla urządzeń końcowych.
- AP, K - Punkt logiczny, zakończenie okablowania poziomego w postaci 1 złącza RJ45, będące punktem przyłączeniowym dla urządzeń końcowych - podłączony do osobnego panela krosowego w PPD.

W celu łatwego zarządzania okablowaniem strukturalnym każdy moduł RJ45 w punkcie logicznym musi posiadać oznaczanie jednoznacznie je identyfikujące. Wykonawca oznaczy gniazda logiczne sieci komputerowej wg poniższego schematu:
A/B/C, gdzie:
A – numer szafy dystrybucyjnej,
B – numer panelu w szafie,
C – numer portu w panelu.
Przykład: GPD/1/1-2

Punkty logiczne PL (gniazda przyłączeniowe użytkowników) należy zorganizować w postaci modułów RJ45 keystone montowanych w adapterze z tworzywa sztucznego o wymiarach 45x45mm (format Mosaic). Ten uniwersalny standard montażowy zapewni organizację punktów logicznych w zależności od potrzeb - w formie natynkowej.

1.2 Graniczne długości

Długość łącza stałego (permanent link) okablowania strukturalnego, tj. odległość pomiędzy złączem RJ45 w PL a złączem RJ45 w patchpanelu po stronie punktu dystrybucyjnego, nie może przekroczyć 90 metrów. Kabel przyłączeniowy od PL do urządzenia końcowego, nie może przekroczyć długości 5 metrów. Podobnie kabel krosowy w punkcie dystrybucyjnym, pomiędzy patchpanelem a urządzeniem aktywnym, nie może przekroczyć długości 5 metrów. Całość łącza z okablowaniem szafowym oraz okablowaniem obszaru

roboczego, czyli kanał (channel), nie może w sumie przekroczyć 100 metrów. Wykonawca tak zaprojektuje rozmieszczenie pośrednich punktów dystrybucyjnych, aby powyższe odległości zostały zachowane dla każdego punktu logicznego.

1.3 Funkcje okablowania

Sieć strukturalna pełnić będzie funkcję okablowania dla potrzeb:

- instalacji telefonicznej (np. VoIP, ISDN),
- sieci LAN dla potrzeb administracyjnych,
- okablowania dla potrzeb instalacji teletechnicznych (np. CCTV, SSWiN, KD, IPTV).

1.4 Wymagania dotyczące okablowania strukturalnego

Wymagania i główne założenia dotyczące systemu okablowania strukturalnego:

- Zastosowane rozwiązanie ma pochodzić od jednego dostawcy systemu okablowania strukturalnego i ma być objęte jednolitą i spójną gwarancją na okres minimum 25 lat obejmując wszystkie elementy pasywne toru transmisyjnego.
- Wymaga się, aby 25-letnia gwarancja była standardowym elementem oferowanego systemu i nie może być oferowana „specjalnie dla tej inwestycji" przez wykonawcę, dostawcę, dystrybutora, a nawet przez producenta.
- Wszystkie podsystemy, tj. system okablowania logicznego i telefonicznego muszą być opracowane (tj. zaprojektowane, wykonane i wdrożone do oferty rynkowej) przez producenta jako kompletne rozwiązania, celem uzyskania maksymalnych zapasów transmisyjnych (marginesów pracy). Niedopuszczalne jest stosowanie rozwiązań składanych „Mix&Match" od różnych dostawców komponentów (różne źródła dostaw kabli, modułów gniazd RJ45, paneli, kabli krosowych, itd).
- Wszystkie komponenty systemu okablowania mają być zgodne z wymaganiami obowiązujących norm wg.:

  - ISO/IEC 11801,
  - EN 50173-1,
  - ANSI/TIA/EIA 568-C.2

- Lokalizacja gniazd oraz punktów dystrybucyjnych zostanie ustalona na podstawie wizji lokalnej i orientacyjnej lokalizacji umieszczonej na planach załączonych do postępowania. (podane dane są orientacyjne i zamawiający nie bierze odpowiedzialności za ich prawidłowe wyliczenie)
- Instalacja teletechniczna wykonana będzie jako ekranowana sieć okablowania strukturalnego klasy EA (komponenty minimum kategorii 6A), poprowadzona kablem o paśmie przenoszenia minimum 700MHz. Konstrukcja kabla pozwala osiągnąć wysokie parametry transmisyjne, oraz zmniejszyć przesłuchy NEXT i PSNEXT oraz zmniejszenie przesłuchów obcych Alien Crosstalk. Kabel musi spełniać wymagania stawiane komponentom przez najnowsze normy.

2. SZCZEGÓŁOWY OPIS ZAPROJEKTOWANYCH KOMPONENTÓW OKABLOWANIA STRUKTURALNEGO

2.1 Specyfikacja komponentów dla połączeń szkieletowych

Dla okablowania szkieletowego projektuje się 19” przełącznicę światłowodową wyposażoną w panel krosowy z adapterami SC simplex/MTRJ/E2000/LC duplex (umożliwiający wykonanie do 24 spawów włókien światłowodowych w 1U przestrzeni w szafie rack) lub SC duplex/LC quad (umożliwiający wykonanie do 96 spawów włókien światłowodowych w 1U przestrzeni w szafie rack). Każdy panel światłowodowy musi być wykonany z wysokiej jakości stali o grubości 2 mm zapewniającej wysoką wytrzymałość I sztywność urządzenia. Wymaga się, aby szuflada przełącznicy wraz z polem krosowym mogła swobodnie się wysuwać na prowadnicach kulkowych oraz pozostawać w stanie blokady dzięki znajdującym sie z przodu panela elementom zwalniającym. Zastosowanie powyższych rozwiązań gwarantuje wysoki komfort pracy zarówno w czasie instalacji, jak i przy ewentualnych pracach serwisowych. Wymaga się, aby każdy panel światłowodowy posiadał w standardzie zestaw uchwytów montażowych oraz dławic.

Połączenia szkieletowe pomiędzy przełącznicami światłowodowymi umieszczonymi w GPD i PPD należy wykonać w oparciu o uniwersalny jednomodowy kabel światłowodowy z luźną tubą. Kabel światłowodowy musi posiadać jednomodowe włókna 9/125 µm spełniające wymagania standardu G.652.D. Musi charakteryzować się niskim pikiem wodnym (ang. low water peak fiber) i wydajnością transmisyjną OS2. Konstrukcja kabla musi opierać się na luźnej tubie wypełnionej ochronnym żelem amortyzującym (niekapiącym i wolnym od silikonu), zawierającej 4, 6, 8, 12, 24 lub 48 włókna światłowodowe 9/125µm w pokryciu zewnętrznym 250µm. W celu łatwej identyfikacji włókna światłowodowe mają być oznaczone przez producenta na całej długości różnymi kolorami.
Osłona zewnętrzna zaprojektowanego kabla światłowodowego ma być uniepalniona, bezhalogenowa i o niskiej emisji dymu LSOH (ang. Low Smoke Zero Halogen). Ponadto tuba od zewnątrz musi być opleciona elementem wzmacniającym z wodoszczelnych włókien szklanych E-Glass, co gwarantuje zwiększenie odporności kabla na działanie sił zewnętrznych tj. rozciąganie, uderzenie, ściskanie i skręcanie. Projektowany kabel światłowodowy musi spełniać wymagania obowiązującej dyrektywy CPR (Construction Products Directive) opierającej się na zharmonizowanej normie europejskiej EN 50575:2014. Kabel światłowodowy musi charakteryzować się klasą reakcji na ogień: Dca s2 d2 a2 (światłowody od 4-24 włókien) oraz Eca (światłowód 48 włóknowy) wg specyfikacji technicznej EN13501-6. Klasyfikacja ogniowa musi być potwierdzona odpowiednią deklaracją właściwości użytkowych (ang. DoP – Declaration of Performance). Ponadto wymaga się, aby powłoka projektowanego kabla była oznaczona odpowiednim znakiem CE.

2.2 Specyfikacja kabla instalacyjnego

Specyfikacja Kabla F/FTP kat. 6A/7 700 MHz
Do wykonania instalacji należy zastosować kabel kat. 6A o konstrukcji F/FTP (kabel ekranowany z indywidualnym ekranem z folii aluminiowej dla każdej z par oraz wspólnym ekranem z folii aluminiowej dla całego kabla). Minimalne wymagania elementów okablowania strukturalnego to Kategoria 6A (komponenty) /Klasa EA (wydajność całego systemu).

- EN 50173-1:2018
- EN 50173-2:2018
- IEC 61156-5:2012 (Ed. 2.1)
- TIA-568.2-D:2018
- EN 50288-11-1:2012
- ISO/IEC 11801-1:2017 (Ed. 1.0)
- ISO/IEC 11801-2:2017 (Ed. 1.0)

Zgodność kabla instalacyjnego z powyższymi normami musi zostać potwierdzona certyfikatem niezależnego laboratorium badawczego (np. Force Technology).

Do każdego portu RJ45 punktu logicznego należy doprowadzić kabel skrętkowy 4-parowy, który należy rozprowadzić zgodnie z trasami pokazanymi na planach (podkładach budowlanych) .Każdy kabel skrętkowy, 4-parowy należy zakończyć na pojedynczym module RJ45 (gnieździe RJ45). Nie dopuszcza się rozdziału jednego kabla 4-parowego na większą ilość portów (nie dopuszcza się wkładek i przejściówek rozdzielających). Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 7,2mm. Nie dopuszcza się kabli o większej średnicy zewnętrznej. Kabel ten ma zapewniać pozytywne parametry transmisyjne w całym paśmie minimum 700MHz. Projektowany kabel musi posiadać zewnętrzną powłokę LSOH nie wydzielającą szkodliwych toksyn podczas spalania. W celu odróżnienia kabli okablowania strukturalnego od kabli innych instalacji teletechnicznych powłoka kabla ma posiadać kolor zielony. Wymaga się, aby kabel posiadał euroklasę Dca s1,d1,a1 zgodnie z dyrektywą CPR.

Cechy kabla:

- Konstrukcja F/FTP
- Powłoka bezhalogenowa w kolorze zielonym.
- Zgodny z kategorią 6A/7
- Znacznik długości od 500 do 0, co 1m.
- Testowany do 700 MHz
- Powłoka zewnętrzna: LSOH
- Średnica zewnętrzna: 7,0mm(±0,2mm)
- Temperatura podczas układania: -10ºC do +50ºC
- Temperatura podczas pracy: -30ºC do +70ºC
- Średnica przewodnika: 23 AWG
- Euroklasa Dca- s1a,d1,a1

Kabel powinien posiadać ekran wspólny dla wszystkich par w postaci folii poliestrowej pokrytej warstwą aluminium, ułożonej warstwą przewodzącą do wewnątrz. Podczas instalacji należy pamiętać o odpowiednich promieniach gięcia kabla. Instalacja ze zbyt małym promieniem gięcia kabla może doprowadzić do pogorszenia właściwości transmisyjnych w torze.
Należy zastosować kabel F/FTP w celu zapewnienia wysokich właściwości transmisyjnych. Ekran z folii umieszczony na każdej z par zabezpiecza przed przesłuchami wewnątrz kabla, zaś folia umieszczona na wszystkich parach dodatkowo zabezpiecza przed niepożądanymi zewnętrznymi zakłóceniami działającymi na kabel. Taka konstrukcja kabla zapewnia optymalne zabezpieczenie przed skutkami oddziaływań pola elektromagnetycznego na kabel, przez co bardzo szybka transmisja realizowana takim kablem zapewnia poprawność przesyłania danych nawet na bardzo długich torach kablowych.

2.3 Specyfikacja panelu krosowego

Kable należy zakończyć na panelach modularnych.
Panele rozdzielcze powinny umożliwiać wpinanie 24 modułów RJ45 typu keystone, takich samych jak w gniazdach abonenckich. Panel powinien posiadać 24 porty i wysokość 1U. Panel musi posiadać zintegrowaną prowadnicę kabli przychodzących, co zapewni swobodne uchwycenie kabli i eliminacje naprężeń związanych z wagą doprowadzonych kabli. Ponad to panel musi być oznaczony logo wybranego producenta.

2.4 Specyfikacja modułu RJ45

Gniazda abonenckie wykonać w oparciu o ekranowane moduły typu keystone kategorii 6A mocowane w odpowiednich adapterach dopasowanych do osprzętu elektroinstalacyjnego.

Moduł musi spełniać wymagania kategorii 6A (klasy EA) wg poniższych norm:
- EN 50173-1:2018
- EN 50173-2:2018
- IEC 60603-7-41:2010
- TIA-568.2-D:2018
- IEC 60512-99-002:2019
- ISO/IEC 11801-1:2017 (Ed. 1.0)
- ISO/IEC 11801-2:2017 (Ed. 1.0)

Zgodność modułu RJ45 z powyższymi normami musi zostać potwierdzona certyfikatem niezależnego laboratorium badawczego (np. Force Technology).

Dopuszcza się stosowanie tylko modułów ekranowanych, co jest następstwem zastosowania kabla ekranowanego, w celu zapobiegania negatywnym skutkom oddziaływania zewnętrznych pól elektromagnetycznych. Należy użyć modułów beznarzędziowych w celu zapewnienia powtarzalności parametrów połączeniowych. Beznarzędziowa metoda zarabiania modułów pozwala na wykonanie połączeń w szybki sposób, bez potrzeby używania specjalistycznych narzędzi i gwarantując rozszycie kabla na module w sposób całkowicie zgodny z zaleceniem producenta.

Moduł musi także wspierać funkcję Power over Ethernet. Moduł musi być zgodny ze standardem Keystone. Złącza IDC modułów powinny mieć możliwość podłączenia żył o AWG 22-26. Niezbędnym elementem każdego modułu jest plastikowa zaślepka montowana bezpośrednio na module (nie w gnieździe) w celu zabezpieczenia przed zabrudzeniami które mogą spowodować pogorszenie parametrów transmisyjnych modułu. Moduł powinien posiadać oznaczenia kolorystyczne ułatwiające przyłączenie kabla w sekwencji 568B lub 568A

2.5 Specyfikacja punktów dystrybucyjnych

Dla Głównego Punktu Dystrybucyjnego należy dostarczyć 2 szafy stojące RACK 19” o wysokości 42U i głębokości 1000mm, przeznaczone do montażu osprzętu pasywnego jak i aktywnego. Szafa musi charakteryzować się wytrzymałą, skręcaną konstrukcją, która umożliwia demontaż szafy i instalację jej w trudno dostępnych pomieszczeniach. Demontaż szafy musi być możliwy bez specjalistycznych narzędzi. Szafa musi mieć możliwość demontażu lub zamiany kierunku otwarcia drzwi. Wymagane jest aby osłony boczne były pełne, zdejmowane za pomocą zamków z kluczem i posiadały otwory perforacji w górnej części.
Szafa stojąca RACK 19” powinna posiadać 4 belki montażowe 19” z numeracją wysokości użytkowej „U” oraz regulacją głębokości. Przepusty kablowe w dachu i podłodze muszą mieć możliwość zastosowania szczotek lub filtrów przeciwpyłowych w celu zabezpieczenia wiązek kablowych i ochrony przed dostawaniem się kurzu do wnętrza szafy. Wymaga się malowania proszkowego szaf w kolorze RAL 7035 (szary) lub RAL 9005 (czarny). Szafa musi być wyposażona w cokół o wysokości 100 mm z przepustem szczotkowym do wprowadzenia kabli w tylnej ściance cokołu. Szafa musi posiadać w komplecie zestaw linek uziemiających.

Tabelaryczne zestawienie parametrów technicznych dla szafy: 800x1000mm

Wymiary	800x1000mm, 42U
Nośność	Min 1000kg
Rodzaj drzwi przednich	Przeszklone w metalowej ramie z metalowym uchwytem wychylnym
Rodzaj drzwi tylnych	Perforacja 75% - jednoskrzydłowe
Kąt otwarcia drzwi	180°
Cokół	100mm z przepustem szczotkowym w tylnej ścianie
Podstawa	Wyposażona w zestaw filtracyjny z przepustem szczotkowym do wprowadzenia kabli
Belki nośne 19”	Wykonane z profili o grubości 2mm z numeracją jednostek użytkowych oraz płynną regulacją ustawienia głębokości
Uziemienie	Zestaw linek uziemiających prowadzących do każdego elementu szafy
Kolor	RAL 7035 (szary)
Osłony boczne	Każda osłona boczna wyposażona w dwa zamki zamykane na klucz. Perforacja w górnej części

Dla Pośrednich Punktów dystrybucyjnych należy dostarczyć szafy wiszące RACK 19” o wysokości 16U, przeznaczone do montażu okablowania. Szafa ma mieć konstrukcję skręcaną i być dostępna w wersji zmontowanej bądź do samodzielnego montażu. Szafa musi być wyposażona w podwójny stelaż 19” (z przodu i z tyłu). Wymagana nośność szafy to minimum 60kg. Aby zapewnić elastyczność instalacji wymaga się aby szafa posiadała możliwość wyprowadzenia kabli z góry z dołu i od tyłu, zdejmowane osłony boczne, zamykane na zamek. W celu zapewnienia właściwej sztywności szafy i stabilności montażu szafa musi posiadać ścianę tylną. Szafa powinna możliwość zmiany strony mocowania drzwi. Ponad to szafa powinna być wyposażona w dedykowany panel wentylacyjny dachowy, 2 wentylatorowy.

3. GWARANCJA

Całość rozwiązania ma być objęta jednolitą, spójną 25-letnią gwarancją systemową producenta. Gwarancja musi być udzielona klientowi końcowemu bezpośrednio przez producenta, a nie od dystrybutora okablowania.

Gwarancja systemowa ma obejmować:

- gwarancję systemową (Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź 25-letniej eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione)
- gwarancję parametrów łącza/kanału (Producent zagwarantuje, że łącze stałe bądź kanał transmisyjny

zbudowany z jego komponentów prze okres 25 lat będzie charakteryzował się parametrami transmisyjnymi przewyższającymi wymogi stawiane przez normę ISO/IEC 11801:2002/Am2: 2010 dla okablowania klasy EA)

- gwarancję aplikacji (Producent zagwarantuje, że na jego systemie okablowania przez okres 25 lat będą pracowały dowolne aplikacje (współczesne i stworzone w przyszłości), które zaprojektowane były (lub będą) dla systemów okablowania klasy EA (w rozumieniu normy ISO/IEC 118012nd edition:2010)

4. TESTY KOŃCOWE

Po zakończeniu prac instalację należy poddać pomiarom i badaniom sprawdzającym.
Wykonawstwo pomiarów powinno być zgodne z normą PN-EN 50346:2004/A1+A2:2009. Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą PN-EN 14763-3:2009/A1:2010. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

Należy użyć miernika dynamicznego (analizatora), który posiada aktualny certyfikat potwierdzający dokładność jego wskazań.

Analizator okablowania wykorzystany do pomiarów musi charakteryzować się przynajmniej IV klasą dokładności wg IEC 61935-1/Ed. 3 (proponowane urządzenia to np. FLUKE DSX 5000).

W przypadku sieci miedzianej pomiary należy wykonać w konfiguracji pomiarowej łącza stałego (ang. „Permanent Link") – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego.
W przypadku sieci miedzianej pomiary należy wykonać w konfiguracji pomiarowej kanału razem z kablami krosowymi (ang. „channel") – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego. Kable krosowe, które zostały użyte do przeprowadzenia pomiarów należy przekazać inwestorowi.
Wymagane parametry testu dla kabli miedzianych:

- Wire Map – mapa połączeń,
- Length – długość,
- Propagation delay – opóźnienie propagacji,
- Delay skew – opóźnienie skrośne,
- NEXT – near end cross-talk,
- PSNEXT – Power sum next,
- ACR – attenuation to crosstalk ratio,
- PSACR – Power sum ACR,
- ELFEXT,
- PSELFEXT,
- Insertion loss – straty wtrąceniowe,
- Return loss – straty odbiciowe.

Okablowanie światłowodowe testować zgodnie z wymaganiami dla przewodów optycznych:

- test tłumienności i parametru Return loss zestawem OCTS o dokładności +/- 0.2dB lub lepszej z dwóch stron każdego kabla, w dwóch oknach optycznych 850nm i 1300nm,
- pomiar reflektometrem optycznym (OTDR) kabli szkieletowych,

Uwaga:

Testy końcowe powinny być wykonywane tylko po faktycznym ukończeniu realizacji. Nie należy akceptować żadnych wyników mieszczących się w marginesie błędu. Wyniki testów należy przekazać Inwestorowi przed wykonaniem weryfikacji końcowej systemu.

5. ZALECENIA INSTALACYJNE

- Trasy kablowe - pionowe należy wykonać z trwałych elementów (drabinek) umożliwiających przymocowanie kabli oraz zachowanie odpowiednich promieni gięcia kabli na zakrętach. Rozmiary (pojemność) kanałów kablowych należy dobrać uwzględniając maksymalną liczbę kabli zaprojektowanych w danym miejscu instalacji przy uwzględnieniu co najmniej 20% wolnej przestrzeni na potrzeby ewentualnej rozbudowy systemu. Zajętość światła kanałów kablowych przez kable obliczono w miejscach zakrętów – dla maksymalnej znamionowej średnicy kabla - przy całkowitym wypełnieniu światła kanału kablami na zakręcie, kanał będzie wówczas na prostym odcinku wypełniony w 40%. Przy realizacji tras kablowych pod potrzeby okablowania należy wziąć pod uwagę wymagania normy PN-EN 50174-2:2010/A1:2011 dotyczące równoległego prowadzenia różnych instalacji w budynku, m.in. instalacji zasilającej i zapewnić odpowiednie odległości pomiędzy okablowaniem.
- Maksymalna długość kabla instalacyjnego skrętkowego (od punktu dystrybucyjnego do gniazda końcowego) nie może w żadnym przypadku przekroczyć 90 metrów.
- Okablowanie powinno być ciągłe na całej długości toru bez złącz i spawów od stanowiska roboczego do panelu rozdzielczego.
- Wszystkie cztery pary każdego kabla powinny być zakończone w pojedynczym module.
- Wymaga się standardowej sekwencji połączeń T568A lub T568B.
- Proces montażu ma gwarantować najwyższą powtarzalność. Maksymalny rozplot pary transmisyjnej na złączu modularnym RJ45 nie może być większy niż 6 mm.
- Każdy kabel powinien mieć trwałe oznaczenie na dwóch końcach przy zakończonych modułach wg przyjętego systemu numeracji.
- Wszystkie ekrany kabli telekomunikacyjnych i transmisji danych oraz związane z nimi urządzenia powinny być poprawnie uziemione w punktach dystrybucyjnych zgodnie z wymaganiami odnośnych norm.
- Każdy stelaż szafy powinien być podłączony do listwy uziemiającej zgodnie z wymogami norm.
- Odpowiednie bariery ogniowe powinny być zastosowane dla kabli przechodzących przez ściany i przegrody stanowiące rozdzielnie stref ogniowych budynku. Nieużywane szachty i piony technologiczne powinny być zabezpieczone przed przenikaniem ognia.
- Wszystkie instalowane kable powinny być poprawnie umieszczone w rurkach kablowych, na drabinkach kablowych, w rynienkach lub w kanałach instalacyjnych. Jeśli zastosowanie elementów ochronnych dla medium transmisyjnego jest niemożliwe, pojedyncze kable mogą być formowane w wiązki, starannie prowadzone, poprawnie osłonięte, przymocowane i zabezpieczone za pomocą opasek kablowych do konstrukcji nośnej budynku.
- Okablowanie powinno być prowadzone w sposób uporządkowany i zgodnie z wytycznymi producenta. Wszystkie używane opaski kablowe powinny być rzepowe i ręcznie zaciskane tylko w punktach gdzie nie ma zagięć i skręceń.
- Jeśli używana jest rurka osłonowa, maksymalna liczba zagięć większych niż 90º między punktami przeciągania nie powinna przekraczać 2.
- Wszystkie kable światłowodowe i miedziane powinny być instalowane i mocowane zgodnie z wytycznymi producenta. Podczas układania kabli instalator powinien dbać o to, aby kabel nie był narażony na nacisk i zagięcia.
- Po instalacji kabla, instalator powinien się upewnić, że wszystkie części kabla są prawidłowo zamocowane i nie ma żadnych naprężeń wzdłuż drogi prowadzenia kabla i na jego końcach.
- Szczególną uwagę należy zachować przy układaniu kabli kat.6A i światłowodowych, aby zachować ich promień gięcia zgodnie z wytycznymi producenta kabli. Kable kategorii 6A nie powinny mieć mniejszego promienia zgięcia niż 8x średnica kabla podczas instalacji i 4x średnica kabla podczas eksploatacji, kable światłowodowe nie powinny mieć promienia mniejszego niż 10x jego średnica.

B. Wymagania dla lokalizacji Lubin, Jelenia Góra, Wałbrzych (kat.5e)

Podstawą do opracowania zagadnień związanych z okablowaniem strukturalnym są normy okablowania strukturalnego.

Normy europejskie dotyczące okablowania strukturalnego – wymagań ogólnych i specyficznych dla danego środowiska:

- *ISO/IEC11801:2011 - Information technology - Generic cabling for customer premises*
- *PN-EN 50173-1:2011 Technika Informatyczna – Systemy okablowania strukturalnego - Część 1: Wymagania ogólne*
- *PN-EN 50173-2:2008/A1:2011E Technika Informatyczna – Systemy okablowania strukturalnego - Część 2: Budynki biurowe;*

Normy europejskie pomocnicze - w zakresie instalacji:

- *PN-EN 50174-1:2010/A1:2011E Technika informatyczna. Instalacja okablowania - Część 1 - Specyfikacja i zapewnienie jakości;*
- *PN-EN 50174-2:2010/A1:2011E Technika informatyczna. Instalacja okablowania -Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków;*
- *PN-EN 50174-3:2014-02 Technika informatyczna. Instalacja okablowania -Część 3 - Planowanie i wykonawstwo instalacji na zewnątrz budynków;*
- *PN-EN 50346:2004/A2:2010P Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania*
- *PN-EN 50310:2016-09 Sieci połączeń wyrównawczych w budynkach i innych obiektach budowlanych z instalacjami telekomunikacyjnymi*

W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy.

Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami norm obowiązujących w czasie realizacji zadania, przy uwzględnieniu wszystkich wymagań opisanych w dokumentacji projektowej a zdefiniowane przez dokumenty wskazane powyżej.

System okablowania oraz wydajność komponentów na etapie oddania instalacji do użytku musi pozostać w zgodzie z wymaganiami norm PN-EN50173-1:2011 i ISO/IEC11801:2011.

1. ZAŁOŻENIA OGÓLNE DLA OKABLOWANIA STRUKTURALNEGO

1.1 Struktura okablowania

System okablowania strukturalnego składać się będzie z trzech sektorów zgodnych z normą europejską EN50173-1:
1. Okablowanie poziome,
2. Okablowanie obszaru roboczego.

Na potrzeby niniejszego opracowania, przyjęto oznaczenia:

- GPD – Główny punkt dystrybucyjny, szafa 19” wyposażona w elementy pasywne i aktywne systemu okablowania strukturalnego, będąca centralnym punktem sieci okablowania strukturalnego.
- PL3 – Punkt logiczny, zakończenie okablowania poziomego w postaci 3 złączy RJ45, będące punktem przyłączeniowym dla urządzeń końcowych.
- PL2 – Punkt logiczny, zakończenie okablowania poziomego w postaci 2 złączy RJ45, będące punktem przyłączeniowym dla urządzeń końcowych.
- T, - Punkt logiczny, zakończenie okablowania poziomego w postaci 1 złącza RJ45, będące punktem przyłączeniowym dla urządzeń końcowych.
- AP, K - Punkt logiczny, zakończenie okablowania poziomego w postaci 1 złącza RJ45, będące punktem przyłączeniowym dla urządzeń końcowych - podłączony do osobnego panela krosowego w PPD.

W celu łatwego zarządzania okablowaniem strukturalnym każdy moduł RJ45 w punkcie logicznym musi posiadać oznaczanie jednoznacznie je identyfikujące. Projektuje się numerację gniazd logicznych sieci komputerowej wg poniższego schematu:
A/B/C, gdzie:
A – numer szafy dystrybucyjnej,
B – numer panelu w szafie,
C – numer portu w panelu.
Przykład: GPD/1/1-2

Punkty logiczne PL (gniazda przyłączeniowe użytkowników) należy zorganizować w postaci modułów RJ45 keystone montowanych w adapterze z tworzywa sztucznego o wymiarach 45x45mm (format Mosaic). Ten uniwersalny standard montażowy zapewni organizację punktów logicznych w zależności od potrzeb - w formie natynkowej.

1.2 Graniczne długości

Długość łącza stałego (permanent link) okablowania strukturalnego, tj. odległość pomiędzy złączem RJ45 w PL a złączem RJ45 w patchpanelu po stronie punktu dystrybucyjnego, nie może przekroczyć 90 metrów. Kabel przyłączeniowy od PL do urządzenia końcowego, nie może przekroczyć długości 5 metrów. Podobnie kabel krosowy w punkcie dystrybucyjnym, pomiędzy patchpanelem a urządzeniem aktywnym, nie może przekroczyć długości 5 metrów. Całość łącza z okablowaniem szafowym oraz okablowaniem obszaru roboczego, czyli kanał (channel), nie może w sumie przekroczyć 100 metrów. Wykonawca tak zaprojektuje rozmieszczenie pośrednich punktów dystrybucyjnych, aby powyższe odległości zostały zachowane dla

każdego punktu logicznego.

1.3 Funkcje okablowania

Sieć strukturalna pełnić będzie funkcję okablowania dla potrzeb:

- instalacji telefonicznej (np. VoIP, ISDN),
- sieci LAN dla potrzeb administracyjnych,
- okablowania dla potrzeb instalacji teletechnicznych (np. CCTV, SSWiN, KD, IPTV).

1.4 Wymagania dotyczące okablowania strukturalnego

Wymagania i główne założenia dotyczące systemu okablowania strukturalnego:

- Zastosowane rozwiązanie ma pochodzić od jednego dostawcy systemu okablowania strukturalnego i ma być objęte jednolitą i spójną gwarancją na okres minimum 25 lat obejmując wszystkie elementy pasywne toru transmisyjnego.
- Wymaga się, aby 25-letnia gwarancja była standardowym elementem oferowanego systemu i nie może być oferowana „specjalnie dla tej inwestycji" przez wykonawcę, dostawcę, dystrybutora, a nawet przez producenta.
- Wszystkie podsystemy, tj. system okablowania logicznego i telefonicznego muszą być opracowane (tj. zaprojektowane, wykonane i wdrożone do oferty rynkowej) przez producenta jako kompletne rozwiązania, celem uzyskania maksymalnych zapasów transmisyjnych (marginesów pracy). Niedopuszczalne jest stosowanie rozwiązań składanych „Mix&Match" od różnych dostawców komponentów (różne źródła dostaw kabli, modułów gniazd RJ45, paneli, kabli krosowych, itd).
- Wszystkie komponenty systemu okablowania mają być zgodne z wymaganiami obowiązujących norm wg.:

  - ISO/IEC 11801,
  - EN 50173-1,
  - ANSI/TIA/EIA 568-C.2 .

- Lokalizacja gniazd oraz punktów dystrybucyjnych zostanie ustalona na podstawie wizji lokalnej i orientacyjnej lokalizacji umieszczonej na planach załączonych do postępowania. (podane dane są orientacyjne i zamawiający nie bierze odpowiedzialności za ich prawidłowe wyliczenie).
- W obiekcie projektuje się instalację teletechniczną, która wykonana będzie jako nieekranowana sieć okablowania strukturalnego klasy D (komponenty minimum kategorii 5e), poprowadzona kablem o paśmie przenoszenia minimum 200MHz. Konstrukcja kabla pozwala osiągnąć wysokie parametry transmisyjne, oraz zmniejszyć przesłuchy NEXT i PSNEXT oraz zmniejszenie przesłuchów obcych Alien Crosstalk. Kabel musi spełniać wymagania stawiane komponentom przez najnowsze normy.

2. SZCZEGÓŁOWY OPIS ZAPROJEKTOWANYCH KOMPONENTÓW OKABLOWANIA STRUKTURALNEGO

2.1 Specyfikacja kabla instalacyjnego

Specyfikacja kabla U/UTP kat. 5e LSOH 200 MHz
Do wykonania instalacji należy zastosować kabel kat. 5e o konstrukcji U/UTP (kabel nieekranowany)5e o konstrukcji U/UTP (kabel nieekranowany). Minimalne wymagania elementów okablowania strukturalnego to Kategoria 5e (komponenty) /Klasa D (wydajność całego systemu).

- EN 50173-1:2018-07
- ISO/IEC 11801 Edition 2.2
- ANSI/TIA-568-C.0/C.1/C.2
- IEC 60754-2

Zgodność kabla instalacyjnego z powyższymi normami musi zostać potwierdzona certyfikatem niezależnego laboratorium badawczego (np. Force Technology).

Do każdego portu RJ45 punktu logicznego należy doprowadzić kabel skrętkowy 4-parowy, który należy rozprowadzić zgodnie z trasami pokazanymi na planach (podkładach budowlanych). Każdy kabel skrętkowy, 4-parowy należy zakończyć na pojedynczym module RJ45 (gnieździe RJ45). Nie dopuszcza się rozdziału jednego kabla 4-parowego na większą ilość portów (nie dopuszcza się wkładek i przejściówek rozdzielających). Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 4,8mm. Nie dopuszcza się kabli o większej średnicy zewnętrznej. Kabel ten ma zapewniać pozytywne parametry transmisyjne w całym paśmie minimum 200MHz. Projektowany kabel musi posiadać zewnętrzną powłokę LSOH nie wydzielającą szkodliwych toksyn podczas spalania. W celu odróżnienia kabli okablowania strukturalnego od kabli innych instalacji teletechnicznych powłoka kabla ma posiadać kolor fioletowy.
Wymaga się, aby kabel posiadał euroklasę Dca s2,d2, a1 zgodnie z dyrektywą CPR.

Cechy kabla:

- Konstrukcja U/UTP
- Powłoka bezhalogenowa w kolorze fioletowym.
- Zgodny z kategorią 5e
- Znacznik długości od 305 do 0, co 1m.
- Testowany do 200 MHz
- Powłoka zewnętrzna: LSOH
- Średnica zewnętrzna: 4,8 mm
- Średnica przewodnika: 23 AWG
- Euroklasa Dca- s2, d2, a1

Podczas instalacji należy pamiętać o odpowiednich promieniach gięcia kabla. Instalacja ze zbyt małym promieniem gięcia kabla może doprowadzić do pogorszenia właściwości transmisyjnych w torze.

2.2 Specyfikacja panelu krosowego

Kable należy zakończyć na panelach modularnych.
Panele rozdzielcze powinny umożliwiać wpinanie 24 modułów RJ45 typu keystone, takich samych jak w gniazdach abonenckich. Panel powinien posiadać 24 porty i wysokość 1U. Panel musi posiadać zintegrowaną prowadnicę kabli przychodzących, co zapewni swobodne uchwycenie kabli i eliminacje

naprężeń związanych z wagą doprowadzonych kabli. Ponad to panel musi być oznaczony logo wybranego producenta.

2.3 Specyfikacja modułu RJ45

Gniazda abonenckie wykonać w oparciu o nieekranowane moduły typu keystone kategorii 5e mocowane w odpowiednich adapterach dopasowanych do osprzętu elektroinstalacyjnego.

Moduł musi spełniać wymagania kategorii 5e (klasy D) wg poniższych norm:
- EN 50173-1:2018
- EN 50173-2:2018
- TIA-568.2-D:2018
- IEC 60512-99-002:2019
- ISO/IEC 11801-1:2017 (Ed. 1.0)
- ISO/IEC 11801-2:2017 (Ed. 1.0)

Zgodność kabla instalacyjnego z powyższymi normami musi zostać potwierdzona certyfikatem niezależnego laboratorium badawczego (np. Force Technology).

Należy użyć modułów zarabianych beznarzędziowo. Bezarzędziowa metoda zarabiania modułów pozwala na dokładne wykonanie połączeń, gwarantując rozszycie kabla na module w sposób całkowicie zgodny z zaleceniem producenta.. Maksymalny rozplot pary transmisyjnej nie może być większy niż 6mm od złącza.

Moduł musi być zgodny ze standardem Keystone. Złącza IDC modułów powinny mieć możliwość podłączenia żył o AWG 23-26. Moduł powinien posiadać oznaczenia kolorystyczne ułatwiające przyłączenie kabla w sekwencji 568B lub 568A.

2.4 Specyfikacja punktów dystrybucyjnych

Dla Pośrednich Punktów dystrybucyjnych należy dostarczyć szafy wiszące RACK 19” o wysokości 16U, przeznaczone do montażu okablowania. Szafa ma mieć konstrukcję skręcaną i być dostępna w wersji zmontowanej bądź do samodzielnego montażu. Szafa musi być wyposażona w podwójny stelaż 19” (z przodu i z tyłu). Wymagana nośność szafy to minimum 60kg. Aby zapewnić elastyczność instalacji wymaga się aby szafa posiadała możliwość wyprowadzenia kabli z góry z dołu i od tyłu, zdejmowane osłony boczne, zamykane na zamek. W celu zapewnienia właściwej sztywności szafy i stabilności montażu szafa musi posiadać ścianę tylną. Szafa powinna możliwość zmiany strony mocowania drzwi. Ponad to szafa powinna być wyposażona w dedykowany panel wentylacyjny dachowy, 2 wentylatorowy.

3. GWARANCJA

Całość rozwiązania ma być objęta jednolitą, spójną 25-letnią gwarancją systemową producenta. Gwarancja musi być udzielona klientowi końcowemu bezpośrednio przez producenta, a nie od dystrybutora okablowania.

Gwarancja systemowa ma obejmować:

- gwarancję systemową (Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji

bądź 25-letniej eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione)

- gwarancję parametrów łącza/kanału (Producent zagwarantuje, że łącze stałe bądź kanał transmisyjny zbudowany z jego komponentów prze okres 25 lat będzie charakteryzował się parametrami transmisyjnymi przewyższającymi wymogi stawiane przez normę ISO/IEC 11801:2002/Am2: 2010 dla okablowania klasy D)

- gwarancję aplikacji (Producent zagwarantuje, że na jego systemie okablowania przez okres 25 lat będą pracowały dowolne aplikacje (współczesne i stworzone w przyszłości), które zaprojektowane były (lub będą) dla systemów okablowania klasy D (w rozumieniu normy ISO/IEC 118012nd edition:2010)

4. TESTY KOŃCOWE

Po zakończeniu prac instalację należy poddać pomiarom i badaniom sprawdzającym.
Wykonawstwo pomiarów powinno być zgodne z normą PN-EN 50346:2004/A1+A2:2009. Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą PN-EN 14763-3:2009/A1:2010. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

Należy użyć miernika dynamicznego (analizatora), który posiada wgrane oprogramowanie umożliwiające pomiar parametrów według aktualnie obowiązujących norm. Sprzęt pomiarowy musi posiadać aktualny certyfikat potwierdzający dokładność jego wskazań.

Analizator okablowania wykorzystany do pomiarów musi charakteryzować się przynajmniej IV klasą dokładności wg IEC 61935-1/Ed. 3 (proponowane urządzenia to np. FLUKE DSX 5000).

W przypadku sieci miedzianej pomiary należy wykonać w konfiguracji pomiarowej łącza stałego (ang. „Permanent Link") – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego.
W przypadku sieci miedzianej pomiary należy wykonać w konfiguracji pomiarowej kanału razem z kablami krosowymi (ang. „channel") – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego. Kable krosowe, które zostały użyte do przeprowadzenia pomiarów należy przekazać inwestorowi.
Wymagane parametry testu dla kabli miedzianych:

- Wire Map – mapa połączeń,
- Length – długość,
- Propagation delay – opóźnienie propagacji,
- Delay skew – opóźnienie skrośne,
- NEXT – near end cross-talk,
- PSNEXT – Power sum next,
- ACR – attenuation to crosstalk ratio,
- PSACR – Power sum ACR,
- ELFEXT,
- PSELFEXT,
- Insertion loss – straty wtrąceniowe,
- Return loss – straty odbiciowe.

Okablowanie światłowodowe testować zgodnie z wymaganiami dla przewodów optycznych:

- test tłumienności i parametru Return loss zestawem OCTS o dokładności +/- 0.2dB lub lepszej z dwóch stron każdego kabla, w dwóch oknach optycznych 850nm i 1300nm,
- pomiar reflektometrem optycznym (OTDR) kabli szkieletowych,

Uwaga:
Testy końcowe powinny być wykonywane tylko po faktycznym ukończeniu realizacji. Nie należy akceptować żadnych wyników mieszczących się w marginesie błędu. Wyniki testów należy przekazać Inwestorowi przed wykonaniem weryfikacji końcowej systemu.

6. ZALECENIA INSTALACYJNE

- Trasy kablowe - pionowe należy wykonać z trwałych elementów (drabinek) umożliwiających przymocowanie kabli oraz zachowanie odpowiednich promieni gięcia kabli na zakrętach. Rozmiary (pojemność) kanałów kablowych należy dobrać uwzględniając maksymalną liczbę kabli zaprojektowanych w danym miejscu instalacji przy uwzględnieniu co najmniej 20% wolnej przestrzeni na potrzeby ewentualnej rozbudowy systemu. Zajętość światła kanałów kablowych przez kable obliczono w miejscach zakrętów – dla maksymalnej znamionowej średnicy kabla - przy całkowitym wypełnieniu światła kanału kablami na zakręcie, kanał będzie wówczas na prostym odcinku wypełniony w 40%. Przy realizacji tras kablowych pod potrzeby okablowania należy wziąć pod uwagę wymagania normy PN-EN 50174-2:2010/A1:2011 dotyczące równoległego prowadzenia różnych instalacji w budynku, m.in. instalacji zasilającej i zapewnić odpowiednie odległości pomiędzy okablowaniem.
- Maksymalna długość kabla instalacyjnego skrętkowego (od punktu dystrybucyjnego do gniazda końcowego) nie może w żadnym przypadku przekroczyć 90 metrów.
- Okablowanie powinno być ciągłe na całej długości toru bez złącz i spawów od stanowiska roboczego do panelu rozdzielczego.
- Wszystkie cztery pary każdego kabla powinny być zakończone w pojedynczym module.
- Wymaga się standardowej sekwencji połączeń T568A lub T568B.
- Proces montażu ma gwarantować najwyższą powtarzalność. Maksymalny rozplot pary transmisyjnej na złączu modularnym RJ45 nie może być większy niż 6 mm.
- Każdy kabel powinien mieć trwałe oznaczenie na dwóch końcach przy zakończonych modułach wg przyjętego systemu numeracji.
- Wszystkie ekrany kabli telekomunikacyjnych i transmisji danych oraz związane z nimi urządzenia powinny być poprawnie uziemione w punktach dystrybucyjnych zgodnie z wymaganiami odnośnych norm.
- Każdy stelaż szafy powinien być podłączony do listwy uziemiającej zgodnie z wymogami norm.
- Odpowiednie bariery ogniowe powinny być zastosowane dla kabli przechodzących przez ściany i przegrody stanowiące rozdzielnie stref ogniowych budynku. Nieużywane szachty i piony technologiczne powinny być zabezpieczone przed przenikaniem ognia.
- Wszystkie instalowane kable powinny być poprawnie umieszczone w rurkach kablowych, na drabinkach kablowych, w rynienkach lub w kanałach instalacyjnych. Jeśli zastosowanie elementów ochronnych dla medium transmisyjnego jest niemożliwe, pojedyncze kable mogą być formowane w wiązki, starannie prowadzone, poprawnie osłonięte, przymocowane i zabezpieczone za pomocą opasek kablowych do konstrukcji nośnej budynku.
- Okablowanie powinno być prowadzone w sposób uporządkowany i zgodnie z wytycznymi producenta. Wszystkie używane opaski kablowe powinny być rzepowe i ręcznie zaciskane tylko w punktach gdzie nie ma zagięć i skręceń.
- Jeśli używana jest rurka osłonowa, maksymalna liczba zagięć większych niż 90º między punktami przeciągania nie powinna przekraczać 2.
- Wszystkie kable światłowodowe i miedziane powinny być instalowane i mocowane zgodnie z wytycznymi producenta. Podczas układania kabli instalator powinien dbać o to, aby kabel nie był narażony na nacisk i zagięcia.
- Po instalacji kabla, instalator powinien się upewnić, że wszystkie części kabla są prawidłowo zamocowane i nie ma żadnych naprężeń wzdłuż drogi prowadzenia kabla i na jego końcach.

- Szczególną uwagę należy zachować przy układaniu kabli kat.5e i światłowodowych, aby zachować ich promień gięcia zgodnie z wytycznymi producenta kabli. Kable kategorii 5e nie powinny mieć mniejszego promienia zgięcia niż 8x średnica kabla podczas instalacji i 4x średnica kabla podczas eksploatacji, kable światłowodowe nie powinny mieć promienia mniejszego niż 10x jego średnica.

2. Dostawa, instalacja i konfiguracja urządzeń sieci aktywnej

W ramach postępowania Wykonawca ma dostarczyć wymienione niżej urządzenia.

Lokalizacja Wrocław

Zasilacze UPS do serwerowni – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Moc wyjściowa czynna	Min 2700 W
Obudowa	Obudowa typu RACK 19". Musi być dostarczona wraz z kompletem szyn umożliwiających montaż.
Wyjście	Sinusoidalny kształt napięcia wyjściowego Zniekształcenie napięcia wyjściowego < 5% Zakres napięcia wyjściowego – 220V/230V/240V Częstotliwość napięcia wyjściowego – 50/60Hz
Wejście	Zakres napięcia wejściowego – 160V-294V Zakres częstotliwości napięcia wejściowego 47 do 70 Hz
Próg przełączenia	160V-294V
Wydajność	Minimum 99%
Czas podtrzymania z baterii	3 min przy 100% obciążenia 10 min przy 50% obciążenia
Zabezpieczenie	wejście - przeciwzwarciowe i przeciwprzepięciowe wyjście - przeciwzwarciowe i przeciążeniowe
Gniazda przyłącza wyjściowego	Minimum 8 sztuk IEC C13 10A
Porty	Min.1x USB, 1x RJ45
Inne	Zimny start. Przewód zasilający zakończony wtyczką z uziemieniem. Oprogramowanie zarządzająco – monitorujące. Dźwiękowa sygnalizacja rozładowania baterii. Wyświetlacz LCD. Możliwość instalacji dodatkowych modułów bateryjnych gwarantujących dłuższe czasy podtrzymania zasilania. Wczesna analiza błedów. Obsługa SNMP
Certyfikaty	Zgodność z dyrektywą RoHS UE lub równoważną.
Gwarancja	60 miesięcy

Urządzenie UTM - do serwerowni głównej – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Wymagania ogólne	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej

	na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP
ZAPORA KORPORACYJNA (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 6. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).
SYSTEM (IPS)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. 6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma mieć możliwość ochrony między innymi przed atakami

	typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
KSZTAŁTOWANIE PASMA	1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch
OCHRONA ANTYWIRUSOWA	1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.
OCHRONA ANTYSPAM	1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: **a.** białe/czarne listy, **b.** DNS RBL, **c.** heurystyczny skaner. 3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)	1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 3. SSL VPN musi działać w trybach Tunel i Portal. 4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

	6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.
FILTR DOSTĘPU DO STRON WWW	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator musi mieć możliwość dodawania własnych kategorii URL. 4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 7. blokowanie dostępu do adresu URL, 8. zezwolenie na dostęp do adresu URL, 9. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 10. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 11. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 12. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 13. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 14. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 15. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. 16. Chmurowy filtr URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych
UWIERZYTELNIANIE	1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 2. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: **a.** SSL, **b.** Radius, **c.** Kerberos. 4. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 5. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.

	6. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 8. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 9. Rozwiązanie powinno wspierać technologię Link Aggregation.
POZOSTAŁE USŁUGI I FUNKCJE	1. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. 5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 6. Urządzenie musi posiadać usługę DNS Proxy. 7. Urządzenie musi posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 8. Urządzenie musi posiadać możliwość wykrywanie słabych punktów sieci firmowej poprzez wyszukiwanie nieaktualnych wersji oprogramowania oraz oprogramowania posiadającego luki bezpieczeństwa.
ADMINISTRACJA URZĄDZENIEM	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 3. Komunikacja może odbywać się na porcie innym niż https (443 TCP).

	4. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 6. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 7. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 8. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 9. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 10. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 11. Urządzenie musi posiadać funkcjonalność anonimizacji logów.
RAPORTOWANIE	1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 4. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy.
PARAMETRY SPRZĘTOWE	1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 240 GB. 2. Liczba portów Ethernet 10/100/1000Mbps – min. 8. 3. Urządzenie musi pozwalać na podłączenie minimum jednej karty rozszerzeń z 8 miedzianymi interfejsami Ethernet 10/100/1000Mbps lub 4 miedzianymi interfejsami Ethernet 10Gbps lub 8 światłowodowymi interfejsami 1Gbps lub 4 światłowodowymi interfejsami 10Gbps. Ew. karty rozszerzeń nie są częścią postępowania przetargowego. 4. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 5. Przepustowość Firewall – min. 15 Gbps. 6. Przepustowość Firewall wraz z włączonym systemem IPS – min. 8 Gbps.

	7. Przepustowość filtrowania Antywirusowego – min. 2 Gbps. 8. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 3 Gbps. 9. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 1000. 10. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 150. 11. Obsługa min. VLAN 256. 12. Liczba równoczesnych sesji - min. 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę. 13. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 14. Urządzenie jest nielimitowane na użytkowników. 15. Wymaga się, aby dostawa obejmowała również support minimum 4 godziny w każdym miesiącu kalendarzowym w czasie trwania umowy polegającym na zdalnym administrowaniu urządzeniem. 16. Wymaga się, aby dostawa obejmowała również wymianę urządzenia w przypadku awarii na następny dzień roboczy z opcją wyjęcia i zachowania dysku twardego, na którym znajdują się wrażliwe dane. 17. Wymaga się, aby dostawa obejmowała również minimum 60-miesięczną gwarancję producentów na dostarczone elementy systemu oraz wszystkie dodatkowe licencje dla wszystkich funkcji bezpieczeństwa.

Przełączniki 1 GB Ethernet do serwerowni – 4 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej

	konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED.
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN,

	priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich

	funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m
Gwarancja	60 miesięcy

Przełączniki do serwerowni głównej - szkielet 10 Gb + podłączenie serwerów – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Charakterystyka sprzętowa	Porty 10GBase-T/SFP+ typu Combo (IEEE 802.3ae) - liczba portów co najmniej 4. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 20 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego oraz dedykowany port Ethernet do zarządzania Out-of-Band, a także w port umożliwiający podłączenie zewnętrznych czujników zdarzeń, których wyzwolenie spowoduje wysłanie powiadomienia SNMP i port umożliwiający podłączenie zewnętrznego elementu wykonawczego wyzwalanego po wystąpieniu alarmu. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 4

	jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 80 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Musi istnieć możliwość użycia dodatkowego zasilacza nadmiarowego. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 480 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 357 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 49100 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 1020 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 512 MB. Pamięć Flash - nie mniej niż 128 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 12280 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 4 MB. Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -3 stopni Celsjusza. Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 48 stopni Celsjusza. Przełącznik powinien posiadać ochronę przeciwprzepięciową na portach miedzianych co najmniej do 1 kV. Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 140000 godzin.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 250 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych. Powinna istnieć możliwość uwierzytelnienia klienta przed dostarczeniem mu strumienia Multicast. Urządzenie powinno umożliwiać konfigurację filtrów dla protokołu IGMP ograniczających adresy IPv4 grup multicast do których poszczególni klienci mogą się przyłączać. Urządzenie powinno umożliwiać również konfigurację filtrów dla protokołu MLD ograniczających adresy grup IPv6 multicast do których poszczególni klienci mogą się przyłączać. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 64 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego,

	część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED. Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 2. Sprzęt powinien obsługiwać co najmniej 14 jednocześnie skonfigurowanych pierścieni. Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6. Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko kierowanego do określonego adresu IP) oraz kopiowania ruchu na port monitorujący znajdujący się w innym przełączniku. Urządzenie powinno umożliwiać dostarczanie ruchu na wiele portów fizycznych na których obecne są te same adresy IP i MAC co pozwala na bezpośrednie przyłączenie klastrów serwerów posługujących się pojedynczym wirtualnym adresem IP i MAC. Urządzenie powinno umożliwiać tunelowanie ruchu kontrolnego L2, w tym protokołów GVRP i STP oraz protokołów CDP i VTP (01-00-0C-CC-CC-CC i 01-00-0C-CC-CC-CD).
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu i pozwalać na tworzenie tzw. podwójnych VLANów. Parametry podwójnego tagowania powinny być konfigurowalne przez administratora, w tym funkcja powinna umożliwiać klasyfikację co najmniej wg adresów MAC, adresów IP, CVID, priorytetu 802.1p, protokołu IP i portu. Powinna być też możliwość tworzenia specjalnych sieci VLAN dla przenoszenia ruchu typu multicast i rozdzielenia tak przenoszonego ruchu na klientów żądających przyłączenia do danej grupy multicast. Urządzenie powinno umożliwić utworzenie co najmniej 5 takich sieci VLAN. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno umożliwiać tworzenie VLANów, które będą zapewniały funkcjonalność tworzenia wielu grup portów w ramach których porty będą mogły się komunikować, ale zablokowana będzie komunikacja pomiędzy portami w różnych grupach oraz wszystkie grupy będą mogły komunikować się z grupą portów wspólnych. Wszystkie porty należące do takich VLANów powinny pozostać nietagowane. Przełącznik powinien obsługiwać także sieci VLAN oparte o podsieci IP - co najmniej 510 wpisów. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci

	VLAN. Powinna istnieć możliwość liczenia w pakietach przepływającego przez VLAN ruchu.
Funkcjonalności warstwy 3	Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 256 takich interfejsów. Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 256 takich interfejsów; oraz możliwość utworzenia wielu interfejsów IP na pojedynczej skonfigurowanej sieci VLAN - co najmniej 256 takich interfejsów. Musi istnieć możliwość skonfigurowania specjalnego interfejsu IP, który jest cały czas dostępny w sieci niezależnie od pozostałej konfiguracji przełącznika. Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą odpowiadanie na zapytania ARP w imieniu urządzenia znajdującego się w innej podsieci VLAN. Przełącznik musi posiadać funkcjonalność Gratuitous ARP. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. Urządzenie musi posiadać również funkcjonalność umożliwiającą przekazywanie zapytań DNS do odpowiednich serwerów DNS w sieci (wewnętrznych lub zewnętrznych). Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 96 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. Serwer DHCP musi mieć możliwość przydzielania dowolnych opcji DHCP. Serwer DHCP musi także obsługiwać delegację prefiksów DHCPv6. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 1K wpisów oraz umożliwiać wprowadzenie co najmniej 512 wpisów statycznych. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 32250 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 16128 takich tras dla IPv6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 4090 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 1024 takich tras dla IPv6. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 250 takich tras) oraz dla IPv6 (co najmniej 120 tras). Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4 oraz dla IPv6. Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery. Przełącznik musi być wyposażony w funkcjonalność umożliwiającą trasowanie ruchu w różnych kierunkach w zależności od zawartości pakietów (np. na podstawie adresu źródłowego IP lub protokołu IP). Przełącznik musi umożliwiać redystrybucję tras routingu pomiędzy różnymi protokołami routingu skonfigurowanymi na urządzeniu. Urządzenie powinno umożliwiać konfigurację protokołów routingu dynamicznego: RIP v1 i v2, RIPng. Urządzenie powinno obsługiwać także protokół umożliwiający utworzenie wirtualnego routera i zapewniającego dostępność sieci zewnętrznej po awarii jednego z urządzeń fizycznych bez potrzeby specjalnej rekonfiguracji klientów w sieci. Protokół powinien wspierać adresację IPv6.
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do

	odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, adresu IPv6, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu. W przypadku wykrycia ruchu iSCSI, urządzenie powinno również być w stanie obsługiwać ten ruch ze skonfigurowanym dla niego priorytetem, WRR, DRR, WDRR. Urządzenie powinno obsługiwać tzw. CIR. Przełącznik powinien umożliwiać kontrolę kongestii ruchu WRED. Przełącznik powinien posiadać obsługę powiadamiania o kongestii zgodnie z IEEE 802.1Qau, a także obsługiwać Flow Control zgodnie ze standardem 802.1Qbb i posiadać wsparcie dla alokowania przepustowości pomiędzy klasami ruchu zgodnie ze standardem 802.1Qaz. Urządzenie powinno umożliwiać limitowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Powinna istnieć funkcjonalność limitowania pasma dla określonego typu ruchu (np. odbywającego się na danym porcie TCP lub UDP) z granulacją nie większą, niż 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, flagi protokołu TCP, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 dla ruchu wejściowego i wyjściowego z portów przełącznika, a także umożliwiać tworzenie statystyk dla ACL i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN. Musi istnieć też możliwość niezależnej filtracji ruchu kierowanego do procesora przełącznika w celu jego dodatkowej ochrony.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 12K takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać współpracę z serwerem RADIUS w celu realizacji tzw. Accountingu dla przyłączonych użytkowników.

	Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Urządzenie musi współpracować z funkcjonalnością Microsoft NAP w celu wymuszenia separacji maszyn nie będących w zgodzie z obowiązującą polityką bezpieczeństwa w sieci oraz z funkcjonalnością DHCP NAP. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC, jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać możliwość filtrowanie protokołu sieci LAN NetBIOS. Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 1 pps), Multicast (z krokiem minimalnym co najwyżej 1 pps), Broadcast (z krokiem minimalnym co najwyżej 1 pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet - również poprzez adres IPv6. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również

	poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON oraz RMONv2 i obsługiwać protokół sFlow. Urządzenie musi obsługiwać protokół 802.1ag umożliwiający zdalne wykrywanie przerw połączeń w sieci oraz protokół Y.1731. Przełącznik musi obsługiwać protokół 802.3ah umożliwiający separację domeny Ethernet operatora od sieci Ethernet klienta. Urządzenie musi posiadać funkcję wykrywania połączeń jednokierunkowych. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP i DHCPv6 oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik powinien posiadać wbudowanego klienta SMTP. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6 oraz musi wspierać protokół synchronizacji czasu zgodny z IEEE1588. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego oraz wspierać traceroute dla IPv6. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach oraz wykrywanie długości linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 10 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do

	bezpośredniego połączenia przełączników w stos – długość min 1m
Pozostałe	Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. Sprzęt powinien być objęty dożywotnią gwarancją oraz dodatkowo przez minimum 5 lat po zakończeniu jego produkcji.

Zasilacze UPS do szafek rack piętra – 4 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Moc pozorna	1500 VA
Moc rzeczywista	1050 W
Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
Liczba, typ gniazd wyjściowych	8 x IEC320 C13 (10A)
Czas podtrzymania dla 100% obciążenia	5 min
Czas podtrzymania przy 50% obciążenia	13 min
Tolerancja napięcia wejściowego	184V - 276 V
Częstotliwość znamionowa	50/60 Hz autodetekcja
Zimny start	Tak
Interfejs komunikacyjny	USB RS232 DB-9 żeński (HID) styki przekaźnikowe mini-blok zacisków do zdalnego załączania zdalny wyłącznik awaryjny
Sygnały akustyczne	• Awaria • Niski stan naładowania baterii • Przeciążenie • Serwis
Typ obudowy	Rack 2U
Gwarancja	60 miesięcy

Przełączniki Ethernet do szaf w punktach PPD – 10 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również

	moduły gigabitowe SFP obsadzane w zatokach SFP+. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED.
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN.

	Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6.

	Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m
Gwarancja	60 miesięcy

Przełącznik PoE do szaf w punktach PPD – 4 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne

Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) z zasilaniem PoE zgodnym z IEEE 802.3at - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Musi istnieć możliwość uruchamiania zasilania PoE na portach sterowana kalendarzem. Urządzenie musi umożliwiać aktywne monitorowanie podłączonego urządzenia klienckiego PoE i w przypadku wykrycia jego braku wyłączać, a następnie ponownie włączać zasilanie na porcie. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Przełącznik musi zapewniać budżet mocy dla urządzeń PoE na poziomie co najmniej 370 watów. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB. Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -3 stopni Celsjusza. Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 48 stopni Celsjusza. Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 270000 godzin.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych.

	Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED. Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 1. Sprzęt powinien obsługiwać co najmniej 1 jednocześnie skonfigurowanych pierścieni. Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82, a także umożliwiać przechwytywanie zapytań DHCP od klienta i, po dodaniu opcji 82, przekazywanie ich do serwera DHCP znajdującego się w tej samej sieci VLAN, w której znajduje się klient. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6. Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko kierowanego do określonego adresu IP).
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
Funkcjonalności warstwy 3	Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów. Przełącznik musi posiadać funkcjonalność Gratuitous ARP. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio

	przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras). Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4. Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.

	Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i

	odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m
Pozostałe	Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. Sprzęt powinien być objęty dożywotnią gwarancją oraz dodatkowo przez minimum 5 lat po zakończeniu jego produkcji.

Punkty dostępowe Wifi – 12 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne

Wymagania ogólne	Obsługa standardów: IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.3, IEEE 802.3ab, IEEE 802.3at, IEEE 802.3x, IEEE 802.1Q, 802.11d, 802.11h, 802.1D. Zakres częstotliwości pracy: 2.4GHz - 2.4835GHz, 5.18GHz - 5.32GHz, 5.745GHz - 5.825GHz. Interfejs radiowy o konfiguracji co najmniej 2x2:2 dla pasma 2.4 GHz oraz dwa interfejsy radiowe o konfiguracji co najmiej 2x2:2 dla pasma 5 GHz (teoretyczna przepustowość zagregowana do 2100 Mbps). Rodzaj anten: anteny wewnętrzne o zysku co najmniej 3dBi. 2 porty typu Ethernet 1000Base-T z funkcją Auto-Negotiation oraz Auto MDI/MDI-X i możliwością ich agregacji w celu zwiększenia całkowitej przepustowości. Funkcja zasilania urządzenia zgodnie ze standardem 802.3at. Wbudowany, dostępny z zewnątrz port konsoli szeregowej w standardzie RS-232. Funkcja skanowania kanałów i automatycznego wyboru kanału najmniej zakłóconego. Dostępny z zewnątrz, sprzętowy przycisk Reset. Dostępny z zewnątrz przycisk Power. Możliwość regulacji mocy nadajnika (co najmniej 10 poziomów mocy). Funkcja rozkładania klientów na różne punkty dostępowe w zależności od zdefiniowanego obciążenia. Możliwość tworzenia co najmniej 15 wirtualnych punktów dostępowych na pojedynczy interfejs radiowy (różne SSID oraz rodzaje zabezpieczeń) i mapowania ich do sieci VLAN w standardzie 802.1Q. Funkcja przekierowania klienta na określoną stronę Web po przyłączeniu się klienta do sieci. Możliwość przydzielania klientów do różnych sieci VLAN w zależności od informacji otrzymanych z uwierzytelniającego klientów serwera RADIUS. Możliwość pracy w trybie autonomicznym oraz w trybie zarządzania przez zewnętrzny kontroler sieci bezprzewodowej, bez konieczności wymiany oprogramowania. Możliwość priorytetyzacji ruchu w oparciu o mechanizm WMM. Możliwość pracy w trybie AP oraz WDS, obsługa protokołu 802.1D. Wsparcie funkcji Airtime Fairness.
Zabezpieczenia:	Obsługa standardów WPA/WPA2 EAP/PSK, WPA3. Uwierzytelnianie na serwerze RADIUS przy użyciu: EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP. Możliwość Filtrowania adresów MAC. Obsługa uwierzytelniania 802.1X. Możliwość konfiguracji do 4 serwerów RADIUS w celu zapewnienia wysokiej niezawodności pracy. Możliwość wyłączenia rozgłaszania SSID niezależnie dla każdego rozgłaszanego SSID. Możliwość uruchomienia trybu separacji klientów bezprzewodowych, w którym klienci bezprzewodowi podłączeni do tego samego SSID nie mogą komunikować się pomiędzy sobą. Możliwość konfiguracji niezależnego VLANu do zarządzania urządzeniem (z możliwością wyboru tagowania 802.1Q lub bez). Możliwość uwierzytelniania punktu dostępowego za pomocą wbudowanego klienta 802.1X. Możliwość wyłączania nadajników radiowych w skonfigurowanych przedziałach czasowych. Możliwość ograniczenia zarządzania urządzeniem przez zdefiniowanie

	autoryzowanych, źródłowych adresów IP.
Zarządzanie:	Web UI (http/https) Telnet, SSH SNMP v3 Obsługa IPv4 oraz IPv6. zewnętrzny centralny kontroler sieci bezprzewodowej. Możliwość zmiany portu zarządzania dla HTTP. Wbudowany klient SNTP. Możliwość wyświetlania statystyk: liczby wysłanych/odebranych ramek, przyłączonych klientów. Przechowywanie logów: lokalnie, zewnętrzny serwer Syslog. Możliwość upgrade firmware za pomocą interfejsu Web. Możliwość wpisania informacji dodatkowych: nazwa systemu, położenie systemu, kontakt administracyjny. Możliwość łączenia punktów dostępowych w klastry (co najmniej 7 urządzeń) - wszystkie punty dostępowe powinny powielać zmiany konfiguracyjne na jednym z nich.
Inne:	Obudowa okrągła w kolorze białym przeznaczona do montażu na suficie. Certyfikat UL2043 oraz EN60601-1-2. MTBF: > 700’000 godzin Bezpłatna aktualizacja oprogramowania. Dożywotnia gwarancja + minimum 5 lat obsługi gwarancyjnej po zakończeniu produkcji.

Kontroler sprzętowy do punktów dostępowych AP wraz z niezbędnymi licencjami – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Wymagania ogólne	Możliwość rozszerzenia pojemności kontrolera do, co najmniej, 60 punktów dostępowych poprzez wykupienie dodatkowej licencji. Możliwość uruchomienia funkcjonalności Router (Route Failover, RIPv2), Firewall (NAT/PAT, filtrowanie ruchu) oraz VPN (IPSec, SSL) po wykupieniu dodatkowej licencji. Możliwość łączenia kontrolera w klastry do, co najmniej 4, kontrolerów. Połączenie w klaster powinno umożliwiać wymianę informacji o skonfigurowanych profilach bezprzewodowych i przyłączonych klientach. Współpraca z punktami dostępowymi pracującymi w standardach: 802.11a, 802.11b, 802.11g, 802.11n. Funkcjonalność Fast Roaming umożliwiająca przemieszczanie się użytkownika pomiędzy punktami dostępowymi bez przerywania połączenia bezprzewodowego i konieczności ponownego uwierzytelniania. Funkcjonalność powinna umożliwiać roaming pomiędzy punktami dostępowymi zlokalizowanymi zarówno w tej samej podsieci IP, jak i pomiędzy podsieciami IP. Obsługa Fast Roaming pomiędzy różnymi kontrolerami w klastrze. Możliwość konfiguracji do 64 SSID i przechowywania ich w pamięci kontrolera. Automatyczne dostosowanie mocy nadajników zarządzanych punktów dostępowych wymuszane ręcznie bądź automatycznie co określony czas. Automatyczne dostosowanie kanałów pracy zarządzanych punktów dostępowych wymuszane ręcznie bądź automatycznie co określony czas. Automatyczne podnoszenie mocy sąsiednich punktów dostępowych po wykryciu awarii jednego z nich.

	Automatyczne równoważenie obciążenia punktów dostępowych na podstawie liczby użytkowników bądź obciążenia sieci bezprzewodowej. Możliwość centralnego uaktualniania firmware na punktach dostępowych z poziomu kontrolera. Automatyczne sprawdzanie dostępności nowych wersji firmware. Automatyczne wykrywanie przyłączonych punktów dostępowych. Wykrywanie wszystkich urządzeń bezprzewodowych w zasięgu zarządzanej sieci bezprzewodowej (również klientów pracujących w trybie Ad-Hoc). Monitorowanie klientów przyłączonych do każdego zarządzanego punktu dostępowego. Uwierzytelnianie punktów dostępowych lokalnie lub na serwerze RADIUS. Centralne zarządzanie profilami punktów dostępowych. Obsługa do 250 sieci VLAN w standardzie 802.1Q do których może być mapowany ruch z różnych SSID rozgłaszanych przez punkty dostepowe. Obsługa Port-based VLAN oraz Subnet-based VLAN. Możliwość uwierzytelniania użytkowników bezprzewodowych w oparciu o interfejs Web w lokalnej bazie danych bądź na zewnętrznym serwerze RADIUS, LDAP lub Active Directory. Możliwość włączenia wzajemnej izolacji przyłączonych użytkowników bezprzewodowych. Punkty dostępowe muszą mieć możliwość pracy w trybie zarządzania przez kontroler oraz w trybie autonomicznym w przypadku, gdy kontroler zarządzający nie jest dostępny. Funkcjonalność ta musi być dostępna bez konieczności wymiany oprogramowania, zaś tryb pracy powinien być przełączany automatycznie. Funkcjonalność wykrywania włamań (IDS) w sieci bezprzewodowej w tym co najmniej: - rozgłaszanie skonfigurowanego w sieci SSID z obcego AP - rozgłaszanie skonfigurowanego w sieci SSID z obcego AP ze sfałszowanym adresem MAC - rozgłaszanie ukrytego SSID skonfigurowanego w sieci z obcego AP - rozgłaszanie AP ze sfałszowanym adresem MAC na innym kanale, niż rzeczywisty autoryzowany AP z tym adresem MAC w sieci - rozgłaszanie skonfigurowanego SSID w sieci z nieprawidłowym zestawem zabezpieczeń - rozgłaszanie nieprawidłowego SSID w sieci z autoryzowanego AP - praca AP na kanale nie dozwolonym w danym kraju - wykrywanie nieautoryzowanego urządzenia w trybie WDS - wykrywanie nieautoryzowanego AP w zasięgu sieci przewodowej Możliwość zarządzania przez: WebUI, SSH, Telnet, SSL, SNMP v1/2c/3, Konsola lokalna RS-232. Zarządzanie przez SSH, Telnet, konsolę lokalną musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Możliwość uwierzytelniania dostępu administracyjnego na serwerze RADIUS. Wbudowany serwer oraz klient DHCP/BOOTP. Funkcja współpracy z serwerem SYSLOG. Gwarancja Limited Lifetime oraz dodatkowo przez 5 lat po zakończeniu produkcji.
Wyposażenie/licencje	Wraz z urządzeniem dostarczyć licencje pozwalające na zarządzenie punktami AP dostarczonymi w ramach bieżącego postępowania.

Lokalizacja Lubin

Urządzenie UTM - 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Wymagania ogólne	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokalizacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 6. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).
SYSTEM (IPS)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

	5. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. 6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
KSZTAŁTOWANIE PASMA (Traffic Shapping)	1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA	1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.
OCHRONA ANTYSPAM	1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)	1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny –

	lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 3. SSL VPN musi działać w trybach Tunel i Portal. 4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.
FILTR DOSTĘPU DO STRON WWW	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator musi mieć możliwość dodawania własnych kategorii URL. 4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 7. blokowanie dostępu do adresu URL, 8. zezwolenie na dostęp do adresu URL, 9. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 10. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 11. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 12. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 13. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 14. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 15. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.
UWIERZYTELNIANIE	1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 2. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu,

	który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 4. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 5. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 8. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA	1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 6. Urządzenie musi posiadać usługę DNS Proxy.
ADMINISTRACJA URZĄDZENIEM	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

	2. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 3. Komunikacja może odbywać się na porcie innym niż https (443 TCP). 4. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 6. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 7. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 8. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 9. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 10. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 11. Urządzenie musi posiadać funkcjonalność anonimizacji logów.
RAPORTOWANIE	1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 4. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy
PARAMETRY SPRZĘTOWE	1. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 2. Liczba portów Ethernet 10/100/1000Mbps – min.8. 3. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 4. Przepustowość Firewall – min. 2 Gbps. 5. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – min. 1.6 Gbps. 6. Przepustowość filtrowania Antywirusowego – min. 400 Mbps.

	7. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 350 Mbps. 8. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 50. 9. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 10. Obsługa min. VLAN 64. 11. Liczba równoczesnych sesji - min. 200 000 i nie mniej niż 15000 nowych sesji/sekundę. 12. Urządzenie jest nielimitowane na użytkowników. 13. Urządzenie musi mieć możliwość utworzenia 4096 reguł filtrowania. 14. Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów. 15. Wymaga się, aby dostawa obejmowała również minimum 60-miesięczną gwarancję producentów na dostarczone elementy systemu oraz licencje dla wszystkich funkcji bezpieczeństwa.

Zasilacz UPS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Moc pozorna	1500 VA
Moc rzeczywista	1050 W
Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
Liczba, typ gniazd wyjściowych	8 x IEC320 C13 (10A)
Czas podtrzymania dla 100% obciążenia	5 min
Czas podtrzymania przy 50% obciążenia	13 min
Tolerancja napięcia wejściowego	184V - 276 V
Częstotliwość znamionowa	50/60 Hz autodetekcja
Zimny start	Tak
Interfejs komunikacyjny	USB RS232 DB-9 żeński (HID) styki przekaźnikowe mini-blok zacisków do zdalnego załączania zdalny wyłącznik awaryjny
Sygnały akustyczne	• Awaria • Niski stan naładowania baterii • Przeciążenie • Serwis
Typ obudowy	Rack 2U
Gwarancja	60 miesięcy

Przełączniki Ethernet – 3 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne

Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP.

	Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED.
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN.

	Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego

	dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m
Gwarancja	60 miesięcy

Przełącznik PoE – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) z zasilaniem PoE zgodnym z IEEE 802.3at - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Musi istnieć możliwość uruchamiania zasilania PoE na portach sterowana kalendarzem. Urządzenie musi umożliwiać aktywne monitorowanie podłączonego urządzenia klienckiego PoE i w przypadku wykrycia jego braku wyłączać, a następnie ponownie włączać zasilanie na porcie. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Przełącznik musi zapewniać budżet mocy dla urządzeń PoE na poziomie co najmniej 370 watów. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB. Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -3

	stopni Celsjusza. Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 48 stopni Celsjusza. Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 270000 godzin.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED. Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 1. Sprzęt powinien obsługiwać co najmniej 1 jednocześnie skonfigurowanych pierścieni. Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82, a także umożliwiać przechwytywanie zapytań DHCP od klienta i, po dodaniu opcji 82, przekazywanie ich do serwera DHCP znajdującego się w tej samej sieci VLAN, w której znajduje się klient. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6. Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko kierowanego do określonego adresu IP).
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
Funkcjonalności warstwy 3	Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów. Przełącznik musi posiadać funkcjonalność Gratuitous ARP. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na

	wskazany adres IP w sieci. Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras). Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4. Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL.

	Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych

	urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m

Pozostałe	Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. Sprzęt powinien być objęty dożywotnią gwarancją oraz dodatkowo przez minimum 5 lat po zakończeniu jego produkcji.

Punkty dostępowe Wifi – 3 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Wymagania ogólne	Obsługa standardów: IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.3, IEEE 802.3ab, IEEE 802.3at, IEEE 802.3x, IEEE 802.1Q, 802.11d, 802.11h, 802.1D. Zakres częstotliwości pracy: 2.4GHz - 2.4835GHz, 5.18GHz - 5.32GHz, 5.745GHz - 5.825GHz. Interfejs radiowy o konfiguracji co najmniej 2x2:2 dla pasma 2.4 GHz oraz dwa interfejsy radiowe o konfiguracji co najmiej 2x2:2 dla pasma 5 GHz (teoretyczna przepustowość zagregowana do 2100 Mbps). Rodzaj anten: anteny wewnętrzne o zysku co najmniej 3dBi. 2 porty typu Ethernet 1000Base-T z funkcją Auto-Negotiation oraz Auto MDI/MDI-X i możliwością ich agregacji w celu zwiększenia całkowitej przepustowości. Funkcja zasilania urządzenia zgodnie ze standardem 802.3at. Wbudowany, dostępny z zewnątrz port konsoli szeregowej w standardzie RS-232. Funkcja skanowania kanałów i automatycznego wyboru kanału najmniej zakłóconego. Dostępny z zewnątrz, sprzętowy przycisk Reset. Dostępny z zewnątrz przycisk Power. Możliwość regulacji mocy nadajnika (co najmniej 10 poziomów mocy). Funkcja rozkładania klientów na różne punkty dostępowe w zależności od zdefiniowanego obciążenia. Możliwość tworzenia co najmniej 15 wirtualnych punktów dostępowych na pojedynczy interfejs radiowy (różne SSID oraz rodzaje zabezpieczeń) i mapowania ich do sieci VLAN w standardzie 802.1Q. Funkcja przekierowania klienta na określoną stronę Web po przyłączeniu się klienta do sieci. Możliwość przydzielania klientów do różnych sieci VLAN w zależności od informacji otrzymanych z uwierzytelniającego klientów serwera RADIUS. Możliwość pracy w trybie autonomicznym oraz w trybie zarządzania przez zewnętrzny kontroler sieci bezprzewodowej, bez konieczności wymiany oprogramowania. Możliwość priorytetyzacji ruchu w oparciu o mechanizm WMM. Możliwość pracy w trybie AP oraz WDS, obsługa protokołu 802.1D. Wsparcie funkcji Airtime Fairness.
Zabezpieczenia:	Obsługa standardów WPA/WPA2 EAP/PSK, WPA3. Uwierzytelnianie na serwerze RADIUS przy użyciu: EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP. Możliwość Filtrowania adresów MAC. Obsługa uwierzytelniania 802.1X. Możliwość konfiguracji do 4 serwerów RADIUS w celu zapewnienia wysokiej niezawodności pracy. Możliwość wyłączenia rozgłaszania SSID niezależnie dla każdego rozgłaszanego SSID. Możliwość uruchomienia trybu separacji klientów bezprzewodowych, w którym klienci bezprzewodowi podłączeni do tego samego SSID nie mogą

	komunikować się pomiędzy sobą. Możliwość konfiguracji niezależnego VLANu do zarządzania urządzeniem (z możliwością wyboru tagowania 802.1Q lub bez). Możliwość uwierzytelniania punktu dostępowego za pomocą wbudowanego klienta 802.1X. Możliwość wyłączania nadajników radiowych w skonfigurowanych przedziałach czasowych. Możliwość ograniczenia zarządzania urządzeniem przez zdefiniowanie autoryzowanych, źródłowych adresów IP.
Zarządzanie:	Web UI (http/https) Telnet, SSH SNMP v3 Obsługa IPv4 oraz IPv6. zewnętrzny centralny kontroler sieci bezprzewodowej. Możliwość zmiany portu zarządzania dla HTTP. Wbudowany klient SNTP. Możliwość wyświetlania statystyk: liczby wysłanych/odebranych ramek, przyłączonych klientów. Przechowywanie logów: lokalnie, zewnętrzny serwer Syslog. Możliwość upgrade firmware za pomocą interfejsu Web. Możliwość wpisania informacji dodatkowych: nazwa systemu, położenie systemu, kontakt administracyjny. Możliwość łączenia punktów dostępowych w klastry (co najmniej 7 urządzeń) - wszystkie punty dostępowe powinny powielać zmiany konfiguracyjne na jednym z nich.
Inne:	Obudowa okrągła w kolorze białym przeznaczona do montażu na suficie. Certyfikat UL2043 oraz EN60601-1-2. MTBF: > 700’000 godzin Bezpłatna aktualizacja oprogramowania. Dożywotnia gwarancja + minimum 5 lat obsługi gwarancyjnej po zakończeniu produkcji.

Lokalizacja Wałbrzych

Urządzenie UTM - 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Wymagania ogólne	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć

	możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokalizacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 6. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).
SYSTEM (IPS)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. 6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
KSZTAŁTOWANIE PASMA (Traffic Shapping)	1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).

	4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA	1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.
OCHRONA ANTYSPAM	1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)	1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 3. SSL VPN musi działać w trybach Tunel i Portal. 4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.
FILTR DOSTĘPU DO STRON WWW	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator musi mieć możliwość dodawania własnych kategorii URL. 4. Urządzenie nie jest limitowane pod względem kategorii URL

	dodawanych przez administratora. 5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 7. blokowanie dostępu do adresu URL, 8. zezwolenie na dostęp do adresu URL, 9. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 10. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 11. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 12. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 13. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 14. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 15. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.
UWIERZYTELNIANIE	1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 2. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 4. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 5. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

	4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 8. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA	1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 6. Urządzenie musi posiadać usługę DNS Proxy.
ADMINISTRACJA URZĄDZENIEM	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 3. Komunikacja może odbywać się na porcie innym niż https (443 TCP). 4. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 6. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 7. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 8. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 9. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 10. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego

	serwera zarządzanego przez administratora. 11. Urządzenie musi posiadać funkcjonalność anonimizacji logów.
RAPORTOWANIE	1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 4. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy
PARAMETRY SPRZĘTOWE	1. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 2. Liczba portów Ethernet 10/100/1000Mbps – min.8. 3. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 4. Przepustowość Firewall – min. 2 Gbps. 5. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – min. 1.6 Gbps. 6. Przepustowość filtrowania Antywirusowego – min. 400 Mbps. 7. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 350 Mbps. 8. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 50. 9. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 10. Obsługa min. VLAN 64. 11. Liczba równoczesnych sesji - min. 200 000 i nie mniej niż 15000 nowych sesji/sekundę. 12. Urządzenie jest nielimitowane na użytkowników. 13. Urządzenie musi mieć możliwość utworzenia 4096 reguł filtrowania. 14. Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów. 15. Wymaga się, aby dostawa obejmowała również minimum 60-miesięczną gwarancję producentów na dostarczone elementy systemu oraz licencje dla wszystkich funkcji bezpieczeństwa.

Zasilacz UPS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Moc pozorna	1500 VA

Moc rzeczywista	1050 W
Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
Liczba, typ gniazd wyjściowych	8 x IEC320 C13 (10A)
Czas podtrzymania dla 100% obciążenia	5 min
Czas podtrzymania przy 50% obciążenia	13 min
Tolerancja napięcia wejściowego	184V - 276 V
Częstotliwość znamionowa	50/60 Hz autodetekcja
Zimny start	Tak
Interfejs komunikacyjny	USB RS232 DB-9 żeński (HID) styki przekaźnikowe mini-blok zacisków do zdalnego załączania zdalny wyłącznik awaryjny
Sygnały akustyczne	• Awaria • Niski stan naładowania baterii • Przeciążenie • Serwis
Typ obudowy	Rack 2U
Gwarancja	60 miesięcy

Przełączniki Ethernet – 3 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V.

	Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED.
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego

	na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę

	internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m
Gwarancja	60 miesięcy

Przełącznik PoE – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) z zasilaniem PoE zgodnym z IEEE 802.3at - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Musi istnieć możliwość uruchamiania zasilania PoE na portach sterowana kalendarzem. Urządzenie musi umożliwiać aktywne monitorowanie podłączonego

	urządzenia klienckiego PoE i w przypadku wykrycia jego braku wyłączać, a następnie ponownie włączać zasilanie na porcie. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Przełącznik musi zapewniać budżet mocy dla urządzeń PoE na poziomie co najmniej 370 watów. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB. Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -3 stopni Celsjusza. Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 48 stopni Celsjusza. Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 270000 godzin.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać

	protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED. Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 1. Sprzęt powinien obsługiwać co najmniej 1 jednocześnie skonfigurowanych pierścieni. Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82, a także umożliwiać przechwytywanie zapytań DHCP od klienta i, po dodaniu opcji 82, przekazywanie ich do serwera DHCP znajdującego się w tej samej sieci VLAN, w której znajduje się klient. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6. Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko kierowanego do określonego adresu IP).
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
Funkcjonalności warstwy 3	Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów. Przełącznik musi posiadać funkcjonalność Gratuitous ARP. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras). Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4. Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej:

	wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany.

	Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji

	z serwera TFTP w sieci. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m
Pozostałe	Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. Sprzęt powinien być objęty dożywotnią gwarancją oraz dodatkowo przez minimum 5 lat po zakończeniu jego produkcji.

Punkty dostępowe Wifi – 3 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Wymagania ogólne	Obsługa standardów: IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.3, IEEE 802.3ab, IEEE 802.3at, IEEE 802.3x, IEEE 802.1Q, 802.11d, 802.11h, 802.1D. Zakres częstotliwości pracy: 2.4GHz - 2.4835GHz, 5.18GHz - 5.32GHz, 5.745GHz - 5.825GHz. Interfejs radiowy o konfiguracji co najmniej 2x2:2 dla pasma 2.4 GHz oraz dwa interfejsy radiowe o konfiguracji co najmiej 2x2:2 dla pasma 5 GHz (teoretyczna przepustowość zagregowana do 2100 Mbps). Rodzaj anten: anteny wewnętrzne o zysku co najmniej 3dBi. 2 porty typu Ethernet 1000Base-T z funkcją Auto-Negotiation oraz Auto MDI/MDI-X i możliwością ich agregacji w celu zwiększenia całkowitej przepustowości. Funkcja zasilania urządzenia zgodnie ze standardem 802.3at.

	Wbudowany, dostępny z zewnątrz port konsoli szeregowej w standardzie RS-232. Funkcja skanowania kanałów i automatycznego wyboru kanału najmniej zakłóconego. Dostępny z zewnątrz, sprzętowy przycisk Reset. Dostępny z zewnątrz przycisk Power. Możliwość regulacji mocy nadajnika (co najmniej 10 poziomów mocy). Funkcja rozkładania klientów na różne punkty dostępowe w zależności od zdefiniowanego obciążenia. Możliwość tworzenia co najmniej 15 wirtualnych punktów dostępowych na pojedynczy interfejs radiowy (różne SSID oraz rodzaje zabezpieczeń) i mapowania ich do sieci VLAN w standardzie 802.1Q. Funkcja przekierowania klienta na określoną stronę Web po przyłączeniu się klienta do sieci. Możliwość przydzielania klientów do różnych sieci VLAN w zależności od informacji otrzymanych z uwierzytelniającego klientów serwera RADIUS. Możliwość pracy w trybie autonomicznym oraz w trybie zarządzania przez zewnętrzny kontroler sieci bezprzewodowej, bez konieczności wymiany oprogramowania. Możliwość priorytetyzacji ruchu w oparciu o mechanizm WMM. Możliwość pracy w trybie AP oraz WDS, obsługa protokołu 802.1D. Wsparcie funkcji Airtime Fairness.
Zabezpieczenia:	Obsługa standardów WPA/WPA2 EAP/PSK, WPA3. Uwierzytelnianie na serwerze RADIUS przy użyciu: EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP. Możliwość Filtrowania adresów MAC. Obsługa uwierzytelniania 802.1X. Możliwość konfiguracji do 4 serwerów RADIUS w celu zapewnienia wysokiej niezawodności pracy. Możliwość wyłączenia rozgłaszania SSID niezależnie dla każdego rozgłaszanego SSID. Możliwość uruchomienia trybu separacji klientów bezprzewodowych, w którym klienci bezprzewodowi podłączeni do tego samego SSID nie mogą komunikować się pomiędzy sobą. Możliwość konfiguracji niezależnego VLANu do zarządzania urządzeniem (z możliwością wyboru tagowania 802.1Q lub bez). Możliwość uwierzytelniania punktu dostępowego za pomocą wbudowanego klienta 802.1X. Możliwość wyłączania nadajników radiowych w skonfigurowanych przedziałach czasowych. Możliwość ograniczenia zarządzania urządzeniem przez zdefiniowanie autoryzowanych, źródłowych adresów IP.
Zarządzanie:	Web UI (http/https) Telnet, SSH SNMP v3 Obsługa IPv4 oraz IPv6. zewnętrzny centralny kontroler sieci bezprzewodowej. Możliwość zmiany portu zarządzania dla HTTP. Wbudowany klient SNTP. Możliwość wyświetlania statystyk: liczby wysłanych/odebranych ramek, przyłączonych klientów. Przechowywanie logów: lokalnie, zewnętrzny serwer Syslog. Możliwość upgrade firmware za pomocą interfejsu Web. Możliwość wpisania informacji dodatkowych: nazwa systemu, położenie

	systemu, kontakt administracyjny. Możliwość łączenia punktów dostępowych w klastry (co najmniej 7 urządzeń) - wszystkie punty dostępowe powinny powielać zmiany konfiguracyjne na jednym z nich.
Inne:	Obudowa okrągła w kolorze białym przeznaczona do montażu na suficie. Certyfikat UL2043 oraz EN60601-1-2. MTBF: > 700'000 godzin Bezpłatna aktualizacja oprogramowania. Dożywotnia gwarancja + minimum 5 lat obsługi gwarancyjnej po zakończeniu produkcji.

Lokalizacja Jelenia Góra

Urządzenie UTM - 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Wymagania ogólne	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokalizacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 6. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).
SYSTEM (IPS)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu

	sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. 6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
KSZTAŁTOWANIE PASMA (Traffic Shapping)	1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA	1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.
OCHRONA ANTYSPAM	1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 3. W przypadku ochrony w oparciu o DNS RBL administrator może

	modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)	1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 3. SSL VPN musi działać w trybach Tunel i Portal. 4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.
FILTR DOSTĘPU DO STRON WWW	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator musi mieć możliwość dodawania własnych kategorii URL. 4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 7. blokowanie dostępu do adresu URL, 8. zezwolenie na dostęp do adresu URL, 9. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 10. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 11. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 12. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 13. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 14. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 15. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.

UWIERZYTELNIANIE	1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 2. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 4. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 5. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 8. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA	1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji

	dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 6. Urządzenie musi posiadać usługę DNS Proxy.
ADMINISTRACJA URZĄDZENIEM	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 3. Komunikacja może odbywać się na porcie innym niż https (443 TCP). 4. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 6. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 7. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 8. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 9. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 10. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 11. Urządzenie musi posiadać funkcjonalność anonimizacji logów.
RAPORTOWANIE	1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 4. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy
PARAMETRY SPRZĘTOWE	1. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.

	2. Liczba portów Ethernet 10/100/1000Mbps – min.8. 3. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 4. Przepustowość Firewall – min. 2 Gbps. 5. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – min. 1.6 Gbps. 6. Przepustowość filtrowania Antywirusowego – min. 400 Mbps. 7. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 350 Mbps. 8. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 50. 9. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 10. Obsługa min. VLAN 64. 11. Liczba równoczesnych sesji - min. 200 000 i nie mniej niż 15000 nowych sesji/sekundę. 12. Urządzenie jest nielimitowane na użytkowników. 13. Urządzenie musi mieć możliwość utworzenia 4096 reguł filtrowania. 14. Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów. 15. Wymaga się, aby dostawa obejmowała również minimum 60-miesięczną gwarancję producentów na dostarczone elementy systemu oraz licencje dla wszystkich funkcji bezpieczeństwa.

Zasilacz UPS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Moc pozorna	1500 VA
Moc rzeczywista	1050 W
Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
Liczba, typ gniazd wyjściowych	8 x IEC320 C13 (10A)
Czas podtrzymania dla 100% obciążenia	5 min
Czas podtrzymania przy 50% obciążenia	13 min
Tolerancja napięcia wejściowego	184V - 276 V
Częstotliwość znamionowa	50/60 Hz autodetekcja
Zimny start	Tak
Interfejs komunikacyjny	USB RS232 DB-9 żeński (HID) styki przekaźnikowe mini-blok zacisków do zdalnego załączania zdalny wyłącznik awaryjny
Sygnały akustyczne	• Awaria • Niski stan naładowania baterii

	• Przeciążenie • Serwis
Typ obudowy	Rack 2U
Gwarancja	60 miesięcy

Przełączniki Ethernet – 3 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji

	MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED.
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika.

	Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia.

	Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m
Gwarancja	60 miesięcy

Przełącznik PoE – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) z zasilaniem PoE zgodnym z IEEE 802.3at - liczba portów co najmniej 24. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Musi istnieć możliwość uruchamiania zasilania PoE na portach sterowana kalendarzem. Urządzenie musi umożliwiać aktywne monitorowanie podłączonego urządzenia klienckiego PoE i w przypadku wykrycia jego braku wyłączać, a następnie ponownie włączać zasilanie na porcie. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 6 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 40 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Przełącznik musi zapewniać budżet mocy dla urządzeń PoE na poziomie co najmniej 370 watów. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 16300 adresów

	MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 510 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 9210 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 1,5 MB. Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -3 stopni Celsjusza. Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 48 stopni Celsjusza. Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 270000 godzin.
Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 510 grup multicast w tym możliwość utworzenia co najmniej 256 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 31 grup multicast w tym możliwość utworzenia co najmniej 31 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 16 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED. Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 1. Sprzęt powinien obsługiwać co najmniej 1 jednocześnie skonfigurowanych pierścieni. Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82, a także umożliwiać przechwytywanie zapytań DHCP od klienta i, po dodaniu opcji 82, przekazywanie ich do serwera DHCP znajdującego się w tej samej sieci VLAN, w której znajduje się klient. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6. Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko kierowanego do określonego adresu IP).
Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN.

	Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
Funkcjonalności warstwy 3	Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów. Przełącznik musi posiadać funkcjonalność Gratuitous ARP. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras). Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4. Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 126 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych

	użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 240 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.
Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres

	IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na

	portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.
Wyposażenie	Wraz z urządzeniami należy dostarczyć po 2 szt modułów komunikacyjnych zaprojektowanych do obsługi odległości do 550 metrów, Obsługa pełnego dupleksu, prędkości 10 Gigabit na kablach światłowodowych oraz kabel do bezpośredniego połączenia przełączników w stos – długość min 1m
Pozostałe	Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. Sprzęt powinien być objęty dożywotnią gwarancją oraz dodatkowo przez minimum 5 lat po zakończeniu jego produkcji.

Punkty dostępowe Wifi – 4 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Wymagania ogólne	Obsługa standardów: IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.3, IEEE 802.3ab, IEEE 802.3at, IEEE 802.3x, IEEE 802.1Q, 802.11d, 802.11h, 802.1D. Zakres częstotliwości pracy: 2.4GHz - 2.4835GHz, 5.18GHz - 5.32GHz, 5.745GHz - 5.825GHz. Interfejs radiowy o konfiguracji co najmniej 2x2:2 dla pasma 2.4 GHz oraz dwa interfejsy radiowe o konfiguracji co najmiej 2x2:2 dla pasma 5 GHz (teoretyczna przepustowość zagregowana do 2100 Mbps). Rodzaj anten: anteny wewnętrzne o zysku co najmniej 3dBi. 2 porty typu Ethernet 1000Base-T z funkcją Auto-Negotiation oraz Auto MDI/MDI-X i możliwością ich agregacji w celu zwiększenia całkowitej przepustowości. Funkcja zasilania urządzenia zgodnie ze standardem 802.3at. Wbudowany, dostępny z zewnątrz port konsoli szeregowej w standardzie RS-232. Funkcja skanowania kanałów i automatycznego wyboru kanału najmniej zakłóconego. Dostępny z zewnątrz, sprzętowy przycisk Reset. Dostępny z zewnątrz przycisk Power. Możliwość regulacji mocy nadajnika (co najmniej 10 poziomów mocy). Funkcja rozkładania klientów na różne punkty dostępowe w zależności od zdefiniowanego obciążenia. Możliwość tworzenia co najmniej 15 wirtualnych punktów dostępowych na pojedynczy interfejs radiowy (różne SSID oraz rodzaje zabezpieczeń) i mapowania ich do sieci VLAN w standardzie 802.1Q. Funkcja przekierowania klienta na określoną stronę Web po przyłączeniu się klienta do sieci. Możliwość przydzielania klientów do różnych sieci VLAN w zależności od informacji otrzymanych z uwierzytelniającego klientów serwera RADIUS. Możliwość pracy w trybie autonomicznym oraz w trybie zarządzania przez zewnętrzny kontroler sieci bezprzewodowej, bez konieczności wymiany oprogramowania. Możliwość priorytetyzacji ruchu w oparciu o mechanizm WMM. Możliwość pracy w trybie AP oraz WDS, obsługa protokołu 802.1D. Wsparcie funkcji Airtime Fairness.
Zabezpieczenia:	Obsługa standardów WPA/WPA2 EAP/PSK, WPA3. Uwierzytelnianie na

	serwerze RADIUS przy użyciu: EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP. Możliwość Filtrowania adresów MAC. Obsługa uwierzytelniania 802.1X. Możliwość konfiguracji do 4 serwerów RADIUS w celu zapewnienia wysokiej niezawodności pracy. Możliwość wyłączenia rozgłaszania SSID niezależnie dla każdego rozgłaszanego SSID. Możliwość uruchomienia trybu separacji klientów bezprzewodowych, w którym klienci bezprzewodowi podłączeni do tego samego SSID nie mogą komunikować się pomiędzy sobą. Możliwość konfiguracji niezależnego VLANu do zarządzania urządzeniem (z możliwością wyboru tagowania 802.1Q lub bez). Możliwość uwierzytelniania punktu dostępowego za pomocą wbudowanego klienta 802.1X. Możliwość wyłączania nadajników radiowych w skonfigurowanych przedziałach czasowych. Możliwość ograniczenia zarządzania urządzeniem przez zdefiniowanie autoryzowanych, źródłowych adresów IP.
Zarządzanie:	Web UI (http/https) Telnet, SSH SNMP v3 Obsługa IPv4 oraz IPv6. zewnętrzny centralny kontroler sieci bezprzewodowej. Możliwość zmiany portu zarządzania dla HTTP. Wbudowany klient SNTP. Możliwość wyświetlania statystyk: liczby wysłanych/odebranych ramek, przyłączonych klientów. Przechowywanie logów: lokalnie, zewnętrzny serwer Syslog. Możliwość upgrade firmware za pomocą interfejsu Web. Możliwość wpisania informacji dodatkowych: nazwa systemu, położenie systemu, kontakt administracyjny. Możliwość łączenia punktów dostępowych w klastry (co najmniej 7 urządzeń) - wszystkie punty dostępowe powinny powielać zmiany konfiguracyjne na jednym z nich.
Inne:	Obudowa okrągła w kolorze białym przeznaczona do montażu na suficie. Certyfikat UL2043 oraz EN60601-1-2. MTBF: > 700’000 godzin Bezpłatna aktualizacja oprogramowania. Dożywotnia gwarancja + minimum 5 lat obsługi gwarancyjnej po zakończeniu produkcji.