Załącznik nr 1_I_do IPU

SPECYFIKACJA TECHNICZNA

CZĘŚĆ I

Zakup usług transmisji danych na potrzeby obsługi systemów informatycznych, zapewnienia dostępu do centralnych i lokalnych baz danych oraz świadczenie usług video dla jednostek Prokuratur i Sądów Apelacyjnych, w tym obsługę systemów Biura do Spraw Przestępczości Zorganizowanej i Systemu Informatycznego Schengen dla Sądów – SIS-SAD i innych wskazanych jednostek (Użytkowników) Ministerstwa Sprawiedliwości

Objaśnienia użytych skrótów:

Lp.	*skrót*	*opis*
1.	BPZ	Biuro do Spraw Przestępczości Zorganizowanej
2.	Centrala BPZ	Telekomunikacyjny centralny węzeł dostępowy Biura ds. Przestępczości Zorganizowanej
3.	CRZ	Centralny Rejestr Zastawów
4.	KRS	Krajowy Rejestr Sądowy
5.	MS	Ministerstwo Sprawiedliwości
6.	NKW	Nowa Księga Wieczysta
7.	PA	Prokuratura Apelacyjna
8.	PO	Prokuratura Okręgowa
9.	POPD	Podstawowy Ośrodek Przetwarzania Danych MS
10.	PR	Prokuratura Rejonowa
11.	SA	Sąd Apelacyjny
12.	SIP	System Informatyczny Prokuratury
13.	SO	Sąd Okręgowy
14.	SR	Sąd Rejonowy
15.	WPZ	Wydział Zamiejscowy BPZ
16.	ZOPD	Zapasowy Ośrodek Przetwarzania Danych MS
17.	ACL	Access Control List
18.	AV	Antyvirus
19.	BGP	Brder Gateway Protocol
20.	CPE	Customer Provider Equipment
21.	DSL	Digital Subscriber Line
22.	EIGRP	Enhanced Interior Gateway Routing Protocol
23.	full-mesh	Sieć kratowa dla połączeń punkt-punkt z redundancją
24.	HDLC	High-Level Data Link Control
25.	HSDPA	High Speed Downlink Packet Access
26.	IPS/IDS	Intrusion Prevention Systems/Intrusion Detection Systems
27.	IPSec	Protokół bezpiecznej komunikacji IP
28.	ISO/OSI	Open System Interconnection
29.	łącze TD	Łącze teletransmisji danych
30.	OSPF	Open Shortest Path First
31.	P2P	peer-to-peer

32.	PE	Provider Edge Router
33.	PPP	Point to Point Protocol
34.	PPP Multilink	Rozszerzenie Point-to-Point
35.	QoS	Quality of Service
36.	RIPv2	Routing Information Protocol v2
37.	SDH/PDH	Synchronous Digital Hierarchy/Plesiochronous Digital Hierarchy
38.	SLA	Service Level Agreement
39.	SSL	Secure Socket Layer VPN
40.	SSL	Secure Socket Layer
41.	VLAN	Virtual Local Area Network
42.	VoIP	Voice over IP
43.	VPN	Virtual Private Network
44.	VRF	Virtual Routing and Forwarding

Spis treści:

I. Definicje 2
II. Przedmiot zamówienia: 4
III. Zakres świadczonych usług 8
IV. Struktura fizyczna sieci 12
V. Struktura logiczna sieci 14
VI. Bezpieczeństwo 15

I. Definicje

Użytkownik - Zamawiający i jednostki Zamawiającego wskazane w Załącznikach nr 1,2,3,4, cz. I do IPU oraz inne jednostki, którym uprawnienia do korzystania z usługi transmisji danych zostaną nadane przez Zamawiającego,

Łącze dostępowe - łącze transmisji danych, które pozwala na połączenie lokalizacji Zamawiającego z węzłem dostępowym sieci transmisji danych Wykonawcy. Łącze to musi być zakończone w każdej lokalizacji Zamawiającego urządzeniem dostępowym (CE) oraz ewentualnie innymi urządzeniami niezbędnymi do realizacji łącza (np.: modemy kablowe, multipleksery, urządzenia IDU, itp.),

Urządzenie dostępowe (CE) – urządzenie w lokalizacji Zamawiającego, dostarczone, zainstalowane we wskazanym przez Zamawiającego miejscu i zarządzane przez Wykonawcę. Urządzenie to stanowi zakończenie łącza dostępowego oraz udostępnia interfejs przyłączeniowy lub interfejsy przyłączeniowe zapewniające podłączenie do sieci VPN urządzeń i sieci Zamawiającego,

Interfejs przyłączeniowy - interfejs w standardzie FastEthernet 10/100 (Eth 10/100) lub GigabitEthernet 10/100/1000 (Eth 10/100/1000) zlokalizowany w urządzeniu dostępowym CE, za pomocą którego Użytkownik w danej placówce ma dostęp do usługi transmisji danych VPN. Interfejs przyłączeniowy w urządzeniu dostępowym CE

jest punktem, w którym świadczona jest usługa transmisji danych VPN o zdefiniowanych przez Zamawiającego parametrach,

Router PE – router brzegowy sieci Wykonawcy umieszczony w węźle sieci Wykonawcy, do którego dołączone jest urządzenie dostępowe (CE) za pomocą łącza dostępowego,

CoS - *(ang. Class of Service)* - zdefiniowana przez Wykonawcę usługa podziału ruchu wg. priorytetu,

IP - *(ang. Internet Protocol*) - protokół transmisji danych używany przez systemy informatyczne,

LAN - *(ang. Local Area Network)* - lokalna sieć transmisji danych obejmująca swym zasięgiem pojedynczą jednostkę Zamawiającego,

Lokalizacja — adres siedziby Zamawiającego, w tym wyznaczone pomieszczenie znajdujące się w siedzibie Zamawiającego, do którego Zamawiającemu przysługuje tytuł prawny, a w którym są zainstalowane urządzenia aktywne oraz będzie instalowane urządzenie dostępowe CE wraz z zakończeniem łącza dostępowego,

Okno serwisowe - przedział czasu przeznaczony na wykonywanie prac konserwacyjno-modernizacyjnych w sieci Wykonawcy mogących skutkować brakiem dostępu Zamawiającego do usługi transmisji danych IP VPN,

Pasmo transmisyjne IP - dostępna dla Zamawiającego przepustowość łącza wyrażona w kbps lub Mbps określająca szybkość przesyłania danych w ramach świadczonej usługi transmisji danych VPN,

QoS - *(ang. Quality of Service)* - parametry definiujące wymagania jakościowe względem łączy telekomunikacyjnych realizowane przez: kształtowanie ruchu, ograniczanie przepustowości, nadawanie priorytetów, zarządzanie parametrami jakościowymi, unikanie natłoku w sieci, itp.,

SLA — *(ang. Service Level Agreement)* - parametry określające niezawodność i jakość usługi transmisji danych VPN określone w Umowie z Wykonawcą,

Usługa IP VPN - usługa transmisji danych świadczona przez Wykonawcę gwarantująca logiczną separację ruchu danych od innych klientów Wykonawcy na poziomie warstwy 3 modelu ISO/OSI oraz zapewniająca możliwość połączeń typu „każdy z każdym" (ang. *full mesh),*

Brak dostępności usługi - przerwa w świadczeniu usługi (brak połączenia z użytkownikiem Zamawiającego) liczona od momentu wykrycia przez Stanowisko Monitorowania i zgłoszenia jej braku przez Zamawiającego do Biura Obsługi Klienta (BOK) lub wykrycia obniżenia parametrów usługi poniżej wartości określonych w umowie jako „Parametry SLA" tj. obniżenia przepustowości łącza poniżej wartości nominalnej a kończąca się w momencie przywrócenia usługi. Przerwy w dostarczaniu usługi spowodowane koniecznością wykonania prac konserwacyjno - modernizacyjnych (okna serwisowe) w sieci Wykonawcy w terminach ustalonych w umowie, Zamawiający traktuje jako zachowanie ciągłości usługi,

WAN - *(ang. Wide Area Network*) - rozległa sieć transmisji danych Wykonawcy obejmująca swym zasięgiem wszystkich, zdefiniowanych Umową Użytkowników Zamawiającego,

VPN - *(ang. Virtual Private Network)* - struktura logiczna sieci kreowana w ramach fizycznej infrastruktury sieci rozległej Wykonawcy, zapewniająca możliwości zestawiania połączeń pomiędzy użytkownikami sieci transmisji danych w warstwie trzeciej modelu OSI,

„IP VPN – **CENTRALA"** - sieć transmisji danych pozwalająca na połączenie rozproszonych geograficznie jednostek Zamawiającego zgodnie z wymaganiami określonymi w SIWZ.

II. Przedmiot zamówienia:

1. Zakup usług transmisji danych dla zabezpieczenia wymiany danych i transmisji video dla obsługi informatycznej jednostek organizacyjnych resortu sprawiedliwości:
   1) zestawienie i uruchomienie zabudowanych urządzeniami aktywnymi trzech Centralnych Telekomunikacyjnych Węzłów Dostępowych MS w lokalizacjach POPD, ZOPD oraz Centrali BPZ Zamawiającego,
   2) zestawienie, uruchomienie zabudowanych urządzeniami aktywnymi łączy dostępowych i włączenie w system wymiany danych 11 Prokuratur Apelacyjnych lub innych odpowiadających im jednostek organizacyjnych,
   3) zestawienie, uruchomienie zabudowanych urządzeniami aktywnymi łączy dostępowych i włączenie w system wymiany danych 11 Sądów Apelacyjnych,
   4) zestawienie, uruchomienie zabudowanych urządzeniami aktywnymi łączy dostępowych i włączenie w system wymiany danych 11 Wydziałów Zamiejscowych Biura do Spraw Przestępczości Zorganizowanej,
   5) zestawienie, uruchomienie zabudowanych urządzeniami aktywnymi łączy dostępowych i włączenie w system wymiany danych 9 jednostek Centralnych Ministerstwa Sprawiedliwości,

   i zapewnienie przez okres 32 miesięcy od daty odbioru zestawionych i uruchomionych łączy dostępowych do wszystkich jednostek oraz świadczenie usług transmisji danych w oparciu o zestawione wirtualne sieci dedykowane IP VPN - „VPN CENTRALA". Wykaz lokalizacji Użytkowników zawierający adres miejsca instalacji (zakończenia łącza), wymagania na pasmo transmisyjne, zamieszczono w załącznikach do specyfikacji technicznej cz. I _do IPU:

   - zał. nr 1 cz. I - zestawienie jednostek Prokuratur Apelacyjnych
   - zał. nr 2 cz. I - zestawienie jednostek Sądów Apelacyjnych
   - zał. nr 3 cz. I - zestawienie jednostek Biura do Spraw Przestępczości Zorganizowanej
   - zał. nr 4 cz. I - zestawienie jednostek Centralnych MS.
   - zał. nr 5 cz. I – urządzenie_bezpieczeństwa dla IP VPN Centrala_specyfikacja techniczno-funkcjonalna
   - zał. nr 6 cz. I – plan adresacji IP dla Sądów i Prokuratur Apelacyjnych
   - zał. nr 7 cz. I – urządzenie_bezpieczeństwa dla BPZ_specyfikacja techniczno-funkcjonalna

2. Zamawiający wymaga zapewnienia usług transmisji danych w oparciu o wykreowane wirtualne sieci dedykowane transmisji danych IP VPN, zestawiane w zasobach technicznych operatora telekomunikacyjnego/dostawcy usługi transmisji danych dla zabezpieczenia wymiany danych drogą elektroniczną pomiędzy jednostkami organizacyjnymi resortu oraz świadczenia usług poprzez zestawienie, uruchomienie i wdrożenie rozwiązania polegającego na:

   1) na poziomie Centrali MS (VPN CENTRALA) – organizacji, budowie i uruchomieniu 2 telekomunikacyjnych centralnych węzłów dostępowych (POPD/ZOPD) zabezpieczonych urządzeniami bezpieczeństwa teleinformatycznego i zestawienie w sieci IP VPN dostawcy 22 zabudowanych urządzeniami aktywnymi łączy dostępowych do wszystkich Prokuratur i Sądów Apelacyjnych oraz 9 jednostek centralnych MS,

   2) organizacji, budowie i uruchomieniu węzła dostępowego w Centrali Biura do Spraw Przestępczości Zorganizowanej w lokalizacji Warszawa Al. Ujazdowskie 11 zabezpieczonego urządzeniem bezpieczeństwa teleinformatycznego i wykreowanie IP VPN PZ w oparciu o zestawione w sieci Operatora – Dostawcy usług 11 relacji łączności do wszystkich Wydziałów Zamiejscowych Biura do Spraw Przestępczości Zorganizowanej zlokalizowanych w 11 Prokuraturach Apelacyjnych,

   3) zapewnieniu styku telekomunikacyjnego pomiędzy VPN CENTRALA a 22 VPN APELACJA (SĄDOWA/PROKURATORSKA) z wykorzystaniem dynamicznego protokołu routing'u i na wniosek Zamawiającego połączenie sieci IP VPN Centrala - IP VPN Apelacja, po uruchomieniu infrastruktury sieciowej zamawianej lokalnie.

   4) w każdym węźle (IP VPN APELACJA) przewiduje się instalację pary routerów i urządzenia bezpieczeństwa: router CE i urządzenie bezpieczeństwa operatora lokalnego oraz routera CE dostarczanego przez dostawcę usługi VPN CENTRALA będącego przedmiotem niniejszego zamówienia,

   5) router CE stanowiący węzeł dostępowy IP VPN APELACJA oraz urządzenie bezpieczeństwa instalowane na węźle IP VPN APELACJA nie są objęte przedmiotem niniejszego zamówienia,

   6) w ramach usług w sieci transmisji danych Zamawiającego zbudowanej na bazie sieci IP VPN Wykonawcy muszą istnieć możliwości pozwalające na:
      a) konfigurację topologii sieci w funkcji rodzaju klasy ruchowej (np. dla klasy ruchowej typu DATA czy VoIP powinna być możliwość skonfigurowania struktury każdy-z-każdym, tak aby połączenia były nawiązywane bezpośrednio pomiędzy lokalizacjami Zamawiającego,
      b) wykonanie konfiguracji urządzenia dostępowego CE z uwzględnieniem co najmniej następujących elementów, przy założeniu że docelowo zakres świadczonych usług będzie obejmować nowe lokalizacje, które będą łączone poprzez sieci IP VPN innych wykonawców (Operatora IP VPN APELACJA) w ramach innych zamówień:
         i. mapa z kierunku od Operatora IP VPN APELACJA do Wykonawcy przedmiotu zamówienia,
         ii. mapa w kierunku do Operatora IP VPN APELACJA,
         iii. informacja dla protokołu BGP o konieczności transmitowania informacji community,

iv. oznaczenie na wejściu z routera CE Operatora IP VPN APELACJA ścieżki BGP odpowiednim community (tak aby prefixy, które się klasyfikują na to community były wysłane w kierunku do CE Operatora IP VPN APELACJA, a pozostałe prefixy skasowane),
v. zastosowanie mechanizmów: prefix-list w route-mapach, ACL, distribute-list,

c) zmianę przynależności danej jednostki organizacyjnej MS do określonej innej grupy jednostek (lokalizacji).

3. Prezentację graficzną podłączenia poszczególnych Użytkowników (lokalizacji) MS do sieci IP VPN Wykonawcy przedstawiono na rys. nr 1 Specyfikacji Technicznej – Część I.

4. Dostarczenie i udostępnienie w siedzibie Zamawiającego (POPD) stanowiska monitorowania i weryfikacji jakości świadczonych usług w zakresie podstawowych parametrów sieciowych przez służby informatyczne Zamawiającego wraz z niezbędnym oprogramowaniem umożliwiającym:

1. monitorowanie parametrów SLA dla całej sieci WAN, w szczególności parametrów łączy dostępowych, gwarantowanej przepustowości i obciążenia łączy, z poziomu jednej konsoli monitorującej;
2. automatyczne odkrywanie urządzeń znajdujących się w monitorowanej sieci i dodawanie ich do bazy urządzeń podlegających monitorowaniu;
3. graficzna wizualizacja odpowiedzi monitorowanych urządzeń na pakiety ICMP, ECHO wysyłane przez stację monitorującą;
4. dynamiczne (w czasie rzeczywistym),graficzne wyświetlanie mapy logicznej i fizycznej topologii sieci (z routerem w każdej lokalizacji włącznie);
5. monitorowanie w czasie rzeczywistym (uwzględniając prędkość sieci komputerowej i częstotliwość odpytywania) parametrów pracy urządzeń sieciowych;
6. testowanie poprawności zdalnych połączeń;
7. gromadzenie bieżących parametrów pracy monitorowanych urządzeń sieciowych dzięki wykorzystaniu protokołu SNMP oraz graficzna wizualizacja całej topologii sieci na podstawie zgromadzonych danych;
8. graficzna prezentacja zebranych danych w postaci wykresów tygodniowych, miesięcznych, rocznych;
9. generowanie komunikatów w wyniku zdarzeń i symptomów potencjalnych zagrożeń oraz reagowanie na nie za pomocą zdefiniowanych przez użytkownika akcji takich jak wysłanie powiadomienia poprzez email lub SMS, wysłanie trapów SNMP lub uruchomienie lokalnego/zdalnego programu lub skryptu.

Stanowisko monitorowania powinno zawierać:

1) odpowiednio do tego celu wyposażoną jednostkę centralną w następującej konfiguracji:

- procesor typu x86 wielordzeniowy, SSE3, z technologią obsługi wielowątkowości
- płyta główna Internal bus FSB 1066 MHz, BIOS type FLASH EPROM z

procedurą energy saving oraz plug & play, zgodna z normą Energy Star, wyposażona w porty 1x RS232, 1xCentronics, klawiatury PS/2, myszy PS/2, 8xUSB 2.0 w tym min 2 x USB 2.0 na przednim panelu komputera oraz w sloty 1xPCI Express 16, 1x PCI Express 1, 3 PCI, Ethernet 10/100/1000Mb/s Base TX Wake-On-LAN - karta zintegrowana z płytą główną, zintegrowana karta dźwiekowa

- pamięć 2 GB RAM DDR2 800 MHz, z możliwością rozszerzenia do 4 GB, dwa wolne sloty po zainstalowaniu 2 GB, 4 złącza DIMM.
- 2 szt. dysków twardych o pojemności min. 500 GB każdy, 7200rpm SATA II 16 MB cache NCQ,
- oprogramowanie MS Windows XP Profesional PL lub równoważne, na oddzielnym nośniku CD, bez konieczności aktywowania przez Internet lub telefon
- napęd optyczny DVD-R/RW, nagrywanie płyt dwuwarstwowych z oprogramowaniem do nagrywania płyt CD i DVD,
- Karta graficzna PCI Express z pamięcią 512 MB RAM wyposażoną w złącza DSUB oraz DVI, rozdzielczość 1600x1200@85 Hz,
- monitor LCD 20" aktywna matryca TFT, kąt widzenia min. 160/160 stopni, jasność 300 cd/m2, kontrast 700:1, średni czas reakcji 8 ms, matryca min. 1600x1200@85 Hz, plamka 0,294 mmm, wejście analogowe VGA, wejście cyfrowe DVI wraz z kablami analogowym i cyfrowym umożliwiającym podłączenie monitora do oferowanego komputera, polskie menu, zintegrowane głośniki i zasilacz. Certyfikaty: TCO-03,możliwość zamontowania na ścianie, wraz ze wszystkimi elementami niezbędnymi do montażu na każdym rodzaju powierzchni,monitor zgodny z normą Energy Star
- Możliwość zainstalowania dodatkowych dysków twardych wewnątrz obudowy.
- Obudowa typu tower, powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzającym komputerem, zasilacz min 315 W.
- Wszystkie niezbędne przewody do podłączenia i poprawnej pracy komputera, kabel łączący komputer z gniazdkiem UTP (linka) o długości 3m kat. 5, wszystkie niezbędne i aktualne sterowniki i Service Pack-i do zainstalowanych urządzeń na oddzielnych nośnikach CD, instrukcja obsługi komputera w języku polskim, filtr przeciwzakłóceniowy (min. 5 gniazd elektrycznych i długości przewodu zasilającego 3 metry)
- Zdalny upgrade BIOS komputera –przez Internet lub za pomocą fabrycznego oprogramowania.
- Możliwość zabronienia zapisu na dyskietkę-funkcja w BIOS-ie komputera.
- Możliwość blokowania portów wejścia/ wyjścia- funkcja w BIOS-ie komputera.
- Wszystkie niezbędne elementy do prawidłowej pracy stacji roboczej
- Oprogramowanie pozwalające na zarządzanie komputerem w sieci oraz umożliwiające min. na:
  automatyczną rejestrację i informowanie o następujących parametrach:
  -temperatura procesora,
  -zdalne zablokowanie stacji dysków, portów szeregowych i równoległych,
  -zdalną konfigurację i uaktualnienia BIOS-u [Update BIOS],zdalne wyłączanie komputera w sieci,
  -zdalny restart komputera w sieci,
  -realizowanie funkcji Wake On LAN [WOL],
  -otrzymywanie informacji WMI [Windows Management Instrumentation],
  - kontrola czujnika otwarcia obudowy.

Ww. oprogramowanie musi być przeznaczone dla oferowanej jednostki centralnej komputera i być oznaczone logiem jej producenta.

- Komputer musi posiadać diody kontrolne służące do sygnalizowania i diagnozowania stanu pracy komputera oraz problemów z komputerem.
- Głośność jednostki centralnej w/g normy ISO 9296 (bez nośników maks. 33 dB).
- Wsparcie techniczne producenta-dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera
- Komputer powinien posiadać następujące certyfikaty:
  - Certyfikat Microsoft w zakresie kompatybilności z systemami Windows XP lub równoważny
  - Obecność produktu na Microsoft Hardware Compatibility List lub równoważny
  - Certyfikat ISO 9001:2000 na cały proces produkcji lub równoważny
  - Certyfikat ISO 1400 lub równoważny
  - Deklaracja zgodności CE
- klawiatura, mysz optyczna z odpowiednią podkładką.

Zakres prac po stronie Wykonawcy:

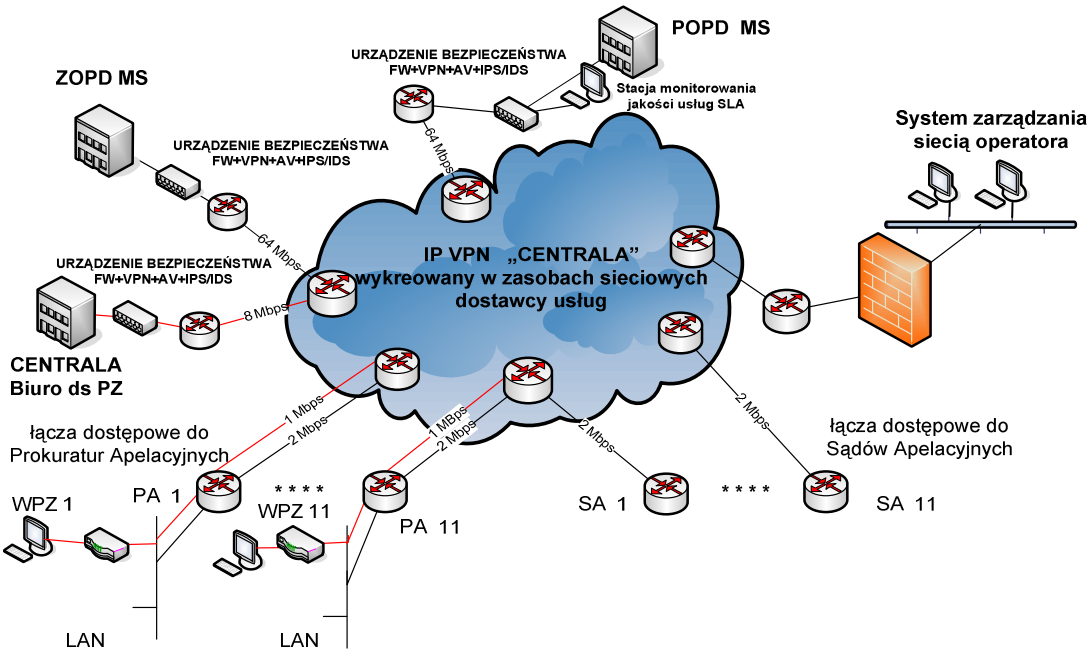
1. pierwszy dysk twardy podzielony na dwie partycje w stosunku 1/3 do 2/3
2. Instalacja i konfiguracja systemu operacyjnego MS Windows XP Professional PL z aktualnymi w momencie dostawy, dostarczonymi od producenta sterownikami urządzeń**,** Service Packami i poprawkami do systemu operacyjnego, system powinien być aktywowany.
4.Instalacja oprogramowania do nagrywania płyt CD i DVD.

2) zainstalowane oprogramowanie specjalistyczne przeznaczone do monitorowania jakości usług transmisji danych świadczonych przez Wykonawcę.

III. Zakres świadczonych usług

Zamawiający wymaga by zamawiane usługi obejmowały:

1. Dostawę urządzeń i uruchomienie telekomunikacyjnych węzłów dostępowych w trzech lokalizacjach centralnych Zamawiającego – POPD, ZOPD i Centrala BPZ (każdy węzeł wyposażony w router i urządzenie bezpieczeństwa), oraz urządzeń dostępowych we wszystkich wyspecyfikowanych w zał. 1, 2, 3, 4 cz. I_do IPU, lokalizacjach zdalnych. Wszystkie urządzenia muszą być dostarczone, zainstalowane i uruchomione przez Wykonawcę i są jego własnością w okresie świadczenia usług i po ich zakończeniu.



Rozwiązanie IP VPN CENTRALA z dołączonymi węzłami dostępowymi Prokuratur i Sądów Apelacyjnych

2. Dla realizacji powyższego Wykonawca musi zestawić 22 łącza dostępowe zabudowane urządzeniami sieciowymi do 11 Prokuratur Apelacyjnych i 11 Sądów Apelacyjnych Zamawiającego oraz do 9 jednostek centralnych Zamawiającego. W ramach oferowanej usługi Wykonawca zobowiązany jest do instalacji i uruchomienia łączy dostępowych do wszystkich Prokuratur i Sądów Apelacyjnych o przepustowości gwarantowanej 2 Mbps każde, oraz:

   1) zapewnienia kompleksowego rozwiązania IP VPN w ramach udostępnianej sieci telekomunikacyjnej umożliwiającego połączenie rozproszonych geograficznie 22 jednostek organizacyjnych resortu sprawiedliwości - Apelacji w jedną wydzieloną bezpieczną sieć transmisji danych,

   2) wszystkie urządzenia dostępowe w lokalizacjach zdalnych powinny komunikować się z routerami zainstalowanymi w lokalizacjach centralnych Zamawiającego POPD i ZOPD a jednostki zamiejscowe Biura do Spraw Przestępczości Zorganizowanej z Centralą BPZ,

   3) skonfigurowania na routerach usługowych operatora tablic VRF (VPN Routing Forwarding) oddzielnie dla każdej z jednostek. Informacje sieciowe dotyczące każdego z VPN-ów powinny być przechowywane w oddzielnych tablicach routingowych VRF na routerach Wykonawcy,

   4) docelowo, umożliwić konfigurację wydzielonych podsieci TD pozwalających na wymianę danych z wykorzystaniem IP VPN w relacjach węzły dostępowe VPN CENTRALA - wszystkie węzły dostępowe jednostek podległych poszczególnym apelacjom na terenie kraju oraz zestawienie połączeń dla obsługi centralnych systemów informatycznych (System Informatyczny Prokuratur - SIP, System Informatyczny Schengen dla jednostek organizacyjnych Prokuratury - SIS-SIP oraz System Informatyczny Schengen dla Sądów - SIS-SAD) oraz zapewnić dostęp ich użytkownikom do centralnych baz danych z wykorzystaniem łączy połączonych struktur sieciowych VPN APELACJA – VPN CENTRALA. W ramach lokalizacji POPD,

ZOPD oraz węzła centralnego BPZ zostaną wskazane po stronie sieci lokalnych zasoby teleinformatyczne, w tym zasoby bazodanowe, z których każdy będzie przypisany do właściwej podsieci VPN (VPN_S lub VPN_P i VPN_BPZ). Zakres uprawnień w dostępie do zasobów teleinformatycznych po stronie lokalizacji POPD, ZOPD oraz węzła centralnego BPZ dla każdej sieci VPN (do poziomu pojedynczej lokalizacji wchodzącej w skład danej sieci VPN) zostanie zdefiniowany przez Zamawiającego na etapie uruchamiania usługi,

5) zapewnienia bezpieczeństwa teleinformatycznego i ochrony transmisji z wykorzystaniem urządzeń bezpieczeństwa sieciowego, uruchomionych w węzłach telekomunikacyjnych VPN CENTRALA (POPD, ZOPD, Centrala BPZ) realizujących kontrolę dostępu (firewall), poufność danych (IPsec VPN oraz SSL VPN), ochronę przed atakami (IPS/IDS), kontrolę pasma oraz ruchu (QoS i Traffic Shaping) oraz kontrolę komunikatów sieciowych (IM oraz aplikacji P2P). Wykonawca dostarczy, zainstaluje, uruchomi urządzenia oraz uruchomi i utrzyma system bezpieczeństwa teleinformatycznego w udostępnionej strukturze sieciowej w lokalizacjach POPD, ZOPD i Centrala BPZ. Specyfikację techniczną urządzenia bezpieczeństwa zamieszczono w zał. nr 5 cz. I_do IPU. Wykonawca zapewni Zamawiającemu zdalne przeglądanie pełnej konfiguracji urządzeń bezpieczeństwa.

6) świadczenie usług zarządzania i administrowania urządzeniami CE w trakcie obowiązywania umowy obejmujące:
   a) zdalne zarządzanie konfiguracją logiczną sieci oraz utrzymanie urządzeń CE,
   b) zmiany konfiguracji urządzeń CE na wniosek Zamawiającego,
   c) naprawę lub wymianę uszkodzonego urządzenia CE,
   d) rozwiązywanie problemów eksploatacyjnych przy pomocy Help Desk,
   e) zapewnienie Zamawiającemu zdalnego przeglądania pełnej konfiguracji urządzeń CE zainstalowanych we wszystkich lokalizacjach Zamawiającego.

3. Przyjęte rozwiązanie musi udostępniać następujący zakres usług, parametry techniczne transmisji danych i parametry SLA na poziomie VPN CENTRALA:

1) Wykreowanie IP VPN łączących wszystkie prokuratury i sądy apelacyjne z Podstawowym Ośrodkiem Przetwarzania Danych - POPD i Zapasowym Ośrodkiem Przetwarzania Danych - ZOPD Zamawiającego oraz zapewnienie dostępu do sieci wszystkim jednostkom organizacyjnym MS wyspecyfikowanym w zał. 1, 2 cz. I_do IPU z przepustowością gwarantowaną łączy dostępowych na poziomie 2 Mbps,

2) wykreowanie IP VPN łączącego wszystkie Wydziały Zamiejscowe Biura do Spraw Przestępczości Zorganizowanej z węzłem telekomunikacyjnym Centrala MS WPZ oraz zapewnienie dostępu do sieci wszystkim jednostkom wyspecyfikowanym w zał. 3 cz. I_do IPU z przepustowością łączy dostępowych na poziomie 1 Mbps, w ramach 2 Mbps łączy dostępowych zestawionych do Prokuratur Apelacyjnych,

3) zapewnienie dostępu do sieci wszystkim jednostkom centralnym MS wyspecyfikowanym w zał. 4 cz. I_do IPU z przepustowością łączy dostępowych na poziomie 2 Mbps,

4) Zamawiający wymaga, by na etapie realizacji zamówienia przepustowość łączy dostępowych do POPD i ZOPD wynosiła min 64 Mbps z możliwością zwiększenia do 155 Mbps (STM1),

5) jednocześnie Zamawiający określa przepustowość łącza dostępowego do Centrali BPZ na poziomie 8 Mbps,

6) Zamawiający wymaga zapewnienia następujących, minimalnych parametrów usług SLA, w ramach świadczenia usług w sieci IP VPN w relacjach end-to-end:
   a) gwarancja przepustowości na poziomie 100% dostarczonego pasma,
   b) dostępność usługi na poziomie co najmniej:
      i. 99,5% miesięcznie,
      ii. 99,7% rocznie;
   c) czas reakcji na awarię nie dłużej niż 30 minut, liczonych od godziny zgłoszenia
   d) czas usunięcia awarii nie dłużej niż:
      i. dla lokalizacji POPD, ZOPD oraz węzła Centrala BPZ - 4 godziny, liczone od godziny zgłoszenia awarii
      ii. dla pozostałych lokalizacji - 12 godzin, liczonych od godziny zgłoszenia awarii
   e) opóźnienie pakietów dla ruchu typu DATA_1 nie więcej niż 90ms,
   f) utrata pakietów dla ruchu typu DATA_1 nie więcej niż 0,2%,
   g) Zamawiający nie definiuje parametrów jakościowych ruchu pakietów w klasie Best Effort, co wynika ze specyfiki tej klasy ruchowej.

W przypadku rozszerzenia ilości klas (rozszerzenie o klasy DATA_2, DATA_3, VoIP oraz WIDEO) Zamawiający będzie wymagał następujących parametrów jakościowych względem tych klas:

- w przypadku klas DATA_2, DATA_3 parametry jakościowe nie mogą być gorsze jak dla klasy DATA_1,
- w przypadku klasy WIDEO,
   a) opóźnienie pakietów dla ruchu typu WIDEO nie więcej niż 70ms,
   b) utrata pakietów dla ruchu typu WIDEO nie więcej niż 0,1%,
- w przypadku klasy VoIP:
   a) utrata pakietów nie może przekraczać 0,1%,
   b) opóźnienie pakietów nie może przekraczać 50ms,
   c) zmienność opóźnienia nie może przekraczać 20ms.

Zamawiający wymaga aby parametry jakościowe były mierzone z użyciem 10 datagramów UDP wysyłanych w okresie nie dłuższym niż co 5 minut pomiędzy urządzeniami dostępowymi CE. Wyniki pomiarów powinny być uśredniane w okresach nie dłuższych niż 1 godzina.

2. Zamawiający wymaga, by usługa serwisu technicznego obejmowała usuwanie problemów pracy z siecią po ich zgłoszeniu przez Zamawiającego na specjalnie do tego celu wydzielony bezpłatny numer telefoniczny do Call Center operatora (Biura Obsługi Klienta), dostępny bez przerwy - 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

3. Wszelkie prace serwisowe wymagające dostępu do routerów i modemów, powinny być dokonywane przez Wykonawcę zdalnie. W przypadkach, gdy zdalny dostęp z przyczyn technicznych nie będzie możliwy, odpowiednie działania mające na celu przywrócenie poprawnej pracy urządzeń i łącza powinny być wykonywane w lokalizacji Zamawiającego po wcześniejszym uzgodnieniu terminu i zakresu prac z Zamawiającym.

4. Zamawiający wymaga zagwarantowania minimalnego zakresu usług serwisowych świadczonych na rzecz Zamawiającego, tj.:
   1) zdalne zarządzanie konfiguracją fizyczną i logiczną sieci oraz utrzymanie urządzeń CE,
   2) zarządzanie siecią i monitorowanie stanu technicznego infrastruktury udostępnionej Zamawiającemu,
   3) dokonywanie konfiguracji interfejsów dla celów dołączenia do sieci LAN i WAN,
   4) konfigurację adresacji IP zgodnie z ustaleniami z Zamawiającym,
   5) zmianę konfiguracji urządzeń CE na wniosek Zamawiającego,
   6) naprawę lub wymianę uszkodzonego urządzenia CE,
   7) wykrywanie awarii i naprawa łączy dostępowych.

IV. Struktura fizyczna sieci

1. Udostępniana struktura sieciowa powinna być zbudowana na bazie wysokowydajnej platformy sieciowej pozwalającej na realizację połączeń „ każdy z każdym".

2. Łącza dostępowe muszą być łączami symetrycznymi o gwarantowanej przepustowości, tak aby zapewnić wydajną i niezawodną komunikację.

3. Zamawiający przy budowie łączy dostępowych dopuszcza następujące rodzaje mediów :
   1) łącza światłowodowe zakończone urządzeniami pracującymi w systemie SDH/PDH lub jako ciemne włókno bezpośrednio łączące router PE Wykonawcy z routerem CE w lokalizacji Zamawiającego,
   2) łącza radiowe punkt-punkt lub punkt-wielopunkt pracujące w paśmie koncesjonowanym w systemie SDH/PDH,
   3) łącza z zastosowaniem par kabli miedzianych z zastosowaniem urządzeń pracujących w technologii G.SHDSL.
4. Wszystkie węzły sieci Wykonawcy do których będą budowane łącza dostępowe jednostek resortu powinny być połączone z siecią operatora telekomunikacyjnego co najmniej dwiema niezależnymi drogami (dwa niezależne łącza w górę sieci).

5. Dla zapewnienia odpowiedniej skalowalności infrastruktury sieciowej i bezpieczeństwa transmisji danych, zapewnienia prywatności i izolacji różnych kanałów VPN konfigurowanych przez Wykonawcę, łącza dostępowe nie mogą być budowane z wykorzystaniem :
   1) zasobów publicznej sieci Internet,
   2) infrastruktury znajdującej się poza terytorium Polski,
   3) łączy asymetrycznych w technologii DSL,
   4) łączy satelitarnych,
   5) komutowanych łączy telefonicznych,
   6) łączy technologii radiowych w paśmie nie podlegającym koncesjonowaniu w Urzędzie Regulatora,
   7) technologii Wi-Fi i technologii HSDPA.

6. Zamawiający wymaga, aby do wskazanych lokalizacji Wykonawca doprowadził łącza dostępowe zabudowane routerami do szaf teletechnicznych wskazanych przez Użytkowników lokalnych.

7. Wydziały Zamiejscowe Biura do Spraw Przestępczości Zorganizowanej znajdują się w tych samych budynkach co odpowiadające im Prokuratury Apelacyjne, wobec czego Zamawiający dopuszcza zestawienie jednego łącza dostępowego do tych lokalizacji. Wyjątek stanowi Wydział Zamiejscowy BPZ w Gdańsku, zlokalizowany w Sopocie przy ul. Niepodległości 741b, gdzie Wykonawca powinien zestawić dodatkowe łącze dostępowe o przepustowości 1 Mbps. Zamawiający wymaga aby łącza dostępowe dla lokalizacji Prokuratur Apelacyjnych i Wydziałów Zamiejscowych Biura do Spraw Przestępczości Zorganizowanej były podzielone na dwa odseparowane od siebie VLAN-y zakończone na urządzeniu dostępowym CE na dwóch różnych interfejsach przyłączeniowych.

8. W sieci IP VPN pomiędzy routerami PE powinna być zapewniona separacja logiczna realizowana z wykorzystaniem protokołu BGP. W ramach warstwy drugiej (L2) Zamawiający dopuszcza stosowanie następujących protokołów: PPP Multilink, PPP, HDLC.

9. Do wymiany informacji routingowej pomiędzy siecią Zamawiającego, a siecią Wykonawcy powinien być wykorzystywany jeden z dostępnych protokołów routingu: RIPv2, OSPF, BGP lub EIGRP. Urządzenia dostępowe CE dostarczone przez Wykonawcę muszą wspierać każdy z tych protokołów dla interfejsów przyłączeniowych.

10. Zamawiający wymaga, aby Wykonawca wykorzystał jako urządzenia dostępowe CE routery IP dostarczone wraz z niezbędnym okablowaniem, osprzętem i oprogramowaniem umożliwiającym realizowanie założonych funkcjonalności. Nie dopuszcza się wykorzystywania jako urządzeń dostępowych CE wyłącznie mostów lub modemów oraz innych urządzeń pracujących w warstwie drugiej modelu ISO/OSI.

11. Urządzenia dostępowe CE muszą zapewnić odpowiednią ilość interfejsów przyłączeniowych:
    1) co najmniej dwa interfejsy przyłączeniowe Eth 10/100 dla lokalizacji Sądów Apelacyjnych, Prokuratur Apelacyjnych i Wydziałów Zamiejscowych Biura do Spraw Przestępczości Zorganizowanej (przy czym dla jednostek Prokuratur Apelacyjnych i Wydziałów Zamiejscowych Biura do Spraw Przestępczości Zorganizowanej powinno być instalowane pojedyncze urządzenie dostępowe CE ze względu na zlokalizowanie tych jednostek w tych samych budynkach z wyjątkiem Wydziału Zamiejscowego BPZ w Gdańsku),
    2) co najmniej dwa interfejsy przyłączeniowe Eth 10/100 dla lokalizacji jednostek centralnych Ministerstwa Sprawiedliwości,
    3) co najmniej trzy elektryczne interfejsy przyłączeniowe Eth 10/100/1000 dla lokalizacji POPD i ZOPD oraz dwa interfejsy dla Centrali BPZ.

12. Instalowane przez wykonawcę urządzenia CE muszą mieć możliwość dwukrotnego zwiększenia podanych wyżej ilości interfejsów przyłączeniowych z zachowaniem rodzaju interfejsu (Eth 10/100 lub Eth 10/100/1000) i umożliwiać:
    1) podłączenie do co najmniej ośmiu sieci IP VPN za pomocą pojedynczego łącza dostępowego poprzez wirtualizację procesów routingowych dla lokalizacji POPD, ZOPD i do co najmniej trzech sieci IP VPN za pomocą pojedynczego łącza dostępowego poprzez wirtualizację procesów routingowych dla pozostałych typów lokalizacji, w tym w Centrali BPZ,
    2) wirtualizację ścieżki danych pomiędzy urządzeniem dostępowym CE i urządzeniem w lokalizacji Zamawiającego w trybie pracy w więcej niż jednej sieci IP VPN, np. za pomocą technologii tuneli GRE (ang. *Generic Routing Encapsulation)* lub kreowanie VLAN (ang. *Virtual Local Area Network)*,
    3) oddzielenie informacji routingowych (za pomocą protokołów routingu

dynamicznego OSPF i BGP) pochodzących z różnych sieci IP VPN,
4) odczyt parametrów SNMP (ang. *Simple Network Management Protocol)* - tryb tylko do odczytu dla Użytkownika.

13. Zamawiający wymaga zróżnicowania ruchu według klas QoS w ramach pasma gwarantowanego na urządzeniu dostępowym CE z zapewnieniem:
    1) możliwości zdefiniowania minimum 2 klas QoS ruchu z możliwością późniejszego rozszerzenia do 4 klas ruchu, z gwarancją definiowania dowolnego podziału pasma według potrzeb Zamawiającego z uwzględnieniem dwóch klas multimedialnych. Rozszerzenie nie może powodować konieczności fizycznej wymiany urządzeń dostępowych i związanych z tym przerw w działaniu sieci. Sieć WAN musi umożliwiać implementację mechanizmów QoS zgodnie z modelem DiffServ (ang. *Differentiated Sevices)* i wsparciem dla IP DSCP (ang. *Differentiated Sevices Code Point)* IP Precedence zgodnie z RFC 2474 i 2475,
    2) możliwości kierowania ruchu do wskazanej klasy ruchowej na podstawie: IP Precedence, DSCP, adresu źródłowego, adresu docelowego, numeru portu UDP/TCP źródłowego, numeru portu UDP/TCP docelowego, mechanizmów ACL oraz dowolnej kombinacji w/w parametrów,
    3) możliwości reklasyfikowania (w przypadku wysycenia pasma QoS klasy wyższej, automatycznego reklasyfikowania ruchu do klasy niższej) i oznaczania pakietów IP w oparciu o podane wyżej kryteria na urządzeniu dostępowym CE.

14. Zamawiający wymaga, aby Wykonawca obsługiwał adresy IP używane przez Zamawiającego w dotychczas eksploatowanych sieciach rozległych z puli określonej w dokumencie RFC 1918 (ang. *Requests For Comments)*. Szczegółowy plan adresacji sieci zostanie przekazany Wykonawcy po zawarciu Umowy.

V. Struktura logiczna sieci

1. Struktura logiczna udostępnianej przez Wykonawcę usługi transmisji danych w sieci operatora telekomunikacyjnego musi umożliwiać konfigurację dostępu użytkowników do usług i uwzględniać:
    1) przynależność danej jednostki organizacyjnej resortu do określonej grupy jednostek (lokalizacji),
    2) korzystanie danej jednostki z określonych zasobów bazodanowych czy aplikacji,
    3) podział udostępnianego pasma na klasy ruchowe: / data_1 /data_2/ data_n, besteffort,
    4) elastyczną topologię rozwiązania w zależności od klasy (np.: topologia gwiazdy dla klas ruchowych: besteffort, / data_1 / data_n oraz topologia każdy z każdym dla klasy ruchowej WIDEO i VoIP) niezależnie od lokalizacji).

2. W ramach struktury logicznej sieci Zamawiającego muszą zostać zdefiniowane następujące VPN obejmujące swym zasięgiem wskazanych Użytkowników (lokalizacje), z określonymi możliwościami w zakresie transmisji danych z poszczególnych lokalizacji w ramach danych sieci VPN:
    1) sieć VPN łącząca wszystkie lokalizacje Sądów Apelacyjnych a po uruchomieniu VPN APELACJA i podłączeniu do sieci Sądów Okręgowych oraz Sądów Rejonowych (VPN_S). Sieć **VPN_S** – połączy wszystkie lokalizacje Sądów Apelacyjnych, Okręgowych i Rejonowych z lokalizacjami POPD i ZOPD,
    2) sieć VPN łącząca wszystkie lokalizacje Prokuratur Apelacyjnych a po uruchomieniu VPN APELACJA i podłączeniu do sieci Prokuratur Okręgowych oraz Prokuratur

Rejonowych (VPN_P). Sieć **VPN_P** – połączy wszystkie lokalizacje Prokuratur Apelacyjnych Okręgowych i Rejonowych z lokalizacjami POPD i ZOPD ,

3) sieć VPN łącząca wszystkie Wydziały Zamiejscowe Biura do Spraw Przestępczości Zorganizowanej zlokalizowane w 11 Prokuraturach Apelacyjnych (VPN-BPZ). Sieć **VPN_BPZ** – połączy wszystkie lokalizacje Wydziałów Zamiejscowych Biura do Spraw Przestępczości Zorganizowanej z węzłem Centrala BPZ,
4) sieć VPN łącząca wszystkie lokalizacje Systemu Informatycznego Prokuratur po uruchomieniu VPN APELACJA i podłączeniu sieci Prokuratur Okręgowych oraz Prokuratur Rejonowych **(VPN_SIP)**,
5) sieć VPN System Informatyczny Schengen dla jednostek organizacyjnych Prokuratury SIS-SIP po uruchomieniu VPN APELACJA i podłączeniu do sieci Prokuratur Okręgowych **(VPN_SIS-SIP)**,
6) sieć VPN System Informatyczny Schengen dla Sądów – (SIS-SAD) po uruchomieniu VPN APELACJA i podłączeniu do sieci Sądów Okręgowych **(VPN_SIS-SAD)**,

3. Poszczególne sieci IP VPN powinny mieć dostęp do współdzielonych zasobów sieciowych po stronie Systemów Centralnych POPD/ZOPD.

4. Zakres uprawnień w dostępie dla każdej sieci VPN (do poziomu pojedynczej lokalizacji/pojedynczego użytkownika) zostanie zdefiniowany na etapie uruchomienia usług i eksploatacji po zawarciu umowy.

5. Poszczególne jednostki organizacyjne MS muszą mieć zapewnioną możliwość komunikacji z określonymi Systemami Resortowymi, przy czym ze względu na centralizację transmisja danych powinna być nawiązywana bezpośrednio w relacji od danej jednostki MS (niezależnie od tego w ramach którego VPN-a została zdefiniowana) do określonego Systemu Resortowego.

6. Ze względu na konieczność podziału pasma na klasy ruchowe a tym samym konieczność realizacji wielu usług w ramach pojedynczego łącza do danej lokalizacji, na etapie uruchomienia usług i eksploatacji udostępnionej infrastruktury sieciowej musi być możliwa konfiguracja sieci zapewniająca dostęp do usług zależna od rodzaju klasy ruchowej i topologii sieci:
   1) dla transmisji typu DATA (ruch resortowy przypisany do klas data_1 / data_2 / data_n), sieci VPN_S oraz VPN_P powinna być możliwość skonfigurowania struktury wielopoziomowej gwiazdy ze względu na podległość poszczególnych jednostek względem jednostek nadrzędnych,
   2) dla transmisji typu usług WIDEO i VoIP (ruch głosowy) poszczególne lokalizacje MS w ramach VPN APELACJA i VPN CENTRALA po połączeniu sieci (niezależnie od tego w ramach którego VPN-a zostały zdefiniowane) powinny mieć możliwość nawiązania połączenia bezpośrednio pomiędzy sobą.

VI. Bezpieczeństwo

1. Bezpieczeństwo teleinformatyczne udostępnionej struktury sieciowej powinno wynikać z przyjętej technologii budowy sieci IP VPN zrealizowanej na potrzeby świadczenia usług transmisji danych przez Zamawiającego poprzez wykorzystywanie polityk zapewniających prywatność oraz izolację różnych VPN konfigurowanych w sieci

Wykonawcy.

2. W celu zapewnienia bezpieczeństwa transmisji danych, zapewnienia prywatności i izolacji różnych kanałów VPN konfigurowanych przez Wykonawcę łącza dostępowe nie mogą być budowane na bazie zasobów publicznej sieci Internet.

3. Informacje sieciowe każdego VPN powinny być przechowywane w oddzielnych tablicach routingowych VRF na routerach usługowych.

4. W ramach realizacji umowy Zamawiający wymaga:
   1) dostarczenia urządzeń bezpieczeństwa do lokalizacji POPD, ZOPD i Centrali BPZ o konfiguracji zgodnej z wymaganiami Zamawiającego. Wymagania techniczne i funkcjonalne dotyczące systemu zabezpieczeń z wykorzystaniem sieciowych urządzeń bezpieczeństwa zamieszczono w załączniku nr 5 oraz nr 7 cz.I_do IPU,
   2) zapewnienia gwarancji, serwisu technicznego urządzeń zawartym w pkt III ppkt 2 ppkt 6 oraz SLA,zawartym w pkt III ppkt 3 ppkt 6,
   3) przekazania dokumentacji powykonawczej oraz konfiguracji urządzeń bezpieczeństwa wraz z przekazaniem haseł zabezpieczających dostęp do urządzeń,
   4) przeprowadzenia szkoleń dla 2 administratorów bezpieczeństwa teleinformatycznego Zamawiającego w zakresie monitorowania bezpieczeństwa sieciowego i polityk zabezpieczeń oraz utrzymania systemu bezpieczeństwa sieciowego,
   5) zapewnienia asysty technicznej w siedzibie Zamawiającego w zakresie eksploatowanych urządzeń bezpieczeństwa w wymiarze 8 godzin miesięcznie w okresie obowiązywania umowy w zakresie rekonfiguracji urządzeń i zmian polityk bezpieczeństwa pod kątem dodatkowych potrzeb Zamawiającego.

5. Urządzenia bezpieczeństwa sieciowego powinny realizować kontrolę dostępu (firewall), poufność danych (IPSec VPN oraz SSL VPN), ochronę przed atakami (IPS/IDS), kontrolę pasma oraz ruchu (QoS i Traffic Shaping) oraz kontrolę komunikatów sieciowych (IM oraz aplikacji P2P).