ZAŁĄCZNIK NR 1 DO SWZ
Postępowanie nr OPC/BIT/2024/014

Opis przedmiotu zamówienia (OPZ)

Wykonanie systemu IDS wraz z technologią MPLS-TP przeznaczonego do monitorowania sieci i systemów przemysłowych w ZMPG S.A. (z prawem opcji)

I. Opis przedmiotu zamówienia

1. **Przedmiot <u>zamówienia podstawowego</u>** obejmuje:
   1.1. w Etapie 1:
      1.1.1. opracowanie projektu uwzględniającego sieć MPLS-TP zgodnie z wytycznymi projektowymi dla sieci OT (cz. IX.) oraz system monitorowania IDS (cz. II.)
      1.1.2. dostawę urządzeń MPLS-TP (cz. VI. oraz VII.) wraz z systemem centralnego zarządzania i nadzoru siecią MPLS-TP, który będzie umożliwiać między innymi konfigurację urządzeń i usług, zarządzanie siecią, nadzór i obsługę sytuacji awaryjnych w całej sieci (cz. VIII.)
      1.1.3. dostawę licencji systemu monitorowania IDS (cz. III. oraz V.) – licencja dla 1000 asset-ów (przy czym asset stanowi każde wykryte urządzenie biorące udział w komunikacji posiadające adres IP i/lub adres MAC); VLAN-y technologiczne i sieci dodatkowe powinny być monitorowane niezależnymi instancjami systemu monitorowania zgodnie z pkt 2. załącznika „Przedmiot zapytania MPLS-OT"; system monitorowania ma realizować ciągły monitoring sieci i systemów automatyki przemysłowej z uwzględnieniem:
         1.1.3.1. inwentaryzacji systemów
         1.1.3.2. monitorowania zmian w architekturze i komunikacji logicznej
         1.1.3.3. monitorowania ruchu w protokołach przemysłowych
         1.1.3.4. wykrywania wrogich zachowań w rozproszonej sieci przemysłowej
         1.1.3.5. obsługi realizowanej przez centralną konsolę zarządzania alarmami
         1.1.3.6. możliwości realizacji zadania zarówno w architekturze rozproszonej jak i scentralizowanej
      1.1.4 dostawę systemu centralnego zarządzania alarmami, który będzie umożliwiać zarządzenie instancjami systemów IDS do określonych VLAN-ów (cz. IV)
   1.2. w Etapie 2:
      1.2.1 instalację i konfigurację urządzeń sieci MPLS-TP i systemu zarządzania oraz testy systemu MPLS-TP (cz. XI.)
      1.2.2 uruchomienie i wdrożenie pełnego systemu IDS przeznaczonego do monitorowania sieci i systemów przemysłowych obejmującego swoim działaniem wszystkie VLAN-y ujęte w załączniku „Przedmiot zapytania MPLS-OT" dla maksymalnie 1000 asset-ów (cz. X)
   1.3. w Etapie 3:
      1.3.1. przeprowadzenie wszelkiego wymaganego instruktażu powdrożeniowego z obsługi systemów oraz zdarzeń (cz. XIV.)
      1.3.2. przekazanie dokumentacji powykonawczej (cz. XII.)
2. **Przedmiot zamówienia <u>w prawie opcji</u>** obejmuje:
   2.1. w Etapie 1:
      2.1.1.opracowanie projektu rozbudowy sieci MPLS-TP zgodnie z wytycznymi projektowymi dla sieci OT (cz. IX.) oraz system monitorowania IDS (cz. II.)

2.1.2. dostawę urządzeń MPLS-TP (cz. VI. oraz VII.) wraz z systemem centralnego zarządzania i nadzoru siecią MPLS-TP (cz. VIII.)

2.2. w Etapie 2:

2.2.1. rozbudowę systemu IDS wraz z techniką MPLS-TP przeznaczonego do monitorowania sieci i systemów przemysłowych w ZMPG S.A., w zakresie określonym w SWZ (wraz z załącznikami)

2.2.2. rozszerzenie licencji systemu monitorowania IDS (cz. III.) o monitorowanie dodatkowych asset'ów w liczbie do 500 [do 500 monitorowanych adresów IP / MAC biorących udział w ruchu z monitorowanych systemów], Zamawiający prosi o przedstawienie ceny dla 500 asset'ów oraz o podanie ceny per licencja

2.2.3. dostarczona licencja musi być typu tzw. „Enterprise", czyli musi umożliwiać instalację systemu IDS jako kilku instancji fizycznych

2.2.4. system monitorowania realizuje ciągły monitoring sieci i systemów automatyki przemysłowej z uwzględnieniem:

2.2.4.1. inwentaryzacji systemów

2.2.4.2. monitorowania zmian w architekturze i komunikacji logicznej

2.2.4.3. monitorowania ruchu w protokołach przemysłowych

2.2.4.4. wykrywania wrogich zachowań w rozproszonej sieci przemysłowe

2.2.4.5. obsługi realizowanej przez centralną konsolę zarządzania alarmami

2.2.4.6. możliwości realizacji zadania zarówno w architekturze rozproszonej jak i scentralizowanej

2.2.5. podłączenie nowych instancji systemu ciągłego monitorowania do używanego przez Zamawiającego systemu centralnego zarządzania alarmami, który umożliwia zarządzenie instancjami systemów IDS dla określonych VLAN-ów

2.2.6. przeniesienie i rekonfigurację istniejących oraz instalację i konfigurację nowych urządzeń sieci MPLS-TP wraz z rekonfiguracją i konfiguracją systemu zarządzania systemu MPLS-TP (cz. XI.)

2.2.7. uruchomienie i parametryzację kolejnych instancji systemu IDS w ramach dostarczonej licencji (do 500 nowych asset'ów)

2.2.8. zbudowanie wzorca sieci (tzw. baseline) dla nowo objętych monitorowaniem przez system IDS podsieci systemów OT

2.2.9. opis monitorowanej infrastruktury (assetów) w systemie IDS zgodnie z oczekiwaniami Zamawiającego

2.2.10. wykonanie niezbędnych analiz ruchu sieciowego i opracowanie rekomendacji w zakresie zabezpieczeń dla monitorowanych VLAN-ów

2.3. w Etapie 3:

2.3.1. przeprowadzenie instruktażu powdrożeniowego

2.3.2. przekazanie dokumentacji powykonawczej

3. Zamawiający gwarantuje serwer wraz z wirtualizacją (VMware) parametrach zawartych w *Załącznik 1* pkt 4:

Lista dodatkowych wymagań oraz protokołów stanowi *Załącznik nr 1* do OPZ.

Schemat poglądowy z podziałem na zamówienie podstawowe i w prawie opcji stanowi *Załącznik nr 2* do OPZ.

II. System monitorowania

1. System monitorowania - założenia ogólne
   1.1. Licencja oprogramowania systemu monitorowania IDS ma być licencją w modelu subskrypcji na okres 36 m-cy z gwarancją aktualizacji w okresie obowiązywania umowy (36 m-cy)
   1.2. Licencja ma obsługiwać do 1000 assetów w ramach zamówienia podstawowego oraz do 500 dodatkowych asset'ów w ramach prawa opcji, przy czym asset stanowi każde urządzenie biorące udział komunikacji posiadające adres IP i/lub adres MAC
   1.3. Licencja ma umożliwiać instalacje na dowolnej ilości serwerów a ograniczona może być tylko ilością monitorowanych assetów
   1.4. Wymaga się objęcia systemu sterowania rozwiązaniem do ciągłego monitorowania i wykrywania zagrożeń na podstawie pasywnej analizy ruchu sieciowego – IDS
   1.5. Identyfikacja niezgodności w ruchu sieciowym oraz wykrywanie zagrożeń musi być oparte o analizę pakietów oraz głęboką analizę pakietów (ang. Deep packet inspection - DPI) dla przemysłowych protokołów komunikacyjnych *Załącznik nr 1*
   1.6. Rozwiązanie do ciągłego monitorowania musi składać się z elementów pozwalających na zbudowanie elastycznej architektury umożliwiającej monitorowanie obiektów posiadających od kilkunastu do ponad stu urządzeń. Szczegółowe wymagania funkcjonalne dla elementów systemu monitorowania przedstawione są w części III.
   1.7. W skład systemu monitorowania powinny wchodzić:
      1.7.1. Centralna konsola IDS - system do prezentacji i zarządzania zdarzeniami zbieranymi z podrzędnych mu systemów/sensorów/sond systemu IDS – centralna konsola powinna być umieszczona w centrali spółki
      1.7.2. Systemy IDS –autonomiczny system analizy ruchu sieciowego i wykrywania incydentów, rozwiązanie ma działać pasywnie w oparciu o kopię ruchu sieciowego dostarczonego z portów mirror przełączników:
         1.7.2.1. przez infrastrukturę MPLS-TP oraz przez istniejącą infrastrukturę sieciową Zamawiającego – na etapie zamówienia podstawowego
         1.7.2.2. wyłącznie przez infrastrukturę MPLS-TP – na etapie rozszerzenia zamówienia podstawowego o prawo opcji
         Rozwiązanie ma umożliwiać monitorowanie sieci wymienionych w *Załączniku nr 1* ppkt 2.1 oraz ppkt 2.2 niezależnymi instancjami systemu IDS
   1.8. Zdarzenia identyfikowane przez system ciągłego monitorowania muszą być na bieżąco wysyłane do podmiotu świadczącego usługę SOC
   1.9. System ciągłego monitorowania IDS musi mieć funkcjonalność tworzenia cyfrowego obrazu sieci, który może być wykorzystany przez system automatyzujący analizę ryzyka
   1.10. Po stronie Wykonawcy jest zapewnienie usług transmisji danych dla systemu IDS realizowanych w oparciu o technikę MPLS-TP

III. Wymagania dla systemu monitorowania w trybie ciągłym

Zamawiający oczekuje przedstawienia oferty wdrożenia systemu klasy IDS (Intrusion Detection System). System musi być pasywnym rozwiązaniem monitorowania bezpieczeństwa sieci i inwentaryzacji. System musi analizować kopię ruchu sieciowego dostarczoną z portów mirror/span przełączników sieciowych. System powinien umożliwiać monitorowanie sieci rozproszonej geograficznie. System powinien być rozwiązaniem programowym – niezależnym od platformy sprzętowej pochodzącej od konkretnego dostawcy. System musi umożliwiać wdrożenie jako maszyna wirtualna. System musi zapewniać wysoki poziom skalowalności umożliwiając monitorowanie małych obiektów (do 50 assetów) jak również całych grup obiektów (powyżej 500 assetów). System monitorowania najmniejszych obiektów musi działać na standardowym komputerze przemysłowym 4 rdzenie CPU, do 16 GB RAM.

1. Wymagania główne
   1.1. System musi zapewniać możliwość monitorowania sieci rozproszonej geograficznie oraz współpracować z opcjonalnymi sondami sprzętowymi
   1.2. System musi umożliwiać bezpośrednie podłączenie do niego źródeł ruchu (kopia ruchu z portów mirror/SPAN)
   1.3. System musi umożliwiać analizę zapisu ruchu sieciowego w postaci wgranych do systemu plików PCAP system powinien obsługiwać pliki o rozmiarze do 10 G
   1.4. System musi dostarczać dane niezbędne do prowadzenia procesów Oceny Ryzyka (Risk Assesment) dla sieci ICS
   1.5. System musi dostarczać API, umożliwiające integrację aplikacji autorskich Zamawiającego z bazą danych rozwiązania
   1.6. System musi działać w trybie pasywnym (bez generowania dodatkowego ruchu w monitorowanej sieci)
   1.7. System musi dostarczać funkcje audytu działań jego użytkowników i zapewniać możliwość przesyłania danych o tych akcjach za pomocą protokołu syslog
2. Funkcje analityczne i wspierające analizę
   2.1. System musi umożliwiać analizę danych zebranych w trakcie pracy
   2.2. Każdy zestaw danych prezentowanych przez system musi zapewniać:
      2.2.1. Filtrowanie prezentowanych danych na podstawie zawartości wpisu, danych takich jak treść alarmu, adresy IP, MAC oraz metadanych takich jak np. godzina utworzenia
      2.2.2. Wszystkie dane tabelaryczne pozyskane z systemu powinny być eksportowane do formatów JSON, PDF i CSV, jak również możliwe do uzyskania za pomocą API
      2.2.3. Każdy wpis w zestawach danych dot. Zdarzeń (konsola alarmów) musi zapewniać możliwość uzyskania dokładniejszych informacji o przyczynie i urządzeniach biorących udział w komunikacji oraz dostęp do zapisów pakietów w formie plików PCAP
   2.3. System musi zapewnić możliwość utworzenia dowolnego raportu na podstawie zapytań do bazy danych oraz możliwość generowania raportu z całości okresu działania systemu a także powinien zapewniać możliwość przesyłania raportów okresowych za pomocą wiadomości e-mail
   2.4. System musi zapewniać prezentację wektorów ataku w formie graficznej na mapie
   2.5. System musi wspierać analizę ryzyka, przez umożliwienie tworzenia grup procesów biznesowych i określenie zasobów, od których procesy te zależą a także krytyczności procesów
   2.6. System musi wspierać analizę DPI dla protokołów przemysłowych ujętych w *Załącznik nr 1* pkt. 1.
   2.7. System musi zapewnić możliwość dodawania komentarzy do alarmów oraz zapewnić możliwość definicji procedur postępowania dla kategorii alarmów (Playbook)
   2.8. System musi zapewnić możliwość pobrania wszystkich plików PCAP powiązanych z alarmami wykrytymi przez system oraz zbierać pliki PCAP przez okres co najmniej 21 dni z całości ruchu
3. Wykrywanie anomalii
   3.1. System musi raportować wykryte anomalie w komunikacji sieciowej na warstwach 2, 3, 4, 7 modelu ISO/OSI
   3.2. System musi dostarczać sygnaturowy mechanizm detekcji z regułami dla środowiska przemysłowego, a także dostarczać sygnatury zagrożeń dla protokołów przemysłowych oraz sygnatury zagrożeń dla protokołów IT
   3.3. System musi dostarczać behawioralny mechanizm detekcji
   3.4. System musi przedstawiać rekomendacje dla wykrytych problemów wykrytych w sieci, zasobach i konfiguracji samego systemu monitorowania, w odniesieniu do norm lub dobrych praktyk stosowanych w sieciach OT
   3.5. System musi dostarczać mechanizm wspierający śledzenie postępów prac związanych z rekomendacjami np. oznaczenie zadań jako rozwiązane, otwarte/w trakcie analizy, ignorowane, odroczone

3.6. System musi raportować zdarzenia inwentaryzacyjne takie jak wykrycie nowych zasobów w sieci, wykrycie nowych połączeń w sieci, wykrycie nowych adresów MAC, wykrycie prób komunikacji do sieci Internet, wykrycie zbyt długiej przerwy w komunikacji zasobu

3.7. System musi raportować wykryte anomalie i zdarzenia bezpieczeństwa m.in.:

3.7.1. podejrzenie ataku MitM (np. ARP Spoofing)

3.7.2. skanowanie portów i sieci

3.7.3. zdarzenia wykryte przez silnik sygnaturowy w tym znane ataki sieciowe oraz znane charakterystyki ruchu złośliwego oprogramowania

3.7.4. zdarzenia pasujące do zdefiniowanych przez administratora reguł zrealizowanych w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych które zostały wymienione w Złączniku nr 1.

3.8. System musi dostarczać dane o wykrytych anomaliach w postaci czytelnej centralnej konsoli alarmów

3.8.1. Konsola alarmów musi czytelnie oddzielać alarmy aktywne (nowe) od przetworzonych (archiwalne)

3.8.2. Konsola alarmów musi dostarczać następujących informacji wadze zdarzenia (jego dotkliwość), dacie pierwszego wykrycia, dacie ostatniej modyfikacji, źródle ruchu oraz celu, a także wskazywać protokoły wykorzystane w komunikacji

3.9. System musi umożliwiać raportowanie wykrycia dowolnego ruchu sieciowego o zadanej przez Zamawiającego charakterystyce w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych)

3.10. System musi analizować i prezentować anomalie protokołów przemysłowych m.in.:

3.10.1. nieautoryzowana komunikacja przemysłowa

3.10.2. anomalie protokołów przemysłowych

3.10.3. naruszenie zdefiniowanej polityki komunikacji przemysłowej

4. Możliwości konfiguracji i modyfikacji zasad detekcji

4.1. System musi dostarczać niezbędnych danych do zrozumienia zasad działania reguł (Treść reguły, odniesienia do źródeł takich jak bazy CVE, Baza wiedzy Microsoft, Framework MITRE ATT&CK, itp.) oraz umożliwiać czytelny podgląd wszystkich reguł i ich wyjątków

4.2. System musi umożliwiać modyfikację istniejących oraz tworzenie nowych sygnatur oraz umożliwiać włączanie i wyłączanie dowolnych sygnatur dla dowolnego komponentu systemu OT

4.3. System musi umożliwiać modyfikację i tworzenie nowych wyjątków dla sygnatur na podstawie parametrów warstw 2, 3, 4, 7 modelu ISO/OSI bezpośrednio z konsoli alarmów po wystąpieniu zdarzenia, a także przed wystąpieniem zdarzenia oraz w trakcie okresu tworzenia wzorca ruchu sieciowego

4.4. System w trybie nauki musi generować sugerowany wzorzec ruchu, który po przeglądzie i jego akceptacji utworzy automatycznie niezbędne wyjątki dla sygnatur

4.5. System musi zapewniać możliwość tworzenia nowych i modyfikację istniejących (bezczynny/detekcja/nauka) trybów pracy pozwalając włączać i wyłączać poszczególne silniki detekcji uruchomionych w poszczególnych trybach i dostosowywać ich konfigurację, w celu precyzyjnego określenia zachowania metod detekcji

4.6. System musi umożliwiać prowadzenie działań proaktywnego wyszukiwania zagrożeń w sieci (Threat Hunting)

4.7. System w czasie pracy musi automatycznie w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych zgodnych z zapisami *Załącznik nr 1*) tworzyć sugestie detekcji, dotyczące zaobserwowanego ruchu, które operator może włączyć i dostosować aby wykorzystać je jako reguły dodatkowe wzbogacające detekcję sygnaturową

4.8. System musi, za pomocą kreatora obecnego w GUI systemu, umożliwiać tworzenie własnych reguł detekcji, w celu wzbogacenia detekcji sygnaturowej, w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych zgodnie z *Załącznik nr 1* pkt 1.

4.9. System musi umożliwiać przypisanie dowolnego dostępnego mechanizmu DPI do dowolnego portu TCP/UDP oraz umożliwiać tworzenie własnych modułów DPI dla protokołów autorskich

4.10. System musi umożliwiać precyzyjne określenie zakresu adresacji sieci będącej siecią chronioną/monitorowaną (tzw. sieć domowa, ang. home net) oraz umożliwiać definicję zaufanych adresów IP spoza sieci chronionej

4.11. System musi dostarczyć mechanizm ograniczenia wolumenu analizowanego ruchu przez filtrowanie ruchu przychodzącego np. na podstawie identyfikatora VLAN

5. Funkcje Inwentaryzacyjne

5.1. System musi zapewniać funkcje automatycznego wykrywania zasobów systemów automatyki i sterowania takich jak PLC, HMI, Serwer SCADA, OPC Serwer, Serwer Historian, Stacje operatorskie, stacje inżynierskie, Router i przypisywać im automatycznie określony typ oraz umożliwiać przypisywanie własnych typów dla urządzeń niezdefiniowanych przez producenta systemu

5.2. System musi inwentaryzować urządzenia komunikujące się z wykorzystaniem warstwy 2 ISO/OSI i wyższych oraz inwentaryzować urządzenia komunikujące się wyłącznie w warstwie 2 ISO/OSI (tj. nieposiadające adresu IP)

5.3. System musi wykonywać pasywną identyfikację systemu operacyjnego (minimum rodziny systemów Microsoft Windows) urządzenia i jego wersji

5.4. System musi udostępniać dane o zinwentaryzowanych zasobach i połączeniach w formie tabelarycznej i umożliwiać eksportowanie tych danych do formatów co najmniej: JSON, CSV, PDF

5.5. System musi aktualizować zestawy danych o zasobach i połączeniach w trybie ciągłym. Jest to równoznaczne z odświeżaniem tych danych w tabelach i na mapie połączeń

5.6. System musi prezentować informacje o wykorzystywanych protokołach w połączeniach sieciowych w formie tabelarycznej i umożliwiać eksportowanie tych danych do formatów co najmniej: JSON, CSV, PDF

5.7. System musi prezentować informacje o wykorzystywanych protokołach w połączeniach sieciowych w formie graficznej na mapie i umożliwiać eksportowanie widoku do pliku graficznego PNG

5.8. System musi rozpoznawać automatycznie przypisanie urządzeń do stref (zones) według standardu IEC 62443 oraz rozpoznawać automatycznie kanały komunikacyjne (conduits) pomiędzy strefami zgodnie ze standardem IEC 62443

5.9. System musi określać producenta urządzenia na podstawie zebranych danych

5.10. System musi wykonywać analizę podatności na podstawie wykrytych lub podanych przez administratora wersji systemu operacyjnego

5.11. System musi analizować wykorzystanie pasma przez każdy zasób i połączenie sieciowe

5.12. System musi umożliwiać dodawanie do karty urządzenia zdefiniowanych przez administratora kryteriów opisu danego zasobu/urządzenia, akcja ta powinna być dostępna globalnie dla urządzeń oraz lokalnie dla pojedynczego urządzenia. Systemu musi umożliwiać filtrowanie danych po stworzonych kryteriach oraz umożliwiać ich eksport do plików CSV, JSON, PDF. Dane te powinny być też dostępne w raporcie generowanym przez system

5.13. System musi zapewnić możliwość importu pliku w formacie minimum CSV, w celu wykonania wsadowej modyfikacji minimum nazwy, typu, producenta, każdego z wykrytych urządzeń

5.14. System musi umożliwiać grupowanie urządzeń w monitorowanej sieci w zależności od ich wpływu na poszczególne procesy biznesowe zachodzące w organizacji. Jedna grupa (proces biznesowy) może zawierać wiele urządzeń, a każde urządzenie może być członkiem wielu grup

5.15. System musi zapewnić możliwość modyfikacji wagi alarmów w zależności od krytyczności procesu biznesowego/typu urządzenia/indywidualnych wymogów urządzenia i właściciela systemu
5.16. System musi umożliwić edycję danych o producencie urządzenia, a także umożliwiać edycję nazw zasobów oraz dodawanie komentarzy do zasobów
5.17. System musi umożliwiać przypisanie więcej niż jednego adresu MAC do urządzenia, umożliwiając inwentaryzację klastrów systemów
5.18. System musi umożliwiać edycję danych o wykrytym systemie operacyjnym (w minimalnym wariancie dla MS Windows) wraz z informacjami o aktualizacjach nałożonych na ten system
5.19. System musi analizować i prezentować w karcie zasobu dodatkowe informacje w oparciu o analizę wykrytego ruchu protokołów ujętych w Z*łączniku nr 1*.
5.20. System musi analizować i prezentować przesyłane przez sieć komendy protokołów przemysłowych ujętych w Z*ałączniku 1*.

6. Interfejs oraz funkcje mapy
   6.1. System musi dostarczać czytelnych informacji na temat istotnych zdarzeń zaobserwowanych w sieci (alarmów) oraz informacji o trybie pracy rozwiązania (bezczynny/detekcji/nauki)
   6.2. System musi umożliwiać świadome przełączanie między trybami pracy wg. harmonogramu oraz ręcznie
   6.3. System musi dostarczać funkcje prezentowania zebranych danych o zasobach i ich połączeniach w postaci graficznej (Mapa połączeń), mapa musi być interaktywna, tj. umożliwiać uzyskanie szczegółowej informacji o prezentowanych na niej zasobach lub połączeniach (np. poprzez zaznaczenie urządzenia/połączenia kliknięciem)
   6.4. Interfejs musi posiadać możliwość zmiany języka na język polski oraz angielski
   6.5. Funkcja mapy musi wyświetlać schemat połączeń logicznych pomiędzy węzłami sieci oraz umożliwiać tworzenie własnych widoków w modelach: przepływu, PERA, zdefiniowanym przez użytkownika minimum zmieniając geometryczne rozłożenie obiektów na mapie
   6.6. Funkcja mapy musi umożliwiać wykorzystanie zdefiniowanych procesów biznesowych w celu stworzenia osobnych widoków mapy, ułatwiających analizę
   6.7. System musi prezentować na mapie fakt wykrycia routerów na trasie połączeń
   6.8. System musi prezentować na mapie kierunek komunikacji pomiędzy urządzeniami, a także wskazywać na mapie urządzenia zagrożone i dotknięte anomaliami
   6.9. System musi umożliwiać tworzenie własnych widoków mapy na podstawie grup procesów biznesowych lub z wykorzystaniem filtrowania zasobów (kluczem powinny być minimum adresy IP, adresy MAC, podsieci, producenci, cechy komunikacji jak np. komunikowanie się przez router lub lokalizacja poza siecią chronioną) oraz umożliwiać zapis widoku mapy do pliku graficznego
7. Integracje
   7.1. System musi umożliwiać integrację z dowolnym rozwiązaniem SIEM oraz wspierać przesyłanie danych za pomocą protokołu syslog w formatach CEF i LEEF
   7.2. System musi umożliwiać integrację z dowolnym rozwiązaniem kolejkowania pracy (np. ITSM) poprzez wysyłanie wiadomości e-mail
   7.3. System musi zapewniać granularną kontrolę przesyłanych danych protokołu syslog w zależności od: źródła powstawania komunikatów (silnika detekcji) oraz wagi komunikatu (krytyczność alarmu)
   7.4. System musi umożliwiać przesłanie dowolnego zestawu informacji do dowolnej ilości odbiorców syslog, lub e-mail oraz umożliwiać tworzenie i przesyłanie za pomocą wiadomości e-mail raportów okresowych o wykrytych anomaliach i zdarzeniach, zawierające minimum adresy źródłowe i docelowe, daty wystąpienia alarmów i treści alarmów
   7.5. System musi integrować się jako odbiorca danych ze strumieni syslog, w celu wzbogacenia wewnętrznej bazy danych
   7.6. System musi integrować się z kolejkami workflow wybranych rozwiązań firewall, w celu przesyłania sugestii reguł firewalla, Lista rozwiązań stanowi *Załącznik nr 1* pkt 3.

7.7. System musi dostarczać API, dla integracji z dowolną aplikacją tworzoną w Organizacji
7.8. System musi integrować się z usługą Active Directory w celu zarządzania kontami użytkowników systemu
7.9. System powinien integrować się z rozwiązaniem RSA SecureID
7.10. System powinien dostarczać lokalne zarządzanie kontami użytkowników
7.11. System powinien dostarczać mechanizm zarządzania uprawnieniami użytkowników co najmniej dla trzech zdefiniowanych ról

8. Kontrola poprawności działania systemu
   8.1. System musi zapewniać podgląd stanu systemu, w tym:
      8.1.1. Użycie CPU
      8.1.2. Użycie pamięci RAM
      8.1.3. Wykorzystanie miejsca na dysku
      8.1.4. Wykorzystanie pasma na każdym z interfejsów
   8.2. System musi zapewniać możliwość monitorowania jego stanu za pomocą protokołu SNMP
   8.3. System powinien generować rekomendacje dotyczące stanu jego konfiguracji oraz bezpieczeństwa

IV. Wymagania dla centralnego systemu nadzoru nad alarmami

1. Zamawiający oczekuje przedstawienia oferty wdrożenia centralnego systemu nadzoru nad oferowanymi rozwiązaniami klasy NSM/IDS. Wymagania główne:
   1.1. System musi być kompatybilny z wybranym przez Zamawiającego rozwiązaniem IDS/NSM
   1.2. System musi zapewniać możliwość monitorowania sieci rozproszonej geograficznie
   1.3. System musi umożliwiać tworzenie logicznych segmentów zawierających jeden lub więcej systemów NSM/IDS
   1.4. System musi umożliwiać precyzyjne przydzielanie dostępu użytkowników z poziomem uprawnień Administrator/Ekspert/Analityk dla członków grupy odpowiedzialnej za konkretny obiekt:
      1.4.1. Indywidualnie dla każdego segmentu monitorującego konkretny obiekt
      1.4.2. Do każdej z grup segmentów monitorujących konkretne obiekty
      1.4.3. Globalnie do wszystkich segmentów
   1.5. System musi agregować dane z poszczególnych segmentów i przedstawiać je wyłącznie uprawnionym użytkownikom
   1.6. System może prezentować dane z poszczególnych systemów w postaci mapy uwzględniającej ich rozmieszczenie geograficzne
   1.7. System musi agregować dane sumaryczne dotyczące ilości alarmów, połączeń i zasobów
   1.8. System musi dostarczać czytelnych danych o alarmach wykrytych przez poszczególne silniki systemy IDS/NSM. Minimalnie system musi wskazywać alarmy cyberbezpieczeństwa i inwentaryzacji zasobów sieci
   1.9. System musi umożliwiać scentralizowaną pracę z alarmami obecnymi w poszczególnych platformach IDS w tym:
      1.9.1. archiwizację alarmów
      1.9.2. dodawanie komentarzy
      1.9.3. tworzenie wyjątków
      1.9.4. przegląd, sortowanie i filtrowanie alarmów
   1.10. System musi umożliwiać scentralizowaną pracę z zasobami zinwentaryzowanymi na poszczególnych instancjach IDS
   1.11. System musi dostarczać funkcje audytu działań jego użytkowników i zapewniać możliwość przesyłania danych o tych akcjach za pomocą protokołu syslog
   1.12. System musi umożliwiać aktualizację oprogramowania na wszystkich rozwiązaniach IDS, będących pod kontrolą centralnego systemu zarządzania

1.13. System musi integrować się z usługą Active Directory w celu zarządzania kontami użytkowników systemu
1.14. System powinien integrować się z rozwiązaniem RSA SecureID
1.15. System powinien dostarczać lokalne zarządzanie kontami użytkowników
1.16. System powinien dostarczać mechanizm zarządzania uprawnieniami użytkowników RBAC
1.17. System musi zapewniać podgląd stanu systemu, w tym:
1.17.1. użycie CPU
1.17.2. użycie pamięci RAM
1.17.3. wykorzystanie miejsca na dysku
1.17.4. wykorzystanie pasma na każdym z interfejsów
1.18. System musi zapewniać możliwość monitorowania jego stanu za pomocą protokołu SNMP

V. Wymagania dla FW

1. FW ma służyć do zabezpieczenia styku podsieci OT z systemami biznesowymi poprzez zbudowanie strefy DMZ. Wymagania ogólne dla zabezpieczenia i monitorowania komunikacji w obrębie systemów OT:
1.1. Obudowa o wysokości 1U dostosowana do implementacji w szafie RACK 19”
1.2. Urządzenie służące do monitorowania i zabezpieczenia komunikacji musi mieć funkcjonalność firewall’a klasy Stateful Inspection w celu filtrowania ruchu sieciowego z wykorzystaniem reguł opisujących dopuszczony ruch sieciowy za pomocą:
1.2.1.adresu IP źródła komunikacji
1.2.2.źródłowego portu TCP lub UDP
1.2.3.adresu IP celu
1.2.4.docelowego portu TCP lub UDP
1.2.5.protokołu warstwy aplikacyjnej
1.2.6.harmonogramów czasowych
1.3. Urządzenie ma mieć możliwość aktywowania licencji zapewniającej analizę protokołów przemysłowych co najmniej takich, jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV)
1.4. Urządzenie musi mieć funkcjonalność routera i możliwość realizowania routingu w oparciu o:
1.4.1.reguły statyczne
1.4.2.protokoły dynamiczne: OSPF, RIP
1.5. Urządzenie musi posiadać możliwość tworzenia reguł dla translacji adresów NAT i przekierowania portów PAT
1.6. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing)
1.7. Urządzenie musi posiadać możliwość filtrowania ruchu w trybie transparentnym dla wskazanych portów. Oznacza to możliwość egzekwowania wszystkich polityk firewalla dla portów zgrupowanych jako bridge (ta sama podsieć IP bez routingu)
1.8. Urządzenie musi tworzyć logi zarówno dla komunikacji dozwolonej jak i zablokowanej
1.9. Urządzenie musi mieć wewnętrzną pamięć pozwalającą na zapis i przechowywanie logów lokalnie
1.10. Urządzenie musi wysyłać logi za pomocą protokołu syslog do min. 3 określonych serwerów logów / SIEM przy jednoczesnym zdefiniowaniu:
1.10.1. Protokołu i portu dla przekazywania logów
1.10.2. Kategorii (ang. facility)

1.10.3. Rodzaju logów przekazywanych, min: logi dot. połączeń, logi z firewalla, IPS/IDS, alarmy, dzienniki systemowe

1.11. Urządzenie musi posiadać funkcjonalność IPS z możliwością przełączenia w tryb IDS czyli tylko monitorowania bez blokowania w przypadku wykrycia zagrożeń lub anomalii

1.12. Wbudowany IPS/IDS musi być oparty o sygnatury wykrywające znane zagrożenia i ataki sieciowe

1.13. Urządzenie musi zapewniać możliwość dodawania własnych sygnatur IPS

1.14. Urządzenie musi być wyposażone w minimum osiem miedzianych interfejsów Ethernet 10/100/1000 Mbit/s (z których każdy można dowolnie zdefiniować jako np. WAN, LAN, BRIDGE, MANAGEMENT lub DMZ) oraz minimum dwa interfejsy światłowodowe 1GbE

1.15. Urządzenie powinno umożliwiać instalację modułu rozszerzeń z poniższej listy:

1.15.1. moduł z 8 interfejsami miedzianymi 2,5Gbit/s

1.15.2. moduł z 4 interfejsami miedzianymi 10Gbit/s

1.15.3. moduł z 4 interfejsami światłowodowymi 1Gbit/s

1.15.4. moduł z 8 interfejsami światłowodowymi 1Gbit/s

1.15.5. moduł z 4 interfejsami światłowodowymi 10Gbit/s

1.16. Urządzenie musi mieć możliwość kreowania interfejsów VLAN oraz GRE

1.17. Urządzenie musi umożliwiać tworzenie sieci VPN opartych o IPSec i SSL VPN

1.18. Możliwa do skonfigurowania liczba tuneli VPN IPSec – minimum 1000

1.19. Urządzenie ma być wyposażone w dysk SSD o pojemności powyżej 200 GB

1.20. Obsługa interfejsów 802.11q (VLAN) – minimum 256

1.21. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive

1.22. Urządzenie nie może narzucać limitu na liczbę użytkowników

1.23. Liczba reguł filtrowania – minimum 16384

1.24. Liczba tras statycznego routingu – minimum 5120

1.25. Liczba tras dynamicznego routingu – minimum 10000

1.26. Skaner antywirusowy ma być dostarczany w ramach licencji

1.27. Urządzenie musi być wyposażone w moduł TPM

1.28. Urządzenie powinno umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja)

1.29. SSL VPN ma działać co najmniej w trybach tunelu i portalu

1.30. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover)

1.31. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based

1.32. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:

1.32.1. lokalną bazę użytkowników (wewnętrzny LDAP)

1.32.2. zewnętrzną bazę użytkowników (zewnętrzny LDAP)

1.32.3. usługę katalogową Microsoft Active Director

1.33. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP

1.34. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:

1.34.1. SSL

1.34.2. Radius

1.34.3. Kerberos

1.35. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy

1.36. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta

1.37. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny

1.38. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego

1.39. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa przez zaszyfrowany protokół HTTPS
1.40. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP
1.41. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami
1.42. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
1.43. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku
1.44. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS)
1.45. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX
1.46. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
1.46.1. manualnego eksportu do pliku w dowolnym momencie czasu
1.46.2. automatycznego eksportu na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
1.47. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z dedykowanego serwera zarządzanego przez administratora
1.48. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika
1.49. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu
1.50. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania
1.51. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego
1.52. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta
1.53. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3
1.54. Możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji
1.55. Okres wsparcia zgodnie z zapisami OPZ w zakresie wszystkich wymaganych licencji
1.56. Gwarancja zgodnie z zapisami OPZ

VI. Wymagania dla systemu MPLS-TP

1. Topologia
   1.1. Wyposażenie sieciowe powinno umożliwiać tworzenie sieci o dowolnej topologii, w tym między innymi:
      1.1.1. topologia pierścienia, w tym pierścienia z podpierścieniami
      1.1.2. „mesh”
      1.1.3. połączenia liniowe
      1.1.4. dowolne kombinacje powyższych
   1.2. Sieć jest kontrolowana za pomocą scentralizowanego systemu zarządzania bez dynamicznej płaszczyzny sterowania
   1.3. W dowolnym momencie możliwe jest zidentyfikowanie przepływów ruchu dla każdej indywidualnej aplikacji / usługi
2. Zasady działania
   2.1. Działanie systemu oparte jest na technice MPLS-TP (RFC 5654)

2.2. Aktywne węzły połączone są łączami Ethernet
2.3. Multipleksowanie z podziałem czasu (TDM) jako warstwa fizyczna nie jest dozwolone
2.4. Różne przepływy ruchu w sieci są zorganizowane w ramach tuneli i łączy emulowanych („pseudowires")
2.5. Sieć musi obsługiwać połączenia punkt-punkt i wielopunktowe
2.5.1. w przypadku połączeń punkt-punkt musi istnieć możliwość tworzenia przezroczystych połączeń dla każdego typu protokołu
2.6. Sieć musi umożliwiać przesyłanie sygnałów zorientowanych na podział czasu (TDM) przy użyciu emulacji obwodu
2.7. Przepływy ruchu będą identyfikowane po stronie wejściowej sieci jako oparte na porcie lub na VLAN
2.8. Należy stosować ścisłą kontrolę ruchu przychodzącego i wychodzącego w celu zagwarantowania pasma i wydajności każdej usłudze oraz unikania zakłóceń między ruchem w poszczególnych emulowanych łączach („pseudowires")
2.9. Przełączanie redundantne w warunkach awarii realizowane jest automatycznie w oparciu o standard MPLS-TP (RFC 6372)
2.10. Zastosowanie zastrzeżonych (własnościowych) protokołów nie jest dozwolone
2.11. W celu optymalizacji dozwolone jest tworzenie mechanizmów redundancji za pomocą alternatywnych technik:
2.11.1. musi być to połączenie istniejących standardów publicznych, takich jak ERPS (ITU G.8032)
2.11.2. istniejące publiczne protokoły muszą działać wewnątrz infrastruktury MPLS-TP
2.12. Wszystkie parametry i działania służące do zarządzania siecią, w tym początkowa konfiguracja i wykrywanie, muszą być prowadzone za pośrednictwem systemu zarządzania siecią
2.13. System zarządzania siecią powinien prowadzić użytkownika (operatora) za pomocą kreatorów przez kolejne etapy konfiguracji poszczególnych elementów sieci i usług

3. Specyfikacja zgodności MPLS-TP
3.1. Oferowany sprzęt powinien być zgodny z wytycznymi MPLS-TP, co oznacza zgodność z następującymi normami i rekomendacjami: MPLS-TP to technologia i musi być oznaczona zgodność z dokumentami. Musi się tu pojawić to spełnienie wymagań w dokumentach RFC np. https://en.wikipedia.org/wiki/MPLS-TP
3.1.1. RFC3985: Pseudo Wire Emulation Edge to Edge Architecture
3.1.2. RFC5317: JWT Report on MPLS Architectural Considerations for a Transport Profile
3.1.3. RFC4448: Encapsulation Methods for Transport of Ethernet over MPLS Networks
3.1.4. RFC5462: Multiprotocol Label Switching (MPLS)
3.1.5. RFC5586: MPLS Generic Associated Channel
3.1.6. RFC5654: Requirements of a MPLS Transport Profile
3.1.7. RFC5718: In-band communication channel
3.1.8. RFC5860: Requirements OAM for MPLS-TP
3.1.9. RFC5880: Bidirectional Forwarding Detection (BFD)
3.1.10. RFC5921: A Framework for MPLS in Transport Networks
3.1.11. RFC5950: network management for MPLS-TP
3.1.12. RFC5951: network management requirements for MPLS-based transport networks
3.1.13. RFC5960: MPLS Transport Profile Data Plane Architecture
3.1.14. RFC6291: Guidelines for the Use of the "OAM" Acronym in the IETF
3.1.15. RFC6371: Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks
3.1.16. RFC6372: MPLS-TP Survivability Framework
3.1.17. RFC6426: On demand connectivity verification
3.1.18. RFC6428: Proactive connectivity verification
3.1.19. RFC6669: An Overview of the Operations, Administration, and Maintenance (OAM) toolset for MPLS-Based Transport Networks

3.1.20. G.8032: ERP
3.1.21. G.8101: Terms and definitions for MPLS Transport Profile
3.1.22. G.8110: MPLS layer network architecture
3.1.23. G.8110.1: Architecture of the Multi-Protocol Label Switching transport profile layer network
3.1.24. G.8112: Interfaces for the MPLS Transport Profile layer network
3.1.25. G.8113.1: Operations, administration and maintenance mechanism for MPLS-TP in packet transport networks
3.1.26. G.8113.2: Operations, administration and maintenance mechanisms for MPLS-TP networks using the tools defined for MPLS
3.1.27. G.8121: Characteristics of MPLS-TP equipment functional blocks
3.1.28. G.8121.1: Characteristics of MPLS-TP equipment functional blocks supporting ITU-T G.8113.1/Y.1372.1
3.1.29. G.8121.2: Characteristics of MPLS-TP equipment functional blocks supporting ITU-T G.8113.2/Y.1372.2
3.1.30. G.8131: Linear protection switching for transport MPLS (T-MPLS) networks
3.1.31. G.8151: Management aspects of the MPLS-TP network element

4. Dostępność i niezawodność
   4.1. W celu zapewnienia maksymalnej dostępność systemu i usług oraz w ramach minimalizacji czasu ewentualnych przestojów, należy zastosować następujące mechanizmy i środki:
      4.1.1. Redundancja (przełączanie protekcyjne) dla usług w postaci APS („Automatic Protection Switching”), czyli automatyczne przełączanie zgodnie z MPLS-TP
         4.1.1.1. Ścieżka rezerwowa aktywowana automatycznie, gdy na roboczej ścieżce wystąpi usterka
         4.1.1.2. Scenariusz przełączania aktywny/zapasowy zdefiniowany w sieci za pośrednictwem systemu zarządzania siecią i znany użytkownikowi
         4.1.1.3. Przełączanie nie może opierać się na dynamicznych protokołach routingu, lecz być deterministyczne
         4.1.1.4. Ewentualne przełączanie tras musi być dwukierunkowe, by zapobiegać generowaniu opóźnienia różnicowego – co oznacza, że w przypadku awarii pojedynczego włókna w parze, zarówno łącza nadawcze, jak i odbiorcze muszą zostać przełączone
      4.1.2. Maksymalny czas rekonfiguracji w przypadku awarii węzła lub przerwania łącza nie może przekroczyć 50 ms dla usług o redundancji typu 1:1
      4.1.3. W przypadku usług TDM musi istnieć możliwość redundancji o konfiguracji 1+1 zapewniającej brak utraty pakietów (tzw. przełączania bezstratnego)
         4.1.3.1. Musi istnieć możliwość skompensowania różnicy opóźnień między szybszą a wolniejszą ścieżką w sieci, aby uniknąć ‘skoku’ opóźnienia dla usługi TDM w momencie przełączenia na ścieżki zapasową
         4.1.3.2. Efektem zastosowania redundancji o konfiguracji 1+1 musi być stałe (to znaczy takie same w przypadku obu tras) i predefiniowane opóźnienie dla usługi TDM
      4.1.4. W każdym urządzeniu wymagane są dwa zasilacze pracujące w trybie redundantnym
      4.1.5. W przypadku urządzeń instalowanych w szczególnie istotnych z punktu widzenia użytkownika lokalizacjach, moduły odpowiadające za sterowanie i przełączające ruchu powinny mieć opcję pełnej redundancji
      4.1.6. Dane konfiguracyjne powinny być przechowywane lokalnie w każdym węźle, w celu zapewnienia szybkiego restartu po całkowitej utracie zasilania
      4.1.7. Dane konfiguracyjne dotyczące danego węzła są przechowywane w pamięci wymiennej, co umożliwia łatwą wymianę sprzętu bez przeładowywania konfiguracji
      4.1.8. Wszystkie urządzenia w sieci są zawsze dostępne z poziomu systemu zarządzania siecią, nawet jeśli nie są skonfigurowane.
      4.1.9. Każde łącze MPLS-TP przenosi ruch związany z zarządzaniem (DCN) w dedykowanym pseudołączu („pseudowire”) MPLS-TP o zadanym paśmie, co gwarantuje brak wpływu

ruchu zarządzania na usługi. Gwarantuje to również osiągalność węzłów przez system zarządzania siecią.

4.1.10. Baza danych zawierająca wszystkie istotne informacje dotyczące konfiguracji systemu powinna być utworzona w systemie zarządzania siecią

4.1.11. Jeśli dane konfiguracyjne zostaną utracone w węźle, system zarządzania siecią musi mieć możliwość zdalnego przywrócenia danych

4.1.12. W celu zwiększenia niezawodność sieci, powinno być możliwe rozłożenie łączy do innych węzłów w sieci między różne karty interfejsów

4.1.13. Wysoką niezawodność urządzeń należy udowodnić, przedstawiając wartości parametru MTBF dla każdego pojedynczego modułu oraz przez ogólne obliczenie MTBF dla systemu

5. Parametry środowiskowe

5.1. Ze względu na zastosowanie w sektorach o krytycznym znaczeniu, urządzenia muszą być przygotowane pod kątem spełnienia warunków środowiskowych przedstawionych w takich standardach, jak:

5.1.1.IEEE 1613

5.1.2.IEC 61850-3

5.1.3.EN50121-4

5.1.4. Lub równoważnych spełniający wymogi środowiskowe i testowe w innych sektorach np. chemiczny, wojskowy

5.2. Urządzenia muszą być wykonane z wysokiej jakości materiałów, bez użycia powłok malowanych / lakierowanych

5.3. Chłodzenie urządzeń (z ewentualnym wyłączeniem urządzenia o charakterze serwerowym) musi być zapewniane pasywnie, to znaczy bez stosowania jakichkolwiek elementów ruchomych (np. wentylatorów)

5.4. Urządzenia (z ewentualnym wyłączeniem węzła o charakterze serwerowym) muszą pracować w szerokim zakresie temperatur (co najmniej od -25°C do +65°C)

5.5. Urządzenia powinny zapewniać możliwość montażu na szynie DIN lub w tradycyjnej szafie telekomunikacyjnej 19”

5.6. Producent urządzeń musi zagwarantować na piśmie komercyjną dostępność systemu, urządzeń, części zapasowych oraz gotowość do udzielania wsparcia dla sprzętu i oprogramowania przez minimum 15 lat od dnia zakupu

6. Połączenia między urządzeniami

6.1. System musi dawać możliwość łączenia węzłów za pomocą interfejsów optycznych oraz elektrycznych

6.2. Dostępne powinny być różne typy laserów optycznych w zakresie 850 – 1550 nm oraz odbiorniki gwarantujące możliwość odbioru sygnałów dla różnych odległości

6.3. Zestaw modułów optycznych zawiera również lasery współdziałające ze sprzętem CWDM i DWDM, w ramach zwielokrotnienia z podziałem długości fali

6.4. W przypadku, gdy dostępny jest tylko jeden światłowód, węzły mogą być łączone za pomocą modułów optycznych typu BiDi, które wykorzystują dwie długości fal na jednym włóknie, aby rozróżnić nadawanie i odbiór

7. Pasmo w systemie

7.1. Węzły należy łączyć za pomocą jednego lub wielu łączy typu GbE lub 10GbE

7.2. W celu zwiększenia przepustowości musi istnieć możliwość korzystania z wielu łączy między dwoma węzłami bez modernizacji całej sieci

7.3. Węzły dostępowe powinny mieć zdolność przełączania na poziomie co najmniej 10 Gbit/s

7.4. Węzły agregacyjnej powinny mieć zdolność przełączania na poziomie co najmniej 60 Gbit/s

7.5. Węzły rdzeniowe powinny mieć zdolność przełączania na poziomie co najmniej 700 Gbit/s (wszystkie w trybie pełnego dupleksu)

7.6. System musi zapewniać możliwość rozbudowy w celu zastosowania łączy o pojemności 40GbE

VII. Wymagania sprzętowe dla urządzeń

1. Wymagania ogólne
   1.1. Węzły sieciowe są dostępne:
      1.1.1. w postaci urządzeń o budowie modularnej (dla średnich i dużych zapotrzebowań)
      1.1.2. w postaci urządzeń kompaktowych o zwartej budowie (dla obiektów małych)
   1.2. Urządzenia modularne zapewniają możliwość instalacji dodatkowych modułów lub wymianę istniejących
   1.3. Urządzenia kompaktowe pozwalają uruchamiać dodatkowe funkcjonalności w oparciu o licencje
   1.4. Węzły sieciowe składają się z:
      1.4.1. obudowy
      1.4.2. dwóch redundantnych zasilaczy (wszystkie) z możliwością wymiany podczas pracy (dla urządzeń modularnych)
      1.4.3. wymiennych (dla urządzeń modularnych) lub zintegrowanych (dla urządzeń kompaktowych) modułów interfejsów
      1.4.4. wymiennych (dla urządzeń modularnych) lub zintegrowanych (dla urządzeń kompaktowych) modułów systemowych
   1.5. Gniazda („sloty") umożliwiają instalowanie modułów dla różnych interfejsów, karty interfejsów mogą być wymieniane podczas pracy urządzenia lub zamienianie na inne (w przypadku urządzeń modularnych)
   1.6. Urządzenia modularne muszą mieć możliwość takiej budowy i konfiguracji węzła, aby wszystkie elementy urządzenia mające bezpośredni wpływ na poprawne przenoszenie danych były redundantne. Dotyczy takich funkcji jak:
      1.6.1. etykietowanie MPLS-TP
      1.6.2. przełączanie ruchu
      1.6.3. zasilanie węzła
   1.7. W docelowym modelu musi być możliwe opcjonalne tworzenie sieci o dostępności określanej na poziomie 99,999%.
2. Chassis
   2.1. Obudowa daje możliwość montaży w stojaku lub szafie telekomunikacyjnej 19" lub na szynie DIN
   2.2. Charakteryzuje się przemysłową konstrukcją
   2.3. Wszystkie podłączenia dla interfejsów lub zasilania są dostępne wyłącznie z przodu, od frontu urządzenia (wyjątkiem może być zasilanie dla kompaktowych urządzeń montowanych na szynie DIN)
   2.4. W przypadku urządzeń modularnych moduły interfejsów powinny być łatwe do zainstalowania oraz musi istnieć możliwość umieszczania i wyjmowania kart interfejsów podczas pracy urządzeń bez wpływu na obecne już w urządzeniu karty
   2.5. W celu optymalizacji projektu sieci, dostępne są różnorodne typy obudów z różną liczbą gniazd i różną pojemnością
   2.6. Chassis powinny obsługiwać styki wejściowe i styki wyjściowe, wywołujące alarm lokalny lub odbierające alarm lokalny i przekazujące go do systemu zarządzania siecią
3. Moduł centralny (matryca przełączająca)
   3.1. Moduł centralny w urządzeniu powinien łączyć dwie funkcje:
      3.1.1. funkcję centralnego modułu sterującego w danym węźle
      3.1.2. przełączanie pakietów miedzy interfejsami klienckimi a siecią MPLS-TP
   3.2. Każde urządzenie musi być wyposażone w fizyczny lub logiczny centralny moduł sterujący i przełączający:
      3.2.1. moduł odpowiedzialny za rozpoczynanie, kończenie lub przekazywanie ruchu etykietowanego w ramach tuneli i pseudołączy
   3.3. Moduł centralny może pełnić funkcję Label Edge Router (początek i koniec tunelu) oraz Label Switch Router (przełączanie tunelu)

3.4. Fizyczny moduł centralny powinien posiadać wyświetlacz umożliwiający szybką wstępną diagnostykę węzła
3.5. Centralny moduł przełączający powinien odpowiadać za wykonywanie automatycznego przełączania protekcyjnego zgodnie ze standardem MPLS-TP w wariancie „1:1”:
3.5.1. w trybie „revertive” oraz „non-revertive”
3.5.2. w czasie poniżej 50 ms
3.5.3. za pomocą komunikatów kontroli ciągłości opartych na BFD
3.6. Przełączanie protekcyjne realizowane ze wsparciem sprzętowym
3.7. Obsługa monitorowania OAM w oparciu o ITU-T Y.1713 dla pomiarów opóźnień i strat, by umożliwić monitorowanie usług
3.8. Obsługa Sync-E
3.9. Obsługa precyzyjnego protokołu taktowania IEEE 1588v2 w trybie transparentnego taktowania
3.9.1. znacznik czasu wykonany sprzętowo na kartach interfejsu w celu zagwarantowania maksymalnej dokładności
3.10. Dostępność w platformie chassis obsługujących dwa centralne moduły przełączające:
3.10.1. jeden działa jako aktywny, a drugi w trybie gotowości „hot-standby”
3.10.2. konfiguracja synchronizowana w czasie rzeczywistym między modułami
3.10.3. w przypadku awarii modułu aktywnego, moduł pasywny staje się aktywnym i zapewnia ciągłość przekazywania usług

4. Zasilanie
4.1. Chassis wyposażone w dwa zasilacze (redundantne i równoważące obciążenie).
4.2. Wspierane zakresy napięć w urządzeniach modularnych:
4.2.1. 18 VDC do 60 VDC
4.2.2. 83 VDC do 300 VDC
4.2.3. 115 VAC i 230 VAC
4.3. W razie potrzeby musi istnieć możliwość łączenia źródeł zasilania AC i DC w tym samym węźle modularnym
4.4. W przypadku awarii jednego z dwóch redundantnych zasilaczy, drugi automatycznie przejmie zadanie pierwszego i węzeł pracuje zapewniając pełnię funkcjonalności
4.5. W przypadku zastosowania w urządzeniach modularnych zasilania PoE dla jednostek klienckich, ze względów bezpieczeństwa i niezawodności nie wolno przekazywać zasilania z wewnętrznych zasilaczy:
4.5.1. zasilanie dla PoE dostarczane za pośrednictwem zewnętrznego źródła zasilania
4.5.2. węzeł służy jedynie do kontroli i przenoszenia zasilania PoE do urządzenia końcowego

5. Interfejsy klienckie
5.1. System zapewnia obsługę następujących interfejsów klienckich:
5.1.1. GbE / FE
5.1.2. 10GbE
5.1.3. 40GbE
5.1.4. IP Routing
5.1.5. C37.94
5.1.6. E1/T1
5.1.7. Serial (m.in. RS-232 / -422, /-485, X.21, V.35)
5.1.8. 2W/4W E&M
5.1.9. G.703 Co Directional
5.1.10. Optical Low Speed
5.1.11. FXS
5.2. Wszystkie moduły interfejsów są zarządzane i konfigurowane w systemie zarządzania siecią
5.3. Interfejsy Ethernet:
5.3.1. służą do realizacji zarówno połączeń między węzłami system (połączeń MPLS-TP) jak i do przyłączania usług klienckich
5.3.2. za ich pomocą możliwe jest tworzenie różnych sieci logicznych w ramach sieci fizycznej

5.3.3. istnieje możliwość skonfigurowania portów użytkownika tak, że każdy funkcjonuje w ramach oddzielnej usługi Ethernet.
5.3.4. możliwe jest przypisanie portu użytkownika do więcej niż jednej usługi Ethernet
5.3.4.1. możliwe jest kierowanie ruchu w oparciu o identyfikatory VLAN-ID
5.3.5. system dostarcza co najmniej następujące informacje:
5.3.5.1. stan portu aktywny / nieaktywny
5.3.5.2. połączenie aktywne / nieaktywne
5.3.5.3. dane dotyczące ruchu Ethernet
5.3.5.4. funkcja portu (kliencki / port połączeniowy)
5.3.6. powinna istnieć możliwość aktywacji zasilania przez Ethernet w oparciu o standardy 802.3af i 802.3at dla każdego portu obsługującego PoE
5.3.7. karta interfejsu typu Ethernet musi być w stanie przenosić duże ramki (tzw. „jumbo frames") o rozmiarze do 9198 bajtów
5.3.8. porty muszą być w stanie przenosić synchronizację za pośrednictwem protokołu Sync-E
5.3.9. ze względów bezpieczeństwa musi istnieć możliwość:
5.3.9.1. wyłączenia nieużywanych portów
5.3.9.2. zastosowania listy kontroli dostępu opartej na adresie MAC i adresie IP (w celu ułatwienia zastosowania, konfiguracja tych list dostępu jest wykonana za pomocą zautomatyzowanej procedury na platformie zarządzania siecią)
5.3.9.3. ograniczenia rozmiaru tabeli MAC w celu uniknięcia ataków typu „DoS"

6. Interfejsy E1:
6.1. dane T1/E1 są przesyłane przez sieć za pośrednictwem emulacji SAToP (RFC4553) lub CESoPSN (RFC5086)
6.2. wymienny moduł interfejsu T1/E1 posiada co najmniej 4 porty
6.3. istnieje możliwość zapewnienia mechanizmów redundancji w ramach standardu MPLS-TP, w tym w wariancie z bezstratnym przełączaniem (bez utraty pakietów):
6.3.1. w tym przypadku następuje skompensowanie różnicy opóźnienia między ścieżką aktywną i zapasową
6.3.2. opóźnienie między końcami nie ulega zmianie w chwili przełączeniu z aktywnego traktu na zapasowy
6.4. karta interfejsu T1/E1 jest w stanie dostarczyć zegar do węzła sieci w celu synchronizacji
6.5. moduł posiada pętlę zwrotną dla portów:
6.5.1. dając możliwość testowania błędów bitowych
6.5.2. zapewniając informacje statusowe
6.5.3. umożliwiając diagnozowanie połączeń bez obecności na obiekcie

7. Interfejsy szeregowe "serial":
7.1. muszą być obsługiwane następujące standardy:
7.1.1. RS232 synchroniczny i asynchroniczny
7.1.2. RS422 synchroniczny i asynchroniczny
7.1.3. RS485 asynchroniczny
7.1.4. X.21
7.1.5. V.35
7.2. interfejsy dostępne w ramach jednego typu modułu
7.3. dla obsługi RS-232/422/485: obsługa szybkości transmisji od 1200 bps do 115200 bps
7.4. dla trybu synchronicznego: obsługa nx64 kbit/s
7.5. możliwość zmniejszenia liczby interfejsów szeregowych na karcie w celu obsługi większej liczby sygnałów sterujących (takich jak RTS, TCS, dodatkowe taktowanie)
7.6. karta powinna obsługiwać zoptymalizowany układ pinów, aby zmaksymalizować liczbę dostępnych interfejsów
7.7. dla każdego sygnału sterującego (RTS, CTS,….) musi istnieć możliwość wyboru, czy sygnał danych jest przesyłany, ignorowany lub wymuszany na stałym poziomie „1" lub „0" – w celu umożliwienia różnym aplikacjom wykorzystania karty w jak najwydajniejszy sposób
7.8. dane szeregowe i odpowiadające im sygnały sterujące będą przesyłane przez sieć MPLS-TP:

7.8.1. za pośrednictwem emulacji łącza w przypadku usług synchronicznych punkt-punkt
7.8.2. przez konwersję „serial to Ethernet" dla wszystkich innych aplikacji
7.8.3. tryb „serial to Ethernet" musi obejmować możliwość tworzenia konfiguracji „master – slave" dla typowych aplikacji odpytywania

7.9. w aplikacjach wielopunktowych musi istnieć możliwość wykonania konfiguracji z dwoma urządzeniami typu „master" kontrolującymi zestaw urządzeń „slave" bez wykorzystywania większej ilości zasobów w sieci
7.9.1. dwa urządzenia „master" muszą być w stanie komunikować się urządzeniami „slave" oraz między sobą
7.9.2. odpowiedzi od stacji „slave" muszą trafiać jednocześnie do dwóch stacji „master"
7.9.3. karta powinna realizować ciągłą weryfikację czy „master" może dotrzeć do wszystkich urządzeń „slave", wykonywaną podczas trybu normalnej pracy

7.10. moduł posiada pętlę zwrotną dla portów:
7.10.1. dając możliwość testowania błędów bitowych
7.10.2. zapewniając informacje o stanie

7.11. Karta interfejsów szeregowych powinna wyświetlać za pośrednictwem diod LED na panelu przednim co najmniej następujące informacje:
7.11.1. obecność zasilania OK/NOK
7.11.2. stan modułu OK/NOK
7.11.3. aktywność nadawania
7.11.4. aktywność odbioru

VIII. Wymagania dla systemu zarządzania siecią MPLS-TP

1. Sieć urządzeń MPLS-TP powinna być wyposażona w przyjazny dla użytkownika system zarządzania siecią NMS:
   1.1. umożliwia on operatorowi efektywne zarządzanie i monitorowanie całej sieci
2. Pełnia funkcjonalności związanych z tzw. FCAPS („Fault, Configuration, Accounting, Performance and Security") musi być realizowana za pośrednictwem sieciowego systemu zarządzania NMS:
   2.1. w oczekiwanym systemie NMS konfiguracja sieci jest wykonywana w sposób pozostający bez wpływu na już uruchomione usługi
   2.2. ewentualne awarie są wykrywane, zdiagnozowane i mogą być naprawione
   2.3. umowy i ustalenia dotyczące poziomu świadczenia usług są monitorowane i zapewniane
   2.4. ze względów bezpieczeństwa użytkownicy są logowani i tworzona jest historia ich działań
3. NMS musi posiadać między innymi następujące funkcjonalności:
   3.1. konfiguracja sieci
   3.2. konfiguracja usług
   3.3. monitorowanie i diagnostyka
   3.4. aktywacja-dezaktywacja modułów interfejsów
   3.5. przydział przepustowości
   3.6. rejestracja alarmów i zdarzeń
   3.7. graficzna reprezentacja sieci
4. Architektura systemu NMS powinna być oparta na relacji serwer – klient:
   4.1. musi istnieć możliwość podłączenia wielu aktywnych klientów do serwera NMS
   4.2. musi być możliwe zarządzanie siecią z lokalnych lub zdalnych lokalizacji przez wielu użytkowników
5. W celu zapewnienia niezawodności, system musi mieć możliwość redundancji i tzw. 'ciepłej' gotowości („warm standby")
6. Automatyczne przełączanie protekcyjne
   6.1. Platforma zarządzania nie może brać aktywnego udziału w zapewnieniu redundancji (automatycznego przełączania tras) w sieci
   6.2. W tym przypadku narzędzie służy do wykrycia i zgłoszenia zdarzenia operatorowi sieci

6.3. Po wprowadzeniu informacji, sieć urządzeń działa autonomicznie i zapewnia rekonfigurację tras w sytuacjach błędów lub uszkodzeń łączy
6.4. Z powyższego względu konieczne jest, aby algorytm rekonfiguracji tras funkcjonował bezpośrednio w samych węzłach
6.5. Odpowiednie dane dotyczące konfiguracji są przechowywane w nieulotnej pamięci każdego węzła

7. Baza danych systemu NMS
   7.1. System NMS powinien zawierać bazę danych sieciowych, zawierającą wszelkiego rodzaju informacje, nazwy węzłów, konfiguracje węzłów, w tym zainstalowane moduły interfejsów
   7.2. Musi istnieć możliwość dokonywania „on-line" następujących zmian:
      7.2.1. aktywacja lub dezaktywacja kart interfejsów
      7.2.2. dodawanie lub usuwanie kart interfejsów
      7.2.3. dodawanie, zmiana lub usuwanie usług
   7.3. Każda zmiana powinna automatycznie aktualizować bazę danych na dysku twardym serwera oraz pamięć nieulotną odpowiedniego węzła (węzłów)
   7.4. Musi istnieć możliwość wykorzystania bazy danych do przywrócenia konfiguracji sieci w przypadku utraty ustawień jednego lub większej liczby węzłów
   7.5. Preferowane jest wykorzystanie technologii MySQL dla obsługi baz danych systemu NMS, wymagane jest wykorzystanie rozwiązania nielicencjonowanego (bezpłatnego)
8. Zarządzanie użytkownikami i rejestracja działań
   8.1. System NMS musi wspierać zarządzanie użytkownikami, dla których definiowane są różne role (różne uprawnienia)
   8.2. System NMS posiada dziennik zdarzeń „event log" (dotyczący zdarzeń systemowych) oraz wspiera ścieżkę audytu (dotyczącą działań użytkowników), co pozwala na odtwarzanie działań, które mają miejsce w sieci wraz ze zdefiniowaniem przez kogo są prowadzone
9. Połączenie sieciowe
   9.1. System zarządzania NMS powinien łączyć się z elementami sieci za pośrednictwem protokołu SNMPv3
   9.2. Połączenie NMS z węzłami sieci musi być zapewniane za pośrednictwem tzw. kanałów wewnątrz pasma („in-band")
   9.3. Kanały komunikacyjne typu „in-band" muszą być ustanawiane automatycznie między poszczególnymi węzłami sieci
   9.4. Sieć zarządzania oparta jest na standardowych protokołach routingu
10. Zarządzanie konfiguracją
   10.1. Dostęp do systemu NMS powinien być możliwy za pośrednictwem dowolnego urządzenia w sieci MPLS-TP, z wykorzystaniem interfejsu zarządzania typu Ethernet
   10.2. Za pośrednictwem NMS musi być możliwe skonfigurowanie urządzeń tworzących sieć, takich jak:
      10.2.1. węzły
      10.2.2. moduły sieciowe
      10.2.3. moduły interfejsów
      10.2.4. transceivery optyczne
   10.3. Narzędzie powinno dostarczać operatorowi odpowiednie wskazówki dotyczące tego, które gniazda („sloty") można wyposażyć w dany sprzęt
   10.4. Tworzenie usług w sieci powinno być możliwe za pomocą kreatorów usług, które:
      10.4.1. zapewniają możliwość wykonania wszystkich niezbędnych kroków
      10.4.2. zapewniają możliwość określenia parametrów usług w przyjazny i logiczny sposób
      10.4.3. pozwalają skonfigurować w szczególności parametry takie jak:
         10.4.3.1. przepustowość (pasmo) usługi
         10.4.3.2. jakość usług (QoS)
         10.4.3.3. redundancja
         10.4.3.4. opóźnienie
         10.4.3.5. przebieg (trasowanie) usługi w sieci

10.4.4. w każdych warunkach pozwalają użytkownikowi zastąpić sugerowane parametry własnymi danymi
10.4.5. 'pilnują' poprawności ustawień i ostrzegają użytkownika w przypadku próby wprowadzenia danych wywołujących niezgodność w konfiguracji sieci
10.4.6. chronią operatora przed błędami konfiguracji spowodowanymi 'czynnikiem ludzkim', takimi jak na przykład:
10.4.6.1. przekroczenie fizycznej przepustowości łącza
10.4.6.2. niezgodność etykiet MPLS-TP
10.4.6.3. powielenie etykiet MPLS-TP
10.4.6.4. przypisanie zbyt małego pasma dla usług o określonych przepływnościach
10.4.6.5. niezgodność typów kart czy typów interfejsów w węźle
10.4.6.6. próba skonfigurowania usług na karcie / porcie nie wspierającym tego typu usług

10.5. Oczekiwana jest możliwość wstępnego skonfigurowania („prekonfiguracji") sieci i usług bez posiadania aktywnego połączenia z siecią urządzeń (tzw. działanie „off-line")

10.6. Działania w systemie NMS powinny być wykonywane za pomocą graficznego interfejsu użytkownika (GUI) lub za pomocą skryptów

10.7. Musi istnieć możliwość gromadzenia urządzeń w logiczną grupę w celu jej łatwego wyboru podczas konfigurowania sieci (na przykład grupowanie ze względu na region geograficzny)

11. Monitorowanie i „network assurance"

11.1. Możliwość łatwego monitorowania funkcjonowania sieci, obejmującego między innymi graficzną reprezentację:
11.1.1. łączy fizycznych
11.1.2. tuneli MPLS
11.1.3. usług w sieci

11.2. W dowolnym momencie musi istnieć możliwość wizualizacji, które tunele i pseudołącza („pseudowires") pracują w danym fizycznym łączu w sieci

11.3. Dane dotyczące wydajności powinny być wizualizowane w oparciu o pomiary OAM wykonywane przez urządzenia sieciowe

11.4. Musi istnieć możliwość monitorowania danych związanych z jakością usług (QoS):
11.4.1. wizualizacja polityk dla usług
11.4.2. wizualizacja mechanizmów kolejkowania w każdym węźle

11.5. Monitorowanie musi być bezpośrednią częścią systemu NMS, realizowane bez użycia narzędzi zewnętrznych firm trzecich

11.6. Jako minimum, system NMS musi być w stanie wizualizować:
11.6.1. średnią przepustowość (pasmo)
11.6.2. średni rozmiar ramki
11.6.3. bajty zgodne i przekroczone

11.7. Dostępne są następujące narzędzia zapewniania usług:
11.7.1. test błędów bitowych dla interfejsów E1, C37.94, OLS, „serial", CODIR z możliwością wykonania pętli zwrotnej
11.7.2. test poziomu sygnału dla interfejsu 2/4Wire E&M
11.7.3. test opóźnienia „end-to-end" dla tuneli punkt-punkt MPLS-TP
11.7.4. test opóźnienia „end-to-end" dla interfejsów E1, C37.94, OLS, „serial", CODIR, 2/4Wire E&M

12. Graficzny interfejs użytkownika GUI

12.1. Powinna istnieć możliwość logicznej wizualizacji elementów sieci:
12.1.1. z węzłami odwzorowanymi na schemacie w celu przedstawienia fizycznej lokalizacji urządzeń

12.2. Musi istnieć możliwość wyboru widoków infrastruktury sieci na różnych poziomach, ukazujących łącza, tunele i/lub usługi dla określonej grupy usług należących do tej samej aplikacji

12.3. Graficzny interfejs użytkownika powinien być konfigurowalny w taki sposób, aby różne okna informacyjne mogły być dołączone do różnych lokalizacji w interfejsie użytkownika NMS:
12.3.1. graficzny interfejs użytkownika może być modyfikowany w zależności od potrzeb operatora w danym momencie lub
12.3.2. może być dostosowany do innych nośników wyświetlania (ekranów czy ścian wyświetlacza)
12.4. W celu wsparcia działań diagnostycznych powinien istnieć łatwy sposób porównywania ustawień różnych elementów sprzętowych przez przeglądanie różnych parametrów w widoku stylu arkusza danych

13. Raportowanie
13.1. System zarządzania siecią powinien umożliwiać tworzenie raportów w formacie pdf lub csv
13.2. Wszelkie informacje przechowywane w bazie danych powinny być możliwe do udostępnienia
13.3. W systemie zapewniany jest mechanizm tworzenia niestandardowych raportów, na przykład w oparciu o XML
13.4. Powinno być możliwe oznakowanie raportów za pomocą znaku graficznego

14. Interfejs ‘północny’ SNMP
14.1. System musi zapewnić dostępność prywatnej bazy MIB w celu umożliwienia monitorowania całej sieci MPLS-TP z poziomu systemu ‘parasolowego’
14.1.1. system NMS funkcjonuje jako „proxy” w stosunku do urządzeń obecnych w poszczególnych węzłach

15. Zarządzanie urządzeniami zewnętrznymi („third-party”)
15.1. System zarządzania siecią powinien mieć możliwość monitorowania urządzeń firm trzecich, w podobny sposób w jaki ma to miejsce dla węzłów MPLS-TP
15.2. Oczekiwania stawiane w tym zakresie i dotyczące funkcjonowania to między innymi:
15.2.1. komunikacja z urządzeniami za pomocą SNMPv2 lub SNMPv3
15.2.2. wszelkie informacje w publicznej lub prywatnej bazie MIB powinny być czytelne, ‘przetłumaczone’ na łatwy do zrozumienia tekst i wyświetlane w oknie właściwości; powinno to być możliwe dla informacji globalnych lub dla portów tych urządzeń
15.2.3. graficzna wizualizacja zarządzanego urządzenia jest możliwa podczas tworzenia określonego typu urządzenia w systemie zarządzania siecią NMS
15.2.4. powinna istnieć możliwość wyboru portów Ethernet wymagających zarządzania
15.2.5. urządzenie zewnętrzne powinno być częścią topologii sieci
15.2.6. stan łączy od węzłów MPLS-TP do urządzeń zewnętrznych powinien być nadzorowany
15.2.7. niestandardowe alarmy muszą być konfigurowalne i wyświetlane na liście alarmów systemu zarządzania siecią NMS

16. Szyfrowanie transmisji
16.1. Powinna być możliwe zastosowanie szyfrowania transmisji w łączach MPLS-TP w celu zapobiegania nieautoryzowanemu dostępowi do danych i związanego z tym przechwycenia i ‘podsłuchania’ przesyłanych informacji
16.2. Rekomendowana jest realizacja szyfrowania za pomocą techniki MACsec (w warstwie 2)
16.3. Oczekiwane są między innymi:
16.3.1. zapewnienie szyfrowania pełnego strumienia danych użytkowych
16.3.2. możliwość uruchomienia funkcjonalności dla poszczególnych łączy z poziomu systemu nadzoru NMS
16.3.3. wspieranie sprzętowe szyfrowania bezpośrednio na karcie MPLS-TP (szyfrowanie nie może obciążać procesora matrycy)
16.4. Powinno być możliwe takie zaprojektowanie sieci, aby w momencie jej wdrożenia zapewnić sprzętowe przygotowanie łączy pod uruchomienie funkcjonalności szyfrowania:
16.4.1. funkcjonalność ta powinna być obecna w urządzeniach już od momentu ich wdrożenia
16.4.2. ewentualne uruchomienie szyfrowania może nastąpić przez aktywowanie opcji

16.4.3. z poziomu systemu nadzoru NMS
16.4.4. jedyną dopuszczalną ingerencją w strukturę sieci jest wówczas ewentualne wprowadzenie licencji
16.4.5. zmiany sprzętowe są wykluczone

17. Parametry serwera dla systemu zarządzania siecią NMS:
    17.1. procesor 2,6 GHz (lub więcej), 6 rdzeni
    17.2. pamięć: 16 GB RAM
    17.3. dysk: 50 GB dostępnej przestrzeni
    17.4. system operacyjny Microsoft Windows: 10 (>= wersja 1607), 11 / Server 2012 / Server 2012 R2 / Server 2016 / Server 2019 / Server 2022 64 bit

IX. Wytyczne projektowe dla sieci OT

1. Zamówienie w zakresie budowy sieci szkieletowej OT opartej o technikę MPLS-TP obejmuje:
    1.1. wykonanie projektu sieci z uwzględnieniem zakresu zamówienia podstawowego oraz ewentualnego rozszerzenia w prawie opcji
    1.2. dostawy urządzeń
    1.3. uruchomienie sprzętu i oprogramowania dla zakresu zamówienia podstawowego oraz ewentualną rekonfigurację, doposażenie istniejących urządzeń i uruchomienie nowego sprzętu i oprogramowania dla zakresu prawa opcji
    1.4. konfigurację tuneli MPLS-TP i usług dla zakresu zamówienia podstawowego oraz ewentualną rekonfigurację istniejących tuneli MPLS-TP i usług i konfigurację nowych tuneli MPLS-TP i usług dla zakresu prawa opcji
    1.5. testy weryfikacyjne
    1.6. przeprowadzenie zaawansowanego instruktażu dla personelu Zamawiającego
    1.7. gwarancję
2. Wymagania w zakresie wykonania projektu sieci
    2.1. Konieczne jest przygotowanie projektu wykonawczego sieci telekomunikacyjnej
    2.2. Za powstanie i przygotowanie dokumentacji projektowej odpowiedzialny jest wykonawca
    2.3. Dokumentacja projektowa musi zostać uzgodniona z Zamawiającym
    2.4. Dokumentacja projektowa musi uwzględniać wszystkie wymagania przedstawione w niniejszym dokumencie oraz rekomendacje zawarte w „Koncepcji budowy sieci szkieletowej OT opartej o technikę MPLS-TP”
    2.5. Wykonawca przekaże Zamawiającemu dokumentację w postaci elektronicznej w ustalonej formie
    2.6. Projekt zostanie przygotowany w języku polskim
    2.7. Podstawowa zawartość dokumentacji projektowej musi obejmować między innymi:
        2.7.1. harmonogram prac wraz z opisem wymagań dla każdego z etapów w zakresie podstawowym i w prawie opcji
        2.7.2. opis szczegółowego zakresu dostarczanych rozwiązań, w tym funkcjonalności, cech produktów oraz zgodności z wymaganiami normatywami i prawnymi
        2.7.3. szczegółowy opis funkcjonalny rozwiązań
        2.7.4. harmonogram i opis testów dostarczanych rozwiązań
3. Wymagania w zakresie dostawy urządzeń dla zamówienia podstawowego
    3.1. Wymagane jest dostarczenie jednego urządzenia o charakterystyce zgodnej z kompletacją węzła typu rdzeniowego
    3.2. Kompletacja węzła typu rdzeniowego:
        3.2.1. chassis o następujących parametrach / właściwościach:
            3.2.1.1. montaż w szafie serwerowej 19”
            3.2.1.2. wysokość nie przekraczająca 12 RU

3.2.1.3. modularna konstrukcja umożliwiająca montaż wymiennych kart interfejsów, wymiennych kart matryc przełączających, wymiennych kart zasilaczy, wymiennej karty nadzorczej
3.2.1.4. możliwość zasilania zarówno 48 VDC jak i 230 VAC (również miksu obu)
3.2.1.5. możliwość montażu co najmniej 15 kart interfejsów (mających dostęp do co najmniej 60 portów 10Gbit/s w kierunku magistrali / szyny komunikacyjnej)
3.2.1.6. możliwość jednoczesnego wyposażenia węzła w co najmniej 24 porty 10GbE (liniowe/klienckie) + 16 portów GbE (liniowe/klienckie) + 32 porty GbE (klienckie)
3.2.1.7. wykluczone zastosowanie wbudowanych 'na stałe' w chassis interfejsów optycznych/elektrycznych, portów komunikacyjnych, kart transmisyjnych, wentylatorów, itp.
3.2.1.8. obsługa połączeń typu MPLS-TP na portach GbE, 10GbE, 40GbE i w przyszłości 100GbE co najmniej w konfiguracji E-LINE, E-LAN, pierścień, podpierścień
3.2.1.9. możliwość udostępnienia m.in. interfejsów GbE, 10GbE, 40GbE, E1, RS-232/422/485
3.2.1.10. dostępność wszystkich złączy, kart, portów i interfejsów, styków zasilania itp. od frontu urządzenia
3.2.1.11. oznaczenie CE i zgodność z wymaganiami Dyrektywy 93/68/EC

3.2.2. wyposażenie w dwa redundantne wymienne moduły zasilające 230 VAC, z możliwością wymiany / zmiany 'na gorąco' (przy wyjęciu jednego z modułów węzeł zachowa pełną funkcjonalność i sprawność w oparciu o drugi z nich)

3.2.3. wyposażenie w jeden wymienny moduł matrycy przełączającej (MPLS-TP) o minimalnej nieblokowalnej pojemności 60x 10 Gbit/s
3.2.3.1. z możliwością bezprzerwowego doposażenia węzła w drugi redundantny moduł matrycy przełączającej, co pozwoli na pracę obu matryc w trybie 'ciepłej gotowości' oraz zapewni opcję wymiany 'na gorąco' (przy wyjęciu jednego z modułów węzeł zachowa pełną funkcjonalność i sprawność w oparciu o drugi z nich)

3.2.4. wyposażenie w interfejs 10GbE wraz z optyką typu XFP/SFP+ BiDi (na jedno włókno) o zasięgu 10 km na potrzeby realizacji połączenia MPLS-TP do węzła typu agregacyjnego
3.2.4.1. możliwość uruchomienia drugiego interfejsu 10GbE przez ewentualne wyposażenie w optykę typu XFP/SFP+ BiDi (na jedno włókno) o zasięgu 10 km w celu uzyskania pełnej redundancji połączenia do węzła agregacyjnego: gdzie wyłączenie, niedostępność lub wymiana optyki jednego z tych interfejsów nie spowoduje jakiegokolwiek zakłócenia w pracy drugiego z nich
3.2.4.2. wymiana jakiegokolwiek modułu, karty, interfejsu czy innego elementu węzła niezwiązanego bezpośrednio z przenoszeniem danych przez interfejs 10GbE nie może spowodować zakłócenia w pracy tego interfejsu

3.2.5. wyposażenie w dwa interfejsy 10GbE z optyką typu XFP/SFP+ MM 1310 nm na potrzeby realizacji połączeń z systemem monitorowania:
3.2.5.1. wyłączenie, niedostępność lub wymiana optyki dowolnego z tych interfejsów nie może spowodować zakłócenia w pracy interfejsu 10 GbE zapewniającego połączenie do węzła typu agregacyjnego
3.2.5.2. wyłączenie, niedostępność lub wymiana dowolnego z tych interfejsów nie może spowodować jakiejkolwiek przerwy w pracy interfejsu na innej karcie transmisyjnej

3.2.6. wyposażenie w cztery interfejsy GbE wraz z optyką typu SFP BiDi (na jedno włókno) o zasięgu 20 km na potrzeby realizacji połączeń do węzłów dostępowych:
3.2.6.1. interfejsy dostępne na co najmniej dwóch osobnych kartach transmisyjnych
3.2.6.2. wyłączenie, niedostępność lub wymiana optyki jednego z tych interfejsów nie może spowodować jakiejkolwiek przerwy w pracy innego z nich

3.2.6.3. wyłączenie, niedostępność lub wymiana jednego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować jakiejkolwiek przerwy w pracy interfejsów 10GbE

3.2.6.4. wymiana jakiegokolwiek modułu, karty, interfejsu czy innego elementu węzła niezwiązanego bezpośrednio z przenoszeniem danych przez interfejs GbE nie może spowodować zakłócenia w pracy tego interfejsu

3.2.7. wyposażenie w cztery interfejsy GbE RJ45 na potrzeby realizacji redundantnych połączeń z firewall'em OT:

3.2.7.1. interfejsy dostępne na co najmniej dwóch osobnych kartach transmisyjnych

3.2.7.2. wyłączenie, niedostępność lub wymiana wkładki optycznej jednego z redundantnych interfejsów w parze bądź wymiana karty transmisyjnej z nim związanej nie może spowodować jakiegokolwiek zakłócenia w pracy drugiego interfejsu z danej redundantnej pary

3.2.7.3. wyłączenie, niedostępność lub wymiana wkładki optycznej jednego z redundantnych interfejsów w parze bądź wymiana karty transmisyjnej z nim związanej nie może spowodować jednoczesnego zakłócenia lub niedostępności w pracy obu interfejsów z innej pary

3.2.7.4. wyłączenie lub wymiana dowolnego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować zakłócenia w pracy któregokolwiek z interfejsów 10 GbE

3.2.8. zapewnienie niezależności matryc przełączających od interfejsów transmisyjnych - innymi słowy wykluczone jest ewentualne zastosowanie interfejsów transmisyjnych umiejscowionych na kartach matryc przełączających ruch na potrzeby obsługi połączeń MPLS-TP lub połączeń zewnętrznych

3.2.9. zapewnienie możliwości uruchomienia szyfrowania na każdym łączu MPLS-TP bez ingerencji w konfigurację sprzętową węzła (dopuszczalne jedynie ewentualne wprowadzenie odpowiedniej licencji):

3.2.9.1. w szczególności zapewnienie możliwości uruchomienia szyfrowania jednocześnie na wszystkich łączach MPLS-TP wychodzących z węzła

3.2.9.2. uruchomienie szyfrowania dla danego łącza powinno odbyć się z poziomu systemu zarządzania siecią bez dokonywania jakichkolwiek zmian sprzętowych, przełączeń fizycznych lub logicznych, rekonfiguracji tuneli MPLS-TP i usług itp.

3.2.10. brak lub możliwość całkowitego wyłączenia lokalnego dostępu z zewnątrz do konfiguracji i zarządzania węzłem:

3.2.10.1. innymi słowy brak lub możliwość całkowitego wyłączenia portu konsoli, portu zarządzania itd.

3.2.11. obsługa co najmniej następujących protokołów i mechanizmów:

3.2.11.1. MPLS-TP, ERPS, IEEE 1588v2, Sync-E

3.2.11.2. protekcja 1:1

3.2.11.3. MSTP, IGMP, 'broadcast and multicast storm control'

3.2.11.4. QoS: min. 3 poziomy hierarchizacji, 4000 kolejek, '802.1p priority evaluation'

3.2.11.5. autentykacja w oparciu o IEEE 802.1x

3.2.11.6. mechanizm ACL w oparciu o adresy MAC i IP ('black/white list')

3.2.11.7. SNMPv3 (szyfrowane) w komunikacji konfiguracji i zarządzania

3.2.11.8. możliwość wyłączenia wszystkich nieużywanych portów

3.2.11.9. automatyczne zestawianie kanałów zarządzania na portach MPLS-TP (w oparciu o dedykowany i niedostępny z zewnątrz tunel

3.2.11.10. OAM wspierany sprzętowo: automatyczne i niezależne od sterowania przełączanie protekcyjne w oparciu o mechanizm BFD, 'Performance Monitoring' oparty na Y.1731

3.2.12. zastosowanie wymiennej pamięci (np. w postaci karty SD), umożliwiającej szybką wymianę modułów matryc przełączających wraz z przeniesieniem konfiguracji węzła

3.3. Wymagane jest dostarczenie jednego urządzenia o charakterystyce zgodnej z kompletacją węzła typu agregacyjnego

3.4. Kompletacja węzła typu agregacyjnego:

3.4.1. chassis o następujących parametrach / właściwościach:

3.4.1.1. montaż w szafie 19" lub na szynie DIN

3.4.1.2. wysokość nie przekraczająca 3 RU

3.4.1.3. modularna konstrukcja umożliwiająca montaż wymiennych kart interfejsów, wymiennych kart matryc przełączających, wymiennych kart zasilaczy, wymiennej karty nadzorczej

3.4.1.4. możliwość zasilania zarówno 48 VDC jak i 230 VAC (również miksu obu)

3.4.1.5. możliwość montażu co najmniej 10 kart interfejsów (mających dostęp do co najmniej 4 portów 10Gbit/s i 24 portów 1Gbit/s w kierunku magistrali / szyny komunikacyjnej)

3.4.1.6. możliwość jednoczesnego wyposażenia węzła w co najmniej 4 porty 10GbE (liniowe/klienckie) + 16 portów GbE (liniowe/klienckie) + 12 portów GbE (klienckie)

3.4.1.7. wykluczone zastosowanie wbudowanych 'na stałe' w chassis interfejsów optycznych/elektrycznych, portów komunikacyjnych, kart transmisyjnych, wentylatorów, itp.

3.4.1.8. obsługa połączeń typu MPLS-TP na portach GbE i 10GbE co najmniej w konfiguracji E-LINE, E-LAN, pierścień, podpierścień

3.4.1.9. możliwość udostępnienia m.in. interfejsów GbE, 10GbE, E1, RS-232/422/485

3.4.1.10. pasywne chłodzenie, realizowane bez zastosowania wentylatorów i jakichkolwiek innych ruchomych elementów

3.4.1.11. dostępność wszystkich złączy, kart, portów i interfejsów, styków zasilania itp. od frontu urządzenia

3.4.1.12. wzmocniona konstrukcja charakterystyczna dla przemysłowych zastosowań, możliwość pracy w zakresie temperatur co najmniej od –30 do +65°C

3.4.1.13. oznaczenie CE i zgodność z wymaganiami Dyrektywy 93/68/EC

3.4.2. wyposażenie w dwa redundantne wymienne moduły zasilające 230 VAC, z możliwością wymiany / zmiany 'na gorąco' (przy wyjęciu jednego z nich węzeł zachowa pełną funkcjonalność i sprawność w oparciu o drugi moduł)

3.4.3. wyposażenie w jeden wymienny moduł matrycy przełączającej (MPLS-TP) o minimalnej nieblokowalnej pojemności 4x 10 Gbit/s + 24x 1 Gbit/s

3.4.3.1. z możliwością bezprzerwowego doposażenia węzła w drugi redundantny moduł matrycy przełączającej, co pozwoli na pracę obu matryc w trybie 'ciepłej gotowości' oraz zapewni opcję wymiany 'na gorąco' (przy wyjęciu jednego z modułów węzeł zachowa pełną funkcjonalność i sprawność w oparciu o drugi z nich)

3.4.4. wyposażenie w interfejs 10GbE wraz z optyką typu XFP/SFP+ BiDi (na jedno włókno) o zasięgu 10 km na potrzeby realizacji połączenia MPLS-TP do węzła typu rdzeniowego

3.4.4.1. możliwość uruchomienia drugiego interfejsu 10GbE w celu uzyskania pełnej redundancji połączenia do węzła agregacyjnego: gdzie wyłączenie, niedostępność lub wymiana jednego z tych interfejsów nie spowoduje jakiegokolwiek zakłócenia w pracy drugiego z nich

3.4.4.2. wymiana jakiegokolwiek modułu, karty, interfejsu czy innego elementu węzła niezwiązanego bezpośrednio z przenoszeniem danych przez interfejs 10GbE nie może spowodować zakłócenia w pracy tego interfejsu

3.4.5. wyposażenie w cztery interfejsy GbE wraz z optyką typu BiDi (na jedno włókno) o zasięgu 20 km na potrzeby realizacji połączeń MPLS-TP do węzłów typu dostępowego

3.4.5.1. możliwość uruchomienia drugiego zestawu czterech interfejsów GbE w celu uzyskania pełnej redundancji połączeń do węzłów dostępowych: gdzie wyłączenie, niedostępność lub wymiana jednego z interfejsów danej pary nie spowoduje jakiegokolwiek zakłócenia w pracy drugiego z nich

3.4.5.2. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów 10 GbE

3.4.6. wyposażenie w osiem interfejsów GbE RJ45 na potrzeby realizacji połączeń lokalnych:

3.4.6.1. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów 10 GbE

3.4.6.2. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów GbE realizujących połączenia MPLS-TP do węzłów typu dostępowego

3.4.7. zapewnienie wyprowadzenia kopii ruchu (inaczej obrazu ruchu – tzw. 'port mirroring', „Port Monitor") z portów obsługujących połączenia w węźle agregacyjnym i przekierowania jej za pośrednictwem odseparowanej usługi w sieci MPLS-TP do węzła typu rdzeniowego

3.4.8. zapewnienie niezależności matrycy przełączającej od interfejsów transmisyjnych - innymi słowy wykluczone jest ewentualne zastosowanie interfejsów transmisyjnych umiejscowionych na karcie matrycy przełączającej ruch na potrzeby obsługi połączeń MPLS-TP lub połączeń zewnętrznych

3.4.9. zapewnienie możliwości uruchomienia szyfrowania na każdym łączu MPLS-TP bez ingerencji w konfigurację sprzętową węzła (dopuszczalne jedynie ewentualne wprowadzenie odpowiedniej licencji):

3.4.9.1. w szczególności zapewnienie możliwości uruchomienia szyfrowania jednocześnie na wszystkich łączach MPLS-TP wychodzących z węzła

3.4.9.2. uruchomienie szyfrowania dla danego łącza powinno odbyć się z poziomu systemu zarządzania siecią bez dokonywania jakichkolwiek zmian sprzętowych, przełączeń fizycznych lub logicznych, rekonfiguracji tuneli MPLS-TP i usług itp.

3.4.10. brak lub możliwość całkowitego wyłączenia lokalnego dostępu z zewnątrz do konfiguracji i zarządzania węzłem:

3.4.10.1. innymi słowy brak lub możliwość całkowitego wyłączenia portu konsoli, portu zarządzania itd.

3.4.11. obsługa co najmniej następujących protokołów i mechanizmów:

3.4.11.1. MPLS-TP, ERPS, IEEE 1588v2, Sync-E

3.4.11.2. protekcja 1:1

3.4.11.3. MSTP, IGMP, 'broadcast and multicast storm control'

3.4.11.4. QoS: min. 3 poziomy hierarchizacji, 4000 kolejek, '802.1p priority evaluation'

3.4.11.5. autentykacja w oparciu o IEEE 802.1x

3.4.11.6. mechanizm ACL w oparciu o adresy MAC i IP ('black/white list')

3.4.11.7. SNMPv3 (szyfrowane) w komunikacji konfiguracji i zarządzania

3.4.11.8. możliwość wyłączenia wszystkich nieużywanych portów

3.4.11.9. automatyczne zestawianie kanałów zarządzania na portach MPLS-TP (w oparciu o dedykowany i niedostępny z zewnątrz tunel)

3.4.11.10. OAM wspierany sprzętowo: automatyczne i niezależne od sterowania przełączanie protekcyjne w oparciu o mechanizm BFD, 'Performance Monitoring' oparty na Y.1731

3.4.12. zastosowanie wymiennej pamięci (np. w postaci karty SD), umożliwiającej szybką wymianę modułów matryc przełączających wraz z przeniesieniem konfiguracji węzła

3.5. Wymagane jest dostarczenie jedenastu urządzeń o charakterystyce zgodnej z kompletacją węzła typu dostępowego

3.6. Kompletacja węzła typu dostępowego

3.6.1. chassis o kompaktowej zabudowie o następujących parametrach / właściwościach:

3.6.1.1. montaż na szynie DIN

3.6.1.2. wymiary nieprzekraczające wysokości 180 mm, szerokości 90 mm i głębokości 155 mm (z uwzględnieniem klipsu DIN, styków zasilania itp.)

3.6.1.3. konstrukcja wyposażona w logicznie realizowane funkcjonalności modułów interfejsów, modułu matrycy przełączającej, modułów zasilaczy, modułu nadzorczego

3.6.1.4. obsługa połączeń typu MPLS-TP na portach GbE i 10GbE co najmniej w konfiguracji E-LINE, E-LAN, pierścień, podpierścień

3.6.1.5. możliwość udostępnienia m.in. interfejsów GbE, 10GbE, RS-232/422/485

3.6.1.6. pasywne chłodzenie, realizowane bez zastosowania wentylatorów i jakichkolwiek innych ruchomych elementów

3.6.1.7. dostępność wszystkich interfejsów komunikacyjnych od frontu urządzenia

3.6.1.8. wzmocniona konstrukcja charakterystyczna dla przemysłowych zastosowań, możliwość pracy w zakresie temperatur co najmniej od –30 do +65 ‘C

3.6.1.9. oznaczenie CE i zgodność z wymaganiami Dyrektywy 93/68/EC

3.6.1.10. wyposażenie w dwa redundantne moduły zasilające 24/48 VDC (węzeł musi zachować pełną funkcjonalność i sprawność w oparciu tylko o jedno zasilanie) wraz z adapterami napięcia 230 VAC

3.6.1.11. wyposażenie w moduł matrycy przełączającej o minimalnej nieblokowalnej pojemności 4x 10 Gbit/s + 24x 1 Gbit/s

3.6.1.12. dostępność co najmniej dwóch interfejsów GbE / 10GbE w postaci portów SFP/SFP+, każdy interfejs niezależnie może funkcjonować jako port MPLS-TP lub jako port kliencki

3.6.1.13. dostępność co najmniej dwóch interfejsów GbE w postaci portów SFP, każdy interfejs niezależnie może funkcjonować jako port MPLS-TP lub jako port kliencki

3.6.1.14. dostępność sześciu portów GbE w postaci kieszeni SFP lub styków RJ45 na potrzeby realizacji przyłączeń lokalnych

3.6.2. wyposażenie interfejsów GbE w wymienną optykę typu BiDi (na jedno włókno) na potrzeby realizacji połączeń MPLS-TP do węzłów typu agregacyjnego lub rdzeniowego w liczbie zgodnej z Tabelą 1

Tabela 1 Liczba i typ interfejsów BiDi w węzłach dostępowych

węzeł	**interfejsy MPLS-TP**
D1	2x SFP GbE BiDi 20km
D2	1x SFP GbE BiDi 20km
D3	1x SFP GbE BiDi 20km
D4	1x SFP GbE BiDi 20km
D5	1x SFP GbE BiDi 20km
D6	2x SFP GbE BiDi 20km
D7	1x SFP GbE BiDi 20km
D8	2x SFP GbE BiDi 20km
D9	1x SFP GbE BiDi 20km
D10	1x SFP GbE BiDi 20km
D11	1x SFP GbE BiDi 20km

3.6.3. zapewnienie wyprowadzenia kopii ruchu (inaczej obrazu ruchu – tzw. ‘port mirroring’, „Port Monitor”) z portów obsługujących połączenia w węźle dostępowym i przekierowania jej za pośrednictwem odseparowanej usługi w sieci MPLS-TP do węzła typu rdzeniowego

3.6.4. zapewnienie możliwości uruchomienia szyfrowania na każdym łączu MPLS-TP bez ingerencji w konfigurację sprzętową węzła (dopuszczalne jedynie ewentualne wprowadzenie odpowiedniej licencji):

3.6.4.1. w szczególności zapewnienie możliwości uruchomienia szyfrowania jednocześnie na wszystkich łączach MPLS-TP wychodzących z węzła

3.6.4.2. uruchomienie szyfrowania dla danego łącza powinno odbyć się z poziomu systemu zarządzania siecią bez dokonywania jakichkolwiek zmian sprzętowych, przełączeń fizycznych lub logicznych, rekonfiguracji tuneli MPLS-TP i usług itp.

3.6.5. brak lub możliwość całkowitego wyłączenia lokalnego dostępu z zewnątrz do konfiguracji i zarządzania węzłem

3.6.5.1. innymi słowy brak lub możliwość całkowitego wyłączenia portu konsoli, portu zarządzania itd.

3.6.6. obsługa co najmniej następujących protokołów i mechanizmów:

3.6.6.1. MPLS-TP, ERPS, IEEE 1588v2, Sync-E

3.6.6.2. protekcja 1:1

3.6.6.3. MSTP, IGMP, 'broadcast and multicast storm control'

3.6.6.4. QoS: min. 3 poziomy hierarchizacji, 4000 kolejek, '802.1p priority evaluation'

3.6.6.5. autentykacja w oparciu o IEEE 802.1x

3.6.6.6. mechanizm ACL w oparciu o adresy MAC i IP ('black/white list')

3.6.6.7. SNMPv3 (szyfrowane) w komunikacji konfiguracji i zarządzania

3.6.6.8. możliwość wyłączenia wszystkich nieużywanych portów

3.6.6.9. automatyczne zestawianie kanałów zarządzania na portach MPLS-TP (w oparciu o dedykowany i niedostępny z zewnątrz tunel)

3.6.6.10. OAM wspierany sprzętowo: automatyczne i niezależne od sterowania przełączanie protekcyjne w oparciu o mechanizm BFD, 'Performance Monitoring' oparty na Y.1731

3.6.7. zastosowanie wymiennej pamięci (np. w postaci karty SD), umożliwiającej szybką wymianę urządzenia wraz z przeniesieniem konfiguracji węzła

4. Wymagania w zakresie dostawy systemu konfiguracji, zarządzania i nadzoru NMS dla zamówienia podstawowego

4.1. Wymagane jest dostarczenie wraz z urządzeniami systemu konfiguracji i zarządzania siecią zgodnego z wymaganiami przedstawionymi w niniejszym dokumencie oraz z rekomendacjami zawartymi w „Koncepcji budowy sieci szkieletowej OT opartej o technikę MPLS-TP"

4.2. W szczególności wymagane jest w kontekście systemu NMS:

4.2.1. dostarczenie oprogramowania i licencji umożliwiających uruchomienie serwera podstawowego

4.2.1.1. z możliwością uzupełnienia systemu o zapasowy serwer

4.2.1.2. w układzie dwóch serwerów obie instancje znajdują się na dwóch oddzielnych maszynach serwerowych

4.2.1.3. w układzie dwóch serwerów obie instancje działają w trybie „warm standby", zapewniającym ciągłość pracy systemu NMS w przypadku uszkodzenia lub niedostępności serwera podstawowego

4.2.2. dostarczenie systemu umożliwiającego połączenie się aplikacją kliencką z serwerem z dowolnego miejsca w sieci, które posiada łączność z serwerem

4.2.2.1. brak ograniczenia licencyjnego co do lokalizacji, liczby użytkowników, liczby aplikacji klienckich itp.

4.2.3. dostarczenie wszelkiego oprogramowania i licencji niezbędnych do osiągnięcia pełni wskazanych w niniejszym dokumencie funkcjonalności oczekiwanych na dzień przekazania urządzeń i systemu Zamawiającemu, niezależnie od tego czy wszystkie będą w tym dniu wykorzystywane

4.2.4. zapewnienie dożywotniej dostępności wszystkich wymaganych przez Zamawiającego właściwości i funkcjonalności dotyczących urządzeń i systemu zarządzania siecią NMS

4.2.4.1. zabronione jest stosowanie ograniczenia czasowego dla licencji czy funkcjonalności, formy 'wygasania' licencji czy funkcjonalności bądź jakiejkolwiek innej właściwości prowadzącej do utraty przez Zamawiającego nabytych funkcjonalności

4.2.4.2. zabronione jest stosowanie odnawialnych cyklicznych licencji i innych analogicznych form

4.2.5. dostarczenie systemu posiadającego graficzny interfejs użytkownika realizujący pełnię funkcjonalności z poziomu sieci
4.2.5.1. wykluczone jest stosowanie rozwiązań zewnętrznych (firm trzecich) w celu osiągnięcia pełni funkcjonalności
4.2.5.2. zabronione jest osiąganie funkcjonalności w sposób, który wymagałby od użytkownika lub operatora bezpośredniego działania na pojedynczych urządzeniach sieciowych
4.2.6. konieczne jest zastosowanie systemu posiadającego interfejs użytkownika zarówno w języku polskim i języku angielskim:
4.2.6.1. wskazane jest, aby wybór języka był powiązany z konkretnym użytkownikiem systemu NMS

5. Wymagania w zakresie rozszerzeń i dostawy urządzeń dla prawa opcji
5.1. Wymagane jest rozszerzenie urządzenia Zamawiającego o charakterystyce zgodnej z kompletacją węzła typu rdzeniowego:
5.1.1. doposażenie w drugi redundantny wymienny moduł matrycy przełączającej (MPLS-TP) o minimalnej nieblokowalnej pojemności 60x 10 Gbit/s
5.1.1.1. co pozwoli na pracę obu matryc w trybie 'ciepłej gotowości' oraz zapewni opcję wymiany 'na gorąco' (przy wyjęciu jednego z modułów węzeł zachowa pełną funkcjonalność i sprawność w oparciu o drugi z nich)
5.1.2. doposażenie do osiągnięcia liczby dwunastu interfejsów 10GbE wraz z optyką typu XFP/SFP+ BiDi (na jedno włókno) o zasięgu 10 km na potrzeby realizacji sześciu redundantnych połączeń MPLS-TP do węzłów typu agregacyjnego (tj. na potrzeby realizacji tzw. gałęzi głównych)
5.1.2.1. każdy węzeł agregacyjny musi być dostępny przez dwa całkowicie niezależne interfejsy XFP/SFP+, gdzie wyłączenie, niedostępność lub wymiana jednego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować jakiegokolwiek zakłócenia w pracy drugiego z nich
5.1.2.2. interfejsy te powinny być również niezależne od jakichkolwiek innych interfejsów obsługiwanych przez węzeł (np. dotyczących tzw. pierścienia pośredniego, wyjść do systemów OT, wyjść lokalnych itp.)
5.1.2.3. wymiana jakiegokolwiek modułu, karty, interfejsu czy innego elementu węzła nie może spowodować jednoczesnego zakłócenia w pracy obu interfejsów 10GbE zapewniających redundantną łączność do tego samego węzła typu agregacyjnego
5.1.3. wyposażenie w dwa interfejsy 10GbE wraz z optyką typu XFP/SFP+ BiDi (na jedno włókno) o zasięgu 10 km na potrzeby realizacji połączeń w pierścieniu pośrednim
5.1.3.1. oba interfejsy dostępne na osobnych kartach transmisyjnych
5.1.3.2. wyłączenie, niedostępność lub wymiana jednego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować jakiejkolwiek przerwy w pracy drugiego z nich
5.1.3.3. wymiana jakiegokolwiek modułu, karty, interfejsu czy innego elementu węzła nie może spowodować jednoczesnego zakłócenia w pracy obu interfejsów 10GbE zapewniających łączność w ramach pierścienia pośredniego
5.1.4. doposażenie do osiągnięcia liczby czterech interfejsów 10GbE rozdzielonych równomiernie na co najmniej dwa niezależne moduły (karty) transmisyjne z optyką typu XFP/SFP+ MM 1310 nm na potrzeby realizacji połączeń z serwerami OT oraz systemem monitorowania:
5.1.4.1. wyłączenie, niedostępność lub wymiana optyki dowolnego z tych interfejsów nie może spowodować zakłócenia w pracy innego interfejsu 10 GbE
5.1.4.2. wyłączenie, niedostępność lub wymiana interfejsu lub karty transmisyjnej z nim związanej nie może spowodować jakiejkolwiek przerwy w pracy interfejsu na innej karcie transmisyjnej
5.1.4.3. wyłączenie lub wymiana dowolnego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować zakłócenia w pracy któregokolwiek

z interfejsów 10 GbE będących częścią gałęzi głównych lub jednoczesnego zakłócenia w pracy obu interfejsów 10 GbE będących częścią pierścienia pośredniego

5.1.5. doposażenie do osiągnięcia liczby dziesięciu interfejsów GbE RJ45 na potrzeby realizacji redundantnych połączeń z firewall'em OT:

5.1.5.1. wyłączenie, niedostępność lub wymiana wkładki optycznej jednego z redundantnych interfejsów w parze bądź wymiana karty transmisyjnej z nim związanej nie może spowodować jakiegokolwiek zakłócenia w pracy drugiego interfejsu z danej redundantnej pary

5.1.5.2. wyłączenie, niedostępność lub wymiana wkładki optycznej jednego z redundantnych interfejsów w parze bądź wymiana karty transmisyjnej z nim związanej nie może spowodować jednoczesnego zakłócenia lub niedostępności w pracy obu interfejsów z innej pary

5.1.5.3. wyłączenie lub wymiana dowolnego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować zakłócenia w pracy któregokolwiek z interfejsów 10 GbE

5.1.6. wyposażenie w cztery interfejsy GbE RJ45 na potrzeby realizacji przyłączeń lokalnych

5.1.7. zapewnienie niezależności matryc przełączających od interfejsów transmisyjnych - innymi słowy wykluczone jest ewentualne zastosowanie interfejsów transmisyjnych umiejscowionych na kartach matryc przełączających ruch na potrzeby obsługi połączeń MPLS-TP lub połączeń zewnętrznych

5.1.8. zapewnienie możliwości uruchomienia szyfrowania na każdym łączu MPLS-TP bez ingerencji w konfigurację sprzętową czy licencyjną węzła:

5.1.8.1. w szczególności zapewnienie możliwości uruchomienia szyfrowania jednocześnie na wszystkich łączach MPLS-TP przychodzących/wychodzących z węzła

5.1.8.2. uruchomienie szyfrowania dla danego łącza powinno odbyć się z poziomu systemu zarządzania siecią bez dokonywania jakichkolwiek zmian sprzętowych, przełączeń fizycznych lub logicznych, rekonfiguracji tuneli MPLS-TP i usług, wprowadzania dodatkowych licencji lub urządzeń itp.

5.1.9. brak lub możliwość całkowitego wyłączenia lokalnego dostępu z zewnątrz do konfiguracji i zarządzania węzłem:

5.1.9.1. innymi słowy brak lub możliwość całkowitego wyłączenia portu konsoli, portu zarządzania itd.

5.1.10. obsługa co najmniej następujących protokołów i mechanizmów:

5.1.10.1. MPLS-TP, ERPS, IEEE 1588v2, Sync-E

5.1.10.2. protekcja 1:1

5.1.10.3. MSTP, IGMP, 'broadcast and multicast storm control'

5.1.10.4. QoS: min. 3 poziomy hierarchizacji, 4000 kolejek, '802.1p priority evaluation'

5.1.10.5. autentykacja w oparciu o IEEE 802.1x

5.1.10.6. mechanizm ACL w oparciu o adresy MAC i IP ('black/white list')

5.1.10.7. SNMPv3 (szyfrowane) w komunikacji konfiguracji i zarządzania

5.1.10.8. możliwość wyłączenia wszystkich nieużywanych portów

5.1.10.9. automatyczne zestawianie kanałów zarządzania na portach MPLS-TP (w oparciu o dedykowany i niedostępny z zewnątrz tunel)

5.1.10.10. OAM wspierany sprzętowo: automatyczne i niezależne od sterowania przełączanie protekcyjne w oparciu o mechanizm BFD, 'Performance Monitoring' oparty na Y.1731

5.1.11. zastosowanie wymiennej pamięci (np. w postaci karty SD), umożliwiającej szybką wymianę modułów matryc przełączających wraz z przeniesieniem konfiguracji węzła

5.2. Wymagane jest rozszerzenie urządzenia Zamawiającego o charakterystyce zgodnej z kompletacją węzła typu agregacyjnego:

5.2.1. doposażenie w drugi redundantny wymienny moduł matrycy przełączającej (MPLS-TP) o minimalnej nieblokowalnej pojemności 4x 10 Gbit/s + 24x 1 Gbit/s
  5.2.1.1. co pozwoli na pracę obu matryc w trybie 'ciepłej gotowości' oraz zapewni opcję wymiany 'na gorąco' (przy wyjęciu jednego z modułów węzeł zachowa pełną funkcjonalność i sprawność w oparciu o drugi z nich)
5.2.2. doposażenie do osiągnięcia liczby dwóch interfejsów 10GbE wraz z optyką typu XFP/SFP+ BiDi (na jedno włókno) o zasięgu 10 km na potrzeby realizacji redundantnego połączenia MPLS-TP do węzła typu rdzeniowego (tj. na potrzeby realizacji tzw. gałęzi głównych)
  5.2.2.1. każdy z interfejsów dostępny na osobnej karcie transmisyjnej
  5.2.2.2. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować jakiegokolwiek zakłócenia w pracy drugiego z nich
  5.2.2.3. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować jakiegokolwiek zakłócenia w pracy któregokolwiek z innych interfejsów w węźle
  5.2.2.4. wymiana jakiegokolwiek modułu, karty, interfejsu czy innego elementu węzła nie może spowodować jednoczesnego zakłócenia w pracy obu redundantnych interfejsów 10GbE zapewniających łączność węzła agregacyjnego z węzłem rdzeniowym
5.2.3. doposażenie do osiągnięcia liczby ośmiu interfejsów GbE wraz z optyką typu BiDi (na jedno włókno) o zasięgu 20 km na potrzeby realizacji połączeń MPLS-TP do węzłów typu dostępowego
  5.2.3.1. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów 10 GbE
  5.2.3.2. wymiana jakiegokolwiek innego modułu / karty / interfejsu / elementu węzła nie może spowodować zakłócenia w pracy interfejsów GbE zapewniających łączność węzła agregacyjnego z węzłami dostępowymi
  5.2.3.3. (dopuszczalne jest wykorzystanie modułów interfejsów i/lub optyki GbE zwolnionych z węzła typu rdzeniowego)
5.2.4. doposażenie do osiągnięcia liczby sześciu interfejsów GbE RJ45 na potrzeby realizacji połączeń lokalnych
  5.2.4.1. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów 10 GbE
  5.2.4.2. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów GbE realizujących połączenia MPLS-TP do węzłów typu dostępowego
5.2.5. zapewnienie wyprowadzenia kopii ruchu (inaczej obrazu ruchu, "Port Monitor", "Port Mirroring") z portów w węźle i przekierowania jej za pośrednictwem odseparowanej usługi w sieci MPLS-TP do węzła typu rdzeniowego
5.2.6. zapewnienie niezależności matryc przełączających od interfejsów transmisyjnych - innymi słowy wykluczone jest ewentualne zastosowanie interfejsów transmisyjnych umiejscowionych na kartach matryc przełączających ruch na potrzeby obsługi połączeń MPLS-TP lub połączeń zewnętrznych
5.2.7. zapewnienie możliwości uruchomienia szyfrowania na każdym łączu MPLS-TP bez ingerencji w konfigurację sprzętową czy licencyjną węzła:
  5.2.7.1. w szczególności zapewnienie możliwości uruchomienia szyfrowania jednocześnie na wszystkich łączach MPLS-TP przychodzących/wychodzących z węzła
  5.2.7.2. uruchomienie szyfrowania dla danego łącza powinno odbyć się z poziomu systemu zarządzania siecią bez dokonywania jakichkolwiek zmian sprzętowych,

przełączeń fizycznych lub logicznych, rekonfiguracji tuneli MPLS-TP i usług, wprowadzania dodatkowych licencji lub urządzeń itp.

5.2.8. brak lub możliwość całkowitego wyłączenia lokalnego dostępu z zewnątrz do konfiguracji i zarządzania węzłem:

5.2.8.1. innymi słowy brak lub możliwość całkowitego wyłączenia portu konsoli, portu zarządzania itd.

5.2.9. obsługa co najmniej następujących protokołów i mechanizmów:

5.2.9.1. MPLS-TP, ERPS, IEEE 1588v2, Sync-E

5.2.9.2. protekcja 1:1

5.2.9.3. MSTP, IGMP, 'broadcast and multicast storm control'

5.2.9.4. QoS: min. 3 poziomy hierarchizacji, 4000 kolejek, '802.1p priority evaluation'

5.2.9.5. autentykacja w oparciu o IEEE 802.1x

5.2.9.6. mechanizm ACL w oparciu o adresy MAC i IP ('black/white list')

5.2.9.7. SNMPv3 (szyfrowane) w komunikacji konfiguracji i zarządzania

5.2.9.8. możliwość wyłączenia wszystkich nieużywanych portów

5.2.9.9. automatyczne zestawianie kanałów zarządzania na portach MPLS-TP (w oparciu o dedykowany i niedostępny z zewnątrz tunel)

5.2.9.10. OAM wspierany sprzętowo: automatyczne i niezależne od sterowania przełączanie protekcyjne w oparciu o mechanizm BFD, 'Performance Monitoring' oparty na Y.1731

5.2.10. zastosowanie wymiennej pamięci (np. w postaci karty SD), umożliwiającej szybką wymianę modułów matryc przełączających wraz z przeniesieniem konfiguracji węzła

5.3. Wymagane jest dostarczenie pięciu nowych urządzeń o charakterystyce zgodnej z kompletacją węzła typu agregacyjnego:

5.3.1. chassis o następujących parametrach / właściwościach:

5.3.1.1. montaż w szafie 19" lub na szynie DIN

5.3.1.2. wysokość nie przekraczająca 3 RU

5.3.1.3. modularna konstrukcja umożliwiająca montaż wymiennych kart interfejsów, wymiennych kart matryc przełączających, wymiennych kart zasilaczy, wymiennej karty nadzorczej

5.3.1.4. możliwość zasilania zarówno 48 VDC jak i 230 VAC (również miksu obu)

5.3.1.5. możliwość montażu co najmniej 10 kart interfejsów (mających dostęp do co najmniej 4 portów 10Gbit/s i 24 portów 1Gbit/s w kierunku magistrali / szyny komunikacyjnej)

5.3.1.6. możliwość jednoczesnego wyposażenia węzła w co najmniej 4 porty 10GbE (liniowe/klienckie) + 16 portów GbE (liniowe/klienckie) + 12 portów GbE (klienckie)

5.3.1.7. wykluczone zastosowanie wbudowanych 'na stałe' w chassis interfejsów optycznych/elektrycznych, portów komunikacyjnych, kart transmisyjnych, wentylatorów, itp.

5.3.1.8. obsługa połączeń typu MPLS-TP na portach GbE i 10GbE co najmniej w konfiguracji E-LINE, E-LAN, pierścień, podpierścień

5.3.1.9. możliwość udostępnienia m.in. interfejsów GbE, 10GbE, E1, RS-232/422/485

5.3.1.10. pasywne chłodzenie, realizowane bez zastosowania wentylatorów i jakichkolwiek innych ruchomych elementów

5.3.1.11. dostępność wszystkich złączy, kart, portów i interfejsów, styków zasilania itp. od frontu urządzenia

5.3.1.12. wzmocniona konstrukcja charakterystyczna dla przemysłowych zastosowań, możliwość pracy w zakresie temperatur co najmniej od –30 do +65°C

5.3.1.13. oznaczenie CE i zgodność z wymaganiami Dyrektywy 93/68/EC

5.3.2. wyposażenie w dwa redundantne wymienne moduły zasilające 230 VAC, z możliwością wymiany / zmiany 'na gorąco' (przy wyjęciu jednego z nich węzeł zachowa pełną funkcjonalność i sprawność w oparciu o drugi moduł)

5.3.3. wyposażenie w dwa redundantne wymienne moduły matryc przełączających (MPLS-TP) o minimalnej nieblokowalnej pojemności 4x 10 Gbit/s + 24x 1 Gbit/s, z możliwością wymiany ‘na gorąco’ (przy wyjęciu jednego z modułów węzeł zachowa pełną funkcjonalność i sprawność w oparciu o drugi z nich)

5.3.4. wyposażenie w dwa interfejsy 10GbE wraz z optyką typu XFP/SFP+ BiDi (na jedno włókno) o zasięgu 10 km na potrzeby realizacji redundantnych połączeń MPLS-TP do węzła typu rdzeniowego (tj. na potrzeby realizacji tzw. gałęzi głównych)

5.3.4.1. każdy z interfejsów dostępny na osobnej karcie transmisyjnej

5.3.4.2. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować jakiegokolwiek zakłócenia w pracy drugiego z nich

5.3.4.3. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej z nim związanej nie może spowodować jakiegokolwiek zakłócenia w pracy któregokolwiek z innych interfejsów w węźle

5.3.4.4. wymiana jakiegokolwiek modułu, karty, interfejsu czy innego elementu węzła nie może spowodować jednoczesnego zakłócenia w pracy obu redundantnych interfejsów 10GbE zapewniających łączność węzła agregacyjnego z węzłem rdzeniowym

Tabela 2 Liczba interfejsów GbE BiDi w węzłach agregacyjnych

Węzeł	A2	A3	A4	A5	A6
liczba interfejsów GbE	1	3	6	7	1

5.3.5. wyposażenie w interfejsy GbE wraz z wymienną optyką typu BiDi (na jedno włókno) o zasięgu 20 km na potrzeby realizacji połączeń MPLS-TP do węzłów typu dostępowego w liczbie zgodnej z Tabelą 1:

5.3.5.1. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów 10 GbE

5.3.5.2. wymiana jakiegokolwiek innego modułu / karty / interfejsu / elementu węzła nie może spowodować zakłócenia w pracy interfejsów GbE zapewniających łączność węzła agregacyjnego z węzłami dostępowymi

5.3.6. wyposażenie w co najmniej sześć interfejsów GbE RJ45 na potrzeby realizacji połączeń lokalnych:

5.3.6.1. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów 10 GbE

5.3.6.2. wyłączenie lub wymiana jednego z tych interfejsów lub karty transmisyjnej związanej z tymi interfejsami nie może spowodować jakiejkolwiek przerwy w pracy interfejsów GbE realizujących połączenia MPLS-TP do węzłów typu pośredniego/dostępowego

5.3.7. zapewnienie wyprowadzenia kopii ruchu (inaczej obrazu ruchu, “Port Monitor”, “Port Mirroring”) z portów obsługujących połączenia lokalne i przekierowania jej za pośrednictwem odseparowanej usługi w sieci MPLS-TP do węzła typu rdzeniowego

5.3.8. zapewnienie niezależności matrycy przełączającej od interfejsów transmisyjnych - innymi słowy wykluczone jest ewentualne zastosowanie interfejsów transmisyjnych umiejscowionych na karcie matrycy przełączającej ruch na potrzeby obsługi połączeń MPLS-TP lub połączeń zewnętrznych

5.3.9. zapewnienie możliwości uruchomienia szyfrowania na każdym łączu MPLS-TP bez ingerencji w konfigurację sprzętową czy licencyjną węzła:

5.3.9.1. w szczególności zapewnienie możliwości uruchomienia szyfrowania jednocześnie na wszystkich łączach MPLS-TP przychodzących/wychodzących z węzła

5.3.9.2. uruchomienie szyfrowania dla danego łącza powinno odbyć się z poziomu systemu zarządzania siecią bez dokonywania jakichkolwiek zmian sprzętowych, przełączeń fizycznych lub logicznych, rekonfiguracji tuneli MPLS-TP i usług, wprowadzania dodatkowych licencji lub urządzeń itp.

5.3.10. brak lub możliwość całkowitego wyłączenia lokalnego dostępu z zewnątrz do konfiguracji i zarządzania węzłem:

5.3.10.1. innymi słowy brak lub możliwość całkowitego wyłączenia portu konsoli, portu zarządzania itd.

5.3.11. obsługa co najmniej następujących protokołów i mechanizmów:

5.3.11.1. MPLS-TP, ERPS, IEEE 1588v2, Sync-E

5.3.11.2. protekcja 1:1

5.3.11.3. MSTP, IGMP, 'broadcast and multicast storm control'

5.3.11.4. QoS: min. 3 poziomy hierarchizacji, 4000 kolejek, '802.1p priority evaluation'

5.3.11.5. autentykacja w oparciu o IEEE 802.1x

5.3.11.6. mechanizm ACL w oparciu o adresy MAC i IP ('black/white list')

5.3.11.7. SNMPv3 (szyfrowane) w komunikacji konfiguracji i zarządzania

5.3.11.8. możliwość wyłączenia wszystkich nieużywanych portów

5.3.11.9. automatyczne zestawianie kanałów zarządzania na portach MPLS-TP (w oparciu o dedykowany i niedostępny z zewnątrz tunel)

5.3.11.10. OAM wspierany sprzętowo: automatyczne i niezależne od sterowania przełączanie protekcyjne w oparciu o mechanizm BFD, 'Performance Monitoring' oparty na Y.1731

5.3.12. zastosowanie wymiennej pamięci (np. w postaci karty SD), umożliwiającej szybką wymianę modułów matryc przełączających wraz z przeniesieniem konfiguracji węzła

5.4. Wymagana jest relokacja jedenastu posiadanych urządzeń o charakterystyce zgodnej z kompletacją węzła typu dostępowego dostarczanych w ramach zamówienia podstawowego

5.5. Wymagane jest dostarczenie siedemnastu urządzeń o charakterystyce zgodnej z kompletacją węzła typu dostępowego dla Wariantu 1

5.6. Wymagane jest dostarczenie dziewięciu urządzeń o charakterystyce zgodnej z kompletacją węzła typu dostępowego dla Wariantu 2

5.7. Kompletacja węzła typu dostępowego:

5.7.1. węzeł o kompaktowej zabudowie, realizowany w dwóch wariantach w zależności od lokalnych potrzeb transmisyjnych na danym obiekcie

5.7.2. węzeł o następujących parametrach / właściwościach dla Wariantu 1:

5.7.2.1. montaż w szafce/stojaku 19"

5.7.2.2. wysokość 1 RU, głębokość poniżej 300 mm

5.7.3. węzeł o następujących parametrach / właściwościach dla Wariantu 2:

5.7.3.1. montaż na szynie DIN

5.7.3.2. wymiary nieprzekraczające wysokości 180 mm, szerokości 90 mm i głębokości 155 mm (z uwzględnieniem klipsu DIN, styków zasilania itp.)

5.7.4. węzeł o następujących parametrach / właściwościach charakterystycznych zarówno dla Wariantu 1 oraz Wariantu 2:

5.7.4.1. konstrukcja wyposażona w logicznie realizowane funkcjonalności modułów interfejsów, modułu matrycy przełączającej, modułów zasilaczy, modułu nadzorczego

5.7.4.2. obsługa połączeń typu MPLS-TP na portach GbE i 10GbE co najmniej w konfiguracji E-LINE, E-LAN, pierścień, podpierścień

5.7.4.3. możliwość udostępnienia m.in. interfejsów GbE, 10GbE, RS-232/422/485

5.7.4.4. pasywne chłodzenie, realizowane bez zastosowania wentylatorów i jakichkolwiek innych ruchomych elementów

5.7.4.5. dostępność wszystkich interfejsów komunikacyjnych od frontu urządzenia

5.7.4.6. wzmocniona konstrukcja charakterystyczna dla przemysłowych zastosowań, możliwość pracy w zakresie temperatur co najmniej od –30 do +65 'C

5.7.4.7. oznaczenie CE i zgodność z wymaganiami Dyrektywy 93/68/EC

5.7.4.8. wyposażenie w dwa redundantne moduły zasilające 24/48 VDC (węzeł musi zachować pełną funkcjonalność i sprawność w oparciu tylko o jedno zasilanie) wraz z adapterami napięcia 230 VAC

5.7.4.9. wyposażenie w moduł matrycy przełączającej o minimalnej nieblokowalnej pojemności 4x 10 Gbit/s + 24x 1 Gbit/s

5.7.4.10. dostępność co najmniej dwóch interfejsów GbE / 10GbE w postaci portów SFP/SFP+, każdy interfejs niezależnie może funkcjonować jako port MPLS-TP lub jako port kliencki

5.7.4.11. dostępność co najmniej dwóch interfejsów GbE w postaci portów SFP, każdy interfejs niezależnie może funkcjonować jako port MPLS-TP lub jako port kliencki

5.7.4.12. dostępność co najmniej dwudziestu (Wariant 1) lub sześciu (Wariant 2) portów GbE w postaci kieszeni SFP lub styków RJ45 na potrzeby realizacji przyłączeń lokalnych

5.7.5. wyposażenie interfejsów GbE / 10GbE w wymienną optykę typu BiDi (na jedno włókno) na potrzeby realizacji połączeń MPLS-TP do węzłów typu agregacyjnego lub rdzeniowego w liczbie zgodnej z Tabelą 2

Tabela 3 Liczba i typ interfejsów BiDi w węzłach dostępowych

węzeł	**interfejsy MPLS-TP**
D12	2x SFP GbE BiDi 20km
D13	2x SFP GbE BiDi 20km
D14	2x SFP GbE BiDi 20km
D15	1x SFP GbE BiDi 20km
D16	1x SFP GbE BiDi 20km
D17	1x SFP GbE BiDi 20km
D18	1x SFP GbE BiDi 20km
D19	1x SFP GbE BiDi 20km
D20	1x SFP GbE BiDi 20km
D21	1x SFP GbE BiDi 20km
D22	1x SFP GbE BiDi 20km
D23	1x SFP GbE BiDi 20km
D24	1x SFP GbE BiDi 20km
D25	1x SFP GbE BiDi 20km
D26	1x SFP GbE BiDi 20km
D27	1x SFP GbE BiDi 20km
D28	1x SFP GbE BiDi 20km
D29	1x SFP GbE BiDi 20km
D30	1x SFP GbE BiDi 20km
D31	1x SFP GbE BiDi 20km
D32	1x SFP GbE BiDi 20km
D33	1x SFP GbE BiDi 20km
D34	2x SFP+ 10GbE BiDi 10km
D35	2x SFP+ 10GbE BiDi 10km
D36	2x SFP+ 10GbE BiDi 10km
D37	2x SFP+ 10GbE BiDi 10km

5.7.6. zapewnienie wyprowadzenia kopii ruchu (inaczej obrazu ruchu – tzw. ‘port mirroring’, „Port Monitor”) z portów obsługujących połączenia w węźle dostępowym i przekierowania jej za pośrednictwem odseparowanej usługi w sieci MPLS-TP do węzła typu rdzeniowego

5.7.7. zapewnienie możliwości uruchomienia szyfrowania na każdym łączu MPLS-TP bez ingerencji w konfigurację sprzętową czy licencyjną węzła:

5.7.7.1. w szczególności zapewnienie możliwości uruchomienia szyfrowania jednocześnie na wszystkich łączach MPLS-TP przychodzących/wychodzących z węzła

5.7.7.2. uruchomienie szyfrowania dla danego łącza powinno odbyć się z poziomu systemu zarządzania siecią bez dokonywania jakichkolwiek zmian sprzętowych, przełączeń fizycznych lub logicznych, rekonfiguracji tuneli MPLS-TP i usług, wprowadzania dodatkowych licencji lub urządzeń itp.

5.7.8. brak lub możliwość całkowitego wyłączenia lokalnego dostępu z zewnątrz do konfiguracji i zarządzania węzłem

5.7.8.1. innymi słowy brak lub możliwość całkowitego wyłączenia portu konsoli, portu zarządzania itd.

5.7.9. obsługa co najmniej następujących protokołów i mechanizmów:

5.7.9.1. MPLS-TP, ERPS, IEEE 1588v2, Sync-E

5.7.9.2. protekcja 1:1

5.7.9.3. MSTP, IGMP, 'broadcast and multicast storm control'

5.7.9.4. QoS: min. 3 poziomy hierarchizacji, 4000 kolejek, '802.1p priority evaluation'

5.7.9.5. autentykacja w oparciu o IEEE 802.1x

5.7.9.6. mechanizm ACL w oparciu o adresy MAC i IP ('black/white list')

5.7.9.7. SNMPv3 (szyfrowane) w komunikacji konfiguracji i zarządzania

5.7.9.8. możliwość wyłączenia wszystkich nieużywanych portów

5.7.9.9. automatyczne zestawianie kanałów zarządzania na portach MPLS-TP (w oparciu o dedykowany i niedostępny z zewnątrz tunel)

5.7.9.10. OAM wspierany sprzętowo: automatyczne i niezależne od sterowania przełączanie protekcyjne w oparciu o mechanizm BFD, 'Performance Monitoring' oparty na Y.1731

5.7.10. zastosowanie wymiennej pamięci (np. w postaci karty SD), umożliwiającej szybką wymianę urządzenia wraz z przeniesieniem konfiguracji węzła

6. Wymagania w zakresie rozszerzenia systemu konfiguracji, zarządzania i nadzoru NMS dla prawa opcji

6.1.1. rozszerzenie oprogramowania i licencji w celu uruchomienia serwera zapasowego:

6.1.1.1. obie instancje tj. serwer podstawowy i serwer zapasowy pracujące na dwóch oddzielnych maszynach serwerowych

6.1.1.2. obie instancje działające w trybie „warm standby", zapewniającym ciągłość pracy systemu NMS w przypadku uszkodzenia lub niedostępności serwera podstawowego

6.1.2. dostarczenie wszelkiego oprogramowania i licencji niezbędnych do osiągnięcia pełni wskazanych w niniejszym dokumencie funkcjonalności oczekiwanych na dzień przekazania urządzeń i systemu Zamawiającemu, niezależnie od tego czy wszystkie będą w tym dniu wykorzystywane

6.1.2.1. w szczególności objęcie systemem wszystkich węzłów, urządzeń i funkcjonalności związanych z rozszerzeniem węzłów, urządzeń i sieci

6.1.3. zapewnienie dożywotniej dostępności wszystkich wymaganych przez Zamawiającego właściwości i funkcjonalności dotyczących urządzeń i systemu zarządzania siecią NMS

6.1.3.1. zabronione jest stosowanie ograniczenia czasowego dla licencji czy funkcjonalności, formy 'wygasania' licencji czy funkcjonalności bądź jakiejkolwiek innej właściwości prowadzącej do utraty przez Zamawiającego nabytych funkcjonalności

6.1.3.2. zabronione jest stosowanie odnawialnych cyklicznych licencji i innych analogicznych form

6.1.4. dostarczenie systemu posiadającego graficzny interfejs użytkownika realizujący pełnię funkcjonalności z poziomu sieci

6.1.4.1. wykluczone jest stosowanie rozwiązań zewnętrznych (firm trzecich) w celu osiągnięcia pełni funkcjonalności

6.1.4.2. zabronione jest osiąganie funkcjonalności w sposób, który wymagałby od użytkownika lub operatora bezpośredniego działania na pojedynczych urządzeniach sieciowych

7. Inne wymagania dotyczące dostawy urządzeń i oprogramowania
   7.1. Dostarczone do Zamawiającego urządzenia, system zarządzania oraz wyposażenie muszą być nowe, kompletne, wolne od wad i posiadać wymagane prawem certyfikaty, atesty, deklaracje zgodności CE itp.
   7.2. Wykonawca zobowiązany jest dostarczyć, na własny koszt i ryzyko, wyposażenie w miejsce dostawy oraz we wskazane przez Zamawiającego miejsce dokonania jego montażu (na terenie Polski)
   7.3. Dostawa obejmuje transport wyposażenia do Zamawiającego, rozładunek, wniesienie do wskazanych pomieszczeń
   7.4. Koszty ubezpieczenia przedmiotu zamówienia na czas transportu obciążają Wykonawcę
   7.5. Przy dostawie Wykonawca zobowiązany jest dołączyć instrukcje obsługi w języku polskim lub w języku angielskim

X. Wdrożenie systemu IDS

Wdrożenie systemu musi być realizowane po dokładnym rozpoznaniu systemów automatyki, a proces wdrożenia powinien obejmować jest z następujących kroków:

1. Założenie użytkowników systemu lokalnych (poświadczenia przechowywane w lokalnej bazie danych systemu) lub zdalnych (uwierzytelnianie przez serwery AD lub RSA Secure ID) oraz określenie ról w systemie (co najmniej analityk, ekspert, administrator)
2. Konfiguracja profili detekcji pod kątem zachowania w trybach nauki i detekcji, w szczególności zdefiniowanie czy w trybie nauki system reaguje lub nie na znane zagrożenia wykrywane z wykorzystaniem sygnatur
3. Uruchomienie systemu / systemów IDS w trybie nauki
4. Weryfikacja zidentyfikowanych urządzeń pod kątem kompletności, typów, charakterystyki (dodatkowych danych) pozyskanej z ruchu sieciowego
5. Zdefiniowanie w systemie zaufanych wewnętrznych sieci oraz zaakceptowanych podsieci zewnętrznych stanowiących część monitorowanego systemu
6. Edycja, w razie potrzeby, typu wykrytych urządzeń (PLC, HMI, Serwer, Stacja inżynierska itd.)
7. Wprowadzenie dodatkowych wzbogacających inwentaryzację danych opisowych dla urządzeń (informacje zdefiniowane przez użytkownika), np.: lokalizacja urządzenia, osoba odpowiedzialna, kontakt do serwisu, itp.
8. Weryfikacja zidentyfikowanych połączeń z wykorzystaniem mapy, listy połączeń itp.
9. Weryfikacja zidentyfikowanych protokołów sieciowych, w szczególności wykorzystywanych numerów portów przez protokoły przemysłowe
   9.1. Edycja, zmiana przypisanych numerów portów do nazw protokołów, w przypadku działania danego protokołu na innym niż domyślny porcie
   9.2. Określenie rodzaju analizy DPI dla protokołu działającego na niestandardowym porcie
10. Przegląd listy alarmów wygenerowanych przez system w trakcie nauki
11. Budowa i akceptacja wzorca zachowania sieci przemysłowej (baseline)
    11.1. Weryfikacja utworzonych w trybie nauki przez moduł odpowiednie moduły sugerowanych reguł detekcji, ew. edycja tych reguł, dodanie do wzorca sieci lub do reguł alertowania, dokumentacja reguł dodanych do baseline
    11.2. Utworzenie nowych własnych reguł detekcji, które będą oparte o:
       11.2.1. Warstwę L2: VLAN, Ethertype, adres MAC źródła, adres MAC celu
       11.2.2. Warstwę L3: adres IP źródła, adres IP celu, protokół TCP, UDP, ICMP
       11.2.3. Warstwę L4: protokoły/porty

11.2.4. Warstwę L7: określenie typu głębokiej analizy pakietów (DPI) w warstwie aplikacyjnej dla protokołów przemysłowych określonych w *Załącznik nr 1*.

11.3. Weryfikacja utworzonych w trybie nauki przez oparty o moduł sygnatury sugerowanych reguł, ew. edycja reguł, dodanie do wzorca sieci lub do reguł alertowania, dokumentacja reguł dodanych do baseline

12. Weryfikacja i ew. edycja przypisania zidentyfikowanych urządzeń do stref bezpieczeństwa określonych w standardzie IEC 62443
    12.1. Przypisanie urządzeń do właściwej strefy (zone), zgodnie z wytycznymi określonymi przez zespół zamawiającego
    12.2. Zdefiniowanie docelowego poziomu bezpieczeństwa dla danej strefy w zakresie SL-0 do SL-4, zgodnie z wytycznymi określonymi przez zespół zamawiającego
13. Zdefiniowanie grup urządzeń (procesów biznesowych) i przypisanie do nich zidentyfikowanych urządzeń
    13.1. Określenie nazwy procesu biznesowego
    13.2. Wprowadzenie opisu
    13.3. Określenie poziomu krytyczności procesu biznesowego
14. Sporządzenie potrzebnych widoków na mapie z wykorzystaniem filtrów (typ urządzenia, protokół, adres IP, nazwa, producent,…), procesów biznesowych, i trybów prezentacji urządzeń na mapie (model Purdue, widok przepływów, własny widok zdefiniowany przez zamawiającego)
15. Przełączenie systemu w tryb detekcji
16. Przegląd i rozwiązywanie alarmów i podpowiedzi wygenerowanych przez system, dostrojenie systemu aby nie generował alarmów typu false positive
17. Eliminacja alertów typu false positive, w tym:
    17.1. Przeniesieniu wybranych, przeanalizowanych alertów do wzorca zachowania sieci
    17.2. Wprowadzeniu niezbędnych zmian w konfiguracji silników detekcji
    17.3. Przeniesieniu wybranych alarmów do archiwum i/lub ich usunięcie
    17.4. Sporządzenie dokumentacji dotyczącej przeprowadzonych analiz
18. Integracja z SOC przygotowanie konfiguracji dla współpracy z systemami SIEM lub serwerem SYSLOG
    18.1. Zdefiniowanie profilów dotyczących przekazywania alarmów (co najmniej low, medium, high) i pochodzących, z wybranych silników detekcji
    18.2. Określenie jakie zdarzenia dot. logowania użytkowników będą przekazywane
19. Konfiguracja powiadomień za pomocą wiadomości e-mail
    19.1. Konfiguracja współpracy z zewnętrznym serwerem e-mail
    19.2. konfiguracja listy odbiorców wiadomości e-mail
20. Przekazanie systemu do eksploatacji
    20.1. W ramach uruchomienia i optymalizacji systemu Wykonawca deklaruje że przeprowadzi próby funkcjonalne systemu z udziałem służb Zamawiającego

XI. Wdrożenie i testy systemu MPLS

1. Wymagania w zakresie uruchomienia sprzętu i oprogramowania dla sieci MPLS-TP
   1.1. Wymagane jest wykonanie montażu urządzeń w ramach zamówienia podstawowego oraz ewentualnej relokacji, rozbudowy i montażu urządzeń w ramach prawa opcji we wskazanych przez Zamawiającego szafach
   1.2. Montaż musi być wykonywany przez doświadczony personel:
      1.2.1. posiadający odpowiednie uprawnienia
      1.2.2. posiadający certyfikację producenta sprzętu lub autoryzowanego przedstawiciela producenta
   1.3. W ramach uruchomienia podstawowego jak i prawa opcji oczekiwane jest wykonanie niezbędnego okablowania dostarczonych urządzeń w obrębie istniejących szaf w zakresie:
      1.3.1. zasilania urządzeń

1.3.2. wyprowadzenia portów liniowych MPLS-TP oraz portów klienckich
1.3.3. (połączenia między węzłami w zakresie Zamawiającego)
1.4. Wykonawca musi wykonać instalację systemu nadzoru NMS:
1.4.1. dla serwera podstawowego i ewentualnego serwera zapasowego na wskazanych przez Zamawiającego urządzeniach
1.4.2. dla aplikacji klienckich łączących się z serwerem
1.5. Konieczne jest uruchomienie i konfiguracja wszystkich urządzeń oraz systemu NMS dla zamówienia podstawowego oraz konfiguracja i rekonfiguracja urządzeń oraz systemu NMS dla prawa opcji:
1.5.1. wraz z pełną konfiguracją fizyczną i logiczną
1.5.2. w szczególności dla wszystkich określonych przez Zamawiającego tuneli MPLS-TP oraz usług OT
1.6. Wymagane jest przekazanie Zamawiającemu kopii konfiguracji urządzeń i sieci, która zapewni możliwość odtworzenia prawidłowego stanu
1.7. Realizacja prac następuje w oparciu o najlepsze praktyki i standardy bezpieczeństwa transmisji danych, między innymi IEC 62443
1.8. Niezbędne jest dostarczenie dokumentacji powykonawczej
2. Wymagania w zakresie testów weryfikacyjnych
2.1. W ramach uruchomienia sprzętu i oprogramowania konieczne jest wykonanie testów weryfikacyjnych
2.2. Testy weryfikacyjne mają potwierdzić prawidłowość wykonanego montażu i konfiguracji zarówno urządzeń jak i systemu NMS
2.3. Testy powinny potwierdzać między innymi:
2.3.1. prawidłowość funkcjonowania sieci w stanie ‘normalnej’ pracy
2.3.1.1. prawidłowość reagowania sieci na sytuacje awaryjne, w szczególności w zakresie poprawności przekazywanych komunikatów, alarmów itp.
2.3.2. poprawność zachowania systemu w zakresie zapobiegania wprowadzeniu przez użytkownika niewłaściwych konfiguracji, błędnych ustawień, nadsubskrypcji pasma itp.
2.3.3. zachowanie poprawności przenoszenia danych w różnych scenariuszach redundancji i protekcji
2.3.4. zachowanie poprawności przenoszenia danych i funkcjonowania mechanizmów protekcyjnych w przypadku całkowitej niedostępności systemu zarządzania siecią
2.3.5. poprawność odtwarzania kopii zapasowych w przypadku utraty informacji lub wymiany elementów sieciowych
2.3.6. prawidłowość powrotu urządzeń i systemu zarządzania do właściwej pracy po ustąpieniu przyczyn powodujących nieprawidłowości, na przykład:
2.3.6.1. w przypadku całkowitej utraty źródeł zasilania
2.3.6.2. w przypadku całkowitego odcięcia węzła od sieci
2.3.6.3. w przypadku utraty serwera systemu zarządzania
2.4. Szczegółowy zakres testów musi zostać uzgodniony przed ich rozpoczęciem
2.5. Niezbędne jest dostarczenie dokumentacji wykonanych testów

XII. Serwis oraz wsparcie w zakresie zainstalowanych systemów

1. Wraz z dostawą systemów monitorowania oraz centralnego zarządzania alarmami powinno być zagwarantowane:
1.1. Wsparcie techniczne w języku polskim na okres minimum 3 lat, wsparcie powinno obejmować:
1.1.1. dostęp do najnowszych wersji oprogramowania
1.1.2. pobieranie sygnatur dla podatności
1.1.3. suwanie Awarii
1.1.4. Rozwiązywanie problemów konfiguracyjnych,

1.1.5. Proaktywne działania inżynierów on-site
1.1.6. Pośrednictwo w zgłaszaniu „case-ów" do producentów
1.1.7. dostęp do pomocy technicznej w dni robocze w godzinach 8:00- 16:00

2. Wraz z dostawą systemu MPLS-TP powinno być zagwarantowane:
   2.1. Objęcie wszystkich urządzeń i oprogramowania rękojmi na co najmniej 3 lata, w ramach rękojmi należy zapewnić:
      2.1.1. możliwość naprawy / wymiany urządzeń posiadających wady
      2.1.2. możliwość naprawy stwierdzonych nieprawidłowości w zakresie oprogramowania
      2.1.3. kontakt z Wykonawcą i dostęp do pomocy technicznej w dni robocze w godzinach 8:00 – 16:00
      2.1.4. dostęp do aktualizacji i najnowszych wersji oprogramowania
   2.2. Należy zapewnić możliwość ewentualnego przedłużenia gwarancji na kolejne lata
3. Warunki świadczenia wsparcia technicznego przez inżynierów Wykonawcy:
   a. Usuwanie awarii:
   • Obsługa awarii świadczona jest w reżimie 24h/7/365;
   • Jako awarię rozumie się zdarzenie, którego efektem jest niedostępność systemu lub świadczonej przez niego krytycznej usługi
   • Czas reakcji na zgłoszenie – 4 godziny;
   • Za czas reakcji rozumie się czas pomiędzy wpłynięciem zgłoszenia, a potwierdzeniem przyjęcia zgłoszenia i rozpoczęcia działań mających na celu usunięcie awarii.
   b. Rozwiązywanie zdalne problemów konfiguracyjnych
   • Jako problemy konfiguracyjne rozumie się zapytania dotyczące działania systemu w odniesieniu do konfiguracji systemów, działających w [NAZWA FIRMY] objętych niniejszą umową;
   • Wsparcie techniczne świadczone jest w godzinach roboczych;
   • Za godziny robocze przyjmuje się godziny 8-17 w dniach poniedziałek – piątek z wyłączeniem dni ustawowo wolnych od pracy.
   • Czas reakcji na zgłoszenie – 8 godzin roboczych
   • Za czas reakcji rozumie się czas pomiędzy wpłynięciem zgłoszenia, a potwierdzeniem przyjęcia zgłoszenia i rozpoczęcia działań mających na celu rozwiązanie problemu.
   c. Proaktywne działania inżynierów Wykonawcy w trakcie wizyt serwisowych (na życzenie klienta 1 dzień on-site dwa razy do roku) mające na celu optymalizację i rozwój systemów poprzez:
   • Tuning konfiguracji,
   • Sprawdzenie poprawności działania,
   • Aktualizację systemu
   • Optymalizacja działania systemu,
   • Rekomendacje zmian w architekturze i konfiguracji,
   • Powiadomienia o dostępności aktualizacji oprogramowania,
   • Informacja o nowych funkcjonalnościach rozwiązania
   • Odpowiedzi na pytania,
   d. Pośrednictwo w zgłaszaniu „case-ów" do producentów:
   • Pośredniczenie w zgłaszaniu case'ów (problemów technicznych) dla pracowników Zamawiającego przez inżynierów Wykonawcy;
   • Monitorowanie obsługi zgłoszonych do producenta case'ów
   • Raportowanie postępów w rozwiązywaniu case'ów do wskazanych pracowników Zamawiającego
   • Obsługa w j. polskim.

4. Sposób zgłaszania awarii oraz zapotrzebowania na wsparcie techniczne inżynierów wykonawcy:
   a. Zgłaszanie awarii:

5. Zawarcie umowy na wsparcie techniczne wymaga posiadania przez klienta aktywnego wsparcia technicznego producenta na wszystkie systemy objęte umową wsparcia technicznego przez cały okres jej trwania

XIII. Instruktaż

1. Wykonawca na własny koszt przeszkoli zespoły Zamawiającego z zakresu administracji i pracy z systemem IDS, administracji i pracy z systemem centralnego zarzadzania alarmami oraz administracji i pracy z urządzeniami i systemem MPLS-TP. Instruktaż musi być przeprowadzony w języku polskim w oparciu o materiały szkoleniowe w języku polskim (preferowany) lub angielskim. Koszty związane z przygotowaniem i przeprowadzeniem instruktaż pokrywa Wykonawca. Zamawiający pokrywa jedynie ewentualny koszt pracownika delegowanego na instruktaż. Zamawiający wymaga by przedstawiciele zespołu zamawiającego mogli aktywnie uczestniczyć w procesie wdrożenia systemu i tym samym budować kompetencje.
2. Wykonawca przeprowadzi dla personelu odpowiedzialnego za systemy przemysłowe instruktaż online budujący świadomość z zakresu bezpieczeństwa systemów OT/ICS.
3. W zakresie instruktażu MPLS-TP między innymi przekaże wiedzę dotyczącą:
   3.1. podstaw teoretycznych
   3.2. konfiguracji urządzeń i określania parametrów
   3.3. tworzenia, modyfikacji i usuwania tuneli MPLS i usług w sieci
   3.4. administracji systemem zarządzania siecią
   3.5. obsługi alarmów oraz sytuacji planowych i awaryjnych
   3.6. aktualizacji i tworzenia kopii zapasowych
4. W programie szkoleń przewidziane muszą być:
   4.1. sesje teoretyczne
   4.2. ćwiczenia praktycznie z czynnym udziałem przedstawicieli Zamawiającego
5. Zakres szkoleń powinien w sposób adekwatny przekładać się na czas trwania instruktażu.
6. instruktaż musi być realizowany przez przedstawicieli producenta rozwiązania lub osoby posiadające autoryzację i certyfikację producenta rozwiązania.

XIV. Rękojmia

1. Wszystkie licencje i system (urządzenia) maja mieć zagwarantowane wsparcie na 3 lata od dnia uruchomienia usługi systemów.
2. Wszystkie urządzenia muszą posiadać rękojmię na 5 lat liczoną od dnia uruchomienia systemów.

XV. DODATKOWE WYMAGANIA

Zamawiający ze względu na specyfikę przedmiotu zamówienia dot. cyberbezpieczeństwa elementów infrastruktury krytycznej wymaga, aby na etapie realizacji przedmiotu zamówienia **co najmniej jedna osoba odpowiedzialna za jego realizację** posiadała wymagane kompetencje potwierdzone podanymi niżej certyfkatami:

a) Certyfikat(ty) dot. opracowywania i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji **uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert, tj. co najmniej jeden z podanych certyfikatów,** o których mowa w *Rozporządzeniu Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa*, tj.: **CGEIT, CIA, CISA, CISM, CISSP, CRISC, SSCP, CBCI, CBCP.**

b) Certyfikat(ty) dot. projektowanie, budowy i utrzymania systemów monitorowania i detekcji incydentów oraz wsparcia funkcjonowania operacyjnego centrum bezpieczeństwa (SOC)/Zespołu Reagowania na Incydenty Bezpieczeństwa, **tj. co najmniej jeden z podanych certyfikatów,** o których mowa w *Rozporządzeniu Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa*, tj.: **BTL1, BTL2, CAP, CASP+, CAWFE, CEH, CEH Master, CISM, CCFE, CDRP, CFSR, CISM, CCFE, CDRP, CFSR, CISSP, CHFI, COBIT, Foundation, CPENT, CSSLP, CNFE, CySA+,**

eCDFP, eCMAP, GCCC, GCDA, GCFA, GCFE, GCIH, GCSA, GISP, GMON, GNFA, GASF, GSE, GSLC, GSOC, GSOM, GWEB, OSCP, OSEE, OSEP, PenTest+, Security+, SSCP.

c) Certyfikat(ty) **dot. wdrożenia, konfigurowania, obsługi** oferowanego rozwiązania MPLS-TP **wydawany przez producenta rozwiązania MPLS-TP lub przez niego akredytowany.**

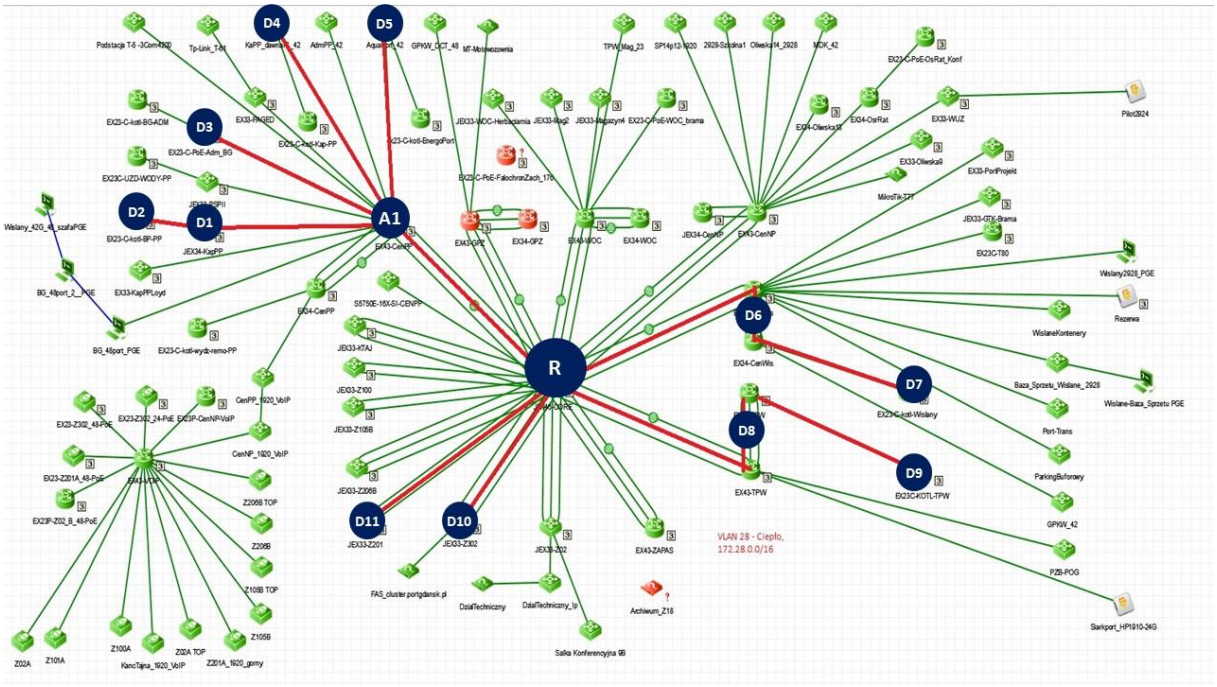
Zamawiający dopuszcza spełnienie ww. wymagań przez zespół osób, które łącznie będą spełniać wymagania określone powyżej w pkt a)-c).

Załącznik nr 1 do OPZ

1. Lista protokołów objętych DPI
   1.1. DNP3.0 protokół działa na wielu niestandardowych portach DPI ma być realizowany dla każdego z nich.
   1.2. Modbus.
   1.3. Siemens S7.
2. Lista monitorowanych VLAN:
   2.1. VLAN 27 (Energetyka), 28 (Ciepło), 1050 (Media), 1055 (Mgmt Media), 1060 (Media Ciepło) – instancja podstawowa systemu IDS.
   2.2. Sieć proBOX – osobna instancja systemu IDS.
3. Istniejące FW obiektowe
   3.1. Fortigate.
4. Parametry Serwera
   4.1. CPU 32 core 64 wątki
   4.2. 128GB 4x1.92GB SSD + 2x8TB
   4.3. 2x10GB SFP+ wkładki MM + 4x1GB RJ45
   4.4. 2x900W
   4.5. iRMC

Załącznik nr 2 schemat podglądowy

Sieć MPLS-TP – zamówienie podstawowe:



Sieć MPLS-TP – prawo opcji: