Załącznik nr 3B do SIWZ

Lista spełnienia warunków szczegółowych OPZ dla poszczególnych urządzeń sieciowych

dla postępowania na

„Dostawę i wdrożenie urządzeń warstwy aktywnej w ramach projektu Sieć Szerokopasmowa Polski wschodniej – województwo podlaskie”

ECM Group Polska SA
00-124 Warszawa, Rondo ONZ 1, tel. (22) 333 73 57, fax (22) 540 62 26
e-mail: office@ecmg.pl, www.ecmg.pl
KRS 0000409702, NIP 5252248357, REGON 015252550

Śląska Sieć Metropolitalna Sp. z o.o.
44-100 Gliwice, ul. Bojkowska 37 lok. 3, tel. (32) 461-22-10, fax (32) 441-90-16
e-mail: biuro@ssm.silesia.pl, www.ssm.silesia.pl
KRS 0000322774, NIP 6312578261, REGON 241069249

Wykonawca musi wypełnić wszystkie rubryki tabeli za wyjątkiem tych zaczernionych. Wykonawca potwierdzając w tabeli posiadany parametr przez urządzenie zaoferowane w ofercie, musi załączyć dokument techniczny, lub inny dokument autoryzowany przez producenta lub dystrybutora urządzeń na teren polski, o spełnieniu wymagań określonych w tabeli. Wykonawca w takim dokumencie, musi wskazać dany parametr. Nie dopuszcza się oświadczeń wykonawcy lub podwykonawcy w zakresie spełnienia warunków OPZ. Parametry w ostatniej kolumnie tabeli muszą zostać precyzyjne wskazane w dokumencie załączonym.

Minimalne parametry dla konfiguracji urządzeń warstwy transportu sieci SSPW			
Wymagany parametr zgodnie z pkt. OPZ	Oferowany parametr (lub potwierdzenie "TAK" Jeżeli Wykonawca realizuje funkcje w sposób dokładny jak w wymaganiu)	Rodzaj załączonego dokumentu, złożonego na potwierdzenie parametru (dokumenty techniczne autoryzowane przez producenta lub dystrybutora na teren polski danego urządzenia lub karty katalogowe)	Miejsce w załączonym dokumencie wskazujący dany parametr (strona, rozdział, punkt lub wers)
6) Urządzenia DWDM muszą być urządzeniami możliwymi do zamontowania w szafie 19’ RACK lub szafie dedykowanej. W przypadku montażu w szafie dedykowanej, szafę taką należy dostarczyć.			
7) Urządzenia pełniące funkcję DWDM muszą komunikować się za pomocą światłowodu jednomodowego G-652D wykorzystując jedną parę włókien w każdym kierunku.			
8) Warstwa optyczna ma powstać w oparciu o multipleksery DWDM drop&insert, jako warstwy transportowej dla połączeń urządzeń warstwy IP wyposażonych w interfejsy 100GE.			
9) W urządzeniach należy stosować przeźroczyste przełączniki optyczne (przesyłany sygnał będzie przełączany pomiędzy urządzeniami bez potrzeby konwersji z sygnału optycznego na elektryczny). Przełączniki optyczne muszą umożliwiać przełączanie zarówno			

pojedynczych kanałów optycznych, jak i ich grup.			
10) Każdy węzeł DWDM powinien realizować funkcjonalność dowolny kolor, dowolny kierunek (colorless, directionless). Przełączanie musi być możliwe zarówno bez zmiany długości fali przesyłanego sygnału, jak i ze zmianą długości fali, z uwzględnieniem zajętości kanałów optycznych w łączu.			
11) Urządzenie musi opierać się o wkładki czarno-białe, nie może być urządzeniem opierającym się o tzw. kolorowe wkładki. Wykonawca w celu realizacji połączeń DWDM musi wykorzystywać do tego celu dedykowane urządzenia DWDM. Nie dopuszcza się stosowania urządzeń realizujących funkcję DWDM w sposób odmienny niestandardowy i nie gwarantujący pewności połączeń.			
12) Sieć transportowa oparta na urządzeniach DWDM musi być zbudowana zgodnie z wymaganiami ITU-T w szczególności: ITU-T G.872, ITU-T G.709, ITU-T G959.1.			
13) Urządzenie musi mieć możliwość rekonfiguracji usług świadczonych przez sieć transportową możliwą do realizacji w sposób zdalny w szczególności zmiana długości fali, zmiana kierunku nadawania kanału optycznego itp.			
14) Należy zastosować rozwiązania pozwalające na przesyłaniu minimum 80 kanałów optycznych (lambd) zgodnie z siatką kanałów określoną w zaleceniu ITU-T G.694.1.			
16) System powinien być zaprojektowany i skompensowany,			

tak aby przenosił kanały/lambdy 2,5Gbps i 10Gbps.			
17) System powinien być zaprojektowany i skompensowany, tak aby przenosił kanały/lambdy 40Gbps oraz 100Gbps (sygnały koherentne i nie koherentne).			
18) Wymagana jest możliwość zestawiania kanałów optycznych 10GE, 40GE, 100GE, pomiędzy dowolnymi lokalizacjami w zaoferowanej sieci DWDM, bez regeneracji 3R (stosowanie kart transponderów optycznych jedynie w docelowych lokalizacjach terminacji usług, możliwość optycznego pass-through bez konieczności inwestycji środków w węzłach pośrednich).			
19) Wzmacniacze w urządzeniach DWDM muszą realizować monitorowanie parametrów optycznych sygnału wejściowego i wyjściowego, temperatury.			
20) System musi umożliwiać wymianę modułu zarządzającego bez przerwy w transmisji danych na transponderach i innych modułach.			
21) System powinien bazować na urządzeniach modularnych – wyposażonych w ilość slotów dających możliwość minimum podwojenia ilości zainstalowanych w pierwotnej konfiguracji kart interfejsów liniowych, klienckich, filtrów, wzmacniaczy i pozostałych komponentów struktury optycznej.			
22) System musi posiadać pełną możliwość zdalnej zmiany konfiguracji usług za pomocą systemu zarządzania bez konieczności fizycznej interwencji administratora w którykolwiek z węzłów sieci.			

23) Kanały 100Gbps powinny być przesyłane w pojedynczych kanałach optycznych z odstępem 50 GHz. Nie jest dopuszczalne dostarczanie interfejsów liniowych 100Gbps, tworzonych w oparciu o kilka kanałów nośnych np. 4 x 25Gbps czy 10 x 10Gbps.			
24) System DWDM musi pozwalać na stosowanie elastycznej (mieszanej) struktury jednostek ODU0, ODU1, ODU2, ODU3 w obrębie kanału optycznego oraz zawierać strukturę OTN dla jednostek ODU0, ODU1, ODU2, ODU3, ODU4.			
25) System musi pozwalać na wyposażenie w dodatkowe, uniwersalne karty dla sygnałów 10Gbps z interfejsem klienckim w formatach SFP+ lub XFP (obsługa sygnałów, co najmniej: 10G LAN, 10G WAN, STM, OTU-2/OTU-2e). Wymagana jest zgodność z ITU-T G.709.			
26) System musi pozwalać na wyposażenie w dodatkowe, uniwersalne karty dla sygnałów z zakresu 155 Mbit/s – 10Gbps z interfejsami klienckim w standardzie SFP lub SFP+/XFP (obsługa sygnałów co najmniej: STM-1/4/16/64, GE, 10GE, FC1/2/4/8). Wymagana zgodność mapowania z ITU-T G.709.			
27) Dla sygnałów o przepustowościach poniżej 2.5 G, system powinien obsługiwać metodę agregowania większej ilości usług w kanały OTU1 lub OTU2/ OTU2e.			
28) Zastosowany system DWDM musi pozwalać na zastosowanie węzłów typu: terminal końcowy, optyczna, rekonfigurowalna krotnica przelotowa (ROADM) o minimum 4 kierunkach			

transmisyjnych, wzmacniak optyczny dwukierunkowy, OTN.			
29) Wszystkie węzły systemu DWDM powinny zapewniać funkcjonalność agregacji i przełączania jednostek ODU/OTU zgodnie strukturą ITU-T G709, pomiędzy wszystkimi kanałami optycznymi i interfejsami klienckimi uruchomionymi w półce systemowej.			
30) Urządzania DWDM powinny zapewniać funkcjonalności elastycznego przełączania i agregacji różnorodnych jednostek struktury zwielokrotnienia ODU w jednostki transportowe OTU zgodnie z standardem ITU-T G709. Do tego celu wszystkie węzły sieci DWDM powinny posiadać zintegrowane matryce przełączające w warstwie struktury „Optic Transport Network". Urządzenia powinny zapewniać możliwość agregacji dowolnego zestawu połączeń usługowych (o różnorodnych przepustowościach z zakresu 155M-10G), przy wykorzystaniu mapowania w jednostki ODUk bezpośrednio w pojedynczą jednostkę transportową OTU4.			
31) W celu szybkiej eliminacji i obsługi awarii urządzenia DWDM muszą obsługiwać mechanizmy Generalized Multi-Protocol Label Switching zgodnie z RFC 3945 i Automatically Switched Optical Network zgodnie z ITU-T G.8080.			
32) System musi mieć możliwość zapewniania zabezpieczenia typu SNCP dla wszystkich jednostek ODUk.			
33) Zastosowany system musi umożliwiać transport optycznych kanałów warstw wyższych, co najmniej typu:			

a) PDH: E1/E3			
b) synchronicznego (SDH) STM-1/STM-4/STM-16/STM-64,			
c) Ethernet 1GbE,10GE,			
d) 40GE i 100GE koherentne i nie koherentne			
e) interfejsów SAN (FC1G, FC2G, FC4G, FC8G, FC10G)			
f) interfejsów OTU-2/ OTU2e			
g) sygnałów cyfrowych video DVB (SDI), np. HDMI dla monitoringu wideo.			
34) Dla każdego typu usługi musi istnieć możliwość uruchomienia połączenia w trybie bez protekcji lub co najmniej z zabezpieczeniem 1+1 w trybie SNC na poziomie poszczególnych jednostek ODU/OTU struktury zwielokrotnionej matryc przełączających.			
35) System musi umożliwiać zestawienie kanałów roboczych i protekcyjnych pomiędzy dowolnymi interfejsami liniowymi w obrębie półki systemowej.			
36) System musi posiadać dostępność mechanizmów protekcji i restoracji w połączeniach DWDM.			
37) Architektura systemu DWDM musi realizować funkcjonalność ROADM (rekonfigurowalna optyczna krotnica transferowa) – optyczny węzeł transferowy (Optical Add Drop Multiplekser) z dodatkową funkcjonalnością zdalnej rekonfiguracji, przełączania kanałów optycznych w domenie optycznej, w ramach dostępnych w danym węźle kierunków sieci.			
38) System DWDM musi umożliwiać budowanie węzłów typu ROADM o ilości kierunków N>=4 (przełączanie dowolnego kanału optycznego na dowolny z N			

kierunków optycznych). Rekonfigurowalność musi być możliwa dla wszystkich kanałów optycznych.			
39) Urządzenie musi być przystosowane do przenoszenia strumieni klienckich SDH/PDH, FC i GE w warstwie 1, strumieni synchronicznych lub synchronizacji 1588v2 metodą hop by hop.			
40) Wszystkie urządzenia DWDM muszą posiadać przynajmniej 4 wolne interfejsy klienckie uniwersalne, wspierające sygnały STM64, 10GE LAN/WAN PHY, OTU-2/OTU2e.			
41) Węzeł DWDM dwukierunkowy (bez łącza skrośnego) musi mieć możliwość zestawienia kanałów optycznych 100GE, które podłączone zostaną do portów typu „dowolny kierunek" przestrajalnej sekcji multipleksacji. Łączna liczba interfejsów zgodna z ilością kierunków na węźle +1 (realizacja traffic on demand).			
42) Każdy węzeł DWDM z łączem skrośnym musi posiadać dodatkowy lub dodatkowe interfejsy 100GE dla umożliwienia połączenia skrośnego w trzecim kierunku połączenia oraz dodatkowe wolne interfejsy 100GE dla każdego kierunku DWDM.			
43) Urządzenie DWDM musi terminować kanały optyczne 100G, które należy podłączyć do portów urządzenia szkieletowego IP. Połączenia 100GE nie mogą być wykonane z pomięciem matrycy przełączającej OTN.			
44) W każdym węźle DWDM należy przewidzieć gotowe do podłączenia kanały cyfrowe SDH/PDH minimum 2xE1, E3, 2x STM-1, STM-4 i STM 64. Dopuszcza się możliwość rozszycia kanałów			

wysokich w dół przy użyciu zewnętrznego multipleksera SDH/PDH w przypadku braku możliwości realizacji w warstwie DWDM.			
49) Każde urządzenie DWDM musi posiadać wsparcie „end-to-end” dla transmisji 10G/40G/100G OSNR w zakresie raportowania i monitorowania dla natychmiastowej odpowiedzialności SLA.			
51) Każdy z zasilaczy może zapewniać każdemu z urządzeń pełną moc niezbędną do normalnego działania.			
53) System powinien umożliwiać zdalne monitorowanie i zarządzanie kanałami optycznymi i całym spektrum sygnału wielokanałowego DWDM			
54) Urządzenia DWDM muszą posiadać interfejs typu FE/GE służący do ich zarządzania poprzez połączenia tych portów do systemu out-of-band.			
55) Urządzenia DWDM muszą umożliwiać odczyt mocy optycznej sygnałów odbieranych na kartach liniowych (transponderach) zarówno po stronie portu liniowego jak i klienckiego.			
56) Urządzenie DWDM musi umożliwiać przeniesienie sygnałów DVB np.HDMI z kamer w węzłach szkieletowych do CZS.			
57) Każde urządzenie musi być wyposażone w nieulotną pamięć o pojemności pozwalającej na przechowywanie minimum dwóch wersji oprogramowania systemowego.			
59) Urządzenie musi zapewniać zbieranie statystyk dotyczących, jakości transmisji z bieżącego interwału min. 24 godzinnego i 15			

minutowego.			
60) Urządzenia muszą umożliwiać zdalną aktualizację oprogramowania. Procedura aktualizacji musi być odporna na ewentualne błędy i przerwy w transmisji oprogramowania na urządzenie. Proces związany z aktualizacją oprogramowania w urządzeniach DWDM nie może powodować przerw w ruchu.			
62) Urządzenie DWDM musi zapewniać odczyt zdarzeń, które wystąpiły w urządzeniu (ang. między innymi: alarmy dotyczące funkcjonowania urządzenia, alarmy dotyczące poprawności transmisji, przekroczenia zdefiniowanych progów (ang. threshold) wartości różnych parametrów (np. temperatury, poziomów mocy odbieranych sygnałów optycznych, błędów w transmisji), logowania użytkowników do systemu, przerwania światłowodu, podstawowych parametrów optycznych światłowodu itp.			

Minimalne parametry dla konfiguracji urządzeń Route Reflector			
Wymagany parametr zgodnie z pkt. OPZ	Oferowany parametr (lub potwierdzenie "TAK" Jeżeli Wykonawca realizuje funkcje w sposób dokładny jak w wymaganiu)	Rodzaj załączonego dokumentu, złożonego na potwierdzenie parametru (dokumenty techniczne autoryzowane przez producenta lub dystrybutora na teren polski danego	Miejsce w załączonym dokumencie wskazujący dany parametr (strona, rozdział, punkt lub wers)

		urządzenia lub karty katalogowe)	
3) Urządzenia pełniące funkcje „route-reflector” muszą być urządzeniami modularnymi typu router.			
6) Urządzania muszą posiadać modularną obudowę, przeznaczona do montażu w szafie 19”.			
7) Urządzenie modularne musi mieć wydajność pojedynczego slotu każdego urządzenia segmentu szkieletu sieci na poziomie sumy ilości portów znajdujących się na kartach danego slotu - „wirespeed”, np. w przypadku 12 portów 10GE obsługiwanej przez kartę umieszczonej w slocie urządzenia, wydajność tego slotu musi wynosić 120Gbps. Nie dopuszcza się nadsubskrypcji wydajności slotu w stosunku do sumy ilości portów.			
9) Wymagane jest aby wszystkie zainstalowane porty mogły działać jednocześnie.			
10) Architektura sprzętowa proponowanego routera powinna opierać się o tzw. pasywny backplane (ang. „passive backplane”).			
11) Wszystkie moduły kart linowych interfejsów muszą wspierać funkcję wymiany tzw. ,,na gorąco” (ang. hot-swap). Usuwanie lub dodawanie dowolnej karty liniowej interfejsów nie może degradować usług na pozostałych kartach liniowych			

interfejsów.			
12) Każde urządzenie musi mieć co najmniej jeden interfejs Ethernetowy 10/100/1000 Mbps przeznaczony do zarządzania urządzeniem w modelu Out Of band.			
14) Urządzenia powinny zapewniać obsługę synchronizacji częstotliwości przez implementację protokołów SyncE.			
15) Każde z urządzeń musi posiadać redundantny system zasilania. W przypadku awarii jednego z zasilaczy 48VDC, każdy kolejny zasilacz musi przejąć system w pełni obciążony.			
16) Urządzenia muszą posiadać funkcje statycznej agregacji portów przy pomocy protokołu LACP.			
17) Wszystkie urządzenia szkieletu IP muszą wspierać minimum następujące funkcje warstwy 3 OSI, opisane za pomocą norm informatycznych RFC (ang. Request for Comments):			
a) protokół OSPFv2 zgodnie z RFC2328 i protokół OSPFv3 zgodnie z RFC 2740,			
b) protokół IS-IS zgodnie z RFC 1142 i mechanizm „Three-Way Handshake for IS-IS” zgodnie z RFC 3373,			
c) mechanizm „Use of OSI IS-IS for routing in TCP/IP and Dual Environments” zgodnie z RFC 1195 i mechanizm „Dynamic Hostname Exchange Mecha-nism for IS-IS” zgodnie z RFC			

2763,			
d) mechanizm „IS-IS extensions for Traffic Engineering" zgodnie z RFC 3784 i mechanizm IS-IS Mesh Groups zgodnie z RFC 2973,			
e) mechanizm BFD dla protokołu ISIS i BGP,			
f) protokół BGPv4 zgodnie z RFC 1771,			
g) funkcję „BGP confederation" zgodnie z RFC 3065 i funkcję „BGP route reflector" zgodnie z RFC 2796,			
h) funkcję „BGP graceful restart" oraz wspierać funkcję autentykacji MD5 dla protokołu BGP zgodnie z RFC 2385 i mechanizm "Carrying Label Information in BGP-4" zgodnie z RFC 3107,			
i) funkcję BGP Route Flap Dampening zgodnie z RFC 2439,			
j) protokół ,,IPv6 Neighbor Discovery" zgodnie z RFC 2461 i IPv6 static routing,			
k) protokół BGP4+ zgodnie z RFC 4271,			
l) protokół IGMPv2 zgodnie z RFC2236 i protokół IGMPv3 zgodnie z RFC3376,			
m) protokół PIM-DM lub PIM-SM zgodnie z RFC 3973 oraz RFC 2362 i protokół PIM-SSM zgodnie z RFC 3569,			
n) protokół MP-BGP zgodnie z RFC 2858 i protokół VRRP zgodnie z RFC 5798,			
o) pamięć umożliwiająca obsługę minimum 6 milionów wpisów w tablicy RIB i minimum 2 milionów w tablicy			

FIB dla IPv4 oraz pamięć umożliwiająca obsługę minimum 2 milionów wpisów w tablicy RIB i minimum 500 tysięcy w tablicy FIB dla IPv6.			
18) .W celu łatwej migracji z protokołu IPv4 do protokołu IPv6, proponowane urządzenia szkieletu IP muszą zapewniać podstawowe mechanizmy takie jak tunelowanie (konfigurowane manualnie i automatycznie) dla wariantów IPv4 w IPv6, IPv6 w IPv4 i mechanizm „dual stack”.			
19) Urządzenia i karty linowe interfejsów muszą wspierać protokół IPv6 bez konieczności rozbudowy sprzętowej.			
20) Wszystkie urządzenia szkieletu IP muszą wspierać minimum następujące funkcje VPN/MPLS, opisane za pomocą norm informatycznych RFC (ang. Request for Comments):			
a) sprzętowa obsługa protokołów MPLS VPN i MPLS L2VPN			
b) obsługa statycznych ścieżek LSP			
c) obsługa BFD dla LSP max. 50ms			
d) obsługa protokołu LDP zgodnie z RFC 3036			
e) obsługa BFD dla LDP			
f) obsługa Fast Reroute dla LDP			
g) tunelowanie LDP over RSVP-TE.			
h) obsługa Graceful Restart dla LDP zgodnie z RFC 3478			

i) obsługa mechanizmu MPLS TE zgodnie z RFC 2702			
j) obsługa mechanizmów niezawodności dla MPLS TE: FRR, BFD, RSVP GR dla m.in. RFC 4090			
k) obsługa mechanizmu MPLS OAM zgodnie z 3429 lub RFC 4379 oraz RFC 4377 lub RFC 6425			
l) obsługa protokołu GRE zgodnie z RFC 2784			
m) obsługa protokołu IGP shortcut zgodnie z RFC 3906			
n) obsługa „RSVP-TE: Extensions to RSVP for LSP Tunnels” zgodnie z RFC 3209			
o) obsługa „TE Extensions to OSPF v2” zgodnie z RFC 3630			
p) obsługa BGP/MPLS IP VPN zgodnie z RFC 2547			
q) obsługa FRR dla BGP/MPLS IP VPN i GR dla BGP/MPLS IP VPN			
r) obsługa tuneli VLL w trybach Circuit Cross Connect (CCC) lub Switched Virtual Circuit (SVC), Kompella lub Martini zgodnie z RFC 4906			
s) obsługa mechanizmu Pseudo-Wire Emulation Edge to Edge (PWE3) zgodnie z RFC 3985			
t) obsługa protokołu VPLS oraz hierarchicznego VPLS			
u) obsługa agregowania tuneli VLL w tunelach VPLS, VPLS w L3VPN oraz VLL w L3VPN, w trybie VPLS muszą pracować w trybach Martini oraz AD (Auto Discovery) zgodnie z RFC 4761 oraz RFC 4762			

21) Każde z urządzeń musi mieć możliwość zarządzania zdalnego oraz lokalnego poprzez port konsoli lub Secure Shell w wersji minimum drugiej oraz minimum 1000 instancji VRF.			
22) Urządzenia muszą obsługiwać technikę podwyższania oprogramowania urządzenia (Upgrade) bez przestoju urządzenia w sieci (metoda ISSU).			
23) Urządzenia powinny posiadać nieulotną pamięć o wielkości pozwalającej na minimum przechowywanie dwóch wersji oprogramowania urządzenia.			
24) Urządzenia muszą być zarządzalne poprzez minimum SNMP v1, 2 i 3 oraz pakiety grupy Flow oraz posiadać wewnętrzny syslog.			

Minimalne parametry dla konfiguracji urządzeń funkcyjnych dostępu do sieci SSPW/IXP			
Wymagany parametr zgodnie z pkt. OPZ	Oferowany parametr (lub potwierdzenie "TAK" Jeżeli Wykonawca realizuje funkcje w sposób dokładny jak w wymaganiu)	Rodzaj załączonego dokumentu, złożonego na potwierdzenie parametru (dokumenty techniczne autoryzowane przez producenta lub dystrybutora na teren polski danego urządzenia lub karty katalogowe)	Miejsce w załączonym dokumencie wskazujący dany parametr (strona, rozdział, punkt lub wers)
5) Urządzanie lub urządzenia powinny posiadać obudowę modularną, przeznaczona do montażu w szafie 19”.			
6) Urządzenie modularne musi mieć wydajność pojedynczego slotu każdego urządzenia segmentu szkieletu sieci na poziomie sumy ilości			

portów znajdujących się na kartach danego slotu - „wirespeed”, np. w przypadku 12 portów 10GE obsługiwanej przez kartę umieszczonej w slocie urządzenia, wydajność tego slotu musi wynosić 120Gbps. Nie dopuszcza się nadsubskrypcji wydajności slotu w stosunku do sumy ilości portów.			
7) Każde urządzenie musi mieć możliwość minimum podwojenia ilości portów użytych w początkowej konfiguracji w tym urządzeniu – dodatkową ilość wolnych slotów.			
8) Wszystkie elementy krytyczne każdego urządzenia typu matryca przełączająca, moduły routujące muszą zostać zdublowane w każdym z urządzeń, w taki sposób aby awaria jednego z nich nie powodowała spadku wydajności całego urządzenia per slot.			
9) Wymagane jest aby wszystkie zainstalowane porty mogły działać jednocześnie z pełną prędkością.			
10) Wszystkie moduły kart linowych interfejsów muszą wspierać funkcję wymiany tzw. ,,na gorąco” (ang. hot-swap). Usuwanie lub dodawanie dowolnej karty liniowej interfejsów nie może degradować usług na pozostałych kartach liniowych interfejsów.			
11) Każde urządzenie musi mieć			

co najmniej jeden interfejs Ethernetowy 10/100/1000 Mbps przeznaczony do zarządzania urządzeniem w modelu Out Of band.			
12) Architektura sprzętowa urządzeń musi być oparta o tzw. rozproszony model dystrybucji (ang. „distributed forwarding architecture") i implementacja wszystkich usługi takich jak IPv4, MPLS L3VPN, MPLS L2VPN, VPLS, Multicast, IPv6, powinna również spełniać warunek rozproszonego modelu dystrybucji co pomaga zapobiegać powstawaniu problemów z wydajnością lub inaczej powstawaniu problemu tzw. „wąskiego gardła".			
13) Urządzenie powinno zapewniać obsługę synchronizacji częstotliwości przez implementację protokołów SyncE.			
14) Każde z urządzeń musi posiadać redundantny system zasilania. W przypadku awarii jednego z zasilaczy 48VDC, każdy kolejny zasilacz musi przejąć system w pełni obciążony.			
15) Wszystkie urządzenia szkieletu IP muszą wspierać minimum następujące funkcje warstwy 3 OSI, opisane za pomocą norm informatycznych RFC (ang. Request for Comments):			
a) protokół OSPFv2 zgodnie z RFC2328 i protokół OSPFv3 zgodnie z RFC 2740			
b) 2 typy sąsiedztwa możliwe			

do nawiązania przez protokół OSPF takie jak: Broadcast, NBMA, P2P and P2MP,			
c) mechanizm „OSPF graceful restart" zgodnie z RFC 3623 i mechanizm „OSPF Opaque LSA Option" zgodnie z RFC 2370,			
d) mechanizm BFD dla protokołu OSPF			
e) mechanizm OSPF NSSA Option zgodnie z RFC 3101 i mechanizm OSPF Database Overflow zgodnie z RFC 1765,			
f) protokół IS-IS zgodnie z RFC 1142,			
g) mechanizm „Three-Way Handshake for IS-IS" zgodnie z RFC 3373 i mechanizm „Use of OSI IS-IS for routing in TCP/IP and Dual Environments" zgodnie z RFC 1195,			
h) mechanizm „Dynamic Hostname Exchange Mechanism for IS-IS" zgodnie z RFC 2763 i mechanizm „IS-IS extensions for Traffic Engineering" zgodnie z RFC 3784,			
i) mechanizm IS-IS Mesh Groups zgodnie z RFC 2973,			
j) mechanizm BFD dla protokołu ISIS i BGP,			
k) protokół BGPv4 zgodnie z RFC 1771,			
l) funkcję „BGP confederation" zgodnie z RFC 3065 i funkcję „BGP route reflector" zgodnie z RFC 2796,			
m) funkcję „BGP graceful restart" oraz wspierać funkcję autentykacji MD5 dla protokołu BGP zgodnie z RFC 2385 i mechanizm "Carrying Label			

Information in BGP-4” zgodnie z RFC 3107,			
n) funkcję BGP Route Flap Dampening zgodnie z RFC 2439			
o) protokół ,,IPv6 Neighbor Discovery” zgodnie z RFC 2461 i IPv6 static routing,			
p) protokół BGP4+ zgodnie z RFC 4271,			
q) protokół IGMPv2 zgodnie z RFC2236 i protokół IGMPv3 zgodnie z RFC3376,			
r) protokół PIM-DM lub PIM-SM zgodnie z RFC 3973 oraz RFC 2362 i protokół PIM-SSM zgodnie z RFC 3569,			
s) protokół MP-BGP zgodnie z RFC 2858,			
t) protokół VRRP zgodnie z RFC 5798 lub RFC 3768,			
u) pamięć umożliwiająca obsługę minimum 6 milionów wpisów w tablicy RIB i minimum 2 milionów w tablicy FIB dla IPv4 oraz pamięć umożliwiająca obsługę minimum 2 milionów wpisów w tablicy RIB i minimum 500 tysięcy w tablicy FIB dla IPv6.			
16) .W celu łatwej migracji z protokołu IPv4 do protokołu IPv6, urządzenia funkcyjne muszą zapewniać podstawowe mechanizmy takie jak tunelowanie (konfigurowane manualnie i automatycznie) dla wariantów IPv4 w IPv6, IPv6 w IPv4 i mechanizm „dual stack”.			
17) Urządzenia i karty linowe interfejsów muszą wspierać protokół IPv6 bez konieczności rozbudowy sprzętowej.			

18) Wszystkie urządzenia funkcyjne muszą wspierać minimum następujące funkcje VPN/MPLS, opisane za pomocą norm informatycznych RFC (ang. Request for Comments):			
a) sprzętowa obsługa protokołów MPLS VPN i MPLS L2VPN			
b) obsługa statycznych ścieżek LSP			
c) obsługa BFD dla LSP max. 50ms			
d) obsługa protokołu LDP zgodnie z RFC 3036			
e) obsługa BFD dla LDP			
f) obsługa Fast Reroute dla LDP			
g) tunelowanie LDP over RSVP-TE.			
h) obsługa Graceful Restart dla LDP zgodnie z RFC 3478			
i) obsługa mechanizmu MPLS TE zgodnie z RFC 2702			
j) obsługa mechanizmów niezawodności dla MPLS TE: FRR, BFD, RSVP GR dla m.in. RFC 4090			
k) obsługa mechanizmu MPLS OAM zgodnie z RFC 3429 lub RFC 4379 oraz RFC 4377 lub RFC 6425			
l) obsługa protokołu IGP shortcut zgodnie z RFC 3906			
m) obsługa „RSVP-TE: Extensions to RSVP for LSP Tunnels” zgodnie z RFC 3209			
n) obsługa „TE Extensions to OSPF v2” zgodnie z RFC 3630			
o) obsługa BGP/MPLS IP VPN zgodnie z RFC 2547			
p) obsługa FRR dla BGP/MPLS			

IP VPN i GR dla BGP/MPLS IP VPN			
q) obsługa tuneli VLL w trybach Circuit Cross Connect (CCC) lub Switched Virtual Circuit (SVC), Kompella lub Martini lub równoważny zgodnie z RFC 4906			
r) obsługa mechanizmu Pseudo-Wire Emulation Edge to Edge (PWE3) zgodnie z RFC 3985			
s) obsługa protokołu VPLS oraz hierarchicznego VPLS			
t) obsługa agregowania tuneli VLL w tunelach VPLS, VPLS w L3VPN oraz VLL w L3VPN, w trybie VPLS muszą pracować w trybach Martini oraz AD (Auto Discovery) zgodnie z RFC 4761 oraz RFC 4762			
19) Każde z urządzeń funkcyjnych musi posiadać minimum 8000 list kontroli dostępu (ACL), musi mieć możliwość zarządzania zdalnego oraz lokalnego poprzez port konsoli lub Secure Shell w wersji minimum drugiej oraz minimum 2000 instancji VRF.			
20) Urządzenia muszą mieć możliwość wykrywania problemów na łączu pomiędzy urządzeniami za pomocą minimum protokołów EFM (802.3ah) i CFM (802.1ag).			
21) Urządzenia powinny posiadać nieulotną pamięć o wielkości pozwalającej na minimum przechowywanie dwóch wersji oprogramowania urządzenia.			
22) Urządzenia muszą być			

zarządzalne poprzez minimum SNMP v1, 2 i 3 oraz pakiety grupy Flow oraz posiadać wewnętrzny syslog.			
23) Każde urządzenie musi posiadać minimum dwa redundantne zasilacze 48VDC pozwalające na pracę każdego z nich niezależnie z pełnym obciążeniem urządzenia.			

Minimalne parametry dla konfiguracji urządzeń bezpieczeństwa dostępu do sieci IXP			
Wymagany parametr zgodnie z pkt. OPZ	Oferowany parametr (lub potwierdzenie "TAK" Jeżeli Wykonawca realizuje funkcje w sposób dokładny jak w wymaganiu)	Rodzaj załączonego dokumentu, złożonego na potwierdzenie parametru (dokumenty techniczne autoryzowane przez producenta lub dystrybutora na teren polski danego urządzenia lub karty katalogowe)	Miejsce w załączonym dokumencie wskazujący dany parametr (strona, rozdział, punkt lub wers)
4) Połączenia poprzez węzeł IXP muszą być możliwe do zdefiniowania jako połączenia przeźroczyste dla systemu bezpieczeństwa oraz połączenia filtrowane przez system bezpieczeństwa – firewall.			
5) System musi być systemem modularnym lub klastrowalnym przeznaczonym do montażu w szafie RACK z dwoma niezależnymi redundantnymi zasilaczami 48V DC.			
6) System musi działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym.			
7) System musi mieć możliwość jednoczesnej konfiguracji i pracy			

poszczególnych interfejsów sieciowych w różnych trybach (Access, Trunk, Hybrid).			
8) Interfejsy funkcjonujące w trybie transparentnym nie mogą posiadać skonfigurowanych adresów IP, również nie mogą wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.			
9) Każde urządzenie musi posiadać wydajność nie mniejszą niż 20Gb/s dla kontroli firewall z włączoną funkcją kontroli aplikacji oraz nie mniej niż 5 Gb/s przy włączonych wszystkich mechanizmach dla kontroli zawartości.			
10) Każde z urządzeń musi obsługiwać nie mniej niż 1700000 jednoczesnych połączeń (sesji), oraz nie mniej niż 100000 nowych sesji na sekundę.			
11) Urządzenia muszą obsługiwać (mechanizm filtrowania URL, mechanizmy IPS, mechanizmy AntyVirus dla wybranych strumieni ruchu).			
12) Minimalne funkcje zabezpieczeń realizowane poprzez firewall:			
a) obsługa IEEE 802.1q – jednoczesne wykorzystanie nie mniej niż 512 z puli 4096 VLANów,			
b) subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych, pracujących w trybie L2 i L3,			
c) system musi realizować zadania kontroli dostępu			

(filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji,			
d) system, zgodnie z ustaloną polityką, musi prowadzić kontrolę ruchu sieciowego pomiędzy określanymi obszarami sieci (strefami bezpieczeństwa),			
e) polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów,			
f) protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ),			
g) system zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną,			
h) system zabezpieczeń musi identyfikować co najmniej 1000 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS, nie mniej niż: Skype, Gadu-Gadu, Tor, BitTorrent, eMule,			
i) system zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych			

aplikacji (jeśli tworzenie takich sygnatur wymaga zewnętrznych narzędzi i/lub wsparcia producenta, to muszą być one dostarczone wraz z systemem),			
j) system zabezpieczeń musi umożliwiać zarządzanie, kontrolę i wgląd w ruch nierozpoznany przez urządzenie,			
k) system zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN,			
l) system zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego,			
m) system zabezpieczeń musi umożliwiać blokowanie transmisji plików, nie mniej niż: dll, doc, docx, ppt, pptx, xls, xlsx, rar, zip, exe, gzip, pdf, pgp, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME,			
n) system zabezpieczeń musi umożliwiać uruchomienia			

modułu inspekcji antywirusowej, kontrolującego przynajmniej protokoły poczty elektronicznej (SMTP, POP3, IMAP), FTP oraz HTTP i HTTPS. Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń,			
o) system zabezpieczeń musi umożliwiać uruchomienie modułu inspekcji antywirusowej dla strefy bezpieczeństwa,			
p) Dostarczona platforma musi posiadać możliwość wykreowania min. 5 instancji wirtualnych typu Firewall,			
q) Dostarczona platforma musi zapewnić możliwość rozbudowy niezależnych instancji wirtualnych typu Firewall do min. 100 bez konieczności rozbudowy sprzętowej, a jedynie poprzez dodatkowe licencje kupowane indywidualnie dla klientów.			
13) Minimalne wartości funkcji Intrusion Prevention:			
a) system zabezpieczeń musi umożliwiać uruchomienie modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent			

systemu zabezpieczeń,			
b) system zabezpieczeń musi umożliwiać uruchomienie modułu IPS/IDS dla strefy bezpieczeństwa,			
c) system zabezpieczeń musi umożliwiać uruchomienie modułu antyspyware. Baza sygnatur AS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń,			
d) system zabezpieczeń musi umożliwiać uruchomienie modułu antyspyware dla strefy bezpieczeństwa,			
e) system zabezpieczeń musi umożliwiać uruchomienie modułu filtrowania stron WWW w zależności od kategorii treści. Baza modułu filtrowania może być przechowywana na urządzeniu lub w innym miejscu sieci SSPW i regularnie aktualizowana w sposób automatyczny,			
f) system zabezpieczeń musi umożliwiać uruchomienie modułu filtrowania stron WWW dla strefy bezpieczeństwa,			
g) system zabezpieczeń musi posiadać funkcję wykrywania sieci Botnet,			
h) system zabezpieczeń musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP,			

i) system zabezpieczeń transparentnie ustala tożsamość użytkowników sieci (integracja z LDAP lub AD funkcjonującym w CZS),			
j) Polityka kontroli dostępu (firewall) precyzyjnie definiuje 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. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników,			
k) zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę internetowa za pomocą protokołu http i https . Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem,			
l) 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,			

m) system zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT,			
n) 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,			
o) system zabezpieczeń zapewnia możliwość bezpiecznego zdalnego dostępu do chronionych zasobów w oparciu o standard SSL VPN minimum 10 klientów,			
p) urządzenie zabezpieczeń musi posiadać wbudowany dysk do przechowywania logów i raportów,			
r) system zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie (w trybie Active-Passive lub w trybie Active-Active) poprzez zakup drugiego urządzenia.			

Minimalne parametry dla konfiguracji urządzeń węzła dystrybucji i NGA			
Wymagany parametr zgodnie z pkt. OPZ	Oferowany parametr (lub potwierdzenie "TAK" Jeżeli Wykonawca realizuje funkcje w sposób dokładny jak w wymaganiu)	Rodzaj załączonego dokumentu, złożonego na potwierdzenie parametru (dokumenty techniczne autoryzowane przez producenta lub dystrybutora na teren polski danego urządzenia lub karty katalogowe)	Miejsce w załączonym dokumencie wskazujący dany parametr (strona, rozdział, punkt lub wers)
4) Urządzenie dystrybucji IP musi być urządzeniem modularnym lub			

niemodularnym możliwym do zamontowania bezpośrednio w szafie 19' RACK.			
8) Każde urządzenie dystrybucyjne w węźle dystrybucyjnym musi zostać wyposażone w dwa zasilacze 48V DC, mogące pracować z pełną mocą pojedynczo.			
9) Każde z urządzeń dystrybucyjnych musi mieć wydajność bazową przełącznika w ilości sumy zainstalowanych portów 10GE oraz portów 1GE w przypadku urządzenia niemodularnego lub wydajność slotu dla sumy ilości portów na każdej karcie rozszerzeń dla każdego slotu w przełączniku modularnym – wire speed.			
10) Urządzenie musi mieć możliwość wymiany zasilaczy bez przerwy w jego działaniu.			
11) Urządzenie musi obsługiwać przełączanie w warstwie drugiej i trzeciej modeli ISO/OSI.			
12) Urządzenie musi posiadać co najmniej jeden interfejs przeznaczony do zarządzania urządzeniem w modelu Out Of band.			
13) Karty z interfejsami lub zainstalowane interfejsy stałe 10GE lub 1 GE muszą wspierać minimum 8 kolejek QoS oraz minimum 3 stopniowy HQoS.			
14) Urządzenie musi mieć możliwość statycznej agregacji portów przy pomocy protokołu minimum LACP oraz musi mieć możliwość stworzenia minimum 20 grup portów zagregowanych			

po minimum 4 portów.			
15) Każde urządzenie dystrybucyjne musi obsługiwać routing IPv4, IPv6 statyczny oraz dynamiczny przy pomocy protokołów minimum BGP, OSPF, IS-IS, RIP, RIPv2.			
16) Urządzenie musi sprzętowo obsługiwać MPLS VPN, LDP i tunele VLL.			
17) Urządzenie musi obsługiwać statyczne ścieżki LSP oraz minimum 200 VSI dla protokołu VPLS.			
18) Urządzenie musi obsługiwać protokoły Internetowe BGP/MPLS IP VPN oraz tunele RSVP-TE.			
19) Urządzenie musi wspierać Quality of Service poprzez minimum:			
a) kreowanie klas ruchu w oparciu o access control lists (ACLs), IEEE 802.1p precedence, IP, DSCP oraz Type of Service (ToS) precedence;			
b) wsparcie dla metod zapobiegania i przeciwdziałania zatorom: priority queuing, weighted round robin (WRR), weighted random early discard (WRED), deficit round robin (DRR) lub ich odpowiedniki;			
c) minimum 8 kolejek per port fizyczny lub logiczny.			
20) Urządzenie musi mieć możliwość zdalnej konfiguracji i zarządzania poprzez SNMP v 1, 2 i 3 oraz grupę protokołów typu Flow.			
21) Urządzenie musi mieć możliwość lokalnej konfiguracji			

poprzez port konsoli oraz posiadać lokalny syslog.			
22) System dystrybucyjny musi być w pełni zdalnie zarządzalny za pomocą jednego systemu zarządzania znajdującego się w CZS.			
23) Wszystkie porty elektryczne i optyczne muszą mieć możliwość zdalnej aktywacji i dezaktywacji.			