

**Znak sprawy: EZ/ZP/9/2020/RI Załącznik nr 1 do SIWZ**

**Szczegółowy Opis Przedmiotu Zamówienia**

**Dostawa i wdrożenie klastra urządzeń UTM oraz oprogramowania do analizy ruchu sieciowego**

**dla Wojewódzkiego Szpitala Zespolonego w Kielcach**

Kielce 2020

#

Spis treści

[Rozdział I. 2](#_Toc29239509)

[Rozdział I. Założenia początkowe oraz wymagania ogólne 3](#_Toc29239510)

[I.1 Wprowadzenie 3](#_Toc29239511)

[I.2 Cel projektu 3](#_Toc29239512)

[I.3 Akty prawne 4](#_Toc29239513)

[I.4 Szczegółowy przedmiot zamówienia 4](#_Toc29239514)

[I.5 Termin realizacji Przedmiotu Zamówienia 6](#_Toc29239515)

[I.6 Organizacja wdrożenia 6](#_Toc29239516)

[I.6.1 Założenia podstawowe 6](#_Toc29239517)

[I.6.2 Przygotowanie Dokumentacji 7](#_Toc29239518)

[I.6.3 Harmonogram wdrożenia 7](#_Toc29239519)

[I.6.4 Dokumentacja Powykonawcza 7](#_Toc29239520)

[I.6.5 Odbiór Przedmiotu Zamówienia 8](#_Toc29239521)

[I.6.6 Dostawa i instalacja oprogramowania do analizy ruchu sieciowego 9](#_Toc29239522)

[I.6.7 Instruktaże stanowiskowe 9](#_Toc29239523)

[I.6.8 Testy 9](#_Toc29239524)

[I.6.9 Dodatkowe zobowiązania Wykonawcy 10](#_Toc29239525)

[Rozdział II. Szczegółowy opis przedmiotu zamówienia 11](#_Toc29239526)

[II.1 Modernizacja sieci LAN w zakresie dostawy i wdrożenia klastra urządzeń UTM 11](#_Toc29239527)

[II.1.1 UTM 12](#_Toc29239528)

[II.2 Oprogramowanie do analizy ruchu sieciowego: 15](#_Toc29239529)

[Rozdział III. Gwarancja 17](#_Toc29239530)

[III.1.1 Usługi gwarancyjne 17](#_Toc29239531)

# 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, ze szczególnym uwzględnieniem dostarczanego i wdrażanego oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego.

## Ogólny opis przedmiotu zamówienia

**Dostawa i wdrożenia klastra urządzeń UTM oraz oprogramowania do analizy ruchu sieciowego.**

1. Przedmiot zamówienia niniejszego postępowania przetargowego obejmuje dostawę, instalację, konfigurację i wdrożenie:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Ilość** |
| II.1.1 | UTM | 1kpl (2 szt.) |
| II.2.1 | Oprogramowanie do analizy ruchu sieciowego | 1 |

1. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
2. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie
z zapisami SOPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
3. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, niniejszymi zapisami SOPZ oraz Umowy.
4. 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 Załączniku nr 2 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.
5. 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.
6. 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.
7. 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 wszystkie w całości 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 dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.

## Termin realizacji Przedmiotu Zamówienia

Termin realizacji całości Przedmiotu zamówienia wynosi 50 dni kalendarzowych od 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 klastra urządzeń UTM muszą być one oznakowane w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczony w oryginalnych opakowaniach fabrycznych.
6. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
7. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
8. 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.
9. 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 w oddziałach pracowników i chorych oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiającego.

### 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 Powykonawcza.
4. Dokumentacja będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będzie prowadzona weryfikacja i odbiór prac realizowanych w ramach Przedmiotu zamówienia.
5. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia warunkuje rozpoczęcie prac Wykonawcy.
6. Harmonogram wdrożenia zostanie opracowane w oparciu o wymagania określone w niniejszym SOPZ.

### Harmonogram wdrożenia

Wykonawca zobowiązany jest opracować na podstawie SIWZ wraz z załącznikami, szczegółowy harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 14 dni od podpisania Umowy.

### Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Przedmiotu Zamówienia 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, deinstalacji, reinstalacji 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 możliwości stosowania standardowych procedur poprawnej eksploatacji dla rozwiązań wspierających (sprzętowych lub aplikacyjnych).
1. Dokumentacja procesu parametryzacji:
* wyszczególnienie wszystkich parametryzowanych elementów systemu 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.

#### Wymagania szczegółowe:

Dokumentacja powykonawcza logicznej struktury sieci, po skonfigurowaniu klastra urządzeń 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
 |

### Odbiór Przedmiotu Zamówienia

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

### Dostawa i instalacja oprogramowania do analizy ruchu sieciowego

Oprogramowanie rozumiane jako oprogramowanie dostarczone i zainstalowane na Infrastrukturze serwerowej posiadanej przez Zamawiającego oraz w istniejących systemach informatycznych zgodnie z wymaganiami niniejszego Szczegółowego Opisu Przedmiotu Zamówienia w taki sposób, aby zapewnić prawidłowe funkcjonowanie infrastruktury sprzętowej oraz istniejących systemów informatycznych na wszystkich stanowiskach pracy (stanowiska komputerowe) Zamawiającego.

### Instruktaże stanowiskowe

1. Wykonawca zaplanuje w uzgodnieniu z Zamawiającym i przeprowadzi instruktaże stanowiskowe dla wskazanych przez Zamawiającego administratorów (min. 3 osoby) w łącznym wymiarze nie mniej niż 12 osobogodzin.
2. Podczas instruktaży musi zostać przekazana niezbędna wiedza w zakresie umożliwiającym samodzielne administrowanie urządzeniami oraz oprogramowaniem, w tym co najmniej aktualizacji firmware, konfiguracji urządzeń UTM 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.

### Testy

1. W ramach postepowania 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 zamówienia 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. Zamawiający w końcowej fazie wdrożenia oczekuje realizacji przez Wykonawcę testów bezpieczeństwa. Testy obejmować będą swym zakresem:
	* 1. Testy poprawności konfiguracji i parametryzacji sprzętu sieciowego aktywnego na styku komunikacji z zewnętrzną siecią.
5. 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 Dodatek 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.

# Szczegółowy opis przedmiotu zamówienia

## Modernizacja sieci LAN w zakresie dostawy i wdrożenia klastra urządzeń UTM

1. W ramach budowy sieci LAN Wykonawca dostarczy i wdroży aktywne urządzenia sieciowe
o minimalnych parametrach określonych poniżej.
2. Wykonawca w ramach dostarczenia urządzeń klasy UTM i wdrożenia ich w środowisku informatycznym Zamawiającego zobowiązany jest do skonfigurowania dostarczonych urządzeń wg wymagań Zamawiającego na podstawie udostępnionej konfiguracji z obecnie używanych urządzeń UTM firmy Fortinet, z zachowaniem aktualnej funkcjonalności, pracujących w trybie wysokiej dostępności (klaster HA), w tym w szczególności konfiguracje:
* interfejsów sieciowych, w tym fizycznych z agregacją i VLAN,
* routingów,
* polis (z uwzględnieniem AV), obiektów,
* translacji adresów SNAT, DNAT,
* profili bezpieczeństwa (filtrowanie stron www, kontrola aplikacji, IPS, inspekcja SSL),
* kategorii stron z możliwością własnych modyfikacji,
* tuneli VPN: SSL, IPSEC (w tym z podwójną translacją NAT) zapewniających:

- łączność pomiędzy lokalizacjami Zamawiającego z wykorzystaniem urządzeń UTM FG100D, FG80C, FG60D, FG40C;

- kanały dostępowe dla serwisów i usług zewnętrznych,

* kont użytkowników, grup,
* monitoringu łączy WAN.
1. Ze względu na charakter działalności jaką prowadzi Zamawiający (świadczenie usług medycznych 24/7/365) Wykonawca zobowiązany jest, w ramach wykonania przedmiotu umowy, do zminimalizowania przerwy w działaniu infrastruktury sieciowej szpitala działającej w oparciu o urządzenia UTM. W tym celu ewentualne przerwy związane z wdrożeniem dostarczonego rozwiązania nie przekroczą łącznie 30 minut, a czas i termin zostanie ustalony z Zamawiającym.
2. Dostarczone urządzenia UTM (2 szt. – 1 komplet) muszą zostać skonfigurowane do pracy w trybie wysokiej dostępności (HA).
3. 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.
4. Wszystkie urządzenia muszą być fabrycznie nowe wyprodukowane po 1 stycznia 2019r.

### UTM

Wymagane dostarczenie 2 szt. urządzeń UTM (1 kpl) spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |
| --- |
| **Wymagania minimalne** |
| Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. System bezpieczeństwa musi zostać dostarczony w trybie wysokiej dostępności co najmniej Active/Passive (1 komplet = 2 urządzenia). Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:1. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
2. System musi wspierać IPv4 oraz IPv6
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP
5. System musi posiadać wbudowany port:

- konsoli szeregowej- USB - umożliwiający co najmniej zapis i wczytanie pliku konfiguracyjnego oraz instalację oprogramowania poprzez dysk USB1. System realizujący funkcję Firewall musi dysponować minimum 16 interfejsami miedzianymi Ethernet 10/100/1000.
2. System realizujący funkcję Firewall musi posiadać minimum 2 interfejsy optyczne SFP.
3. Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
4. W zakresie Firewall’a obsługa nie mniej niż 1 500 000 jednoczesnych połączeń oraz 60 000 nowych połączeń na sekundę.
5. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
	* Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
	* Ochrona przed wirusami – antywirus
	* Poufność danych - IPSec VPN oraz SSL VPN
	* Ochrona przed atakami - Intrusion Prevention System
	* Kontrola stron Internetowych :
	* a) moduł kontroli WWW musi być pogrupowanych w 65 kategorii tematycznych.
	* b) w ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam.
	* c) filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
	* d) administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
	* e) moduł kontroli WWW musi korzystać z chmurowej bazy danych zawierającej co najmniej 40 milionów adresów URL.
	* Kontrola zawartości poczty – antyspam (dla protokołów SMTP, POP3)
	* Kontrola pasma oraz ruchu (QoS i Traffic shaping)
	* Kontrola aplikacji
	* Ochrona przed malware co najmniej dla protokołów HTTP, SMTP, POP3, FTP
	* Analiza ruchu szyfrowanego protokołem SSL
6. Wydajność systemu Firewall minimum 20 Gbps
7. Wydajność ochrony przed atakami (IPS) minimum 2 Gbps
8. Wydajność VPN IPSec, nie mniej niż 4 Gbps
9. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
10. Polityki Firewall muszą uwzględniać co najmniej adresy IP, protokoły, usługi sieciowe, reakcje zabezpieczeń, rejestrowanie zdarzeń.
11. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
	* Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
	* Wsparcie dla IKE v1 oraz v2
	* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
	* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
	* Praca w topologii Hub and Spoke oraz Mesh
	* Obsługa ssl vpn w trybach portal oraz tunel
12. Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
13. Translacja (jeden do jeden oraz jeden do wielu) adresów NAT adresu źródłowego i NAT adresu docelowego oraz translację PAT.
14. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
15. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
16. Silnik antywirusowy musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR
17. Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów i być aktualizowana automatycznie.
18. Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
19. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox, OneDrive) powinny być kontrolowane.
20. Kontrola aplikacji szczególnie istotnych z punktu widzenia bezpieczeństwa: proxy, P2P.
21. Kontrola aplikacji musi umożliwiać definiowanie wyjątków oraz własnych sygnatur.
22. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
23. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
	* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
	* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
	* Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
	* Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
24. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów IPFIX/netflow lub sflow.
25. System musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall
26. Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+.
27. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
28. Licencje dla wszystkich wymienionych powyżej funkcji bezpieczeństwa na okres minimum 36 miesięcy.
 |

## Oprogramowanie do analizy ruchu sieciowego:

|  |
| --- |
| **Wymagania minimalne** |
| Wymaga się, aby oprogramowanie było w pełni kompatybilne z dostarczanym urządzeniem UTM o następujących minimalnych parametrach technicznych: * 1. System musi mieć możliwość logowania na podstawie danych wysyłanych za pomocą protokołu co najmniej syslog.
	2. System logowania i raportowania w formie maszyny wirtualnej musi stanowić centralne repozytorium danych gromadzonych przez urządzenia firewall UTM Zamawiającego.
	3. Maszyna wirtualna musi mieć możliwość uruchomienia w następujących środowiskach minimum: VMware i Microsoft Hyper-V.
	4. Obsługa powierzchni dyskowej - minimum 1TB.
	5. Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
	6. Wyświetlanie nowych logów w czasie rzeczywistym. Funkcjonalność ta może być realizowana bezpośrednio na urządzeniu lub w oprogramowaniu do analizy.
	7. Możliwość korzystania z oprogramowania analizy ruchu systemowego podczas aktywnej subskrypcji urządzenia UTM.
	8. System musi umożliwiać analizę logów w ilości min. 3GB/dzień. Licencja, jeżeli jest wymagana na tę funkcjonalność, musi być zawarta w cenie.
	9. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
* Listę najczęściej wykrywanych ataków.
* Listę najbardziej aktywnych użytkowników.
* Listę najczęściej wykorzystywanych aplikacji.
* Listę najczęściej odwiedzanych stron www.
* Listę krajów , do których nawiązywane są połączenia.
	1. System musi zapewniać konfigurację powiadomień poprzez: SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa
	2. Generowanie raportów co najmniej w formatach: HTML, CSV.
	3. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
	4. Funkcję definiowania własnych raportów.

Dostarczone oprogramowanie do analizy ruchu sieciowego musi umożliwiać analizę i raportowanie wszelkiego rodzaju logów wysyłane przez dostarczone urządzenie UTM oraz posiadać wsparcie producenta oprogramowania. |

# Gwarancja

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na niniejszy przedmiot zamówienia:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Okres gwarancji (minimalny)** |
| II.1.1 | UTM | Minimum 36 miesięcy gwarancji producenta,obejmująca również licencjedla wszystkich funkcji bezpieczeństwa. |
| II.2.1 | Oprogramowanie do analizy ruchu sieciowego | Minimum 36 miesięcy |

1. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru bez uwag przez Zamawiającego.

### Usługi gwarancyjne

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami jak poniżej:
2. **Awaria -** Kategoria Wady w sprzęcie/urządzeniu lub oprogramowaniu powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której oprogramowanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Przedmiotu Zamówienia;
3. **Błąd** - Należy przez to rozumieć Wadę oprogramowania oznaczającą jego funkcjonowanie niezgodne z opisem w Dokumentacji oraz SOPZ, uniemożliwiające działanie mniej istotnej funkcjonalności dostarczonego rozwiązania.
4. **Usterka -** Należy przez to rozumieć kategorię Wady w sprzęcie/urządzeniu oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi.
5. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie w okresie dostępności Wykonawcy wskazanym w Tabeli 1 i Tabeli 2, w zależności od tego czego Wada dotyczy, poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany „SZ”) przy czym:
6. System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
7. Za skuteczne przyjęcie zgłoszenia Wady uważać 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.
8. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
9. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
10. Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:

**Tabela 1 Usługi gwarancji klastra urządzeń UTM**

| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE ZASTĘPCZE** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY lub wymiany urządzenia** |
| --- | --- | --- | --- | --- |
| AWARIA | 24/7/365 | niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia. W przypadku dostarczenia urządzenia zastępczego o niegorszych parametrach, czas naprawy nie dłuższy, niż 14 dni |
| USTERKA | nie dotyczy | niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia |

**Tabela 2 usługi gwarancji oprogramowanie do analizy ruchu sieciowego**

| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE ZASTĘPCZE** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY** |
| --- | --- | --- | --- | --- |
| AWARIA | W dni robocze pomiędzy 8.00 a 16.00. Zgłoszenie przesłane po 16.00, traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8.00 | niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 96 godzin od czasu przyjęcia zgłoszenia |
| BŁĄD | nie dotyczy | niezwłocznie nie później niż 2 dni robocze od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 14 dni od dnia przyjęcia zgłoszenia |
| USTERKA | nie dotyczy | niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia |

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,
4. usunięcie Wady oprogramowania, nastąpi poprzez przekazanie poprawki lub nowej wersji. Każda nowa poprawka lub nowa wersja musi posiadać unikalny numer.
5. Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy,
6. wykonywania serwisu oprogramowania na poniższych zasadach:
	* 1. przekazania Zamawiającemu informacji o nowych wersjach oprogramowania drogą elektroniczną na wskazany adres e-mail Zamawiającego,
		2. udostępniania nowych wersji oprogramowania poprzez ustaloną witrynę internetową lub serwer ftp, w szczególności związanych z wejściem w życie nowych przepisów prawa lub zawierających nowe funkcjonalności; w przypadku, w którym udostępnianie następować będzie w związku ze zmianą przepisów prawa, Wykonawca zobowiązany będzie do jej dokonania na nie mniej niż 14 dni przed dniem wejścia w życie tych przepisów. W uzasadnionych przypadkach, Zamawiający dopuści, aby Wykonawca udostępnił odpowiednie zmiany w terminach umożliwiających Zamawiającemu wywiązanie się ze zmienionych przepisów prawa.
		3. każda nowa wersja musi posiadać unikalny numer;
		4. wraz z nową wersją Wykonawca zobowiązany jest do przekazania nowej wersji Dokumentacji Powykonawczej wraz z procedurą instalacji oraz informacją o parametryzacji i konfiguracji.
		5. świadczenia usług w postaci konsultacji, porad, wsparcia technicznego w zakresie wdrożenia oraz użytkowania oprogramowania, przy czym:
* usługi będą świadczone w dni robocze w godzinach od 8 do 16 w języku polskim,
* tryb zgłaszania: telefonicznie, e-mail, faxem lub poprzez System Zgłoszeń,
* konsultacje i porady będą udzielane na bieżąco podczas rozmowy telefonicznej lub w postaci elektronicznej, jeżeli wynika to z przedmiotu usługi, jednak nie później niż w ciągu 3 dni roboczych od skierowania zapytania. Jeżeli nie jest możliwe wykonanie usługi w ciągu 3 dni roboczych, Wykonawca uzgodni z Zamawiającym inny termin konsultacji lub porady.

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 8.00 do 16.00 w każdym dniu roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.