Dokumentacja do projektu

Rozbudowa miejskiej szerokopasmowej sieci szkieletowej

dla

Urzędu Miasta Lublin

Spis treści

1. Charakterystyka projektu

1.1. Zakres zamówienia

Przedmiotem zamówienia jest dostarczenie i uruchomienie infrastruktury teleinformatycznej zbudowanej w oparciu o urządzenia sieciowe do realizacji usług komunikacyjnych. Będzie ona stanowiła bazę do budowy systemów informatycznych służących do dystrybucji i udostępniania szeroko rozumianych treści i usług w ramach miejskiej szerokopasmowej sieci szkieletowej oraz gminnych jednostek oświatowych.

Projekt rozbudowy ma zapewnić możliwość bezpiecznej i wydajnej komunikacji w ramach obiektów podłączonych do miejskiej szerokopasmowej sieci szkieletowej. Centra usług, które będą świadczone na rzecz zdalnych jednostek, zlokalizowane będą w budynkach Urzędu Miasta i obsługiwane przez Urząd Miasta Lublin. Sposób wykorzystania infrastruktury w głównej mierze będzie polegał na zdalnym dostępie do zasobów i usług oferowanych przez Urząd Miasta ale będzie również zapewniał wydajny i bezpieczny dostęp do sieci Internet. Infrastruktura zapewniać będzie możliwość wykorzystania nowoczesnych technologii takich jak komunikacja multimedialna czy zdalny dostęp.

W ramach realizacji zamówienia wykonawca, do wskazanych lokalizacji, dostarczy i zainstaluje wszystkie komponenty sprzętowe wraz z niezbędnymi elementami montażowymi i połączeniowymi. Dodatkowo dostarczy on oprogramowanie wraz z licencjami oraz komponentami niezbędnymi do jego prawidłowego działania. Wykonawca zapewni kompletność, wzajemną zgodność oraz współpracę wszystkich sprzętowych i programowych komponentów systemu.

Połączenia pomiędzy lokalizacjami biorącymi udział w projekcie realizowane będą za pomocą łączy posiadanych przez Zamawiającego. Dostarczenie usługi internetowej i zapewnienie fizycznych możliwości komunikacji pomiędzy lokalizacjami wchodzącymi w skład 162 gminnych jednostek oświatowych nie jest przedmiotem niniejszego zamówienia.

1.2. Harmonogram realizacji

Planowany jest wstępny podział realizacji prac w projekcie na etapy. Poniżej znajduje się lista etapów.

1. Przygotowanie projektu.
2. Dostawa urządzeń
3. Uruchomienie
4. Testy i odbiór

1.3. Planowane usługi

Dzięki rozbudowie infrastruktury teleinformatycznej możliwe będzie udostępnienie szeregu usług księgowych i edukacyjnych, mających charakter interaktywny i nieinteraktywny dla gminnych jednostek oświatowych.

W szczególności planowane jest udostępnienie następujących usług oferowanych w ramach zasobów Urzędu Miasta Lublin:

1) System księgowy dla szkół,
2) Dziennik elektroniczny dla szkół,
3) Portal edukacyjny (zbiór witryn szkół, udostępnianie zasobów plikowych, e-learning w oparciu o platformę Moodle i inne systemy edukacyjne).

Pozostałe usługi wspólne dla jednostek oświatowych:

1) Bezpieczny dostęp do Internetu dla podłączonych jednostek,
2) Telefonia IP (aktualnie udostępniana w oparciu o technologię Siemens),
3) Sieci WiFi (aktualnie udostępniana w oparciu o technologię Extreme Networks oraz dla niektórych jednostek oświatowych w oparciu o technologię Ubiquiti Networks),
4) VPN kliencki (aktualnie oparty o technologię Palo Alto Networks).

Na potrzeby świadczenia w/w usług dostarczona i rozbudowana zostanie infrastruktura teleinformatyczna, umożliwiająca ich realizację.

1.4. Miejsca realizacji projektu

W projekcie usługi będą realizowane przez sprzęt i oprogramowanie umieszczone w następujących lokalizacjach w Lublinie:

1. Serwerownia numer 1 Urzędu Miasta Lublin (DC 1) zlokalizowana w budynku znajdującym się pod adresem al. Racławickie 5. Serwerownia ta wyposażona jest szafy Rack. Docelowe szafy do montażu urządzeń sieciowych posiadają doprowadzone zasilania: gwarantowane 16 A i niegwarantowane 16 A.
1. Serwerownia numer 2 Urzędu Miasta Lublin (DC 2) zlokalizowana w budynku znajdującym się pod adresem Plac Łokietka 1.
2. Serwerownia numer 3 Urzędu Miasta Lublin (DC 3) zlokalizowana w budynku znajdującym się pod adresem ul. Wieniawska 14.

Chłodzenie każdej serwerowni jest wystarczające i wynosi ok 45 kW w pierwszej lokalizacji (Al. Racławickie 5), a w pozostałych dwóch serwerowniach moc chłodzenia jest mniejsza, aczkolwiek wystarczająca.

2. Opis wymagań projektu

2.1. Architektura rozwiązania

Architektura rozwiązania zakłada rozmieszczenie urządzeń w trzech niezależnych geograficznie rozproszonych serwerowniach. Pierwsza z nich, główna (DC 1), zlokalizowana jest na Alejach Racławickich 5. Druga (DC 2), która obecnie spełnia rolę serwerowni zapasowej, znajduje się na Placu Łokietka 1 w Ratuszu. Trzecia (DC 3) natomiast spełnia funkcję agregacyjną dla zewnętrznych lokalizacji oraz jednostek oświatowych. Dodatkowym założeniem jest istnienie połączeń światłowodowych typu single-mode pomiędzy serwerowniami DC 1 i DC 2 oraz pomiędzy DC 2 i DC 3 o długości nieprzekraczającej 10 km.

W projekcie rozbudowy sieci zastosowane zostały technologie oraz urządzenia odpowiedniej klasy, zapewniające wymagane liczby interfejsów, przepustowość, a także gwarantujące wymaganą w danym obszarze infrastruktury funkcjonalność. Przy doborze urządzeń zostały przyjęte odpowiednie marginesy pojemności komunikacyjnych dla przyszłej rozbudowy infrastruktury. Infrastruktura została podzielona ze względu na implementacje różnych funkcjonalności, z których wynika podział urządzeń sieciowych na poniższe warstwy funkcjonalne:

1. **Szkielet sieci (tzw. rdzeń - Core)** zbudowany został w oparciu o wysokowydajne przełączniki rdzeniowe rozmieszczone w trzech, geograficznie rozproszonych lokalizacjach. W każdej z tych lokalizacji znajduje się zestaw pary urządzeń należących do tej samej serii, a lokalizacje te zostały połączone w pierścień za pomocą podwójnych interfejsów 40 Gb/s. Powoduje to stworzenie wysoce redundantnej, wydajnej i elastycznej konfiguracji do podłączania innych lokalizacji bez względu na miejsce fizycznego doprowadzenia połączeń światłowodowych. Urządzenia tej warstwy będą wykorzystywane do zrealizowania poniższych połączeń:
   1.1. Porty 40 Gb wykorzystane do zbudowania rdzenia sieci opartego o topologię ringu, za pomocą którego zostaną połączone ze sobą trzy lokalizacje DC;
   1.2. Porty do podłączenia przełączników warstwy dystrybucyjnej;
   1.3. Porty do podłączenia przełączników Data Center;
   1.4. Porty do przełączników warstwy dostępowej;
   1.5. Połączenia do zdalnych lokalizacji jednostek Urzędu Miasta;
   1.6. Urządzenia odpowiedzialne za komunikację z warstwą zewnętrzną, takie jak router, firewall czy w przyszłości firewalle aplikacyjne, sondy IPS/IDS itp.
2. **Warstwa dystrybucyjna** zbudowana została w oparciu o przełączniki tej samej serii w celu ujednolicenia oraz uproszczenia konfiguracji, zarządzania i serwisowania. Przełączniki te terminują zarówno światłowodowe jak i miedziane połączenia Gigabit Ethernet. Do tych przełączników będą podłączone:
   2.1. Urządzenia końcowe, takie jak przełączniki do których podłączone są kamery;
   2.2. Urządzenia lokalne – inne niż serwery.
3. **Warstwa Data Center** planowana jest w oparciu o przełączniki dedykowane do środowisk serwerowych, charakteryzujące się bardzo wysoką wydajnością wewnętrzną i dużą gęstością interfejsów. Do przełączników tej warstwy będą dołączone następujące urządzenia:

3.1. Serwery za pomocą interfejsów 10Gbps Ethernet;
3.2. Serwery za pomocą interfejsów 1Gbps Ethernet.

4. **Warstwa WAN** stworzona za pomocą routerów agregujących urządzenia rozproszone po zdalnych jednostkach oświatowych. Urządzenia w tej warstwie charakteryzują się możliwością implementacji protokołów stosowanych w sieciach operatorskich takich jak MPLS.

5. **Warstwa Security** oparta o układ dwóch firewalli działających w klastrze wysokiej dostępności, realizująca filtrację i zabezpieczenie komunikacji pomiędzy infrastrukturą a siecią Internet oraz pomiędzy różnymi grupami urządzeń w obrębie sieci.

6. **Warstwa dostępowa** - warstwę tę stanowią przełączniki dostępowe realizujące styk urządzeń końcowych z siecią. Przełączniki te są geograficznie rozproszone w ramach lokalizacji UM i dołączone do sieci za pomocą światłowodowych interfejsów 10G bezpośrednio do portów urządzeń z warstwy rdzenia.

2.2. Wymagania ogólne

1. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem, nie odświeżane) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu realizacji procedur opisanych w zakresie Zamówienia. Wykonawca jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo do inspekcji sprzętu przed jego rozpakowaniem).
2. Dostarczane rozwiązania muszą odpowiadać wymaganiom Polskich Norm przenoszących normy europejskie lub norm innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy.
3. Urządzenia wraz z zainstalowanym na nich oprogramowaniem muszą pochodzić z legalnego źródła i być przeznaczone do użytkowania na terenie Unii Europejskiej.
4. Zamawiający wykona testy weryfikacyjne poszczególnych funkcjonalności przed wyborem oferty; założenia testów są opisane w dalszej części dokumentu.
5. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
6. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy albo ostatniej opublikowanej) na dzień poprzedzający dzień składania ofert.
7. Oferowane rozwiązania w dniu składania ofert muszą być powszechnie dostępne w sprzedaży (nie dopuszcza się rozwiązań i funkcjonalności planowanych do wprowadzenia, będących w fazie implementacji przez producenta).
8. Oferowane rozwiązania w dniu składania ofert nie mogą być przez producenta oficjalnie (biuletyny produktowe, informacje publiczne) przeznaczone do wycofania z produkcji lub sprzedaży.
9. Wszystkie wymagane funkcjonalności muszą być dostępne w oferowanych rozwiązaniach w dniu składania oferty.

10. Oferowane rozwiązania muszą zapewniać funkcjonowanie wszystkich usług w nie zmniejszonym zakresie (urządzenia muszą oferować tą samą lub lepszą funkcjonalność w odniesieniu do funkcjonalności w oferowanej w momencie dostarczenia urządzenia) w czasie trwania gwarancji.
11. Wykonawca dokona dezinstalacji urządzeń, które nie będą wykorzystywane, obecnie znajdujących się u Zamawiającego w trzech serwerowniach (DC1, DC2 DC3).
12. Wykonawca dokona instalacji wszystkich zakupionych urządzeń w trzech serwerowniach (DC1, DC2, DC3).
13. Terminy prac przełączeniowych zostaną uzgodnione z Zamawiającym. Wszelkie prace związane z montażem i uruchomieniem urządzeń muszą być wykonywane poza godzinami pracy urzędu (tj. pomiędzy godz 16.00 – 7.00). Przerwy w pracy sieci i dostępności usług spowodowane tymi pracami muszą być każdorazowo konsultowane i zatwierdzane przez Zamawiającego.
14. W ramach Zamówienia Wykonawca dostarczy wszystkie niezbędne elementy konieczne do zainstalowania i uruchomienia dostarczanej infrastruktury, w celu realizacji przedmiotu umowy, w szczególności:
    14.1. licencje systemów operacyjnych, baz danych wymaganych przez poszczególne komponenty,
    14.2. Moduły QSFP/SFP/SFP+.
    14.3. kable przyłączeniowe, zasilające, krosowe.

Wszystkie takie elementy muszą być zgodne z formalnymi rekomendacjami producentów poszczególnych systemów.

2.3. Wymagania gwarancyjne

1. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy w języku polskim (telefon, e-mail) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
2. Pozostałe wymagania precyzuje umowa.

2.4. Wymagania dla instalacji i uruchomienia

1. Wymaga się od wykonawcy by realizacja przedmiotu umowy została oparta o metodykę zarządzania projektem Prince 2 lub równoważną, tj. zapewniającą osiągnięcie zamierzonych celów jakościowych przy jednoczesnej minimalizacji możliwości niepowodzenia przedsięwzięcia.
2. Wykonawca wyznaczy osobę odpowiedzialną za realizację i koordynację zamówienia oraz zarządzanie całością przedsięwzięcia. Zamawiający wyznaczy po swojej stronie osobę koordynują prace, a także wskaże osoby kontaktowe w każdej lokalizacji, w której wykonywane będą prace.
3. Wszystkie prace muszą być prowadzone z zachowaniem należytej staranności, zgodnie z najlepszymi praktykami branżowymi.
4. Wykonawca przeprowadzi testy akceptacyjne (odbiorcze) uruchomionego rozwiązania zgodnie z przygotowaną i zaakceptowaną przez Zamawiającego na etapie przygotowania projektu wykonawczego procedurą testów akceptacyjnych (odbiorczych).

5. Wykonawca dostarczy dokumentację powykonawczą uruchomionego rozwiązania.

2.5. Wymagana zawartość projektu i dokumentacji powykonawczej

W ramach realizacji zamówienia, wykonawca przygotuje projekt infrastruktury teleinformatycznej, obejmujący co najmniej:

1. Szczegółowy wykaz wykorzystywanego sprzętu i oprogramowania w poszczególnych lokalizacjach,
2. Diagramy połączeń elementów sprzętowych w ramach infrastruktury obejmujące topologię, typy interfejsów.
3. Mechanizmy integracyjne między poszczególnymi komponentami,
4. Diagramy połączeń poszczególnych komponentów aplikacyjnych dla poszczególnych systemów, obejmujące wykorzystywane interfejsy komunikacyjne,
5. Plan rozmieszczenia i wykorzystania zasobów poszczególnych komponentów aplikacyjnych (serwery, przestrzeń dyskowa, oprogramowanie wirtualizacyjne),
6. Plan adresacji sieciowej,
7. Plan numeracyjny komponentów komunikacyjnych,
8. Schemat nazewniczy komponentów,
9. Ramowy opis bazowej konfiguracji poszczególnych elementów,
10. Ramowy opis polityki zabezpieczenia poszczególnych komponentów,
11. Wykaz scenariuszy testów akceptacyjnych (odbiorczych) umożliwiających weryfikację wymaganego zakresu instalacji i wstępnego uruchomienia dostarczanych w poszczególnych etapach komponentów. Scenariusze testów odbiorczych muszą zapewniać weryfikację komunikacji w wymaganym zakresie.

Przed rozpoczęciem dostaw i instalacji projekt musi być uzgodniony z Zamawiającym i przez niego zaakceptowany.

Po zakończeniu dostaw, uruchomienia i testów wykonawca dostarczy dokumentację powykonawczą, zawierającą:

1. Projekt wraz z zaakceptowanymi przez Zamawiającego zmianami i odstępstwami w stosunku do projektu.
2. Opis konfiguracji dostarczonych urządzeń i oprogramowania, kopie konfiguracji itp.
3. Zestawienie urządzeń wraz z numerami seryjnymi, oznaczeniami, rozmieszczeniem, wartością urządzeń.
4. Pozytywne wyniki wszystkich testów.

2.6. Zakres szkolenia dla administratorów

Instruktaż wdrożeniowy

W ramach uruchomienia infrastruktury teleinformatycznej wykonawca przeprowadzi instruktaż stanowiskowy dla co najmniej 10 wskazanych pracowników (administratorów infrastruktury) Zamawiającego (dopuszcza się podział osób na grupy), obejmujący:

1. Zapoznanie się z komponentami infrastruktury sieciowej, w tym co najmniej:
   1.1. Opis wykorzystywanych komponentów,
   1.2. Struktura i topologia poszczególnych systemów,
   1.3. Zadania poszczególnych komponentów.
2. Konfiguracja poszczególnych komponentów (w zakresie niezbędnym do zarządzania dostarczoną infrastrukturą), w tym co najmniej:
   2.1. Konfiguracja komponentów infrastruktury rozmieszczonej w serwerowniach,
   2.2. Zarządzanie kopiami zapasowymi,
   2.3. Zarządzanie licencjami.
3. Wykorzystanie narzędzi i systemów zarządzających, w tym co najmniej:
   3.1. Obsługa interfejsów zarządzania poszczególnych systemów,
   3.2. Obsługa systemów zarządzania i automatyzacji,
   3.3. Kreowanie usług w systemach automatyzacji.
4. Mechanizmy diagnostyki typowych problemów eksploatacyjnych.

Szczegółowy zakres instruktażu zostanie ustalony na etapie przygotowania projektu, uwzględniając zaoferowane komponenty. Szkolenie zostanie przeprowadzone przez instruktora posiadającego certyfikaty potwierdzającego jego wiedzę z prezentowanych technologii. Instruktaż będzie przeprowadzony w formie warsztatów w siedzibie wskazanej przez Zamawiającego, wykorzystując uruchomianą platformę informatyczną. Termin szkoleń musi zostać uzgodniony z Zamawiającym. Instruktaż obejmie co najmniej 40 godzin zajęć (dla każdej z grup uczestników). Materiały przygotowane w ramach instruktażu pozostaną własnością uczestników szkolenia.

Szkolenia autoryzowane

Wykonawca zapewni Zamawiającemu autoryzowane szkolenia z oferowanych produktów w następującym zakresie i wymiarze.

Obszar/zakres	Wymiar czasu szkolenia	Ilość osób
Routing i switching	40h	4 osoby
Data Center	40h	4 osoby
Firewall segmentu brzegowego	40h	4 osoby
Splunk Enterprise	40h	4 osoby

Wszystkie szkolenia muszą odbywać się w autoryzowanym centrum szkoleniowym danego producenta. Wykonawca musi pokryć wszystkie koszty związane z uczestnictwem wyznaczonych przedstawicieli Zamawiającego w szkoleniu, w szczególności: bilety komunikacyjne, pobyt w hotelu, catering podczas szkolenia (co najmniej 1 przerwa obiadowa, 3 przerwy kawowe na dzień szkoleniowy).
Zamawiający dopuszcza możliwość dostarczenia voucherów na w/w szkolenia. W takim przypadku data ważności vouchera nie może być krótsza niż 12 miesięcy od daty podpisania protokołu odbioru końcowego dla całego projektu.

2.7. Testy weryfikujące

W ramach postępowania Zamawiający wymaga przeprowadzenia testów weryfikujących oferowanych rozwiązań obowiązkowo przed wyborem oferty. Celem przeprowadzenia procedury testowej jest weryfikacja zgodności urządzeń i oprogramowania z wymaganiami. Wszelkie testy będą przeprowadzane przez Wykonawcę na jego koszt i ryzyko. Wykonawca będzie zobowiązany do dostarczenia na potrzeby testów egzemplarza wzorcowego oferowanego rozwiązania obejmującego:

1. Oferowane urządzenia:
   1.1. Przełącznik rdzenia (typ 1 i 2)
   1.2. Przełącznik Data Center
   1.3. Firewall segmentu brzegowego
   1.4. Router segmentu brzegowego
2. Platformę sprzętową umożliwiającą uruchomienie niezbędnych komponentów,
3. Wymagane do uruchomienia powyższych elementów licencje (dopuszczalne wersje testowe bez ograniczeń funkcjonalnych ważne w okresie trwania testów),
4. Kompletną dokumentację dostarczanych elementów i systemów w języku polskim lub angielskim (lub wskazanie publicznie dostępnych stron internetowych z lokalizacją dokumentacji).

Testy zostaną przeprowadzone w środowisku laboratoryjnym, aby zmaksymalizować dostępność urządzeń i możliwość ich rekonfiguracji do potrzeb danego scenariusza testowego. Zamawiający zapewni środowisko laboratoryjne, spełniające typowe wymagania pracy urządzeń aktywnych (kontrola parametrów środowiskowych, szafy rack 19” do instalacji urządzeń, zasilanie gwarantowane) oraz wykwalifikowany personel prowadzący testy. Zamawiający zastrzega

możliwość weryfikacji wszystkich parametrów i funkcjonalności w odniesieniu do każdego z wymogów.

2.7.1. Opis procedury testowej

Testy odbędą się we wskazanym przez Zamawiającego miejscu na terenie Polski w siedzibie Zamawiającego. Wykonawca będzie zobowiązany do dostarczenia tam urządzeń podlegających testom w ustalonym terminie oraz odebrania ich po zakończeniu procedury testowej.

Wszystkie testy odbywać się będą w obecności przedstawicieli Zamawiającego, oraz przedstawicieli Wykonawcy.

Konfigurację urządzeń będą przeprowadzali przedstawiciele Wykonawcy lub instytucji prowadzącej procedurę testową. W przypadku konfiguracji urządzeń przez przedstawicieli Wykonawcy, konfiguracja będzie analizowana przez prowadzących testy. Wszelkie zmiany konfiguracji będą dokumentowane, wszelkie restarty urządzeń, zmiana wersji oprogramowania systemowego i inne istotne zmiany środowiska testowego prowadzone w trakcie procedury muszą być zgłoszone prowadzącym testy. W przypadku stwierdzenia przez prowadzących testy odstępstw od tej zasady, mogą oni nakazać powtórzenie danego testu lub grupy testów. Weryfikacja poszczególnych funkcjonalności poddawanych testom musi być prowadzona na konkretnych urządzeniach lub modułach aplikacyjnych, dla których wymagania te były określone.

Wszystkie przeprowadzone testy muszą dać mierzalne wyniki – w przypadku zaobserwowania niestabilności pracy urządzeń lub funkcjonalności, wymagane jest powtórzenie testu. Jeżeli praca urządzeń zostanie ustabilizowana (trzykrotne powtórzenie testu da powtarzalne wyniki), w takim przypadku test zostanie zaliczony.

W przypadku zaobserwowania usterek urządzeń lub oprogramowania, potwierdzonych przez Wykonawcę i prowadzących testy, Wykonawcy przysługuje prawo do wymiany wadliwych komponentów (w ciągu 2 dni roboczych). W przypadku, gdy wymiana nie doprowadzi do pozytywnego wyniku testu, zostanie on uznany za nie zaliczony.

Procedura testowa:

1) Bazując na scenariuszu danego testu, przedstawiciele prowadzącego testy określają zasady konfiguracji systemów. Wykonawcy przysługuje prawo do zaproponowania zmian, o ile określone zasady naruszać będą wymagania w zakresie funkcjonalności urządzeń,
2) Wykonawca lub prowadzący testy przeprowadza konfigurację systemów do testu,
3) Przeprowadzona zostaje próba testu,
4) W przypadku negatywnego wyniku testu, Wykonawca lub prowadzący testy diagnozuje przyczyny,
5) O ile przyczyny negatywnego wyniku testu mają charakter błędów konfiguracyjnych, wprowadzane są poprawki i próba jest powtarzana,
6) O ile przyczyny negatywnego wyniku testu mają charakter niezgodności funkcjonalnej, test zostaje uznany za nie zaliczony,
7) W przypadku pozytywnego wyniku testu test zostaje uznany za zaliczony,

8) Sporządzana zostaje dokumentacja testu, obejmująca wersje oprogramowania systemowego urządzeń, ich konfigurację, opis przeprowadzonego testu i wyniki.

Testy mogą dotyczyć weryfikacji dowolnej funkcjonalności wymaganej dla poszczególnych elementów określonych w punktach 3 i 4

2.7.1.1.Urządzenia testujące

Testy muszą zostać wykonane dedykowanym urządzeniem typu „appliance" umożliwiającym wygenerowanie ruchu większego niż wymagany w procedurze testowej, a także umożliwiające generowanie ruchu na podstawie pliku zawierającego podsłuchany (za pomocą sniffera) rzeczywisty ruch występujący w sieci Zamawiającego. Urządzenie testujące musi być dostarczone przez Wykonawcę. Wymagania co do urządzenia testującego:

1) Urządzenie generujące ruch musi mieć możliwość testowania parametrów wydajnościowych urządzeń sieciowych takich jak przełączniki, routery, firewalle.
2) Urządzenie generujące ruch musi symulować pracę zarówno klienta jak i serwera dla testowanych aplikacji (odbiornik, nadajnik).
3) Urządzenie musi pozwalać (w przypadku przeprowadzenia testu firewalla) na wykonanie testów w trybie bridge (L2) jak i w trybie routing (L3).
4) Urządzenie musi mieć możliwość wygenerowania ruchu o wolumenie większym, niż wymagany przez Zamawiającego maksymalny wolumen ruchu dla oferowanego urządzenia.
5) Urządzenie musi posiadać predefiniowane przez producenta próbki symulujące ruch generowany prze różnego rodzaju aplikacje, grupy aplikacji oraz protokoły HTTP Enterprise, Windows Update, Facebook, Google Email, Microsoft Exchange, Oracle, Enterprise Mix.
6) Urządzenie musi mieć możliwość wygenerowania ruchu dla wybranej grupy aplikacji, o określonym wolumenie i określonej liczbie symulowanych użytkowników.
7) Urządzenia powinno posiadać możliwość automatycznego przerwania testu, jeśli liczba błędów przekroczy określoną wartość.
8) W czasie prowadzonego testu urządzenie musi na bieżąco raportować informacje o generowanym ruchu. W czasie testu powinny być dostępne takie informacje jak:
    a. sumaryczny wolumen generowanego ruchu,
    b. wolumen ruchu na poszczególnych interfejsach,
    c. liczba wygenerowanych transakcji (poprawne oraz nieudane),
    d. liczba wygenerowanych sesji TCP, liczba jednoczesnych sesji TCP, liczba sesji TCP/sec.
9) Po zakończeniu testów urządzenie musi wygenerować raport z wykonanego testu zawierający conajmniej informacje o:
    a. wolumenie wygenerowanego ruchu,
    b. procentowym udziale poszczególnych aplikacji w wolumenie generowanego ruchu,
    c. ilości błędów w generowanym ruchu,
    d. liczbie wygenerowanych sesji TCP,
    e. ruchu wygenerowanym na poszczególnych interfejsach.

Generator powinien symulować rzeczywisty ruch występujący w sieci klienta/w sieciach typu enterprise.

2.7.2. Procedura testów urządzeń typu przełącznik, router

Testy urządzeń sieciowych mają umożliwić praktyczną weryfikację określonej w specyfikacji funkcjonalności. Procedura testowa zależeć będzie od rodzaju i sposobu działania weryfikowanej funkcjonalności. Weryfikacji poddawane będą wszystkie dodatkowe punktowane funkcjonalności z wyłączeniem mierzenia parametrów wydajnościowych.

Wymagania wobec testów oraz procedura ich przeprowadzenia:

1. Wykonawca w terminie wykonania testów musi przekazać Zamawiającemu kompletne środowisko testowe, w szczególności sprzęt i oprogramowanie składające się na oferowany system oraz wszelkie inne elementy konieczne do przeprowadzenia testów. Po wykonaniu testów Wykonawca zabierze dostarczone przez siebie urządzenia.
2. Miejsce i sposób przeprowadzenia testów:

a. Testy odbywać się będą w siedzibie Zamawiającego.

b. Czas trwania testów nie może być dłuższy niż 6 godzin zegarowych. Wykonawca będzie miał prawo przygotowania środowiska testowego w miejscu testów dwie godziny zegarowe przed początkiem testów. Czas ten może zostać wykorzystany przez Wykonawcę do przygotowania się do testów.

c. W celu realizacji testów (podczas przygotowania oraz przeprowadzenia) Wykonawca może korzystać tylko i wyłącznie z środowiska testowego przez siebie dostarczonego. Wyjątek stanowią tutaj urządzenia prezentacyjne: rzutnik, ekran, monitor.

d. Podczas testów Wykonawca zobowiązany jest do udzielania Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane rozwiązanie posiada wymagane funkcjonalności.

e. W przypadku wystąpienia podczas testów problemów lub błędów Wykonawca ma prawo do podjęcia czynności zmierzających do ich eliminacji/usunięcia, w szczególności może dokonywać niezbędnych z jego punktu widzenia modyfikacji prezentowanego środowiska testowego, w ramach czasu przewidzianego na testy, o którym mowa w ppkt. b powyżej.

f. Z przeprowadzonych testów Zamawiający sporządzi protokół.

g. Testy muszą być prowadzone w języku polskim.

2.7.3. Procedura testów urządzeń typu firewall segmentu brzegowego

Testy muszą zostać wykonane dedykowanym urządzeniem typu „appliance” umożliwiającym wygenerowanie ruchu o wymaganej charakterystyce i wolumenie, a także umożliwiające

generowanie ruchu na podstawie pliku zawierającego podsłuchany (za pomocą sniffera) rzeczywisty ruch występujący w sieci Zamawiającego. Zamawiający dopuszcza możliwość wykorzystania gotowych próbek zaimplementowanych w dedykowanym urządzeniu typu appliance.

Wymagania na urządzenie testujące zostało opisane powyżej w punkcie 2.7.1.1.

Wymagania wobec testów oraz procedura ich przeprowadzenia:

1. Wykonawca w terminie wykonania testów musi przekazać Zamawiającemu kompletne środowisko testowe, w szczególności sprzęt i oprogramowanie składające się na oferowany system oraz wszelkie inne elementy konieczne do przeprowadzenia testów. Po wykonaniu prezentacji Wykonawca zabierze dostarczone przez siebie urządzenia.
2. Miejsce i sposób przeprowadzenia testów:

a. Prezentacja odbywać się będzie w siedzibie Zamawiającego. Szczegółowe informacje nt. miejsca oraz terminu przeprowadzenia testów Wykonawca zostanie poinformowany osobnym pismem.

b. Czas trwania testów nie może być dłuższy niż 6 godzin zegarowych. Wykonawca będzie miał prawo przygotowania środowiska testowego w miejscu testów dwie godziny zegarowe przed początkiem testów. Czas ten może zostać wykorzystany przez Wykonawcę do przygotowania się do testów.

c. W celu realizacji testów (podczas przygotowania oraz przeprowadzenia) Wykonawca może korzystać tylko i wyłącznie z środowiska testowego przez siebie dostarczonego. Wyjątek stanowią tutaj urządzenia prezentacyjne: rzutnik, ekran, monitor.

d. Podczas testów Wykonawca zobowiązany jest do udzielania Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane rozwiązanie posiada wymagane funkcjonalności.

e. W przypadku wystąpienia podczas testów problemów lub błędów Wykonawca ma prawo do podjęcia czynności zmierzających do ich eliminacji/usunięcia, w szczególności może dokonywać niezbędnych z jego punktu widzenia modyfikacji prezentowanego środowiska testowego, w ramach czasu przewidzianego na testy, o którym mowa w ppkt. b powyżej. Po przekroczeniu czasu na testy, tj. po upływie 6 godzin zegarowych, zadania które nie zostały wykonane w zadanym czasie zostaną uznane za niewykonane.

f. Z przeprowadzonych testów Zamawiający sporządzi protokół.

g. Testy muszą być prowadzone w języku polskim.

3. Wymagania dla urządzenia testującego.

a. Testy muszą być wykonane dedykowanym urządzeniem typu appliance umożliwiającym wygenerowanie ruch o wymaganej charakterystyce i wolumenie. Nie dopuszcza się testów wykonywanych z poziomu stacji roboczej / serwera.

b. Urządzenie generujące ruch musi symulować pracę zarówno klienta jak i serwera dla testowanych aplikacji (odbiornik / nadajnik).

c. W czasie prowadzonego testu urządzenie musi na bieżąco raportować o wolumenie ruchu po stronie nadajnika jak i po stronie odbiornika.

d. Po zakończeniu każdego z testów urządzenie musi wygenerować raport z wykonanego testu.

e. Urządzenie musi pozwalać na przeprowadzenie testu firewalla pracującego w trybie bridge (L2) jak i w trybie routing (L3).

f. Urządzenie musi mieć możliwość wygenerowania ruchu o wolumenie minimum 15 Gbps.

g. Urządzenie musi mieć możliwość wygenerowania ruchu dla wybranej grupy aplikacji, o określonym wolumenie

4. Wymagania w zakresie konfiguracji firewalla

a. Przed rozpoczęciem testów, Wykonawca dostarczy Zamawiającemu pełną konfigurację testowanego NGFW.

b. W czasie testu należy aktywować wszystkie funkcjonalności firewalla typu NGFW: kontrola aplikacji, IPS, AV, URL Filtering.

c. Wszystkie moduły inspekcyjne muszą mieć zainstalowane najnowsze aktualizacje sygnatur oraz baz URL.

d. Moduły inspekcyjne muszą mieć wyłączone opcje fail-open.

e. Moduły inspekcyjne IPS oraz AV muszą analizować cały ruch (analiza wszystkich danych przesłanych w sesji).

f. Konfiguracja modułu firewalla i kontroli aplikacji - w czasie testu polityka zezwalała będzie na dowolny ruch/aplikację (reguła ANY ANY ACCEPT).

g. Konfiguracja modułu IPS – domyślna polityka producenta.

h. Konfiguracja AV – domyślna polityka producenta.

i. Konfiguracja URL – domyślna polityka producenta.

j. Konfiguracja logowania – włączone logowanie dla wszystkich modułów.

5. Generator powinien wygenerować ruch na podstawie pliku zawierającego ruch pozyskany przez Zamawiającego w jego sieci poprzez sniffing. Plik z ruchem zostanie dostarczony przez Zamawiającego Wykonawcom przed rozpoczęciem testów. Zamawiający dopuszcza możliwość wykorzystania gotowych próbek zaimplementowanych w dedykowanym urządzeniu typu appliance w celu wygenerowania ruchu - do testów należy przyjąć profil ruchu typu „Enterprise MIX”.

6. Przed wykonaniem testu generatorem wykonane zostaną wstępne testy potwierdzające poprawne działanie modułów inspekcyjnych oraz logowania.

7. Stan wyjściowy:

a. Firewall skonfigurowany jak do testu generatorem (tryb bridge-mode)

b. Przebieg testu:

Lp.	Nazwa testu	Opis	Oczekiwany wynik	Wynik pozytywny (tak / nie)
1.	Weryfikacja konfiguracji	Wskazanie konfiguracji potwierdzającej, że wszystkie wymagane moduły zostały uruchomione i skonfigurowane zgodnie z wymaganiami.	Potwierdzenie w konfiguracji włączenia funkcjonalności	
2.	Test rozpoznania aplikacji	Nawiązać połączenie dowolną aplikacją.	Informacja w logu potwierdzająca rozpoznanie aplikacji	
3.	Test AV – protokół HTTP	Przesłanie pliku eicar protokołem HTTP.	Próba przesłania pliku powinna zostać zablokowana	
4.	Test AV – protokół HTTP, plik skompresowany	Przesłanie skompresowanego pliku eicar protokołem HTTP.	Próba przesłania pliku powinna zostać zablokowana	
5.	Test IPS	Wygenerowanie dowolnego zdarzenia rozpoznanego przez IPS	Informacja w logu	
6.	Test URL	Zablokowanie dostępu do przykładowej strony (predefiniowanej lub zdefiniowanego na czas testu URL)	Zablokowanie dostępu. Informacja w logu zawierająca zablokowany URL oraz kategorię strony.	

8. Weryfikacja konfiguracji generatora: Celem testu będzie weryfikacja poprawności działania generatora

9. Stan wyjściowy:

a. Test powinien zostać wykonany bez urządzeń na ścieżce ruchu – porty nadajnika i odbiornika połączone bezpośrednio. W ramach testu należy wygenerować ruch zgodnie ze specyfikacją opisaną w punkcie 5

b. Przebieg testu:

Lp.	Nazwa testu	Opis	Oczekiwany wynik	Wynik pozytywny (tak / nie)

1.	Weryfikacja konfiguracji generator – 15 Gbps	Generacja ruchu o wolumenie 15 Gbps na podstawie pliku z ruchem Zamawiającego lub gotowych próbek zaimplementowanych w dedykowanym urządzeniu *) czas trwania testu – 5 min	Potwierdzenie uzyskanych wyników w statystykach generatora oraz w raporcie końcowym.	

*) Sumaryczny ruch (Tx + Rx)

10. Testy firewalla z użyciem generatora, stan wyjściowy:

a. Przebieg testu:

Lp.	Nazwa testu	Opis	Oczekiwany wynik	Wynik pozytywny (tak / nie)
1.	Test 15 Gbps – pełna funkcjonalność	Generacja ruchu o wolumenie 15 Gbps *) czas trwania testu – 5 min Włączona pełna funkcjonalność urządzenia (ochrona Intrusion Prevention, antywirus, filtracja aplikacji i kategoryzacja URL)	Poprawne działanie urządzenia, prawidłowa kategoryzacja ruchu	

*) Sumaryczny ruch (Tx + Rx)
**) Powyższy testy urządzenia firewall zostanie powtórzony 3 krotnie. Aby wynik testów został uznany za pozytywny, za każdym razem test powinien zakończyć się wynikiem pozytywnym

3. Ogólne wymagania funkcjonalne

O ile wymagania szczegółowe dla poszczególnych urządzeń nie stanowią inaczej, dostarczane urządzenia teleinformatyczne (w szczególności przełączniki, routery, firewalle) muszą spełniać poniższe wymagania minimalne:

1. Urządzenia muszą być przystosowane do montażu w standardowych szafach teleinformatycznych rack 19”.
2. Urządzenia należy dostarczyć je wraz z wszystkimi niezbędnymi elementami montażowymi do montażu w szafie rack 19".
3. Urządzenia należy dostarczyć z wszystkimi niezbędnymi kablami zasilającymi.
4. Urządzenia muszą mieć możliwość zasilania prądem zmiennym o napięciu 230V.
5. Urządzenie pozwala na wymianę zasilaczy i wentylatorów w trakcie pracy (tzw. *hot-swap*).
6. Urządzenia mają zapewnić zasoby przetwarzania (moc obliczeniową, pamięć operacyjną i stałą, zasoby sieciowe) pozwalające na stabilną i niezawodną pracę.
7. Z uwagi na ograniczone zasoby techniczne Zamawiającego, poniższe klasy urządzeń muszą pochodzić od jednego producenta:
    1. Przełącznik rdzenia (typ 1)
    2. Przełącznik rdzenia (typ 2)
    3. Przełącznik Data Center
    4. Przełącznik dystrybucyjny (typ 1)
    5. Przełącznik dystrybucyjny (typ 2)
    6. Przełącznik dostępowy (typ 1)
    7. Przełącznik dostępowy (typ 2)
    8. Przełącznik dostępowy (typ 3)
    9. Router segmentu brzegowego
    10. Router zdalny

W celu zmaksymalizowania niezawodności systemu, infrastruktura musi zapewnić odpowiedni poziom niezawodności, zarówno przez duplikację komponentów, jak i ich rozmieszczenie w różnych lokalizacjach fizycznych.

3.1. Klasy i rozmieszczenie urządzeń

Infrastruktura teleinformatyczna składa się z następujących klas urządzeń:

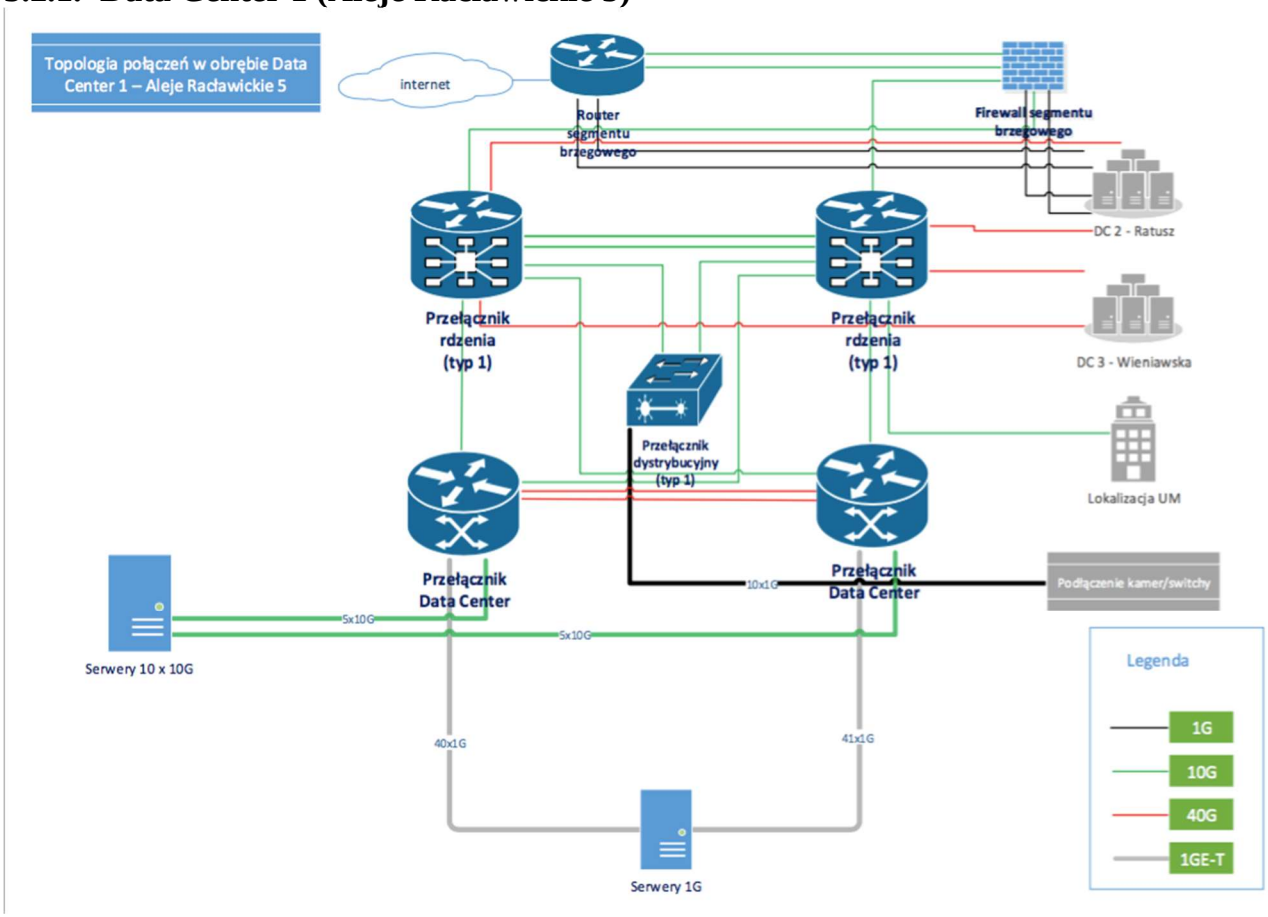
1. Przełącznik sieciowy dedykowany do obsługi rdzenia sieci, nazwany w dalszej części specyfikacji: "**Przełącznik rdzenia**".
2. Przełącznik sieciowy dedykowany do obsługi środowisk serwerowych, nazwany w dalszej części specyfikacji: "**Przełącznik Data Center**".
3. Przełącznik dostępowy dedykowany do obsługi połączeń z innych przełączników, nazwany w dalszej części specyfikacji: "**Przełącznik dystrybucyjny**".
4. Przełącznik dostępowy dedykowany do obsługi urządzeń końcowych takich jak komputery PC, nazwany w dalszej części specyfikacji: "**Przełącznik dostępowy**".
5. Firewall segmentu brzegowego do obsługi styku z siecią Internet, nazwany w dalszej części specyfikacji: "**Firewall segmentu brzegowego**".
6. Przełącznik do obsługi sieci w jednostkach oświatowych, nazwany w dalszej części specyfikacji "**Router zdalny**".
7. Router do obsługi styku z siecią Internet, nazwany w dalszej części specyfikacji "**Router segmentu brzegowego**".

Urządzenia zostały przypisane do następujących lokalizacji i występują w następujących ilościach:

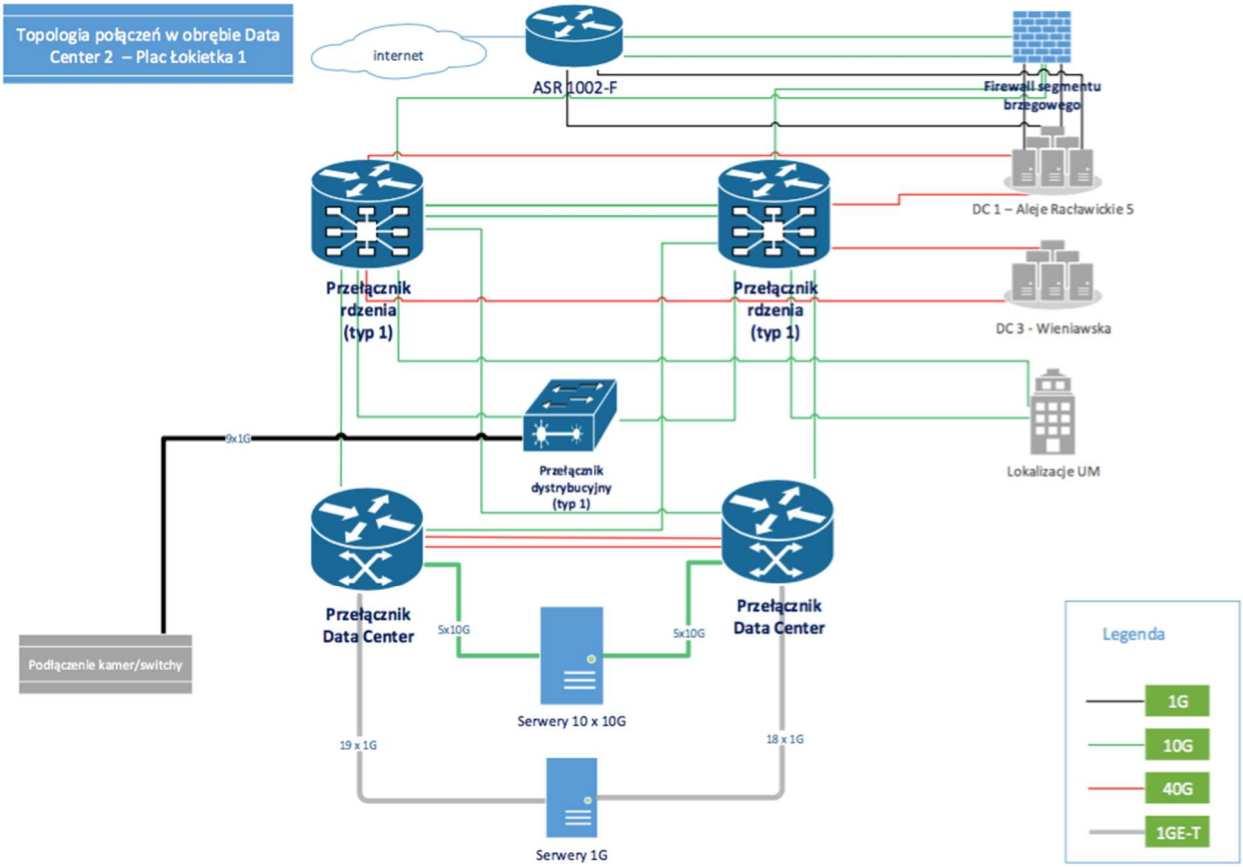
Typ urządzenia	DC1	DC2	DC3	Dostawa do siedziby Zamawiającego
Przełącznik rdzenia (typ 1)	2	2		
Przełącznik rdzenia (typ 2)			2	
Przełącznik Data Center	2	2		
Przełącznik dystrybucyjny (typ 1)	1	1	1	
Przełącznik dystrybucyjny (typ 2)			1	
Przełącznik dostępowy (typ 1)			48	
Przełącznik dostępowy (typ 2)			5	
Przełącznik dostępowy (typ 3)			5	
Firewall segmentu brzegowego	1	1		
Router zdalny				20
Router segmentu brzegowego	1			

3.2. Topologie połączeń w poszczególnych lokalizacjach

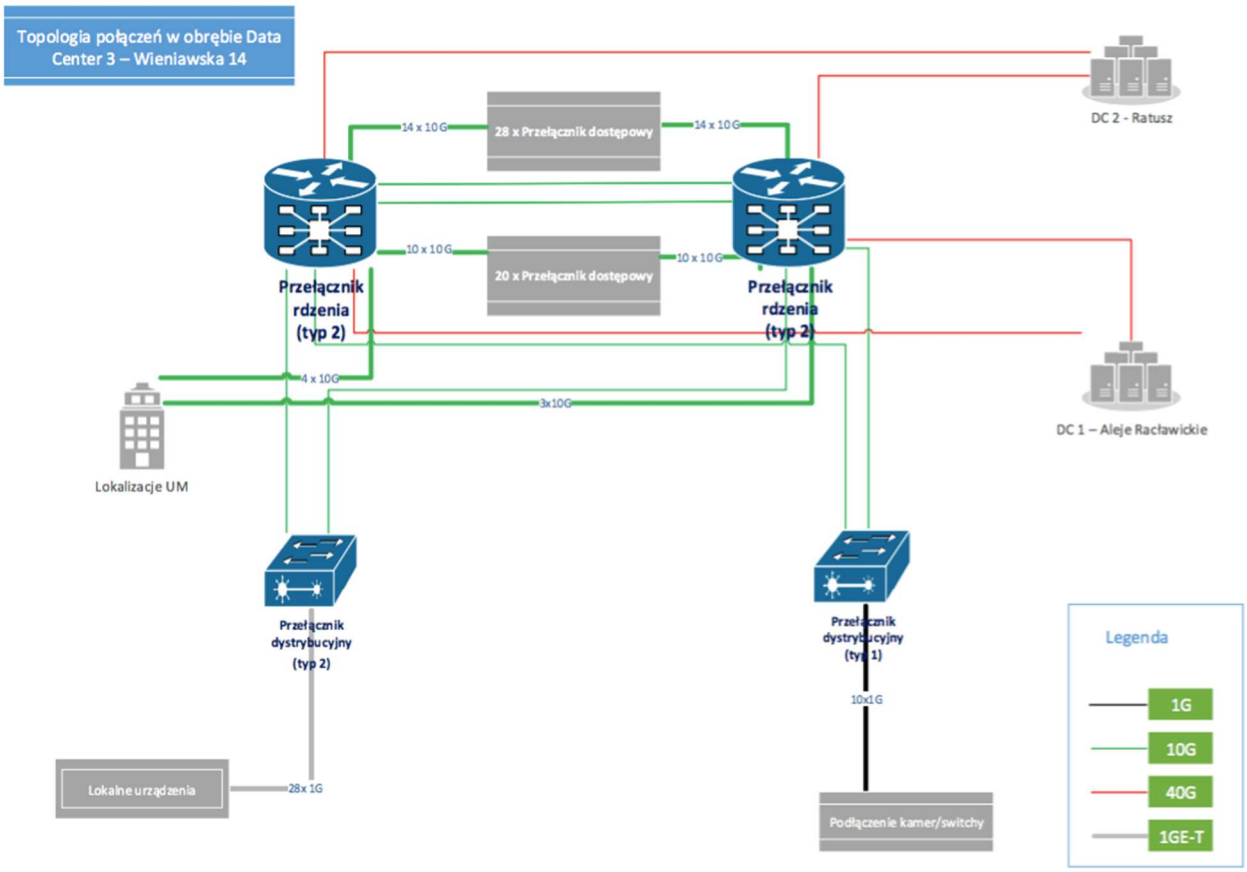
3.2.1. Data Center 1 (Aleje Racławickie 5)



3.2.2. Data Center 2 (Plac Łokietka 1)



3.2.3. Data Center 3 (Wieniawska 14)



4. Wymagania funkcjonalne techniczne klas urządzeń i systemów

4.1. Przełącznik rdzenia (typ 1)

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1.	Typ i liczba portów – 24 porty 1/10G SFP+ oraz 2 porty 40G QSFP. Dopuszczalna nadsubskrypcja na portach nie większa niż 2:1.	Bezwzględnie
2.	Porty SFP+ obsługujące wkładki: 1000BaseT, 100BaseFX, 1000Base-SX/-LX/-BX, 10GBase-SR/-LR/-ER/-ZR.	Bezwzględnie
3.	Porty QSFP obsługujące wkładki: 40GBase-SR4/-LR4/-ER4/-SR-BD/-CU.	Bezwzględnie
4.	Możliwość stworzenia wirtualnego systemu złożonego z 2 urządzeń będących przedmiotem opisu zarządzanego jako całość. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów 10/40-Gigabit Ethernet oraz modułów optycznych. Musi istnieć możliwość terminowania połączeń typu "*link aggregation*" na dwóch przełącznikach tworzących taki system wirtualny ("*multi-chassis link aggregation*") zgodnie z 802.3ad.	Bezwzględnie
5.	Przepustowość - minimum 160 Gb/s full duplex oraz szybkość przełączania - minimum 120 mln p/s dla przełączania L2 oraz routingu IPv4 i minimum 60 mln p/s dla routingu IPv6	Bezwzględnie
6.	Minimum 100 000 wpisów w tablicy adresów MAC.	Bezwzględnie
7.	Minimum 256 000 wpisów w tablicy routingu IPv4.	Bezwzględnie
8.	Minimum 128 000 wpisów w tablicy routingu IPv6.	Bezwzględnie
9.	Minimum 128 000 tras multicast IPv4.	Bezwzględnie

10.	Minimum 64 000 tras multicast IPv6.	Bezwzględnie
11.	Minimum 50 000 wpisów ACE (Access Control Entries) na potrzeby realizacji polityk QoS i bezpieczeństwa.	Bezwzględnie
12.	Obsługa ramek Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame).	Bezwzględnie
13.	Obsługa protokołów routingu statycznego i dynamicznego zarówno dla IPv4 jak i IPv6.	Bezwzględnie
14.	Obsługa protokołów routingu warstwy 3 dla IPv4: OSPF, IS-IS, BGPv4.	Bezwzględnie
15.	Obsługa protokołów routingu warstwy 3 dla IPv6: OSPFv3, MP-BGP.	Bezwzględnie
16.	Mechanizm Non-Stop-Forwarding.	Bezwzględnie
17.	Obsługa sprzętowa ruchu multicastowego, w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD.	Bezwzględnie
18.	Możliwość rozszerzenia funkcjonalności (bez konieczności dokonywania zmian sprzętowych, a jedynie zakup licencji/wersji oprogramowania) o obsługę MPLS, L3 VPN, VPLS, MPLS TE, LDP, MPLS traceruote.	Bezwzględnie
20.	Obsługa sprzętowa tunelowania GRE.	Bezwzględnie
21.	Mechanizm BFD (Bidirectional Forwarding Detection) co najmniej dla protokołu OSPFv2 i OSPFv3.	Bezwzględnie
22.	IEEE 802.1w Rapid Spanning Tree (w tym Per-VLAN Rapid Spanning Tree - PVRST+).	Bezwzględnie
23.	IEEE 802.1s Multiple Spanning Tree Protocol.	Bezwzględnie
24.	IEEE 802.3ad Link Aggregation Control Protocol (w tym multi-chassis link aggregation).	Bezwzględnie
25.	Obsługa min. 8 kolejek, w tym co najmniej jedna kolejka ze statusem strict priority.	Bezwzględnie
26.	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC,	Bezwzględnie

	źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.	
27.	Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP.	Bezwzględnie
28.	Definiowanie polityk QoS per port i per VLAN.	Bezwzględnie
29.	Mechanizm automatyczny QoS.	Bezwzględnie
30.	Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend.	Bezwzględnie
31.	Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu.	Bezwzględnie
32.	Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard.	Bezwzględnie
33.	Weryfikacja źródła pakietu względem tablicy routingu (uRPF) – sprzętowo zarówno dla IPv4 i IPv6.	Bezwzględnie
34.	Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP.	Bezwzględnie
35.	Listy kontroli dostępu także dla IPv6.	Bezwzględnie
36.	Mechanizmy ochrony warstwy kontrolnej.	Bezwzględnie
37.	Możliwość zarządzania przez protokoły SNMPv3, SSHv2.	Bezwzględnie
38.	Zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Gigabit Ethernet.	Bezwzględnie
39.	Uwierzytelnianie i autoryzacja w oparciu o serwer RADIUS lub TACACS+.	Bezwzględnie

40.	Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN.	Bezwzględnie
41.	Definiowanie skryptów określających polityki przekazywania zdarzeń do systemów zarządzających (korelacja, zależności parametrów, diagnostyka, definicja alarmów).	Bezwzględnie
42.	Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.	Bezwzględnie

Parametry i funkcjonalności dodatkowe dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*)	Liczba punktów za spełnienie wymagania
1.	Każdy z portów liniowych obsługuje standard IEEE 802.1AE (szyfrowanie ruchu) z pełną wydajnością łącza.	Opcjonalne	11
2.	Duże bufory pakietów – 250MB per port 10GE.		
3.	Możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow) lub odpowiednik (bez samplowania). Konieczna jest obsługa/buforowanie minimum 1.000.000 wpisów. Funkcjonalność obsługiwana sprzętowo i wspierająca ruch IPv4, IPv6, MPLS oraz multicast.		
4.	Wysokość nie większa niż 2RU.		
5.	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.		
6.	Porty SFP oraz SFP+ obsługujące odpowiednio wkładki: 1000Base-CU oraz 10GBase-CU.		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona. Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

4.2. Przełącznik rdzenia (typ 2)

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1.	Typ i liczba portów – 40 porty 1/10G SFP+ oraz 2 porty 40G QSFP. Dopuszczalna nadsubskrypcja na portach nie większa niż 2:1.	Bezwzględnie
2.	Porty SFP+ obsługujące wkładki: 1000BaseT, 100BaseFX, 1000Base-SX/-LX/-BX, 10GBase-SR/-LR/-ER/-ZR.	Bezwzględnie
3.	Porty QSFP obsługujące wkładki: 40GBase-SR4/-LR4/-ER4/-SR-BD/-CU.	Bezwzględnie
4.	Możliwość stworzenia wirtualnego systemu złożonego z 2 urządzeń będących przedmiotem opisu zarządzanego jako całość. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów 10/40-Gigabit Ethernet oraz modułów optycznych. Musi istnieć możliwość terminowania połączeń typu "*link aggregation*" na dwóch przełącznikach tworzących taki system wirtualny ("*multi-chassis link aggregation*") zgodnie z 802.3ad.	Bezwzględnie
5.	Przepustowość - minimum 160 Gb/s full duplex oraz szybkość przełączania - minimum 120 mln p/s dla przełączania L2 oraz routingu IPv4 i minimum 60 mln p/s dla routingu IPv6.	Bezwzględnie
6.	Minimum 100 000 wpisów w tablicy adresów MAC.	Bezwzględnie
7.	Minimum 256 000 wpisów w tablicy routingu IPv4.	Bezwzględnie
8.	Minimum 128 000 wpisów w tablicy routingu IPv6.	Bezwzględnie
9.	Minimum 128 000 tras multicast IPv4.	Bezwzględnie
10.	Minimum 64 000 tras multicast IPv6.	Bezwzględnie
11.	Minimum 50 000 wpisów ACE (Access Control Entries) na potrzeby realizacji polityk QoS i bezpieczeństwa.	Bezwzględnie
12.	Obsługuje ramek Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame).	Bezwzględnie
13.	Obsługa protokołów routingu statycznego i dynamicznego zarówno dla IPv4 jak i IPv6.	Bezwzględnie

14.	Obsługa protokołów routingu warstwy 3 dla IPv4: OSPF, IS-IS, BGPv4.	Bezwzględnie
15.	Obsługa protokołów routingu warstwy 3 dla IPv6: OSPFv3, MP-BGP.	Bezwzględnie
16.	Mechanizm Non-Stop-Forwarding.	Bezwzględnie
17.	Obsługuje sprzętowo ruch multicastowy w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD.	Bezwzględnie
18.	Możliwość rozszerzenia funkcjonalności (bez konieczności dokonywania zmian sprzętowych, a jedynie zakup licencji/wersji oprogramowania) o obsługę MPLS, L3 VPN, VPLS, MPLS TE, LDP, MPLS traceruote.	Bezwzględnie
20.	Obsługa sprzętowa tunelowania GRE.	Bezwzględnie
21.	Mechanizm BFD (Bidirectional Forwarding Detection) co najmniej dla protokołu OSPFv2 i OSPFv3.	Bezwzględnie
22.	IEEE 802.1w Rapid Spanning Tree (w tym Per-VLAN Rapid Spanning Tree - PVRST+).	Bezwzględnie
23.	IEEE 802.1s Multiple Spanning Tree Protocol.	Bezwzględnie
24.	IEEE 802.3ad Link Aggregation Control Protocol (w tym multi-chassis link aggregation).	Bezwzględnie
25.	Obsługa min. 8 kolejek, w tym co najmniej jedna kolejka ze statusem strict priority.	Bezwzględnie
26.	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, żródłowy/docelowy port TCP.	Bezwzględnie
27.	Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP.	Bezwzględnie
28.	Definiowanie polityk QoS per port i per VLAN.	Bezwzględnie
29.	Mechanizm Automatycznego QoSu	Bezwzględnie

30.	Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend.	Bezwzględnie
31.	Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu.	Bezwzględnie
32.	Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard.	Bezwzględnie
33.	Weryfikacja źródła pakietu względem tablicy routingu (uRPF) – sprzętowo zarówno dla IPv4 i IPv6.	Bezwzględnie
34.	Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP.	Bezwzględnie
35.	Listy kontroli dostępu także dla IPv6.	Bezwzględnie
36.	Mechanizmy ochrony warstwy kontrolnej.	Bezwzględnie
37.	Możliwość zarządzania przez protokoły SNMPv3, SSHv2.	Bezwzględnie
38.	Zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Gigabit Ethernet.	Bezwzględnie
39.	Uwierzytelnianie i autoryzacja w oparciu o serwer RADIUS lub TACACS+.	Bezwzględnie
40.	Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN.	Bezwzględnie
41.	Definiowanie skryptów określających polityki przekazywania zdarzeń do systemów zarządzających (korelacja, zależności parametrów, diagnostyka, definicja alarmów).	Bezwzględnie

42.	Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.	Bezwzględnie

Parametry i funkcjonalności dodatkowe dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*)	Liczba punktów za spełnienie wymagania
1.	Każdy z portów liniowych obsługuje standard IEEE 802.1AE (szyfrowanie ruchu) z pełną wydajnością łącza.	Opcjonalne	11
2.	Duże bufory pakietów – 250MB per port 10GE.		
3.	Możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow) lub odpowiednik (bez samplowania). Konieczna jest obsługa/buforowanie minimum 1.000.000 wpisów. Funkcjonalność obsługiwana sprzętowo i wspierająca ruch IPv4, IPv6, MPLS oraz multicast.		
4.	Wysokość nie większa niż 2RU.		
5.	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.		
6.	Porty SFP oraz SFP+ obsługujące odpowiednio wkładki: 1000Base-CU oraz 10GBase-CU.		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona. Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

4.3. Przełącznik Data Center

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1.	Typ i liczba portów – 48 portów 1/10G SFP+ oraz 6 porty 40/100G QSFP28 Ethernet.	Bezwzględne
2.	Wraz z urządzeniem należy dostarczyć: 2 moduły 48x100/1000 RJ-45 z 4 portami uplink 10GE SFP+ moduły te mogą być realizowane w formie modułów wewnętrznych przełącznika lub modułów wyniesionych.	Bezwzględne
3.	Porty SFP+ obsługujące wkładki: 1000BaseT, 100BaseFX, 1000Base-SX/-LX/-EX/-ZX/-BX, 10GBase-SR/-LR/-LRM/-ER/-ZR/-CU. Porty QSFP28 obsługujące wkładki: 40GBase-SR4/-LR4/-ER4/SR-BD/-CU/-AOC.	Bezwzględne
4.	Opóźnienie poniżej 2 µs.	Bezwzględne
5.	Przepustowość 3.6Tbps.	Bezwzględne
6.	Prędkość przełącznika „wirespeed” dla każdego portu (zarówno dla ruchu L2, jak i L3).	Bezwzględne
7.	Bufor pakietów – minimum 40MB.	Bezwzględne
8.	Minimum 16GB pamięci oraz 64GB pamięci flash.	Bezwzględne
9.	Ramki Jumbo (minimum 9216 bajtów).	Bezwzględne
10.	Sprzętowe przełączanie pakietów w warstwie L3.	Bezwzględne
11.	Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP).	Bezwzględne
12.	Routing w oparciu o trasy statyczne.	Bezwzględne
13.	Obsługa protokołu VRRPv3.	Bezwzględne
14.	Statyczny i dynamiczny NAT (Network Address Translation).	Bezwzględne
15.	Routing dynamiczny IPv4 i IPv6 (OSPF, IS-IS, BGP).	Bezwzględne
16.	Policy Based Routing (PBR) dla IPv4 i IPv6.	Bezwzględne

17.	Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryby ASM (Any Source Multicast), BiDir (Bidirectional Shared Tree) oraz SSM (Source Specific Multicast); MSDP.	Bezwzględne
18.	Wsparcie dla 1000 instancji VRF.	Bezwzględne
19.	Obsługa łącznie minimum 128 000 prefixów oraz wpisów hosta w tablicy routingu.	Bezwzględne
20.	4 000 wejściowych oraz 1 000 wyjściowych wpisów dla ACL - access control list.	Bezwzględne
21.	Wsparcie dla 4094 sieci VLAN 802.1Q.	Bezwzględne
22.	Obsługa 90.000 adresów MAC.	Bezwzględne
23.	Private VLAN.	Bezwzględne
24.	IEEE 802.1s Multiple Spanning Tree (MST) – 64 instancje.	Bezwzględne
25.	Obsługa Rapid Spanning Tree (802.1w) per VLAN – minimum 500 instancji.	Bezwzględne
26.	Spanning Tree EdgePort, Root Guard, Bridge Assurance lub odpowiadający.	Bezwzględne
27.	Tunelowanie Q-in-Q.	Bezwzględne
28.	Ramki Pause (IEEE 802.3x).	Bezwzględne
29.	IGMP v2/v3, IGMP Snooping.	Bezwzględne
30.	Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach (MCEC, vPC lub odpowiadający mechanizm).	Bezwzględne
31.	Link Aggregation Control Protocol (LACP).	Bezwzględne
32.	BFD (Bidirectional Forwarding Detection).	Bezwzględne
33.	Obsługa IEEE 802.1p (CoS).	Bezwzględne
34.	Klasyfikacja QoS w oparciu o listy (ACL (Access control list).	Bezwzględne
35.	Bezwzględne (strict-priority) kolejkowanie na wyjściu.	Bezwzględne
36.	Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający.	Bezwzględne
37.	Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych.	Bezwzględne

38.	Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.	Bezwzględne
39.	Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych.	Bezwzględne
40.	Wejściowe ACL (standardowe oraz rozszerzone).	Bezwzględne
41.	ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu.	Bezwzględne
42.	Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP).	Bezwzględne
43.	ACL oparte o VLAN-y (VACL).	Bezwzględne
44.	ACL oparte o porty (PACL).	Bezwzględne
45.	Mechanizm DHCP Snooping.	Bezwzględne
46.	Mechanizm ARP Inspection.	Bezwzględne
47.	Mechanizm IP Source Guard.	Bezwzględne
48.	Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.	Bezwzględne
49.	Możliwości zarządzania i konfiguracji.	Bezwzględne
50.	Dedykowany port zarządzający RJ-45 100/1000.	Bezwzględne
51.	Dedykowany port konsoli.	Bezwzględne
52.	Port USB.	Bezwzględne
53.	RBAC (Role-Based Access Control).	Bezwzględne
54.	Możliwość uwierzytelniania administratorów w oparciu o serwery RADIUS lub TACACS+.	Bezwzględne
55.	SSHv2, SNMPv2 i v3, Syslog.	Bezwzględne
56.	Network Time Protocol (NTP).	Bezwzględne
57.	Diagnostyka procesu BOOT.	Bezwzględne
58.	Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback).	Bezwzględne
59.	Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing).	Bezwzględne

60.	Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (SPAN) – minimum 4 sesje.	Bezwzględne
61.	Interfejs programistyczny REST API wraz z upublicznionym SDK.	Bezwzględne
62.	Wbudowany interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API.	Bezwzględne
63.	Wsparcie dla NETCONF i zarządzania poprzez XML.	Bezwzględne
64.	Możliwość zainstalowania klienta Chef.	Bezwzględne
65.	Możliwość zainstalowania agenta Puppet.	Bezwzględne

Parametry i funkcjonalności dodatkowe dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*	Liczba punktów za spełnienie wymagania
1.	Przełącznik musi mieć możliwość dołączania zewnętrznych, wyniesionych modułów GigabitEthernet oraz 10 GigabitEthernet. Dołączenie modułów nie może być zrealizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3 a jedynie w ramach domeny fizycznej bądź stosu. Porty modułu wyniesionego muszą być udostępniane do zarządzania i monitorowania z poziomu przełącznika centralnego.	Opcjonalne	8
2.	Obsługa standardu 25GE CU Ethernet na wszystkich 48 portach przełącznika.		
3.	Przepustowość wewnętrznej magistrali przełączającej minimum 3.6Tbps.		

4.	Możliwość instalacji wentylatorów zapewniających przepływ powietrza przód-tył lub tył-przód zależnie od potrzeb.		
5.	Wsparcie standardu 100G Ethernet na 6 portach QSFP36 przełącznika, obsługa wkładek 100GBase-SR4/-LR4/-CU/-AOC.		
6.	Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP.		
7.	Wysokość modułu nie więcej 1RU.		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona. Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

4.4. Przełącznik dystrybucyjny (typ 1)

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1.	Typ i liczba portów – 24 porty Gigabit Ethernet SFP oraz 2 porty 1/10G SFP+.	Bezwzględne
2.	Dodatkowy slot przeznaczony na moduł rozszerzeń z możliwością jego wymiany "na gorąco" (ang. hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły zawierające: • Minimum 4-porty Gigabit Ethernet z gniazdami SFP • Minimum 2-porty 10 Gigabit Ethernet SFP+, przy czym wymagane jest, aby w przypadku wykorzystania pojedynczego łącza 10 GE SFP+ istniała możliwość instalacji dodatkowych 2 portów Gigabit Ethernet SFP (wymaga się dostarczenia takiego modułu wraz z przełącznikiem).	Bezwzględne
3.	Porty SFP obsługujące wkładki 100BaseFX i 1000Base-T/-SX/-LX/-EX/-ZX/-BX.	Bezwzględne
4.	Porty SFP+ obsługujące wkładki 10GBase-SR/-LR/-ER/-ZR/-BX/-CU.	Bezwzględne
5.	Możliwość stworzenia wirtualnego systemu złożonego ze stosu co najmniej 8 urządzeń będących przedmiotem opisu zarządzanego jako całość dostępnego pod jednym adresem IP. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać tworzenie połączeń z możliwością typu "*link aggregation*" na różnych fizycznie przełącznikach tworzących taki system wirtualny ("*multi-chassis link aggregation*") zgodnie z 802.3ad.	Bezwzględne
6.	Przepustowość - minimum 92 Gb/s oraz szybkość przełączania – minimum 68.4 Mp/s.	Bezwzględne
7.	Minimum 2 GB pamięci DRAM i 2 GB pamięci typu flash.	Bezwzględne

8.	Minimum 32 000 wpisów w tablicy adresów MAC.	Bezwzględne
9.	Minimum 24 000 wpisów w tablicy routingu IPv4.	Bezwzględne
10.	Możliwość utworzenia minimum 4 000 sieci VLAN oraz 1000 interfejsów SVI.	Bezwzględne
11.	Minimum 3000 wpisów ACE (Access Control Entries) na potrzeby realizacji polityk QoS i bezpieczeństwa.	Bezwzględne
12.	Obsługa ramek Ethernet o wielkości nie mniejszej niż 9198 bajtów (tzw. Jumbo Frame).	Bezwzględne
13.	Obsługa protokołów routingu statycznego i dynamicznego zarówno dla IPv4 jak i IPv6.	Bezwzględne
14.	Obsługa protokołów routingu warstwy 3 dla IPv4: RIPv1/v2, OSPF, BGP, IS-IS, PIM-SM.	Bezwzględne
15.	Obsługa protokołów routingu warstwy 3 dla IPv6: OSPFv3, RIPng.	Bezwzględne
16.	Obsługa Policy Base Routing.	Bezwzględne
17.	Obsługa IGMPv1/v2/v3 i MLDv1/v2 Snooping.	Bezwzględne
18.	IEEE 802.1w Rapid Spanning Tree (w tym Per-VLAN Rapid Spanning Tree - PVRST+).	Bezwzględne
19.	IEEE 802.1s Multiple Spanning Tree Protocol.	Bezwzględne
20.	IEEE 802.3ad Link Aggregation Control Protocol (w tym multi-chassis link aggregation).	Bezwzględne
21.	Obsługa co najmniej 128 instancji protokołu STP.	Bezwzględne
22.	Obsługa min. 8 kolejek, dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi z możliwością ustawienia bezwzględnego priorytetu kolejki w stosunku do innych (Strict Priority).	Bezwzględne
23.	Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek.	Bezwzględne
24.	Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kb/s (policing, rate limiting). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik.	Bezwzględne
25.	Kontrola sztormów dla ruchu broadcast/multicast/unicast.	Bezwzględne

26.	Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.	Bezwzględne
27.	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.	Bezwzględne
28.	Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP.	Bezwzględne
29.	Możliwość uruchomienia usługi serwera DHCP.	Bezwzględne
30.	Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend.	Bezwzględne
31.	Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia). Minimum 3000 wpisów dla list kontroli dostępu (ACE).	Bezwzględne
32.	Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu.	Bezwzględne
33.	Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal WWW).	Bezwzględne
34.	Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.	Bezwzględne
35.	Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.	Bezwzględne
36.	Wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem.	Bezwzględne
37.	Obsługa żądań Change of Authorization (CoA) zgodnie z RFC 5176.	Bezwzględne

38.	Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Gurad.	Bezwzględne
39.	Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard).	Bezwzględne
40.	Mechanizmy ochrony warstwy kontrolnej.	Bezwzględne
41.	Obsługa protokołów SNMPv3, SSHv2, SCP, HTTPS, Syslog – z wykorzystaniem protokołów IPv4 i IPv6.	Bezwzględne
42.	Obsługa protokołu NTP.	Bezwzględne
43.	Obsługa protokołu LLDP i LLDP-MED lub CDP.	Bezwzględne
44.	Zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Gigabit Ethernet.	Bezwzględne
45.	Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.	Bezwzględne
46.	Plik konfiguracyjny urządzenia musi być 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 musi być możliwe uruchomienie urządzenia z nową konfiguracją.	Bezwzględne
47.	Wbudowane makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (telefon IP, kamera	Bezwzględne
48.	Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.	Bezwzględne
49.	Uwierzytelnianie i autoryzacja w oparciu o serwer RADIUS lub TACACS+.	Bezwzględne

50.	Lokalna i zdalna obserwacja ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN (RSPAN).	Bezwzględne
51.	Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.	Bezwzględne

Parametry i funkcjonalności dodatkowe dla urządzenia

Lp.	Nazwa parametru	Typ wymagania *	Liczba punktów za spełnienie wymagania
1.	Obsługa standardu IEEE 802.1AE (szyfrowanie ruchu) z pełną wydajnością łącza na każdym z portów dostępowych.	Opcjonalne	6
2.	Funkcjonalność bramy dla usług mDNS.		
3.	Możliwość współdzielenia mocy zasilaczy, tzn. zasilacze muszą stanowić zasób wspólny dla przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania” mocy dla innych jednostek w stosie) – dla grup liczących do co najmniej 4 przełączników.		
4.	Możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 24.000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow.		
5.	Wbudowany analizator pakietów.		
6.	Wysokość nie większa niż 1RU.		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona. Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

4.5. Przełącznik dystrybucyjny (typ 2)

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1.	Typ i liczba portów – 48 portów Gigabit Ethernet 10/100/1000Base-T oraz 4 porty 1/10G SFP+.	Bezwzględne
2.	Dodatkowy slot przeznaczony na moduł rozszerzeń z możliwością jego wymiany "na gorąco" (ang. hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły zawierające: • Minimum 4-porty Gigabit Ethernet z gniazdami SFP, • Minimum 2-porty 10 Gigabit Ethernet SFP+, przy czym wymagane jest, aby w przypadku wykorzystania pojedynczego łącza 10 GE SFP+ istniała możliwość instalacji dodatkowych 2 portów Gigabit Ethernet SFP, • Minimum 4-porty 10 Gigabit Ethernet z gniazdam SFP+ (wymaga się dostarczenia takiego modułu wraz z przełącznikiem).	Bezwzględne
3.	Porty SFP obsługujące wkładki 100BaseFX i 1000Base-T/-SX/-LX/-EX/-ZX/-BX.	Bezwzględne
4.	Porty SFP+ obsługujące wkładki 10GBase-SR/-LR/-ER/-ZR/-BX/-CU.	Bezwzględne
5.	Możliwość stworzenia wirtualnego systemu złożonego ze stosu co najmniej 8 urządzeń będących przedmiotem opisu zarządzanego jako całość dostępnego pod jednym adresem IP. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać tworzenie połączeń z możliwością typu "*link aggregation*" na różnych fizycznie przełącznikach tworzących taki system wirtualny ("*multi-chassis link aggregation*") zgodnie z 802.3ad.	Bezwzględne
6.	Przepustowość - minimum 176 Gb/s oraz szybkość przełączania – minimum 68.4 Mp/s.	Bezwzględne
7.	Minimum 2 GB pamięci DRAM i 2 GB pamięci typu flash.	Bezwzględne

8.	Minimum 32 000 wpisów w tablicy adresów MAC.	Bezwzględne
9.	Minimum 24 000 wpisów w tablicy routingu IPv4.	Bezwzględne
10.	Możliwość utworzenia minimum 4 000 sieci VLAN oraz 1000 interfejsów SVI.	Bezwzględne
11.	Minimum 3000 wpisów ACE (Access Control Entries) na potrzeby realizacji polityk QoS i bezpieczeństwa.	Bezwzględne
12.	Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9198 bajtów (tzw. Jumbo Frame).	Bezwzględne
13.	Obsługa protokołów routingu statycznego i dynamicznego zarówno dla IPv4 jak i IPv6.	Bezwzględne
14.	Obsługa protokołów routingu warstwy 3 dla IPv4: RIPv1/v2, OSPF, BGP, IS-IS, PIM-SM.	Bezwzględne
15.	Obsługa protokołów routingu warstwy 3 dla IPv6: OSPFv3, RIPng.	Bezwzględne
16.	Obsługa Policy Base Routing.	Bezwzględne
17.	Obsługa IGMPv1/v2/v3 i MLDv1/v2 Snooping.	Bezwzględne
18.	IEEE 802.1w Rapid Spanning Tree (w tym Per-VLAN Rapid Spanning Tree - PVRST+).	Bezwzględne
19.	IEEE 802.1s (Multiple Spanning Tree Protocol - MSTP).	Bezwzględne
20.	IEEE 802.3ad Link Aggregation Control Protocol (w tym multi-chassis link aggregation).	Bezwzględne
21.	Obsługa co najmniej 128 instancji protokołu STP.	Bezwzględne
22.	Obsługa min. 8 kolejek, dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi z możliwością ustawienia bezwzględnego priorytetu kolejki w stosunku do innych (Strict Priority).	Bezwzględne
23.	Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek.	Bezwzględne
24.	Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kb/s (policing, rate limiting). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik.	Bezwzględne
25.	Kontrola sztormów dla ruchu broadcast/multicast/unicast.	Bezwzględne

26.	Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.	Bezwzględne
27.	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.	Bezwzględne
28.	Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP.	Bezwzględne
29.	Możliwość uruchomienia usługi serwera DHCP.	Bezwzględne
30.	Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend.	Bezwzględne
31.	Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia). Minimum 3000 wpisów dla list kontroli dostępu (ACE).	Bezwzględne
32.	Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu.	Bezwzględne
33.	Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal WWW).	Bezwzględne
34.	Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.	Bezwzględne
35.	Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.	Bezwzględne
36.	Wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem.	Bezwzględne
37.	Obsługa żądań Change of Authorization (CoA) zgodnie z RFC 5176.	Bezwzględne

38.	Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Gurad.	Bezwzględne
39.	Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard).	Bezwzględne
40.	Mechanizmy ochrony warstwy kontrolnej.	Bezwzględne
41.	Obsługa protokołów SNMPv3, SSHv2, SCP, HTTPS, Syslog – z wykorzystaniem protokołów IPv4 i IPv6.	Bezwzględne
42.	Obsługa protokołu NTP.	Bezwzględne
43.	Obsługa protokołu LLDP i LLDP-MED lub CDP.	Bezwzględne
44.	Zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Gigabit Ethernet.	Bezwzględne
45.	Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.	Bezwzględne
46.	Plik konfiguracyjny urządzenia musi być 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 musi być możliwe uruchomienie urządzenia z nową konfiguracją.	Bezwzględne
47.	Wbudowane makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (telefon IP, kamera).	Bezwzględne
48.	Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.	Bezwzględne
49.	Uwierzytelnianie i autoryzacja w oparciu o serwer RADIUS lub TACACS+.	Bezwzględne

50.	Lokalna i zdalna obserwacja ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN (RSPAN).	Bezwzględne
51.	Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.	Bezwzględne

Parametry i funkcjonalności dodatkowe dla urządzenia

Lp.	Nazwa parametru	Typ wymagania *	Liczba punktów za spełnienie wymagania
1.	Obsługa standardu IEEE 802.1AE (szyfrowanie ruchu) z pełną wydajnością łącza na każdym z portów dostępowych.	Opcjonalne	6
2.	Funkcjonalność bramy dla usług mDNS.		
3.	Możliwość współdzielenia mocy zasilaczy, tzn. zasilacze muszą stanowić zasób wspólny dla przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania” mocy dla innych jednostek w stosie) – dla grup liczących do co najmniej 4 przełączników.		
4.	Możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 24.000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow.		
5.	Wbudowany analizator pakietów.		
6.	Wysokość nie większa niż 1RU.		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona.

Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

4.6. Przełącznik dostępowy: typ 1, 2, 3

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1.	Liczba i rodzaj interfejsów zgodnie z zestawieniem w tabeli	Bezwzględnie
2.	Porty SFP+ obsługujące wkładki: 1000BaseT, 1000Base-SX/-LX/-EX/-ZX/-BX, 10GBase-SR/-LR/-LRM/-ER/-ZR/-CU.	Bezwzględnie
3.	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność łączenia w stosy. Wsparcie minimum 8 jednostek w stosie. Magistrala stakująca o przepustowości co najmniej 80Gb/s. Możliwość tworzenia połączeń EtherChannel zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie ("*Cross-stack EtherChannel*").	Bezwzględnie
4.	Urządzenie musi posiadać minimum 512MB pamięci DRAM i 128MB pamięci flash.	Bezwzględnie
5.	Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB.	Bezwzględnie
6.	Obsługa minimum 1000 sieci VLAN.	Bezwzględnie
7.	Przepustowość przełącznika minimum 108Gb/s (216Gb/s full duplex).	Bezwzględnie
8.	Minimum 16 000 wpisów w tablicy adresów MAC.	Bezwzględnie
9.	Minimum 16 statycznych tras dla routingu IPv4 i IPv6.	Bezwzględnie
10.	Wsparcie dla minimum 128 instancji protokołu STP.	Bezwzględnie
11.	Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame).	Bezwzględnie

12.	Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping.	Bezwzględnie
13.	Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server.	Bezwzględnie
14.	Obsługa protokołu NTP.	Bezwzględnie
15.	IEEE 802.1w Rapid Spanning Tree.	Bezwzględnie
16.	IEEE 802.1s Multiple Spanning Tree.	Bezwzględnie
17.	IEEE 802.3ad (Link Aggregation Control Protocol) w tym Cross-stack link aggregation.	Bezwzględnie
18.	Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych.	Bezwzględnie
19.	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, żródłowy/docelowy port TCP.	Bezwzględnie
20.	Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP.	Bezwzględnie
21.	Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi. Wymagana jest możliwość skonfigurowania minimum 256 różnych ograniczeń.	Bezwzględnie
22.	Mechanizm automatyczny QoS.	Bezwzględnie
23.	Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend.	Bezwzględnie

24.	Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x z możliwością przydziału listy kontroli dostępu (ACL) i VLANu, obsługa Guest VLAN. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1x. Zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1x, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o WWW. Wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie.	Bezwzględnie
25.	Obsługa co najmniej następujących mechanizmów: Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard. Mechanizmy zgodnie z IEEE 802.3ad (obsługa tych mechanizmów na interfejsach "*link aggregation*").	Bezwzględnie
26.	Obsłuta podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard).	Bezwzględnie
27.	Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP.	Bezwzględnie
28.	Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6.	Bezwzględnie
29.	Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.	Bezwzględnie
30.	Obsługa żądań Change of Authorization (CoA) zgodnie z RFC 5176.	Bezwzględnie
31.	Funkcjonalność Protected Port.	Bezwzględnie
32.	Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.	Bezwzględnie
33.	Mechanizmy ochrony warstwy kontrolnej.	Bezwzględnie
34.	Ma możliwość zarządzania przez SNMPv3 oraz SSH v2, HTTP/S z wykorzystaniem IPv4 i IPv6.	Bezwzględnie

35.	Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Ethernet.	Bezwzględnie
36.	Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+.	Bezwzględnie
37.	Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN.	Bezwzględnie
38.	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.	Bezwzględnie
39.	Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.	Bezwzględnie
40.	Obsługa protokołu LLDP i LLDP-MED CDP.	Bezwzględnie
41.	Makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (telefon IP).	Bezwzględnie

4.6.1. Przełącznik dostępowy typ 1

Lp.	**Nazwa parametru**	**Typ wymagania***
Typ i liczba portów – minimum 48 portów 10/100/1000 RJ-45 oraz minimum 2 porty uplink 10Gigabit Ethernet SFP+.		Bezwzględnie

4.6.2. Przełącznik dostępowy typ 2

Lp.	**Nazwa parametru**	**Typ wymagania***

Typ i liczba portów – minimum 48 portów 10/100/1000 RJ-45 oraz minimum 4 porty uplink 1 Gigabit Ethernet SFP.	Bezwzględnie

4.6.3. Przełącznik dostępowy typ 3

Lp.	Nazwa parametru	Typ wymagania *
Typ i liczba portów – minimum 24 portów 10/100/1000 RJ-45 z PoE+ oraz minimum 4 porty uplink 1 Gigabit Ethernet SFP.		Bezwzględnie
Zasilanie na portach według standardu 802.3at PoE+. Minimalny budżet mocy PoE+ dla przełącznika to 370W		Bezwzględnie

parametry i funkcjonalności dodatkowe dla urządzeń

Lp.	Nazwa parametru	Typ wymagania *	Liczba punktów za spełnienie wymagania
1.	Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet). Możliwość hibernowania przełącznika w określonych godzinach celem dodatkowego oszczędzania energii.	Opcjonalne	15
2.	Przełącznik posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow lub odpowiednik (bez samplowania). Funkcjonalność wspierająca ruch IPv4, IPv6 oraz ruch głosowy.		
3.	Wysokość nie większa niż 1RU, a głębokość nie większa niż 60cm.		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona. Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

4.7. Firewall segmentu brzegowego

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1	Dedykowane, fizyczne urządzenie zabezpieczeń sieciowych znajdujące się w obudowie typu rack.	Bezwzględnie
2	Minimalna liczba i rodzaj portów: 20 portów 10 Gigabit oraz 4 porty 40 Gigabit Ethernet + dodatkowe porty pozwalające na zestawienie clustra HA active / pasive	Bezwzględnie

3	Dysk o pojemności nie mniejszej niż 120 GB	Bezwzględnie
4	Dedykowany port do zarządzania out-of-band.	Bezwzględnie
5	Wydajność przynajmniej 14 Gb/s dla ruchu IPSec VPN.	Bezwzględnie
6	Przepustowość w ruchu nie mniej niż 35 Gb/s dla kontroli firewall z włączoną funkcją kontroli aplikacji.	Bezwzględnie
7	Obsługa minimum 300.000 nowych połączeń na sekundę.	Bezwzględnie
8	Obsługa minimum 8.000.000 jednoczesnych połączeń.	Bezwzględnie
9	Obsługa minimum 4.000 tuneli IPsec	Bezwzględnie
10	Obsługa minimum 10.000 tuneli SSL VPN	Bezwzględnie
11	Obsługa minimum 450 stref bezpieczeństwa	Bezwzględnie
12	Obsługa minimum 19.000 polityk firewall	Bezwzględnie
13	Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona Intrusion Prevention, antywirus, filtracja aplikacji i kategoryzacja URL) nie mniejsza niż 17 Gb/s.	Bezwzględnie
14	W architekturze rozwiązania występują moduł zarządzania oraz moduł przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.	Bezwzględnie
15	Rozwiązanie ma posiadać możliwość podłączenia urządzeń firewall w klastrze pod scentralizowany system zarządzania.	Bezwzględnie
16	Umożliwienie stworzenia i konfiguracji minimum 25 wirtualnych firewalli. Możliwość rozbudowy urządzenia w celu rozszerzenia konfiguracji do obsługi definicji minimum 125 wirtualnych firewalli.	Bezwzględnie
17	Zapewniona obsługa dla IPv6.	Bezwzględnie
18	System zabezpieczeń firewall działa zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.	Bezwzględnie

19	Zapewnienie możliwości definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.	Bezwzględnie
20	Polityka zabezpieczeń firewall uwzględnia adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, oraz umożliwia rejestrowanie zdarzeń i alarmowanie.	Bezwzględnie
21	Zapewniona statyczna i dynamiczna translacja adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.	Bezwzględnie
22	Zapewnienie możliwości statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.	Bezwzględnie
23	Zapewniona obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Możliwość tworzenia subinterfejsów VLAN, które to mogą być kreowane na interfejsach sieciowych pracujących zarówno w trybie L2 jak i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.	Bezwzględnie
24	Zapewnione działanie urządzenia w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym (tzn. w warstwie 2 modelu OSI) oraz trybie pasywnego nasłuchu (tzn. TAP). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych, jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.	Bezwzględnie
25	Tryb pracy urządzenia ma być ustalany na poziomie konfiguracji interfejsu sieciowego. System umożliwia pracę we wszystkich dostępnych trybach (router, transparentny oraz pasywnego nasłuchu) na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (wirtualny system, wirtualna domena,).	Bezwzględnie
26	Zapewniona obsługa protokołów routingu dynamicznego, przynajmniej BGP, RIP i OSPF.	Bezwzględnie

27	Urządzenie musi być produktem o uznanej na rynku pozycji i musi odpowiadać opisowi wymagań sformułowanych dla grupy „Leaders” lub „Chellengers” raportu Gartnera pt. „Magic Quadrant of Enterprise Network Firewalls – 2015” lub „Magic Quadrant of Enterprise Network Firewalls – 2016”	Bezwzględnie
28	Urządzenie umożliwia zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.	Bezwzględnie
29	Możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.	Bezwzględnie
30	Możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.	Bezwzględnie
31	Możliwość integracji ze środowiskiem wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.	Bezwzględnie
32	Posiadanie funkcji ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.	Bezwzględnie
33	Umożliwienie realizacji zadań kontroli dostępu (filtracji ruchu sieciowego), poprzez kontrolę ruchu na poziomie warstw sieciowej, transportowej oraz aplikacji.	Bezwzględnie
34	Możliwość pracy w konfiguracji odpornej na awarie w trybie klastra Active-Passive i Active-Active.	Bezwzględnie

35	Zestawianie i obsługa 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. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji (w przypadku gdy jest to funkcjonalność licencjonowana, wymagane jest dostarczenie licencji na ilość tuneli IPsec i SSL VPN wymaganych w SIWZ w pkt. 5.7 poz. 9 i 10)	Bezwzględnie
36	Możliwość uruchomienia modułu filtrowania stron WWW per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (interfejs sieciowy, strefa bezpieczeństwa).	Bezwzględnie
37	Możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.	Bezwzględnie
38	Posiadanie modułu inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak http, smtp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.	Bezwzględnie
39	Możliwość uruchomienia modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (interfejs sieciowy, strefa bezpieczeństwa).	Bezwzględnie
40	Posiadanie modułu umożliwiającego wykrywanie i blokowanie ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.	Bezwzględnie

41	Posiadanie modułu anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.	Bezwzględnie
42	Możliwość uruchomienia modułu inspekcji anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu anty-spyware uruchamiany był per urządzenie lub jego część (interfejs sieciowy, strefa bezpieczeństwa).	Bezwzględnie
43	Możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.	Bezwzględnie
44	Posiadanie sygnatur DNS wykrywających i blokujących ruch do domen uznanych za złośliwe.	Bezwzględnie
45	Możliwość sprawdzenia wpływu nowo pobranych aktualizacji sygnatur IPS (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.	Bezwzględnie
46	Funkcjonalność podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).	Bezwzględnie
47	Posiadanie funkcji wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.	Bezwzględnie
48	Możliwość identyfikacji co najmniej 1000 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS: Skype, Gadu-Gadu, Tor, BitTorrent, eMule.	Bezwzględnie
49	Możliwość automatycznej identyfikacji aplikacji 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.	Bezwzględnie
50	Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.	Bezwzględnie

51	Możliwość blokowania transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.	Bezwzględnie
52	Możliwość skanowania całości ruchu pod kątem zaistnienia podatności, a nie wyłącznie wybranych próbek ruchu.	Bezwzględnie
53	Zapewnienie inspekcji komunikacji szyfrowanej dla protokołu HTTPS (HTTP szyfrowane protokołem TLS/SSL) dla ruchu wychodzącego do serwerów zewnętrznych (komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi posiadać możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.	Bezwzględnie
54	Możliwość transparentnego ustalania tożsamość użytkowników sieci w oparciu o Active Directory. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług w sieci i musi być 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.	Bezwzględnie
55	Możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia.	Bezwzględnie
56	Urządzenie umożliwia czytanie oryginalnych adresów IP stacji końcowych z nagłówkaX-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje, w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.	Bezwzględnie

57	Urządzenie nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.	Bezwzględnie
58	Zarządzanie systemu zabezpieczeń odbywa się z linii poleceń (CLI) oraz z graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.	Bezwzględnie
59	Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.	Bezwzględnie
60	Interfejs administracyjny urządzenia jest w języku polskim lub angielskim.	Bezwzględnie
61	Możliwość uwierzytelniania administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+.	Bezwzględnie
62	Możliwość stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (baza lokalna, LDAP i RADIUS).	Bezwzględnie
63	Budowa oprogramowania zarządzającego w oparciu o koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.	Bezwzględnie
64	Konsola zarządzająca, logująca i raportująca umożliwia korelowanie zbieranych zdarzeń i informacji oraz budowanie na ich podstawie wielu, dostosowanych do potrzeb Zamawiającego raportów. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowaniu stron WWW. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.	Bezwzględnie

65	Możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatace co najmniej PDF	Bezwzględnie
66	Konsola zarządzająca, logująca i raportująca ma umożliwiać pracę w trybie kolektora logów zbierającego jedynie dane z systemów bezpieczeństwa lub w trybie pełnej analizy w celu optymalizacji procesu zbierania logów. Powinna istnieć możliwość rozbudowy systemu zarządzającego, logującego i raportującego o kolejne urządzenia tak aby umożliwić zwiększenie pojemności lub/i wydajności całego systemu w przyszłości. Nie dopuszcza się systemu w którym występuje konieczność rozdzielenia funkcji raportowania i logowania oraz funkcji zarządzania na dwa różne systemy fizyczne lub logiczne.	Bezwzględnie
67	Możliwość usuwania logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.	Bezwzględnie
68	Konsola zarządzająca, logująca i raportująca ma umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur oraz funkcje audytu i backupu konfiguracji. Konsola zarządzania ma posiadać możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.	Bezwzględnie
69	W przypadku gdy urządzenie pozwala na jednoczesną pracę dwu lub więcej administratorów musi istnieć wbudowany w system mechanizm umożliwiający jednemu z administratorów uzyskanie wyłączności na wprowadzanie zmian. W tym czasie pozostali zalogowani użytkownicy nie mogą być w stanie dokonać żadnych zmian w konfiguracji.	Bezwzględnie
70	Obsługa przesyłania logów do min. 3 zdefiniowanych serwerów Syslog. Administrator urządzenia ma mieć możliwość zdefiniowania, dla każdej reguły bezpieczeństwa, innego serwera Syslog.	Bezwzględnie

Parametry i funkcjonalności dodatkowe dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*)	Liczba punktów za spełnienie wymagania
1	Istnieje możliwość objęcia dostarczanych firewalli Systemem zarządzania , który będzie zarządzać również posiadanymi przez Zamawiającego firewallami Palo Alto PA3020 (2 sztuki) - w zakresie nie mniejszym niż opisane w pkt 63-77 wymagań obligatoryjnych	Opcjonalne	19
2	Polityka zabezpieczeń firewall uwzględnia strefy bezpieczeństwa		
3	Posiadanie modułu inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak imap, pop3, ftp, kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.		
4	Możliwość uruchomienia modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (interfejs sieciowy, strefa bezpieczeństwa).		
5	Możliwość ręcznego tworzenia sygnatur IPS dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta		

Lp.	Nazwa parametru	Typ wymagania*)	Liczba punktów za spełnienie wymagania
6	Możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.		
7	Zezwolenie dostępu dla aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (w IPS lub innym module UTM).		
8	Możliwość definiowania i przydzielania różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi istnieć możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.		
9	Możliwość analizy i blokowania plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.		
10	Możliwość ochrony przed atakami typu „Drive-by-download” poprzez skonfigurowanie strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.		

Lp.	Nazwa parametru	Typ wymagania*)	Liczba punktów za spełnienie wymagania
11	Zapewnienie inspekcji komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.		
12	System zabezpieczeń firewall musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH		
13	Posiadanie interfejsu XML API będącego integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).		
14	Możliwość uwierzytelniania administratorów za pomocą serwera Kerberos.		
15	Możliwość stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (baza lokalna, LDAP i RADIUS).		

Lp.	Nazwa parametru	Typ wymagania*)	Liczba punktów za spełnienie wymagania
16	Wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 120 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.		
17	Włączenie logowania na dysk nie obniża wydajność urządzenia.		
18	Budowanie reguł zabezpieczeń firewall zgodne z ustaloną polityką opartą o profile oraz obiekty. Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa. Konsola zarządzania ma posiadać możliwość automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.		
19	Przynajmniej dwa dyski o pojemności nie mniejszej niż 120 GB połączone w RAID 1 (2 x 120 GB).		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona.
Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

4.8. Router segmentu brzegowego

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1.	Typ i liczba portów – minimum 6 portów Gigabit Ethernet SFP oraz minimum 2 porty 10 Gigabit Ethernet SFP+.	Bezwzględnie
2.	Możliwość rozbudowy między innymi o następujące porty: • 1 port 10 Gigabit Ethernet, • 8 portów Gigabit Ethernet, • 4 interfejsy ATM STM1 lub 2 interfejsy STM4.	Bezwzględnie
3.	Porty SFP+ obsługujące wkładki: 1000BaseT, 100BaseFX, 1000Base-SX/-LX/-EX/-ZX/-BX, 10GBase-SR/-LR/-LRM/-ER/-ZR/-CU.	Bezwzględnie
4.	Porty SFP obsługujące wkładki 100BaseFX i 1000Base-T/-SX/-LX/-EX/-ZX/-BX	
5.	Minimum 16GB pamięci RAM.	Bezwzględnie
6.	Dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet 10/100/1000 oraz port AUX.	Bezwzględnie
7.	Port USB.	Bezwzględnie
8.	Przepustowość urządzenia nie mniejsza niż 20Gbps.	Bezwzględnie
9.	Wydajność routingu mierzona dla ruchu IPv4 (pakiety 64 bajtowe) nie mniejsza niż 19Mpps.	Bezwzględnie
10.	Urządzenie posiada dedykowany akcelerator kryptograficzny osiągający wydajność 5 Gbps dla ruchu IMIX.	Bezwzględnie
11.	Urządzenie obsługuje minimum 2 000 000 prefiksów w tablicach routingu IPv4.	Bezwzględnie
12.	Urządzenie obsługuje minimum 2 000 000 prefiksów w tablicach routingu IPv6.	Bezwzględnie
13.	Urządzenie obsługuje minimum 100 000 tras multicast.	Bezwzględnie
14.	Urządzenie obsługuje 4000 tuneli GRE.	Bezwzględnie

15.	Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP.	Bezwzględnie
16.	Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP.	Bezwzględnie
17.	Urządzenie obsługuje Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter).	Bezwzględnie
18.	Urządzenie umożliwia uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu Forwarding), umożliwiając wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci. Obsługa 8000 instancji VRF.	Bezwzględnie
19.	Urządzenie obsługuje funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.	Bezwzględnie
20.	Urządzenie obsługuje funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF.	Bezwzględnie
21.	Urządzenie obsługuje multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN.	Bezwzględnie
22.	Obsługa MPLS, w szczególności: LDP, EoMPLS, VPLS, MPLS L3 VPN, MPLS TE, MPLS FRR w trybach protekcji łącza oraz węzła.	Bezwzględnie
23.	System modularny umożliwiający aktualizację poszczególnych modułów programowych niezależnie od siebie.	Bezwzględnie
24.	Redundancja procesów rutingowych realizowana poprzez uruchomienie dwóch kopii systemu operacyjnego – jeśli wymaga to dodatkowej licencji jest dostarczenie nie jest wymagane.	Bezwzględnie
25.	Funkcjonalność IP Fast ReRoute (RFC 5286).	Bezwzględnie
26.	BGP Prefix-Independent Convergence (PIC).	Bezwzględnie
27.	Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP.	Bezwzględnie
28.	Funkcjonalność VRRP.	Bezwzględnie

29.	Klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN zarówno dla IPv4 jak i IPv6.	Bezwzględnie
30.	Hierarchiczny QoS (H-QoS) - 3 poziomy.	Bezwzględnie
31.	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP.	Bezwzględnie
32.	Dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek.	Bezwzględnie
33.	Algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek.	Bezwzględnie
34.	Możliwość obsługi jednej kolejki z priorytetem w stosunku do innych mechanizm ograniczania ilości ruchu w kolejce priorytetowej.	Bezwzględnie
35.	Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.	Bezwzględnie
36.	Możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting).	Bezwzględnie
37.	Mechanizm WRED.	Bezwzględnie
38.	Możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS.	Bezwzględnie
39.	Sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu.	Bezwzględnie
40.	Unicast RPF (Reverse Path Forwarding).	Bezwzględnie
41.	Listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL.	Bezwzględnie
42.	Obsługa 4000 list kontroli dostępu (ACL) – z liczbą wpisów nie mniejszą niż 50 000 wpisów dla IPv4 / 25 000 wpisów dla IPv6 dla wszystkich list ACL.	Bezwzględnie
43.	Dostęp administracyjny oparty o role z przypisanymi uprawnieniami.	Bezwzględnie

44.	Ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU.	Bezwzględnie
45.	Logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU.	Bezwzględnie
46.	Ma możliwość zarządzania przez SNMPv3 oraz SSH v2, HTTP/S z wykorzystaniem IPv4 i IPv6.	Bezwzględnie
47.	Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Ethernet.	Bezwzględnie
48.	Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+.	Bezwzględnie
49.	Obsługuje MPLS OAM.	Bezwzględnie
50.	Umożliwia pisanie skryptów konfiguracyjnych.	Bezwzględnie
51.	Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.	Bezwzględnie
52.	Obsługa protokołu LLDP i LLDP-MED lub CDP.	Bezwzględnie
53.	obsługuje protokół Netflow ze wsparciem dla multicast oraz IPv4/IPv6, wielkość cache’a nie mniejsza niż 2 000 000 wpisów	Bezwzględnie
54.	posiada narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP	Bezwzględnie
55.	posiada obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+	Bezwzględnie
56.	urządzenie posiada możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów	Bezwzględnie

Parametry i funkcjonalności dodatkowe dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*	Liczba punktów za spełnienie wymagania
1.	Urządzenie musi zapewniać możliwość pełnego przeniesienia konfiguracji z posiadanego przez Zamawiającego routera serii ASR1000.	Opcjonalne	6
2.	Urządzenie umożliwia dołożenie przestrzeni dyskowej typu SSD o pojemności 400 GB		
3.	Wysokość nie większa niż 2RU.		
4.	Możliwość uruchomienia funkcjonalności analizy i klasyfikacji pakietów w warstwie 2-7 polegającej na przeszukiwaniu pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków. Urządzenie musi być sprzętowo przygotowane do uruchomienia danej funkcjonalności. Jeżeli funkcja ta wymaga dodatkowych licencji ich dostarczenie nie jest wymagane, jednakże urządzenie musi umożliwiać ich uruchomienie bez konieczności dokonywania zmian sprzętowych.		

5.	Możliwość uruchomienie usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, przy czym klasyfikacja ta: • opiera się na kilku mechanizmach gwarantujących poprawne rozpoznawanie wielu aplikacji / protokołów, • udostępnia 3 atrybuty opisujące daną aplikację / protokół (atrybuty ułatwiają konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji / protokołów - na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji. Urządzenie musi być sprzętowo przygotowane do uruchomienia danej funkcjonalności. Jeżeli funkcja ta wymaga dodatkowych licencji ich dostarczenie nie jest wymagane, jednakże urządzenie musi umożliwiać ich uruchomienie bez konieczności dokonywania zmian sprzętowych.		

6.	Funkcjonalność zapory ogniowej typu statefull (ang. statefull firewall), przy czym zapora ogniowa: • umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji), • obsługuje ruch IPv4 oraz IPv6, • umożliwia konfigurację polityk per wirtualna tablica routingu (VRF), • umożliwia obsługę 2 000 000 równoczesnych sesji, • umożliwia zestawianie 200 000 nowych połączeń HTTP na sekundę. Urządzenie musi być sprzętowo przygotowane do uruchomienia danej funkcjonalności. Jeżeli funkcja ta wymaga dodatkowych licencji ich dostarczenie nie jest wymagane, jednakże urządzenie musi umożliwiać ich uruchomienie bez konieczności dokonywania zmian sprzętowych.		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona. Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

4.9. Router zdalny

Parametry i funkcjonalności bezwzględnie wymagane dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*
1	Typ i liczba portów - dwa interfejsy WAN Gigabit Ethernet 10/100/1000, z czego jeden combo RJ-45 lub SFP (możliwość wyposażenia we wkładkę światłowodową).	Bezwzględnie
2	Port SFP+ obsługujący wkładki: 1000BaseT, 100BaseFX, 1000Base-SX/-LX/-BX.	Bezwzględnie
3	Wbudowany przełącznik zarządzalny 8-portowy 10/100/1000 RJ45.	Bezwzględnie
4	Chłodzenie pasywne (bez wentylatorów).	Bezwzględnie
5	Zasilacz zewnętrzny 230V AC.	Bezwzględnie
6	Routing IPv4 i IPv6 – statyczny i dynamiczny (RIP, OSPF, BGP).	Bezwzględnie
7	Routing multicast – PIM-DM, PIM-SM, PIM-SSM. Obsługa protokołów IGMP v2/3 i MLDv2.	Bezwzględnie
8	Policy based routing (PBR).	Bezwzględnie
9	Unicast Reverse Path Forwarding (uRPF).	Bezwzględnie
10	Routing między sieciami VLAN w oparciu o trunking 802.1Q.	Bezwzględnie
11	Obsługa DHCP w zakresie Client, Server oraz Relay.	Bezwzględnie
12	Obsługa wirtualnych instancji routingu (VRF) - 8 instancji.	Bezwzględnie
13	Obsługa protokołu NTP.	Bezwzględnie
14	Obsługa BFD.	Bezwzględnie
15	Generic routing encapsulation (GRE) i multipoint GRE (MGRE).	Bezwzględnie
16	Obsługa funkcji Metro Ethernet – E-LMI i Ethernet OA&M.	Bezwzględnie
17	Interfejs komend (CLI).	Bezwzględnie

18	Obsługa SNMPv3, SSHv2.	Bezwzględnie
19	Tekstowy plik konfiguracyjny z możliwością edycji off-line.	Bezwzględnie
20	Możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów.	Bezwzględnie
21	Możliwość eksportu statystyk ruchowych za pomocą protokołu NetFlow lub równoważnego.	Bezwzględnie
22	Obsługa mechanizmów AAA (authentication, authorization, accounting) z wykorzystaniem protokołów RADIUS i TACACS+.	Bezwzględnie
23	Port konsoli szeregowej.	Bezwzględnie
24	Port USB z możliwością podłączenia pamięci flash.	Bezwzględnie
25	Funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall).	Bezwzględnie
26	Funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall).	Bezwzględnie
27	Obsługa list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP.	Bezwzględnie
28	Obsługa 50 tuneli IPSec VPN.	Bezwzględnie
29	Wsparcie dla Public Key Infrastructure (PKI).	Bezwzględnie
30	Zaimplementowana technologia umożliwiającą szyfrowanie IPSec ruchu unicast IPv4 bez konieczności tworzenia tuneli, z wykorzystaniem protokołu Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547.	Bezwzględnie
31	Obsługa IEEE 802.1X dla portów przełącznika.	Bezwzględnie
32	Ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU.	Bezwzględnie
33	Możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługa ruchu (Policing, Shaping) w oparciu o klasę ruchu.	Bezwzględnie
34	Obsługa mechanizmów kolejkowania ruchu: z obsługą kolejki absolutnego priorytetu, ze statyczną alokacją pasma dla typu ruchu, WFQ.	Bezwzględnie

35	WRED (Weighted Random Early Detection).	Bezwzględnie
36	Mechanizm ograniczania pasma dla określonego typu ruchu.	Bezwzględnie

Parametry i funkcjonalności dodatkowe dla urządzenia

Lp.	Nazwa parametru	Typ wymagania*)	Liczba punktów za spełnienie wymagania
1.	MPLS Multiprotocol Label Switching	Opcjonalne	5
2.	Możliwość rozszerzenia funkcjonalności o funkcję optymalizatora ruchu sieciowego		
3.	Sprzętowy akcelerator szyfrowania dla 3DES, AES 128, AES 192, AES 256		

* – Wymaganie „Bezwzględne” oznacza, że w przypadku niespełniania dowolnego wymagania oznaczonego jako bezwzględne, Oferta zostanie odrzucona. Wymaganie „Opcjonalne” oznacza, że Wykonawca może ale nie musi zaoferować wyższe parametry. Wyższe parametry będą dodatkowo punktowane na etapie oceny Oferty.

** – Potwierdzić spełnianie wymagania, poprzez pozostawienia „Tak” dla wymagań „Bezwzględnych” lub skreślić niepotrzebne dla wymagań „Opcjonalnych”.

4.10.Moduły połączeniowe i kable

W ramach wdrożenia Wykonawca wyposaży dostarczone urządzenia w następujące wkładki/moduły i kable (ilości określone w tabeli są wartościami minimalnymi, ilość rzeczywista modułów zostanie określona w projekcie):

Lp.	Opis	Prędkość	Odległość*	Rodzaj kabla FO	Typ gniazda FO	Ilość sztuk
1.	QSFP 40Gbps moduł optyczny	40Gbps	10km	SMF (1310nm)	LC	12
2.	QSFP 40Gbps moduł kablowy (miedziany)	40Gbps	1m			4
3.	SFP+ 10GBASE-SR moduł optyczny	10Gbps	300m (OM3)	MMF (850nm)	LC	131
4.	SFP+ 10GBASE-LR moduł optyczny	10Gbps	10km	SMF (1310nm)	LC	43
5.	SFP+ 10GBASE-CU moduł kablowy (miedziany)	10Gbps	1m			8
6.	SFP+ 10GBASE-CU moduł kablowy (miedziany)	10Gbps	3m			32
7.	SFP 1000BASE-LH moduł optyczny	1Gbps	10km	SMF (1310nm)	LC	10

* - oznacza minimalną odległość jaką powinno gwarantować połączenie z użyciem danego rodzaju wkładek/modułów.

4.11.System zarządzania

Wykonawca musi dostarczyć System Zarządzania Infrastrukturą Sieciową (SZIS) zapewniający następujące funkcjonalności:

1) zbieranie statystyk z wykorzystaniem SNMP,
2) narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci,
3) możliwość manualnego dodawania urządzeń,
4) narzędzia wyświetlania urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu,
5) mapa topologii urządzeń z połączeniami oraz wizualizacja alarmów na urządzeniach,
6) narzędzia do zdalnej konfiguracji urządzeń w zakresie: predefiniowanej konfiguracji dla poszczególnych typów urządzeń, automatycznej konfiguracji portów,
7) funkcje archiwizacji konfiguracji, przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń, porównywania konfiguracji,
8) narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych,
9) narzędzie umożliwiające zbieranie informacji o parametrach urządzeń, przynajmniej takich jak: zajętość CPU, zajętość pamięci, dostępność, ilość portów, utylizacja portów,
10) mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie,
11) zbieranie statystyk za pomocą Netflow,
12) monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania pozwalające na analizę: ilości i charakterystyki ruchu, czas odpowiedzi, czas transakcji oraz opóźnienie,
13) narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku,
14) narzędzie do zbierania alarmów pochodzących z urządzeń, kategoryzacji alarmów,
15) informowanie o alarmach/incydentach przez notyfikację email,
16) praca w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci,
17) interfejs bazujący na HTML5,
18) budowanie widoków przez użytkownika,
19) funkcje szybkiej nawigacji wraz z szybkim wyświetlaniem informacji przy zbliżeniu kursora myszy do interesującego obiektu,

20) hierarchizacja zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów lub zewnętrznego serwera uwierzytelniającego,

21) narzędzia pozwalające na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy,

22) współpraca z serwerami czasu (NTP),

23) narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku,

24) tworzenie raportów dotyczących urządzeń sieciowych, urządzeń klienckich oraz wydajności sieci,

25) tworzenie raportów dotyczących końca życia oraz sprzedaży urządzeń oraz raportów dotyczących luk bezpieczeństwa na urządzeniach sieciowych,

26) narzędzie pozwalające na monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania, pozwalające na analizę, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie,

27) narzędzie pozwalające na diagnostykę działania urządzenia przez wykonanie ping, traceroute, połączenie się z urządzeniem przez telnet, ssh, http, https,

28) wyświetlanie wykresów korelujących zmiany w konfiguracji ze zdarzeniami na urządzeniu w celu lepszej i szybszej diagnostyki problemów,

29) współpraca z systemem od uwierzytelniania i autoryzacji urządzeń klienckich i użytkowników w celu zbierania informacji o polityce dostępowej nałożonej na urządzenie oraz w celu generowania raportów dotyczących statystyk AAA,

30) API REST do integracji z innymi narzędziami/systemami,

31) system powinien być dostarczony w najnowszej dostępnej wersji,

32) wspiera wysoką dostępność i pracę w trybie active-standby (nie wymaga się dostarczania systemu w wysokiej dostępności),

33) umożliwia synchronizację danych między systemami redundantnymi,

34) dopuszcza się dostarczenia systemu zarządzania w formie maszyn wirtualnych pracujących pod VMware ESXi,

35) nie wymaga się dostarczenia platformy sprzętowej pod system do zarządzania.

36) SZIS musi umożliwiać zarządzanie w co najmniej w/w zakresie następującymi typami urządzeń:

    Posiadanymi aktualnie przez zamawiającego, tj.:

a. Przełączniki Cisco: C2950, C2960, C3560 - 250 szt.
b. Rutery Mikrotik, platformy: TILE, MIPSBE, SMIPS, PPC- 50 szt.
c. Łącza radiowe Ubiquiti: NanoBridge M, NanoBeam M, NanoStation M, Air Fiber24 – 150 szt.
d. Punkty dostępowe WiFi: Ubiquiti Unifi- 250 szt.
e. Firewall Palo Alto 3020 – 1 szt.
f. Ruter Cisco ASR 1000 - 1 szt.

Jak również nabywane w ramach niniejszego postępowania:

i. Przełącznik rdzenia (typ 1),
ii. Przełącznik rdzenia (typ 2),
iii. Przełącznik Data Center,
iv. Przełącznik dystrybucyjny (typ 1),
v. Przełącznik dystrybucyjny (typ 2),
vi. Przełącznik dostępowy (typ 1),
vii. Przełącznik dostępowy (typ 2),
viii. Przełącznik dostępowy (typ 3),
ix. Router segmentu brzegowego,
x. Router zdalny.

4.12.Rozbudowa systemu SIEM

Zamawiający posiada System SIEM oparty na technologii Splunk Enterprise (specyfikacja licencji poniżej). Zamawiający wymaga rozbudowy Systemu SIEM z zachowaniem wszystkich posiadanych

funkcjonalności oraz objęcia rozbudowanego Systemu SIEM wsparciem producenta przez okres gwarancji wskazany w umowie.

Licencje obecnie posiadane przez Zamawiającego:

Numer produktu	Opis	Uwagi
SE-P-LIC	Splunk Enterprise - Perpetual License - 20 GB/day	Licencja 20GB / dzień
SE-P-ESUP	Splunk Enterprise - Enterprise Support	Support do dnia: 2016-10-18

Licencje po rozbudowie, które powinien posiadać Zamawiający:

Numer produktu	Opis	Uwagi
SE-P-LIC	Splunk Enterprise - Perpetual License - 40 GB/day	Licencja 40GB / dzień
SE-P-ESUP	Splunk Enterprise - Enterprise Support	Support: 36 miesięcy

Uwaga!

Support producenta powinien obejmować rozbudowaną licencję tj. 40GB/dzień przez cały okres trwania gwarancji.

4.13.Zakres wdrożenia

Architektura sieci zakłada stworzenie sieci rdzeniowej opartej o trzy niezależne i odległe geograficznie lokalizacje.

Wykonawca dostarczy sprzęt i przeprowadzi instalację urządzeń we wskazanych w projekcie lokalizacjach na własny koszt. Instalacja urządzeń odbędzie się pod nadzorem osób wskazanych przez Zamawiającego w terminach uzgodnionych z Zamawiającym.

Wszystkie urządzenia zostaną przekazane na stan zamawiającego w momencie podpisania protokołu odbioru. Wykonawca zobowiązany jest do ubezpieczenia na własny koszt dostarczanych urządzeń na czas od momentu dostawy do momentu podpisania protokołu odbioru.

Wykonawca dostarczy wszelkie niezbędne akcesoria oraz okablowanie niezbędne do uruchomienia dostarczonego sprzętu.

Komunikacja w obrębie rdzenia zostałaby oparta o dedykowane połączenia światłowodowe i technologię 40Gbps Ethernet w topologii podwójnego pierścienia. Poziom redundancji i niezawodności zwiększony jest poprzez zastosowanie redundancji urządzeń w każdej lokalizacji. W oparciu o sieć szkieletową byłyby podłączane pozostałe lokalizacje Urzędu Miasta. W dwóch lokalizacjach znajdują się zasoby serwerowe Urzędu. W tych lokalizacjach będą zastosowane

przełączniki dedykowane do środowisk serwerowych. W celu zapewnienia redundancji zostaną zastosowane duplikacje switchy i technologie rozproszonych agregacji łącz. W projektowanej sieci routing do publicznej sieci Internet odbywał się będzie za pomocą pary dedykowanych routerów do obsługi protokołu BGP. Jeden z tych routerów jest aktualnie w użyciu w sieci Urzędu Miasta.

W niniejszej sekcji została przedstawiona przykładowa koncepcja konfiguracji usług wchodzących w skład części technicznej wdrożenia. W skład tych usług wchodzą konfiguracje następujących elementów:

1. Topologii sieciowej w warstwie L2 - konfiguracja agregacji fizycznych połączeń pomiędzy urządzeniami za pomocą technologii EtherChannel.
2. Instancji sieci VRF - stworzenie listy sieci VRF z numeracją i przypisaniem do nich sieci VLAN wraz z proponowaną adresacją IP.
3. Routingu dynamicznego w sieci szkieletowej - dla dystrybucji tras do adresów wykorzystywanych w sesjach iBGP/LDP/OSPF.
4. Protokołów związanych z przypisaniem ramek/pakietów do poszczególnych instancji VRF (MPLS/MBGP/OSPF).
5. Sieci zarządzania w oparciu o dedykowaną instancję VRF.
6. Przykładowej numeracji adresację sieci LAN w obrębie sieci dla serwerów/maszyn wirtualnych.

Wykonawca uruchomi i skonfiguruje system zarządzania w zakresie opisanych funkcjonalności dla wszystkich urządzeń wymienionych w punkcie 4.11

4.14.Procedura odbiorowa

Po zakończeniu prac wdrożeniowych zostanie przeprowadzona procedura odbioru działającej instalacji. Celem procedury weryfikacyjnej jest sprawdzenie poprawności działania i konfiguracji komponentów wchodzących w skład infrastruktury objętej niniejszym postępowaniem przetargowym. W szczególności zostaną wykonane następujące prace:

Infrastruktura fizyczna Data Center 1, 2 , 3

1. Montaż urządzeń infrastruktury DC:
    1.1. Sprawdzenie poprawności instalacji urządzeń infrastruktury DC pod kątem montażu fizycznego, zgodnie z zaleceniami producenta (chłodzenie, zasilanie, odległość montażowa w szafach).
    1.2. Sprawdzenie poprawności oznakowania urządzeń w szafach montażowych.

1.3.Sprawdzenie poprawności wykonania okablowania i oznakowania w obrębie szaf montażowych.

1.4.Ocena estetyki montażu.

2. Komponenty zasilania infrastruktury DC:

2.1.Sprawdzenie poprawności podłączeń faz zasilania.

2.2.Sprawdzenie poprawności podłączeń zasilaczy redundantnych.

2.3.Sprawdzenie bezprzerwowej pracy urządzeń w przypadku awarii pojedynczej linii zasilającej.

Infrastruktura LAN

3. Zarządzanie urządzeniami ze stacji zarządzającej:

3.1.Sprawdzenie systemu zarządzającego do urządzeń wymaganych przez SIWZ.

4. Dostęp do sieci Internet z urządzeń sieciowych:

4.1.Sprawdzenie działania dostępu do sieci Internet.

4.2.Sprawdzenie działania połączeń redundantnych do sieci Internet.

4.3.Sprawdzenie bezprzerwowej łączności do/z sieci Internet w przypadku awarii łącza podstawowego.

4.4.Sprawdzenie bezprzerwowej łączności do/z sieci Internet w przypadku awarii firewalla/routera podstawowego.

4.5.Weryfikacja tablicy routingu do sieci Internet.

5. Weryfikacja komunikacji w obrębie wdrożonej infrastruktury:

5.1.Sprawdzenie łączności IP pomiędzy urządzeniami Core.

5.2.Sprawdzenie poprawności routingu IP w sieci Core.

5.3.Sprawdzenie poprawności działania redundancji w sieci Core.

5.4.Weryfikacja łączności punkt-punkt pomiędzy urządzeniami Core.

5.5.Weryfikacja tablicy routingu sieci w poszczególnych obszarach sieci.

5.6.Wyłączenie urządzeń redundantnych i weryfikacja dostępności komunikacji.

5.7.Sprawdzenie poprawności działania infrastruktury i wydajności.

6. Weryfikacja zgodności dokumentacji powykonawczej z wdrożoną infrastrukturą.

6.1.Weryfikacja zestawienia urządzeń.

6.2.Weryfikacja schematów połączeń

6.3.Weryfikacja planu adresacji.

6.4.Weryfikacja konfiguracji urządzeń.

Rezultaty ww. czynności zostaną opisane w dokumencie zawierającym podsumowanie prac związanych z odbiorem infrastruktury. Dokument ten musi zostać zatwierdzony przez Zamawiającego.

Do protokołu odbiorowego Wykonawca załączy:

1. Zaakceptowaną przez Zamawiającego dokumentację powykonawczą
2. Oryginały dokumentów poświadczające gwarancję producenta świadczoną na rzecz Zamawiającego na okres gwarancji na przedmiot umowy.
3. Dokumenty potwierdzające przeprowadzenie instruktaży stanowiskowych oraz odbycia szkoleń autoryzowanych (lub dostarczenie voucherów)
4. Dokumenty potwierdzające wykupienie wszelkich obowiązkowych subskrypcji oraz licencji niezbędnych do funkcjonowania dostarczonej infrastruktury teleinformatycznej na okres gwarancji
5. Zamawiający wymaga załączenia do końcowego protokołu odbioru dla każdego dostarczanego urządzenia/materiału Certyfikatu Pochodzenia lub innego dokumentu wystawionego przez producenta lub jego lokalnego przedstawiciela (zawierającego między innymi dane identyfikacyjne produktu pozwalające na jego identyfikację: kod produktu, nr seryjny) potwierdzający, że dany dostarczony produkt jest fabrycznie nowy, jest oznakowany symbolem CE, pochodzi z autoryzowanej sieci sprzedaży – oficjalnego kanału sprzedaży na rynek europejski.