



ZARZĄD DRÓG MIASTA KRAKOWA

ul. Centralna 53, 31-586 Kraków, centrala tel. +48 12 61 67 000, fax: +48 12 61 67 417, email: sekretariat@zdmk.krakow.pl

Załącznik nr 7
do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Projekt:	Rozwój Systemu Informacji dla podróżujących na obszarze Krakowskiego Obszaru Funkcjonalnego
Zamówienie:	Most pośredniczący do wymiany danych w czasie rzeczywistym oraz hurtownia danych

Kraków, dn. 27.09.2019r.

SPIS TREŚCI

1	OGÓLNY OPIS PROJEKTU	4
1.1	Zakres Projektu.....	4
1.2	Terminy realizacji.....	4
1.3	Wymagania ogólne	4
1.4	Architektura systemu	5
2	ŹRÓDŁA DANYCH	6
2.1	Wymagania ogólne	6
2.2	Dane z Systemu Sterowania Ruchem.....	6
2.2.1	VTnet.....	6
2.2.2	Sitraffic Scala	6
2.3	Dane z systemu pomiarowego sieci drogowej	7
2.4	Dane z systemu pomiarowego sieci dróg rowerowych	7
2.5	Dane z systemów obsługi parkingów	7
2.6	Dane z systemów zarządzania komunikacją publiczną	7
2.7	Dane meteorologiczne	8
2.8	Dane z bazy danych o wypadkach.....	8
2.9	Dane z systemu ostrzegania o utrudnieniach w sieci drogowej	8
2.10	Dane z systemu ostrzegania o utrudnieniach w sieci komunikacji miejskiej.. Błąd! Nie zdefiniowano zakładki.	
2.11	Dane z kamer Systemu Sterowania Ruchem.....	9
3	PLATFORMA INTEGRACYJNA (WARSTWA ETL)	10
3.1	Wymagania ogólne	10
3.2	Filtracja danych	10
3.3	Agregacja danych	10
4	MAGAZYN DANYCH OPERACYJNYCH – WYMIANA DANYCH W CZASIE RZECZYWSITYM	11
4.1	Wymagania ogólne	11
4.2	Wymagania techniczne.....	11
4.3	Dane dostępne dla aplikacji zewnętrznych.....	12
4.4	Dane przekazywane do hurtowni	12
5	CENTRALNA HURTOWNIA DANYCH.....	14
5.1	Architektura	14
5.2	Wymagania techniczne.....	14



6	DOSTĘP DO DANYCH.....	15
6.1	Aplikacje analityczne i eksploracja danych.....	15
6.2	Interfejsy dostępu do bazy operacyjnej	15
6.3	Interfejsy dostępu do systemu analiz.....	16
6.4	Przykłady wykorzystania.....	16
7	SYSTEM ANALITYCZNY	17
7.1	Wymagania ogólne	17
7.2	Rozkład ruchu w sieci.....	17
7.3	Wykrywanie nieprawidłowości uzyskiwanych danych.....	18
7.4	Statystyki wypadkowości	18
8	ZARZĄDZANIE SYSTEMEM.....	20
8.1	Wymagania ogólne	20
8.2	Zarządzanie źródłami danych	20
8.3	Zarządzanie platformą integracyjną	21
8.4	Zarządzanie hurtownią danych	21
8.5	Zarządzanie analizami	21
8.6	Zarządzanie użytkownikami.....	21
8.7	Status systemu	21
8.8	Logi operacyjne	21
9	ARCHITEKTURA SYSTEMÓW KOMPUTEROWYCH	23
9.1	Wymagania odnośnie serwerów	23
9.2	Wymagania odnośnie sieci serwerowni	24
9.3	Wymagania odnośnie aplikacji klienckich	25
9.4	Wymagania odnośnie dostępności.....	29
9.5	Licencje, prawa autorskie i hasła dostępu	29
9.6	Szkolenia	30
9.7	Uwagi końcowe	31
10	PROTOKOŁY WYMIANY DANYCH	33
10.1	Wymagania ogólne	33
10.2	Wymagania formalne	33
10.3	Warunki szczegółowe.....	34
10.4	Wymaganie otwartości systemów	34
11	INFORMACJE I WYMAGANIA DODATKOWE	35
12	OBOWIĄZKI WYKONAWCY	36

1 OGÓLNY OPIS PROJEKTU

1.1 Zakres Projektu

W ramach projektu zmodernizowany zostanie system tablic zmiennej treści na najważniejszych trasach wjazdowych do Krakowa co pozwoli na dostarczanie poszerzonej informacji, w tym dotyczącej czasu przejazdu na danych odcinkach, trasach alternatywnych oraz parkingach Park & Ride. Przeprowadzona zostanie integracja z istniejącym systemem monitoringu dróg celem automatyzacji pozyskania danych i szacowania informacji o czasie przejazdu.

Prace przewidziane w ramach projektu:

- budowa kanalizacji światłowodowej (połączenie centralnego systemu z istniejącymi stacjami pogodowymi (zawierającymi tablice zmiennej treści) na głównych trasach wlotowych oraz głównych ciągach komunikacyjnych w Mieście;
- dostawa nowych wyświetlaczy do tablic zmiennej treści, pozwalających na wyświetlenie większej ilości informacji;
- modernizacja istniejącego systemu tablic – wymiana niezbędnych elementów oraz wykonanie prac informatycznych w zakresie transmisji danych do tablic zmiennej treści;
- budowa systemu predykcji czasu przejazdu, w tym uzupełnienie ciągów komunikacyjnych o punkty pomiarowe czasu przejazdu oraz uzupełnienie danych z zewnętrznych systemów;
- implementacja interfejsów API do wymiany danych pomiędzy systemami o wartościach pomiarowych oraz danych surowych po stronie nowego systemu oraz wybranych istniejących systemów ITS.

Dokument ten zawiera informacje o hurtowni danych i interfejsów udostępniających dane oraz wymagania w stosunku do nowych urządzeń i funkcjonalności jaką należy zapewnić.

1.2 Terminy realizacji

Wykonawca w ciągu 1 miesiąca od momentu podpisania umowy przedstawi do zatwierdzenia Harmonogram prac / Program Robót przy czym uwzględni w powyższym Harmonogramie Kamienie Milowe opisane w umowie

1.3 Wymagania ogólne

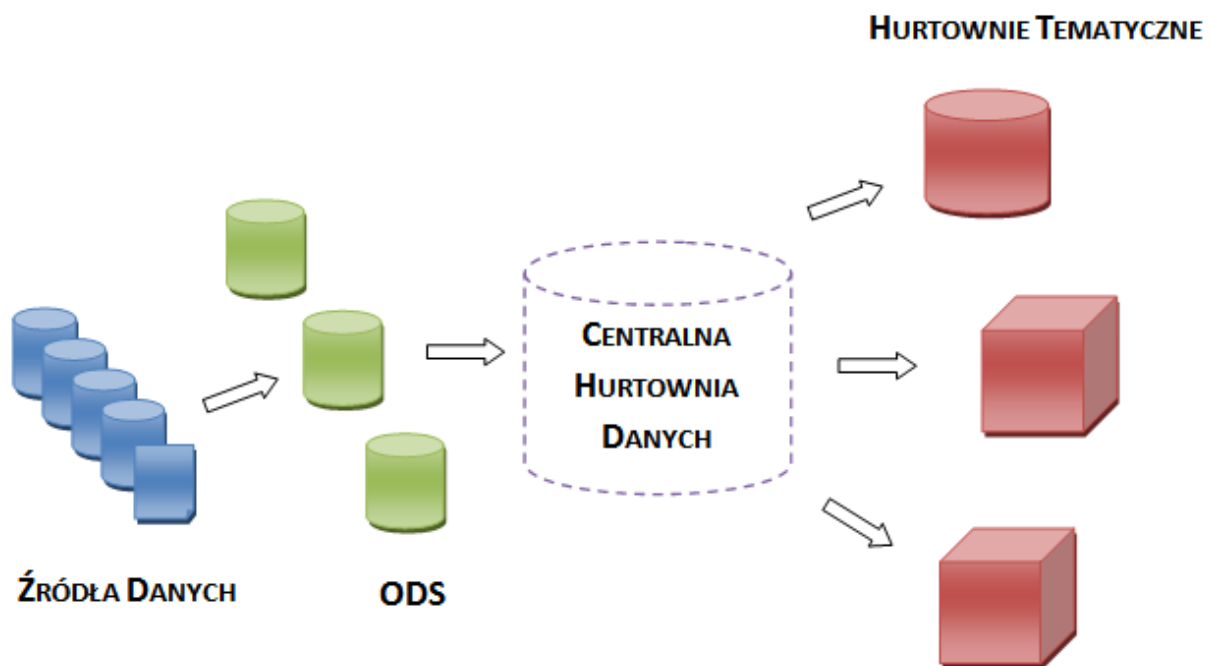
Zamówienie winno być zrealizowane kompletnie zgodnie z wymaganiami Zamawiającego określonymi w niniejszym Opisie Przedmiotu Zamówienia (OPZ), Programie Funkcjonalno-Użytkowym (PFU) oraz Specyfikacji Istotnych Warunków Zamówienia (SIWZ) oraz Umowie. Oznacza to przede wszystkim, że wszystkie funkcje wymienione w opisie poszczególnych Zadań winny być zaimplementowane oraz współpracować z funkcjami już istniejącymi w Krakowie.



W wypadku wystąpienia potrzeby zlecenia prac uzupełniających Zamawiający oczekuje od Wykonawcy określenia kosztorysu i zakresu zleczanych prac. Obydwa elementy będą przedmiotem negocjacji z Wykonawcą.

1.4 Architektura systemu

Zalecana przez Zamawiającego architektura ogólna dostarczanego systemu przedstawiona jest na poniższym rysunku:



Wykonawca może zaproponować inną architekturę jeśli uzna, że zalecana przez Zamawiającego jest niewystarczająca lub nieoptymalna w niektórych obszarach zastosowania. Jednak zmiana architektury ogólnej musi zostać uargumentowana przez Wykonawcę i zaakceptowana przez Zamawiającego.

2 ŹRÓDŁA DANYCH

W ramach realizacji tej części Wykonawca jest zobowiązany do:

- Opracowanie szczegółowej specyfikacji technicznej i funkcjonalnej dostarczanego oprogramowania,
- Opracowanie dokumentacji technicznej rozwiązania,
- Dostawy i montażu w serwerowni Zamawiającego,
- Przeprowadzenia testów odbiorczych (FAT i SAT),
- Przeprowadzenia szkoleń.

2.1 Wymagania ogólne

Wykonawca ma za zadanie zaimplementować zestaw protokołów do wymiany danych z systemami zewnętrznymi. Częstotliwość i zakres pobierania danych ma być zależna od wykorzystywanego protokołu oraz potrzeb algorytmów przetwarzających te dane (por. rozdział 7). Każda instancja interfejsu powinna mieć możliwość konfiguracji częstotliwości, tzn. połączenie do różnych dostawców tym samym interfejsem powinno mieć możliwość ustawienia własnej częstotliwości odświeżania danych.

2.2 Dane z Systemu Sterowania Ruchem

Należy zaimplementować interfejs komunikacyjny w celu pobierania danych o natężeniu ruchu i przebiegów programów sygnalizacji z obu systemów sterowania ruchem.

2.2.1 VTnet

Posiada zaimplementowany protokół komunikacyjny OTS2. Należy skonfigurować protokół po stronie systemu VTnet oraz wdrożyć protokół po stronie systemu zbierania danych. Konfigurację po stronie systemu VTnet może przeprowadzić tylko producent systemu (GEVAS software).

Protokół OTS2 przesyła dane o zmianie stanu detektorów i te dane należy przetworzyć na poszczególne pojazdy.

2.2.2 Sitraffic Scala

Należy zaimplementować jeden z dwóch dostępnych protokołów danych czasu rzeczywistego. Oba protokoły może zaimplementować tylko producent systemu (SIEMENS).

Protokół OCIT-I przesyła dane o zmianie stanu detektorów i te dane należy przetworzyć na poszczególne pojazdy.

Protokół OCIT-C/OCPI2 przesyła dane co 90s o liczbie pojazdów, które przejechały w tym okresie.

2.3 Dane z systemu pomiarowego sieci drogowej

Należy zaimplementować interfejs komunikacyjny w celu pobierania danych o natężeniu ruchu na sieci ulicznej z implementowanego systemu przetwarzania danych. Z tego systemu będą przekazywane następujące informacje:

- aktualnych i prognozowanych czasach przejazdu,
- aktualnych warunków ruchu w sieci (poziom swobody ruchu, średnia prędkość),
- poszczególnych zarejestrowanych podróży przez sieć,
- wyświetlanych komunikatach na tablicach VMS,
- danych meteorologicznych.

Protokół komunikacyjny zostanie przekazany w trakcie realizacji po jego wyspecyfikowaniu przez Wykonawcę zadania na budowę systemu pomiarowego. Do szacowania pracy należy założyć, że będzie bazował na technologiach webowych (SOAP, JSON, XML, HTTP, itp.).

2.4 Dane z systemu pomiarowego sieci dróg rowerowych

Należy zaimplementować i uruchomić interfejs pobierający dane o natężeniu ruchu rowerowego z bazy danych systemu liczącego. Struktura bazy danych zostanie przekazana na etapie Wykonawstwa a sposób uzyskania dostępu uzgodniony między Wykonawcą a Zamawiającym na etapie projektowania.

2.5 Dane z systemów obsługi parkingów

Należy zaimplementować i uruchomić interfejs komunikacyjny z hurtownią danych o systemie komunikacyjnym Zamawiającego w celu pobierania informacji o wolnych miejscach parkingowych na parkingach P&R.

Interfejs należy zbudować w formie aplikacji z obsługą wtyczek, tak aby nowe systemy parkingowe można było obsługiwać za pomocą tego samego interfejsu. Należy także wykonać dokumentację API wtyczek wraz z przykładem użycia i sposobem konfiguracji, dodawania i usuwania poszczególnych wtyczek z interfejsu.

Protokół komunikacyjny zostanie przekazany w trakcie realizacji po jego wyspecyfikowaniu przez Wykonawcę zadania na budowę hurtowni danych. Do szacowania pracy należy założyć, że będzie bazował na technologiach webowych (SOAP, JSON, XML, HTTP, itp.).

2.6 Dane z systemów zarządzania komunikacją publiczną

Należy zaimplementować i uruchomić interfejs komunikacyjny z systemami zarządzania flotą TTSS (producentem jest firma Trapeze) oraz flotą firmy Mobilis (producentem jest firma SIMS) w celu pobierania informacji o danych operacyjnych tych systemów, w tym:

- lokalizacja pojazdów,
- numer pojazdu, numer brygady, typ pojazdu, aktualne odchylenie od rozkładu jazdy,
- prognozowane czasy odjazdu z przystanków,
- zapewnienie pojazdów (jeśli dostępne),
- inne dostępne w danym systemie.

Dla pobierania poszczególnych danych mogą zostać opracowane odrębne protokoły w zależności od częstotliwości pobierania danych oraz potrzeby udostępniania na potrzeby aplikacji zewnętrznych.

Wykonawca opracuje i uzgodni z Zamawiającym przy współpracy producentów systemów wykorzystywane protokoły komunikacyjne, który zostaną następnie przez Wykonawcę zaimplementowane po stronie hurtowni danych oraz po stronie systemów zewnętrznych.

2.7 Dane meteorologiczne

Należy zaimplementować i uruchomić interfejs komunikacyjny z hurtownią danych Zamawiającego w celu wysyłania informacji o danych meteorologicznych pozyskiwanych ze stacji pogodowych.

Protokół komunikacyjny zostanie przekazany w trakcie realizacji po jego wyspecyfikowaniu przez Wykonawcę aplikacji. Do szacowania pracy należy założyć, że będzie bazował na technologiach webowych (SOAP, JSON, XML, HTTP, itp.).

2.8 Dane z bazy danych o wypadkach

Należy zaimplementować i uruchomić interfejs pobierania danych z bazy danych o wypadkach systemu Kraksa będącą w posiadaniu Zamawiającego w celu udostępnienia i analizy statystyk.

Wykonawcy na etapie realizacji zostanie udostępniona struktura bazy danych. Zawartością bazy są pola tekstowe, numeryczne oraz zeskanowane dokumenty w formacie tiff.

2.9 Dane z systemu zajęcia pasa drogowego

Należy zaimplementować i uruchomić interfejs komunikacyjny z systemem oraz bazą danych realizującą zakres zarządzania pasem drogowym TEKA, dotyczącym zajęcia pasa drogowego w zakresie awarii, rozkopów, umieszczeń itp. będącą w posiadaniu Zamawiającego w celu dalszej dystrybucji danych.

Wykonawca opracuje i uzgodni z Zamawiającym, wykorzystywany w tym celu protokół komunikacyjny, służący do pobierania danych z systemu zajęcia pasa drogowego i agregacji tych w hurtowni danych w celu ich dalszej dystrybucji.



2.10 Dane z kamer Systemu Sterowania Ruchem

Należy pobierać zrzuty z kamer z platformy Avigilon będącej w posiadaniu Zamawiającego. Zrzuty z poszczególnych kamer są składowane na serwerze FTP.

3 PLATFORMA INTEGRACYJNA (WARSTWA ETL)

W ramach realizacji tej części Wykonawca jest zobowiązany do:

- Opracowanie szczegółowej specyfikacji technicznej i funkcjonalnej dostarczanego oprogramowania,
- Opracowanie dokumentacji technicznej rozwiązania,
- Dostawy i montażu w serwerowni Zamawiającego,
- Przeprowadzenia testów odbiorczych (FAT i SAT),
- Przeprowadzenia szkoleń.

3.1 Wymagania ogólne

Oprogramowanie ma za zadanie zarządzanie interfejsami i połączeniami z poszczególnymi źródłami danych, filtracja i oznaczanie danych niepewnych, agregacja oraz przesłanie do systemu udostępniania oraz hurtowni danych.

3.2 Filtracja danych

Filtry statystyczne używane przez aplikację powinny mieć możliwość okresowej kalibracji za pomocą danych zgromadzonych w hurtowni.

Jeśli dokładne filtrowanie danych nie będzie znacząco bardziej czasochłonne niż wersja wstępna można zrezygnować z podwójnego filtrowania i używać tylko jednej wersji.

3.3 Agregacja danych

Dane pozyskane z źródeł zewnętrznych należy przetworzyć i ewentualnie wstępnie zagregować do postaci, jaka ma być udostępniana na potrzeby interfejsów dla aplikacji zewnętrznych.

Jeśli dane nie będą udostępniane a tylko bezpośrednio ładowane do hurtowni danych ich agregacja może odbywać się tak często jak jest to potrzebne z punktu widzenia optymalizacji pracy oprogramowania i wykorzystywanego sprzętu.

Przedziały agregacji dla poszczególnych rodzajów danych zostaną ustalone przez Wykonawcę i Zamawiającego na etapie projektowania hurtowni danych z uwzględnieniem potrzeb oprogramowania analizującego (por. rozdział 7).

4 MAGAZYN DANYCH OPERACYJNYCH – WYMIANA DANYCH W CZASIE RZECZYWSITYM

W ramach realizacji tej części Wykonawca jest zobowiązany do:

- Opracowanie szczegółowej specyfikacji technicznej i funkcjonalnej dostarczanego magazynu,
- Opracowanie dokumentacji technicznej rozwiązania,
- Dostawy i montażu w serwerowni Zamawiającego,
- Przeprowadzenia testów odbiorczych (FAT i SAT),
- Przeprowadzenia szkoleń.

4.1 Wymagania ogólne

Magazyn danych operacyjnych, który będzie podstawą działania oprogramowania integracyjnego ma za zadanie także umożliwić dostęp do danych aktualnych zebranych ze źródeł na potrzeby systemów zewnętrznych.

Dostęp do danych przez aplikacje zewnętrzne będzie się odbywał za pomocą protokołów komunikacyjnych opisanych w rozdziale 6.2. Jeśli rozwiązanie proponowane przez Wykonawcę dla magazynu danych operacyjnych uniemożliwia realizację funkcji podstawy pracy systemu integracyjnego oraz jednoczesnego udostępniania danych należy magazyn zrealizować w dwóch częściach.

Dane pozyskiwane ze źródeł będą w części przekazywane tylko do hurtowni, w części tylko udostępniane (bez archiwizacji) a w części będą przekazywane do hurtowni i udostępniane. Wstępny podział danych do udostępnienia i przekazania do hurtowni mieści się w rozdziałach 4.3 i 4.4. Na etapie projektowania rozwiązania oraz informacji o wszystkich możliwych danych pobieranych ze źródeł obie listy zostaną doszczegółowione.

4.2 Wymagania techniczne

Minimalny okres przechowywania danych w magazynie danych operacyjnych musi pozwolić na zagregowanie ich do postaci wymaganych w rozdziale 3.3. Zakłada się, że ten okres będzie wynosił nie mniej niż 24h jednak ze względów praktycznych zaleca się aby był większy o 2-3 razy niż wymagane minimum w celu zapewnienia możliwości przyjęcia danych archiwalnych ze źródeł danych w razie zerwania komunikacji na dłuższy okres czasu.

Moc obliczeniowa i projektowana architektura instalowanego sprzętu informatycznego powinna umożliwiać bieżące przetwarzania danych otrzymywanych ze źródeł oraz obsługę zapytań z aplikacji zewnętrznych a w razie konieczności zwiększenie dostępnej mocy obliczeniowej i magazynowej.

W projektowaniu dostępnej mocy obliczeniowej oraz wydajności podsystemu pamięci masowej należy mieć na uwadze, że różne źródła danych mają różną częstotliwość wysyłania danych po dostępnych protokołach – od informacji o każdej zmianie stanu urządzeń nawet

kilka razy w sekundzie do przesyłania wstępnie zagregowanych danych raz na kilkadziesiąt minut.

Podsystem odpowiedzialny za komunikację z aplikacjami zewnętrznymi należy tak skalować, aby dla protokołów ogólnodostępnych (por. rozdział 6.2) była możliwość obsługi do 2000 konkurencyjnych zapytań na sekundę dla jednego interfejsu. Dla pozostałych typów interfejsów wymagana wydajność zależy od liczby danych wysyłanych takim interfejsem przy założeniu maksymalnie kilku użytkowników zadających pytanie jednocześnie.

Ponadto należy przygotować interfejs przekazujący dane do Krajowego Punktu Dostępowego realizowanego przez GDDKiA. Protokołem komunikacyjnym używanym w KPD jest Datex II.

4.3 Dane dostępne dla aplikacji zewnętrznych

Udostępnieniu na zewnątrz podlegają dane:

- natężenie ruchu na detektorach,
- aktualny czas przejazdu na odcinkach sieci,
- aktualne warunki ruchu na odcinkach sieci,
- aktualne informacje wyświetlane na tablicach VMS,
- aktualne informacje przesyłane z stacji pogodowych,
- lokalizacja pojazdów,
- numer pojazdu, numer brygady, typ pojazdu, aktualne odchylenie od rozkładu jazdy,
- spis numerów technicznych pojazdów niskopodłogowych,
- prognozowane czasy odjazdu z przystanków,
- informacje z aplikacji ostrzegającej o utrudnieniach w sieci drogowej,
- informacje z aplikacji ostrzegającej o utrudnieniach w sieci komunikacji publicznej,
- zdjęcia okresowo wykonywane z kamer Systemu Sterowania Ruchem.
- zajęcia pasa drogowego

Agregacja danych zgodnie z rozdziałem 3.3. Zakres danych może ulec zmianie na etapie projektowania systemu.

4.4 Dane przekazywane do hurtowni

Przekazaniu do hurtowni po agregacji podlegają dane:

- natężenie ruchu na detektorach,
- realizowane programy sygnalizacji,
- aktualny czas przejazdu na odcinkach sieci,
- prognoza czasu przejazdu na odcinkach sieci,
- podróże odbyte przez sieć przez pojazdy,
- informacje przesyłane z stacji pogodowych,



- zarejestrowane czasy przejazdu pomiędzy przystankami,
- zapelnienie pojazdów pomiędzy przystankami,
- prognozowane czasy odjazdu z przystanków,
- informacje z aplikacji ostrzegającej o utrudnieniach w sieci drogowej,

Agregacja danych zgodnie z rozdziałem 3.3. Zakres danych może ulec zmianie na etapie projektowania systemu.



5 CENTRALNA HURTOWNIA DANYCH

W ramach realizacji tej części Wykonawca jest zobowiązany do:

- Opracowanie szczegółowej specyfikacji technicznej i funkcjonalnej dostarczanego magazynu,
- Opracowanie dokumentacji technicznej rozwiązania,
- Dostawy i montażu w serwerowni Zamawiającego,
- Przeprowadzenia testów odbiorczych (FAT i SAT),
- Przeprowadzenia szkoleń.

5.1 Architektura

Ze względu na dużą różnorodność przechowywanych danych Zamawiający zaleca, aby rozwiązanie architektralne była zaimplementowane w formie hurtowni tematycznych dotyczących każdego z rodzaju danych osobno, i dostępnych przez wspólny interfejs dostępu (hurtownia wirtualna – por. rozdział 1.1).

Model logiczny oraz fizyczny poszczególnych hurtowni tematycznych może być odmienny w zależności od struktury przechowywanych w nim danych oraz wymagań narzędzi analitycznych, jakie będą nich używane.

5.2 Wymagania techniczne

Minimalny okres przechowywania danych w hurtowni powinien być nie mniejszy niż 5 lat. Moc obliczeniowa i projektowana architektura logiczna powinna umożliwiać bieżące przetwarzanie zapytań analitycznych a w razie konieczności zwiększenie dostępnej mocy obliczeniowej i magazynowej.

W projektowaniu dostępnej mocy obliczeniowej oraz wydajności podsystemu pamięci masowej należy mieć na uwadze wymagania dostarczanych przez Wykonawcę narzędzi analitycznych.

6 DOSTĘP DO DANYCH

W ramach realizacji tej części Wykonawca jest zobowiązany do:

- Opracowanie szczegółowej specyfikacji technicznej i funkcjonalnej dostarczanego oprogramowania,
- Opracowanie dokumentacji technicznej rozwiązania,
- Dostawy i montażu w serwerowni Zamawiającego,
- Przeprowadzenia testów odbiorczych (FAT i SAT),
- Przeprowadzenia szkoleń.

6.1 Aplikacje analityczne i eksploracja danych

Interfejs dostępu do danych powinien umożliwiać zrealizowane kwerendy po różnych bazach tematycznych hurtowni za pomocą jednego zapytania.

Dokumentacja języka zapytań wraz ze strukturą baz danych ma zostać uzgodniona z Zamawiającym na etapie projektowania systemu. Zalecane jest aby stosować ogólnie stosowane standardy języka zapytań (np. SQL).

6.2 Interfejsy dostępu do bazy operacyjnej

Wykonawca opracuje i uzgodni z Zamawiającym protokoły komunikacyjne (API), które będą umożliwiały pobieranie danych zawartych w bazie operacyjnej przez aplikacje zewnętrzne. Zależnie od rodzaju danych dostęp do danych przez poszczególne protokoły będzie możliwy w następujący sposób:

- dostęp ogólnodostępny – odpowiedź na zapytanie za każdym razem kiedy zostaje ono przesłane przez interfejs, możliwość ograniczenia ogólnej liczby zapytań,
- dla zarejestrowanego użytkownika – aby uzyskać dostęp do protokołu każda instancja aplikacji musi mieć zalogowanego użytkownika zarejestrowanego w systemie z możliwością ograniczenia liczby instancji uruchomionych jednocześnie,
- dla zarejestrowanej aplikacji – dostęp tylko w komunikacji serwer – serwer.

Dla każdego z protokołów osobno zostanie określony przez Wykonawcę, Zamawiającego w porozumieniu z zainteresowanymi stronami trzecimi tryby w jakim będą pracować poszczególne interfejsy. Należy przewidzieć, że tryby możliwe będą do zrealizowania to m.in.:

- pobieranie danych,
- subskrypcja z pobieraniem danych,
- subskrypcja z informacją o zaktualizowaniu danych i następnie pobieranie danych
- subskrypcja i następnie automatycznie wysyłanie danych po aktualizacji w bazie operacyjnej.



Zamawiający zaleca aby opracowywane protokoły bazowały na technologiach webowych (SOAP, JSON, XML, HTTP, itp.) i były zgodne z zapisami rozdziału 0.

6.3 Interfejsy dostępu do systemu analiz

Z założenia dostęp bezpośrednio do bazy danych hurtowni nie będzie możliwy z systemów zewnętrznych. Jedynym wyjątkiem są dane o wypadkowości, jakie Zamawiający ma zamiar udostępnić za pośrednictwem systemu analiz. Z tego powodu Wykonawca opracuje API lub stronę WWW, za pomocą której będzie można wykonać zapytania do części hurtowni odpowiedzialnej za przechowywanie statystyk wypadkowości tak aby podmioty zewnętrzne mogły wygenerować interesujące ich statystyki.

6.4 Przykłady wykorzystania

Wraz z opracowaniem interfejsów komunikacyjnych Wykonawca opracuje przykłady wykorzystania każdego z tych interfejsów tak, aby potencjalne strony trzecie były w stanie opracować własne systemy zapytań.

Dokumentacja ta będzie udostępniona dla stron zainteresowanych pobieraniem danych z bazy operacyjnej Zamawiającego.

7 SYSTEM ANALITYCZNY

W ramach realizacji tej części Wykonawca jest zobowiązany do:

- Opracowanie szczegółowej specyfikacji technicznej i funkcjonalnej dostarczanego oprogramowania,
- Opracowanie dokumentacji technicznej rozwiązania,
- Dostawy i instalacji w siedzibie Zamawiającego,
- Przeprowadzenia testów odbiorczych (FAT i SAT),
- Przeprowadzenia szkoleń.

7.1 Wymagania ogólne

Aplikacja służąca do wyświetlania raportów nie może uzależniać wyświetlenia raportu od czasu w jakim trwa jego generacja. Aplikacja nie może też przestać reagować na polecenia użytkownika a w szczególności polecenie zamknięcia do czasu otrzymania raportu.

Wszystkie raporty uzyskane z systemu analiz powinny mieć możliwość eksportu oraz wydruku. Parametry eksportu oraz druku powinny być możliwie dowolne do ustalenia łącznie z ustaleniem indywidualnej skali i obszaru z jakiej zostanie wykonany eksport / wydruk.

7.2 Rozkład ruchu w sieci

Dane pozyskane z systemów sterowania ruchem oraz systemu pomiarowego sieci drogowej, po odsianiu przez podsystem wykrywania danych błędnych, powinny być tak integrowane ze sobą aby uzyskać rozkład przestrzenny przemieszczania pojazdów przez sieć pomiędzy poszczególnymi wierzchołkami grafu (używanego modelu sieci).

Model sieci wykorzystywany przy przetwarzaniu danych powinien uwzględniać punkty pomiarowe jakie są dostępne w sieci. Lokalizacja punktów powinna być ustalana na bazie mapy GIS, która zostanie zaimplementowana w module. Podkład mapowy powinien też służyć do wyświetlania danych przetworzonych przez oprogramowanie.

Podkład GIS powinien być dostarczony przez Wykonawcę. Dostarczony podkład powinien zapewniać częste aktualizacje, aby możliwe było na bieżąco uwzględnianie zmian w sieci drogowej i transportowej miasta. Zamawiający oceni częstość aktualizacji podkładu na podstawie historii aktualizacji dostarczanych map. Podkład zostanie oceniony jako często aktualizowany jeżeli aktualizacje wykorzystywanego podkładu w ciągu ostatnich dwóch lat nie następowały rzadziej niż raz na kwartał. Licencja podkładu GIS ma być zgodna z wymaganiami opisanymi w rozdziale 9.5.

Dane o podróżach i natężeniach ruchu powinny być agregowane do formy wymaganej przez oprogramowanie. Dane zagregowane powinny być w taki sposób aby mogły być generowane statystyki oparte na filtrach:

- Okres czasu z minimalnym przedziałem 5 minut

- Podział na poszczególne dni
- Rodzaj ruchu (zgodnie z podziałem możliwym do uzyskania z systemu pomiarowego sieci drogowej).

Dane zagregowane mają umożliwić generację, z uwzględnieniem ww. filtrów, do formy rozkładu ruchu oraz kartogramu. Rozkład ruchu ma być możliwy do generowania dla:

- Całej objętej sieci
- Wybranego obszaru (odcinki graniczne stają się punktami wejścia / wyjścia)
- Dla konkretnego odcinka (dla pojazdów przejeżdżających przez ten odcinek) tak dla obu kierunków jak i dla wybranego kierunku

Kartogramy mają być możliwe do generowania dla:

- Skrzyżowania
- Wybranego obszaru
- Całej sieci

7.3 Wykrywanie nieprawidłowości uzyskiwanych danych

Analiza ma za zadanie porównywać dane o natężeniach ruchu i podróżach w sieci w taki sposób aby wykrywać, że niektóre źródła danych zwracają dane nie pasujące do obliczonych z porównywanych źródeł.

Analiza ma pozwolić na zwiększenie dokładności uzyskiwanych danych z punktów pomiarowych w sieci do wartości akceptowalnych i umożliwiających generowanie statystycznie ufnych rozkładów ruchu w sieci. Poprawne działanie detekcji przyczyni się także do lepszej pracy systemów sterowania ruchem.

Wykrywane mają być także anomalie w pracy źródeł takie jak zaburzenia pracy, uszkodzenia, brak połączenia. Logika aplikacji powinna zestawiać ze sobą dane dotyczące poszczególnych odcinków sieci (jeśli są dostępne) tak aby wykluczyć anomalie związane np. z robotami drogowymi (np. wyłączenie pasa ruchu, które spowoduje brak pomiarów na jednym z detektorów na skrzyżowanie, ale zwiększy czas przejazdu przez odcinek sieci), wypadkami, itp.

Użytkownik ma mieć możliwość parametryzowania zakresu danych, okresu czasu i częstotliwości uruchamiania analizy.

7.4 Statystyki wypadkowości

Analiza ma obejmować budowę raportów wypadkowości z poszczególnych ulic i skrzyżowań na terenie miasta Krakowa. Filtrowanie powinno być możliwe po:

- ulicy,
- skrzyżowaniu,



- rodzaju wypadku,
- rodzajów uczestników,
- zakresie czasu zdarzenia.

Raporty wygenerowane przez system analizy będą głównie eksportowane na potrzeby stron trzecich.

8 ZARZĄDZANIE SYSTEMEM

Zamawiający oczekuje dostarczenia aplikacji zarządzającej, która będzie umożliwiała konfigurowanie, sprawdzanie i zmianę statusu oraz kontrole pracy poszczególnych elementów.

W ramach realizacji tej części Wykonawca jest zobowiązany do:

- Opracowanie szczegółowej specyfikacji technicznej i funkcjonalnej dostarczanego oprogramowania,
- Opracowanie dokumentacji technicznej rozwiązania,
- Dostawy i instalacji w siedzibie Zamawiającego,
- Przeprowadzenia testów odbiorczych (FAT i SAT),
- Przeprowadzenia szkoleń.

8.1 Wymagania ogólne

Dostarczana aplikacja powinna być niezależnym programem w formie webowej. Dostęp do aplikacji będzie odbywał się z sieci wewnętrznej Zamawiającego oraz z sieci Internet w związku z czym strona prezentowana użytkownikowi przed odbiorem ma przejść pozytywnie testy penetracyjne.

Podczas pracy użytkownik nie powinien musieć wypełniać kolejno procedury postępowania, a w szczególności nie może zostać zablokowany przez niewypełnienie któregoś poprzedniego kroku. W szczególności użytkownik nie powinien być zmuszony do własnoręcznego zakładania warstw pośredniczących a nawet takie warstwy nie powinny być zakładane jeśli wykonywane są czynności ad-hoc.

8.2 Zarządzanie źródłami danych

Aplikacja ma umożliwiać proste modyfikowanie źródeł danych w tym dodawanie, usuwanie oraz zmiana parametrów. Zakłada się, że nowe źródła danych będą tego samego typu i będą przysyłać informacje w takim samym formacie jak istniejące już w systemie.

Modyfikacja źródeł danych ma odbywać się poprzez odpowiedni interfejs użytkownika. Interfejs ma mieć funkcję bieżącego podpowiadania rodzajów i zasięgu danych wprowadzanych. Użytkownik w celu dodania nowych źródeł danych nie może być w żaden sposób zmuszany do bezpośredniej edycji bazy danych.

Jeśli założona przez użytkownika modyfikacja źródeł danych powoduje potrzebę zmodyfikowania także modelu sieci transportowej, która wykorzystywana jest do przetwarzania danych, to taka modyfikacja musi być możliwa poprzez graficzny interfejs użytkownika w formie pracy na mapie.

8.3 Zarządzanie platformą integracyjną

Aplikacja ma umożliwiać zarządzanie interfejsami udostępniania danych w tym określanie maksymalnej jednoczesnej liczby zapytań jaką ma obsługiwać interfejs, jacy użytkownicy lub jakie aplikacje mają prawo z niego korzystać, zarządzać profilami użytkowników i aplikacji uprawnionych do korzystania z poszczególnych interfejsów.

Ponadto zarządca systemu ma mieć możliwość konfigurowania działania elementów filtrowania danych, agregacji i częstotliwości przesyłania danych do interfejsów zewnętrznych oraz centralnej hurtowni.

8.4 Zarządzanie hurtownią danych

Aplikacja ma umożliwiać zarządzanie przestrzenią dyskową, czasem procesora dla poszczególnych zadań obliczeniowych, użytkownikami i aplikacjami analitycznymi mającymi dostęp do poszczególnych obszarów hurtowni.

8.5 Zarządzanie analizami

Narzędzie wykorzystywane do budowania analiz powinno umożliwić Zamawiającego na budowaniu własnych raportów. Dla każdego z raportów istniejących w systemie użytkownik o odpowiednich uprawnieniach powinien mieć możliwość zmiany zakresu danych, częstotliwości uruchamiania i punktu docelowego składowania.

8.6 Zarządzanie użytkownikami

Aplikacja ma umożliwiać graficzne zarządzanie użytkownikami i ich uprawnieniami tak bezpośrednio per użytkownik jak i per grupa użytkowników. Wykonawca uzgodni i następnie wdroży domyślne dostępne grupy użytkowników mając na uwadze funkcjonalność zapewnianą przez dostarczanych system.

8.7 Status systemu

Na mapie logicznej systemu powinien być zaznaczony status wszystkich urządzeń fizycznych, stan pracującego oprogramowania oraz statystyki. Dla ułatwienia przejrzystości zaleca się, aby status poszczególnych elementów był unifikowany do grup elementów (np. instancje tego samego oprogramowania) i był wyświetlany status zbiorczy a dopiero po wybraniu elementu był wyświetlany status indywidualny.

Grupowanie elementów oraz wyświetlane dane szczegółowe o pracy elementów systemu należy uzgodnić z Zamawiającym na etapie projektowania systemu.

8.8 Logi operacyjne

Aplikacja ma posiadać system logowania wszystkich operacji wykonywanych przez jego użytkowników. Integralną częścią aplikacji powinno być także dostępne dla



administratora narzędzie odczytywania i przeglądania tych logów z możliwością filtrowania po wszystkich dostępnych danych zapisywanych w logu.

9 ARCHITEKTURA SYSTEMÓW KOMPUTEROWYCH

9.1 Wymagania odnośnie serwerów

Architektura serwerów dostarczonych w ramach niniejszego Kontraktu powinna zostać dostosowana do architektury stosowanej w serwerowni ZDMK tj. szafy RACK.

Wszystkie aplikacje zmieniające lub instalowane jako nowe mają pracować na dostarczonych komponentach.

W ramach zadania wykonawca dostarczy:

- Moc obliczeniowa dostarczanych komponentów powinna wystarczyć do obsługi wszystkich instalowanych i przenoszonych aplikacji + 25% zapasu.
- Serwery sterujące pracą systemów mają być instalowane jako maszyny wirtualne na ww. urządzeniu. Dla każdej używanej maszyny wirtualnej należy dostarczyć licencję na używany system operacyjny.
- Stosowany system wirtualizacji ma umożliwiać podłączanie urządzeń USB (szczególnie kluczy sprzętowych) do poszczególnych maszyn wirtualnych.
- System zarządzania hostami i maszynami wirtualnymi umożliwiający automatyczne podnoszenie maszyn w razie awarii, przenoszenie maszyn wirtualnych pomiędzy maszynami fizycznymi „w locie”, wyrównywanie obciążenia serwerów fizycznych poprzez przenoszenie maszyn wirtualnych. Jeśli system zarządzania jest licencjonowany, w zależności od ilości maszyn fizycznych lub wirtualnych,.
- Architektura połączeń musi umożliwiać zarządzanie maszynami zainstalowanymi obecnie oraz zainstalowanymi w ramach pozostałych Kontraktów zawartych w projekcie na „Rozbudowę Systemu Zarządzania Transportem Publicznym w Krakowie”.
- Zalecany systemem hosta - ESXi.
- Macierz dyskową na przestrzeń storage dla dostarczonych systemów wraz wszystkimi elementami łączącymi macierz z modułem serwerowym za pomocą połączenia gwarantującego wykorzystanie pełnej wydajności instalowanej macierzy dysków.
- Macierz dyskowa musi umożliwiać rozbudowę o nowe obudowy dla dysków.
- Dostawę dysków twardych o łącznej pojemności wystarczającej do pracy i przechowywania danych dla wszystkich przenoszonych i instalowanych aplikacji. Należy użyć jak najmniejszą ilość dysków.
- Serwery sterujące pracą systemów mają być instalowane jako maszyny wirtualne na dostarczonych urządzeniach. Dla każdej używanej maszyny wirtualnej należy dostarczyć licencję na używany system operacyjny. Zakupione licencje muszą umożliwiać przenoszenie systemów pomiędzy serwerami.
- System zarządzania hostami i maszynami wirtualnymi musi umożliwiać automatyczne podnoszenie maszyn w razie awarii, przenoszenie maszyn wirtualnych pomiędzy maszynami fizycznymi „w locie”, wyrównywanie obciążenia serwerów fizycznych poprzez przenoszenie maszyn wirtualnych.

- Ilość zasobów w zwirtualizowanych serwerach fizycznych (pamięć RAM, ilość procesorów, ilość kart sieciowych) powinna być dobrana tak, aby nie wykorzystywały więcej niż 70% mocy obliczeniowej przydzielonych procesorów lub/i 70% zajętości pamięci przy normalnej pracy maszyn wirtualnych pracujących na tych serwerach.
- Zasoby dyskowe serwerów powinny pracować w RAID6, a dostarczane rozwiązania powinny być wyposażone w mechanizmy inkrementacyjnego backupu wykonywanego automatycznie.
- Maszyna wirtualna powinna zostać przełączona automatycznie z jednego serwera fizycznego na drugi w przypadku kiedy nastąpi wyczerpanie zasobów.
- Dwa wydajne serwery do przetwarzania aplikacji serwerowych, wzajemnie redundantne, z redundantnymi zasilaczami i kartami sieciowymi (główne zastosowanie: zbieranie danych dotyczących ruchu i obsługa kamer ANPR oraz tablic VMS)
- Każdy z serwerów umieszczonych w pomieszczeniu serwerowym powinien być wyposażony w minimum 2 redundantne zasilacze i 2 redundantne karty sieciowe każda po 4 porty w konfiguracji: 4 x 1GbE, 4 x 10GbE. Porty kart sieciowych, będą podłączone do różnych torów komunikacyjnych.
- Dostarczony przez Wykonawcę sprzęt, będący wyposażeniem pomieszczenia serwerowego musi pracować poprawnie w temperaturze w przedziale od +10°C do +35°C.
- Dostarczony przez Wykonawcę sprzęt, będący wyposażeniem pomieszczenia serwerowego musi pracować poprawnie przy wilgotności powietrza od 5% do 80%.
- Wykonawca musi dostarczyć komplet dokumentacji technicznej oraz gwarancyjnej na sprzęt dostarczony na potrzeby działania systemu.

9.2 Wymagania odnośnie sieci serwerowni

Architektura sieci skonfigurowanej w ramach niniejszego Kontraktu powinna zostać dostosowana do architektury stosowanej w serwerowni Centrum Sterowania Ruchem.

Połączenie systemu z resztą sieci musi zostać przeprowadzone w oparciu o istniejący Stack Switchy Extreme X440-G2-48t-10GE4. Na potrzeby realizacji funkcjonowania Systemu Wykonawca powinien dostarczyć fabrycznie nowy przełącznik wraz z okablowaniem do pełnej integracji z istniejącym Stackiem Extreme X440-G2-48t-10GE4 oraz wykreować osobny VLAN oddzielający System od istniejącej struktury sieci. Serwery powinny być podłączone ze ww. stackiem switchy co najmniej dwoma połączeniami w agregacji portów zgodnej ze standardem IEEE (LACP). Na potrzeby funkcjonowania sieci Systemu (np. połączeń pomiędzy serwerami) należy zbudować w szafie rack przełącznika switch zarządzalny o następującej funkcjonalności:

- Wszystkie porty o minimalnej przepustowości 1 Gb/s, ilość portów musi być wystarczająca do podłączenia wszystkich urządzeń wchodzących w skład systemu plus należy zachować rezerwę (minimum tyle samo wolnych portów co zajętych);
- Posiadać minimum 2 porty SFP;
- Posiadać wsparcie dla agregacji portów (LACP);

- W pełni wspierać obsługę VLAN zgodnie ze standardami IEEE;
- Zapewniać obsługę ACL;
- Zapewniać pracę zarówno w warstwie drugiej jak i trzeciej (L2 i L3);
- Możliwość zarządzania przełącznikiem z poziomu różnych VLANów i interfejsów sieciowych z wykorzystaniem bezpiecznych protokołów sieciowych (SSH oraz HTTPS);
- Wsparcie dla protokołu NTP, SNMPv3, IPv4 oraz IPv6;
- Wsparcie mechanizmów QoS (Quality of Service);
- Posiadać redundantny zasilacz i wentylator,
- Zapewniać aktualizacje firmware'u bez przerwy w działaniu urządzenia,
- Możliwość montażu w istniejącej szafie rack przy wykorzystaniu maksymalnie wysokości 1U dla pojedynczego urządzenia,
- Na wszystkie wyżej wymienione funkcje muszą być zakupione odpowiednie licencje.

W razie niewystarczającej infrastruktury sieciowej po stronie Zamawiającego, Wykonawca dostarczy lub wymieni istniejące urządzenia zapewniając wymaganą funkcjonalność jak i zachowa w pełni funkcjonowanie istniejących rozwiązań.

Dla celów udostępniania danych na potrzeby użytkowników zewnętrznych należy dostarczyć urządzenie typu UTM przez które będzie trasowany cały ruch pomiędzy aplikacjami stron trzecich oraz interfejsami komunikacyjnymi całej sieci ITS Zamawiającego.

Urządzenie UTM ma posiadać następującą funkcjonalność:

- Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
- Urządzenie musi zapewniać obsługę dla IPv6.
- Urządzenie musi zapewnić możliwość statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.
- Urządzenie nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
- Reguły zabezpieczeń firewall zgodnie z ustaloną polityką opartą o profile oraz obiekty. Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa. Konsola zarządzania posiada możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.
- Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
- Urządzenie musi zapewnić możliwość skanowania całości ruchu pod kątem zaistnienia podatności, a nie wyłącznie wybranych próbek ruchu.

- Urządzenie musi identyfikować co najmniej 1800 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Gadu-Gadu, Tor, BitTorrent, eMule.
- Urządzenie musi zapewnić możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.
- Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność podmieniania adresów domen uznanych za złośliwe na zdefiniowany adres lokalny w odpowiedziach na zapytania DNS w celu wykrycia hostów z sieci wewnętrznej które próbują nawiązać komunikację ze złośliwymi domenami.
- Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPsec i IKE w konfiguracji site-to-site. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.
- Urządzenie musi zapewniać zestawienie przynajmniej 1024 równoczesnych sesji SSL VPN.
- Urządzenie musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres 12 miesięcy.
- Urządzenie musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej, kontrolującego przynajmniej protokoły: SMTP, HTTP i HTTPS oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres 12 miesięcy.
- Urządzenie musi posiadać możliwość rozbudowy o moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP. Baza kategorii stron musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny.
- Urządzenie musi zapewnić również możliwość dodania własnej lub zmiany predefiniowanej kategoryzacji URL. W ramach tego zamówienia Zamawiający nie wymaga dostarczenia subskrypcji dla tej usługi.
- Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować
- prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
- Urządzenie musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
- Urządzenie musi działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym (tzn. w warstwie 2 modelu OSI) oraz trybie pasywnego nasłuchu
- (tzn. TAP). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych.
- W architekturze rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.

- Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active.
- Urządzenie musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Możliwość utworzenia min. 2000 reguł dla różnego rodzaju ruchu sieciowego..
- Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.
- Urządzenie musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
- Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.
- Urządzenie musi być dostarczone jako dedykowane urządzenie zabezpieczeń sieciowych (appliance).
- Urządzenie musi być urządzeniem o uznanej na rynku pozycji i muszą znajdować się w kwadracie „Leaders” lub „Challengers” raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls -Październik 2018”
- Urządzenie nie może znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
- Urządzenie musi być w obudowie typu rack.
- Urządzenie musi być dostarczone w konfiguracji z minimum 12 portami 1000BaseT i 8 portami Gigabit SFP.
- Urządzenie musi zapewniać wydajność przynajmniej 2,5 Gbps dla ruchu IPSec VPN.
- Urządzenie musi umożliwiać zestawienie przynajmniej 1024 równoczesnych tuneli VPN IPSec.
- Urządzenie musi posiadać przepustowość w ruchu nie mniej niż 5 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji oraz akceptować nie mniej niż 57 000 połączeń na sekundę. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona Intrusion Prevention, antywirus, filtracja aplikacji i kategoryzacja URL) nie może być mniejsza niż 3,1 Gbps.
- Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP i OSPF.
- Rozwiązanie musi posiadać możliwość podłączenia urządzeń firewall w klastrze pod scentralizowany system zarządzania.
- Zarządzanie systemem zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.
- Urządzenie firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.

- Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy z naprawą w trybie naprawa następnego dnia roboczego i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres 12 miesięcy.
- Urządzenie musi być wyposażone w dedykowany port zarządzania out-of-band.
- Urządzenie musi mieć możliwość rozbudowy dla osiągnięcia możliwości definicji min. 10 wirtualnych firewalli.
- W przypadku gdy urządzenie pozwala na jednoczesną pracę dwu lub więcej administratorów musi istnieć wbudowany w system mechanizm umożliwiający jednemu z administratorów uzyskanie wyłączności na wprowadzanie zmian. W tym czasie pozostali zalogowani użytkownicy nie mogą być w stanie dokonać żadnych zmian w konfiguracji.
- Urządzenie musi umożliwiać przesyłanie logów do kilku zdefiniowanych serwerów Syslog. Administrator urządzenia musi mieć możliwość zdefiniowania, dla każdej reguły bezpieczeństwa, innego serwera Syslog.
- Administrator urządzenia musi mieć możliwość przeglądania z poziomu urządzenia informacji o plikach które zostały wysłane do analizy w systemie "Sand-Box", informacji jak przesłane pliki zachowywały się w środowisku testowym, które z nich i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki przesyłali.
- Urządzenie musi posiadać funkcjonalność pozwalającą administratorowi urządzenia na konfigurację rodzaju pliku (przynajmniej exe, dll), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.
- Urządzenie musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesję w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
- Urządzenie zabezpieczeń musi posiadać wbudowany twardego dysku do przechowywania logów i raportów. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
- Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.
- Musi istnieć możliwość dostarczenia fizycznej lub wirtualnej platformy zarządzającej pozwalającej na centralne zarządzanie, logowanie i raportowanie zdarzeń z podłączonych do niej firewalli.
- Konsola zarządzająca, logująca i raportująca musi mieć możliwość korelowania zbieranych zdarzeń i informacji oraz budowania na ich podstawie wielu, dostosowanych do potrzeb Zamawiającego raportów. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowaniu stron WWW. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.

- Konsola zarządzająca, logująca i raportująca musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur oraz funkcje audytu i backupu konfiguracji. Konsola zarządzania posiada możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.
- Konsola zarządzająca wieloma instancjami firewalli nie jest przedmiotem tego postępowania.

9.3 Wymagania odnośnie aplikacji klienckich

Wymagane jest, aby wszystkie aplikacje klienckie dostarczane w ramach niniejszego Kontraktu, a mające pracować na tych stacjach roboczych, powinny prawidłowo pracować w systemie Windows 7 Professional PL w wersji 64bit oraz w Windows 10 Professional PL 64bit.

Dostarczone aplikacje, powinny być najbardziej aktualnymi wersjami dostępnego oprogramowania w momencie instalacji oraz powinny być zaktualizowane do najnowszych wersji najpóźniej w dniu obioru końcowego niniejszego zamówienia.

9.4 Wymagania odnośnie dostępności

Należy zapewnić funkcjonalność sprawowania funkcji administracyjnych oraz obsługowych każdej instalowanej aplikacji jak i systemów operacyjnych na których one działają z dowolnego miejsca poprzez sieć Internet. Wymagane jest aby transmisja była zabezpieczona przez protokół SSL oraz szyfrowany tunel VPN.

Wszystkie hasła dostępu (w szczególności administracyjne, poza indywidualnymi, przypisanymi konkretnym użytkownikom systemu) oraz dokumentacje pełnego opisu systemu należy przekazać do Zamawiającego najpóźniej w dniu odbioru końcowego niniejszego zamówienia.

Jeżeli wsparcie systemu odbywać się będzie zdalnie, za pomocą powyższych środków, Wykonawca do momentu przekazania dostarczy pełną listę osób i użytkowników wykonujących czynności serwisowe.

9.5 Licencje, prawa autorskie i hasła dostępu

Po zakończeniu realizacji poszczególnych części, a przed kompleksowym odbiorem systemu należy wykonać:

- przekazanie wszystkich haseł dostępu (w szczególności administracyjnych, z wyłączeniem indywidualnych, uprzednio przypisanych konkretnym użytkownikom systemu).
- przekazanie licencji na całe dostarczone w ramach Kontraktu oprogramowanie z uwzględnieniem, że:

- dostarczony w kontrakcie podkład GIS nie może być objęty płatną licencją w żadnej formie (wraz z aktualizacjami), a licencja na oprogramowanie bazy danych GIS ma umożliwić Zamawiającemu korzystanie z samej bazy oraz jej zawartości zarówno na potrzeby Zamawiającego jak i stron trzecich w przypadkach potrzeby przyszłościowej rozbudowy systemu centralnego;
- licencja na oprogramowanie analityczne powinna umożliwiać równoczesną pracę dowolnej liczby użytkowników;
- zobowiązanie do przeniesienia na Zamawiającego autorskich praw majątkowych do protokołów wymiany danych z systemami zewnętrznymi, o ile stanowią one utwór w rozumieniu prawa autorskiego, i wyrażenie zgody na ich wykorzystanie przez Zamawiającego na następujących polach eksploatacji:
 - powielanie kodu lub tłumaczenie jego formy (dekompilacja), modyfikowanie (tłumaczenie, przystosowanie lub jakiegokolwiek inne zmiany) bez ograniczania warunków tych czynności, w celu wykorzystania dla celów współdziałania z innymi programami komputerowymi, rozwoju lub innych form korzystania o podobnej lub zbliżonej formie;
 - rozpowszechnianie w sieci Internet, w sieciach zamkniętych oraz na tablicach zewnętrznych informacji uzyskanych na podstawie danych zebranych przez dostarczone oprogramowania w ramach niniejszego kontraktu;
- wraz z przekazaniem praw nastąpi przekazanie kodów źródłowych dla całego wymagane przez Zamawiającego oprogramowania;
- kod źródłowy wraz z dokumentacją, zostanie dostarczony na rzecz Zamawiającego na nośnikach CD/DVD – w ilości 2 kopii

9.6 Szkolenia

W ramach dostawy urządzenia sieciowego typu Firewall, Wykonawca musi zapewnić min. 3 dniowe szkolenie dla 5 administratorów w siedzibie Zamawiającego. Zamawiający dopuszcza zorganizowanie szkolenia poza siedzibą firmy, po warunkiem pokrycia wszystkich kosztów takiego szkolenia. Po zakończeniu szkolenia wymagane jest wystawienie certyfikatu potwierdzającego ukończenie szkolenia z zakresu przedstawionego poniżej. Szkolenie musi być prowadzone przez wykwalifikowany personel, posiadający certyfikaty producenta dostarczanego urządzenia sieciowego typu Firewall.

Zakres szkolenia:

1. Wprowadzenie.
 - Architektura sprzętowa
 - Funkcjonalność urządzenia
2. Administracja i zarządzanie:
 - Zarządzanie konfiguracją

- System oraz aktualizacje oprogramowania
 - Aktualizacja sygnatur
 - Logi i filtry
3. Implementacja systemu firewall:
- Strefy bezpieczeństwa
 - Konfiguracja interfejsów V-wire
 - Konfiguracja interfejsów L3
 - Konfiguracja wirtualnych routerów
 - Wprowadzenie do polityk bezpieczeństwa
 - Konfiguracja NAT
 - Konfiguracja tuneli VPN site-to-site
 - Konfiguracja tuneli VPN client-to-site Global Protect
4. Kontrola aplikacji:
- Administracja
 - Konfigurowanie grup i filtrów aplikacji
5. Filtry zawartości:
- Polityki bezpieczeństwa
 - Profile bezpieczeństwa:
 - Antywirus
 - Antyspyware
 - Podatności
 - Filtrowanie URL
 - Blokowanie plików oraz WildFire
 - Filtrowanie danych
 - Ochrona strefowa
6. Integracja z bazami danych użytkowników na przykładzie AD
7. Konfiguracja QoS
8. Raportowanie
9. Szkolenie z zasad bezpieczeństwa sieci:
- routing,
 - zasad bezpieczeństwa sieci
 - procedury zabezpieczające przed nieuprawnionym dostępem z zewnątrz,
 - wykrywanie i zapobieganie ataków.

9.7 Uwagi końcowe

Wszystkie dostarczone systemy operacyjne mają zostać wyposażone w program antywirusowy. Program powinien mieć włączoną funkcję automatycznej aktualizacji bazy wirusów, rootkitów, spam-u, malwar-u, itp. oraz silnika wyszukiwującego. Raz na tydzień w porze nocnej powinno zostać przeprowadzone pełne skanowanie systemu. Wykonawca ma



obowiązek zapewnić aktualną licencję na to oprogramowanie przez cały okres trwania Kontraktu oraz Okres Gwarancji.

System musi posiadać oprogramowanie diagnozujące prawidłowość działania urządzeń systemu. Aplikacja monitorująca wszystkie urządzenia sieciowe i serwerowe będzie mierzyła co najmniej takie parametry jak: wykorzystanie procesora, pamięci i dysku, procesy, usługi, a także wykorzystanie sieci. W razie wykrycia usterek musi istnieć możliwość wysyłania wiadomości e-mail do listy mailingowej (pojedynczych adresów lub grup adresów) informujących o nieprawidłowościach w działaniu Systemu. Zakres adresów na które będą wysyłane powiadomienia oraz zakres usterek, które będą podlegać procedurze informowania (per adres lub grupa adresów) mają być w pełni modyfikowalne przez administratora Systemu ze strony Zamawiającego.

10 PROTOKOŁY WYMIANY DANYCH

10.1 Wymagania ogólne

W celu zapewnienia dalszej rozbudowy systemu, obszarowej, ilościowej, jakościowej i funkcjonalnej, w drodze współpracy z różnymi dostawcami Zamawiający oczekuje, że proponowany przez Wykonawcę system będzie jak najbardziej otwarty, w szczególności poprzez zastosowanie odpowiednich interfejsów.

Zamawiający wymaga, aby budowa systemu w jak najszerszym stopniu uwzględniała standardy otwarte tak jak to rozumie Komisja Europejska w dokumencie „European Interoperability Framework for Paneuropean Government services” z 2004 roku.

W zakresie protokołów komunikacji modelem odniesienia jest model OSI (Open System Interconnection) zdefiniowany przez ISO oraz ITU-T opisujący strukturę komunikacji sieciowej jak niżej:

Warstwa odniesienia w modelu OSI	Wymagane protokoły dla Systemu
Warstwa aplikacji	XML lub HTML – dla struktury przesyłanych danych. W zastosowaniach, gdzie prędkość transmisji danych odgrywa ważną rolę, dopuszcza się inne metody (np. pliki tekstowe lub binarne). Warunkiem jest przekazanie pełnego opisu struktury protokołu i przesyłanych za jego pomocą danych.
Warstwa prezentacji	kodowanie ASCII lub Unicode – dla danych znakowych, RTF lub PDF – dla danych blokowych, JPEG, PNG lub BMP – dla obrazów, MPEG2, MPEG4 lub SEQ – dla materiału video, MP3 lub Ogg – dla materiałów audio (lub innego zgodnego z zaleceniem UE)
Warstwa sesji	JMS lub kompatybilny z JMS (lub innego zgodnego z zaleceniem UE)
Warstwa transportowa	TCP lub UDP (lub innego zgodnego z zaleceniem UE)
Warstwa sieciowa	IP (lub innego zgodnego z zaleceniem UE)
Warstwa łącza danych	IEEE 802.3z 1000Base-LX lub RS-232 lub RS-485 (lub innego zgodnego z zaleceniem UE)
Warstwa fizyczna	technologie dostępne nie będące w sprzeczności z wymaganiami dla warstw wyższych

10.2 Wymagania formalne

Wszelkie opracowywane i wykorzystywane protokoły wymiany danych powinny być przedstawione przez Wykonawcę do akceptacji przez Zamawiającego. Do prośby o akceptację

powinna zostać przekazana dokumentacja techniczna umożliwiająca stwierdzenie przez Zamawiającego jaką funkcjonalność posiada przedstawiany protokół.

10.3 Warunki szczegółowe

Licencja na protokół transmisji danych może być przedstawiona w dwóch wersjach:

- jako protokół otwarty do wykorzystania przez każdego producenta podobnych urządzeń lub
- jako protokół zamknięty, którego producent udostępni całą jego specyfikację do dowolnego wykorzystania przez Zamawiającego na potrzeby miasta Krakowa.

Jeśli w stosowanym protokole istnieje możliwość stosowania dodatkowych pól definiowanych przez producenta urządzenia, i producent korzysta z tej możliwości, wszystkie dodatkowe pola należy wyspecyfikować i podać format danych jakie są nimi przesyłane wraz z opisem czego one dotyczą.

Wszystkie wykorzystywane pola w używanym protokole mają być jasno opisane jakie wartości przechowują oraz do czego są wykorzystywane przesyłane nimi dane. Dokumentacja protokołu może być stworzona przez twórców protokołu lub przez Wykonawcę.

10.4 Wymaganie otwartości systemów

Wykonawca zagwarantuje, że w trakcie trwania kontraktu, a także w okresie gwarancji Zamawiający będzie miał prawo podłączenia do systemu dowolnego nowego źródła danych, który zostanie uznany przez Zamawiającego za zgodny z wykorzystywanymi przez ten system protokołami przesyłania danych. Podłączenie takiego źródła nie będzie powodowało utraty gwarancji.

Jeśli Wykonawca dostarcza oprogramowanie, które powinno być zintegrowane z wykorzystywanymi obecnie przez Zamawiającego systemami lub w jakikolwiek sposób powinno z nim współpracować a nie jest ich modulem programowym, wykorzysta do komunikacji pomiędzy dostarczonym systemem a systemami zewnętrznymi protokoły danych nowe lub obecnie istniejące. Dokumentacja tych protokołów ma zostać przekazana do Zamawiającego. Strony implementujące protokoły zostały opisane w rozdziale 2.

11 INFORMACJE I WYMAGANIA DODATKOWE

Dokumenty, raporty, korespondencja w ramach Kontraktu będzie prowadzona w języku polskim w formie papierowej i elektronicznej. Standardem w korespondencji będzie pakiet MS Office 2007 lub 2010, do opracowania harmonogramów będzie służył MS Project (Wykonawca może zaproponować inny program o takich samych funkcjonalnościach), do opracowywania rysunków zalecany Corel Draw.

Dokumenty, dokumentacje i korespondencje winny być opatrywane logotypem wg wzoru przekazanego przez Zamawiającego.

Zamawiający przekaże do stosowania wzory wszystkich wymaganych raportów z postępu i stanu realizacji prac, raportów inspekcyjnych, protokołów odbiorów częściowych i końcowego, protokołów Prób Eksploatacyjnych oraz innych dokumentów mających być w użyciu w ramach realizacji Projektu.

Przez cały czas trwania gwarancji, Wykonawca będzie usuwał wszelkie wady i wymieniał części, które uległy uszkodzeniu z przyczyn innych niż nieprawidłowe obchodzenie się lub niewłaściwe użytkowanie, w terminie maksymalne 24 godzin licząc od czasu zgłoszenia konieczności takiej naprawy lub wymiany.

Wykonawca przedstawi listę części zamiennych jakie dostarczy. Lista ma obejmować taki zakres części i ilości, aby zapewnić stałą gotowość operacyjną zabudowywanych przez niego urządzeń, z uwzględnieniem średniego czasu do naprawy oraz czasu koniecznego do uzupełnienia składowanych części.

Na podstawie ww. listy Wykonawca dostarczy Zamawiającemu partię części zamiennych w ilości zapewniającej uzyskanie ww. gotowości operacyjnej. W dostarczanej partii części zamiennych powinny się znaleźć przynajmniej po jednej sztuce z każdego elementu wymienionego w tej liście.

W trakcie trwania Kontraktu oraz w przez cały okres trwania gwarancji Wykonawca będzie przekazywał całą wiedzę dotyczącą dostarczanego systemu, jego poszczególnych komponentów oraz odpowiadał na wszystkie techniczne pytania na powyższe tematy zadawane przez pracowników Zamawiającego w sposób pełny i wyczerpujący.



12 OBOWIĄZKI WYKONAWCY

Wykonawca winien:

- wykonywać swoje obowiązki i uprawnienia za pomocą personelu posiadającego odpowiednią wiedzę i doświadczenie w zagadnieniach związanych z realizacją Kontraktu, jak również, w przypadku gdy prawo tego wymaga, posiadających stosowane uprawnienia, zezwolenia itd.; rozpocząć, realizować i zakończyć Kontrakt zgodnie z Warunkami Kontraktowymi zawartymi w Umowie z Zamawiającym.
- aktywnie i kompetentnie działać na rzecz realizacji Kontraktu, przestrzegając wszelkich przepisów prawa, mających zastosowanie przy jego realizacji, w sposób bezpieczny dla ludzi i środowiska.