Załącznik nr 3_III_do IPU

SPECYFIKACJA TECHNICZNA

CZĘŚĆ III

Zakup usług transmisji danych na potrzeby obsługi teletransmisyjnej jednostek organizacyjnych Służby Więziennej (SW) w celu zapewnienia dostępu do centralnych baz danych w oparciu o udostępnione łącza dostępowe do sieci transmisji danych Wykonawcy zapewniającej połączenie do Ośrodka Przetwarzania Danych i Służby Więziennej (OPD SW) i połączenia „każdy z każdym" wszystkich jednostek Służby Więziennej oraz zapewnienia centralnego dostępu jednostek organizacyjnych SW do sieci Internet.

Objaśnienia użytych skrótów:

Lp.	*skrót*	*opis*
1.	AS	Areszt Śledczy
2.	COSSW	Centralny Ośrodek Szkolenia Służby Więziennej
3.	CZSW	Centralny Zarząd Służby Więziennej
4.	ODK	Ośrodek Doskonalenia Kadr
5.	OISW	Okręgowy Inspektorat Służby Więziennej
6.	OPD SW	Ośrodek Przetwarzania Danych SW
7.	OZ	Oddział Zewnętrzny
8.	SW	Służba Więzienna
9.	ZK	Zakład Karny
10.	AV	Antyvirus
11.	BGP	Border Gateway Protocol
12.	CE	Customer Equipment
13.	full-mesh	Sieć kratowa dla połączeń punkt-punkt z redundancją
14.	IPS/IDS	Intrusion Prevention Systems/Intrusion Detection Systems
15.	IPSec	Protokół bezpiecznej komunikacji IP
16.	P2P	peer-to-peer
17.	PE	Provider Edge Router
18.	QoS	Quality of Service
19.	SLA	Service Level Agreement
20.	SSL	Secure Socket Layer VPN
21.	VoIP	Voice over IP
22.	VPN	Virtual Private Network
23.	VRF	Virtual Routing and Forwarding

Spis treści:

I. Definicje

Użytkownik - Zamawiający i jednostki Zamawiającego wskazane w zał. nr 1 cz. III_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 przy czym:

1. dla łączy dostępowych o przepustowości 2 Mbps i wyższej mierzona w warstwie 3 modelu ISO/OSI,
2. dla łączy dostępowych o przepustowości niższej niż 2 Mbps (1 Mbps, 512 kbps, 256 kbps, 128 kbps) mierzonej w warstwie transmisyjnej modelu ISO/OSI, w której udostępniane pasmo IP w stosunku do zamawianego łącza zostaje obniżone o wymagany narzut wynikający z zastosowanej technologii,
3. dla zbiorczych łączy dostępowych STM1 o przepustowości możliwej do osiągnięcia, z uwzględnieniem zastosowanej technologii.

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.

II. Przedmiot zamówienia:

1. Zakup usług transmisji danych dla obsługi informatycznej jednostek organizacyjnych Służby Więziennej poprzez zestawienie i uruchomienie zabudowanego urządzeniami aktywnymi Telekomunikacyjnego Węzła Dostępowego SW w lokalizacji Zamawiającego (OPD SW) i włączenie w system wymiany danych 202 łączy dostępowych zabudowanych urządzeniami aktywnymi do jednostek organizacyjnych Służby Więziennej. Wykaz lokalizacji Użytkowników zawierający adres miejsca instalacji (zakończenia łącza), wymagania na pasmo transmisyjne, zamieszczono w zał. nr 1 cz. III_do IPU

2. Zapewnienie bezpiecznego, centralnego dostępu do sieci Internet wszystkim jednostkom organizacyjnym SW.

3. Przeniesienie aktualnie eksploatowanych systemów i aplikacji użytkowych Zamawiającego (NoeNET, Poczta) z aktualnie eksploatowanych sieci transmisji danych do struktury świadczenia usług TD udostępnionej w przedmiotowym postępowaniu.

4. Dostarczenie i udostępnienie w siedzibie Zamawiającego (OPD SW) 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 minimalnej 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 32" aktywna matryca TFT, kąt widzenia min. 160/160 stopni, jasność 300 cd/m2, kontrast 700:1, średni czas reakcji 8 ms, matryca min. 1360x768, 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.

5. Zapewnienie świadczenia usług transmisji danych przez okres 32 miesięcy liczony od daty uruchomienia i oddania łączy do eksploatacji przeniesienia połączeń z obecnie eksploatowanej sieci TD do struktury będącej przedmiotem zamówienia.

Zamawiający wymaga zapewnienia usług transmisji danych w oparciu o wykreowaną wirtualną sieć dedykowaną transmisji danych IP VPN, zestawianą w zasobach technicznych operatora telekomunikacyjnego/dostawcy usługi transmisji danych dla zabezpieczenia wymiany danych drogą elektroniczną pomiędzy jednostkami organizacyjnymi SW, dostępu do lokalnych i centralnych baz danych Służby Więziennej poprzez zestawienie, uruchomienie i wdrożenie rozwiązania polegającego na:

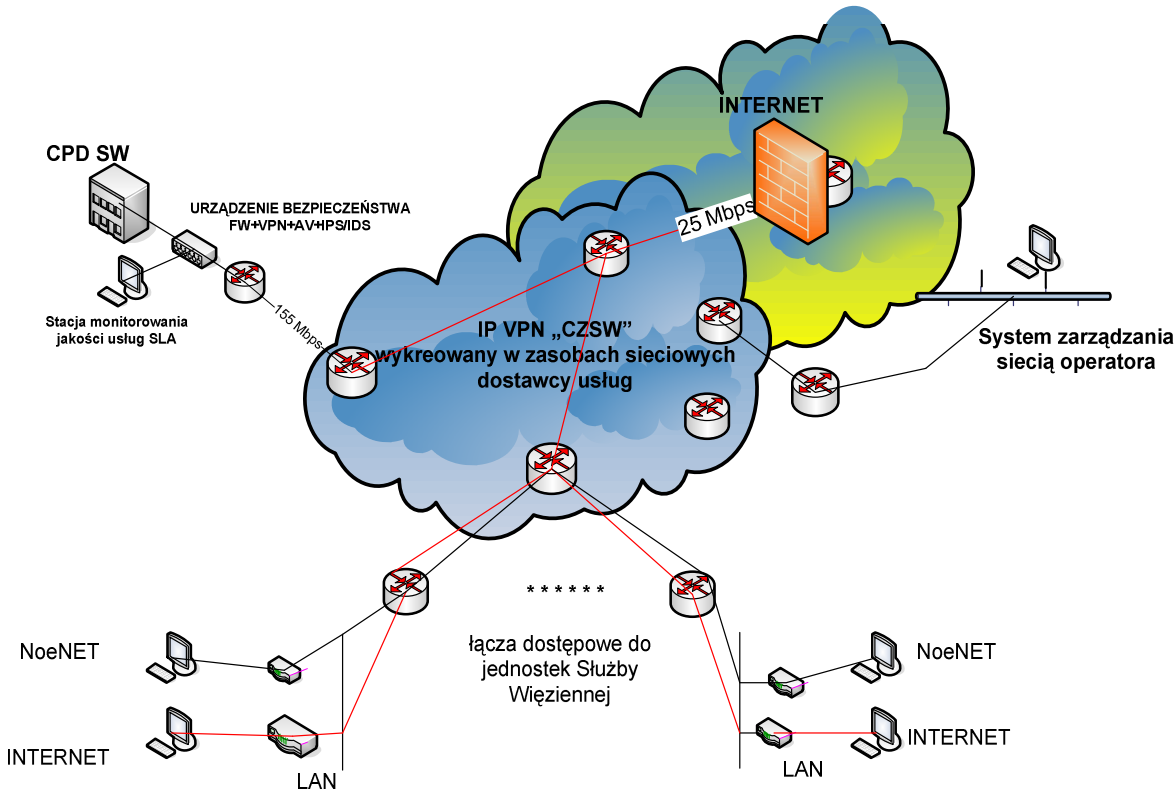
1) na poziomie CZSW (VPN_SW) – organizacji, budowie i uruchomieniu telekomunikacyjnego węzła dostępowego (OPD SW) podłączonego łączem dostępowym o przepustowości 155 Mbps (STM1), zabezpieczonego urządzeniem bezpieczeństwa teleinformatycznego,

2) uruchomienie w sieci dostawcy usług IP VPN Służby Więziennej oraz zestawienie 202 zabudowanych urządzeniami aktywnymi łączy dostępowych do wszystkich jednostek SW ,
3) zapewnieniu bezpiecznego, centralnego dostępu do sieci Internet obsługiwanego i zabezpieczonego przez Wykonawcę poprzez bezpieczną bramę dostępową w zasobach operatora telekomunikacyjnego o przepustowości 25 Mbps.

III. Zakres świadczonych usług

Zamawiane usługi muszą obejmować:

1. Dostawę, instalację urządzeń i uruchomienie telekomunikacyjnego węzła dostępowego w lokalizacji Zamawiającego (OPD SW w lokalizacji CZSW). Węzeł powinien być wyposażony w router i urządzenie bezpieczeństwa o parametrach technicznych zapewniających co najmniej realizację funkcji wymaganych przez Zamawiającego a wyspecyfikowanych w załączniku nr 2 cz. III_do IPU oraz urządzeń dostępowych we wszystkich podległych lokalizacjach zdalnych. Wszystkie urządzenia muszą być dostarczone, zainstalowane i uruchomione przez Wykonawcę i są jego własnością w okresie świadczenia usług i po ich zakończeniu.



Rys. 1. Rozwiązanie IP VPN na potrzeby obsługi transmisyjnej systemów informatycznych Służby Więziennej

---

2. Zestawienie 202 łączy zabudowanych urządzeniami sieciowymi do wszystkich jednostek organizacyjnych SW. W ramach oferowanej usługi operator telekomunikacyjny/dostawca usług zobowiązany jest do instalacji i uruchomienia łączy dostępowych oraz:

1) zapewnienia kompleksowego rozwiązania IP VPN w ramach własnej/dzierżawionej sieci telekomunikacyjnej umożliwiającego połączenie rozproszonych geograficznie 202 jednostek organizacyjnych SW w jedną wydzieloną bezpieczną sieć transmisji danych. Wszystkie urządzenia dostępowe w lokalizacjach zdalnych powinny komunikować się z routerem zainstalowanym w lokalizacji centralnej SW (OPD SW),
2) skonfigurowania na routerach usługowych operatora tablic VRF (VPN Routing Forwarding) oddzielnie dla każdej z jednostek,
3) umożliwienia wymiany danych poprzez własną sieć telekomunikacyjną w relacjach Centralny Węzeł Dostępowy (OPD SW) - wszystkie węzły dostępowe podłączonych do sieci jednostek SW oraz zestawienie połączeń dla obsługi systemu informatycznego SW NoeNET.
4) zapewnienia zintegrowanego dostępu wszystkich jednostek SW do sieci Internet poprzez łącza współdzielone przez wszystkie lokalizacje Zamawiającego. Łącza te powinny być doprowadzone do routera brzegowego operatora/dostawcy usług przez Internet Gateway i zarządzany Firewall. Centralny dostęp do sieci Internet powinien być zrealizowany w zasobach dostawcy i przez niego utrzymywany oraz w pełni zarządzany,
5) zapewnienia bezpieczeństwa teleinformatycznego transmisji danych operacyjnych i ochrony transmisji z wykorzystaniem urządzenia bezpieczeństwa sieciowego uruchomionego w węźle OPD SW realizującego kontrolę dostępu (firewall), ochronę przed wirusami (AV), poufność danych (IPsec VPN oraz SSL VPN), ochronę przed atakami (IPS/IDS), kontrolę zawartości poczty (antyspam), kontrolę pasma oraz ruchu (QoS i Traffic Shaping) oraz kontrolę komunikatów sieciowych (IM oraz aplikacji P2P),
6) realizację usług zarządzania urządzeniami CE w trakcie obowiązywania umowy obejmujących:
   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 świadczone przez operatora telekomunikacyjnego dla VPN SW, w tym:
   1) wykreowanie IP VPN łączącego wszystkie jednostki organizacyjne SW. Zamawiający wymaga, by na etapie realizacji zamówienia przepustowość łącza dostępowego do OPD SW wynosiła min 155 Mbps,
   2) zapewnienie dostępu do sieci TD jednostkom organizacyjnym SW z gwarantowaną przepustowością zgodnie z załącznikiem nr 1 cz. III_do IPU,
   3) Zamawiający wymaga zapewnienia następujących, minimalnych parametrów usług SLA, jakie muszą być gwarantowane przez operatora telekomunikacyjnego/ dostawcę usług w ramach świadczenia usług w sieci IP VPN dla wszystkich klas ruchowych:
      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, liczony od godziny zgłoszenia awarii
      d) czas usunięcia awarii nie dłużej niż:

i. dla lokalizacji OPD SW - 4 godziny, liczone od godziny zgłoszenia awarii
ii. dla pozostałych lokalizacji - 24 godziny, liczone 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.

4. 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, dostępny 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.
5. Wszelkie prace serwisowe wymagające dostępu do routerów i modemów, powinny być dokonywane przez operatora 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 klienta po wcześniejszym uzgodnieniu terminu i zakresu z Zamawiającym.
6. 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 sieciowej 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 lokalizacja zdalna – centralna baza danych (OPD SW) oraz połączeń „ każdy z każdym".
2. Łącza dostępowe muszą być łączami symetrycznymi o gwarantowanej przepustowości, tak aby zapewnić wydajną i niezawodną komunikację.
3. Wszystkie węzły sieci operatora do których będą budowane łącza dostępowe jednostek SW powinny być połączone z siecią operatora conajmniej dwiema niezależnymi drogami (dwa niezależne łącza w górę sieci) i nie powinny być realizowane z zastosowaniem technologii radiowych w paśmie nie podlegającym koncesjonowaniu w Urzędzie Regulatora.
4. Dla zapewnienia odpowiedniej skalowalności infrastruktury sieciowej i bezpieczeństwa transmisji danych, zapewnienia prywatności i izolacji różnych kanałów VPN konfigurowanych przez dostawcę usług telekomunikacyjnych, łącza dostępowe nie mogą być budowane na bazie zasobów publicznej sieci Internet.
5. Zamawiający wymaga, aby do wskazanych w załączniku nr 1 cz. III do IPU lokalizacji Wykonawca doprowadził zabudowane routerami łącza dostępowe do szaf teletechnicznych wskazanych przez Użytkowników lokalnych.
6. Do wymiany informacji routingowej pomiędzy siecią Zamawiającego (OPD SW), a

siecią Wykonawcy powinien być wykorzystywany jeden z dostępnych protokołów routingu: RIPv2 (ang. *Routing Information Protocol)*, OSPF (ang. *Open Shortest Path First)*, BGP (ang. *Border Gateway Protocol)*. Urządzenia dostępowe (CE) dostarczane przez Wykonawcę muszą wspierać co najmniej każdy z tych protokołów dla interfejsów przyłączeniowych.

7. Zamawiający wymaga, aby Wykonawca wykorzystał jako urządzenia dostępowe (CE) routery IP dostarczone wraz z niezbędnym okablowaniem i osprzętem. Nie dopuszcza się wykorzystywania jako urządzeń dostępowych (CE) wyłącznie mostów lub modemów oraz innych urządzeń pracujących w warstwie drugiej ISO/OSI *(Open System Interconnection)*.
8. Ponadto urządzenia dostępowe (CE) muszą zapewnić:
   1) możliwość podłączenia do co najmniej trzech sieci IP VPN za pomocą pojedynczego łącza dostępowego poprzez wirtualizację procesów routingowych,
   2) wirtualizację ścieżki danych pomiędzy urządzeniem dostępowym CE i urządzeniem Zamawiającego w trybie pracy w więcej niż jednej sieci IP VPN, np. za pomocą technologii tuneli GRE (ang. *Generic Routing Encapsulation)* lub 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 Zamawiającego).
9. 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 QoS, z gwarancją definiowania innego, ustalonego między Zamawiającym i Wykonawcą podziału pasma w ramach dostępnych możliwości technicznych z uwzględnieniem możliwości zdefiniowania 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 przypisania ruchu do konkretnej klasy QoS w oparciu o: IP Precedence, IP DSCP, adres IP docelowy, adres IP źródłowy, port UDP (ang. *User Datagram Protocol) /TCP (ang. Transmission Control Protocol)* docelowy, port UDP/TCP źródłowy lub dowolną kombinację tych 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).
10. 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).* Zamawiający przekaże Wykonawcy plan adresacji na etapie podpisywania umowy.

V. Struktura logiczna sieci

1. Struktura logiczna udostępnianej 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: *besteffort / data_1*
4) elastyczną topologię rozwiązania w zależności od klasy (np.: topologia gwiazdy dla klas ruchowych: besteffort, / data_1 oraz topologia każdy z każdym dla klasy ruchowej WIDEO i VoIP) niezależnie od lokalizacji).

2. Wydzielone grupy lokalizacji muszą mieć możliwość utworzenia własnych sieci VPN o określonym statusie, w tym:
   1) sieć IP VPN łącząca wszystkie jednostki Służby Więziennej (ZK, AŚ, OISW, OZ, ODK) (VPN_SW),
   2) sieć IP VPN łącząca wszystkie jednostki Służby Więziennej włączone w system NoeNET (VPN_NoeNET).
3. Poszczególne sieci IP VPN powinny mieć dostęp do współdzielonych zasobów sieciowych po stronie Systemów Centralnych OPD SW.
4. Zakres uprawnień w dostępie dla każdej sieci VPN (do poziomu pojedynczej lokalizacji/pojedynczego użytkownika) zostanie zdefiniowany indywidualnie na etapie uruchomienia usług i eksploatacji po podpisaniu umowy.
5. Ze względu na podział 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 usług zależnie od rodzaju klasy ruchowej i topologii sieci:
   1) dla transmisji typu DATA (ruch przypisany do klasy data_1) w sieci VPN_NoeNET powinna być możliwość skonfigurowania struktury wielopoziomowej gwiazdy ze względu na podległość poszczególnych jednostek względem jednostek nadrzędnych,
   2) dla transmisji typu usług WIDEO oraz VoIP poszczególne lokalizacje SW (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 dostawcę usług łącza dostępowe dla systemów operacyjnych Zamawiającego 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 przedmiotowego zamówienia Zamawiający wymaga:
   1) dostarczenia urządzenia bezpieczeństwa do lokalizacji OPD SW o konfiguracji zgodnej z wymaganiami Zamawiającego. Wymagania techniczne i funkcjonalne dotyczące systemu zabezpieczeń z wykorzystaniem sieciowych urządzeń bezpieczeństwa zamieszczono w załączniku nr 2 cz. III_do IPU,
   2) włączenia w system transmisji, uruchomienia i skonfigurowania urządzenia oraz budowy i zarządzania systemem bezpieczeństwa teleinformatycznego zgodnie z wymaganiami polityki bezpieczeństwa uzgodnionej z Zamawiającym po podpisaniu

umowy,

3) zapewnienia gwarancji i serwisu technicznego urządzenia zgodnie z SLA zawartym w pkt III pkt 3 ppkt 3),
4) przekazania dokumentacji powykonawczej oraz konfiguracji urządzenia bezpieczeństwa wraz z przekazaniem haseł zabezpieczających dostęp do urządzenia oraz 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 eksploatowanego urządzenia bezpieczeństwa w wymiarze 8 godzin miesięcznie w okresie obowiązywania umowy w zakresie rekonfiguracji urządzeń i zmian polityk bezpieczeństwa pod kątem dodatkowych potrzeb Zamawiającego.

5. Urządzenie bezpieczeństwa sieciowego powinno realizować kontrolę dostępu (firewall), ochronę przed wirusami (AV), poufność danych (IPSec VPN oraz SSL VPN), ochronę przed atakami (IPS/IDS), kontrolę zawartości poczty (antyspam), kontrolę pasma oraz ruchu (QoS i Traffic Shaping) oraz kontrolę komunikatów sieciowych (IM oraz aplikacji P2P).