Załącznik nr 6 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

W ramach zadania należy zaprojektować i wykonać:

I. **W ramach zadania „Centrum zarządzania siecią" - Węzeł centralny – zlokalizowany w Urzędzie Miasta Ełku, ul. Piłsudskiego 2 składający z się z następujących instalacji teletechnicznych i urządzeń:**

I. 1. Instalacji techniczne:
W ramach Systemu Zasilania Gwarantowanego:
- **System zasilania gwarantowanego (agregat prądotwórczy)** wraz z kompletną instalacją, rozruchem i układem wydechowym, instruktażem eksploatacyjnym, dokumentacją wykonawczą, całość wdrożenia objęta 2-letnim serwisem gwarancyjnym
- **Układ redundantnych jednostek systemu napięcia gwarantowanego UPS** o mocy do 30kVA każda (obciążenie w granicach 15KW, praca redundantna 2 jednostek)
- **System klimatyzacji typu SPLIT** w pomieszczeniu serwerowni
- Urządzenie pomiarowe sieci umożliwiające dokonywanie podstawowych pomiarów sieci optycznej.
W ramach Systemu dozoru i ochrony p. poż.:
- System detekcji i gaszenia pożaru pomieszczenia serwerowni
- System kontroli dostępu do pomieszczenia serwerowni

I.2 Urządzenia Aktywne Węzła Centralnego – Centrum Zarządzania Siecią:

W ramach zakupu urządzeń technicznych sieci:

- Przełącznik sieciowy szkieletowy - MPLS - 1szt.
- Zarządzany przełącznik serwerowy z wbudowaną funkcją obsługi BGP – 1szt.
- Kompletny system zabezpieczeń klasy UTM posiadający m.in. takie mechanizmy jak: AV, IPS, Web Filtering, Firewall, IPSEC i SSL VPN – **1szt.**
- **System centralnego logowania i raportowania** (analiza ruchu i logów w sieci szerokopasmowej) – **1 szt.**
- System zarządzania bezpieczeństwem i analizą ruchu xFlow w sieci (klasa SIEM) – **1 szt.**
- Sprzętowy sieciowy IDS – 1 szt.
- instruktaż powdrożeniowy dla przełączników MPLS i serwerowych wraz z systemem zarządzania
- stacja zarządzania siecią
- instruktaż powdrożeniowy z systemów bezpieczeństwa
System zabudowy węzła Rack 42 złożony z:
-**Szafa telekomunikacyjna 80x80 cm o poj. stelaża 19'' 42U z cokołem**, wyposażona w:
a) zintegrowany moduł wentylacyjny

b) system monitoringu środowiskowego PPOŚ wyposażony w czujniki temperatury, wilgotności, zalania, otwarcia drzwi, kamera CCTV, wraz z modułem oprogramowania centralnego zarządzania i obsługi alertów dźwiękowych (sygnalizator dźwiękowy)
c) listwy zasilające
d) system kontroli dostępu do szafy
e) patch panel (zakończenie światłowodu)

Architektura połączeń i topologia zaplanowanej sieci zostały przedstawione poniżej w niniejszym dokumencie.

W ramach powyższego zakresu Wykonawca obejmie całość sprzętu i oprogramowania (z wyłączeniem agregatu prądotwórczego i klimatyzacji) 5-letnią gwarancją i dostarczy wszelkie niezbędne subskrypcje i szczepionki obejmujące wszystkie mechanizmy bezpieczeństwa wymagane w postępowaniu i mające zapewnić aktualizację wszystkich opisanych w tym dokumencie funkcjonalności, do końca okresu gwarancyjnego (tj. przez 5 lat).
Dla klimatyzacji i agregatu prądotwórczego okres gwarancji wynosi 2 lata.

Wymaga się, aby dostawa obejmowała:

- Gwarancję producentów na dostarczone elementy sieci i bezpieczeństwa
- Serwis producentów do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie bezpieczeństwa wymaganym w tym postępowaniu oraz aktualizacji kompletnego oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producentów elementów bezpieczeństwa i urządzeń aktywnych
- Dostarczenie deklaracji zgodności CE na dostarczony sprzęt (wraz z dostawą)

II. W ramach zadania „Wyposażenie Węzłów" - Węzły dostępowe (pozostałe lokalizacje) – 17 lokalizacji:

- **Przełącznik sieciowy dostępowy warstwy L2**, z funkcjonalnością tunelowania ruchu 801.1q (17 szt.)

W ramach podzadania „system zabudowy węzła Rack 42"
- **Jednostkę systemu napięcia gwarantowanego UPS** o mowy 2kVA (17 szt.)
- System kontroli dostępu do szafy 42"
- System dozoru i kontroli dostępu.

Zamawiający wymaga montażu urządzeń aktywnych tj. przełączników dostępowych LAN i jednostek napięcia gwarantowanego UPS w istniejących szafach telekomunikacyjnych 42U.

Szafa – 800x800x2057 (szafy stojące z czterema 19`` belkami nośnymi z możliwością regulacji głębokości drzwi z uchwytem klamkowym i standardowym kluczem, zdejmowane osłony boczne i tylna wejście kablowe w płycie górnej i dolnej, dach z perforacją do instalacji paneli wentylacyjnymi).

W ramach powyższego zakres wskazany w pkt. II. Wykonawca obejmie 5-letnią gwarancją i dostarczy wszelkie niezbędne subskrypcje, szczepionki, aktualizacje oprogramowani, mające zapewnić aktualizację wszystkich opisanych w tym dokumencie funkcjonalności, do końca okresu gwarancyjnego (tj. przez 5 lat).

Wymaga się, aby dostawa obejmowała:

- Gwarancję producentów na dostarczone elementy sieci i bezpieczeństwa
- Serwis producentów do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie bezpieczeństwa wymaganym w tym postępowaniu oraz aktualizacji kompletnego oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producentów elementów bezpieczeństwa i urządzeń aktywnych
- Dostarczenie deklaracji zgodności CE na dostarczony sprzęt (wraz z dostawą)

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w dokumentacji).

- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów – do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy
- Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem), wraz ze sprzętem dostarczyć należy oświadczenie producenta potwierdzające datę produkcji urządzeń
- Musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej.
- W momencie składania oferty wszystkie elementy architektury muszą być dostępne w sprzedaży przez producenta
- Wraz z dostawą sprzętu należy dostarczyć dokument wydany przez producenta, poświadczający datę produkcji sprzętu
- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie wymaganym w SIWZ – do oferty należy dostarczyć odpowiednie oświadczenia Wykonawcy. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa)

- Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
- Do każdego urządzenia musi być dostarczony komplet nośników umożliwiających odtworzenie oprogramowania zainstalowanego w urządzeniu.
- W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:
    - zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację), oraz
    - zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych

  Jeżeli inspekcja, o której mowa powyżej wykaże niezgodność produktów z umową lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie osób producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 5% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Strony w związku z inspekcją, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych
- Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy) na dzień poprzedzający dzień składania ofert
- Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
    - połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
    - łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
    - zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
    - wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
    - do oferty zostanie dołączony szczegółowy opis zespołu, obejmujący schematy połączeń, określenie które elementy zestawu odpowiadają za poszczególne funkcjonalności itp.

- W ofercie należy umieścić szczegółowe konfiguracje oferowanych urządzeń (identyfikatory katalogowe, opisy itp.), pozwalające je jednoznacznie zidentyfikować.
- Zamawiający wymaga dostarczenia wraz z ofertą kart katalogowych do następujących urządzeń/systemów:

a) urządzeń aktywnych sieci, tj. przełącznika MPLS i przełączników w lokalizacja wyniesionych, przełącznika serwerowego z wbudowaną funkcją obsługi BGP
b) urządzeń bezpieczeństwa sieciowego IT (tj. systemu zabezpieczeń klasy UTM, systemu centralnego logowania i raportowania (analiza ruchu i logów w sieci szerokopasmowej), systemu zarządzania bezpieczeństwem i analizą ruchu xFlow w sieci (klasa SIEM) i sprzętowego, sieciowego IDS
c) urządzeń teletechnicznych tj. UPS, agregatu prądotwórczego i klimatyzacji

- Wszystkie wymagane funkcjonalności muszą być dostępne w dniu składania oferty. Zamawiający zastrzega sobie możliwość:
    - wystąpienia do Oferenta o wskazanie w publicznie dostępnej dokumentacji producenta (strona WWW) potwierdzenia spełnienia wymogów; nie spełnienie tego warunku w ciągu 2 dni roboczych będzie skutkowało odrzuceniem oferty,
    - wystąpienia do producenta rozwiązania o potwierdzenie spełniania wymogów,
    - przeprowadzenia testów przed wyborem oferty – dostawcy będą na żądanie Zamawiającego zobowiązani do dostarczenia urządzeń testowych w ciągu 30 dni od wezwania.
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50 Hz.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.

A) Wymagania szczegółowe dla instalacji technicznych i urządzeń aktywnych węzła centralnego „Centrum zarządzania siecią”

I. System zabudowy węzła rack 19” wraz z monitoringiem środowiska – 1 szt.

Założenia:

- niezbędna ochrona urządzeń zainstalowanych w serwerowni Centrum Zarządzania Siecią Szerokopasmową Urzędu Miasta Ełk,

- wymagany monitoring wizualny (kamery), temperatury, wilgotności, otwarcia drzwi wejściowych do pomieszczenia, wizualna i dźwiękowa kontrola dostępu do szafy z czytnikiem kompatybilnym z kartą zbliżeniową PVC EM 125 kHz, sygnalizacja alarmu, oraz możliwość rozbudowy,

- rejestracja zdarzeń: sygnały i wartości parametrów oraz możliwość nagrywania obrazu z kamer – możliwość obsługi (monitorowanie i konfiguracja) szyfrowanym połączeniem za pomocą aplikacji webowej,
- możliwość nastawiania progów alarmowych dla 5 poziomów alarmów

Wymagane minimalne parametry techniczne systemu szaf 19" (Szafa rackowa z wyposażeniem):

- szafa dystrybucyjna 800x800, drzwi szklane, z cokołem wentylowanym z filtrem
- panel wentylacyjny o wydajności min 350 m3 z możliwością rozbudowy do min 1000m3/h, sterowanym wielopoziomowo z systemu monitorowania
- zamek ryglowany z klawiaturą i czytnikiem kart zbliżeniowych PVC EM 125 kHz kontrolowany przez system monitoringu środowiska
- panel światłowodowy 24xFO SC
- panel UTP kat 6 24xRJ45
- 2 x listwa zasilająca min 8 gniazd
- panel porządkujący
- wzmocnienia umożliwiające montaż UPS- ów
- możliwa rozbudowa o klimatyzator montowany do ściany bocznej

Monitoring środowiska

W ramach zadania Wykonawca zainstaluje w systemie szaf 19" następujące wyposażenie monitoringu środowiska:

- 2 x kamera IP,
- Czujnik otwarcia drzwi,
- 2 x czujnik temperatury (wewnątrz szafy i na zewnątrz),
- czujnik wilgotności powietrza,
- sygnalizator alarmowy na zewnątrz pomieszczenia.

Monitoring środowiskowy szafy 19" powinien charakteryzować następującymi minimalnymi parametrami:

- minimum 8 sterowanych gniazd zasilających, IEC (230 VAC, 8A), możliwość zdalnego załączania i wyłączania urządzeń,
- sterowanie wyjściami za pomocą progów i parametrów

- kontrola zaniku napięcia zasilania 230V
- kontrola zaniku napięcia sterowania 12V
- oddzielne zasilanie warstwy sterującej umożliwiające zasilanie z UPS
- zapamiętywanie ustawień w przypadku utraty zasilania
- wejście 1-wire RJ12 do pomiaru temperatur i wilgotności
- konfiguracja 5-u progów temperatury, sterownie wentylatorami , grzałkami , klimatyzacją
- kontrola dostępu do szafy dystrybucyjnej oparta na kartach zbliżeniowych PVC EM 125 kHz, z konfiguracją i zapisem osób otwierających szafę, sterowanie klamką elektromagnetyczną.
- min. 2 wejścia NO/NC z zasilaniem 12V do czujników
- funkcja resetera urządzeń sieciowych
- funkcja przywracania ustawień fabrycznych
- watchdog sprzętowy
- komunikacja z urządzeniem: Ethernet 10Base-T
- wysyłanie informacji o zdarzeniach poprzez e-mail
- aktualizacje oprogramowania on- line
- obserwacja wideo monitorowanych obiektów za pomocą kamer IP

Wycena musi zawierać wszystkie niezbędne do instalacji elementy systemu, w szczególności wszelkie elementy montażowe oraz niezbędne okablowanie i konwertery, oraz oprogramowanie.

II. Agregat prądotwórczy.

Zamawiający wymaga dostarczenia i wdrożenia do pracy w Centrum Zarządzania Siecią Szerokopasmową agregatu w obudowie wyciszonej, zamocowanego na stałe na systemie dwuosiowym (D MC do 3500 kg, osie na zawieszeniu mechanicznym, koło podporowe dyszla,
dyszel sztywny z hamulcem najazdowym, zaczep kulowy, podpory postojowe, instalacja elektryczna i oświetlenie, homologacja lub dopuszczenie do transportu po drogach publicznych). Agregat umieszczony na fundamencie z dylatacja obrzeżową.
Dostarczony sprzęt musi być objęty **2-letnim** serwisem producenckim/ lub autoryzowanego dystrybutora proponowanego rozwiązania.

Wykonawca w ramach zadania wykona:
- dokumentację wykonawczą z niezbędnym projektem budowlanym (jeżeli konieczne)
- projekt powykonawczy
- instruktaż eksploatacyjny
- układ wydechowy - ostateczna długość instalacji zostanie potwierdzona w projekcie wykonawczym, wycena musi uwzględniać wycenę ryczałtową za 20mb. instalacji)
- monitoring miejsca ustawienia agregatu (zaprojektuje, dostarczy i uruchomi) system złożony z minimum 2 kamer.
- agregat ma być dostarczony z pełnym bakiem paliwa,
- Wykonawca w porozumieniu z Zamawiającym ustali a następnie wykona oznaczenie i kolorystykę agregatu,

- Wykonawca zaprojektuje i wykona połączenie elektryczne agregatu z systemem UPS i systemem zasilania gwarantowanego istniejących serwerowni Zamawiającego.

Wykonawca musi dostarczyć agregat prądotwórczy o parametrach nie gorszych niż:

1) **Moc** – ciągła PRP min. 100kVA, moc dorywcza LTP min. 110kVA
2) **Moc czynna przy cos fi = 0,8** wynosi min. 80 KW dla PRP i min. 88 KW dla dorywczej
3) **Zbiornik paliwa** – min. 180l
4) **Konstrukcja** - Stalowa, spawana rama z układem tłumienia drgań - silent bloki. Stalowy zbiornik paliwa zintegrowany w ramie. Tłumiki wydechu: min. 9dB(A) - Compact. Złączka kompensacyjna wydechu dla wersji Compact.
5) **Silnik** - rzędowy, chłodzony cieczą, spełnia normy: przynajmniej: ISO 3046 / DIN 6271, BS 5514
6) **Regulator obrotów** - regulator elektroniczny min. 1.500rpm +/- 1%
7) **Układ ogrzewania bloku silnika** – grzałka w bloku silnika min. 1000W.
8) **Start** - akumulator rozruchowy wraz z automatyczną ładowarką.
9) **Prądnica** - alternator synchroniczny 4 biegunowy z automatycznym regulatorem napięcia +/- 0,5%. Alternator spełnia normy: IEC 34.1, NEMA MG 21, BS 4999.
10) **Konstrukcja** - jednołożyskowa, z samocentrującym sprzęgłem mocowanym w kole zamachowym silnika diesla.
11) **Głośność** – maks. 70 dB@7m, obudowa akustyczna odporna na warunki atmosferyczne.
12) **Tablica automatyki** – Mikroprocesorowy system sterowania i kontroli wyposażony przynajmniej w:
    - moduł AMF / automatyczny start
    - sygnalizacja LED
    - ekran LCD / parametry pracy, komunikaty
    - przyciski funkcjonalne AUTO/RECZNY/TEST/Start / Stop/Reset
    - sterowanie grzałką bloku silnika
    - automatyczna ładowarka baterii akumulatora
    - współpraca z układem SZR' a
    - ręczne sterowanie układem SZR
    - rejestr alarmów i zdarzeń
13) **Układ SZR** – 160 A – zbudowany w oparciu o przełącznik z napędem elektrycznym z możliwością ręcznego przełączania w sytuacji awarii napędu elektrycznego. Możliwość konfigurowania progów zadziałania SZR i czasów przełączania.
14) Masa sucha zespołu prądotwórczego – maks. 1800 kg netto.
15) Wymiary zespołu prądotwórczego: maks. (Dx S x W) 280x110x180cm.
16) **Certyfikat** – CE

III. System Klimatyzacji.

Założenia instalacyjne dla systemu klimatyzacji do serwerowni Centrum Zarządzania Siecią.

Moc chłodnicza przewidywanych klimatyzatorów – min. 14,5kW.
Zamawiający wymaga dostarczenia urządzeń, które będą dobrane w systemie N+1.

Ze względu na brak dokładnego projektu oraz niewystarczającą przestrzeń w podłodze technicznej (20-30 cm) pomieszczenia o powierzchni 24 mkw., należy dostarczyć urządzenia SPLIT typu ściennego. Urządzenia muszą pracować w trybie ON- OFF.

Zamawiający wymaga dostarczenia systemu klimatyzacji przy powyższych założeniach oraz minimalnych wymaganiach wydajnościowych:

- Wydajność chłodnicza – min. 14,5kW
- Wydajność grzewcza – min. 16,5kW
- Zasilanie – 400/3/50 (V/Ø/Hz)
- Osuszanie – min. 6 l/h
- Poziom ciśnienia akustycznego jednostki wew. – maks. 46dB(A)
- Poziom ciśnienia akustycznego jednostki zew. – maks. 54dB(A)
- Wydajność powietrza – min. 2 200 m^3/h
- Pobór prądu – maks. 10 A
- Prąd rozruchowy – 70 A
- Pobór mocy – maks. 5,50kW
- Współczynnik EER – przynajmniej 2,80
- Czynnik chłodniczy – R410A

Urządzenie musi być wyposażone w tzw. zestaw pracy całorocznej tj. regulator obrotów wentylatora oraz grzałkę karteru sprężarki. Pozwoli to na pracę urządzenia w trybie chłodzenia przy ujemnych temperaturach powietrzna na zewnątrz.
Dodatkowo urządzenia będą wyposażone w zestaw pracy naprzemiennej co pozwoli na równomierną pracę obu urządzeń, a w przypadku awarii któregoś z urządzeń, drugie sprawne przejmie rolę głównego urządzenia

Kompletna instalacja klimatyzacji oraz wszystkie użyte urządzenia, muszą być objęte **2 letnim serwisem gwarancyjnym.**

Zakres zadania dla systemu klimatyzacji obejmuje:

- wykonanie projektów wykonawczego, budowlanego (jeżeli niezbędny) i projektu powykonawczego
-dostawę wraz z kompleksom montażem, włącznie w wszelkimi niezbędnymi pracami budowlanymi
-pełną instalację rozprowadzenia powierza w pomieszczeniu
- szkolenie eksploatacyjne

Wymagania w zakresie obsługi gwarancyjnej klimatyzacji:

- niezbędne przeglądy w ciągu całego okresu obowiązywania gwarancji
-czas reakcji na zgłoszenie awarii maks. 48h,
-czas usunięcia awarii nie wymagającej wymiany i naprawy osprzętu technicznego nie przekraczający 48h.
-usunięcie awarii wymagającej wymiany i naprawy osprzętu technicznego w czasie nie przekraczającym 14 dni od daty zlecenia naprawy

IV. Systemy wczesnej detekcji pożaru i gaszenia pożaru w pomieszczeniu serwerowni Centrum Zarządzania Siecią.

Systemy wczesnej detekcji pożaru i gaszenia pożaru zostaną zainstalowane w pomieszczeniu serwerowni Centrum Zarządzania Siecią.

IV.1 System detekcji pożaru.
Zamawiający określa minimalne wymagania techniczno-funkcjonalne dla systemu wczesnej detekcji pożaru w sposób następujący:

- Parametry zastosowanych czujek zasysających muszą być podane w sposób zgodny z normą EN 54-20
- Klasa zabezpieczenia obiektu musi być zgodna z przykładami aplikacji podanymi w tabeli 7 normy EN 54-20 albo lepsza – klasa min B
- Należy stosować czujki, które umożliwiają śledzenie rozwoju pożaru i realizację różnych scenariuszy w zależności od stopnia zadymienia.
- Dla umożliwienia śledzenia rozwoju pożaru zakres użytecznych nastaw czujki powinien wynosić co najmniej: od 0,06% zaciemnienia na metr do 6.5% zaciemnienia na metr.
- Dla umożliwienia realizacji różnych scenariuszy w zależności od stopnia zadymienia czujka powinna posiadać co najmniej 2 progi alarmowe dowolnie programowalne w całym zakresie podanym wyżej.
- Należy stosować czujki, dla których zostały opracowane specjalizowane metodologie obliczeń istotnych parametrów przepływowych i czułościowych, w szczególności komputerowe programy obliczeniowe dedykowane dla poszczególnych typów czujek.
- Projektant systemu sygnalizacji pożaru wykorzystującego zasysającą czujkę dymu obowiązany jest podać metodykę obliczeń istotnych parametrów czujki umożliwiających określenie klasy systemu właściwej dla zastosowania będącego przedmiotem projektu, a w szczególności:
    - obliczeń przepływów powietrza przez detektor, rury oraz poszczególne otwory próbkujące,
    - obliczeń czasów transportu dla najdalszych otworów próbkujących,
    - obliczeń czułości poszczególnych otworów próbkujących,
    - obliczeń stopnia zrównoważenia czułości wszystkich otworów próbkujących.

Akceptowalne są obliczenia wykonane przy użyciu:

- programów dostarczanych przez producenta danego sprzętu dedykowanych dla użytych detektorów,
- metod powszechnie stosowanych w mechanice płynów. W tym przypadku projektant musi przedstawić stosowaną metodologię (wzory i założenia - w szczególności upraszczające).

Zastosowane metodologia musi umożliwić ponowne przeliczenie systemu w przypadku konieczności wprowadzenia zmian na etapie wykonywania instalacji.

- Instalator systemu sygnalizacji pożaru wykorzystującego zasysającą czujkę dymu powinien przestawić:
    - autoryzację producenta lub dystrybutora,
    - zalecaną przez producenta lub dystrybutora metodykę uruchomienia systemu (formularz, check list, lub podobny dokument),

raport z uruchomienia na formularzu producenta lub dystrybutora.

- System zasysający z rurarzem PCV i jednostką detekcyjną z wbudowanym wentylatorem zasysającym powietrze.
- Kompletny rurarz PCV systemu wraz z trójnikami, kolanami, zaślepkami i uchwytami. Montaż rurarzu stały przez sklejenie części i osadzenie w uchwytach montażowych.
- monitorowanie przepływu powietrza, sygnalizacja usterki przy zmianie jego bilansu zgodnie z PN EN 54-20.
- Zasilanie systemu z certyfikowanego zasilacza buforowego. Czas podtrzymania zasilania min. 30h w stanie dozoru i 30 min w stanie alarmu.
- Nadzorowanie stanu alarmu i usterki systemu zasysającego przez nadrzędny system sygnalizacji pożaru.

IV.2 System gaszenia pożaru.
Zamawiający określa minimalne wymagania techniczno-funkcjonalne dla systemu gaszenia pożaru w sposób następujący:

1. Wydajność systemu zdolna ugasić pożar w ciągu 10 min.
2. System oparty na środku gaśniczym w postaci aerozolu.
3. System nie wymagający zapewnienia szczelności chronionego pomieszczenia i stosowania otworów dekompresyjnych
4. System musi posiadać certyfikat Instytutu Energetyki stwierdzający możliwość stosowania środka gaśniczego do gaszenia urządzeń pod napięciem
5. Wymagany jest certyfikat Polskiej jednostki badawczej
6. System bezpieczny dla ludzi i środowiska naturalnego
7. Kompletne rozwiązanie instalacji gaśniczej
8. Kompletne rozwiązanie instalacji sterowania gaszeniem pożaru.
9. **Certyfikaty**
   Generatory aerozolu gaśniczego posiadają certyfikaty:
   - certyfikat CNBOP nr 2475/2007 + aneks nr A1/2475/2007
   - certyfikat Laboratorium Wysokich Napięć Instytutu Energetyki nr EWN56/E/07
   - atest Państwowego Zakładu Higieny nr PHZ/HT-2059/2006

V. System napięcia gwarantowanego UPS.

Zamawiający wymaga dostarczenia, wdrożenia i objęcia 5 letnim sytemu napięcia gwarantowanego (UPS) składającego się z 1 jednostki 30KVA ,

Zamawiający wymaga przeszkolenie personelu eksploatacyjnego / administratora sieci w miejscu instalacji w zakresie pełnej obsługi systemu.

- Minimalne wymagania techniczno-funkcjonalne dla jednostek UPS (węzeł centralny)
- Ma zapewniać ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójnym przetwarzaniem przy zupełnych lub chwilowych zanikach napięcia, znacznych spadkach napięcia i wahaniach częstotliwości w sieci energetycznej, przez cały czas pracy urządzenia

- Ma zapewniać możliwość zwiększenia mocy UPS w trakcie jego eksploatacji: -upgrade min. 10 % (upgrade rozumiany jako programowe i sprzętowe zwiększenie mocy wyjściowej, a nie dostawienie następnego urządzenia)
- Być fabrycznie nowe tj. data ich produkcji nie może być wcześniejsza niż 6miesięcy przed datą zapytania ofertowego
- Częstotliwość wejścia i wyjścia zgodne z obowiązującymi w Polskich Normach tj.:
  3x400V częstotliwość50 Hz
- Ma posiadać wejście trójfazowe 4-ro lub 5-cio przewodowe (TN- C* lub TN -S*)
- Ma mieć wyjście trójfazowe 5-cio przewodowe
- Ma zapewnić napięcie wejściowe 173 – 485 V +/- 2 %
- Współczynnik mocy PF > 0,95
- Ma być wyposażone w dwa bezprzerwowe przełączniki obejściowe
- Ma być wyposażone w zdalny wyłącznik ppoż. (możliwy do wyniesienia na odległość min 50 m i zabezpieczony przed przypadkowym użyciem) umożliwiający wyłączenie napięcia wyjściowego urządzenia UPS w przypadku wystąpienia pożaru lub innych zagrożeń losowych
- Ma być wyposażone w hermetyczne, bezobsługowe akumulatory o minimalnej żywotności 6-9 lat
- Ma spełniać normy kompatybilności elektromagnetycznej EN 55022, EN 55011, EN 50091 (IEC 62040)
- Ma być wyposażone w osprzęt techniczny i oprogramowanie pozwalające na: - kontrolę i zarządzanie pracą urządzenia UPS z wykorzystaniem protokołu SNMP, automatyczne zamknięcie systemu operacyjnego stacji roboczych pracujących pod kontrolą systemu operacyjnego MS WINDOWS xx
- Ma zapewnić następujące parametry pracy: - stabilizacja napięcia wyjściowego przy obciążeniu statycznym , stabilizacja napięcia wyjściowego =<3% przy obciążeniu dynamicznym zmieniającym się od 100% do 0% i odwrotnie w czasie 10ms, stabilizacja częstotliwości napięcia wyjściowego 1% przy pracy z baterii
- Ma zapewnić częstotliwość przebiegu napięcia wyjściowego zgodną z częstotliwością przebiegu napięcia wejściowego przy odchyłkach częstotliwości napięcia 45-55 Hz. Urządzenie ma zapewnić regulację tolerancji częstotliwości wejściowej automatycznie lub skokowo co 0,5 Hz.
- Ma zapewnić sinusoidalny przebieg napięcia wyjściowego bez względu na charakter obciążenia, współczynnik odkształceń napięcia tzw. THDu<5% dla obciążeń nieliniowych i liniowych oraz współczynnik odkształceń prądu wejściowego THDi < 10% (z filtrem lub poprzez odpowiednią konstrukcję prostownika)
- Prąd zwarciowy wygenerowany przez falownik > 5 In
- Ma zapewnić czas reaktywacji baterii nie dłuższy niż 8 godzin liczony od pełnego
  rozładowania do 80% pojemności znamionowej baterii
- Praca hybrydowa
- Ma być odporne na przeciążenie przez podany czas do poziomu min:- 120%
- Ma posiadać filtry RFI w celu eliminacji zakłóceń wysokiej częstotliwości zgodnie z normami EN 55022 A lub B, EN 50091-2
- Ma posiadać zabezpieczenie przeciwprzepięciowe wewnętrzne lub zewnętrzne

uwzględniające IV poziom ochrony tj. 1,5kV, zgodny z normami EN 50091 i IEC62040

- Ma posiadać zakres synchronizacji częstotliwości napięcia wyjściowego do wejściowego (regulowany skokowo co 0,5 Hz)
- Współczynnik szczytu 5:1
- Ma posiadać możliwość pracy z niesymetrycznym obciążeniem poszczególnych faz w zakresie 10 – 100% obciążenia
- Ma posiadać automatyczną diagnostykę parametrów urządzenia na panelach wewnętrznych
- Ma posiadać automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem
- Ma posiadać możliwość wydłużenia czasu podtrzymania napięcia
- Ma posiadać układ „łagodnego startu" i „ zimny start"
- Ma posiadać czujnik temperatury i wilgotności jako zintegrowana część UPS
- Ma zapewniać automatyczne wyłączanie napięcia wyjściowego urządzenia UPS po zamknięciu systemów lub możliwość jego wyłączania poprzez wyniesiony panel
- Dziennik zdarzeń
- Ma być wyposażony we wbudowany lub znajdujący się przy UPS-e panel, który wyświetlałby:-

- stan pracy UPS-a (UPS / praca normalna / Obciążenie odbiorów / Praca bateryjna / Praca w trybie obejściowym / +aktywne alarmy i powiadomienia / + stan baterii)
- ZDARZENIA - Wyświetla listę aktywnych zdarzeń systemowych oraz chronologiczny rejestr zdarzeń systemowych
- IDENTYFIKACJA - Typ UPS / nr produktu / numer seryjny / wersja oprogramowania
- stan pracy UPS (UPS / praca normalna / Obciążenie odbiorów / Praca bateryjna / Praca w trybie obejściowym / +aktywne alarmy i powiadomienia / + stan baterii)
- POMIARY - WYJŚCIE / napięcie / prąd / częstotliwość/ moc; BATERIE / napięcie prąd / czas podtrzymania; WEJŚCIE / napięcie, prąd częstotliwość;

- Ma posiadać certyfikat: TUV lub CE
- Ma posiadać opcję wyposażenia w osprzęt techniczny i oprogramowanie (odpowiednia ilość licencji) umożliwiające automatyczne, zdalne zamknięcie

VI. System kontroli dostępu do pomieszczenia serwerowni.

Zamawiający zakłada rozbudowę istniejącego w urzędzie systemu kontroli dostępu do pomieszczeń. Wykonawca we własnym zakresie, po wykonaniu wizji lokalnej pomieszczenia (zalecane przez Zamawiającego), określi zakres rozbudowy.

Zamawiający posiada w Urzędzie system Roger RACS składający się z następujących elementów:

1. Centrala systemu kontroli dostępu RACS CPR32-SE-BRD

- możliwość podłączenia do 32 kontrolerów serii PR w ramach jednej sieci (podsystemu)

- zegar czasu rzeczywistego z podtrzymaniem bateryjnym
- nieulotny bufor 250.000 zdarzeń
- programowalne linie wejściowe i wyjściowe
- zasilanie 18VAC lub 12VDC
- zasilacz buforowy 1.5A
- dwa wyjścia przekaźnikowe 1.5A/30V
- dwa wyjścia tranzystorowe 1A/15V
- cztery wejścia NO/NC
- komunikacja przez RS485

- sygnalizacja stanów alarmowych
- możliwość aktualizacji oprogramowania firmowego (fleszowanie)

2. Zewnętrzny kontroler dostępu PR311SE

- wbudowany czytnik zbliżeniowy EM 125 kHz
- niebieskie podświetlenie klawiatury
- możliwość dołączenia czytnika zewnętrznego (obustronna kontrola przejścia)
- możliwość dołączenia dwóch czytników pracujących w formacie Wiegand (PR411DR)
- zasilanie: 12V DC
- dwa programowalne wyjścia tranzystorowe 1A
- możliwość instalacji na zewnątrz
- komunikacja przez RS485
- kolor: ciemnoszary, jasnoszary, ciemnoszary z niebieskim podświetleniem klawiatury

- dowolna topologia magistrali komunikacyjnej
- 1000 użytkowników w systemie
- ochrona antysabotażowa (tamper)
- możliwość podziału systemu na podsystemy (maks. 250 podsystemów)
- 250.000 zdarzeń w buforze (funkcje dostępne tylko w systemach wyposażonych w centralę CPR32-SE)
- lokalny anti-passback
- globalny anti-passback (funkcje dostępne tylko w systemach wyposażonych w centralę CPR32-SE)
- globalne sterowanie stanem uzbrojenia z podziałem na strefy alarmowe (funkcje dostępne tylko w systemach wyposażonych w centralę CPR32-SE)
- możliwość dołączenia ekspandera we/wy typ XM-2
- integracja z systemem alarmowym za pośrednictwem linii we/wy
- trzy programowalne linie wejściowe NO/NC
- tryby drzwi: Normalny, Zablokowane, Odblokowane i Warunkowo Odblokowane
- tryby identyfikacji: Karta lub PIN, Karta i PIN, tylko Karta, Tylko PIN
- szybkie programowanie (ok. 15 sekund na każdy kontroler w systemie)
- szybka aktualizacja uprawnień użytkownika (ok. 3 sekund na każdy kontroler w systemie)
- współbieżne konfigurowanie podsystemów (ilość podsystemów nie zwiększa czasu przesyłania ustawień)

- obsługa dodatkowych użytkowników typu „gość” definiowanych indywidualnie na każdym kontrolerze
- 99 harmonogramów czasowych (funkcje dostępne tylko w systemach wyposażonych w centralę CPR32-SE)
- 250 grup dostępu (funkcje dostępne tylko w systemach wyposażonych w centralę CPR32-SE)
- gwarancja: 12 miesięcy

3. Karta zbliżeniowa PVC EM 125 kHz

VII. Infrastruktura aktywna (sieć MPLS) i systemy bezpieczeństwa sieci i użytkowników.

Informacje ogólne.

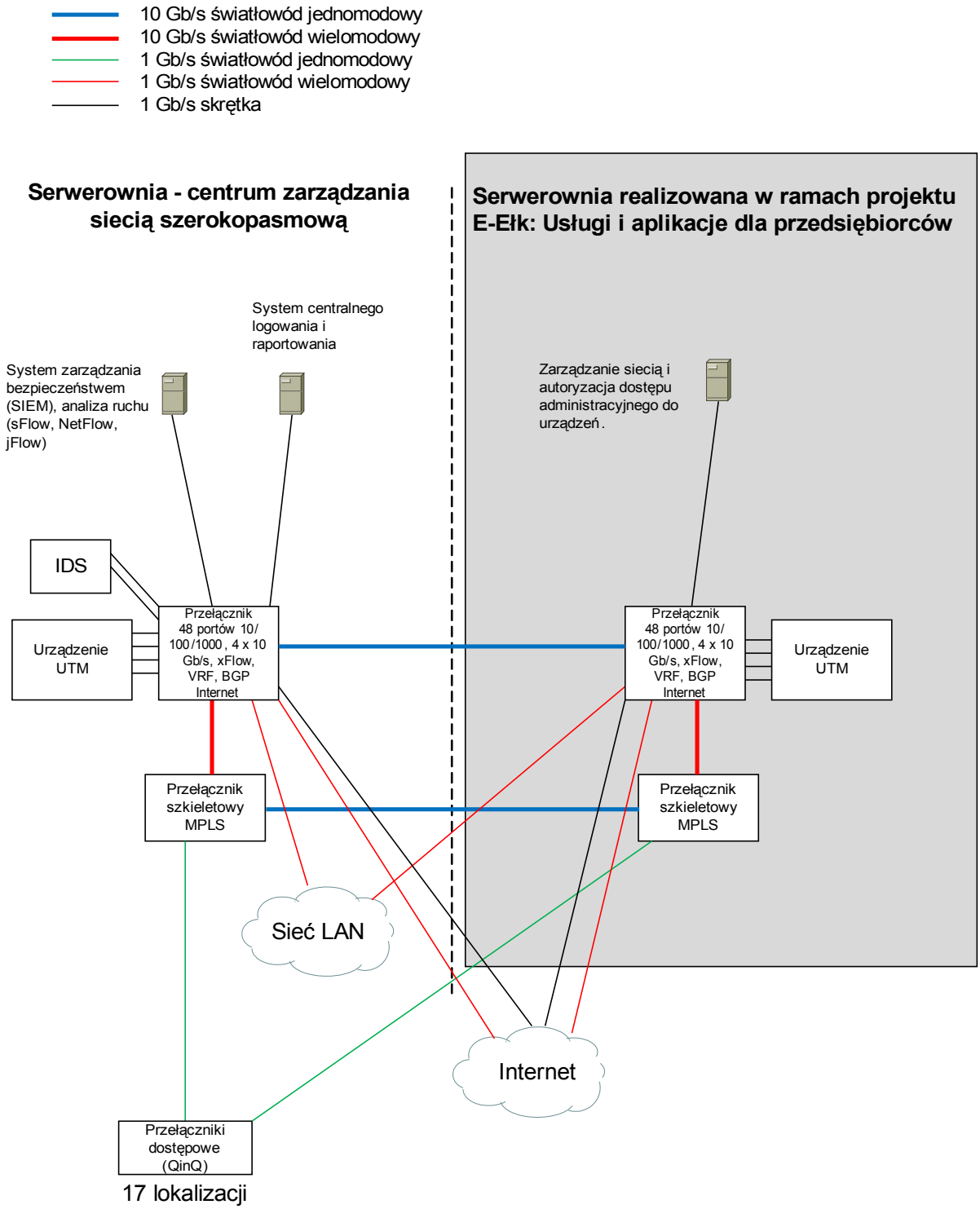
Zadaniem Wykonawcy będzie zaprojektowanie i zbudowanie Centrum Zarządzania Siecią Szerokopasmową, w oparciu o:

- Dwa redundantne urządzenia rdzeniowe (funkcjonalność MPLS) połączone ze sobą łączem 10 Gb/s. Węzły rdzeniowe będą zlokalizowane w Serwerowniach znajdujących się w budynku Urzędu przy ul. Piłsudskiego 2
- 17 urządzeń dostępowych (funkcjonalność tunelowania ruchu 801.1q) połączonych łączami 1 Gb/s do obu urządzeń rdzeniowych.
- Dwa przełączniki serwerowe z funkcjonalnością routingu BGP (obsługa pełnej tablicy sieci Internet).
- Dwa urządzenia bezpieczeństwa klasy UTM (*Unified Threat Management*).
- System ochrony IPS.
- Aplikacje zarządzające systemem teleinformatycznym:
    - Zarządzanie siecią i autoryzacja dostępu administracyjnego do urządzeń.
    - System zarządzania bezpieczeństwem (SIEM - Security Information and Event Management) oraz analiza ruchu (sFlow, NetFlow, jFlow itp.).
    - System centralnego logowania i raportowania.

W ramach niniejszego projektu należy dostarczyć:

- **Jedno urządzenie rdzeniowe MPLS**
- **Jeden przełącznik serwerowy z funkcjonalnością routingu BGP**
- **17 urządzeń dostępowych**
- **Jedno urządzenie klasy UTM**
- **Jedno urządzenie klasy IDS wraz z niezbędnym oprogramowaniem.**
- **System zarządzania bezpieczeństwem, analiza ruchu (Slow, NetFlow, jFlow)**
- **System centralnego logowania i raportowania**
- **Wkładki optyczne – liczba i rodzaj wyspecyfikowano w poniższej tabeli**

Schemat planowanej sieci przedstawia poniższy rysunek.
Na rysunku szarym prostokątem zaznaczono elementy systemu teleinformatycznego, które będą dostarczone w ramach innego projektu: E-Ełk Usługi i aplikacje dla przedsiębiorców.



Rysunek 1. Schemat połączeń

W ramach projektu „e-Ełk: Usługi i aplikacje dla przedsiębiorców” będą dostarczone następujące urządzenia:

- Enterasys NetSight Advanced Bundle (nr katalogowy NS-AB-50) – jako system zarządzania siecią i autoryzacją dostępu administracyjnego do urządzeń
- przełącznik Enterasys SSA (nr katalogowy SSA-T1068-0652) – jako przełącznik serwerowy z wbudowaną funkcjonalnością routingu BGP
- przełącznik Cisco ME3600x (nr katalogowy ME-3600X-24FS-M) – jako przełącznik szkieletowy MPLS, oraz

- Fortigate 621B (nr katalogowy FOR-FG-621B-BDL) – jako urządzenie UTM.

Wykonawca będzie miał obowiązek zintegrować dostarczany w ramach tego postępowania sprzęt z systemami podanymi powyżej w zakresie przedstawionym poniżej w dokumentacji technicznej.

Oferent wdroży między innymi następujące funkcjonalności na podstawie wcześniej stworzonego projektu technicznego:

- Integracja dostarczanych przełączników z systemem zarządzania posiadanym przez Zamawiającego tj. Enterasys NetSight Advanced Bundle
- Stworzenie klastra dwóch urządzeń rozmieszczonych w obu serwerowniach na bazie posiadanego urządzenia Fortigate 621B i objęcie ich wspólnym systemem logowania i raportowania.
- Zbudowanie klastra przełączników rdzeniowych MPLS w oparciu o posiadany przełącznik Cisco ME3600X oraz dołączenie do tej struktury 17 przełączników dostępowych w lokalizacjach wyniesionych, z utrzymaniem funkcjonalności sieci przedstawionej w dalszej części dokumentu.
- Zbudowanie redundantnego systemu dostępu do Internetu na bazie dwóch przełączników serwerowych z wbudowaną funkcjonalnością routingu BGP

Zakłada się zbudowanie systemu wyposażonego w następujące mechanizmy zwiększające niezawodność:

- Dwa urządzenia rdzeniowe MPLS
- Dwa przełączniki serwerowe z wbudowaną funkcjonalnością routingu BGP podpięte do wspólnego, posiadanego przez zamawiającego, systemu zarządzania Enterasys NetSight
- Dwa urządzenia klasy UTM objęte wspólnym systemem logowania i monitorowania
- Redundantne zasilacze w urządzeniach rdzeniowych, dostępowych oraz w przełącznikach serwerowych
- Połączenia urządzeń rdzeniowych oraz przełączników serwerowych zapewniające redundancję
- Redundantne połączenia do węzłów dostępowych
- Redundantne połączenia do istniejącej infrastruktury sieciowej w węźle centralnym
- Redundantne połączenia do sieci Internet

Założenia funkcjonalne:

- MPLS w warstwie rdzeniowej

- Urządzenia dostępowe powinny umożliwiać uzyskanie funkcjonalności wirtualizacji logicznej na poziomie warstwy drugiej modelu sieciowego ISO/OSI

- Urządzenia dostępowe powinny posiadać zaimplementowane funkcje, które umożliwią efektywną współpracę z urządzeniami rdzeniowymi (tunelowanie 802.1q).

Wyspecyfikowane poniżej urządzenia powinny zostać wyposażone w następującą liczbę portów (wartości minimalne):

- Urządzenie rdzeniowe MPLS: dwa porty (gniazda na wkładki) 10Gb/s, 24 porty (gniazda na wkładki) 1Gb/s

- Urządzenie dostępowe: 2 porty (gniazda na wkładki) 1Gb/s, 24 porty 10/100Base-T

- Przełącznik serwerowy: 48 portów 10/100/1000, 4 porty (gniazda na wkładki) 1/10Gb/s

Pozostałe elementy systemu będą dostarczone w ramach projektu: E-Ełk Usługi i aplikacje dla przedsiębiorców.
UWAGA: Wykonawca niniejszego postępowania musi w pełni zintegrować dostarczone w ramach obu projektów elementy.

Poniższa tabela przedstawia podsumowanie liczby wkładek optycznych, które należy dostarczyć w ramach niniejszego projektu:

Urządzenia	Wkładka 10GBASE-SR	Wkładka 10GBASE-LR	Wkładka 1000Base-LX	Wkładka 1000Base-SX
Rdzeniowe MPLS	2	2	48	
Dostępowe			34	
Przełączniki serwerowe	2	2		4

VII.1 Przełącznik szkieletowy MPLS - 1 szt.

Zamawiający określa minimalne wymagania techniczno-funkcjonalne dla przełącznika szkieletowego w sposób następujący:

- przełącznik modularny lub o zamkniętej konfiguracji, posiadający:
  - porty dostępowe (UNI) - min. 24 porty 1000BaseX ze stykiem definiowanym przez moduły konwerterów SFP lub równoważne, umożliwiające obsługę konwerterów w standardach T, SX, ZX, LX/LH, CWDM, DWDM oraz umożliwiać transmisję dwukierunkową na pojedynczym włóknie światłowodowym
  - porty dołączeniowe (NNI) – min. 2 porty 10GBaseX ze stykiem definiowanym przez moduły konwerterów SFP+ lub równoważne, umożliwiające obsługę konwerterów w standardach SR, LR, CU

- wbudowane redundantne, wymienne zasilacze i panele z wentylatorami, zasilanie 230V AC,
- wydajność przełączania min. 65Mpps / 44Gbps,
- certyfikat Metro Ethernet Forum - MEF9 - (EPL, EVPL, ELAN) i MEF14 (EPL, EVPL, ELAN),
- praca w zakresie temperatur: 0-40°C
- możliwość montażu w szafie 19", wysokość nie większą niż 3RU,
- funkcjonalności przełączania Ethernet:
    - możliwość obsługi min. 16.000 adresów MAC, 4.000 sieci VLAN i VLAN ID,
    - obsługa tzw. Jumbo Frames (9000 bajtów) na portach Gigabit Ethernet,
    - IEEE 802.1s Rapid Spanning Tree
    - IEEE 802.1w Multi-Instance Spanning Tree
    - możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP)
    - tworzenie instancji Rapid Spanning Tree per VLAN
    - możliwość zapewnienia redundancji interfejsów warstwy drugiej bez wykorzystania protokołów rodziny STP poprzez skonfigurowanie interfejsu zapasowego
    - obsługa L2PT (L2 Protocol Tunelling).
    - obsługa 802.1Q tunnelling (Q-in-Q tunnelling).
    - mapowanie (translacja) tagów 802.1Q 1:1, 1:2, 2:1
- funkcjonalności routingu IP:
    - możliwość obsługi min. 20.000 tras routingowych unicast i 1000 multicast (dla IPv4),
    - obsługa routingu IPv4: statyczny, RIPv2, ISIS, OSPF, BGPv4
    - możliwość wirtualizacji tablicy routingu – utrzymywania niezależnych, osobnych tablic rutingu dla poszczególnych segmentów sieci, przypisywania interfejsów fizycznych i logicznych (dotyczy routingu unicast i multicast)
    - obsługa Bidirectional Forwarding Detection (BFD)
    - routing multicast:
        - IGMP v1/v2/v3
        - IGMP Snooping v1/v2/v3
        - PIM sparse mode,
        - Source Specific Multicast
    - sprzętowo przygotowany do obsługi IPv6
- funkcjonalności przełączania MPLS
    - obsługa LDP, T-LDP
    - obsługa enkapsulacji VPWS / EoMPLS
    - MPLS L3VPN (IPv4)
    - MPLS TE

  - MPLS FRR
  - MPLS L2 VPN – EoMPLS
- funkcjonalności bezpieczeństwa sieciowego
  - obsługa VRRP, HSRP lub równoważnego protokołu,
  - mechanizmy ochrony drzewa Spanning-Tree,
  - mechanizmy zapobiegania sztormom ruchu rozgłoszeniowego (broadcast storm)
  - mechanizm ograniczania ilości adresów MAC
  - obsługa list kontroli dostępu (ACL):
    - filtracja w warstwach 2-4,
    - ACL dla VLAN, portów (fizycznych i wirtualnych)
- funkcjonalności zapewnienia jakości ruchu (QoS):
  - obsługa hierarchicznego QoS
  - klasyfikacja ruchu w oparciu o: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, VLAN ID (min. dwa poziomy zagnieżdżenia), DSCP, MPLS EXP
  - obsługa kolejki z bezwzględnym priorytetem w stosunku do innych (Strict Priority), z ograniczaniem ruchu w kolejce priorytetowej,
  - możliwość zmiany przez urządzenie pola 802.1p (CoS), IP ToS/DSCP, MPLS EXP
  - możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting) w oparciu o VLAN ID, DSCP, CoS, adres IP, adres MAC, MPLS EXP
  - możliwość kształtowania (shaping) ruchu wyjściowego
  - dynamiczna alokacja kolejek dla interfejsów, dostępne min. 4.000 kolejek per urządzenie
- funkcjonalności związane z zarządzaniem urządzeniem:
  - funkcjonalność zdalnej diagnostyki połączeń optycznych zgodna z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring lub równoważne)
  - funkcjonalność monitorowania jakości usług na bazie aktywnych próbników ruchu – pomiar min. dostępności, opóźnienia, jego zmian, strat pakietów,
  - obsługa SNMPv3,
  - obsługa SSH,
  - obsługa RADIUS,
  - zarządzanie poprzez interfejs CLI (konsolę),
  - obsługa E-OAM (802.1ag, 802.3ah, E-LMI),
  - obsługa MPLS OAM
  - obsługa Link Layer Discovery Protocol (LLDP, LLDP-MED),
  - możliwość tworzenia makr konfiguracyjnych (zestaw komend konfiguracyjnych, aplikowanych pojedynczym poleceniem),

- min. 5 poziomów dostępu administracyjnego (z możliwością określenia zakresu dostępnych poleceń na poszczególnych poziomach),
- możliwość podłączenie zewnętrznych źródeł sygnałów alarmowych (np. otwarcie drzwi do serwerowni, przekroczenie progowej temperatury w serwerowni) i wysłanie alarmu systemowego w przypadku wystąpienia takich alarmów. Zamawiający dopuszcza rozwiązanie zewnętrzne,
- możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,
- plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line. Konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się restartów urządzenia po dokonaniu zmian.
- plik konfiguracyjny urządzenia musi być zabezpieczony przed niepowołanym dostępem oraz zmianami – tylko osoby uwierzytelnione powinny posiadać dostęp do pliku konfiguracyjnego

Warunki serwisu i gwarancji dla przełączników MPLS

- na dostarczany sprzęt musi być udzielona min. 60-miesięczna gwarancja; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta
- serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego; usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu następnego dnia roboczego od momentu zdiagnozowania usterki; Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań
- Dostarczenie urządzenia przez producenta na wymianę w ciągu następnego dnia roboczego(usługa w standardzie Next Business Day)
- W przypadku Sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki

- Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego
- Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:
    - pobieranie nowych wersji oprogramowania
    - dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej
    - dostęp do pomocy technicznej producentów

VII.2 Kompletny system zabezpieczeń klasy UTM- 1 szt.

Zamawiający określa minimalne wymagania techniczno-funkcjonalne dla przełącznika szkieletowego w sposób następujący:

UWAGA: Zamawiający, z uwagi na podniesienie bezpieczeństwa i uproszczenie zarządzania siecią, wymaga aby urządzenie realizujące funkcję bezpieczeństwa opisane w tym punkcie pochodziły od jednego producenta i współpracowały z centralnym systemem logowania i raportowania (pkt. VII.3) pochodzącym od tego samego producenta co urządzenia realizujące funkcje bezpieczeństwa.
Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Dla elementów systemu bezpieczeństwa obsługujących centralny punkt sieci w lokalizacji serwerowni Centrum Zarządzania Siecią, Wykonawca zapewni wszystkie poniższe funkcjonalności:

- System powinien być zaprojektowany w taki sposób aby możliwa była jego rozbudowa w celu wyeliminowania pojedynczego punktu awarii. W tym celu powinien zapewnić co najmniej:
- Możliwość łączenia w klaster Active-Active lub Active- Passive każdego z elementów systemu.
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- Monitoring stanu realizowanych połączeń VPN z możliwością implementacji mechanizmów redundancji
- System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
- System realizujący funkcję Firewall powinien dysponować minimum 18 portami Ethernet 10/100/1000Base- TX oraz powinien mieć możliwość rozbudowy o 4 dodatkowe interfejsy typu Ethernet 10/100/1000Base- TX lub SFP
- Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLAN y w oparciu o standard 802.1Q.

- W zakresie Firewall obsługa nie mniej niż 1 milion jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę
- Przepustowość Firewall: nie mniej niż 15Gbps
- Wydajność szyfrowania AES lub 3DES: nie mniej niż 3Gbps.

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:

- kontrola dostępu - zapora ogniowa klasy Stateful Inspection
- ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
- poufność danych - IPSec VPN oraz SSL VPN
- ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
- kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM
- kontrola zawartości poczty – Antyspam [AS] (dla protokołów SMTP, POP3, IMAP) oraz ich wersji szyfrowanych z wykorzystaniem SSL
- kontrola pasma oraz ruchu [QoS, Traffic Shaping]
- Kontrola aplikacji oraz rozpoznawanie ruchu P2P
- Możliwość analizy ruchu szyfrowanego SSL
- Możliwość cachowania obiektów dla protokołu http
- Ochrona przed wyciekiem poufnej informacji (DLP)

Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 250 Mbps
Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min. 500Mbps
W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:

- Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
- Dostawca musi dostarczyć nielimitowanego klienta VPN współpracującego z proponowanym rozwiązaniem.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
- Praca w topologii Hub and Spoke oraz Mesh
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.

Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
- haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
- haseł dynamicznych (RADIUS, RSA Secure ID) w oparciu o zewnętrzne bazy danych
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.

Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty:

- ICSA dla funkcjonalności IPSec VPN, IPS, Antywirus
- ICSA lub EAL4 dla funkcjonalności Firewall

Elementy systemu powinny być zarządzane lokalnie za pomocą protokołów co najmniej: HTTPS, SSH jak i mieć możliwość współpracy z dedykowanymi do centralnego zarządzania i monitorowania platformami.
W przypadku awarii systemu powinna istnieć możliwość podmiany systemy w ciągu jednej godziny.
Dostawca musi dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 5 lat, w całym zakresie usług opisanym powyżej i wymaganym przez Zamawiającego. System powinien być objęty serwisem gwarancyjnym producenta przez okres 5 lat, z gwarantowanym czasem usunięcia awarii w trakcie następnego dnia roboczego.
Serwis powinien być realizowany przez Producenta rozwiązania lub Autoryzowanego Dystrybutora Producenta, mającego swoją lokalizację serwisową na terenie Polski.
Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy (należy podać adres WWW). W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania, Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późna. zm."

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania
- Dostarczenie deklaracji zgodności CE na dostarczony sprzęt (wraz z dostawą).

VII.3 System centralnego logowania i raportowania (analiza ruchu i logów w sieci)- 1 szt.

Zamawiający określa minimalne wymagania techniczno-funkcjonalne dla systemu centralnego logowania i raportowania w sposób następujący:

Lp.	Parametr	Minimalne wymagania techniczne
1.	Architektura systemu ochrony	System logowania i raportowania powinien stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta.

2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
3.	Parametry fizyczne systemu	Nie mniej niż 4 porty Ethernet 10/100/1000 Powierzchnia dyskowa - minimum 1 TB Opcjonalnie mechanizm zarządzania dyskami RAID (0,1)
4.	Funkcjonalności podstawowe i uzupełniające	System musi zapewniać: • Składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników • Możliwość gromadzenia zawartości przesyłanych za pośrednictwem protokołów Web, FTP, email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci • Kwarantannę dla współpracujących z nim urządzeń. Kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki. • Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących • Wyświetlanie nowych logów w czasie rzeczywistym • Analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy • Analizę podatności stacji w sieci wraz z możliwością raportowania wykrytych luk • Export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych)
5. A	Parametry wydajnościowe	Urządzenie musi obsługiwać: • Do 2000 urządzeń sieciowych • Do 6000 urządzeń klienckich /VPN- client/
6. A	Aktualizacje sygnatur sprawdzeń	System powinien opcjonalnie umożliwiać: α. Planowania aktualizacji bazy sprawdzeń w czasie (Scheduler)
7.	Zarządzanie	System udostępnia: β. Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH i konsolę szeregową
8. 8.	Zasilanie	Zasilanie z sieci 230V/50Hz.
9. 9.	Instalacja i konfiguracja	Instalacja i konfiguracja systemu powinna być przeprowadzona przez uprawnionego inżyniera posiadającego aktualny certyfikat producenta.

10. 10.	Serwisy, szkolenia i usługi	System powinien być objęty serwisem gwarancyjnym producenta przez okres 5 lat. System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy w ciągu 8 godzin. Serwis powinien być realizowany przez Producenta rozwiązania lub Autoryzowanego Dystrybutora Producenta, mającego swoją lokalizację serwisową na terenie Polski, posiadającego certyfikat ISO 9001 w zakresie usług serwisowych (należy dołaczyć go do oferty). Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy (należy podać adres www), z gwarantowanym czasem usunięcia awarii w ciągu następnego dnia roboczego. Dostawca musi okazać zaświadczenie informujące o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem do naprawy u dystrybutora na terenie polski.

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania

VII.4 Zarządzany przełącznik serwerowy z wbudowaną funkcją obsługi BGP – 1szt.

Zamawiający określa minimalne wymagania techniczno-funkcjonalne dla przełącznika serwerowego z wbudowaną funkcją obsługi BGP, w sposób następujący:

1. Przełącznik musi posiadać minimum 48 portów 10/100/1000 Base - TX oraz 4 porty 10G-BASE-X Ethernet SFP+.
2. Musi zapewniać przepustowość dla całego systemu przynajmniej 120Gbps.
3. Musi zapewniać poziom wydajności systemu na poziomie przynajmniej 90Mpps.
4. Musi obsługiwać minimum 2 wewnętrzne redundantne zasilacze sieciowe typu hot-swap.
5. Musi obsługiwać standardy PoE 802.3af/at
6. Musi obsługiwać SNMPv1, SNMPv2c oraz SNMPv3
7. Musi obsługiwać RMON (Statistics, History, Alarms, Events, Host, HostTopN, Matrix, Capture, Filter).
8. Sprzętowa obsługa routingu IPv4 i IPv6
9. Musi obsługiwać funkcje routingu, w tym: trasy statyczne, OSPF v1/v2, RIPv1/RIPv2, IPv4, routing Multicast (IGMP v1/v2/v3, PIM-SM), Policy Based Routing, Route Maps, VRRP.
10. Musi posiadać mapę tras dla obsługi VRF (Virtual Routing and Forwarding), BGP, OSPF.
11. Musi wspierać pełną tablicę protokołu BGP.
12. Authentykacja MD5 dla protokołów routing
13. Musi oferować zintegrowane funkcje balansowania ruchu w warstwie L4.
14. Musi obsługiwać wielowarstwową klasyfikacje pakietów.
15. Musi obsługiwać IP Class of Service (COS).
16. Musi obsługiwać wiele mechanizmów kolejkowania (SPQ, WFQ, WRR, Hybrid).

17. Musi obsługiwać kontrolę poziomu pasma wychodzącego i przychodzącego w każdym przepływie.
18. Musi obsługiwać technologię 802.1w, 802.1s
19. Pojemność tablicy MAC minimum 65000.
20. Musi obsługiwać opcje Port/VLAN mirroring (jeden do jednego, jeden do wielu, wielu do wielu)
21. Musi obsługiwać technologię 802.3ad Link Aggregation, 48 grup, 48 portów.
22. Musi obsługiwać ograniczniki poziomu ruchu oparte o pasmo lub liczenie pakietów (pps), z progami pasma pomiędzy 8Kbps i 10Gbps.
23. Musi obsługiwać technologię RADIUS Accounting.
24. Musi obsługiwać technologię TACACS+.
25. Musi mieć możliwość ograniczania liczby nowych lub ustanowionych przepływów lub pakietów, które mogą być zaprogramowane na indywidualnym porcie przełącznika by zwalczyć atak DoS.
26. Musi obsługiwać technologie IEEE 802.1X Port Based Network Access, uwierzytelnianie oparte o adres MAC oraz Port Based Web Authentication.
27. Musi obsługiwać dynamiczne i statyczne blokowanie portów oparte o adresy MAC.
28. Musi mieć możliwość automatycznego ograniczania liczby przepływów na porcie i przypisywania akcji do zdefiniowanych ograniczeń.
29. Musi obsługiwać LLDP oraz LLDP- MED.
30. Musi zapewniać kompletne, niepodzielone, nie samplowane dane NetFlow (v5/v9), lub równoważne, ale nie samplowane.
31. Musi automatycznie śledzić informacje o lokalizacji użytkownika/ urządzenia, zbierając przy tym takie informacje jak adres MAC stacji końcowej, czy dane z warstwy 3 (adres IP, itp.) i przekazuje do aplikacji zarządzającej.
32. Musi mieć możliwość określenia lokalizacji urządzenia końcowego w czasie rzeczywistym, w przypadku wystąpienia zdarzenia.
33. Obsługa zewnętrznego systemu logowania zdarzeń SYSLOG, RMON(9 grup), SMON(RFC 2613) VLAN i statystyki
34. Obsługa synchronizacji czasu w oparciu o zewnętrzny serwer SNTP lub NTP
35. Obsługa SNMP v1/v2/v3
36. Sprzętowa obsługa nie samplowanego NetFlow na każdym porcie bez straty wydajności urządzenia lub równoważne, ale nie samplowane.
37. Obsługa SSH klient i serwer,
38. Obsługa Telnet, TFTP, TACACS+, RFC 3580, RADIUS EAP 802.1x, RFC 2865, RFC 2866

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania

Uwaga: W ramach tego zadania Wykonawca włączy dostarczony przełącznik do Systemu Zarządzania (Enterasys Netsight Bundle) charakteryzujący się następującymi funkcjonalnościami i zapełni pełną integrację środowiska istniejące z zaplanowanym w tym postępowaniu:

1. System zarządzania ma architekturę klient-serwer (możliwość instalacji serwera i klienta/ów na oddzielnych maszynach) oraz umożliwia instalację w wersji *standalone* na jednej maszynie.

2. System zarządzania zapewnia możliwość automatycznej wizualizacji mapy urządzeń w sieci wraz z automatycznym wykrywaniem połączeń między tymi urządzeniami (urządzenia wykorzystują LLDP/CDP/STP/VLAN/OSPF).
3. Mapa urządzeń zobrazowuje łącza aktywne i nieaktywne między urządzeniami.
4. System umożliwia tworzenie i zarządzanie VLAN- ami.
5. System posiada narzędzie do łatwego zlokalizowania urządzenia sieciowego: Kojarząc IP z adresem MAC, posiadającego zduplikowany adres MAC lub IP, wyszukuje podane urządzenie po adresie MAC lub IP i wskazuje, na jakim przełączniku i porcie ono występuje.
6. System umożliwia definiowania i zbierania alarmów. Alarmy są grupowane ze względu na ważność i kategorię.
7. System ma możliwość zainstalowania na systemie operacyjnym Microsoft Windows Serwer 2003/2008 lub Linuks.
8. System zarządzania jest zgodny z protokołem SNMP v3.
9. System umożliwia zobrazowanie urządzeń w sposób graficzny (widok panelu czołowego urządzeń z zaznaczonymi portami oraz obrazuje stany tych portów różnymi kolorami). Umożliwia blokowanie i odblokowywanie portów z poziomu aplikacji.
10. System zarządzania zapewnia min. 1 licencję serwera, minimum 5 licencji dla klientów podłączonych do serwera w trybie klient-serwer lub minimum 5 licencji na stanowisku samodzielnym w trybie *standalone*.
11. Klient systemu zarządzania jest dostępny z poziomu WWW.
12. System zarządzania siecią umożliwia zbieranie zdarzeń z przełączników.
13. System zarządzania siecią umożliwia pobranie i aktualizację konfiguracji urządzeń.
14. System zarządzania siecią umożliwia aktualizację *firmware*.
15. System zarządzania obsługuje min. 50 urządzeń w sieci, przy czym urządzenia rozumiane są jako jednostki administracyjne/zarządzane (np. stos przełączników).
16. System zarządzania umożliwia instalację wtyczek (*plug-in*), które umożliwią np. reagowanie na pojawiające się zagrożenia i w trybie on- line zmienianie odpowiednich polityk/ACL dostępu na urządzeniach sieciowych
17. System posiada narzędzie do zarządzania z poziomu systemu.
18. System pozwala na operacje z poziomu systemu uruchamiane centralnie, takie jak odkrywanie urządzeń, zarządzanie zdarzeniami, zbieranie logów zdarzeń i obsługa aplikacji.
19. System udostępnia możliwości modyfikacji, filtrowania i tworzenia własnych elastycznych obrazów sieci.
20. System pozwala na wyświetlanie danych w postaci tabeli lub grafów oraz na wiele OID wybieralnych przez użytkowników.
21. System posiada narzędzie do szybkiego i łatwego odnajdywania fizycznych lokalizacji użytkowników końcowych i systemów oraz określania sposobów ich podłączenia.
22. System umożliwia realizacje zaplanowanych zdarzeń i zadań wykonywanych przez użytkownika oraz planowanie zdarzeń na przyszłość.
23. System ma możliwość podglądu i wyboru obiektów MIB wyświetlanych w postaci drzewa oraz zawiera kompilator dla nowych MIB lub pochodzących od innych dostawców.
24. System umożliwia pełną konfiguracje sieci VLAN wraz z ich monitoringiem.
25. System zapewnia pełne wsparcie dla zdalnego zarządzania wszystkimi urządzeniami sieciowymi, włączając w to urządzenia zarządzane przez SNMP MIB- I lub MIB- II.

System jest wyposażony w aplikację do zarządzania elementami , która posiada:

1. wbudowaną możliwość definiowania reguł/polis dla wszystkich użytkowników, aplikacji, protokołów, VLAN-ów i portów w danej sieci, przynajmniej o następujących funkcjonalnościach:
   a) Posiada zdolność automatycznego egzekwowania raz zdefiniowanych polis na chronionych elementach infrastruktury sieci.
   b) Posiada możliwość definiowania polis dotyczących ograniczania pasma, ograniczania szybkości nowych połączeń sieciowych, priorytetyzowania mechanizmów QoS warstw 2 i 3, stosowania etykiet pakietów, izolowania/poddawania kwarantannie wybranego portu lub VLANa oraz uruchamiania predefiniowanych działań.
   c) Posiada możliwość rozprowadzania polis w całej sieci za pomocą jednego kliknięcia.
   d) Zapewnia automatyczną funkcjonalność w celu zapewnienia dostępu do odpowiednich usług dla każdego użytkownika, niezależnie od miejsca jego logowania do sieci.
   e) pozwala na łatwą implementację, administrację i rozwiązywanie problemów.
   f) Zapewnia kontrolę zdarzeń (logi).
   g) Współpracuje z dotychczasowymi metodami uwierzytelniania.
   h) Obsługuje technologie autentykacji: 802.1x, Radius i MAC

2. Posiada wbudowane szerokie możliwości inwentaryzacji i zmiany opcji zarządzania, przynajmniej o następujących funkcjonalnościach:
   a) Zapewnia możliwość dokładnego katalogowania urządzeń według ich typu.
   b) Ma możliwość pozyskiwania informacji na temat urządzeń takich jak numer seryjny, nadana etykieta, wersja oprogramowania, typ CPU oraz pamięć.
   c) umożliwia prezentację dokładnych informacji na temat konfiguracji, obejmujących datę i czas zapisu konfiguracji, wersję oprogramowania i rozmiar pliku.
   d) Zapisuje dane na temat atrybutów urządzeń i raportować jakiekolwiek zmiany w urządzeniu.
   e) Dostarcza informacje na temat jakichkolwiek zmian w oprogramowaniu i konfiguracji urządzenia.
   f) zapewnia zbiór danych na temat operacji związanych z zarządzaniem spisem urządzeń.
   g) Ma możliwość generowania szczegółowych raportów dla celów katalogowania urządzeń sieciowych.
   h) Posiada możliwość przesyłania do jednego urządzenia lub kilku jednocześnie:
      1) Firmware
      2) obrazów rozruchowych EPROM
      3) szablonów konfiguracji w postaci tekstowej (ASCII)
   i) ma możliwość planowania okresowych kopii zapasowych konfiguracji urządzeń.

3. Pozwala nietechnicznym użytkownikom na łatwe aktywowanie/dezaktywowanie predefiniowanych polis, o przynajmniej następującej funkcjonalności:
   a) pozwala administratorom IT na łatwe definiowanie liczby prekonfigurowanych polis sieciowych i desygnowanie wybranych osób do aktywowania/dezaktywowania tych polis.
   b) ma możliwość natychmiastowego zezwalania lub blokowania działań sieciowych obejmujących dostęp do sieci Web, pocztę elektroniczną i sieć p2p.
   c) jest łatwa do konfiguracji i wdrażania i posiadać prosty, bazujący na sieci Web interfejs aplikacji zarządzającej.
   d) Nie wymaga y jakiekolwiek oprogramowania klienckiego dla końcowych użytkowników lub agenci oprogramowania.

4. W inteligentny sposób współdziała z zaawansowanymi aplikacjami bezpieczeństwa w celu automatycznej reakcji na zagrożenia bezpieczeństwa sieci i spełnia poniższe minimalne wymagania:
   a) udostępnia dynamiczne i konfigurowalne rozwiązania powstrzymywania zagrożeń z szeroką gamą opcji reagowania, tworzenia logów zdarzeń i oceniania
   b) Identyfikuje fizyczną lokalizację źródła ataku i profil użytkownika.
   c) Posiada możliwość podejmowania działań opartych o wcześniej zdefiniowane reguły postępowania w wypadku zagrożeń, informując o podjętych działaniach system IDS przy wykorzystaniu komunikatu Inform SNMPv3.
   d) Ma możliwość automatycznego wyłączania lub izolowania źródła niedozwolonego lub niewłaściwego ruchu zidentyfikowanego przez system IDS/IPS/SIEM/Firewall w szczególności tymi opisanymi w innych punktach.
   e) Zapewnia dokładną kontrolę użytkowników i aplikacji pod względem podejrzanych i nieautoryzowanych działań sieci.
   f) Zapewnia dokładną kontrolę na poziomie portów obejmującą wykrywanie zagrożeń i określanie typów zdarzeń
   g) Zapewnia gromadzenie logów zdarzeń i raportowanie.
   h) Ma możliwość poddania kwarantannie użytkownika podłączonego do danego portu
   i) Ma możliwość izolowania i poddawania kwarantannie źródła ataku, bez wpływu na pracę innych użytkowników oraz istotnych dla urzędu aplikacji i systemów.
   j) Ma możliwość dynamicznej odmowy, ograniczania lub zmieniania właściwości dostępu użytkownika do sieci.

Uwaga: Dostawa wyżej opisanego systemu zarządzania nie jest przedmiotem dostawy w ramach tego postępowania.

VII.5 System zarządzania bezpieczeństwem i analiza ruchu xFlow w sieci (klasa SIEM) – 1 szt.

W celu poprawy bezpieczeństwa sieci, Wykonawca dostarczy i wdroży rozwiązanie klasy SIEM (Security Information and Event Management).

Ujednolicony system korelacji informacji bezpieczeństwa oraz analizator zachowań sieci musi realizować następujące, minimalne funkcjonalności i wymagania techniczne:

1. Rozwiązanie musi realizować centralne zarządzanie wszystkimi komponentami systemu korelacji informacji, zdarzeń i analizy behawioralnej sieci
2. Rozwiązanie musi być zdolne do tworzenia kont wielu użytkownikom oraz przypisywania im uprawnień do konkretnych zakresów adresacji IP, które będą monitorowane.
3. Rozwiązanie musi umożliwiać dostęp w oparciu o zakres uprawnień (*role based access*).
4. Rozwiązanie musi wspierać możliwość zarządzania, analizy oraz raportowania z poziomu przeglądarki WWW (GUI).
5. Rozwiązanie musi wspierać identyfikację aplikacji używających portów innych niż standardowo przypisane, oraz aplikacje, które są tunelowane na inne porty (np. HTTP jako transport dla MS Instant Messenger musi być wykryte jako *Instant Messenger* – a nie jako HTTP).
6. Rozwiązanie musi wspierać automatyczne uaktualnianie informacji przy minimalnym zaangażowaniu użytkownika.
7. System musi obsługiwać informacje przesyłane szyfrowanym połączeniem pomiędzy komponentami.
8. Rozwiązanie musi wspierać zbieranie informacji z różnorodnych zabezpieczeń oraz różnorodnych urządzeń sieciowych

9. Rozwiązanie musi wspierać kolekcjonowanie wydarzeń związanych z bezpieczeństwem sieci oraz logi z różnych urządzeń od różnych producentów.
10. Rozwiązanie musi tworzyć i utrzymywać profile urządzeń, które są zlokalizowane w obrębie sieci.
11. Rozwiązanie musi identyfikować ruch w sieci pochodzący z różnych aplikacji od różnych producentów. Proszę dostarczyć listę aktualnie wspieranych aplikacji oraz producentów.
12. Rozwiązanie musi integrować dane ze skanerów podatności różnych producentów tworząc jednocześnie profile urządzeń. Rozwiązanie musi wspierać Netflow, JFlow, SFlow.
13. Musi wspierać możliwość zbierania informacji o bezpieczeństwie oraz o sieci bez umieszczania agentów oraz mechanizmów typu *host-based* na istniejących klientach końcowych albo na serwerach.
14. Rozwiązanie musi wspierać zewnętrzne mechanizmy magazynowania danych.
15. System musi wspierać przechwytywanie informacji oraz ich dokładna analizę. Suma tych informacji musi być konfigurowalna dla każdego ze strumieni (flow) z osobna.
16. Rozwiązanie musi wykrywać wydarzenia typu „zero- day".
17. Rozwiązanie musi uczyć się na bieżąco normalnego zachowania sieci oraz eksponować pojawiające się na bieżąco zmiany.
18. Rozwiązanie musi wykrywać ataki typu *denial-of-service* (DoS) oraz *distributed denial-of-service* (DDoS).
19. Rozwiązanie musi wykrywać i przedstawiać ruch dotyczący obserwowanych zagrożeń powstających w sieci.
20. Rozwiązanie musi umożliwiać tworzenie rozszerzonych profili i widoków przy pomocy każdego z dostępnych rodzajów przepływów transmisji danych, zewnętrznych źródeł danych lub wcześniej stworzonych profili ruchu.
21. Rozwiązanie musi zapewniać możliwość automatycznego skalowania wrażliwości raportowanych zdarzeń w zależności od słabych punktów wykazywanych przez urządzenia końcowe.
22. Rozwiązanie musi zapewniać możliwość dodawania/przypisywania i zmiany skali wrażliwości do monitorowanych urządzeń bezpieczeństwa.
23. Rozwiązanie musi alarmować bazując na obserwowanych zagrożeniach bezpieczeństwa pochodzących z monitorowanych urządzeń.
24. Rozwiązanie musi alarmować bazując na obserwowanych anomaliach oraz zmianach w zachowaniu się sieci i urządzeń związanych z jej bezpieczeństwem.
25. Rozwiązanie musi alarmować zgodnie z wcześniej ustaloną polityka.
26. Rozwiązanie musi rozróżniać poziomy alarmów, tworząc ich hierarchie w oparciu o priorytety. Poziomy musza być przypisane na podstawie od różnorodnych charakterystyk takich jak: urządzenia sieciowe i końcowe, protokoły i aplikacje.
27. Rozwiązanie musi posiadać mechanizm konfigurowania raportów w celu generowania raportów szytych na miarę.
28. Rozwiązanie musi posiadać możliwość kreowania i przypisywania raportów zgodnie z wcześniej ustalonym planem.
29. Rozwiązanie musi posiadać szablony do łatwego kreowania i dostarczania raportów w oparciu wielopoziomowy ranking, począwszy od zagadnień operacyjnych do biznesowych.
30. Rozwiązanie musi posiadać panel informacyjny do szybkiej wizualizacji z rozróżnieniem na bezpieczeństwo i wykorzystanie sieci.
31. Rozwiązanie musi ułatwiać użytkowanie i konfigurowanie poprzez system szablonów lub konfiguratorów przyspieszających i ułatwiających operacje administracyjne.
32. Rozwiązanie musi posiadać wydajność co najmniej 1000 zdarzeń na sekundę oraz 25 000 strumieni (Flows) na minutę.
33. Rozwiązanie musi zapewniać rozbudowę o kolejne 2500 zdarzeń na sekundę oraz musi umożliwiać podłączenie dodatkowego zewnętrznego wirtualnego kolektora strumieni.

34. Rozwiązanie musi zapewniać redundancję zasilaczy 1+1, co najmniej RAID 1 oraz co najmniej 4 porty 10/100/1000Base-T.
35. W celu podejmowania automatycznych działań prewencyjnych, rozwiązanie musi integrować się z opisanymi w tym dokumencie systemami bezpieczeństwa tj. sieciowym IDS (wymagania pkt. VII.6 oraz systemem zarządzania siecią, którego funkcjonalność została opisana w tym dokumencie w pkt. VII.4.).

Uwaga: System zarządzania bezpieczeństwem klasy SIEM musi integrować się z systemem zarządzania siecią Enterasys Netsight Advanced Bundle na poziomie Modułu ASM (Automatic Security Manager). Wykonawca przeprowadzi integrację obu środowisk w ramach tego projektu.

Moduł ASM wspiera następujące funkcjonalności:

α) udostępnia dynamiczne i konfigurowalne rozwiązania powstrzymywania zagrożeń z szeroką gamą opcji reagowania, tworzenia logów zdarzeń i oceniania

β) Identyfikuje fizyczną lokalizację źródła ataku i profil użytkownika.

χ) Posiada możliwość podejmowania działań opartych o wcześniej zdefiniowane reguły postępowania w wypadku zagrożeń, informując o podjętych działaniach system IDS przy wykorzystaniu komunikatu Inform SNMPv3.

δ) Ma możliwość automatycznego wyłączania lub izolowania źródła niedozwolonego lub niewłaściwego ruchu zidentyfikowanego przez system IDS/IPS/SIEM/Firewall w szczególności tymi opisanymi w innych punktach.

ε) zapewnia dokładną kontrolę użytkowników i aplikacji pod względem podejrzanych i nieautoryzowanych działań sieci.

φ) zapewnia dokładną kontrolę na poziomie portów obejmującą wykrywanie zagrożeń i określanie typów zdarzeń

γ) zapewnia gromadzenie logów zdarzeń i raportowanie.

η) Ma możliwość poddania kwarantannie użytkownika podłączonego do danego portu

ι) Ma możliwość izolowania i poddawania kwarantannie źródła ataku, bez wpływu na pracę innych użytkowników oraz istotnych dla urzędu aplikacji i systemów.

φ) Ma możliwość dynamicznej odmowy, ograniczania lub zmieniania właściwości dostępu użytkownika do sieci.

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania

VII.6 Sprzętowy sieciowy IDS (1 szt.)

System IDP ma być tak zaprojektowany, aby mógł analizować i zabezpieczyć sieć na styku z operatorem dostępu do Internetu, oraz każdym produkcyjnym serwerem instalowanym na potrzeby sieci szerokopasmowej i Urzędu Miasta Ełku.

System musi być zarządzany z centralnej konsoli i charakteryzować się następującymi minimalnymi kryteriami:

1. Musi wspierać zcentralizowaną konfiguracje, kontrolę Sieci i Host Sensorów wraz z wielopoziomowym systemem konfiguracji i realizacji polityk bezpieczeństwa.
2. Musi umożliwiać zarządzanie do minimum 25 sensorów. Oraz umożliwiać rozbudowę do nieograniczonej ilości sensorów.
3. Musi wspierać architekturę klient/serwer wspierając kontrolę bazującą na rolach.
4. Musi wspierać centralne przechowywanie licencji do łatwego zarządzania licencjami dla sond.
5. Musi posiadać graficzny, intuicyjny interfejs użytkownika do łatwego zarządzania.
6. Musi wspierać skalowalną architekturę oraz łatwą rozszerzalność w przypadku zwiększonej potrzeb analizy ruchu.
7. Musi posiadać możliwość rozszerzonego raportowania oraz możliwość zarządzania zdarzeniami w celu monitorowania w czasie rzeczywistym, analizy historii zdarzeń, oraz prognozowania na ich podstawie.
8. Musi umożliwiać podgląd zdarzeń zarówno w czasie rzeczywistym jak i z danych historycznych.
9. Musi wspierać automatyczną dystrybucje aktualnych sygnatur.
10. Musi wspierać tworzenie rozszerzonych sygnatur dla detekcji wszelkich zdarzeń, które są krytyczne dla różnych środowisk.
11. Musi oferować łatwe do zrozumienia, zagregowane dane o wykrytych zdarzeniach, klasyfikowane po poziomie zagrożenia i czasie detekcji.
12. Musi umożliwiać użytkownikowi na wgląd w cała sesję przypisaną do zdarzenia oraz wgląd w powiązane do niego pakiety.
13. Musi umożliwiać instalację i zarządzanie sondami HIDS/HIPS poprzez instalacje dodatkowych licencji.
14. Musi umożliwiać instalację kart sieciowych pracujących w trybie Fail- Open oraz uruchomienie funkcjonalności IPS poprzez wgranie dodatkowej licencji.
15. W celu podejmowania automatycznych działań prewencyjnych, rozwiązanie IDS musi się integrować z systemem zarządzania siecią, którego funkcjonalność została opisana w tym dokumencie w pkt. VII.4., a który nie jest przedmiotem tego postępowania.

IDS dla styku z Internetem

Rozwiązanie IDS musi umożliwiać wykrywanie luk w ochronie danych i bezpieczeństwie z poziomu sieci oraz poprzez dedykowaną aplikacje automatyczne reagować na zagrożenia i charakteryzować się następującymi minimalnymi kryteriami:

1. Wysokiej wydajności architektura umożliwiająca monitorowanie na minimum 8 interfejsach Gigabit-Ethernet za pomocą jednego Sensora, umożliwiająca rozbudowę do 20 interfejsów Gigabit-Ethernet lub 16 interfejsów pracujących w trybie Fail- Open (IPS).
2. Możliwość rozbudowy do systemu IPS, poprzez instalacje dodatkowej licencji oraz kart Fail- Open.
3. Wydajność systemu przy pełnym obciążeniu sygnaturami nie mniejsza niż 1 G/s.
4. Możliwość stosowania wirtualnych Sensorów dla lepszej skalowalności w zespolonych sieciach. (wirtualne Sensory dla VLAN, adresów IP i portów TCP/UDP).

5. Otwarty, bazujący na XML bank sygnatur z ponad 3500 zdefiniowanymi sygnaturami.
6. Proste tworzenie sygnatur specyficznych dla danego użytkownika
7. IDS „Evation Counter Measures“ jako metoda umożliwiająca wykrywanie „częściowych“ ataków.
8. Dekodowanie dużej ilości protokołów (HTTP, UNICODE, SNMP, TELNET, FTP, RPC, DNS, SMTP i SMB) w celu rozpoznania ataków ukrytych w aplikacjach.
9. Możliwość analizy pakietów w warstwach 2-7.
10. Automatyczne dzielenie serii pakietów w danej sesji, gdy tylko sygnatura jest wywoływana.
11. Wykrywanie anomalii IP.
12. Rozpoznawanie high port shell-code i „slow scans“.
13. Wykrywanie skanowania portów.
14. Rozpoznawanie nadużyć sieciowych.
15. Nie dający się podważyć przez fragmenty IP albo niepełne sesje TCP/UDP i „Stick“.
16. Scentralizowane zarządzanie obejmujące IPS/IDS/HIDS/HIPS.
17. Rozpoznawanie „Backdoor“ i „Rogue Server“.
18. Urządzenie musi być również wyposażone przez producenta w bezpieczny system operacyjny (optymalny dla bezpieczeństwa i wydajności).

Uwaga: Centralna konsola zarządcza (dedykowana aplikacja do zarządzania) dla sprzętowego, sieciowego klastra urządzeń IDS musi dać się zintegrować z systemem zarządzania siecią Enterasys Netsight Advanced Bundle na poziomie Modułu ASM (Automatic Security Manager). Wymaganą integrację wykona wykonawca.

Moduł ASM wspiera następujące funkcjonalności:

a) udostępnia dynamiczne i konfigurowalne rozwiązania powstrzymywania zagrożeń z szeroką gamą opcji reagowania, tworzenia logów zdarzeń i oceniania
b) Identyfikuje fizyczną lokalizację źródła ataku i profil użytkownika.
c) Posiada możliwość podejmowania działań opartych o wcześniej zdefiniowane reguły postępowania w wypadku zagrożeń, informując o podjętych działaniach system IDS przy wykorzystaniu komunikatu Inform SNMPv3.
d) Ma możliwość automatycznego wyłączania lub izolowania źródła niedozwolonego lub niewłaściwego ruchu zidentyfikowanego przez system IDS/IPS/SIEM/Firewall w szczególności tymi opisanymi w innych punktach.
e) zapewnia dokładną kontrolę użytkowników i aplikacji pod względem podejrzanych i nieautoryzowanych działań sieci.
f) zapewnia dokładną kontrolę na poziomie portów obejmującą wykrywanie zagrożeń i określanie typów zdarzeń
g) zapewnia gromadzenie logów zdarzeń i raportowanie.
h) Ma możliwość poddania kwarantannie użytkownika podłączonego do danego portu
i) Ma możliwość izolowania i poddawania kwarantannie źródła ataku, bez wpływu na pracę innych użytkowników oraz istotnych dla urzędu aplikacji i systemów.
j) Ma możliwość dynamicznej odmowy, ograniczania lub zmieniania właściwości dostępu użytkownika do sieci.

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania

Instruktaż dla systemów bezpieczeństwa IT

Wdrożenie musi być zakończone bezpłatnym instruktażem, który odbędzie się w siedzibie Wykonawcy. Instruktażu musi dokonać certyfikowany inżynier Wykonawcy posiadający odpowiednio wysoki poziom certyfikacji producenta zaoferowanych urządzeń, odpowiadających przedmiotowi zamówienia.

Podczas instruktażu muszą zostać przekazane informacje niezbędne do eksploatacji zaproponowanych systemów. Instruktażem zostaną objęte 2 osoby w wymiarze 40 godzin. Językiem wykładowym będzie język polski.

Zakres instruktażu:
Routing (1 dzień)

- Przegląd technologii routingu i omówienie, budowa i konfiguracja ACL,
- Routing statyczny, RIP
- Technologia, konfiguracja i implementacja OSPF
- Konfiguracja list dostępowych ACL
- Konfiguracja Virtual Router Redundancy Protocol (VRRP)

Switching (1 dzień)

- Zarządzanie urządzeniami, Firmware upgrade,
- Podstawowa konfiguracja – zagadnienia (Security methods (SNMPv3), konfirguracja, zarządzanie Alarmami i zdarzeniami przy wykorzystaniu systemu zarządzania
- Konfiguracja 802.1Q VLAN's, Spanning Tree (802.1w / 1s) oraz Link Aggregation (802.3ad)

System IDS (1 dzień)

- Omówienie metod i wytycznych dotyczących instalacji systemu głównego i klienta
- Przegląd konfiguracji i procesu wdrażania agentów i rozmieszczenia czujników, struktura katalogów, walidacja procesów
- Przegląd wirtualnych czujników sieci i instrukcje dotyczące konfiguracji segregacji ruchu w sieci.
- Instalacja i rozmieszczenie czujników typu Host, przypisywanie polityk, rozmieszczenie czujników, techniki instalacji.
- Przegląd koncepcji polityki sieci, sygnatury i polityki hostów. Polityki główne sieci, polityki własne, biblioteki sygnatur.
- Omówienie narzędzi analiz i sprawozdań, zasady powiadamiania i alarmów.

System klasy Security Information and Event Management (SIEM) (1 dzień)

- Przegląd rozwiązania

- Wytyczne dotyczące najlepszych praktyk i metod instalacji systemów klasy SIEM
- Omówienie administracji SIEM, konfiguracja konsoli
- Przegląd przepływów jako podstawy do realizacji analizy zachowań behawioralnych w sieci (Network Behavioral Anomaly Detection)
- Przegląd logów, zasilanie danymi z zewnętrznych systematów
- Przegląd domyślnych polityk do wykrywania przypadków naruszenia bezpieczeństwa.
- Przegląd domyślnych wartowników (algorytmy NBAD)
- Raporty zgodności.

Podsumownie (1 dzień)
- Powtórzenie omówionych technologii
- Sposoby rozwiązywania problemów
- Dyskusja dotycząca możliwości i systemu eksploatacji poszczególnych systemów.

VIII. **Urządzenie pomiarowe sieci umożliwiające dokonywanie podstawowych pomiarów sieci optycznej.**

IX. **Stacja zarządzania siecią – komputer typu laptop o minimalnych parametrach: matryca min 17", dysk twardy minimum 500 GB, pamięć RAM minimum 4 GB, wyposażony w system operacyjny w wersji 64 bitowej umożliwiający uruchomienie aplikacji do zarządzania dostarczonymi w ramach niniejszego zamówienia urządzeniami.**

B) Wymaganie szczegółowe dla urządzeń w lokalizacjach wyniesionych - „Wyposażenie Węzłów".

Informacje Ogólne.

Zamawiający, w lokalizacjach wyniesionych, wymaga montażu urządzeń aktywnych tj. przełączników dostępowych LAN i jednostek napięcia gwarantowanego UPS w istniejących szafach telekomunikacyjnych 42U SZAFA – 800x800x2057 (szafy stojące z czterema 19`` belkami nośnymi z możliwością regulacji głębokości drzwi z uchwytem klamkowym i standardowym kluczem, zdejmowane osłony boczne i tylna wejście kablowe w płycie górnej i dolnej, dach z perforacją do instalacji paneli wentylacyjnych).

I. Przełączniki dostępowe (17 szt.)

Zamawiający wymaga zrealizowania tego zakresu w sposób opisany powyżej i wykonanie integracji sieci pomiędzy przełącznikami dostępowymi i przełącznikami szkieletowymi MPLS.

Minimalne wymagania techniczno-funkcjonalne dla przełączników dostępowych:

- przełącznik modularny lub o zamkniętej konfiguracji, posiadający:
  - porty dostępowe (UNI) - min. 24 porty 10/100
  - porty dołączeniowe (NNI) – min. 2 porty 1000BaseX ze stykiem definiowanym przez moduły konwerterów SFP lub równoważne, umożliwiające pracę jako porty 10/100/1000

    - wszystkie porty 1000BaseX muszą umożliwiać obsługę konwerterów w standardach T, SX, ZX, LX/LH, CWDM, DWDM oraz umożliwiać transmisję dwukierunkową na pojedynczym włóknie światłowodowym.
- wbudowane redundantne, wymienne zasilacze i panele z wentylatorami, zasilanie 230V AC,
- wydajność przełączania min. 6Mpps / 8Gbps,
- Certyfikat Metro Ethernet Forum - MEF9 - (EPL, EVPL, ELAN) i MEF14 (EPL, EVPL, ELAN),
- praca w zakresie temperatur: 0-40°C
- możliwość montażu w szafie 19", wysokość nie większą niż 3RU,
- funkcjonalności przełączania Ethernet:
    - możliwość obsługi min. 8.000 adresów MAC, 1.000 sieci VLAN oraz 4.000 VLAN ID,
    - obsługa tzw. Jumbo Frames (9000 bajtów) na portach Gigabit Ethernet,
    - IEEE 802.1s Rapid Spanning Tree
    - IEEE 802.1w Multi-Instance Spanning Tree
    - możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP)
    - tworzenie instancji Rapid Spanning Tree per VLAN
    - możliwość zapewnienia redundancji interfejsów warstwy drugiej bez wykorzystania protokołów rodziny STP poprzez skonfigurowanie interfejsu zapasowego
    - obsługa L2PT (L2 Protocol Tunneling).
    - obsługa 802.1Q tunnelling (Q-in-Q tunnelling).
    - mapowanie (translacja) tagów 802.1Q 1:1, 1:2
- funkcjonalności routingu IP (możliwe do zaimplementowania po zakupie dodatkowej licencji lub wbudowane):
    - możliwość obsługi min. 5.000 tras routingowych unicast i 1.000 multicast,
    - obsługa routingu IPv4: statyczny, RIPv2, ISIS, OSPF, BGPv4
    - możliwość ingerencji w decyzje routingowe w oparciu o polityki (policy-based routing),
    - możliwość wirtualizacji tablicy routingu – utrzymywania niezależnych, osobnych tablic routingu dla poszczególnych segmentów sieci, przypisywania interfejsów fizycznych i logicznych (dotyczy routingu unicast i multicast)
    - routing multicast:
        - IGMP v1/v2/v3
        - IGMP Snooping v1/v2/v3
        - PIM sparse mode,
        - Source Specific Multicast
        - Multicast VLAN Registration
    - sprzętowo przygotowany do obsługi IPv6
- funkcjonalności bezpieczeństwa sieciowego
    - obsługa DHCP server, client, relay,
    - obsługa opcji 82 DHCP,
    - możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu z pozostawieniem możliwości komunikacji z portem nadrzędnym,
    - mechanizm ograniczania ilości obsługiwanych adresów MAC per port przełącznika,

  - autoryzacja użytkowników/portów w oparciu o IEEE 802.1x z opcją przypisania VLANu,
  - mechanizmy ochrony drzewa Spanning-Tree,
  - mechanizmy zapobiegania sztormom ruchu rozgłoszeniowego (broadcast storm),
  - obsługa list kontroli dostępu (ACL):
    - filtracja w warstwach 2-4,
    - ACL dla VLAN,
    - ACL dla portu,
  - mechanizmy ochrony przed atakami związanymi z protokołami ARP i DHCP (DHCP snooping, inspekcja ARP).
  - mechanizmy ochrony warstwy zarządzającej urządzenia (Control Plane) przed atakami DDoS oraz filtracja ruchu zarządzającego
  - możliwość kopiowania ruchu z określonego portu/VLANu na inny port/VLAN urządzenia (mirror)
- funkcjonalności zapewnienia jakości ruchu (QoS):
  - klasyfikacja ruchu w oparciu o: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, VLAN ID,
  - obsługa kolejki z bezwzględnym priorytetem w stosunku do innych (Strict Priority), z ograniczaniem ruchu w kolejce priorytetowej,
  - możliwość zmiany przez urządzenie pola 802.1p (CoS) oraz IP ToS/DSCP,
  - możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting) w oparciu o VLAN ID, DSCP, CoS, adres IP, adres MAC,
  - możliwość kształtowania (shaping – dotyczy portów NNI) i ograniczania (rate limiting, policing) ruchu wyjściowego
- funkcjonalności związane z zarządzaniem urządzeniem:
  - wszystkie interfejsy NNI muszą obsługiwać funkcjonalność zdalnej diagnostyki połączeń optycznych zgodna z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring lub równoważne
  - funkcjonalność monitorowania jakości usług na bazie aktywnych próbników ruchu – pomiar min. dostępności, opóźnienia, jego zmian, strat pakietów,
  - obsługa SNMPv3,
  - obsługa SSH,
  - obsługa RADIUS,
  - zarządzanie poprzez interfejs CLI (konsolę),
  - obsługa E-OAM (802.1ag, 802.3ah, E-LMI Y.1731),
  - obsługa Link Layer Discovery Protocol (LLDP, LLDP-MED),
  - możliwość tworzenia makr konfiguracyjnych (zestaw komend konfiguracyjnych, aplikowanych pojedynczym poleceniem),
  - min. 5 poziomów dostępu administracyjnego (z możliwością określenia zakresu dostępnych poleceń na poszczególnych poziomach),
  - możliwość podłączenie zewnętrznych źródeł sygnałów alarmowych (np. otwarcie drzwi do serwerowni, przekroczenie progowej temperatury w serwerowni) i wysłanie alarmu systemowego w przypadku wystąpienia takich alarmów. Zamawiający dopuszcza rozwiązanie zewnętrzne,
  - możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,

- plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off - line. Konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się restartów urządzenia po dokonaniu zmian.
- plik konfiguracyjny urządzenia musi być zabezpieczony przed niepowołanym dostępem oraz zmianami – tylko osoby uwierzytelnione powinny posiadać dostęp do pliku konfiguracyjnego,

Minimalny zakres instruktażu powdrożeniowego.

Wdrożenie musi być zakończone bezpłatnym instruktażem, który musi się odbyć w siedzibie Zamawiającego. Instruktażu musi dokonać instruktor (certyfikowany przedstawiciel dostawcy sprzętu) lub certyfikowany inżynier wykonawcy posiadający najwyższy poziom certyfikacji (Routing, Swiching) producenta zaoferowanych urządzeń, odpowiadających przedmiotowi zamówienia.

Podczas instruktażu muszą zostać przekazane informacje niezbędne do eksploatacji zaproponowanego rozwiązania.
Instruktażem zostaną objęte 4 osoby w wymiarze 24 godzin, każda.

Minimalny zakres instruktażu:

- Konfiguracja urządzeń typu przełącznik LAN
- Konfiguracja i używanie list kontroli dostępu
- Translacja adresów NAT i PAT
- Konfiguracja routingu:
  - Konfiguracja protokołu OSPF
  - Konfiguracja protokołu RIP
  - Redystrybucja pomiędzy protokołami routingu
  - Konfiguracja protokołu BGP w tym MBGP
- Konfiguracja MPLS
  - L2 VPN
  - L3 VPN
  - Wirtualne tablice routingu na urządzeniach CE
  - Routing pomiędzy urządzeniami PE i CE

Poziom merytoryczny instruktażu powinien umożliwiać osobom ubieganie się w przyszłości o autoryzowany certyfikat i zdanie stosownych egzaminów.

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania

II. System napięcia gwarantowanego UPS w lokalizacjach wyniesionych.

Zamawiający wymaga dostarczenia, wdrożenia i objęcia 5 letnim serwisem gwarancyjnym Systemu Napięcia Gwarantowanego (UPS) składającego się z 17 jednostek UPS 2kVA dostarczonych i uruchomionych we wszystkich 17 lokalizacjach niniejszego postępowania (po jednej sztuce).

Zamawiający wymaga aby dostarczone jednostki UPS były przewidziane do montażu typu Rack 19".

Minimalne wymagania techniczno-funkcjonalne dla UPS 2KVA (węzeł dostępowy)

PARAMETRY	**Parametry minimalne**
Moc pozorna	2200VA
moc rzeczywista	1500W
Architektura UPSa	line-interactive
Liczba, typ gniazd wyj. z podtrzymaniem zasilania	6xIEC 320 C13
Typ gniazda wejściowego	kabel zamontowany na stałe do UPSa zakończony wtyczką Unischuko
Filtracja napięcia wyjściowego	Filtr przeciwzakłóceniowy RFI-EMI tłumik warystorowy
Czas podtrzymania dla obciążenia 100%:	min 5 min
Czas podtrzymania przy obciążeniu 50%:	min 15 min
podstawowy zakres napięcia wejściowego	~160V - ~264V +/-2%
rozszerzony zakres napięcia wejściowego	~150V - ~280V +/-2%
Czas przełączania na pracę bateryjną	< 3ms
kształt napięcia na pracy bateryjnej	sinus
Zimny start	Wymagane
Układ automatycznej regulacji napięcia (AVR):	Wymagane
Porty komunikacji	RS232 i USB, opcja karty SNMP
Sygnalizacja stanu	na panelu przednim przy pomocy diod LED – włączenia do sieci zasilającej; praca z akumulatora; przeciążenia akumulatora
Alarmy dźwiękowe:	praca z baterii, znaczne wyczerpanie baterii
Typ obudowy:	Rack 19", wysokość max 3U
Głębokość	Maks. 400mm
Filtr linii telefonicznej	Wymagane
Filtr sieci LAN	wymagane
Możliwość podpięcia modułu bateryjnego	tak - opcja
Wyposażenie standardowe	instrukcja obsługi, oprogramowanie w języku polskim na CD, kabel szeregowy RS232 (DB9), kabel USB

Czas ładowania baterii wewnętrznych do 90%	3h