**Załącznik nr 1A do SIWZ**

**Szczegółowy Opis Przedmiotu Zamówienia**

**Dostawa i Wdrożenie Infrastruktury**

**Serwerowej i Sieciowej**

**dotyczy części 1 zamówienia**

Kielce 2020

Spis treści

[Rozdział I. Założenia początkowe oraz wymagania ogólne 3](#_Toc58838505)

[I.1 Wprowadzenie 3](#_Toc58838506)

[I.2 Cel projektu 3](#_Toc58838507)

[I.3 Akty prawne 4](#_Toc58838508)

[I.4 Ogólny opis przedmiotu zamówienia 4](#_Toc58838509)

[I.5 Termin realizacji Przedmiotu Zamówienia 6](#_Toc58838510)

[I.6 Organizacja wdrożenia 7](#_Toc58838511)

[I.6.1 Założenia podstawowe 7](#_Toc58838512)

[I.6.2 Przygotowanie Dokumentacji 8](#_Toc58838513)

[I.6.3 Harmonogram wdrożenia 8](#_Toc58838514)

[I.6.4 Analiza Przedwdrożeniowa 8](#_Toc58838515)

[I.6.5 Dokumentacja Powykonawcza 9](#_Toc58838516)

[I.6.6 Odbiory 11](#_Toc58838517)

[I.6.7 Testy 11](#_Toc58838518)

[I.6.8 Dodatkowe zobowiązania Wykonawcy 11](#_Toc58838519)

[I.6.9 Instruktaże stanowiskowe 12](#_Toc58838520)

[Rozdział II. Szczegółowy opis przedmiotu zamówienia 13](#_Toc58838521)

[II.1 Modernizacja sieci LAN w zakresie dostawy i wdrożenia aktywnych urządzeń sieciowych 13](#_Toc58838522)

[II.1.1 Przełącznik szkieletowy – 2 szt. 15](#_Toc58838523)

[II.1.2 Przełącznik dostępowy typ 1 – 1 szt. 18](#_Toc58838524)

[II.1.3 Przełącznik dostępowy typ 2 – 6 szt. 24](#_Toc58838525)

[II.1.4 Przełącznik dostępowy typ 3 – 4 szt. 30](#_Toc58838526)

[II.1.5 Moduły stackujące – 7 szt. 36](#_Toc58838527)

[II.1.6 Moduły SFP/SFP+/QSFP/kable DAC – 1 komplet 36](#_Toc58838528)

[II.1.7 Firewall – 2 szt. (1klaster) 37](#_Toc58838529)

[Rozdział III. Gwarancja 43](#_Toc58838530)

[III.1.1 Usługi gwarancyjne 44](#_Toc58838531)

# Założenia początkowe oraz wymagania ogólne

## Wprowadzenie

W projekcie „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego (InPlaMed WŚ), w ramach Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego na lata 2014-2020 (RPOWŚ 2007-2014)”, bierze udział Województwo Świętokrzyskie - będące Liderem Projektu, w imieniu którego zadania realizowane są przez Urząd Marszałkowski Województwa Świętokrzyskiego i 8 podmiotów leczniczych jednostek organizacyjnych Województwa oraz 12 podmiotów leczniczych będących jednostkami organizacyjnymi powiatów.

## Cel projektu

Głównym celem Projektu „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego” jest wdrożenie Elektronicznej Dokumentacji Medycznej (EDM) w placówkach medycznych objętych projektem, z zastosowaniem rozwiązań technologicznych i organizacyjnych zapewniających ciągłość działania oraz zgodność z regulacjami i wymogami prawnymi, protokołami przyjętymi w ochronie zdrowia, a także wytycznymi Centrum Systemów Informacyjnych Ochrony Zdrowia, jako instytucji państwowej, której zadaniem jest budowa oraz wspieranie i monitorowanie procesów budowy systemów informacyjnych w ochronie zdrowia. Cel ten przekłada się na usprawnienie zarządzania i podniesienie jakości procesów leczniczych.

Ponadto zakłada się budowę usług elektronicznych w obszarze ochrony zdrowia, świadczonych w ramach poszczególnych placówek medycznych biorących udział w projekcie oraz całego regionu, na rzecz pacjentów oraz personelu medycznego, w jak najszerszym możliwym do realizacji pod względem finansowym, organizacyjnym i prawnym zakresie.

Kluczową usługą budowaną w ramach Projektu będzie gromadzenie i udostępnianie elektronicznej dokumentacji medycznej (EDM) w sposób zapewniający nienaruszalność i bezpieczeństwo przechowywania danych w długim okresie czasu, przy jednoczesnym zapewnieniu łatwego dostępu dla wszystkich uprawnionych użytkowników oraz zachowaniu wysokiej wydajności działania.

Zakłada się osiągnięcie celów Projektu poprzez rozbudowę i rozszerzenie aktualnego stanu informatyzacji poszczególnych placówek medycznych uczestniczących w projekcie z możliwością w przyszłości rozbudowy o kolejne e-usługi i funkcjonalności, w tym także budowę integracyjnej warstwy regionalnej.

Zakres rozbudowy i rozszerzenia aktualnego stanu informatyzacji poszczególnych placówek medycznych został w ramach projektu zaktualizowany indywidualnie dla poszczególnych placówek medycznych uczestniczących w projekcie na podstawie analizy stanu aktualnego. W ramach projektu zakładane jest - w zależności od indywidualnych potrzeb placówek medycznych - zarówno dostarczenie wymaganych w ramach projektu funkcjonalności biznesowych realizowanych poprzez dostawę nowych systemów dziedzinowych (lub dostosowanie i integrację zastanych medycznych systemów dziedzinowych) oraz lokalnych repozytoriów EDM. Przewidywana jest także rozbudowa warstwy infrastrukturalno–systemowej poprzez dostawę komponentów i rozwiązań w obszarze sieciowym, sprzętowym oraz oprogramowania systemowego.

## Akty prawne

Dostarczone rozwiązania teleinformatyczne muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Muszą pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem.

## Ogólny opis przedmiotu zamówienia

**Część 1** – **modernizacja sieci LAN w zakresie dostawy i wdrożenia sieciowej infrastruktury sprzętowej w postaci urządzeń aktywnych.**

1. Przedmiot zamówienia niniejszego postepowania przetargowego dla części 1 obejmuje:
2. **modernizacja sieci LA**N w zakresie dostawy i wdrożenia sieciowej infrastruktury sprzętowej:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Ilość** |
| **Rozdział II.1** | **Modernizacja sieci LAN** |  |
| **AKTYWNE URZĄDZENIA SIECIOWE** |
| II.1.1 | Przełącznik szkieletowy | 2 szt. |
| II.1.2 | Przełącznik dostępowy typ 1 | 1 szt. |
| II.1.3 | Przełącznik dostępowy typ 2 | 6 szt. |
| II.1.4 | Przełącznik dostępowy typ 3 | 4 szt. |
| II.1.5 | Moduły stackujące | 7 szt. |
| II.1.6 | Moduły SFP/SFP+/QSFP/kable DAC | 1 kpl. |
| II.1.7 | Firewall  | 2 szt. (1 klaster) |

1. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
2. Wszystkie dostarczane:

- Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem Przedmiotu Zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy
w poszczególnych Etapach).

- Komponenty (rozumiane jako integralna część dostawy i wdrożenia Przedmiotu Zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.

1. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie
z zapisami SOPZ dla część 2w uzgodnieniu z Zamawiającym zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
2. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, niniejszymi zapisami SOPZ oraz Umowy.
3. Ilekroć w niniejszym SOPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 30 ust. 1-3 Pzp należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 30 ust. 4 ustawy Pzp dopuszcza produkty równoważne opisywanym w treści SIWZ. Jeżeli zapisy zawarte w niniejszym wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 29 ust. 3 ustawy PZP, dopuszcza składanie ofert na „produkty” równoważne. Wszelkie „produkty” pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.
4. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia lub elementu, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
5. Zamawiający wymaga, aby zaoferowane rozwiązanie było rozwiązaniem istniejącym, działającym, gotowym do wdrożenia i zapewniającym realizację wszystkich wymaganych w SIWZ
(w szczególności SOPZ) funkcjonalności na dzień składania ofert i nie może być w fazie opracowywania, budowy, testów, projektowania itp.
6. Wszelkie dostarczane urządzenia:
* Muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta
i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
* Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
* Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
* Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
* Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
* Urządzenia muszą być wyprodukowane po dniu 1 stycznia 2020r.

## Termin realizacji Przedmiotu Zamówienia

Termin realizacji całości Przedmiotu zamówienia dla Części 1 wynosi **90 dni** od dnia podpisania Umowy.

## Organizacja wdrożenia

### Założenia podstawowe

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia.
2. Wykonawca w Harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji i wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
5. W przypadku dostarczania Infrastruktury Sprzętowej UTM i przełączników musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczona w oryginalnych opakowaniach fabrycznych.
6. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
7. Realizacja przedmiotu zamówienia będzie realizowana w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
8. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
9. Obiekty podlegające inwestycji (obiekty służby zdrowia w których świadczone są usługi medyczne) są użytkowane w trybie ciągłym w czasie godzin pracy przez cały okres wykonywania Przedmiotu Zamówienia, co może powodować utrudnienia w miejscu prowadzenia prac. Nie ma możliwości całkowitego wyłączenia i zamknięcia w/w obiektów lub ich części na czas realizacji Przedmiotu Zamówienia. Poszczególne prace będą realizowane etapowo, tak aby zachować ciągłość świadczenia usług medycznych.
10. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających na terenie pracowników i chorych.

### Przygotowanie Dokumentacji

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacja, Dokumentacja PZ), która składa się z nw. zakresów:
2. Harmonogram Wdrożenia
3. Dokumentacja Analizy Przedwdrożeniowej (DAP).
4. Dokumentacja Powykonawcza
5. Dokumentacja będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone
i odbierane poszczególne etapy realizowane w ramach Przedmiotu zamówienia.
6. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia warunkuje rozpoczęcie prac Wykonawcy.
7. Harmonogramem wdrożenia zostanie opracowany w oparciu o wymagania określone w niniejszym SOPZ dla części 1.

### Harmonogram wdrożenia

1. Wykonawca zobowiązany jest opracować na podstawie SIWZ wraz z załącznikami, szczegółowy harmonogram wdrożenia, który zostanie dostarczony do Zamawiającego w terminie do **21 dni kalendarzowych** od podpisania Umowy.

### Analiza Przedwdrożeniowa

1. Analiza przedwdrożeniowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę mający na celu analizę środowiska biznesowego i informatycznego Zamawiającego.
W wyniku przeprowadzenia Analizy przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwana dalej DAP), na podstawie, której będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia. Dokumentacja Analizy Przedwdrożeniowej będzie podlegała uzgodnieniu i akceptacji Zamawiającego.

Dokumentacja Analizy Przedwdrożeniowej (DAP) zostanie dostarczona Zamawiającemu w terminie do **21 dni kalendarzowych** od daty podpisania Umowy.

1. Dokumentacja Analizy Przedwdrożeniowej DAP powinna zawierać w szczególności:

|  |
| --- |
| **Zawarość DAP – wymagania ogolne** |
| * wykaz oraz szczegółowy opis i harmonogram prac
 |
| * architektura rozwiązania
 |
| * przygotowanie planu instalacji Infrastruktury z uwzględnieniem rozmieszczenia sprzętu w lokalizacjach Zamawiającego
 |
| * szczegółową specyfikację oprogramowania – jeżeli dotyczy
 |
| * wykaz oraz szczegółowy opis i harmonogram niezbędnych prac konfiguracyjnych
 |
| * ustawienia konfiguracyjne urządzeń i oprogramowania
 |
| * propozycje scenariuszy testowych uwzględniających zakres czynności operacyjnych, które należy wykonać w celu potwierdzenia, że wskazane wymagane funkcjonalności zostały prawidłowo skonfigurowane i działają zgodnie z opisami procesów
 |
| * harmonogram instruktażu personelu oraz administratorów SSI
 |
| **Zarządcze** |
| * plan i sposób komunikacji Stron
 |
| **Infrastruktura Sieciowa** |
| * podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty
 |
| * analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji wymagań, sposób testowania i odbioru
 |
| * karty katalogowe urządzeń potwierdzające spełnienie wymagań
 |
| * dokumentację i plan dostaw
 |
| * Plan, opis instalacji i wdrożenia oprogramowania wdrażanego wraz z aktywną Infrastrukturą sieciową
 |
| * listę Komponentów, które będę podlegały osobnym odbiorom – jeżeli dotyczy
 |
| * szczegółowe uzgodnienia Stron Umowy dotyczące zakresu i sposobu integracji dostarczanych rozwiązań z istniejącą infrastrukturą u Zamawiającego
 |
| * zakres prac realizowanych przez podwykonawców,
 |
| * szczegółowy zakres i zawartość pozostałej Dokumentacji
 |

### Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta powinna zawierać:

#### Wymogi ogólne:

1. Konfiguracja musi obejmować wszystkie urządzenia wdrożone, zainstalowane w ramach dostawy.
2. Przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje:
* sieć (adresacja IP, itp.),
* listę zainstalowanego oprogramowania, itp.,
1. Opis architektury logicznej:
* schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze.
1. Procedury lub instrukcje instalacji, reinstalacji, deinstalacji oraz aktualizacji.
* szczegółowy opis postępowania w przypadku tworzenia lub zmian w środowisku; jeśli wykorzystywane są procedury innych dostawców (dla standardowych komponentów wystarczy wskazać w dokumentacji szczegółowe odniesienie do procedur standardowych właściwych dla tych komponentów).
1. Procedury standardowe:
* opis stosowania standardowych procedur poprawnej eksploatacji urządzeń,
1. Dokumentacja procesu parametryzacji:
* wyszczególnienie wszystkich parametryzowanych elementów wraz z opisem ich znaczenia i dopuszczalnych wartości oraz stosowanych wartości domyślnych.
1. Dokumenty z testów:
* plan testów, scenariusze testowe i protokoły z testów akceptacyjnych,
1. Instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania – jeżeli dotyczy.

#### 2) Wymagania szczegółowe:

Dokumentacja powykonawcza logicznej struktury sieci po skonfigurowaniu UTM oraz podłączeniu hostów do sieci komputerowej powinna zawierać co najmniej:

|  |
| --- |
| **Dokumentacja Powykonawcza logicznej struktury sieci** |
| * Informacje ogólne
 |
| * Opis sposobu i struktury adresacji logicznej sieci
 |
| * Ogólny schemat logicznej struktury sieci
 |

### Odbiory

1. Odbiór Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji.
2. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej Dodatek nr 4 do SIWZ.

### Testy

1. W ramach realizacji umowy zostaną przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób lub podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbioru końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem końcowym Przedmiotu Zamówienia.

### Dodatkowe zobowiązania Wykonawcy

1. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Wykonanie w całości Przedmiotu Zamówienia w zakresie określonym w Umowie będącej Dodatkiem nr 4 do SIWZ.
3. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres
i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
4. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
5. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
6. Współdziałanie z osobami wskazanymi przez Zamawiającego.

### Instruktaże stanowiskowe

1. Wykonawca zaplanuje w uzgodnieniu z Zamawiającym i przeprowadzi instruktaże stanowiskowe dla wskazanych przez Zamawiającego administratorów w łącznym wymiarze nie mniej niż 120 osobogodzin.
2. Podczas instruktaży musi zostać przekazana niezbędna wiedza w zakresie umożliwiającym samodzielne administrowanie urządzeniami, w tym co najmniej aktualizacji firmware, konfiguracji urządzeń UTM i przełączników w zakresie funkcjonalności wskazanych w SOPZ.
3. Instruktaże stanowiskowe zostaną przeprowadzone w miejscu instalacji Przedmiotu Zamówienia. W przypadku potrzeby Zamawiający zapewni we własnym zakresie pomieszczenie dla przeprowadzenia instruktaży stanowiskowych.

# Szczegółowy opis przedmiotu zamówienia

## Modernizacja sieci LAN w zakresie dostawy i wdrożenia aktywnych urządzeń sieciowych

1. Przedmiotem zamówienia jest modernizacja infrastruktury IT Zamawiającego, w wyniku której powstanie architektura pozwalająca na niezawodną i bezpieczną pracę systemów informatycznych. Oznacza to zagwarantowanie bezpieczeństwa fizycznego i środowiskowego przez odseparowanie pomieszczeń o znaczeniu krytycznym dla przetwarzania i gromadzenia danych, w szczególności elektronicznej dokumentacji medycznej, jak również zapewnienie infrastruktury zapasowej umożliwiającej zabezpieczenie ciągłości działania systemów na wypadek awarii.
2. W ramach realizacji Zamówienia zmodernizowane zostaną poniższe obszary IT, w sposób niezbędny do stworzenia dwóch, wydajnych i odpornych na awarię ośrodków przetwarzania danych (Data Center) DC1 - podstawowym i DC2 - zapasowym:

- przetwarzania i składowania danych (serwery, macierze, wirtualizacja),

- transmisji danych, komunikacji (sieć LAN i Data Center),

- ochrony danych (system kopii zapasowych),

- bezpieczeństwa danych (ochrona kluczowych zasobów).

1. System przetwarzania danych składać się będzie łącznie z 12 serwerów fizycznych (9 będących przedmiotem niniejszego postępowania) oraz 3 obecnie posiadanych przez zamawiającego.
2. Architektura rozwiązania zakłada rozmieszczenie serwerów w dwóch niezależnych geograficznie serwerowniach. 7 serwerów typu Blade, dostarczonych w ramach niniejszego postępowania umieszczonych zostanie w podstawowym ośrodku obliczeniowym DC1. Obecnie posiadane przez Zamawiającego serwery Blade wraz z 2 szt. serwerów typu RACK (dostarczonymi w ramach niniejszego postępowania) zlokalizowane będą w zapasowym ośrodku DC2.
3. Serwery w obu ośrodkach zainstalowane będą miały hypervisora wirtualizacyjnego i podłączone zostaną za pomocą dwóch fabryk sieci SAN do macierzy dyskowych, pomiędzy którymi uruchomiona zostanie asynchroniczna replikacja danych. Dzięki takiej architekturze powstanie odporne na awarie środowisko, umożliwiające automatyczne uruchamianie maszyn wirtualnych w ośrodku zapasowym w wyniku wystąpienia awarii lub konieczności przeprowadzenia prac konserwacyjnych.
4. Dodatkowo zaplanowane jest utworzenie rozproszonego geograficznie klastra dwóch serwerów fizycznych z oprogramowaniem bazodanowym firmy Oracle. Ze względu na rygorystyczne warunki licencyjne producenta oprogramowania bazodanowego serwery te muszą zostać „niezwirtualizowane”.
5. Szkielet sieci (rdzeń/core) zbudowany zostanie w oparciu o dwa wysokowydajne przełączniki rdzeniowe zlokalizowane w GPD (główny punkt dystrybucyjny) znajdujący się w DC1. Przełączniki tworzyć będą klaster za pomocą tzw. wirtualnego stackowania i zachowywać się będą jak jedno urządzenie z punktu widzenia protokołów L2 i L3 bez względu na fizyczne zlokalizowanie urządzeń. Dzięki zastosowaniu w/w urządzeń powstanie wydajna, odporna na awarię i łatwo skalowalna infrastruktura zapewniająca nieprzerwaną pracę wszystkich urządzeń podłączonych do sieci LAN.
6. W warstwie dostępowej celem modernizacji jest zwiększenie ilości portów dla urządzeń końcowych podłączanych do sieci oraz umożliwienie transmisji danych w technologii 10G z LPD (lokalnych punktów dystrybucyjnych) do rdzenia sieci za pomocą istniejących światłowodów jednomodowych.
7. W tym celu przewidziana jest wymiana przełączników nieposiadających interfejsów światłowodowych 10G. Ze względu na ograniczone środki Zamawiającego wymagane jest, aby nowe przełączniki mogły zostać połączone w stos z obecnie posiadanymi.
8. W warstwie bezpieczeństwa obszarów przetwarzania danych DC przewidziana jest instalacja odpornego na awarię klastra zapór sieciowych posiadających przepustowość umożliwiającą zapewnienie bezpiecznej komunikacji pomiędzy różnymi grupami użytkowników/urządzeń w obrębie sieci.
9. Backup realizowany będzie w dwóch lokalizacjach. W jednej z nich znajdować się będzie biblioteka taśmowa wraz z hostem backupowym, a w drugiej umieszczony zostanie host backup wraz z urządzeniem deduplikującym. Backup wykonywany będzie metodą D2D2T (disk to disk to tape) z wykorzystaniem posiadanej przez Zamawiającego biblioteki taśmowej. Taki sposób pozwoli maksymalnie wykorzystać potencjał sieci backupowej i serwerów backup. System musi zostać skonfigurowany tak aby posiadał dostęp do jednego DC a w razie awarii zostanie przełączony do drugiego DC. Rozwiązanie to pozwoli na odtwarzanie maszyn wirtualnych w dowolne miejsce w obrębie jednej konsoli zarządzającej systemem wirtualizacji. Backup obejmować będzie całe środowisko wirtualne i klaster serwerów bazodanowych ORACLE.
10. W ramach budowy sieci LAN, Wykonawca dostarczy aktywne urządzenia sieciowe
o minimalnych parametrach opisanych poniżej.
11. Sprzęt musi pochodzić z autoryzowanego przez jego producenta kanału dystrybucji w UE
i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.
12. Wszystkie urządzenia muszą być fabrycznie nowe wyprodukowane po 1 stycznia 2020r.

### Przełącznik szkieletowy – 2 szt.

Wymagane jest dostarczenie i instalacja 2 szt. przełączników spełniających poniżej opisane minimalne parametry funkcjonalne.

|  |  |
| --- | --- |
| **L.p.** | **Minimalne Wymagania** |
|  | Przełączniki, pracujące jako core sieci muszą tworzyć jeden stack z możliwością rozpięcia w przyszłości pomiędzy dwoma serwerowniami (max. odległość to 500m). Zatem przełącznik musi umożliwiać łączenie w klaster z drugim takim samym urządzeniem poprzez tzw. wirtualne stakowanie. Urządzenia w klastrze zachowują się jak jedno urządzenie w punktu widzenia protokołów L2 i L3. Na chwilę dostawy przełączniki będą zainstalowane w pojedynczym punkcie dystrybucyjnym. |
|  | Przełączniki muszą być dostarczone ze wszystkimi komponentami do instalacji w szafie rack 19''. |
|  | Przełączniki muszą być wyposażone w wymienne moduły wentylatorów. |
|  | Przełączniki muszą zostać wyposażone w zasilacz redundantny do pracy w trybie 1:1. |
|  | Przełączniki muszą być typu standalone, wyposażone w minimum 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz minimum 4 porty 40/100Gb QSFP. |
|  | Porty SFP / SFP+ / SFP28 muszą umożliwiać zastosowanie następujących modułów (wkładek) interfejsowych: |
|  | Dla transmisji 1Gb/s (SFP), |
|  | Dla transmisji 10Gb/s (SFP+), |
|  | Dla transmisji 25Gb/s (SFP28). |
|  | Każdy przełącznik musi zapewnić wydajność: |
|  | musi posiadać minimum 32MB bufor pamięci współdzielonej przez wszystkie porty, |
|  | musi posiadać wydajność przełączania minimum 990 Gbps full duplex, |
|  | musi posiadać wydajność przesyłania minimum 940 Mpps , |
|  | musi obsługiwać minimum:  |
|  | 4000 sieci VLAN, interfejsów SVI, |
|  | 80000 adresów MAC, |
|  | 200000 tras IPv4, |
|  | 150000 tras IPv6, |
|  | Ilość wpisów ACE dla list ACL – minimum 27000 wpisów |
|  | 32000 tras multicast. |
|  | Każdy przełącznik musi zapewnić następujące funkcjonalności: |
|  | Obsługa protokołu NTP, |
|  | Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, |
|  | Obsługa standardu 802.1AE (szyfrowanie ruchu) 128-bit z prędkością linerate dla każdego z interfejsów, |
|  | System operacyjny przełącznika musi umożliwiać wgrywanie poprawek bez konieczności restartowania platformy, |
|  | System operacyjny przełącznika musi mieć możliwość konfiguracji za pomocą protokołu NETCONF i modelowania YANG oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, |
|  | Możliwość uruchamiania skryptów Python bezpośrednio na przełączniku, |
|  | Przełącznik realizuje następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: |
|  | IEEE 802.1w Rapid Spanning Tree, |
|  | Per-VLAN Rapid Spanning Tree (PVRST+) lub technologia równoważna, |
|  | IEEE 802.1s Multi-Instance Spanning Tree, |
|  | Obsługa minimum 500 instancji protokołu STP, |
|  | Obsługa protokołu LLDP i LLDP-MED, |
|  | Przełącznik musi zapewnić funkcjonalność Layer 2 traceroute, |
|  | te umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC, |
|  | Funkcja serwera DHCP, |
|  | Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością: |
|  | dynamicznego przypisania użytkownika do określonej sieci VLAN, |
|  | dynamicznego przypisania listy ACL, |
|  | Przełączik musi realizować następujące mechanizmy związane z zapewnieniem, jakości usług w sieci: |
|  | 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, |
|  | Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), |
|  | Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, |
|  | Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting) na wejściu i wyjściu, |
|  | Kontrola sztormów dla ruchu broadcast/multicast/unicast, |
|  | Obsługa ramek jumbo (9216 bajtów), |
|  | Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP na porcie na wejściu i wyjściu w ścieżce komunikacyjnej, |
|  | Realizacja routingu statycznego i dynamicznego dla IPv4 i IPv6 w zakresie: |
|  | dla IPv4: OSPF, ISIS, BGP, |
|  | dla IPv6: OSPFv3, |
|  | Funkcjonalności Policy-based routing, |
|  | Obsługa protokołu redundancji bramy (VRRP), |
|  | Musi umożliwiać enkapsulację ruchu przy pomocy VXLAN’ów, |
|  | Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia. |
|  | W zakresie zarządzania przełącznik musi: |
|  | posiadać sprzętowo realizowane tworzenie statystyk ruchu w oparciu o NetFlow lub sFlow, wielkość tablicy monitorowanych strumieni wynosi minimum 80 000, |
|  | posiadać dedykowany port Ethernet do zarządzania out-of-band, |
|  | posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych.  |
|  | być wyposażony w port konsoli, |
|  | umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, |
|  | zapewnić obsługę protokołów SNMPv3, SSHv2, SCP, syslog – z wykorzystaniem protokołów IPv4 i IPv6. |

### Przełącznik dostępowy typ 1 – 1 szt.

Wymagane jest dostarczenie i instalacja 1 szt. przełącznika spełniającego poniżej opisane minimalne parametry funkcjonalne.

|  |  |
| --- | --- |
| **L.p** | **Minimalne Wymagania** |
|  | Przełącznik wyposażony 48 portów 10/100/1000BaseT RJ-45 wspierających standard IEEE 802.3at PoE+. |
|  | Budżet mocy przeznaczony na funkcje PoE nie mniejszy niż 720W. |
|  | Przełączniki muszą być dostarczone ze wszystkimi komponentami do instalacji w szafie rack 19''. |
|  | Przełączniki muszą posiadać redundantne wentylatory. |
|  | Każdy przełącznik musi posiadać minimum jeden zasilacz. |
|  | Każdy przełącznik musi umożliwiać zastosowanie dwóch zasilaczy i redundancji zasilania (możliwość instalacji/wymiany „na gorąco” – ang. hot swap). |
|  | Pobór mocy nie więcej jak 1000W. |
|  | Wysokość przełącznika nie więcej jak 1RU. |
|  | Każdy przełącznik musi posiadać porty typu UPLINK z możliwością obsadzenia wkładami (w zależnie od potrzeb): |
|  | 4x1G SFP, |
|  | poty SFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000BaseEX, 1000Base-ZX, 1000Base-BX-D/U. |
|  | Jeżeli którakolwiek z opisanych funkcjonalności wymaga licencji wymaga się jej dostarczenie na okres 3 lat. |
|  | Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: |
|  | Przepustowość w ramach stosu - 80Gb/s, |
|  | 8 urządzeń w stosie, |
|  | Zarządzanie poprzez jeden adres IP, |
|  | Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, |
|  | Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2), |
|  | Stackowanie z zaoferowanymi przełącznikami dostępowymi NET-SW-10G, NET-SW-P10G, NET-SW-P1G. |
|  | Przełącznik musi posiadać minimalne parametry wydajnościowe: |
|  | Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych i większych (przełącznik line-rate): 175Gbps, |
|  | Przepustowość przełącznika (switching capacity): |
|  | 130Mpps, |
|  | Bufor pakietów – 6MB, |
|  | Pamięć DRAM – 2GB, |
|  | Pamięć flash – 4GB, |
|  | Obsługa: |
|  | 1000 sieci VLAN, 500 interfejsów SVI, |
|  | 16000 adresów MAC, |
|  | 4000 tras IPv4, |
|  | 1500 tras IPv6, |
|  | 1000 tras multicast, |
|  | Ilość wpisów ACE dla list ACL –1500 wpisów, |
|  | Musi posiadać sprzętową realizowane tworzenie statystyk ruchu w oparciu o NetFlow lub sFlow, wielkość tablicy monitorowanych strumieni wynosi minimum 16 000.  |
|  | Przełącznik musi zapewnić obsługę protokołu NTP. |
|  | Przełącznik musi zapewnić obsługę IGMPv1/2/3 i MLDv1/2 Snooping. |
|  | Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: |
|  | IEEE 802.1w Rapid Spanning Tree, |
|  | Per-VLAN Rapid Spanning Tree (PVRST+) lub równoważny, |
|  | IEEE 802.1s Multi-Instance Spanning Tree, |
|  | Obsługa minimum 64 instancji protokołu STP, |
|  | Przełącznik musi zapewnić obsługę protokołu LLDP i LLDP-MED. |
|  | Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC. |
|  | Przełącznik musi zapewnić obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego. |
|  | Przełącznik musi zapewnić możliwość uruchomienia funkcji serwera DHCP. |
|  | Przełącznik musi zapewnić mechanizmy związane z bezpieczeństwem sieci: |
|  | Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), |
|  | Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, |
|  | Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, |
|  | Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, |
|  | Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, |
|  | Możliwość uwierzytelniania użytkowników w oparciu o portal WWW dla klientów bez suplikanta 802.1X, |
|  | Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, |
|  | Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, |
|  | Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal WWW), |
|  | Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, |
|  | 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), |
|  | Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, |
|  | Obsługa list kontroli dostępu (ACL) następujących typów: |
|  | Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, |
|  | możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia) |
|  | Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128), |
|  | Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), |
|  | Funkcja Private VLAN. |
|  | Przełącznik musi zapewniać mechanizmy związane z zapewnieniem jakości usług w sieci: |
|  | Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, |
|  | Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), |
|  | Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, |
|  | Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting) w kierunku wejściowych i wyjściowym dla portu Ethernet, |
|  | Kontrola sztormów dla ruchu broadcast/multicast/unicast, |
|  | Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP na wejściu i wyjściu z portu Ethernet. |
|  | Przełącznik musi zapewniać obsługę protokołów i mechanizmów routingu (jeżeli funkcjonalność wymaga specjalnej licencji, Zamawiający nie wymaga takiej licencji) : |
|  | Routing statyczny dla IPv4 i IPv6, |
|  | Routing dynamiczny – RIP, OSPF, ISIS, |
|  | Policy-based routing (PBR), |
|  | Routing multicastów - PIM-SM, PIM-SSM, |
|  | Multicast Source Discovery Protocol (MSDP), |
|  | Obsługa protokołu redundancji bramy (VRRP), |
|  | musi umożliwiać enkapsulację ruchu przy pomocy VXLAN’ów. |
|  | Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN. |
|  | Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.). |
|  | Przełącznik musi zapewnić zarządzanie poprzez: |
|  | Port konsoli, |
|  | Dedykowany port Ethernet do zarządzania out-of-band, |
|  | Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, |
|  | Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 |
|  | Możliwość konfiguracji za pomocą protokołu NETCONF i modelowania YANG oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, |
|  | Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB, |
|  | Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: |
|  | Monitoring pracy przełącznika w zakresie: |
|  | Użycie CPU, |
|  | Użycie pamięci, |
|  | Temperatura pracy, |
|  | Podstawowe informacje systemowe: rodzaj sprzętu, czas pracy, czas systemowy, oprogramowanie, data i czas ostatniej zmiany konfiguracji, |
|  | Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, wykorzystanie PoE, |
|  | Informacji o urządzeniach sąsiednich podłączonych do przełącznika, |
|  | Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, |
|  | Statystyki ruchu (Rx/Tx) na poszczególnych portach L3, |
|  | Konfigurację przełącznika w zakresie: |
|  | * Konfiguracja interfejsów L2:
 |
|  | * Konfiguracja interfejsów L3,
 |
|  | * Tworzenie i konfiguracja sieci VLAN,
 |
|  | * Konfiguracja protokołu STP,
 |
|  | * Tworzenie i konfiguracja wirtualnych instancji routingu (VRF),
 |
|  | * Konfiguracja routingu statycznego,
 |
|  | * Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
 |
|  | * Tworzenie i przypisanie list kontroli dostępu ACL,
 |
|  | * Konfiguracja i uruchomienie NetFlow lub sFlow,
 |
|  | Administracja przełącznika w zakresie: |
|  | * Zdalne uruchamianie komend linii poleceń,
 |
|  | * Czas systemowy w tym protokół NTP,
 |
|  | * Konta administracyjne,
 |
|  | * Upgrade oprogramowania,
 |
|  | * Backup konfiguracji,
 |
|  | * Zdalny restart urządzenia,
 |
|  | * Konfiguracja i dostęp przez SNMP,
 |
|  | * Narzędzie PING i TRACEROUTE,
 |
|  | * Przeglądanie logów systemowych.
 |
|  | Przełącznik musi mieć możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie. |
|  | Przełącznik musi mieć możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku. |

### Przełącznik dostępowy typ 2 – 6 szt.

Wymagane jest dostarczenie i instalacja 6 szt. przełączników spełniających poniżej opisane minimalne parametry funkcjonalne.

|  |  |
| --- | --- |
| **L.p** | **Wymagania Minimalne** |
|  | Przełącznik wyposażony 48 portów 10/100/1000BaseT RJ-45. |
|  | Przełączniki muszą być dostarczone ze wszystkimi komponentami do instalacji w szafie rack 19''. |
|  | Przełączniki muszą posiadać redundantne wentylatory. |
|  | Każdy przełącznik musi posiadać minimum jeden zasilacz. |
|  | Każdy przełącznik musi umożliwiać zastosowanie dwóch zasilaczy i redundancji zasilania (możliwość instalacji/wymiany „na gorąco” – ang. hot swap). |
|  | Pobór mocy nie więcej jak 125W. |
|  | Wysokość przełącznika nie więcej jak 1RU. |
|  | Każdy przełącznik musi posiadać porty typu UPLINK z możliwością obsadzenia wkładami (w zależnie od potrzeb): |
|  | 4x10G SFP+, |
|  | 4x1G SFP, |
|  | 4x 1G i 10G SFP i SFP+, |
|  | poty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: |
|  | Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U, |
|  | Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax. |
|  | Jeżeli którakolwiek z opisanych funkcjonalności wymaga licencji wymaga się jej dostarczenie na okres 3 lat. |
|  | Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: |
|  | Przepustowość w ramach stosu - 80Gb/s, |
|  | 8 urządzeń w stosie, |
|  | Zarządzanie poprzez jeden adres IP, |
|  | Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, |
|  | Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2), |
|  | Stackowanie z zaoferowanymi przełącznikami dostępowymi NET-SW-10G, NET-SW-P10G, NET-SW-P1G. |
|  | Przełącznik musi posiadać minimalne parametry wydajnościowe: |
|  | Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych i większych (przełącznik line-rate): 175Gbps, |
|  | Przepustowość przełącznika (switching capacity):  |
|  | 130Mpps, |
|  | Bufor pakietów – 6MB, |
|  | Pamięć DRAM – 2GB, |
|  | Pamięć flash – 4GB. |
|  | Obsługa: |
|  | 1000 sieci VLAN, 500 interfejsów SVI, |
|  | 16000 adresów MAC, |
|  | 4000 tras IPv4, |
|  | 1500 tras IPv6, |
|  | 1000 tras multicast, |
|  | Ilość wpisów ACE dla list ACL –1500 wpisów, |
|  | musi posiadać sprzętową realizowane tworzenie statystyk ruchu w oparciu o NetFlow lub sFlow, wielkość tablicy monitorowanych strumieni wynosi minimum 16 000. |
|  | Przełącznik musi zapewnić obsługę protokołu NTP. |
|  | Przełącznik musi zapewnić obsługę IGMPv1/2/3 i MLDv1/2 Snooping. |
|  | Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: |
|  | IEEE 802.1w Rapid Spanning Tree, |
|  | Per-VLAN Rapid Spanning Tree (PVRST+) lub równoważny, |
|  | IEEE 802.1s Multi-Instance Spanning Tree, |
|  | Obsługa minimum 64 instancji protokołu STP, |
|  | Przełącznik musi zapewnić obsługę protokołu LLDP i LLDP-MED. |
|  | Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC. |
|  | Przełącznik musi zapewnić obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego. |
|  | Przełącznik musi zapewnić możliwość uruchomienia funkcji serwera DHCP. |
|  | Przełącznik musi zapewnić mechanizmy związane z bezpieczeństwem sieci: |
|  | Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), |
|  | Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, |
|  | Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, |
|  | Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, |
|  | Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, |
|  | Możliwość uwierzytelniania użytkowników w oparciu o portal WWW dla klientów bez suplikanta 802.1X, |
|  | Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, |
|  | Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, |
|  | Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal WWW), |
|  | Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, |
|  | 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), |
|  | Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, |
|  | Obsługa list kontroli dostępu (ACL) następujących typów: |
|  | Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, |
|  | możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia), |
|  | Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128), |
|  | Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), |
|  | Funkcja Private VLAN. |
|  | Przełącznik musi zapewniać mechanizmy związane z zapewnieniem jakości usług w sieci: |
|  | Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, |
|  | Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), |
|  | Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, |
|  | Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting) w kierunku wejściowych i wyjściowym dla portu Ethernet, |
|  | Kontrola sztormów dla ruchu broadcast/multicast/unicast, |
|  | Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP na wejściu i wyjściu z portu Ethernet. |
|  | Przełącznik musi zapewniać obsługę protokołów i mechanizmów routingu (jeżeli funkcjonalność wymaga specjalnej licencji, Zamawiający nie wymaga takiej licencji) : |
|  | Routing statyczny dla IPv4 i IPv6, |
|  | Routing dynamiczny – RIP, OSPF, ISIS, |
|  | Policy-based routing (PBR), |
|  | Routing multicastów - PIM-SM, PIM-SSM, |
|  | Multicast Source Discovery Protocol (MSDP), |
|  | Obsługa protokołu redundancji bramy (VRRP), |
|  | musi umożliwiać enkapsulację ruchu przy pomocy VXLAN’ów. |
|  | Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN. |
|  | Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.). |
|  | Przełącznik musi zapewnić zarządzanie poprzez: |
|  | Port konsoli, |
|  | Dedykowany port Ethernet do zarządzania out-of-band, |
|  | Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, |
|  | Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 |
|  | Możliwość konfiguracji za pomocą protokołu NETCONF i modelowania YANG oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, |
|  | Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB, |
|  | Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: |
|  | Monitoring pracy przełącznika w zakresie: |
|  | * Użycie CPU,
 |
|  | * Użycie pamięci,
 |
|  | * Temperatura pracy,
 |
|  | * Podstawowe informacje systemowe: rodzaj sprzętu, czas pracy, czas systemowy, oprogramowanie, data i czas ostatniej zmiany konfiguracji,
 |
|  | * Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, wykorzystanie PoE,
 |
|  | * Informacji o urządzeniach sąsiednich podłączonych do przełącznika,
 |
|  | * Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN,
 |
|  | * Statystyki ruchu (Rx/Tx) na poszczególnych portach L3,
 |
|  | Konfigurację przełącznika w zakresie: |
|  | * Konfiguracja interfejsów L2:
 |
|  | * Konfiguracja interfejsów L3,
 |
|  | * Tworzenie i konfiguracja sieci VLAN,
 |
|  | * Konfiguracja protokołu STP,
 |
|  | * Tworzenie i konfiguracja wirtualnych instancji routingu (VRF),
 |
|  | * Konfiguracja routingu statycznego,
 |
|  | * Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
 |
|  | * Tworzenie i przypisanie list kontroli dostępu ACL,
 |
|  | * Konfiguracja i uruchomienie NetFlow lub sFlow,
 |
|  | Administracja przełącznika w zakresie: |
|  | * Zdalne uruchamianie komend linii poleceń,
 |
|  | * Czas systemowy w tym protokół NTP,
 |
|  | * Konta administracyjne,
 |
|  | * Upgrade oprogramowania,
 |
|  | * Backup konfiguracji,
 |
|  | * Zdalny restart urządzenia,
 |
|  | * Konfiguracja i dostęp przez SNMP,
 |
|  | * Narzędzie PING i TRACEROUTE,
 |
|  | * Przeglądanie logów systemowych.
 |
|  | Przełącznik musi mieć możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie. |
|  | Przełącznik musi mieć możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku. |

### Przełącznik dostępowy typ 3 – 4 szt.

Wymagane dostarczenie 4 szt. przełączników spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **L.p** | **Wymagania Minimalne** |
|  | Przełącznik wyposażony 48 portów 10/100/1000BaseT RJ-45 wspierających standard IEEE 802.3at PoE+. |
|  | Budżet mocy przeznaczony na funkcje PoE nie mniejszy niż 720W. |
|  | Przełączniki muszą być dostarczone ze wszystkimi komponentami do instalacji w szafie rack 19''. |
|  | Przełączniki muszą posiadać redundantne wentylatory. |
|  | Każdy przełącznik musi posiadać minimum jeden zasilacz. |
|  | Każdy przełącznik musi umożliwiać zastosowanie dwóch zasilaczy i redundancji zasilania (możliwość instalacji/wymiany „na gorąco” – ang. hot swap). |
|  | Pobór mocy nie więcej jak 1000W. |
|  | Wysokość przełącznika nie więcej jak 1RU. |
|  | Każdy przełącznik musi posiadać porty typu UPLINK z możliwością obsadzenia wkładami (w zależnie od potrzeb): |
|  | 4x10G SFP+, |
|  | 4x1G SFP, |
|  | 4x 1G i 10G SFP i SFP+, |
|  | poty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: |
|  | Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U, |
|  | Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax. |
|  | Jeżeli którakolwiek z opisanych funkcjonalności wymaga licencji wymaga się jej dostarczenie na okres 3 lat. |
|  | Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: |
|  | Przepustowość w ramach stosu - 80Gb/s, |
|  | 8 urządzeń w stosie, |
|  | Zarządzanie poprzez jeden adres IP, |
|  | Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, |
|  | Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2), |
|  | Stackowanie z zaoferowanymi przełącznikami dostępowymi typ 1, typ 2 i typ3  |
|  | Przełącznik musi posiadać minimalne parametry wydajnościowe: |
|  | Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych i większych (przełącznik line-rate): 175Gbps, |
|  | Przepustowość przełącznika (switching capacity):  |
|  | 130Mpps, |
|  | Bufor pakietów – 6MB, |
|  | Pamięć DRAM – 2GB, |
|  | Pamięć flash – 4GB, |
|  | Obsługa: |
|  | 1000 sieci VLAN, 500 interfejsów SVI,, |
|  | 16000 adresów MAC, |
|  | 4000 tras IPv4, |
|  | 1500 tras IPv6, |
|  | 1000 tras multicast, |
|  | Ilość wpisów ACE dla list ACL –1500 wpisów, |
|  | musi posiadać sprzętową realizowane tworzenie statystyk ruchu w oparciu o NetFlow lub sFlow, wielkość tablicy monitorowanych strumieni wynosi minimum 16 000. |
|  | Przełącznik musi zapewnić obsługę protokołu NTP. |
|  | Przełącznik musi zapewnić obsługę IGMPv1/2/3 i MLDv1/2 Snooping. |
|  | Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: |
|  | IEEE 802.1w Rapid Spanning Tree, |
|  | Per-VLAN Rapid Spanning Tree (PVRST+), |
|  | IEEE 802.1s Multi-Instance Spanning Tree, |
|  | Obsługa minimum 64 instancji protokołu STP. |
|  | Przełącznik musi zapewnić obsługę protokołu LLDP i LLDP-MED. |
|  | Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC. |
|  | Przełącznik musi zapewnić obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego. |
|  | Przełącznik musi zapewnić możliwość uruchomienia funkcji serwera DHCP. |
|  | Przełącznik musi zapewnić mechanizmy związane z bezpieczeństwem sieci: |
|  | Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), |
|  | Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, |
|  | Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, |
|  | Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, |
|  | Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, |
|  | Możliwość uwierzytelniania użytkowników w oparciu o portal WWW dla klientów bez suplikanta 802.1X, |
|  | Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, |
|  | Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, |
|  | Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal WWW), |
|  | Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, |
|  | 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), |
|  | Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, |
|  | Obsługa list kontroli dostępu (ACL) następujących typów: |
|  | Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, |
|  | możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia), |
|  | Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128), |
|  | Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), |
|  | Funkcja Private VLAN. |
|  | Przełącznik musi zapewniać mechanizmy związane z zapewnieniem jakości usług w sieci: |
|  | Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, |
|  | Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), |
|  | Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, |
|  | Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting) w kierunku wejściowych i wyjściowym dla portu Ethernet |
|  | Kontrola sztormów dla ruchu broadcast/multicast/unicast, |
|  | Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP na wejściu i wyjściu z portu Ethernet. |
|  | Przełącznik musi zapewniać obsługę protokołów i mechanizmów routingu (jeżeli funkcjonalność wymaga specjalnej licencji, Zamawiający nie wymaga takiej licencji): |
|  | Routing statyczny dla IPv4 i IPv6, |
|  | Routing dynamiczny – RIP, OSPF, ISIS, |
|  | Policy-based routing (PBR), |
|  | Routing multicastów - PIM-SM, PIM-SSM, |
|  | Multicast Source Discovery Protocol (MSDP), |
|  | Obsługa protokołu redundancji bramy (VRRP), |
|  | musi umożliwiać enkapsulację ruchu przy pomocy VXLAN’ów. |
|  | Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN. |
|  | Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.). |
|  | Przełącznik musi zapewnić zarządzanie poprzez: |
|  | Port konsoli, |
|  | Dedykowany port Ethernet do zarządzania out-of-band, |
|  | Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, |
|  | Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 |
|  | Możliwość konfiguracji za pomocą protokołu NETCONF i modelowania YANG oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, |
|  | Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB, |
|  | Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: |
|  | Monitoring pracy przełącznika w zakresie: |
|  | * Użycie CPU,
 |
|  | * Użycie pamięci,
 |
|  | * Temperatura pracy,
 |
|  | * Podstawowe informacje systemowe: rodzaj sprzętu, czas pracy, czas systemowy, oprogramowanie, data i czas ostatniej zmiany konfiguracji,
 |
|  | * Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, wykorzystanie PoE,
 |
|  | * Informacji o urządzeniach sąsiednich podłączonych do przełącznika,
 |
|  | * Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN,
 |
|  | * Statystyki ruchu (Rx/Tx) na poszczególnych portach L3,
 |
|  | Konfigurację przełącznika w zakresie: |
|  | * Konfiguracja interfejsów L2:
 |
|  | * Konfiguracja interfejsów L3,
 |
|  | * Tworzenie i konfiguracja sieci VLAN,
 |
|  | * Konfiguracja protokołu STP,
 |
|  | * Tworzenie i konfiguracja wirtualnych instancji routingu (VRF),
 |
|  | * Konfiguracja routingu statycznego,
 |
|  | * Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
 |
|  | * Tworzenie i przypisanie list kontroli dostępu ACL,
 |
|  | * Konfiguracja i uruchomienie NetFlow lub sFlow,
 |
|  | Administracja przełącznika w zakresie: |
|  | Zdalne uruchamianie komend linii poleceń, |
|  | Czas systemowy w tym protokół NTP, |
|  | Konta administracyjne, |
|  | Upgrade oprogramowania,  |
|  | Backup konfiguracji,  |
|  | Zdalny restart urządzenia, |
|  | Konfiguracja i dostęp przez SNMP, |
|  | Narzędzie PING i TRACEROUTE, |
|  | Przeglądanie logów systemowych. |
|  | Przełącznik musi mieć możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie. |
|  | Przełącznik musi mieć możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku. |

### Moduły stackujące – 7 szt.

Wraz z przełącznikami muszą być dostarczone moduły stackujące wraz z kablami o długości minimum 0,5 m umożliwiające łączenie dostarczonych przełączników typu 1, typ 2, typ 3 ze sobą i z posiadanymi przez Zamawiającego przełącznikami serii Cisco 9200L.

### Moduły SFP/SFP+/QSFP/kable DAC – 1 komplet

Wymagane dostarczenie kompletu modułów spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **L.p.** | **Minimalne Wymagania Techniczne** |
|  | Należy dostarczyć następujące, minimalne ilości modułów: |
|  | Moduły kompatybilne z przełącznikami szkieletowymi LAN |
|  | Kabel DAC 10Gb SFP+ 1m – 2 sztuki, |
|  | Moduł SFP+ 10Gb SR – 4 sztuki, |
|  | Moduł SFP+ 10Gb LR – 54 sztuki, |
|  | Moduł SFP 1Gb-LX - 4 sztuki, |
|  | Moduły kompatybilne z przełącznikami dostępowymi typ1, typ 2, typ 3 z cz. 1 zamówienia przetargowego  |
|  | Moduł SFP+ 10Gb LR – 14 sztuk, |
|  | Moduły kompatybilne z przełącznikami dostępowymi Cisco 2960x, Cisco 2960s, Cisco C4510R+E oraz Cisco 9200L posiadanymi przez Zamawiającego  |
|  | Moduł SFP+ 10Gb LR – 33 sztuki, |
|  | Moduły kompatybilne z firewallami PaloAlto PA 850 posiadanymi przez Zamawiającego  |
|  | Moduł SFP 1Gb-LX – 4 sztuki, |
|  | Moduł SFP 1Gb-SX – 4 sztuki. |
|  | Jeżeli Wykonawca uzna, że do realizacji jego koncepcji zawartej konieczne jest dostarczenie większej ilości w/w modułów w takim przypadku muszą one zostać uwzględnione i skalkulowane w jego ofercie.  |

### Firewall – 2 szt. (1klaster)

1. Wymagane jest dostarczenie 2 szt. urządzeń spełniających poniżej opisane minimalne parametry funkcjonalne.
2. Ze względu na charakter działalności jaką prowadzi Zamawiający (świadczenie usług medycznych) Wykonawca zobowiązany jest, w ramach wykonania przedmiotu umowy, do zminimalizowania przerwy w działaniu infrastruktury sieciowej szpitala działającej w oparciu o dostarczane urządzenia. W tym celu ewentualne przerwy związane z wdrożeniem dostarczonego rozwiązania należy ograniczyć do minimum, a czas i termin zostanie ustalony z Zamawiającym.
3. W ramach realizacji zamówienia Wykonawca dostarczy, skonfiguruje, wdroży i uruchomi zaporę ogniową co najmniej w zakresie:
* Wniesienia, ustawienia i fizycznego montażu zapory ogniowej w miejscu wskazanym przez Zamawiającego.
* Podłączenia zapory ogniowej do infrastruktury Zamawiającego z uwzględnieniem specyfiki sieci Zamawiającego.
* Wykonania procedury aktualizacji firmware dostarczonej zapory ogniowej do najnowszej wersji oferowanej przez producenta sprzętu.
* Zaadresowanie zapory ogniowej zgodnie z przydzielonymi przez administratorów Zamawiającego adresami IP.
* Konfiguracja klastra HA wraz z rozszyciem łączy WAN.
* Konfiguracja routing na zaporze zgodnie z zaleceniami administratorów Zamawiającego.
* Konfiguracja podsieci LAN zgodnie z zaleceniami administratorów Zamawiającego. W chwili obecnej Zamawiający ma uruchomione 4 węzły dostępowe.
* Konfiguracja VLAN na dostarczonych urządzeniach zgodnie z zaleceniami administratorów Zamawiającego.
* Należy skonfigurować polityki bezpieczeństwa dostarczone w ramach zakupionych licencji (IPS, antywirus, web filtering), VPN, DMZ, NAT zgodnie z tzw. Best-practices oraz zaleceniami Zamawiającego.
* Należy skonfigurować dostęp do urządzeń SSH oraz HTTPS dla uprawnionych pracowników Zamawiającego.

|  |  |
| --- | --- |
| **L.p** | **Minimalne Wymagania** |
|  | Proponowane rozwiązanie musi być fizycznym urządzeniem zabezpieczeń sieciowych przeznaczonym do montażu w szafie RACK i posiadać co najmniej wszystkie wymienione poniżej cechy: |
|  | Minimalna liczba i rodzaj portów: 10 portów 1000 BaseT, oraz 4 porty 10 Gigabit SFP+ lub 4 porty 1000 BaseT, oraz 16 portów 10 Gigabit SFP+. Firewall musi być wyposażony w 3 moduły SFP+ 10Gb-SR oraz 1 moduł SFP+ 10Gb-LR. |
|  | Minimum 2 dyski SSD o pojemności nie mniejszej niż 480 GB w konfiguracji RAID. |
|  | Minimum 2 redundantne zasilacze AC. |
|  | Pamięć DRAM minimum 32 GB. |
|  | Dedykowany port do zarządzania out-of-band. |
|  | Przepustowość ruchu nie mniej niż 12 Gbps dla kontroli NGFW (Firewall, Application Control, IPS). |
|  | Wydajność przynajmniej 9 Gb/s dla ruchu IPSec VPN (AES-128). |
|  | Przepustowość w ruchu nie mniej niż 60 Gb/s dla kontroli firewall. |
|  | Obsługa minimum 200 000 nowych połączeń na sekundę. |
|  | Obsługa minimum 8 000 000 jednoczesnych połączeń. |
|  | Obsługa minimum 3 000 polityk/reguł firewall. |
|  |  |
|  | Rozwiązanie ma posiadać możliwość podłączenia urządzeń firewall w klastrze pod scentralizowany system zarządzania. |
|  | Musi zapewniać obsługę dla IPv6. |
|  | System zabezpieczeń firewall musi działać 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. |
|  | Musi zapewniać możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta. |
|  | Polityka zabezpieczeń firewall uwzględnia adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji oraz umożliwia rejestrowanie zdarzeń i alarmowanie. |
|  | Musi zostać 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. |
|  | Musi zapewniać możliwość statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6. |
|  | 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 minimum 4000 znaczników VLAN. |
|  | Zapewnione działanie urządzenia w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym (tzn. w warstwie 2 modelu OSI). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych. |
|  | Tryb pracy urządzenia ma być ustalany na poziomie konfiguracji interfejsu sieciowego. System umożliwia pracę we wszystkich dostępnych trybach (router, transparentnego) na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.) |
|  | Zapewniona obsługa protokołów routingu dynamicznego, przynajmniej BGP, RIP i OSPF. |
|  | System zabezpieczeń firewall musi być produktem o uznanej marce na rynku bezpieczeństwa IT.  |
|  | Urządzenie umożliwia zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a Także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. |
|  | Możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników |
|  | Możliwość integracji ze środowiskiem wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) 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. |
|  | Posiada funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
|  | Posiadanie funkcji ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
|  | Umożliwienie realizacji zadań kontroli dostępu (filtracji ruchu sieciowego), poprzez kontrolę ruchu na poziomie warstw sieciowej, transportowej oraz aplikacji |
|  | Możliwość pracy w konfiguracji odpornej na awarie w trybie klastra Active-Passive i Active-Active. |
|  | 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 |
|  | 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 (np. interfejs sieciowy, strefa bezpieczeństwa). |
|  | Możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. |
|  | Posiadanie modułu inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak: http, smtp 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. |
|  | Możliwość uruchomienia modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
|  | 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. |
|  | Możliwość uruchomienia modułu inspekcji anty- malware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł anty-spyware uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
|  | Posiadanie sygnatur DNS wykrywających i blokujących ruch do domen uznanych za złośliwe. |
|  | 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). |
|  | Posiadanie funkcji wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej lub przy użyciu bazy domen. |
|  | Możliwość identyfikacji co najmniej 1000 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS [m.in](http://m.in/).: Skype, Gadu-Gadu, Tor, BitTorrent, eMule. |
|  | 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. |
|  | Możliwość blokowania transmisji plików Możliwość skanowania całości ruchu pod kątem zaistnienia podatności, a nie wyłącznie wybranych próbek ruchu. |
|  | Zapewnienie inspekcji komunikacji szyfrowanej dla protokołu HTTPS (HTTP szyfrowane protokołem TLS/SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie). 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-malware), filtracja plików i URL. |
|  | System musi posiadać możliwość wykrywania ataków 0-day przez emulację plików w środowisku sandbox. Funkcja ta może zostać zrealizowana jako usługa działająca w chmurze producenta oferowanego rozwiązania. |
|  | Funkcja sandbox musi posiadać możliwość analizy przynajmniej następujących typów plików: .7z, .bat, .CAB, .cmd, .dll, .doc, .docx, .exe, .gz, .jar, js, .msi, .pdf,.ppt, .pptx, .pps, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .ps1, .rar, .rtf, .sldm, .swf, .vbs, .wsf, .xlt, .xls, .xlsx, .xltx, .xlsm, .xltm .xlsb, .xlam, .xz, .zip. |
|  | System musi mieć możliwość wykrywania i raportowania o wykrytych zagrożeniach jak również musi istnieć możliwość zablokowania plików uznanych za niebezpieczne. |
|  | Emulacja plików musi być wykonywana w co najmniej następujących wersjach systemu operacyjnego: Microsoft Windows 7, 8, 8.1, 10. |
|  | Wszystkie opracje związane z działaniem modułu sandbox muszą być realizowane w data center zlokalizowanym na terenie Uni Europejskiej. |
|  | 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. |
|  | Urządzenie umożliwia czytanie oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje, w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia. |
|  | Urządzenie nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej. |
|  | Zarządzanie systemu zabezpieczeń odbywa się z linii poleceń (CLI) oraz z graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. |
|  | 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. |
|  | Interfejs administracyjny urządzenia jest w języku polskim lub angielskim. |
|  | Możliwość uwierzytelniania administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+. |
|  | W ramach zamówienia dostarczyć należy opiekę techniczną dla wszystkich dostarczanych komponentów ważnej przez okres 3 lat Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. |
|  | W ramach zamówienia dostarczyć subskrypcję na funkcjonalność sandbox, aktualizację bazy ataków IPS, definicji aplikacji, definicji wirusów oraz bazy kategorii stron WWW na okres 1 roku. |
|  | Wszystkie funkcjonalności muszą być realizowane bezpośrednio na dostarczonym urządzeniu bez konieczności instalacji dodatkowych urządzeń fizycznych lub wirtualnych. |

# Gwarancja

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na niniejszy przedmiot zamówienia:
2. **modernizacja sieci LAN** w zakresie dostawy i wdrożenia sieciowej infrastruktury sprzętowej

|  |  |  |
| --- | --- | --- |
| **Poz. OPZ** | **Opis** | **Okres gwarancji (minimalny)** |
| **AKTYWNE URZĄDZENIA SIECIOWE** |
| II.1.1 | Przełącznik szkieletowy | 36 miesięcy gwarancji producenta obejmująca wszystkie elementy (również zasilacze i wentylatory) |
| II.1.2 | Przełącznik dostępowy typ 1 | 36 miesięcy gwarancji producenta obejmująca wszystkie elementy (również zasilacze i wentylatory) |
| II.1.3 | Przełącznik dostępowy typ 2 | 36 miesięcy gwarancji producenta obejmująca wszystkie elementy (również zasilacze i wentylatory) |
| II.1.4 | Przełącznik dostępowy typ 3 | 36 miesięcy gwarancji producenta obejmująca wszystkie elementy (również zasilacze i wentylatory) |
| II.1.5 | Moduły stackujące | 36 miesięcy gwarancji producenta |
| II.1.6 | Moduły SFP/SFP+/QSFP/kable DAC | 36 miesięcy gwarancji |
| II.1.7 | Firewall | 36 miesięcy gwarancji producenta obejmująca wszystkie elementy (również zasilacze i wentylatory) |

1. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.
2. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzeń oraz wsparcia technicznego.

### Usługi gwarancyjne

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu zamówienia rozumianych jako Awaria lub Usterka zgodnie z definicjami jak poniżej:
2. **Awaria -** Kategoria Wady w Sieciowej Infrastrukturze Sprzętowej i brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której urządzenie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia
3. **Usterka -** Należy przez to rozumieć kategorię Wady w Sieciowej Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
4. Przyjęcie zgłoszenia przez Wykonawcę, odbywać się będzie w okresie dostępności Wykonawcy wskazanym w Tabeli 1, w zależności od tego czego wada dotyczy, poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany „SZ”) przy czym:
5. System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
6. za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności
z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady.
7. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
8. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
9. Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:

**Tabela 1 Usługi gwarancji aktywnych urządzeń sieciowych**

| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE ZASTĘPCZE\*** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY** |
| --- | --- | --- | --- | --- |
| AWARIA | Dnie roboczeponiedziałek – piątek, godz. 07:00-15:00 | niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 3 dni od czasu przyjęcia zgłoszenia |
| USTERKA | nie dotyczy | niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 14 dni od dnia przyjęcia zgłoszenia |

\*nie dotyczy wymiany sprzętu

1. dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,
2. czasy naprawy mogą być inne niż wskazane w powyższych tabelach, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2),
3. w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,

Uwaga:

W przypadku zapisu terminu jako:

* Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
* Godziny Robocze należy rozumieć godziny od 7.00 do 15.00 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.