Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

1. Wprowadzenie

Ogólnopolska Sieć Edukacyjna ma na celu zapewnienie dostępu do szybkiego, bezpiecznego Internetu dla szkół. OSE jest publiczną siecią telekomunikacyjną, opartą o istniejącą infrastrukturę szerokopasmową wybudowaną w ramach inwestycji komercyjnych oraz dofinansowanych ze środków publicznych w ramach Programu Operacyjnego Polska Cyfrowa. Za uruchomienie i utrzymanie Sieci, oraz w szczególności za dostarczenie szkołom usługi dostępu do Internetu o symetrycznej przepustowości co najmniej 100 Mb/s wraz z kompleksowymi usługami bezpieczeństwa sieciowego, w tym ochrony przed zagrożeniami dla prawidłowego rozwoju uczniów, odpowiedzialny jest Operator OSE.

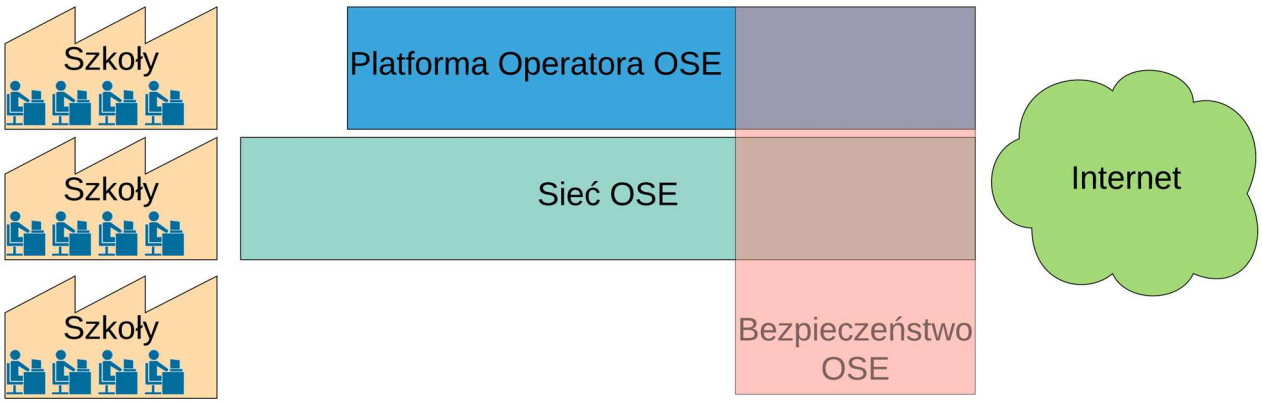
Operatorem OSE został NASK - Państwowy Instytut Badawczy (zwany dalej" „NASK"), nadzorowany przez Ministra Cyfryzacji.

W Polsce istnieje 25 015 szkół zlokalizowanych w 19 500 lokalizacjach. Podstawowym zadaniem OSE ma być zapewnienie szkołom w Polsce możliwości dostępu do bezpiecznego Internetu i zasobów edukacyjnych wraz z szeregiem usług powiązanych, w tym:
1) Zapewnienie usług dostępu do sieci Internet o przepływności minimum 100 Mb/s symetrycznie,
2) Zapewnienie usług bezpieczeństwa umożliwiających ochronę użytkowników,
3) Zapewnienie dostawcom treści edukacyjnych dostępu do użytkowników sieci OSE.
4) Umożliwienia wspomagania procesu kształcenia w szkole.

W ramach budowy OSE planuje się uruchomienie sieci rozległej transmisji danych, systemów bezpieczeństwa wraz z systemami wsparcia obejmującymi m.in. systemy zarządzania tożsamością, OSS, BSS, SIEM jak również urządzenia abonenckie (CPE), przełączniki, AP sieci bezprzewodowej. Usługi obejmować będą swoim zasięgiem terytorium Polski. Sieć OSE, zbudowana będzie z węzłów zlokalizowanych na terenie 16 województw.

1.1. Koncepcja OSE

NASK, jako operator OSE zapewniający dostęp do internetu dla szkół realizuje swoje działania w oparciu o trzy podstawowe obszary:



1. Sieć OSE - Infrastruktura telekomunikacyjna wykorzystywana do świadczenia przez Operatora OSE usług dostarczanych klientom (takich jak m.in dostęp do internetu). Dostęp szkolny do internetu jest realizowany w czterech podstawowych wariantach:

a. OSE - operator dostępowy odpowiada jedynie za łącze do szkoły, instalację i konfigurację punktu dostępowego realizuje operator OSE i on dostarcza wszystkie urządzenia,

b. POPC - instalacja punktu dostępowego w szkole i dostarczenie łącza dostępowego ze szkoły do sieci szkieletowej jest w odpowiedzialności beneficjenta POPC, operator OSE odpowiada jedynie za konfigurację punktu dostępowego i ewentualną rozbudowę o dodatkowe urządzenia (np. switche)

c. MAN - punkt dostępowy i sieć dostępowa jest w odpowiedzialności OPS/szkoły, w odpowiedzialności operatora OSE może znaleźć się agregacja pomiędzy łączami dostępowymi a siecią szkieletową, operator OSE odpowiada za usługę, ale MAN realizuje wszelkie prace związane z konfiguracją punktu dostępowego w szkole.

d. ODN - punkt dostępowy jest w odpowiedzialności OPS / szkoły, część łącza jest w odpowiedzialności ODN, a część w odpowiedzialności OSE, przebieg łącza jest wydłużony o dodatkowy węzeł - Powiatowy Punkt Wymiany Ruchu

2. Platforma Operatora OSE - platforma złożona z komponentów informatycznych, których celem jest wsparcie wszelkiej działalności NASK, jako Operatora OSE (w tym m.in. zarządzanie infrastrukturą sieciową, działania sprzedażowe czy rozliczanie wydatków) składające się z dwóch typów komponentów:

   a. Systemy OSE - systemy informatyczne tworzone lub rozwijane na potrzeby operatora OSE

   b. Systemy NASK - systemy informatyczne wykorzystywane w ramach podstawowej działalności NASK PIB, które zostaną zintegrowane z rozwiązaniem na potrzeby OSE

3. Bezpieczeństwo OSE - komponenty warstwy sieciowej, sprzęt oraz oprogramowanie, których celem jest zapewnienie bezpieczeństwa teleinformatycznego sieci OSE oraz jej użytkownikom.

2. Definicje

Definicja	Wyjaśnienie
ADC (Application Delivery Controller)	system realizujący równomierne rozłożenie obciążenia na Urządzenia należące do Systemów ADC, NG Firewall, inspekcji ruchu SSL/TLS
Administratorzy OSE	komórka organizacyjna odpowiadająca za utrzymanie sieci OSE
Beneficjent POPC	przedsiębiorca telekomunikacyjny będący beneficjentem działania POPC 1.1, budujący łącza światłowodowe do jednostek oświatowych
Centralny Węzeł Bezpieczeństwa	węzeł Bezpieczeństwa zlokalizowany w Węźle Centralnym dostarczający mechanizmy ochrony Zasobów obliczeniowych OSE
Lokalizacja węzła / Kolokacja	miejsce fizyczne, powierzchnia kolokacyjna, w którym pracuje Węzeł sieci / Węzeł Bezpieczeństwa.
Węzeł agregacyjny	węzeł do którego dołączone są łącza dostępowe do szkół, węzeł ten nie ma bezpośredniego połączenia do sieci Internet
Węzeł bezpieczeństwa	zestaw Urządzeń wraz z Oprogramowaniem, realizujących funkcje bezpieczeństwa (m.in. dekrypcja SSL, funkcjonalność IPS, NG Firewall itd.). Zamawiający wyróżnia dwa typy Regionalny Węzeł Bezpieczeństwa oraz Centralny Węzeł Bezpieczeństwa
Węzeł szkieletowy	węzeł zapewniający przeniesienie ruchu z węzłów agregacyjnych do sieci Internet, a także inżynierię ruchu, na styku sieci OSE z Internetem
Węzeł sieci	zespół urządzeń pracujących w jednej lokalizacji, zapewniających komunikację użytkownikom sieci (Szkołom) z siecią Internet. Węzeł wraz z innymi węzłami, z którymi jest połączony za pośrednictwem łączy szkieletowych, stanowi sieć OSE. Częścią węzła są Regionalne i Centralne Węzły Bezpieczeństwa.
Partner serwisowy	podmiot realizujący usługi techniczne w jednostkach oświatowych w zakresie podłączania szkół do OSE oraz serwisowania na terenie szkoły świadczonych przez OSE usług
Dostawca łącza dostępowego	przedsiębiorca telekomunikacyjny budujący łącza światłowodowe do jednostek oświatowych, także Beneficjent POPC, dzierżawiący je na rzecz operatora OSE
Operator Agregujący	przedsiębiorca telekomunikacyjny, zbierający od Dostawców łączy dostępowych łącza do jednostek oświatowych, agregujący je w warstwie Ethernet oraz oddający operatorowi OSE w Węźle Agregacyjnym
Operator Sieci Regionalnej	operator sieci dostępowych zapewniający obsługę informatyczną dla jednostek edukacyjnych. Szkoły zgłaszają wszelkie problemy do OSR, który ewentualnie przekazuje je do OSE. OSR to sieci miejskie (MAN) i sieć Ośrodku Doskonalenia Nauczycieli (ODN).
Dostawca sieci szkieletowej	przedsiębiorca telekomunikacyjny, udostępniający swoją infrastrukturę na potrzeby budowy szkieletu OSE, czyli łączy pomiędzy węzłami OSE
Dostawca kolokacji	podmiot świadczący na rzecz Zamawiającego usługi kolokacji w centrum przetwarzania danych, w którym zlokalizowany jest Węzeł centralny i/lub Węzeł agregacyjny sieci OSE

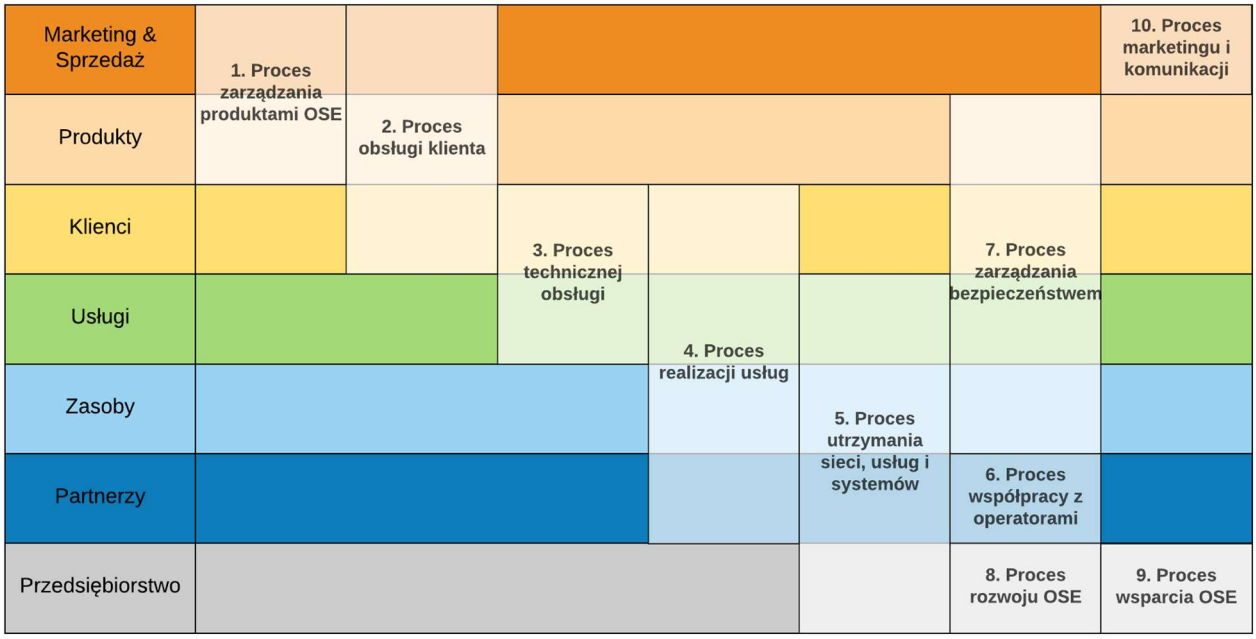
Definicja	Wyjaśnienie
Jednostka oświatowa	placówka edukacyjna należąca do systemu oświaty w Polsce, w szczególności szkoła podstawowa, gimnazjum, szkoły ponadgimnazjalne, policealne, artystyczne, inne szkoły specjalne i placówki oświatowo-wychowawcze oraz opiekuńcze z wyłączeniem szkół dla dorosłych
Operator OSE	przedsiębiorca telekomunikacyjny świadczący usługi dostępu do Internetu za pośrednictwem OSE na rzecz Jednostek edukacyjnych, Operator OSE odpowiada za podłączanie Jednostek Oświatowych, a następnie obsługuje je na bazie wewnętrznych i zewnętrznych struktur organizacyjnych, zawierających między innymi Centrum Kontaktu, Centrum Zarządzania Siecią oraz Centrum Zarządzania Bezpieczeństwem;
Centralny Węzeł Bezpieczeństwa	węzeł Bezpieczeństwa zlokalizowany w Węźle Centralnym, zapewniający ochronę Zasobów obliczeniowych OSE
IdP (Identity Provider)	system służący do tworzenia, utrzymywania i udostępniania tożsamości dla celów uwierzytelniania i autoryzacji dla zewnętrznych podmiotów.
LDAP (Lightweight Directory Access Protocol)	protokół przeznaczony do korzystania z usług katalogowych. Jest to również nazwa własna usługi katalogowej przechowującej informacje o użytkownikach i ich atrybutach.
System NG Firewall(NGFW – Next Generation Firewall)	system kontrolujący dostęp do sieci w oparciu o polityki, klasyfikujące ruch bazujący na informacjach pozyskanych z protokołów działających w 4 i 7 warstwie OSI, z wykorzystaniem mechanizmów statefull packet inspection, intrusion prevetion system, application control, antivirus.
Portal OSE	portal umożliwiający obsługę usług w sieci OSE, w tym zgłaszanie problemów technicznych, zmian w zakresie świadczonych usług, kreowanie i modyfikowanie kont Użytkowników Sieci OSE oraz ich parametrów
Regionalny Węzeł Bezpieczeństwa	węzeł Bezpieczeństwa zlokalizowany w Węźle Regionalnym i obsługujący Szkoły podłączone do danego Węzła Regionalnego.
SAML (Język Security Assertion Markup Language)	protokół służący do wymiany danych uwierzytelniania i autoryzacji w domenach zabezpieczeń. W modelu domeny SAML dostawca tożsamości jest specjalnym typem urzędu uwierzytelniania. Dostawca tożsamości SAML jest jednostką systemową, która wydaje zapewnienie uwierzytelniania w połączeniu z profilem SSO SAML. Strona ufająca, która zużywa te zapewnienie uwierzytelniania, jest nazywana dostawcą usług SAML.
Ustawa OSE	ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej
Użytkownicy Sieci OSE	użytkownicy usług Sieci OSE w tym m.in.: uczniowie, nauczyciele, pracownicy administracyjni oraz inni upoważnieni przez administratora danych usług Sieci OSE
Zasoby obliczeniowe OSE	infrastruktura serwerowa udostępniona w celu zapewnienia mocy obliczeniowej t.j. procesory, pamięć RAM, przestrzeń dyskowa wybudowana na potrzeby systemów i usług OSE. Zasoby są umieszczone w dwóch węzłach centralnych OSE w lokalizacjach: Warszawa i Poznań.
PWR (Punkt Wymiany Ruchu)	Punkt Wymiany Ruchu internetowego (IX - z ang. Internet eXchange Point) to miejsce, gdzie operatorzy, przedsiębiorcy telekomunikacyjni (w rozumieniu Ustawy Prawo

Definicja	Wyjaśnienie
	Telekomunikacyjne) i dostawcy treści i usług internetowych wymieniają się ruchem IP pomiędzy swoimi sieciami.
PPWR (Powiatowy Punkt Wymiany Ruchu)	Regionalny PWR pośredniczący w ruchu pomiędzy węzłem abonenckim a PWR-em w sieciach ODN.
MAN	Sieć miejska - operatorzy sieci regionalnych w rejonach miejskich
ODN	Ośrodek Doskonalenia Nauczycieli - jeden z Operatorów Sieci Regionalnych obsługujących szkoły.
Radius	Remote Authentication Dial In User Service – usługa zdalnego uwierzytelniania użytkowników, używana głównie z systemami telekomunikacyjnymi. Zdefiniowana w następujących RFC: RFC 2865, RFC 2866, RFC 3579
SNMP	Rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami sieciowymi i serwerami za pośrednictwem sieci IP . Do transmisji wiadomości SNMP wykorzystywany jest głównie protokół UDP: standardowo port 161 wykorzystywany jest do wysyłania i odbierania żądań, natomiast port 162 wykorzystywany jest do przechwytywania sygnałów *trap* od urządzeń. Protokół znany jest i wykorzystywany w następujących wersjach SNMPv1 – pierwsza wersja, która została opublikowana w 1988 roku w dokumencie RFC 1067 (z późniejszymi zmianami w RFC 1098 oraz RFC 1157). W tej wersji protokołu bezpieczeństwo oparte jest na tak zwanych *communities*, które są pewnego rodzaju nieszyfrowanymi hasłami umożliwiającymi zarządzanie urządzeniem. SNMPv2 – eksperymentalna wersja protokołu, określana także SNMPv2c, opisana w dokumencie RFC 1901. SNMPv3 – obsługująca uwierzytelnianie oraz szyfrowaną komunikację wykorzystującą szyfrowanie SHA i MD5.
SSH	Standard protokołów szyfrowania komunikacji typu klient-serwer , a także serwer-klient Protokoły z rodziny SSH korzystają zwykle z portu 22 protokołu TCP. Protokół SSH jest zaimplementowany na warstwie aplikacji modelu OSI w ramach połączenia TCP. Protokół SSH jest opisany szczegółowo w RFC 4251 i 4254.
SYSLOG	Program, który umożliwia rejestrowanie zachodzących zdarzeń przy pomocy scentralizowanego mechanizmu logowania. Działa on na porcie 514 udp / tcp. Cały mechanizm jest opisany w następujących RFC 5424 i 3164
VRF	Technologia pozwalająca koegzystować wielu instancjom tablic routingu na tym samym routerze w tym samym czasie. Głównym aspektem tej funkcjonalności jest separacja wirtualnych tablic routingu wobec siebie bez potrzeby zastosowania wielu ruterów.
VPN	Tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi, za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Można opcjonalnie kompresować

Definicja	Wyjaśnienie
	lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa. Określenie "wirtualna" oznacza, że sieć ta istnieje jedynie, jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak, jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne. Rozwiązania oparte na VPN stosowane są np. w sieciach korporacyjnych firm, których zdalni użytkownicy pracują ze swoich domów na niezabezpieczonych łączach. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie).
SMTP	Protokół internetowy wykorzystywany do przekazywania poczty elektronicznej w Internecie. Standard został zdefiniowany w dokumencie RFC 821, a następnie zaktualizowany w 2008 roku w dokumencie RFC 5321.
SIP	SIP współgra z kilkoma innymi protokołami i jest zaangażowany jedynie w część sygnalizacyjną sesji komunikacyjnej. SIP występuje jako nośnik Session Description Protocol (SDP), który opisuje transportowane multimedia w sieci, np. używane porty IP, używany kodek itp. Pierwsza zaproponowana wersja standardu (SIP 2.0) została zdefiniowana w RFC 2543. Protokół następnie uszczegółowiono w RFC 3261 , jakkolwiek wiele implementacji używa wskazówek z tymczasowych wersji próbnych (ang. *draft*).
SIEM	system tożsamy z funkcjami Log Management (LM) odpowiedzialny za logowanie zdarzeń z urządzeń sieciowych, systemów operacyjnych oraz aplikacji. System LM posiada funkcjonalności takie jak: zbieranie logów, agregację logów oraz przeszukiwanie, raportowanie i tworzenie reguł korelacyjnych
System Retencji	system odpowiedzialny za zbieranie logów i zdarzeń z urządzeń sieciowych, posiada funkcjonalności takie jak: zbieranie logów, agregację logów, retencję logów oraz przeszukiwanie i raportowanie.
SWG **(Security Web Gateway)**	System zapewniający funkcje ochrony użytkownika sieci OSE związane z potencjalnym dostępem do treści nielegalnych i szkodliwych w Internecie.
VLAN	Wirtualna sieć lokalna (VLAN = *virtual local area network*) to sieć wydzielona logicznie (w warstwie łącza danych - w modelu OSI warstwa 2) w ramach innej, większej sieci fizycznej.

3. Architektura biznesowa Operatora OSE

NASK Państwowy Instytut Badawczy funkcjonując, jako Operator Ogólnopolskiej Sieci Edukacyjnej realizuje te same działania jak każdy inny operator telekomunikacyjny, jednakże w sposób dopasowany do specyfiki OSE. Celem działania operatora jest świadczenie usług dostarczanych na bazie sieci teleinformatycznej. W związku ze świadczeniem usług operator musi realizować wiele funkcjonalności powiązanych z całym cyklem życia produktu od tworzenia jego koncepcji poprzez wdrażanie i dostarczanie klientom, aż po jego wycofanie. Kluczowym elementem działania każdego operatora jest jego katalog produktów określający wartości (produkty), jakie oferuje swoim klientom, sposób ich oferowania i dostarczania, sposób ich realizacji (czy na bazie własnych zasobów, czy też partnerów), sposób rozliczeń się z klientami. Dodatkowo należy pamiętać, że operator telekomunikacyjny jest przedsiębiorcą i w związku z tym realizuje wszelkie działania związane z prowadzeniem przedsiębiorstwa, takie jak finanse, księgowość, gospodarka magazynowa, zarządzanie IT itp. Całość funkcjonowania Operatora OSE oraz jego podział na poszczególne obszary biznesowe można opisać wykorzystując mapę procesów przedsiębiorstwa telekomunikacyjnego zdefiniowanego przez TMForum w ramach eTOM. Poniżej znajduje się diagram mapy biznesowej dla Operatora OSE.

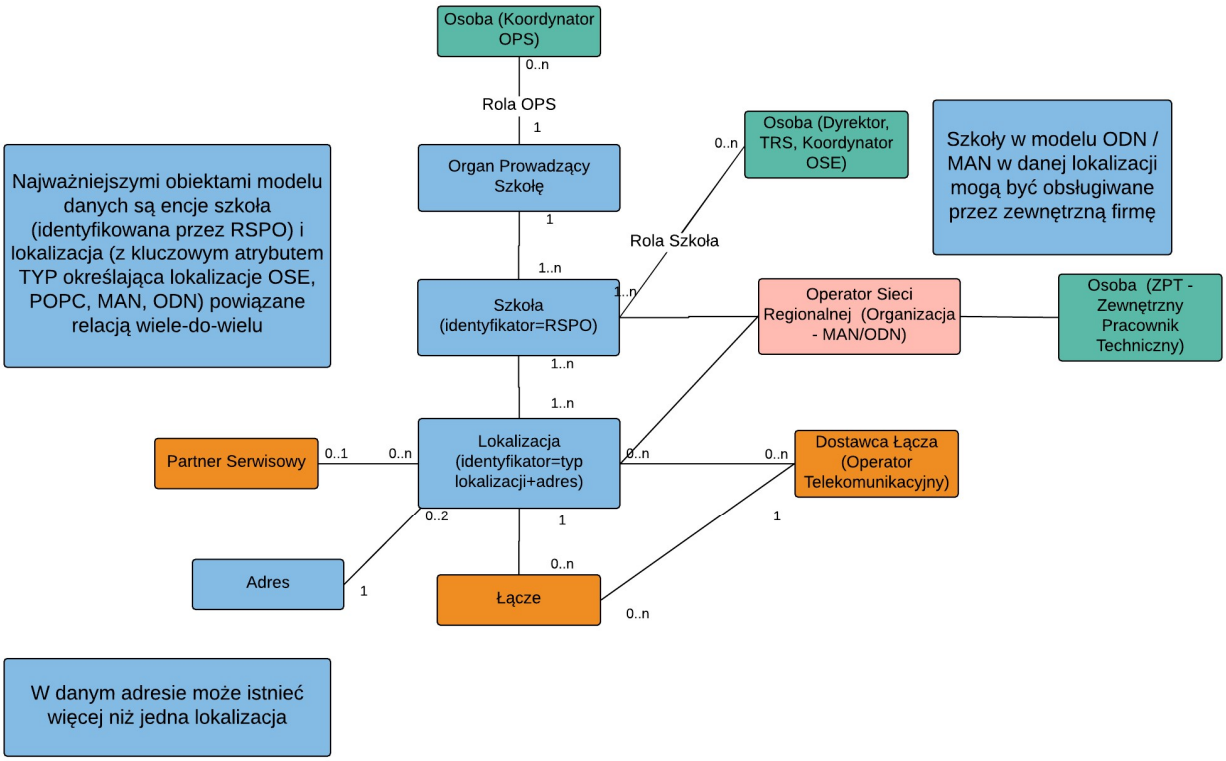


Konfiguracja biznesowa

W ramach opisu architektury biznesowej znajdują się informacje dotyczące konfiguracji (i modeli danych) wykorzystywanej w procesach biznesowych, takich jak np. konfiguracja katalogu produktów, SLA zgłoszeń, procesów obsługowych czy reklamacyjnych. Należy założyć, iż podane w dokumencie konfiguracje są przykładowe i ich celem jest jedynie przekazanie zakresu wymaganych danych, struktury biznesowego modelu danych oraz skali i złożoności zagadnienia.

3.1. Architektura danych operatora OSE

W ramach kompleksowej realizacji zadań / procesów związanych z zapewnieniem bezpiecznego dostępu do internetu konieczne jest operowanie na dużej ilości różnorodnych danych. Poniżej znajduje się diagram ogólnego modelu danych w obszarze BSS.



Procesy realizowane w obszarze BSS koncentrują się wokół dwóch podstawowych obiektów:

- Szkoły - placówki edukacyjnej, będącej klientem Operatora OSE
- Lokalizacji - czyli miejsca świadczenia usług

Pomiędzy szkołą a lokalizacją zachodzi relacja wiele-do-wielu - wiele szkół może być w jednej lokalizacji, ale również jedna szkoła może występować w wielu lokalizacjach.

Osoby

Za zapewnienie dostępu do internetu dla szkoły odpowiedzialny jest Organ Prowadzący Szkołę, osobą go reprezentującą w procesach biznesowych jest Koordynator OPS.

Szkolę w kontaktach z OSE reprezentuje Dyrektor i jest on użytkownikiem odpowiedzialnym za administrację pozostałymi użytkownikami OSE w szkole. W procesach biznesowych występują w roli użytkowników jeszcze Techniczny Reprezentant Szkoły (TRS) oraz Koordynator OSE. Dyrektor jest odpowiedzialny za zarządzanie bazą użytkowników dla swojej szkoły. Należy zwrócić uwagę, że poszczególne osoby mogą być użytkownikami w wielu szkołach. Np. dana osoba może być TRS-em w więcej niż jednej szkole.

Szkoła

Wszystkie główne procesy operatora OSE realizowane są w kontekście szkoły. Zanim możliwe będzie pozyskanie szkoły musi zostać wstępnie przygotowana infrastruktura telekomunikacyjna, dopiero szkoła w ramach harmonogramu może uzyskać możliwość zgłoszenia się do OSE.

Po zgłoszeniu szkoły do OSE Dyrektor jest odpowiedzialny za zarządzanie użytkownikami, tworzenie odpowiednich kont dla użytkowników, którzy będą mieli uprawnienia do zarządzania usługami OSE i zgłaszaniem ewentualnych problemów. Szkoła jest nadzorowana przez Organ Prowadzący Szkołę w ramach, którego jest wyznaczona osoba w roli Koordynatora OPS.

W przypadku szkół w lokalizacjach obsługiwanych przez Operatora Sieci Regionalnej (MAN / ODN) użytkownicy szkolni nie mogą zgłaszać problemów technicznych bezpośrednio do operatora OSE, problemy muszą być zgłaszane do Operatorów Sieci Regionalnych i dopiero ich pracownicy po weryfikacji mogą zgłaszać ewentualne problemy do Operatora OSE.

Lokalizacja

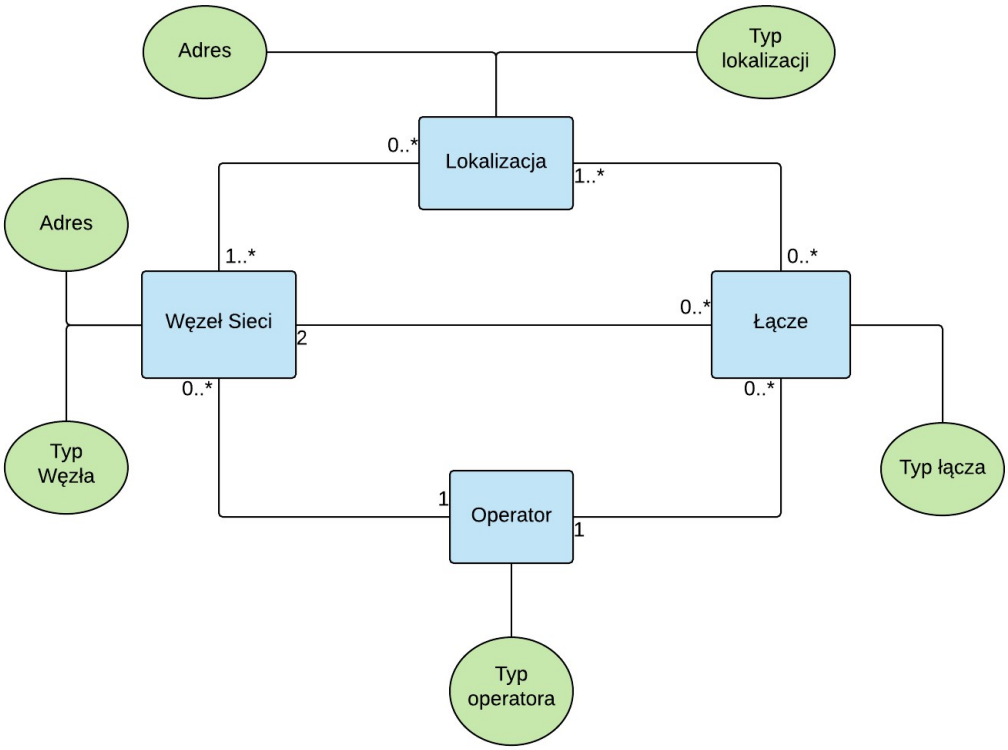
Główną encja danych, wokół której koncentrują się działania związane z usługami OSE jest lokalizacja, grupująca wszystkie szkoły znajdujące się pod jednym adresem i podłączane w tym samym modelu świadczenia usług (OSE / POPC / MAN / ODN).

Dla każdej lokalizacji jest określony Partner Serwisowy odpowiedzialny za realizację prac w szkołach. W przypadku szkół ODN / MAN jego rolę może pełnić NASK lub Operator Sieci Regionalnej (OSR).

Dla każdej lokalizacji jest z góry określony przebieg łącza sieci dostępowej, czyli wskazani operatorzy odpowiedzialny za łączą pomiędzy poszczególnymi punktami wraz ze wskazaniem odpowiedzialnego za łącze (OSE / OSR).

Łącza dostępowe

Kolejnym istotnym elementem modelu danych jest obszar łączy dostępowych, czyli infrastruktury sieciowej służącej do połączenia węzła abonenckiego w szkole z węzłem agregacyjnym sieci szkieletowej.



W przeciwieństwie do tradycyjnego modelu operatora telekomunikacyjnego gdzie przebieg jest wyznaczany w momencie podłączenia (lub wywiadu technicznego), w przypadku OSE zanim szkoła będzie miała możliwość zgłoszenia się do OSE przebieg łącz dla lokalizacji zostaje wcześniej ustalony, czyli z góry wiadomo, jaki operator dostarczy, jakie łącza, które będą przechodzić przez jasno określone węzły sieci.

3.2. Katalog produktów Ogólnopolskiej Sieci Edukacyjnej

Produkty OSE

Nazwa	Opis produktu	Model rozliczeniowy	Ograniczenia techniczne	Ograniczenia biznesowe	Produkty składowe	Produkty Wymagane	Instalacja Aktywacja
Produkty główne							
Internet OSE	Dostęp do Internetu poprzez sieć szkieletową OSE o prędkości synchronicznej 100Mb/s na bazie komercyjnie istniejących łączy operatorów	Abonament, instalacja, cena rozdzielna dla regionów	Dostępność łącza w lokalizacji Dostępność partnera serwisowego w lokalizacji	Minimalny czas pomiędzy rezygnacją a ponownym podłączeniem (konfiguracja)	Urządzenie CPE (tylko dla jednej szkoły w lokalizacji), Urządzenie AP, Urządzenie SW		Instalacja łącza (operator) Instalacja punktu dostępowego (partner serwisowy) Instalacja VLAN
Internet OSE POPC	Dostęp do Internetu poprzez sieć szkieletową OSE o prędkości synchronicznej 100Mb/s na bazie łączy budowanych w ramach POPC				Urządzenie AP, Urządzenie SW		Instalacja łącza (operator) Instalacja punktu dostępowego (operator) Rozbudowa punktu dostępowego (partner serwisowy) Instalacja VLAN
Internet OSE MAN	Dostęp do Internetu poprzez sieć szkieletową OSE o prędkości synchronicznej 100Mb/s na dostępu zapewnianego przez OPS przy wykorzystaniu sieci miejskich (MAN)		Dostępność łącza w lokalizacji		Urządzenie CPE (opcjonalnie dla jednej szkoły w lokalizacji)		Instalacja punktu dostępowego (szkoła) (opcja) Instalacja VLAN (opcja)
Internet OSE ODN	Dostęp do Internetu poprzez sieć szkieletową OSE o prędkości synchronicznej 100Mb/s na bazie łączy znajdujących się w ODN przy wykorzystaniu też łączy komercyjnych operatorów		Dostępność łącza w lokalizacji, dostępność ODN w lokalizacji Dostępność partnera serwisowego w lokalizacji				Instalacja punktu dostępowego (szkoła) (opcja) Instalacja VLAN (opcja)

Nazwa	Opis produktu	Model rozliczeniowy	Ograniczenia techniczne	Ograniczenia biznesowe	Produkty składowe	Produkty Wymagane	Instalacja Aktywacja
Podwyższona Prędkość	Zwiększenie prędkości internetu powyżej 100Mb/s w paczkach po 50Mb/s (n paczek). Produkt płatny na podstawie wyceny od dostawcy łącza.	Abonament, instalacja, cena rozdzielna dla regionów	Do maksymalnej przepustowości łącza	Maksymalnie liczba miesięcznych aktywacji		Internet OSE lub Internet OSE POPC lub Internet OSE MAN lub Internet OSE ODN	Dostosowanie przepustowości łącza
Ochrona przed szkodliwym oprogramowaniem	Zaawansowana ochrona sieci szkolnej przed włamaniami i złośliwym oprogramowaniem. **Uwaga: Produkt wymaga zgody na inspekcję ruchu szyfrowanego SSL.**	Abonament, instalacja		Maksymalnie liczba miesięcznych aktywacji	System zapobiegania włamań (IPS), Antywirus (AV), Certyfikat SSL	[Internet OSE lub Internet OSE POPC lub Internet OSE MAN lub Internet OSE ODN] i CPE OSE	Instalacja certyfikatu SSL Instalacja oprogramowania IPS Instalacja oprogramowania AV
Ochrona użytkownika OSE	Zaawansowana ochrona użytkowników szkolnych na kilku poziomach bezpieczeństwa poprzez filtrowanie treści. **Uwaga: Produkt wymaga zgody na inspekcję ruchu szyfrowanego SSL**	Abonament, instalacja		Maksymalnie liczba miesięcznych aktywacji	Certyfikat SSL	[Internet OSE lub Internet OSE POPC lub Internet OSE MAN lub Internet OSE ODN] I Ochrona przed szkodliwym oprogramowaniem	Ustawienie poziomu filtracji
Wsparcie Techniczne Szkoły	Wsparcie techniczne dla szkoły w rozwiązywaniu problemów IT niepowiązanych z OSE. Produkt o ograniczonej dostępności – indywidualnie negocjowany.	Użycie		Maksymalna liczba użyć miesięcznie / rocznie (konfiguracja)		Internet OSE lub Internet OSE POPC	Wizyta partnera serwisowego we wskazanym terminie
Rekonfiguracja Sieci Szkolnej	Dostosowanie istniejącej sieci szkolnej do dostępu do internetu w ramach OSE	Użycie		Dostępna opcjonalnie dla instalacji w lokalizacjach OSE i POPC. Niedostępne w		Internet OSE lub Internet OSE POPC	Wizyta partnera serwisowego we wskazanym terminie

Nazwa	Opis produktu	Model rozliczeniowy	Ograniczenia techniczne	Ograniczenia biznesowe	Produkty składowe	Produkty Wymagane	Instalacja Aktywacja
				lokalizacjach MAN			
Monitorowanie zachowań	Monitorowanie zachowań i wykrywanie potencjalnych zagrożeń wynikających z zachowań odbiegających od prawidłowego profilu a także w wyniku porównania zachować z profilem potencjalnych zagrożeń	Abonament		Maksymalnie liczba miesięcznych aktywacji			Instalacja certyfikatu SSL
Bezpieczeństwo użytkownika mobilnego	Aplikacja oferująca funkcjonalność filtrowania treści na urządzeniu końcowym ucznia.	Abonament	Dostępność aplikacji na platformie mobilnej klienta	Maksymalnie liczba miesięcznych aktywacji	Certyfikat SSL	Internet OSE lub Internet OSE POPC lub Internet OSE MAN	Instalacja certyfikatu SSL Pobranie i instalacja oprogramowania Aktywacja konta
Produkty składowe							
Urządzenie CPE	Zakończenie sieci telekomunikacyjnej znajdujące się u klienta.						
Urządzenie AP	Urządzenie dostępowe (wyposażone w moduł WIFI)						
Urządzenie SW	Przełącznik sieciowy						
Rekonfiguracja Sieci Szkolnej	Dostosowanie istniejącej sieci szkolnej do dostępu do internetu w ramach OSE						
System zapobiegania włamaniom (IPS)	System zapobiegający włamaniom do sieci komputerowej						

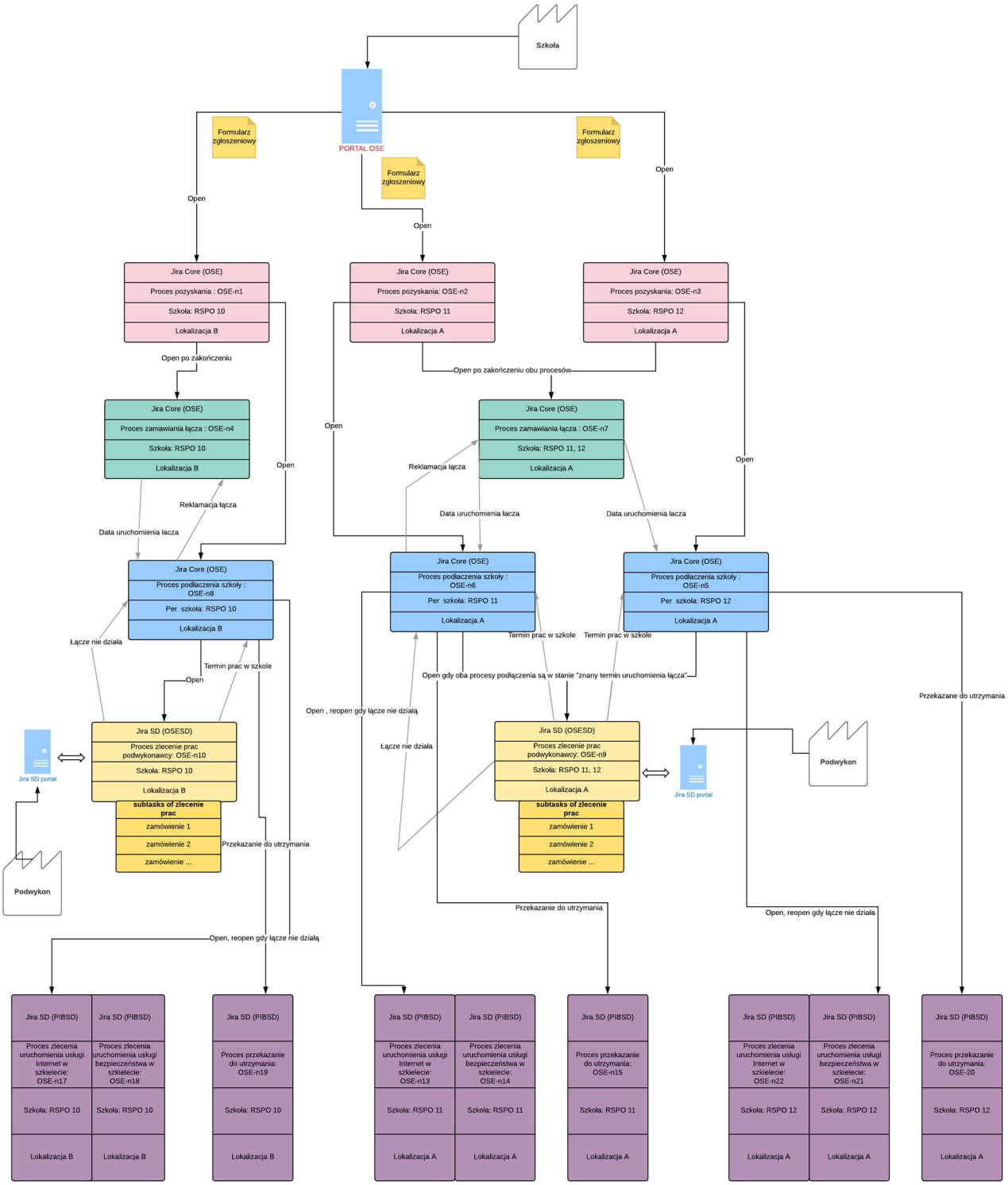
Nazwa	Opis produktu	Model rozliczeniowy	Ograniczenia techniczne	Ograniczenia biznesowe	Produkty składowe	Produkty Wymagane	Instalacja Aktywacja
Antywirus (AV)	Ochrona przed złośliwym oprogramowaniem						
Certyfikat SSL	Certyfikat SSL						

Oferty w ramach Ogólnopolskiej Sieci Edukacyjnej

W poszczególnych kanałach dostępowych powinny się pokazywać jedynie oferty dostępne dla wybranego klienta (zawierające produkty dostępne w związku z konkretną lokalizacją klienta), co oznacza konieczność wcześniejszej identyfikacji klienta. Głównym czynnikiem determinującym dostępność ofert jest lokalizacja, na podstawie, której wiadomo, jaki operator będzie świadczyć dostęp do internetu oraz w jakim modelu OSE/ POPC / MAN./ ODN (Dla części lokalizacji może nie być dostępnego żadnego operatora, ale powinna być znana data dostępności produktów).

3.3. Główne procesy operatora OSE

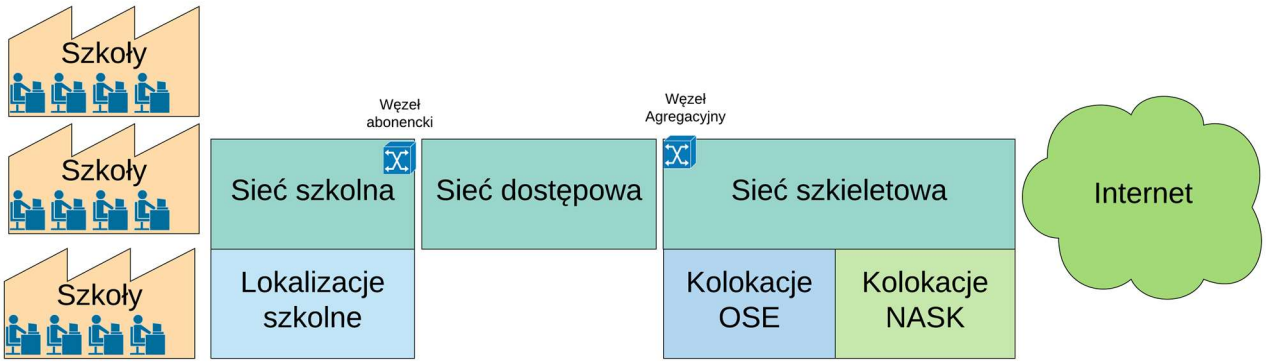
Jednym z głównych zadań, jakie są postawione przed operatorem OSE jest realizacja podłączeń a następnie obsługa poszczególnych szkół skupionych w lokalizacjach. Całość procesów związanych z podłączeniem szkoły (oraz modyfikacją usługi dostępu) jest zdekomponowana na procesy, które są realizowane wokół różnych encji: szkół, lokalizacji, partnerów serwisowych. Powoduje to konieczność zapewnienia odpowiedniej orkiestracji przebiegu zamówień. Poniżej została zaprezentowana poglądowa mapa przebiegu procesów i ich wzajemnej synchronizacji.


Szkoła
PORTAL OSE
Formularz zgłoszeniowy
Formularz zgłoszeniowy
Formularz zgłoszeniowy
Open
Open
Open
Open
Jira Core (OSE)
Proces pozyskania : OSE-n1
Szkoła: RSPO 10
Lokalizacja B
Jira Core (OSE)
Proces pozyskania: OSE-n2
Szkoła: RSPO 11
Lokalizacja A
Jira Core (OSE)
Proces pozyskania: OSE-n3
Szkoła: RSPO 12
Lokalizacja A
Open po zakończeniu
Open po zakończeniu obu procesów
Jira Core (OSE)
Proces zamawiania łącza : OSE-n4
Szkoła: RSPO 10
Lokalizacja B
Jira Core (OSE)
Proces zamawiania łącza : OSE-n7
Szkoła: RSPO 11, 12
Lokalizacja A
Open
Open
Reklamacja łącza
Reklamacja łącza
Data uruchomienia łacza
Data uruchomienia łacza
Data uruchomienia łacza
Jira Core (OSE)
Proces podłaczenia szkoły : OSE-n8
Per szkoła: RSPO 10
Lokalizacja B
Jira Core (OSE)
Proces podłaczenia szkoły : OSE-n6
Per szkoła: RSPO 11
Lokalizacja A
Jira Core (OSE)
Proces podłaczenia szkoły : OSE-n5
Per szkoła: RSPO 12
Lokalizacja A
Łącze nie działa
Termin prac w szkole
Termin prac w szkole
Termin prac w szkole
Open
Open gdy oba procesy podłączenia są w stanie "znany termin uruchomienia łącza"
Przekazane do utrzymania
Open , reopen gdy łącze nie działą
Łącze nie działa
Jira SD portal
Jira SD (OSESD)
Proces zlecenie prac podwykonawcy: OSE-n10
Szkoła: RSPO 10
Lokalizacja B
subtasks of zlecenie prac
zamówienie 1
zamówienie 2
zamówienie ...
Jira SD (OSESD)
Proces zlecenie prac podwykonawcy: OSE-n9
Szkoła: RSPO 11, 12
Lokalizacja A
subtasks of zlecenie prac
zamówienie 1
zamówienie 2
zamówienie ...
Jira SD portal
Podwykon
Podwykon
Przekazanie do utrzymania
Przekazanie do utrzymania
Open, reopen gdy łącze nie działą
Open, reopen gdy łącze nie działa
Jira SD (PIBSD)
Proces zlecenia uruchomienia usługi Internet w szkielecie: OSE-n17
Szkoła: RSPO 10
Lokalizacja B
Jira SD (PIBSD)
Proces zlecenia uruchomienia usługi bezpieczeństwa w szkielecie: OSE-n18
Szkoła: RSPO 10
Lokalizacja B
Jira SD (PIBSD)
Proces przekazanie do utrzymania: OSE-n19
Szkoła: RSPO 10
Lokalizacja B
Jira SD (PIBSD)
Proces zlecenia uruchomienia usługi Internet w szkielecie: OSE-n13
Szkoła: RSPO 11
Lokalizacja A
Jira SD (PIBSD)
Proces zlecenia uruchomienia usługi bezpieczeństwa w szkielecie: OSE-n14
Szkoła: RSPO 11
Lokalizacja A
Jira SD (PIBSD)
Proces przekazanie do utrzymania: OSE-n15
Szkoła: RSPO 11
Lokalizacja A
Jira SD (PIBSD)
Proces zlecenia uruchomienia usługi Internet w szkielecie: OSE-n22
Szkoła: RSPO 12
Lokalizacja A
Jira SD (PIBSD)
Proces zlecenia uruchomienia usługi bezpieczeństwa w szkielecie: OSE-n21
Szkoła: RSPO 12
Lokalizacja A
Jira SD (PIBSD)
Proces przekazanie do utrzymania: OSE-20
Szkoła: RSPO 12
Lokalizacja A

4. Sieć OSE

Podstawowym zadaniem OSE ma być zapewnienie jednostkom oświatowym w Polsce możliwości dostępu do bezpiecznego Internetu i zasobów edukacyjnych z przepustowością nie mniejszą niż 100Mb/s (symetrycznie).
Analizując różnice w sposobie realizacji podłączenia poszczególnych lokalizacji, w jakich znajdują się jednostki oświatowe, należy wskazać na istnienie trzech zasadniczych grup, tj. lokalizacje obecnie już będące w zasięgu sieci szerokopasmowej (część z nich już korzysta z dostępu do sieci Internet), lokalizacje planowane do podłączenia w ramach prywatnych inwestycji operatorów telekomunikacyjnych oraz lokalizacje podłączane w ramach POPC, działanie 1.1.

W celu świadczenia usług szerokopasmowego dostępu do internetu niezbędne jest zapewnienie odpowiedniej infrastruktury telekomunikacyjnej łączącej szkołę / lokalizację (wraz z jej siecią i sprzętem informatycznym) do zasobów sieci internet. Cały przebieg tzw. Sieci OSE możemy podzielić na trzy segmenty zgodnie z poniższym rysunkiem.



- Sieć szkolna - infrastruktura sieciowa znajdująca się w lokalizacjach szkolnych, której celem jest zapewnienie łączności dla urządzeń w szkole (zarówno klienckich jak i elementów sieciowych) z punktem dostępowym (CPE). Punkt styku sieci szkolnej z otoczeniem nazywany jest węzłem abonenckim. Zapewnienie odpowiedniej kolokacji dla infrastruktury szkolnej znajduje się w odpowiedzialności placówki szkolnej i jej dyrektora.
- Sieć dostępowa - infrastruktura sieciowa dostarczana przez innych operatorów telekomunikacyjnych zapewniająca łączność pomiędzy lokalizacją szkolną a siecią szkieletową.
- Sieć szkieletowa - Infrastruktura sieciowa zapewniająca łączność pomiędzy węzłami sieci OSE oraz siecią OSE a siecią Internet. Sieć szkieletowa będzie znajdować się po części w ramach kolokacji dzierżawionych od podmiotów zewnętrznych, a w pewnej części w kolokacji NASK

Lokalizacje szkolne będą podłączane do sieci OSE w jednym z czterech modeli:

1. OSE (standardowy) - szkoły podłączane i konfigurowane w ramach OSE
    a. rozdzielenie prac w sieci dostępowej i szkolnej
    b. operator sieci dostępowej doprowadza jedynie zakończenie do lokalizacji szkolnej
    c. prace w szkole realizowane są przez Operatora OSE
    d. Obsługa dla szkoły jest świadczona przez OSE
2. POPC - podłączenie szkół będzie realizowane w ramach I Osi priorytetowej Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 „Powszechny dostęp do szybkiego internetu”

a. w takim przypadku instalacja punktu dostępowego będzie realizowana przez beneficjenta POPC, zapewnia on również urządzenia CPE i AP

b. dodatkowo instalacja będzie rozszerzana przez Operatora OSE o urządzenia SW.

c. Obsługa dla szkoły jest świadczona przez OSE (za serwis CPE odpowiada beneficjent POPC)

3. MAN (Sieci Miejskie) - w szkole istnieje już łącze dostarczane w ramach sieci miejskiej

   a. w szkole nie będzie realizowanych żadnych prac poza opcjonalnym dodaniem CPE dostarczanego przez Operatora OSE - modyfikacja sieci w ramach odpowiedzialności dyrektora szkoły

   b. Obsługa dla szkoły jest świadczona przez Operatora Sieci Regionalnej (MAN), który dalej ewentualnie zgłasza problemy od OSE

   c. Na potrzeby części prac w sieci szkolnej może zostać przypisany przez OSE Partner Serwisowy

4. ODN (Ośrodek Doskonalenia Nauczycieli) - szkoła posiada infrastrukturę gotową do podłączenia do sieci

   a. Operator sieci dostępowej doprowadza zakończenie do lokalizacji szkolnej (inny niż ODN, łącza zamawiane bezpośrednio przez operatora OSE)

   b. Podłączenie istniejącej w szkole infrastruktury sieciowej do doprowadzonego łącza jest w odpowiedzialności szkoły

   c. Operator OSE może opcjonalnie dostarczyć dodatkowe CPE - modyfikacja sieci w ramach odpowiedzialności dyrektora szkoły

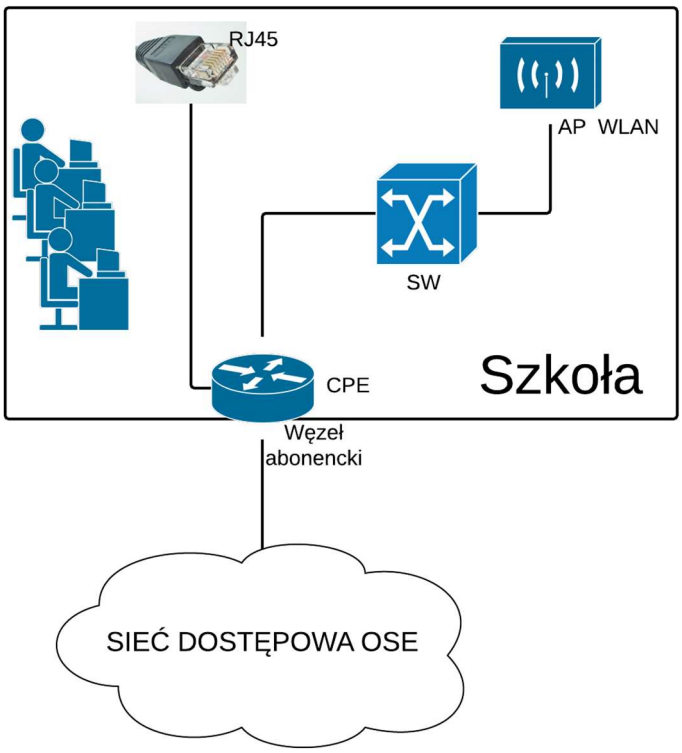
   d. Obsługa dla szkoły jest świadczona przez Operatora Sieci Regionalnej (MAN), który dalej ewentualnie zgłasza problemy od OSE

   e. Na potrzeby części prac w sieci szkolnej może zostać przypisany przez OSE Partner Serwisowy

4.1. Sieć szkolna

Sieci lokalne w jednostkach oświatowych, co do zasady, nie będą w ramach podłączania do OSE modernizowane, jednakże zakłada się możliwość przeprowadzenia ograniczonych prac rekonfiguracyjnych w celu umożliwienia korzystania z dostarczonych usług. Decyzja o wykonywaniu tych prac będzie podejmowana ad hoc, podczas wizyty partnera serwisowego.

Architektura sieci szkolnej z perspektywy OSE przedstawiona jest na poniższym obrazku:



Infrastruktura telekomunikacyjna doprowadzana jest przez operatorów do poszczególnych lokalizacji, w jakich znajdują się szkoły. Należy jednakże zauważyć, że pomiędzy szkoła a lokalizacją zachodzi relacja wiele do wielu. Oznacza to, iż w lokalizacji może występować wiele szkół, lub szkoła może znajdować się w wielu lokalizacjach. Dodatkowo zdarzają się sytuacje, gdy szkoła w danej lokalizacji posiada więcej niż jeden budynek. Mogą się również zdarzyć sytuacje, że pod jednym adresem znajdować się będę szkoły o różnym modelu podłączania, czyli w danym adresie może występować więcej niż jedna lokalizacja (lokalizacja grupuje szkoły w jednym adresie podłączane i obsługiwane w tym samym modelu podłączania).

Za fizyczną instalacją oraz konfiguracją urządzeń w jednostce oświatowej, a także przełączenie sieci lokalnej, odpowiadać będzie partner serwisowy . Rolą partnera serwisowego będzie wsparcie jednostki oświatowej podczas uruchomienia, a także późniejsza opieka nad dostarczanymi przez OSE usługami. Proces instalacji urządzeń brzegowych w jednostkach oświatowych będzie realizowany z wykorzystaniem narzędzi automatyzujących konfigurację sprzętu pod kątem konkretnych potrzeb sieci lokalnej i świadczonych usług.

Obsługa techniczna jednostki oświatowej będzie świadczona w zakresie dostarczanych przez OSE usług oraz obsługi urządzenia dostępowego CPE. Dla wszystkich tych usług powstanie jeden punkt kontaktu (tzw. SPOC – Single Point of Contact) odpowiedzialny za przyjmowanie zgłoszeń. Podstawowym kanałem komunikacyjnych z operatorem OSE będzie Portal OSE, wspierany przez infolinię telefoniczną (CallDesk).

Dla lokalizacji OSE/POPC szkoła będzie obsługiwana przez Operatora OSE, w przypadku lokalizacji MAN / ODN szkoła będzie obsługiwana przez Operatora Sieci Regionalnej, który dopiero po wstępnej analizie będzie przekazywał problemy do Operatora OSE.

Podstawowym założeniem jest, iż w przypadku, gdy szkoła występuje w więcej niż jednej lokalizacji lub ma więcej niż jeden budynek w tej samej lokalizacji podłączenie jest realizowane wyłącznie do jednego budynku w podstawowej lokalizacji. Wyjątkiem od tej reguły jest sytuacja, gdy druga lokalizacja jest

objęta interwencją POPC 1.1 – wtedy beneficjent POPC w ramach oddzielnych prac podłącza drugą lokalizację.

Poniższa tabela szczegółowo rozpisuje dostępne warianty realizacji i sposób zapewnienia sprzętu w lokalizacji

Model podłączenia	Liczba lokalizacji	Liczba budynków	Liczba szkół	CPE	SW	AP	Uwagi
OSE	1	1	1	1szt. dostarcza OSE	1szt. dostarcza OSE	1szt. dostarcza OSE	
POPC	1	1	1	1szt. dostarcza POPC	1szt. dostarcza OSE	1szt. dostarcza POPC	
OSE	1	2	1	1szt. dostarcza OSE	1szt. dostarcza OSE	1szt. dostarcza OSE	Instalacja wykonywana wyłącznie w jednym budynku
POPC	1	2	1	1szt. dostarcza POPC	1szt. dostarcza OSE	1szt. dostarcza POPC	Instalacja wykonywana wyłącznie w jednym budynku
OSE	1	1	2+	1szt. dostarcza OSE	1+szt. dostarcza OSE	2+szt. dostarcza OSE	Zależnie od projektu 1SW na wszystkie szkoły, albo każda szkoła będzie miała własny switch
POPC	1	1	2+	1szt. dostarcza POPC	2+szt. dostarcza OSE	1szt. dostarcza POPC 1+szt. dostarcza OSE	Zależnie od projektu 1SW na wszystkie szkoły, albo każda szkoła będzie miała własny switch W ramach POPC dostarczany jest jeden komplet sprzętu (CPE+AP) per lokalizacja
OSE	1	2	2	1szt. dostarcza OSE	1+szt. dostarcza OSE	2+szt. dostarcza OSE	Zależnie od projektu 1SW na wszystkie szkoły, albo każda szkoła będzie miała własny switch
POPC	1	2	2	1szt. dostarcza POPC	2+szt. dostarcza OSE	1szt. dostarcza POPC 1+szt. dostarcza OSE	Zależnie od projektu 1SW na wszystkie szkoły, albo każda szkoła będzie miała własny switch W ramach POPC dostarczany jest jeden komplet sprzętu (CPE+AP) per lokalizacja
OSE	2	2	1	1szt. dostarcza OSE	1szt. dostarcza OSE	1szt. dostarcza OSE	Instalacja wykonywana wyłącznie w jednym budynku / lokalizacji
POPC	2	2	1	2szt. dostarcza POPC	2szt. dostarcza OSE	2szt. dostarcza POPC	Wyłącznie gdy lokalizacja jest objęta interwencją POPC, w przeciwnym przypadku podłączana jest wyłącznie jedna lokalizacja (sprzęt po 1 szt.)

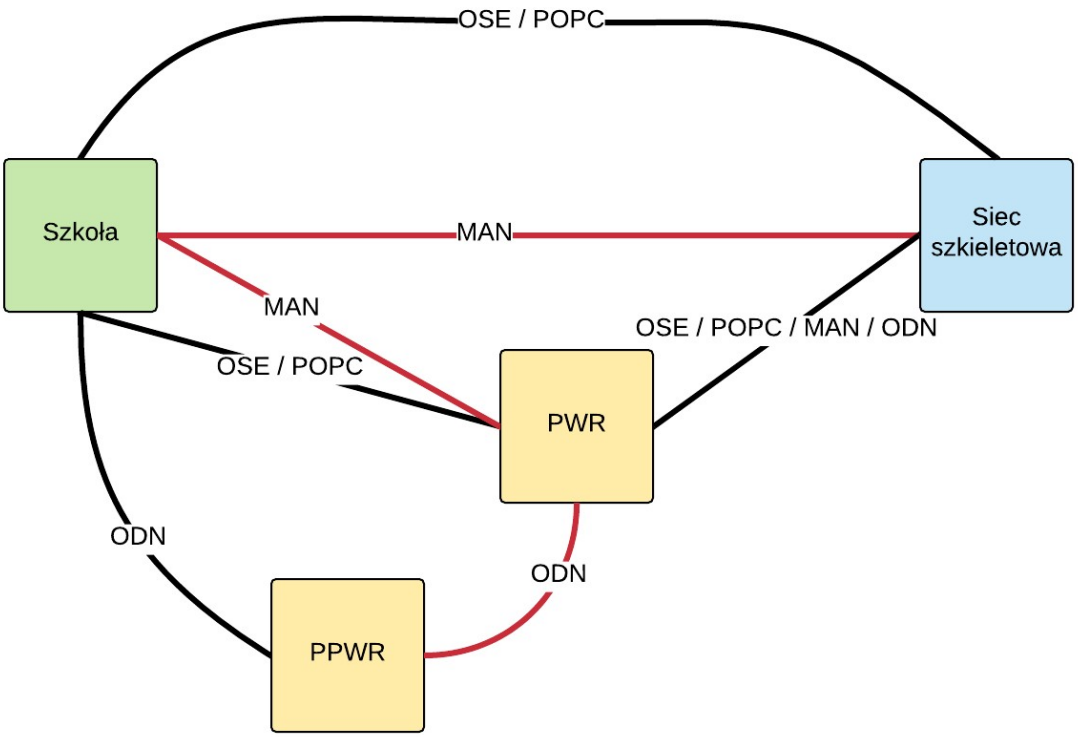
Model podłączenia	Liczba lokalizacji	Liczba budynków	Liczba szkół	CPE	SW	AP	Uwagi
MAN	*	*	n	0-n dostarcza OSE	0-n dostarcza OSE	0-n dostarcza OSE	Możliwe dostarczenie urządzeń OSE do szkół. Operator Sieci Regionalnej (MAN) może pełnić rolę Partnera Serwisowego, dostarczenie urządzeń może być realizowane przez Operatora OSE, ewentualnie zostanie wybrany zewnętrzny partner serwisowy (jak dla lokalizacji OSE/POPC)
ODN	*	*	n	0-n dostarcza OSE	0-n dostarcza OSE	nie dotyczy	Możliwe dostarczenie urządzeń OSE do szkół. Operator Sieci Regionalnej (ODN) może pełnić rolę Partnera Serwisowego, dostarczenie urządzeń może być realizowane przez Operatora OSE, ewentualnie zostanie wybrany zewnętrzny partner serwisowy (jak dla lokalizacji OSE/POPC)

Urządzenia dostępowe CPE

Kluczowym elementem sieci szkolnej z punktu widzenia systemu OSS będą urządzenia dostępowe - CPE. System provisioningu musi zarządzać zdalnie konfiguracją tych urządzeń - w przypadku urządzeń zarządzanych przez OSE, lub wysyłać mailowo konfigurację urządzeń do Operatora Sieci Regionalnej (w przypadku urządzeń będących własnością MAN / ODN). Należy zwrócić uwagę na dużą możliwą różnorodność urządzeń. O ile urządzenia kupowane przez Operatora OSE będą znane z dużym wyprzedzeniem (można więc będzie przygotować dla nich profile konfiguracji z dużym zapasem czasowym), to w przypadku urządzeń dostarczanych przez beneficjentów POPC model urządzenia będzie znany z 1-2 tygodniowym wyprzedzeniem. Provisioing musi więc zapewniać szybkie i elastyczne dodawanie nowych modeli urządzeń do konfiguracji.

4.2. Sieć dostępowa

Połączenie pomiędzy lokalizacją szkolną (węzeł abonencki), a siecią szkieletową OSE (węzeł agregacyjny) realizowana jest za pośrednictwem tzw. sieci dostępowej. Możliwe warianty realizacji połączenia w sieci szkieletowej zależą od modelu podłączenia szkoły / lokalizacji. (na poniższym rysunku łącza zaznaczone na czarno są w odpowiedzialności operatora OSE, a łącza zaznaczone na czerwono są w odpowiedzialności operatora sieci regionalnej)



Wyróżniamy następujące przebiegi łącz w sieci dostępowej:

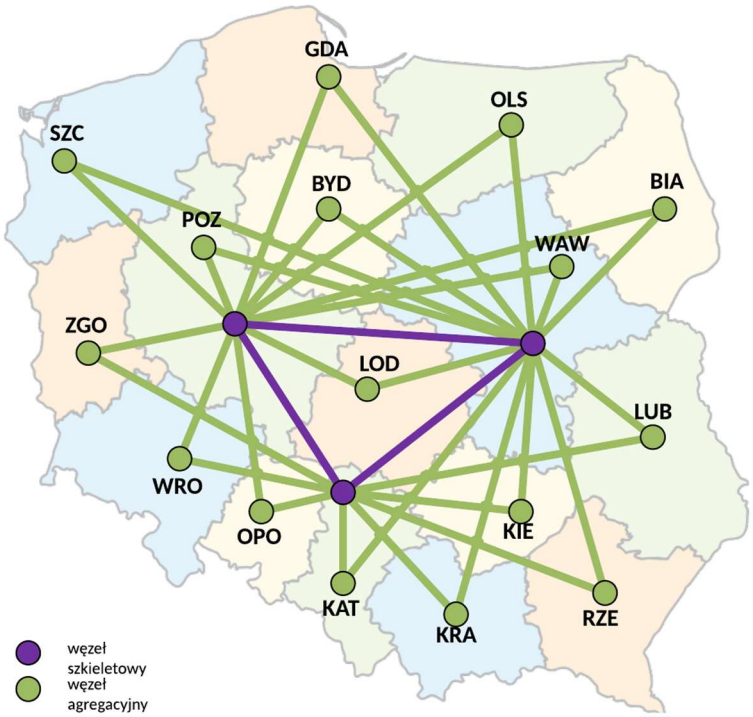
Model Podłączenia	Przebieg łącza	Odpowiedzialność za łącze
OSE / POPC	Węzeł abonencki → Węzeł agregacyjny	Operator OSE
OSE / POPC	Węzeł abonencki → PWR → Węzeł agregacyjny	Operator OSE
MAN	Węzeł abonencki → Węzeł agregacyjny	Operator Sieci Regionalnej (MAN)
MAN	Węzeł abonencki → PWR → Węzeł agregacyjny	Operator Sieci Regionalnej (MAN)
ODN	Węzeł abonencki → PPWR → PWR → Węzeł agregacyjny	Za łącze PPWR→PWR odpowiada Operator Sieci Regionalnej (ODN) Za pozostały przebiego odpowiada operator OSE

Konfiguracja sieci dostępowej

Za konfigurację po stronie sieci dostępowej będzie odpowiedzialny operator zapewniający łączę zarówno dla łącz zarządzanych przez OSE jaki i pozostałych (MAN / ODN). W procesie zamawiania łącza konieczne jest więc przekazanie pełnej konfiguracji, jaka ma być ustawiona dla łącza. Z uwagi na fakt braku aktywnych urządzeń OSE w sieci dostępowej monitoring łączy musi być realizowany na jej brzegach (węzeł abonencki w szkole i węzeł agregacyjny w sieci szkieletowej). Aby było możliwe szybkie analizowanie i rozwiązywanie problemów w systemach odpowiedzialnych za Troube Ticketing muszą być informacje o całym przebiegu łącza wraz z informacją o operatorach odpowiedzialnych za poszczególne odcinki.

4.3. Sieć szkieletowa

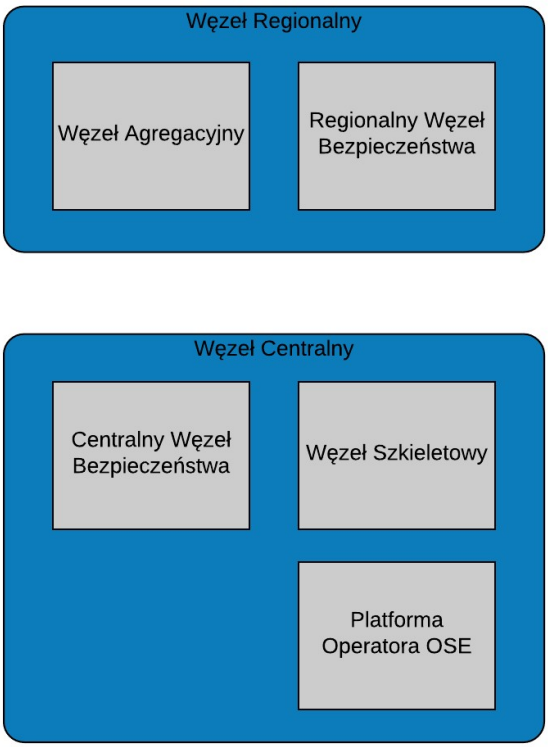
W zakresie sieci szkieletowej operator OSE będzie opierał się na łączach dzierżawionych od operatorów telekomunikacyjnych, nie jest rozważana budowa własnej infrastruktury kablowej. Przeprowadzony przez NASK Dialog Techniczny z operatorami telekomunikacyjnymi wskazał na potrzebę budowy 16 węzłów OSE, zlokalizowanych w miastach wojewódzkich, w celu agregowania ruchu z jednostek oświatowych z terenu całego kraju (węzły agregacyjne). Trzy spośród tych węzłów powinny pełnić również rolę węzłów centralnych (węzły szkieletowe). Pozostałe węzły będą połączone do węzłów centralnych. Lokalizacje węzłów została wybrana przez NASK Państwowy Instytut Badawczy w ramach odrębnych, wewnętrznych procesów zakupowych, w wyniku których zostali wyłonieni dostawcy Usług kolokacji w poszczególnych centrach przetwarzania danych. Zamawiający planuje również objęcie wszystkich "kolokacji" jednym, wspólnym systemem zarządzania.



Węzły sieci

W sieci OSE będą dwa funkcjonalne rodzaje węzłów:

- Węzły Regionalne, w których skład będą wchodzić Węzły Agregacyjne (do których będą dołączone łącza ze szkół) oraz Regionalne Węzły Bezpieczeństwa
- Węzły Centralne, w których skład będą wchodzić Węzły Szkieletowe, Centralne Węzły Bezpieczeństwa oraz Zasoby Obliczeniowe OSE (będące platformą dla systemów OSE). Do Węzłów Szkieletowych dołączone będą Węzły Agregacyjne. Węzły te będą także zapewniały łączność do sieci Internet.



Węzły Szkieletowe będą zlokalizowane w tych samych miejscach co Węzły Agregacyjne, za wyjątkiem węzła WAW / WAW Core, w którym Węzeł Agregacyjny będzie umieszczony w innej lokalizacji niż Węzeł Szkieletowy (oba węzły będą zlokalizowane na terenie Warszawy). Urządzenia pełniące funkcje obu węzłów będą oddzielne.

Każdy węzeł OSE wyposażony zostanie w urządzenia sieciowe, Infrastrukturę bezpieczeństwa, przełączniki sieci lokalnej, niezbędne zasoby obliczeniowe operatora OSE (komponenty systemów z grupy OSS: Systemu Retencji Logów, Systemu FP/PM), rutery shadow oraz urządzenia sieci zarządzającej, zapewniające dostęp administracyjny do wszystkich urządzeń zlokalizowanych w węźle. Infrastruktura sieciowa w węzłach OSE będzie się opierać o następujące typy/modele urządzeń:

- rutery - Juniper MX (960 i 10003)
- CG-NAT - Juniper SRX (4600)
- LAN - Juniper QFX (10008, 10003, 5110 i 5120)
- rutery shadow - Juniper SRX320

Konfiguracja sieci szkieletowej:

Zadaniem systemu odpowiedzialnego za provisioning będzie automatyczna konfiguracja urządzeń w sieci szkieletowej (zarówno urządzeń sieciowych jak i urządzeń bezpieczeństwa). Pomimo iż architektura sieci szkieletowej będzie się charakteryzować minimalną zmiennością to jednakże dla obszaru Service Order Manager (SOM) dużym wyzwaniem będzie choreografia skonfigurowania poszczególnych elementów sieci. System provisioningu w wyniku zlecenia z obszaru SOM będzie musiał móc dla każdego zlecenia aktywacji / modyfikacji / usługi przeprowadzić proces automatycznej zmiany konfiguracji urządzeń w sieci szkieletowej wykorzystując komponenty Element Manager dostarczane wraz z urządzeniami sieciowymi

i bezpieczeństwa lub konfigurując urządzenia bezpośrednio przy użyciu interfejsu udostępnianego przez te urządzenia.

4.4. Koncepcja świadczenia usługi dla szkoły

W szkołach zainstalowane będą urządzenia CPE, świadczące usługi dla sieci lokalnych w szkołach.

Na urządzeniach tych lokalne adresy IPv4 z pul prywatnych zgodnych z RFC1918 / BCP5 translowane są (NAT 1:1) do adresów z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153). Jednocześnie dla klientów IPv6 zaalokowana jest pula adresów GUA z puli przydzielonej dla sieci OSE przez RIPE (w sieci OSE nie będą używane adresy prywatne IPv6).

Ruch od urządzeń CPE umieszczonych w szkołach przenoszony jest przez łącza, w technologii Ethernet, operatorów agregujących do Węzłów Agregacyjnych sieci OSE, gdzie jest oddawany do urządzeń agregujących sieci OSE na interfejsach 10GE oraz 1GE. Ruch do każdego urządzenia CPE jest oddawany na oddzielnych VLANach, przy następujących założeniach:

- każda szkoła jest terminowana na oddzielnym VLANie lub VLANach,
- z każdej szkoły może być skreowanych kilka VLANów (do pięciu), przy czym każdy z nich terminowany jest po stronie szkoły w oddzielnym VRF, a od strony sieci OSE każdy traktowany jest jako oddzielne łącze z własną adresacją i routingiem; Separacja VLANów tworzona jest na potrzeby kreowania różnych usług, w tym usług posiadających różne polityki bezpieczeństwa;
- ruch zarządzania do urządzenia CPE jest oddzielony od ruchu produkcyjnego szkoły obsługiwanej przez to CPE i terminowany jest na oddzielnym VLANie,
- ww. VLANy mogą być oddane w jednym z dwóch modeli:
    - jako VLAN z pojedynczym tagowaniem, zgodnie ze standardem IEEE 802.1q lub,
    - jako VLAN z podwójnym tagowaniem, zgodnie ze standardem IEEE 802.1ad, przy czym ruch z pojedynczej szkoły ma wspólny S-TAG oraz EtherType = 0x88a8.

Ruch odebrany w Węźle Agregacyjnym kierowany jest do Węzła Bezpieczeństwa.

Następnie odebrany ruch z Regionalnego Węzła Bezpieczeństwa kierowany jest do Węzłów Szkieletowych, a następnie do sieci Internet. Pomiędzy Węzłem Bezpieczeństwa, a wyjściem do sieci Internet ruch IPv4 przechodzi przez instancję CG-NAT, gdzie jest translowany do publicznych adresów IPv4 przydzielonych dla sieci OSE.

Separacja ruchu

Ruch zarządzania (zarówno dla urządzeń CPE jak też urządzeń sieci OSE) traktowany jest jako ruch zaufany i jest oddzielony od ruchu produkcyjnego do / ze szkół. Separacja tego ruchu w sieci OSE powinna nastąpić na poziomie VFR, logical system lub podobnym (tj. zapewniającym separację tablic routingu oraz wykluczającym wzajemny dostęp do ruchu z poszczególnych strumieni).

QoS

W sieci OSE wdrożony będzie QoS z następującymi założeniami:

- klasyfikacja odbywa się na urządzeniu agregacyjnym sieci OSE,

- najwyższy priorytet w sieci ma ruch z klasy Network Control, obejmujący ruch kontrolny protokołów routingu (IGP, BGP, MPLS, itd.) – ruch ma zagwarantowane 3% pasma na interfejsach szkieletowych sieci (tj. interfejsach pomiędzy urządzeniami sieci OSE bez uwzględnienia urządzeń CPE);
- ruch w klasie MGMT (ruch zarządzania, w szczególności ruch do / z systemów OSS, ruch sesji terminalowych do urządzeń sieciowych, ruch do kolektorów logów) – ruch ma zagwarantowane 5% pasma na interfejsach sieci (w tym na interfejsach pomiędzy urządzeniami sieci OSE a urządzeniami CPE);
- ruch w klasie BE (Best Effort) obejmujący ruch produkcyjny do / ze szkół – ruch ma zagwarantowane 50% pasma na wszystkich interfejsach;
- w sieci OSE musi być przygotowana możliwość uruchomienia ruchu w klasach:
    - VOICE – ruch priorytetowy – nie więcej niż 5% pasma;
    - INTVIDEO (Interactive Video) – ruch gorszy niż NC a lepszy niż MGMT – zagwarantowane 20% pasma;
    - scavenger (less-than best-effort) – ruch bez gwarancji pasma.

5. Bezpieczeństwo OSE

W sieci OSE będą dwa funkcjonalne rodzaje węzłów:

- Węzeł Regionalny składa się z Węzła Agregacyjnego, do którego będą dołączone łącza ze szkół, oraz z Regionalnego Węzła Bezpieczeństwa.
- Węzeł Centralny, składa się z Węzła Szkieletowego, do którego będą dołączone Węzły Agregacyjne. Węzły te będą także zapewniały łączność do sieci Internet oraz zapewnią połączenie z Zasobami obliczeniowymi OSE. Centralny Węzeł Bezpieczeństwa będzie zlokalizowany tylko w dwóch Węzłach Centralnych.

Węzły Centralne mogą być zlokalizowane w tych samych Obiektach co Węzły Regionalne, ale Urządzenia pełniące funkcje obu węzłów będą oddzielne.

Każdy węzeł OSE wyposażony zostanie w urządzenia sieciowe, elementy Infrastruktury bezpieczeństwa, przełączniki sieci lokalnej, systemy OSS, systemy BSS zlokalizowane w węźle oraz w urządzenia sieci zarządzania, zapewniające dostęp administracyjny do wszystkich Urządzeń zlokalizowanych w Węźle.

Każdy z 16 Regionalnych Węzłów Bezpieczeństwa będzie zawierać komponenty realizujące podstawowe funkcjonalności, m.in:

- zapewnianie bezpieczeństwa teleinformatycznego użytkownikom sieci OSE,
- wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym,
- wykrywanie i blokowanie zdefiniowanych aplikacji webowych,
- monitorowanie ruchu sieciowego i zapisywanie najważniejszych wydarzeń do logu.

Dwa Centralne Węzły Bezpieczeństwa będą zawierać komponenty realizujące funkcjonalności ochrony Zasobów obliczeniowych OSE, tzn. będą:

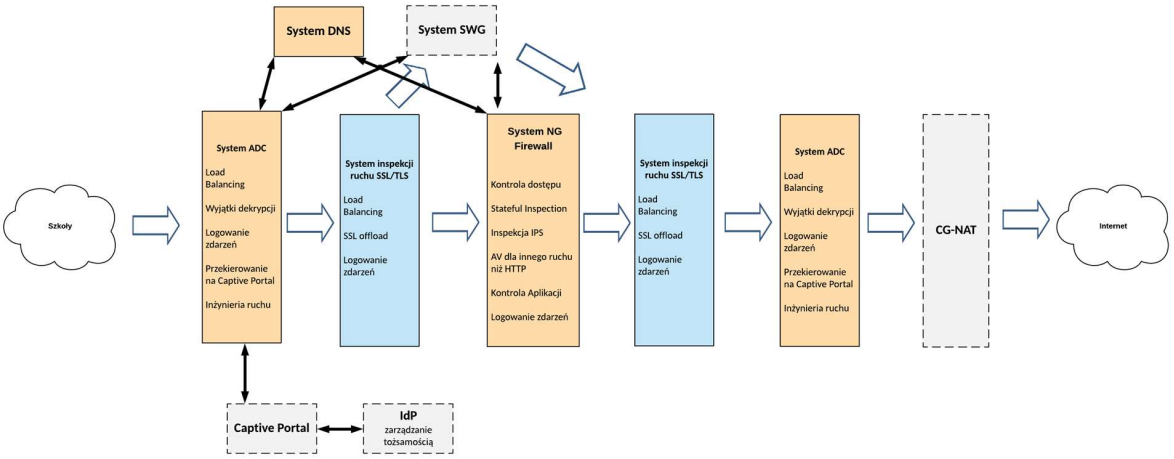
- zapewniać bezpieczeństwo teleinformatyczne Zasobów obliczeniowych OSE i systemów wsparcia
- wykrywać i zapobiegać włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym

Ponad to w każdym Regionalnym Węźle Bezpieczeństwa zostaną zainstalowane mechanizmy ochrony użytkownika sieci OSE, realizowane w oparciu o systemy klasy SWG.

5.1. Architektura Infrastruktury Bezpieczeństwa

Architektura Infrastruktury bezpieczeństwa składa się z Systemu ADC, Systemu inspekcji SSL/TLS, Systemu NG Firewall, Systemu DNS, Systemu zarządzającego oraz Systemu SWG.

Poniżej zaprezentowano schemat blokowy przepływu danych w Regionalnych Węzłach Bezpieczeństwa. Schemat zawiera systemy Zamawiającego, składające się na Infrastrukturę bezpieczeństwa.



Infrastruktura bezpieczeństwa zostanie oparta o urządzenia/systemy zastępujących producentów:

- ADC (LTM) – F5 Networks
- SSLO (deszyfracja) – F5 Networks
- SSL VPN, ADC, WAF – F5 Networks
- Firewall – Fortigate
- DNS – InfoBlox

Koncepcja przepływu danych

- Cały ruch (100%) od CPE, po przejściu przez Węzeł agregacyjny, przechodzi przez System ADC, który dokonuje deszyfracji SSL wewnętrznie lub z wykorzystaniem Urządzeń dedykowanych. Inspekcji podlega 100% ruchu SSL/TLS z pominięciem wybranych domen, pobranych z pól SNI lub CN certyfikatu, należących do kategorii treści określonych przez Zamawiającego. Informację na temat kategorii do jakiej należy dana domena, System ADC uzyska poprzez współpracę z Systemem DNS.
- Po dokonaniu deszyfracji, cały ruch zostanie przekierowany do Systemu NG Firewall, gdzie będą zdefiniowane polityki dotyczące ruchu warstwy 3 /4 i uruchomione zostaną funkcjonalności IPS (100% ruchu), AV (9% ruchu - inspekcji AV będzie podlegał ruch niezwiązany z ruchem webowym HTTP/HTTPS) i Kontroli aplikacji (100% ruchu). W przypadku kiedy będzie to żądanie do serwisów web (HTTP, HTTPS), System przekieruje cały taki ruch do Systemu SWG.
- Po dokonaniu inspekcji treści, ruch jest kierowany ponownie do Systemu ADC, lub na urządzeniu dedykowanym do obsługi ruchu SSL/TLS, w celu ponownej szyfracji SSL.
- Ruch wychodzi z Regionalnego Węzła Bezpieczeństwa i kierowany jest zgodnie z tablicą routingu Węzła szkieletowego. W przypadku potrzeby skierowania ruchu do sieci Internet, przed opuszczeniem Węzła Centralnego, dokonywana jest translacja CGNAT do adresacji publicznej.
- Ruch zarządzania (zarówno dla CPE jak też urządzeń sieci OSE) traktowany jest jako ruch zaufany i jest oddzielony od ruchu produkcyjnego do / ze szkół. Separacja tego ruchu w sieci OSE następuje na poziomie VFR, logical system lub podobnym.

Systemy Wsparcia

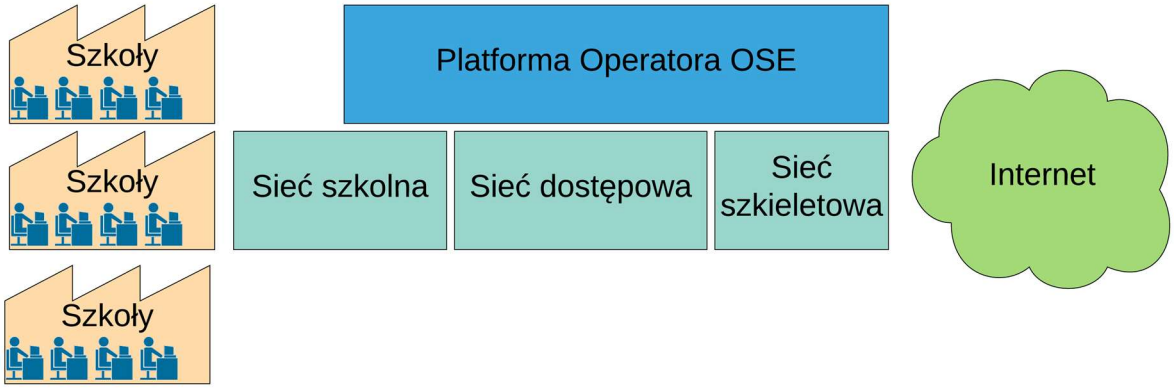
Zamawiający planuje większość procesów realizować w sposób zautomatyzowany. Systemy i infrastruktura objęte zostaną zintegrowane z centralnymi systemami nadzorującymi działanie wszystkich elementów sieci OSE.

6. Platforma Operatora OSE

Platforma Operatora OSE (POOSE), ***której częścią są systemy OSS będące przedmiotem zamówienia,*** służy do wsparcia działalności NASK PIB jako operatora telekomunikacyjnego w obszarze Ogólnopolskiej Sieci Edukacyjnej.

Systemy nadzoru OSE muszą zapewniać Operatorowi OSE możliwość spełniania wszystkich jego obowiązków i zadań wynikających z ustawy o OSE. Zgodnie z Art. 5 ustawy o OSE do zadań Operatora OSE należy:

- przygotowanie OSE w sposób umożliwiający świadczenie z jej wykorzystaniem usług, bezpiecznego dostępu do internetu, jej eksploatację, utrzymanie, usuwanie awarii, modernizację oraz nadzór nad jej funkcjonowaniem;
- świadczenie szkole usługi szerokopasmowego dostępu do Internetu o symetrycznej przepustowości co najmniej 100 Mb/s;
- świadczenie szkole usług bezpieczeństwa teleinformatycznego, obejmujących ochronę przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego;



Dodatkowo NASK PIB jako Operator OSE realizujący projekt OSE również przy dofinansowaniu z projektów unijnych musi przy wykorzystaniu platformy nadzoru OSE móc spełnić następujące wymagania:

- Kwalifikowalność wydatków
- Kontrola projektu
- Sprawozdawczość, rozliczenie projektu i jego dokumentacja
- Promowanie i znakowanie produktów projektu
- Zapewnienie trwałości projektu

Główne zadania stawiane POOSE są następujące:

- Obsługa klientów (szkół)
- Prowadzenie działalności operatora telekomunikacyjnego
- Zarządzanie i rozliczanie prac partnerów serwisowych

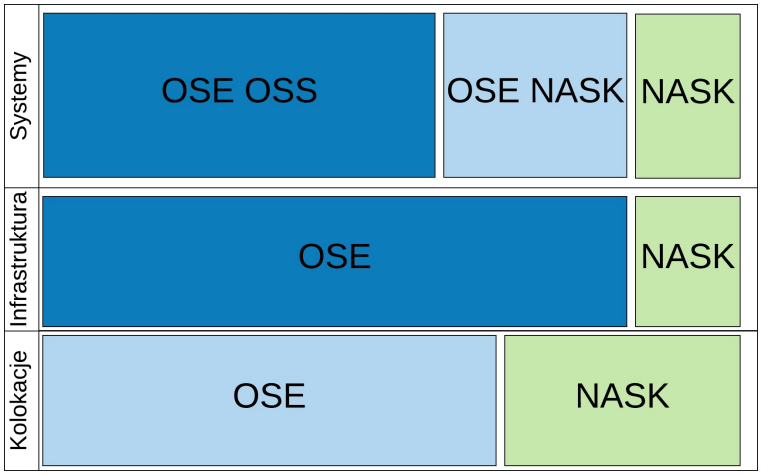
- Zarządzanie i rozliczanie dostawców sprzętu
- Zarządzanie i rozliczanie usług operatorów sieci dostępowej / agregacyjnej / szkieletowej
- Monitorowanie sieci i systemów bezpieczeństwa OSE
- Zarządzanie punktami dostępu w szkołach
- Zarządzanie bezpieczeństwem w ramach dedykowanego Portalu bezpieczeństwa
- Wsparcie rozliczania projektu OSE

Architektura referencyjna

W ramach Platformy Operatora OSE wyróżniamy 3 główne obszary:

- Systemy informatyczne wspierające realizację działań operatora OSE,
- Infrastrukturę umożliwiającą działanie systemów POOSE,
- Kolokacje, w których znajdować się będzie infrastruktura

Obszary te dzielą się na segmenty zgodnie z poniższym rysunkiem:

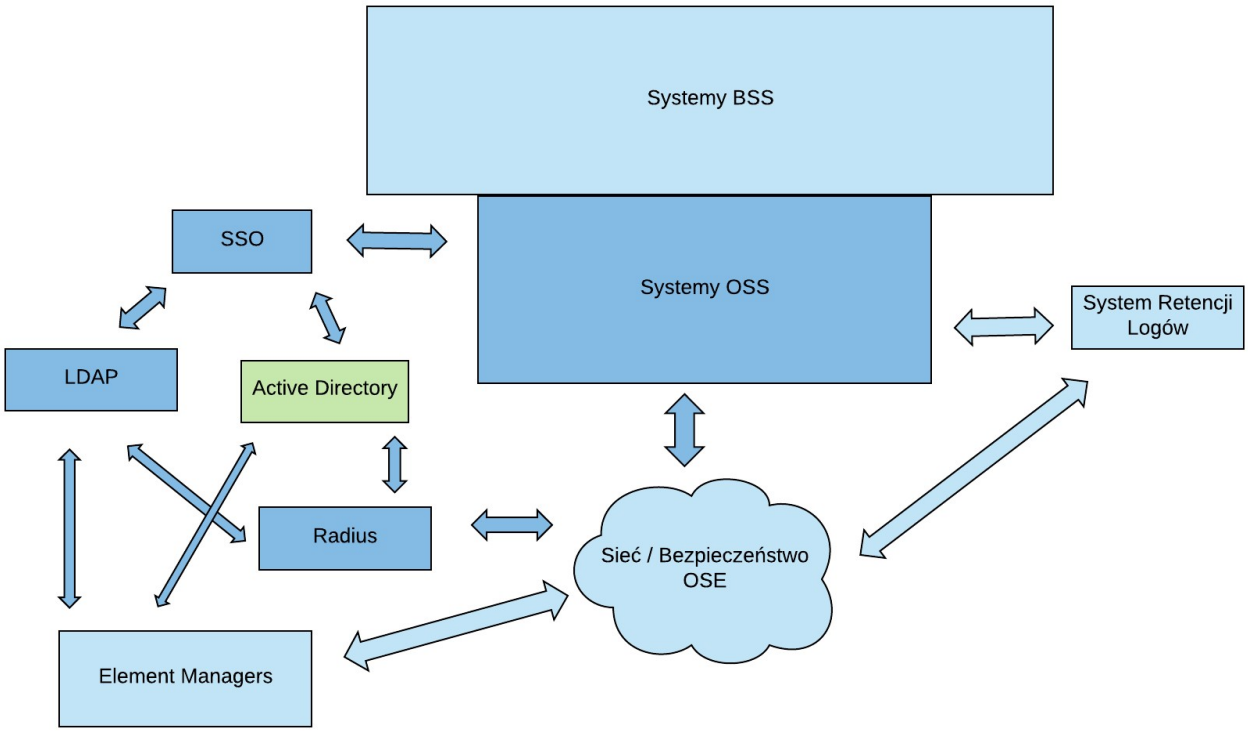


- W obszarze kolokacji wyróżniamy lokalizację własną NASK oraz lokalizacje pozyskiwane na potrzeby OSE w innych postępowaniach
- W ramach infrastruktury obecne rozwiązania bazują na infrastrukturze NASK, natomiast w ramach postępowania zostanie wdrożona infrastruktura na potrzeby wszystkich systemów wspierających operatora OSE
- Systemy w ramach platformy operatora OSE możemy podzielić na trzy grupy:
    - Systemy NASK - to są systemy wspierające bieżącą działalność NASK, które będą również wykorzystywane na potrzeby OSE

- Systemy OSE NASK - to systemy rozwijane przez NASK pod dedykowane potrzeby operatora OSE (rozwijane zarówno przez zespoły NASK jak i dostawców)
- Systemy OSE OSS - to systemy będące zakresem postępowania zakupowego, których celem jest realizacja funkcjonalności OSS-owych dla docelowej sieci OSE

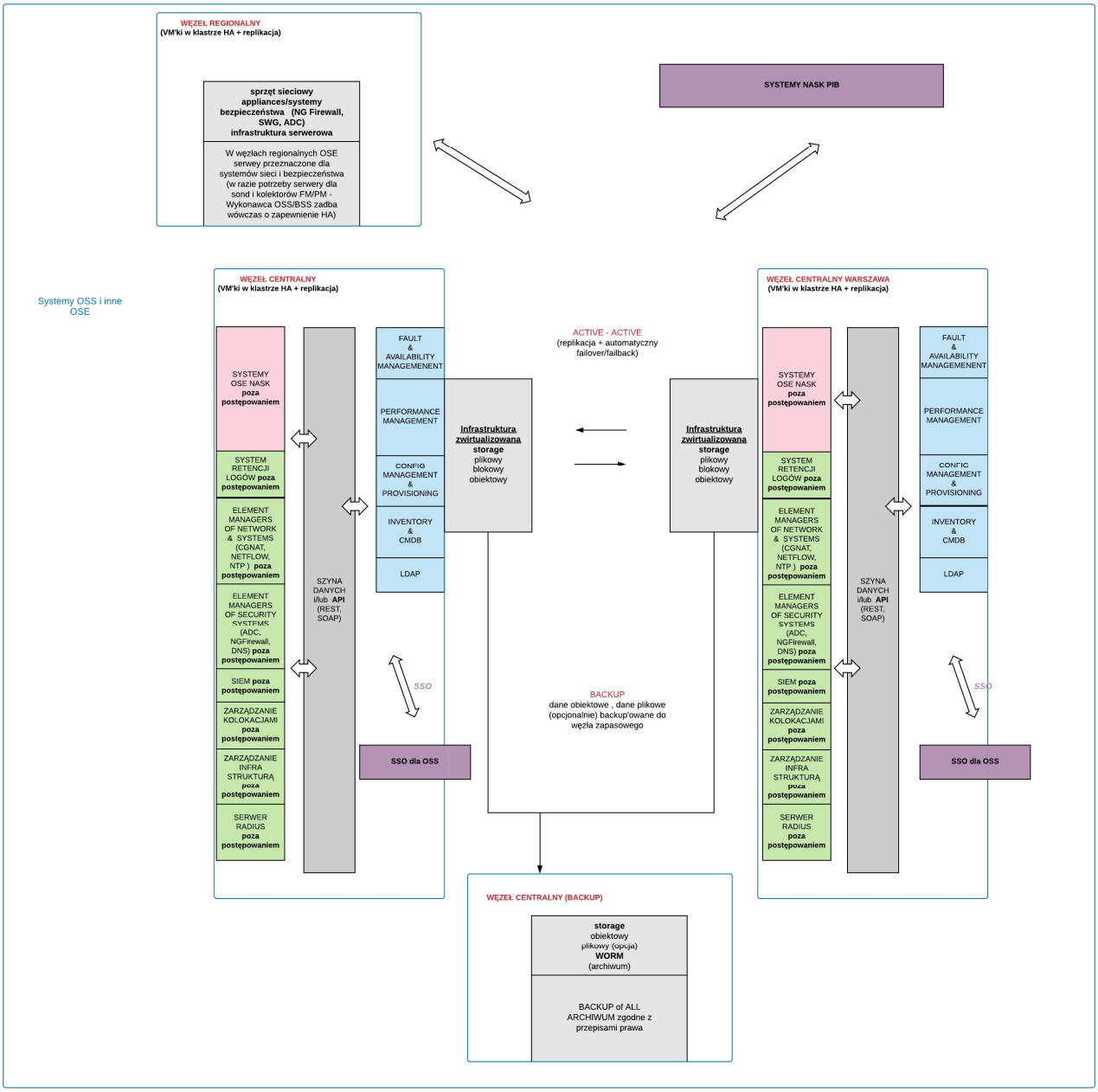
6.1 Warstwa aplikacyjna

Wysokopoziomowy model Platformy Operatora OSE:



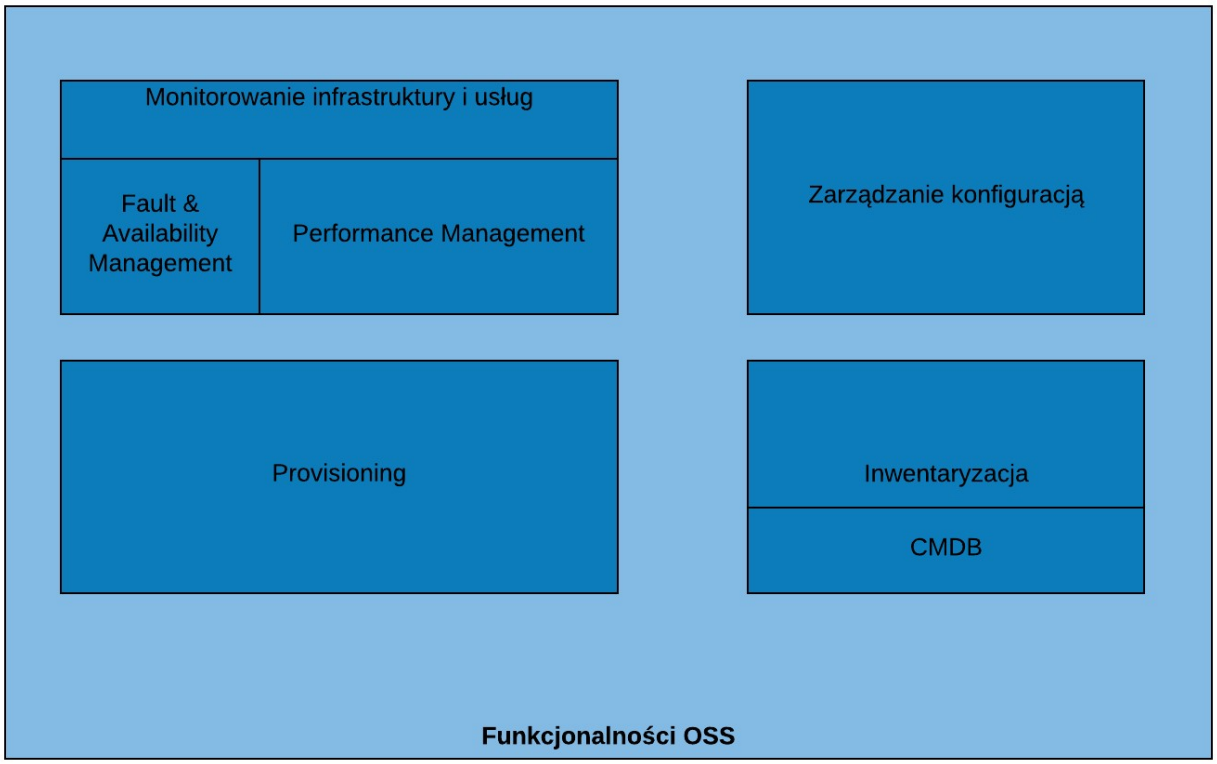
Systemy BSS - systemy wspierające realizacji zadań w obszarze BSS, za które odpowiada NASK rozwijając je samodzielnie lub za pośrednictwem dostawców. W systemach tych znajdują się zarówno komponenty dedykowane pod OSE takie jak Portal czy CRM jak również systemy wykorzystywane przez cały NASK takie jak system Finansowo-Księgowy, kancelaryjny czy magazynowy.
Systemy OSS - są to komponenty będące zakresem postępowania, których celem jest wspieranie działań operatora OSE w obszarze procesów OSS-owych

Większy poziom szczegółowości POOSE widać na poniższym rysunku:



6.1.1. Funkcjonalności obszaru OSS

Wymagane w ramach przedmiotu zamówienia systemy obszaru OSS zostały zgrupowane wokół funkcjonalności zgodnie z poniższym rysunkiem:



Fault & availability management - wsparcie pracy zespołów NOC, SOC i IT w zakresie utrzymania sieci, usług i systemów OSE.

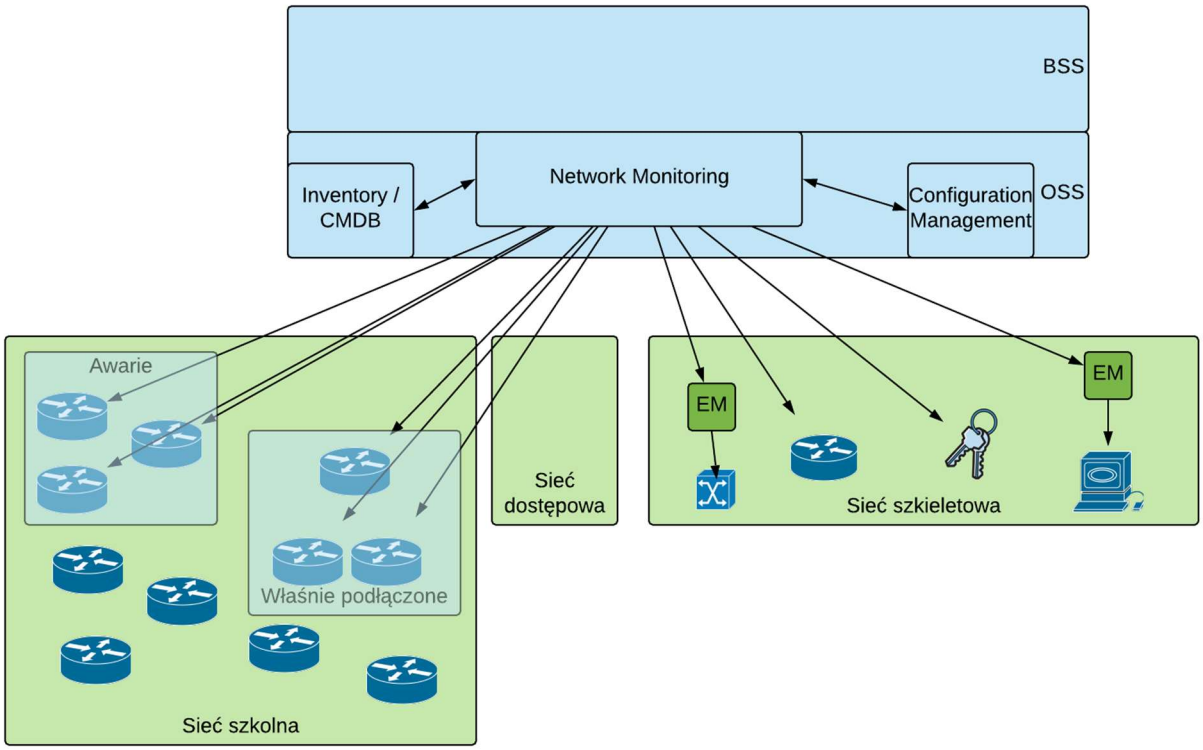
Należy pamiętać przy tym o uwarunkowaniach związanych z monitorowaniem sieci OSE

W przypadku sieci szkieletowej rozumianej jako urządzenia sieciowe i urządzenia bezpieczeństwa wymagany jest standardowy / pełny monitoring wszystkich elementów sieci. W ramach rozwiązania OSS powinna zostać dostarczona platforma zapewniająca pełen widok na sieć szkieletową, usługi bezpieczeństwa, portal, inne elementy OSE i zapewniająca pełną widoczność wszystkich problemów. W szczególności należy zwrócić uwagę na to, że system OSS, jako system parasolowy dla wszystkich innych systemów dziedzinowych obsługiwany będzie przez stosunkowo niewielki zespół NOC i musi zapewnić szybką analizę stanu sieci (zwłaszcza w sytuacji awarii), zatem jedną z pryncypialnych funkcjonalności, jakie system ma posiadać jest RCA (Root Cause Analisys).

W przypadku sieci szkolnej z uwagi na potencjalną ilość urządzeń zakładane jest monitorowanie w następującym zakresie:

- W ramach podłączenia i przez pewien czas po podłączeniu monitorowane będą urządzenia CPE (fault & availability, performance) oraz SW,AP (performance)
- W przypadku problemów / awarii i przy decyzji, że niezbędna jest dodatkowa diagnoza będzie włączany monitoring urządzenia CPE (fault & availability, performance) oraz urządzeń SW, AP (performance). W tych okresach alarmy z CPE będą kierowane przez System Retencji Logów do systemu FM oraz w tych okresach system PM będzie pobierał dane performance'owe do statystyk z urządzeń CPE, SW i AP (z tych ostatnich dwóch po odpowiednim przekonfigurowaniu tych urządzeń)
- Dodatkowo niezbędny jest monitoring ruchu w kontekście VLANów szkoły, całej szkoły oraz lokalizacji - zakłada się, że ruch per VLAN będzie zbierany z subinterface'u urządzenia szkieletowego

w węźle OSE oraz zebrane dane odpowiednio sumowane by otrzymać ruch per szkoła i per lokalizacja



Z uwagi na:

- uwarunkowania techniczne - wiele różnych modeli stawianych w szkołach urządzeń i związana z tym implementacja MIB w systemie FM versus to że informacje w SYSLOG są wystarczające i bez dodatkowego nakładu pracy
- logistyczne - jedynie CPE jest w pełni zarządzane przez operatora OSE, a urządzenia SW i AP są przekazywane szkole w jej administrację

operator rezygnuje ze zbierania trap'ów SNMP z urządzeń stawianych w szkole, wysyłane będą wyłącznie logi z urządzenia CPE (SYSLOG) i do systemu monitoringu będą one trafiać za pośrednictwem Systemu Retencji Logów

Performance management - swoją funkcjonalnością ma wspierać procesy utrzymania sieci, usług i systemów OSE a w szczególności monitorować wydajność urządzeń i wykorzystanie zasobów sieci OSE.

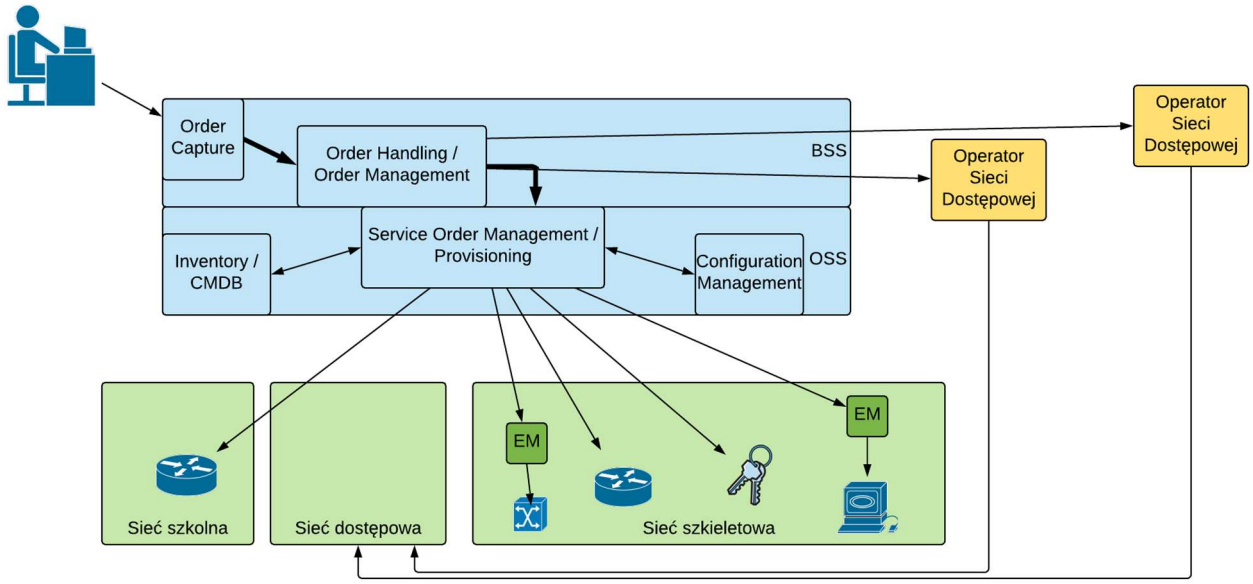
Zarządzanie konfiguracją - zarządzanie konfiguracją (w tym backupy i wersjonowanie) masowej ilości urządzeń OSE - większość tych urządzeń to heterogeniczny sprzęt instalowany w szkołach w różnorakich modelach i z różnorodną konfiguracją (zależną od producenta sprzętu). System Config Manager musi objąć swym zasięgiem zarówno sprzęt sieciowy jak i urządzenia bezpieczeństwa OSE w węzłach regionalnych i centralnych. Zarządzaniem konfiguracjami i backupowaniem serwerów OSE ma być

realizowane przez dedykowany system do zarządzania infrastrukturą serwerową dostarczony przez Wykonawcę razem z tą infrastrukturą.

Provisioning - automatyzacja procesów obejmuje szereg działań, które są tożsame z provisioningiem niezbędnych konfiguracji w systemach i na sprzęcie OSE a także usług w systemach, co oznacza co najmniej:

- uzupełnienie/implementacja konfiguracji urządzenia CPE w szkole i urządzeń szkieletowych przy pomocy automatycznych skryptów/polityk itp.,
- uzupełnienie konfiguracji urządzeń w Config Manager (wyzwolenie zaciągnięcia nowej konfiguracji urządzenia, potem cykliczna kontrola zmian w konfiguracji) ,
- uzupełnienie danych w systemach dotyczących inwentaryzacji zasobów (OSS) i stanów magazynowych (BSS Zamawiającego),
- uruchomienie odpowiednich pomiarów jakości sieci i zbierania zdarzeń i alarmów (Fault & Availability Management),
- uruchomienie odpowiednich pomiarów performance'owych w tym pomiarów ruchu w sieci szkieletowej i pomiarów ruchu generowanego przez szkoły (Performance Managment),
- inicjowanie automatycznego procesu generowania raportów ruchu i przekazywania ich do Centralnego Systemu Raportowego Zamawiającego,
- uruchomienie pomiarów urządzeń CPE w okresie 3 tygodni od podłączenia szkoły do OSE
- uruchomienie monitoringu łącz,
- uruchomienie monitoringu świadczonych przez OSE usług (co najmniej dostęp do internetu i usługi bezpieczeństwa)

W architekturze platformy operatora OSE w domenie OSS konieczne jest zapewnienie funkcjonalności związanej z realizacją konfiguracji oraz zmian konfiguracji na urządzeniach sieciowych i urządzeniach/systemach bezpieczeństwa w szkielecie a także urządzeń CPE w szkołach, czyli tzw. docelowy provsioning usług. Z uwagi na specyfikę sieci OSE działania te będą dotyczyć sieci szkolnej i docelowej sieci szkieletowej, zgodnie z poniższym obrazkiem.



Oba te obszary mają charakterystyczne dla nich wyzwania.

W sieci szkolnej provisioning będzie w miarę prostym i standardowym działaniem, jednakże wyzwaniem będzie zapewnienie obsługi różnych modeli urządzeń. O ile przypadku lokalizacji OSE dostępne modele urządzeń będą znane wcześniej (zostaną zakupione w oddzielnym przetargu) to w przypadku lokalizacji POPC lista dostępnych modeli urządzeń może się zmieniać dynamicznie, gdyż za ich dostarczenie odpowiada beneficjent POPC na podstawie własnych uwarunkowań. Natomiast dla modeli podłączenia MAN / ODN w podstawowym wariancie to na Operatorach Sieci Regionalnych (OSR) spoczywa obowiązek zapewnienia i skonfigurowania urządzać dostępowych (CPE) w sieci szkolnej. W takiej sytuacji po stronie operatora OSE będzie jedynie przygotowanie konfiguracji i przesłanie jej do OSR. W pewnych sytuacjach może się zdarzyć, że będą tam dostawiane urządzenia OSE, należy wtedy zapewnić możliwość ich automatycznej konfiguracji.

Provisioning usług sieciowych i bezpieczeństwa (firewalling) na urządzeniach w szkołach w trakcie podłączenia szkoły do OSE będzie obejmował:

- przygotowanie konfiguracji urządzeń CPE,SW,AP (w przypadku dwóch ostatnich konfiguracja danego typu urządzenia będzie identyczna w każdej szkole (sieci szkolne bazują na takich samych sieciach prywatnych)
- w zależności od możliwości danego modelu CPE
    - przygotowanie konfiguracji w formie pliku do wgrania na urządzenie w celu przekazania do Podwykonawcy wykonującego instalację w szkole (najmniej preferowane i stosowane w ostateczności)
    - automatyczne załadowanie docelowej konfiguracji CPE na urządzenie po nawiązaniu łączności z urządzeniem posiadającym inicjalną konfigurację
    - automatyczne załadowanie docelowej konfiguracji CPE na urządzenie z zastosowaniem mechanizmu ZTP (Zero Touch Provisioning)
- w przypadku urządzeń SW i AP instalowanych w szkołach konfiguracja danego typu urządzenia będzie identyczna dla każdej szkoły (sieci szkolne bazują na identycznych sieciach prywatnych). W szczególności urządzenia SW (które są dostarczane wyłącznie przez Zamawiającego) będą fabrycznie

przygotowywane z inicjalną konfiguracja OSE, natomiast dla urządzeń AP (które mogą być dostarczane przez Zamawiającego lub beneficjenta POPC) będzie przygotowywana inicjalna konfiguracja OSE (per model urządzenia) celem wgrania jej na urządzenie przez Podwykonawcę wykonującego instalację w szkole.

Należy założyć co najmniej, że w trakcie "życia usługi" w ramach procesu zmian usług na urządzeniach CPE będą mogły ulegać zmianie:

- parametry związane z przepustowością łącza
- przydzielone adresy publicznych
- inne elementy konfiguracji (w ramach masowych zmian konfiguracji wspólnej dla wszystkich CPE)

Architektura sieci szkieletowej będzie bardziej skomplikowana, chociaż dużym ułatwieniem będzie zamknięty i dobrze znany katalog urządzeń sieciowych. Przed provisioningiem będzie stało zadanie właściwego skonfigurowania wszystkich urządzeń w sieci szkieletowej. Dostępne będą dwa sposoby provisioningu : poprzez Element Manager'y/systemy zarządzające dedykowane do danych urządzeń lub poprzez bezpośrednią komunikację z urządzeniami.

W przypadku potrzeby realizacji provisioningu przy użyciu Element Manager'a/systemu zarządzającego należy założyć wykorzystanie udokumentowanego API producenta tego systemu.

W przypadku provisioningu urządzeń sieciowych w sieci szkieletowej OSE masowe użycie provisioningu usług sieciowych w szkielecie sieci będzie miało miejsce w trakcie procesu podłączania szkoły do OSE i będzie obejmowało:

- konfigurację parametrów L2
- konfigurację adresacji IPv4 / IPv6
- konfigurację routingu statycznego w stronę szkoły
- konfigurację QoS na łączu

W przypadku provisioningu urządzeń i systemów bezpieczeństwa w sieci szkieletowej OSE również ułatwieniem będzie znany katalog urządzeń i systemów oraz fakt że urządzenia danego producenta będą posiadać dedykowane systemy zarządzania. Realizacja provisioningu usług bezpieczeństwa w szkielecie OSE zakłada użycie udokumentowanego API producenta do systemów i do systemów zarządzania. Provisioning ten jednak komplikuje mnogość tych systemów i operacji które trzeba na nich wykonać w celu konfiguracji usługi.

<u>Proces podłączenia szkoły</u> zakłada

- dodanie adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153)
- dodanie ww. adresu podsieci IP do konfigurowalnych polityk na systemach: ACD, NGFW, SWG, DNS

- inicjacja w systemie SWG generowania raportów bezpieczeństwa dla danej szkoły na podstawie predefiniowanych przez Zamawiającego szablonów (ostatecznie raporty wystawiane na Portalu OSE)
- określenie w systemie SWG harmonogramu generowania raportów dla danej szkoły

Proces zmiany konfiguracji usług zakłada modyfikację parametrów polityk zdefiniowanych per szkoła na poszczególnych systemach, w tym w szczególności choć nie wyłącznie:

- Na systemie ADC:
- Wyjątki definiujące jaki ruch ma nie podlegać dekrypcji SSL, np. na podstawie źródłowych lub docelowych adresów IP, adresów URL zawartych w parametrach certyfikatu (pola: SNI lub CN)
- Na systemie NGFW:
- Tworzenie dedykowanych polityk per szkoła blokujących lub przepuszczających ruch z/do zadanych adresów IP, nawiązywany na określonych portach TCP/UDP
- Włączanie i wyłączanie ruchu mailowego (m. in. protokoły IMAP, POP3) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej
- Na systemie DNS:
- Włączenie / wyłączenie lub zmiana listy kategorii treści przypisanych do polityk określających poziom ochrony użytkowników OSE
- Na systemie SWG:
- Tworzenie dedykowanych polityk per szkoła
- Dodawanie i usuwanie kategorii blokowanych, skonfigurowanych w polityce dla danej szkoły
- Dodawanie i usuwanie zawartości statycznych list, zawierających adresu URL, definiujących wyjątki od polityki blokowania dla danej szkoły
- Włączanie i wyłączanie ruchu mailowego (protokoły HTTP i HTTPS) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej
- Potencjalna zmiany w generowaniu raportów bezpieczeństwa dla danej szkoły na podstawie predefiniowanych przez Zamawiającego szablonów
- Potencjalna zmiana harmonogramu generowania raportów dla danej szkoły

Inwentaryzacja - zbieranie i udostępnianie wszelkich informacji na temat zasobów sieci OSE - zaczynając od informacji technicznych (zarówno o zasobach aktywnych jak i pasywnych, zarówno o zasobach będących własnością Operatora OSE jak i beneficjentów POPC a także o na temat zasobów dzierżawionych jak łącza czy kolokacje) kończąc na informacjach na temat świadczonych usług i ich parametrach. Obiektami w systemie Inwentaryzacji będą co najmniej:

- serwery i systemy w centrach kolokacyjnych,
- łącza dzierżawione w szkielecie, łącza agregacyjne i dostępowe do jednostek oświatowych,

- lokalizacje węzłów szkieletowych (regionalnych i centralnych),
- sprzęt kolokacyjny OSE umiejscowionym w lokalizacjach węzłów,
- sprzęt i systemy sieciowe i bezpieczeństwa zainstalowane w węzłach OSE (dane szczegółowe, np. hardware, software, licencje, serwis itp.),
- lokalizacje jednostek oświatowych (dane teleadresowe, partner serwisowy obsługujący szkołę, operator łącza podłączającego szkołę itp.),
- sprzęt zainstalowany w danej jednostce oświatowej,
- połączenia pomiędzy urządzeniami,
- katalog dostępnych typów urządzeń i producentów,
- katalog dostępnego oprogramowania,
- katalog świadczonych usług (powiązanie z zasobami technicznymi sieci OSE, parametry usług, powiązanie między usługami)

6.1.2. Funkcjonalności obszaru BSS

Systemy obszaru BSS (***który nie jest przedmiotem zamówienia***) możemy zgrupować wokół funkcjonalności zgodnie z poniższym rysunkiem:

Centrum Kontaktu - obszar funkcjonalny odpowiedzialny za wsparcie działań związanych z kontaktem z klientami poprzez wszelkie kanały komunikacyjne takie jak. np. IVR czy Call Center.

Katalog Produktów - obszar funkcjonalny odpowiedzialny za wsparcie wszelkich działań związanych z zarządzaniem produktami, cyklem życia produktów, ofertami, cennikami, monitorowaniem produktów, zapewnieniem odpowiednich zasobów dla produktów.

Zarządzanie Klientami - podstawowy obszar funkcjonalny wspierający realizację wszelkich działań skoncentrowanych na klientach, zarządzaniem informacją o kliencie, jego produktach, umowach, realizacja procesów dostarczania produktów (order management)

Zarządzanie Partnerami - obszar funkcjonalny wspierający zarządzanie relacjami i kontaktami z partnerami takimi jak operatorzy czy partnerzy serwisowi, zarządzanie pracami (workforce management)

Rozliczenia - obszar grupujący funkcjonalności związane z rozliczeniami z klientami i partnerami, rozliczanie produktów, rozliczanie zamówień od partnerów i dostawców, zarządzanie należnościami, windykację

Zarządzanie Dokumentami - obszar funkcjonalny wspierający zarządzanie dokumentami, składowanie, generowanie, udostępnianie, zarządzanie wzorcami dokumentów, archiwizację

Centralny System Raportowy - funkcjonalność odpowiedzialna za generowania wszystkich raportów : finansowych, operacyjnych, SLA, rozliczeniowych, performance'wych a także raportów bezpieczeństwa w szkołach.

Łańcuch Dostaw - obszar funkcjonalny do wsparcia procesów logistycznych i magazynowych

Zarządzanie IT - zarządzanie zasobami informatycznymi przedsiębiorstwa, środowiskami IT, procesami rozwoju i utrzymania systemów

Zarządzanie Przedsiębiorstwem - zarządzanie przedsiębiorstwem, prowadzenie finansów i rozliczeń przedsiębiorstwa, zarządzanie wiedzą i kapitałem ludzkim

Silnik Procesów Biznesowych - komponent wspierający realizację procesów we wszystkich obszarach funkcjonalnych

6.2. Warstwa infrastruktury

6.2.1. Wstęp

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Wymagane jest dostarczenie infrastruktury aplikacyjno-sprzętowej, która będzie się składać na środowisko uruchomieniowe oraz dodatkowo będzie dostarczała zasobów dla środowisk testowych. Głównym celem istnienia zwirtualizowanej infrastruktury obliczeniowej jest zapewnienie zasobów dla:

- systemów OSS
- systemów NASK OSE (takich jak. np. Portal OSE czy inne systemy BSS OSE)
- przechowywanie danych blokowych i obiektowych
- wirtualnej sieci – SDN
- backupu środowiska i systemu odtwarzania po awarii

- systemu zarządzania tożsamością
- systemu zarządzania kolokacjami OSE
- systemów zarządzania, monitorowania chmury i opcjonalnie automatyzacji
- systemu klasy SIEM (Security Information and Event)
- systemu Retencji Logów
- systemu Contact Center
- systemów wspierające infrastrukturę OSE (Element Manangery, systemy zarządzania itp.)

Pozostałe wymagania dla dostawcy przy projektowaniu środowiska:

- zapewnienie odpowiedniej mocy obliczeniowej i powierzchni do składowania danych dla powyższych systemów jak również dla systemów pomocniczych;
- wysoka skalowalność rozwiązania i efektywne wykorzystanie zasobów sprzętowych poprzez implementację środowiska na platformie zwirtualizowanej;
- zapewnienie wysokiej dostępności, integralności i poufności informacji przechowywanych w środowisku;
- efektywne przechowywanie i analiza logów pochodzących z różnych źródeł
- automatyzacja i efektywne wykonywanie kopii zapasowych zapewniających możliwość odtworzenia systemu oraz bezstratnego odtworzenia danych i dokumentów na wypadek katastrofy (Disaster Recovery Plan) ;
- możliwości zapewnienia niezmienności przechowywanych danych;
- uproszczenie zarządzania infrastrukturą, przechowywaniem danych, bezpieczeństwem i wprowadzaniem zmian w infrastrukturze;
- zapewnienie odpowiedniej ilości licencji na oprogramowanie w infrastrukturze.

Założeniem projektu architektury jest maksymalna integracja systemów w ramach platformy i uproszczenie procesów dokonywania zmian w systemach. Zbudowanie środowiska które zminimalizuje ilości administratorów potrzebnych do utrzymania go. Służyć temu ma uruchomienie wszystkich możliwych elementów odpowiedzialnych za obsługę, nadzorowanie i zarządzanie infrastrukturą w formie maszyn wirtualnych na zasobach chmury, a także ujednolicenie technologii używanej do budowy środowiska.

6.2.2. Założenia techniczne

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Wymagana jest architektura zbudowana w modelu chmury prywatnej. Architektura musi zakładać, że infrastruktura obliczeniowa ma być rozciągniętą pomiędzy dwoma centralnymi aktywnymi ośrodkami przetwarzania danych (**OPD**) – OPD1 i OPD2, trzeci centralny ośrodek (OPD3) będzie pełnił rolę świadka oraz miejsca przechowywania kopii zapasowych wraz z archiwum. Architektura zakłada również 16 regionalnych ośrodków przetwarzania danych z których każdy będzie podłączony do centralnych OPD.

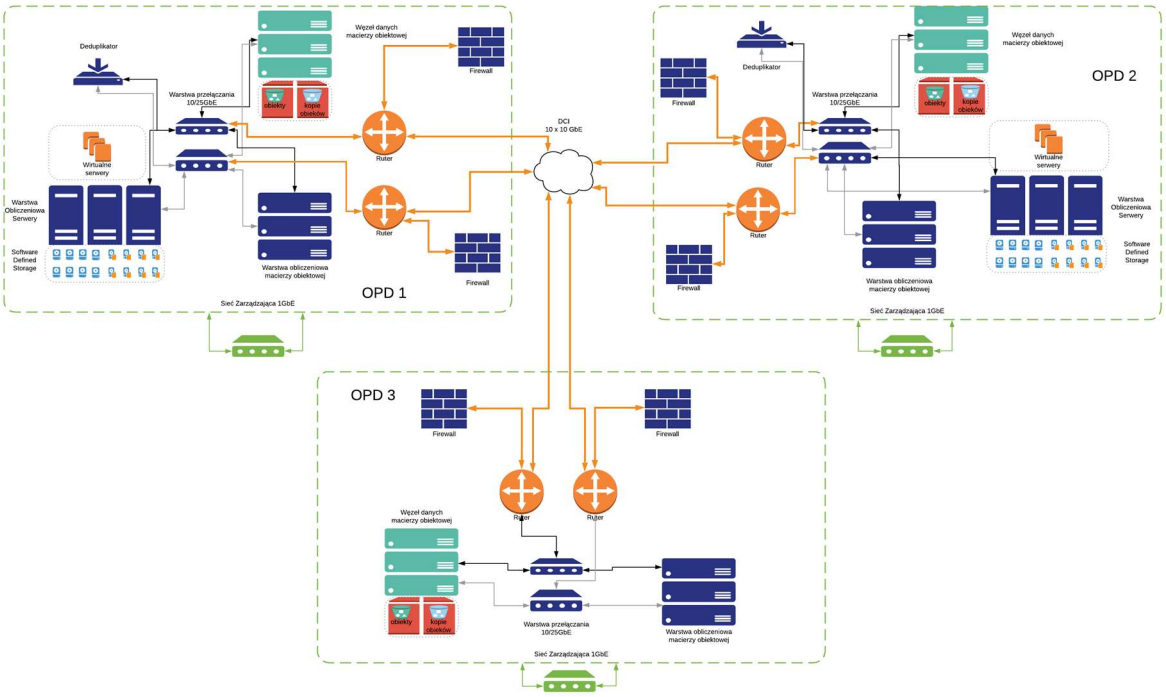
Środowiska w regionalnych ośrodkach będą różnej wielkości, ich rozmiar będzie dostosowany do potrzeb systemów SIEM i ściśle uzależniony od ilości logów zbieranych w danym regionie. Trzy regionalne ośrodki danych będą mieściły się w tych samych centrach danych co centralne ośrodki przetwarzania danych. W celu zapewnienia odpowiedniej ciągłości działania, **OPD** będą znacznie oddalone od siebie w celu zminimalizowania wpływu zdarzeń losowych na ciągłość działania systemu. Pomiędzy wybranymi centrami będzie dostępna wydajna sieć umożliwiająca synchronizację i replikację krytycznych danych.

Wymagana jest taka architektura rozwiązania która zminimalizuje nakłady pracy ludzkiej związanej z procesem utrzymania i integracji stosu obliczeniowego, sieciowego, pamięci masowych oraz wirtualizacji. Wymaga się użycia rozwiązań pozwalających zautomatyzować zarządzanie infrastrukturą. Poniżej zebrano główne założenia techniczne infrastruktury chmury obliczeniowej, które dostawca musi spełnić w kontekście infrastruktury obliczeniowej:

1. Infrastruktura chmury obliczeniowej ma być jak najbardziej zintegrowana i prosta w zarządzaniu oraz odporna na awarie, musi obejmować zarówno warstwę sprzętową, jak i część niezbędnego oprogramowania.
2. Możliwe wszystkie system muszą być uruchamiane jako maszyny wirtualne.
3. Infrastruktura zostanie tak zaplanowana, aby zapewnić pełną ciągłość działania w przypadku całkowitej awarii jednego z dwóch głównych węzłów OPD1 i OPD2.
4. Wszystkie typy danych będą chronione poziomem nadmiarowości min. N+1
5. Wdrożone rozwiązanie informatyczne musi pracować w architekturze redundantnej. Replikacja musi być zrealizowana w taki sposób, dwa główne ośrodki (OPD1 i OPD2) mogły korzystać z systemów storage na których uruchomione będą usługi produkcyjne - czyli np. połowa zasobów dyskowych musi być dostępna w każdym OPD, reszta musi być wykorzystana na replikację.
6. Architektura rozwiązania musi umożliwiać przełączenie przetwarzania pomiędzy węzłami przetwarzania danych – z jednego głównego OPD do drugiego i odwrotnie.
7. Rozwiązanie infrastruktury chmury obliczeniowej w ramach głównych OPD musi posiadać funkcjonalność, która pozwala na zautomatyzowany failover oraz failback infrastruktury maszyn wirtualnych w przypadku wystąpienia awarii jednego z głównych OPD.
8. *Wdrażane rozwiązanie informatyczne chmury obliczeniowej musi umożliwiać ochronę przetwarzanych w nim danych, w tym gwarantować ich:*
    - *rozliczalność - zapewniać możliwość rozliczenia osoby, która uzyskała dostęp do informacji na podstawie mechanizmów identyfikacji i uwierzytelnienia*
    - *ochronę przed nieautoryzowanymi, nieprzewidywalnymi, niezamierzonymi modyfikacjami informacji,*
    - *ochronę poufność informacji np. danych osobowych,*
    - *zachowanie spójność danych,*
    - *zapewniać dostęp do informacji.*
9. Rozwiązanie musi wspierać proces automatycznego logowania (SSO) jak i manualnego (za pomocą loginu i hasła).

10. Rozwiązanie musi posiadać mechanizmy kontroli dostępu, możliwość budowy zasad oraz polityk w zakresie haseł.
11. Planowane do wdrożenia rozwiązanie informatyczne chmury obliczeniowej musi wspierać architekturę, która zapewni, że awaria jednego elementu rozwiązania informatycznego chmury obliczeniowej dostępnego w ramach pojedynczego OPD nie powoduje niedostępności usługi/rozwiązania informatycznego chmury obliczeniowej, a jedynie spadek jej wydajności. Warunek ten nie musi zostać spełniony, jeżeli awarii ulega ostatni element danego typu.
12. Przyjęto, że każdy system programowy i możliwie każdy sprzętowy wykorzystywany w chmurze musi posiadać natywne API, lub umożliwiać automatyzację procesów m.in. poprzez integrację z systemami OSS.
13. Dostęp do rozwiązania infrastruktury obliczeniowej dla administratorów musi być możliwy m.in. za pośrednictwem przeglądarki internetowej (np. połączenie szyfrowane SSL).
14. Architektura rozwiązania informatycznego chmury obliczeniowej musi umożliwiać tworzenie klastra wysokiej dostępności (HA) w obrębie OPD oraz pozwalać na wdrożenie mechanizmu niezawodności (DR) pomiędzy OPD 1 i 2.

Modelowa infrastruktura chmury obliczeniowej jest przedstawiona na poniższym schemacie. Poszczególne części opisane są w kolejnych akapitach.



6.2.3. Ośrodki przetwarzania danych

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Wymaga się dostarczenia Infrastruktury opartej o trzy główne ośrodki przetwarzania danych, zrealizowanej jako klastry, jak i 16 wysoko dostępnych ośrodków regionalnych.

Planowana infrastruktura obliczeniowa ma być rozdzielona na dwa aktywne ośrodki przetwarzania danych (OPD1 i OPD2). W każdym z tych ośrodków będzie dostępna równoważna infrastruktura sieciowa. Odpowiednia przepustowość zarówno do WAN, jak i sieci pomiędzy OPD będą zapewnione przez OSE. OPD1 i OPD2 będą miejscem przechowywania kopii zapasowych środowiska na potrzeby zapewnienia ciągłości działania po awarii OPD. W szczególności:

- kopie zapasowe maszyn wirtualnych wraz z ich konfiguracją i obrazami wraz z archiwum,
- konfigurację wirtualnych centrów danych zawierającą konfigurację sieci, storage-u, automatyzację, logi, konfigurację wirtualizatorów etc..
- kopie zapasowe plików i obiektów,
- backup baz danych aplikacji wraz z katalogami użytkowników i ich uprawnieniami,
- backup systemów zarządzających, monitorujących, raportujących, bezpieczeństwa, konfigurację urządzeń fizycznych (przełączników, ruterów, firewall-i)

Trzeci ośrodek przetwarzania danych (OPD3) nie będzie posiadał infrastruktury obliczeniowej, SDS jak również SDN. Ośrodek ten będzie posiadał część obiektowego systemu przetwarzania danych.

Dla zapewnienia efektywnego, bezpiecznego, a także szybkiego przesyłania i składowania danych pomiędzy ośrodkami, dostawca powinien wykorzystać systemy zapewniające mechanizmy deduplikacji, kompresji i szyfrowania danych.

System przechowywania danych blokowych musi znajdować się w OPD1 i OPD2 i być wykorzystywany możliwie tylko do udostępniania danych dla systemów wirtualizacji.
Dane plikowe (Plik) i blokowe (Blok) z OPD1 będą replikowane do OPD2 a z OPD2 do OPD1.
Infrastruktura serwerowa musi zostać zaprojektowana w taki sposób aby zapewnić działanie systemu przy awarii jednego fizycznego serwera w klastrze (nadmiarowość N+1), jak również w przypadku awarii całego ośrodka OPD (odtwarzanie po awarii – Disaster Recovery).
Dla zapewnienia większej elastyczności, odporności na awarie sprzętu, lepszego wykorzystania zasobów serwerowych, a także automatyzację zadań administracyjnych należy zastosować technologie wirtualizacji zasobów obliczeniowych i sieciowych, jak również wirtualizacji zasobów przechowujących dane.

Infrastruktura obliczeniowa musi zostać zrealizowana jako zestaw klastrów lokalnych w obu centralnych OPD (OPD1 i OPD2). Rozwiązanie musi posiadać mechanizmy wysokiej dostępności (HA) wbudowane w oprogramowanie zarządzające środowiskiem wirtualnym.

We wszystkich centralnych ośrodkach OPD musi zostać rozproszony system archiwum opartego o obiektowy system przechowywania plików (Obiekt + WORM), do którego przesyłane będą dane przeznaczone do składowania długoterminowego. Dane archiwalne będą składowane na tym samym urządzeniu, które obsługuje dane aktywne. Separacja powinna zostać wykonana za pomocą

mechanizmów programowych. Dodatkowo dla zapewnienia wysokiego bezpieczeństwa danych archiwalnych, dane te powinny mieć możliwość zabezpieczenia technologią WORM - Write once read many, która pozwoli na zapisanie informacji na urządzeniu, ale nie pozwoli jej usunąć lub zmodyfikować.

6.2.4. Skalowalność systemu

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Budowane środowisko powinno być stworzone na platformie sprzętowej o wydajności i poziomie bezpieczeństwa odpowiednim dla powyższych założeń. Istotne jest aby środowisko było możliwie uniwersalne, otwarte na potencjalne zmiany, przy jednoczesnym zachowaniu wsparcia wielu technologii. W warstwie fizycznej należy wyróżnić komponenty:

- komponenty infrastruktury sieciowej,
- serwery zapewniające moc obliczeniową chmury i bezpieczne przechowywanie danych,
- zasoby storage pozwalające na bezpieczne przechowywanie danych,
- systemy bezpieczeństwa oraz systemy monitorowania i zarządzania infrastrukturą.

Wymagane jest, aby budowa infrastruktury została oparta o tzw. „building blocks" w kontekście całości architektury, dotyczy to również sieci. Sieć powinna być zaprojektowana taki sposób, aby wymagana rozbudowa zasobów serwerowych lub storage była łatwo policzalna i nie wymagała ciągłych zmian w rdzeniu sieci. Narzędzia oraz procesy zastosowane w rozwiązaniu, służące do zarządzania infrastrukturą, powinny działać w sposób całkowicie zintegrowany i holistyczny. Rozwiązanie powinno posiadać budowę modularną, i charakteryzować się dużą elastyczność w tworzeniu połączeń konfiguracyjnych poszczególnych komponentów. Poszczególne elementy systemu powinny być zwirtualizowane, przy zachowaniu przez infrastrukturę fizyczną wymaganej zdolności do przeprowadzania dynamicznych zmian przy zapewnieniu wysokiej niezawodności. Konstrukcji rozwiązania powinna umożliwiać eliminowanie jednorazowych prac projektowych i łatwą i szybką wymianę uszkodzonych modułów wymienić bez konieczności wyłączania całego systemu. Rozwiązania ma łączyć w sobie elastyczność systemów ogólnego przeznaczenia i środowisk przetwarzania w chmurze oraz prostotę dedykowanego urządzenia (ew. bloku). Oznaczać się możliwością szybkiego tworzenia, wdrażania i zmian pod kątem aplikacji za pomocą sprawdzonych wzorców. Aktualizacje wersji wszystkich komponentów powinny być realizowane możliwie dla całego modułu i w prosty sposób.

Wymagane jest aby środowiska w regionalnych centrach danych zapewniały wysoką dostępność na wypadek awarii jednego serwera.

6.2.5. Szczegółowe wymagania na infrastrukturę docelową (poza zakresem postępowania)

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Opis metryki

Nazwa obszaru	Tytuł
Platforma wirtualizacyjna – wymagania funkcjonalne	Wirtualizacja mocy obliczeniowej
	Moduł wirtualizacji przestrzeni dyskowej
	Moduł wirtualizacji funkcji sieciowych
	Moduł monitorowania i zarządzania pojemnością i efektywnością platformy
	Moduł monitoringu środowiska sieciowego
	Moduł zarządzania cyklem życia platformy
Opis infrastruktury wirtualizacyjnej	Infrastruktura dla środowiska produkcyjnego
	Wymagania ilościowe dla warstwy oprogramowania
	Wymagania ogólne dla warstwy sprzętowej dla serwerów w węzłach centralnych
	Wymagania ogólne dla warstwy sprzętowej dla serwerów w węzłach regionalnych
Obiektowy system składowania danych	Ogólne wymagania techniczne dla obiektowego systemu składowania danych
	Wymagania dotyczące skalowalności, budowy i architektury obiektowego systemu składowania dokumentów
	Szczegółowe wymagania funkcjonalne dla obiektowego systemu składowania danych
Backup i Archiwizacja	Deduplikatory
	Wymagane funkcjonalności oprogramowania do zabezpieczania danych
	Wymagania dotyczące backupu serwerów (Data Center)
	Wymagania funkcjonalności – dotyczących monitorowania, raportowania oraz przeszukiwania backupów
	Wymagania funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk wirtualnych

6.2.5.1. Platforma wirtualizacyjna - wymagania funkcjonalne

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Wirtualizacja mocy obliczeniowej

Oferowana równoważna warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki:

Treść wymagania
Wirtualizator, który wspiera rozwiązanie Microsoft® Clustering Services - Cluster uruchomiony na maszynach wirtualnych z systemem operacyjnym Microsoft® Windows ze wsparciem dla failover clustering, SQL clustering, i

Treść wymagania
AlwaysOn Availability Groups. Wsparcie takie musi być udokumentowane na ogólnodostępnejstronie producenta oprogramowania.
Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z przedziału 1 do 128 procesorowych
Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM
Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych
Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji
Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root
Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii
Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją.
Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury
Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych
System musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w wirtualnych maszynach
Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn
Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana
Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 60 TB
Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu
Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji sieci (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi

Treść wymagania
odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe)
Wirtualizator musi wspierać TPM 2.0 oznacza to min. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, że wirtualizator uruchomił w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego
Wirtualizator musi mieć włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Windows 10 oraz Windows Server 2016.
Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym wszystkie standardowe funkcjonalności wirtualizatora tj. wysoka dostępność czy przenoszenie maszyn wirtualnych bez ich wyłączania pomiędzy różnymi serwerami fizycznymi działa prawidłowo. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedzialny za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora
UEFI virtual BIOS – wirtualne maszyny uruchomione na systemie do wirtualizacji z wykorzystaniem technologii - Unified Extended Firmware Interface (UEFI)
Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów
Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K
Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej
Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi
System musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego oraz wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervizor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany)

Moduł wirtualizacji przestrzeni dyskowej

Treść wymagania
Oferowane rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD
Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji odczytu / zapisu (Read/Write IO) po stronie serwerów fizycznych
Rozwiązanie musi posiadać możliwość budowania własnych schematów konfiguracji dyskowej dla przestrzeni akcelerującej operacje Read/Write (cache) oraz dla przestrzeni budującej pojemność. Wymagana jest możliwość zmiany konfiguracji zarówno pod kątem dostępności, wydajności jak i pojemności "w locie"
Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania

Treść wymagania
Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z konsolą zarządzającą platformą wirtualizacyjną
Rozwiązanie musi zapewniać obsługiwanie dysków wirtualnych maszyn do rozmiaru min. 60TB,
Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy oprogramowania i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych, aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: dysk cache'ujący, dysk pojemnościowy
Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej zarówno w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
Rozwiązanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek niedostępności danych lub awarii sprzętowej w taki sposób, aby zabezpieczane dane można było rozlokować między różnymi szafami rack/chassis
Rozwiązanie musi zapewniać wsparcie dla rozwiązań sprzętowych różnych producentów i posiadać oficjalną stronę producenta na której znajduje się lista wspieranych lub rekomendowanych konfiguracji. Rozwiązanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych serwerach wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawce/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery)
Rozwiązanie musi zapewniać możliwość rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej
Rozwiązanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych
Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (np.: sfałszowaniem) za pomocą weryfikacji sum kontrolnych
Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache'owania" operacji odczytu / zapisu (Read/Write IO)
Oprogramowanie do wirtualizacji podsystemu dyskowego (SDS) musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja), wirtualizacji serwerów (Hypervizor) oraz wirtualizacji sieci IP (SDN) na wszystkich poziomach wsparcia
Rozwiązanie musi mieć możliwość konfiguracji domen niezawodnościowych. Oznacza to możliwość zgrupowania serwerów fizycznych w domenę, a następnie wymuszenie, aby dane po względem niezawodności posiadały swoją kopię na innej domenie, np. serwery znajdują się w kilku szafach rack, na bazie szafy rack tworzona jest domena niezawodnościowa
Rozwiązanie musi wspierać co najmniej 12 węzłów w jednym logicznym klastrze
Rozwiązanie powinno wspierać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych. Wymagane wsparcie dla min.: technologii deduplikacji oraz technologii implementującej mechanizmy znane z RAID5 i RAID6 za pomocą oprogramowania

Treść wymagania
Oferowane urządzenia/oprogramowanie ma pochodzić z bieżącej linii produkcyjnej, ma być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla niego ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowane rozwiązania posiadają nowszą wersję, następcę oprogramowania – należy zaoferować rozwiązanie najnowsze
Jeżeli do poprawnego działania dostarczanego modułu niezbędne jest wykorzystanie dodatkowych komponentów/licencji, nie ujętych w szczegółowym opisie wymagań, to należy je przewidzieć i dodatkowo dostarczyć w ramach proponowanej oferty w ramach danego

Moduł wirtualizacji funkcji sieciowych

Treść wymagania
Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) oparciu o środowiska wirtualne.
Oferowane oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych.
Rozwiązanie musi posiadać funkcję wirtualnego przełącznika, umożliwiającego tworzenie logicznych segmentów sieci L2. Wirtualny przełącznik musi być wspierany bezpośrednio przez producenta wirtualizatora serwerów.
Rozwiązanie musi posiadać funkcję wirtualnego routera, zapewniającego funkcję bramy domyślnej dla środowiska maszyn wirtualnych.
Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN.
Oferowane oprogramowanie musi zapewnić funkcjonalność łączenia (bridging) środowiska zwirtualizowanego oraz niezwirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów.
Rozwiązanie musi umożliwiać funkcję translacji adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego (DNAT)
Rozwiązanie musi posiadać funkcję dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego
Oferowane oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API
Oprogramowanie do wirtualizacji sieci (SDN) musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja), wirtualizacji serwerów (Hypervizor) na wszystkich poziomach wsparcia.
Oferowane oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie hypervisora/wirtualnego interfejsu sieciowego, dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych przełączników lub firewalli
Możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci i na tym samym fizycznym serwerze
Rozwiązanie musi umożliwiać wykorzystanie dynamicznych obiektów do tworzenia reguł polityk bezpieczeństwa: Wymagane min.: nazwa maszyny wirtualnej, nazwa switcha wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny
Rozwiązanie powinno oferować w ramach platformy, możliwość terminowania tuneli IPSeC site-to-site

Treść wymagania
Rozwiązanie powinno umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu antywirus/antymalware w postaci bez agentowej, tj. instalowane na wirtualizatorze serwerów, ale poza wirtualną maszyną
Rozwiązanie musi umożliwiać przekierowanie wybranego ruchu L2 do rozwiązania firm trzecich z obszaru bezpieczeństwa
Oferowane oprogramowanie musi zapewnić funkcjonalność rozkładania/równoważenia ruchu – tj. funkcja wirtualny Load Balancer musi być realizowana i w pełni zintegrowana z platformą do wirtualizacji sieci.

Moduł monitorowania i zarządzania pojemnością i efektywnością platformy

Treść wymagania
Wymagania ogólne
Rozwiązanie musi zapewniać konsolę graficzną za pomocą, której będzie możliwość automatycznej instalacji i konfiguracją następujących modułów: • Wirtualizacja mocy obliczeniowej • Wirtualizacji funkcji sieciowych • Wirtualizacji przestrzeni dyskowej • Monitorowania i zarządzania pojemnością i efektywnością platformy
Rozwiązanie musi zapewniać centralną konsolę graficzną za pomocą, której będzie możliwość automatycznego tworzenia, modyfikowania, usuwania i konfigurowania wirtualnych maszyn
Rozwiązanie musi zapewniać centralną konsolę graficzną za pomocą, której będzie możliwość wymiany uszkodzonego serwera fizycznego
Rozwiązanie musi zapewniać centralną konsolę graficzną za pomocą, której będzie możliwość dodania dodatkowego serwera fizycznego w celu zwiększenia pojemności
Rozwiązanie musi posiadać możliwość definiowania sieci wirtualnych, które łączą maszyny wirtualne w ramach zarządzanej platformy
Administrator rozwiązania musi posiadać możliwość definiowania sieci wewnętrznych jak i sieci zewnętrznych połączonych do sieci fizycznej - pozwalającej na komunikację np. do Internetu za pomocą np. NAT
Rozwiązanie niezależne od producenta sprzętu, możliwy provisioning wirtualizatora systemów operacyjnych na tzw. bare-metal ze wsparciem dla min. takich producentów jak: Dell, IBM, Huawei, Cisco etc..
Posiadanie wsparcia dla platform: Hyper-V (SCVMM), VMware
Rozwiązanie musi umożliwiać rezerwację zasobów fizycznych dla wybranych grup użytkowników oraz pełną kontrolę tych zasobów w obrębie wskazanej grupy użytkowników
Rozwiązanie musi mieć możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych i określania dla nich zasobów fizycznych

Treść wymagania
Rozwiązanie musi się integrować z innymi systemami zewnętrznymi typu: CMDB, DNS, IPAM, Load Balancer, Servcie Desk, Monitoring, Puppet, Chef jako plug-iny lub napisanych od początku w języku programowania. Efektem powyższej integracji musi być w pełni automatyczny proces tworzenia i zarządzania usługą niewymagający czynności ręcznych
Rozwiązanie musi posiadać możliwość granularnego zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej roli, opartego na rolach: np.: Tenant Admin, Service Architect, Network Architect
Rozwiązanie musi dostarczać mechanizmy monitorowania statusów zdarzeń, notyfikacji o tych zdarzeniach, umożliwiać śledzenie i kontrolę zmian w konfiguracji wszystkich usług, za pomocą min. powiadomień e-mail
Oferowane oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API
Rozwiązanie musi umożliwiać zunifikowane mechanizmy uaktualnienia całego stosu oprogramowania wirtualizującego oraz definiowania zakresu tych aktualizacji
Wymagania szczegółowe
Platforma będzie w stanie zbierać informacji na temat wydajności pod kątem zarządzania pojemnością
Platforma musi w sposób inteligentny przewidywać trendy związane z pojemnością środowiska
Platforma musi posiadać moduł odpowiedzialny za analizę środowiska pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, HDD)
Platforma będzie w stanie tworzyć unikalne/dedykowane Data Center, tzw. Będzie możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektach. Obiekty mogą pochodzić z różnych Data Center objętych tym rozwiązaniem.
Platforma będzie w stanie tworzyć unikalne/dedykowane profile pojemności, tzn. będzie możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektach
Platforma będzie w stanie monitorować infrastrukturę SDS
Platforma w obrębie monitorowania będzie posiadała rozwiązanie generowania alertów na podstawie szeregu anomalii i symptomów, a nie pojedynczych monitorowanych metryk
Platforma będzie dostarczała informacji na temat rekomendowanych działań mających na celu utrzymanie środowiska wirtualnego sprawnego
Platforma będzie w stanie dostarczać analizę głównego problemu (root-cause) oraz rekomendacji z nimi związane
Platforma powinna posiadać wbudowane integracje z zewnętrznym kolektorem logów i zdarzeń
System musi wizualizować online obciążenie środowiska wirtualnego wraz z tzw. funkcjonalnością „drill down”
System musi posiadać funkcjonalność graficznej prezentacji wyników (dashboard)
System musi posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich wytworzenia
System powinien automatycznie tworzyć linie bazowe określające typowe zachowanie elementów systemu w danym czasie

Treść wymagania
System powinien dokonywać predykcji wykorzystania zasobów maszyn wirtualnych na podstawie analiz zebranych danych
System powinien umożliwiać przeglądanie linii trendu monitorowanych parametrów
System musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń fizycznych jak i wirtualnych
System musi umożliwiać monitorowanie w czasie rzeczywistym (przeglądane informacje w trybie rzeczywistym - maksymalne dopuszczalne opóźnienie nie większe niż 5 min.)
System musi zbierać oraz prezentować w formie wykresów oraz tabelaryczno-tekstowej zbiorczo oraz osobno dla każdego OS aktualne i historyczne dane dotyczące utylizacji CPU, RAM, HDD oraz interfejsów sieciowych
System musi umożliwiać przeglądanie wszystkich zbieranych statystyk w dowolnie wybranym zakresie czasu w postaci wykresów
System powinien umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, Ethernet, RAM, HDD)
Możliwość uruchamiania ręcznego automatycznych zadań (w tym modyfikujących parametry maszyn wirtualnych) w zależności od aktualnych alarmów, ostrzeżeń, powiadomień, obciążenia
Alarmowanie sytuacji nietypowych (system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o np. nie normalnym w tym dniu zwiększonym obciążeniu elementu platformy wirtualnej)
Możliwość dowolnego konfigurowania alertów w środowisku dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie),
System umożliwia definiowanie alertów związanych z: zarządzaniem pojemnością; zarządzeniem wydajnością; anomaliami w środowisku ; zarządzanie dostępnością
Narzędzie musi mieć możliwość przypisania alertu do administratora/operatora rozwiązującego problem
Rozwiązanie musi mieć możliwość realizacji funkcji automatycznego lub półautomatycznego równoważenia obciążenia serwerów fizycznych w obrębie klastra logicznego.
Rozwiązanie musi integrować się z częścią wirtualizującą zarówno w warstwie przetwarzania (Hypervisor) jak i sieci (SDN)
Rozwiązanie musi posiadać możliwość zastosowania dodatkowych adapterów umożliwiających integrację w systemami monitorującymi infrastrukturę firm trzecich
Rozwiązanie musi posiadać możliwość zastosowania dodatkowych paczek monitorujących dla rozwiązań firm trzecich
Rozwiązanie musi umożliwiać konfiguracje trybu wysokiej dostępności HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu
Rozwiązanie musi posiadać możliwość zastosowania dodatkowych adapterów odpowiadających za monitorowanie systemów zewnętrznych takie jak: macierze dyskowe, chmury obliczeniowe, serwery fizyczne, przełączniki LAN/SAN i inne, umożliwiając tym samym wykorzystanie dedykowanych mechanizmów monitorujących określone komponenty
Rozwiązanie musi umożliwiać elastyczne dostosowanie wyglądu interfejsu użytkownika w zależności od indywidualnych potrzeb konkretnego użytkownika

Treść wymagania
Rozwiązanie musi posiadać funkcję tzw. konfiguratora własnych raportów, który musi umożliwiać tworzenie zaawansowanych raportów dotyczących wszystkich aspektów funkcjonowania platformy sprzętowo-programowej
Rozwiązanie musi posiadać funkcję tzw. konfiguratora własnych widoków zgromadzonych danych, który musi umożliwiać tworzenie zaawansowanych widoków dotyczących wszystkich monitorowanych metryk
Rozwiązanie musi posiadać funkcję tzw. konfiguratora własnych pulpitów kierowniczych (tzw. dashboard) na podstawie zgromadzonych danych w rozwiązaniu. Za pomocą tej funkcjonalności rozwiązanie musi umożliwiać tworzenie zaawansowanych pulpitów kierowniczych (dashborad)
Rozwiązanie musi posiadać funkcjonalność monitorowania systemów operacyjnych (np. Windows, Linux) za pomocą zainstalowanego agenta w monitorowanym systemie operacyjnym
Moduł monitoringu środowiska sieciowego
Rozwiązanie musi mieć możliwość analizowania przepływów sieciowych w warstwie sieciowej wirtualizacji
Rozwiązanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego oraz fizycznego
Rozwiązanie musi mieć możliwość wykorzystania wbudowanego kolektora w celach dalszej analizy ruchu
Rozwiązanie musi mieć możliwość wizualizacji ścieżki logicznej i przejść w relacji vm-vm, wskazanie komponentów sieciowych w topologii logicznej i fizycznej - przełączników, routerów, firewalli oraz połączeń między nimi z uwzględnieniem komponentów wirtualnych
Rozwiązanie musi mieć możliwość informowania i wizualizacji połączeń maszyn wirtualnych do zasobów dyskowych, połączenia do hosta (wirtualizatora) i wyjścia na zewnątrz do sieci fizycznej
Rozwiązanie musi posiadać funkcjonalność API

Moduł zarządzania cyklem życia platformy

Oprogramowanie musi spełniać poniższe warunki:

Treść wymagania
Konsola do automatycznej instalacji i/lub konfiguracji oprogramowania do wirtualizacji serwerów fizycznych, macierzy dyskowej typu SDS na serwerach, wirtualizacji sieci typu SDN wraz z mechanizmami bezpieczeństwa. Dodatkowo rozwiązanie musi być w stanie aktualizować wszystkie komponenty oprogramowania.
Rozwiązanie musi posiadać narzędzia skracające proces wdrażania stosu oprogramowania infrastrukturalnego do wirtualizacji serwerów x86, wirtualizacji sieci oraz tworzenia macierzy dyskowej typu SDS poprzez zautomatyzowaną instalację oprogramowania, tworzenie klastrów obliczeniowych (w tym na potrzeby klastrów obliczeniowych pod serwery wirtualne), zarządzania i wdrażanie maszyn wirtualnych infrastruktury
Rozwiązanie musi posiadać narzędzia automatyzujące konfigurację następujących elementów: serwerów x86, fizycznej sieci w tym VLAN, przestrzeni dyskowej, itp.
Rozwiązanie musi umożliwiać zunifikowane mechanizmy uaktualnienia całego stosu oprogramowania wirtualizującego oraz definiowania harmonogramu i zakresu tych aktualizacji

6.2.5.2. Opis infrastruktury wirtualizacyjnej

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Infrastruktura dla środowiska produkcyjnego

Treść wymagania
Środowisko produkcyjne w centralnych ośrodkach przetwarzania danych poza infrastrukturą przeznaczona na systemy OSS, powinno dodatkowo sumarycznie posiadać: • min. 2100 vCPU (vCPU = Ilość fizyczna procesorów x Ilość rdzeni fizycznych w procesorze (bez HT)) • min. 8270 GB RAM • min. 480 TB przestrzeni użytkowej pamięci blokowej (SDS) na platformie All Flash (przed deduplikacją i kompresją). • min. 600 TB przestrzeni użytkowej pamieć obiektowej (po uwzględnieniu Erasure Coding) zainstalowanej w trzech ośrodkach, system odporny na awarie jednego ośrodka. System pamięci obiektowej wdrożony musi być w trzech centralnych ośrodkach przetwarzania danych.
Cała infrastruktura obliczeniowa w centralnym ośrodku przetwarzania danych nie powinna zajmować więcej przestrzeni w szafach rakowych niż 138 U, jak również nie może zużywać więcej mocy niż 88kW. Wymogi te dotyczą dwóch centralnych ośrodków przetwarzania danych i każdy z nich może pomieścić nie więcej niż 138 U i nie może zużyć mocy większej niż 88kW.
Cała infrastruktura obliczeniowa w trzecim centralnym ośrodku przetwarzania danych nie powinna zajmować więcej przestrzeni w szafach rakowych niż 30 U, jak również nie może zużywać więcej mocy niż 9kW.
Każdy regionalny ośrodek przetwarzania danych powinien składać się z min. dwóch serwerów wraz z dyskami tworząc klaster wysokiej dostępności HA w obszarze przetwarzania (CPU) jak i pamięci masowej (SDS).Środowisko produkcyjne w szesnastu regionalnych ośrodkach przetwarzania danych powinno sumarycznie posiadać: • min. 520 vCPU (bez HT) • min. 2200 GB RAM • min. 96 TB przestrzeni użytkowej pamięci blokowej (SDS).
Cała infrastruktura obliczeniowa w każdym z regionalnych ośrodków przetwarzania danych nie powinna zajmować więcej przestrzeni w szafach rakowych niż 6 U, jak również nie może zużywać więcej mocy niż 4,5 kW.

Wymagania ilościowe warstwy oprogramowania

Treść wymagania
Licencje dla centralnych ośrodków przetwarzania danych. Wymagane jest dostarczenie licencji zintegrowanej platformy wirtualizacyjnej pozwalającej na jej instalację na wszystkich dostarczonych serwerach i dla wszystkich maszyn wirtualnych działających na platformie dla centralnych ośrodków przetwarzania danych.

Treść wymagania
Moduły które muszą być dostarczone w ramach zintegrowanej platformy dla centralnych ośrodków przetwarzania danych: • Moduł wirtualizacji mocy obliczeniowej • Moduł wirtualizacji przestrzeni dyskowej • Moduł wirtualizacji funkcji sieciowych • Moduł monitorowania i zarządzania pojemnością i efektywnością platformy • Moduł zarządzania cyklem życia platformy w warstwie sprzętowej
Licencje dla regionalnych ośrodków przetwarzania danych. Wymagane jest dostarczenie licencji zintegrowanej platformy wirtualizacyjnej pozwalającej na jej instalację na min. 64 CPU lub wszystkich maszyn wirtualnych działających na platformie dla regionalnych ośrodków przetwarzania danych. Wymagane jest dostarczenie oprogramowania tego samego producenta zintegrowanej platformy wirtualizacyjnej dla regionalnych ośrodków przetwarzania danych jak w centralnych ośrodkach przetwarzania danych. Moduły które muszą być dostarczone w ramach zintegrowanej platformy dla regionalnych ośrodków przetwarzania danych: • Moduł wirtualizacji mocy obliczeniowej • Moduł wirtualizacji przestrzeni dyskowej

Wymagania ogólne dla warstwy sprzętowej dla serwerów w węzłach centralnych

Dostawca powinien zapewnić serwery spełniające poniższe wymagania.

Obszar	Treść wymagania
Ogólne	Wszystkie serwery te muszą być dostarczone w takiej samej konfiguracji, wraz z kablami sieciowymi potrzebnymi do podłączenia ich do sieci. Dodatkowe serwery zapewnią zasoby pod inne systemy instalowane na platformie wirtualizacyjnej wraz z nadmiarowymi serwerami, zasobami pod środowisko testowe i zarządzające platformy wirtualizacyjnej.
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 24 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory, w tym każdy minimalnie dwudziestordzeniowy klasy x86 umożliwiające przez oferowany model serwera osiągnięcie wyniku min. 105 punktów w teście SPEC CPU2017 Floating Point Speed w układzie dwuprocesorowym. Wynik dla oferowanego modelu serwera musi być dostępny na stronie www.spec.org.

Obszar	Treść wymagania
RAM	Minimum 256GB min. 2666MT/s RDIMM DDR4 z możliwością rozbudowy do minimum 1024GB. Płyta główna wyposażona w min. 24 sloty na pamięć RAM i co najwyżej połowa slotów może być zajęta.
	Oferowany serwer musi oferować następujące zabezpieczenia pamięci RAM: ECC, Memory Mirroring, Memory demand and patrol scrubbing, Memory Rank Sparing, SDDC (lub Fast Fault Tolerance)
Diagnostyka	Panel LCD lub LED umieszczony na froncie serwera, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze lub za pomocą dedykowanego oprogramowania do zarządzania infrastrukturą serwerową.
Gniazda PCI	- minimum 8 slotów PCI Express (w tym min. 2 sloty PCI Express x16 generacji 3). Wszystkie sloty muszą być uniwersalne (umożliwiające instalowanie między innymi kart Ethernet).
Interfejsy sieciowe/FC/SAS	Wbudowane 4 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ nie zajmujących uniwersalnych slotów PCI lub dodatkowa karta czteroportowa 10Gb Ethernet w standardzie SFP+ jeśli wymaganie z punktu O32.3.F7 będzie spełnione pomimo dodanej karty.
	Przynajmniej dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT;
	Dodatkowa karta min. czteroportowa 10Gb Ethernet w standardzie SFP+.
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD, NVMe.
	Zainstalowane 2 karty SD lub 2 dyski M.2 lub 2 dyski SSD, każdy o pojemności min 16GB, skonfigurowane w RAID 1, przeznaczone do instalacji sytemu wirtualizacyjnego.
Dysk SSD pod cache	min. 800GB Hot Swap NVMe Dyski muszą być w stanie zapisać minimalnie 7300 TBW jak również być w stanie dokonać ponad 30000 zapisów na sekundę. Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Cache.
Dysk SSD pod capacity	min. 1.92TB Hot Swap Dyski muszą być w stanie zapisać minimalnie 2000 TBW jak również być w stanie dokonać ponad 15000 zapisów na sekundę. Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Capacity.
Kontroler RAID	Kontroler RAID obsługujący passthrough lub HBA
Ogólne	Oferowane urządzenia/oprogramowanie ma pochodzić z bieżącej linii produkcyjnej, ma być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla niego ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowane rozwiązania posiadają nowszą wersję, następcę oprogramowania – należy zaoferować rozwiązanie najnowsze. Serwer należy dostarczyć wraz z okablowaniem sieciowym potrzebnym do podłączenia serwera do sieci (min. 6 sztuk)

Obszar	Treść wymagania
	Jeżeli do poprawnego działania dostarczanych urządzeń niezbędne jest wykorzystanie dodatkowych komponentów/licencji, nie ujętych w szczegółowym opisie wymagań, to należy je przewidzieć i dodatkowo dostarczyć w ramach proponowanej oferty.
Wbudowane porty	min. 2 porty USB z przodu obudowy oraz min. 2 porty USB 3.0 z tyłu obudowy, 2 porty VGA lub 1 port VGA i jeden Display Port, min. 1 port RS232 (DB9), w/w porty nie mogą być uzyskane za pomocą przejściówek
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 500W każdy o sprawności min. 94% lub klasie sprawności nie mniejszą niż 80 PLUS Gold.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) • szyfrowane połączenie (SSLv3 lub TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • integracja z Active Directory • możliwość obsługi przez dwóch administratorów jednocześnie • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232 (DB9). • Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, min. 8GB lub możliwość dostępu do zewnętrznej pamięci USB/FLASH 8GB
	Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: • Wsparcie dla serwerów • Wsparcie dla protokołów– WMI, SNMP, IPMI, Linux SSH • Możliwość eksportu raportu do CSV, HTML • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Generowanie alertów przy zmianie stanu urządzenia • Możliwość przejęcia zdalnego pulpitu

Obszar	Treść wymagania
	• Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej).
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
	Serwer musi posiadać deklaracja CE.
	Microsoft Windows Server min. w wersji 2016x64 – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://www.windowsservercatalog.com/
	Vmware ESXi 6.7, ESXi 6.5, vSAN – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://www.vmware.com/resources/compatibility/search.php
	Red Hat Enterprise Linux 7.6 (RHEL) – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://access.redhat.com/ecosystem/search/#/ecosystem
Warunki gwarancji	W przypadku awarii dysków dyski twarde pozostają własnością Zamawiającego
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Wymagania ogólne dla warstwy sprzętowej dla serwerów w regionach

Obszar	Treść wymagania
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 24 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory, w tym każdy minimalnie dziesięciordzeniowy klasy x86 umożliwiające przez oferowany model serwera osiągnięcie wyniku min. 75 punktów w teście

Obszar	Treść wymagania
	SPEC CPU2017 Floating Point Speed w układzie dwuprocesorowym. Wynik dla oferowanego modelu serwera musi być dostępny na stronie www.spec.org.
RAM	Minimum 128GB min. 2666MT/s RDIMM DDR4 z możliwością rozbudowy do minimum 1024GB. Płyta główna wyposażona w min. 24 sloty na pamięć RAM i co najwyżej połowa slotów może być zajęta.
	Oferowany serwer musi oferować następujące zabezpieczenia pamięci RAM: ECC, Memory Mirroring, Memory demand and patrol scrubbing, Memory Rank Sparing, SDDC (lub Fast Fault Tolerance)
Diagnostyka	Panel LCD lub LED umieszczony na froncie serwera, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze lub za pomocą dedykowanego oprogramowania do zarządzania infrastrukturą serwerową.
Gniazda PCI	- minimum 8 slotów PCI Express (w tym min. 2 sloty PCI Express x16 generacji 3). Wszystkie sloty muszą być uniwersalne (umożliwiające instalowanie między innymi kart Ethernet).
Interfejsy sieciowe/FC/SAS	Wbudowane 4 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ nie zajmujących uniwersalnych slotów PCI lub dodatkowa karta czteroportowa 10Gb Ethernet w standardzie SFP+ jeśli wymaganie z punktu O32.3.F7 będzie spełnione pomimo dodanej karty.
	Przynajmniej dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT;
	Dodatkowa karta min. czteroportowa 10Gb Ethernet w standardzie SFP+.
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD, NVMe.
	Zainstalowane 2 karty SD lub 2 dyski M.2 lub 2 dyski SSD, każdy o pojemności min 16GB, skonfigurowane w RAID 1, przeznaczone do instalacji sytemu wirtualizacyjnego.
Dysk SSD pod cache	min. 400GB Hot Swap NVMe Dyski muszą być w stanie zapisać minimalnie 4000 TBW jak również być w stanie dokonać ponad 12000 zapisów na sekundę. Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Cache.
Dysk pod capacity	min. 1.92TB Hot Swap Dyski muszą być w stanie zapisać minimalnie 1000 TBW jak również być w stanie dokonać ponad 12000 zapisów na sekundę. Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Capacity.
Kontroler RAID	Kontroler RAID obsługujący passthrough lub HBA
Ogólne	Oferowane urządzenia/oprogramowanie ma pochodzić z bieżącej linii produkcyjnej, ma być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla niego ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowane rozwiązania posiadają nowszą wersję, następcę oprogramowania – należy zaoferować rozwiązanie najnowsze.

Obszar	Treść wymagania
	Serwer należy dostarczyć wraz z okablowaniem sieciowym potrzebnym do podłączenia serwera do sieci (min. 10 sztuk) Jeżeli do poprawnego działania dostarczanych urządzeń niezbędne jest wykorzystanie dodatkowych komponentów/licencji, nie ujętych w szczegółowym opisie wymagań, to należy je przewidzieć i dodatkowo dostarczyć w ramach proponowanej oferty.
Wbudowane porty	min. 2 porty USB z przodu obudowy oraz min. 2 porty USB 3.0 z tyłu obudowy, 2 porty VGA lub 1 port VGA i jeden Display Port, min. 1 port RS232 (DB9), w/w porty nie mogą być uzyskane za pomocą przejściówek
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 500W każdy o sprawności min. 94% lub klasie sprawności nie mniejszą niż 80 PLUS Gold.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) • szyfrowane połączenie (SSLv3 lub TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • integracja z Active Directory • możliwość obsługi przez dwóch administratorów jednocześnie • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232 (DB9). • możliwość zarządzania bezpośredniego poprzez złącze USB • Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, min. 8GB lub możliwość dostępu do zewnętrznej pamięci USB/FLASH 8GB
	Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: • Wsparcie dla serwerów • Wsparcie dla protokołów– WMI, SNMP, IPMI, Linux SSH • Możliwość eksportu raportu do CSV, HTML

Obszar	Treść wymagania
	• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Generowanie alertów przy zmianie stanu urządzenia • Możliwość przejęcia zdalnego pulpitu • Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu • Przesyłanie alertów „as-is" do innych konsol firm trzecich • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej).
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
	Serwer musi posiadać deklaracja CE.
	Microsoft Windows Server min. w wersji 2016x64 – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://www.windowsservercatalog.com/
	Vmware ESXi 6.7, ESXi 6.5, vSAN – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://www.vmware.com/resources/compatibility/search.php
	Red Hat Enterprise Linux 7.6 (RHEL) – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://access.redhat.com/ecosystem/search/#/ecosystem
Warunki gwarancji	W przypadku awarii dysków dyski twarde pozostają własnością Zamawiającego
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

6.2.5.3. Obiektowy system składowania danych

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Treść wymagania
Przedmiotem zamówienia jest rozwiązanie dyskowe składające się z trzech identycznych systemów obiektowych, rozmieszczonych w trzech różnych lokalizacjach połączonych łączami Ethernet. Pojemność, musi zostać uzyskana w oparciu o dyski o pojemności minimum 4TB.

Treść wymagania
System w warstwie sprzętowej oraz programowej, poza przełącznikami sieciowymi musi pochodzić od jednego producenta (musi być kompletnym produktem opatrzonym numerem seryjnym). Dopuszcza się rozwiązania w których węzły zarządzające oraz węzły dostępowe instalowane są na zewnętrznej platformie wirtualnej VMware, Hyper-V lub KVM.
System musi być odporny na utratę dowolnej macierzy obiektowej (węzła składującego dane) będącej składową systemu, co oznacza, że awaria taka nie może skutkować utratą danych ani niedostępnością systemu. W przypadku utraty jednej macierzy dyskowej wszystkie składowane dotychczas dane muszą być dostępne w takim samym stopniu jak przed utratą macierzy obiektowej.
System musi posiadać centralny interfejs zarządzający całym systemem, lokalnymi użytkownikami i przyznawanie uprawnień dostępu dla różnych ról.
Ogólne wymagania techniczne dla obiektowego systemu składowania danych.
Przedmiotem zapytania jest dostawa, instalacja i konfiguracja obiektowego systemu składowania danych. Rozwiązanie musi być dostarczone z wraz okablowaniem sieciowym potrzebnym do podłączenia go do sieci.
Wymagana pojemność nie uwzględnia wykorzystania mechanizmów redukcji danych (przed procesem de-duplikacji i kompresji)
Wymagana pojemność musi być dostarczona i zainstalowana w trzech ośrodkach przetwarzania danych.
Należy zapewnić mechanizm asynchronicznej replikacji obiektów pomiędzy ośrodkami za pomocą istniejących łącz Ethernet.
Dostarczane rozwiązanie musi być produktem rozpoznawalnym na rynku, co oznacza, że powinno być wymieniane w raportach niezależnych organizacji, takich jak Gartner, IDC, Gigaom lub ESG (Enterprise Strategy Group).
Dostarczane rozwiązanie (oprogramowanie zarządzające składowaniem danych) musi być obecne na rynku od co najmniej 3 lat
Oferowane rozwiązanie musi być produktem gotowym, posiadającym na moment składania oferty wszystkie wymagane przez Zamawiającego funkcjonalności. Do oferty należy załączyć listę wszystkich komponentów urządzenia. Lista ma zawierać co najmniej nazwy urządzeń, modeli oraz inne informacje pozwalające w sposób jednoznaczny zidentyfikować poszczególne komponenty sprzętowe i programowe.
Oferowane urządzenia i wszystkie jego elementy składowe muszą być fabrycznie nowe i wyprodukowane nie wcześniej niż pół roku przed terminem dostawy do Zamawiającego.
Oferowane urządzenia i wszystkie jego elementy muszą pochodzić od autoryzowanego Dostawcy producenta.
Urządzenia muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
Wraz z rozwiązaniem musi być dostarczony komplet dokumentacji w formie papierowej lub elektronicznej. Dokumentacja papierowa powinna być czytelna. Zamawiający dopuszcza dostawę dokumentacji producenta rozwiązania w językach polskim lub angielskim.
Wraz z rozwiązaniem musi być dostarczony komplet nośników umożliwiający odtworzenie oprogramowania systemowego urządzeń, z których zbudowane jest dostarczone rozwiązanie.
Rozwiązanie musi mieć możliwość podłączenia go do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania komponentów rozwiązania.

Treść wymagania
Wymagania dotyczące skalowalności, budowy i architektury obiektowego systemu składowania danych.
Wszystkie elementy dostarczonego rozwiązania muszą być redundantne, a jego architektura musi zapewniać odporność na wystąpienie pojedynczego punktu awarii w obrębie poszczególnych grup elementów, to jest co najmniej: interfejsów dostępowych kontrolerów, serwerów, zasilaczy, wentylatorów, dysków. Odporność na awarię oznacza, że dostęp do urządzenia oraz do składowanych na nim danych musi być realizowany bez przerywania pracy korzystającej z niego aplikacji/systemu, zapewniając możliwość odczytów wszystkich składowanych danych oraz wykonywania zapisów na urządzenie nawet w przypadku awarii lub wymiany pojedynczego elementu urządzenia z ww. grup urządzeń.
Rozwiązanie powinno być odporne na awarię dowolnego z ośrodków tzn. w przypadku całkowitego zniszczenia infrastruktury oferowanego rozwiązania w jednym z ośrodków wszystkie dane powinny być dostępne, rozwiązanie powinno umożliwiać kontynuację pracy aplikacji, dostępna przestrzeń podczas awarii jednego z ośrodków powinna cały czas wynosić 100% wymaganej wartości netto, po usunięciu awarii dane powinny zostać automatycznie zsynchronizowane pomiędzy trzema ośrodkami.
Architektura rozwiązania musi zapewniać umieszczenie interfejsów dostępowych i dyskowych wewnątrz wszystkich węzłów klastra, realizujących funkcję obiektowego systemu składowania danych.
Wszystkie elementy opisanej powyżej architektury muszą być ze sobą zintegrowane w taki sposób, aby zapewnić automatyczny przepływ danych pomiędzy różnymi warstwami architektury.
Wydajność osiągana w przypadku oferowanej konfiguracji w obrębie węzła, powinna umożliwiać odczyt małych obiektów (16 kB) z prędkością nie mniejszą niż 5000 OBIEKTÓW na sekundę oraz nie mniejszą niż 2GB/s w przypadku dużych obiektów (powyżej 10 MB)
Dostarczone rozwiązanie powinno umożliwiać rozbudowę do co najmniej 40PB przestrzeni bez konieczności zatrzymywania pracy rozwiązania i bez przerywania dostępu do danych.
Dostarczone rozwiązanie powinno umożliwiać rozbudowę do co najmniej 20 węzłów.
Komunikacja pomiędzy węzłami oraz na zewnątrz (czyli dostęp do rozwiązania) musi być realizowana za pomocą interfejsów 10GbE lub 25GbE i SFP+.
W przypadku gdy system wymaga przełączników na potrzeby wewnętrznej komunikacji węzłów dostępowych obiektowego magazynu składowania danych, należy zapewnić redundantne przełączniki LAN 10GbE z odpowiednią ilością portów .
Architektura rozwiązania musi zapewniać możliwość elastycznej rozbudowy poprzez co najmniej dodawanie niezależnie węzłów.
Szczegółowe wymagania funkcjonalne dla obiektowego systemu składowania danych.
Dane w obiektowym magazynie danych muszą być składowane na napędach dyskowych. Nie dopuszcza się rozwiązań zbudowanych w oparciu o napędy taśmowe.
Dostarczone rozwiązanie powinno posiadać wbudowane mechanizmy przechowywania zarówno danych, jak i metadanych (informacji opisujących dane). Nie dopuszcza się wykorzystania rozwiązań plikowych (NAS) jako warstwę przechowywania w systemie składowania danych.
Rozwiązanie powinno posiadać możliwość integracji z aplikacjami za pomocą co najmniej następujących protokołów i interfejsów: HTTP, S3, REST API, NFS. Jeżeli wykorzystanie któregokolwiek z wymienionych protokołów i interfejsów

Treść wymagania
wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć wraz z rozwiązaniem. Musi istnieć możliwość wykorzystania wszystkich protokołów równocześnie.
Rozwiązanie powinno posiadać wbudowane mechanizmy protekcji danych, które gwarantują odczyt wszystkich składowanych danych w przypadku awarii pojedynczego, losowego komponentu architektury (dysku, karty sieciowej, przełącznika LAN, serwera i kontrolera urządzenia).
Zarządzanie wewnętrznymi elementami urządzenia w każdej z lokalizacji powinna być realizowana poza w/w switch'ami dostępowymi, za pomocą dedykowanego do tego switch'a będącego częścią składową oferowanego rozwiązania
W przypadku dysków Zamawiający wymaga, aby dostarczone rozwiązanie wykorzystywało następujące mechanizmy protekcji danych: RAID-6 lub Erasure Coding (EC) dla dysków SAS i SAS-NL
Dostarczone rozwiązanie musi zapewniać i gwarantować niezmienność składowanych w nim obiektów, między innymi poprzez wykorzystanie wbudowanej technologii WORM (Write Once Read Many).
Rozwiązanie musi posiadać możliwość definiowania różnych poziomów retencji przechowywania danych, gwarantujących brak możliwości skasowania danych przed upływem zdefiniowanego czasu.
Rozwiązanie musi posiadać możliwość wykorzystania co najmniej 30 atrybutów metadanych dla pojedynczego obiektu.
Zamawiający wymaga, aby dostarczone rozwiązanie posiadało możliwość zdefiniowania co najmniej 1000 logicznych partycji oraz co najmniej 1000 przestrzeni nazw. Musi istnieć możliwość mapowania i wykorzystania różnych przestrzeni nazw dla różnych aplikacji, w taki sposób, aby dla każdej z tych aplikacji możliwe było definiowanie różnych i niezależnych parametrów i kryteriów składowania danych, w tym co najmniej: retencji, wersjonowania, indeksowania i replikacji.
Rozwiązanie musi pozwalać na zdefiniowanie partycji, w których istnieje możliwość usuwania danych przed upływem retencji oraz partycji, w których usuwanie danych przed upływem retencji jest niemożliwe. Rozwiązanie powinno pozwalać na definiowanie i uruchamianie jednocześnie obydwu typów partycji.
W przypadku partycji, w której istnieje możliwość usuwania danych przed upływem retencji wymagane jest, aby taką operację mógł wykonywać jedynie administrator z odpowiednimi uprawnieniami oraz aby operacja ta była audytowalna, co oznacza, że czynności związane z usuwaniem muszą być rejestrowane w wewnętrznych dziennikach dostarczonego rozwiązania.
Każda ze zdefiniowanych partycji musi mieć możliwość zarządzana przez różnych administratorów.
Rozwiązanie powinno posiadać wbudowany mechanizm wydłużania retencji danych.
Rozwiązania musi posiadać wbudowany natywny mechanizm automatycznego usuwania danych po upływie czasu retencji.
Rozwiązanie musi posiadać swoje własne wbudowane mechanizmy weryfikacji sum kontrolnych składowanych obiektów.
Rozwiązanie powinno posiadać wbudowane mechanizmy redukcji danych, w tym co najmniej kompresję danych. W przypadku niespełnienia opisanego powyżej wymogu, przy spełnieniu pozostałych wymaganych funkcjonalności, oferowane urządzenie powinno oferować przestrzeń min. 200% netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność urządzenia w takim wypadku do min. 250% netto.

Treść wymagania
Rozwiązanie musi posiadać wbudowany mechanizm indeksowania i wyszukiwania metadanych. Musi istnieć możliwość wyszukiwania w oparciu o wewnętrzną wyszukiwarkę oraz interfejs API pozwalający na integrację silnika wyszukiwania z własną aplikacją.
OBIEKTY (archiwizowane DANE oraz opisujące je METADANE) powinny być przechowywane na dyskach których rozmiar dysków nie powinien być mniejszy niż 4TB oraz nie powinien przekraczać rozmiaru 14TB
Rozwiązanie powinno posiadać wbudowany mechanizm wersjonowania obiektów.
Rozwiązanie musi posiadać możliwość szyfrowania danych. Szyfrowanie powinno być realizowane: na dyskach obiektowego magazynu składowania danych i na połączeniu do replikacji pomiędzy ośrodkami.
Rozwiązanie musi posiadać natywnie wbudowane mechanizmy umożliwiające replikację składowanych danych pomiędzy różnymi lokalizacjami z wykorzystaniem sieci LAN/WAN i protokołu HTTP. Zastosowanie niniejszego mechanizmu musi również spełniać wymagania replikacji metadanych, uprawnień, polityki retencji oraz niezmienności danych tzn. awaria urządzenia w lokalizacji podstawowej nie może eliminować gwarancji niezmienności danych na platformie zdalnej.
Replikacja powinna być możliwa zarówno w trybie Active/Passive, czyli w trybie, w którym do odczytu i zapisu udostępniona jest replikowana przestrzeń nazw tylko w jednym ośrodku, jak i w trybie Active/Active, w którym do odczytu i zapisu udostępnione są replikowane przestrzenie nazw w każdym ośrodku.
Replikacja powinna być możliwa pomiędzy co najmniej 5 ośrodkami. W każdym z tych ośrodków replikowana przestrzeń nazw musi być jednocześnie dostępna do zapisu i odczytu w przypadku replikacji w trybie Active/Active
Rozwiązanie powinno wspierać różne topologie replikacji danych w tym co najmniej: 1-do-wielu, 1-do-1, wiele-do-1.
Rozwiązanie powinno posiadać możliwość zarządzania co najmniej poprzez graficzny interfejs użytkownika oraz poprzez API.
Każda macierz (węzeł) obiektowa musi być wyposażona w minimum 4 porty 10GbE lub 4 porty 25GbE dedykowane do przesyłania danych oraz minimum 1 port 1GbE do zarządzania.
Każda macierz obiektowa musi umożliwiać instalację dysków NL SAS 7,2kRPM o pojemnościach 4TB lub 8TB lub 10TB lub 12TB.
Dostęp do danych SYSTEMU za pośrednictwem S3 API, Swift API oraz NFS v3.
Możliwość szyfrowania składowanych obiektów algorytmem AES-256
Możliwość kompresji składowanych danych.
Możliwość weryfikacji integralności składowanych obiektów.
Wersjonowanie obiektów na poziomie pojedynczych bucket-ów
Tworzenie logicznie odseparowanych obszarów tzw. „MULTI-TENANCY” w obrębie jednej jak i wielu MACIERZY OBIEKTOWYCH (czyli w obrębie całego SYSTEMU w ramach wielu lokalizacji geograficznych); Wymagana jest możliwość rozdzielnego administrowania (np.: przypisywanie użytkowników, tworzenie praw dostępu, monitorowanie wykorzystania) tak tworzonymi obszarami,
Automatyczny monitoring obejmujący m.in.: utylizację zasobów on-line (w tym CPU, pamięć, sieć), ilość operacji S3, http
Tworzenie alertów i powiadomień dot. stanu SYSTEMU, automatyczne przesyłanie ich poprzez e-mail

Treść wymagania
Możliwość autentykacji z użyciem AD/LDAP dla użytkowników SYSTEMU.
Dostarczony sprzęt powinien być nowy, nie używany dotąd w innych projektach. Zamawiający dopuszcza rozpakowanie sprzętu w celu weryfikacji jego skompletowania i braku usterek. Na etapie odbioru sprzętu Zamawiający będzie wymagał dostarczenia dokumentów potwierdzających datę produkcji sprzętu (oświadczenie producenta lub inne dokumenty)
Całość dostarczonego sprzętu objęta będzie 60-miesięczną gwarancją, opartą o gwarancję producenta, umożliwiającą naprawy sprzętu, wymianę wadliwych podzespołów i części. Gwarancja musi umożliwiać dostęp do najnowszych wersji oprogramowania (firmware) oraz poprawek i łatek dla oprogramowania.
Czas trwania gwarancji będzie liczony od daty podpisania protokołu odbioru sprzętu i oprogramowania przy czym odbiór ten nastąpi po uruchomieniu i konfiguracji urządzeń w lokalizacjach wskazanych przez Zamawiającego
Gwarancja będzie realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Wykonawca zapewni możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta
Rozwiązanie musi być dostarczone wraz z okablowaniem sieciowym potrzebnym do podłączenia go do sieci.
W przypadku awarii dysków dyski twarde pozostają własnością Zamawiającego

6.2.5.4. Backup i Archiwizacja

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

Planowane jest, że do celów testowego/cyklicznego sprawdzania możliwości odtworzeniowych z backupów będzie wykorzystywane środowisko testowe. Przyjęto, że wszystkie dane będą przechowywane i archiwizowane w następującym modelu:

1. Codzienna kopia środowiska chmury – 7 dni (7 kopii)
2. Tygodniowa kopia środowiska chmury – 4 tygodni (4 kopie)
3. Miesięczna kopia środowiska chmury – 12 miesięcy (12 kopii)
4. Roczna kopia środowiska chmury – 2 lata (1 kopia)

Treść wymagania
Dostawca musi zapewnić mechanizm backup - restore, który będzie wykorzystywany w środowisku wirtualnym jego zadaniem będzie zapisywanie kopii i przywracanie systemów za pomocą snapshotów. Należy pamiętać, że wirtualizacja serwerowa nie może wnikać w to, co dzieje się w logice aplikacyjnej wewnątrz uruchomionych maszyn wirtualnych. Dopuszcza się zabezpieczanie dodatkowo mechanizmami „tradycyjnych" backupów agentowych kiedy zajdzie taka konieczność w wyjątkowych przypadkach. Cześć danych należy archiwizować z o wiele dłuższym czasem retencji, a nie tylko backup'ować, w związku z tym należy zapewnić archiwum obiektowe WORM gdzie mają trafiać zdefiniowane dane. Archiwum musi posiadać funkcjonalność która nie pozwoli na zmianę ani wykasowanie danych i będzie równomiernie rozproszone pomiędzy trzema ośrodkami OPD celem zapewnienia bezpieczeństwa danych po awarii OPD (nawet głównego).

Treść wymagania
Wymagana jest możliwość określania RPO i RTO dla zabezpieczanych danych, rozwiązanie ma się cechować szybką implementacją i integracją z środowiskiem chmury OSE, minimalnym ryzykiem oraz relatywnie niskimi nakładami kapitałowymi i kosztami operacyjnymi.
Rozwiązanie musi być zoptymalizowane dla infrastruktury wirtualnej i wykorzystywać istniejące w niej mechanizmy związane z wykonywaniem backupów i odtwarzania uwzględniając standardy charakterystyczne dla obszaru wirtualizacji.
Od strony licencjonowania rozwiązanie powinno charakteryzować się skalowalnością i łatwością rozbudowy i pozwalać w prosty sposób planować rozbudowę środowiska i związane z tym inwestycje.
System do tworzenia kopii zapasowych musi współpracować z architekturą wirtualizacyjną, minimalizować nakłady pracy potrzebnych do konfiguracji i obsługi środowiska. Możliwie uprościć codzienne czynności bez utraty funkcjonalności i przy zwiększeniu elastyczności i szybkości odtwarzania czy automatyzacji. Założenia przy tworzeniu kopii zapasowych oraz odtwarzania danych: 1. 2 główne OPD są aktywne, gdzie w każdym z nich zaimplementowane jest urządzenie do tworzenia backupu odpowiedzialne za tworzenie kopii zapasowych drugiego ośrodka – w OPD1 tworzone są backupy OPD2 a w OPD2 kopie zapasowe z OPD1, 2. Wszystkie OPD będą połączone pomiędzy sobą logiczną siecią backup, 3. Wszystkie węzły pomiędzy sobą są połączone linkami gwarantującymi możliwość wykonania się kopii zapasowej w założonym oknie backup, 4. Okno potrzebne na wykonywanie kopii zapasowej zawiera się pomiędzy godziną 22 - 6, 5. Wirtualne serwery w regionalnych OPD będą bezstanowymi serwerami i nie wymagają regularnego backup-u.
Dane archiwalne będzie można definiować na żądanie.
Wymagane jest, aby infrastruktura przechowywania kopii zapasowych była niezależna fizycznie od zasobów dyskowych chmury OSE (niezależne urządzanie typu appliance, dedykowane serwery itp.). Zakłada się, że ze względu na rozmiar archiwum może być ono współdzielone z urządzeniami oferującymi dostęp do zasobów obiektowych, ale utrzymywane w innej instancji/koszyku/puli zasobów o bardzo ograniczonym dostępie.

Deduplikatory

Treść wymagania
Urządzenie musi być przeznaczone do de-duplikacji i przechowywania kopii zapasowych.
Dostarczone urządzenia muszą oferować przestrzeń min. 130TB netto (powierzchni użytkowej) bez uwzględniania redukcji danych (deduplikacji i/lub kompresji). Wymagana skalowalność do minimum 170TB netto.
Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade'ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
Oferowane urządzenie musi posiadać minimum: - 4 porty Ethernet 10 Gb/s BaseT. Wymagana możliwość obsługi każdym portem protokołów CIFS, NFS, zapewniającymi deduplikacje na źródle. Urządzenie musi być dostarczone z wraz okablowaniem sieciowym potrzebnym do podłączenia go do sieci. Urządzenie należy dostarczyć wraz z okablowaniem sieciowym potrzebnym do podłączenia do sieci.

Treść wymagania
Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: CIFS, NFS; zapewniającymi deduplikację na źródle.
Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, do oferowanej pojemności urządzenia
Oferowane pojedyncze urządzenie musi osiągać za-agregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 3TB/h (dane podawane przez producenta) oraz co najmniej 5 TB/h z wykorzystaniem de-duplikacji na źródle (dane podawane przez producenta).
Urządzenie musi pozwalać na jednoczesną obsługę minimum 150 strumieni w tym jednocześnie: - zapis danych minimum 50 strumieniami; - odczyt danych minimum 50 strumieniami; - replikacja minimum 50 strumieniami. Dane mogą pochodzić z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS) oraz dowolnych interfejsów LAN w tym samym czasie.
Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.
Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany nie może zostać ponownie zapisany w obrębie tego samego urządzenia. Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.
W przypadku niespełnienia opisanego powyżej wymogu globalnej de-duplikacji, przy spełnieniu pozostałych wymaganych funkcjonalności, oferowane urządzenie powinno oferować przestrzeń min. 200% netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność urządzenia w takim wypadku do min. 250% netto
Proces de-duplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)
Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
Urządzenie musi umożliwiać de-duplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.
De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.

Treść wymagania
W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane dostarczenie licencji umożliwiających zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
Urządzenie musi wspierać de-duplikację na źródle poprzez sieć minimum dla następujących systemów operacyjnych: - Windows, Linux (RedHat, SuSE)
Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: - jeden do jednego ; - wiele do jednego; - jeden do wielu; - kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).
Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
Replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących
Replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu
Replikacja zarządzana jest z poziomu wymaganej aplikacji
Aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6.
Każda półka dyskowa lub grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych.
Oferowane urządzenie musi umożliwiać wykonywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u.
Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). Urządzenie musi pozwalać na przechowywanie minimum 100 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy

Treść wymagania
zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia).
Urządzenie musi mieć możliwość podziału na logiczne części pracujące równolegle. Producent musi oficjalnie wspierać pracę 10-ciu logicznych części pracujących równolegle z pełną wydajnością urządzenia.
Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: • CIFS • NFS
Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność typu WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.
Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): • możliwość zdjęcia blokady przed upływem ważności danych • brak możliwości zdjęcia blokady przed upływem ważności danych (compliance) Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.
Urządzenie musi mieć możliwość przechowywania danych niezmienialnych: • Video • Grafika • Pliki pdf na udziałach CIFS/NFS. Wymagane jest formalne wsparcie producenta dla przechowywania w/w danych na urządzeniu.
Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.
Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.
Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.

Treść wymagania
Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie .
Urządzenie musi mieć możliwość zarządzania poprzez: • Interfejs graficzny dostępny z przeglądarki internetowej • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
W przypadku awarii dysków dyski twarde pozostają własnością Zamawiającego

Wymagane funkcjonalności oprogramowania do zabezpieczania danych

Treść wymagania
Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu do zabezpieczania środowiska Data Center (baz danych, maszyn wirtualnych, serwerów plików, serwerów wolno stojących).
Wymagane jest dostarczenie wszystkich modułów oprogramowania tak, aby zapewnić backup całości wyspecyfikowanego środowiska oraz spełnić wszystkie wymienione w niniejszej tabeli funkcjonalności. Wymagane wsparcie na oferowane oprogramowanie realizowane przez producenta w okresie min. 5 lat, umożliwiające zgłoszenia w trybie 24x7 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania.

Backup i Archiwizacja - Wymagania dotyczące backupu serwerów (Data Center)

Treść wymagania
Wymagane jest aby oprogramowanie backupowe zapewniało backup środowiska minimum 10 milionów plików w czasie krótszym niż 1 godzina - jako pełny backup (podany wolumen oraz czas backup'u zostały przytoczone dla zobrazowania wymaganej wydajności)
Wymagane jest aby oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach Windows oraz Linux
W trakcie backupu oprogramowanie backupowe musi wykonywać kopie zapasowe fizycznych bloków a nie plików. Wymagana możliwość odtworzenia pojedynczego pliku.
W celu minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików znajdujących się na zabezpieczanym wolumenie .
Wymagane jest aby oprogramowanie backupowe zapewniało szybki inkrementalny backup blokowy wielomilionowych systemów plików na maszynach Windows oraz Linux.

Treść wymagania
W trakcie backupu inkrementalnego wielomilionowych systemów plików na maszynach Windows oraz Linux oprogramowanie backupowe musi odczytywać tylko te fragmenty dysku które zmieniły się od ostatniego backupu (wykorzystanie mechanizmu CBT)
Oprogramowanie backupowe nie może odczytywać zmienionych plików, jedynie zmienione bloki na dysku.
W celu minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików backupu inkrementalnego znajdujących się na zabezpieczanym wolumenie.
Oprogramowanie backupowe musi mieć możliwość łączenia backupu blokowego pełnego i inkrementalnego w jeden pełen backup.
Po połączeniu backupu pełnego i inkrementalnego muszą być dostępne dwa backupy pełne: dotychczas dostępny backup pełny i nowy backup pełny uzyskany w drodze łączenia z backupem inkrementalnym.
Oferowane rozwiązanie backupowe musi przechowywać całość własnych informacji (informacje o backupach, mediach) w centralnym pojedynczym katalogu, skopiowanie centralnego katalogu systemu backupu na inną maszynę musi pozwolić na uruchomienie na drugiej maszynie serwera backupu identycznego z oryginalnym. Proces klonowania centralnego katalogu może odbywać się przy wyłączonych procesach backupowych (zapewnienie spójności wewnętrznej bazy danych systemu backupowego).
Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności.
Oprogramowanie backupowe musi mieć możliwość backupu własnej bazy danych na następujące nośniki: - urządzenie dyskowe; -urządzenie de-duplikacyjne.
Oprogramowanie backupowe musi mieć możliwość automatycznego wykonywania backupu własnej bazy danych.
Oprogramowanie backupowe po każdorazowym backupie wewnętrznej bazy danych musi raportować poprzez e-mail miejsce, w którym znajduje się ostatni backup wewnętrznej bazy danych oprogramowania backupowego.
Backup własnej bazy danych musi pozwalać na odtworzenie wszystkich ustawień systemu backupowego na zupełnie nowej, świeżo zainstalowanej instancji oprogramowania backupowego.
Oprogramowanie backupowe musi mieć możliwość (wymagane formalne wsparcie producenta oprogramowania backupowego) działania jako wirtualna maszyna systemu VMware, Hyper-V, bądź KVM.
Oprogramowanie backupowe musi umożliwiać łączenie strumieni backupowych z wielu zabezpieczanych serwerów w sieci LAN.
Oprogramowanie backupowe musi mieć możliwość klonowania backupów między dowolnymi mediami: • dyskowymi (CIFS, NFS) • (opcjonalnie) de-duplikacyjnymi;
Oprogramowanie backupowe musi zapewniać różny czas ważności danych na podstawowym nośniku i nośniku zawierającym kopię (replikę backupu). Definicja czasu przechowywania kopii (repliki) powinna być określenia w momencie definiowania zadania duplikacji/klonowania zarówno z interfejsu graficznego jak i z command line.
Oprogramowanie backupowe musi mieć możliwość przechowywania informacji o zbackupowanych systemach plików na dwa sposoby:

Treść wymagania
- system backupu przechowuje informację o całym zadaniu backupowym jak również o pojedynczych plikach pozwalając na odtworzenie zarówno całego systemu plików jak również pojedynczego pliku; - system backupu przechowuje jedynie informację o całym zadaniu backupowym systemu plików pozwalając na odtworzenie tylko całego systemu plików jednak minimalizując wewnętrzna bazę danych (nie przechowuje informacji o każdym ze zbackupowanych plików).
Oprogramowanie backupowe musi pozwalać na następujące rodzaje backupu systemu plików: • Pełny; • Różnicowy; • Inkrementalny; • lub inne łączące funkcjonalności powyższych
Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych w jeden pełen backup. Proces ten musi być niewidoczny dla systemu plików którego dotyczą backupy pełne i inkrementalne. Proces odtworzenia danych z połączonego backupu pełnego i inkrementalnego musi być identyczny z odtworzeniem danych z normalnie wykonanego backupu pełnego w zakresie zarządzania i wydajności
Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z oferowanego urządzenia deduplikacyjnego.
Oprogramowanie backupowe musi pozwalać na zatrzymanie procesu backupu oraz jego wznowienie od momentu zatrzymania
W przypadku nieudanego backupu dla systemu plików (na przykład zerwanie łączności), oprogramowanie backupowe musi pozwalać na wznowienie backupu od ostatnio poprawnie zbackupowanego katalogu jak również pliku
W przypadku konsoli oprogramowania backupowego wymagana możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte
Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, CentOS), Solaris
Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS SQL, Oracle, IBM DB2, mySQL
W przypadku baz danych system musi umożliwiać inicjalizację backupu poprzez określone zdarzenie: np. ilość logów, czas który upłynął od ostatniego zdarzenia lub inne zdarzenie zdefiniowane przez użytkownika
Oprogramowanie backupowe musi mieć możliwość odtwarzania pojedynczego serwera Windows bez ponownej instalacji systemu operacyjnego.
Rozwiązanie backupowe musi mieć możliwość odtworzenia plików na docelową maszynę w oddziale z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego.
Wymagana możliwość odtworzenia danych z zabezpieczanego serwera / komputera jak również z konsoli systemu backupowego. Oprogramowanie backupowe musi umożliwiać zarządzanie bezpośrednią replikacją backupów między urządzeniami przeznaczonymi do duplikacji.

Wymaga funkcjonalności – dotyczących monitorowania, raportowania oraz przeszukiwania backupów

Treść wymagania
W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego.
W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów: • Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych) • Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych) • Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów • Zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami • Zestawienie zabezpieczanych systemów plików które w ogóle nie są backupowane, a co najmniej raz zostały zbackupowane • Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii) • Najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów) • Lista najwolniejszych/najszybszych zabezpieczanych maszyn • Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego • Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego się odtwarzamy) • Liczba danych backupowanych dziennie • Liczba zadań backupowych dziennie • Zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN) • Zużycie mediów backupowych • Aktualna konfiguracja systemu backupowego • Historia zmian konfiguracji systemu backupowego • Posiadane licencje systemu backupowego
W ramach dostarczonych licencji wymagana możliwość przeszukiwania backupów z poziomu graficznego interface'u (GUI)

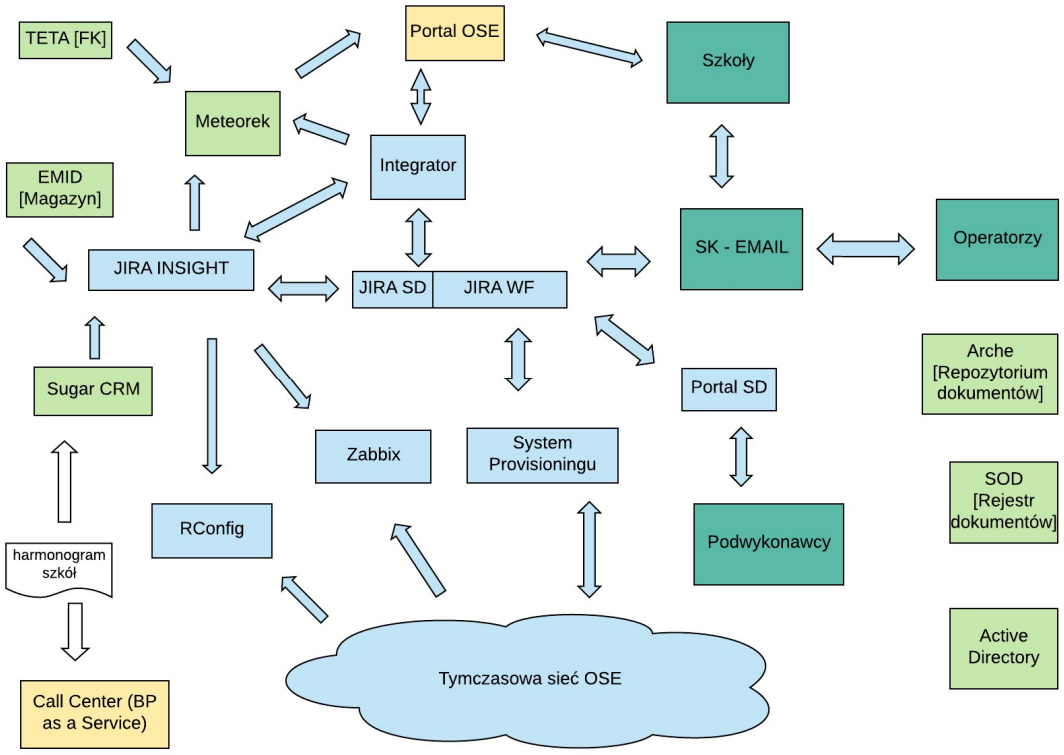
Backup i Archiwizacja - Wymaga funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk wirtualnych

Treść wymagania
Integracja na poziomie Plug-in z systemami zarządzania wirtualizacją
Wsparcie dla funkcjonalności HA wirtualizatora , automatycznego dystrybuowania zasobów warstwy compute i storage.
Możliwość integracji z systemami inteligentnego zarządzania infrastrukturą fizyczną, wirtualna i chmurą.
Rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie wirtualizacyjnej.
Skalowalność zapewniająca wsparcie dla 500 VM w obrębie pojedynczego systemu do zarządzania centrum danych.
Zabezpieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla najnowszych wersji wirtualizatora.
Możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM), wymagane wsparcie dla min. 50 CONSISTENCY GROUP
Możliwość skryptowego tworzenia planów RECOVERY.
Zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT'ów) na poziomie plików maszyny wirtualnej (wirtualnego dysku) oraz RDM, niezależnie od użytego storage'u (tzw. Storage Agnostic - warunkiem jest wsparcie przez producenta wirtualizatora), wymagane wsparcie dla połączeń: iSCSI, NAS oraz DAS
Odporność na kilkusekundowe problemy (przeciążenie, zaniki) związane z siecią WAN
Wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN
Możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, …).
Proponowane rozwiązanie powinno umożliwiać: - stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska; - operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami; - MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe.
Możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK.
Granularność umożliwiająca pominięcie określonych plików maszyny wirtualnej (wirtualnego dysku) związanych z wirtualnymi serwerami VM objętych protekcją
Architektura FAULT-TOLERANT, brak pojedynczego punktu awarii.
Działanie rozwiązania będącego przedmiotem zapytania nie może mieć żadnego negatywnego wpływu na wydajność zabezpieczanych maszyn i aplikacji.
Wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie kilku minut
możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM)
Możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie.

Treść wymagania
Możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM).
Rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu.
Wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS.
Możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację.

6.3. Koncepcja wdrożenia OSS

Celem umożliwienia świadczenia usług OSE zgodnie z wymaganiami ustawowymi przygotowane zostało i wdrożone rozwiązanie przejściowe, które obecnie jest ciągle rozwijane. Funkcjonuje ono w oparciu o systemy dedykowane dla OSE jak również systemy NASK już wcześniej istniejące. Wszystko to funkcjonuje we współpracy z tymczasową siecią OSE.

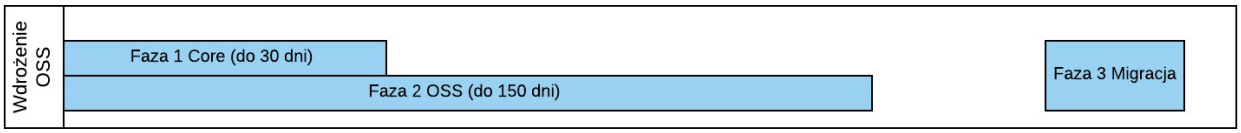


Pomimo iż obecnie systemy te nie zapewniają pełnego wsparcia, to podlegając ciągłemu rozwojowi spełniają istotną rolę w procesach biznesowych Operatora OSE w ramach procesów pozyskiwania i podłączania szkół. Zbierają też, gromadzą i przetwarzają dane związane z działalnością OSE, które będą również niezbędne w przyszłości. W ramach wdrożenia docelowej sieci OSE konieczne jest również zapewnienie odpowiednich systemów do jej obsługi, których obecnie nie ma w architekturze operatora OSE. Systemy wraz z ich wdrożeniem są elementem postępowania zakupowego.

Wdrożenie rozwiązania docelowego dla Operatora OSE będzie realizowane w kilku fazach aby zapewnić jak najszybsze dostarczanie niezbędnych funkcjonalności.

Koncepcja wdrożenia OSS ewoluuje dostosowując się do rozwoju sytuacji w OSE.

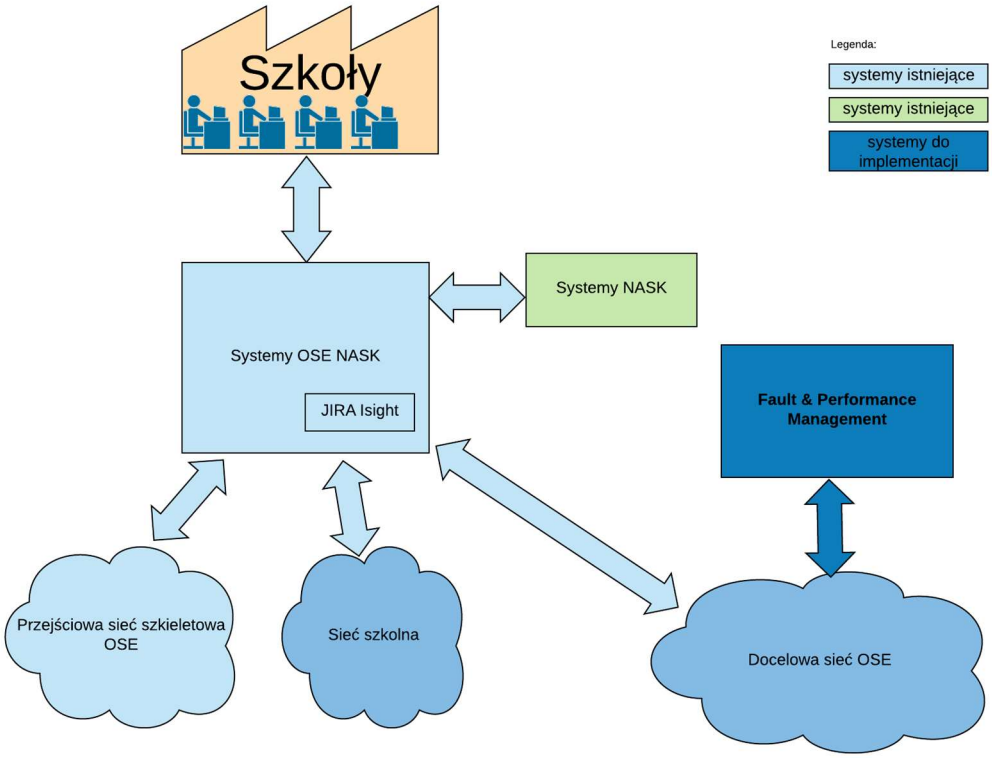
6.3.1. Wdrożenie warstwy aplikacyjnej



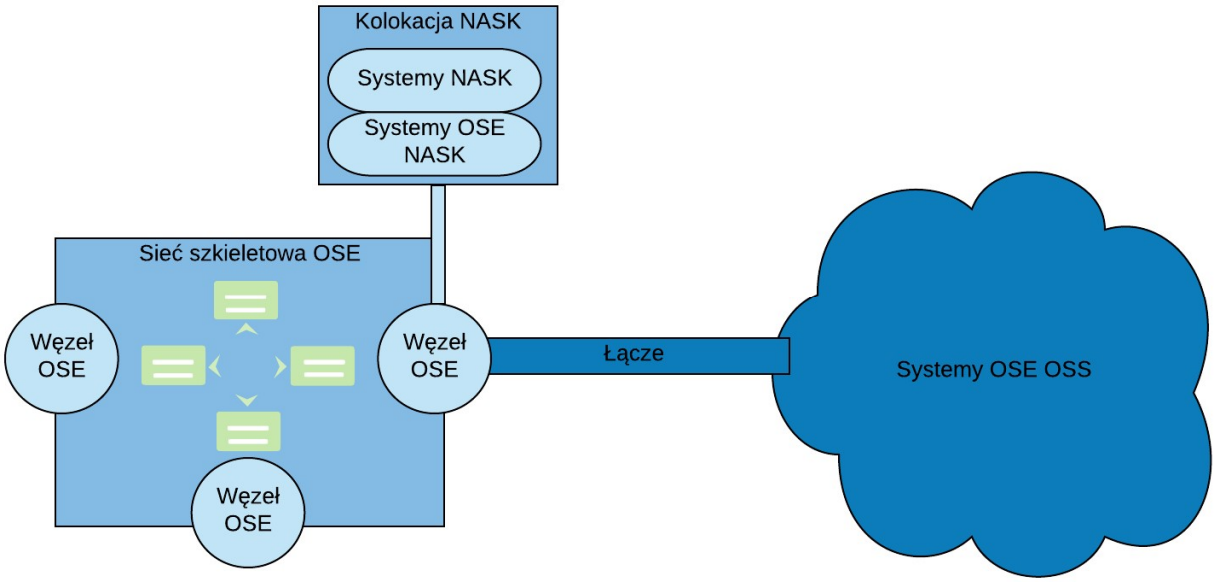
Faza 1 - Core

W celu zapewnienia odpowiedniej jakości usług dostępu do internetu dla ciągle rosnącej liczby użytkowników konieczne jest zbudowanie sieci szkieletowej o odpowiednich parametrach wydajnościowych. Uruchomienie sieci szkieletowej wymaga też zapewnienia odpowiednich systemów bezpieczeństwa. Oba elementy znajdują się poza zakresem przetargu.

Do nadzorowania ich poprawnego działania konieczne są systemy odpowiedzialne za monitorowanie docelowej sieci szkieletowej (Fault & Performance Management), które muszą zostać wdrożone jak najszybciej. Dodatkowo w fazie tej należy zapewnić platformę / narzędzie do provisioningu usług w sieci (bez implementacji procesów provisioningu oraz bez udostępniania jego API dla innych systemów).



Wdrażane rozwiązanie musi zostać oparte o zasoby infrastrukturalne zapewnione w formie usługi wraz z zapewnionym łączem do węzła centralnego OSE:



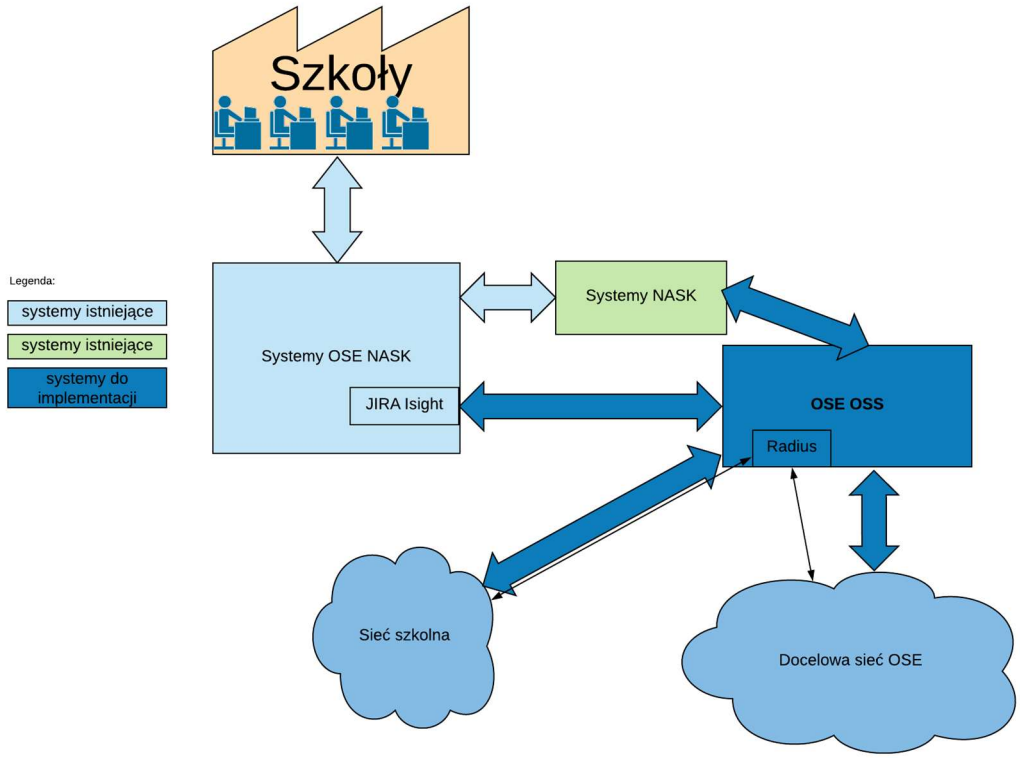
W ramach realizacji wdrożenia w fazie tej przeprowadzone zostaną następujące działania:

- Zapewnienie zasobów infrastrukturalnych wraz z łączem do węzła OSE - w formie usługi
- Wdrożenie systemów Fault & Performance Management w podstawowym zakresie do monitorowania docelowej sieci szkieletowej OSE
- Uruchomienie inventory dla docelowej sieci szkieletowej OSE
- Uruchomienie narzędzia do provisioningu usług

Cel realizacji fazy: Zapewnienie monitorowania docelowej sieci szkieletowej OSE

Faza 2 - Wdrożenie OSS

Kluczowym etapem wdrażanie Rozwiązania jest dostarczenie docelowych systemów OSS spełniających wszystkie wymagania Zamawiającego oraz ich integrację z pozostałymi systemami Zamawiającego (oraz z wcześniej wdrożonymi elementami rozwiązania).



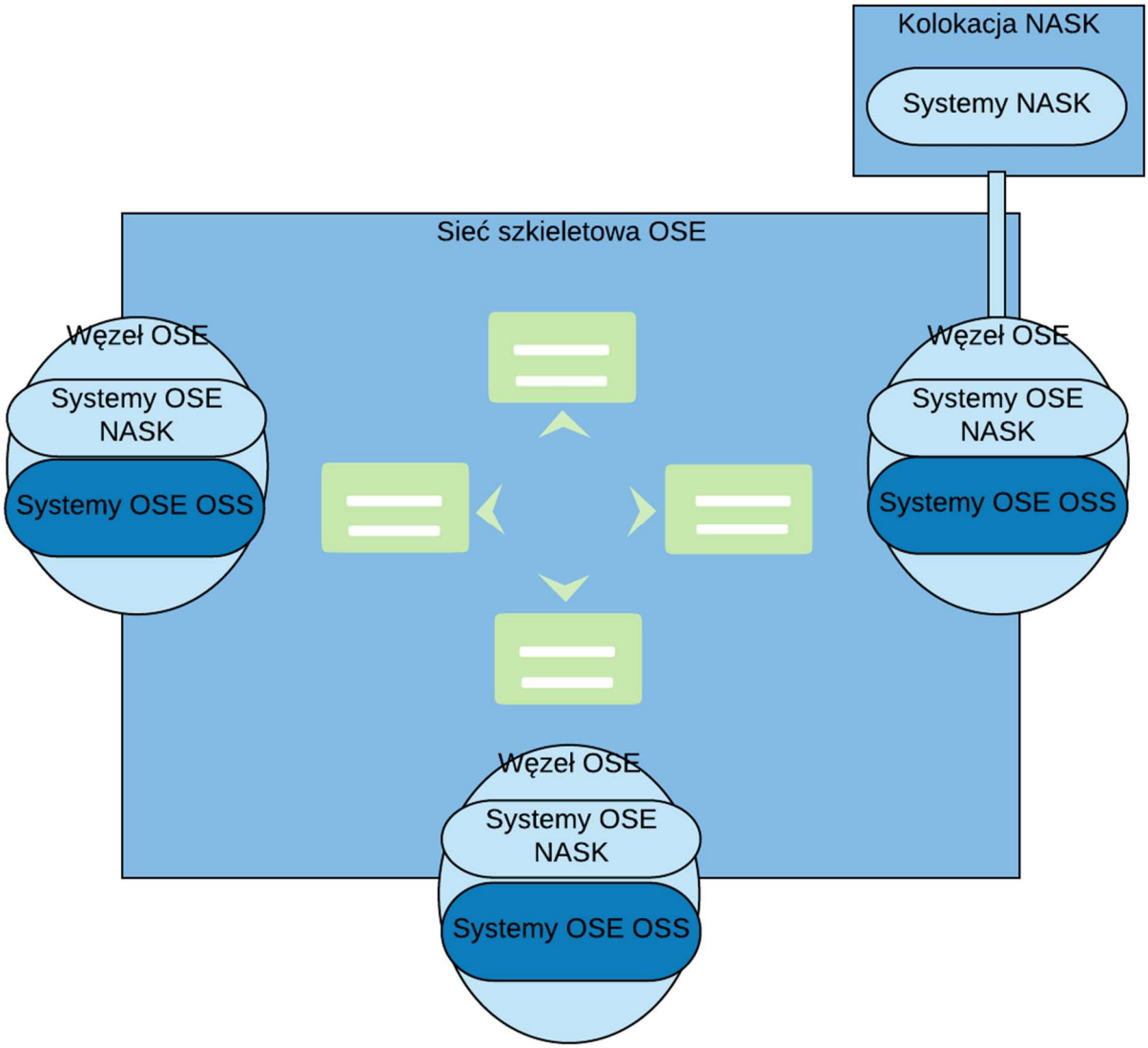
W ramach fazy 2 zostaną zrealizowane następujące działania:

- wdrożenie systemów OSE OSS (Fault, Performance, Config, Inventory, Provisioning)
- wdrożenie SSO, LDAP i integracja z systemem Radius-a zamawiającego
- integracja systemów OSE OSS z systemami OSE NASK (w tym z Insight) i NASK
- integracja systemów OSE OSS z s systemem raportowym NASK
- migracja szkół, które zostały wcześniej podłączone do sieci docelowej OSE i były obsługiwane przez systemy OSE NASK
- migracja danych inventory (CMDB) dla wcześniej podłączonych szkół

Cel realizacji fazy: Zapewnienie odpowiednio wydajnego środowiska realizującego wszystkie funkcjonalności związane z zarządzaniem usługami ściśle zintegrowanego z docelową siecią OSE i w pełni zautomatyzowanego.

Faza 3 - Migracja

Ostatnim krokiem w procesie wdrażania OSS będzie przeniesienie wcześniej wdrożonych systemów na docelową infrastrukturę umiejscowioną w węzłach OSE.



W ramach prac tej fazy zostaną zrealizowane następujące działania:

- Migracja systemów i danych z usługi na docelową infrastrukturę

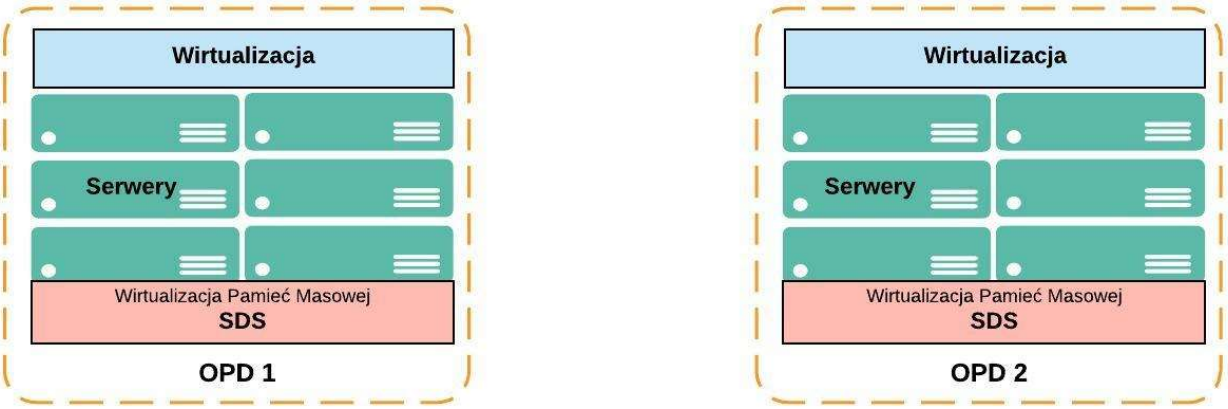
Cel realizacji Fazy: zapewnienie jednego środowiska OSS do obsługi OSE.

6.3.2. Wdrożenie infrastruktury docelowej

(zapisy niniejszego rozdziału nie należą do zakresu przedmiotu niniejszego postępowania, a stanowią informacje uzupełniające, przedstawiane przez Zamawiającego w celu przygotowania oferty i właściwego zrozumienia przedmiotu zamówienia)

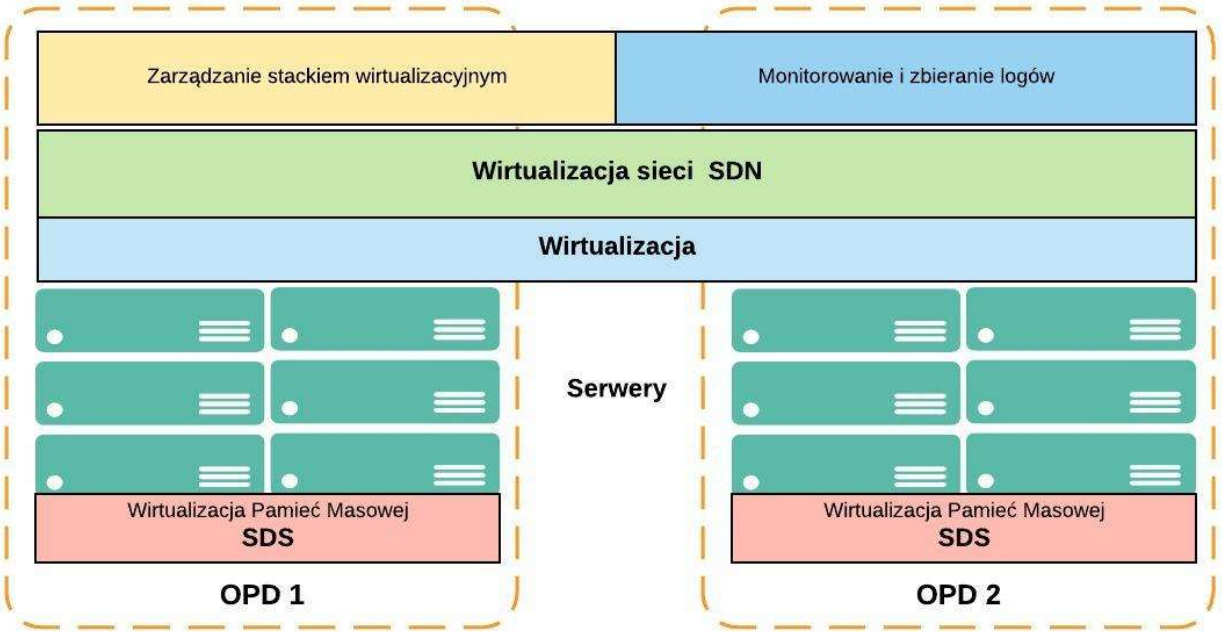
Instalacja sprzętu pod wirtualizację

W tej fazie w dwóch głównych ośrodkach przetwarzania danych (Warszawa i Poznań) dostawca instaluje serwery i podłącza je do zainstalowanej już sieci LAN. Instalowana zostaje warstwa wirtualizacyjnej mocy obliczeniowej wraz z wirtualizacją przestrzeni dyskowej SDS.



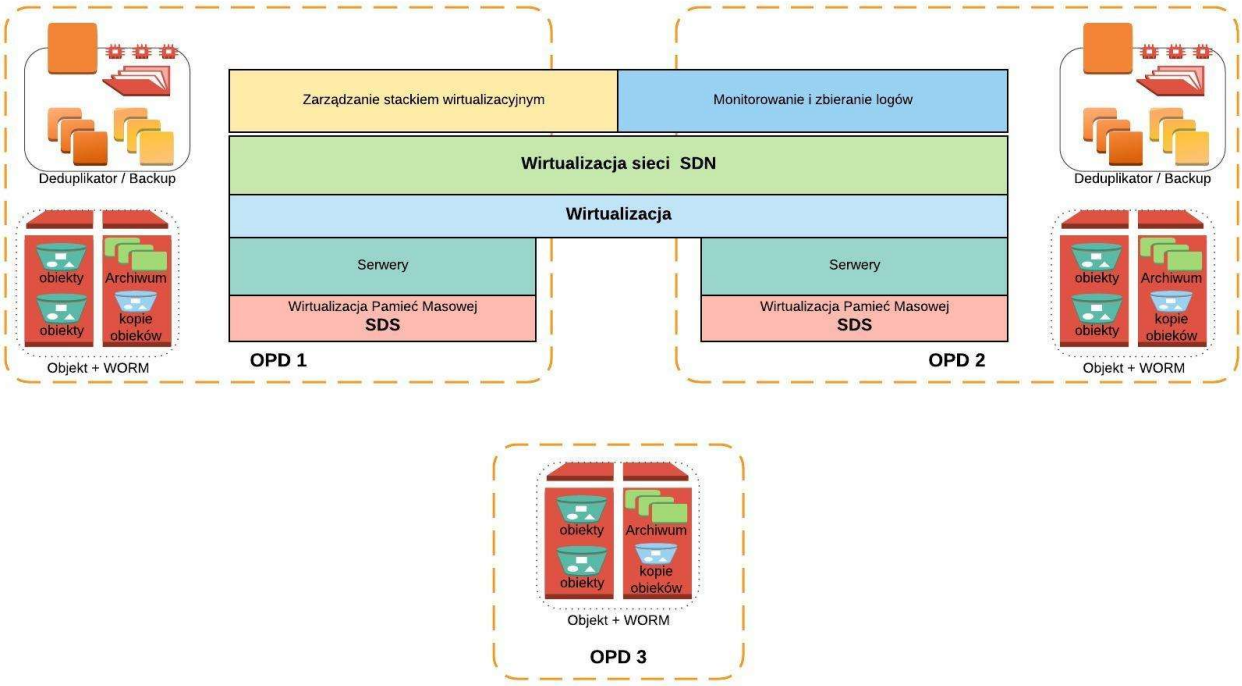
Instalacja zarządzającej warstwy wirtualizacji, wirtualnej sieci wraz z monitorowaniem i kolekcja logów.

W tej fazie dostawca instaluje moduły zarządzania pojemnością i efektywnością platformy, a także moduł zbierania logów z infrastruktury . Instalowana zostaje warstwa wirtualizacji funkcji sieciowych.



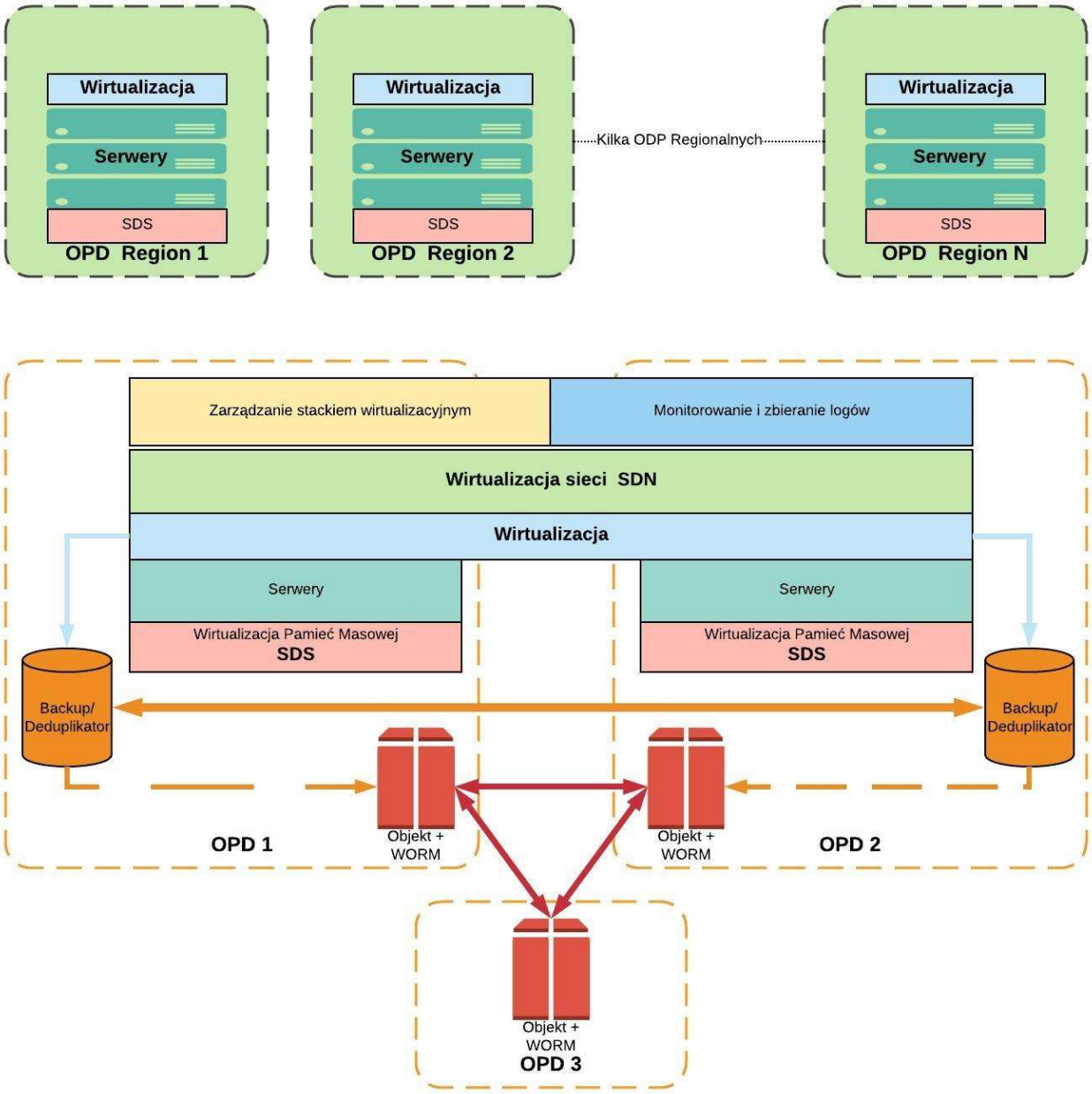
Instalacja systemu backup wraz z obiektowym systemem składowania danych.

W tej fazie dostawca instaluje rozwiązania do backup-u wraz z deduplikatorami jak również system odtwarzania po awarii . W trzech głównych ośrodkach przetwarzania danych zainstalowany zostaje system obiektowego składowania danych.



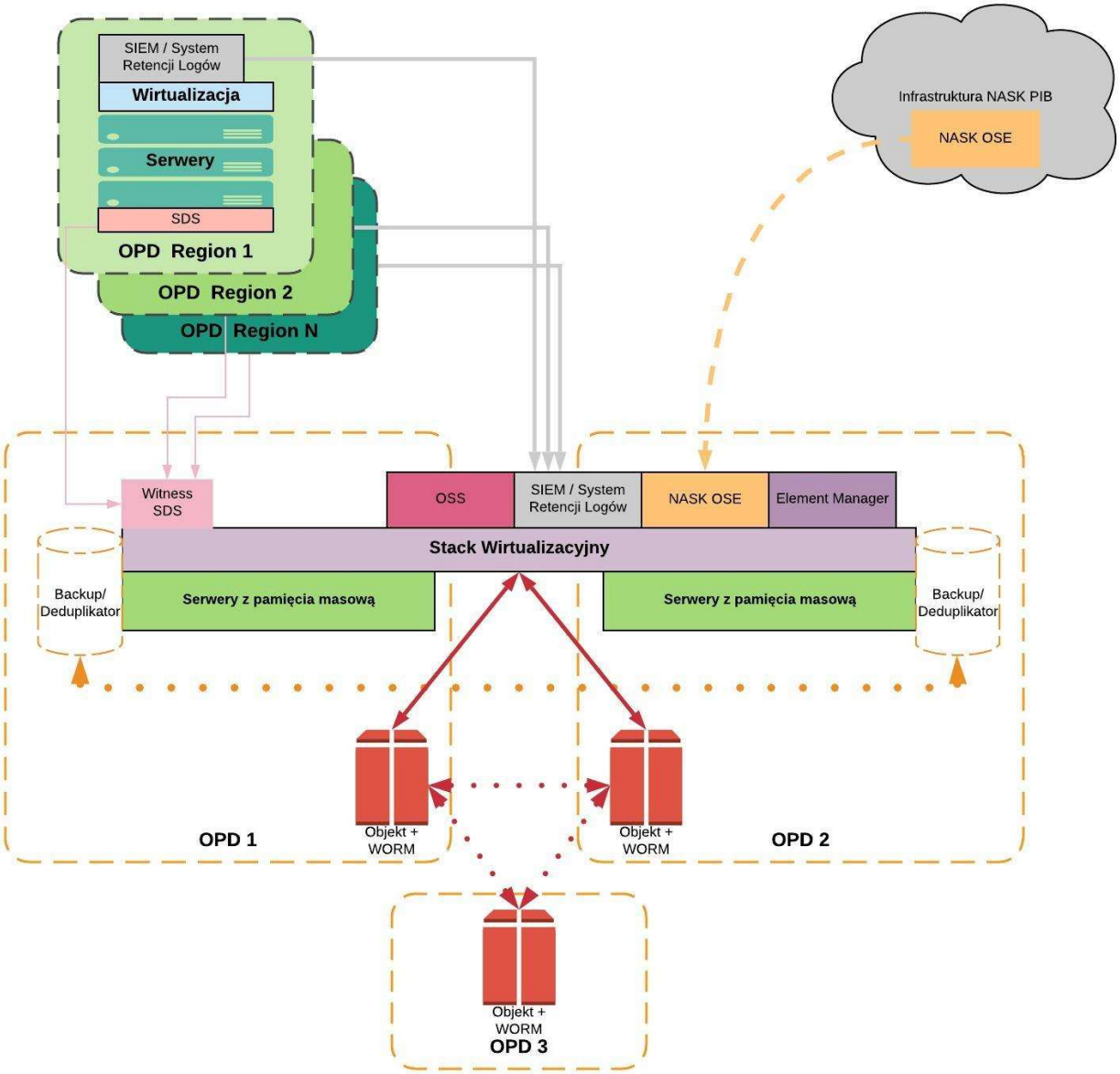
Instalacja regionalnych ośrodków przetwarzania danych i konfiguracja systemów backup i DR

W tej fazie regionalnych ośrodkach przetwarzania danych (w tym 3 centralnych ośrodkach pełniących podwójną rolę) dostawca instaluje serwery i podłącza je do zainstalowanej już sieci LAN. Instalowana zostaje warstwa wirtualizacyjnej mocy obliczeniowej wraz z wirtualizacją przestrzeni dyskowej SDS. Skonfigurowana zostaje replikacja pomiędzy ośrodkami dla systemów backupowych/deduplikatorów. Skonfigurowane zostaje rozproszenie danych na trzy ośrodki w obiektowym systemie składowania danych. Skonfigurowane zostaje archiwum dla backupu na obiektowym systemie składowania danych.



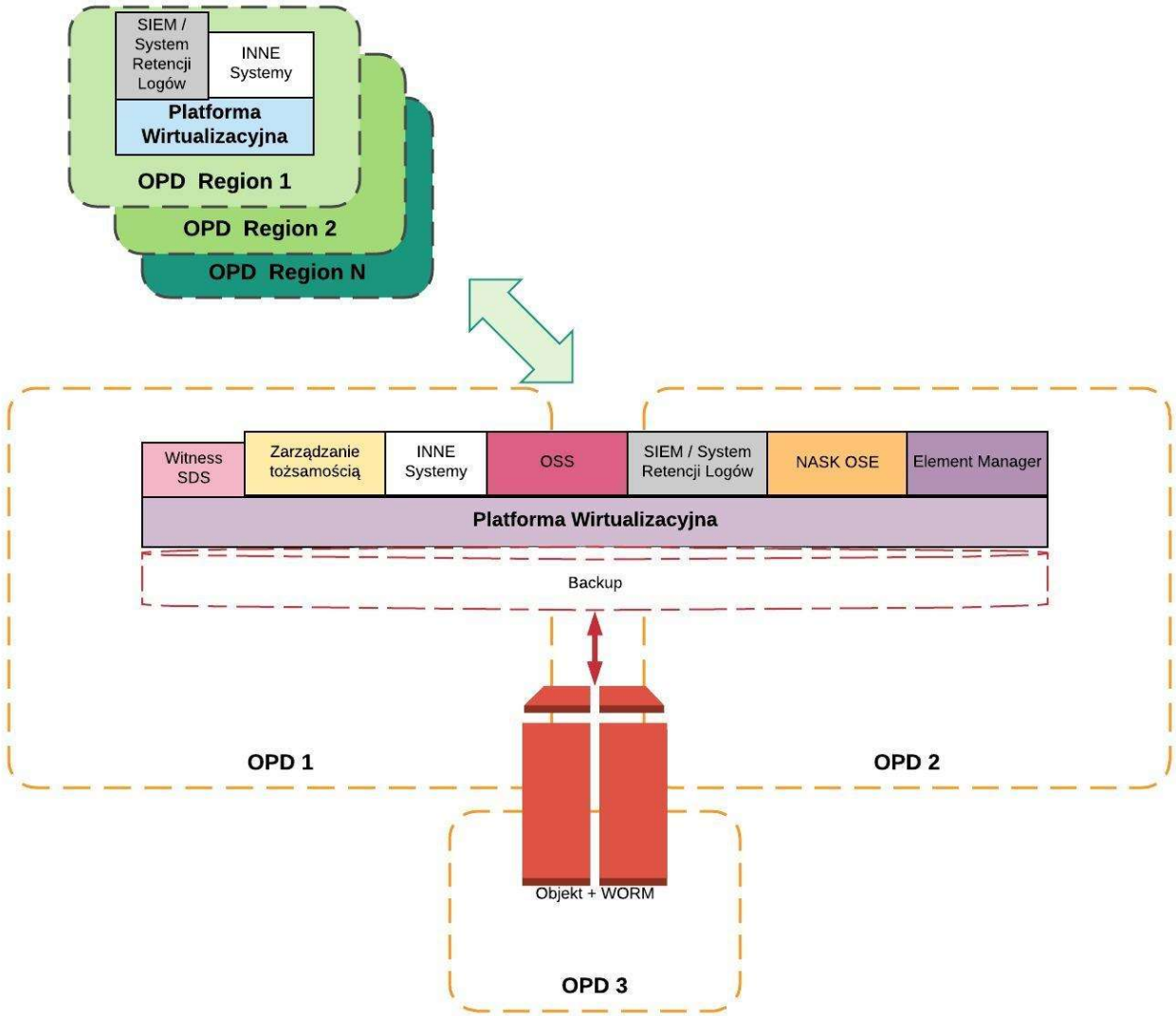
Gotowość platformy do instalowania i migrowania aplikacji.

Centralnej platforma wirtualizacyjna jest gotowa do instalowania systemów OSS (zgodnie z harmonogramem wdrożenia warstwy aplikacyjnej) oraz migracji/instalacji systemów nie będących w zakresie postępowania tj. systemów NASK OSE, SIEM / System Retencji Logów, Element Manager-ów. Część systemów jest integrowana z obiektowym systemem składowania danych. System SIEM / System Retencji Logów jest instalowany w regionalnych centrach przetwarzania danych.



Gotowość platformy do instalowania dodatkowych systemów i aplikacji.

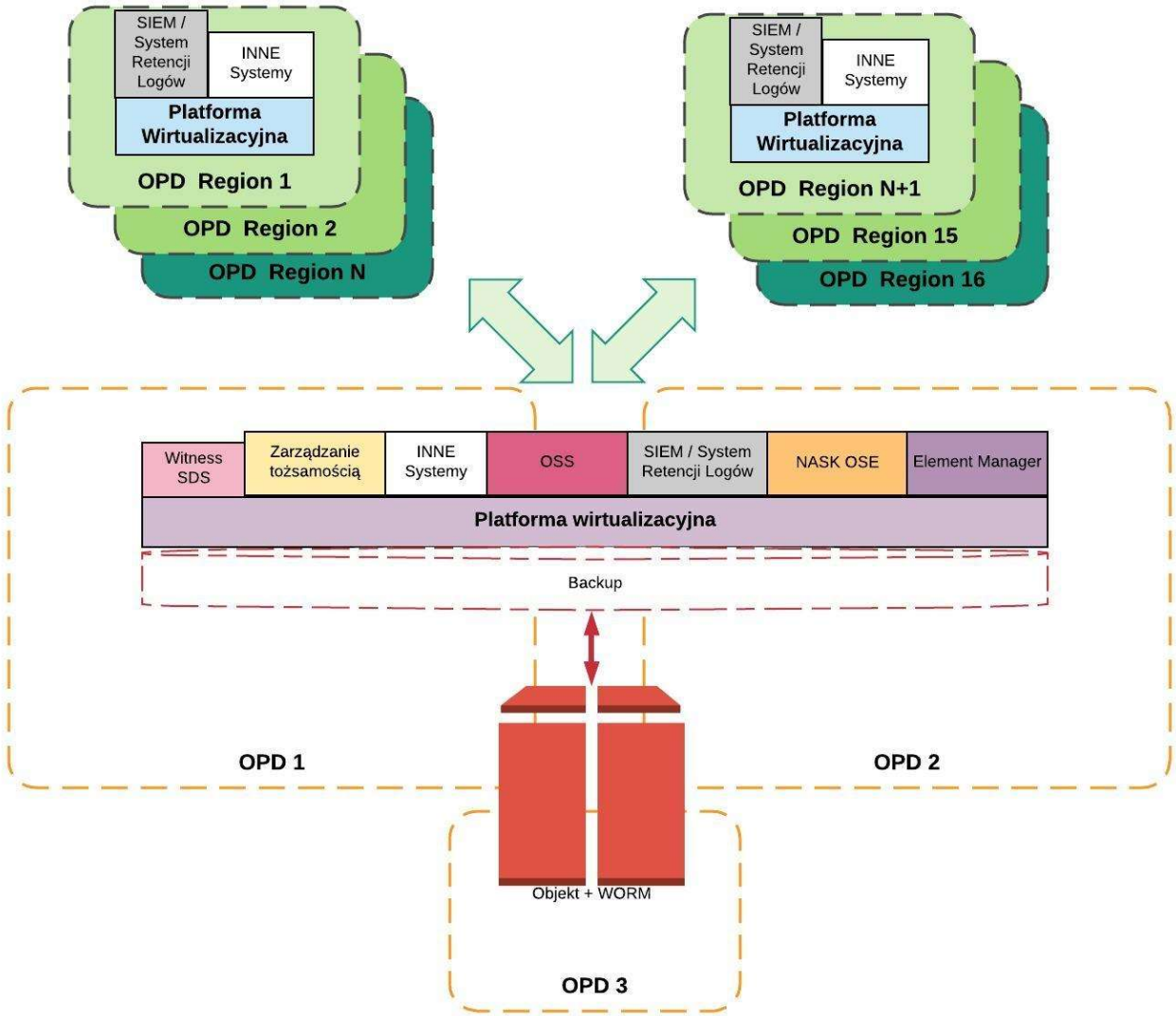
Na centralnej platformie wirtualizacyjnej zainstalowane zostaną pomocnicze systemy. W regionalnych centrach przetwarzania danych zainstalowane zostają serwery NTP, DHCP i inne systemy pomocnicze.



Instalacja pozostałych regionalnych centrów danych.

W tej fazie w pozostałych regionalnych ośrodkach przetwarzania danych dostawca instaluje serwery i podłącza je do zainstalowanej już sieci LAN.

W dołączonych regionalnych ośrodkach przetwarzania danych zainstalowane zostają systemy pomocnicze i SIEM / System Retencji Logów.



6.4. Koncepcja wsparcia rozwoju OSE

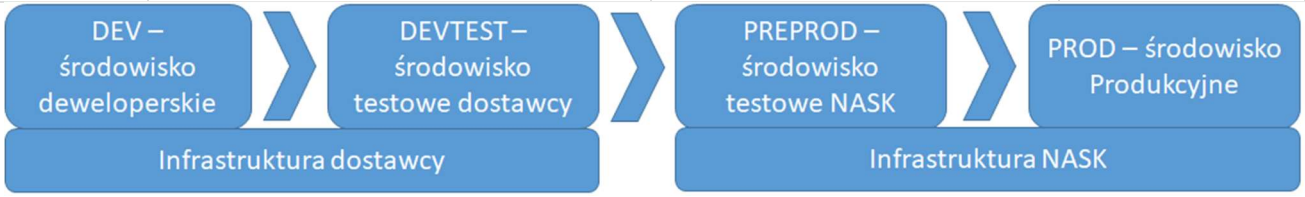
W celu zapewnienia odpowiedniego wsparcia dla procesów rozwojowych konieczne jest zapewnienie odpowiedniego środowiska do testowania rozwiązań wspierającego proces wdrożeniowy oraz platformy do dokumentowania rozwiązań.

6.4.1. Zarządzanie środowiskami

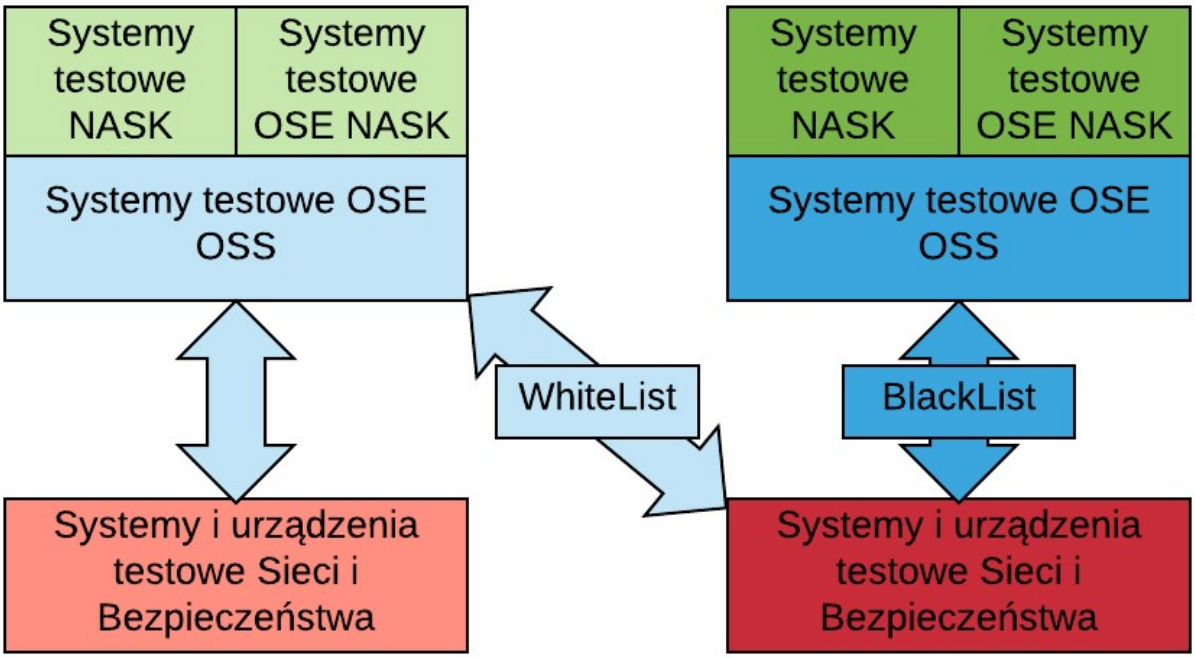
Środowiska

Środowisko	Definicja	Integracja z siecią i systemami bezpieczeństwa	Odpowiedzialność za zasoby infrastrukturalne dostawcy
Środowisko deweloperskie (DEV)	Środowisko służące do rozwoju oprogramowania, zawierające wyłącznie systemy dostawcy oprogramowania. Po stronie dostawcy jest zaślepienie integracji z	Brak sieci	Dostawca

Środowisko	Definicja	Integracja z siecią i systemami bezpieczeństwa	Odpowiedzialność za zasoby infrastrukturalne dostawcy
	otoczeniem oraz przygotowanie symulacji wywołań z systemów nie należących do jego środowiska		
Środowisko testów wewnętrznych (DEVTEST)	Środowisko służące do testów po stronie dostawcy, nie zawierające systemów innych dostawców. Po stronie dostawcy jest zaślepienie integracji z otoczeniem oraz przygotowanie symulacji wywołań z systemów nie należących do jego środowiska.	Brak sieci	Dostawca
Środowisko testów akceptacyjnych (PREPROD)	Środowisko służące realizacji testów akceptacyjnych. Zawierające wersje testowe systemów o ile istnieją. Po stronie Wykonawcy systemów OSS jest przygotowanie emulatorów/symulatorów dla systemów nie występujących w środowisku testowym.	Integracja ze środowiskiem testowym sieci i środowiskiem testowym bezpieczeństwa. Na potrzeby bardziej zaawansowanych testów możliwe jest podłączenie do produkcyjnego środowiska sieci i bezpieczeństwa w oparciu o mechanizm WhiteList-y.	Usługa chmurowa / infrastruktura OSE
Środowisko produkcyjne (PROD)	Środowisko zapewniające produkcyjne działanie systemów, w pełni zintegrowane.	Pełna integracja z siecią oparta o mechanizm tzw. BlackList - lokalizacje testowe, dla których wywołania nie będą wysyłane do sieci.	Usługa chmurowa / infrastruktura OSE

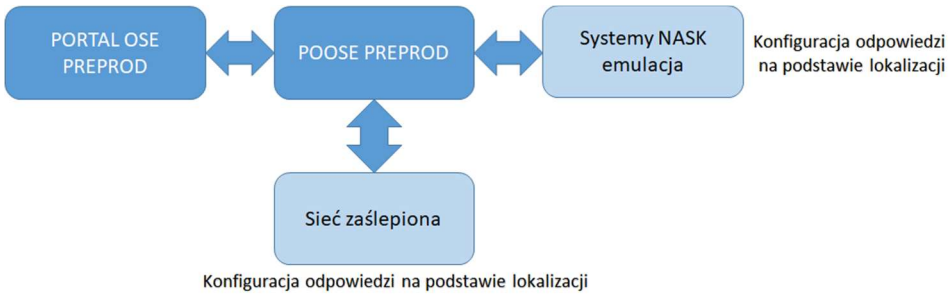


Schemat powiązania środowisk testowych i produkcyjnych:



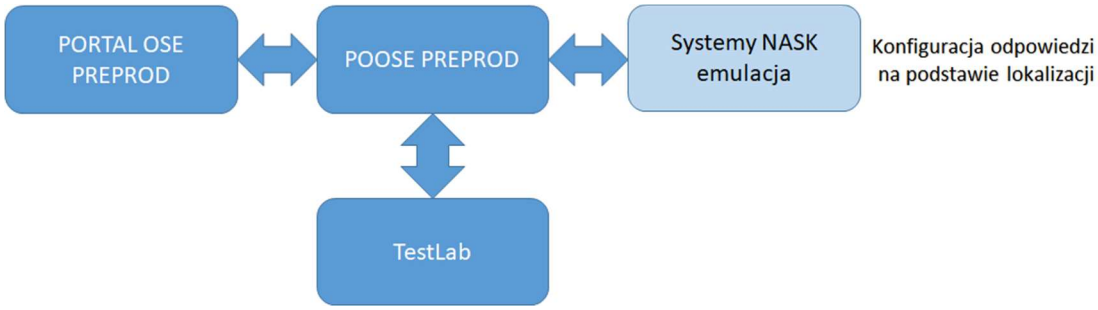
Warianty realizacja testów akceptacyjnych

Wariant 1. minimalny



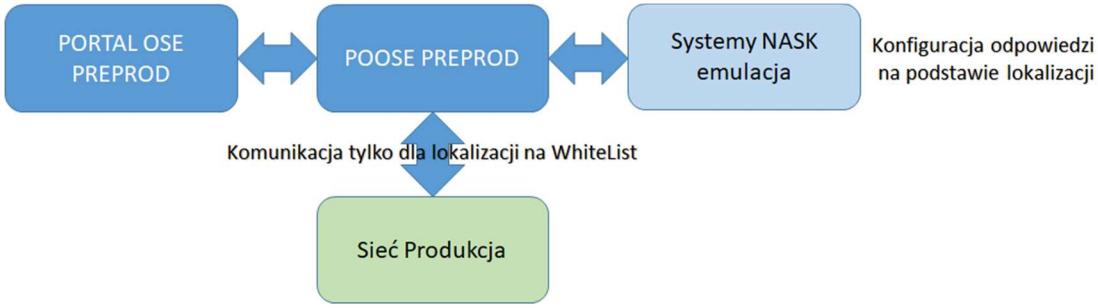
Ustawienia konfiguracji	
Zmienna	Wartość
Environment	Test
Network	None

Wariant 2. z TestLab



Ustawienia konfiguracji	
Zmienna	Wartość
Environment	Test
Network	Test

Wariant 3. z siecią produkcyjną



Ustawienia konfiguracji	
Zmienna	Wartość
Environment	Test
Network	Prod

Wariant 4. testy produkcyjne

Ustawienia konfiguracji	
Zmienna	Wartość

Ustawienia konfiguracji	
Environment	Prod
Network	Prod

Emulatory systemów na potrzeby środowiska testów akceptacyjnych

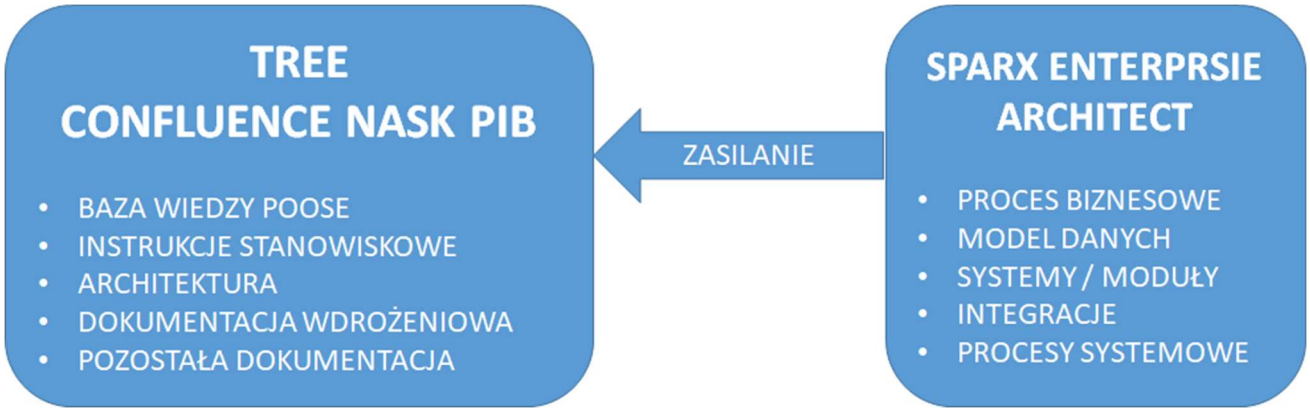
W celu umożliwienia realizacji testów akceptacyjnych należy przygotować narzędzia symulujące działanie systemów nie występujących w środowisku testowym.

Dla każdej integracji wychodzącej z OSE OSS należy przygotować odpowiednią symulację wywołań pozwalającą na skonfigurowanie odpowiedzi w następujący sposób:

- Dla każdej integracji powinien istnieć identyfikator (np. lokalizacja)
- Musi być możliwe skonfigurowanie odpowiedzi w ramach każdego wywołania dla wybranego identyfikatora (np. dla lokalizacji A odpowiedź poprawna, parametry X,Y; dla lokalizacji B odpowiedź negatywna parametr Z; itp.)
- Musi być możliwe skonfigurowanie odpowiedzi domyślnej dla przypadków wywołań z identyfikatorem nie występującym w konfiguracji

Dla każdej integracji przychodzącej do OSE OSS musi być możliwe przygotowanie wzorca wywołania z możliwością podmiany identyfikatora w wywołaniu.

6.4.2. Dokumentacja architektury środowiska IT



Do udokumentowania Rozwiązania należy wykorzystać TREE (Confluence NASK PIB). Do zamodelowania architektury należy wykorzystać narzędzie SPARX Enterprise Architect zapewniając jednocześnie jego integrację z TREE, tak aby wszelkie zmiany w modelach powodowały aktualizację dokumentacji na TREE.

7. Opis przedmiotu zamówienia

7.1. Opis ogólny

Przedmiotem zamówienia jest wdrożenie Systemów OSS, zwanych dalej Systemami lub Rozwiązaniem, zgodnie z przedstawionymi w dokumencie fazami i uwarunkowaniami wdrożenia, dotyczącymi uruchomienia Systemów OSS na świadczonej przez Wykonawcę w formie usługi infrastrukturze obliczeniowej do wskazanego węzła OSE wraz z migracjami i przełączeniem zarządzania infrastrukturą OSE z obecnego rozwiązania Zamawiającego na rozwiązanie docelowe oraz wykonaniem integracji ze wskazanymi systemami Zamawiającego a także migracja na docelową infrastrukturę obliczeniową Zamawiającego. W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do:

- wykonania projektu architektury Systemów OSS uwzględniającego wszystkie fazy wdrożenia (Projekt techniczny Systemów) zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie i z uwzględnieniem informacji zawartych w dostarczonych dokumentach oraz na bazie analizy środowiska operacyjnego i biznesowego Operatora OSE
- uruchomienie usługi infrastruktury obliczeniowej dla Systemów OSS (wraz z uruchomieniem łącza i transmisją danych do wskazanego węzła OSE) umożliwiającej maksymalne ich zautomatyzowanie, integrację i niezawodność, zgodnie z wykonanym wcześniej przez Wykonawcę i zaakceptowanym przez Zamawiającego Projektem technicznym, obejmującego wszystkie założone fazy
- wdrożenia rozwiązania „pod klucz” (zwanego dalej Rozwiązaniem lub Systemami OSS) obejmującego obszar systemów nadzoru klasy OSS (Operation Support System), serwer LDAP, jego integrację z serwerem Radius i z systemami Zamawiającego, zgodnie z wykonanym wcześniej przez Wykonawcę i zaakceptowanym przez Zamawiającego Projektem technicznym na tymczasowej infrastrukturze obliczeniowej świadczonej przez Wykonawcę w formie usługi wraz z możliwością jej przedłużenia
- świadczenia usługi udostępnienia infrastruktury obliczeniowej dla systemów OSS (usługa chmurowa świadczona na terenie Europejskiego Obszaru Gospodarczego) wraz z transmisją danych do wskazanego przez Zamawiającego węzła OSE niezbędnej do prawidłowego ich działania zgodnie z wymaganiami Zamawiającego (na systemy i infrastrukturę) wraz z możliwością jej przedłużenia
- integracji Systemów OSS z systemami Zamawiającego, wskazanymi przez Zamawiającego, wdrożonymi na potrzeby projektu OSE oraz z systemami NASK
- przeprowadzenia instruktaży dla pracowników Zamawiającego, zgodnie z wymaganiami opisanymi w załączniku "Zakres Instruktażu"
- przygotowania i uruchomienia środowiska testowego pod kolejne fazy wdrożenia jak również do wykorzystania w pracach rozwojowych Rozwiązania w przyszłości
- wykonania Planu Testów
- przeprowadzenia testów przy udziale Zamawiającego
- dostarczenia dokumentacji poszczególnych modułów i dokumentacji powykonawczej całego Rozwiązania
- świadczenia usług gwarancyjnych dla dostarczonego oprogramowania, zgodnie z wymaganiami Zamawiającego

- zapewnienia usług wsparcia producenckiego oraz wsparcia dla wdrożonego Rozwiązania zgodnie z wymaganiami Zamawiającego
- po okresie wdrożenia przekazania utrzymania Systemów OSS Zamawiającemu
- przygotowania Planu migracji
- migracji zarządzania urządzeniami OSE z obecnych przejściowych systemów OSS NASK do rozwiązania docelowego wdrożonego w wyniku niniejszego postępowania, z uwzględnieniem wszystkich faz wdrożenia oraz migracji danych
- migracji wdrożonych Systemów OSS z tymczasowej infrastruktury obliczeniowej świadczonej przez Wykonawcę w formie usługi na docelową infrastrukturę obliczeniową Zamawiającego
- udzielenia Gwarancji

Systemy muszą zostać wdrożone zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie RFP. Wszystkie wymagania i parametry, w tym techniczne, funkcjonalne i wydajnościowe zawarte w niniejszym dokumencie mają charakter obligatoryjny. Wykonawca zobowiązany jest do spełnienia wymagań obligatoryjnych w ramach ceny oferowanego rozwiązania.

Wykonawca jest zobowiązany do zaproponowania Rozwiązania optymalnego pod względem jak najmniejszej ilości komponentów różnych producentów.

7.1.1. Beneficjenci systemu OSS

Podane poniżej liczby osób obsługujących sieć OSE ukazują założenia NASK w zakresie zasobów osobowych. Należy przyjąć, że systemy OSS dostarczone przez Wykonawcę w ramach zakupionych licencji będą musiały obsłużyć podaną poniżej w tabeli liczbę użytkowników korzystających z podanych funkcjonalności. Zamawiający będzie mógł zmieniać ilość zamawianych licencji na użytkowników zgodnie z wyceną tych licencji i zgodnie ze swoim zapotrzebowaniem w danym momencie (o ile licencjonowanie systemów OSS będzie oparte na ilości użytkowników).

Funkcje systemów OSS operatora OSE	Dział Realizacji Podłączeń ***35 osób***	Dział współpracy z Operatorami ***6 osób***	Dział utrzymania (NOC & SOC) ***80 osób***	Zespół Obsługi Incydentów Bezpieczeństwa ***6 osób***	Dział IT (rozwój i utrzymanie OSS/BSS & infrastrukturą serwerową) ***28 osób***	Kadra zarządzająca ***4 osoby***
Single Sign On	X	X	X	X	X	X
Fault & Performance Management (liczba jednoczesnych użytkowników = 60)	X	X	X		X	
Config Management (liczba jednoczesnych użytkowników = 60)	X		X		X	

Service & Config Provisionig (liczba jednoczesnych użytkowników = 60)	X		X		X	
Zarządzanie wirtualizacją i orchestracją w DC w systemie DCIM (liczba jednoczesnych użytkowników = 40, ***zakup poza postępowaniem zakupowym na OSS***)					X	
Inwentaryzacja sieci i usług (liczba jednoczesnych użytkowników = 120)	X	X	X	X	X	
Generowanie raportów operacyjnych z systemów OSS na temat stanu sieci i usług OSE (liczba jednoczesnych użytkowników = 100)	X	X	X	X	X	X
SIEM (***zakup poza postępowaniem zakupowym na OSS***)			X		X	
Element Managers dla urządzeń sieciowych w szkielecie OSE (***zakup poza postępowaniem zakupowym na OSS***)			X		X	
Element Managers dla systemów bezpieczeństwa : ADC, NGFW, SWG, DNS Filtering (***zakup poza postępowaniem zakupowym na OSS***)			X			
System Retencji Logów (***zakup poza postępowaniem zakupowym na OSS***)			X	X	X	
System zarządzania kolokacjami OSE (***zakup poza postępowaniem zakupowym na OSS***)			X		X	

7.1.2. Informacje mające wpływ na architekturę rozwiązania

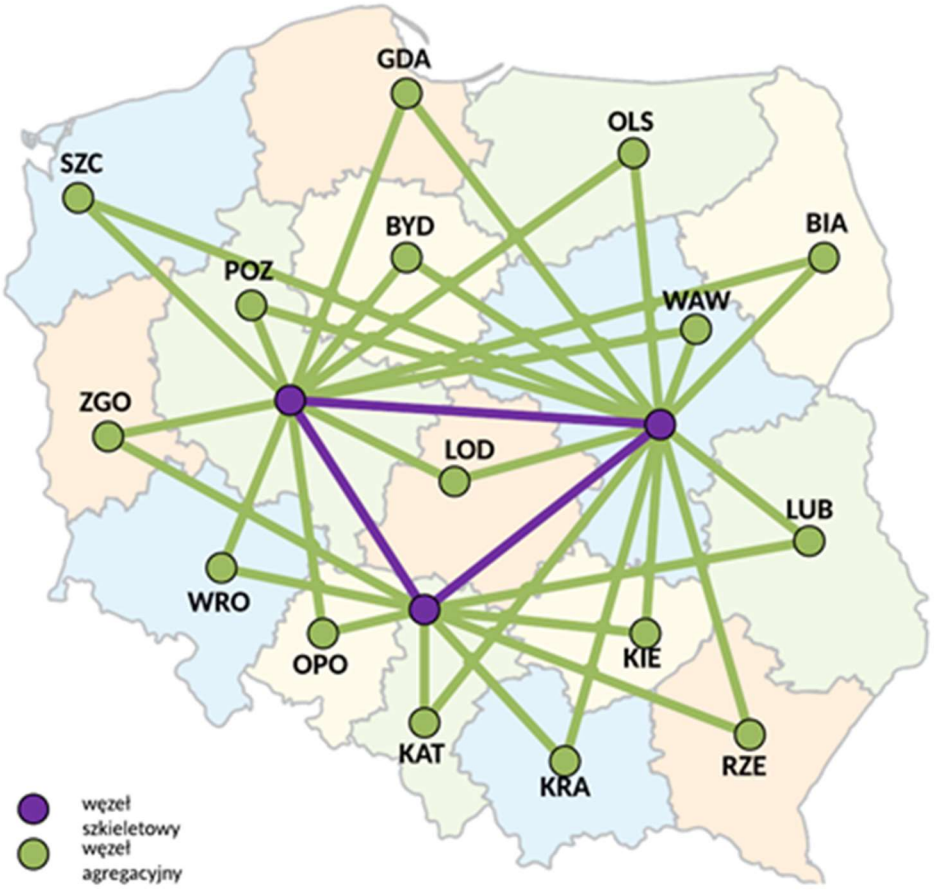
Rozwiązanie musi uwzględniać ilościowy rozkład elementów sieci, harmonogram jej wzrostu zapewniając odpowiednią wydajność funkcjonalności systemowych

I SIEĆ SZKIELETOWA

województwo	węzeł	liczba dołączonych szkół
mazowieckie	WAW	3 806

województwo	węzeł	liczba dołączonych szkół
śląskie	KAT	3 447
wielkopolskie	POZ	2 184
małopolskie	KRA	2 157
łódzkie	LOD	1 553
dolnośląskie	WRO	1 424
pomorskie	GDA	1 363
lubelskie	LUB	1 348
podkarpackie	RZE	1 328
kujawsko-pomorskie	TOR	1 194
warmińsko-mazurskie	OLS	1 132
zachodniopomorskie	SZC	942
świętokrzyskie	KIE	921
podlaskie	BIA	921
lubuskie	ZGO	712
opolskie	OPO	582
suma		**25 014**

Schemat połączeń Węzłów Agregacyjnych i Węzłów Szkieletowych jest pokazany poniżej.



W każdym **Węźle Szkieletowym Węzła Centralnego** będą m. in. styki do operatorów zewnętrznych oferujących wymianę ruchu. Ilości interfejsów będą następujące:

węzły centralne	**ilość interfejsów**			
	100GE	40GE	10GE	1GE
WAW-Core	15	6	15	10
POZ-Core	6	2	10	10
KAT-Core	8	4	10	10

Każdy ***Węzeł Agregacyjny Węzła Regionalnego*** wyposażony będzie w następujące ilości portów agregujących ruch do / ze szkół:

węzły regionalne	minimalna ilość interfejsów	
	10GE	1GE
WAW	30	45
KAT	24	15
KRA	12	20
POZ	15	15
RZE	8	35
LUB	8	35
WRO	10	20
LOD	10	15
GDA	10	15
TOR	8	20
SZC	6	15
OLS	8	15
KIE	6	15
BIA	6	15
OPO	5	15
ZGO	5	15

Sieć szkieletowa	
Węzły	W sieci OSE będą dwa rodzaje Węzłów: • Węzły Regionalne, w których skład będą wchodzić Węzły Agregacyjne (do których będą dołączone łącza ze szkół) oraz Regionalne Węzły Bezpieczeństwa. • Węzły Centralne, w których skład będą wchodzić Węzły Szkieletowe, Centralne Węzły Bezpieczeństwa oraz Zasoby Obliczeniowe OSE (będące platformą dla systemów OSS / BSS). Do Węzłów Szkieletowych dołączone będą Węzły Agregacyjne. Węzły te będą także zapewniały łączność do sieci Internet. • Węzły Szkieletowe będą zlokalizowane w tych samych miejscach co Węzły Agregacyjne, za wyjątkiem węzła WAW / WAW Core, w którym Węzeł Agregacyjny będzie umieszczony w innej lokalizacji niż Węzeł Szkieletowy (oba węzły będą zlokalizowane na terenie Warszawy).

Sieć szkieletowa	
	Urządzenia pełniące funkcje obu węzłów będą oddzielne, za wyjątkiem przełączników sieci lokalnej, które będą świadczyć usługi na rzecz zarówno Węzła Agregacyjnego jak i Węzła Szkieletowego. 3 Węzły Centralne i 16 Węzłów Regionalnych dostarczane będą stopniowo w roku 2019. Planowana gotowość kolokacyjna Węzłów Centralnych to ok. 15.06.2019, planowana gotowość wszystkich Węzłów Regionalnych to 09.2019
Łącza	40 łączy szkieletowych, czyli łączy pomiędzy węzłami OSE 20 łączy tranzytowych, czyli łączy z wyjściem z sieci OSE do Internetu
Urządzenia sieci	Sumarycznie około 130-150 urządzeń (licząc również instancje wirtualne na urządzeniach, należy założyć o 1/3 więcej) Funkcjonalnie per typ węzła: • urządzenia w węźle szkieletowym : router, router reflektor, shadow router • urządzenia w węźle agregacyjnym : router, przełącznik LAN, shadow router sieć LAN w węźle do 3 urządzeń fizycznych sieć MGMT w węźle : router, switch, terminal serwer Ilości urządzeń per funkcja: • rutery : Juniper MX960: 3 szt. oraz Juniper MX10003: 16 szt. • rutery shadow: Juniper SRX320: 19 szt. (po jednym do węzłów agregacyjnych i szkieletowych) • urządzenia CG-NAT: Juniper SRX4600: ok. 40 szt. (dwa do trzech na węzeł) • urządzenia LAN: Juniper QFX10008: 3 szt. , Juniper QFX10003 (w 13 węzłach ok. dwa na węzeł) oraz Juniper QFX 5111 lub 5110 (w 13 węzłach ok. dwa na węzeł) • urządzenia sieci zarządzającej: będzie doprecyzowane na etapie projektu technicznego Charakterystyka warstwy adresacji i rutingu: • w agregacji ~10 prefixów IPv4, 1 prefix IPv6 (+ globalne tablice routingu - w sumie ok. 1M) • instancji wirtualnych nie mniej niż 3 w węźle agregacyjnym (w przypadku uruchomienia usług VPN ~10k VRF w sieci + ~50k prefixów)

Sieć szkieletowa	
Ilość modeli provisionowanych urządzeń	ok. 15 typów (w sumie w agregacji , szkielecie, LAN i zarządzaniu) szacunki obejmują potencjalne plany rozwoju sieci o kolejne urzadzenia
Systemy	Dwie instancje (primary + secondary) systemów Element Manager do integracji (Juniper Network Director)
Monitorowanie	~100 tys. łącz (logicznych w sumie szkieletowych i dostępowych) ~20 tys. łącz fizycznych około 130 urządzeń (należy założyć nawet max. 150 urządzeń)
Ilość raportów ze statystyk	~25 rodzajów raportów : między innymi 95-percentyl, ruch w GNR, ruch na interfejsach szkieletowych i tranzytowych (średni w godzinach roboczych, max, 95 percentyl), statystyki z protokołów routingu (BGP), opóźnienia i straty na łączach, statystyki z CG-NAT,
Konfiguracje urządzeń	dla urządzeń szkieletowych / agregacyjnych 50 historycznych (rolowane + 5 punktów przywracania konfiguracji)
Wersje oprogramowania	jedna wersja per urządzenie (czyli dwie - aktualna i kandydująca) - ok. 10 typów urządzeń

Liczba portów	• fizycznych tyle ile łącz
	• logicznych szkieletowych ~10 w agregacji , ~100 w szkielecie
	• logicznych do szkół ~145 tys. w tym :
	  ○ 5 VLAN'ów per szkoła = 5 * 25 tys. = 125 tys.
	  ○ jeden VLAN zarządzający do lokalizacji = 1 * 20 tys = 20 tys.

II SIEĆ DOSTĘPOWA

Liczba łącz dostępowych w relacjach PWR (Punkt Wymiany Ruchu) - lokalizacja szkolna :

Ilość uruchomionych na dany rok	
Łącza	Dostępowe - około 19-20 tysięcy, dostarczane w ramach harmonogramu podłączania szkół:. 2019 – 12,7 tys. 2020 – 19 tys. 2021 - 19,5 tys.

Liczba łącz agregacyjnych w relacjach węzeł OSE - PWR (Punkt Wymiany Ruchu) :

Województwo	Punkt Styku	Docelowa Liczba 10GE	Docelowa liczba 1GE2
MAZOWIECKIE	Warszawa	15	32
LUBELSKIE	Lublin	4	25
PODLASKIE	Białystok	4	4
MAŁOPOLSKIE	Kraków	9	13
ŚLĄSKIE	Katowice	16	4
KUJAWSKO-POMORSKIE	Bydgoszcz	5	7
POMORSKIE	Gdańsk	6	5
WIELKOPOLSKIE	Poznań	10	4
WARMIŃSKO-MAZURSKIE	Olsztyn	5	4
OPOLSKIE	Opole	2	8
ŁÓDZKIE	Łódź	7	4
ŚWIĘTOKRZYSKIE	Kielce	4	4
ZACHODNIOPOMORSKIE	Szczecin	4	5
LUBUSKIE	Zielonagóra	3	4
DOLNOŚLĄSKIE	Wrocław	6	8
PODKARPACKIE	Rzeszów	4	24
Razem		**104**	**155**

III SIEĆ SZKOLNA

Liczba podłączeń							Liczba podłączeń do końca danego roku					
Rok	**Liczba lokalizacji**	**Liczba szkół**	**Ilość CPE**	**Ilość SW**	**Ilość AP**	**Łączna ilość urządzeń**	**Liczba lokalizacji**	**Liczba szkół**	**Ilość CPE**	**Ilość SW**	**Ilość AP**	Łączna ilość urządzeń
do końca roku 2019	12 700	19 050	12 700	19 050	19 050	50 800	12 700	19 050	12 700	19 050	19 050	50 800
w roku 2020	6 300	5 450	6 300	5 450	5 450	17 200	19 000	24 500	19 000	24 500	24 500	68 000
w roku 2021	500	500	500	500	500	1 500	19 500	25 000	19 500	25 000	25 000	69 500
RAZEM	***19 500***	***25 000***	**19 500**	**25 000**	**25 000**	**69 500**	***19 500***	***25 000***	**19 500**	**25 000**	**25 000**	**69 500**

Sieć szkolna	
Szafy	Szafy w lokalizacjach szkolnych - jedna na lokalizację
Urządzenia	jedno CPE na lokalizację, jeden SW i jeden AP na szkołę topologia logiczna: 1 VRF na lokalizację: 1 prefix IPv4 + 1 IPv6 oraz 3 VRF na szkołę: ca. 5 prefixów IPv4 i 3 IPv6 (w sumie)

Ruch sieciowy

Węzeł agregacyjny	**Ruch do szkół**		**Ruch ze szkół**	
	pasmo	*pakiety*	*pasmo*	*pakiety*
	[Mb/s]	*[kpps]*	*[Mb/s]*	*[kpps]*
WAW	160 990	55 531	58 610	20 217
KAT	145 810	50 293	53 080	18 310
POZ	92 380	31 865	33 630	11 601
KRA	91 240	31 471	33 220	11 458
LOD	65 690	22 659	23 920	8 249

Sieć szkolna

	WRO	60 240	20 777	21 930	7 564
	GDA	57 650	19 887	20 990	7 240
	LUB	57 020	19 668	20 760	7 160
	RZE	56 170	19 376	20 450	7 054
	TOR	50 510	17 421	18 390	6 342
	OLS	47 880	16 516	17 430	6 013
	SZC	39 850	13 744	14 510	5 004
	KIE	38 960	13 438	14 180	4 892
	BIA	38 960	13 438	14 180	4 892
	ZGO	30 120	10 388	10 960	3 782
	OPO	24 620	8 492	8 960	3 092

Monitorowanie	• ilość monitorowanych urządzeń CPE w szkole przez **pierwsze 3 tygodnie od podłączenia** lokalizacji szkolnej do OSE oraz w wyniku **niezbędnej diagnostyki problemów :** 19,5 tys. • ilość monitorowanych urządzeń SW i AP w szkole w wyniku **niezbędnej diagnostyki problemów** : ~ 25 tys. (AP +SW) = ~50 tys. • ilość monitorowanych łącz fizycznych w lokalizacji szkolnej (przy założeniu 1,5 szkoły na lokalizację szkolną) : ~ 3,5 • ilość urządzeń szkolnych wysyłających alarmy (tylko SYSLOG i via System Retencji Logów) przez **pierwsze 3 tygodnie od podłączenia** lokalizacji szkolnej do OSE oraz w wyniku **niezbędnej diagnostyki problemów :** ~19,5 tys. (**tylko CPE**)
Ilość statystyk	• ruch z lokalizacji szkolnej / szkoły / VLANu szkoły jest zbierany po stronie szkieletu sieci z subinterface'ów urządzeń sieciowych w węzłach OSE (per szkoła do 5 VLAN), co daje max. **145 tys.** statystyk (25 tys. * 5 VLAN szkolny + 19,5 tys. * 1 VLAN zarządzający) - **zapewnienie funkcjonalności non-stop zbierania/prezentowania/przetwarzania/archiwizowania (nie tylko w okresach 3 tyg. po podłączeniu do OSE i w okresach 2 tyg. w wyniku diagnozy problemów) statystyk ruchu z lokalizacji szkolnych/szkół/VLAN szkolnych ma być wydzieloną częścią oferty, którą Zamawiający może zamówić oddzielnie w ramach prawa opcji** • typy statystyki zbierane po stronie lokalizacji szkolnej przez **pierwsze 3 tygodnie od podłączenia** lokalizacji szkolnej do OSE na CPE **:** statystyka dostępności ok. ~2,5 statystyki łącz statystyka RAM statystyka CPU

Sieć szkolna	
	• typy statystyki zbierane po stronie lokalizacji szkolnej przez z w wyniku **niezbędnej diagnostyki problemów** na CPE, SW, AP : CPE: dostępność, ~2,5 statystyki łącz RAM, CPU SW: 2 statystyki łącza, RAM, CPU AP: 1 statystyka łącza, RAM, CPU, ilość użytkowników WLAN
Konfiguracje	1 bazowa (moment instalacji), 3 punkty przywracania konfiguracji, 5 rolowanych

Modele urządzeń instalowanych w szkole (provisioning CPE) lista na dzień opublikowania RFP - będzie się sukcesywnie powiększać		
Modele CPE	***Modele SW***	***Modele AP***
FortiGate-81E-POE		FortiAP-221C
FortiGate-101E		FortiAP-221E
Firewall Huawei USG6320	Huawei S1720-10GW-2P-E	Huawei AP4050DN
Huawei USG6330 AC	DCN S4600-28P-SI-R2	
Huawei USG6510E	Huawei S5720-28TP-LI	
MikroTik CCR1009-7G-1C-1S+		Access Point Ubiquiti UniFi AC Long Range

Usługi	
Ilość rodzajów usług uruchamianych w sieci OSE	~10 rodzajów z wariantami w tym: • Internet 100Mbs • Internet powyżej 100Mbs • IPSEC • VLAN - wiele wariantów: STANDARD, NO SEC, PUBLIC WLAN, inne) • Internet via MAN/ODN (agregacja dostępu dla wielu szkół) • inne
Monitorowanie	ilość monitorowanych usług: • ~25 tys. usług dostępu do Internetu

Usługi	
	• ~75 tys. usług VPN - 3 obecne VLANy: , STANDARD (security internet), NO SEC, PUBLIC WLAN • ~50 tys. usług VPN - dodatkowe 2 VLANy na przyszłe usługi • poniżej 1 tys. dodatkowych relacji pomiarowych w ramach monitorowania usług ad. hoc

ilość monitorowanych szkół jednocześnie w związku z nadzorem przez pierwsze 3 tygodnie po podłączeniu szkół do OSE

Parametry	Wszystkie urządzenia	Uwagi	Samo CPE (Fault, tylko monitoring per lokalizacja)
Ilość tyg. monitorowania szkoły	3	wymóg biznesowy	3
Ilość szkół podłączanych dziennie (szczyt trwający przez 3 tygodnie)	150	wymóg biznesowy 200, ale przyjmujemy 150 ponieważ pik nie będzie trwał non-stop przez 3 tygodnie założenie: 1,5 szkoły na lokalizację, zatem samego CPE będzie 100 sztuk	100
przybliżona ilość dni monitorowanych w tygodniu	6	6 a nie 7 bo w weekendy nie będą zakładane nowe monitoringi	6
Ilość podłączeń przez 21 dni (podłączenia przez 7 dni w tygodniu)	2700		1800
średnia ilość urządzeń na szkołę	2,5	założenie: 1,5 szkoły na lokalizację SW + AP + CPE (0,5 bo CPE jest per lokalizacja, wiec per szkoła mniej niż 1)	1
max ilość urządzeń równolegle monitorowanych	**6750**		**1800**

ilość monitorowanych szkół jednocześnie w związku z awariami			
Parametry	***Wszystkie urządzenia***	***Uwagi***	***Samo CPE (Fault)***
Ilość urządzeń w szkołach (w przybliżeniu)	70 000	20 tys. lokalizacji * CPE + 25 tys. szkół * (SW+AP)	20 000
Współczynnik awarii (w skali miesiąca)	1,50%	założenie	1,50%
Wyliczenia	***Wszystkie urządzenia***	***Jednostka***	***Samo CPE (Fault)***
Ilość awarii w miesiącu	1050	urządzenia	300
Długość okresu monitoringu diagnostycznego	2	tygodnie	2
Sumaryczny czas monitoringu	2100	tygodnie (suma z wszystkich urządzeń)	600
Średnia ilość urządzeń równolegle monitorowanych	**525**	urządzenia per miesiąc, zatem w przybliżeniu "Sumaryczny czas monitoringu" /4	**150**

Wniosek : w roku 2019, 2020 i 2021 przyjąć 7000 urządzeń równolegle monitorowanych, od 2022 roku 1000 urządzeń równolegle monitorowanych (nie ma podłączeń nowych szkół, ale mogą być zmiany lokalizacji szkół, stąd liczba większa niż 525)

Rozwiązanie musi uwzględniać architekturę obszaru bezpieczeństwa zapewniając odpowiednią wydajność i zasoby do obsługi

IV URZĄDZENIA BEZPIECZEŃSTWA W SZKIELECIE

Urządzenia	
ilość monitorowanych urządzeń/systemów	ponad 400 urządzeń razem w węzłach bezpieczeństwa (centralnych i regionalnych) Będą to urządzenia następujących producentów: • firewall'e ***Fortinet*** : 277 szt.

Urządzenia	
	• system DNS ***Infoblox***: 18 szt. • LTM, SSL VPN, ADC, WAF ***F5 Networks*** : 36 szt. • SSLO (deszyfracja) ***F5 Networks*** : 92 szt. Monitorowanie: • pasywne (SNMP TRAP, SYSLOG) • aktywne (ICMP, SNMP.)
ilość provisionowanych modeli urządzeń bezpieczeństwa w szkielecie	ok 20 typów (agregacja, szkielet, LAN, zarządzanie)
ilość wersji software dla wszystkich urządzeń bezpieczeństwa	Zalecane jest, aby wszędzie była ta sama wersja software'u - ok 20 typów urządzeń
ilość integracji z systemami bezpieczeństwa	Zakłada się, że ilość systemów zarządzania (Element Managerów = EM) w obszarze bezpieczeństwa będzie znaczna - należy założyć, że niezbędne będą integracje z następującymi systemami : • 2 EM do urządzeń ADC (Aplication Delivery Controller) firmy F5 Networks w 2 węzłach centralnych • 16 EM do systemu SWG (Security Web Gateway) w 16 węzłach regionalnych • 2 EM do NG Firewall firmy Fortinet w 2 węzłach centralnych • 2 instancje systemu zarządzania do DNS Infoblox w 2 węzłach centralnych • 2 instancje Systemu Retencji Logów w 2 węzłach centralnych • 2 instancje Systemu Zarządzania Tożsamością (wdrożenie systemu w dalszych etapach projektu OSE) ww. integracje zakładają: • provisioning i modyfikację usług bezpieczeństwa na ADC, SWG, NGFirewall, DNS (**Zamawiający nie wyklucza w tym zakresie zastosowania zagregowanego API,** dokładny opis w rozdz. "Provisioning") • forwardowanie logów z urządzeń CPE w szkołach do OSS Fault Management (via system Retencji Logów, w okresach 3 tyg. od połączenia szkoły do OSE i w okresach diagnostyki problemów) • wysyłanie alarmów (SYSLOG, trap SNMP) z urządzeń/systemów bezpieczeństwa do OSS Fault Management

Urządzenia	
	• zbieranie statystyk performance'owych z urządzeń/systemów bezpieczeństwa do OSS Performance Management
metody integracji	Metody integracji docelowych systemów OSS z urządzeniami i systemami bezpieczeństwa: • wymiana danych standardowymi mechanizmami typu REST API • wymiana plików konfiguracyjnych (TXT, CSV, XML, JSON) • przy pomocy standardowych protokołów (np. SNMP, NETCONF, SSH, TELNET)

Usługi	
ilość polityk bezpieczeństwa	maksymalnie 15 per szkoła
ilość urządzeń podłączonych do serwera RADIUS ilość autoryzacji na dobę w serwerze RADIUS	urządzenia CPE + urządzenia szkieletowe + systemy EM : ~ 20 tys. (CPE) + 130-150 (sieć) + ponad 400 (bezpieczeństwo) + EM ~ 20,6 tys. ok. 300 wystąpień
Funkcjonalności usług w regionalnych węzłach bezpieczeństwa	• Zapewnienie bezpieczeństwa teleinformatycznego użytkownikom sieci OSE • Wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym. • Zabezpieczanie bazujące na adresacji sieciowej, użytkownikach oraz zawartości transmitowanej poprzez sieć teleinformatyczną. • Mechanizmy ochrony użytkowników przed zaawansowanymi zagrożeniami oraz mechanizmy kontroli aplikacji webowych. • Mechanizmy autoryzacji i autentykacji użytkowników i mapowania ich do adresu IP. • Monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do logu. • Mechanizmy przypisania polityk kontroli treści użytkownikom. • Mechanizmy ochrony użytkownika sieci OSE, realizowane w oparciu o systemy klasy SWG
Funkcjonalności usług w centralnych węzłach bezpieczeństwa	• Zapewnienie bezpieczeństwa teleinformatyczne zasobów obliczeniowych i systemów wsparcia • Wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym

Monitorowanie	
dzienna ilość alarmów z systemów bezpieczeństwa	1400 alarmów dziennie na urządzenie bezpieczeństwa w sieci szkieletowej plus alarmy typu Fault z urządzeń w szkole (tylko CPE) - forwarding z Systemu Retencji Logów (założenie zbierania logów 3 tyg. po podłączeniu szkoły do OSE i ad. hoc w razie niezbędnej diagnostyki)
ilość statystyk z urządzeń/systemów bezpieczeństwa (per węzeł centralny/regionalny)	z węzłów centralnych ok 20 z węzłów regionalnych ok 100

V ALARMY

Alarmy SIEĆ SZKIELETOWA

założenie: 1400 alarmów dziennie na urządzenie szkieletowe (sieciowe i bezpieczeństwa)

Maksymalna ilość urządzeń sieci we wszystkich węzłach	*Maksymalna ilość urządzeń bezpieczeństwa w węźle*	*Liczba Centralnych Węzłów Bezpieczeństwa*	*Liczba Regionalnych Węzłów Bezpieczeństwa*	*SIEĆ ilość urządzeń*	*SIEĆ średnia ilosć alarmów na dzień*	*BEZPIECZEŃSTWO ilość urządzeń/systemów*	*BEZPIECZEŃSTWO średnia ilość alarmów na dzień*	*Łączna średnia ilość alarmów na dzień*	*Łączna średnia ilość alarmów w roku*
150	22	2	16	150	210 000	423	592 200	802 200	292 803 000

Alarmy SIEĆ SZKOLNA (dane z zakładki "ilość urządzeń w szkole" - SAMO CPE)

założenie: 20 alarmów na jedno CPE (dziennie)

Rok	*Ilość urządzeń CPE na raz monitorowanych*	*Ilość alarmów na dzień*	*Łączna ilość alarmów w roku*
2019	1 950	39 000	14 235 000
2020	1 950	39 000	14 235 000
2021	1 950	39 000	14 235 000

Alarmy SIEĆ SZKOLNA (dane z zakładki "ilość urządzeń w szkole" - SAMO CPE)			
2022	150	3 000	1 095 000

Alarmy SIEĆ SZKIELETOWA + SZKOLNA			
Rok	***Łączna ilość alarmów dziennie (razem)***	***EPH - Events per Hour (razem)***	***EPS - Events per Second (razem)***
2019	841 200	35 050,00	9,74
2020	841 200	35 050,00	9,74
2021	841 200	35 050,00	9,74
2022	805 200	33 550,00	9,32

VI STATYSTYKI

Statystyki performance'owe SIEĆ SZKIELETOWA

założenie: ok. 25 statystyk na urządzenie sieciowe, ok. 25 statystyk na urządzenie bezpieczeństwa w węźle centralnym, 50 statystyk na urządzenie w węźle regionalnym

Średnia ilość urządzeń bezpieczeństwa w węźle	***Liczba Centralnych Węzłów Bezpieczeństwa***	***Liczba Regionalnych Węzłów Bezpieczeństwa***	***SIEĆ ilość urządzeń***	***SIEĆ ilość statystyk***	***BEZPIECZEŃSTWO ilość urządzeń/systemów***	***BEZPIECZEŃSTWA ilość statystyk***	***Ilość statystyk razem***
23,5	2	16	150	3 750	423	19 975	23 725

Statystyki performance'owe SIEĆ SZKOLNA

założenie: max 10 statystyk na jedno urządzenia w szkole

Statystyki performance'owe SIEĆ SZKOLNA		
Rok	***Ilość urządzeń w szkole równolegle monitorowanych***	***Ilość statystyk ze szkoły***
2019	7 000	70 000
2020	7 000	70 000
2021	7 000	70 000
2022	1 000	10 000

Statystki ruchu (całość)						
Rok	***ilość dostępowych łącz fizycznych***	***ilość szkół***	***ilość max dostępowych łącz logicznych***	***przybliżona ilość statystyk ruchu (szkielet, agregacja, dostęp) - suma dwóch kolejnych kolumn***	***przybliżona ilość statystyk ruchu w VLAN szkolnych (dane dla wydzielonej części oferty - Zamawiający zamawia tę część w ramach prawa opcji)***	***przybliżona ilość statystyk ruchu szkielet/agregacja/dostęp - bez VLAN szkolnych (dane dla głównej części oferty)***
2019	12 700	19 050	107 950	108 060	95 250	12 810
2020	19 000	24 500	141 500	141 610	122 500	19 110
2021	19 500	25 000	144 500	144 610	125 000	19 610
2022	19 500	25 000	144 500	144 610	125 000	19 610

Rozwiązanie musi uwzględniać uwarunkowania aplikacyjne w zakresie ilości użytkowników, realizowanych procesów, przetwarzanych danych i harmonogramu rozwoju zapewniając odpowiednią wydajność systemów, dostępność funkcjonalności i zasoby do przechowywania i przetwarzania danych

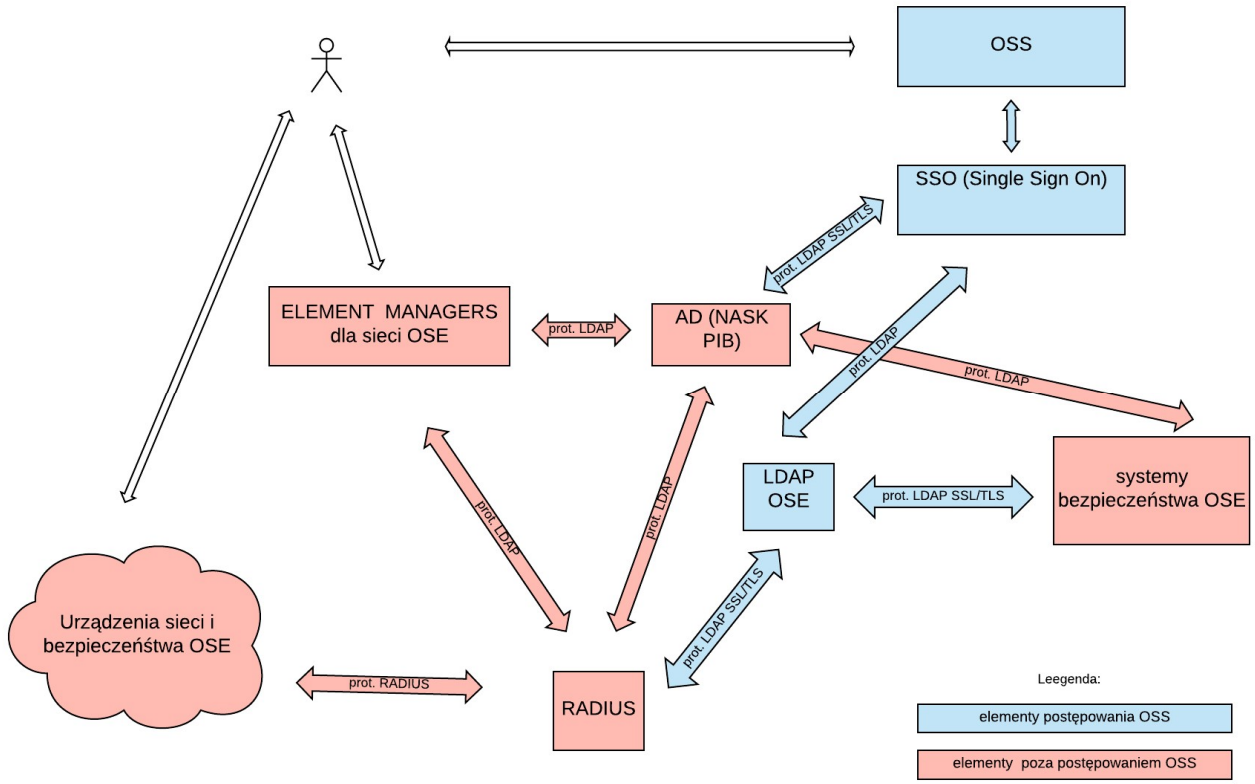
7.2. Opis funkcjonalności dla całego rozwiązania

7.2.1. Uwierzytelnianie i autoryzacji dla użytkowników wewnętrznych i dla partnerów OSE

Wdrożenie systemów OSS musi zapewnić uwierzytelnienie i autoryzację użytkowników systemów OSS oraz uwierzytelnienie użytkowników Element Manager'ów do urządzeń sieci i bezpieczeństwa, użytkowników systemów na potrzeby sieci OSE (np. SIEM, System Retencji Logów, inne) oraz w dostępie do urządzeń OSE. Funkcjonalność pojedynczego logowania SSO (Single Sign On) musi być zapewniona w dostępie do systemów OSS. System SSO musi zostać zintegrowany z katalogiem użytkowników Zamawiającego AD (Active Directory) oraz z dedykowanym katalogiem użytkowników dla partnerów OSE (np. LDAP) również implementowanym przez Wykonawcę. Usługa katalogowa dla partnerów OSE ma być zintegrowana z serwerem Radius (system Zamawiającego) i potencjalnie z innymi systemami NASK OSE przy wykorzystaniu protokołu LDAP SSL/TLS.

W ramach wdrożenia sieci OSE planowane jest w przyszłości wdrożenie centralnego systemu uwierzytelniania użytkowników wewnętrznych i zewnętrznych operatora OSE - System Zarządzania Tożsamością (kupowany w oddzielnym postępowaniu zakupowym). W związku z tym należy zagwarantować zdolność techniczną Rozwiązania do przełączenia w łatwy sposób na korzystanie z tego systemu.

Architektura systemu uwierzytelnienia i autoryzacji użytkowników OSE przedstawiona jest na schemacie poniżej:



Zatem muszą być spełnione poniższe wymagania :

Nr Wymagania	Treść Wymagania
O42.F1	Wszystkie systemy w ramach Rozwiązania lub Rozwiązanie jako całość musi zapewnić uwierzytelnianie i autoryzację użytkowników z uwzględnieniem grup i ról użytkowników (zgodnie z metodą RBAC - Role Based Access Control) oraz dostęp tylko do tych zasobów, do których użytkownicy mają uprawnienia.
O42.F2	Wszystkie systemy w ramach Rozwiązania będą korzystać z jednego systemu uwierzytelniania i autoryzacji zwanym dalej Systemem Autoryzacji, który jest wymagany jako integralna część oferowanego Rozwiązania.
O42.F3	Wszystkie systemy Rozwiązania muszą mięc zdolność korzystania z zewnętrznego systemu autoryzacji (potencjalnie dostarczonego w przyszłości przez Zamawiającego) wraz z funkcjonalnością SSO na podstawie standardów wymienionych w O42.F5 i O42.F15.
O42.F4	System Autoryzacji w Rozwiązaniu musi być przeznaczony do autoryzacji użytkowników OSE w tym pracowników NASK i partnerów NASK. System Autoryzacji i utrzymania sesji (Single Sign On) służyć ma dla potrzeby wewnętrznych użytkowników systemów OSS.
O42.F5	System Autoryzacji umożliwi autoryzację również elementom spoza Rozwiązania, takim jak Element Managery sieci i systemy bezpieczeństwa. System Autoryzacji musi umożliwiać komunikację z systemami zewnętrznymi uwzględniając to, że serwer Radius to system Zamawiającego a usługa katalogowa LDAP będąca częścią Rozwiązania ma być zintegrowana z niniejszym serwerem Radius i innymi systemami Zamawiającego przy użyciu protokołu LDAP SSL/TLS Nie jest wymagane przeniesienie sesji bez powtórnego logowania dla urządzeń zewnętrznych.
O42.F6	Zamawiający może w przyszłości podjąć decyzję o wprowadzeniu zewnętrznego System Tożsamości OSE (SSO). Rozwiązanie powinno być otwarte na taką możliwość i zapewniać możliwość przezroczystego uwierzytelniania swoich użytkowników i administratorów za pomocą mechanizmu typu Single Sign On przy wykorzystaniu protokołu SAML w wersji 2.0. Profile SAML SSO muszą wspierać przynajmniej: Web Browser SSO Profile Enhanced Client or Proxy (ECP) Profile Identity Provider Discovery Profile Single Logout Profile Name Identifier Management Profile
O42.F7	Rozwiązanie musi umożliwiać Zamawiającemu upload pliku xml zawierającego metadane serwera służącego jako Identity Provider (IdP) lub umożliwiać pobranie takiego pliku bezpośrednio z serwera IdP. Po wgraniu takiego pliku System musi odbierać tokeny protokołu SAML ze skonfigurowanego serwera IdP i na ich podstawie wykonywać uwierzytelnianie użytkowników.
O42.F8	Rozwiązanie musi umożliwiać obsługę skonfigurowanych po stronie IdP i zdefiniowanych przez Zamawiającego pól, które nie wchodzą w skład domyślnej konfiguracji tokenu SAML (custom attributes)

Nr Wymagania	Treść Wymagania
O42.F9	System autoryzacji musi umożliwiać tworzenie i zarządzanie: rolami, zasobami, aplikacjami, grupami użytkowników
O42.F10	Każdy niezależny system w ramach zamawianego Rozwiązania powinien wspierać funkcjonalność „Single Sign On" polegającej na jednorazowej autoryzacji w Systemie Autoryzacji tylko jeden raz w trakcie trwania sesji użytkownika niezależnie z ilu aplikacji oferowanego rozwiązania będzie korzystał.
O42.F11	System Autoryzacji musi definiować typy dostępu do zasobu: odczyt/zmiana/usunięcie/inne
O42.F12	System Autoryzacji musi wspierać przynajmniej jeden z następujących standardów: • SAML 2.0 • OAuth • OpenID
O42.F13	System Autoryzacji musi w bezpieczny i zaszyfrowany sposób przechowywać dane użytkowników i ich hasła
O42.F14	System Autoryzacji musi umożliwiać definiowanie polityk zarządzania hasłami
O42.F15	Polityki tworzenia haseł Systemu Autoryzacji powinny móc zawierać ograniczenia i wymuszenia co do kategorii stosowanych znaków i ich ilości (minimalna ilość znaków specjalnych, cyfr itd.)
O42.F16	Polityki zarządzania hasłami Systemu Autoryzacji powinny wymuszać zmianę hasła po upływie konfigurowalnego w systemie czasu
O42.F17	Polityki zarządzania hasłami Systemu Autoryzacji powinny uniemożliwiać zmianę hasła na jedno z X haseł poprzednich, gdzie X powinno być konfigurowalne
O42.F18	Polityki zarządzania zmianą hasła oraz złożoności hasła (dwa powyższe punkty) mogą być aplikowane per grupa użytkowników
O42.F19	System Autoryzacji musi posiadać bezpieczną procedurę tworzenia hasła początkowego, jego przekazania użytkownikowi i wymuszenia zmiany po pierwszym użyciu.
O42.F20	System Autoryzacji musi mieć możliwość wymuszenia zmiany hasła dla danego użytkownika lub grupy użytkowników na żądanie administratora systemu.
O42.F21	System Autoryzacji musi dostarczać silnik zarządzania politykami - regułami dostępu
O42.F22	Silnik zarządzania politykami musi umożliwiać definicję zasobów, aplikacji, uprawnień, typów uprawnień.
O42.F23	Silnik zarządzania politykami musi umożliwiać dodawanie uprawnień do danych zasobów i aplikacji na podstawie: - grup użytkowników - zakresów IP - typu klienta (przeglądarka, aplikacja mobilna itd.)
O42.F24	Silnik zarządzania politykami musi umożliwiać stworzenie dowolnej ilości polityk
O42.F25	System Autoryzacji musi udostępniać API dla systemów zewnętrznych umożliwiające autentykację i zapytania o uprawnienia do zasobów

Nr Wymagania	Treść Wymagania
O42.F26	System Autoryzacji musi móc obsługiwać więcej niż jedno repozytorium grup i użytkowników, w szczególności mogą to być jednocześnie repozytoria typu: LDAP, AD
O42.F27	System Autoryzacji musi umożliwiać dodawanie, usuwanie i modyfikację użytkowników i grup w dowolnym z podłączonych repozytoriów
O42.F28	System Autoryzacji musi umożliwiać wyszukiwanie grup, użytkowników, aplikacji, uprawnień i zasobów według wzajemnych relacji takich jak: użytkownicy z danej grupy, użytkownicy z przydzielonym uprawnieniem do danego zasobu, grupa zasobów per system itd.
O42.F29	Delegowani użytkownicy powinni móc zarządzać całością uprawnień dla grup i użytkowników do wybranych aplikacji i zasobów; Delegacja uprawnień administracyjnych per aplikacja/obszar aplikacji.
O42.F30	Delegowani użytkownicy powinni móc tworzyć grupy i nowych użytkowników
O42.F31	Delegowani użytkownicy powinni móc tworzyć zasoby w ramach aplikacji.
O42.F32	System Autoryzacji musi definiować następujące typy dostępu do zasobów, operacji i aplikacji: - użytkownik może dokonać operacji na danym zasobie tylko jeśli ma wprost przydzielone uprawnienie do działania na tym zasobie - użytkownik może dokonać operacji na danym zasobie za zgodą innego użytkownika (model jednorazowej akceptacji przez przełożonego); wielostopniowa autoryzacja operacji
O42.F33	System Autoryzacji musi umożliwiać procedurę czasowej delegację uprawnień z jednego użytkownika na drugiego za zgodą użytkownika trzeciego (transfer uprawnień na czas urlopu)
O42.F34	System Autoryzacji musi umożliwiać czasowe blokowanie kont przez administratorów oraz ich odblokowywanie.
O42.F35	System Autoryzacji musi umożliwiać czasowe blokowanie kont z zadanej grupy użytkowników przez administratorów oraz ich podobne odblokowywanie
O42.F36	System Autoryzacji musi przechowywać logi pełnej historii zdarzeń takich jak (ale nie ograniczonych do): logowanie i próby logowania, operacje na zasobach – typu odczyt, modyfikacja, zapis, modyfikacje uprawnień użytkowników, dodawanie grup i użytkowników, kasowanie obiektów, autoryzacje do konkretnych aplikacji.
O42.F37	Logi powinny przechowywać typ klienta z którego dokonywano w/w operacji, login name, adres IP/hostname źródłowy, czas/timestamp logowania (próby udane i nieudane), timestamp dokonywanych operacji
O42.F38	Parametry przechowywane w logach powinny być konfigurowalne
O42.F39	System musi umożliwiać raportowanie dostępów i operacji z filtrowaniem per zasób, aplikacja, grupa, zakres czasowy itp.

7.2.2. Rozwiązanie musi spełniać następujące wysokopoziomowe wymagania:

Identyfikator wymagania	Treść wymagania
O46.F3	Rozwiązanie musi umożliwiać inwentaryzację infrastruktury sieciowej i serwerowej sieci OSE (w tym urządzeń aktywnych i pasywnych sieci OSE, urządzeń bezpieczeństwa,łączy dzierżawionych i własnych, urządzeń OSE zainstalowanych w centrach danych i w dzierżawionych miejscach kolokacyjnych)
O46.F4	Rozwiązanie musi umożliwiać inwentaryzację świadczonych usług w powiązaniu z inwentaryzacją infrastruktury sieci OSE z uwzględnieniem graficznej prezentacji inwentaryzowanych elementów
O46.F5	Rozwiązanie musi zapewnić funkcjonalność Fault & Performance Management infrastruktury OSE
O46.F6	Rozwiązanie musi umożliwiać provisioning konfiguracji urządzeń CPE oraz konfigurację urządzeń szkieletowych w ramach provisioningu usług (urządzenia sieciowe i bezpieczeństwa) Rozwiązanie musi również umożliwiać hurtowe zmiany konfiguracji na wielu ww. urządzeniach na raz (mechanizm musi wspierać wybór konfigurowanych urządzeń zarówno z poziomu systemu jak i wsadowo z pliku CSV)
O46.F7	Rozwiązanie musi umożliwić zarządzanie konfiguracją i oprogramowaniem urządzeń sieci OSE z uwzględnieniem wersjonowania i archiwizacji danych
O46.F8	Rozwiązanie musi wspierać zarządzanie centrami danych rozlokowanych w węzłach sieci OSE
O46.F9	Rozwiązanie musi prezentować działanie sieci i usług OSE w postaci statystyk z uwzględnieniem różnych grup docelowych (NOC/SOC OSE, partnerzy OSE, klienci końcowi)
O46.F11	Rozwiązanie musi cechować się niezawodnością - systemy nadzoru powinny pracować w trybie wysokiej dostępności, powinna być zapewniona pełna funkcjonalność przy awarii pojedynczego elementu czy węzłów centralnych (funkcjonalność Data Recovery)
O46.F12	Rozwiązanie musi wspierać współpracę z heterogeniczną infrastrukturą sieciową (w szczególności w szkołach)
O46.F14	Rozwiązanie musi zapewniać skalowalność - co oznacza rozwiązanie w pełni funkcjonalne a jednocześnie optymalne wydajnościowo bez względu na ilość podłączonych do OSE szkół
O46.F15	Dostęp dla użytkowników systemów OSS do poszczególnych funkcjonalności powinien być możliwy zarówno z poziomu poszczególnych aplikacji serwujących daną funkcjonalność (z uwzględnieniem SSO) jak również z poziomu centralnego FrontEnd'u (portal Web/strona WW dostępne przy użyciu protokołu HTTP/HTTPS) zgodnie z założonym profilem użytkownika (po przejściu uwierzytelnienia i autoryzacji)
O46.F16	dostęp do Rozwiązania musi być możliwy przy pomocy standardowych przeglądarek Web zarówno z poziomu urządzeń stacjonarnych jak i mobilnych (w szczególności dotyczy to dostępu dla podwykonawców/partnerów serwisowych)
O46.F17	w pełni funkcjonalne Rozwiązane ale o mniejszej wydajności niż Rozwiązanie produkcyjne musi być uruchomione w środowisku testowym zaimplementowanym przez Dostawcę
O46.F18	Całość infrastruktury (zarówno na potrzeby OSS jak i innych projektów OSE) musi zostać umiejscowiona w kolokacjach NASK lub dzierżawionych przez NASK w ramach projektu OSE

Identyfikator wymagania	Treść wymagania
O46.F19	Całe rozwiązanie warstwy aplikacyjnej musi zostać osadzone na tymczasowej infrastrukturze obliczeniowej będącej przedmiotem zamówienia lub po migracji na docelowej infrastrukturze zapewnionej przez Zamawiającego (umiejscowionej w kolokacjach NASK własnych lub dzierżawionych). Nie dopuszczalne jest umieszczenie jakiejkolwiek części Rozwiązania poza ww. wariantami infrastruktury.
O46.F20	Wprowadzanie i modyfikacji danych adresowych w Rozwiązaniu musi być weryfikowane na zgodność z bazą TERYT. Baza TERYT jest podstawą dla danych adresowych w Rozwiązaniu. Dostarczenie i aktualizacja bazy Teryt pozostaje w gestii Wykonawcy
O46.F23	Rozwiązanie musi być zwymiarowane zgodnie z informacjami zawartymi w rozdziale "Informacje mające wpływ na architekturę Rozwiązania"
O46.F24	Wszystkie funkcjonalności Rozwiązania muszą być udokumentowane w postaci dokumentacji technicznej użytych technologii i zastosowanych rozwiązań (w szczególności wszystkich używanych API). Dokumentacja ta musi być przekazana Zamawiającemu na etapie akceptacji dokumentu LLD. W przypadku gdy funkcjonalność jest wytwarzana na etapie wdrożenia musi ona zostać udokumentowana i uzupełniona w przekazanej Zamawiającemu dokumentacji technicznej przez Wykonawcę. Dokumentacja techniczna musi być odpowiednio uporządkowana tak by była możliwość jej łatwego przeszukiwania.
O46.F25	W przypadku zastosowania gotowego oprogramowania dokumentacja producenta tego oprogramowania musi zostać dołączona do dokumentacji technicznej całego Rozwiązania
O46.F26	Interface użytkownika systemów wdrożonych w ramach Rozwiązania musi być zaimplementowany w języku polskim lub/i angielskim.
O46.F27	Dostarczona Zamawiającemu dokumentacja wdrożonych systemów w ramach Rozwiązania musi być napisana w języku polskim lub/i angielskim.

7.2.3. Wymagania na rozwój systemów

Ze względu na to, ze systemy OSS będą zintegrowane z obecnymi systemami BSS Zamawiającego Wykonawca musi zapewnić możliwość wykonania niezbędnych integracji w środowisku testowym w celu ich należytego przetestowania.

Identyfikator wymagania	Treść wymagania
O47.F1	Należy udokumentować architekturę w ramach SPARX Enterprise Architect opisując m.in.: - model danych - wszystkie systemy (uwzględniając również podział na moduły) - integrację między poszczególnymi systemami (modułami) - procesy systemowe (diagramy sekwencji) - dla każdej aplikacji/modułów należy wskazać alokację funkcjonalności TAM poziom 2(Telecom Application Map z Frameworx) - w ramach Enterprise Architect należy odwzorować model TAM

Identyfikator wymagania	Treść wymagania
O47.F2	Należy utworzyć bazę wiedzy OSS na platformie TREE (Confluence NASK PIB) wykorzystując architekturę udokumentowaną w ramach SPARX Enterprise Architect, oraz co najmniej: - instrukcje stanowiskowe - dokumentację wdrożeniową - dokumentację administracyjną - dokumentację środowisk testowych - pozostałą dokumentację OSS
O47.F3	Należy stworzyć integrację pomiędzy Sparx EA oraz TREE, umożliwiając aktualizowanie bazy wiedzy OSS na TREE w wyniku zmian opisu architektury na SPARX EA
O47.F4	Należy utworzyć i skonfigurować repozytorium architektury OSS w ramach narzędzia Sparx EA w zakresie potrzebnym do dokumentowania projektu.
O47.F5	Należy zapewnić 4 licencje "floating" dla bieżącej wersji narzędzia Sparx Enterprise Architect dla zespołu Zamawiającego oraz odpowiednią ilość licencji dla zespołu Wykonawcy. Licencje minimum w edycji "Unified"
O47.F6	Wszelkie integracje z siecią muszą być wyposażone w odpowiednie mechanizmy (whiteList i blackList) umożliwiające testowanie: - rozpoznawanie na podstawie konfiguracji, czy środowisko jest produkcyjne czy testowe (oddzielnie środowisko aplikacyjne i sieci) - w przypadku środowiska testowego aplikacyjnego i produkcyjnego sieci, wywołania do sieci są realizowane wyłącznie dla lokalizacji skonfigurowanych na whiteList, dla pozostałych zwracany jest zawsze sukces wraz z ewentualnym zestawem standardowych danych - w przypadku środowiska produkcyjnego (aplikacyjnego i sieci) sprawdzana jest blackList i dla lokalizacji na niej występujących nie realizowane jest wywołanie do sieci a jedynie zwracany jest komunikat o sukcesie wraz ze standardowym zestawem parametrów - w przypadku środowiska testowego aplikacyjnego i sieci sprawdzana jest blackList i dla lokalizacji na niej występujących nie realizowane jest wywołanie do sieci a jedynie zwracany jest komunikat o sukcesie wraz ze standardowym zestawem parametrów
O47.F7	Systemy w środowisku testowym muszą posiadać identyczną funkcjonalność jak systemy w środowisku produkcyjnym. Środowisko testowe ma służyć do testowania kolejnych wersji developerskich przygotowywanych przez Dostawcę Rozwiązania po to, by po ich zaakceptowaniu móc w sposób sprawny uruchamiać kolejne wersje systemów w środowisku produkcyjnym (wdrożenia kolejnych wersji produkcyjnych leżą w zakresie odpowiedzialności Wykonawcy).
O47.F8	Systemy uruchamiane w środowisku testowym muszą być uruchamiane jako niezależna instancja od środowiska produkcyjnego i nie mogą powodować dodatkowych kosztów, w tym kosztów licencyjnych po stronie Zamawiającego.
O47.F9	Należy dostarczyć systemy zarówno dla środowiska produkcyjnego jak i środowiska testowego. Aplikacje nie mogą mieć rozróżniać na jakim typie środowiska pracują, z wyjątkiem integracji z siecią, która na podstawie konfiguracji musi uwzględniać blackListy i whiteListy.
O47.F10	Środowisko testowe OSE OSS musi mieć możliwość zintegrowania ze środowiskiem produkcyjnym sieci i bezpieczeństwa.

Identyfikator wymagania	Treść wymagania
O47.F11	Dla wszystkich integracji wychodzących z systemów środowiska OSE OSS z systemami zewnętrznymi (czyli wywołań systemów spoza OSE OSS przez systemy Rozwiązania) Wykonawca musi przygotować zaślepki / symulatory integracji pozwalające na skonfigurowanie odpowiedzi w następujący sposób: - dla każdej integracji powinien istnieć identyfikator (np. lokalizacja) - musi być możliwe skonfigurowanie odpowiedzi w ramach każdego wywołania dla wybranego identyfikatora (np. dla lokalizacji A odpowiedź poprawna, parametry X,Y; dla lokalizacji B odpowiedź negatywna parametr Z; itp.) - musi być możliwe skonfigurowanie odpowiedzi domyślnej dla przypadków wywołań z identyfikatorem nie występującym w konfiguracji
O47.F12	Dla każdej integracji przychodzącej do OSE OSS musi być możliwe przygotowanie wzorca wywołania z możliwością podmiany identyfikatora w wywołaniu.
O47.F13	Wykonawca musi zapewnić taki sposób zarządzania danymi testowymi w środowisku produkcyjnym, aby wszelkie generowanie raportów wykluczało ze swojej zawartości dane testowe.

Zgodnie z wymaganiami dotyczącymi równoważności rozwiązań, Zamawiający dopuszcza w ramach realizacji przedmiotu zamówienia zastąpienie obecnie posiadanego i wykorzystywanego przez Zamawiającego rozwiązania Sparx Enterprise Architect wdrożonym przez Wykonawcę rozwiązaniem równoważnym. W celu spełnienia wymogu równoważności, oprócz spełnienia wymagań zawartych w zapytaniu ofertowym, Wykonawca jest zobowiązany do zapewnienia kompatybilności i dopasowania zastosowanego komponentu Rozwiązania do istniejącej architektury korporacyjnej Zamawiającego (posiadanych przez Zamawiającego systemów, opisanych w niniejszym Zapytaniu Ofertowym), co jest rozumiane jako spełnienie następujących wymagań:

- zastosowane narzędzie musi realizować podstawowe funkcjonalności repozytorium architektonicznego umożliwiając zarządzanie wszystkimi obiektami wskazanymi przez zamawiającego jako dokumentowane w repozytorium
- zastosowane narzędzie musi umożliwiać tworzenie widoków na podstawie danych znajdujących się w repozytorium
- zastosowane narzędzie musi umożliwiać modelowanie cyklu życia artefaktów architektury biznesowej (takich jak procesy biznesowe) oraz architektury IT (systemy, moduły, infrastruktura).
- zastosowane narzędzie musi wspierać pracę grupową i umożliwiać jednoczesną pracę wieloosobową nad obiektami w repozytorium
- zastosowane narzędzie musi umożliwiać modelowanie z zastosowaniem notacji UML dla wszystkich rodzajów diagramów zdefiniowanych w UML
- zastosowane narzędzie musi umożliwiać modelowanie z zastosowaniem notacji BPMN
- zastosowane narzędzie musi umożliwiać zarządzanie wymaganiami, mapowanie ich na systemy realizujące wymagania i powiązanie ich z procesami biznesowymi
- zastosowane narzędzie musi umożliwiać generowanie dokumentacji w prosty sposób, czyli poprzez użycie ekranu do generowania, bez konieczności przygotowywania skryptów

- zastosowane narzędzie musi być oparte o bazę danych umożliwiając dostęp do danych w repozytorium za pośrednictwem zapytań bazodanowych (narzędzie musi wspierać co najmniej bazy danych Microsoft, Oracle, MySQL, PostgreSQL)
- zastosowane narzędzie musi umożliwiać eksportowanie / migrowanie repozytorium do Sparx Enterprise Architect posiadanego przez Zamawiającego.

Ewentualne zapewnianie funkcjonalności znajduje się po stronie wykonawcy. Aby zapewnić równoważność narzędzia należy zapewnić wyrównanie wiedzy i zasobów licencyjnych obecnie znajdujących się po stronie zamawiającego co oznacza:

- zapewnienie dodatkowych 5 licencji do narzędzia równoważnego (oprócz obecnie wymaganych w zapytaniu ofertowym)
- przeszkolenie 3 osób w zakresie administracji narzędziem, tworzenia i zarządzania repozytorium (oprócz obecnie wymaganych w zapytaniu ofertowym)
- przeszkolenia 10 osób w zakresie wykorzystania narzędzia, modelowania, zarządzania modelami, raportowania, konfigurowania (oprócz obecnie wymaganych w zapytaniu ofertowym).

7.3. Opis funkcjonalności dotyczących integracji

7.3.1. Automatyzacja, integracja i elastyczność całości rozwiązania

Sposoby i poziomy integracji docelowego stosu systemów OSS z urządzeniami sieci OSE i systemami NASK OSE i NASK, elastyczność Rozwiązania oraz automatyzacja zarówno integracji jak i wewnętrznych procesów Rozwiązania musi być maksymalna ze względu na skalę sieci OSE i potencjalną złożoność procesów operatora OSE.

Nr Wymagania	Treść Wymagania
O43.F1	Rozwiązanie musi się cechować maksymalnym stopniem automatyzacji procesów - w szczególności procesów związanych z provisioningiem usług i ich modyfikacji w sieci OSE jak i z utrzymywaniem świadczonych tych usług.
O43.F2	Rozwiązanie ma być spójną platformą systemową i aplikacyjną, wewnętrznie integrującą wszystkie wymagane funkcjonalności
O43.F3	Dostawca musi dostarczyć w ramach Rozwiązania kompletną platformę, co oznacza dopasowane środowisko aplikacyjne, systemowe , wirtualizacyjne i sprzętowe tak by spełniało wszystkie wymagania Zamawiającego
O43.F4	Rozwiązanie musi pozwalać na elastyczne definiowanie co najmniej następujących elementów: - scenariuszy provisioningu - scenariuszy pomiarów - urządzeń OSE instalowanych w szkole - urządzeń w szkielecie sici OSE - systemów sieciowych i bezpieczeństwa

Nr Wymagania	Treść Wymagania
	- łącz fizycznych i logicznych w warstwie dostępowej, agregacyjnej i szkieletowej - usług świadczonych przez OSE i usług wewnętrznych w ramach systemów nadzoru operatora OSE - statystyk i raportów - pól dla danych wykorzystywanych w systemach OSS - słowników stosowanych w systemach OSS
O43.F5	Rozwiązanie musi być gotowe na komunikację z urządzeniami OSE przy użyciu standardowych mechanizmów : - SNMP - Syslog - Netconf - Telnet - SSH - HTTP - REST API - pliki o standardowych formatch: TXT, CSV XML, JSON (np. pliki konfiguracyjne)
O43.F6	Rozwiązanie musi być gotowe na integracje przy użyciu standardowych mechanizmów integracji z systemami : - Element Managerami urządzeń sieciowych i bezpieczeństwa , - systemami bezpieczeństwa i sieci (np. System Retencji Logów, SWG, DNS, anty-DDos, system Zarzadzania Kolokacjami OSE) - systemami zewnętrznymi (NASK OSE, np. : Jira WF, Insight, sugarCRM, Centralny system Raportowy) oraz - przy pomocy protokołu SNMP, Syslog (monitoring systemów) - poprzez wymianę plików w standardowych formatach (co najmniej CSV, JSON, XML, XLS) - poprzez API (co najmniej REST API, SOAP) - poprzez skrypty integracyjne
O43.F7	Rozwiązanie musi być gotowe na integracje przy użyciu standardowych mechanizmów integracji i komunikacji z innymi systemami Zamawiającego: - pliki w standardowych formatach (co najmniej CSV, JSON, XML, XLS) - co najmniej REST API i SOAP - HTTP/HTTPS np. przekierowanie stron - na poziomie baz danych (ODBC, JDBC, skrypty SQL, inne) - na poziomie wymiany poczty elektronicznej (protokół SMTP) - skrypty integracyjne
O43.F8	Rozwiązanie musi zapewniać płynną skalowalność dla co najmniej 20-to krotnego zwiększenia liczby użytkowników systemów, co oznacza, że przy liniowym zwiększaniu zasobów infrastrukturalnych proporcjonalnie do przyrostu użytkowników nie wystąpi spadek wydajności.
O43.F9	W przypadku danych zesłownikowanych występujących w innych systemach Zamawiającego musi być zapewniona w Rozwiązaniu implementacja tych słowników oraz gotowość na elastyczne definiowanie kolejnych słowników.

7.3.2. Integracja z systemami zewnętrznymi

Aby pokazać złożoność i mnogość integracji Rozwiązania z systemami NASK OSE i NASK poniżej przedstawione zostały niezbędne do implementacji integracje z konkretnymi systemami :

systemy NASK OSE

- do 2 Element Managerów do ADC (w 2 węzłach centralnych, F5 Networks)
- do 16 Element Managerów do systemu SWG (w 16 węzłach regionalnych)
- do 2 Element Managerów do systemów NG Firewall (w 2 węzłach centralnych, Fortinet)
- 2 instancje Element Managera do urządzeń sieciowych (w 2 węzłach centralnych - jedna zapasowa, Juniper Network Director)
- 2 instancje SIEM (w 2 węzłach centralnych)
- 2 instancje Systemu Retencji Logów
- 2 instancje systemu zarządzania do systemu DNS (w 2 węzłach centralnych, Infoblox)
- 2 instancje Systemu Zarządzania Kolokacjami (zakup systemu w odrębnym postępowaniu zakupowym, jedna zapasowa)
- 2 instancje systemu anty-DDoS (w 2 węzłach centralnych)
- Jira WF i SD (procesy biznesowe OSE)
- Insight (OSE master Inventory)

Zamawiający nie wyklucza w zakresie systemów bezpieczeństwa zastosowania zagregowanego API

systemy NASK PIB

- SugarCRM
- Centralny System Raportowy
- Tree Confluence
- Active Directory (repozytorium użytkowników - pracownicy NASK PIB)
- Serwer Pocztowy

Nr Wymagania	Treść Wymagania
O44.F1	Rozwiązanie musi zapewniać spójność słowników stosowanych w obszarach zarówno OSE OSS jak i pozostałych systemach Zamawiającego.
O44.F2	Rozwiązanie musi zostać zintegrowane z innymi systemami Zamawiającego (np. z Insight, sugarCRM) celem pobierania danych w obszarze : kontrahentów, lokalizacji usług , urządzeń itp.
O44.F3	Rozwiązanie musi umożliwiać integrację z Element Managera'mi systemów bezpieczeństwa (NGFW, ADC, DNS, SWG) poprzez standardowe protokoły i otwarte mechanizmy integracyjne:

Nr Wymagania	Treść Wymagania
	- poprzez API (co najmniej REST API) - poprzez wymianę plików w standardowych formatach (co najmniej TXT, CSV, XML, JSON)
O44.F4	Rozwiązanie musi zapewniać provisioning usług i konfiguracji systemów bezpieczeństwa co najmniej na systemach NGFW, SWG, ADC, DNS z wykorzystaniem dedykowanych Element Managerów, interfejsów REST API lub modyfikacji plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym), co najmniej w zakresie: -Tworzenia i modyfikacji polityk bezpieczeństwa -Zmiany polityk bezpieczeństwa dla szkoły -> usunięcie jednego adresu IP z polityki A i dodanie go do polityki B -Dodawania wyjątków do polityk bezpieczeństwa -Włączania / wyłączania poszczególnych usług dla określonych przez zakres adresów IP Szczegółowy opis provisoningu został umieszczony w SOPZ w rozdziale "Opis funkcjonalności OSS", podrozdział "Provisioning"
O44.F5	Musi być zapewniona integracja wbudowanej w Rozwiązanie funkcjonalności Fault Management z urządzeniami OSE, systemami bezpieczeństwa, Element Managerami oraz systemami OSE w zakresie odbierania alarmów za pomocą protokołów/mechanizmów: - SYSLOG - SNMP trap - forwardowanie alarmów (np. z CPE via System Retencji Logów)
O44.F6	Musi być zapewniona integracja wbudowanej w Rozwiązanie funkcjonalności Performance Management z urządzeniami i systemami bezpieczeństwa oraz z systemami OSE - komunikacja protokołem SNMP ver. 2c lub ver. 3 , muszą być monitorowane co najmniej następujące parametry: - CPU – Idle time - CPU – Percentage spent on processes in the user space - CPU – Percentage spent on process in the system space - Memory – Total Free - Memory – Total Real - Memory – Avail. Swap - Storage – disk usage
O44.F7	Rozwiązanie musi zapewniać dla systemu SWG monitoring działania usługi poprzez: - monitoring polegający na cyklicznym wykonywaniu zapytania HTTP GET na stronę podaną przez Zamawiającego i podlegającą filtracji stronę WWW oraz sprawdzenie czy pojawia się strona blokowania, - monitoring polegający na wykonywaniu zapytania HTTP GET na podaną przez Zamawiającego stronę WWW i weryfikacja certyfikatu, którym podpisana jest ww. strona. Parametry certyfikatu powinny być tożsame z certyfikatem wgranym na systemie SWG
O44.F8	Musi być zapewniona integracja wbudowanej w Rozwiązanie funkcjonalności Fault Management z Systemem Retencji Logów w zakresie odbierania alarmów na temat działania i dostępności sieci za pomocą protokołów/mechanizmów: - SYSLOG - SNMP trap - forwardowanie alarmów zebranych z urządzeń CPE w szkołach (tylko SYSLOG)
O44.F9	System musi mieć możliwość przekazywania cyklicznych zaagregowanych danych i/lub raportów do Centralnego System Raportowego Zamawiającego co najmniej w zakresie:

Nr Wymagania	Treść Wymagania
	- alarmów, statystyk z FM i PM - danych inwentarzowych z CRM - danych dotyczących rozkładu ruchu w sieci OSE (w szczególności ruchu generowanego przez szkoły per VLAN/szkoła/lokalizacja szkolna) przy pomocy co najmniej: - wymiany danych standardowymi mechanizmami typu REST API - wymiany plików (TXT, CSV, XML, JSON) - wymiany plików graficznych - plików raportowych (PDF, XLS)
O44.F10	Musi być zapewniona integracja wbudowanej w Rozwiązanie funkcjonalności Performance Management z systemem SIEM - komunikacja protokołem SNMP ver. 2c lub ver. 3 , muszą być monitorowane co najmniej następujące parametry: - CPU – Idle time - CPU – Percentage spent on processes in the user space - CPU – Percentage spent on process in the system space - Memory – Total Free - Memory – Total Real - Memory – Avail. Swap - Storage – disk usage
O44.F11	Rozwiązanie musi umożliwiać integrację z Element Managera'mi szkieletowych urządzeń sieciowych poprzez standardowe protokoły i otwarte mechanizmy integracyjne. Rozwiązanie musi zostać zintegrowane przy założeniach : - integracja z Element Managerami odbywa się poprzez API - integracja m. in. służy uruchomieniu provisioningu usług i ich konfiguracji na szkieletowych urządzeniach sieciowych - w przypadku gdy niemożliwy jest provisioning bezpośrednio na szkieletowych urządzeniach sieciowych należy wykorzystać dedykowane funkcje Element Managerów dostępne poprzez interfejsy API lub poprzez modyfikację plików konfiguracyjnych - możliwość odbierania alarmów poprzez protokoły syslog i snmp trap (forwardowanie) a także możliwość pobierania alarmów poprzez udostępnione API Element Managera - odbieranie wyników pomiarów performance'owych poprzez udostępnione API Element Managera - zarządzanie pomiarami w relacjach E2E zakładanych na ruterach shadow via Element Manager - Juniper network Director (zakładanie pomiarów i pobieranie wyników pomiarów)
O44.F12	Rozwiązanie musi zapewnić mechanizm wzbogacania danych w innych systemach OSE (np. SWG) o dane zawarte w Inventory OSS na podstawie wybranych danych wejściowych (np. RSPO, id lokalizacji, adres IP) . Należy założyć różne metody udostępniania danych, co najmniej: - RESP API - pliki płaskie (np. XLC, CSV, JSON, XML)
O44.F13	Rozwiązanie musi zostać zintegrowane z zewnętrznym systemem zarządzania/monitorowania środowiskiem kolokacyjnym. Zamawiający zamierza jednym spójnym systemem objąć wszystkie centra kolokacyjne OSE. Należy założyć standardowe protokoły i otwarte mechanizmy integracyjne - co najmniej: - REST API - wymiana plików o standardowych formatach (TXT, CSV, XML, JSON, XLS)

Nr Wymagania	Treść Wymagania
O44.F14	Rozwiązanie musi być zintegrowane z systemem pocztowym NASK (niezbędne pod kontem co najmniej powiadomień oraz raportowania)
O44.F15	Rozwiązanie musi być zintegrowane z systemem anty-DDoS implementowanym przez NASK PIB co najmniej w zakresie : - odbierania z systemu anty-DDoS alarmów (SNMP Trap, Syslog) - monitorowania (availability & performance) systemu anty-DDoS (SNMP) - automatycznego zakładania ticketów w systemie OSS/BSS w wyniku alarmu na temat wykrytego ataku na sieć OSE - automatyczne akcje w wyniku alarmu na temat wykrytego ataku na sieć OSE (mail, wykonanie skryptu w shell)
O44.F16	system SSO implementowany przez Wykonawcę musi być zintegrowany z systemem Active Directory Zamawiającego w celu autoryzacji i uwierzytelniania użytkowników będących pracownikami NASK PIB
O44.F17	Rozwiązanie musi być zintegrowany z Centralnym Systemem Raportowym Zamawiającego w celu składowania w nim raportów. Preferowany kierunek przepływu danych to od systemu OSS do systemu raportowego, zatem Rozwiązanie musi posiadć mechanizmy "wystawiania" danych ze wszystkich swoich podsystemów składowych. Musi być wsparcie dla co najmniej: - REST API - export plików w standardowych formatach (np. TXT, CSV, XLS, XML, JSON) - widoki HTTP/HTTPS
O44.F18	Rozwiązanie musi zapewniać integrację z systemami BSS Zamawiającego (np. JIra SD) celem automatyzacji pozyskania informacji o pracach planowych i awariach masowych operatorów łącz. Informacje o okresach prac planowym muszą być użyte do "wyciszenia" alarmów z niedostępnością urzadzeń i usług a także odpowiedniego wyliczanie statystyk dostęnośći. Informacje o awariach masowych muszą być użyte do wzbogacenia raportów z działania sieci.
O44.F19	Należy zapewnić integrację repozytorium architektonicznego Sparx Enterprise Architect z TREE Confluence umożliwiając odświeżanie informacji na Tree na podstawie zmian w EA. Rozwiązanie powinno umożliwiać odświeżanie co najmniej następujących danych: - systemów / modułów (modeli wraz z opisami) - integracji pomiędzy modułami / systemami - diagramów sekwencji (modeli wraz z opisami kroków) - modeli klas / danych (modeli wraz z opisami)
O44.F20	Rozwiązanie wdrażane w obszarze OSS komunikację z innymi systemami zamawiającego powinno realizować w modelu usługowym zgodnym z koncepcją SOA (Service Oriented Architecture) w oparciu o usługi integracyjne.
O44.F21	System musi pozwalać na integrację poprzez zagregowane API - integracja z jednym systemem, który posiada integracje z kolejnymi systemami i zapewnia przeniesienie komunikacji dotyczącej np. żądań provisioningowych z OSS do tych systemów (w szczególności dotyczy to provisioningu usług na systemach bezpieczeństwa)

7.3.3. Usługi OSS

Rozwiązanie wdrażane w obszarze OSS komunikację z innymi systemami zamawiającego powinno realizować z wykorzystaniem poniżej zdefiniowanego katalogu usług OSS.

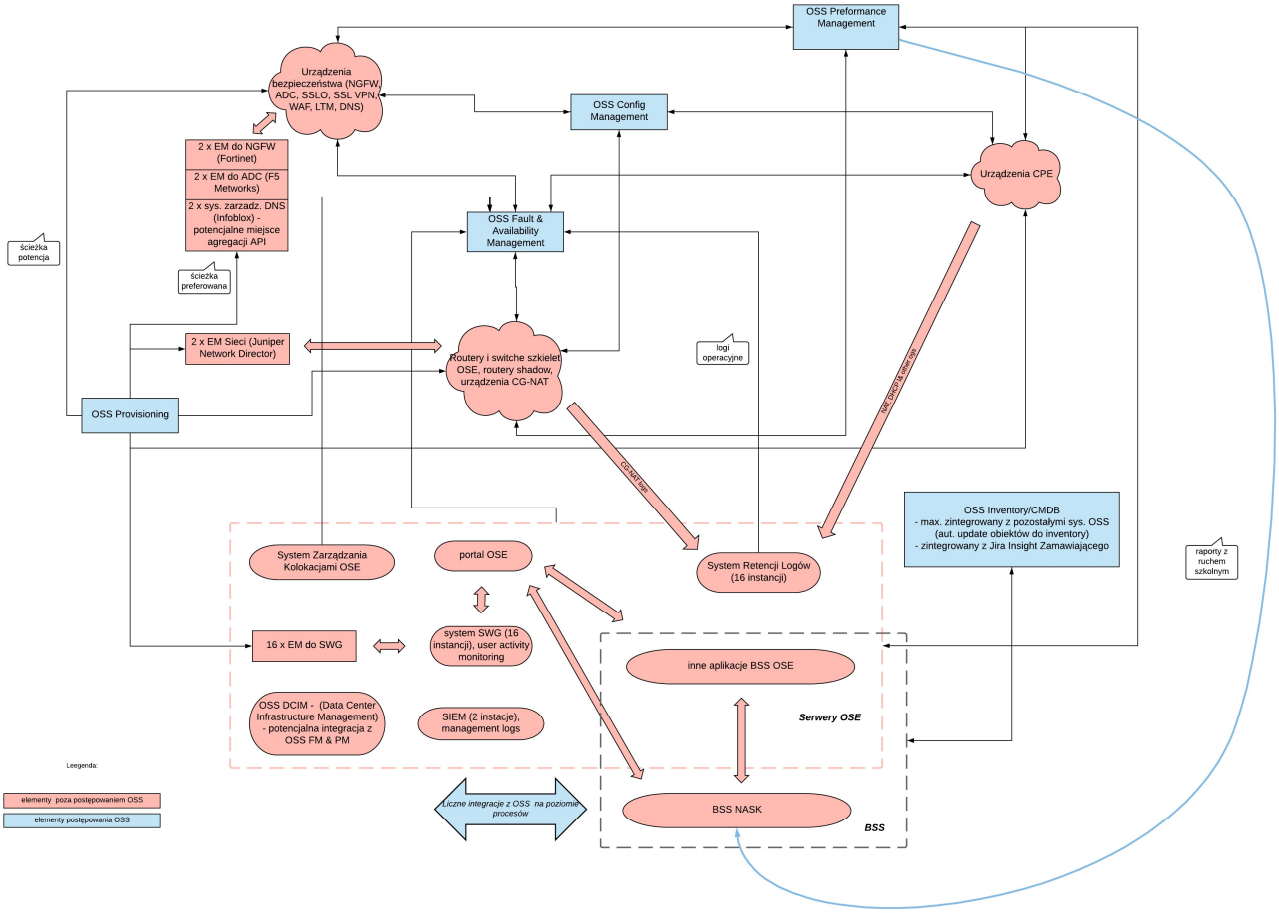
Identyfikator wymagania	Treść wymagania
O45.F1	Wykonawca wdroży usługę integracyjną udostępniającą możliwość zarządzania danymi operatora telekomunikacyjnego przypisywanego do łącza dostępowego (dodawanie nowego operatora, zmiana danych, przypisywanie do łącza, zmiana przypisania do łącza). Usługa będzie realizowała modyfikację danych w Rozwiązaniu. Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F2	Wykonawca wdroży usługę integracyjną umożliwiającą zlecenie wykonania pomiarów diagnostycznych dla wskazanej usługi na sieci OSE. Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F3	Wykonawca wdroży usługę integracyjną umożliwiająca pobranie wyników zleconych wcześniej pomiarów diagnostycznych wskazanej usługi na sieci OSE. Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F4	Wykonawca wdroży usługę integracyjną umożliwiająca przekazanie wyników zleconych wcześniej pomiarów diagnostycznych wskazanej usługi na sieci OSE do systemu jaki zlecił realizację pomiarów. Usługa będzie wywoływana z Rozwiązania w wyniku zakończenia realizacji zlecenia pomiaru diagnostycznego.
O45.F5	Wykonawca wdroży usługę integracyjną umożliwiającą pobranie danych wskazanej usługi wraz z parametrami oraz informacją na jakich zasobach jest realizowana. Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F6	Wykonawca wdroży usługę integracyjną umożliwiającą pobranie danych dotyczących zajętości punktu dostępowego, czyli lokalizacji. Na podstawie danych o lokalizacji będą zwracane informację o parametrach łącza doprowadzonego przez operatora do lokalizacji, oraz o usługach i parametrach obecnie realizowanych na danym łączy w punkcie dostępowym. Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F7	Wykonawca wdroży usługę integracyjną umożliwiającą przekazanie do Rozwiązania informacji o zarejestrowaniu nowej pracy planowej, lub zmianie danych / stanu wcześnie zarejestrowanej pracy planowej, lub o wystąpieniu awarii masowej. W wywołaniu będzie przekazywane dane zdarzenia oraz lista lokalizacji/ zasobów sieciowych i/lub usług dotkniętych zdarzeniem. Usługa będzie wywoływana z systemów OSE NASK / NASK.
O45.F8	Wykonawca wdroży usługę integracyjną umożliwiającą pobranie całego przebiegu łącza dla wskazanej lokalizacji szkolnej. W odpowiedzi będą przekazywane zarówno parametry techniczne łącza jak i formalne (operator odpowiedzialny). Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F9	Wykonawca wdroży usługę intgeracyjną umożliwiającą pobieranie i rezerwację (modyfikacje rezerwacji) zasobów logicznych wykorzystywanych w procesie dostarczania / provisoningu usług takich jak np.. numery IP. Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.

Identyfikator wymagania	Treść wymagania
O45.F10	Wykonawca wdroży usługę integracyjną umożliwiającą pobranie informacji o technicznych możliwościach świadczenia usług w danej lokalizacji (lub ewentualnej informacji o przyszłym terminie możliwości świadczenia usług). Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F11	Wykonawca wdroży usługę integracyjną umożliwiającą pobranie informacji o zleceniach provisioningu usług dla wskazanej lokalizacji (z możliwością filtrowania po zakresie dat, statusie). Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F12	Wykonawca wdroży usługę umożliwiającą zarządzanie wskazanym zleceniem provisioningu usług (jego wstrzymanie, anulowanie, wznowienie). Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F13	Wykonawca wdroży usługę integracyjną umożliwiającą składanie zleceń provisioningu usług. W zakresie zleceń musi być możliwa zarówno aktywacja usług, dezaktywacja jak i modyfikacja parametrów aktywnych usług. Usługa będzie możliwa do wywołania z dowolnego systemu OSE NASK / NASK.
O45.F14	Wykonawca wdroży usługę integracyjną umożliwiającą poinformowanie systemu jaki złożył zlecenie provisioningu usług o zmianie statusu tego zlecenia. Usługa będzie wywoływana przez Rozwiązanie odpowiedzialny za realizację provisioningu w wyniku zmiany statusu operacji provisioningu usług.

7.4. Opis funkcjonalności dla obszaru OSS

Wszystkie elementy systemu OSS mają być z założenia maksymalnie ze sobą zintegrowane i zautomatyzowane. Te założenia dotyczą też integracji z siecią OSE i systemami Zamawiającego.

Celem lepszego zrozumienia tych integracji poniżej przedstawiony został poglądowy rysunek przepływów pomiędzy systemami OSS a siecią i systemami OSE Zamawiającego:



7.4.1. Monitorowanie infrastruktury i usług OSE (Fault & Availability oraz Performance Management)

Systemy monitorowania sieci OSE powinny obejmować dwie poniższe domeny systemów, które realizują zadania modelu zarządzania siecią telekomunikacyjną FCAPS (Fault, Configuration, Accounting, Availability, Performance, Security):

- Fault & Availability Management (FM) – moduł pozwalający na wykrywanie i kontrolowanie awarii i usterek występujących w OSE poprzez ciągłe monitorowanie wszystkich elementów systemu, aktywne monitorowanie ich dostępności oraz odbiór i przetwarzanie zdarzeń pasywnych z monitorowanej infrastruktury.
- Performance Management (PM) – moduł pozwalający na monitorowanie w sposób ciągły wydajności wszystkich elementów systemu OSE i przekazywanie informacji na temat wykrytych problemów do systemu FM.

Obydwie ww. domeny monitoringu muszą być zaprojektowane warstwowo tak by wyodrębnić warstwy funkcjonalne, które pozwolą uelastycznić architekturę systemu monitorowania - warstwy te obejmują:

- warstwę kolekcji danych – odpowiedzialnej za udostępnienie interfejsów południowych i pobieranie danych z elementów monitorowanej infrastruktury. Realizowane są tu również zadania wstępnej filtracji i normalizacji danych, konfiguracji trybu i sposobu monitorowania elementów, jak również zadania związane z wykrywaniem infrastruktury sieciowej i włączaniem jej do struktur monitorowania;
- warstwę agregacji i przetwarzania – odpowiedzialnej za procesowanie, korelację i składowanie kolekcjonowanych danych w ramach centralnego repozytorium. W warstwie tej realizowane są również zadania związane z analizą danych, ich korelacją, integracją z innymi systemami OSS/BSS oraz wspomaganiem obsługi operatorskiej (m. in. automatycznymi eskalacjami);
- warstwę prezentacji – realizującej zadania związane z szeroko pojętym raportowaniem stanu monitorowanej infrastruktury, zarówno w formie prezentacji w czasie rzeczywistym, jak i udostępnianiem raportów historycznych czy predykcji utylizacji sieci w formie trendów. W ramach tej warstwy umieszczamy również zadania związane z przydzielaniem odpowiednich poziomów dostępu użytkownikom systemu w zależności od ich roli w strukturach organizacyjnych zapewniały możliwość pracy w modelu z rozproszoną kolekcją zdarzeń i danych wydajnościowych. Systemy powinny zapewnić możliwość uruchamiania zewnętrznych, względem modułów centralnych, kolektorów danych wydajnościowych i sond kolekcjonujących zdarzenia pasywne.

Wymaga się, aby systemy Fault & Availability oraz Performance Management zapewniały możliwość pracy w modelu z rozproszoną kolekcją zdarzeń i danych wydajnościowych. Systemy powinny zapewnić możliwość uruchamiania zewnętrznych, względem modułów centralnych, kolektorów danych wydajnościowych i sond kolekcjonujących zdarzenia pasywne.

Kolektory i sondy mają agregować zebrane dane i przekazywać je do systemu centralnego. Taka architektura zapewnia następujące korzyści:

- rozłożenie obciążenia systemu związanego ze znaczną ilością monitorowanych urządzeń/systemów;
- buforowanie danych na poziomie kolektorów/sond i odciążenie centralnych systemów;
- możliwość filtracji szumu informacyjnego na poziomie sond;
- optymalizację pracy systemu poprzez wstępne procesowanie i normalizację zdarzeń na poziomie sond/kolektorów;
- zwiększoną elastyczność konfiguracji systemu poprzez możliwość dostosowywania parametrów poszczególnych kolektorów/sond do specyfiki monitorowanego segmentu sieci;
- skalowalność horyzontalną i możliwość prostej rozbudowy systemu poprzez dołożenie dodatkowych sond/kolektorów i/lub instancji systemu centralnego.

W szczególności obydwa systemy muszą mieć możliwość integracji z systemami typu Element Managers w celu odbierania alarmów oraz pobierania danych wydajnościowych. NASK planuje wdrożenie wielu Element Manager'ów: w obszarze sieciowym, w obszarze bezpieczeństwa, w obszarze zarządzania infrastrukturą serwerową oraz w obszarze zarządzania środowiskiem kolokacyjnym. Operator OSE będzie kolokował swoje urządzenia w 16tu centrach kolokacyjnych w całej Polsce. W celu sprawnego

monitorowania środowiska kolokacyjnego (dzierżawione szafy z niezbędnymi czujnikami parametrów środowiska) zostanie wdrożony wspólny system zarządzania, który swym zasięgiem obejmie wszystkie kolokacje - zarówno centrum kolokacyjne NASK jak i pozostałe centra (dzierżawione szafy).

Obydwa systemy (FM i PM) muszą w wygodny sposób prezentować zbierane informacje tak, aby w szybki sposób można było wyszukiwać przyczynę awarii oraz wyszukiwać stosowne statystyki i raporty pomimo dużej ilości danych pochodzących z wszystkich urządzeń OSE - w szczególności z rozbiciem tych informacji na logiczne i geograficzne obszary a także per jednostki oświatowe i świadczone im usługi. System Performance Management musi być ściśle zintegrowany z częścią Fault & Availability Management, obydwa systemy w ramach Rozwiązania mają być prezentowane w uspójnionym jednym logowaniem interface'ie graficznym.

Podstawowe funkcje wymagane w warstwie prezentacji to:

- własny, spójny interfejs operatorski i administracyjny,
- podstawowym interfejsem systemu ma być aplikacja webowa, stanowiąca konsolę operatorsko-administracyjną,
- interfejs systemu ma umożliwiać dostosowywanie widoków, dashboardów, etc. do specyficznych wymagań użytkowników,
- interfejs webowy systemu powinien być przystosowany do jego wykorzystania w ramach NOC i SOC operatora OSE
- dostępność udokumentowanego API systemu, które pozwoli na pobranie odpowiednich danych za pomocą aplikacji/systemu odpowiedzialnego za wystawienie danych np. do portalu OSE
- natywny interfejs webowy systemu monitorowania powinien być wspierany przez popularne przeglądarki internetowe

Istotnym aspektem warstwy prezentacji systemów jest mechanizm raportowy, który musi mieć możliwość generowania raportów w swoim natywnym mechanizmie, ale również być źródłem danych dla centralnego systemu raportowania (system w NASK PIB), gdzie raporty typowo technicznych aspektów będą mogły być porównane z aspektami biznesowymi. Zwłaszcza w przypadku systemu Performance Management tych raportów będzie bardzo dużo i muszą one spełniać szereg wymagań, a w szczególności:

- system musi udostępniać predefiniowane zestawy raportów, na przykład grupowane ze względu na typy dostępnych pomiarów, typ raportu, usługę. Przykładowe predefiniowane raporty:
    - raporty prezentujące statystyki ruchu sieciowego (m. in. utylizację interfejsów, opóźnienia, jitter);
    - raporty dostępności za określony czas;
    - raporty porównawcze np. tego samego typu raportu dla dwóch różnych elementów, pozwalających na analizę wskaźników wydajnościowych w tym samym okresie pomiaru; o Raport wszystkich wskaźników monitorowanych na danym typie elementu; o Raporty typu Top N według różnych kryteriów;

- raporty typu inventory korzystające z zasobów określonych w ramach procesu automatycznego wykrywania siec

- system powinien umożliwiać definiowanie harmonogramów dla automatycznego generowania raportów oraz ich udostępniania, np. poprzez email;
- użytkownicy systemu muszą mieć możliwość tworzenia własnych raportów, udostępniania ich w postaci szablonów innym użytkownikom. Narzędzie służące tworzeniu raportów powinno posiadać intuicyjny graficzny interfejs;
- generowanie raportów w standardowych formatach np. PDF, CSV oraz XLS
- szablony raportów udostępniane w ramach systemu (domyślne i utworzone przez użytkowników) powinny zapewniać parametryzację, np. określenie zakresu czasowego, czy listy interfejsów.

Systemy monitorowania sieci OSE powinny obejmować dwie poniższe domeny systemów, które realizują zadania modelu zarządzania siecią telekomunikacyjną FCAPS (Fault, Configuration, Accounting, Performance, Security):

- Fault & Availability Management (FM) – moduł pozwalający na wykrywanie i kontrolowanie awarii i usterek występujących w OSE poprzez ciągłe monitorowanie wszystkich elementów systemu, aktywne monitorowanie ich dostępności oraz odbiór i przetwarzanie zdarzeń pasywnych z monitorowanej infrastruktury.
- Performance Management (PM) – moduł pozwalający na monitorowanie w sposób ciągły wydajności wszystkich elementów systemu OSE i przekazywanie informacji na temat wykrytych problemów do systemu FM.

Obydwie ww. domeny monitoringu muszą być zaprojektowane warstwowo tak by wyodrębnić warstwy funkcjonalne, które pozwolą uelastycznić architekturę systemu monitorowania - warstwy te obejmują:

- warstwę kolekcji danych – odpowiedzialnej za udostępnienie interfejsów południowych i pobieranie danych z elementów monitorowanej infrastruktury. Realizowane są tu również zadania wstępnej filtracji i normalizacji danych, konfiguracji trybu i sposobu monitorowania elementów, jak również zadania związane z wykrywaniem infrastruktury sieciowej i włączaniem jej do struktur monitorowania;
- warstwę agregacji i przetwarzania – odpowiedzialnej za procesowanie, korelację i składowanie kolekcjonowanych danych w ramach centralnego repozytorium. W warstwie tej realizowane są również zadania związane z analizą danych, ich korelacją, integracją z innymi systemami OSS/BSS oraz wspomaganiem obsługi operatorskiej (m. in. automatycznymi eskalacjami);
- warstwę prezentacji – realizującej zadania związane z szeroko pojętym raportowaniem stanu monitorowanej infrastruktury, zarówno w formie prezentacji w czasie rzeczywistym, jak i udostępnianiem raportów historycznych czy predykcji utylizacji sieci w formie trendów. W ramach tej warstwy umieszczamy również zadania związane z przydzielaniem odpowiednich poziomów dostępu użytkownikom systemu w zależności od ich roli w strukturach organizacyjnych zapewniały możliwość pracy w modelu z rozproszoną kolekcją zdarzeń i danych wydajnościowych. Systemy powinny zapewnić możliwość uruchamiania zewnętrznych, względem modułów centralnych, kolektorów danych wydajnościowych i sond kolekcjonujących zdarzenia pasywne.

Wymaga się, aby systemy Fault & Availability oraz Performance Management zapewniały możliwość pracy w modelu z rozproszoną kolekcją zdarzeń i danych wydajnościowych. Systemy powinny zapewnić możliwość uruchamiania zewnętrznych, względem modułów centralnych, kolektorów danych wydajnościowych i sond kolekcjonujących zdarzenia pasywne.

Kolektory i sondy mają agregować zebrane dane i przekazywać je do systemu centralnego. Taka architektura zapewnia następujące korzyści:

- rozłożenie obciążenia systemu związanego ze znaczną ilością monitorowanych urządzeń/systemów;
- buforowanie danych na poziomie kolektorów/sond i odciążenie centralnych systemów;
- możliwość filtracji szumu informacyjnego na poziomie sond;
- optymalizację pracy systemu poprzez wstępne procesowanie i normalizację zdarzeń na poziomie sond/kolektorów;
- zwiększoną elastyczność konfiguracji systemu poprzez możliwość dostosowywania parametrów poszczególnych kolektorów/sond do specyfiki monitorowanego segmentu sieci;
- skalowalność horyzontalną i możliwość prostej rozbudowy systemu poprzez dołożenie dodatkowych sond/kolektorów i/lub instancji systemu centralnego.

W szczególności obydwa systemy muszą mieć możliwość integracji z systemami typu Element Managers w celu odbierania alarmów oraz pobierania danych wydajnościowych. NASK planuje wdrożenie wielu Element Manager'ów: w obszarze sieciowym, w obszarze bezpieczeństwa, w obszarze zarządzania infrastrukturą serwerową oraz w obszarze zarządzania środowiskiem kolokacyjnym. Operator OSE będzie kolokował swoje urządzenia w 16tu centrach kolokacyjnych w całej Polsce. W celu sprawnego monitorowania środowiska kolokacyjnego (dzierżawione szafy z niezbędnymi czujnikami parametrów środowiska) zostanie wdrożony wspólny system zarządzania, który swym zasięgiem obejmie wszystkie kolokacje - zarówno centrum kolokacyjne NASK jak i pozostałe centra (dzierżawione szafy).

Obydwa systemy (FM i PM) muszą w wygodny sposób prezentować zbierane informacje tak, aby w szybki sposób można było wyszukiwać przyczynę awarii oraz wyszukiwać stosowne statystyki i raporty pomimo dużej ilości danych pochodzących z wszystkich urządzeń OSE - w szczególności z rozbiciem tych informacji na logiczne i geograficzne obszary a także per jednostki oświatowe i świadczone im usługi. System Performance Management musi być ściśle zintegrowany z częścią Fault & Availability Management, obydwa systemy w ramach Rozwiązania mają być prezentowane w uspójnionym jednym logowaniem interface'ie graficznym.

Podstawowe funkcje wymagane w warstwie prezentacji to:

- własny, spójny interfejs operatorski i administracyjny,
- podstawowym interfejsem systemu ma być aplikacja webowa, stanowiąca konsolę operatorsko-administracyjną,
- interfejs systemu ma umożliwiać dostosowywanie widoków, dashboardów, etc. do specyficznych wymagań użytkowników,

- interfejs webowy systemu powinien być przystosowany do jego wykorzystania w ramach NOC i SOC operatora OSE
- dostępność udokumentowanego API systemu, które pozwoli na pobranie odpowiednich danych za pomocą aplikacji/systemu odpowiedzialnego za wystawienie danych np. do portalu OSE
- natywny interfejs webowy systemu monitorowania powinien być wspierany przez popularne przeglądarki internetowe

Istotnym aspektem warstwy prezentacji systemów jest mechanizm raportowy, który musi mieć możliwość generowania raportów w swoim natywnym mechanizmie, ale również być źródłem danych dla centralnego systemu raportowania (system w NASK PIB), gdzie raporty typowo technicznych aspektów będą mogły być porównane z aspektami biznesowymi. Zwłaszcza w przypadku systemu Performance Management tych raportów będzie bardzo dużo i muszą one spełniać szereg wymagań, a w szczególności:

- system musi udostępniać predefiniowane zestawy raportów, na przykład grupowane ze względu na typy dostępnych pomiarów, typ raportu, usługę. Przykładowe predefiniowane raporty:
    - raporty prezentujące statystyki ruchu sieciowego (m. in. utylizację interfejsów, opóźnienia, jitter);
    - raporty dostępności za określony czas;
    - raporty porównawcze np. tego samego typu raportu dla dwóch różnych elementów, pozwalających na analizę wskaźników wydajnościowych w tym samym okresie pomiaru; o Raport wszystkich wskaźników monitorowanych na danym typie elementu; o Raporty typu Top N według różnych kryteriów;
    - raporty typu inventory korzystające z zasobów określonych w ramach procesu automatycznego wykrywania siec
- system powinien umożliwiać definiowanie harmonogramów dla automatycznego generowania raportów oraz ich udostępniania, np. poprzez email;
- użytkownicy systemu muszą mieć możliwość tworzenia własnych raportów, udostępniania ich w postaci szablonów innym użytkownikom. Narzędzie służące tworzeniu raportów powinno posiadać intuicyjny graficzny interfejs;
- generowanie raportów w standardowych formatach np. PDF, CSV oraz XLS
- szablony raportów udostępniane w ramach systemu (domyślne i utworzone przez użytkowników) powinny zapewniać parametryzację, np. określenie zakresu czasowego, czy listy interfejsów.

7.4.1.1 Funkcjonalność Fault & Availability Management

Celem systemu Fault & Availability Management jest wsparcie pracy zespołów NOC, SOC i IT w zakresie utrzymania sieci, usług i systemów OSE. System musi być elastyczny i pozwalać na monitowanie zarówno działania szkieletu sieci OSE jak i sieci agregacyjnej i dostępowej a także heterogenicznych urządzeń OSE instalowanych w sieci LAN w szkołach.

System Fault Management ma pozwalać na zbieranie alarmów (pasywny monitoring) wygenerowanych bezpośrednio przez urządzenia i systemy sieciowe w szkielecie OSE oraz w jednostkach oświatowych, przez systemy w centrach kolokacji, aplikacje czy dowolne elementy infrastruktury teleinformatycznej potrafiące poinformować system nadrzędny (Fault Managment) o swoim stanie, natomiast System Availability Management pozwoli na sprawdzanie dostępności urządzeń i usług (aktywne monitorowanie) w szczególności systemy te będą monitorować:

- wszystkie urządzenia sieciowe sieci szkieletowej zainstalowane w węzłach centralnych i regionalnych (rutery, switche, firewalle, urządzenia SWG, inne)
- infrastruktura serwerowa, systemowa i aplikacyjna w centrach danych (jak systemy: SIEM, Retencja, Portal OSE, inne)
- urządzenia OSE w szkołach
- urządzenia sieci zarządzającej
- systemy typu Element Management nadzorujące urządzenia sieciowe i systemy zarządzania urządzeniami bezpieczeństwa w węzłach centralnych
- dedykowane systemy sieci/bezpieczeństwa (jak Retencja, SWG, inne) w węzłach regionalnych

W przypadku systemu Fault Management bardzo ważną rolę odgrywa wspomniana wyżej warstwa agregacji i przetwarzania, która odpowiedzialna jest za procesowanie, korelację i składowanie kolekcjonowanych danych w ramach centralnego repozytorium. W warstwie tej realizowane są głównie zadania związane z analizą danych, ich korelacją, integracją z innymi systemami OSS/BSS oraz wspomaganiem obsługi operatorskiej. Centralne repozytorium zdarzeń powinno zapewniać następujące główne funkcjonalności w zakresie przetwarzania danych:

- podstawową korelację zdarzeń:
    - deduplikację, czyli identyfikację alarmów dotyczącą dokładnie tego samego zdarzenia i przechowywanie go w repozytorium, jako jednego rekordu,
    - automatyczną korelację ON/OFF, czyli parowanie zdarzeń, które oznaczają wystąpienie awarii i jej zakończenie,
    - filtrację, automatyczne usuwanie z określonych widoków alarmów na podstawie zdefiniowanego kryterium,
    - eskalację – automatyczne powiadomienia wywoływane na podstawie alarmów (opisane szczegółowo w dalszej części dokumentu).
- automatyczne wykonywanie akcji (np. skryptu) na podstawie zarejestrowanych zdarzeń pozwalające na automatyczne wykonywanie akcji naprawczych takich jak np. restart usługi czy restart portu urządzenia. Wywołanie akcji może być realizowane poprzez integrację z systemem Config Manager i wykorzystanie zadań konfiguracyjnych zdefiniowanych w tym systemie; mechanizmy archiwizacji zdarzeń aktywnych w bazie zdarzeń historycznych;
- diagnostykę i monitoring wydajności przetwarzania zdarzeń/alarmów.

Podobnie bardzo istotnym elementem systemu Fault Management jest możliwość analizy kolekcjonowanych danych i ich korelacja. W przypadku infrastruktury OSE spodziewana jest kolekcja

bardzo znaczącej ilości danych i z tego względu ważne jest, aby system udostępniał, co najmniej zestaw poniższych podstawowych automatyzacji, które pozwalają na efektywną analizę danych:

- deduplikacja – grupowanie komunikatów dotyczących dokładnie tego samego zdarzenia w ramach jednego rekordu. W ramach funkcjonalności pożądane jest, aby był dostęp do informacji na temat czasu pierwszego i ostatniego wystąpienia zdarzenia, liczby wystąpień itp.
- automatyczna korelacja ON/OFF polegająca na parowaniu zdarzeń informujących o zaistnieniu awarii oraz o jej zakończeniu. Zdarzenia podlegające takiej korelacji po zakończeniu awarii mają ustawiany niższy priorytet i są przechowywane jeszcze przez określony czas, jednak docelowo są automatycznie usuwane zgodnie z założona polityką czyszczenia i archiwizacji zdarzeń w bazie.
- filtrację zdarzeń – funkcjonalność realizowana już w warstwie kolekcji systemu, ale również w warstwie przetwarzania pozwalająca na grupowanie zdarzeń zgodnie z określonymi potrzebami, np.w przypadku zdarzeń tzw. bezstanowych, które nie podlegają korelacji ON/OFF, a mimo wszystko powinny być odnotowane i zaprezentowane użytkownikom systemu lub system powinien umożliwiać ich automatyczne usuwanie z repozytorium, np. po potwierdzeniu przez operatora albo poprzez możliwość definiowania czasu przechowywania takiego zdarzenia w systemie
- kategoryzację danych – funkcjonalność, która zapewni możliwość oznaczania i agregowania kolekcjonowanych zdarzeń w ramach zdefiniowanych w systemie grup i/lub kategorii, na przykład przydzielanie urządzeń i ich zdarzeń do odpowiednich rejonów geograficznych lub według kryteriów organizacyjnych;
- wzbogacanie zdarzeń w zakresie informacji dostępnych w pozostałych systemach OSS/BSS (w szczególności Inventory i CRM)

Bardzo użyteczną funkcjonalnością związaną z monitorowaniem awarii w sieci jest funkcjonalność automatycznego wykrywania topologii sieci i związanego z tym mechanizmu wykrywania przyczyny pierwotnej awarii (RCA - Root Cause Analysis). Ta wymagana funkcjonalność będzie ograniczać ilość zdarzeń generowanych w systemie w przypadku awarii (zwłaszcza awarii masowych). Funkcjonalność automatycznego wykrywania sieci wraz z funkcją RCA oraz z możliwością prezentacji topologii sieci z różnej perspektywy np. widoki topologii warstwy 2 lub 3 dostępne są w ramach dedykowanych aplikacji realizujących funkcje Topology Management. Zakłada się, że dostarczone Rozwiązanie powinno mieć tę funkcjonalność zaimplementowaną przynajmniej w obszarze węzłów OSE.

<u>Założenia dotyczące architektury pomiarów</u>

1. W zakresie Fault & Availability Management sieć szkieletowa OSE, czyli wszystkie urządzenia w węzłach centralnych i regionalnych OSE (zarówno urządzenia sieciowe jak i urządzenia i systemy bezpieczeństwa oraz serwery) będą wysyłać pewne spectrum syslogów i trapów SNMP (zdefiniowane na etapie HLD). Zakłada się również uruchomienie monitoringu przy pomocy RTT ICMP dostępności urządzeń (na ip adresu loopback) , portów fizycznych i logicznych (na adresy skonfigurowane na portach) jak również przy pomocy protokołu TCP dostępności usług (odpowiedzi pakietów wysłanych do zdefiniowany port TCP) z częstotliwością, co najmniej 300 sekund. W przypadku braku dostępności generowany jest alarm do systemu Fault & Availability Management (brak dostępności będzie wynikać z założonych kryteriów zdefiniowanych na poziomie HDL).

2. W przypadku urządzeń zainstalowanych w szkole trapy SNMP nie będą wysyłane, pakiety syslog natomiast będą przesyłane tylko z CPE i tylko w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki zgłoszonych przez szkołę problemów. Logi z CPE będą przesyłane do kolektora systemu Retencji Logów ze względu na ograniczoną funkcjonalność urządzeń CPE (brak możliwości wysyłania logów do dwóch Fault Managerów jednocześnie). Logi istotne ze względu na utrzymanie urządzeń (zdefiniowane na etapie HLD) będą następnie przekierowywane z ww. kolektora do systemu Fault & Availability Management. Aktywny monitoring CPE przy pomocy pakietów RTT ICMP będzie prowadzony tylko w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki zgłoszonych przez szkołę problemów. W przypadku urządzeń SW i AP monitoring taki będzie aktywowany tylko w przypadku zgłoszonych problemów ze szkoły i po decyzji operatora OSE i skonfigurowaniu dostępu do tych urządzeń by był możliwy, zatem tylko w szczególnych przypadkach. Zakłada się częstotliwość pomiarów RTT ICMP na poziomie 300 sekund.

Wymagania funkcjonalne

Podobszar	Nr Wymagania	Treść Wymagania
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F1	system musi monitorować dostępność (aktywny monitoring RTT ICMP) wszystkich aktywnych interface'ów fizycznych i logicznych na urządzeniach szkieletowych uwzględniając również rutery logiczne oraz instancje VRF
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F2	system musi odbierać wysyłane do niego z urządzeń sieciowych i urządzeń/systemów bezpieczeństwa zainstalowanych w sieci szkieletowej trapy SNMP v2c, v3
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F3	system musi odbierać logi SYSLOG (zgodne z RFC 5424) wysyłane do niego z urządzeń sieciowych i urządzeń/systemów bezpieczeństwa zainstalowanych w sieci szkieletowej, należy założyć że urządzenia będą logowały zdarzenia z severity co najmniej warning (warning i bardziej krytyczne)
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F4	system musi przyjmować alarmy generowane w wyniku przekroczeń progów założonych na pomiarach performance'owych zarówno pobieranych z urządzeń przy pomocy protokołu SNMP z dowolnych urządzeń OSE jak i jako strumień danych telemetrycznych ze szkieletowych urządzeń sieciowych OSE
Szczególne wymagania pod kątem monitorowania	O11.F5	system musi mieć możliwość odbierania i odpowiedniego interpretowania wysyłanych do niego trap'ów SNMP v2c, v3 z urządzeń zainstalowanych w

Podobszar	Nr Wymagania	Treść Wymagania
dostępności urządzeń w sieci LAN w szkołach		szkołach (CPE, Switch , Acces Point wi-fi) - potencjalnie operator OSE może zadecydować w dowolnym momencie projektu, że incydentalnie trapy SNMP będą wysyłane z urządzeń zainstalowanych w szkołach
Szczególne wymagania pod kątem monitorowania dostępności urządzeń w sieci LAN w szkołach	O11.F6	urządzenia CPE w szkołach będą wysyłać logi typu SYSLOG (zgodne z RFC 5424) do kolektora systemu Retencji Logów (z obszarów DHCP i NAT, na temat stanu urządzenia itp.) ponieważ funkcjonalność CPE (kupowane sukcesywnie w przetargach i dostarczane przez beneficjentów POCP) może nie pozwalać na przesyłanie logów SYSLOG równolegle do dwóch odbiorców : Fault Managera i Systemu Retencji Logów. Zatem : - system musi wspierać otrzymywanie/pobieranie logów SYSLOG z Systemu Retencji Logów (severity z poziomu warning i bardziej krytyczne) na temat stanu urządzeń CPE - należy założyć że standardowa metoda komunikacji to wysyłanie logów przez System Retencji Logów do systemu OSS FM, natomiast potencjalną konieczność pobierania tych logów przez system OSS FM z systemu Retencji Logów należy traktować jako podejście rezerwowe na wypadek problemów z metodą standardową
Szczególne wymagania pod kątem monitorowania dostępności urządzeń w sieci LAN w szkołach	O11.F7	system musi odbierać pakiety syslog przesyłane z CPE (via system Retencji Logów) w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki (należy założyc średnio do 2 tygodni) zgłoszonych przez szkołę problemów ; należy uwzględnić wymiarowanie przedstawione w rozdz. "Informacje mające wpływ na architekturę Rozwiązania"
Szczególne wymagania pod kątem monitorowania dostępności urządzeń w sieci LAN w szkołach	O11.F8	system musi prowadzić aktywny monitoring dostępności urządzenia CPE przy pomocy pakietów RTT ICMP w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki (należy założyc średnio do 2 tygodni) zgłoszonych przez szkołę problemów; należy uwzględnić wymiarowanie przedstawione w rozdz. "Informacje mające wpływ na architekturę Rozwiązania"
Szczególne wymagania pod kątem monitorowania dostępności urządzeń w sieci LAN w szkołach	O11.F9	system musi jednoznacznie identyfikować urządzenia po adresie (np. loopback) i dokonywać jego translacji na nazwę urządzenia by prezentować alarmy per nazwa urządzenia celem prostszej identyfikacji źródła alarmu (schemat nazewnictwa urządzeń będzie zdefiniowany przez Zamawiającego na etapie wdrożenia - należy założyć, że w nazwach urządzeń będą zaszyte informacje terytowe)
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F10	standardowo urządzenia OSE w szkołach typu Switch i Access Pointy wi-fi nie będą standardowo wysyłać logów SYSLOG i trapów SNMP do systemu, jednakże system musi być gotowy na ich odbieranie ad. hoc. w miarę potrzeb w celu diagnostyki tych urządzeń (należy założyc średnio do 2 tygodni takiej diagnostyki)
Szczególne wymagania pod kątem monitorowania	O11.F11	system musi umożliwiać integrację z dedykowanym systemem zarządzania infrastrukturą serwerową (będącą częścią Rozwiązania) na poziomie odbierania

Podobszar	Nr Wymagania	Treść Wymagania
urządzeń infrastruktury serwerowej		logów SYSLOG (zgodnie z FRC 5424) i trapów SNMP (v2c, v3) a także na poziomie standardowych mechanizmów integracji (co najmniej REST API, pliki w formatach CSV, TXT, XML, JSON) celem prezentowania najważniejszych alarmów dla NOC/SOC w jednym miejscu, czyli w systemie typu umbrella (Fault Management)
Wymagania wspólne	O11.F12	alarmy, które trafiają do systemu Fault Management muszą być raportowane do operatorów w NOC przy założeniu różnej gradacji alarmów (np. operator III linii widzi tylko alarmy krytyczne) oraz grupowania alarmów (np. operatorzy systemów bezpieczeństwa widzą tylko alarmy dotyczące bezpieczeństwa lub wydzielona część NOC widzi tylko alarmy z danego obszaru geograficznego sieci OSE)
Wymagania wspólne	O11.F13	system musi zapewniać możliwość generowania raportów zbiorczych, które będą dostępne np. dla kierownictwa operatora OSE
Wymagania wspólne	O11.F14	system musi wspierać implementację architektury rozproszonej – możliwość kolekcji danych poprzez wydzielone dedykowane moduły programowe (sondy)
Wymagania wspólne	O11.F15	Celem mniejszego obciążania łącz pomiędzy węzłami OSE system musi zostać zaimplementowany w architekturze rozproszonej, by kolekcja zdarzeń znajdowała się jak najbliżej źródła zdarzenia; należy uwzględnić architekturę zapewniającą to, że logiczne warstwy systemu wymagające większej wydajności i niezawodności (warstwa prezentacji i przetwarzania danych) były ulokowane w węzłach centralnych; jednocześnie system monitorowania musi wspierać bezagentowy sposób kolekcji danych (czyli bez konieczności instalowania dedykowanego oprogramowania na monitorowanym urządzeniu/systemie) przy użyciu standardowych protokołów (ICMP, SNMP)
Wymagania wspólne	O11.F16	system musi mieć możliwość monitorowania działania sieci OSE w sposób pasywny (odbieranie alarmów) jak również w sposób aktywny (wysyłanie pakietów RTT ICMP , badanie dostępności dedykowanych portów TCP, inne) - w wyniku przekroczenia zadanych parametrów pomiarów (np. czas odpowiedzi, wielkość strat pakietów, wielkość opóźnienia) generowany jest alarm z poziomu tegoż systemu (Fault & Availability Management)
Wymagania wspólne	O11.F17	system musi odbierać i prezentować alarmy wygenerowane przez system Performace Management (w ramach Rozwiązania będącego przedmiotem zamówienia) a także z dowolnego systemu OSE przy zachowaniu standardowych formatów odbieranych pakietów (SNMP Trap , SYSLOG)
Wymagania wspólne	O11.F18	sondy odbierające alarmy muszą mieć możliwość filtracji kolekcjonowanych danych
Wymagania wspólne	O11.F19	sondy odbierające alarmy muszą normalizować odebrane alarmy i mieć możliwość formatowania danych

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O11.F20	sondy odbierające alarmy muszą zapewnić mechanizmy wzbogacania alarmów bazując na prostych strukturach danych zapisywanych co najmniej w plikach płaskich oraz w danych z bazy Inventory/CMDB
Wymagania wspólne	O11.F21	system musi mieć funkcjonalność elastycznego logowania parametrów pracy sond oraz zdarzeń (alarmów) w formie nieprzetworzonej
Wymagania wspólne	O11.F22	sondy muszą zapewniać prawidłowe działanie systemu, bez utraty danych w przypadku utraty komunikacji z innymi komponentami systemu, przez okres 36 godzin
Wymagania wspólne	O11.F24	system musi mieć możliwość dostosowywania parametrów poszczególnych sond do specyfiki monitorowanego elementu
Wymagania wspólne	O11.F25	system musi posiadać skalowalność horyzontalną i możliwość prostej rozbudowy systemu poprzez dołożenie dodatkowych sond i/lub instancji systemu centralnego
Wymagania wspólne	O11.F26	zaimplementowane w systemie sondy muszą mieć możliwość odbierania przesyłanym do nich pakietów SNMP trap (v2c, v3) oraz pakietów SYSLOG (zgodnie z RFC 5424)
Wymagania wspólne	O11.F27	system musi posiadać udokumentowane API w zakresie kolekcji danych, za pomocą którego możliwa będzie integracja systemu z elementami infrastruktury przy wykorzystaniu innych protokołów niż SNMP, SYSLOG - co najmniej REST API, protokoły TCP/UDP, odczyt plików płaskich, telnet/ssh monitoring aktywny musi w zakresie monitorowania dostępności (Availability Maangement) spełniać następujące wymagania: - wysyłanie pakietów ICMP echo (sprawdzenie osiągalności urządzenia, sygnalizowanie przekroczenia zadanego poziomu strat pakietów / opóźnienia) - wysyłanie zapytań SNMP o wskazany OID (porównanie wyniku z zadaną wartością liczbową lub tekstową) - wysyłanie zapytań SQL do wskazanej bazy danych, porównanie wyniku z zadaną wartością liczbową lub tekstową - badanie dostępności stron Web poprzez weryfikację czasów odpowiedzi na zapytania HTTP/HTTPS i porównywanie ich z zadanymi wartościami liczbowymi oraz weryfikację zwracanych kodów błędów - badanie czasów pobierania stron Web, transferu plików przy pomocy protokołu FTP/TFTP/HTTP - wysyłanie pakietów TCP/UDP (sprawdzenie, czy możliwe jest połączenie się na zadany port), alarmowanie braku odpowiedzi (np. timeout, connection refused) oraz przekroczeń oczekiwanego czasu odpowiedzi, w szczególności sprawdzanie usług : - SMTP, POP3, IMAP - DNS - SSL, SSH, TELNET - SIP - możliwość wykonywania pomiarów w konkretnych relacjach pomiarowych z użyciem mechanizmów pomiarowych typu Two-Way : TWAMP (zgodnie z RFC 5357) lub/i przy użyciu rozwiązania producenta urzadzeń sieciowych w szkielecie

Podobszar	Nr Wymagania	Treść Wymagania
		sieci OSE - Juniper RPM ; w przypadku braku możliwości wykorzystania ww. mechanizmów rmożliwe jest wykorzystanie systemu Zamawijącego typu Element Manager do urzadzeń sieciowych w szkielecie OSE (Juniper Network Director) dokonując z nim integracji przy pomocy API
Wymagania wspólne	O11.F28	monitoring pasywny musi wykorzystywać co najmniej protokoły SNMP i Syslog, należy założyć możliwość implementacji innych interfejsów integracji, np. z wykorzystaniem API
Wymagania wspólne	O11.F29	w zakresie moitoringu pasywnego system musi zapewnić domyślną obsługę zdarzeń, dla których nie zdefiniowano żadnych reguł przetwarzania, aby uniknąć sytuacji, w której informacja o awarii dotychczas nierozpoznanej i niezdefiniowanej w systemie nie zostanie przetworzona i zaprezentowana użytkownikom
Wymagania wspólne	O11.F30	system musi zapewniać metody eskalacji; wymagane jest zapewnieni mozliwości konfiguracji co najmniej następujących akcji automatycznych: - uruchomienie zewnętrznego skryptu - wysyłanie wiadomości email - wysyłanie wiadomości SMS
Wymagania wspólne	O11.F31	system musi mieć możliwość konfiguracji powiadamiania/eskalacji dla grupy monitorowanych elementów jak i niezależnie dla każdego monitorowanego elementu konfiguracja eskalacji musi opierać się co najmniej na: - typach zdarzeń/alarmów, dla których wysyłane jest powiadomienie - przedziałach czasowych, w których wysyłane jest powiadomienia (wsparcie dla kaledarza roboczego i nieroboczego - definiowanie kalendarza)
Wymagania wspólne	O11.F32	system musi zapewniać możliwość kreowania powiadomienia/eskalacji na podstawie pól alarmu (np. czas wystąpienia zdarzenia, nazwa monitorowanego elementu, opis zdarzenia) oraz dodawania własnych treści (np. dodatkowy opis wyjaśniający zdarzenie)
Wymagania wspólne	O11.F33	system musi umożliwiać integrację z zewnętrzynymi systemami typu Element Managers w celu kolekcji danych o awariach, zdarzeniach - system musi być gotowy na możliwość pobierania danych z Element Manager'ów z obszaru sieci, bezpieczeństwa, z systemów zarządzania infrastruktrurą serwerową (część Rozwiązania) oraz środowiskiem kolokacyjnym poprzez API (API zostanie udokumenrtowane przez dostawców ww. Element Managerów i systemów)
Wymagania wspólne	O11.F34	system musi zapewniać integrację z systemem Inventory sieci OSE celem co najmniej identyfikacji źródeł alarmów oraz celem ich wzbogacania
Wymagania wspólne	O11.F35	system musi zapewniać agregację informacji o stanach poszczególnych elementów w ramach zdefiniowanej usługi, tak aby na podstawie parametrów pracy jej elementów składowych określić jej aktualny status
Wymagania wspólne	O11.F36	systemu musi w sposób automatyczny udostępniać swoje dane (zdarzenia/alarmy) w miarę potrzeb pozostałym elementom zaimplementowanym w Rozwiązaniu

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O11.F37	system musi umożliwiać automatyczne wykrywanie topologii sieci na poziomie warstwy 3 i 2 modelu ISO/OSI i prezentację jej w sposób graficzny
	O11.F38	system musi umożliwiać kreowanie imiennych użytkowników o różnych poziomach dostępu (np. ReadOnly, ReadWrite, Admin etc.)
Wymagania wspólne	O11.F39	Widoki poszczególnych komponentów wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund dla 90% przypadków, dla pozostałych 10% przypadków czas generowania nie może być dłuższy niż 15 sekund, przy czym w przypadku braku komunikacji z elementem zewnętrznym (poza rozwiązaniem wdrażanym w ramach umowy) musi pojawić się stosowny komunikat.
Wymagania wspólne	O11.F40	system musi umożliwiać tworzenie grup użytkowników, np. w celu kreowania większych pakietów uprawnień dla wielu użytkowników, dla których wymagany jest jednakowy poziom dostępu
Wymagania wspólne	O11.F41	system musi mieć możliwość definiowania ról/profili, które przypisane do użytkowników lub ich grup będą warunkować różne poziomy dostępu (np. dostęp do panelu administracyjnego) i różne uprawnienia (np. wykonywanie operacji zapisu) w ramach systemu
Wymagania wspólne	O11.F42	system musi mieć możliwość restrykcji prezentacji elementów monitorowanej infrastruktury w celu: - ograniczenia dostępu użytkownikom tylko do ich infrastruktury (np. dla partnera OSE w danym regionie) - wyświetlania jedynie tych elementów, za które dany użytkownik jest odpowiedzialny
Wymagania wspólne	O11.F43	system musi udostępniać interfejsy integracji pozwalających m.in. na integrację z: - elementami i/lub systemami sieciowymi w celu kolekcji danych o awariach (np. z Element Manager'ów) - zewnętrznymi źródłami danych w celu wzbogacania informacji o awariach
Wymagania wspólne	O11.F44	system musi wspierać konfigurację korelacji obsługi zdarzeń z wykorzystaniem informacji o zależnościach funkcjonalnych między elementami infrastruktury OSE, musi być również możliwość dopisywania korelacji "ręcznie"
Wymagania wspólne	O11.F45	system musi mieć możliwość budowy interfejsów integracji do innych systemów OSS i systemów BSS Zamawiajacego lub też szyny danych, tak aby umożliwić: - publikację danych systemu (eventów, alarmów, kolekcjonowanych metryk) w zewnętrznych systemach, np. w szynie danych monitorowaną przez system typu BPM - wykorzystywanie danych z systemów zewnętrznych do wzbogacania i korelacji zdarzeń. System powinien umożliwiać wzbogacanie alarmów o informacje pobrane z zewnętrznych źródeł danych typu Inventory (np. nazwy klienta, nazwy urządzenia) - eksport danych do systemów zewnętrznych, na przykład w celach raportowych, prezentacji statystyk

Podobszar	Nr Wymagania	Treść Wymagania
		- współpracę systemu w ramach zdefiniowanych procesów operacyjnych, np. obsługa zgłoszeń serwisowych - eskalację informacji o zidentyfikowanych awariach - integrację z systemami typu Trouble Ticketing umożliwiającą automatyczne i półautomatyczne kreowanie/aktualizację/zamykanie zgłoszeń na podstawie zarejestrowanych alarmów
Wymagania wspólne	O11.F46	system musi zapewniać podstawową korelację zdarzeń: - deduplikację, czyli identyfikację alarmów dotyczącą dokładnie tego samego zdarzenia i przechowywanie go w repozytorium, jako jednego rekordu (w szczególności flap'owanie interface'ów) - filtrację i automatyczne usuwanie widoczności alarmu z określonych widoków na podstawie zdefiniowanego kryterium - kategoryzację danych - możliwość oznaczania i agregowania kolekcjonowanych zdarzeń w ramach zdefiniowanych w systemie grup i/lub kategorii - eskalację z alarmu – automatyczne powiadomienia wywoływane na podstawie alarmu i jego zidentyfikowanej treści - wzbogacanie zdarzeń w zakresie informacji dostępnych w systemach zewnętrznych
Wymagania wspólne	O11.F47	system musi zapewniać automatyczną korelację zdarzeń ON/OFF, czyli parowanie zdarzeń które oznaczają wystąpienie awarii i jej zakończenie (zastosowanie np. dla flapowania interface'ów)
Wymagania wspólne	O11.F48	system musi zapewniać automatyczne wykonywanie akcji (np. skryptu) na podstawie zarejestrowanych zdarzeń/alarmów
Wymagania wspólne	O11.F49	system musi zapewniać mechanizmy archiwizacji zdarzeń/alarmów aktywnych w bazie zdarzeń/alarmów historycznych
Wymagania wspólne	O11.F50	system musi posiadać mechanizmy umożliwiające diagnostykę i monitorowanie wydajności przetwarzania alarmów
Wymagania wspólne	O11.F51	podstawowym interfejsem systemu musi być aplikacja webowa, stanowiąca konsolę operatorsko-administracyjny
Wymagania wspólne	O11.F52	system musi zapewnić możliwość integracji z Centarnym System Raportowym Zamawiajacego celem przekazywania danych niezbędnych do analiz operacyjnych np. dotyczących jakości świadczonych szkołom usług
Wymagania wspólne	O11.F53	system musi udostępniać informację typu audytowego pozwalającego na weryfikację działań użytkowników zawierającą co najmniej następujące danych: - czas logowania użytkownika - adres/hostname źródłowy - niepoprawne próby logowania - błędy wykonywania działań w ramach interfejsu użytkownika, ze wskazaniem danych użytkownika - inne informacje wspomagające diagnostykę i identyfikację naruszeń

Podobszar	Nr Wymagania	Treść Wymagania
		bezpieczeństwa system wymagany czas przechowywania danych audytowych to 12 miesięc
Wymagania wspólne	O11.F54	system musi posiadać predefiniowane widoki prezentujące stan monitorowanej infrastruktury; widoki te powinny jednak umożliwiać modyfikację, a także powinna być możliwość kreowania nowych widoków, także w oparciu o te istniejące
Wymagania wspólne	O11.F55	system musi umożliwiać konfigurację własnych stron prezentacji (zespołu widoków), które równocześnie mogłyby zostać przypisane konkretnym użytkownikom lub grupom użytkowników
Wymagania wspólne	O11.F56	system musi posiadać: - zestaw predefiniowanych elementów wizualizacyjnych, za pomocą których użytkownik może budować złożone widoki (dashboardy) : - listy/tabele zdarzeń - różnego typu wykresy pozwalające na prezentację danych ilościowych i statystycznych (np. grafy, pie-chart'y, histogramy - mapy topologii oraz mapy budowane statycznie z możliwością podłożenia mapy bitowej lub wektorowej jako tło pod mapę siec - możliwość budowy struktury hierarchicznej, pozwalającej na przejście „od ogółu do szczegółu" (tzw. funkcjonalność „drill-down"); funkcjonalność ta ma pozwalać na budowę ogólnych widoków prezentujących w sposób wysokopoziomowy aktualny stan monitorowanej sieci, jednocześnie pozwalać na szybkie wyświetlenie widoków bardziej szczegółowych, np. dotyczących konkretnej monitorowanej lokalizacji lub urządzenia - możliwość zdefiniowania zindywidualizowanych map/widoków użytkowników umożliwiających przeglądanie fragmentów monitorowanej sieci
Wymagania wspólne	O11.F57	lista alarmów dostępna w systemie musi zapewniać następujące funkcjonalności: - możliwość filtracji prezentowanych alarmów - odpowiednie oznaczanie różnych priorytetów alarmów, np. poprzez zróżnicowaną kolorystykę - sortowanie listy alarmowej według prezentowanych kolumn - możliwość kreowania widoków alarmów poprzez wyświetlanie wybranych atrybutów w formie osobnych kolumn listy - możliwość dynamicznego przeszukiwania listy
Wymagania wspólne	O11.F58	elementy warstwy prezentacji muszą pozwalać na wykonywanie z ich poziomu kontekstowych akcji (uzależnione od uprawnień użytkownika, konfigurowalne per profil/grupa/użytkownik), np. : - potwierdzanie alarmu - zmiana priorytetu alarmu - przypisanie użytkownika
Wymagania wspólne	O11.F59	system w zakresie prezentacji musi zapewniać funkcjonalności raportowe związane zarówno z obsługą zdarzeń bieżących jak i historycznych i zapewniać

Podobszar	Nr Wymagania	Treść Wymagania
		następujące funkcje: - prezentacja danych w formach tabelarycznych i graficznych z możliwością agregowania (grupowania) danych - predefiniowane raporty dostępne per element, grupa elementów - możliwość generowania porównawczych raportów zbiorczych, np. w celu określenia najbardziej awaryjnych elementów bądź typów elementów - eksport raportów do plików w popularnych formatach (co najmniej CSV, XLS, TXT) - możliwość kreowania własnych raportów wymagany czas przechowywania zdarzeń historycznych to 12 miesięcy wymagany czas przechowywania raportów to 12 miesięcy
Wymagania wspólne	O11.F60	system musi zapewniać mechanizmy kontroli swojego działania umożliwiające : - przeprowadzanie diagnostyki funkcjonowania systemu (troubleshooting) - dynamiczne serwisy logowania i śledzenia konfigurowane w trakcie działania system - przeprowadzanie weryfikacji czynności wykonywanych przez użytkowników systemu - podgląd dziennika zdarzeń systemowych oraz akcji podejmowanych przez użytkownika (np. dodanie bądź usunięcie obiektu)
Wymagania wspólne	O11.F61	system musi mieć możliwość wykonywania kompletnego backupu konfiguracji systemu oraz zbieranych danych wraz z możliwością bezproblemowego odtworzenia
Wymagania wspólne	O11.F62	system musi mieć możliwość uruchomienia odrębnej, niezależnej instancji testowej systemu bez dodatkowych kosztów licencji lub przy wykorzystaniu licencji ze środowiska produkcyjnego
Wymagania wspólne	O11.F63	system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń przez cały okres obowiązywania Umowy
Wymagania wspólne	O11.F64	system musi zapewniać automatyczny provisioning pomiarów typu availabilty oraz możliwości poprawnego odbioru alarmów w wyniku provisioningu nowej usługi w sieci OSE (w systemie provisionigu będącego integralną częścią Rozwiazania)
Wymagania wspólne	O11.F65	system musi mieć możliwość czasowego wyłączenia powiadomień/eskalacji dla danej osoby (np. w czasie urlopu) lub dla pojedynczego monitorowanego elementu lub grupy elementów
Wymagania wspólne	O11.F66	system musi zapewniać funkcjonalność RCA (root cause analysis) - analiza źródłowej przyczyny awarii musi opierać się również na topologii sieci
Wymagania wspólne	O11.F67	system musi zapewniać funkcjonalność Topology Managment (przynajmniej w obszarze węzłów OSE i sieci szkieletowej

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O11.F68	system musi posiadać dedykowany silnik korelacji i możliwość definiowania własnych automatyzacji i korelacji
Wymagania wspólne	O11.F69	system musi mieć możliwość budowy integracji z systemem provisioningu w kierunku do systemu provisioningu pozwalającą na automatyczne wywoływanie akcji naprawczych
Wymagania wspólne	O11.F70	elementy warstwy prezentacji muszą pozwalać na wykonywanie z ich poziomu kontekstowych akcji (uzależnione od uprawnień użytkownika, konfigurowalne per profil/grupa/użytkownik) : - dodawanie komentarzy do alarmu - tworzenie zgłoszenia w systemie Service Desk - uruchamianie skryptu (np. z akcją naprawczą)
Wymagania wspólne	O11.F71	system musi mieć możliwość ustalania harmonogramów dla automatycznego generowania i dystrybucji raportów albo w ramach OSS lub/i przy wykorzystaniu Cenralnego Systemu Raportowego
Wymagania wspólne	O11.F72	system musi wspierać funkcjonalność okien serwisowych, które mają wpływ na pozostałe elementy systemu (np. nie wystawiania alarmów z pomiarów Availability w trakcie trwania okna): - możliwość definiowania okien serwisowych - definiowanie okien serwisowych w wyniku integracji z procesem biznesowym (działu utrzymania) - prezentacja graficzna w raportach i statystykach - dostępność historii
Wymagania wspólne	O11.F73	system musi mieć możliwość integracji z mapami online, np. OpenStreetMap czy Google Maps
Wymagania wspólne	O11.F74	Rozwiązanie musi zawierać: - proaktywny monitoring urządzeń w szkielecie, punktów styku i dostępności systemów OSE - wizualizację geograficzną, śledzenie alarmów, tresholdy etc. - zobrazowanie graficznie zależności między awarią a infrastrukturą OSE

7.4.1.2 Funkcjonalność Performance Management

System Performance Management swoją funkcjonalnością ma wspierać procesy utrzymania sieci, usług i systemów OSE a w szczególności monitorować wydajność urządzeń i wykorzystanie zasobów sieci OSE.

System Performance Management ma pozwalać na zbieranie danych związanych z wydajnością urządzeń w szkielecie OSE i w jednostkach oświatowych, z systemów w centrach kolokacji, także aplikacji i świadczonych w sieci OSE usług oraz obciążenia ruchem łącz szkieletowych i dostępowych. Zakres

monitorowania obejmował będzie co najmniej te same elementy infrastruktury, co system Fault & Availability Management. System ma monitorować dużą ilość różnorodnych urządzeń, łącz i systemów, parametrów itp. W celu prezentacji tych danych będą generowane automatycznie statystyki oraz raporty. Ze względu na dużą ilość danych wydajność bazy danych jak i wszelkie zaimplementowane mechanizmy bazodanowe i graficzne muszą gwarantować odpowiednią wydajność.

Rozwiązanie musi wygodnie prezentować statystyki i raporty z pomiarów a także umożliwiać tworzenie widoków w różnych aspektach zainteresowania i dla różnych grup użytkowników.

Muszą być prezentowane, co najmniej:

- statystyk on-line i raporty z jakości działania sieci i usług OSE (opóźnienia, straty, jittery, dostępność urządzeń i serwisów),
- statystyki i raporty parametrów ruchowych w szkielecie OSE oraz na łączach do szkół (konieczne badanie ruchu per VLAN szkolny - szkoła może mieć jednocześnie do 5 VLAN),
- statystyki i raporty wydajności serwerów i urządzeń sieciowych (CPU, RAM itp.)
- statystyki i raporty środowiskowe (temperatura w urządzeniach, temperatura w szafach kolokacyjnych itp.)
- raporty z pomiarów jakości sieci w relacjach pomiędzy węzłami OSE

System musi zapewnić następujące główne funkcjonalności związane z kolekcją danych:

- monitoring sieci w warstwie 2 i 3 modelu ISO/OSI;
- monitoring przy użyciu wielorakich protokołów: ICMP, SNMP, RPING, HTTP, HTTPS oraz opcjonalnie OAM
- monitoring w relacjach pomiarowych E2E przy użyciu protokołów typu Two-Way: TWAMP lub/i rozwiązania producenta urzadzeń sieciowych Juniper - RPM, w przypadku braku możliwości wykorzystania ww. mechanizmów możliwe jest wykorzystanie systemu Zamawiającego typu Element Manager do urządzeń sieciowych w szkielecie OSE (Juniper Network Director) dokonując z nim integracji przy pomocy API
- współpraca systemu monitoringu z ruterami shadow bezpośrednio lub via Element Manager do urządzeń sieciowych Zamawiającego (Juniper Network Director)
- monitoring parametrów jakościowych (opóźnienia, straty, jittery w warstwie IP) w szczególności mierzone/wyliczane w okresach dostępności
- monitoring aplikacji, systemów operacyjnych, urządzeń serwerowych i sieciowych; ze względu na spodziewaną różnorodność typów elementów infrastruktury OSE (system powinien zapewniać szeroki wachlarz gotowych rozwiązań monitorowania)
- monitoring parametrów jakościowych łącz a w szczególności monitoring ruchu, poziomu błędów itp. na łączach szkieletowych i dostępowych do jednostek oświatowych:
- monitoring ruchu w szkielecie sieci (ruch do CPE w szkole mierzony na subinterface'ach urządzeń w węzłach OSE)
- pomiary serwisów świadczonych w systemach OSE

- konfiguracja metody monitoringu i próbkowania – możliwość regulacji częstotliwości odpytywania poszczególnych elementów sieciowych, jak również sposobu pobierania danych (np. wybór odpowiedniego protokołu)
- potencjalnie automatyczne wykrywanie typu urządzeń, systemów, aplikacji i usług na podstawie, którego możliwe będzie automatyczne tworzenie pomiarów - w zakresie wykrywania system powinien wspierać, co najmniej poniższe protokoły: ICMP, skanowanie TCP/UDP, SNMP, SSH, WebService
- system powinien udostępniać panel konfiguracyjny wykrywania za pomocą, którego można określić podstawowe parametry procesu, np.: zakresy sieci IP, wykluczenia podsieci, określanie parametrów dostępu (np. community)
- system powinien umożliwiać przypisanie domyślnych szablonów monitorowania na podstawie danych pozyskanych w wyniku procesu wykrywania infrastruktury
- system musi posiadać funkcjonalność automatycznego tworzenia pomiarów z poziomu zewnętrznych systemów np. z poziomu systemu provisioningu poprzez udostępnienie dedykowanego API

<u>Założenia dotyczące architektury pomiarów</u>

1. W zakresie Performance Management (PM) sieć szkieletowa OSE, czyli wszystkie urządzenia w węzłach centralnych i regionalnych OSE (zarówno urządzenia sieciowe jak i urządzenia i systemy bezpieczeństwa) będą co odpytywane co najmniej o standardowe parametry wydajnościowe (jak w tabeli poniżej). W przypadku serwerów objętych wirtualizacją w węzłach centralnych monitoring będzie wykonywany przez system DCIM (Data Center Infrastructure Monitoring - kupowany w oddzielnym postępowaniu wraz z infrastrukturą docelową) - zakłada się możliwość przekazywania informacji pomiędzy systemem DCIM a Performance Management. Istotnym pomiarem wykonywanym na urządzeniach w szkielecie sieci OSE jest pomiar interafce'ów i subinterface'ów - jest on niezbędny w celu monitoringu wysycenia zamawianych u operatorów łącz jak i wykrywania błędów. W tym kontekście należy założyć, że:
    - muszą być wykonywane pomiary utylizacji interface'ów/subinterface'ów oraz błędy na interface'ach (również w kontekście VLANów zarządzających zakończonych w lokalizacjach szkolnych - ca. 19,5 tys.)
    - muszą być wykonywane stosowne pomiary i wyliczenia na bazie pomiaru ruchu na portach fizycznych i logicznych na urządzeniach sieciowych w węzłach OSE
    - musi być wykonywane raportowanie stanu wysycenia łącz oraz kontrola przekroczenia założonych progów wysycenia łącz i alarmowanie tych przekroczeń
    - statystyki ruchu z ostatniej doby są przetrzymywane w postaci próbek z dokładnością 5 minutową
    - statystyki ruchu z ostatniego tygodnia są przetrzymywane w postaci zagregowanych próbek z dokładnością do 15 minut
    - statystyki ruchu z ostatniego miesiąca są przetrzymywane w postaci zagregowanych próbek z dokładnością do 30 minut

- statystyki ruchu z ostatniego roku są przetrzymywane w postaci zagregowanych próbek z dokładnością do 60 minut
- zagregowane statystyki roczne są przechowywane do 5 lat wstecz

2. W przypadku urządzeń CPE zainstalowanych w szkołach pomiary performance'owe jak i potencjalnie pomiary utylizacji portów downstream i upstream będą wykonywane tylko w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki zgłoszonych przez szkołę problemów. W przypadku urządzeń typu switch (SW) i access point wi-fi (AP) monitoring taki będzie aktywowany w przypadku zgłoszonych problemów ze szkoły i po decyzji operatora OSE na temat diagnozy problemu oraz skonfigurowaniu dostępu do tych urządzeń z systemu PM. Zakłada się częstotliwość pomiarów performance'wych standardowo na poziomie 300 sekund. Pomiary diagnostyczne mają za zadanie również wykrycie potencjalnego wysycenia łacz dostępowych do lokalizacji szkolnych.
3. Zakłada się również konieczność pomiarów relacji w szkielecie sieci OSE typu FULL MESH między 19-toma węzłami OSE (16 regionalnych i 3 centralne) pomiędzy ruterami shadow - pomiary opóźnień, strat pakietów i wielkości jittera w tych relacjach i w klasach ruchu. W początkowym okresie sieci OSE będą zaimplementowane 2 klasy ruchu: NC (Network Control) i BE (Best Effort), docelowo w szkielecie sieci OSE będzie zaimplementowanych do 5 klas ruchu. Zamawiający w sieci szkieletowej będzie stosował klasy ruchu i sposób kolejkowania w oparciu o CBQoS. Pomiary będą wykonywane z częstotliwością 300 sekund. Routery shadow będą dostarczone przez Zamawiającego i będą to rutery Juniper SRX320. Zarządzanie pomiarami na ruterach shadow pozostaje w obowiązku Wykonawcy, który:
    a. może wykorzystać własne Rozwiązanie OSS w celu komunikacji z ruterami shadow
    b. może wykorzystać funkcjonalność systemu Element Manager dla sieci OSE (Juniper Network Director) i jego API by zlecać temu systemowi zakładanie pomiarów na ruterach shadow oraz by pobierać wyniki pomiarów z tego systemu
    c. ostatecznie Rozwiązanie musi umożliwić generowanie raportów z wynikami tych pomiarów i przekazywanie ich do Centralnego Systemu Raportowego Zamawiającego by z niego dalej publikować raporty na temat jakości sieci na portalu OSE

W tabeli poniżej przedstawiono zestawienie typów pomiarów, jakie co najmniej powinny być realizowane przez system w ramach poszczególnych obszarów monitorowania. Zakłada się, że Wykonawca przeanalizuje optymalność przestawionego planu pomiarów i jeśli zaistnieje taka potrzeba to po akceptacji Zamawiającego wprowadzi stosowne modyfikacje.

Obszar monitorowania	Pomiary	Częstotliwość	Uwagi
Urządzenia w sieci szkieletowej	Dostępność urządzenia/interfejsów	1 minuta	
	Opóźnienia	5 minut	
	Straty pakietów	5 minut	
	Jitter	5 minut	
	Utylizacja interfejsów	5 minut	

Obszar monitorowania	Pomiary	Częstotliwość	Uwagi
	Błędy na interfejsach Utylizacja CPU Utylizacja pamięci Parametry środowiskowe – voltage, temperatura	5 minut 5 minut 5 minut 5 minut	
Monitoring parametrów jakościowych pomiędzy węzłami OSE (pomiary na ruterach shadow)	Dedykowane relacje pomiarowe E2E (w klasach ruchu): Opóźnienia Straty pakietów Jitter	5 minut 5 minut 5 minut	opcjonalnie - w razie doraźnej potrzeby - częstotliwość może zostać zwiększona do 1 minuty
Urządzenia OSE w jednostkach oświatowych	Dostępność urządzenia CPE Utylizacja interfejsów, błędy na interface (upstream, downstream) Utylizacja CPU Utylizacja pamięci Opcjonalnie: Opóźnienia sieci Straty pakietów Jitter	5 minuta 5 minut 5 minut 5 minut 5 minut 5 minut 5 minut	w okresach 3 tygodni po uruchomieniu szkoły oraz w przypadku diagnostyki problemu z usługą/urządzeniem na CPE w okresach 3 tygodni po uruchomieniu szkoły oraz w przypadku diagnostyki problemu z usługą/urządzeniem, na SW i AP tylko w przypadku diagnostyki problemu z usługą/urządzeniem j.w. j.w. j.w. j.w. j.w.
Infrastruktura serwerowa i aplikacje	Dostępność serwerów i aplikacji Statystyki wydajnościowe serwerów i systemów wirtualnych: CPU, RAM, load average, zajętość dysku, service'u itp.	5 minut 5 minut 5 minut	Dostępność aplikacji weryfikowana na podstawie dostępności określonych portów, usług, procesów.

Obszar monitorowania	Pomiary	Częstotliwość	Uwagi
	WebMonitoring – monitorowanie dostępności stron WWW poprzez dedykowane sekwencje testowe Monitorowanie specyficznych usług aplikacji (dostępności portów TCP,UDP)	5 minut	

System Performance Management w warstwie agregacji i przetwarzania będzie realizować zadania związane z procesowaniem i kolekcjonowanych danych wydajnościowych, głównie ich agregacją.

Najważniejsze funkcjonalności, które muszą charakteryzować system:

- Agregacja danych: dane z różnych źródeł mogą być kolekcjonowane z różnymi interwałami a system powinien zaprezentować dane dla różnych przedziałów czasowych, zatem zapewniać mechanizmy agregacji i uśredniania danych.
- Korelacja danych wydajnościowych, w tym ewaluacja danych pochodzących z różnych źródeł (np. kalkulacja złożonych metryk)
- Wspomaganie identyfikacji problemu na podstawie analizy krzyżowej danych z różnych urządzeń. (kompleksowa analiza wydajności sieci umożliwiająca porównywanie wskaźników dotyczących różnych elementów może wspomagać znacząco diagnostykę i pozwalać na szybszą identyfikację problemu)
- Możliwość generowania alarmów i notyfikacji dotyczących przekroczenia zadanych progów (także wielopoziomowych) oraz odchyleń od linii bazowych (monitorowanie wydajności infrastruktury pozwala na proaktywne monitorowanie i reagowanie na problemy zanim faktycznie wystąpią)
- Wyznaczanie trendów i prognoz z uwzględnieniem ich konfigurowalnych okresów (funkcjonalność istotne z perspektywy planowania pojemności sieci)
- Automatyczna predykcja wysycenia zasobów (przede wszystkim pojemności łącz) w oparciu o uśrednione dane historyczne i wyznaczanie trendów
- Posiadanie udokumentowanego API, za pośrednictwem, którego będzie możliwa implementacja niestandardowych interfejsów integracji, a także publikacja zgromadzonych i zagregowanych danych w innych systemach Zamawiającego (BSS, Portal OSE)

Wymagania funkcjonalne

Podobszar	Nr Wymagania	Treść Wymagania
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F1	dla łącz szkieletowych system musi przedstawiać wizualizacje zajętości łącz w stylu network weathermap
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F2	system musi mieć możliwość monitoringu relacji pomiarowych E2E pomiędzy węzłami OSE z uwzględnieniem klas ruchu i VRF następujących parametrów i: - opóźnień w warstwie IP (we wszystkich klasach usług i wszystkich relacjach międzywęzłowych) - strat pakietów w warstwie IP (we wszystkich klasach usług i wszystkich relacjach międzywęzłowych) - jittera w warstwie IP (we wszystkich klasach usług i wszystkich relacjach międzywęzłowych)
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F3	system musi zapewnić pomiary w relacjach E2E pomiędzy węzłami OSE a dokładnie pomiędzy ruterami shadow (Juniper SRX320) przy pomocy protokołu typu Two-Way: TWAMP lub/i przy użyciu rozwiązania producenta urządzeń sieciowych w szkielecie sieci OSE (Juniper RPM), wymagane jest od Wykonawcy : - zarządzanie pomiarami na ruterach typu shadow - zapewnienie wykonywania pomiarów opóźnień, strat pakietów, jitter (z uwzględnieniem klas ruchu i vrf) - zapewnienie w systemie statystyk i raportów z ww. pomiarów w przypadku braku możliwości wykorzystania ww. mechanizmów w dostarczanym Rozwiązaniu Zamawiający dopuszcza wykorzystanie systemu Zamawiającego typu Element Manager (EM) do urządzeń sieci (Juniper Network Director) - Wykonawca wówczas wdroży integrację z EM wykorzystując API systemu EM ostatecznie Rozwiązanie musi umożliwić generowanie raportów z wynikami pomiarów w relacjach i przekazywanie ich do Centralnego Systemu Raportowego Zamawiającego
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F4	system musi zapewniać możliwość konfigurowania specyficznych pomiarów diagnostycznych (np. wykonanie pomiaru w określonej klasie ruchu) i wywoływania ich „na żądanie”
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F5	system musi zbierać informacje co najmniej o : - wydajności urządzeń (zajętość CPU, zajętość RAM, zajętość FIB w przypadku urządzeń sieciowych itd.) - zajętości łącz (szkieletowych, agregacyjnych, dostępowych, uplinków na podstawie counterów na interface'ach fizycznych i logicznych oraz alarmować przekroczenia treshold'ów

Podobszar	Nr Wymagania	Treść Wymagania
		- błędach na interface'ach - parametrach środowiskowych (temperatura powietrza chłodzącego, zasilanie itp.)
Szczególne wymagania dotyczące monitorowania urządzeń w sieci LAN w szkołach	O12.F6	system musi zbierać parametry dotyczące parametrów łącz z każdego aktywnego inetrface'u i subinterface'u
Szczególne wymagania dotyczące monitorowania urządzeń w sieci LAN w szkołach	O12.F7	system musi mieć możliwość zbierania parametrów z interface'ów fizycznych i logicznych z portów WAN i LAN na CPE
Szczególne wymagania dotyczące monitorowania urządzeń w sieci LAN w szkołach	O12.F8	w przypadku urządzeń CPE zainstalowanych w szkołach system musi wykonywać pomiary performance'owe jak i pomiary utylizacji portów w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki (należy założyć średnio do 2 tygodni) zgłoszonych przez szkołę problemów, system musi w tych okresach badać dostępność CPE pod kątem oceny działania łącza od lokalnego dostawcy
Szczególne wymagania dotyczące monitorowania urządzeń w sieci LAN w szkołach	O12.F9	w przypadku urządzeń SW i AP zainstalowanych w szkołach system musi monitorować performance i utylizację portów tych urządzeń w okresach diagnostyki (należy założyć średnio do 2 tygodni) w przypadku zgłoszonych problemów ze szkoły - w celu wykonania tych pomiarów będzie odpowiednio skonfigurowany dostęp do urządzeń należy założyć, że okresy diagnostyczne mogą mieć miejsce w razie potrzeby również w okresach 3 tygodni po podłączeniu szkoły
Wymagania wspólne	O12.F10	system musi umożliwiać integrację z Centralnym Systemem Raportowym Zamawiającego (CSR) na poziomie standardowych mechanizmów integracji (co najmniej REST API oraz poprzez wymianę plików w standardowych formatach - CSV, XML, JSON, XLS) w celu raportowania najważniejszych parametrów wydajnościowych infrastruktury w jednym miejscu, czyli w CSR
Wymagania wspólne	O12.F11	system musi posiadać wsparcie dla architektury rozproszonej – możliwość kolekcji danych poprzez wydzielone dedykowane moduły programowe (kolektory)
Wymagania wspólne	O12.F12	celem mniejszego obciążania łącz pomiędzy węzłami OSE system musi zostać zaimplementowany w architekturze rozproszonej tak by kolekcja danych znajdowała się możliwie jak najbliżej źródła danych; należy uwzględnić architekturę zapewniającą to, że logiczne warstwy systemu wymagające większej wydajności i niezawodności (warstwa prezentacji i przetwarzania danych) były ulokowane w węzłach centralnych
Wymagania wspólne	O12.F13	kolektory muszą zapewniać możliwość konfiguracji częstotliwości pollingu per monitorowany element i/lub typ elementu

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O12.F14	system musi być tak wyskalowany (performance, storage itp.) aby zapewnić wydajny monitoring wszystkich wymaganych parametrów z minimalną częstotliwością pollingu równą 300 sekund
Wymagania wspólne	O12.F15	kolektory muszą zapewnić prawidłowe działanie systemu bez utraty danych na wypadek braku łączności z jednostką centralna systemu przez okres 36 godzin
Wymagania wspólne	O12.F16	system standardowo musi przechowywać: - surowe dane pomiarowe przez 6 miesięcy - dane zaagregowane przez 12 miesiące jednakże z uwzględnieniem wyjątków: 1. statystyki ruchowe (szkielet, agregacja, dostęp - w tym per VLAN szkoły): - statystyki ruchu z ostatniej doby mają być przechowywane w postaci próbek z dokładnością 5 minutową - statystyki ruchu z ostatniego tygodnia mają być przechowywane w postaci zaagregowanych próbek z dokładnością do 15 minut - statystyki ruchu z ostatniego miesiąca mają być przechowywane w postaci zaagregowanych próbek z dokładnością do 30 minut - statystyki ruchu z ostatniego roku mają być przechowywane w postaci zaagregowanych próbek z dokładnością do 60 minut - zaagregowane statystyki roczne z ruchu mają być przechowywane do 5 lat wstecz 2. statystyki performance'owe (typu CPE, memory, storage, temp. , itp.): - próbki surowe (5 minutowe) mają być przechowywane 3 tygodnie
Wymagania wspólne	O12.F17	system musi dawać możliwość elastycznego konfigurowania parametrów agreagacji i przechowywania danych pomiarowych per urządzenie/ grupa urządzeń/typ pomiaru
Wymagania wspólne	O12.F18	system musi mieć możliwość dostosowywania parametrów poszczególnych kolektorów do specyfiki monitorowanego segmentu sieci
Wymagania wspólne	O12.F19	system musi zapewniać skalowalność horyzontalną i możliwość prostej rozbudowy systemu poprzez dołożenie dodatkowych kolektorów i/lub instancji części centralnej
Wymagania wspólne	O12.F20	system musi posiadać dokumentowane API pozwalające na budowę dodatkowych typów interfejsów północnych i południowych
Wymagania wspólne	O12.F21	system musi prezentować statystyki z pomiarów a także umożliwiać tworzenie widoków w różnych aspektach zainteresowania i dla różnych grup użytkowników
Wymagania wspólne	O12.F22	system musi zapewniać monitoring sieci w warstwie 2 i 3 modelu ISO/OSI
Wymagania wspólne	O12.F23	system musi zapewniać monitoring przy użyciu co najmniej następujących protokołów: RTT ICMP, SNMP, RPING, HTTP, HTTPS (protokół OAM do wykorzystania w dalszych etapach projektu OSE)
Wymagania wspólne	O12.F24	system musi mieć możliwość pomiarów kolejek dla poszczególnych klas ruchu na interface'ach i subinterface'ach urządzeń sieciowych w szkielecie OSE
Wymagania wspólne	O12.F25	system musi zapewniać monitoring parametrów wydajnościowych systemów będących zarówno częścią Rozwiązania jak i systemów OSE poza Rozwiązaniem takich jak :

Podobszar	Nr Wymagania	Treść Wymagania
		- Element Managery dla urzadzeń sieciowych - system Retencji Logów - systemy zarządzające do systemów bezpieczeństwa - systemy bezpieczeństwa : SIEM, SWG, DNS (Infoblox) , ADC, SSLO, SSL VPN, WAF (F5 Networks), inne - systemy dodatkowe jak NTP, LDAP - systemy BSS Zamawiającego - portale OSE, inne Ze względu na spodziewaną różnorodność typów elementów infrastruktury OSE system powinien zapewniać szeroki wachlarz gotowych rozwiązań monitorowania (predefiniowane template'y)
Wymagania wspólne	O12.F26	system musi zgłaszać przekroczenia założonych tresholdów/progów na zdefiniowanych pomiarach, w szczególności na pomiarach: - wydajności urządzeń i systemów (zajętość CPU, zajętość RAM, zajętość FIB w przypadku urządzeń sieciowych itd.) - zajętości łącz (szkieletowych, agregacyjnych, dostępowych, uplinków) - parametrów środowiskowych (temperatura powietrza chłodzącego, zasilanie itp.)
Wymagania wspólne	O12.F27	przekroczenia progów pomiarowych muszą skutkować wygenerowaniem alarmu przesłanego do systemu Fault Management
Wymagania wspólne	O12.F28	dla przekroczeń progów pomiarowych system musi wspierać generowanie alarmów na podstawie wielopoziomowych progów i linni bazowych
Wymagania wspólne	O12.F29	system musi umożliwiać pomiary jakości ruchu (opóźnienia, straty pakietów, jitter) dla ruchu typu HTTP / HTTPS, RTT ICMP, TCP, UDP
Wymagania wspólne	O12.F30	system musi przedstawiać wykresy zajętości łącz (dla wszystkich łącz na poziomie łącza fizycznego i łącza logicznego), w szczególności mają być zbierane cyklicznie co najmniej : - ruch IN i OUT z inteface'ów i subinterface'ów (VLAN per szkoła) na urządzeniach w węzłach OSE oraz prezentowane w postaci statystyk graficznych - poziom błędów z interface'u na urządzeniach w węzłach OSE oraz prezentowane w postaci statystyk graficznych
Wymagania wspólne	O12.F31	Rozwiązanie musi prezentować statystyki ruchu per VLAN szkolny (zakłada się, że per szkoła może zostać skonfigurowanych do 5 VLAN) , opis statystyki ma zawierać dane identyfikujące szkołę i jej usługę (np. nazwa, RSPO, nr VLAN) Dane identyfikujące usługę mają być pobierane z systemów BSS Zamawiającego zintegrowanych z systemami OSS
Wymagania wspólne	O12.F32	system na podstawie pomiarów ruchu musi generować cykliczne raporty 95-percentyla i GNR (Godzina Największego Ruch) i przekazywać je do Centralnego Systemu Raportowego Zamawiającego

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O12.F33	pomiar ruchu generowanego przez szkoły musi polegać na odnotowaniu co 5 minut liczby przesłanych bajtów w każdym kierunku, na tej podstawie mają być określane różne parametry/charakterystyki ruchu, co najmniej: - 95-ty percentyl średnich pięciominutowych określany jako największa średnia 5-cio minutowa spośród próbek średnich 5-cio minutowych pozostałych po odjęciu 5% z próbek z największymi wartościami w zadanym okresie, w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym - Godzina Największego Ruchu (GNR) określana jako początek godziny (z dokładnością do 5-ciu minut) w trakcie której przesłano największą liczbę bajtów – w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym (dla doby GNR zawiera się w przedziale od godziny 0:00 do 23:00, dla tygodnia od niedzieli godzina 0:00 do soboty godzina 23:00, dla miesiąca od pierwszego dnia miesiąca, godzina 0:00 do ostatniego dnia miesiąca, godzina 23:00) - średni ruch w GNR w Mb/s określany jako: [Średni_ruch_w_GNR] = ([liczba_przesłanych_bajtów](w_czasie_GNR+60_minut) - [liczba_przesłanych_bajtów](w_czasie_GNR)) x 8 / 3600 / 1000 000 w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym - średnią prędkość 5-cio minutowa przesyłania danych w Mb/s wg formuły: [Średnia_5-cio_minutowa](w_czasie_t) = ([liczba_przesłanych_bajtów](w_czasie_t) - [liczba_przesłanych_bajtów](w_czasie_t-5_minut)) x x 8 / 300 / 1 000 000
Wymagania wspólne	O12.F34	system musi wspierać badanie wysycenia wszystkich łącz a w szczególności łącz dostępowych i eskalować mailowo w oparciu o kilka poziomów wysyceń łącz
Wymagania wspólne	O12.F35	system musi monitorować działanie portalu OSE (czasy odpowiedzi, czasy ładowanie stron itp.)
Wymagania wspólne	O12.F36	system musi umożliwiać konfigurację kolektorów i próbkowania – możliwość regulacji częstotliwości odpytywania poszczególnych elementów sieciowych, jak również sposobu pobierania danych (np. wybór odpowiedniego protokołu), próbkowanie ma być wyzwalane systemowo zgodnie ze skonfigurowanym harmonogramem lub przez operatora z konsoli
Wymagania wspólne	O12.F37	system musi zapewniać możliwość exportu danych do standardowych formatów plików (co najmniej CSV, XLS, XML, JSON) z pomiarów „real-time” na żądanie użytkownika
Wymagania wspólne	O12.F38	system musi zapewniać możliwość chwilowego wyłączenia monitorowania wybranych urządzeń przez operatora
Wymagania wspólne	O12.F39	system musi zapewniać możliwość zapisania konfiguracji monitoringu (zestawu metryk performance'owych) dla danego typu urządzenia oraz odtworzenia tego monitoringu dla kolejnych urządzeń danego typu
Wymagania wspólne	O12.F40	system musi udostępniać panel konfiguracyjny wykrywania monitorowanych urządzeń za pomocą którego można określić podstawowe parametry procesu wykrywania, np. zakresy sieci IP, wykluczenia podsieci, określanie parametrów dostępu (np. community) itp.

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O12.F41	system musi umożliwiać przypisanie domyślnych szablonów monitorowania na podstawie danych pozyskanych w wyniku procesu wykrywania infrastruktury
Wymagania wspólne	O12.F42	system musi umożliwiać automatyczne tworzenie pomiarów np. z poziomu systemu provisioningu poprzez udostępnienie dedykowanego API i/lub automatyczne tworzenie pomiarów dla urządzeń spełniających określone założenia
Wymagania wspólne	O12.F43	system musi zapewniać agregację danych, dane z różnych źródeł mogą być kolekcjonowane z różnymi interwałami, jednocześnie system musi prezentować dane dla jeszcze innych przedziałów czasowych, wobec tego system musi zapewniać mechanizmy zarówno agregacji jak i uśredniania danych
Wymagania wspólne	O12.F44	system musi wspierać identyfikację problemu (i przesłanie stosowanego alarmu do Fault Management) na podstawie analizy krzyżowej danych z różnych urządzeń (kompleksowa analiza wydajności sieci umożliwiająca porównywanie wskaźników dotyczących różnych elementów może wspomagać znacząco diagnostykę i pozwalać na szybszą identyfikację problemu)
Wymagania wspólne	O12.F45	system musi udostępniać udokumentowane API, za pośrednictwem którego będzie możliwa implementacja niestandardowych interfejsów integracji, a także umożliwić przekazywanie zgromadzonych i zaagregowanych danych do innych systemów Zamawiającego
Wymagania wspólne	O12.F46	system musi mieć możliwość integracji z dziedzinowymi systemami zarządzania w celu potencjalnego pobierania z nich danych (w szczególności performance'owych) - w sieci OSE będą implementowane Element Manager'y w obszarze sieci, w obszarze bezpieczeństwa oraz system zarządzania środowiskiem kolokacyjnym
Wymagania wspólne	O12.F47	system musi umożliwiać przygotowywanie danych do weryfikacji raportów SLA: - z jakości świadczonych szkołom usług (zakłada się, że raporty SLA będą generowane tylko na podstawie zgłoszeń, jednak nie wyklucza się innego podejścia w przyszłości) - z jakości usług świadczonych przez operatorów łącz (weryfikacja działania łącz dzierżawionych oraz gwarantowanych na nich parametrów usług)
Wymagania wspólne	O12.F48	podstawowym interfejsem systemu musi być aplikacja webowa, stanowiąca konsolę operatorsko-administracyjną
Wymagania wspólne	O12.F49	system musi zapewnić możliwość integracji z Centralny Systemem Raportowym Zamawiającego celem przekazywania danych do raportów OSE - między innymi ruchu z łącz szkieletowych/agregacyjnych/dostępowych
Wymagania wspólne	O12.F50	widoki poszczególnych komponentów wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund dla 90% przypadków, dla pozostałych 10% przypadków czas generowania nie może być dłuższy niż 15 sekund, przy czym w przypadku braku komunikacji z elementem zewnętrznym (poza rozwiązaniem wdrażanym w ramach umowy) musi pojawić się stosowny komunikat
Wymagania wspólne	O12.F51	każdy z użytkowników systemu monitorowania powinien posiadać swoje własne imienne konto

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O12.F52	system musi zapewnić możliwość ustanowienia jednego lub więcej użytkowników z uprawnieniami administratora systemu
Wymagania wspólne	O12.F53	system musi umożliwiać tworzenie grup użytkowników, np. w celu kreowania większych pakietów uprawnień dla wielu użytkowników, dla których wymagany jest jednakowy poziom dostępu
Wymagania wspólne	O12.F54	system musi umożliwiać definiowanie ról, które przypisane do użytkowników lub ich grup będą warunkować różne poziomy dostępu (np. dostęp do panelu administracyjnego) i różne uprawnienia (np. wykonywanie operacji zapisu) w ramach systemu
Wymagania wspólne	O12.F55	system musi mieć możliwość restrykcji prezentacji elementów infrastruktury OSE w celu: - ograniczenia dostępu użytkownikom tylko do ich infrastruktury (np. dla partnera OSE w danym regionie) - wyświetlania jedynie tych elementów, za które dany użytkownik jest odpowiedzialny
Wymagania wspólne	O12.F56	system musi udostępniać informację typu audytowego pozwalającą na weryfikację działań użytkowników, dostarczającą następujące dane: - czas logowania użytkownika - adres/hostname źródłowy - niepoprawne próby logowania - błędy wykonywania działań w ramach interfejsu użytkownika, ze wskazaniem danych użytkownika - inne informacje wspomagające diagnostykę i identyfikację naruszeń bezpieczeństwa systemu
Wymagania wspólne	O12.F57	system musi posiadać predefiniowane widoki prezentujące stan monitorowanej infrastruktury - widoki te powinny jednak umożliwiać modyfikację, a także powinna być możliwość kreowania nowych widoków, także w oparciu o te istniejące
Wymagania wspólne	O12.F58	system w ramach interfejsu użytkownika musi pozwalać na przejrzystą wizualizację kolekcjonowanych metryk/statystyk: - podstawową formą prezentacji w systemie muszą być różnego rodzaju wykresy m. in. : - liniowe - kołowe, tzw. pie-chart's - histogramy - grafy - dane powinny być również prezentowane w formie tabelarycznej - wykresy muszą być dynamicznie odświeżane - wykresy muszą zapewniać dynamiczne skalowanie danych i jednostek
Wymagania wspólne	O12.F59	system musi w zakresie statystyk zapewniać następującą funkcjonalność: - wspierać co najmniej następujące parametry w zakresie konfiguracji kolekcji i archiwizacji: - częstotliwość pomiarów - parametry agregacji pomiarów i czas archiwizacji - wspierać możliwość indywidualnego dostosowania prezentacji raportów

Podobszar	Nr Wymagania	Treść Wymagania
		- sposób prezentacji danych - różnorodność dostępnych widoków - informacje dedykowane dla odbiorcy końcowego
Wymagania wspólne	O12.F60	system musi umożliwiać eksport prezentowanych danych do plików zewnętrznych w standardowych formatach co najmniej CSV, JSON , XML , XLS
Wymagania wspólne	O12.F61	użytkownicy muszą mieć możliwość konfiguracji własnych dashboardów z wykorzystaniem dostępnych elementów wizualizacji
Wymagania wspólne	O12.F62	widoki w systemie muszą umożliwiać dynamiczne zmiany parametrów prezentacji, np. zakresów czasowych czy wybranych monitorowanych elementów
Wymagania wspólne	O12.F63	system musi udostępniać predefiniowane zestawy raportów, na przykład grupowane ze względu na typy dostępnych monitorów czy typów raportu. Przykładowe predefiniowane raporty: - raporty prezentujące statystyki ruchu sieciowego (m. in. utylizację interfejsów, opóźnienia, jitter) - raporty dostępności za określony czas - raporty porównawcze np. tego samego typu raportu dla dwóch różnych elementów, pozwalających na analizę wskaźników wydajnościowych w tym samym okresie pomiaru. - raport wszystkich wskaźników monitorowanych na danym typie elementu - raporty typu Top N według różnych kryteriów - raporty typu inventory korzystające z zasobów określonych w ramach procesu automatycznego wykrywania sieci Wymagany czas przechowywania raportów to 12 miesięcy
Wymagania wspólne	O12.F64	użytkownicy systemu muszą mieć możliwość tworzenia własnych raportów oraz potencjalnie udostępniania ich w postaci szablonów innym użytkownikom
Wymagania wspólne	O12.F65	system musi zapewnić generowanie raportów w standardowych formatach co najmniej PDF, XLS
	O12.F66	szablony raportów udostępniane w ramach systemu (domyślne i utworzone przez użytkowników) powinny zapewniać parametryzację, np. określenie zakresu czasowego, czy listy interfejsów
Wymagania wspólne	O12.F67	system musi zapewniać konfigurowalne mechanizmy logowania umożliwiające : - przeprowadzanie diagnostyki funkcjonowania systemu (troubleshooting) - dynamiczne serwisy logowania i śledzenia konfigurowane w trakcie działania systemu - przeprowadzanie weryfikację czynności wykonywanych przez użytkowników systemu system musi posiadać dziennik dla śledzenia zdarzeń systemowych oraz akcji podejmowanych przez użytkownika (np. dodanie bądź usunięcie obiektu), wymagany czas przechowywania danych audytowych to 12 miesięcy
Wymagania wspólne	O12.F68	system musi mieć możliwość uruchomienia odrębnej, niezależnej instancji testowej systemu bez dodatkowych kosztów licencyjnych lub z wykorzystaniem tych samych licencji co w środowisku produkyjnym

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O12.F69	system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych/monitorowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń przez cały okres obowiązywania Umowy
Wymagania wspólne	O12.F70	system musi mieć możliwość wykonywania kompletnego backupu konfiguracji systemu oraz zbieranych danych wraz z możliwością bezproblemowego odtworzenia
Wymagania wspólne	O12.F71	system musi zapewniać metody powiadomień i eskalacji (po przekroczeniach progów - także wielokrotnych) : - akcje automatyczne, np. uruchomienie zewnętrznego skryptu - wysyłanie wiadomości email - wysyłanie wiadomości SMS (zapewnienie bramki SMS pozostaje w gestii Zamawiajacego)
Wymagania wspólne	O12.F72	system musi zapewniać automatyczny provisioning pomiarów w wyniku aktywacji nowej usługi lub jej zmiany (w systemie provisionigu będącego integralną częścią Rozwiazania)
Wymagania wspólne	O12.F73	system musi umożliwiać uruchamianie na żądanie pomiarów typu „real-time”, które pozwolą w trybie on-line śledzić zmiany monitorowanego parametru wydajnościowego, bez konieczności automatycznego zapisu pomiaru w systemie
Wymagania wspólne	O12.F74	Rozwiązanie musi wspierać automatyczne wykrywanie typu urządzeń/systemów na podstawie którego możliwe będzie automatyczne tworzenie pomiarów - w zakresie wykrywania system powinien wspierać co najmniej następujące protokoły: RTT ICMP, skanowanie TCP/UDP, SNMP, SSH
Wymagania wspólne	O12.F75	system musi umożliwiać korelację danych wydajnościowych , w tym ewaluacja danych pochodzących z różnych źródeł - np. kalkulacja złożonych metryk (w niektórych przypadkach odczytanie pojedynczej metryki na danym elemencie nie daje właściwego obrazu wartości wskaźnika i konieczna jest jego kalkulacja na podstawie kilku różnych odczytów), zatem system musi zapewniać możliwość implementacji reguł kalkulacji złożonych metryk
Wymagania wspólne	O12.F76	system musi mieć możliwość wyznaczania trendów i prognoz z uwzględnieniem ich konfigurowalnych okresów
Wymagania wspólne	O12.F77	system musi zapewnić elastyczność w zakresie realizacji pomiarów – wybór pomiędzy predefiniowanymi operacjami pomiarowymi a konfiguracją dowolnych scenariuszy pomiarowych
Wymagania wspólne	O12.F78	Rozwiązanie musi umożliwiać wyliczanie wewnętrznych parametrów SLA dla zasobów technicznych (urzadzenie, system) bazując na zebranych danych z pomiarów w systemie Performance Management. Wymagany czas przechowywania wyliczonych parametrów SLA wynosi 12 mmiesięcy
Wymagania wspólne	O12.F79	system musi mieć możliwość ustalania harmonogramów dla automatycznego generowania i dystrybucji raportów

Podobszar	Nr Wymagania	Treść Wymagania
Wymagania wspólne	O12.F80	szablony raportów udostępniane w ramach systemu (domyślne i utworzone przez użytkowników) powinny zapewniać parametryzację, np. określenie zakresu czasowego, czy listy interfejsów
Wymagania wspólne	O12.F81	Rozwiązanie musi wspierać funkcjonalność okien serwisowych, które mają wpływ na elementy systemu (np. nie wysyłanie alarmów do Fault Management po przekroczeniu progu w trakcie trwania okna), zatem system ma posiadać wsparcie dla funcjonalności: - możliwość definiowania okien serwisowych - definiowanie okien serwisowych w wyniku integracji z systemami BSS Zamawiającego - prezentacja graficzna w raportach i statystykach - dostępność historii - uwzględnienie okien serwisowych w naliczaniu wewnętrznych parametrów SLA per zasób techniczny (urzadzenie, system)
Wymagania wspólne	O12.F82	system musi mieć możliwość harmonogramowania zbierania statystyk performance'owych celem optymalizacji obciążenia procesami pomiarowym mierzonych urządzeń jak i samego systemu pomiarowego
Wymagania wspólne	O12.F83	system musi spełniać następujące założenia dotyczące pomiarów ruchu: - monitoring wysycenia łącz poprzez cykliczny pomiar portów fizycznych i logicznych (a także wyliczenia i raportowanie stanu wysycenia) - statystyki ruchu z ostatniej doby są przetrzymywane w postaci próbek z dokładnością 5 minutową - statystyki ruchu z ostatniego tygodnia są przetrzymywane w postaci zaagregowanych próbek z dokładnością do 15 minut - statystyki ruchu z ostatniego miesiąca są przetrzymywane w postaci zaagregowanych próbek z dokładnością do 30 minut - statystyki ruchu z ostatniego roku są przetrzymywane w postaci zaagregowanych próbek z dokładnością do 60 minut - zaagregowane statystyki roczne są przechowywane do 5 lat wstecz
Wymagania wspólne	O12.F84	oprócz statystyk z interace'ów i subinterface'ów system musi zapewnić wydajność dla monitoringu pozostałych statystyk performace'owych z założeniem : - nie mniej niż 10 stastyk per szkieletowe urządzenie sieciowe - nie mniej niż 15 statystyk per szkieletowe urządzenie bezpieczeństwa - nie mniej niż 5 statystyk per urządzenie w lokalizacji szkolnej

7.4.1.2.1 Część funkcjonalności Performance Management zamawiana w ramach prawa opcji

W związku z tym, że architektura sieci OSE zakłada zakończenia VLAN szkolnych na urządzeniach w węzłach OSE oraz ze względu na skalę i uwarunkowania utrzymaniowe urządzeń CPE w szkołach, miejscem zbierania statystyk ruchu generowanego przez szkoły są interface'y/subinterface'y na

urządzenia w węzłach OSE (Juniper) . W przypadku zbierania statystyk przy pomocy protokołu SNMP w węzłach OSE, gdzie ilość szkół per węzeł będzie bardzo duża, zachodzi ryzyko wysokiego obciążenia tych urządzeń. Zatem, aby zapobiec takiej sytuacji Zamawiający zakłada potencjalne wykorzystanie systemu Telemetrii (wdrożonego poza postępowaniem zakupu systemów OSS) celem zbierania najbardziej obciążających statystyk ruchu ze szkół strumieniowo (a nie przy pomocy zapytań protokołu SNMP). Jednakże Zamawiający nie wyklucza możliwości użycia protokołu SNMP do niniejszych pomiarów (pomiary i statystyki ruchu z 125 tys. VLAN szkolnych) i dlatego też system OSS musi wspierać wykonywanie wspomnianych pomiarów i statystyk. Jeżeli realizacja przedmiotowej funkcjonalności wymaga licencji, Wykonawca jest zobowiązany do ich zapewnienia na rzecz Zamawiającego w ramach wynagrodzenia z tytułu realizacji prawa opcji. Zamawiający jest uprawniony do zamówienia niniejszej funkcjonalności w ramach skorzystania z prawa opcji, na zasadach opisanych we wzorze Umowy. Wykonawca jest zobowiązany do wdrożenia przedmiotowej funkcjonalności w terminie do 1 miesiąca od daty otrzymania zamówienia, na zasadach analogicznych jak opisane w Umowie.

Założenia dotyczące architektury pomiarów

Funkcjonalność Performance Management (PM) zamawiana opcjonalnie zawiera pomiary ruchu wykonywane na urządzeniach w szkielecie sieci OSE z subinterface'ów będacych zkończeniami VLAN szkolnych - pomiary te są niezbędne w celu monitoringu wysycenia zamawianych u operatorów łącz oraz monitoringu wykorzystania pasma przez poszczególne szkoły w lokalizacji. Ilośc tych pomiarów i statystyk jest znaczna ze względu na ilość szkół w sieci OSE i ilość możliwych VLAN konfigurowanych per szkoła (25 tys. szkół * 5 VLAN). W tym kontekście należy założyć, że:

- każda szkoła może mieć skonfigurowanych do 5 VLAN'ów (wyniesionych na warstwie II do węzła OSE) i jest konieczny monitoring ruchu per każdy VLAN oddzielnie
- musi być zapewnione wyliczanie wykorzystania zamówionej przez szkołę przepływności, jako suma ruchu we wszystkich VLANach danej szkoły
- musi być zapewnione wyliczanie wykorzystanej przepustowości z danej lokalizacji szkolnej, jako suma ruchu we wszystkich VLANach wszystkich szkół w lokalizacji
- muszą być wykonywane stosowne pomiary i wyliczenia na bazie pomiaru ruchu na portach fizycznych i logicznych na urządzeniach sieciowych w węzłach OSE
- musi być zapewnione raportowanie stanu wysycenia łącz oraz kontrola przekroczenia założonych progów wysycenia łącz i alarmowanie tych przekroczeń
- statystyki ruchu z ostatniej doby są przetrzymywane w postaci próbek z dokładnością 5 minutową
- statystyki ruchu z ostatniego tygodnia są przetrzymywane w postaci zagregowanych próbek z dokładnością do 15 minut
- statystyki ruchu z ostatniego miesiąca są przetrzymywane w postaci zagregowanych próbek z dokładnością do 30 minut
- statystyki ruchu z ostatniego roku są przetrzymywane w postaci zagregowanych próbek z dokładnością do 60 minut
- zagregowane statystyki roczne są przechowywane do 5 lat wstecz

Wymagania funkcjonalne:

Nr Wymagania	Treść Wymagania
O18.F1	system musi spełniać następujące założenia dotyczące pomiarów i statystyk ruchu: - cykliczny pomiar ruchu (co 300 sekund) per każdy VLAN danej szkoły oddzielnie z interface'ów logicznych na urządzeniach szkieletowych OSE - generowanie i prezentowanie statystyk ruchu per pojedynczy VLAN danej szkoły - generowanie i prezentacja statystyk ruchu per szkoła (suma ruchu we wszystkich VLANach danej szkoły) - generowanie i prezentacja ruchu per lokalizacja szkolna (suma ruchu we wszystkich VLANach wszystkich szkół w lokalizacji) - monitoring wysycenia łącz poprzez cykliczny pomiar portów fizycznych i logicznych urządzeniach szkieletowych OSE (też wyliczenia, raportowanie i alertowanie stanu wysycenia do BSS) - wyliczanie generowanej przez szkołę przepływności jako suma ruchu we wszystkich VLANach danej szkoły (raportowanie do BSS) - wyliczanie generowanej z danej lokalizacji szkolnej przepływności jako suma ruchu we wszystkich VLANach wszystkich szkół w lokalizacj (raportownaie do BSS)
O18.F2	system musi zapewniać, że: - statystyki ruchu z ostatniej doby są przetrzymywane w postaci próbek z dokładnością 5 minutową - statystyki ruchu z ostatniego tygodnia są przetrzymywane w postaci zaagregowanych próbek z dokładnością do 15 minut - statystyki ruchu z ostatniego miesiąca są przetrzymywane w postaci zaagregowanych próbek z dokładnością do 30 minut - statystyki ruchu z ostatniego roku są przetrzymywane w postaci zaagregowanych próbek z dokładnością do 60 minut - zaagregowane statystyki roczne są przechowywane do 5 lat wstecz
O18.F3	pomiar ruchu generowanego przez szkoły musi polegać na odnotowaniu co 5 minut liczby przesłanych bajtów w każdym kierunku, na tej podstawie mają być określane różne parametry/charakterystyki ruchu, co najmniej: - 95-ty percentyl średnich pięciominutowych określany jako największa średnia 5-cio minutowa spośród próbek średnich 5-cio minutowych pozostałych po odjęciu 5% z próbek z największymi wartościami w zadanym okresie, w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym - Godzina Największego Ruchu (GNR) określana jako początek godziny (z dokładnością do 5-ciu minut) w trakcie której przesłano największą liczbę bajtów – w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym (dla doby GNR zawiera się w przedziale od godziny 0:00 do 23:00, dla tygodnia od niedzieli godzina 0:00 do soboty godzina 23:00, dla miesiąca od pierwszego dnia miesiąca, godzina 0:00 do ostatniego dnia miesiąca, godzina 23:00) - średni ruch w GNR w Mb/s określany jako: [Średni_ruch_w_GNR] =

Nr Wymagania	Treść Wymagania
	([liczba_przesłanych_bajtów](w_czasie_GNR+60_minut) - [liczba_przesłanych_bajtów](w_czasie_GNR)) x 8 / 3600 / 1000 000 w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym - średnią prędkość 5-cio minutowa przesyłania danych w Mb/s wg formuły: [Średnia_5-cio_minutowa](w_czasie_t) = ([liczba_przesłanych_bajtów](w_czasie_t) - [liczba_przesłanych_bajtów](w_czasie_t-5_minut)) x x 8 / 300 / 1 000 000
O18.F4	system musi zapewnić możliwość integracji z Centralnym Systemem Raportowym Zamawiającego celem przekazywania danych do raportów OSE - raportów z danymi z ruchu przeliczonymi i prezentowanymi w kontekście : -VLAN szkoły - szkoły (odpowiednia sumaryzacja ruchu z poszczególnych VLAN) - lokalizacji szkolnej ((odpowiednia sumaryzacja ruchu z poszczególnych VLAN wszystkich szkół w lokalizacji)
O18.F5	system musi zgłaszać przekroczenia założonych tresholdów/progów na pomiarach zajętości łącz (wysycenie łącz) dostępowych na zasadzie badania ruchu generowanego na wszytskich VLANach wszystkich szkół w danej lokalizacji szkolnej w porównaniu z zamówioną od operatora przepustowością na dane łacze dostępowe
O18.F6	system zbierania statystyk ruchu musi bazować na wdrożonej w Fazie I funkcjonalności Performance Management; wymagania, które muszą być spełnione przez system, stawiane obszarowi Performance Management w zakresie zbierania i prezentowania statystyk ruchowych muszą byc spełnione również w ramach funkcjonalności Performance Management zamawianej opcjonalnie

7.4.2. Zarządzanie konfiguracją (Config Manager)

Skala sieci OSE (ok. 25 tys. jednostek oświatowych) niesie za sobą zarządzanie konfiguracją ogromnej ilości urządzeń - dodatkowo gro tych urządzeń to heterogeniczny sprzęt instalowany w szkołach o różnorakich modelach i z różnoraką konfiguracją (zależną od producenta sprzętu). System Config Manager musi objąć swym zasięgiem zarówno sprzęt sieciowy jak i urządzenia/systemy bezpieczeństwa OSE. Należy wziąć pod uwagę to, że część prac konfiguracyjnych (dot. urządzeń w szkołach) będzie wykonywana przez podwykonawców/partnerów serwisowych OSE, którzy muszą mieć możliwość zdalnego korzystania z systemu usprawniającego zarządzanie konfiguracjami urządzeń - oczywiście z uwzględnieniem nadanych uprawnień do funkcjonalności i do puli urządzeń, za którą odpowiadają. Config Manager musi bardzo ściśle współpracować z systemem Provisionigu i Inventory gdyż jest dla nich referencją w zakresie aktualnych konfiguracji zainstalowanych urządzeń jak i szablonów konfiguracji dla danego typu/modelu urządzeń. Częścią obszaru zarządzania konfiguracją ma być też funkcjonalność IPAM (IP Address Management) - system ten będzie dostawcą puli adresowej oraz puli numeracji VLAN używanych w konfiguracji urządzeń. Config Management musi być zintegrowany z Inventory celem identyfikacji urządzeń zainstalowanych w sieci OSE, ich aktualnymi i historycznymi konfiguracji a także

identyfikacji zainstalowanego oprogramowania na urządzeniach. System w połączeniu z Inventory ma pozwalać na implementację funkcjonalności CMDB.

Poniżej przedstawione zostały szczególnie istotne wymagania dla systemu Config Manager:

- wyszukiwanie urządzeń w sieci oraz automatyczne i cykliczne zaciąganie ich konfiguracji so systemu, funkcjonalność ta powinna być dostępna dla każdego urządzenia wprowadzonego do systemu w zakresie, który udostępnia producent urządzenia, system musi umożliwiać również definiowanie przedziałów czasowych, w jakich konfiguracja będzie pobierana z możliwością wyspecyfikowania konkretnych godzin dla danych grup urządzeń
- akwizycja specyficznych informacji z urządzenia, system powinien umożliwić pobranie specyficznych danych z urządzenia i przechowanie ich w stosownych zasobach, umożliwiając ich wykorzystanie podczas kreowania późniejszych schematów konfiguracji
- modyfikacja konfiguracji, system powinien umożliwiać ręczną modyfikację konfiguracji, tworzenie schematów dla grup urządzeń zarówno logicznych jak i lokalizacyjnych, w celu późniejszego zastosowania dla danej partii urządzeń bez potrzeby ręcznego wybierania
- wersjonowanie konfiguracji, system po pobraniu konfiguracji z urządzenia lub utworzeniu nowego schematu powinien tworzyć spójne nazewnictwo dla przechowywanych zasobów, pozwalające w łatwy sposób określić, które z plików są nowsze i z kiedy dokładnie pochodzą
- porównywanie konfiguracji, system powinien posiadać możliwość śledzenia zmian konfiguracji w czasie oraz porównywania wybranych 2 lub więcej zapisów konfiguracji z danego czasu.
- eksportowanie konfiguracji do standardowych formatów plików
- zarządzanie oprogramowaniem zainstalowanym na urządzeniach (mile widziana integracja z systemami pakietowania danego producenta sprzętu)
- zdalne wykonywanie komend na żądanie administratora systemu, w tym również shutdown i reboot urządzenia
- uruchamianie narzędzi diagnostycznych (np. ping, traceroute) z poziomu zarządzanego urządzenia
- możliwość działania bezagentowego z wykorzystaniem jednego z dostępnych protokołów komunikacyjnych, brak konieczności instalowania dedykowanego oprogramowania na zdalnych systemach
- możliwość zlecania zadań czasowych, które będą cyklicznie wykonywane na grupach urządzeń - takie podejście pozwoli na realizowanie cyklicznych zadań automatyzacji zależnych od bieżącej struktury i stanu sieci
- możliwość komunikacji statusów wykonanych zadań poprzez różne media dla administratorów lub grup użytkowników - funkcjonalność ta może być zrealizowana poprzez integrację z systemem FM, który realizuje funkcje eskalacji i powiadomień (funkcjonalność zapewni możliwość szybkiej reakcji służb utrzymaniowych w przypadku problemów technicznych przy realizacji zadań automatyzacji)
- możliwość wykonywania i logowania przez system pełnego audytu wykonywanych zmian w systemach/urządzeniach, wraz z logami dotyczącymi danych użytkownika, który zmiany wykonał jak również informacje, czego dotyczyły i jakie były ich wartości.

Założenia dotyczące architektury zarządzania konfiguracjami i oprogramowaniem

1. W przypadku urządzeń szkieletowych (urządzenia sieciowe i urządzenia bezpieczeństwa) system Config Management ma zapewniać funkcjonalność zarządzania konfiguracją i oprogramowaniem przez cały czas trwania Umowy, co oznacza pobieranie konfiguracji i oprogramowania z urządzeń, ich wersjonowanie i porównywanie a także wgrywanie ich na urządzenia. System ma zapewnić masowe i harmonogramowane zmiany konfiguracji i oprogramowania na urządzeniach.
2. W przypadku zarządzania konfiguracją urządzeń zainstalowanych w szkołach system Config Management ma zapewniać funkcjonalność zarządzania konfiguracją przez cały czas trwania Umowy. Zakłada się jednocześnie, że w przypadku CPE jest to pełne zarządzanie wersjami konfiguracji i oprogramowania a w przypadku SW i AP jest to inwentaryzacja konfiguracji i oprogramowania inicjalnego na tych urządzeniach gdyż operator OSE nie będzie administrował urządzeniami SW i AP a jedynie zapewniał ich instalację i uruchomienie inicjalne (wraz z konfiguracją) zatem musi posiadać inicjalną konfigurację i oprogramowanie tych urządzeń w przypadku ich awarii i gwarancyjnej wymiany na nowe. Dodatkowo dla urządzeń SW i AP niezbędna jest również baza użytkowników i haseł oraz SSID (dla AP) wykorzystywane w konfiguracjach inicjalnych.

Wymagania funkcjonalne

Nr Wymagania	Treść Wymagania
O13.F1	system musi zapewniać repozytorium konfiguracji wszystkich urządzeń OSE (szkieletowych: sieciowych, bezpieczeństwa, serwerów a także urządzeń zainstalowanych w szkołach) wraz z jej wersjonowaniem
O13.F2	repozytorium konfiguracji musi przechowywać zapisane konfiguracje w uwspólnionym formacie (np. TXT, XLM, JSON, inne) - w szczególności dla urządzeń CPE pochodzących od różnych producentów – format ten ma być dopasowany do wymagań/możliwości systemu provisioningu
O13.F3	system musi zapewniać repozytorium szablonów konfiguracji wraz z wersjonowaniem - do wykorzystania przez system provisioningu (musi być zachowana ścisła integracja pomiędzy tymi systemami)
O13.F4	system musi zapewniać repozytorium oprogramowania instalowanego na urządzeniach OSE wraz z jego wersjonowaniem
O13.F5	system musi umożliwiać dystrybucję oprogramowania na urządzenia: jego walidację i instalację oraz zbieranie informacji o zainstalowanym oprogramowaniu
O13.F6	informacje prezentowane przez system muszą być zintegrowane z Inventory będącego częścią Rozwiązania (które między innymi będzie posiadać dane CRMowe) tak by w kontekście oglądanej konfiguracji było wiadomo jakiego fizycznego urządzenia dotyczą, gdzie jest ono zainstalowane i dla jakiej szkoły świadczy usługi - dotyczy sprzętu w szkołach)

Nr Wymagania	Treść Wymagania
O13.F7	system musi być oparty o powszechnie dostępne standardy i technologie do komunikacji z urządzeniami (np. SNMP, NETCONF, XML, REST API, JSON, JMX, IPMI) - stosowane odpowiednio w zależności od możliwości zarządzanych urządzeń
O13.F8	system musi zapewniać wyszukiwanie urządzeń w sieci i ściąganie ich konfiguracji
O13.F9	system musi zapewniać akwizycję specyficznych informacji z urządzenia, przechowanie ich w stosownych zasobach umożliwiając ich wykorzystanie podczas kreowania późniejszych schematów konfiguracji (w systemie provisioningu)
O13.F10	system musi zapewniać możliwość modyfikacji konfiguracji (tworzenie szablonów konfiguracji dla modeli urządzeń i grup urządzeń zarówno logicznych jak i lokalizacyjnych, w celu późniejszego zastosowania dla danej partii urządzeń bez potrzeby ręcznego wybierania)
O13.F11	system musi umożliwiać porównywanie konfiguracji w celu wykrywania wprowadzonych zmian
O13.F12	system musi umożliwiać cofnięcie konfiguracji do wcześniejszych wersji, w przypadku urządzeń provision'owanych automatycznie z systemu provisioningu- musi to być zsynchronizowane z systemem provisioningu
O13.F13	system musi zapewniać możliwość eksportu konfiguracji do standardowych formatów plików (co najmniej TXT, XML)
O13.F14	system musi posiadać funkcjonalność zarządzania oprogramowaniem zainstalowanym na urządzenia
O13.F15	system musi posiadać wbudowane narzędzia diagnostyczne pozwalające na sprawdzenie komunikacji z urządzeniem
O13.F16	system musi umożliwiać oznaczanie konfiguracji bazowej dla konkretnego urządzenia OSE w szkole (konfiguracja bazowa to pełna konfiguracja urządzenia z konkretnymi wpisanymi parametrami typu adresacja, vlan, hasła)
O13.F17	system musi zapewniać konfigurację procesu archiwizacji, porównywania i wersjonowania konfiguracji urządzeń oraz podgląd statusu tych operacji
O13.F18	system musi pozwalać na zmianę podstawowych parametrów konfiguracyjnych systemu
O13.F19	każdy z użytkowników systemu powinien posiadać swoje własne imienne konto
O13.F20	Widoki poszczególnych komponentów wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund dla 90% przypadków, dla pozostałych 10% przypadków czas generowania nie może być dłuższy niż 15 sekund, przy czym w przypadku braku komunikacji z elementem zewnętrznym (poza rozwiązaniem wdrażanym w ramach Umowy) musi pojawić się stosowny komunikat. Wyjątek może stanowić widok pobierania konfiguracji z urządzenia, ponieważ czasochłonność tego procesu zależy od możliwości danego urządzenia i jego czasów odpowiedzi.
O13.F21	system musi zapewnić możliwość ustanowienia jednego lub więcej użytkowników z uprawnieniami administratora systemu

Nr Wymagania	Treść Wymagania
O13.F22	system musi umożliwiać tworzenie grup użytkowników, np. w celu kreowania większych pakietów uprawnień dla wielu użytkowników, dla których wymagany jest jednakowy poziom dostępu
O13.F23	system musi umożliwiać definiowanie ról, które przypisane do użytkowników lub ich grup będą warunkować różne poziomy dostępu (np. dostęp do panelu administracyjnego) i różne uprawnienia (np. wykonywanie operacji zapisu) w ramach systemu
O13.F24	system musi mieć możliwość restrykcji prezentacji poszczególnych konfiguracji w celu wyświetlania jedynie tych elementów, do których dany użytkownik jest uprawniony
O13.F25	system musi udostępniać informację typu audytowego pozwalającą na weryfikację działań użytkowników, dostarczającą następujące dane: - czas logowania użytkownika - adres/hostname źródłowy - niepoprawne próby logowania - błędy wykonywania działań w ramach interfejsu użytkownika, ze wskazaniem danych użytkownika - inne informacje wspomagające diagnostykę i identyfikację naruszeń bezpieczeństwa systemu
O13.F26	system musi zapewniać funkcjonalność elastycznego (zgodnie z założoną polityka Zamawiającego) przydzielania zasobów konfiguracyjnych niezbędnych do konfiguracji ułsug na urzadzeniach OSE takich jak adresacja IP (v4 i v6) , numery VLAN, inne w zakresie zarządzania adresacją IP (IPAM - IP Adress Management) muszą być spełnione następujące wymagania: - IPAM musi pozwalać na planowanie przydzielania adresacji urządzeniom OSE - IPAM musi pozwalać na śledzenie przydzielonej adresacji - IPAM musi pozwalać na zarządzanie i przydzielanie zarówno pojedynczych adresów IP (IP4 i IPv6) oraz sieci IPv4 i IPv6 - w szczególności system IPAM musi zapewnić: - obszary do wpisania informacji, na podstawie których system będzie wiedział jakie adresy IP ma rezerwować i zwracać : Hostname CPE, Nazwa szkoły, adres/id szkoły np. RSPO - przydzielanie adresów, które rezerwuje i zwrot adresu IP wcześniej określonego jako adres pojedynczy/zakres(pierwszy możliwy) - umożliwość zwrotu adresów – zwolnienie ich w bazie (pojedynczo lub zakresami [x - y], system sam zidentyfikuje pulę, do której ma zwrócić adres/adresy - możliwość podglądu kompletnej historii aktywności przydzielania/zwalniania adresów IP (z opcją wyszukaj co najmniej z okresów: wczoraj/ostatni tydzień/ostatni miesiąc/całość), podgląd logów aktywności - zwracanie informacji (całe zestawienia): - wpisanie nazwy szkoły: zwraca adres szkoły oraz adresy ip jeżeli już zostały przydzielone wcześniej, dodatkowo nazwę CPE. - wpisanie konkretnego adresu ip/zakresu: zwraca nazwę, adres szkoły oraz nazwę CPE - wpisanie adresu szkoły: zwraca nazwę szkoły i adresy ip przydzielone do niej, jeżeli istnieją. - podgląd wykorzystania puli adresowej

Nr Wymagania	Treść Wymagania
	szczegółowe polityka przydzielania zasobów będzie uzgodniona na etapie dokumentacji technicznej
O13.F27	Rozwiązanie musi zapewniać funkcjonalność zarządzania statycznymi hasłami do urządzeń – w szczególności chodzi o bazę haseł do użycia na urządzeniach OSE w szkole, muszą być spełnione wymagania : - baza haseł musi prezentować hasła w formie zaszyfrowanej (z możliwością odkrycia dla osób uprzywilejowanych) - baza haseł musi posiadać generator haseł by przydzielać je kolejnym urządzeniom - generator haseł musi umożliwiać tworzenie haseł o założonych parametrach (długość, rodzaje używanych znaków (wielkie/małe litery, cyfry, znaki specjalne, znaki przestankowe) w tym hasła wymawialne - hasła w bazie haseł muszą być skojarzone z konkretnym urządzeniem i w przypadku urządzeń OSE zainstalowanych w szkołach ze szkołą, w której urządzenie jest zainstalowane - hasła dostępne w bezpieczny sposób tylko dla uprawnionych użytkowników
O13.F28	system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń przez cały okres obowiązywania Umowy
O13.F29	system musi zapewniać alarmowanie do systemu FM (Fault Management w ramach Rozwiązania) w przypadku nieudanych wykonań automatycznych zadań z zakresu Config Managment i/lub mailową eskalację do służb utrzymaniowych
O13.F30	w przypadku CPE system musi zapewnić pełne zarządzanie konfiguracją i oprogramowaniem, czyli system powinien archiwizować konfigurację urządzeń CPE w sposób ciągły (konfiguracja ta podlega ciągłemu monitorowaniu i wersjonowaniu). W przypadku urządzeń szkolnych - SW i AP systemy OSS muszą zapewnić inwentaryzację konfiguracji i oprogramowania inicjalnego na urządzeniach dodatkowo dla urządzeń SW i AP niezbędna jest baza użytkowników i haseł oraz baza SSID (dla AP) wykorzystywane w ww. konfiguracjach inicjalnych
O13.F31	Rozwiązanie musi uwzględniać mechanizm nadawania nazw urządzeniom wg ustalonego algorytmu (należy założyć że będzie on bazować między innymi na wartościach terytowych). Algorytm ten zostanie przekazany przez Zamawiającego po podpisaniu umowy i zawarty w dokumencie LLD.
O13.F32	należy zapewnić zarządzanie konfiguracją zarówno środowisk testowych jak i produkcyjnych (również w bazie CMDB)
O13.F33	system IPAM musi zawierać wszystkie zasoby adresowe sieci OSE (IPv4 i IPv6) - zarówno z zakresu adresów sieci prywatnych, adresów typu Shared Space jak i adresów sieci publicznej

7.4.3. Provisionig

Podstawowym założeniem funkcjonowania operatora OSE jest maksymalna automatyzacja powtarzalnych czynności - zwłaszcza konfiguracyjnych i ścisłe ich powiązanie z działaniem procesów operacyjnych i biznesowych OSE. W szczególności procesy pozyskania i podłączania szkół, uruchamiania

usług ale także modyfikacji usług mają być w jak największym stopniu zautomatyzowane. Koncepcja automatyzacji dla procesów OSE obejmuje szereg działań, które są tożsame z provisioningiem niezbędnych konfiguracji w systemach i na sprzęcie OSE, co oznacza, co najmniej:

- uzupełnienie/implementacja konfiguracji urządzeń OSE instalowanym w szkołach na bazie szablonu konfiguracji dla danego modelu urządzenia
- uzupełnienie/implementacja konfiguracji urządzeń szkieletowych sieciowych i bezpieczeństwa (w szczególności konfiguracji usług dla szkół)
- uzupełnienie konfiguracji urządzeń w Config Manager
- uzupełnienie danych w Inventory
- uruchomienie odpowiednich pomiarów (np. pomiarów ruchu VLAN szkolnych) i zbierania zdarzeń i alarmów z nowo instalowanych urządzeń w sieci OSE (Fault & Performance Management),
- uruchomienie monitoringu sieci i usług a co za tym idzie zainicjowanie automatycznego procesu generowania statystyk i raportów w OSS,
- konfiguracja usług sieci i bezpieczeństwa związanych i ich parametrów na urządzeniach/systemach sieci i bezpieczeństwa (np. uruchamianie polityk bezpieczeństwa, ustawianie poziomów filtracji treści itp.)
- integracja z procesami biznesowymi Zamawiającego, które będą wywoływać odpowiednie akcje w system provisioningu
- pobieranie niezbędnych danych do provisioningu z systemów OSS (np. Inventory, IPAM) i systemów BSS Zamawiającego (np. Jira WF, Insight, sugarCRM)

Ze względu na różnorodność urządzeń w sieci OSE system realizujący usługę provisioningu konfiguracji musi wspierać wszystkie standardowe mechanizmy komunikacji i integracji z urządzeniami sieciowymi a także z urządzeniami/systemami bezpieczeństwa oraz z innymi systemami nadzoru OSS będącymi częścią Rozwiązania. Zakłada się, że dostarczona w odrębnych postępowaniach zakupowych infrastruktura i systemy EM sieci i bezpieczeństwa umożliwią automatyzację procesów provisioningowych zapewniając obsługę stosownych mechanizmów integracji i stosowne API do swoich systemów. W szczególności scenariusz provisioningu usług bezpieczeństwa (ze względu na mnogość systemów które musi pokryć) nie wyklucza się użycia zagregowanego API wystawionego tylko z dedykowanego jednego z systemów bezpieczeństwa.

System provisioningu ma pozwolić na budowanie dowolnych algorytmów w celu zamodelowania i przeprowadzenia procesu implementacji usług na urządzeniach (ich konfiguracja) jak i w razie potrzeby w systemach OSS (odczyt/zapis/modyfikacja danych dotyczących urządzeń, konfiguracji i usług). Algorytm taki musi pozwalać na dowolność zachowania algorytmu w tym na zagnieżdżanie algorytmu w algorytmie, podejmowanie decyzji na podstawie danych wejściowych (również pochodzących z systemów trzecich) , wybór ścieżki algorytmu oraz bezpieczne wycofywanie się z przeprowadzonych kroków. Powinien również zapewniać mechanizm transakcyjności - możliwość odwołania, zatrzymania i wznowienia transakcji provisioningowej.

Największym wyzwaniem dla systemu provisioningu jest heterogeniczny sprzęt OSE stawiany w szkołach - CPE (router z funkcjonalnością firewall) , switch LAN i Access Pointy Wi-fi. W szczególności część

urządzeń CPE i Access Point Wi-fi jest dostarczana przez beneficjentów POPC, natomiast wszystkie switche LAN są dostarczane przez operatora OSE. Modele tych urządzeń mogą być znane ze stosunkowo krótkim wyprzedzeniem przed ich instalacją/wymianą w procesach podłączania szkoły do OSE lub w procesie obsługi awarii. Modele kolejnych partii urządzeń kupowanych przez operatora OSE (CPE , SW, AP) w kolejnych postępowaniach zakupowych będą znane sukcesywnie w trakcie trwania projektu.

Założenia dotyczące architektury provisionowania usług

System provisioningu będzie obejmować:

1. uruchamianie usług sieciowych na urządzeniach sieciowych OSE i provisionowania usługi End2End; uruchamianie usług na urządzeniach sieciowych może zostać zaimplementowane poprzez bezpośrednie konfigurowanie urządzeń sieciowych (przy wykorzystaniu wszelkich standardowych mechanizmów udostępnianych na urządzeniach szkieletowych - co najmniej SSH, NETCONF i SNMP) lub/i z wykorzystaniem Element Managera do tych urządzeń (wówczas niezbędna jest integracja via API np. REST API i/lub przy pomocy plików płaskich); provisioning ten będzie aktywowany w procesach biznesowym OSE (np. podłączanie szkoły)
2. uruchamianie usług bezpieczeństwa na urządzeniach/systemach bezpieczeństwa i provisionowania usługi End2End; w przypadku usług bezpieczeństwa mechanizm integracji może zostać zaimplementowany poprzez wykorzystanie Element Managera do urządzeń/ integracji z systemami bezpieczeństwa (wówczas niezbędna jest integracja via API np. REST API i/lub przy pomocy plików płaskich) oraz ewentualnie poprzez bezpośrednie konfigurowanie urządzeń bezpieczeństwa (przy wykorzystaniu wszelkich standardowych mechanizmów udostępnianych na urządzeniach szkieletowych - co najmniej SSH, NETCONF i SNMP) jako mniej preferowany model; provisioning ten będzie aktywowany w procesach biznesowych OSE (np. podłączenie szkoły); prawdopodobnym scenariuszem jest użycie zagregowanego API wystawionego tylko z jednego z systemów bezpieczeństwa (np. z systemu DNS Infoblox).
3. możliwie maksymalną automatyzację konfiguracji urządzeń CPE w lokalizacjach szkolnych - jest ona uzależniona jest od możliwości instalowanego urządzenia w zakresie od maksymalnego, czyli ZTP (Zero Touch Provisioning) do minimalnego, czyli przygotowania jedynie plików konfiguracyjnych
4. modyfikacje usług w trakcie ich trwania (zarówno sieciowych jak i bezpieczeństwa) przy pomocy ww. mechanizmów ; provisioning będzie aktywowany procesami biznesowymi OSE
5. integracje z systemami BSS Zamawiającego, w których przebiegają procesy biznesowe OSE (Jira WF, Insight oraz potencjalnie inne jak: sugarCRM, Centralny System Raportowy oparty o Windows Reporting Services)
6. integracje z innymi systemami OSS będącymi częścią Rozwiązania (w szczególności Inventory/CMDB)
7. konfiguracje subskrypcji streamingu telemetrycznego wysyłanego do systemu Telemetrii z sieciowych urządzeń szkieletowych
8. zmiany (również masowe) w konfiguracji urządzeń (szkieletowych i CPE) zgodnie z bieżącą potrzebą Zamawiającego

System musi umożliwiać integrowanie się co najmniej z następującymi systemami i przy użyciu następujących mechanizmów w celu przeprowadzania akcji provisioningowych:

1. integracje związane z provisioningiem:
    a. integracja z 2 Element Managerami do ADC (w 2 węzłach centralnych, F5 Networks)
    b. integracja z 16 Element Managerami do systemu SWG (w 16 węzłach regionalnych)
    c. integracja z 2 Element Managerami do systemów NG Firewall (w 2 węzłach centralnych, Fortinet)
    d. integracja z 2 instancjami Element Managerów do urządzeń sieciowych (w 2 węzłach centralnych, Juniper Network Director)
    e. integracja z 2 systemami zarządzania do systemu DNS (w 2 węzłach centralnych, Infoblox)
    f. bezpośrednia integracja z urządzeniami sieci i bezpieczeństwa
    g. bezpośrednia integracja z urządzeniami w lokalizacjach szkolnych
2. metody integracji związane z provisioningiem:
    a. interfejs API, np. REST API, SOAP
    b. modyfikacja plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym, np. TXT, XML)
    c. wymiana plików o standardowych formatach, np. TXT, CSV, JSON, XML
    d. użycie skryptów i konfiguracja z poziomu CLI
    e. bezpośrednia komunikacja z urządzeniami, co najmniej poprzez :
        i. protokół SSH (w szczególności wymiana kluczy ssh)
        ii. protokół Telnet
        iii. Netconf
        iv. protokół SNMP ver. 2c-3
        v. integrację poprzez pliki konfiguracyjne

Zamawiający nie wyklucza w zakresie systemów bezpieczeństwa zastosowania zagregowanego API**,** zatem system musi pozwalać na integrację z jednym systemem, który posiada integracje z kolejnymi systemami i zapewnia przeniesienie komunikacji dotyczących żądań provisioningowych z OSS do tych systemów i z powrotem.

System musi umożliwiać akcje provisionigu dotyczące co najmniej:

1. W zakresie aktywacji usług sieciowych szkoły na urządzeniach w szkielecie sieci OSE będzie niezbędne wykonanie następujących czynności:
    a. konfiguracja parametrów L2 interfejsu (pojedynczy VLAN albo podwójne tagowanie - QinQ, do 5 VLAN per szkoła)
    b. konfiguracja do 5 interfejsów logicznych per szkoła plus interfejs logiczny per lokalizacja (interfejsy logiczne mogą być zakończone w rożnych VRF)
    c. konfiguracja routingów VRF-aware
    d. konfiguracja adresacji IPv4 / IPv6 na interfejsie (adresy połączeniowe)
    e. konfiguracja routingu statycznego w stronę szkoły plus community dla tych adresów
    f. konfiguracja QoS na łączu (policer, shaper, RED)
    g. konfiguracja innych parametrów QoS (np. klasyfikacja)
2. W zakresie zmian w usługach sieciowych należy założyć wykonywanie:
    a. konfiguracja związana z zarządzaniem adresami publicznymi przedzielanymi szkołom - dodawanie i zdejmowanie dodatkowych zasobów adresowych (routingi statyczne)
    b. konfiguracja parametrów L2 związanych z dodatkowymi VLAN'ami dla szkół
    c. konfiguracja związana ze zmianą przepływności usługi dostępu do Internetu do szkoły
    d. konfiguracja dodatkowych VRF na urządzeniach CPE w szkołach
3. W zakresie aktywacji usług szkoły na urządzeniach/systemach bezpieczeństwa będzie niezbędne wykonanie następujących czynności:
    a. pobranie z systemu IPAM (będącego częścią Rozwiązania) adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153) i przydzielonego do danej szkoły
    b. dodanie ww. adresu podsieci IP do konfigurowalnych polityk na systemach:
        i. ACD,
        ii. NGFW,
        iii. SWG,
        iv. DNS
    c. na systemie SWG:
        i. inicjacja generowania raportów bezpieczeństwa dla danej szkoły, na podstawie predefiniowanych przez Zamawiającego szablonów (ostatecznie raporty wystawiane będą na Portalu OSE)
        ii. określenie harmonogramu generowania raportów dla danej szkoły
    d. lub wykorzystanie zaagregowanego API przygotowanego na systemie
4. W zakresie zmian w usłudze bezpieczeństwa należy założyć modyfikację parametrów polityk zdefiniowanych per szkoła na poszczególnych systemach, w tym w szczególności, choć nie wyłącznie:
    a. na systemie ADC:

i. wyjątki definiujące, jaki ruch ma nie podlegać dekrypcji SSL, np. na podstawie źródłowych lub docelowych adresów IP, adresów URL zawartych w parametrach certyfikatu (pola: SNI lub CN)

b. na systemie NGFW:

i. tworzenie dedykowanych polityk per szkoła blokujących lub przepuszczających ruch z/do zadanych adresów IP, nawiązywany na określonych portach TCP/UDP

ii. włączanie i wyłączanie ruchu mailowego (m. in. protokoły IMAP, POP3) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej

c. na systemie DNS:

i. włączenie / wyłączenie lub zmiana listy kategorii treści przypisanych do polityk określających poziom ochrony użytkowników OSE

d. na systemie SWG:

i. tworzenie dedykowanych polityk per szkoła

ii. dodawanie i usuwanie kategorii blokowanych, skonfigurowanych w polityce dla danej szkoły

iii. dodawanie i usuwanie zawartości statycznych list, zawierających adresu URL, definiujących wyjątki od polityki blokowania dla danej szkoły

iv. włączanie i wyłączanie ruchu mailowego (protokoły HTTP i HTTPS) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej

v. potencjalna zmiany w generowaniu raportów bezpieczeństwa dla danej szkoły na podstawie predefiniowanych przez Zamawiającego szablonów

vi. potencjalna zmiana harmonogramu generowania raportów dla danej szkoły

e. lub wykorzystanie zaagregowanego API przygotowanego na systemie DNS

5. W systemie DNS (Infoblox) będzie zaimplementowane IP registry, którego zawartość będzie budowana na bazie zawartości IPAM OSS (poprzez integrację via API lub/i okresowy export danych). Szczegółowa architektura tego rozwiązania będzie uzgodniona na etapie dokumentu HLD i LLD.
6. W zakresie aktywacji usług lub zmian w usługach na urządzeniach CPE w szkołach niezbędne jest wykonanie w zależności od możliwości danego modelu CPE:

a. przygotowanie konfiguracji w formie pliku do wgrania na urządzenie w celu przekazania do Podwykonawcy wykonującego instalację w szkole (najmniej preferowane i stosowane w ostateczności)

b. automatyczne załadowanie docelowej konfiguracji CPE na urządzenie po nawiązaniu łączności z urządzeniem posiadającym inicjalną konfiguracji

c. automatyczne załadowanie docelowej konfiguracji CPE na urządzenie z zastosowaniem mechanizmu ZTP (Zero Touch Provisioning)

- W zakresie zmian usług w ramach na urządzeniach CPE będą mogły ulegać zmianie:

a. parametry związane z przepustowością łącza

b. przydzielone adresy publiczne

c. inne elementy konfiguracji (w ramach masowych zmian konfiguracji wspólnej dla wszystkich CPE)

W przypadku urządzeń SW i AP instalowanych w szkołach konfiguracja danego typu urządzenia będzie identyczna dla każdej szkoły (sieci szkolne bazują na identycznych sieciach prywatnych). W szczególności urządzenia SW (które są dostarczane wyłącznie przez Zamawiającego) będą fabrycznie przygotowywane z inicjalną konfiguracja OSE, natomiast dla urzsądzeń AP (które mogą być dostarczane przez Zamawiającego lub beneficjenta POPC) będzie przygotowywana inicjalna konfiguracja OSE (per model urządzenia) celem wgrania jej na fizyczne urządzenie przez Podwykonawcę wykonującego instalację w szkole.

Na etapie Projektu Technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na Infrastrukturze bezpieczeństwa i sieci

Wymagania funkcjonalne

Nr Wymagania	Treść Wymagania
O14.F1	system musi mieć możliwość tworzenia własnych skryptów modułów i wtyczek pozwalających na obsługę niestandardowych urządzeń i protokołów dowolnego producenta i typu
O14.F2	system musi posiadać wbudowane urządzenia diagnostyczne pozwalające na sprawdzenie komunikacji z urządzeniem
O14.F3	system musi mieć możliwość generowanie skryptu do uruchomienia na urządzeniu o ile urządzenie wspiera taką funkcjonalność
O14.F4	system provisoningu musi być zintegrowany z innymi systemami OSS w ramach Rozwiązania oraz z systemami BSS Zamawiającego biorącymi udział w procesie aktywacji usługi (np. Jira WF, Insight i sugarCRM)
O14.F5	system musi umożliwiać wywoływanie/testowanie pojedynczych komend konfiguracyjnych
O14.F6	system musi zapewniać możliwość zmiany podstawowych parametrów konfiguracyjnych systemu
O14.F7	każdy z użytkowników systemu powinien posiadać swoje własne imienne konto
O14.F8	system musi zapewnić możliwość integracji z usługą katalogową LDAP (będącej częścią Rozwiązania) i AD (system Zamawiającego) celem uwierzytelniania i autoryzacji na urządzeniach i systemach OSE
O14.F9	system musi zapewnić możliwość ustanowienia jednego lub więcej użytkowników z uprawnieniami administratora systemu

Nr Wymagania	Treść Wymagania
O14.F10	system musi umożliwiać tworzenie grup użytkowników, np. w celu kreowania większych pakietów uprawnień dla wielu użytkowników, dla których wymagany jest jednakowy poziom dostępu
O14.F11	system musi umożliwiać definiowanie ról, które przypisane do użytkowników lub ich grup będą warunkować różne poziomy dostępu (np. dostęp do panelu administracyjnego) i różne uprawnienia (np. wykonywanie operacji zapisu, dostep do urządzeń do których tylko użytkkownik może mieć upranienia - np. podwykonawca tylko do urządzeń szkoły którą serwisuje) w ramach systemu
O14.F12	system musi mieć możliwość restrykcji uruchomienia provisionowania konfiguracji tylko na urządzeniu/grupie urządzeń/typie urządzeń, do których dany użytkownik ma uprawnienia
O14.F13	system musi udostępniać informację typu audytowego pozwalającą na weryfikację działań użytkowników, dostarczającą następujące dane: - czas logowania użytkownika - adres/hostname źródłowy - niepoprawne próby logowania - błędy wykonywania działań w ramach interfejsu użytkownika, ze wskazaniem danych użytkownika - inne informacje wspomagające diagnostykę i identyfikację naruszeń bezpieczeństwa systemu
O14.F14	system musi mieć odpowiednią wydajność by zapewnić povisioning bazujący na intergacji z : - 2 Element Managerami do ADC (w 2 węzłach centralnych, F5 Networks) - 16 Element Managerami do systemu SWG (w 16 węzłach regionalnych) - 2 Element Managerami do systemów NG Firewall (w 2 węzłach centralnych, Fortinet) - 2 instancjami Element Managerów do urządzeń sieciowych (w 2 węzłach centralnych, Juniper Network Director) - 2 systemami zarządzania do systemu DNS (w 2 węzłach centralnych, Infoblox) - urządzeniami sieci i bezpieczeństwa w szkielecie OSE - urządzeniami w lokalizacjach szkolnych system musi umożliwiać również integrację z zagregowanym API wystawionym z jednego dedykowanego systemu celem wykonania provisioningu na kolejnych systemach
O14.F15	w przypadku provisioningu urządzeń w sieci OSE system musi zapewniać (co oznacza wdrożenie) co najmniej: - możliwość konfiguracji usług wymagajacych konfiguracji na wielu urządzeniach jednocześnie, wraz z walidacją konfiguracji i założeniem konfiguracji "wszystko albo nic" - możliwość provisioningu usług z uwzględnieniem integracji z systemami OSS w ramach Rozwiązania jak i z systemami BSS Zamawiającego (np. sugarCRM, Jira WF i Insight) - możliwość provisioningu niezwiązanego z łączami (np. BGP, ACL) - możliwość provisioningu dowolnej konfiguracji ad hoc. przez upoważnionego użytkownika systemu - integrację systemu z Resource Managment (w szczególności IPAM celem pobrania IP lub celem pobrania numeru VLAN), Inventory i z systemem Config Management będących częścią Rozwiązania w celu wygenerowania właściwej docelowej konfiguracji
O14.F16	w przypadku provisioningu urządzeń CPE system musi zapewniać (co oznacza wdrożeie) co najmniej: W zakresie aktywacji usług lub zmian w usługach na urządzeniach CPE w szkołach w zależności od możliwości danego modelu CPE wykonanie jednego z : - przygotowanie konfiguracji w formie pliku do wgrania na urządzenie w celu przekazania do

Nr Wymagania	Treść Wymagania
	Podwykonawcy wykonującego instalację w szkole (najmniej preferowane i stosowane w ostateczności) - automatyczne załadowanie docelowej konfiguracji CPE na urządzenie po nawiązaniu łączności z urządzeniem posiadającym inicjalną konfiguracji - automatyczne załadowanie docelowej konfiguracji CPE na urządzenie z zastosowaniem mechanizmu ZTP (Zero Touch Provisioning) W zakresie zmian w usługach na urządzeniach CPE będą mogły ulegać zmianie (należy zapewnić ich provisioning) : - parametry związane z przepustowością łącza - przydzielone adresy publiczne - inne elementy konfiguracji (w ramach masowych zmian konfiguracji wspólnej dla wszystkich CPE)
O14.F17	W zakresie provisionigu konfiguracji na urządzeniach sieciowych system musi zapewniać (co oznacza wdrożenie) co najmniej : - konfigurację parametrów L2 interfejsu (pojedynczy VLAN albo podwójne tagowanie - QinQ, do 5 VLAN per szkoła) - konfigurację do 5 interfejsów logicznych per szkoła plus interfejs logiczny per lokalizacja (interfejsy logiczne mogą być zakończone w rożnych VRF) - konfigurację routingów VRF-aware - konfigurację adresacji IPv4 / IPv6 na interfejsie (adresy połączeniowe) - konfigurację routingu statycznego w stronę szkoły plus community dla tych adresów - konfigurację QoS na łączu (policer, shaper, RED) oraz innych parametrów QoS (np. klasyfikacja) - konfigurację związaną z zarządzaniem adresami publicznymi przedzielanymi szkołom - dodawanie i zdejmowanie dodatkowych zasobów adresowych (routingi statyczne) - konfigurację parametrów L2 związanych z dodatkowymi VLAN'ami dla szkół - konfigurację związaną ze zmianą przepływności usługi dostępu do Internetu do szkoły - konfigurację dodatkowych VRF na urządzeniach CPE w szkołach - konfigurację innych elementów (w ramach masowych zmian konfiguracji na urzadzeniach OSE)
O14.F18	w przypadku provisioningu urządzeń/systemów bezpieczeństwa OSE system musi zapewniać (co oznacza wdrożenie zgodnie z zakresem zawartym w LLD) co najmniej : - możliwość provisioningu usług bezpieczeństwa świadczonych szkołom polegających na zapewnieniu różnych poziomów filtracji treści co oznacza ustawianie filtracji w systemie SWG (kupowanym w oddzielnym postępowaniu przetargowym) - provisioningu konfiguracji polityk bezpieczeństwa oraz konfiguracji innych aspektów związanych z firewall'ingiem, load-balancingiem i logowaniem zdarzeń bezpieczeństwa w systemach ADC, NG Firewall, SWG (systemy kupowane w oddzielnym postępowaniach przetargowych) - możliwość definiowania nowych polityk bezpieczeństwa na systemach typu firewall, zgodnie z przygotowanymi wcześniej szablonami - możliwość zarządzania (dodawanie, zmienianie, usuwanie) szablonów polityk bezpieczeństwa - możliwość definiowanie nowych poziomów filtracji w systemie SWG, zgodnie z przygotowanymi wcześniej szablonami Powyższe w szczególności oznacza :

Nr Wymagania	Treść Wymagania
	W zakresie aktywacji usług szkoły na urządzeniach/systemach bezpieczeństwa będzie niezbędne wykonanie następujących czynności: - pobranie z systemu IPAM (będącego częścią Rozwiązania) adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153) i przydzielonego do danej szkoły dodanie ww. adresu podsieci IP do konfigurowalnych polityk na systemach: ACD, NGFW, SWG, DNS - na systemie SWG: * inicjację generowania raportów bezpieczeństwa dla danej szkoły, na podstawie predefiniowanych przez Zamawiającego szablonów (ostatecznie raporty wystawiane będą na Portalu OSE) * określenie harmonogramu generowania raportów dla danej szkoły - lub/i wykorzystanie zaagregowanego API przygotowanego na systemie DNS celem wykonania provisioningu na kolejnych systemach W zakresie zmian w usłudze bezpieczeństwa modyfikację parametrów polityk zdefiniowanych per szkoła na poszczególnych systemach, w tym w szczególności, choć nie wyłącznie: - na systemie ADC: * wyjątki definiujące, jaki ruch ma nie podlegać dekrypcji SSL, np. na podstawie źródłowych lub docelowych adresów IP, adresów URL zawartych w parametrach certyfikatu (pola: SNI lub CN) - na systemie NGFW: * tworzenie dedykowanych polityk per szkoła blokujących lub przepuszczających ruch z/do zadanych adresów IP, nawiązywany na określonych portach TCP/UDP * włączanie i wyłączanie ruchu mailowego (m. in. protokoły IMAP, POP3) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej - na systemie DNS: * włączenie / wyłączenie lub zmiana listy kategorii treści przypisanych do polityk określających poziom ochrony użytkowników OSE - na systemie SWG: * tworzenie dedykowanych polityk per szkoła * dodawanie i usuwanie kategorii blokowanych, skonfigurowanych w polityce dla danej szkoły * dodawanie i usuwanie zawartości statycznych list, zawierających adresu URL, definiujących wyjątki od polityki blokowania dla danej szkoły * włączanie i wyłączanie ruchu mailowego (protokoły HTTP i HTTPS) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej * potencjalna zmiany w generowaniu raportów bezpieczeństwa dla danej szkoły na podstawie predefiniowanych przez Zamawiającego szablonów * potencjalna zmiana harmonogramu generowania raportów dla danej szkoły

Nr Wymagania	Treść Wymagania
	- lub/i wykorzystanie zaagregowanego API przygotowanego na systemie DNS celem wykonania provisioningu na kolejnych systemach
O14.F19	system musi zapewnić następujące metody integracji związane z provisioningiem: - interfejs API, np. REST API, SOAP - modyfikacja plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym, np. TXT, XML) - wymiana plików o standardowych formatach, np. TXT, CSV, JSON, XML - integrację poprzez pliki konfiguracyjne - użycie skryptów i konfiguracja z poziomu CLI
O14.F20	system musi zapewnieć następujące bezpośrednie metody komunikacji z urządzeniami poprzez : - protokół SSH (w szczególności wymiana kluczy ssh) - protokół Telnet - Netconf - protokół SNMP ver. 2c-3
O14.F21	system provisioningu musi zapewniać własny interface graficzny zapewniający możliwość tworzenia scenariuszy provisioningu oraz interface umożliwiający uruchamania wybranych scenaniuszy
O14.F22	system ma pozwolać na budowanie dowolnych algorytmów w celu zamodelowania niezbędnych procesów provisioningu na urządzeniach (ich konfiguracja) jak i w systemach OSS lub BSS (odczyt/zapis/modyfikacja danych dotyczących urządzeń, konfiguracji i usług); algorytm taki musi zapewniać: zagnieżdżanie algorytmu w algorytmie, podejmowanie decyzji na podstawie danych wejściowych (również pochodzących z systemów trzecich) , wybór ścieżki algorytmu oraz bezpieczne wycofywanie się z przeprowadzonych kroków oraz mechanizm transakcyjności (możliwość odwołania, zatrzymania i wznowienia transakcji provisioningowej)
O14.F23	wszystkie wymagane funkcjonalności muszą być dostępne w interface'ie graficznym systemu
O14.F24	system musi zapewniać provisioning urzadzeń, do których autoryzacja przebiega z wykorzystaniem protokołów RADIUS i TACACS+
O14.F25	widoki poszczególnych komponentów wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund dla 90% przypadków, dla pozostałych 10% przypadków czas generowania nie może być dłuższy niż 15 sekund, przy czym w przypadku braku komunikacji z elementem zewnętrznym (poza rozwiązaniem wdrażanym w ramach umowy) musi pojawić się stosowny komunikat.
O14.F26	system musi zapewniać kontrolę użytkowników i grup systemu z możliwością przypisywania im ról pozwalających na definiowanie dostępu do określonych skryptów konfiguracji
O14.F27	system provisioningu musi działać bezagentowo
O14.F28	system musi posiadać możliwość zlecania zadań czasowych; statusy wykonanych zadań muszą być komunikowane różnymi drogami (email, sms, alarm w Fault Management)
O14.F29	system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń przez cały okres obowiązywania Umowy

Nr Wymagania	Treść Wymagania
O14.F30	system provisioningu w celu zapewnienia pełnego provisioningu usługi (nie tylko na urządzeniach i systemach sieciowych i bezpieczeństwa) ale także w systemach BSS Zamawiającego musi być zintegrowany co najmniej z (i w zakresie) : - systemem Inventory w celu uaktualnienia danych w Inventory (np. nowe urządzenie, nowa usługa) - systemem workflow Zamawiającego (Jira WF), procesy biznesowe będą wyzwalały zadania w systemu provisioningu (musi być uwzględniona informacja zwrotna z systemu provisioningu w kierunku Jira o statusie wykonanego zadania) - systemem Performance Management w celu uruchomienia stosownych pomiarów i raportów - systemem Fault & Availability Management w celu uruchomienia stosownych pomiarów dostępności - systemem Config Management w celu uruchomienia automatycznego ściągania konfiguracji z nowego urządzenia
O14.F31	system musi mieć możliwość powtarzalnego i niezawodnego uruchamiania algorytmów provisioningu: - algorytmy muszą być zapisywane w repozytorium algorytmów, celem wersjonowania oraz ponownego ich użycia lub wykorzystania w tworzeniu nowego algorytmu - w przypadku gdy dany krok algorytmu nie powiedzie się co w szczególności może spowodować zatrzymanie całego algorytmu provisioningu musi być możliwość wycofania się z przeprowadzonych już kroków - wszystkie uruchomienia provisioningu muszą być logowane na poziomie wykonywania każdego kroku w algorytmie celem sprawdzenia poprawnego wykonania kroków i całego algorytmu (logi powinny być przetrzymywane co najmniej z ostatnich 3 miesięcy)
O14.F32	system musi mieć możliwość implementacji dowolnego scenariusza/algorytmu provisioningu (scenariusz jest tworzony w dostępnym narzędziu)
O14.F33	algorytm provisioningu musi pozwalać co najmniej na: - bezagentową komunikację ze sprzętem/systemami - sprawdzenie/ściągnięcie aktualnej konfiguracji urządzenia - zmianę konfiguracji urządzenia - wgranie oprogramowania/plików na urządzenie - sprawdzenie oprogramowania i sprzętu oraz stanu urządzenia - wykonanie dowolnej komendy na urządzeniu - wykonanie komend na urządzeniu docelowym. do którego jest dostęp poprzez urządzenie "przesiadkowe" (z systemu jest uruchomiony ruting jedynie do urządzenia "przesiadkowego" i dopiero z urządzenia przesiadkowego jest routing do urządzenia docelowego)
O14.F34	komunikacja z urządzeniem/systemem musi przebiegać w sposób bezpieczny (przy pomocy odpowiedniej autoryzacji dostępu) – w szczególności musi być możliwość korzystania z mechanizmu wymiany kluczy ssh
O14.F35	system musi umożliwiać uruchamianie scenariusza provisioningu co najmniej w następujący sposób: - ręcznie przez administratora - w wyniku wywołania z zewnętrznego skryptu utrzymaniowego - w wyniku wywołania z nadrzędnego procesu czy systemu nadzoru – np. triger'owanie mailem, pojawieniem się pliku, zmianą stanu usługi, alarmem - z wsadowego pliku dostarczającego niezbędnych danych do scenariusza

Nr Wymagania	Treść Wymagania
	- z automatycznym pobieraniem danych z systemów nadzoru (do wykorzystania w scenariuszu) , np. dane usługi, szablon konfiguracji, szczegółowe parametry konfiguracji (IP, VLAN, profil bezpieczeństwa itp.)
O14.F36	system musi umożliwiać masowe uruchamianie algorytmów provisioningu
O14.F37	system musi wspierać komunikację z heterogenicznym sprzętem zainstalowanym w szkołach (w szkołach będą instalowane trzy typy urządzeń: CPE, switch LAN, wi-fi access-point); provisioning będzie dotyczyć konfiguracji urządzeń CPE (ruter z funkcją firewall) - pełne zarządzanie i administrowanie urządzeniem pozostaje w gestii operatora OSE W przypadku switch LAN i Access Point Wi-fi w szkołach operator OSE zapewnia inicjalna konfigurację
O14.F38	system musi posiadać łatwy i intuicyjny interface przeznaczony do tworzenia i uruchamiania algorytmów provisioningu
O14.F39	system musi wspierać integrację z systemami OSE i systemami NASK Zamawiającego co najmniej : - na poziomie API - na poziomie bazodanowym - na poziomie wymiany poczty SMTP
O14.F40	system musi posiadać dostęp do gotowych do wykorzystania bibliotek/funkcji współpracy z istniejącymi na rynku urządzeniami, bazami danych, technologiami integracji (w ramach Rozwiązania)
O14.F41	przed wpisaniem konfiguracji na urządzenie musi być sprawdzane czy jest to konieczne (czy konfiguracja jest już zaimplementowana na urządzeniu)
O14.F42	system musi zapewnić optymalizację ilości sesji nawiązywanych z urządzeniem/systemem (jeżeli algorytm wielokrotnie komunikuje się z tym samym urządzeniem celem wykonania różnych etapów provisioningu konfiguracji, sesja jest zestawiana tylko raz i podtrzymywana na czas wykonania wszystkich operacji na urządzeniu)
O14.F43	w system musi być standardowo wbudowane wysyłanie powiadomień : maile lub/i smsy i/lub alarmy (trapy snmp, syslogi) w wyniku niepoprawnego zakończenia się algorytmu lub w wyniku nieudanego kroku
O14.F44	system musi zapewniać forward'owanie logów i alarmów z działania systemu provisioningu do systemu fault & performance management będącego cześcią Rozwiązania
O14.F45	musi istnieć możliwość generowania prostych raportów/statystyk z przeprowadzanych uruchomień algorytmów provisioningu z informacjami co najmniej kiedy i przez kogo były uruchamiane oraz jaka była ilość udanych i nieudanych prób włącznie z przyczyną problemu
O14.F46	musi istnieć możliwość eksportowania logów/raportów z przeprowadzanych uruchomień i wycofań scenariuszy provisioningu do plików w standardowym formacie (co najmniej TXT, CSV)
O14.F47	w systemie musi istnieć narzędzie do tworzenia algorytmów/scenariuszy provisionigu usług i konfiguracji przez użytkownika systemu po odpowiednim przeszkoleniu
O14.F48	system musi prezentować listy provision'owanego sprzętu (w ramach Rozwiązania)

Nr Wymagania	Treść Wymagania
O14.F49	system musi prezentować listy provision'owanej konfiguracji (w ramach Rozwiązania)
O14.F50	system musi prezentować listy szablonów konfiguracji (w ramach Rozwiązania)
O14.F51	musi istnieć możliwość eksport'owania skonfigurowanych algorytmów/scenariuszy provisioningu do standardowych formatów plików celem ich dokumentacji i łatwiejszej potencjalnej migracji tych algorytmów do innego systemu provisioningu
O14.F52	system musi wspierać wersjonowanie konfiguracji po każdej modyfikacji z możliwością podglądu zmian do 5 wersji wstecz
O14.F53	Rozwiązanie musi zawierać funkcjonalności dostosowujące przetwarzanie do wydajności ograniczając liczbę jednoczesnych wykonań procesów provisioningu do zadanego limitu (procesów per dany scenariusz i lub obciążenia systemu).
O14.F54	Rozwiązanie musi zawierać funkcjonalność do monitorowania przetwarzania procesów provisioningu umożliwiającą śledzenie stanu wykonywanych procesów. Wyniki monitorowania muszą pozwalać na weryfikację poprawności wykonań procesów oraz na potencjalne wykrywanie problemów z wydajnością i komunikacją z provisionowanymi urządzeniami/systemami.
O14.F55	Rozwiązanie musi umożliwić konfigurację alarmów w ramach monitorowania procesów provisioningu. Alarmy muszą być możliwe do ustawienia zarówno dla przypadków przekroczenie zadanych limitów lub obciążenia systemu jak i w przypadku błędów w wykonaniu procesów (w tym w obszarze komunikacji z provisionowanymi urządzeniami/systemami)
O14.F56	Rozwiązanie musi zawierać mechanizm umożliwiający na wznowienie (również masowo) błędnych procesów provisioningu np. po usunięciu błędu lub po modyfikacji parametrów wejściowych dla scenariusza
O14.F57	System musi pozwalać na provisioning poprzez zagregowane API - integracja z jednym dedykowanym systemem, który posiada integracje z kolejnymi systemami i zapewnia przeniesienie komunikacji z OSS do tych systemów i z powrotem
O14.F58	System musi zapewniać możliwość provisionowania konfiguracji w zakresie L3VPN (MPLS/BGP VPN) na urządzeniach agregacyjnych (Juniper)
O14.F59	System musi umożliwiać provisioning parametrów konfiguracyjnych obecnie nie wykorzystywanych ale potencjalnie możliwych do wprowadzania w dalszych etapach projektu OSE i zgodnie z możliwościami urzadzeń OSE (np. konfiguracja VPN Multicast'owych)

7.4.5. Inwentaryzacja OSE (Inventory/CMDB)

System Inwentaryzacji OSE (CMDB) ma szczególną i bardzo ważną rolę w projekcie gdyż jego zadaniem jest zbieranie i udostępnianie wszystkich informacji na temat zasobów OSE - są to, co najmniej:

- informacje techniczne zarówno o zasobach aktywnych jak i pasywnych,

- informacje o zasobach będących własnością Operatora OSE jak i beneficjentów POPC (sprzęt w szkołach),
- informacje na temat zasobów własnych jak i dzierżawionych jak łącza czy miejsca w centrach kolokacyjnych,
- informacje na temat świadczonych usług i ich parametrach,
- typowe informacje inwentarzowe urządzeń zaciągane do systemu w sposób automatyczny (np. numer seryjny, nazwa producenta, model urządzenia, wersje sprzętu i oprogramowania, MAC adress, elementy składowe: chassis, karty, interface'y, dyski itp.)
- typowe informacje inwentarzowe wpisywane do systemu "ręcznie" (np. dane dotyczące gwarancji, SLA, kontakt do wsparcia producenta, numer inwentarzowy itp.)

System Inwentaryzacji/CMDB (Config Management Database) OSE musi objąć swym zasięgiem zarówno sprzęt sieciowy i bezpieczeństwa jak i serwery w węzłach regionalnych i centralnych. W związku z powyższym system musi móc komunikować się z dowolnymi urządzeniami infrastruktury sieciowej, bezpieczeństwa i serwerowej stosowanymi w OSE w celu zebrania informacji o sprzęcie fizycznym i serwerach wirtualnych w węzłach centralnych i regionalnych bądź uzyskać te informacje z systemu DCIM (Data Center Infrastructure Monitoring), będącego elementem przedmiotu zamówienia. System musi także posiadać informacje o dodatkowym sprzęcie w centrach kolokacji (np. szafy telekomunikacyjne, UPS'y, klimatyzatory itp.), zatem system Inventory musi być zintegrowane poprzez API z systemem zarządzania centrum kolokacji Zamawiającego (system kupowany w oddzielnym postępowaniu zakupowym).

System Inventory/CMDB musi także zapewnić identyfikację relacji pomiędzy usługą a infrastrukturą (sprzęt/łącza/serwery), na której ta usługa jest świadczona. W związku z powyższym i w związku z tym, że stanowi on źródło informacji dla pozostałych systemów system Inwentaryzacji OSE musi być zintegrowany z innymi systemami w ramach Rozwiązania oraz z systemami BSS Zamawiającego. System Inventory w ramach Rozwiązania ma pełnić też rolę bazy CMDB. Rozwiązanie, zatem ma dawać pełny widok na wszystkie zasoby sieci OSE.

System Inwentaryzacji ma paszportyzować, co najmniej poniższe zasoby:

- infrastruktura serwerowa,
- łącza szkieletowe, agregacyjne, dostępowe,
- lokalizacje węzłów szkieletowych (regionalnych i centralnych),
- lokalizacje jednostek oświatowych
- sprzęt kolokacyjny OSE umiejscowionym w lokalizacjach węzłów,
- sprzęt i systemy sieciowe i bezpieczeństwa zainstalowane w węzłach OSE (dane szczegółowe, np. hardware, software, licencje, serwis itp.),
- sprzęt zainstalowany w danej jednostce oświatowej,

- katalog dostępnych typów urządzeń i producentów,
- katalog dostępnego oprogramowania, aplikacji, licencji i bibliotek,
- katalog świadczonych usług (powiązanie z zasobami technicznymi sieci OSE, parametry usług, powiązanie między usługami)

Wszystkie obiekty w bazie Inventory/CMDB mają być sparametryzowane pod kątem potencjalnych przyszłych analiz i potrzeb, zatem system musi pozwalać na dodawanie dowolnych atrybutów opisujących obiekty w systemie Inventory. System ma umożliwiać generowanie prostych zbiorczych raportów z wykorzystania dowolnych zasobów w Inventory. Musi być również zintegrowany z Centralnym Systemem Raportowym Zamawiającego w celu generowania cyklicznych raportów.

W szczególności system Inventory/CMDB musi być zintegrowany z innymi systemami Rozwiązania jak z systemami BSS Zamawiającego w zakresie, co najmniej poniższych informacji, aby je wygodnie prezentować:

- parametry serwisowe wybranych obiektów w CMDB
- parametry SLA urządzeń/systemów i usług,
- dane teleadresowe, dane kontaktowe niezbędne w procesie utrzymania sieci OSE,
- dokumentację techniczną/linki do dokumentacji, bazę wiedzy,
- przechowywana korespondencja dotycząca węzłów/kolokacji OSE,
- historia zgłoszeń awarii/prac planowych w wyniku integracji z systemami BSS Zamawiającego,
- linki do statystyk związanych z danym sprzętem / systemem /usługą,
- linki do konfiguracji sprzętowej i softwareowej urządzeń,
- numery seryjne sprzętu i oprogramowania,
- szablony konfiguracji,
- parametry konfiguracji dla provisioningu danego typu/modelu urządzenia i danej usługi

Wdrożone przez Wykonawcę Inventory dla systemów OSE OSS ma być rozszerzoną repliką (w modelu master-slave) w stosunku do inventory w systemach OSE NASK, którym jest przede wszystkim Insight. Masterem danych ma być Insight. Na etapie projektu technicznego zostanie określony szczegółowy zakres danych będących repliką z Insight (bądź innych systemów BSS Zamawiającego) oraz zakres danych pozyskiwanych/wprowadzanych w Inventory niezależnie od systemów BSS Zamawiającego). Należy wziąć pod uwagę, że już obecnie w Insight Zamawiający posiada taki zestaw danych, który pozwala na prowadzenie procesu podłączania szkół w niezbędnym zakresie obejmującym podstawowy model podłączenia szkoły do OSE (OSE i OSE POPC).

W ramach Rozwiązania Wykonawca będzie miał za zadanie wdrożenie odpowiednich mechanizmów do ww. replikacji i modyfikacji danych, aby zapewnić ich spójność i poprawność. Inventory/CMDB OSE OSS może zawierać znacznie większy zestaw danych (zgodnie z potrzebami systemów OSE OSS) i dla tych danych Inventory OSE OSS będzie masterem. Wybór sposobu integracji z Insight i potencjalnie innymi

systemami BSS Zamawiającego będzie częścią projektu technicznego, który wykona Wykonawca przy współpracy z Zamawiającym - nie mniej jednak należy założyć następujące metody integracji:

- interface REST API wystawiany przez systemy BSS Zamawiającego (co najmniej Insight, Jira)
- referencja do obiektów w Insight
- pliki Json, XML, XLS (eksport z systemów Zamawiającego)
- interface REST API wystawiany przez Inventory OSE OSS
- eksport danych z Invetory OSE OSS w standardowych formatach plików (Json, XML, CSV, TXT, XLS, PDF)

Ponieważ obszar Inventory/CMDB spina wszystkie wdrażane systemy OSS pod kątem zasobów, na których te systemy działają jest to najlepsze miejsce by przedstawić wizję wymiany informacji pomiędzy wdrażanymi systemami a systemami trzecimi., zatem w zakresie obszarów integracji Rozwiązania (w tym Inventory) z systemami BSS Zamawiającego należy wyróżnić, co najmniej:

kierunek przepływu danych OSE NASK → OSE OSS

- pobieranie danych inwentarzowych zawartych w systemach Zamawiającego (Insight) celem przedstawiania ich w Inventory OSE OSS
- pobieranie danych usług i danych SLA itp. z umów (kosztowych i przychodowych) zawartych w systemach Zamawiającego (Insight, sugarCRM) celem przedstawiania ich w Inventory OSE OSS
- pobieranie danych biznesowych zawartych w systemach Zamawiającego niezbędnych do provisioningu konfiguracji usług na urządzeniach szkieletowych i szkolnych
- przekazywanie/pobieranie informacji o awariach masowych (od operatorów łącz) z systemów biznesowych Zamawiającego do systemu OSE OSS
- przekazywanie/pobieranie informacji o pracach planowych zarówno operatorów łącz jak i operatora OSE (w szkielecie OSE) z systemów BSS Zamawiającego do systemu OSE OSS celem "wyciszania" alarmów w FM OSS
- inicjacja procesu provisioningu usług przez proces biznesowy w BSS Zamawiającego (Jira) - możliwość przekazania paramentów do systemu provisioningu konfiguracji w OSS i zwrotne informacje o jego statusie zakończenia (również w ramach awarii zgłaszanych przez szkoły i konieczności wymiany sprzętu na nowy, dla którego należy przeprowadzić provisioning właściwej konfiguracji)

kierunek przepływu danych OSE OSS → OSE NASK

- przekazywanie informacji o awariach masowych infrastruktury szkieletowej OSE z FM OSS do systemów BSS Zamawiającego (wystawianie zgłoszeń dla NOC)
- pobieranie/przekazywanie informacji o zasobach w Inventory/CMDB OSE OSS (urządzenia, ich konfiguracje w docelowej sieci sieci szkieletowej i urządzeniach OSE w szkole, inne) przez system Inventory Zamawiającego

- przekazywanie informacji o awariach na urządzeniach/w sieci OSE celem wystawiania zgłoszeń lub/i wzbogacania informacji w zgłoszeniach w procesach biznesowych Zamawiającego związanych z obsługą awarii w Trouble Ticketing/ServiceDesk (Jira SD)
- przekazywanie danych o ruchu w generowanego przez szkoły (per VLAN/szkoła/lokalizacja szkolna) i zbieranym przez system Telemetrii do Centralnego Systemu Raportowego Zamawiającego
- przekazywanie danych o ruchu w generowanego w szkielecie sieci OSE (interface counters) zbieranym przez system Telemetrii do Centralnego Systemu Raportowego Zamawiającego
- przekazywanie wszelkich informacji raportowych do systemów BSS Zamawiającego (co najmniej Centralny System Raportowy)
- przekazywanie informacji mailem lub/i zgłoszeniem w Jira do NOC (w czasie monitoringu w trakcie 3 tyg. od podłaczenia do OSE lub w trakcie 2 tyg. diagnostyki zgłoszonych problemów są alarmy, przekroczenia na statystykach)
- przekazywanie informacji na temat wysycania łącz (na bazie zbieranego ruchu) do procesów biznesowych Zamawiającego inicjujących upgrade łącza - dotyczy to łącz szkieletowych, agregacyjnych i dostępowych; w przypadku tych ostatnich ze względu na to, że nie będzie zbierany non-stop ruch z CPE a w PWR/PPWR Zamawiający nie posiada własnych urządzeń aktywnych, badanie wysycenia łącz dostępowych musi bazować na badaniu wielkości ruchu per lokalizacja szkolna (suma ruchu z wszystkich VLAN wszystkich szkół w danej lokalizacji szkolnej)
- przekazywanie informacji do procesów biznesowych Zamawiającego o tym że szkoła przekracza przepustowowość określoną w umowie na podstawie badania ruchu w VLANach szkoły
- przepływ informacji w związku z procesem masowej zmiany konfiguracji na okreslonej puli urządzeń
- przepływ informacji w związku z procesem upgradu oprogramowania na określonej puli urzadzeń

System Inventory wystawiony w ramach interface'u graficznego Rozwiązania będzie umożliwiał użytkownikom na podgląd lub/i edycję wybranych informacji zawartych w bazie zgodnie z ich uprawnieniami i zgodnie z przyjętymi założeniami obróbki danych per dany obiekt w CMDB.

Wymagania funkcjonalne:

Nr Wymagania	Treść Wymagania
O15.F1	system musi zapewniać dostęp do wybranych funkcjonalności w wyniku właściwej autoryzacji użytkowników zgodnie z przypisanymi im profilami uprawnień: - zarówno używając natywnego mechanizmu autoryzacji systemu OSS - jak i za pośrednictwem mechanizmu Single Sign On dostarczonego przez Wykonawcę
O15.F2	system musi pozwalać na batch'owy import danych ze standardowych formatów plików (co najmnej CSV, JSON, XML, XLS) a także na export do ww. formatów plików
O15.F3	system musi zapewnić identyfikację relacji pomiędzy usługą a infrastrukturą (urzadzenia/łącza/lokalizacje), na której ta usługa jest świadczona

Nr Wymagania	Treść Wymagania
O15.F4	system musi zapewniać funkcjonalność inwentaryzacji zarówno zasobów fizycznych i logicznych jak również zasobów infrastruktury oraz usług i ich parametrów
O15.F5	system musi umożliwiać inwentaryzację sieci zbudowanych w wielu technologiach (m.in. DWDM, SDH/PDH, Ethernet, IP/MPLS backbone, ATM, SDN, IP)
O15.F6	system musi zapewniać inwentaryzację infrastruktury sieciowej, bezpieczeństwa a także centrów kolokayjnych (szafy, serwery, zasilanie, klimatyzacja, przełączniki, routery, karty itp.)
O15.F7	system Inventory (rozumiany też jako CMDB) musi pozwalać przechowywanie i prezentowanie informacji w kontekście zasobów OSE, będą to co najmniej informacje o: - sprzęcie i systemach w sieci OSE (węzły OSE i lokalizacje szkolne) - sprzęcie i systemach w centrach obliczeniowych - serwerach i systemach zainstalowanych w węzłach OSE - dla ww. punktów hardware, software, licencje, biblioteki, serwis itp. - łączach dzierżawionych w szkielecie sieci OSE (przebieg łacza, parametry, dane operatora, gwaratowane parametry SLA itp.) - łączach agregacyjnych i dostępowych do jednostek oświatowych (przebieg łacza, parametry, dane operatora, gwaratowane parametry SLA) - lokalizacjach węzłów szkieletowych (centralnych i regionalnych) - sprzęcie kolokacyjnym OSE umiejscowionym w lokalizacjach węzłów (np. szafy kolokacyjne, parametry typu ilość U, kWh itp.) - lokalizacjach jednostek oświatowych (partner serwisowy obsługujący lokalizację szkolną, operator łącza podłączającego lokalizację szkolną itp., VLAN zarządzający, CPE) - partnerach serwisowych (powiązanie z obsługiwanymi szkołami) - operatorach łącz agregacyjnych i ich powiązań z operatorami łącz dostępowych, z PWR, z węzłami OSE - operatorach łącz dostępowych i ich powiązanie z operatorami łącz agregacyjnych, z lokalizacją szkolną, PWR/PPWR/węzłem OSE - PWRach – Punkach Wymiany Ruchu (dane adresowe, szafa, odpowiedzialność, punkt styku) i ich powiązaniach z łączami dostępowym i agregacyjnym - PPWRach - Powiatowy Punkt Wymiany Ruchu (dane adresowe, szafa, odpowiedzialność, punkt styku) i ich powiązaniach z łączami dostępowym do lokalizacji ODN - kontaktach (zarówno w szkołach, w OPSach, u partnerów serwisowych/podwykonawców, u operatorów łącz itp.) - jednostkach oświatowych (dane teleadresowe, IP, VLANy, sprzęt OSE) i ich powiązanie z lokalizacjami szkolnymi , "masterem" tych danych będą systemy BSS Zamawiającego (Insight, sugarCRM) - połączeniach pomiędzy urządzeniami - katalogu dostępnych typów/modeli urządzeń i producentów (wraz oprogramowaniem) - katalogu dostępnego oprogramowania - aplikacjach - certyfikatach, licencjach, bibiotekach - katalogu świadczonych usług (powiązanie ze sprzętem i ze szkołą) - "masterem" tych danych będą systemy BSS Zamawiającego (Insight, sugarCRM) - innych potencjalnych elementach niezbędnych dla pozostałych systemów ramach Rozwiązania a w szczególności dla systemu provisioningu

Nr Wymagania	Treść Wymagania
	Część wyżej wymienionych danych pochodzi z systemów BSS Zamawiającego, zatem wymagana jest interakcja Inventory z tymi systemami. Sposób implementacji integracji pomiedzy tymi systemami w ramach Rozwiązania pozostaje w gestii Wykonawcy i będzie uzgodniony z Zamawiającym na etapie projektu technicznego . W szczególności dane te będą pochodzić z systemu Zamawiającego pełniącego rolę Master Inventory (Insight) jednak nie wyklucza się innych źródeł danych.
O15.F8	system musi pozwalać na identyfikację położenia poszczególnych urządzeń/elementów sieci OSE w pomieszczeniach, w szafach, na półkach
O15.F9	system musi pozwalać na integrację z systemem zarządzania centrum kolokacji (kupowanym przez Zamawiającego w odrębnym postępowaniu zakupowym) w celu pobierania informacji na temat infrastruktury kolokacyjnej przy wykorzystaniu standardowych mechanizmów integracji - co najmniej: - przy pomocy plików płaskich, co najmniej CSV - plików w standardowych formatach, np. XML, JSON, XLS - przy pomocy co najmniej REST API
O15.F10	system musi umożliwiać generowanie prostych zbiorczych raportów na temat dowolnych zasobów z Inventory oraz przekazywanie/udostępnianie informacji do Centralnego Systemu Raportowego Zamawiającego
O15.F11	system musi być zintegrowany z innymi obszarami funkcyjnymi Rozwiązania Fault & Performance Management , Config & Provisioning Managment, Telemetria) aby wygodnie prezentować w GUI użytkownika systemu / całego Rozwiązania co najmniej następujące informacje : - parametry serwisowe powiązane z kolokcjami/węzłami OSE oraz urządzeniami w szkielecie OSE, - paramery serwisowe powiązane z infrastruktura łącz dzierżawionymi (szkieletowe, agregacyjne, dostępowe PWR, PPWR), - parametry serwisowe powiązane z lokalizacjami szkolnymi/szkołami (urządzeniami i infrastrukturą OSE) - parametry SLA w danym okresie dla urządzeń/systemów OSE jak i dla świadczonych usług, - dane teleadresowe, osoby kontaktowe do lokalizacji szkolnych - dane teleadresowe, różne typy kontaktów do partnerów OSE (dostawcy łacz/kolokacji, podwykonawcy) - przechowywane dokumentacji technicznych / alternatywnie linki do dokumentacji, - przechowywana korespondencja dotycząca węzłów/kolokacji OSE, - historia zgłoszeń awarii sprzętu/ zadań zleconych (w kontekście wybranego sprzętu) - integracja z systemami BSS Zamawiającego (np. Jira SD), - baza wiedzy na temat problemów i rozwiązań, - linki do statystyk związanych z danym sprzętem / systemem /usługą, - konfiguracja hardware'owa i software'owa urządzeń (aktualna i historyczna), - numery seryjne sprzętu i oprogramowania, - szablony konfiguracji dla typów/modeli urządzeń (niebędne dla funkcjonalności provisioningu), - parametry konfiguracji dla provisioningu danego typu/modleu urządzenia i danej usługi , w przypadku usługi dla szkoły nie tylko parametry przydzielane w ramach OSE ale równiez parametry VLANów przydzielanych przez operatorów łacz dostępowych/agregacyjnych - integracja z systemami BSS Zamawiającego (np. Jira WF, Insight)
O15.F12	system musi pozwalać uprawnionym użytkownikom na update informacji/obiektów w bazie Inventory a także automatyczny update obiektów wywołany po stronie systemów BSS

Nr Wymagania	Treść Wymagania
	Zamawiającego: - w wyniku działania procesów biznesowym OSE - poprzez integrację z tymi systemami (np. Insight, Jira WF, inne)
O15.F13	system musi umożliwiać integrację z systemami trzecimi (systemy BSS Zamawiającego) poprzez API np. za pośrednictwem: - REST API, SOAP - za pomocą plików płaskich co najmniej CSV - za pomocą plików w standardowych formatach, np. XML, JSON, XLS - potencjalnej szyny danych Zamawiającego
O15.F14	system musi posiadać wsparcie producenta lub/i społeczności w zakresie typów integracji, integrowanych typów urządzeń/systemów a także rozwoju funkcjonalności pod kątem nowych technologii w trakcie trwania umowy
O15.F15	Widoki poszczególnych komponentów wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund dla 90% przypadków, dla pozostałych 10% przypadków czas generowania nie może być dłuższy niż 15 sekund, przy czym w przypadku braku komunikacji z elementem zewnętrznym (poza rozwiązaniem wdrażanym w ramach umowy) musi pojawić się stosowny komunikat.
O15.F16	system musi pozwalać na dowolne dodawanie nowych atrybutów/zmianę obecnych w obiektach w Inventory, baza CMDB musi umożliwiać rozszerzanie schematu danych o kolejne atrybuty.
O15.F17	systemu musi obrazować niedostępność obiektu typu urządzenie/łącze/system w przypadku wykrycia dla obiektu niedostępności przez system Fault & Availability Management (w ramach Rozwiązania)
O15.F18	w ramach funkcjonalności typu CMDB (baza obiektów/konfiguracji) Rozwiązanie musi : - realizować rejestrowanie, przechowywanie, śledzenie oraz prezentowanie informacji o konfiguracji oraz poszczególnych elementach konfiguracji od momentu ich zarejestrowania w systemie - wersjonowanie elementów konfiguracji. - dostarczyć zaimplementowane i uruchomione mechanizmy wykonywania (automatycznie) pobierania konfiguracji oraz elementów konfiguracji. - umożliwiać tworzenie stanów odniesienia konfiguracji, obejmujący zestaw elementów konfiguracji. - realizować funkcje eksportu (co najmniej plik) i udostępniania wybranej konfiguracji lub wybranego stanu odniesienia konfiguracji. - realizować przechowywanie utworzonych stanów odniesienia konfiguracji oraz ich udostępnianie na życzenie. - porównywanie zarejestrowanych stanów odniesienia konfiguracji ze stanami historycznymi. - udostępniać funkcjonalności umożliwiające importowanie elementów konfiguracji wraz z atrybutami z zewnętrznych baz danych. - udostępniać zewnętrznym systemom zgromadzone dane (API, export).
O15.F19	Rozwiązanie musi prezentować informacje o pracach planowych w odniesieniu do elementów sieci, okresu niedostępności i dotkniętych nią usług - integracja z systemami BSS Zamawiającego

Nr Wymagania	Treść Wymagania
O15.F20	Rozwiązanie musi zapewniać prezentowanie informacji o awariach masowych zarówno w odniesieniu do zasobów dzierżawionych jak i zasobów własnych OSE, okresu niedostępności i dotkniętych nią usług - integracja z systemami BSS Zamawiającego
O15.F21	Łącza (w szczególności pomiędzy lokalizacją Szkoły a Punktem Styku PWR/PPWR) muszą być importowane do systemu wsadowo z pliku (np. txt/excel) ze zdefiniowanymi polami. Łącza muszą być w systemie utworzone automatycznie - wśród pól opisowych będą w szczególnośc statusy (np. planowane do uruchomienia, uruchomione , zlikwidowane itp.) i operatorzy łącz. Musi byc możliwość zmiany pól (w sczególności statusów) w wyniku ich zmiany w procesach biznesowych poprzez integarcję Rozwiązania z systemami BSS Zamawijącego (np. Jira WF)
O15.F22	Rozwiązanie musi pobierać aktualne dane niezbędne utrzymania sieci OSE takie jak dane operatorów łącz, serwisantów urzadzeń itp. poorzez integrację z systemami BSS Zamawiającego jak również wsadowo z pliku
O15.F23	system musi zapewniać przechowywanie danych dotyczących topologii sieci między innymi z uwzględniem : - łącz szkieletowych (łącza pomiędzy węzłami sieci OSE) - musi istnieć mozliwość ręcznego wprowadzania łącz poprzez wskazanie ich lokalizacji - lokalizacji węzłów PWR - Punk wymiany ruchu (szacowana ilość : 80) - łącz dostępowych (od lokalizacji szkoły do PWR) przypisane do lokalizacji - łącz tranzytowych (od PWR do węzła OSE) , łącza te mogą być wprowadzane ręcznie przy czym wybór lokalizacji węzłów (punktów styku) musi być osłownikowany a lokalizacja rozumiana nie tylko przez adres ale również lokalizację w budynku (nr pomieszczenia czy szafa) - ładowanie ww. obiektów może się odbywac na rózne sposoby, np. ręcznie, wsadowo z pliku, poporzez integrację z systemami BSS Zamawiającego (np. Insight lub/i Jira WF w wyniku kroku w procesie biznesowym)
O15.F24	Rozwiązanie musi umożliwiać automatycznie zestawiać relacje pomiedzy PWR a danym Łączem tranzytowym na podstawie danych z systemów BSS Zamawiającego poprzez integrajcę np. z Insight lub/i z Jira WF (w wyniku kroków w procesie biznesowym w którym operator wysyła maila do OSE a tymi danymi). Docelowo w systemie musi istnieć możliwość wyświetlenia w jaki sposób jest zestawione łącze End2End z lokalizacji szkolnej do węzła OSE.
O15.F25	system musi umożliwiać następujące sposoby zasilania go danymi: - ręczne przez uprawnionego użytkownika systemu - wsadowo ze standardowych formatów plików (co najmnej, CSV, XML, JSON, XLS) - automatycznie, w wyniku pobierania danych bezpośrednio z urzadzeń sieciowych, bezpieczeństwa, serwerowych (poprzez co najmniej SNMP, SSH/RCONFIG) - automatycznie via API z systemu DCIM (Data Center Infrastructure Monitoring będącego cześcią Rozwiązania) - automatycznie via API z systemu zarządzania kolokacjami OSE (kupowany w oddzielnym postępowaniu) - integrację co najmniej poprzez REST API, pliki w formacie XML, JSON, XLS, CSV
O15.F26	Rozwiązanie musi zawierać bazę ewidencji konfiguracji - CMDB zintegrowaną z funkcjonalnością zgłaszania incydentów i zgłaszania zmian (integracja z systemami BSS Zamawiającego)
O15.F27	W bazie CMDB muszą być zebrane informacje pochodzące z Inventory OSS a także informacje związane z zarządzaniem elementami IT jak np. rodzaje i terminy gwarancji i wsparcia.

Nr Wymagania	Treść Wymagania
	Uzupełnianie/modyfikacja danych w bazie ma być możliwe zarówno: - ręcznie - z procesów biznesowych i procesów zachodzących w OSS - zasilaniem batchowym - przy pomocy wystawionego dedykowanego API
O15.F28	CMDB musi umożliwiać synchronizację/aktualizację obiektów w bazie CMDB z zasobami którym te obiekty odpowiadają
O15.F29	system Inventory ma być roszerzoną repliką (w modelu master-slave) w stosunku do inventory w systemach OSE NASK (głównym masterem danych będzie system Insight Zamawiającego); w ramach Rozwiązania Wykonawca musi wdrożyć odpowiednie mechanizmy do ww. replikacji i modyfikacji danych aby zapewnić ich spójność i poprawność w Inventory/CMDB OSS - należy nałożyć co najmniej następujące metody integracji: - interface REST API wystawiany przez systemy BSS Zamawiającego (co najmniej Insight, Jira) - referencja do obiektów w Insight - pliki Json, XML, XLS (export z systemów Zamawiającego) - interface REST API wystawiany przez Inventory OSE OSS - export danych z Invetory OSE OSS w standardowych formatach plików (Json, XML, CSV, TXT,XLS, PDF)
O15.F30	system Inventory/CMDB musi pozwalac na : - zaciągane do systemu w sposób automatycznyz urządzeń typowych informacji inwentarzowych (np. numer seryjny, nazwa producenta, model urządzenia, wersje sprzętu i oprogramowania, MAC adress, elementy składowe: chassis, karty, interface'y, dyski itp.) - wpisywanie do systemu innych informacji inwentarzowych (np. dane dotyczące gwarancji, SLA, kontakt do wsparcia producenta, numer inwentarzowy itp.)

7.4.6 Wymagania wspólne dla wszystkich systemów OSS

Nr Wyamagania	Treść Wymagania
O17.F1	Rozwiązanie oferowane przez Wykonawcę musi być zgodne z zapisami przedstawionymi w pkt. 7.4 "Opis funkcjonalności dla obszaru OSS"
O17.F2	w ramach wdrożenia OSS Wykonawca jest zobowiązany do przygotowania konfiguracji konsol operatorskich niezbędny do pracy NOC (Network Operation Center), Wykonawca przygotuje te konsole z wydzieleniem co najmnie 15 widoków dla NOC i 15 dla SOC oraz 10 widoków dla operatorów I linii wsparcia.
O17.F3	system OSS w ramach konfiguracji konsol dla NOC/SOC musi mieć możliwość współdzielenia konsol między użytkownikami w ramach ich uprawnień.
O17.F4	system OSS musi zapewnić możliwość wykrywania urządzeń sieciowych z wykorzystaniem protokołów, co najmniej: ICMP, SSH, TELNET, SNMP (v2c, v3), oraz potencjalnie WMI, JMX, RPC

Nr Wyamagania	Treść Wymagania
O17.F5	systemy OSS muszą być zintegrowane z systemem SMTP Zamawiającego w celu wysyłania maili
O17.F6	interfejs webowy systemów OSS musi być wspierany przez popularne przeglądarki internetowe - co najmniej przez Mozilla Firefox oraz przez Microsoft IE lub Microsoft Edge
O17.F7	interface systemów OSS (co najmniej w zakresie funkcjonalności niezbędnej do wykonywania prac w terenie) musi być dostępny na urządzeniach mobilnych działających na systemach iOS i Android
O17.F8	systemy OSS muszą być dostępne w web'owym interfejsie po zalogowaniu (co najmniej musi być zachowane pojedyncze logowanie dla części OSS i BSS Rozwiązania)
O17.F9	system OSS musi pracować w architekturze HA (High Availability) – co najmniej w oparciu o HA infrastruktury serwerowej
O17.F10	Rozwiązanie musi umożliwiać integrację ze storage obiektowym (protokołem REST API lub S3) w celu przesyłania wybranych danych do archiwum
O17.F11	systemy OSS muszą zapewnić możliwość kreowania nowych użytkowników o różnych poziomach dostępu (np. ReadOnly, ReadWrite, Admin etc.)
O17.F12	Należy zapewnić regularne aktualizacje systemów operacyjnych, systemów w zakresie bezpieczeństwa oraz wersji oprogramowania poprzedzone testami (również regresji) na środowiskach produkcyjnym i preprodukcyjnym. Musi istnieć możliwość wersjonowania i przywracania poprzedniej wersji.
O17.F13	Rozwiązanie musi umożliwiać integrację ze storage obiektowym (protokołem REST API lub S3) w celu przesyłania wybranych danych do archiwum

7.5. Usługa chmury obliczeniowej

Tytuł	Numer obszaru
Zakres prac	O31
Lokalizacje	O32
Bezpieczeństwo Fizyczne	O32.1
Ochrona prywatności i bezpieczeństwa	O32.2
Klasa Centrów Danych	O32.3
Zasilanie energią elektryczną	O32.4
Systemy bezpieczeństwa	O33
Zabezpieczenia przeciwpożarowe	O33.1
Obsługa	O33.2
Wymagania uniwersalne RODO dla Systemów przechowujących Dane Osobowe	O34
Wymagania związane z zabezpieczeniem danych zawierających Dane Osobowe	O34.1

W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do świadczenia usługi Chmury obliczeniowej zapewniającej wdrożenie i funkcjonowanie systemu OSS zgodnie z wymaganiami określonymi w niniejszym dokumencie oraz we Wzorze umowy. Wykonawca jest zobowiązany do konfiguracji przedmiotowej usługi na urządzeniach, których parametry nie mogą powodować potencjalnego ryzyka naruszenia bezpieczeństwa publicznego lub bezpieczeństwa państwa. Okres świadczenia usługi Chmury obliczeniowej w zakresie zamówienia podstawowego oraz prawa opcji został wskazany w Umowie. W ramach świadczenia usługi Chmury obliczeniowej i wynagrodzenia Wykonawcy z tytułu realizacji przedmiotu zamówienia muszą zostać spełnione poniższe wymagania obligatoryjne:

Zakres Prac

Nr wymagania	Treść wymagania
O31.F1	Wykonawca jest zobowiązany do zapewnienia wymaganej zasobów infrastruktury IT w formie usługi Platform as a Service w celu zapewnienia wdrożenie, obsługi i funkcjonowania Systemu OSS.
O31.F2	Wymagany zakres wdrożenia Rozwiązania OSS to środowisko przedprodukcyjne (rozdział 8.1.1) , środowisko produkcyjne, środowisko backup. Wykonawca jest zobowiązany do skonfigurowania usługi chmury obliczeniowej w sposób uwzględniający logiczny podział na co najmniej wyżej wyszczególnione środowiska.
O31.F3	Wszystkie wymagane środowiska muszą zostać wdrożone na wirtualnej prywatnej bądź publicznej chmurze w Centrach Danych należących do państw w ramach EOG.
O31.F4	Wykonawca jest odpowiedzialny za zapewnienie wymaganej infrastruktury obliczeniowej (serwery / maszyny wirtualne), pamięci masowej do hostowania systemu OSS.
O31.F5	Wykonawca jest odpowiedzialny za zapewnienie wymaganej sieci wewnętrznej, transferu danych do internetu i do sieci OSE, połączenie pomiędzy środowiskiem PaaS, a siecią OSE.
O31.F6	Wykonawca jest odpowiedzialny za zapewnienie wymaganej platformy wirtualizacyjnej wraz z jej modułami.
O31.F7	Wykonawca jest odpowiedzialny za zapewnienie przestrzeni do celów backup-u w ramach bezpiecznej i niezawodnej macierzy RAID, fizycznie oddzielonej od serwerów realizujących PaaS.
O31.F8	Wykonawca jest odpowiedzialny za zapewnienie łącza o parametrach gwarantujących korzystanie z usługi Chmury obliczeniowej zgodnie z wymaganiami Zamawiającego. Zakończenie łącza w Centrum LIM al. Jerozolimskie 65/67, 00-697 Warszawa Piętro +3 MMR: MEET.ODF Row 0 Rack 5 ODF NASK3 (30505) numery pól krosowych zostaną ustalone w trybie roboczym. - styk fizyczny 10GBase-LR. - jumbo frames (payload nie mniej niż 9000B). - łącze z tagowaniem VLANów zgodnie z 802.1q - preferowana numeracja VLAN z zakresu 1000 - 1999 -adresy używane przez serwery w usłudze muszą korzystać ze wskazanych przez NASK adresów z puli 10.0.0.0/8

Nr wymagania	Treść wymagania
O31.F9	Wykonawca jest odpowiedzialny za zapewnienie oprogramowania do kontroli zagrożeń, włączając w to oprogramowanie Anti-Spam/Malware/Antivirus.
O31.F10	Wykonawca jest odpowiedzialny za zarządzanie infrastrukturą wirtualną, nadzór nad ciągłością działania, aktualizacje systemu, monitorowanie ruchu i poziomu wykorzystanych zasobów, rozwiązywania zgłaszanych problemów/incydentów.
O31.F11	Wykonawca jest odpowiedzialny za przeprowadzania m.in.: instalacji i konfiguracji serwerów, optymalizacji i monitoringu poszczególnych parametrów maszyny/usługi, wykonywanie aktualizacji, backupu wraz z jego odtwarzaniem oraz do obsługi zgłoszonych problemów/incydentów.
O31.F12	Wykonawca jest odpowiedzialny za zapewnienie odpowiedniej przepustowości i łączności w DC (Data Center), w tym urządzeń końcowych, dla użytkowników końcowych w celu uzyskania dostępu do Systemu OSS.
O31.F13	Zamawiający otrzyma pełny wgląd do wykonywanych kopii bezpośrednio z poziomu konsoli operatora i codzienne raporty z przeprowadzonych backupów i testów odtwarzania backupów.
O31.F14	Zamawiający otrzyma możliwość wykonywania kopii zapasowej dla plików i folderów z konsoli dostarczonej przez Wykonawcę.
O31.F15	Wykonawca jest odpowiedzialny za zapewnienie, że wszystkie dane są szyfrowane w źródle (przed opuszczeniem firmowej sieci) oraz podczas ich transferu i przechowywania. Musi się to odbywać bez negatywnego wpływu na współczynnik redukcji danych.
O31.F16	Wykonawca jest odpowiedzialny za zapewnienie Zamawiającemu odpowiednich licencji w celu korzystania przez Zamawiającego z usługi Chmury obliczeniowej zgodnie z wymaganiami wskazanymi w SOPZ. (włączając w to wszelkie licencje niezbędne do zapewnienia usługi PaaS z backupem oraz do wdrożenia Systemu OSS).
O31.F17	Wykonawca jest odpowiedzialny za zapewnienie Zamawiającemu odpowiednich licencji dla systemów OSS na docelowej infrastrukturze obliczeniowej Zamawiającego, jak i licencji koniecznych do przeprowadzenia Migracji tych systemów na docelową infrastrukturę obliczeniową Zamawiającego.
O31.F18	W ramach usługi chmury obliczeniowej Wykonawca jest odpowiedzialny za zapewnienie ochrony przed atakami DDoS warstwy L4/L7
O31.F19	Wykonawca jest odpowiedzialny za zapewnienie wymaganej infrastruktury sieciowej (w tym przełączników, routerów i zapór ogniowych), aby zapewnić dostępność serwerów zgodnie z wymaganym poziomem SLA.
O31.F20	Wykonawca jest odpowiedzialny za przejęcie pełnej odpowiedzialności administracyjnej nad systemem operacyjnymi oraz bazami danych. Obejmuje to również zaprojektowanie, wdrożenie, utrzymanie ciągłości działania systemu i wsparcie w jego rozwoju.
O31.F21	Wykonawca jest odpowiedzialny za zapewnienie odpowiednio wydajnego środowiska wymaganego do optymalnej pracy systemu OSS, zgodnie z wymaganiami Zamawiającego.
O31.F22	Usługa Chmury obliczeniowej musi być zgodna z międzynarodowymi standardami i wytycznymi dotyczącymi bezpieczeństwa, takimi jak ISO 27001, w celu utrzymania działania infrastruktury obliczeniowej i zapewnienia prywatności danych.

Nr wymagania	Treść wymagania
O31.F23	Procedura zarządzania zmianami i zarządzania konfiguracją jest zdefiniowana i zaimplementowana w celu przetwarzania wszelkich zmian w środowisku / usługach w chmurze. Ta procedura musi obejmować możliwość obsługi przejścia między wyżej wymienionymi środowiskami przed wdrożeniem produkcji. Wykonawca jest zobowiązany uzyskać zgodę Zamawiającego na wszelkie prace i działania Wykonawcy, w tym prace planowe, mające wpływ na świadczoną usługę. Jakiekolwiek działania Wykonawcy w tym zakresie nie mogą mieć wpływu na bezprzerwowe korzystanie przez Zamawiającego z usługi lub pogorszenie jej parametrów.
O31.F24	Wykonawca jest odpowiedzialny za zarządzanie instancjami pamięci masowej, instancjami obliczeniowymi i środowiskami sieciowymi. Wykonawca jest również odpowiedzialny za zarządzanie określonymi kontrolami dotyczącymi współdzielonych punktów styku w granicach autoryzacji bezpieczeństwa, takich jak ustanawianie niestandardowych rozwiązań kontroli bezpieczeństwa. Przykłady obejmują między innymi zarządzanie konfiguracją i poprawkami, skanowanie luk, odzyskiwanie danych po awarii i ochronę danych podczas transportu i odpoczynku, zarządzanie zaporą hosta, zarządzanie poświadczeniami, zarządzanie tożsamością i dostępem oraz zarządzanie konfiguracjami sieci.
O31.F25	Wykonawca jest zobowiązany do zapewnienia wsparcia zespołowi technicznemu Zamawiającego w optymalizacji zasobów w środowisku chmurowym jak również w celu uzyskania lepszej wydajności, a także zapewnienie fizycznego lub wirtualnego dostępu dla personelu Zamawiającego w celu rozwiązania wszelkich problemów związanych z działaniem, utrzymaniem lub naprawą, w celu utrzymania bezproblemowego działania Systemu OSS.
O31.F26	Wykonawca musi zapewnić wymagany poziom SLA (Service Level Agreement) dla usługi, określony w Załączniku nr 8 do Umowy - "Zakres Usług Gwarancji" ; punkt 5.6. "Utrzymanie Dostępności systemu".
O31.F27	Wykonawca musi zapewnić szkolenia wyznaczonym pracownikom Zamawiającego w zakresie korzystania z konsoli i wszelkich innych aspektów technicznych do monitorowania środowiska.

Lokalizacje

Nr wymagania	Treść wymagania
O32.F1	Centra Danych muszą być zlokalizowane na terenie EOG (Europejski Obszar Gospodarczy).

Bezpieczeństwo fizyczne

Nr wymagania	Treść wymagania
O32.1.F1	Centrum Danych musi podlegać kontroli nad ruchem osobowo-materiałowym, poprzez ochronę fizyczną w trybie całodobowym 24/7. Ochrona fizyczna musi być świadczona przez kwalifikowanych pracowników ochrony.
O32.1.F2	W Centrum Danych muszą być stosowane procedury kontroli dostępu.
O32.1.F3	Centrum Danych musi być objęte monitoringiem środowiskowym rejestrującym wszystkie zdarzenia mające wpływ na jego funkcjonowanie. W szczególności monitoringowi muszą podlegać kluczowe

Nr wymagania	Treść wymagania
	elementy systemów zasilania, klimatyzacji i p-poż, w zakresie temperatury i wilgotności w wybranych punktach.
O32.1.F4	Szafa rack lub ciąg szaf rack (tzw. kiosk) musi być wyposażona w system kontroli dostępu (SKD) i musi być pod nadzorem kamer systemu telewizji dozorowej (CCTV).
O32.1.F5	Drzwi przednie i tylne do szafy lub ciągu szaf (kiosku) muszą być zabezpieczone, a jeżeli jest też możliwy dostęp z boku, to drzwi boczne muszą być zamknięte na stałe lub z ewentualną możliwością otwarcia jedynie od środka szafy i zabezpieczone czujnikami otwarcia.
O32.1.F6	Wszystkie instalacje technologiczne pracujące na rzecz Zamawiającego muszą umożliwiać bezprzerwowe serwisowanie.
O32.1.F7	Wykonawca musi zapewnić redundantne połączenie do Centrum Danych.
O32.1.F8	Wykonawca musi skonfigurować usługi na światowej klasy systemach i urządzeniach, nie zagrażających bezpieczeństwu państwa.
O32.1.F9	Wykonawca musi zapewnić system fizycznego i/lub logicznego odizolowania usług poszczególnych klientów.
O32.1.F10	Wykonawca musi zapewnić ścisłe procedury uwierzytelniania użytkowników i administratorów.
O32.1.F11	Wykonawca musi zapewnić procedury i środki umożliwiające monitorowanie wszystkich operacji przeprowadzanych w systemie informacyjnym oraz raportowanie, zgodnie z obowiązującymi przepisami, w przypadku wystąpienia incydentów dotyczących danych klienta.
O32.1.F12	Wykonawca musi zapewnić, że konfiguracja zasobów współdzielonych uniemożliwia wzajemny dostęp do danych na nich ulokowanych poprzez różne podmioty.

Ochrona prywatności i bezpieczeństwa

Nr wymagania	Treść wymagania
O32.2.F1	Wykonawca musi niezwłocznie powiadomić Zamawiającego o każdym przypadku naruszenia zasad bezpieczeństwa, wtargnięcia lub prośby agencji rządowych o dostęp do danych, aby umożliwić Zamawiającemu zarządzanie tymi wydarzeniami proaktywnie.
O32.2.F2	Wykonawca musi zapewnić, że w przypadku zwolnienia zasobów wszystkie bloki pamięci i wszelkie kopie danych, jeśli takie istnieją, zostaną tak usunięte bądź wyzerowane przez Wykonawcę, aby dane nie mogły zostać odzyskane.
O32.2.F3	Wykonawca nie może przetwarzać ani przechowywać danych Zamawiającego poza EOG. Ponadto w żadnych okolicznościach nie będzie przetwarzać ani przechowywać danych w Stanach Zjednoczonych.
O32.2.F4	Wykonawca jest zobowiązany do przetwarzania danych osobowych klienta wyłącznie do celów związanych z właściwą realizacją usług i wyłącznie zgodnie z jego instrukcjami.
O32.2.F5	Dane przechowywane na infrastrukturze Wykonawcy pozostają własnością Zamawiającego.

Nr wymagania	Treść wymagania
O32.2.F6	Wykonawca nie może odsprzedawać danych Zamawiającego ani wykorzystywać ich do celów marketingowych.
O32.2.F7	Wykonawca musi posiadać system zarządzania uprawnieniami ograniczający dostęp do pomieszczeń oraz danych tylko do osób, które muszą go mieć ze względu na pełnione funkcje i zakres obowiązków.

Klasa Centrów Danych

Nr wymagania	Treść wymagania
O32.3.F1	Usługa Chmury obliczeniowej jest świadczona z wykorzystaniem Centrów Danych bazujących na standardach Tier 3 potwierdzonych certyfikatem niezależnej instytucji certyfikującej. Wszystkie istotne aktywne elementy infrastruktury technicznej Centrum Danych zapewniają pracę z poziomem redundancji zgodnie z Tier-3.
O32.3.F2	Wykonawca musi przekazać Zamawiającemu pełne informacje o wszystkich fizycznych lokalizacjach serwerów, na których przetwarzane są lub mogą być przetwarzane dane. Informacja o zmianie lokalizacji serwerów musi być przekazywana Zamawiającemu z rozsądnym wyprzedzeniem, tak by Zamawiający mógł rozważyć ewentualne problemy wynikające z takiej migracji. Wymaganie to dotyczy tym samym nie tylko przekazywania zasobów do państw należących do EOG, a nawet do konkretnych centrów przetwarzania danych.
O32.3.F3	Wykonawca musi zapewnić, że zasoby będą zawsze przechowywane i przetwarzane w Centrach Danych należących do państw w ramach EOG.
O32.3.F4	Wykonawca musi umożliwić Zamawiającemu pełny dostęp do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych przyjmowanych w poszczególnych Centrach Danych.
O32.3.F5	Wykonawca musi określić wspólnie z Zamawiającym zasady przeszukiwania, retencji i usuwania danych dostarczonych przez Zamawiającego.
O32.3.F6	Wykonawca musi raportować wszystkie incydenty bezpieczeństwa danych, ze szczególnym uwzględnieniem tych, które dotyczyć mogą danych osobowych przetwarzanych przez Zamawiającego w chmurze oraz udzielić Zamawiającemu wszelkiej możliwej pomocy przy zwalczaniu skutków takich incydentów bezpieczeństwa.
O32.3.F7	Oferowana usługa musi zapewniać łatwą interoperacyjność i przenaszalność danych pomiędzy różnymi Centrami Danych i dostawcami usług chmurowych.

Zasilanie energią elektryczną

Nr wymagania	Treść wymagania
O32.4.F1	Centrum Danych musi mieć zapewnione zasilanie z dwóch niezależnych źródeł zasilania z dwóch niezależnych stacji energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz agregatów prądotwórczych.

Nr wymagania	Treść wymagania
O32.4.F2	Zasilanie sprzętu wykorzystywanego do świadczenia usługi Chmury obliczeniowej musi być realizowane dwiema niezależnymi, fizycznie oddzielnymi trasami. Zasilanie gwarantowane do każdej szafy rack jest doprowadzone z dwóch niezależnych torów zasilania podtrzymywanych przez zasilacze bezprzerwowe UPS oraz generatory prądotwórcze w każdym z torów.

Systemy bezpieczeństwa

Nr wymagania	Treść wymagania
O33.F1	Każde z pomieszczeń Centrum Danych musi być wyposażone w system kontroli dostępu (SKD).
O33.F2	Dla każdego z przejść wymagających identyfikacji należy zapewnić obraz z kamery.
O33.F3	CCTV - system telewizji przemysłowej będzie zapewniać: o ciągłość nagrań oraz ich archiwizacja na min 60 dni, o kamery IP kolorowe dualne (dzień/noc). o kamery muszą monitorować całość obszaru z uwzględnieniem: każdego ciągu szaf lub każdą szafę wolnostojącą z czterech stron, każdego wejścia z dwóch stron, rozdzielni elektrycznych, stacji trafo, generatora na zewnątrz oraz wewnątrz, magazynu paliw, oraz pomieszczenia UPS-ów, ciągów komunikacyjnych, monitorowania dachu, podejść i wejść do budynku oraz terenu dookoła niego

Zabezpieczenia przeciw pożarowe

Nr wymagania	Treść wymagania
O33.1.F1	Powierzchnia techniczna Centrum Danych musi spełniać wymaganie odporności ogniowej systemu na poziomie EI120 - podłoga techniczna EI60
O33.1.F2	Centrum Danych musi być wyposażone w system oddymiania.
O33.1.F3	Centrum Danych musi być wyposażone w instalację hydrantową i tryskaczową
O33.1.F4	Centrum Danych musi być wyposażone w system gaszenia gazem (bezpieczny dla ludzi).

Obsługa

Nr wymagania	Treść wymagania
O33.2.F1	Wykonawca musi przyjmować zgłoszenia w trybie 24 * 7 * 365, mailowo i telefonicznie

Wymagania uniwersalne RODO dla Systemów przechowujących Dane Osobowe

Nr wymagania	Treść wymagania
O34.F1	System musi umożliwiać ustalenie dawcy każdej danej osobowej.
O34.F2	System musi umożliwiać ustalenie daty pozyskania przez Administratora każdej danej osobowej przetwarzanej w systemie.
O34.F3	System musi umożliwiać ustalenie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu.
O34.F4	System musi umożliwiać ustalenie dla każdej pojedynczej danej osobowej okresu przetwarzania tej danej osobowej i celu przetwarzania tej danej osobowej. Jeden wspólny cel może być przypisywany do grupy kategorii – zakresu danych).
O34.F5	Wprowadzenie zmiany dowolnej danej osobowej w systemie musi prowadzić do aktualizacji tych samych danych osobowych w innych systemach przetwarzających te same dane.
O34.F6	System musi umożliwiać umożliwiać ustalenie maksymalnego okresu przetwarzania tej danej osobowej do każdej pojedynczej danej osobowej.
O34.F7	W przypadku zmiany danych osobowych w Systemie, system musi odnotowywać i umożliwiać wygenerowanie informacji, kto dokonał zmian danych osobowych, z pierwszym wpisem włącznie. W przypadku zmian dokonywanych przez użytkowników musi istnieć możliwość ustalenia, który użytkownik dokonał zmiany.
O34.F8	W przypadku zmiany danych osobowych w Systemie, system musi odnotowywać i umożliwiać wygenerowanie informacji, który użytkownik dokonał zmian danych osobowych (z pierwszym wpisem włącznie)
O34.F9	W przypadku zmiany danych osobowych w Systemie, system musi odnotowywać i umożliwiać wygenerowanie informacji: dokładną datę i godzinę modyfikacji;
O34.F10	W przypadku zmiany danych osobowych w Systemie, system musi odnotowywać i umożliwiać wygenerowanie informacji: co zostało zmienione (zakres zmiany)
O34.F11	W przypadku zmiany danych osobowych w Systemie, system musi odnotowywać i umożliwiać wygenerowanie informacji: informację historyczną – poprzednie wartości, które podlegały zmianie.
O34.F12	W przypadku zmiany danych osobowych w Systemie, system musi odnotowywać i umożliwiać wygenerowanie informacji: źródło informacji o zmianie danych.
O34.F13	System musi umożliwiać aktualizację dowolnej informacji o osobie fizycznej.
O34.F14	System musi zapewniać możliwość wygenerowania raportu nt. zakresu przetwarzanych danych osobowych. Raportowanie musi umożliwiać filtrowanie danych według określonych przez użytkownika kryteriów. Użytkownik musi mieć możliwość ustawienia wielu różnych kryteriów.
O34.F15	System musi zapewniać możliwość wygenerowania raportu nt. procesów operacyjnych, w których przetwarzane są dane osobowe. Raportowanie musi umożliwiać filtrowanie danych według określonych przez użytkownika kryteriów. Użytkownik musi mieć możliwość ustawienia wiele różnych kryteriów.

Nr wymagania	Treść wymagania
O34.F16	System musi zapewniać możliwość wygenerowania raportu nt. źródeł danych osobowych. Raportowanie musi umożliwiać filtrowanie danych według określonych przez użytkownika kryteriów. Użytkownik musi mieć możliwość ustawienia wiele różnych kryteriów.
O34.F17	System musi umożliwiać eksport oraz generowanie raportu wszystkich danych z systemu dot. konkretnej osoby, w tym także danych historycznych i danych po ich sprostowaniu, zmianie, etc. W przypadku sprostowania danych należy zaprezentować dane sprzed i po zmianie, datę zmiany, powód oraz osobę dokonującą zmiany. Format wystawienia danych ma być czytelny dla użytkownika. musi zawierać konkretne dane i wartości.
O34.F18	Wymagane jest dostarczenie funkcjonalności wyszukiwania informacji o osobie fizycznej wg kryteriów: dane identyfikacyjne (imię i nazwisko), dane kontaktowe, dane adresowe. Dodatkowo wyszukiwanie powinno być ograniczone datami, w zależności od zapytania i typu danych.
O34.F19	System musi umożliwiać wyszukiwanie informacji dotyczących konkretnej osoby (wg zdefiniowanych przez użytkownika kryteriów oraz filtrów). System musi umożliwić użytkownikowi zdefiniować więcej niż jedno kryterium i móc zastosować więcej niż jeden filtr. W szczególności wyszukiwanie musi wyszukiwać następujące dane: Imię i Nazwisko; Adres eMail; Wynikiem musi być informacja zawierająca zestawienie czy w systemie są przetwarzane wyszukiwanie dane.
O34.F20	Wymagane jest dostarczenie funkcjonalności umożliwiającej aktualizację danych osoby fizycznej w systemie.
O34.F21	System musi umożliwiać ograniczenie możliwości dostępu do danych przez różne kategorie użytkowników. Wyjątkiem jest grupa użytkowników posiadających odpowiednie uprawnienia.
O34.F22	Dane osobowe, dla których istnieje aktywne ograniczenie przetwarzania, nie mogą być wykorzystywane w procesach operacyjnych, chyba, że istnieje alternatywna podstawa do przetwarzania danych. Po ustaniu ograniczenie przetwarzania, wykorzystywanie w procesach operacyjnych może być wznowione.
O34.F23	System musi umożliwiać usuwanie danych osobowych klienta albo ich anonimizację poprzez: • Usuwanie danych po określonym czasie; • Usuwanie danych po wniesieniu żądania ich usunięcia przez osobę, której dane dotyczą; • Odpowiednie oznaczanie danych upublicznionych plus zapamiętanie informacji o sposobie upublicznienia. System musi umożliwiać wprowadzenia reguł i wyjątków, co do mechanizmu usuwania danych (np. dalsze przechowywanie dla celów statystycznych). Jeśli dane są przechowywane w wielu miejscach, usuwanie danych powinno dotyczyć wszystkich kopii danych osobowych.
O34.F24	System musi umożliwiać usuwanie danych poprzez: • Usunięcie całego rekordu z bazy, (jeśli jest to możliwe); • Nadpisanie (anonimizacja) danych (w takim przypadku również dane w historii zmian powinny być nadpisane). Jeżeli wprowadza się nadpisanie danych, to również dane w historii zmian powinny być nadpisane.
O34.F25	System musi umożliwić automatyczne masowe usuwanie danych osobowych po okresie ich retencji.

Nr wymagania	Treść wymagania
O34.F26	System musi umożliwić na żądanie usunięcie wszystkich lub określonych danych osobowych pojedynczego klienta.
O34.F27	System musi usuwać dane osobowe po ustaniu powodu ich przetwarzania. Dotyczy to np. sytuacji wycofania zgody na przetwarzanie, jeśli nie ma innych podstaw do przetwarzania.

Wymagania związane z zabezpieczeniem danych zawierających Dane Osobowe

Nr wymagania	Treść wymagania
O34.1.F1	Podczas przywracania systemu z kopii zapasowej nie mogą zostać odtworzone dane osobowe, które zostały z systemu usunięte na podstawie wniosków o usunięcie danych.
O34.1.F2	W systemie, który przetwarza dane spseudonimizowane, przetwarzane są jedynie identyfikatory pseudonimizacji, (co skutkuje tym, że użytkownik takiego systemu nie wie, czyje są to dane).
O34.1.F3	System musi umożliwiać trwałe usunięcie danych (prawo do bycia zapomnianym). Usunięcie musi polegać na rzeczywistym usunięciu danych lub nadpisaniu informacją pustą, a nie na zaznaczeniu danego rekordu, jako rekordu skasowanego, który staje się często jedynie niewidocznym z poziomu aplikacji/systemu, ale dalej istnieje w przetwarzanym zbiorze. Nie może być możliwe ponowne "odkrycie" usuniętych danych, przy użyciu odpowiednich programów narzędziowych i dalsze ich przetwarzanie.
O34.1.F4	System musi zabezpieczać przed możliwością zmiany/usunięcia danych osobowych w sposób nieautoryzowany (np. poprzez mechanizm zarządzania uprawnieniami użytkowników)
O34.1.F5	System musi umożliwiać zarządzanie uprawnieniami użytkowników w ten sposób, że dany użytkownik/kategoria posiada dostęp (możliwość wyświetlenia/edycji/wydruku/etc.) dla konkretnych typów danych osobowych.
O34.1.F6	System musi posiadać możliwość zarządzania użytkownikami systemu, w tym: • Istnieje możliwość zarządzania grupami uprawnień oraz pojedynczymi uprawnieniami dla każdego użytkownika (każdy użytkownik może należeć do więcej niż jednej grupy); • Pomimo globalnych ustawień dla grupy użytkownika, admin może modyfikować uprawnienia dla pojedynczego użytkownika (na zasadzie białych i czarnych list); • Daje możliwość blokowania konta użytkownika w każdym momencie z odnotowanie dokładnej daty i godziny zablokowania; • Uniemożliwia przypisanie jednego loginu do więcej niż jednej osoby.
O34.1.F7	System musi nadawać każdemu użytkownikowi odrębny identyfikator i hasło, które jest znane tylko temu użytkownikowi.
O34.1.F8	System musi zabezpieczać dostęp do danych (np. poprzez VPN, SFTP, zdalny pulpit) wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
O34.1.F9	System musi zapewnić autoryzację (np. autoryzacja domenowa), żeby dany identyfikator wykorzystywała tylko osoba, której został on przyznany.
O34.1.F10	W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, system musi określać częstotliwość i zasady zmiany hasła. System musi umożliwiać dowolną konfigurację wymuszającą na

Nr wymagania	Treść wymagania
	użytkownikach odpowiedni poziom trudności hasła. Hasła przechowywane w systemie muszą być szyfrowane.
O34.1.F11	System musi dawać możliwość wykonywania kopii zapasowych.
O34.1.F12	System musi umożliwiać kontrolę poprawności wykonywanych kopii danych i systemu.
O34.1.F13	System musi odnotowywać, kto i kiedy wykonywał kopię danych, oraz wszelki dostęp do danych (w tym fakt generowania raportów, kto, kiedy i jaki raport drukował).
O34.1.F14	System musi zapewniać środki ochrony kopii zapasowych (poprzez kontrolę dostępu, szyfrowanie itd.) nie mniejsze niż zabezpieczenia stosowane systemie produkcyjnym.
O34.1.F15	System musi zapewniać integralność danych w kopii zapasowej. System musi zapewniać regularne testowanie odzyskiwania danych.
O34.1.F16	System musi posiadać fizyczne lub logiczne zabezpieczenia chroniące przed nieuprawnionym dostępem. W przypadku zastosowania logicznych zabezpieczeń system musi zapewniać: • Kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną; • Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych; • możliwość wykrycia nieautoryzowanego dostępu lub złośliwych ataków w systemie.
O34.1.F17	System musi umożliwiać szyfrowanie danych w nim przetwarzanych (przede wszystkim dane osobowe wrażliwe, logi systemowe, informacje alarmowe, kody, pliki cookies) oraz szyfrować transmisję tych danych wychodzących z systemu.
O34.1.F18	System musi umożliwiać maskowanie, zamglenie/zaciemnienie danych lub ich niewyświetlanie w celu ochrony informacji wrażliwych, nieobjętych zakresem upoważnienia lub zbędnych dla celów danego przetwarzania.
O34.1.F19	System musi umożliwiać tworzenie reguł, wg których poszczególne dane są maskowane/zaciemnione.
O34.1.F20	System musi posiadać mechanizm maskowania danych, który musi być stosowany zawsze, gdy dane są przetwarzane w środowiska testowych lub niepełnych wersjach systemowych.
O34.1.F21	System musi umożliwiać, aby podczas odtwarzania systemu z kopii zapasowej zapewnić: - przywrócenie zmian danych wprowadzonych w okresie od wykonania kopii zapasowej do dnia jej odtworzenia - przywrócenie usunięcia danych

7.6. Wymagania wdrożeniowe

7.6.1. Zakres prac dla Fazy 1

Faza 1 obejmuje

- zapewnienie zasobów infrastrukturalnych wraz z łączem do węzła OSE - w formie usługi i świadczenia tej usługi na poziomie zgodnym z założonym SLA

- wdrożenie systemów OSS w bardzo podstawowym zakresie umożliwiającym monitorowanie podstawowych parametrów docelowej sieci szkieletowej OSE (parametry standardowo wbudowane w narzędzie)
- uruchomienie inventory urządzeń docelowej sieci szkieletowej OSE (w wyniku discovery)
- uruchomienie systemu provisioningu jako narzędzia umożliwiającego budowanie scenariuszy provisioningowych (do wykorzystania w razie potrzeby przez szkolone osoby)

Cel realizacji fazy: Zapewnienie monitorowania docelowej sieci szkieletowej OSE oraz narzędzi do provisioningu

Zakres wymagań stawianych Wykonawcy oraz wymaganej funkcjonalności która musi być wdrożony w Fazie 1 jest przedstawiony w tabeli poniżej:

Nr Wymagania	Treść Wymagania
O51.F1	Wykonawca zobowiązuje się do wykonania tej fazy zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy
O51.F2	Wykonawca zobowiązany jest zapewnić zwirtualizowaną infrastrukturę produkcyjną i testową na potrzeby systemów OSS w wersji usługi chmurowej. Infrastruktura musi zapewnić wystarczającą wydajność dla ww. systemów.
O51.F3	Usługa chmurowa infrastruktury zwirtualizowanej dla systemów OSS musi spełniać wymagania przedstawione w dokumencie SOPZ w rozdziale "Wymagania dla usługi chmury obliczeniowej pod OSS"
O51.F4	Wykonawca musi uruchomić wszystkie systemy w ramach OSS w zakresie standardowych funkcjonalności wbudowanych w te systemy, w szczególności: - w zakresie Inventory jest to zbudowanie ewidencji tylko urządzeń szkieletowych OSE - w zakresie Provisioningu jest to uruchomienie narzędzia, które może zostać wykorzystane do przeprowadzenia scenariuszu provisionigu przez odpowiednio przeszkolone osoby
O51.F5	Wykonawca musi przeprowadzić niezbędne prace konfiguracyjne i integracyjne związane z monitorowaniem z poziomu systemu OSS urządzeń szkieletowych zainstalowanych we wszystkich węzłach OSE Wymagany podstawowy poziom monitoringu zakłada wykorzystanie monitorowania parametrów standardowo wbudowanych w narzędzia systemu

7.6.2. Zakres prac dla Fazy 2

Faza 2 obejmuje:

- wdrożenie pełnej funkcjonalności Systemów OSS, integrację ich z systemami OSE NASK,
- wdrożenie SSO, LDAP
- integrację systemów OSE OSS z systemami NASK i OSE NASK (w tym z Insight)

- integrację systemów OSE OSS z s systemem raportowym NASK
- migrację szkół, które zostały wcześniej podłączone do sieci docelowej OSE i były obsługiwane przez systemy OSE NASK
- migrację danych inventory dla wcześniej podłączonych szkół i danych OSS sieci OSE z tymczasowych systemów Zamawiającego (w tym zasoby i adresacja sieci)

Cel realizacji fazy: Zapewnienie odpowiednio wydajnego środowiska realizującego wszystkie funkcjonalności związane z zarządzaniem urządzeniami i usługami ściśle zintegrowanego z docelową siecią OSE i w pełni zautomatyzowanego.

Zakres wymagań stawianych Wykonawcy oraz wymaganej funkcjonalności która musi być wdrożony w Fazie 2 jest przedstawiony w tabeli poniżej:

Nr Wymagania	Treść Wymagania
O52.F1	Wykonawca zobowiązuje się do wykonania tej fazy zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy
O52.F2	Wymagana jest od Wykonawcy realizacja Systemów OSS w pełnej funkcjonalności (w tym Fault & Perforamce Management, Config Management & Provisioning, Inventory), które będą zintegrowane z systemami OSE NASK i NASK w taki sposób by zapewnić spełnienie wszystkich wymagań zdefiniowanych dla obszaru OSS.
O52.F3	Wykonawca stworzy inventory dla systemów OSE OSS jako roszerzoną replikę (w modelu master-slave) w stosunku do inventory w systemach OSE NASK, którym jest Insight. Masterem danych musi być Insight. W ramach rozwiązania należy zapewnić odpowiednie mechanizmy / funkcjonalności do replikacji i modyfikacji danych aby zapewnić ich spójność i poprawność. Inventory OSE OSS może zawierać znacznie większy zestaw danych (zgodnie z potrzebami systemów OSE OSS). Inventory OSE OSS jest masterem wszelkich danych nie znajdujących się Insight.
O52.F4	Komponent zapewniający funkcjonalność Inventory implementowany w ramach wdrożenia Systemów OSS musi zapewniać integrację z systemami BSS Zamawiającego zawierającymi dane inwentaryzacyjne (w tym co najmniej z Insight)
O52.F5	Komponent zapewniający funkcjonalność Inventory implementowany w ramach wdrożenia Systemów OSS musi mieć przygotowany interface API do wystawiania danych systemom trzecim, co najmniej : - dla centralnego systemu raportowego NASK PIB - dla raportów w postaci excel'a z funkcją VBA oraz potencjalnie dla portalu OSE. Musi zostać dokonane stosowne dopasowanie sposobu wystawiania danych (formatów danych, słowników itp.) tak by był on zgodny z procesem raportowania OSE
O52.F6	W komponencie zapewniającym funkcjonalność Inventory w ramach wdrożenia Systemów OSS muszą istnieć analogiczni użytkownicy i grupy użytkowników jak w systemie Insight OSE NASK, z tym

Nr Wymagania	Treść Wymagania
	że autoryzacja i uwierzytelnianie użytkowników w docelowym systemie OSS musi zachodzić w oparciu o zaimplementowany w Rozwiązaniu mechanizm SSO (SIngle Sign On).
O52.F7	Wykonawca zobowiązany jest za przygotowanie i zapewnienie planu awaryjnego, dla sytuacji niepoprawnego działania środowiska po migracji danych. W ramach procedury rollback należy przywrócić dane klientów zmigrowanych do stanu sprzed rozpoczęcia migracji bez jakiegokolwiek wpływu na dane klientów niemigrowanych. Procedura rollback może zostać zastosowana do 12h po zakończeniu migracji i włączeniu systemów (jeżeli były wyłączane)
O52.F8	W ramach usługi chmurowej Wykonawca musi uruchomić środowisko testowe dla systemów z obszaru OSS
O52.F9	Testowe środowisko systemów z obszaru OSS musi zostać uruchomione i zintegrowane z testowym środowiskiem systemów OSE NASK
O52.F10	W ramach wdrożenia w Fazie 2 Wykonawca musi przeprowadzić wszystkie niezbędne integracje obszaru OSS z systemami zewnętrznymi opisanymi w SOPZ w wymaganiach dotyczących integracji
O52.F11	Wykonawca musi uruchomić funkcjonalność SSO w zakresie systemów OSS
O52.F12	Wykonawca musi przeprowadzić niezbędne prace konfiguracyjne i integracyjne związane z zarządzaniem z poziomu systemu OSS urządzeniami i systemami OSE zainstalowanymi w każdym z Węzłów Regionalnych z osobna
O52.F23	Wykonawca musi przeprowadzić niezbędne prace konfiguracyjne i integracyjne związane z provisioningiem usług na urządzeniach i systemach OSE zainstalowanych w każdym z Węzłów Regionalnych z osobna
O52.F14	Wykonawca jest zobowiązany do wdrożenia usługi katalogowej LDAP (dla partnerów OSE) i jej integracji z serwerem Radius (system Zamawiającego) oraz potencjalnie z innymi systemami bezpieczeństwa Zamawiającego (ustalonych na etapie dokumentów HLD/LLD) przy użyciu protokołu LDAP SSL/TLS
O52.F15	Wykonawca musi zmigrować dane z systemów OSE NASK niezbędne do obsługi w systemach OSS wszystkich szkół podłączonych do docelowej sieci szkieletowej (również w zakresie obsługi urządzeń w sieciach szkolnych)
O52.F16	Migracja danych musi być realizowana poza godzinami pracy szkół, w godzinach nocnych z oknem serwisowym nie dłuższym niż 8 godzin.
O52.F17	W wyniku migracji docelowe systemy OSS muszą automatycznie wykryć i zacząć monitorować urządzenia w szkole (zgodnie z założeniami zawartymi w rozdziale 7.4 SOPZ)
O52.F18	W wyniku migracji komponenty realizujące funkcjonalność Inventory muszą zostać odpowiednio uzupełnione danymi związanymi ze szkołą i jej urządzeniami
O52.F19	Migracja danych nie może w żaden sposób negatywnie wpłynąć na wydajność systemów. Po stronie Wykonawcy leży ewentualne zapewnienie odpowiedniej zasobów i wydajności infrastruktury chmurowej
O52.F20	Proces migracji nie może w żaden sposób wpływać na dane usług niemigrowanych

Nr Wymagania	Treść Wymagania
O52.F21	W zakresie migracji znajduje się przeniesienie danych związanych z obszarem OSS (adresacja sieci, ewidencja sieci, usług, monitorowanie usług i wydajności)
O52.F22	Wymagana jest pełna migracja danych dotyczących ruchu w sieci
O52.F23	Wymagana jest pełna migracja danych dotyczących historii zmian na usługach i urządzeniach w sieci
O52.F24	Wymagana jest pełna migracja danych dotyczących konfiguracji urządzeń (również historycznych)
O52.F25	Wykonawca zobowiązany jest za przygotowanie i zapewnienie planu awaryjnego, dla sytuacji niepoprawnego działania środowiska po migracji danych. W ramach procedury rollback należy przywrócić dane klientów zmigrowanych do stanu sprzed rozpoczęcia migracji bez jakiegokolwiek wpływu na dane klientów niemigrowanych. Procedura rollback może zostać zastosowana do 12h po zakończeniu migracji i włączeniu systemów (jeżeli były wyłączane)
O52.F26	Wymagane jest przechowanie historii wszelkich zmian realizowanych w ramach migracji wewnętrznych (w ramach systemu)
O52.F27	Migracja dotyczy zarówno przeniesienia danych pomiędzy systemami jak również aktualizacji danych wewnątrz systemów (bez przenoszenia danych) , czyli migracji wewnętrznej
O52.F28	W ramach migracji należy zasilić danymi systemu OSE OSS tak aby mogły obsługiwać szkoły przełączane z sieci przejściowej na docelową sieć szkieletową OSE. Prace muszą być realizowane w synchronizacji z przenoszeniem usług pomiędzy sieciami, które znajduje się w odpowiedzialności Zamawiającego.
O52.F29	Wykonawca przeprowadzi analizę powdrożeniową weryfikując kompletność wdrożenia rozwiązania (pokrycie realizacji wymagań) oraz jakość dostarczonego rozwiązania (wydajność i stabilność systemów oraz całego środowiska). Raport z analizy zostanie przekazany do Zamawiającego.
O52.F30	W ramach funkcjonalności provisioningu w Fazie 2 Wykonawca musi w terminie do 1 miesiąca od zakończenia Fazy 1 wdrożyć tzw. Aktywator Usług Sieciowych. Aktywator Usług Sieciowych dotyczy provisioningu konfiguracji usług tylko na urządzeniach sieciowych w szkielecie OSE i w lokalizacjach szkolnych (CPE), zatem w celu jego poprawnego działania Wykonawca musi wcześniej zaimplementować funkcjonalność inventory tych urządzeń w systemach OSS. Wprowadzanie parametrów do Aktywatora Usług Sieciowych może zostać zaimplementowane na jeden z dwóch sposobów: - z procesu biznesowego w systemie BSS Zamawiającego poprzez integrację OSS z BSS via API wystawione przez Aktywator Usług Sieciowych - poprzez wystawiony interface web'owy Aktywatora Usług Sieciowych (w przypadku gdy nie będzie jeszcze możliwa integracja z systemami BSS Zamawiającego)
O52.F31	W momencie odbioru Fazy 2 Wykonawca jest zobowiązany do wdrożenia pełnego provisioningu, czyli poszerzenia funkcjonalności Aktywatora Usług Sieciowych zgodnie z wymaganiami tego obszaru opisanymi w SOPZ

7.6.3. Zakres prac dla Fazy 3

Faza 3 obejmuje migrację systemów OSE OSS z infrastruktury zwirtualizowanej świadczonej w formie usługi chmurowej na docelową infrastrukturę zwirtualizowaną zapewnioną przez Zamawiającego

Cel realizacji fazy: zapewnienie środowiska OSS do obsługi OSE działającego na infrastrukturze obliczeniowej OSE

Zakres wymagań stawianych Wykonawcy oraz wymaganej funkcjonalności która musi być wdrożony w Fazie 3 jest przedstawiony w tabeli poniżej:

Nr Wymagania	Treść Wymagania
O53.F1	Wykonawca zobowiązuje się do wykonania tej fazy zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy
O53.F2	W wyniku migracji wydajność procesów OSS (również bazujących na integracjach z systemami sieci, bezpieczeństwa i BSS Zamawiającego) nie może się pogorszyć.
O53.F3	Systemy OSS muszą zostać zmigrowane z infrastruktury obliczeniowej w wersji usługi na infrastrukturę docelową Zamawiającego zgodną z architekturą podaną w dokumencie SOPZ, zatem muszą one być przemigrowane zachowując planowaną architekturę docelową typu active - active. Docelowo systemy OSS muszą zostać rozproszone w dwóch głównych ośrodkach przetwarzania danych i tak zaprojektowane aby w razie całkowitej awarii jednego z ośrodków zachować ciągłość działania.
O53.F4	Migracja systemów OSS z infrastruktury obliczeniowej w wersji usługi do docelowej infrastruktury Zamawiającego nie może zakłócić ciągłości działania systemów OSS (oznacza to również zapewnienie wszystkich danych w systemach) oraz nie może negatywnie wpłynąć na integracje z systemami sieci i bezpieczeństwa. Migracja musi być realizowana poza godzinami pracy szkół w godzinach nocnych w oknie serwisowym (ustalonym na etapie dokumentu LLD) . Zamawiający dopuszcza jednak że potencjalne nieprzewidziane problemy mogą zakłócić działanie systemów OSS najwyżej na okres 1 godziny.
O53.F5	Migracja systemów OSS z infrastruktury obliczeniowej w wersji usługi do docelowej infrastruktury Zamawiającego musi zostać wykonana z zapewnieniem zachowania bezpieczeństwa migrowanych danych. Wszystkie dane podczas migracji muszą być szyfrowane. W przypadku korzystania z serwerów pomostowych muszą być zlokalizowane w usłudze chmurowej świadczonej przez Wykonawcę lub w docelowej infrastrukturze Zamawiającego.
O53.F6	Plan migracji musi uwzględniać migrację backup-u danych do nowego systemu backup-u zlokalizowanego na docelowej infrastrukturze Zamawiającego.
O53.F7	Odpowiedzialność za zapewnienie ciągłości działania integracji systemów OSS z systemami NASK i NASK OSE (w szczególności z systemami sieci i bezpieczeństwa) leży po stronie Wykonawcy
O53.F8	Plan migracji musi zawierać scenariusz na wypadek nie udanej migracji i powrotu do stanu sprzed migracji

Nr Wymagania	Treść Wymagania
O53.F9	Po wykonaniu migracja Wykonawca musi dokonać stosownej analizy działania systemów OSS i w razie potrzeby dokonać optymalizacji zasobów wykorzystywanych przez te system