SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

na Dostawę, konfigurację i uruchomienie infrastruktury informatycznej wraz ze szkoleniami

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Urząd Lotnictwa Cywilnego
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Spis treści

Spis tabel

1 Wstęp

Niniejszy dokument opisuje Przedmiot Zamówienia dostarczany przez Wykonawcę w ramach postępowania na *„Dostawę, konfigurację i uruchomienie infrastruktury informatycznej wraz ze szkoleniami”.*

2 Słownik pojęć

Terminy i skróty ogólne	
Awaria	Uszkodzenie urządzenia lub elementu urządzenia, oprogramowania (sprzętowe, programowe lub konfiguracyjne) lub poważne zakłócenie pracy sprzętu lub oprogramowania powstałe z przyczyn niezależnych od Zamawiającego, w tym wynikające z błędów w konfiguracji poszczególnych elementów rozwiązania, którego skutkiem jest brak możliwości korzystania z niego lub z jego części.
Czas reakcji serwisu	Czas liczony od momentu zarejestrowania zgłoszenia o awarii do czasu powiadomienia zgłaszającego o sposobie i terminie realizacji zgłoszenia oraz rozpoczęcia działań diagnostycznych.
Dzień roboczy	Dzień kalendarzowy od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy.
Godzina	Jednostka miary czasu odpowiadająca równym sześćdziesięciu minutom również poza godzinami roboczymi Zamawiającego.
Godzina robocza/ Roboczogodzina	Okres trwający godzinę zegarową w ramach Godzin pracy Zamawiającego.
Godziny pracy Zamawiającego	Od 8.15 do 16.15, od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
ITIL	Kodeks postępowania dla działów informatyki, zawierający zbiór zaleceń jak efektywnie i skutecznie oferować usługi informatyczne.
Oprogramowanie standardowe	Gotowe oprogramowanie publicznie dostępne w sprzedaży, stanowiące dla organizacji alternatywny sposób pozyskania poza samodzielnym ich wytworzeniem. Oprogramowanie Standardowe jest produktem typu COTS (Commercial Off-The-Shelf).
Produkt	Produkt zarządczy lub specjalistyczny rozumiany w myśl metodyki PRINCE2, który ma być dostarczony przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia zgodnie z SIWZ, w szczególności sprzęt, oprogramowanie, dokumentacja powdrożeniowa, a także wszelkie materiały i informacje, w tym nie podlegające ochronie prawa autorskiego, stworzone lub opracowane przez Wykonawcę i dostarczone Zamawiającemu w ramach realizacji Przedmiotu Zamówienia.
SIWZ	Specyfikacja Istotnych Warunków Zamówienia.
SOPZ	Szczegółowy Opis Przedmiotu Zamówienia.

Terminy i skróty ogólne	
Strony	Zamawiający i Wykonawca.
ULC / Urząd / Zamawiający	Urząd Lotnictwa Cywilnego.
Umowa	Umowa, która zostanie podpisana na realizację Zamówienia.
Wykonawca	Podmiot, który zawrze z Zamawiającym umowę sprawie wykonania Zamówienia.
Zadanie	Wydzielona część Przedmiotu Zamówienia do której realizacji zobowiązany jest Wykonawca. Efektem realizacji Zadania może być wytworzenie Produktu specjalistycznego, który podlega odbiorowi.
Zamówienie	Zamówienie publiczne, którego przedmiot w sposób szczegółowy został opisany w SOPZ.

3 Cel i kontekst zamówienia

Celem zamówienia jest dostawa, konfiguracja i uruchomienie infrastruktury informatycznej wraz ze szkoleniami.

Zamówienie jest współfinansowane przez Unię Europejską w ramach Programu Operacyjnego Polska Cyfrowa (działania 2.2 Wysoka dostępność i jakość e-usług publicznych), w ramach Projektu „Doskonalenie i rozbudowa Zintegrowanego Systemu Informatycznego ZSI-ULC" Program Operacyjny Polska Cyfrowa na lata 2014-2020 Oś Priorytetowa nr 2 „E-administracja i otwarty rząd" Działanie nr 2.2 „Cyfryzacja procesów back-office w administracji rządowej" (3 konkurs) i jako taki podlega regulacjom i zasadom konkursu, Programu Operacyjnego Polska Cyfrowa oraz postanowieniom Porozumienia nr POPC.02.02.00-00-0010/17-00 o dofinansowanie Projektu „Doskonalenie i rozbudowa Zintegrowanego Systemu Informatycznego ZSI-ULC" zawartego pomiędzy Centrum Projektów Polska Cyfrowa a ULC.

4 Opis organizacji Zamawiającego

Działalność Urzędu Lotnictwa Cywilnego określona jest przez art. 21 ust. 2 oraz art. 22 ustawy Prawo Lotnicze (Dz.U. 2019 poz. 1580, z późn. zm.). Za poprawne działanie ULC odpowiada Prezes. Prezes ULC jest powoływany przez Prezesa Rady Ministrów i podlega ministrowi właściwemu do spraw transportu.

Urząd Lotnictwa Cywilnego realizuje swoje podstawowe zadania w zakresie:

- wydawania decyzji administracyjnych w sprawach określonych w Prawie Lotniczym;
- nadzorowania i kontrolowania przestrzegania przepisów prawnych w zakresie lotnictwa cywilnego i lotniczej działalności gospodarczej;
- sprawowania nadzoru nad realizacją zadań przez instytucje zapewniające służby żeglugi powietrznej;
- sprawowania nadzoru nad eksploatacją statków powietrznych;
- certyfikacji podmiotów prowadzących działalność w zakresie lotnictwa cywilnego;
- sprawdzania zdatności sprzętu lotniczego do lotów;
- sprawdzania kwalifikacji personelu lotniczego;
- prowadzenia rejestrów: statków powietrznych, lotnisk, lotniczych urządzeń naziemnych, personelu lotniczego, podmiotów szkolących oraz ewidencji lądowisk;
- podejmowania działań w celu zapewnienia bezpieczeństwa lotów, w tym w szczególności:

  - gromadzenie, ocena, przetwarzanie i przechowywanie w komputerowej bazie danych oraz ochrona i rozpowszechnianie informacji o zdarzeniach lotniczych,
  - badanie i ocena stanu bezpieczeństwa lotów w lotnictwie cywilnym,
  - wydawanie zaleceń profilaktycznych,
  - wymiana danych oraz udostępnianie właściwym organom państw członkowskich Unii Europejskiej i Komisji Europejskiej, na podstawie
  - zgłaszanych zdarzeń, z zachowaniem zasady poufności, informacji dotyczących bezpieczeństwa lotów w lotnictwie cywilnym;
- wydawania wytycznych i instrukcji w sprawach technicznych związanych ze stosowaniem przepisów lotniczych w dziedzinie lotnictwa cywilnego;
- sprawowania nadzoru w zakresie lotnictwa cywilnego nad działalnością służb ochrony lotnisk;
- nadzorowania prowadzenia przez zarządzających lotniskami ewidencji oraz analizowanie uzyskanych danych dla potrzeb związanych z działalnością Prezesa Urzędu;
- nadzorowania organizacji badań lotniczo-lekarskich.

5 Miejsce realizacji

Miejscem realizacji przedmiotu zamówienia, jak również miejscem realizacji dostaw jest siedziba Urzędu Lotnictwa Cywilnego w Warszawie, ul. Marcina Flisa 2, 02-247 Warszawa.

6 Przedmiot Zamówienia

Przedmiotem Zamówienia jest realizacja przez Wykonawcę poniższych zadań:

1. Dostawa infrastruktury sprzętowej oraz oprogramowania wraz z udzieleniem licencji opisanych w rozdziale 8 Dostawa infrastruktury i oprogramowania.
2. Instalacja i konfiguracja dostarczonej infrastruktury sprzętowej i oprogramowania zgodnie z zapisami rozdziału 9 Instalacja i konfiguracja dostarczonej infrastruktury sprzętowej oprogramowania.
3. Przeprowadzenie testów akceptacyjnych wraz z Zamawiającym zgodnie z zapisami rozdziału 14.1 Odbiór sprzętu i oprogramowania wraz z instalacją i konfiguracją.
4. Przygotowanie i dostarczenie dokumentacji powdrożeniowej zgodnie z zapisami rozdziału 11 Dokumentacja.
5. Przeprowadzenie szkoleń dla administratorów w zakresie opisanym w rozdziale 12 Szkolenia

Dodatkowo Wykonawca zobowiązany jest do świadczenia usług asysty technicznej w zakresie każdorazowo ustalanym z Zamawiającym w wymiarze co najmniej 150 roboczogodzin (dokładna liczba roboczogodzin usług asysty technicznej określona zostanie w Umowie na podstawie formularza oferty Wykonawcy) do wykorzystania przez 12 miesięcy od daty podpisania Protokołu Odbioru Przedmiotu Zamówienia bez zastrzeżeń. Szczegółowe warunki asysty technicznej zostały opisane w rozdziale 10 Asysta techniczna.

7 Ogólna koncepcja docelowego rozwiązania

W ramach realizacji Przedmiotu Zamówienia zakładane jest stworzenie środowiska zapewaniającego odpowiednie moce obliczeniowe oraz zaplecze teleinformatyczne pozwalające na uruchomienie Systemu ZSI-ULC (będącego przedmiotem realizacji innego zamówienia).

8 Dostawa infrastruktury i oprogramowania

Dostarczone w ramach postępowania poszczególne elementy infrastruktury muszą spełniać poniższe wymagania:

1. Wszystkie dostarczane urządzenia muszą być fabrycznie nowe.
2. Wszystkie dostarczane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2000 lub normą równoważną.
3. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu, jak i producenta.
4. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
5. Dostarczane urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, a gwarancja lub wsparcie techniczne musi pochodzić od producenta i być świadczona przez producenta lub sieć serwisową producenta na terenie Polski.
6. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: kabli zasilających, kabli FC, kabli DAC, Kabli AOC, kabli Ethernet, kabli optycznych Ethernet 10-40 Gbps oraz innych akcesoriów, niezbędnych do przeprowadzenia kompletnej i prawidłowej instalacji i uruchomienia dostarczonej infrastruktury.

7. Wszystkie proponowane elementy dostarczonej infrastruktury muszą znajdować się na liście kompatybilności producentów dostarczanego sprzętu potwierdzającej współdziałanie ich komponentów.

Wykonawca zobowiązany jest dostarczyć następujące elementy infrastruktury opisane w poniższych rozdziałach. W przypadku wystąpienia w niniejszym Szczegółowym Opisie Przedmiotu Zamówienia zastrzeżonych nazw własnych producentów lub produktów, zgodnie z art. 29 ust. 3 ustawy – Prawo Zamówień Publicznych, dopuszcza się dostarczenie produktów w pełni równoważnych do wymaganych przy pełnym zagwarantowaniu przez Wykonawcę zachowania całkowitej projektowanej funkcjonalności.

Tabela 1 Zakres rzeczowy Zamówienia

Lp.	Rodzaj urządzenia	ilość
1.	Przełącznik rdzeniowy	2
2.	Przełącznik 48 portowy – dostępowy (8 szt. z POE. 10 szt. bez POE)	18
3.	Przełącznik 48 portowy (DataCenter)	4
4.	System WiFi (1 klaster HA (2 instancje), 30 punktów dostępowych)	1
5.	Zapora sieciowa NGFW	2
6.	Zapora sieciowa – oddziałowa	10
7.	Pamięć masowa – blokowa o pojemności 20TB	2
8.	Pamięć masowa – obiektowa na 30TB danych użytkownych	1
9.	Serwery wraz z oprogramowaniem	4
10.	Zasilacze UPS	4
11.	System backupu	1
12.	Usługi wdrożenia	1
13.	Usługi serwisowe	1

8.1 Przełączniki rdzeniowe

Każdy z dostarczanych przełączników rdzeniowych musi spełniać poniższe wymagania:

Tabela 2. Minimalne wymagania dla przełączników rdzeniowych

ID	Wymaganie
1	Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
2	Przełącznik musi posiadać nie mniej niż 48 portów SFP+ oraz 4 porty mogące pracować jako QSFP+.

	Wraz z przełącznikiem wykonawca dostarczy minimum: • 2 wkładki QSFP+ (40 Gb multimode) lub kabel AOC (min. 5m) lub DAC (min. 5m) • 10 wkładek SFP+ (10 Gb multimode) • 12 wkładek RJ45 (1Gb)
3	Przełącznik musi posiadać tryb pracy w którym co najmniej 24 porty mogą być obsadzone wkładkami miedzianymi 1Gbps (SFP 1000BASE-T).
4	Urządzenie musi umożliwiać konwersję portów QSFP+ na porty 4x10Gbps.
5	Urządzenie musi obsługiwać moduły SFP Gigabit Ethernet nie mniej 1000Base-T, SX, LX.
6	Urządzenie musi obsługiwać moduły QSFP28 typu SR4, LR4 oraz przewody optyczne typu Active Optical Cable.
7	Urządzenie musi obsługiwać moduły QSFP+ typu SR4, ESR4, LR4 oraz przewody miedziane typu Direct Attach Cable.
8	Urządzenie musi pozwalać na wykorzystanie modułów światłowodowych oraz okablowania innych producentów.
9	Przełącznik musi posiadać dwa wymienne w trakcie pracy zasilacze AC. Urządzenie musi poprawnie pracować przy awarii jednego z dwóch zasilaczy. Urządzenie musi posiadać wymienne w trakcie pracy moduły wentylacji. Przepływ powietrza przez przełącznik musi być od przodu (wlot) do tyłu (wylot).
10	Urządzenie musi posiadać możliwość zestawienia w stos składający się co najmniej z dziewięciu urządzeń. Łączenie w stos musi być realizowane połączeniami 40Gbps
11	Przełącznik musi być wyposażony w port konsoli oraz dedykowane interfejsy Ethernet RJ45 oraz SFP do zarządzania OOB (out-of-band).
12	Urządzenie musi być wyposażone w co najmniej 4GB RAM oraz dysk SSD o pojemności nie mniej niż 1GB.
13	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh.
14	Zagregowana wydajność przełączania w warstwie 2 nie może być niższa niż 1.4 Tb/s. Urządzenie musi obsługiwać nie mniej niż 1000 Mp/s.
15	Przełącznik musi umożliwiać obsługę nie mniej niż 200 000 adresów MAC.
16	Urządzenie musi obsługiwać tryby przełączania ramek store-and-forward oraz cut-through.
17	Przełącznik musi obsługiwać ramki Jumbo (9k bajtów).
18	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4000.
19	Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 100 grup LAG, po nie mniej niż 16 portów. Przełącznik musi obsługiwać funkcję Multi-chassis LAG.

20	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, a także Multiple Spanning Tree.
21	Przełącznik musi obsługiwać protokół LLDP.
22	Urządzenie musi obsługiwać routing między sieciami VLAN – routing statyczny oraz protokoły routingu dynamicznego: RIP, OSPF, IS-IS, BGP.
23	Przełącznik musi posiadać możliwość obsługi co najmniej 16000 wpisów w tablicy routingu dla IPv4.
24	Urządzenie musi obsługiwać protokoły routingu multicast, nie mniej niż IGMP (v1, v2, v3), PIM-SM oraz MSDP.
25	Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD.
26	Przełącznik musi obsługiwać protokół VRRP.
27	Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: priorytetu w warstwie 2 (802.1p) i wartości pola ToS/DSCP w nagłówkach IP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek.
28	Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci lub interfejsu VLAN dla kryteriów z warstw 2-4. Filtrowanie ruchu musi być realizowane sprzętowo. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
29	Przełącznik musi obsługiwać limitowanie adresów MAC.
30	Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu.
31	W celu integracji z sieciami storage urządzenie musi obsługiwać funkcje: Data Center Bridging Capability Exchange (DCBX), FCoE oraz Priority-based Flow Control (PFC).
32	Przełącznik powinien posiadać funkcje VXLAN, VXLAN L2 i L3 Gataway oraz OVSDB.
33	Urządzenie musi obsługiwać protokół OpenFlow 1.3.
34	Obsługa narzędzi automatyzacji dla co najmniej Chef, Puppet, Python.
35	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną.
36	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
37	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
38	Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z

	autoryzowanego kanału sprzedaży.
39	Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej ważnej przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

Dostarczane przełączniki muszą być w pełni kompatybilne z oprogramowaniem Junos Space v.19.2R1 (znajdować się na liście wsparcia producenta oprogramowania do zarządzania przełącznikami sieciowymi) oraz oprogramowaniem do monitorowania infrastruktury Manage Engine opManager v.12.4.011. Wykonawca dostarczy w takim przypadku dodatkowe licencje wymagane przez producenta oprogramowania JUNOS SPACE.

Jeżeli dostarczane przełączniki nie są kompatybilne z ww. oprogramowaniem do zarządzania, Wykonawca zobowiązany jest do dostarczenia oprogramowania do zarządzania dostarczanymi przełącznikami, umożliwiającego w trybie graficznym (GUI) konfigurację dostarczonych przełączników wraz z wymaganymi licencjami.

8.2 Przełącznik 48 portowy – dostępowy

W ramach postępowania przewidziana jest dostawa 8 sztuk przełączników 48 portowych – dostępowych z opcją zasilania PoE oraz 10 sztuk przełączników 48 portowych – dostępowych bez opcji zasilania PoE.

Tabela 3 Minimalne wymagania dla Przełączników Dostępowych z obsługą PoE oraz bez obsługi PoE

ID	Wymaganie
1	Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
2	Przełącznik musi posiadać 48 portów dostępowych Ethernet 10/100/1000 Auto-MDI/MDIX.
3	Dla Przełączników z obsługą PoE. Przy jednym zasilaczu budżet mocy na potrzeby PoE musi wynosić nie mniej niż 740W. Przy zainstalowanych dwóch zasilaczach budżet mocy na potrzeby PoE musi wynosić nie mniej niż 1440W. Wszystkie przełącznik muszą być wyposażone w dwa zasilacze. Dla przełącznika z obsługą PoE, każdy w portów musi obsługiwać PoE+ (do 30W per interfejs).
4	Przełącznik musi posiadać nie mniej niż 4 porty uplink 10 Gigabit Ethernet SFP+. Korzystanie z portów uplink nie może powodować wyłączenia portów dostępowych 10/100/1000. Porty uplink muszą akceptować również wkładki SFP umożliwiając obsługę połączeń uplink Gigabit Ethernet. Wraz z przełącznikiem wykonawca dostarczy minimum jedną wkładkę SFP+ (10 Gb multimode)
5	Możliwość rozbudowy o co najmniej 2 porty o prędkości co najmniej 10Gb/s.
6	Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 9 urządzeń. Dopuszczalne jest podłączanie do stosu portami uplink 10 Gb/s. Stos musi być widoczny z punktu widzenia zarządzania oraz innych urządzeń sieciowych jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi

	być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup'u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master.
7	Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
8	Przełącznik musi być wyposażony w nie mniej niż 512 MB pamięci Flash oraz 2 GB pamięci DRAM.
9	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
10	Przełącznik musi posiadać architekturę non-blocking. Maksymalna wydajność przełączania w warstwie 2 nie może być niższa niż 216 Gb/s i 190 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 32 000 adresów MAC.
11	Przełącznik musi obsługiwać ramki Jumbo (9k bajtów).
12	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4093. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN, przełącznik musi obsługiwać protokół MVRP.
13	Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grup LAG, maksymalnie nie mniej niż 8 linków w grupie.
14	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D i 802.1w, a także Multiple Spanning Tree zgodnie z IEEE 802.1s (nie mniej niż 64 instancje MSTP).
15	Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
16	Urządzenie musi obsługiwać routing między sieciami VLAN – routing statyczny oraz protokół routingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 4 000.
17	Urządzenie musi posiadać możliwość uruchomienia Ethernet OAM link fault management (LFM) lub Connectivity Fault Detection (CFD). Jeżeli ww. funkcjonalność jest dodatkowo licencjonowana należy wraz z urządzeniem dołączyć taką licencję.
18	Urządzenie musi pozwalać na zarządzanie po IPv6.
19	Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: priorytetu w warstwie 2 (802.1p) i wartości pola ToS/DSCP w nagłówkach IP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
20	Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci lub interfejsu VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
21	Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.

22	Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu).
23	Urządzenie musi obsługiwać protokół SNMP (wersje 2 i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu.
24	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną.
25	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
26	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
27	Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
28	Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej ważnej przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

Dostarczane przełączniki muszą być w pełni kompatybilne z oprogramowaniem Junos Space v.19.2R1 (znajdować się na liście wsparcia producenta oprogramowania do zarządzania przełącznikami sieciowymi) oraz oprogramowaniem do monitorowania infrastruktury Manage Engine opManager v.12.4.011. Wykonawca dostarczy w takim przypadku dodatkowe licencje wymagane przez producenta oprogramowania JUNOS SPACE.

Jeżeli dostarczane przełączniki nie są kompatybilne z ww. oprogramowaniem do zarządzania, Wykonawca zobowiązany jest do dostarczenia oprogramowania do zarządzania dostarczanymi przełącznikami, umożliwiającego w trybie graficznym (GUI) konfigurację dostarczonych przełączników wraz z wymaganymi licencjami.

8.3 Przełącznik 48 portowy (DataCenter)

Tabela 4 Minimalne wymagania przełącznika DataCenter

ID	Wymaganie
1	Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
2	Przełącznik musi posiadać nie mniej niż 48 portów SFP+ oraz 4 porty mogące pracować jako QSFP+ Wraz z przełącznikiem wykonawca dostarczy minimum:

	• 1 wkładki QSFP+ (40 Gb multimode) lub kabel AOC (min. 5m) lub DAC (min. 5m) • 10 wkładek SFP+ (10 Gb multimode) • 12 wkładek SFP (1Gb multimode) • 24 wkładki RJ45 (1Gb)
3	Przełącznik musi posiadać tryb pracy w którym co najmniej 24 porty mogą być obsadzone wkładkami miedzianymi 1Gbps (SFP 1000BASE-T).
4	Urządzenie musi umożliwiać konwersję portów QSFP+ na porty 4x10Gbps.
5	Urządzenie musi obsługiwać moduły SFP Gigabit Ethernet nie mniej 1000Base-T, SX, LX.
6	Urządzenie musi obsługiwać moduły QSFP28 typu SR4, LR4 oraz przewody optyczne typu Active Optical Cable.
7	Urządzenie musi obsługiwać moduły QSFP+ typu SR4, ESR4, LR4 oraz przewody miedziane typu Direct Attach Cable.
8	Urządzenie musi pozwalać na wykorzystanie modułów światłowodowych oraz okablowania innych producentów.
9	Przełącznik musi posiadać dwa wymienne w trakcie pracy zasilacze AC. Urządzenie musi poprawnie pracować przy awarii jednego z dwóch zasilaczy. Urządzenie musi posiadać wymienne w trakcie pracy moduły wentylacji. Przepływ powietrza przez przełącznik musi być od przodu (wlot) do tyłu (wylot).
10	Urządzenie musi posiadać możliwość zestawienia w stos składający się co najmniej z dziewięciu urządzeń. Łączenie w stos musi być realizowane połączeniami 40Gbps lub 100Gbps.
11	Przełącznik musi być wyposażony w port konsoli oraz dedykowane interfejsy Ethernet RJ45 oraz SFP do zarządzania OOB (out-of-band).
12	Urządzenie musi być wyposażone w co najmniej 4GB RAM oraz dysk SSD o pojemności nie mniej niż 1GB.
13	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh.
14	Zagregowana wydajność przełączania w warstwie 2 nie może być niższa niż 1.4 Tb/s. Urządzenie musi obsługiwać nie mniej niż 1000 Mp/s.
15	Przełącznik musi umożliwiać obsługę nie mniej niż 200 000 adresów MAC.
16	Urządzenie musi obsługiwać tryby przełączania ramek store-and-forward oraz cut-through.
17	Przełącznik musi obsługiwać ramki Jumbo (9k bajtów).
18	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4000.
19	Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 100 grup LAG, po nie mniej niż 16 portów. Przełącznik musi obsługiwać funkcję Multi-chassis LAG.

20	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, a także Multiple Spanning Tree.
21	Przełącznik musi obsługiwać protokół LLDP.
22	Urządzenie musi obsługiwać routing między sieciami VLAN – routing statyczny oraz protokoły routingu dynamicznego: RIP, OSPF, IS-IS, BGP.
23	Przełącznik musi posiadać możliwość obsługi co najmniej 16000 wpisów w tablicy routingu dla IPv4.
24	Urządzenie musi obsługiwać protokoły routingu multicast, nie mniej niż IGMP (v1, v2, v3), PIM-SM oraz MSDP.
25	Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD.
26	Przełącznik musi obsługiwać protokół VRRP.
27	Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: priorytetu w warstwie 2 (802.1p) i wartości pola ToS/DSCP w nagłówkach IP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek.
28	Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci lub interfejsu VLAN dla kryteriów z warstw 2-4. Filtrowanie ruchu musi być realizowane sprzętowo. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
29	Przełącznik musi obsługiwać limitowanie adresów MAC.
30	Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu.
31	W celu integracji z sieciami storage urządzenie musi obsługiwać funkcje: Data Center Bridging Capability Exchange (DCBX), FCoE oraz Priority-based Flow Control (PFC).
32	Przełącznik powinien posiadać funkcje VXLAN, VXLAN L2 i L3 Gataway oraz OVSDB.
33	Urządzenie musi obsługiwać protokół OpenFlow 1.3.
34	Obsługa narzędzi automatyzacji dla co najmniej Chef, Puppet, Python.
35	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną.
36	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
37	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
38	Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z

	autoryzowanego kanału sprzedaży.
39	Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej ważnej przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

Dostarczane przełączniki muszą być w pełni kompatybilne z oprogramowaniem Junos Space v.19.2R1 (znajdować się na liście wsparcia producenta oprogramowania do zarządzania przełącznikami sieciowymi) oraz oprogramowaniem do monitorowania infrastruktury Manage Engine opManager v.12.4.011. Wykonawca dostarczy w takim przypadku dodatkowe licencje wymagane przez producenta oprogramowania JUNOS SPACE.

Jeżeli dostarczane przełączniki nie są kompatybilne z ww. oprogramowaniem do zarządzania, Wykonawca zobowiązany jest do dostarczenia oprogramowania do zarządzania dostarczanymi przełącznikami, umożliwiającego w trybie graficznym (GUI) konfigurację dostarczonych przełączników wraz z wymaganymi licencjami.

8.4 System WiFi

Niniejszy rozdział zawiera wymagania dla systemu WiFi tj. systemu złożonego z kontrolera pracującego w trybie HA (min. 2 instancje) oraz 30 punktów dostępowych wraz z wymaganymi do zarządzania licencjami.

8.4.1 Kontrolery WiFi

Tabela 5 Minimalne wymagania na kontrolery systemu WiFi

ID	Wymaganie
1	Rozwiązanie musi zostać dostarczone w formie wirtualnej umożliwiającej instalacje na środowisku zgodnym z VMWare oraz Hyper-V.
2	Dostarczone rozwiązanie musi zarządzać siecią bezprzewodową złożoną z 30 punktów dostępowych z możliwością rozbudowy do 1000 punktów dostępowych poprzez dodanie tylko licencji i zmianę parametrów maszyny wirtualnej.
3	Zamawiający wymaga, aby ruch pomiędzy kontrolerem a punktem dostępowym był tunelowany.
4	Rozwiązanie zostanie uruchomione na dwóch niezależnych maszynach wirtualnych, które będą pracować w klastrze niezawodnościowym. Kontrolery muszą w pełni obsługiwać dostarczane punkty dostępowe.
5	Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall).
6	Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym.

ID	Wymaganie
7	Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania.
8	Kontroler musi zapewniać centralne zarządzanie licencjami, tzn. w architekturze sieci, w której występuje więcej niż jeden kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom. Zamawiający dopuszcza, aby tę funkcję pełnił tak zwany arbiter opisany w dalszej części specyfikacji.
9	Kontroler musi posiadać następujące parametry sieciowe: a) możliwość wdrożenia w warstwie 2 i 3 ISO/OSI; b) wsparcie dla sieci VLAN w tym również trunk 802.1q; c) wbudowany serwer DHCP; d) obsługa SNMPv2, SNMPv3; e) routing dynamiczny OSPF.
10	Kontroler sieci WLAN musi obsługiwać co najmniej: a) Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS b) Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze. c) Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit. d) Autoryzację dostępu użytkowników: i. Typy uwierzytelnienia: IEEE 802.1X (EAP,LEAP,PEAP,EAP-TLS,EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal", 802.1X i MAC. ii. Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia. iii. Wsparcie dla autoryzacji, minimum: Microsoft NAP, CISCO NAC, Pulse Secure NAC, Aruba NAC. iv. Musi umożliwiać utworzenie nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal". v. Musi umożliwiać wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES). vi. Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym. vii. Uwierzytelnienie oraz autoryzacja muszą być możliwa przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+. e) Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających. f) Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu. g) Kontroler musi zapewniać obsługę XML API do uwierzytelnienia.
11	Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci: a) Integracja jednoczesnej transmisji danych i głosu. b) Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming). c) Ograniczanie pasma dla użytkownika oraz dla roli użytkownika. d) Ograniczenie pasma dla poszczególnych aplikacji. e) Ograniczenie pasma dla poszczególnych SSID.

ID	Wymaganie
12	Kontroler musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal).
13	Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni).
14	Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym: a) Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe. b) Stałe monitorowanie pasma oraz usług. c) Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi. d) Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma. e) Przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie. f) Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b). g) Wykrywanie interferencji oraz miejsc bez pokrycia sygnału. h) Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w.
15	Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej co najmniej następujące własności: a) Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia. b) Kopiowanie (mirroring) sesji. c) Szczegółowe logi (per pakiet) do późniejszej analizy. d) ALG (Application Layer Gateway). e) Translacja źródłowa, docelowa adresów IP. f) Identyfikacja i blokowanie ataków DoS. g) Obsługa protokołu GRE. h) Deep packet inspection (DPI). i) Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci wifi.
16	Kontroler musi posiadać funkcję systemu WIDS/ WIPS. Moduł WIPS musi posiadać co najmniej następujące funkcje: a) Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów. b) Identyfikacja i możliwość blokowania sieci Adhoc c) Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging d) Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler e) Identyfikacja błędów konfiguracji klientów WLAN f) Identyfikacja podszywania się pod autoryzowane punkty dostępowe Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w zamawianych dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników.

ID	Wymaganie
17	Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https) i linia komend przez SSH.
18	Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA.

8.4.2 System zarządzania

Zamawiający wymaga, aby dostarczone w ramach postępowania kontrolery realizowały poniższe funkcjonalności. Zamawiający dopuszcza, aby poniższe funkcjonalności były realizowane przez dedykowany system służący do zarządzania i monitorowania pracy wszystkimi urządzeniami tworzącymi sieci WLAN (punkty dostępowe, kontrolery WLAN).

Tabela 6 Minimalne wymagania dla systemu zarządzania

ID	Wymaganie
1	System Zarządzania i Monitoringu tego samego producenta co oferowane urządzania sieci WLAN (punkty dostępowe, kontrolery).
2	System zarządzania dostarczany w formie wirtualnej umożliwiającej instalacje na środowisku zgodnym z VMWare oraz Hyper-V.
3	Obsługa poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW.
4	Zarządzanie wszystkimi punktami dostępowymi, które są przedmiotem tego samego postępowania.
5	System musi posiadać odpowiednią ilość licencji do obsługi punktów dostępowych, kontrolerów działających w trybie HA - minimum 35 licencji. Jeśli wymienione funkcjonalności są realizowane przez dedykowany system zarządzania i monitoringu to należy doliczyć licencje do obsługi kontrolerów dostarczanych w ramach postępowania.
6	Wsparcie dla środowisk heterogenicznych, rozumiane jako możliwość zarządzania z wykorzystaniem SNMP urządzeniami sieciowymi różnych producentów.
7	Automatyczne wykrywanie urządzeń.
8	Bieżące monitorowanie stanu wszystkich podłączonych urządzeń.
9	Funkcja wprowadzania masowych zmian konfiguracji na wielu urządzeniach.
10	Funkcja zbierania i wyświetlania informacji dotyczących pracujących w sieci urządzeń klienckich oraz możliwość ich wyszukania przy użyciu różnych parametrów takich jak: a) system operacyjny b) typ urządzenia c) urządzenia sieci WLAN oraz danego SSID

ID	Wymaganie
11	Funkcja archiwizacji konfiguracji urządzeń.
12	Konfiguracja zadań dla podłączonych urządzeń, w szczególności: a) automatyczna zmiana wersji oprogramowania urządzeń, b) ponowne uruchomienie urządzenia, c) definiowanie przedziałów czasowych, w których dane SSID ma być rozgłaszane.
13	Narzędzie ułatwiające planowanie radiowe dla sieci posiadające możliwość wizualizacji pokrycia radiowego.
14	Funkcja tworzenia map pokrycia (tzw. Heat Map).
15	Panel zarządzający GUI umożliwiający wyświetlanie przynajmniej: a) Wykresu liczby połączonych urządzeń klienckich; b) Wykresu potencjalnej przepustowości urządzeń klienckich; c) Wykresu stosunku sygnał do szumu (SNR) urządzeń klienckich.
16	Funkcja automatycznego wykrycia urządzeń obcych i ich lokalizacji.
17	Funkcja generowania ostrzeżeń i logów dotyczących wykrytych ataków w sieci bezprzewodowej.
18	Funkcja generowania wiadomości email dla administratorów sieci (alerty, ostrzeżenia).
19	Funkcja definiowania poziomu dostępu dla administratorów z przypisanymi: a) Rolami; b) Segmentami sieci, do których uzyskuje się dostęp.
20	Obsługa XMP API

8.4.3 Arbiter dla kontrolerów

W ramach rozwiązania wymagane jest dostarczenie tzw. arbitra dla kontrolerów. Arbiter dostarczany w formie wirtualnej umożliwiającej instalację na środowisku zgodnym z Hyper-V oraz VMware.

Tabela 7 Minimalne wymagania dla tzw. arbitra dla kontrolerów

ID	Wymaganie
1	W ramach rozwiązania wymagane jest dostarczenie tzw. arbitra dla kontrolerów. Arbiter dostarczany w formie wirtualnej umożliwiającej instalację na środowisku zgodnym z Hyper-V oraz VMware. Arbiter musi spełniać poniższe funkcje: a. Zaawansowane możliwości strojenia środowiska radiowego (szumy, duża gęstość):

ID	Wymaganie
	i. Równomierna dystrybucja kanałów w całym systemie ii. Dynamiczna zmiana szerokości kanałów iii. Dostosowanie mocy nadawanego sygnału karty radiowej punktu dostępowego iv. Zbieranie statystyk z 24h i optymalizacja parametrów na podstawie obserwacji zdarzeń historycznych v. Możliwość aktualizacji modułów funkcyjnych bez konieczności aktualizacji całego oprogramowania b. Możliwość budowania hierarchii urządzeń tworzących rozwiązanie bezprzewodowe z centralnym miejscem zarzadzania konfiguracją i licencjami. c. Możliwość wykonywania aktualizacji oprogramowania systemowego w obrębie systemu w trybie bezprzerwowym. d. Możliwość budowania klastrów kontrolerów dla podniesienia niezawodności i dostępności systemu (utrzymanie informacji o sesjach, utrzymania IP na stacji klienta, brak powtórnego uwierzytelnienia). e. Rozwiązanie musi zostać dostarczone w formie redundantnej. f. Arbiter musi zapewnić wsparcie dla: i. Minimum 50 urządzeń ii. Minimum 500 klientów iii. Minimum 5 kontrolerów g. Arbiter musi umożliwiać rozbudowę poprzez dodanie licencji oraz zmianę parametrów maszyny wirtualnej zgodnie z zaleceniem producenta.
2	Minimum 3-letnia gwarancja producenta obejmująca wszystkie elementy. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub podmiot przez niego autoryzowany. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
3	Wszystkie urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Polski. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.
4	Wszystkie elementy rozwiązania muszą pochodzić od jednego producenta.

8.4.4 Punkt dostępowy wraz z oprogramowaniem

Tabela 8 Minimalne wymagania dla punktów dostępowych wraz z oprogramowaniem układowym

ID	Wymaganie
1	Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków.
2	Punkt dostępowy musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz (standard 802.11a/n/ac wave 2) oraz 2.4GHz (standard 802.11b/g/n).
3	Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej oferowanym w ramach niniejszego postępowania.
4	Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i

ID	Wymaganie
	protokół https. b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki. c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI oraz CLI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.
5	Musi być zapewniona funkcja wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego. b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny. c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe. d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję. e. Wirtualny kontroler musi posiadać adres IP, za pomocą którego można zarządzać klastrem. Adres ten, w przypadku awarii musi podążać za nowym wirtualnym kontrolerem i pozostawać bez zmian. f. W ramach jednej grupy (klastra) musi być możliwe używanie Punktów Dostępowych różnego typu, np. w standardzie 802.11n i 802.11ac, które są zarządzane za pomocą tego samego wirtualnego kontrolera. g. Zamawiający wymaga, aby w ramach jednego klastra istniała możliwość pracy minimum 120 urządzeń.
6	Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP.
7	Punkt dostępowy musi mieć możliwość pracy jako analizator widma.
8	W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa.
9	W system musi być wbudowany serwer DHCP.
10	W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów.
11	Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach: a. EAP-TLS b. PEAP-MSCHAPv2 c. PEAP-GTC d. TTLS-MSCHAPv2
12	Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP.
13	Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID.
14	Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.
15	Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez: a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania. b. Zewnętrzny portal WWW.

ID	Wymaganie
16	Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT.
17	Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne.
18	Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż: a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe. b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu. c. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma. d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału. e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz. f. Wsparcie dla 802.11d oraz 802.11h. g. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane.
19	Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrzbudynkowej.
20	Obsługa roamingu klientów w warstwie 2.
21	Obsługa monitoringu przez SNMP.
22	Obsługa logowania na zewnętrznym serwerze SYSLOG.
23	W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
24	W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
25	Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie: a. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością. b. Wykorzystanie pasma. c. Ilość klientów korzystających z systemu/interferujących. d. Ilość ramek wejściowych/wyjściowych dla każdego radia. e. Ilość odrzuconych /błędnych ramek/ dla każdego radia. f. Szum tła dla każdego radia. g. Wyświetlanie logów systemowych.
26	Punkt dostępowy musi posiadać 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.9 dBi dla pasma 5 GHz.
27	Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2.

ID	Wymaganie
28	Specyfikacja radia 802.11a/n/ac wave 2: a. Obsługiwane częstotliwości: - 5.150 ~ 5.250 GHz (low band) - 5.250 ~ 5.350 GHz (mid band) - 5.470 ~ 5.725 GHz (Europa) - 5.725 ~ 5.850 GHz (high band) b. Obsługa technologii OFDM. c. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM d. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm. e. Prędkości transmisji: i. 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a ii. MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11n iii. MCS0-MCS9, NSS = 1-2 (6.5 Mbps do 867 Mbps) dla 802.11ac f. Obsługa HT – kanały 20/40MHz dla 802.11n. g. Obsługa VHT – kanały 20/40/80MHz dla 802.11ac. h. Wsparcie dla technologii DFS (Dynamic frequency selection). i. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac. j. Wsparcie dla: i. MRC (Maximal ratio combining) ii. CDD/CSD (Cyclic delay/shift diversity) iii. STBC (Space-time block coding) iv. LDPC (Low-density parity check) v. Technologia TxBF
29	Specyfikacja radia 802.11b/g/n: a. Częstotliwość 2,400 ~2,4835. b. Technologia direct sequence spread spectrum (DSSS) i OFDM. c. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256-QAM. d. Moc transmisji konfigurowalna przez administratora. e. Prędkości transmisji: i. 1,2,5.5,11 Mbps dla 802.11b ii. 6,9,12,18,24,36,48,54 Mbps dla 802.11g iii. MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11n.
30	Punkt dostępowy musi posiadać co najmniej: a. 1 interfejs 100/1000Base-T: i. z funkcją auto-sensing link oraz MDI/MDX ii. z funkcją PoE b. 1 interfejs konsoli c. zasilanie zgodne z 802.3af d. przycisk przywracający konfigurację fabryczną e. slot zabezpieczający Keningston
31	Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac oraz Passpoint.
32	Parametry pracy urządzenia: a. Temperatura otoczenia (zakres minimalny): 0-40 º C b. Wilgotność (zakres minimalny): 5% - 93%

ID	Wymaganie
33	Zamawiający wymaga, aby oferowany punkt dostępowy posiadał licencje niezbędne do zapewnienia wszystkich funkcjonalności kontrolera opisanego w pozycji „Kontroler sieci bezprzewodowej“.
34	Punkty dostępowe muszą być objęte minimum 36-miesięczną gwarancją producenta. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 45 dni przesyła zamiennik. Gwarancja może wymagać zakupu/posiadania ważnego kontraktu wsparcia technicznego.
35	Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni.
36	Wszystkie urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Polski. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.
37	Wszystkie urządzenia muszą być fabrycznie nowe.

8.5 Zapora sieciowa NGFW

Tabela 9 Minimalne wymagania dla zapory sieciowej NGFW

ID	Wymaganie
1	System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2	System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 6 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 3 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń.
3	System zabezpieczeń firewall musi być wyposażony w co najmniej 8 portów Gigabit Ethernet RJ45, 8 portów 1G/10G SFP/SFP+ lub 8 portów 1G SFP i 2 porty 10G SFP+ Wraz z urządzeniem wykonawca dostarczy minimum jedną wkładkę SFP+ (10 Gb multimode)
4	Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.
5	Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach

ID	Wymaganie
	inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
6	System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.
7	System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jedna tablica routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
8	System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
9	Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
10	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.
11	System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
12	Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 6 Gbit/s.
13	Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole, gdzie definiowane są aplikacje i oddzielne pole, gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile)..
14	Blokownie aplikacji (P2P, IM, itp.) może odbywać się poprzez inne mechanizmy ochrony niż firewall.
15	Kontrola aplikacji może wykorzystać moduł IPS, sygnatury IPS oraz dekodery protokołu IPS.
16	System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
17	System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
18	System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja lub jako parametr polityki dla których dowiązuje się profile ochronne AV, DNS, IPS.

ID	Wymaganie
19	System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif lub blokowane plików w wiadomościach email: 7z, arj, cab, lzh, rar, tar, zip, bzip, gzip, bzip2, xz, bat, msc, uue, mime, base64, binhex, elf, exe, hta, html, jad, class, cod, javascript, msoffice, msofficex, fsg, upx, petite, aspack, prc, sis, hlp, activemime, jpeg, gif, tiff, png, bmp, ignored, unknown, mpeg, mov, mp3, wma, wav, pdf, avi, rm, torrent oraz dodatkowo umożliwia wykorzystanie tworzenia sygnatur IPS do plików nie będących na wymaganej liście.. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
20	System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach lub w danej polityce firewalla.
21	System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików lub będzie dostępna przy próbie otwarcia stron blokowanych przez profil ochronny wykorzystujący kategoryzację producenta I interakcję z Sandbox.
22	System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
23	System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
24	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
25	System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
26	System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
27	System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana 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.
28	System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia lub z RADIUS. Funkcja

ID	Wymaganie
	musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
29	System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku, gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.
30	Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
31	System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
32	System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
33	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
34	System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
35	System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
36	System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania 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.
37	System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
38	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
39	System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
40	System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

ID	Wymaganie
41	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu lub gdzie sygnatury będą pobierane ze wskazanego zewnętrznego repozytorium lub z Sandbox, do którego wcześniej zostaną ręcznie wysłane próbki do skanowania.
42	System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
43	System zabezpieczeń firewall musi posiadać funkcję 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).
44	System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
45	System zabezpieczeń firewall musi posiadać funkcję przeglądania logowanych informacji oraz na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów w celu zapewnienia ochrony.
46	System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
47	System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus, czyli nie mniej niż 3 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
48	Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
49	Administrator musi mieć możliwość konfiguracji rodzaju pliku poddanego analizie typu „Sand-Box".
50	System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia, które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
51	System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację 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.
52	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
53	System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
54	System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się

ID	Wymaganie
	na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
55	System zabezpieczeń firewall musi umożliwiać inspekcję tuneli GRE dla ruchu przesyłanego w tych tunelach.
56	System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.
57	System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.
58	System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
59	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
60	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
61	System zabezpieczeń firewall musi pozwalać na integrację w środowisku 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.
62	Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
63	System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu lub systemie centralnego zarządzania na maszynie wirtualnej bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
64	System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian na urządzeniu lub systemie centralnego zarządzania na maszynie wirtualnej, których są autorami.
65	System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji na urządzeniu lub

ID	Wymaganie
	systemie centralnego zarządzania na maszynie wirtualnej.
66	System zabezpieczeń firewall musi być wyposażony w interfejs XML API lub REST API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
67	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.
68	System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+.
69	System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS) lub serwer zdalny + fallback na lokalne hasło.
70	System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB lub może być realizowane w centralnym systemie przechowywana logów na maszynie wirtualnej. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie. Jeżeli centralny system logowania wymaga licencji musi ona być dostarczona w postepowaniu.
71	System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
72	System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do serwerów Syslog per polityka bezpieczeństwa lub urządzenie.
73	System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
74	System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia lub systemie centralnego zarządzania na maszynie wirtualnej.
75	System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
76	System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
77	System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
78	System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
79	Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej oraz niezbędnych licencji przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą

ID	Wymaganie
	elektroniczną przez producenta oraz polskiego dystrybutora sprzętu lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

8.6 Zapora sieciowa – oddziałowa

Tabela 10 Minimalne wymagania dla zapory sieciowej oddziałowej

ID	Wymaganie
1	Urządzenie musi być wyposażone w co najmniej 2 GB pamięci RAM, pamięć Flash 4 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym.
2	System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł rutingu IP, odpowiedzialny za ustalenie tras rutingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. System operacyjny firewalla musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji.
3	Urządzenie musi być wyposażone w nie mniej niż 5 interfejsów 1GbE RJ45.
4	Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 10 strefami bezpieczeństwa z wydajnością nie mniejszą niż 500 Mb/s liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż 200 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 64 000 równoległych sesji oraz zestawić nie mniej niż 5 000 nowych połączeń/sekundę.
5	Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 256 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 100 Mb/s IMIX.
6	Urządzenie musi obsługiwać tunele IP-IP oraz GRE.
7	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 1000 reguł polityki bezpieczeństwa obsługując przynajmniej 16 stref bezpieczeństwa.
8	Firewall musi umożliwiać rozbudowę o funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention). System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu

ID	Wymaganie
	exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków musi być aktualizowana przez producenta codziennie. Zamawiający nie wymaga dostarczenia licencji IPS w ramach niniejszego postępowania.
9	Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP. Urządzenie musi być w stanie obsłużyć 200 000 wpisów w tablicy routingu oraz forwardingu (data plane).
10	Urządzenie musi obsługiwać co najmniej 32 instancje routingu (wirtualnych routerów).
11	Urządzenie musi obsługiwać co najmniej 1000 sieci VLAN z tagowaniem 802.1Q.
12	Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.
13	Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
14	Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta.
15	Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.
16	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
17	Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
18	Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej oraz niezbędnych licencji przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

8.7 Pamięć masowa – blokowa o pojemności 20TB

Tabela 11 Minimalne wymagania dla pamięci masowej - blokowej.

ID	Wymaganie
1	Macierz musi mieć możliwość zainstalowania w standardowej szafie rack 19" niebędącej przedmiotem zamówienia. Rozmiar jednostki sterującej macierzą nie może przekraczać 4U. Dodawanie kolejnych półek lub dysków musi odbywać się bezprzerwowo.
2	Wymagane dwa moduły sterujące macierzą pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny moduł musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez macierz.
3	Oferowana macierz musi posiadać w chwili dostawy minimum 8 portów pozwalających na podłączenie do infrastruktury 10Gb iSCSI z wykorzystaniem kabli DAC lub z wykorzystaniem wkładek SFP+. Z macierzą dyskową powinno być dostarczone minimum 8 wkładek SFP+ SR lub kabli DAC jeżeli przełącznik pochodzi od tego samego producenta co macierz. Te same porty musza umożliwiać podłączenie do infrastruktury FC 16Gbs. Macierz powinna także umożliwiać bezpośrednie (bez wykorzystania przełączników) podłączenie do 4 hostów w sposób redundantny (każdy host podłączony do dwóch kontrolerów macierzy) z wykorzystaniem protokołu FC.
4	Każdy z modułów sterujących musi być wyposażony w min 8 GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania.
5	Macierz musi obsługiwać dyski twarde typu SSD oraz być przystosowana. Macierz musi być wyposażona w minimum 24 dyski 1.6TB SAS SSD hot-plug o wartości DWPD1 / Read Intensive Macierz musi umożliwiać obsługę minimum 180 dysków.
6	Macierz musi obsługiwać typy protekcji RAID 0,1,5,6,10 oraz powinna posiadać funkcjonalność zarzadzania informacjami o parzystości oraz dyskami spare w całej puli dysków. (w przypadku awarii dysku, do jego obudowy musi być używany każdy dysk z puli).
7	Macierz musi umożliwiać zwiększanie online pojemności poszczególnych wolumenów logicznych oraz dynamiczne alokowanie przestrzeni dyskowej (tzw. „thin provisioning”).
8	Macierz musi posiadać funkcjonalność sprawdzania integralności zapisywanych danych.
9	Wymagana możliwość wykonania minimum 512 kopii migawkowych. Wymagana możliwość definiowania maksymalnej ilości kopii migawkowych. Ponadto macierz powinna posiadać funkcjonalność tworzenia kopii migawkowych ze wskazanych przestrzeni dyskowych.
10	Macierz musi mieć możliwość replikacji asynchronicznej z wykorzystaniem iSCSI lub FC.
11	Wymagana możliwość definiowania globalnych dysków hot-spare. Wymagana możliwość logicznej zamiany dysków z wykorzystaniem dysków nieprzypisanych.
12	Macierz musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp oraz możliwość wysyłania powiadomień awarii do wskazanych odbiorców. Wysyłane powiadomienia musza zawierać nazwę macierzy, informacje o typie zdarzenia, datę i czas wystąpienia zdarzenia oraz krótki opis zdarzenia.
13	Macierz musi mieć możliwość definiowania poziomu zajętości miejsca, po osiągnieciu którego nastąpi wysłanie powiadomienia pod wskazane adresy email.

ID	Wymaganie
14	System zarzadzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy.
15	Macierz musi mieć funkcjonalność automatycznej detekcji podłączonych hostów. Musi być możliwość edycji hostów dodanych w sposób automatyczny.
16	Wymagana jest możliwość logicznego grupowania dysków macierzy (dodawanie dysków do istniejącej grupy oraz tworzenie nowej grupy z dodanych dysków).
17	Macierz musi umożliwiać szyfrowanie zapisywanych na niej danych. Nie wymaga się tej funkcjonalności w chwili dostawy.
18	Macierz musi posiadać możliwość fizycznej identyfikacji (dioda LED) aktywowanej z interfejsu zarzadzania oraz funkcjonalność fizycznego identyfikowania dysków (dioda LED) należących do jednej przestrzeni logicznej.
19	Macierz musi mieć możliwość przypisania wolumenu danych tylko do wybranego hosta należącego do zdefiniowanego klastra.
20	Wymaga się możliwości rozbudowania macierzy do poziomu wydajności przynajmniej 208 000 operacji wejścia wyjścia dla losowego odczytu oraz przynajmniej 94 000 operacji wejścia wyjścia dla losowego zapisu. Wymagana pojemność dla wolumenów z dynamiczną alokacja przestrzeni to przynajmniej 128 TB
21	Dostępne dwa porty zarządzające 1Gbe Base-T w trybie primary/redundant.
22	Zarzadzanie macierzą powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokole https, oraz za pomocą linii komend cli osiągalnej poprzez protokole ssh.
23	Interfejs zarzadzania powinien wylogować sesje po kilku/kilkunastu minutach bezczynności.
24	Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control.
25	Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: - storage admin – pełen dostęp z wyłączeniem ustawień bezpieczeństwa, - monitor – możliwość odczytu konfiguracji.
26	Wymagana jest bezprzerwowa wymiana następujących elementów macierzy: kontrolery, moduły I/O, dyski, zasilacze oraz moduły SFP+.
27	Obsługa systemów operacyjnych hosta: Microsoft Windows Server 2012 R2; 2016, 2019; Red Hat Enterprise Linux (RHEL) 6, 7; SUSE Linux Enterprise Server (SLES) 12, 15; VMware vSphere 6.0, 6.5, 6.7
28	Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej ważnej przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. W przypadku awarii dyski pozostają u Zamawiającego.

8.8 Pamięć masowa – obiektowa na 30TB danych (min 100TB RAW)

Tabela 12 Minimalne wymagania dla pamięci masowej - obiektowej

ID	Wymaganie

ID	Wymaganie
1	Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja obiektowego systemu składowania danych. Rozwiązanie musi zostać dostarczone jako gotowe do pracy urządzenie (ang. appliance) - warstwa sprzętowa oraz programowa (poza urządzeniami sieciowymi) musi pochodzić od jednego producenta (musi być kompletnym produktem opatrzonym numerem seryjnym). Dopuszcza się rozwiązania, w których elementy balansujące ruch sieciowy kierowany do urządzenia instalowane są na zewnętrznej platformie wirtualnej (np. VMware, Hyper-V lub KVM).
2	Rozwiązanie powinno umożliwiać przechowywanie 30 TB danych (pojemność użytkowa), przy czym każdy obiekt powinien być zapisywany w minimum trzech kopiach lub może być zapisany w sposób zapewniający odporność na awarię dwóch dowolnych dysków jednocześnie. Podana pojemność nie uwzględnia wykorzystania mechanizmów redukcji danych (przed procesem kompresji).
3	Rozwiązanie powinno składować dane na napędach dyskowych. Nie dopuszcza się rozwiązań zbudowanych w oparciu o napędy taśmowe. *Minimalna pojemność pojedynczego napędu dyskowego to 4TB.*
4	Rozwiązanie powinno zostać dostarczone w konfiguracji pozwalającej na pracę w dwóch fizycznych lokalizacjach połączonych siecią Ethernet 10Gbps. W raz z urządzeniem Wykonawca dostarczy minimum 2 wkładki SFP+ (10Gb multimode)
5	W przypadku pracy w dwóch lokalizacjach rozwiązanie musi zapewniać możliwość udostępnienia całej dostępnej przestrzeni w postaci jednego ciągłego obszaru przeznaczonego na dane (ang. name space).
6	Rozwiązanie musi być odporne na utratę dowolnego węzła składującego dane i wchodzącego w skład systemu. Awaria taka nie może skutkować utratą danych ani niedostępnością systemu.
7	Dostarczane rozwiązanie musi być produktem rozpoznawalnym na rynku, co oznacza, że powinno być wymieniane w raportach niezależnych organizacji, takich jak Gartner, IDC lub ESG (Enterprise Strategy Group).
8	Dostarczone rozwiązanie musi umożliwiać rozbudowę do co najmniej *100 węzłów.*
9	Dostarczone rozwiązanie musi umożliwiać rozbudowę pojemności do co najmniej *1PB* przestrzeni bez konieczności zatrzymywania pracy rozwiązania i bez przerywania dostępu do danych. *Minimalny krok rozbudowy to dodanie jednego węzła. Rozbudowa może następować przy użyciu węzła o pojemności innej niż pojemność węzłów już pracujących.*
10	Dostarczone rozwiązanie powinno posiadać wbudowane mechanizmy przechowywania zarówno danych jak i metadanych (informacji opisujących dane).
11	Metadane powinny być przechowywane na dedykowanych do tego celu dyskach SSD.
12	Rozwiązanie musi pozwalać na integrację z tradycyjnymi rozwiązaniami przez możliwość symultanicznego dostępu (odczyt i zapis) przez interfejsy plikowe (NFS,CIFS) oraz S3 dla wszystkich przechowywanych obiektów
13	Jeżeli wykorzystanie wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć wraz z rozwiązaniem.
14	Rozwiązanie musi posiadać wbudowane mechanizmy redukcji danych, w tym co najmniej kompresję

ID	Wymaganie
	danych.
15	Rozwiązanie musi posiadać udokumentowaną możliwość współpracy z zewnętrznym silnikiem wyszukiwania ElasticSearch.
16	Rozwiązanie musi posiadać wbudowany mechanizm wersjonowania obiektów.
17	Musi być zapewniona możliwość tworzenia logicznie odseparowanych przestrzeni danych (ang. Multi-Tenancy) w obrębie rozwiązania.
18	*Rozwiązanie powinno umożliwiać migrację danych do chmury publicznej (AWS, Microsoft Azure, Google Cloud Platform) oraz do innych urządzeń obsługujących protokół S3. Licencje zapewniające taką funkcjonalność nie są przedmiotem zapytania.*
19	*Rozwiązanie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność typu WORM).* *Licencje zapewniające taką funkcjonalność nie są przedmiotem zapytania.*
20	Oferowane urządzenia muszą być fabrycznie nowe i wyprodukowane nie wcześniej niż pół roku przed terminem dostawy do Zamawiającego.
21	Oferowane urządzenia i wszystkie jego elementy muszą pochodzić od autoryzowanego Dostawcy producenta.
22	Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej ważnej przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. W przypadku awarii dyski pozostają u Zamawiającego.

8.9 Serwery wraz z oprogramowaniem

8.9.1 Serwery

Tabela 13 Minimalne wymagania dla serwerów

ID	Nazwa elementu, parametru lub cechy	Wymaganie
1	Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
2	Procesor	Architektura x86, maksymalny TDP dla procesora – 125W. Minimalna ilość rdzeni dla procesora – 16, taktowanie procesora nie niższe niż 2.3GHz. Wynik wydajności procesora instalowanego w oferowanym serwerze nie powinien być niższy niż 181 punkty base w teście SPECrate 2017 Integer,

ID	Nazwa elementu, parametru lub cechy	Wymaganie
		opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów.
3	Liczba procesorów	Min. 2
4	Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon)
5	Pamięć operacyjna	Zainstalowane minimum 512GB pamięci RAM o częstotliwości 2933MHz. Minimum 24 sloty na pamięć. Możliwość rozbudowy do 3TB RAM. Wymagana możliwość instalacji pamięci typu persistent memory. Łączna ilość zainstalowanej pamięci RDIMM oraz pamięci persistent memory powinna wynosić minimum 7.5 TB
6	Zabezpieczenie pamięci	memory mirroring, demand scrubing, patrol scrubing, memory rank sparing, ECC, SDDC,
7	Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60Hz. 1 port VGA na tylnym panelu serwera. Wymagana możliwość instalacji portu VGA lub Dispaly Port na panelu przednim.
8	Rozbudowa dysków	Serwer musi posiadać możliwość zainstalowania minimum 8 dysków SAS/SATA, przy czym zainstalowane powinny być minimum 2 dyski SSD o pojemności przynajmniej 240GB każdy.
9	Kontroler dyskowy	Zainstalowany w dedykowanym slocie kontroler sprzętowy z obsługą 8 napędów dyskowych SAS/SATA oraz obsługujący poziomy RAID: 0, 1, 5, 10 ze wsparciem ESXi.
10	Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Platinum.
11	Interfejsy sieciowe	Zintegrowane na płycie głównej 2 porty 10Gb SFP+ wyposażone we wkładki typu SR lub kable DAC. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w punkcie Dodatkowe sloty I/O . Wymagana funkcjonalność wbudowanych portów: NIC teaming, możliwość realizacji bezpośredniego dostępu do pamięci iWARP, SR-IOV, offload sumy kontrolnej stosu TCP/IP, obsługa ramek Jumbo do 9.5Kb lub podział portu 10Gb na 4 porty wirtualne, obsługa VXLAN/NVGRE, wsparcie dla VMware NetQue / VMQ oraz Microsoft VMQ & Dynamic VMQ, obsługa ramek Jumbo do 9200b, wymagana funkcjonalność RDMA, wymagana możliwość aktywowania pełnego sprzętowego wsparcia dla FCoE / iSCSI Dodatkowe dwa porty SFP+ wyposażone we wkładki typu SR lub kable DAC zainstalowane na karcie rozszerzeń. Wymagana funkcjonalność tych portów: wymagana funkcjonalność podziału portu 10Gb na 4 porty wirtualne, obsługa VXLAN/NVGRE, wsparcie dla

ID	Nazwa elementu, parametru lub cechy	Wymaganie
		VMware NetQue / VMQ oraz Microsoft VMQ & Dynamic VMQ, obsługa ramek Jumbo do 9200b, wymagana funkcjonalność RDMA, wymagana możliwość aktywowania pełnego sprzętowego wsparcia dla FCoE / iSCSI lub NIC teaming, możliwość realizacji bezpośredniego dostępu do pamięci iWARP, SR-IOV, offload sumy kontrolnej stosu TCP/IP, wsparcie dla DCB, obsługa ramek Jumbo do 9.5Kb Wraz z urządzeniem Wykonawca dostarczy minimum 4 wkładki SFP+ (10 Gb multimode) lub kable AOC (min. 2m) lub kable DAC (min. 2m) jeżeli dostarczone urządzenia pochodzą od tego samego producenta co zaproponowane przełączniki typy Data Center. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
12	Dodatkowe sloty I/O	Serwer powinien umożliwiać instalacje do 3 kart PCIe. W chwili dostawy serwer powinien umożliwiać obsługę przynajmniej 2 kart PCIe bez instalacji jakichkolwiek dodatkowych komponentów serwera.
13	Dodatkowe porty	• z przodu obudowy: 1x USB 3.0, . Możliwość instalacji portu VGA lub Display Port. • z tyłu obudowy: 2x USB 3.0, 1x DB-15 . Możliwość instalacji portu DB9
14	Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
15	Zarządzanie	Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający: • Monitoring statusu i zdrowia systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, … • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O • Logowanie zdarzeń • Wysyłanie określonych zdarzeń poprzez SMTP, SNMPv3 • Logowanie aktywności użytkowników • Umożliwiający Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediów z wykorzystaniem Java client • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość jednoczesnej pracy do 6 użytkowników Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, REST API.

ID	Nazwa elementu, parametru lub cechy	Wymaganie
		Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarządzenie infrastrukturą serwerów, bez udziału dedykowanego agenta, - przedstawianie graficznej reprezentacji zarządzanych urządzeń,- możliwość skalowania do minimum 560 urządzeń,- udostępnianie szybkiego podgląd stanu środowiska, - udostępnianie podsumowania stanu dla każdego urządzenia, - tworzenie alertów przy zmianie stanu urządzenia, - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, - konsola zarzadzania oparta o HTML 5, - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne, - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń, - definiowanie roli użytkowników oprogramowania, - obsługa REST API, - obsługa SNMP, , Email Forwarding, - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa SSO (single sign on), - przedstawianie historycznych aktywności użytkowników, - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych, - Obsługa NTP, - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesypem plików diagnostycznych,
16	Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł TPM. Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz.
17	Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
18	Obsługa	Możliwość instalacji serwera oraz tzw. Backplane'y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych.
19	Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.
20	Systemy operacyjne	Microsoft Windows Server 2012 R2, 2016, 2019, Red Hat Enterprise Linux 6

ID	Nazwa elementu, parametru lub cechy	Wymaganie
		oraz 7, SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6.5 oraz 6.7.
21	Waga	maximum: 21.9kg
22	Gwarancja	Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej ważnej przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka (tj. procesor, pamięć, VRM, dyski, zasilacze, wentylatory) wymagane jest rozszerzenie poziomu gwarancji do 36 miesięcy 7/24 z gwarantowanym czasem naprawy 24h

8.9.2 Oprogramowanie do wirtualizacji

W warstwie wirtualizacji wymagane jest dostarczenie licencji wraz z konsolą do zarządzania z licencjami na wszystkie procesory dostarczanych serwerów lub równoważne.

Zamawiający obecnie posiada rozwiązanie VMWare vSphere wraz z konsolą do zarządzania vCenter.

Poniżej zawarto warunki równoważności oprogramowania do wirtualizacji serwerów.

Tabela 14 Minimalne wymagania dla oprogramowania do wirtualizacji

ID	Wymaganie
1	Dostarczone oprogramowanie może posłużyć do zbudowania układu klastra niezawodnościowego składającego się z węzłów fizycznych w ilości 3-64 sztuk.
2	Możliwość wirtualizacji serwerów – warstwa musi być rozwiązaniem sprzętowym czyli musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.
3	Możliwość obsługi pamięci masowej przez maszyny wirtualne - musi istnieć możliwość przydzielenia większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM
4	Oprogramowanie musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
5	Oprogramowanie musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda musi mieć 1-10 wirtualnych kart sieciowych.
6	Oprogramowanie musi mieć możliwość podłączenia do 20 urządzeń USB do każdej maszyny wirtualnej.

ID	Wymaganie
7	Oprogramowanie musi mieć możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, zwłaszcza w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
8	System musi posiadać funkcjonalność wirtualnego przełącznika umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Przełącznik wirtualny musi mieć możliwość konfiguracji do 4000 portów. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne.
9	Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych.
10	Oprogramowanie musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
11	Pamięć masowa z obsługą API.
12	Obsługa natywnej pamięci 4K.
13	Możliwość pojedynczego restartu.
14	Szybkie uruchamianie Hypervisor'a z pominięciem maszyny fizycznej.
15	Możliwość migracji pomiędzy instancjami „live obciążeń" maszyn wirtualnych.
16	Obsługa modułu TPM 2.0.
17	Wirtualny moduł TPM 2.0.
18	Obsługa VBS firmy Microsoft.
19	EVC na poziomie maszyny.
20	Szybkie klonowanie wraz z ich pełną konfiguracją i danymi.
21	Możliwość wykonania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania pracy.
22	Rozwiązanie musi posiadać wbudowane interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacji.
23	Rozwiązanie powinno posiadać centralną minimum jedną Centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania ich funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5 oraz musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP. Konsola musi zarządzać w trybie wysokiej dostępności min. pięcioma serwerami.
24	Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie

ID	Wymaganie
	skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
25	Rozwiązanie musi mieć możliwość skalowania infrastruktury typu klaster do ilości 64 serwerów fizycznych pracujących w jednym logicznym układzie.
26	Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. procesory, pamięć RAM, wykorzystanie przestrzeni na dyskach/wolumenach).
27	Rozwiązanie musi zapewnić zdefiniowanie alertów informujących o przekroczeniu wartości progowych.
28	Rozwiązanie musi zapewniać narzędzie zarządzania całością środowiska wirtualizacji w trybie GUI.

8.9.3 Oprogramowanie do automatyzacji

Zamawiający wymaga dostarczenia oprogramowania do automatyzacji procesów instalacji i zarządzania wraz z licencjami umożliwiającymi pracę tego oprogramowania na platformie sprzętowej składającej się co najmniej z **100 elementów zarządzanych**.

Tabela 15 Minimalne wymagania dla oprogramowania do automatyzacji

ID	Wymaganie
1	Platforma automatyzacji procesów (dalej platforma) musi mieć możliwość instalacji na serwerach fizycznych działających pod kontrolą systemu operacyjnego klasy Linux w tym na Red Hat Enterprise Linux 7 lub 8.
2	Platforma musi mieć możliwość instalacji na serwerach wirtualnych działających pod kontrolą systemu operacyjnego klasy Linux w tym Red Hat Enterprise Linux 7 lub 8, działających w środowisku wirtualnym realizowanym przez oprogramowanie typu Vmware, Microsoft Hyper-V i Red Hat Enterprise Virtualiztion.
3	Platforma musi umożliwiać automatyzację procesów instalacji, konfiguracji i modyfikacji elementów sprzętowych jak i oprogramowania, środowiska ICT.
4	Platforma musi być niezależna od zastosowanej infrastruktury sprzętowej na której zostanie zainstalowana i uruchomiona. Wsparcie co najmniej dla produktów HPE, Dell, Cisco, Lenovo, Arista, Juniper, F5, Palo Alto itp.
5	Wymagane jest udokumentowane wsparcie platformy dla zastosowanego sprzętu jak i systemu operacyjnego na którym zostanie zainstalowana.
6	Platforma musi pozwalać na instalacje w trybie klastra, dla zachowania niezawodności rozwiązania. Rozwiązanie musi zostać uruchomione w modelu HA.
7	Platforma musi pozwalać na skalowanie typu Scale-Out, dla zachowania wydajności rozwiązania w różnych segmentach zarządzanego środowiska ICT.

ID	Wymaganie
8	Platforma musi umożliwić zarządzanie środowiskiem ICT w izolowanych segmentach sieci.
9	Algorytmy procesów muszą być opisane w standardowym formacie takim jak XML, YAML lub równoważnym.
10	Platforma musi posiadać graficzny panel do przedstawienia całego zarządzanego środowiska.
11	Platforma musi posiadać mechanizm weryfikacji i raportowania zastosowanych licencji/subskrypcji dla zarządzanego środowiska.
12	Platforma musi posiadać mechanizm RESTful API do integracji z zewnętrznymi elementami środowiska ICT.
13	Platforma musi posiadać możliwość połączenia działania kilku algorytmów/procesów w jeden algorytm/proces.
14	Wymagane wsparcie dla autentykacji na platformie za pomocą mechanizmów: LDAP, Radius, SAML, Google OAuth2, Github, TACACS+ i AzureAD.
15	Platforma musi pozwalać na połączenie z systemem centralnego logowania zdarzeń takich jak: Elastic, Splunk, Sumologic, Loggly lub własny (RESTful API).
16	Platforma musi posiadać centralne zarządzanie systemem uwierzytelniania bez konieczności ujawniania elementów uwierzytelnienia końcowym użytkownikom.
17	Platforma musi posiadać mechanizm powiązania systemu uwierzytelniania z systemami: HashiCorp Vault, CyberArk AIM, CyberArk Conjur, Microsoft Azure Key Vault.
18	Wymagane wsparcie dla generowania metryk elementów platformy za pomocą standardowych protokołów np. Prometheus.
19	Wsparcie dla Platformy musi zostać dostarczane przez producenta platformy prze okres 36 miesięcy w reżimie zgłaszania problemów 24 godziny, 7 dni w tygodniu.

8.10 Zasilacze UPS

Tabela 16 Minimalne wymagania dla zasilaczy UPS

ID	Komponent	Wymaganie
1	Parametry podstawowe	a) Moc na wyjściu co najmniej 3 kVA b) Architektura: on-line lub line interactive c) Obudowa maksymalnie 3U wraz z zestawem szyn montażowych
2	Porty wejścia wyjścia	a) wejście jednofazowe b) wyjście zgodne z dostarczonymi modułami zasilającymi PDU w szafie

ID	Komponent	Wymaganie
		rack c) UPS musi zostać połączy w sposób zapewniający zasilanie awaryjne co najmniej na jednej linii zasilania dochodzącej do dostarczonej szafy
3	Porty komunikacyjne	Porty umożliwiające komunikację: - out-of-band za pomocą portu szeregowego lub USB - sieciowy za pomocą portu Ethernet RJ 45
4	Zarządzanie	Urządzenie musi być wyposażone w kartę umożliwiającą zdalne monitorowanie i zarządzanie dzięki bezpośredniemu połączeniu z siecią za pomocą protokołów HTTP, HTTPS, IPv4, , SNMP, SSH.
5	Gwarancja	3 lat gwarancji od daty odbioru realizowanej w miejscu instalacji sprzętu, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.

8.11 System backupu

Wykonawca zobowiązany jest do dostarczenia wszystkich niezbędnych komponentów systemu do wykonywania i odtwarzania kopii zapasowych dla dostarczanej infrastruktury do systemu ZSI-ULC zainstalowanego na urządzeniach będących przedmiotem niniejszego zamówienia.

Obecnie zamawiający posiada System do backupu Veeam.

Wykonawca zobowiązany jest do:

- dostarczenia i zainstalowania systemu operacyjnego na platformie serwerowej – wspieranego i/lub rekomendowanego przez oprogramowanie do backupu,
- dostarczenie licencji oraz uruchomienie oprogramowania do backupu – zgodnego z wymaganiami zawartymi w **Tabela 17 Minimalne wymagania na oprogramowanie do backupu,**
- dostarczenie i uruchomienie urządzenia do składowania danych – zgodnego z wymaganiami zawartymi w **Tabela 18 Minimalne wymagania dla urządzenia do składowania danych oraz deduplikacji**.
- integrację oprogramowania do backupu z urządzeniem do składowania danych.

Tabela 17 Minimalne wymagania na oprogramowanie do backupu

ID	Wymaganie
1	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
2	Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
3	Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.

ID	Wymaganie
4	Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V.
5	Oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone.
6	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
7	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków lub pozwalać na odtwarzanie danych także w przypadku gdy baza deduplikacyjna jest niedostępna lub uszkodzona.
8	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
9	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie chyba że nie są one wykorzystywane w procesie odtwarzania danych. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
10	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania. Z wyjątkiem sytuacji gdy dedykowani agenci są w cenie licencji bazowej (per CPU) bez ograniczenia co do ilości i typu aplikacji czy systemów.
11	Oprogramowanie musi zapewniać backup jednoprzebiegowy lub za pomocą dedykowane agenta w cenie licencji bazowej per CPU - nawet w przypadku wymagania granularnego odtworzenia.
12	Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshot.
13	Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director.
14	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
15	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
16	Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
17	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
18	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking minimum dla Vmware i Hyper-V.

ID	Wymaganie
19	Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
20	Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
21	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
22	Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
23	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
24	Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli.
25	Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)
26	Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio z backupu, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana minimum dla Vmware.
27	Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor, min. VMware.
28	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
29	Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny VMware bezpośrednio do Microsoft Azure oraz Amazon.
30	Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: - Linux, - ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs, - Windows, - NTFS, FAT, FAT32, ReFS.
31	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
32	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej lub za jego pośrednictwem.
33	Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
34	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych

ID	Wymaganie
35	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze.
36	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze.
37	Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
38	Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows

Tabela 18 Minimalne wymagania dla urządzenia do składowania danych oraz deduplikacji.

ID	Wymaganie
1	Przedmiotem zamówienia jest dostarczenie urządzenia do de-duplikacji i przechowywania danych spełniającego poniższe wymagania.
2	Oferowane urządzenie musi posiadać minimum 1 port 1GbE, minimum 2 portów 10GbE SFP+. Wraz z urządzeniem Wykonawca dostarczy minimum 2 wkładki SFP+ (10 Gb multimode). Urządzenie musi posiadać możliwość rozbudowy do dodatkowych 6 portów 10GbE
3	Oferowany produkt musi posiadać wsparcie dla następujących interfejsów dostępowych: a) CIFS, NFS, OST, RMAN SBT API, b) Deduplikacja na źródle, 1 GbE, 10GbE
4	Urządzenie musi umożliwiać składowanie danych poprzez udostępnianie min 36 zasobów NAS w sieci Ethernet wykorzystując protokoły CIFS, NFS
5	Wymagane jest dostarczenie licencji, pozwalającej na obsługę protokołów CIFS, NFS, OST, replikacji, deduplikacji na źródle do pełnej pojemności urządzenia.
6	Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości.
7	Proces deduplikacji powinien odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia.
8	Oferowany produkt musi posiadać obsługę mechanizmów deduplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, NFS, OST, RMAN SBT API) przechowywanych w obrębie całego urządzenia.
9	Oferowany produkt musi posiadać obsługę deduplikacji na źródle
10	Unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.

ID	Wymaganie
11	Oferowane urządzenie musi wspierać, co najmniej następujące aplikacje HP Data Protector, Symantec NetBackup oraz Backup Exec, EMC Networker, Oracle Secure Backup, TSM, CommVault Simpana, Veeam
12	W przypadku współpracy z aplikacją Symantec NetBackup, urządzenie musi umożliwiać deduplikację na źródle (de-duplikację po stronie media serwera). Deduplikacja taka musi zapewniać by z serwerów do urządzenia były transmitowane tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. Wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność.
13	W przypadku współpracy z aplikacją Oracle RMAN, urządzenie musi umożliwiać deduplikację na źródle (de-duplikację po stronie media serwera). Deduplikacja taka musi zapewniać by z serwerów do urządzenia były transmitowane tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. Wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność.
14	W przypadku współpracy z aplikacją Veeam, urządzenie musi umożliwiać deduplikację na źródle. Deduplikacja taka musi zapewniać by z serwerów do urządzenia były transmitowane tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. Wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność.
15	Deduplikacja taka musi zapewniać by z serwerów do urządzenia były transmitowane tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. Wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność.
16	Dostarczone urządzenie musi posiadać, co najmniej 27 TB powierzchni netto (po odjęciu przestrzeni wykorzystywanej na zabezpieczenie RAID) przeznaczonej na przechowywanie unikalnych segmentów danych (backupów). Urządzenie powinno umożliwiać rozbudowę powierzchni do co najmniej 108 TB netto.
17	Oferowany produkt musi umożliwiać replikację danych realizowaną między urządzeniami. Replikacja powinna umożliwiać szyfrowanie przesyłanych danych - długość klucza minimum 256-bit. Wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność.
18	Urządzenie musi umożliwiać replikację danych z mniejszymi i większymi modelami urządzeń tego samego producenta. Urządzenie musi umożliwiać replikację danych z edycjami wirtualnymi.
19	Replikacja musi być możliwa w trybie co najmniej 10 do 1 (*many to one*) oraz co najmniej 1 do 2 (*fan out*). Kaskadowanie replikacji jest opcjonalne.
20	Oferowany produkt musi umożliwiać sprzętowe szyfrowanie przechowywanych danych realizowaną przez dyski szyfrujące kluczem o długości minimum 256-bit. **Nie jest** wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność.
21	W przypadku replikacji danych między urządzeniami kontrolowanej przez system Symantec NetBackup muszą być możliwe do uzyskania następujące funkcjonalności: ● replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących ● replikacji podlegają tylko te fragmenty danych które nie znajdują się w docelowym urządzeniu aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach

ID	Wymaganie
22	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej (np RAID6 DDP).
23	Oferowane pojedyncze urządzenie musi osiągać wydajność co najmniej 7TB/hr (dane podawane przez producenta, bez deduplikacji na źródle) lub 18TB/h (dane podawane przez producenta, z deduplikacją na źródle)
24	Urządzenie musi być rozwiązaniem kompletnym. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway z uwagi na brak miarodajnych danych dotyczących ich wydajności oraz dostępności. Zamawiający dopuszcza możliwość rozbudowy urządzenia przez dodanie modułów dyskowych.
25	Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt), fabrycznie nowe, pochodzić z oficjalnego kanału sprzedaży w Polsce.
26	Dostarczone urządzenie musi być serwisowane przez producenta lub autoryzowany serwis producenta w języku polskim ze wsparciem na 3 lata w reżimie 5x9xNDB. W przypadku autoryzowanego serwisu producenta na terenie Polski, wymagane jest potwierdzenie kompetencji w zakresie świadczenia usług serwisowych poprzez certyfikat ISO 9001:2015. W celu zapewnienia wysokiej jakości usług wymagane jest, aby jednostka serwisowa posiadała przynajmniej 2 inżynierów z certyfikatami uprawniającymi do napraw urządzenia.

9 Usługa wdrożenia

W ramach wdrożenia Wykonawca zobowiązany jest do uruchomienia sprzętu i oprogramowania zawartego w Tabeli 1, zgodnie z poniższymi wymaganiami.

9.1 Wymagania ogólne

W ramach wdrożenia Wykonawca wykona, dla każdego z zakresów, co najmniej:

1. Oznaczenie sprzętu

   Wszystkie urządzenia dostarczane w ramach niniejszego Zamówienia muszą zostać oznaczone przez Wykonawcę w sposób wskazujący, że Projekt jest współfinansowany przez Unię Europejską ze środków Programu Operacyjnego Polska Cyfrowa. Do oznakowania wykorzystane powinny zostać naklejki promocyjne dostarczone do Zamawiającego w ramach prac związanych z promocją Projektu ZSI-ULC (realizowane w ramach innego zamówienia).

2. Projekt techniczny wdrożenia zawierający minimum:

   Projekt techniczny z poziomem szczegółowości LLD (Low-level design) zostanie uzgodniony i przesłany Zamawiającemu do akceptacji.

   - opis dostarczanych komponentów sprzętowych i programowych,

- dane środowiskowe dla dostarczanego sprzętu,
- projekt instalacji w szafach Zamawiającego,
- sposoby podłączenia zasilania,
- opis połączeń LAN i SAN: adresacja, przydział portów,
- sposoby zarządzania.

3. Instalację i uruchomienie sprzętu zgodnie z uzgodnionym z Zamawiającym Projektem technicznym wdrożenia a w tym co najmniej:
   - Montaż urządzeń w szafach,
   - Podłączenie zasilania,
   - Podłączenie sieci LAN i SAN (kable połączeniowe zapewnia Wykonawca),
   - Uruchomienie urządzeń, zaadresowanie portów, uruchomienie komunikacji,
   - Aktualizacja oprogramowania układowego urządzeń do najnowszej wersji oraz aktualizacja także do najnowszej wersji oprogramowania, systemów operacyjnych, wirtualizatora, itp.,
   - Konfiguracja urządzeń po akceptacji projektu technicznego przez Zamawiającego.
4. Dokumentację testów systemu zawierającą:
   - Zakres testów,
   - Procedury testowe.
5. Dokumentację techniczną zawierającą co najmniej:
   - Szczegółową konfigurację urządzeń, mechanizmy niezawodnościowe,
   - Adresację portów/urządzeń,
   - Procedury i wyniki testów,
   - Procedury utrzymaniowe m.in.:
     a. Administracja serwera, systemu operacyjnego, aplikacji pomocniczych, usług,
     b. Inwentaryzacja zasobów wewnętrznych,
     c. Tworzenie kopii zapasowej i odtwarzanie po awarii,
   - Procedury serwisowe (m.in. obsługa awarii).

Nowo dostarczona infrastruktura musi być dołączona do istniejącej infrastruktury Zamawiającego.

Wykonawca dostarczy szczegółowy wykaz dostarczanego sprzętu oraz licencji.

9.2 Wymagania szczególne

9.2.1 Wymagania szczególne dla przełączników rdzeniowych i Data Center-

W ramach wdrożenia, poza zakresem ogólnym, Wykonawca wykona poniższe prace:

1. konfiguracja klastrów niezawodnościowych za pomocą portów 40 Gbps (lub dedykowanych),
2. podłączenie nowych urządzeń do aktualnie posiadanych przez Zamawiającego Urządzeń, wraz z ich poprawną konfiguracją,
3. podłączenie Przełączników do będącego w posiadaniu przez Zamawiającego systemu do zarządzania przełącznikami sieciowymi,
4. strojenie urządzeń w niezbędnym zakresie m.in.:
    a. konfiguracji adresacji i połączeń,
    b. przeniesienie konfiguracji z aktualnie posiadanych przez Zamawiającego przełączników,
    c. konfiguracja monitoringu,
    d. konfiguracja użytkowników i uprawnień,
5. przeprowadzenie testów akceptacyjnych.

Nowe urządzenia muszą być połączone z aktualnie posiadanymi przez Zamawiającego urządzeniami. Wykonawca realizując projekt musi zapewnić poprawne działanie nowych urządzeń z aktualnie posiadanymi urządzeniami. Dostarczenie nowych urządzeń nie może ograniczyć możliwości korzystania przez Zamawiającego z posiadanej infrastruktury i systemów.

9.2.2 Wymagania szczególne dla Systemu WiFi:

W ramach wdrożenia systemu WiFi Wykonawca przeprowadzi:

1. Opracowanie planu rozmieszczenia punktów dostępowych.
    a. Wizja lokalna środowiska wdrożenia, określenie możliwych punktów oraz sposobu fizycznego montażu punktów dostępowych (uwzględniając tylko istniejące okablowanie w siedzibie Zamawiającego),
    b. Opracowanie optymalnego doboru nastawień parametrów radiowych (tj. kanały nadawania, moc nadawania) dla poszczególnych punktów dostępowych,
    c. Zaproponowanie najodpowiedniejszej lokalizacja bezprzewodowych punktów dostępowych,
    d. Określenie optymalnego doboru ustawień parametrów radiowych dla poszczególnych punktów dostępowych.
2. Wykonanie prac związanych z instalacją i konfiguracją Urządzeń:

e. Dostawa, instalacja i konfiguracja urządzeń aktywnych Sieci WiFi, niezbędnych kontrolerów wraz z licencjami oraz 30 szt. punktów dostępowych sieci bezprzewodowej.
f. Wykonawca uruchomi i skonfiguruje wszystkie elementy i podzespoły do uzyskania pełnej funkcjonalności zgodnie z założeniami dokumentacji przedwdrożeniowej.

3. Uruchomienie i testy poprawności działania sieci bezprzewodowej.

Po ukończeniu prac instalacyjnych i konfiguracyjnych Wykonawca zobowiązany jest do uruchomienia i przetestowania poprawności oraz bezpieczeństwa działania wdrożonej infrastruktury sieci WiFi i przedstawienia wyników Zamawiającemu. W razie wykrycia problemów, uszkodzeń nie wynikających z wadliwego działania urządzeń Zamawiającego, Wykonawca jest zobowiązany do usunięcia wszystkich usterek i ponownego przeprowadzenia testów. Wynikiem wszystkich przeprowadzonych prac powinna być funkcjonująca infrastruktura sieci WiFi wykonana na podstawie wcześniej wykonanego projektu przedwdrożeniowego.

Szczegółowy opis testów:

1) Weryfikacja pracy urządzeń – test ma na celu sprawdzenie czy urządzenia uruchamiają się prawidłowo i czy przy starcie/restarcie nie pojawiają się komunikaty o błędach, występują problemu z konfiguracją urządzeń.
2) Testy komunikacji sieciowej – test ma na celu sprawdzenie poprawności działania komunikacji między poszczególnymi urządzeniami sieci z kilku przykładowych lokalizacji sieci WiFi.
3) Test sieci WiFi – test ma na celu weryfikacje poprawności działania sieci zgodnie z założeniami dokumentacji przedwdrożeniowej. Test ma za zadanie wykazanie poprawnego mobilnego przemieszczania się klienta WiFi pomiędzy różnymi AP bez zbytnich opóźnień czy też niekontrolowanych rozłączeń, utraty przyznanego adresu IP.
    a. Testy dostępu bezprzewodowego wykonane dla pasma 2.4 oraz 5GHz.
    b. Potwierdzenie możliwości dostępu do sieci WLAN poprzez poszczególne SSID we wszystkich wymaganych obszarach/pomieszczeniach.
    c. Weryfikacja działania DHCP dla poszczególnych SSID.
    d. Potwierdzenie możliwości dostępu do sieci korporacyjnej przez odpowiednie SSID, z uwzględnieniem poprawnego działania (ograniczenia) filtracji w dostępie do danego SSID korporacyjnego tylko dla wskazanych grup użytkowników domenowych.

e. Weryfikacja poprawności działania założonych polityk bezpieczeństwa dostępu do WLAN we wszystkich SSID zgodnie z założeniami projektowymi.

Po zakończeniu wszystkich prac Wykonawca zobowiązany jest do wykonania i przekazania Odbiorcy dokumentacji zgodnie z zakresem opisanym w zasadach ogólnych.

9.2.3 Wymagania szczególne dla zapory NGFW:

W ramach wdrożenia, poza zakresem ogólnym, Wykonawca wykona poniższe prace:

1. uruchomienie wszystkich wymaganych przez Zamawiającego modułów bezpieczeństwa,
2. strojenie systemów w niezbędnym zakresie m.in.:
   a. konfiguracja adresacji i połączeń,
   b. przeniesie konfiguracji z aktualnie posiadanych przez Systemów Bezpieczeństwa Zamawiającego (wskazane na etapie tworzenia dokumentacji przed wykonawczej),
   c. przeniesie i optymalizacja polityk i NAT, do warstwy 4 modelu ISO/OSI,
   d. migracja blacklist i whitelist, adresów IP i URL,
   e. konfiguracja użytkowników i uprawnień,
3. uruchomienie funkcjonalności posiadanych przez Zaporę Sieciową Nowej Generacji zgodnie z wytycznymi Zamawiającego,
4. skonfigurowanie 5 tuneli site2site i dwóch bramek SSL VPN, uwzględnionych w projekcie wdrożenia.

9.2.4 Wymagania szczególne dla zapór oddziałowych

W ramach wdrożenia, poza zakresem ogólnym, Wykonawca wykona poniższe prace:

1. uruchomienie wszystkich wymaganych przez Zamawiającego modułów bezpieczeństwa,
2. strojenie systemów w niezbędnym zakresie m.in.:
   a. konfiguracja adresacji i połączeń,
   b. przeniesienie konfiguracji z aktualnie posiadanych przez Zamawiającego Urządzeń,
   c. konfiguracja użytkowników i uprawnień,
   d. konfiguracja niezawodnego szyfrowanego połączenia oddziałów Zamawiającego z centralą.

9.2.5 Wymagania szczególne dla pamięci masowej - blokowej:

W ramach wdrożenia, poza zakresem ogólnym, Wykonawca wykona poniższe prace:

1. Integracja z siecią LAN Zamawiającego, utworzenie wymaganych połączeń logicznych, podsieci, VLAN'ów .
2. Podłączenie do sieci SAN , utworzenie wymaganych aliasów, konfiguracji, mechanizmów mapowania i autoryzacji.
3. Konfiguracja mechanizmów zarządzania dostarczoną macierzą dyskową.
4. Utworzenie wymaganych zasobów dyskowych – RAID, puli, wolumenów, mapowanie na porty macierzy zgodnie z przygotowaną dokumentacją techniczną wdrożenia.
5. Weryfikacja mechanizmów multipath dla udostępnionych zasobów dyskowych.

9.2.6 Wymagania szczególne dla pamięci masowej - obiektowej:

W ramach wdrożenia, poza zakresem ogólnym, Wykonawca wykona poniższe prace:

1. Integracja z siecią LAN Zamawiającego, utworzenie wymaganych połączeń logicznych, podsieci, VLAN'ów.
2. Konfiguracja mechanizmów zarządzania dostarczoną macierzą.
3. Konfiguracja wymaganych zasobów tenant.
4. Konfiguracja mechanizmów replikacji i zabezpieczenia składowanych danych.
5. Integracja z DNS, NTP, AD/LDAP.

9.2.7 Wymagania szczególne dla serwerów:

W ramach wdrożenia, poza zakresem ogólnym, Wykonawca wykona poniższe prace:

1. Integracja z siecią LAN Zamawiającego, utworzenie wymaganych połączeń logicznych, podsieci, VLAN'ów,
2. Podłączenie do sieci SAN , utworzenie wymaganych aliasów, konfiguracji, mechanizmów mapowania i autoryzacji
3. Obsługa serwisowa w czasie trwania umowy, zapewnienie pojedynczego punktu kontaktu w przypadku zgłoszeń dotyczących infrastruktury, systemów operacyjnych oraz aplikacji pomocniczych.

W warstwie wirtualizacji, Wykonawca wykona następujące prace:

1. Instalacja wymaganego oprogramowania systemowego wirtualizacji oraz zarządzającego wraz z wymaganymi na czas wdrożenia poprawkami systemowymi,

2. Podłączenie serwerów do klastra wirtualizacji, integracja z mechanizmami zarządzania klastrem serwerów wirtualizacyjnych
3. Wsparcie i obsługa serwisowa w trakcie trwania umowy dla utworzonej konfiguracji klastra środowiska wirtualizacji.

W warstwie systemów operacyjnych, Wykonawca wykona następujące prace:

1. Przewiduje się wykorzystanie systemów operacyjnych rodziny Linux Debian – o ile nie wystąpią warunki wykluczenia Linux Debian przez aplikacje pomocnicze. Wtedy zostanie wykorzystany system operacyjny z listy wsparcia aplikacji pomocniczych.
2. Ilość VM oraz wersje systemu określone zostaną w projekcie ZSI a Wykonawca zobowiązany jest skonfigurować środowisko zgodnie z wymaganiami projektu ZSI w ramach usług utrzymania lub serwisu infrastruktury.

W warstwie aplikacji pomocniczych, Wykonawca wykona następujące prace:

1. Przygotowanie systemu na potrzeby wykorzystania zestawów instalacyjnych (playbook'ów Ansible),
    a. system ten musi zapewnić odseparowanie wdrażanego środowiska od strefy DMZ,
    b. system musi zapewnić możliwość aktualizacji repozytorium oprogramowania dostarczanego jako subskrypcja z portalu producenta rozwiązania (wymagane połączenie internetowe),
    c. system musi zapewnić pełną rozliczalność logowania użytkowników systemu oraz logować wszystkie polecenia wydawane przez administratora systemu,
    d. system musi zostać poddany utwardzaniu w zakresie bezpieczeństwa. Szczegóły zakresu utwardzenia zostaną wypracowane i przedstawione na etapie przygotowania dokumentacji projektowej systemu.
2. Przygotowanie niezbędnych mechanizmów integracji z DNS, NTP, AD/LDAP,

9.2.8 Wymagania szczególne dla systemu backup

W ramach wdrożenia, poza zakresem ogólnym (instalacja, aktualizacja i konfiguracja oprogramowania do backupu) Wykonawca wykona poniższe prace:

1. Integracja serwera backupu z siecią LAN Zamawiającego, utworzenie wymaganych połączeń logicznych, podsieci, VLAN'ów,
2. Integracja serwera backup oraz urządzenia do składowania danych z infrastrukturą Zamawiającego – systemy DNS, NTP, AD, vCenter,

3. Integracja serwera backupu z urządzeniem do składowania danych,
4. Testy poprawności działania:
    a. Weryfikacja integracji z infrastrukturą Zamawiającego,
    b. Weryfikacja działania urządzenia do składowania danych w dziedzinie:
        i. Poprawności odbioru strumienia danych,
        ii. Poprawności zapisu odebranych danych,
        iii. Poprawności deduplikacji i kompresji danych,
    c. Weryfikacja działania systemu backup w dziedzinie:
        i. Poprawności komunikacji z vCenter,
        ii. Poprawności tworzenia strumienia backupu,
        iii. Poprawności komunikacji z urządzeniem do składowania danych,
        iv. Poprawności odtwarzania danych,
    d. Tworzenie testowych polityk backupu – weryfikacja poprawności,
    e. Integracja z mechanizmami zarządzania infrastrukturą.

10 Asysta techniczna

Wykonawca w ramach realizacji Umowy zapewni możliwość skorzystania z usług asysty technicznej. Usługi asysty technicznej będą świadczone przez Wykonawcę zgodnie z poniższymi wymaganiami:

1. Przykładami usług asysty technicznej, które Wykonawca będzie świadczył na rzecz Zamawiającego są:
    a. Obsługa dodatkowych warsztatów;
    b. Działania doradczo-konsultingowe;
    c. Działania konfiguracyjne, optymalizujące oraz naprawcze w stosunku do zrealizowanych dostaw oraz usług instalacyjnych i konfiguracyjnych;
2. Zamawiającemu przysługują usługi asysty technicznej w wymiarze co najmniej 150 roboczogodzin (dokładna liczba roboczogodzin usług asysty technicznej określona zostanie w Umowie na podstawie formularza oferty Wykonawcy) pracy pracowników Wykonawcy do wykorzystania przez 12 miesięcy od daty podpisania Protokołu Odbioru Przedmiotu Zamówienia bez zastrzeżeń.
3. Zamawiający będzie zlecał Wykonawcy prace w ramach asysty technicznej w miarę potrzeb.

4. Asysta techniczna będzie rozliczana z dokładnością do jednej roboczogodziny. Czas realizacji poszczególnych prac będzie zaokrąglany w górę z dokładnością do jednej roboczogodziny.
5. Asysta techniczna będzie świadczona w siedzibie Zamawiającego lub z miejsca wskazanego przez Zamawiającego, ustalonego z Wykonawcą.
6. W ramach usług w zakresie asysty technicznej do Zamawiającego zostanie przypisany dedykowany specjalista Wykonawcy, który będzie odpowiedzialny za realizację usług w zakresie asysty technicznej dla Zamawiającego, a także za przekazywanie oraz otrzymywanie informacji i komentarzy zwrotnych dotyczących świadczonych usług.
7. Wykonawca najpóźniej w dniu podpisania Protokołu Odbioru Przedmiotu Zamówienia przekaże dane kontaktowe do osoby odpowiedzialnej za odbiór zgłoszeń od Zamawiającego związanych z realizacją usług asysty technicznej.
8. W przypadku wystąpienia potrzeby skorzystania z asysty technicznej, Zamawiający skieruje do Wykonawcy zgłoszenie w godzinach pracy Zamawiającego. Zgłoszenie zawierać będzie co najmniej:
    a. zakres prac do wykonania lub opis problemu do rozwiązania,
    b. (opcjonalnie) określenie proponowanego terminu rozwiązania,
    c. (opcjonalnie) określenie miejsca wykonania usługi,

    Zgłoszenie będzie przekazane Wykonawcy drogą mailową lub telefoniczną.
10. W terminie nie dłuższym niż 1 dzień roboczy (NBD – Next Business Day) od dnia i godziny otrzymania zgłoszenia o asystę techniczną Wykonawca skontaktuje się z Zamawiającym w celu ustalenia szczegółowego zakresu prac, terminu realizacji i szacowanego wymiaru godzin realizacji asysty.
11. Po kontakcie z Zamawiającym, w terminie nie dłuższym niż 1 dzień roboczy (o ile Strony nie ustalą późniejszego terminu) Wykonawca rozpocznie realizację asysty technicznej.
12. Po wykonaniu każdorazowych prac związanych z realizację asysty technicznej i uzyskaniu przez Wykonawcę potwierdzenia ich wykonania przez Zamawiającego, wykonawca przedstawi dokument - Raport z asysty technicznej, zawierający co najmniej:
    a. opis wykonanych prac,
    b. liczbę godzin poświęconych na wykonanie prac,
    c. całkowitą liczbę godzin asysty zrealizowanych w ciągu trwania asysty, których realizacja została potwierdzona przez Zamawiającego.
13. Wykonawca ma prawo odmówić wykonania asysty technicznej o ile:
    a. Zamawiający wyczerpał przysługujący limit roboczogodzin lub zakończył się okres realizacji asysty technicznej,

b. realizacja asysty w zaproponowanym zakresie spowodowałaby przekroczenie przysługującego Zamawiającemu limitu roboczogodzin asysty,

c. realizacja usług asysty wymagałaby złamania obowiązującego prawa.

14. Zamawiający umożliwi Wykonawcy realizację usługi asysty technicznej poprzez udostępnienie wymaganych zasobów technicznych oraz niezbędnych pracowników Zamawiającego.
15. W przypadku konieczności zmiany dokumentacji w wyniku wykonania usług asysty technicznej Wykonawca zobowiązany jest doręczyć zaktualizowaną dokumentację maksymalnie w dwa tygodnie po dostarczeniu przez wykonawcę Raportu z asysty.

11 Dokumentacja powdrożeniowa

W ramach poniższego rozdziału przedstawiono opis dokumentacji powdrożeniowej, która musi zostać przekazana przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia. Dokumentacja powdrożeniowa składa się z dokumentacji administratora oraz dokumentacji powykonawczej.

11.1 Dokumentacja administratora

Dokumentacja administratora powinna zawierać co najmniej:

- instrukcję instalacji, konfiguracji i administracji dostarczonego oprogramowania,
- opis konfiguracji dostarczonego sprzętu i oprogramowania w momencie odbioru jakościowego dostarczonej infrastruktury,
- dokumentację konfiguracji i parametryzacji,
- procedury konfiguracji.

11.2 Dokumentacja powykonawcza

Dokumentacja powykonawcza powinna zawierać co najmniej:

- Projekt techniczny zawierający:
  - Zestawienie sprzętu IT,
  - Zestawienie oprogramowania,
  - Schemat logiczny urządzeń oraz połączeń po między nimi,
  - Opis architektury technologicznej:
    - Metoda opisu,
    - Oprogramowanie aplikacyjne,
    - Infrastruktura oprogramowania,

- Logiczna infrastruktura sprzętowa:
  - Model infrastruktury maszyn logicznych,
  - Model logicznych woluminów danych,
- Opis infrastruktury wirtualizacyjnej,
- Opis fizycznej infrastruktury sprzętowej,
- Opis infrastruktury sieciowej.

- Dokumentacja utrzymaniowa, uwzględniająca m.in.:
  - Sposób monitorowania Systemu;
  - Awarie Systemu:
- Procedury administracyjne – związane z bieżącą eksploatacją.
- Dokumentacja instalacji, uwzględniająca m.in.
  - Schemat logiczny Systemu;
  - Konfigurację Systemu;
- Dokumentacja administratora zawierająca m.in.:
  - Instrukcje dotyczące instalacji;
  - Instrukcje dotyczące konfiguracji;
  - Instrukcje dotyczące administracji;
  - Opis zastosowanej konfiguracji i parametryzacji.

12 Szkolenia

W ramach realizacji Przedmiotu Zamówienia Wykonawca zobowiązany będzie do przeprowadzenia dla Zamawiającego warsztatów i szkoleń z zakresu obsługi dostarczonego sprzętu i oprogramowania. Uczestnikami warsztatów będą osoby wskazane przez Zamawiającego, szczegółowy zakres i harmonogram warsztatów i szkoleń zostanie uzgodniony z Zamawiającym po podpisaniu Umowy.

Wykonawca przeprowadzi warsztaty wdrożeniowe dla każdego wdrożonego obszaru urządzeń i systemów informatycznych w szczególności:

a. Przełączniki sieciowe
b. Urządzenia filtrujące (UTM, NGFW)
c. Macierze
d. Serwery
e. Środowisko Wirtualizacji
f. System Backupu wraz z urządzeniem archiwizującym dane

Warsztat w swoim zakresie ma za zadanie przekazanie informacji o konfiguracji końcowej urządzeń i systemów, podstawowych zmianach, które można wykonać w ramach wdrożenia, elementy utrzymania na które należy zwrócić uwagę oraz monitorowanie ciągłości pracy i bezpieczeństwa

rozwiązania. Dodatkowo Wykonawca zapewni do każdego z urządzeń dokumentację techniczną specyfikującą jego parametry ze wskazaniem modelu danych i finalnym elementami urządzenia lub wersjami licencji oprogramowania oraz dokumentację administracyjną urządzenia wskazującą na możliwe konfiguracje urządzenia poprzez środowiska graficzne lub CLI. Warsztaty odbywały się będą w formie spotkań trwających od 4h-6h.

Wymagania w zakresie warsztatów:

1. Warsztaty zostaną przeprowadzone dla osób wskazanych przez Zamawiającego.
2. Szczegółowe terminy warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym nie później niż 7 dni przed planowanym rozpoczęciem.
3. Warsztaty odbędą się w miejscu zainstalowania sprzętu i oprogramowania w siedzibie Zamawiającego.
4. Warsztaty będą przeprowadzone w języku polskim.
5. Przed rozpoczęciem warsztatów Wykonawca zapewni każdemu uczestnikowi komplet materiałów:
   - Materiały mają zostać dostarczone w formie papierowej i/lub elektronicznej;
   - Materiały muszą obejmować całość zagadnień dotyczących zakresu merytorycznego warsztatów;
6. Na zakończenie warsztatów każdy uczestnik otrzyma dokument potwierdzający ich ukończenie.

Na początku każdego dnia warsztatów Wykonawca sporządzi listę obecności. Udział uczestnika w danym dniu musi zostać potwierdzony jego podpisem. Dostarczenie podpisanych listy obecności jest warunkiem odbioru warsztatów.

Dodatkowo Wykonawca przeprowadzi specjalistyczne certyfikowane szkolenia informatyczne dla administratorów z zakresu dostarczanego sprzętu i oprogramowania, co pozwoli na nabycie przez administratorów specjalistycznej wiedzy umożliwiającej bieżącą obsługę dostarczanych rozwiązań i dalszego ich utrzymania i rozwijania. Ponadto szkolenia związane z wdrażaną infrastrukturą pozwolą na pozyskanie kompetencji umożliwiających skuteczne administrowanie systemem w okresie eksploatacji, zakładane są następujące typy szkoleń:

1. Szkolenie specjalistyczne z obsługi serwerowych systemów operacyjnych - 4 osoby,
2. Szkolenie specjalistyczne z obsługi platform wirtualizacji:
   a. zarządzanie - 4 osoby
   b. optymalizacja i skalowanie – 4 osoby

Szkolenia specjalistyczne zakończą się uzyskaniem powszechnie uznawanych certyfikatów producentów potwierdzających nabycie umiejętności.

13 Terminy realizacji prac

W niniejszym rozdziale opisano terminy realizacji prac Wykonawcy. Ogólne zasady dot. terminów realizacji prac opisują co następuje:

1. Rozpoczęcie prac następuje w chwili zawarcia Umowy pomiędzy Zamawiającym a Wykonawcą.
2. Dostawa sprzętu i oprogramowania musi zostać zrealizowane do 45 dni kalendarzowych od daty podpisania Umowy.
3. Pozostałe Zadania Przedmiotu Zamówienia muszą zostać zrealizowane do 30 dni kalendarzowych od daty podpisania Protokołu Odbioru Ilościowego i nie dłużej niż do 75 dni kalendarzowych od daty podpisania Umowy oraz nie później niż do 30.10.2020r.
4. Okres czasu świadczenia przez Wykonawcę usług asysty technicznej wynosi do 12 miesięcy od daty podpisania Protokołu Odbioru Przedmiotu Zamówienia bez zastrzeżeń.

Tabela 19. Harmonogram realizacji prac.

<table>
<tr><th>Lp.</th><th>Zadanie</th><th>Forma potwierdzenia realizacji Zadania</th><th>Termin zakończenia Zadania</th></tr>
<tr><td>1</td><td>Dostawa sprzętu i oprogramowania</td><td>Odbiór ilościowy. Podpisanie Protokołu Odbioru Ilościowego całości sprzętu i oprogramowania według wzoru z Załącznika nr 1.</td><td>Do 45 dni kalendarzowych od daty podpisania Umowy.</td></tr>
<tr><td>2</td><td>Instalacja i konfiguracja sprzętu</td><td>Telefoniczne lub mailowe potwierdzenie przez Wykonawcę zakończenia wszystkich prac instalacyjnych i konfiguracyjnych.</td><td rowspan="6">Do 30 dni kalendarzowych od daty podpisania Protokołu Odbioru Ilościowego. Nie dłużej niż 75 dni kalendarzowych od daty podpisania Umowy. Nie później niż do 30.10.2020</td></tr>
<tr><td>3</td><td>Przeprowadzenie testów akceptacyjnych</td><td>Odbiór jakościowy. Podpisanie Protokołu Odbioru Jakościowego sprzętu i oprogramowania według wzoru z Załącznika nr 2.</td></tr>
<tr><td>4</td><td>Dostarczenie dokumentacji powdrożeniowej</td><td>Podpisanie Protokołu Odbioru Produktu według wzoru z Załącznika nr 4.</td></tr>
<tr><td>5</td><td>Przeprowadzenie szkoleń administratorów</td><td>Podpisanie Protokołu Odbioru Produktu według wzoru z Załącznika nr 4.</td></tr>
<tr><td colspan="3">Podpisanie Protokołu Odbioru Przedmiotu Zamówienia według wzoru z Załącznika nr 5.</td></tr>
<tr><td>6</td><td>Usługi asysty technicznej</td><td>Dostarczanie Zamawiającemu Raportów z asysty.</td><td>Osiągnięcie limitu puli roboczogodzin lub zakończenie okresu 12 miesięcy od daty podpisania Protokołu Odbioru Przedmiotu Zamówienia.</td></tr>
</table>

14 Procedury weryfikacji i odbioru

Procedurom weryfikacji i odbioru podlegają następujące typy Produktów:

- Sprzęt i oprogramowanie (wraz z przeprowadzonymi pracami instalacyjnymi i konfiguracyjnymi),
- Dokumentacja powdrożeniowa,
- Szkolenia administratorów.

Dla każdego z wymienionych wyżej typów Produktów, w ramach realizacji Przedmiotu Zamówienia stosowana będzie osobna procedura odbioru. Wykonawca zobowiązany jest do realizacji zadań i dostarczania Produktów Zamawiającemu według harmonogramu opisanego w rozdziale 13 Terminy realizacji prac.

Po zatwierdzeniu i odbiorze wszystkich Produktów, procedurze odbioru podlega cały Przedmiot Zamówienia.

14.1 Odbiór sprzętu i oprogramowania wraz z instalacją i konfiguracją

Odbiór dostawy sprzętu i oprogramowania wraz z przeprowadzonymi pracami instalacyjnymi i konfiguracyjnymi zostanie zrealizowany zgodnie z poniższą procedurą i warunkami:

1. Wykonawca zobowiązany jest przed przeprowadzeniem dostawy powiadomić (pisemnie lub poprzez wiadomość e-mail) Zamawiającego o planowanej dostawie (lub jej części), na co najmniej 2 dni robocze przed jej przeprowadzeniem.
2. Wykonawca zobowiązany jest przeprowadzić dostawę przedmiotu dostawy w godzinach uzgodnionych z Zamawiającym.
3. Po dostarczeniu przez Wykonawcę sprzętu oraz oprogramowania Strony podpisują Protokół Odbioru Ilościowego stanowiący **Załącznik nr 1 do SOPZ**. Celem podpisania Protokołu jest potwierdzenie faktycznej ilości sztuk dostarczonej infrastruktury sprzętowej oraz oprogramowania.
4. Wykonawca opracowuje Plan testów akceptacyjnych zawierający co najmniej:
    a. Harmonogram testów akceptacyjnych.
    b. Wykorzystywane procedury testowe (np. procedura przygotowania do rozpoczęcia testów, weryfikacji środowisk, realizacji testów, obsługi błędów i raportowania prac).
    c. Zestawienie sprzętu i oprogramowania podlegającego testom.
    d. Opis środowiska testowego.
    e. Przypadki testowe odpowiadające wymaganiom na sprzęt i oprogramowanie (i uwzględniające m.in. mechanizmy redundancji).

f. Sposób weryfikacji każdego z przypadków testowych.

g. Warunki wstępne i oczekiwany efekt każdego z przypadków testowych.

Plan testów akceptacyjnych musi zostać uzgodniony z Zamawiającym. Zamawiający zastrzega sobie prawo do rozszerzenia przypadków testowych o dowolnie inne, adekwatne wymagania wskazane w SOPZ.

5. Wykonawca przeprowadza instalację i konfigurację dostarczonego sprzętu i oprogramowania na miejscu u Zamawiającego w godzinach uzgodnionych z Zamawiającym.
6. Po zakończeniu prac związanych z instalacją i konfiguracją Wykonawca poinformuje o tym Zamawiającego.
7. Wykonawca w obecności Zamawiającego przeprowadzi testy akceptacyjne zgodnie z przygotowanym przez Wykonawcę Planem testów akceptacyjnych. Protokoły z przeprowadzonych testów muszą zawierać oczekiwane rezultaty oraz wyniki wszystkich testów zawartych w Planie testów akceptacyjnych. Zamawiający zastrzega sobie prawo do samodzielnej weryfikacji dostarczanego sprzętu i oprogramowania o przypadki testowe nieujęte w Planie testów akceptacyjnych, a realizujące wymagania zawarte w ramach SOPZ. Przeprowadzenie testów z wynikiem pozytywnym jest warunkiem odbioru jakościowego dostarczanego sprzętu i oprogramowania wraz z pracami instalacyjnymi i konfiguracyjnymi.
8. Po pozytywnym przeprowadzeniu testów Strony podpisują Protokół Odbioru Jakościowego stanowiący **Załącznik nr 2.** Celem podpisania Protokołu jest potwierdzenie spełnienia przez dostarczany sprzęt i oprogramowanie parametrów technicznych i jakościowych nie gorszych niż wskazane w SOPZ oraz w Formularzu ofertowym, a także spełnienie wymagań dot. konfiguracji i instalacji.
9. W przypadku uzasadnionych uwag do realizacji prac Zamawiający ma prawo odmówić dokonania odbioru. W takim przypadku Wykonawca będzie zobowiązany do ponownego przeprowadzenia prac zgodnie z punktami 5-8 opisanymi niniejszą procedurą.

14.2 Odbiór dokumentacji powdrożeniowej

Dokumentacja powdrożeniowa zgłoszona do odbioru zostanie poddana weryfikacji przez Zamawiającego, zgodnie z opisaną poniżej procedurą:

1. Wykonawca przekazuje dokumentację do odbioru Zamawiającemu wraz z Protokołem Przekazania Produktu stanowiącym **Załącznik nr 3 do SOPZ** w godzinach pracy i w siedzibie Zamawiającego.
2. Zamawiający zapoznaje się z dostarczoną dokumentacją w czasie nie dłuższym niż 2 dni robocze. Jeśli Zamawiający nie zgłasza uwag, to następuje podpisanie Protokołu Odbioru Produktu stanowiącego **Załącznik nr 4 do SOPZ** i tym samym zakończenie procedury odbioru dokumentacji. W przeciwnym wypadku Zamawiający rejestruje uwagi i przekazuje je Wykonawcy.
3. W uzgodnionym z Zamawiającym terminie Wykonawca może zorganizować spotkanie w celu omówienia uwag Zamawiającego.
4. Wykonawca przekazuje w uzgodnionym terminie poprawioną o wskazane przez Zamawiającego uwagi Dokumentację do odbioru Zamawiającego.
5. Jeżeli Zamawiający ponownie zgłosi uwagi do produktu następuje przejście procedury do kroku „3". Jeżeli produkt spełnia wymogi, następuje podpisanie Protokołu Odbioru Produktu i procedura odbioru zostaje zakończona.

Dokumentacja powdrożeniowa będzie dostarczana Zamawiającemu w wersji elektronicznej i papierowej.

14.3 Odbiór szkoleń

Odbiór szkoleń zostanie przeprowadzony zgodnie z poniższą procedurą:

1. Wykonawca przeprowadza szkolenia administratorów wskazanych przez Zamawiającego na warunkach określonych w rozdziale 12 Szkolenia
2. Wykonawca dostarcza Zamawiającemu podpisaną przed uczestników warsztatów listę obecności wraz z jednym z egzemplarzy materiałów warsztatowych oraz Protokołem Przekazania Produktu stanowiącym **Załącznik nr 3 do SOPZ** w godzinach pracy i w siedzibie Zamawiającego.
3. Jeśli Zamawiający nie zgłasza uwag, to następuje podpisanie Protokołu Odbioru Produktu stanowiącego **Załącznik nr 4 do SOPZ** i tym samym zakończenie procedury odbioru warsztatów. W przeciwnym wypadku Zamawiający rejestruje uwagi i przekazuje je Wykonawcy.
4. W uzgodnionym z Zamawiającym terminie Wykonawca może zorganizować spotkanie w celu omówienia uwag Zamawiającego.

5. Wykonawca przekazuje w uzgodnionym terminie poprawione o wskazane przez Zamawiającego uwagi produkty warsztatów do odbioru Zamawiającego.
6. Jeżeli Zamawiający ponownie zgłosi uwagi do produktu następuje przejście procedury do kroku „4". Jeżeli produkt spełnia wymogi następuje podpisanie Protokołu Odbioru Produktu i procedura odbioru zostaje zakończona.

Produkty warsztatów będą dostarczone Zamawiającemu w wersji elektronicznej i papierowej.

14.4 Odbiór Przedmiotu Zamówienia

Procedura odbioru Przedmiotu Zamówienia będzie rozpoczęta wyłącznie w sytuacji, w której zostały odebrane wszystkie Produkty przewidziane do realizacji w ramach Przedmiotu Zamówienia (oprócz godzin asysty technicznej przewidzianej do realizacji po podpisaniu Protokołu Odbioru Przedmiotu Zamówienia). Procedura odbioru Przedmiotu Zamówienia przebiega następująco:

1. Wykonawca przedkłada Zamawiającemu Protokół Odbioru Przedmiotu Zamówienia stanowiący **Załącznik nr 5 do SOPZ**.
2. W przypadku akceptacji realizacji Przedmiotu Zamówienia podpisywany jest Protokół Odbioru Przedmiotu Zamówienia.
3. Podpisanie Protokołu Odbioru Przedmiotu Zamówienia jest równoznaczne z rozpoczęciem okresu świadczenia przez Wykonawcę usług asysty technicznej.

15 Dodatkowe zobowiązania Wykonawcy

Dodatkowe zobowiązania Wykonawcy niewskazane gdzie indziej:

1. Wszelkie działania Wykonawcy w ramach realizacji przedmiotu zamówienia będą oparte o uznane standardy i metodyki wykorzystywane w danym obszarze m.in. ITIL 2011 Edition. Wykonawca będzie realizował Przedmiot Zamówienia z najwyższą starannością, efektywnością oraz zgodnie z najlepszą praktyką i wiedzą zawodową.
2. Wykonawca zobowiązany jest zrealizować Przedmiot Zamówienia w terminach określonych w SIWZ.
3. Wykonawca zobowiązany jest dokonać z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na Przedmiot Zamówienia.
4. Wykonawca będzie zobowiązany, w trakcie realizacji umowy, stosować się do wytycznych bezpieczeństwa systemów IT oraz do wytycznych bezpieczeństwa stosowanych u Zamawiającego. Wytyczne zostaną przekazane po podpisaniu Umowy.

5. Wykonawca będzie współpracował z Zamawiającym na każdym etapie wykonywania Przedmiotu Zamówienia w ramach realizacji Zamówienia.
6. Wykonawca będzie udzielał Zamawiającemu każdorazowo na wniosek Zamawiającego, pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
7. Wykonawca będzie współdziałał z osobami wskazanymi przez Zamawiającego.
8. Wszelkie dane i informacje wytwarzane przez Wykonawcę i utrzymywane w ramach realizacji Przedmiotu Zamówienia są własnością Zamawiającego. Wykonawca zobowiązany jest do przekazania Zamawiającemu wszystkich danych i informacji oraz dokumentów wytwarzanych i gromadzonych w ramach realizacji przedmiotu zamówienia po zakończeniu Umowy. Wykonawca jest zobowiązany do zachowania poufności wszystkich danych i informacji, w których posiadanie wejdzie podczas realizacji przedmiotu Umowy.

16 Dodatkowe zobowiązania Zamawiającego

Dodatkowe zobowiązania Zamawiającego niewskazane gdzie indziej:

1. Udostępnienie dokumentów, materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, niezbędnych do realizacji Przedmiotu Zamówienia.
2. Udzielanie Wykonawcy na bieżąco niezbędnych do realizacji Przedmiotu Zamówienia wyjaśnień oraz przekazywania niezbędnych informacji.
3. Umożliwienie Wykonawcy dostępu do posiadanych przez Zamawiającego obiektów, sprzętu, oprogramowania oraz dokumentacji, niezbędnych do realizacji Przedmiotu Zamówienia, zgodnie z wewnętrznymi regulacjami Zamawiającego w zakresie bezpieczeństwa.

17 Załączniki

Załącznik nr 1 – Protokół Odbioru Ilościowego

Załącznik nr 2 – Protokół Odbioru Jakościowego

Załącznik nr 3 – Protokół Przekazania Produktu

Załącznik nr 4 – Protokół Odbioru Produktu

Załącznik nr 5 – Protokół Odbioru Przedmiotu Zamówienia