PKP INTERCITY
SPÓŁKA AKCYJNA
BIURO INFORMATYKI
Al. Jerozolimskie 142A
02-305 Warszawa

NR BFI-09 076-06-2018

Warszawa, dnia 2018-06-20

Z A P Y T A N I E O I N F O R M A C J Ę

.

W związku z planami zakupu routerów do sieci WAN, zwracamy się do Państwa z prośbą o udzielenie informacji cenowej dotyczącej dostawy, instalacji oraz konfiguracji urządzeń aktywnych - routerów w sieci Zamawiającego.

UWAGA do niniejszego Zapytania! „ PKP INTERCITY" S.A. zastrzega, że:

- *złożenie odpowiedzi na niniejsze Zapytanie o informację jest jednoznaczne z wyrażeniem zgody przez podmiot składający odpowiedź na nieodpłatne wykorzystanie przez Zamawiającego wszystkich, wskazanych w odpowiedzi na Zapytanie o informację danych do ewentualnego przygotowania przez Zamawiającego opisu przedmiotu zamówienia, wartości szacunkowej zamówienia, warunków umowy lub innych dokumentów niezbędnych dla Postępowania zakupowego z zastrzeżeniem, że Zamawiający nie ujawni podmiotom trzecim tych danych, a także źródła ich uzyskania*
- *niniejsze Zapytanie o informację nie jest elementem jakiegokolwiek postępowania o udzielenie zamówienia w rozumieniu ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2017 r. poz. 1579 z późn. zm.), czy też Postępowania zakupowego prowadzonego w oparciu o wewnętrzną procedurę zakupową w „PKP Intercity" S.A.,*
- *niniejsze Zapytanie nie stanowi oferty w rozumieniu ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2016 r. poz. 380 z późn. zm.) niniejsze zapytanie nie stanowi elementu jakiegokolwiek postępowania o udzielenie zamówienia, wobec czego PKP INTERCITY S.A. nie jest zobligowane do wyboru którejkolwiek oferty. Niniejsze pismo nie stanowi również oferty w rozumieniu Kodeksu Cywilnego*.

Przedmiot Zapytania

Do realizacji sieci Zamawiający wykorzysta posiadane łącza WAN. Sieć główna jest realizowana w technologii VPN, sieć backupowa jest realizowana w oparciu o technologię MPLS lub Internet. Sieci VPN, MPLS, i INTERNET będą stanowić sieci transportowe. Zainstalowane routery mają łączyć ruch z sieci transportowej w jedną logiczną sieć WAN. Routery mają współpracować z istniejącą siecią Zamawiającego tworząc jedną dużą logiczną sieć. Obecnie wykorzystywane routery w sieci WAN:

1. Cisco C3900-SPE250/K9
2. Cisco ASR1001

W szczególności sieć ma być tak skonfigurowana, aby:

1. Ruch w sieci WAN był kierowany przez łącze na podstawie:
   a. Tablicy rutingu.
   b. Metryk, takich jak:
      i. Maksymalne opóźnienie pakietów;
      ii. Zmienność opóźnień pakietów;
      iii. Straty w pakietach;
      iv. QoS.

c. Zamawiający oczekuje systemu zarządzania i monitorowania sieci WAN pozwalającego w sposób inteligentny sterować ruchem oraz rozkładać go w sposób równomierny na sieć główną i backupową w szczególności:
   i. System powinien w sposób pasywny lub aktywny monitorować parametry wydajnościowe dla danej klasy ruchu. Pasywny monitoring bazuje na pomiarze metryk wydajnościowych dla danej klasy ruchu, gdy taki ruch jest przesyłany przez sieć. Natomiast tryb aktywny, aktywowany jest automatycznie, gdy nie występuje w sieci ruch danego typu i bazuje na generowaniu przez router próbek ruchu;
   ii. System powinien umożliwiać automatyczny wybór najlepszej ścieżki ruchu dla danej aplikacji lub klasy ruchu w sieci WAN w oparciu o kryteria, jakości lub wydajności pracy sieci;
   iii. System powinien posiadać wbudowane wzorce kryteriów jakościowych (opóźnienie, jitter, straty) dla typowych aplikacji takich jak: wideo czasu rzeczywistego, głos, dane o małej tolerancji na opóźnienie, ruch typu best-effort. Oraz system powinien umożliwiać definiowanie własnych wzorców;
   iv. System powinien realizować centralną konfigurację polityki sterowania ścieżkami ruchu dla danych aplikacji sieciowych (klas ruchu sieciowego) oraz kryteriów wyboru ścieżki;
   v. System powinien w sposób przejrzysty wizualizować topologię sieci WAN wraz z wszystkimi łączami oraz danymi o:
      1. opóźnieniu całkowitym strumienia;
      2. opóźnieniu i ilości danych przesłanych przez klienta;
      3. opóźnieniu i ilości danych przesłanych przez serwer;
      4. opóźnieniu wynikającym z przetwarzania właściwego dla aplikacji;
      5. strat pakietów;
      6. retransmisji;
      7. zmienności opóźnień;
      8. dla ruchu UDP/RTP - informacje o opóźnieniach, zmienności opóźnień, SSRC w przypadku RTP, stratach w pakietach;
   vi. System powinien być wyposażony w generator raportów pozwalający filtrować je w sposób analogiczny do filtrów Wiresharka. Przy czym powinna występować możliwość generowania raportów na bieżąco jak i korzystając z danych historycznych, oraz:
      1. możliwość wyszukiwania po adresach / portach źródłowych i docelowych;
      2. możliwość wyszukiwania po nazwie wykrytej aplikacji;
      3. możliwość wyszukiwania po nazwie oddziału;
      4. możliwość wyszukiwania po DSCP;
      5. możliwość wyszukiwania po URL wykrytej aplikacji HTTP;
      6. powinien pokazywać poziom zajętości pamięci, CPU i przepustowości na interfejsach;
      7. powinien pokazywać informacje o politykach QoS – z podziałem na klasy ruchu i informacją, ile jest strat w ramach klas i jaki jest poziom ruchu w poszczególnej klasie;
      8. powinien informować o wykrytych aplikacjach – ile dana aplikacja wysyła ruchu, wskazanie URL aplikacji http, wskazanie opóźnień, retransmisji;
      9. powinna informować, na którym łączu, jakie są parametry łącza, w jakim stopniu są zajęte łącza, jakimi klasami ruchu;
      10. powinna informować o stanie próbek IP SLA, lub równoważnych;
   vii. System powinien analizować ruchu dla konkretnego strumienia - ze wskazaniem urządzeń, interfejsów, ACL i polityk QoS, przez które przechodzi dany ruch:
      1. analiza pod kątem strat pakietów w kolejkach QoS;
      2. analiza pod kątem wykroczeń poza zdefiniowane progi opóźnień, zmienności opóźnień, strat dla danych klas ruchu;

viii. System powinien umożliwiać wizualizacje ścieżki dla danego ruchu wynikającej ze stanu protokołów routingu - w porównaniu do aktualnego przebiegu tego samego ruchu na bazie informacji z uzyskanych strumieni;
ix. System powinien umożliwiać tworzenia sond IP SLA - dla aplikacji takich jak DHCP, DNS, HTTP, FTP, lub opóźnień, zmienności opóźnień, strat - wraz z wizualizacją wyniku wydajności wynikających z tych sond;
x. System powinien umożliwiać zakładanie alarmów na wykroczenia poza normalne zachowanie w sieci i wysyłania maila w razie np. wykroczenia poza ustalony próg dozwolonych parametrów (np. opóźnień, zmienności opóźnień, strat, retransmisji itp.) dla danej klasy ruchu - a także w przypadkach krytycznych, jak awaria ścieżki / łącza;
xi. System powinien wizualizować strumień ruchu z podziałem na aplikacje, (jeśli zostały wykryte) i numerami portów na interfejsach urządzeń sieciowych;
    1. wskazanie poziomu ruchu na interfejsach;
    2. wskazanie klas polityki QoS na interfejsach wraz ze stratami w poszczególnych klasach ruchu;

2. Ruch między routerami ma być szyfrowany z wykorzystaniem algorytmów DES/3DES/AES lub równoważne dla całości ruchu.
3. Ruch ma być przełączany na ścieżkę zapasową w przypadku awarii łącza głównego oraz:
    a. W pełni redundantna infrastruktura węzłów centralnych, odporność na 2 jednoczesne awarie w lokalizacjach Centralnych;
    b. Czas przerwy dla ruchu w relacji oddział - centrala związany z przełączeniem ścieżki ruchu, która uległa awarii na alternatywną nie dłuższy niż 30 sek;
    c. Czas przerwy dla ruchu w relacji oddział – oddział związany z przełączeniem ścieżki ruchu, która uległa awarii na alternatywną nie dłuższy niż 60 sek;
    4. Ruch w sieci ma być przełączany na router zapasowy w przypadku awarii routera głównego w węzłach wyposażonych w redundantne routery w układzie active-active.
    5. Ruch między routerami powinien wykorzystywać własny protokół rutingu dynamicznego oraz adresacji IP niezależnie od typu i sposobu funkcjonowania sieci transportowych wykorzystywanych do budowy sieci WAN. Funkcjonalność niezależnego transportu powinna bazować na protokole DMVPN/DSVPN (dynamiczne wielopinktowe sieci prywatne), lub równoważnych oraz tworzyć w pełni zarządzaną nakładkę na sieci transportowe.
        a. Powinna występować możliwość obsługi tuneli wielopunktowych po stronie routerów centralnych (w kolokacji) i routerów w oddziałach,
        b. Powinny tworzyć się automatyczne żądania szyfrowania tuneli pomiędzy oddziałami, gdy pojawi się ruch między nimi,
        c. Powinna występować obsługa protokołów rutingu w tunelach takich jak BGP,OSPF lub równoważnych,
        d. Powinna występować automatyczna rejestracja routerów oddziałowych w routerze centralnym w celu zmapowania adresu IP tunelu do adresu IP w sieci transportowej. Możliwość ukrycia routera oddziałowego za NAT. Obsługa trybu statycznego przypisania adresu IP dla routera WAN jak również dynamicznego przypisania w oparciu o DHCP,
        e. Powinien występować brak konieczności dokonywania zmian w konfiguracji routerów centralnych w momencie dołączenia kolejnych placówek oddziałowych,
        f. Powinna występować obsługa ruchu multicast w sieci nakładkowej,
        g. Powinna występować realizacja QoS per tunel – możliwość definiowania na routerze centralnym dla każdego routera oddziałowego innej polityki QoS przypisanej do ruchu tunelowanego w oparciu o przynależność oddziału do danej grupy (kategorii

oddziałów). Eliminacja zjawiska nadsubskrypcji (przepełnienia) łącza w oddziale przez ruch wysyłany przez łącze o większej przepustowości ze strony centrali,

h. Powinna występować jednoczesna obsługa więcej niż jednej sieci DMVPN na routerze oddziałowym w celu tworzenia więcej niż jednej ścieżki transportowej w sieci WAN np. możliwość wykorzystania, jako łącza podstawowego łącza MPLS, jako łącza zapasowego łącza stałego VPN, a jako tzw. łącza „ostatniej szansy" łącza INTERNET,

i. Powinna występować funkcjonalność fVRF (front door VRF) umożliwiająca umieszczenie fizycznego interfejsu połączeniowego do sieci transportowej IP np. interfejs Ethernet, Serial, LTE itd. w wydzielonym w ramach routera fizycznego routerze logicznym (wirtualnej instancji routingu - VRF) w celu separacji controlplane (tablice routingu, tablice przesyłania ruchu) i protokołów routingu używanych w sieci prywatnej i sieciach transportowych. Realizacja funkcjonalności, w której tunel IPSEC/GRE terminowany jest w routerze logicznym (VRF) a pakiety IP po rozszyfrowaniu i dekapsulacji przekazywane są do innego logicznego routera obsługującego ruch prywatny w sieci WAN. Dzięki tej funkcjonalności Zamawiający oczekuje możliwej prostej wymiany łącza dostępowego w danej placówce oddziałowej z operatora A na operatora B lub na łącza internetowe pochodzące od dowolnego operatora bez konieczności ingerowania w sieć nakładkową,

6. W sieci Wan powinny być wdrożone funkcje akceleracji i optymalizacji działania aplikacji:
   a. Zamawiający oczekuje skuteczność redukacji ruchu na łączach WAN do około 50 %;
   b. Kompresje ruchu;
   c. Optymalizacje połączeń TCP;
   d. Zmniejszenie rozmiaru przesyłanych danych poprzez wysyłanie krótkich indeksów numerycznych zamiast powtarzających się bloków danych;
   e. Optymalizacja algorytmu TCP;
   f. Deduplikacja ruchu sieciowego;
   g. Współpraca z centralnym systemem zarządzania optymalizatorami ruchu sieciowego pełniącym funkcje centralnego punkt ich konfiguracji, monitorowania w czasie rzeczywistym, zarządzania błędami i raportowania;
   h. Wsparcie akceleracji dla wielu aplikacji w tym:
      i. CIFS (SMBv2)
      ii. NFSv3
      iii. Exchange 2003/2007/2010 (MAPI)
      iv. Encrypted MAPI
      v. Microsoft SQL
      vi. Oracle
      vii. SSL
      viii. HTTP
      ix. Microsoft Office 365
      i. Funkcjonalność pozwalająca przesyłanie plików do cache'ów oddziałów poza godzinami pracy oddziału;
7. W sieci WAN powinna być wdrożona funkcja działania aplikacji sieciowych w tym:
   a. Realizacja hierarchicznego QoS (H-QOS);
   b. Funkcjonalność sondy IP SLA do mierzenia parametrów ruchu dla protokołu IP;
   c. Ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU;
   d. Realizacja logowania pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU;

e. Funkcjonalność umożliwiająca rozpoznawanie aplikacji do warstwy L7 na bazie analizy zawartości pakietów;
f. Realizacja wydajnego eksportu statystyk ruchowych za pomocą protokołu NetFlow lub równoważnego. W ramach NetFlow obsługa tzw. FlexibleNetFlow umożliwiającego rozszerzenie funkcjonalności NetFlow o możliwość dodawania dodatkowych własnych pól kluczowych i niekluczowych przez użytkownika w celu bardziej szczegółowej identyfikacji i śledzenia statystyk ruchu sieciowego.

Zamawiający oczekuje realizacji sieci WAN w oparciu o routery opisane w:

- Załączniku 1 – typ A
- Załączniku 2 – typ B

w ilościach jak w Tabeli nr 1 poniżej.

Tabela 1. Lista lokalizacji

l.p.	Lokalizacja	Sprzęt	Typ A Ilości	typ B Ilości
1	Gdynia ul. Osada Kolejowa 12	2 x router typ A	2	
2	Szczecin ul. Kanał Parnicki 1k	1 x router typ B		1
3	Bydgoszcz ul. Zygmunta Augusta 7	1 x router typ B		1
4	Białystok ul. Kolejowa 11	1 x router typ B		1
5	Poznań Al. Niepodległości 8	2 x router typ A	2	
6	Łódź ul. Służbowa 10	1 x router typ B		1
7	Wrocław ul. Paczkowska 26	2 x router typ B		2
8	Katowice ul. Murckowska 1	1 x router typ B		1
9	Kraków ul. Półłanki 1	2 x router typ A	2	
10	Skawina ul. Krakowska 43	2 x router typ B		2
11	Rzeszów Plac Dworcowy 1	1 x router typ B		1
12	Warszawa ul. Szlachecka 49	2 x router typ B		2
13	Warszawa tzw. Mała kolokacja	2 x router typ A	2	
14	Warszawa ul. Chłopickiego 53	2 x router typ B		2
15	Warszawa Dworzec Centralny	2 x router typ B		2
16	Warszawa Dworzec Wschodni	1 x router typ B		1
18	Warszawa ul. Szczęśliwicka 62	1 x router typ B		1
19	Piaseczno, kolokacja, ul. Jana Pawła II 66	2 x router typ A	2	

router typ A	10
router typ B	18

Wymagania dotyczące realizacji usługi wsparcia serwisowego:

1. 1 Usługa wsparcia serwisowego będzie świadczona przez 1 rok (365 dni) lub 3 lata
1. 2 Usługi będą świadczone w miejscach lokalizacji sprzętu lub za zgodą Zamawiającego zdalnie, o ile będzie to zgodne z polityką bezpieczeństwa Zamawiającego. Zamawiający zastrzega sobie możliwość zmiany lokalizacji urządzeń w trakcie trwania Umowy, o każdorazowej zmianie

lokalizacji Zamawiający poinformuje Wykonawcę w formie pisemnej, z co najmniej 14-dniowym wyprzedzeniem.

1. 3 Awarie i zgłoszenia będą zgłaszane przez Zamawiającego bezpośrednio w serwisie Wykonawcy w trybie 24x7x365.
1. 4 Awarie będą usuwane w sposób:
   1. 74..1 ciągły od czasu zgłoszenia w trybie 24x7x365 dla pojedynczych urządzeń bez rozwiązań redundantnych,
   1.4.2 ciągły od czasu zgłoszenia w trybie 24x7x365 dla urządzeń redundantnych w przypadku jednoczesnego uszkodzenia obu urządzeń w lokalizacji,
   1.4.3. ciągły w godzinach roboczych dla urządzeń redundantnych w przypadku, gdy uległo awarii tylko jedno urządzenie w lokalizacji.

Przez godziny robocze Zamawiającym rozumie godziny od 8.00 do 16.00 we wszystkie dni z wyłączeniem świąt i dni ustawowo wolne od pracy.

1. 5 Wykonawca dokona naprawy lub udostępni obejście w czasie do 4 godzin dla urządzeń objętych awarią zgodnie z warunkiem 4.4.2, do 6 godzin dla urządzeń objętych awarią zgodnie z warunkiem 4.4.1 oraz do 6 godzin roboczych od zgłoszenia awarii w pozostałych przypadkach.
1. 6 W przypadku stwierdzenia konieczności wymiany dysku twardego, będzie on wymieniony na nowy, wolny od wad, bez konieczności zwrotu uszkodzonego dysku i dokonywania ekspertyzy poza miejscem użytkowania przedmiotu Umowy.
1. 7 W ramach usług wsparcia do obowiązków Wykonawcy należy:
   1.7.1 Prowadzenie CMDB dla sprzętu objętego umową.
   1.7.2 Przeprowadzenie przeglądu okresowego działania urządzenia, co najmniej raz na 6 miesięcy. Przy czym wymagany jest również przegląd urządzeń w ostatnim miesiącu świadczenia wsparcia serwisowego.
   1.7.3 Obsługa i diagnostyka zgłoszonych błędówZgłaszanie błędów i incydentów w serwisie sprzętowym producenta oraz monitorowanie realizacji tych zgłoszeń.
   1.7.4 Eskalacji zgłoszonego Incydentu do Centrum Serwisowego Producenta.
   1.7.5 Wymiana części lub całego elementu uszkodzonej infrastruktury sprzętowej.
   1.7.6 Demontaż i odbiór uszkodzonego Urządzenia.
   1.7.7 Dostarczenie i podłączenie w rack-u Urządzenia (naprawionego lub zastępczego) w tym zamontowanie, podłączenie kabli zasilających AC i DC, podłączenie kabli sieciowych, miedzianych i światłowodowych, dostarczonych przez Klienta.
   1.7.8 Instalację/aktualizację odpowiedniego firmware lub Oprogramowania systemowego, w tej samej wersji, jaka była zainstalowana na Urządzeniu uszkodzonym, zgodnie z licencją posiadaną przez Klienta; wgrywanie dostarczonej przez Klienta konfiguracji.
   1.7.9 Udostępnianie poprawek, aktualizacji i nowych wersji Oprogramowania udostępnianych przez Producenta oraz wskazywanie ryzyk i udzielanie rekomendacji w zakresie pilności ich wprowadzenia.
   1.7.10 Wsparcie telefoniczne Klienta podczas wgrywania firmware'u, konfiguracji, aktualizacji Oprogramowania lub wgrywanie tych elementów podczas przeglądów okresowych po uzgodnieniu takiej potrzeby z Klientem.
   1.7.11 Każdorazowo po naprawie urządzenia oraz w trakcie przeglądów półrocznych przeprowadzenie testu sprawdzającego prawidłowe działanie Urządzenia, uwzględniające inne urządzenia aktywne Klienta.
   1.7.12 Dostarczanie rekomendacji zmian do Zamawiającego w zakresie poprawy, jakości działania urządzenia lub jego środowiska a w szczególności specyfikacji sprzętu w

przypadku potrzeby wzmocnienia/wymiany na wydajniejsze Urządzenia objęte serwisem.

1. 8 Do obowiązków Zamawiającego należeć będzie:
   - 1.8.1 Dokonanie zgłoszenia oraz dostarczenie informacji niezbędnych do poprawnego zarejestrowania zgłoszenia.
   - 1.8.2 Udzielanie informacji dodatkowych, dokumentacji lub wyjaśnień w przypadku, gdy zgłoszenie jest niekompletne lub wymaga uzupełnienia.
   - 1.8.3 Wykonywanie i udostępnianie kopii zapasowych Oprogramowania systemowego i konfiguracji Urządzeń objętych Usługą serwisową.
   - 1.8.4 Udostępnianie podstawowych informacji na temat topologii połączenia Urządzenia z innymi urządzeniami aktywnymi.
   - 1.8.5 Zapewnienie miejsca instalacji urządzenia.
   - 1.8.6 Udostępniania niezbędnych kodów, kluczy, certyfikatów lub tokenów, jeśli są one niezbędne dla odtworzenia konfiguracji urządzenia.
   - 1.8.7 Informowanie o wykonanych samodzielnie aktualizacjach Oprogramowania według zaleceń Wykonawcy.
1. 9 W ramach zakupionych usług wsparcia serwisowego Zamawiającemu zostaną zapewnione:
   - 1.9.1 Bieżące zarządzanie zgłoszeniami serwisowymi składanymi w centrum pomocy technicznej producenta oraz eskalacjami (otwieranie zgłoszeń serwisowych, monitorowanie zgłoszonych problemów bezpośrednio przez Zamawiającego).
   - 1.9.2 Dostęp do ekspertów technicznych Producenta poprzez centrum pomocy technicznej Producenta, obejmujący pomoc ekspertów technicznych Producenta przy diagnostyce problemów związanych z funkcjonowaniem urządzeń Producenta użytkowanych w infrastrukturze Zamawiającego.
1. 10 Nie później niż 10 dni licząc od dnia zawarcia umowy Dostawca zobowiązany będzie dostarczyć Zamawiającemu wszelkie niezbędne dane umożliwiające Zamawiającemu skorzystanie z usług objętych Umową zawierające, co najmniej:
   - 1.10.1 Dane dostępowe do witryny wsparcia technicznego producenta,
   - 1.10.2 Numer aktualnej umowy serwisowej nadawanej przez producenta,
   - 1.10.3 Oświadczenie producenta potwierdzające wykupienie i aktywacje dla Zamawiającego serwisu producenta z wyszczególnieniem okresu ważności (w tym z uwzględnieniem faktu, że na niektóre urządzenia usługa wsparcia może być aktywna w dacie zawarcia umowy). W przypadku urządzeń, dla których usługa serwisu jest aktywna w dacie zawarcia umowy, Usługa wsparcia powinna zostać przedłużona w celu zapewnienia zrównania okresów jej ważności w systemie Producenta.

Terminy składania pytań oraz udzielenie informacji:

1. Termin składania informacji upływa w dniu **29.06.2018 do godziny 11:00** (ewentualne pytania prosimy kierować do dnia 25.06.2018 r. do godziny 12:00).
2. Odpowiedź proszę przesłać w formie e-mail na adres: **it@intercity.pl**

Informacja cenowa

Oczekiwana forma odpowiedzi:

Urządzenia proponowane, jako Model docelowy:

L.P.	Nazwa/Model	Typ i producent	Cena Brutto	Cena netto Instalacji i konfiguracji urządzenia

Koszt serwisu:

L.P.	Typ urządzenia	Serwis roczny	Serwis trzyletni
	router typ A		
	router typ B		

Załącznik nr 1 do Opisu Przedmiotu Zamówienia

Router typ A
Każdy router powinien spełniać poniższe wymagania:

Rodzaj urządzenia
Powinno być urządzeniem pełniącym rolę wielousługowego routera modularnego gotowego do obsługi mechanizmów bezpiecznej i niezawodnej sieci WAN w oparciu o Internet lub VPN MPLS.

Wymagana Architektura:

1. Pozwala na instalację, co najmniej 2 kart sieciowych z interfejsami z możliwością wyłączenia modułu w celu oszczędności energii,
2. Posiada możliwość bezpośredniej komunikacji pomiędzy modułami z pominięciem głównego procesora, jeśli ruch sieciowy nie jest skierowany do routera,
3. Posiada wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych nieprzewidzianych w Umowie. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.

Oczekiwana wydajność:

4. Urządzenie oferuje wydajności, co najmniej 1000 Mbps dla ruchu typu IMIX, co najmniej 800 Mbps dla ruchu szyfrowanego.
5. Wydajność, co najmniej 215 Mbps dla uruchomionej funkcji – agregacja ruchu WAN

Wymagane Oprogramowanie/funkcjonalność:

6. obsługa protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i SSM) oraz routing statyczny,
7. obsługa protokół BGP 4 bajtowych ASN,
8. wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv2,
9. obsługa protokołu IGMPv3,
10. obsługa mechanizmu Unicast Reverse Path Forwarding (uRPF),
11. obsługa tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q,
12. obsługa IPv6 w tym ICMP dla IPv6,
13. obsługa list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP,
14. obsługa NAT dla ruchu IP unicast oraz PAT dla ruchu IP unicast,
15. obsługa wirtualnych instancji routingu (VRF) - co najmniej 64 instancji VRF,
16. obsługa mechanizmu DiffServ,
17. możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu,
18. obsługa mechanizmów kolejkowania ruchu:
    a. z obsługą kolejki absolutnego priorytetu,

b. ze statyczną alokacją pasma dla typu ruchu,

c. WFQ (Weighted fair queueing),

19. obsługa mechanizmu WRED (Weighted random early detection),
20. obsługa mechanizmu Traffic Shaping,
21. obsługa mechanizmu ograniczania pasma dla określonego typu ruchu,
22. obsługa protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego,
23. obsługa protokołu NTP**,**
24. obsługa DHCP w zakresie Client, Server,
25. obsługa tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub równoważny),
26. obsługa mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+,
27. obsługa protokołu MPLS (funkcje LER i LSR),
28. obsługa MPLS over GRE,
29. wsparcie QoS dla MPLS,
30. obsługa MPLS Traffic Engineering,
31. obsługa MPLS VPN,
32. obsługa funkcjonalności Multicast dla MPLS VPN,
33. obsługa funkcjonalności Bidirectional Forwarding Detection (BFD) lub równoważny,
34. dostępność funkcjonalności BFD dla interfejsów skonfigurowanych do współpracy z VRF,
35. obsługa funkcjonalności BFD Echo Mode lub równoważna,
36. wsparcie funkcjonalności BFD (lub równoważna) dla protokołów BGP, OSPF, IS-IS, routingu statycznego oraz VRRP lub równoważna,
37. funkcjonalność PPPoE,
38. wsparcie dla Layer-2 Tunneling Protocol,
39. możliwość integracji z centralnym systemem zarządzania, monitorowania, konfiguracji jak również troubleshootingu,
40. możliwość obsługi przez zcentralizowany system zarządzania w celu zmiany wersji systemu operacyjnego,
41. oferuje zaawansowane funkcjonalności bezpieczeństwa takie jak: Zone Based Firewall (ZBF), IPSec VPN, możliwość uruchomienia dynamicznych sieci VPN w technologii Dynamic Multipoint VPN (DMVPN/DSVPN) lub odpowiednika opartego na otwartych standardach.

Wymagane zarządzanie i konfiguracja:

42. zarządzalne za pomocą SNMPv3,
43. konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface — CLI) jak również interfejsu graficznego (GUI),
44. plik konfiguracyjny urządzenia będzie możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej będzie możliwe uruchomienie urządzenia z nową konfiguracją. Urządzenie musi umożliwiać wykonanie kopii pliku konfiguracyjnego urządzenia na zdalny serwer TFTP lub SCP/SFTP poprzez wysłanie specjalnego żądania z systemu zarządzania siecią wykorzystując protokół lub SNMPv3.

Obudowa:

45. wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej,
46. ma możliwość montażu w szafie rack 19" oraz musi zostać dostarczone z zestawem umożliwiającym montaż w tej szafie,
47. wielkość urządzenia maksymalnie 3U,

Zasilanie:

48. wbudowane dwa zasilacze umożliwiające zasilanie prądem przemiennym 230V,

Wyposażenie:

49. wyposażone w minimum 4 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN/WAN,
50. minimum jeden z interfejsów opisanych powyżej ma możliwość pracy w trybie „dual-physical" z portem RJ45 lub giga bitowym portem światłowodowym definiowanym przez moduł GBIC lub SFP,
51. wyposażone w minimum jeden port USB (min. 1.0). Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych,
52. urządzenie będzie dostarczone z kablami pozwalającymi na podłączenie szeregowej konsoli, jak również kablami zasilającymi,

Wyposażenie dodatkowe urządzenia:

53. 1 szt. SFP GLC-SX-MM 1G, (wkładka wspierana przez producenta sprzętu).

Załącznik nr 2 do Opisu Przedmiotu Zamówienia

Router typ B
Każdy router powinien spełniać poniższe wymagania:

Rodzaj urządzenia
Powinno być urządzeniem pełniącym rolę wielousługowego routera modularnego gotowego do obsługi mechanizmów bezpiecznej i niezawodnej sieci WAN w oparciu o Internet lub VPN MPLS.

Wymagana Architektura:

54. Pozwala na instalację, co najmniej 2 kart sieciowych z interfejsami z możliwością wyłączenia modułu w celu oszczędności energii,
55. Posiada możliwość bezpośredniej komunikacji pomiędzy modułami z pominięciem głównego procesora, jeśli ruch sieciowy nie jest skierowany do routera,
56. Posiada wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych nieprzewidzianych w Umowie. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.

Oczekiwana wydajność:

57. Urządzenie oferuje wydajności, co najmniej 100 Mbps dla ruchu typu IMIX, co najmniej 90 Mbps dla ruchu szyfrowanego.
58. Wydajność, co najmniej 70 Mbps dla uruchomionej funkcji – agregacja ruchu WAN

Wymagane Oprogramowanie/funkcjonalność

59. obsługa protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i SSM) oraz routing statyczny,
60. obsługa protokół BGP 4 bajtowych ASN,
61. wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv2,
62. obsługa protokołu IGMPv3,
63. obsługa mechanizmu Unicast Reverse Path Forwarding (uRPF),
64. obsługa tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q,
65. obsługa IPv6 w tym ICMP dla IPv6,
66. obsługa list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP,
67. obsługa NAT dla ruchu IP unicast oraz PAT dla ruchu IP unicast,
68. obsługa wirtualnych instancji routingu (VRF) - co najmniej 64 instancji VRF,
69. obsługa mechanizmu DiffServ,
70. możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu,
71. obsługa mechanizmów kolejkowania ruchu:
    a. z obsługą kolejki absolutnego priorytetu,

b. ze statyczną alokacją pasma dla typu ruchu,

c. WFQ (Weighted fair queueing),

72. obsługa mechanizmu WRED (Weighted random early detection),
73. obsługa mechanizmu Traffic Shaping,
74. obsługa mechanizmu ograniczania pasma dla określonego typu ruchu,
75. obsługa protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego,
76. obsługa protokołu NTP**,**
77. obsługa DHCP w zakresie Client, Server,
78. obsługa tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub równoważny),
79. obsługa mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+,
80. obsługa protokołu MPLS (funkcje LER i LSR),
81. obsługa MPLS over GRE,
82. wsparcie QoS dla MPLS,
83. obsługa MPLS Traffic Engineering,
84. obsługa MPLS VPN,
85. obsługa funkcjonalności Multicast dla MPLS VPN,
86. obsługa funkcjonalności Bidirectional Forwarding Detection (BFD) lub równoważny,
87. dostępność funkcjonalności BFD dla interfejsów skonfigurowanych do współpracy z VRF,
88. obsługa funkcjonalności BFD Echo Mode lub równoważna,
89. wsparcie funkcjonalności BFD (lub równoważna) dla protokołów BGP, OSPF, IS-IS, routingu statycznego oraz VRRP lub równoważna,
90. funkcjonalność PPPoE,
91. wsparcie dla Layer-2 Tunneling Protocol,
92. możliwość integracji z centralnym systemem zarządzania, monitorowania, konfiguracji jak również troubleshootingu,
93. możliwość obsługi przez zcentralizowany system zarządzania w celu zmiany wersji systemu operacyjnego,
94. oferuje zaawansowane funkcjonalności bezpieczeństwa takie jak: Zone Based Firewall (ZBF), IPSec VPN, możliwość uruchomienia dynamicznych sieci VPN w technologii Dynamic Multipoint VPN (DMVPN/DSVPN) lub odpowiednika opartego na otwartych standardach.

Wymagane zarządzanie i konfiguracja:

95. zarządzalne za pomocą SNMPv3,
96. konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface — CLI) jak również interfejsu graficznego (GUI),
97. plik konfiguracyjny urządzenia będzie możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej będzie możliwe uruchomienie urządzenia z nową konfiguracją. Urządzenie musi umożliwiać wykonanie kopii pliku konfiguracyjnego urządzenia na zdalny serwer TFTP lub SCP/SFTP poprzez wysłanie specjalnego żądania z systemu zarządzania siecią wykorzystując protokół lub SNMPv3.,

Obudowa:

98. wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej,
99. ma możliwość montażu w szafie rack 19" oraz musi zostać dostarczone z zestawem umożliwiającym montaż w tej szafie,
100. wielkość urządzenia maksymalnie 1U,

Zasilanie:

101. wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V,

Wyposażenie:

102. wyposażone w minimum 3 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN/WAN,
103. minimum jeden z interfejsów opisanych powyżej ma możliwość pracy w trybie „dual-physical" z portem RJ45 lub giga bitowym portem światłowodowym definiowanym przez moduł GBIC lub SFP,
104. wyposażone w minimum jeden port USB (min. 1.0). Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych,
105. urządzenie będzie dostarczone z kablami pozwalającymi na podłączenie szeregowej konsoli, jak również kablem zasilający.

Wyposażenie dodatkowe urządzenia:

106. 1 szt. SFP GLC-SX-MM 1G, (wkładka wspierana przez producenta sprzętu).