Załącznik nr 1 do SWZ

Szczegółowy opis Przedmiotu Zamówienia,

opis parametrów technicznych

i dodatkowych wymagań Zamawiającego

SPIS TREŚCI

[1. PRZEDMIOT ZAMÓWIENIA 4](#_Toc63076980)

[1.1. Przedmiotem Zamówienia jest: 4](#_Toc63076981)

[1.2. Ogólne wymagania dla Przedmiotu Zamówienia: 4](#_Toc63076982)

[2. WARUNKI WDROŻENIA I FAZY RELIZACYJNEJ 5](#_Toc63076983)

[3. DOKUMENTACJA POWYKONAWCZA 5](#_Toc63076984)

[4. OGÓLNE WYMAGANIA DLA STOSOWANYCH PRODUKTÓW 5](#_Toc63076985)

[5. SZKOLENIA 6](#_Toc63076986)

[6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE 6](#_Toc63076987)

[6.1. Definicje 7](#_Toc63076988)

[6.2. Klasyfikacja incydentów 8](#_Toc63076989)

[6.3. Zgłaszanie incydentów 8](#_Toc63076990)

[6.4. Rodzaje usług 9](#_Toc63076991)

[6.5. Parametry i warunki świadczenia usług 10](#_Toc63076992)

[6.5.1. Usługi reaktywne 10](#_Toc63076993)

[6.5.2. Usługi proaktywne 11](#_Toc63076994)

[6.5.3. Usługi dodatkowe 11](#_Toc63076995)

[7. WYMAGANIA DLA OBSZARÓW 11](#_Toc63076996)

[7.1. Zestawienie Podsystemów i obszarów Systemu objętego postępowaniem – stan do grudzień 2020 r. 11](#_Toc63076997)

[7.2. Sieć szkieletowa [I\_NET] 12](#_Toc63076998)

[7.2.1. Przełączniki rdzeniowe [I\_NET-SW\_CORE] - efekt Dialogu Technicznego 13](#_Toc63076999)

[7.2.2. Bramy/routery dostępowe/brzegowe [I\_NET-GW] 15](#_Toc63077000)

[7.2.3. System zarządzania adresami IP [I\_NET-CNS\_IPAM] 15](#_Toc63077001)

[7.2.4. Przełączniki dostępowe [I\_NET-SW-ACC] 18](#_Toc63077002)

[7.2.5. Centralne zapory sieciowe [I\_NET-FW\_CORE] 21](#_Toc63077003)

[7.2.6. Zapory sieciowe [I\_NET-FW] 21](#_Toc63077004)

[7.2.7. Szkolenia 24](#_Toc63077005)

[7.2.7.1. Szkolenia autoryzowane 24](#_Toc63077006)

[7.2.7.2. Szkolenia autorskie 25](#_Toc63077007)

[7.3. Sieć bezprzewodowa [I\_WIFI] 25](#_Toc63077008)

[7.3.1. System zarządzania siecią WIFI [I\_WIFI-CTRL] 25](#_Toc63077009)

[7.3.2. Nowe urządzenia 25](#_Toc63077010)

[7.3.3. Szkolenia 26](#_Toc63077011)

[7.3.3.1. Szkolenia autoryzowane 26](#_Toc63077012)

[7.3.3.2. Szkolenia autorskie 26](#_Toc63077013)

[7.4. Bezpieczeństwo informacji [I\_SEC] 26](#_Toc63077014)

[7.4.1. System zdalnego dostępu VPN SSL [I\_SEC-VPN\_SSL] 26](#_Toc63077015)

[7.4.2. Zewnętrzne zapory sieciowe [I\_SEC-FW\_EXT] 27](#_Toc63077016)

[Next Generation Firewall – klaster (2 urządzenia) 27](#_Toc63077017)

[Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. 27](#_Toc63077018)

[7.4.3. System filtrowania treści i ochrony ruchu SMTP [I\_SEC-CF\_MAIL] 27](#_Toc63077019)

[7.4.4. System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem [I\_SEC-SIEM] 28](#_Toc63077020)

[7.4.5. System uwierzytelniania administratorów [I\_SEC-ADM\_AUTH] 28](#_Toc63077021)

[7.4.6. Szkolenia 28](#_Toc63077022)

[7.4.6.1. Szkolenie przez certyfikowanych inżynierów wykonawcy 28](#_Toc63077023)

[7.4.6.2. Szkolenia autorskie 28](#_Toc63077024)

[7.5. Zintegrowany system łączności [I\_UC] 29](#_Toc63077025)

[7.5.1. Bramy głosowe [I\_UC-VG] 29](#_Toc63077026)

[7.6. Środowisko przetwarzania danych [I\_CPD] 29](#_Toc63077027)

[7.6.1. Obudowy serwerów kasetowych - chassis [I\_CPD-BLD\_CHASS] 29](#_Toc63077028)

[7.6.2. Przełączniki Fibre Channel sieci SAN [I\_CPD-SW\_FC] 30](#_Toc63077029)

[7.6.3. Macierz dyskowa [I\_CPD-DA] 31](#_Toc63077030)

[7.6.4. Biblioteka taśmowa [I\_CPD-TL] 31](#_Toc63077031)

[7.6.5. System kopii zapasowych - oprogramowanie [I\_CPD-BKP\_SRV] 32](#_Toc63077032)

[7.6.6. System wirtualizacji [I\_CPD-VRT] 34](#_Toc63077033)

[7.6.6.1. Szkolenia autorskie 35](#_Toc63077034)

[7.7. Zarządzanie infrastrukturą teleinformatyczną [I\_MGMT] 35](#_Toc63077035)

[7.7.1. Konsole administratorskie do zdalnego zarządzania podsystemami infrastruktury teleinformatycznej [I\_MGMT-NMS] 35](#_Toc63077036)

1. PRZEDMIOT ZAMÓWIENIA

Wspierana i aktualizowana w ramach Przedmiotu Zamówienia infrastruktura teleinformatyczna nazywana będzie dalej w dokumencie Systemem, a poszczególne części Przedmiotu Zamówienia nazywane Obszarami (w ich skład wchodzą poszczególne Podsystemy) oznaczane będą kodami/mnemonikami:

|  |  |
| --- | --- |
| **Kod / mnemonik** | **Obszar** |
| I\_NET | sieć szkieletowa |
| I\_WIFI | sieci bezprzewodowa |
| I\_SEC | bezpieczeństwo sieci i zasobów teleinformatycznych |
| I\_UC | system łączności |
| I\_CPD | Centrum Przetwarzania Danych |

* 1. Przedmiotem Zamówienia jest:
1. Przedłużenie gwarancji i wsparcia producenta wskazanych Podsystemów na 36 miesięcy od momentu podpisania umowy.
2. Wdrożenie rozwiązań zastępczych dla wskazanych, opisanych w dalszej części przedmiotu zamówienia, Podsystemów wraz z gwarancją i wsparciem producenta na 36 miesięcy.
3. Przygotowanie dokumentacji powykonawczej uwzględniającej konfigurację, procedury (między innymi: dostępu, konfiguracji, tworzenia kopii zapasowych i odzyskiwania z nich danych) hasła itp. nowych podsystemów.
4. Gwarancja i wsparcie wykonawcy na System 36 miesięcy od momentu podpisania umowy.
5. Szkolenie personelu IT.
	1. Ogólne wymagania dla Przedmiotu Zamówienia:
6. Dla opisanego w ramach Przedmiotu Zamówienia Systemu wymagane jest zapewnienie przez Wykonawcę gwarancji i opieki technicznej (serwisu i wsparcia technicznego) przez cały okres trwania umowy Usługi gwarancyjne, opieka techniczna oraz szkolenia muszą być świadczone w języku polskim.
7. W przypadku nowych Podsystemów Wykonawca musi uwzględnić w kosztach realizacji:
	1. Dostawę, montaż, instalację, podłączenie, uruchomienie dostarczanych urządzeń wraz z niezbędnym osprzętem, a w szczególności: akcesoriami, osprzętem montażowo-instalacyjnym (stelaże, kable przyłączeniowe i zasilające, przewody, patchcordy, przejściówki, opaski, itp),
	2. W przypadku rozwiązań wirtualnych, opisanych w dalszej części przedmiotu zamówienia, koszty urządzeń oraz licencji związanych z wirtualizacją wdrażanych Podsystemów.
	3. Wszystkie dodatkowe licencje dotyczące uruchomienia i działania Podsystemu – w tym te na współpracujących urządzeniach/Podsystemach,
	4. Zaimplementowanie ustawień i polityk z dotychczasowych podsystemów, które zastąpią nowe podsystemy.
	5. Konfigurację i integrację z innymi powiązanymi Podsystemami Zamawiającego.
	6. Zapewnienie szkoleń personelu IT Zamawiającego (szczegółowe wymagania w tym zakresie opisane są w dalszej części niniejszego dokumentu).
8. Wszystkie dostarczone urządzenia i systemy muszą być: nowe, posiadać gwarancję producenta, zamontowane, zainstalowane, skonfigurowane i uruchomione zgodnie z wymaganiami niniejszej specyfikacji, ofertą i dokumentacją projektowo-wykonawczą. Wszystkie dostarczone produkty muszą być wyposażone we wszystkie niezbędne komponenty, podzespoły i licencje.
9. WARUNKI WDROŻENIA I FAZY RELIZACYJNEJ

Warunki wdrożenia i fazy realizacyjnej:

1. Zamawiający przewiduje etapową realizację prac z odbiorami po uruchomieniu każdego Podsystemu.
2. Wdrożenie nowego Podsystemu powiązane być musi z integracją z Podsystemami, z którymi współpracował dotychczasowy Podsystem i z przeniesieniem dotychczasowych konfiguracji, ustawień, polityk itp.
3. Wykonawca zobowiązany jest do przedstawienia niezwłocznie po podpisaniu umowy planowanego harmonogramu prac i planu migracji do nowych podsystemów, aby:
	1. Przewidywać możliwość równoległej realizacji zadań w kilku lokalizacjach i/lub obszarach.
	2. Zapewnić w maksymalnym stopniu ciągłość działalności statutowej Zamawiającego.
	3. Minimalizować uciążliwość prac poprzez wcześniejsze uzgadnianie z Zamawiającym terminów (dni, godzin) ich realizacji (w ramach przyjętego harmonogramu).

Harmonogram musi zostać zatwierdzony przez Zamawiającego.

1. Inżynierowie wykonujący prace wdrożeniowe muszą posiadać odpowiednie kwalifikacje potwierdzone certyfikatami producentów instalowanych produktów.
2. Wykonawca zobowiązany jest do oznaczenia zainstalowanych urządzeń i połączeń za pomocą etykiet z kodami przyjętymi przez Zamawiającego.
3. Miejsca (pomieszczenia) wykonywania prac muszą zostać uporządkowane i przywrócone do stanu nie gorszego niż przed ich rozpoczęciem
4. Odbiory po zakończeniu każdego z etapów i odbiór końcowy przeprowadzone będą po wykonaniu testów akceptacyjnych i zakończeniu ich pozytywnym wynikiem, potwierdzane każdorazowo, obustronnie podpisanym bezusterkowym protokołem odbioru.
5. DOKUMENTACJA POWYKONAWCZA

Wymagania dotyczące dokumentacji powykonawczej:

1. Dokumentacja powykonawcza dotycząca nowych systemów powinna zawierać dokładny opis Podsystemu oraz niezbędne schematy i instrukcje - ostateczne wersje (wraz z komentarzami) plików konfiguracyjnych urządzeń i oprogramowania.
2. Kody na opisach i schematach w dokumentacji powykonawczej muszą być zgodne z faktycznymi oznaczeniami na etykietach urządzeń i połączeń.
3. W trakcie odbioru końcowego Wykonawca przekaże Zamawiającemu 1 egzemplarz dokumentacji powykonawczej w wersji papierowej i 1 egzemplarz w wersji elektronicznej.
4. OGÓLNE WYMAGANIA DLA STOSOWANYCH PRODUKTÓW

Ogólne wymagania Zamawiającego dla stosowanych produktów o ile wymagania szczegółowe dla produktów opisanych w dalszej części dokumentu nie stanowią inaczej:

1. Wymagane jest, aby dostarczany sprzęt był fabrycznie nowy, kompletny i pochodził z legalnego kanału sprzedaży.
2. Wymagane jest aby dostarczany sprzęt był wyprodukowany nie wcześniej niż 6 miesięcy przed dniem zawarcia Umowy dotyczącej Przedmiotu Zamówienia.
3. Urządzenia muszą posiadać tylko oryginalne komponenty i nie dopuszcza się stosowania zamienników. Wyjątkiem jest sytuacja, w której stosowanie zamienników jest dopuszczone przez producenta i nie wpływa na obsługę serwisową urządzeń – w takim przypadku przed podpisaniem umowy wykonawca zobowiązany jest dostarczyć oświadczenie podpisane przez producenta, który wskazuje jakie elementy zamienne są dopuszczalne do użycia bez wpływu na obsługę serwisową w autoryzowanym kanale serwisowym. Oświadczenie musi być sporządzone w oryginale bądź w postaci kopii potwierdzonej za zgodność z oryginałem przez Wykonawcę.
4. Wymagane jest zastosowanie redundantnego (co najmniej w układzie 1:1) zasilania i wentylacji/chłodzenia we wszystkich urządzeniach posiadających taką opcję.
5. W przypadku licencji ograniczonych w czasie wymagane jest zapewnienie ich co najmniej na czas taki, jak oferowany okres serwisu zgodnie z wybranymi przez Wykonawcę warunkami opisanymi w podrozdziale „Warunki serwisu, gwarancji, wsparcia technicznego” rozdziału „Kryteria oceny ofert”.
6. SZKOLENIA

Dla każdego z wdrożonych nowych Podsystemów Wykonawca zapewni dwa rodzaje szkoleń:

1. autoryzowane – realizowane przez autoryzowane centrum szkoleniowe danego producenta
2. autorskie – w formie instruktaży/warsztatów przeprowadzanych w trakcie wdrożenia przez Wykonawcę (mogą być zrealizowane w oparciu o sprzęt i oprogramowanie dostarczone w ramach zamówienia)

przy czym:

1. szkolenia muszą być przeprowadzone, w języku polskim;
2. dla osób biorących udział w szkoleniu zostaną zapewnione materiały szkoleniowe w formie drukowanej i elektronicznej, w języku polskim;
3. w przypadku szkoleń odbywających się w siedzibie Zamawiającego oraz poza siedzibą Zamawiającego wszelkie koszty związane ze szkoleniem pokrywa Wykonawca;
4. zakresy (tematyka) szkoleń autoryzowanych i liczba biorących w nich udział osób opisane są w rozdziałach dotyczących poszczególnych obszarów;
5. liczba osób objętych szkoleniami autorskimi nie powinna być mniejsza od 6, a wymagane czasy ich trwania opisane są w rozdziałach dotyczących poszczególnych obszarów;
6. szczegółowy harmonogram szkoleń zostanie ustalony z wykonawcą wybranym do realizacji zamówienia niezwłocznie po podpisaniu umowy, przy czym szkolenie autorskie powinno być zrealizowane nie później niż 1 miesiąc po uruchomieniu danego Podsystemu, szkolenie autoryzowane zaś przynajmniej 3 miesiące po uruchomieniu Podsystemu, ale nie później niż po 6 miesiącach.
7. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE
8. Gwarancje i serwisy producenta muszą być dostarczone w postaci subskrypcji rejestrowanych bezpośrednio na Zamawiającego i umożliwiać:
	1. Możliwość zakładania zgłoszeń serwisowych bezpośrednio u producenta;
	2. Bezpośredni dostęp do bazy wiedzy i pomocy technicznej TAC producenta Możliwość bezpośredniego pobierania aktualizacji oprogramowania z bazy producenta;
	3. Możliwość monitorowania statusu zgłoszeń w systemie producenta;
	4. Możliwość korzystania z serwisu producenta nawet w przypadku, gdy Wykonawca utraci autoryzację producenta lub nie będzie zdolny do świadczenia serwisu;
9. W przypadku dostarczania innej formy serwisu należy przed podpisaniem umowy dostarczyć oświadczenie producenta potwierdzające, iż przejmuje on wszelkie obowiązki dotyczące świadczenia serwisu w przypadku niewywiązywania się Wykonawcy z zakresu umowy dotyczącego danego producenta.
10. Dla produktów które mają być objęte przedłużeniem gwarancji na powyższych warunkach Wykonawca w terminie do 30 dni od daty podpisania umowy dostarczy dokument potwierdzający wykupienie u producenta gwarancji uprawniające Zamawiającego do korzystania z gwarancji oraz ze wsparcia technicznego na minimum 36 miesięcy. W przypadku stwierdzenia po upływie 30 dni braku tego dokumentu, Zamawiający naliczy karę umowną oraz będzie przysługiwało mu prawo odstąpienia od umowy.
11. Dobór odpowiedniego pakietu serwisowego producenta leży w gestii Wykonawcy. Zamawiający dopuszcza aby serwisy producentów posiadały mniej restrykcyjny czas usuwania awarii, pod warunkiem iż Wykonawca zapewni usuwanie awarii na warunkach określonych w SIWZ. Zamawiający wymaga aby okres serwisu pokrywał się z czasem trwania umowy.
12. Usługi serwisu, gwarancji i wsparcia technicznego muszą być świadczone w języku polskim.

* 1. Definicje

**Incydent** – sytuacja, w której Zamawiający powinien skontaktować się z Wykonawcą w celu uzyskania pomocy w rozwiązaniu zaistniałego problemu.

**Zgłoszenie serwisowe** – powiadomienie Wykonawcy o wystąpieniu incydentu.

**Gotowość serwisowa** – czas (dni, godziny), w którym Wykonawca przyjmuje i rejestruje zgłoszenia serwisowe.

**Czas reakcji** – czas pomiędzy dokonaniem zgłoszenia serwisowego przez Zamawiającego, a momentem rozpoczęcia przez Wykonawcę prac nad usuwaniem problemu będącego przyczyną incydentu.

**Czas naprawy** – czas od chwili dokonania zgłoszenia serwisowego przez Zamawiającego do chwili usunięcia problemu będącego przyczyną incydentu.

**Okres serwisu** – czas świadczenia usług serwisu, gwarancji i wsparcia technicznego

 Wykonawcy i Producenta liczony od dnia obioru końcowego.

**Rozwiązanie tymczasowe** – dokonana przez Wykonawcę zmiana konfiguracji urządzenia i/lub oprogramowania, i/lub stworzenie procedury, i/lub wykonanie określonych czynności mających doprowadzić do przywrócenia działania Systemu i/lub uszkodzonej jego części i/lub funkcji, w zakresie umożliwiającym jego działanie i eksploatację do czasu usunięcia problemu będącego przyczyną incydentu.

**Błąd systemowy** – incydent, który może usunąć wyłącznie producent sprzętu i/lub oprogramowania.

* 1. Klasyfikacja incydentów

W opisie warunków świadczenia usług gwarancyjnych i serwisowych stosowana będzie następująca klasyfikacja incydentów (awarii, usterek, błędów):

|  |  |  |
| --- | --- | --- |
| **Klasy incydentów** | **Opis** | **Możliwe rodzaje incydentu** |
| A – Krytyczny | Sieć telekomunikacyjna Zamawiającego lub główne aplikacje usługowe nie funkcjonują, co ma krytyczny wpływ na działalność Zamawiającego. | System nie działa. Awaria całej sieci, przerwa w działaniu krytycznych elementów sieci lub krytycznych aplikacji. Awaria wszystkich elementów tworzących układ redundantny. Incydent skutkujący odpowiedzialnością prawną, spowodowaną niewydolnością wynikłą z niedostępności sieci lub aplikacji. Brak możliwości zastosowania rozwiązania tymczasowego. |
| B – Wysoki | Sieć lub aplikacje nie ulegają całkowitej awarii, ale skuteczność (dostępność, wydajność, bezpieczeństwo) działania sieci telekomunikacyjnej lub głównych aplikacji usługowych jest znacznie obniżona, co ma istotny wpływ na działalność Zamawiającego. | Incydent, który w znaczący sposób wpływa niekorzystnie na dostępność sieci lub aplikacji. Awaria jednego z dwu lub dwu z kilku elementów tworzących układ redundantny. Działający destrukcyjnie, powtarzający się incydent, który wywiera poważne, lecz tymczasowe skutki. Znaczące braki w wydajności. Brak możliwości natychmiastowego zastosowania rozwiązania tymczasowego. |
| C – Średni | Skuteczność (dostępność, wydajność, bezpieczeństwo) działania sieci lub aplikacji jest wyraźnie obniżona, ale większość działań przebiega nieprzerwanie lub ujawnił się błąd utrudniający działanie Systemu w zakresie pełnej funkcjonalności. | Zidentyfikowane incydenty, które ustępują bez interwencji albo mogą być skutecznie ominięte w wyniku działania Zamawiającego lub dzięki zastosowaniu rozwiązania tymczasowego. Uszkodzenie jednego z kilku elementów tworzących układ redundantny. |
| D – Niski | Skuteczność (dostępność, wydajność, bezpieczeństwo) działania sieci lub aplikacji jest nieznacznie obniżona lub użytkownicy potrzebują informacji lub pomocy, związanych z możliwościami produktu, instalacją systemu lub konfiguracją. | Incydenty nienaglące, o małym znaczeniu, zapytanie techniczne lub prośba o informacje. |

* 1. Zgłaszanie incydentów

Wykonawca zapewni następujące warunki zgłaszania incydentów poprzez prowadzenie ich rejestru:

1. Zgłoszenia serwisowe muszą być przyjmowane przez co najmniej następujące kanały: telefon, e-mail, WWW
2. Każdemu zgłoszeniu musi zostać nadany unikalny numer (identyfikator), pozwalający na jego jednoznaczną identyfikację
3. Zgłoszenie musi zawierać datę, opis incydentu wraz z jego klasyfikacją, dane osoby zgłaszającej, dane osoby prowadzącej obsługę gwarancyjną lub serwisową
4. Wykonawca zapewni Zamawiającemu dostęp do systemu śledzenia stanu obsługi zgłoszenia. Dostęp ten musi być możliwy poprzez następujące kanały komunikacyjne: telefon, e-mail, WWW
5. Lista osób upoważnionych ze strony Zamawiającego do dokonywania zgłoszeń będzie określona w załączniku do protokołu odbioru końcowego.
	1. Rodzaje usług

W ramach świadczeń gwarancyjnych i serwisowych przewiduje się następujące rodzaje usług:

|  |  |
| --- | --- |
| **Nazwa** | **Opis** |
| DIAGNOSTYKA | Zdalne diagnozowanie Systemu w przypadku zgłoszenia jego nieprawidłowej pracy.W ramach usługi wykonywane będą diagnozy incydentów, które nie trwają ciągle, nie dają się odtworzyć lub wystąpiły w przeszłości i należy zbadać powód ich wystąpienia.Wykonawca musi zapewnić dostęp do bezpłatnych narzędzi diagnostycznych producenta. |
| WSPARCIE | Wsparcie techniczne w zakresie rozwiązywania problemów związanych z funkcjonowaniem Systemu, gotowość do podjęcia działań związanych z usuwaniem awarii, błędów i/lub wymianą uszkodzonych elementów Systemu.W ramach usługi rozwiązywany będzie problem, który trwa ciągle lub daje się odtworzyć.Usługa w swoim zakresie musi obejmować zarówno działania zdalne jak i prace na miejscu. Jeśli działania zdalne nie rozwiążą problemu, interwencja jest przeprowadzana na miejscu.Usługa powinna obejmować odtworzenie środowiska w przypadku dostarczenia przez Zamawiającego kopii zapasowych plików konfiguracyjnych.W przypadku wystąpienia błędu systemowego, Wykonawca będzie współpracował z producentem błędnie działającego elementu systemu w celu jego usunięcia.Wykonawca musi zapewnić dostęp do baz wiedzy i przewodników konfiguracyjnych producenta. |
| NAPRAWA | Dostawa części zamiennych, naprawa lub wymiana uszkodzonego urządzenia, systemu lub podsystemu na urządzenie, system lub podsystem sprawny i wolny od wad przez specjalistę Wykonawcy (nie dotyczy urządzeń końcowych np. aparaty telefoniczne, punkty dostępowe, terminale wideo, monitory).Zastępowane urządzenie lub część zamienna będzie po zgłoszeniu wysłane/a do Zamawiającego.  |
| ZAMIANA | Zamiana wadliwie działających urządzeń końcowych Systemu wraz z dostawą nowych urządzeń końcowych wolnych od wad.Koszty przesyłek związanych z usługą (w obie strony) pokrywa Wykonawca.W przypadku braku możliwości zamiany, Wykonawca zobowiązuje się do dostarczenia ekwiwalentnego urządzenia.  |
| AKTUALIZACJA | Dostarczanie aktualizacji oprogramowania objętego Umową zgodnie z udzielonymi licencjami i polityką wsparcia oprogramowania przez jego producenta obejmujące nowsze wersje (upgrade) oraz poprawki (update/patch).W przypadku wystąpienia błędu systemowego oprogramowania Wykonawca opracuje obejścia zgłoszonych problemów i zgłosi problem do producenta w celu uzyskania modyfikacji oprogramowania. Przez cały okres trwania Umowy Wykonawca zapewni dostęp do dedykowanych, oferowanych przez producenta subskrypcji wymaganych do działania oprogramowania (np. sygnatury AV, IPS). |
| ASYSTA | Wsparcie telefoniczne dla administratorów Zamawiającego świadczone przez Wykonawcę w zakresie obsługi, administracji, konfiguracji oprogramowania i urządzeń dostarczonych w ramach Systemu.  |
| KONFIGURACJA  | Zdalne wykonywanie zmian w konfiguracji Systemu. |
| STROJENIE | Wykonywanie zmian w konfiguracji Systemu w siedzibie Zamawiającego.  |
| PRZEGLĄD | Okresowy przegląd polegający na zbadaniu stanu oprogramowania i stanu technicznego urządzeń, zebraniu z rejestrów i logów informacji o błędach oraz wartościach parametrów obciążenia poszczególnych elementów Systemu, analizie zebranych informacji i przeprowadzeniu korekt z niej wynikających. |
| OPTYMALIZACJA | Okresowy przegląd i monitorowanie Systemu w celu optymalizacji jego działania oraz poprawy dostępności, wydajności i bezpieczeństwa zakończony sporządzeniem raportu zawierającego diagnozy, wytyczne, zalecenia i rekomendacje w tym zakresie oraz przeprowadzenie korekt wynikających z raportu. |
| WARSZTATY | Transfer wiedzy w postaci dodatkowych warsztatów/szkoleń z zakresu zaawansowanej administracji serwisowanych technologii dla zespołu IT Zamawiającego prowadzonych przez certyfikowanych specjalistów Wykonawcy.Wspieranie zespołu IT Zamawiającego poprzez konsultacje w rozwiązywaniu pojawiających się w trakcie eksploatacji systemu problemów dotyczących złożonych zagadnień technicznych oraz w celu podniesienia stopnia dostępności, wydajności i bezpieczeństwa systemów informatycznych Zamawiającego.Tematyka warsztatów/szkoleń , konsultacji i ich terminy będą wcześniej uzgadniana pomiędzy stronami. |

***W przypadku świadczenia usług gwarancyjnych i/lub serwisowych Zamawiający nie ponosi żadnych dodatkowych kosztów, w tym związanych z dojazdem
i zakwaterowaniem pracowników Wykonawcy.***

* 1. Parametry i warunki świadczenia usług

W opisie stosowane są następujące oznaczenia:

**g** – godzina robocza tj. godzina w czasie od 8:00 do 16:00 w dni robocze liczona dla jednego specjalisty

**gz** – godzina zegarowa

**d** – dzień roboczy tj. dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy liczony dla jednego specjalisty

**dk** – dzień kalendarzowy

**t** – tydzień kalendarzowy

**m** – miesiąc kalendarzowy

**x** – ilość przez określony czas (np. 8g x 5d oznacza: po 8 godzin roboczych każdego dnia przez każde 5 dni roboczych tj. łącznie 40 godzin roboczych w ciągu 5 dni roboczych) w trakcie całego okresu serwisowego

**/** – ilość na dany okres (np. 8g / 5d oznacza: 8 godzin roboczych rozłożonych na każde 5 dni roboczych tj. łącznie 8 godzin roboczych do wykorzystania w ciągu każdych 5 dni roboczych) w trakcie całego okresu serwisowego.

* + 1. Usługi reaktywne

Wymagane są następujące parametry i warunki świadczenia usług reaktywnych tj. związanych z awariami Systemu (minimalny poziom wsparcia określony jest przy każdym Podsystemie) przez cały okres trwania umowy tj. 36 miesięcy od jej podpisania lub protokolarnego odbiory każdego podsystemu.

|  |  |  |  |
| --- | --- | --- | --- |
| **Obszary** | **Usługi reaktywne** | **Klasy incydentów** | **Warianty pakietów świadczenia usług** |
| **Parametry** | **Podstawowy** | **Rozszerzony** |
| I\_NETI\_SECI\_WIFI\*I\_UC\*I\_CPD | DIAGNOSTYKAWSPARCIENAPRAWAZAMIANAAKTUALIZACJA | A – Krytyczny | Gotowość serwisowaCzas reakcjiCzas naprawyOkres serwisu | 8g x 5d / 1t2g8g36m | 24gz x 7dk / 1t1gz6gz36m |
| B – Wysoki | Gotowość serwisowaCzas reakcjiCzas naprawyOkres serwisu | 8g x 5d / 1t2g12g36m | 24gz x 7dk / 1t1gz8gz36m |
| C – Średni | Gotowość serwisowaCzas reakcjiCzas naprawyOkres serwisu | 8g x 5d / 1t4g16g36m | 24gz x 7dk / 1t2gz12gz36m |
| D – Niski | Gotowość serwisowaCzas reakcjiCzas naprawyOkres serwisu | 8g x 5d / 1t8g48g36m | 24gz x 7dk / 1t8gz40gz36m |
| I\_WIFI\*\*I\_UC\*\* | DIAGNOSTYKAZAMIANAAKTUALIZACJA | C – Średni | Gotowość serwisowaCzas reakcjiCzas naprawyOkres serwisu | 8g x 5d / 1t12g32g36m | 24gz x 7dk / 1t8gz24gz36m |
| D – Niski | Gotowość serwisowaCzas reakcjiCzas naprawyOkres serwisu | 8g x 5d / 1t16g48g36m | 24gz x 7dk / 1t12gz32gz36m |

\*) Kontrolery, serwery

\*\*) Urządzenia terminalne tj. telefony, przystawki, punkty dostępowe, terminale wideo, monitory

* + 1. Usługi proaktywne

Wymagane są następujące parametry i warunki świadczenia usług proaktywnych tj. związanych z eksploatacją Systemu (minimalny poziom wsparcia określony jest przy każdym Podsystemie)przez cały okres trwania umowy tj. 36 miesięcy od jej podpisania lub protokolarnego odbiory każdego podsystemu.

|  |  |  |
| --- | --- | --- |
| **Obszary** | **Usługi proaktywne** | **Warianty pakietów świadczenia usług** |
| **Parametry** | **Podstawowy** | **Rozszerzony** |
| I\_NETI\_SECI\_WIFII\_UCI\_CPD | ASYSTA | Gotowość serwisowaIlośćOkres serwisu | 8g x 5d / 1t1g / 1m36m | 8g x 5d / 1t4g / 1m36m |
| WSPARCIE | Gotowość serwisowaIlośćOkres serwisu | 8g x 5d / 1t3d / 6m36m | 8g x 5d / 1t9d / 6m36m |
| KONFIGURACJA | Gotowość serwisowaIlośćOkres serwisu | 8g x 5d / 1t6g / 6m36m | 8g x 5d / 1t18g / 6m36m |
| STROJENIE | Gotowość serwisowaIlośćOkres serwisu | 8g x 5d / 1t4g / 6m36m | 8g x 5d / 1t12g / 6m36m |
| PRZEGLĄD | Gotowość serwisowaIlośćOkres serwisu | 8g x 5d / 1t2 razy w roku36m | 8g x 5d / 1t2 razy w roku36m |
| OPTYMALIZACJA | Gotowość serwisowaIlośćOkres serwisu | 8g x 5d / 1t4g / 6m36m | 8g x 5d / 1t12g / 6m36m |
| WARSZTATY | Gotowość serwisowaIlośćOkres serwisu | 8g x 5d / 1t3d / 6m36m | 8g x 5d / 1t5d / 6m36m |

Terminy i zakresy (konkretne problemy, zagadnienia, tematy) usług proaktywnych będą wcześniej (w ramach czasu gotowości) uzgadniane obustronnie z wykonawcą wybranym do realizacji zamówienia.

* + 1. Usługi dodatkowe

W przypadku gdy konieczne wsparcie ze strony Wykonawcy będzie przekraczało limity godzinowe opisane w tabeli z punktu 6.5.2. Zamawiający dopuszcza dokupienie godzin pracy serwisanta (zdalnych, lub lokalnych) zgodnie z ceną określoną przez Wykonawcę w ofercie. Zamawiający nie ponosi żadnych dodatkowych kosztów związanych z dojazdem i zakwaterowaniem pracowników Wykonawcy.

1. WYMAGANIA DLA OBSZARÓW
	1. Zestawienie Podsystemów i obszarów Systemu objętego postępowaniem – stan do grudzień 2020 r.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Kod / mnemonik | Podsystem / podobszar | Producent | Model | Nr kat. | Ilość\* |  | Minimalnie wymagany oczekiwany poziom wsparcia: |
| I\_NET |   |
| I\_NET-SW\_CORE | Przełączniki rdzeniowe typu | Juniper Networks | EX 4500 EX4200 | EX4500-40F-VC1-FB | 4 | kpl | Rozszerzony |
| I\_NET-FW\_CORE | Centralne zapory sieciowe | Fortinet | FG-1500D | FG-1500D | 2 | kpl | Rozszerzony |
| I\_NET-GW | Bramy/routery dostępowe/brzegowe | Juniper Networks | MX 80 | MX80-T-AC | 2 | kpl | Rozszerzony |
| I\_NET\_CNS\_IPAM | System zarządzania adresami IP | BlueCat Networks | Proteus 3300 Appliance | P-3300 | 1 | kpl | Rozszerzony |
| I\_WIFI |   |
| I\_WIFI-CTRL | System zarządzania siecią WiFi – kontrolery i zapory sieciowe | Meru Networks | Meru MC4200 | MC4200 | 2 | szt | Podstawowy |
| I\_WIFI-CTRL | System zarządzania siecią WiFi – kontrolery i zapory sieciowe | Fortinet | FortiWiFi | Forti-WLC500D | 2 | szt | Podstawowy |
| I\_SEC |   |
| I\_SEC-VPN\_SSL | System zdalnego dostępu VPN SSL realizowane w oparciu o FG-1500D | Fortinet | FortiGate | FG-1500D | 2 | kpl | Rozszerzony |
| I\_SEC-FW\_EXT | Zewnętrzne zapory sieciowe, system ochrony przed intruzami, filtrowania treści i ochrony ruchu HTTP(S) | PaloAlto Networks | PA-5050 | PAN-PA-5050 | 2 | kpl | Rozszerzony |
| I\_SEC-CF\_MAIL | System filtrowania treści i ochrony ruchu SMTP | Fortinet | FortiMail | FML-200E | 2 | kpl | Podstawowy |
| I\_SEC-SIEM | System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem | Splunk Enterprise | Splunk | Splunk | 2 | kpl | Rozszerzony |
| I\_SEC-ADM\_AUTH | System uwierzytelniania administratorów | Fortinet | FortiAuthenticator | FAC-VM-BASE | 2 | szt. | Podstawowy |
| I\_UC |   |
| I\_UC-VG | Bramy głosowe | Cisco | 2951 Integrated Services Router | C2951-VSEC/K9 | 2 | kpl | Podstawowy |
| I\_CPD |   |
| I\_CPD-BLD\_CHASS | Obudowy serwerów kasetowych – chassis | IBM | BladeCenter H | 88524TG | 2 | kpl | Rozszerzony |
| I\_CPD-BLD\_SRV | Serwery kasetowe | IBM | BladeCenter HS22 | 7870C6G | 12 | kpl | Rozszerzony |
| I\_CPD-SW\_FC | Przełączniki Fibre Channel sieci SAN | IBM | Express IBM System Storage SAN24B-4 | 249824E | 2 | kpl | Rozszerzony |
| I\_CPD-DA | Macierz dyskowa | IBM | Storwize V5030 Disk Control EnclosureStorwize V5030 Disk Expansion Enclosure |  | 2 | kpl | Rozszerzony |
| I\_CPD-TL | Biblioteka taśmowa | IBM | TS3200 Tape Library Model L4U Driveless | 35734UL | 1 | kpl | Podstawowy |
| I\_CPD-BKP\_SRV | System kopii zapasowych – serwer - oprogramowanie | IBM | System x3650M3 | 7945H4G | 1 | kpl | Podstawowy |

* 1. Sieć szkieletowa [I\_NET]

Wymagane jest zapewnienie wsparcia producenta dla Podsystemów posiadanych przez Zamawiającego na 36 miesięcy od daty podpisania umowy, oraz aktualizacja rozwiązań sieciowych posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta na 36 miesięcy od daty podpisania umowy lub protokolarnego odbioru w przypadku dostawy nowych rozwiązań.

* + 1. Przełączniki rdzeniowe [I\_NET-SW\_CORE] - efekt Dialogu Technicznego

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 4 |
| Producent | Juniper Networks |
| Model | 4500 |
| Numer katalogowy | EX4500-40F-VC1-FB |
| Numery seryjne | GX0215478832, GX0212140928, GX0212140988, GX0212140997 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie 4 sztuk przełączników, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | **Przełącznik 1U, 40 portów 10 GbE z redundantnymi zasilaczami i pełnym obsadzeniem modułów wentylatorów, możliwość tworzenia stosu, przepływ powietrza AFI- z przodu do tyłu switcha (model referencyjny przełącznika: Juniper EX4600-40T-AFI,):*** Przełącznik musi posiadać: 40 portów 10 GbE wraz z wkładka mi światłowodowymi jednomodowymi, oraz 4 porty 40 GbE wraz z wkładkami światłowodowymi jednomodowymi,
* Przełącznik musi być wyposażony co najmniej w 8GB pamięci DRAM oraz 32GB pamięci flash.
* Przełącznik musi posiadać możliwość przełączania pakietów na poziomie 1.44 Tbps
* Przełącznik musi obsługiwać VLAN 802.1q.
* Przełącznik musi obsługiwać STP (z możliwością uruchomienia instancji per-vlan), RSTP, MSTP.
* Przełącznik musi obsługiwać agregację portów w grupy zgodnie z LACP (16 portów per grupa).
* Przełącznik musi zapewniać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1v2, routing statyczny i OSPF.
* Przełącznik musi zapewniać obsługę ruchu IP Multicast, w tym funkcjonalność IGMP v1, v2, v3 oraz IGMP Snooping.
* Przełącznik musi posiadać możliwość obsługi IP Multicast z wykorzystaniem protokołów PIM-SM, PIM-SSM, PIM-DM.
* Przełącznik musi posiadać możliwość obsługi funkcjonalności PBR (Policy Based Routing).
* Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP: DHCP Server oraz DHCP Relay.
* Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
	1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
	2. Implementacja czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek
	3. Obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
	4. Obsługa IP Precedence i DSCP.
* Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
	1. Wiele poziomów dostępu administracyjnego poprzez konsolę
	2. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x oraz EAP
	3. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2
	4. Możliwość definiowania listy kontroli dostępu (ACL) na poziomie portów (PACL), VLAN-ów (VACL), interfejsów routera (RACL)
	5. Obsługa DHCP snooping
	6. Obsługa dynamicznej inspekcji ARP.
* Przełącznik musi mieć możliwość synchronizacji zegara czasu za pomocą protokołu NTP.
* Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi być możliwy do edycji w trybie off-line tzn. jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej jest możliwość przechowywania 50 plików konfiguracyjnych. Zmiany aktywnej konfiguracji są widoczne bez częściowych restartów urządzenia po dokonaniu zmian.
* Przełącznik musi posiadać możliwość tworzenia stosu o przepustowości pomiędzy elementami stosu (backplane) 960 Gbps. Urządzenia w stosie współdzielą wspólną tablice MAC oraz routingu, istnieje możliwość zestawienia połączeń typu channel do różnych przełączników w obrębie stosu. Stos musi być widoczny z punktu widzenia zarządzania jako jedno urządzenie.
* Przełącznik musi posiadać możliwość tworzenia stosu łączącego do 10 urządzeń.
* Przełącznik musi umożliwiać kopiowanie ruchu (z portu, VLANu) na określony port (mirror).
* Przełącznik jest wyposażony w redundantny wewnętrzny zasilacz.
* Tablica CAM obsługuje do 288 000 adresów MAC per system.
* Przełącznik obsługuje 4096 VLANów.
* Tablica routingu powinna obsługiwać co najmniej 16 000 wpisów (dla adresów unicast IPv4).
* Przełącznik musi mieć możliwość rozbudowy o sprzętową obsługę IPv6.
* Obsługa routingu PIM, OSPF v2 and v3, RIP v2, RIPnG, BGP, BGPv6, ISIS, IGMP v1, v2, v3.
* Przełącznik obsługuje mechanizm VRF lite.
* Przełącznik musi mieć możliwość wykorzystania mechanizmów protokołu RADIUS oraz 802.1x, w szczególności dynamiczne przypisywanie VLAN-u do portu, w zależności od polityki bezpieczeństwa.
* Przełącznik musi posiadać możliwość pracy jako samodzielne urządzenie.
* Przełącznik musi zapewniać rozproszone przetwarzanie pakietów – logicznie lub fizycznie rozdzielone funkcje kontrolne (routing engine, control plane) od przełączania (forwarding engine, data plane) ruchu.
* Dwa zasilacze (redundancja) w układzie (1 + 1) zasilacze z możliwością podłączenia podczas pracy.
* Obsadzone wszystkie moduły wentylatorów.
* Przełącznik musi obsługiwać następujące Funkcje warstwy 3 (IPv4): • Static routing• Protokoły routingu (RIP, OSPF, IS-IS, BGP, MBGP) • Virtual Router Redundancy Protocol (VRRP) • Protokół dwukierunkowego wykrywania przekazywania (BFD) • Router wirtualny • Przekaźnik protokołu DHCP (Dynamic Host Configuration Protocol) • Protokół rozwiązywania adresów proxy (ARP) • Funkcje multicast • Protokół zarządzania grupami internetowymi (IGMP): v1, v2, v3 • IGMP snooping: v1, v2, v3 • Filtr IGMP • PIM-SM • Multicast Source Discovery Protocol (MSDP) • Bezpieczny login i hasło interfejsu • RADIUS • TACACS + • Filtry wejściowe i wyjściowe: zezwalaj i zabraniaj, filtry portów, filtry VLAN i filtry routowane, w tym filtry portów zarządzania • SSH v1, v2 • Statyczna obsługa ARP • Storm control • Ochrona przed DoS • Dynamiczna inspekcja ARP (DAI) • Snooping DHCP • Przekazywanie oparte na filtrze • IPv4 przez GRE (encap and decap)
* Zgodność z normami Standardy IEEE • IEEE 802.1D • IEEE 802.1w • IEEE 802.1 • IEEE 802.1Q • IEEE 802.1p • IEEE 802.1ad • IEEE 802.3ad • IEEE 802.1AB • IEEE 802.3x • IEEE 802.1Qbb • IEEE 802.1Qaz
* Switch musi mieć możliwość tworzenia stosu z pozostałymi przełącznikami opisanymi w punkcie 7.2.1.
 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 4 |
| Producent | Juniper Networks |
| Model | 4200 |
| Numer katalogowy | EX4500-40F-VC1-FB |
| Numery seryjne |  BP0212018888, BP0212019040, BM0212131338, BM0212131373, BM0212131236, BM0212131354 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie 6 sztuk przełączników, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | **Przełącznik 1U, porty RJ45 48x10/100/1000 z zasilaczem 350W i wentylatorami, sloty uplink 4x10GbE, możliwość tworzenia stosu, plus redundantny zasilacz 1100W (model referencyjny przełącznika: Juniper EX4300-48T, 2x JPSU-350-AC-AFO, EX4300-FAN):*** Przełącznik musi posiadać 48 portów GigabitEthernet 10/100/1000 BaseT.
* Przełącznik musi mieć możliwość instalacji modułu umożliwiającego zamienne wykorzystanie interfejsów GE i 10 GE (np. działające 4 interfejsy GE albo 2 10GE). Uruchomienie któregokolwiek z opisanych portów nie powoduje zablokowania żadnego z 48 podstawowych portów 10/100/1000 BaseT.
* Przełącznik musi umożliwiać instalację modułu 4 portowego GigabitEthernet z możliwością definicji styku za pomocą modułów SFP/SFP+.
* Przełącznik musi być wyposażony co najmniej w 2GB pamięci DRAM oraz 2GB pamięci flash.
* Przełącznik musi posiadać możliwość przełączania pakietów na poziomie 496 Gbps
* Przełącznik musi obsługiwać VLAN 802.1q.
* Przełącznik musi obsługiwać STP (z możliwością uruchomienia instancji per-vlan), RSTP, MSTP.
* Przełącznik musi obsługiwać agregację portów w grupy zgodnie z LACP (16 portów per grupa).
* Przełącznik musi zapewniać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1v2, routing statyczny i OSPF.
* Przełącznik musi zapewniać obsługę ruchu IP Multicast, w tym funkcjonalność IGMP v1, v2, v3 oraz IGMP Snooping.
* Przełącznik musi posiadać możliwość obsługi IP Multicast z wykorzystaniem protokołów PIM-SM, PIM-SSM, PIM-DM.
* Przełącznik musi posiadać możliwość obsługi funkcjonalności PBR (Policy Based Routing).
* Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP: DHCP Server oraz DHCP Relay.
* Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
	1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
	2. Implementacja czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek
	3. Obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
	4. Obsługa IP Precedence i DSCP.
* Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
	1. Wiele poziomów dostępu administracyjnego poprzez konsolę
	2. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x oraz EAP
	3. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2
	4. Możliwość definiowania listy kontroli dostępu (ACL) na poziomie portów (PACL), VLAN-ów (VACL), interfejsów routera (RACL)
	5. Obsługa DHCP snooping
	6. Obsługa dynamicznej inspekcji ARP.
* Przełącznik musi mieć możliwość synchronizacji zegara czasu za pomocą protokołu NTP.
* Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi być możliwy do edycji w trybie off-line tzn. jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej jest możliwość przechowywania 50 plików konfiguracyjnych. Zmiany aktywnej konfiguracji są widoczne bez częściowych restartów urządzenia po dokonaniu zmian.
* Przełącznik musi posiadać możliwość tworzenia stosu o przepustowości pomiędzy elementami stosu (backplane) 320 Gbps. Urządzenia w stosie współdzielą wspólną tablice MAC oraz routingu, istnieje możliwość zestawienia połączeń typu channel do różnych przełączników w obrębie stosu. Stos musi być widoczny z punktu widzenia zarządzania jako jedno urządzenie.
* Przełącznik musi posiadać możliwość tworzenia stosu łączącego do 10 urządzeń.
* Przełącznik musi umożliwiać kopiowanie ruchu (z portu, VLANu) na określony port (mirror).
* Przełącznik jest wyposażony w redundantny wewnętrzny zasilacz.
* Tablica CAM obsługuje do 64 000 adresów MAC per system.
* Przełącznik obsługuje 4093 VLANy.
* Tablica routingu powinna obsługiwać co najmniej 16 000 wpisów (dla adresów unicast IPv4).
* Przełącznik musi mieć możliwość rozbudowy o sprzętową obsługę IPv6.
* Obsługa routingu PIM, OSPF v2 and v3, RIP v2, RIPnG, BGP, BGPv6, ISIS, IGMP v1, v2, v3.
* Przełącznik obsługuje mechanizm VRF lite.
* Przełącznik musi mieć możliwość wykorzystania mechanizmów protokołu RADIUS oraz 802.1x, w szczególności dynamiczne przypisywanie VLAN-u do portu, w zależności od polityki bezpieczeństwa.
* Przełącznik musi posiadać możliwość pracy jako samodzielne urządzenie.
* Przełącznik musi zapewniać rozproszone przetwarzanie pakietów – logicznie lub fizycznie rozdzielone funkcje kontrolne (routing engine, control plane) od przełączania (forwarding engine, data plane) ruchu.
* Switch musi mieć możliwość tworzenia stosu z pozostałymi przełącznikami opisanymi w punkcie 7.2.1

Dostarczone przełączniki muszą być wyposażone w:* **Moduł uplink do przełączników (model referencyjny EX-UM-4X4SFP)** 4-port 10-Gigabit Ethernet SFP+ uplink module (**łącznie 6 sztuki**)
* **Wkładka optyczna SFP+ (model referencyjny EX-SFP-10GE-LR)** SFP+ 10GBase-LR 10 Gigabit Ethernet Optics, 1310nm for 10km transmission on SMF (**łącznie 12 sztuk**)
* Kable Virtual Chassis **EX-QSFP-40GE-DAC-1M (łącznie 10 sztuk**)
 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Bramy/routery dostępowe/brzegowe [I\_NET-GW]

Specyfikacja urządzeń

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | Juniper Networks |
| Model | MX80 |
| Numer katalogowy |  |
| Numery seryjne | F1373, F1459 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Przedłużenie gwarancji i serwisu producenta do 36 miesięcy od daty podpisania umowy |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. System zarządzania adresami IP [I\_NET-CNS\_IPAM]

Specyfikacja urządzeń

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 1 |
| Producent | BlueCat Networks |
| Model | Proteus 3300 Appliance |
| Numer katalogowy | P-3300 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | 1. Architektura Systemu DDI.
	1. System musi być dostarczony w formie 2 maszyn wirtualnych.
	2. Maszyny wirtualne muszą mieć możliwość uruchomienia na systemach Vmware, KVM i Hyper-V.
2. Funkcjonalności Systemu DDI
	1. Pojemność bazy systemu DDI na minimum 100 000 rekordów
	2. Możliwość pełnienia funkcji zarządzania dla 4 urządzeń podsystemów usługowych
	3. Możliwość obsługi do 10 administratorów systemu jednocześnie
	4. System musi posiadać funkcjonalność zarządzania adresami IP – IPAM (IP Address Management).
	5. System musi zarządzać adresami IPv4 i IPv6 pozwalając na graficzną (mapy sieci) oraz obiektową metodę zarządzania adresacją
	6. Funkcjonalność IPAM musi wspierać adresy link-local IPv6.
	7. System musi pozwalać na integrację z usługami VMware vCenter oraz OpenStack, w celu wykonywania procesu odnajdowania maszyn wirtualnych oraz automatycznego tworzenia rekordów DNS (A i PTR) oraz wpisów w bazie IPAM dla tych maszyn
	8. System musi posiadać mechanizmy kontroli wprowadzania danych (poprawność adresów IP, masek itp.)
	9. System musi umożliwiać dodawanie własnych, zdefiniowanych przez użytkownika, atrybutów dla obiektów typu sieci, adresy IP, strefy DNS, rekordy DNS (np. w celu określenia osoby odpowiedzialnej, wydziału, przypisania do określonej usługi biznesowej, podania lokalizacji fizycznej itp.). Atrybuty te muszą umożliwiać definicję typu (w tym co najmniej tekst, lista, liczba całkowita, email, URL, data) i rozmiaru danego atrybutu przez użytkownika systemu. Musi być możliwość stosowania słowników atrybutów z wymuszeniem lub proponowaniem danego typu atrybutu dla danego rodzaju obiektu. System musi umożliwiać dziedziczenie atrybutów w ramach struktury sieci i podsieci
	10. System musi wspierać mechanizm skanowania sieci i hostów/adresów IP (ang. IP Discovery). Mechanizm ten musi działać w trybie na żądanie oraz musi umożliwiać zaplanowanie skanowania periodycznego
	11. System musi posiadać mechanizmy typu „znajdź 10 nieużywanych adresów z sieci X” oraz „znajdź 10 nieużywanych podsieci rozmiaru np. /24 w podsieci np. a.b.c.d/16”. Funkcja musi być dostępna dla IPv4 i IPv6
	12. System musi posiadać funkcjonalność zarządzania numeracją sieci VLAN.
	13. System musi umożliwiać import danych w formacie CSV bezpośrednio z GUI i posiadać szczegółową dokumentację formatu danych importowanych
	14. Producent rozwiązania musi udostępniać bezpłatnie narzędzie do importu danych z innych systemów DNS: Bind oraz Microsoft
	15. System musi posiadać możliwość rozbudowy o zarządzanie usługami DNS i DHCP na serwerach Microsoft Windows 2016.
	16. System musi wspierać realizację usług DHCP dla IPv4 i IPv6
	17. System musi wspierać aktualizację danych DDNS przez usługę DHCP
	18. System musi wspierać na bieżąco informacje o przyznawaniu adresów IP i urządzeniach, którym dany adres został przypisany (adres MAC, czas i data przyznania adresu, IP)
	19. System musi wspierać funkcjonalność DHCP Failover z renegocjacją dostępnych przestrzeni adresowych
	20. Musi istnieć możliwość sprawdzenia dostępności adresu IP przed jego przydzieleniem z czasem ICMP poniżej sekundy
	21. System musi wspierać funkcję rozpoznawania typu urządzenia/systemu stacji, urządzeń mobilnych itp. na podstawie analizy zapytania DHCP. Raportowanie typu urządzenia w historii dzierżaw adresów IP oraz możliwość filtrowania/blokowania przydziału adresu dla wybranych typów urządzeń. (Np. przydziel adres stacji Windows 7/10 ale nie przydzielaj adresu tabletowi i urządzeniu typu smartphone)
	22. System musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System), zarówno jak serwer autorytatywny jak i rekursywny.
	23. Obsługa minimum 20 000 zapytań DNS na sekundę
	24. Obsługa minimum 140 zapytań DHCP na sekundę
	25. System musi być zgodny z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Commnents http://www.ietf.org/rfc.html)
	26. System musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136
	27. System musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996
	28. System musi wspierać protokoły DNS w wersji IPv4 i IPv6
	29. System musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF)
	30. System musi wspierać usługę DNSSEC z automatycznym aktualizowaniem podpisów przy zmianach dokonywanych w strefach DNS
	31. System musi mieć możliwość świadczenia usługi DNS dla usług Active Directory z automatycznym tworzeniem specjalnych rekordów AD z podkreśleniem w nazwie.
	32. System musi wspierać usługę DDNS
	33. System musi wspierać bezpieczną aktualizację rekordów DNS tzw. Secure Update, ze wsparciem dla protokołu GSS-TSIG
	34. System musi umożliwiać kopiowanie i przenoszenie rekordów DNS pomiędzy strefami.
	35. System musi wspierać rekordy DNS SVCB (typ 64) i HTTPS (typ 65).
	36. System musi wspierać funkcjonalność Multimaster DNS z aktualizacją DDNS
	37. System musi obsługiwać mechanizm IDN (Internationalized Domain Names) – (w tym polskie znaki) i posiadać wbudowany konwerter tzw. punycode
	38. System musi umożliwiać logowanie wszystkich zapytań i odpowiedzi DNS.

 1. Zarządzanie i konfiguracja systemu
	1. System musi działać pod kontrolą dedykowanego systemu operacyjnego. System DDI nie może wymagać do swojego działania instalacji określonych wersji innego oprogramowania lub bibliotek.
	2. Zarządzanie Systemem musi odbywać się centralnie za pomocą jednolitego systemu graficznego
	3. System musi posiadać mechanizm Workflow do zarządzania procesem potwierdzania i akceptacji zmian
	4. Zarządzanie systemem musi się odbywać przez przeglądarkę WWW bez potrzeby instalacji specjalnego oprogramowania typu agent, klient itp.
	5. System musi dostarczać mechanizm RESTful Web API do kontroli systemu, wykonywania i automatyzacji zadań wykonywanych za pomocą GUI. Musi być dostarczona pełna dokumentacja systemu API z przykładami zastosowania itp.
	6. System musi pracować jako platforma dystrybucji plików za pomocą protokołów TFTP, FTP, HTTP, oraz oferować usługi synchronizacji czasu za pomocą protokołu NTP (Network Time Protocol)
	7. System musi posiadać funkcję budowy Systemu rozproszonego z synchronizacją danych poprzez sieć IP z centralnym zarządzaniem całym systemem
	8. System musi dostarczać informacje o wszystkich zmianach wprowadzanych przez administratorów (kto, kiedy, co zostało zmienione)
	9. System musi mieć możliwość wysyłania tych informacji do centralnego repozytorium za pomocą mechanizmu Syslog (TCP i UDP)
	10. System musi umożliwiać nadawanie administratorom praw opartych o grupy i role, co pozwala na ograniczenie ich dostępu do wymaganych zasobów. Granulacja uprawnień powinna umożliwiać konfigurowanie uprawnień dla pojedynczych obiektów typu sieć, strefa DNS, rekord DNS
	11. System musi wpierać uwierzytelnianie użytkowników poprzez: lokalną bazę użytkowników, protokół RADIUS, protokół TACACS+, LDAP, Microsoft Active Directory
	12. System musi posiadać wbudowaną bazę danych. Baza danych nie może wymagać żadnych czynności administracyjnych związanych z jej konfiguracją i utrzymaniem
	13. System musi mieć możliwość monitorowania parametrów urządzeń przy użyciu protokołu SNMP (Simple Network Management Protocol)
	14. Dostęp do podstawowej konsoli administracyjnej urządzeń Systemu musi być możliwy poprzez interfejs zdalny dostępny poprzez protokół SSH, z wsparciem dla wersji SSHv2
	15. System musi umożliwiać wykonywanie planowanych kopii bezpieczeństwa do zewnętrznego serwera w celu uproszczenia procedur odzyskiwania w razie awarii (TFTP, FTP, SCP)
	16. Jeżeli licencja na wirtualne urządzenia Systemu DDI jest czasowa to należy dostarczyć licencję na 3 lata.
	17. System musi być objęty co najmniej 3 letnim serwisem świadczonym bezpośrednio przez producenta uprawniającym do wsparcia telefonicznego i www w języku angielskim lub polskim w zakresie rozwiązywania problemów z Systemem oraz dostępem do poprawek i nowych wersji oprogramowania (upgrade).

System Raportowania – 1 szt.1. Architektura urządzenia
	1. System musi być dostarczony w formie maszyny wirtualnej.
	2. Maszyna wirtualna musi mieć możliwość uruchomienia na systemach Vmware, KVM i Hyper-V.
2. Funkcjonalność urządzenia
	1. System musi realizować dedykowane usługi raportowania dla Systemu DDI i być zdolnym do przetwarzania min. 400MB danych źródłowych DDI dziennie
	2. System musi posiadać odpowiednie uprawnienia dla użytkowników związane z dostępem do funkcji raportowania
	3. Wymagane jest generowanie minimum raportów:

• DNS:1. Szybkość aktualizacji DDNS
2. Najczęściej żądane nazwy domen DNS
3. Trend odpowiedzi DNS
4. Trend trafień w bufor DNS (Cache Hit Ratio)
5. Ilość zapytań DNS wg typu zapytań
6. Trend czasu odpowiedzi na zapytania DNS
7. Adresy IP będące źródłem największej ilości zapytań DNS
8. Ilość zapytań DNS dziennie w podziale na poszczególne serwery DNS
9. Największe obciążenie godzinowe wg liczby zapytań DNS dla poszczególnych serwerów
10. Liczba zapytań DNS per serwer DNS
11. Raport odpowiedzi NXDOMAIN / NOERROR
12. Raport błędów SERVFAIL

• bazy adresów IPAM i VLAN:1. Raport użycia adresów sieciowych IPv4
2. Trend użycia adresów sieciowych IPv4
3. Raport podsieci o największej liczbie wykorzystanych adresów IPv4
4. Raport podsieci o największej liczbie wykorzystanych dzierżaw DHCPv4
5. Raport z inwentaryzacji sieci VLAN (lista numerów i nazw sieci VLAN, ich widoków i zakresów VLAN, status, opis, osoba kontaktowa, dział)

• Obciążenia systemu:1. Trend wykorzystania procesora
2. Trend wykorzystania pamięci RAM
3. Ilość ruchu sieciowego per serwer

• DHCP1. historia dzierżaw DHCP IPv4 i IPv6
2. urządzenia klienckie DHCP najbardziej aktywne w określonym czasie
3. ogólna statystyka usługi DHCPv4 (z podziałem na sieci, zakresy DHCP, rodzaj dzierżawy)
4. trend wykorzystania zakresów DHCPv4
5. trend wykorzystania usługi DHCPv4 (liczba dzierżaw na sekundę)
6. trend wykorzystania usługi DHCPv4 (liczba dzierżaw na sekundę) z podziałem na rodzaj pakietu DHCP (Discover, Offer, Request, Acknowledge)
7. raport zmian DHCP fingerprint w określonym czasie
	1. Możliwość definiowania własnych raportów oraz kopiowania raportów w systemie.
8. Zarządzanie i konfiguracja
	1. System Raportowania musi umożliwiać zarządzanie nim z poziomu urządzeń Systemu DDI dostarczonego w ramach niniejszego postępowania
	2. Dostęp do konsoli administracyjnej urządzeń Systemu powinien być możliwy poprzez interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2
	3. System musi być objęty co najmniej 3 letnim serwisem świadczonym bezpośrednio przez producenta uprawniającym do wsparcia telefonicznego i www w języku angielskim lub polskim w zakresie rozwiązywania problemów z System oraz dostępem do poprawek i nowych wersji oprogramowania (upgrade).
 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Przełączniki dostępowe [I\_NET-SW-ACC]

Specyfikacja urządzeń

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Produkt | Przełącznik |
| Ilość sztuk/kompletów produktu | 6 |
| Lokalizacja | Piotrków Trybunalski |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | Switch zarządzalny warstwy 3* Sprzęt fabrycznie nowy
* Urządzenie przeznaczone do montażu w szafie telekomunikacyjnej 19” ze standardowymi stelażami Rack o wysokości obudowy 1U i maksymalnej głębokości 250 mm)
* Urządzenie przystosowane do zasilania bezpośrednio z sieci 230V, 50 Hz, bez dodatkowego zewnętrznego zasilacza niskonapięciowego
* Gniazdo zasilające typu C14 zlokalizowane z tyłu obudowy
* Uchwyt do mocowania linki uziemiającej z tyłu obudowy
* Maksymalny pobór mocy poniżej 50W
* Maksymalny hałas wytwarzany przez urządzenie poniżej 55 dB
* Wewnętrzny system chłodzenia musi zapewniać przepływ powietrza w układzie lewo-prawo z otworami wentylacyjnymi po bokach urządzenia
* Minimum 48 portów RJ-45 10/100/1000 Mbit, pracujących z prędkościami 10 i 100 Mbit w trybach half-duplex oraz full-duplex i w trybie 1000 Mbit full-duplex zlokalizowanych z przodu urządzenia
* Minimum 4 porty SFP+ o przepustowości 1/10 Gbit każdy zlokalizowanych z przodu urządzenia
* Minimum 1 port konsolowy do zarządzania urządzeniem z wiersza poleceń (CLI) zlokalizowany z przodu urządzenia z wejściami RJ45-serial oraz USB Micro-B
* Obsługa następujących protokołów i funkcjonalności: IEEE 802.1AX-2008, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, 802.1s, IEEE 802.1v, IEEE 802.1w, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3az, IEEE 802.3x, IEEE 802.1ad, IEEE 802.1p, RFC 768, RFC 783, RFC 792, RFC 793, RFC 826, RFC 854, RFC 868, RFC 951, RFC 1058, RFC 1256, RFC 1350, RFC 1519, RFC 1542, RFC 1918, RFC 2030, RFC 2131, RFC 2236, RFC 2453, RFC 2865, RFC 2866, RFC 3046, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418, RFC 3575, RFC 3576, RFC 4541, RFC 4675, RFC 4861, RFC 4862, RFC 5905, RFC 1981, RFC 2080, RFC 2081, RFC 2082, RFC 2460, RFC 2464, RFC 2710, RFC 2925, RFC 3019, RFC 3315, RFC 3484, RFC 3513, RFC 3596, RFC 3810, RFC 4022, RFC 4113, RFC 4251, RFC 4252, RFC 4253, RFC 4254, RFC 4291, RFC 4293, RFC 4419, RFC 4443, RFC 5095, RFC 6620, RFC 1155, RFC 1157, RFC 1591, RFC 1901-1907, RFC 1908, RFC 2576, RFC 2578-2580, RFC 2579, RFC 2819, RFC 1112, RFC 3376, RFC 2474, RFC 2475, RFC 2597, RFC 2598, UDLD
* Łączna przepustowość (throughput) na minimalnym poziomie 110 Mpps
* Opóźnienie w trybie pracy 1Gbit poniżej 4 µs dla 64 bajtowych pakietów, w trybie pracy 10Gbit poniżej 3 µs dla 64 bajtowych pakietów
* Przepustowość całkowita urządzenia (switching capacity) minimum 175 Gbps
* Rozmiar sprzętowej tablicy routingu minimum 2000 wpisów IPv4 i 1000 wpisów IPv6, minimum 256 statycznych tras, minimum 200 tras OSPF, minimum 10000 tras RIP
* Rozmiar tablicy adresów MAC minimum 32000 pozycji
* Producent urządzenia musi posiadać usługę, umożliwiającą zarządzanie urządzeniem przez chmurę.
* Obsługa następujących funkcjonalności: VxLAN, obsługa ramek Jumbo powyżej 9000 bajtów, RPVST+, IEEE 802.1Q z obsługą powyżej 4000 identyfikatorów VLAN, IEEE 802.1v, IEEE 802.1ad, GVRP, MVRP, wbudowany serwer DHCP, OSPFv2, OSPFv3, RIPv1, RIPv2,RIPng, routing statyczny, routing według zadanych reguł, blokada wybranych adresów MAC, RADIUS/TACACS+, Radius over TLS (RadSec), blokada pakietów DHCP z nieautoryzowanych serwerów, blokada ARP z nieautoryzowanych serwerów, MAC-pinning, listy kontroli dostępu ACLs, możliwość przypisania uprawnionych adresów MAC do korzystania z danego portu urządzenia, ochrona DoS,
* Zarządzanie urządzeniem z wiersza poleceń (CLI) poprzez port konsolowy oraz sieć IP z protokołem SSHv1/v2
* Zarządzanie poprzez HTTP z protokołem SSL
* Możliwość wymiany danych z urządzeniem za pomocą protokołu SFTP
* Możliwość personalizacji informacji powitalnej wyświetlanej podczas logowania się użytkowników do urządzenia
* Możliwość nadawania poszczególnym portom urządzenia własnych nazw
* Możliwość monitorowania ruchu typu „voip”
* Urządzenie musi posiadać dwa obrazy systemu, zapewniające możliwość przywrócenia wersji poprzedniej po aktualizacji firmware
* Urządzenie musi obsługiwać wiele plików konfiguracji systemu i przechowywać je w nieulotnej pamięci Flash
* Sprzęt musi prawidłowo współpracować z już posiadanym przez zamawiającego sprzętem sieciowym HP Procurve serii 2600 i 2800 oraz Cisco Catalyst serii 2960 w zakresie obsługi VLANów (zwłaszcza typu „voice”) oraz łącz agregowanych
* Wymagane normy bezpieczeństwa: UL 60950-1, 2nd Edition; UL 62368-1: 2nd Edition; EN 60950-1:2006 +A11:2009 +A1:2010

+A12:2011+A2:2013; IEC 60950-1:2005 +A1:2009 +A2:2013; EN 62368-1: 2nd Edition; CSA 22.2 No. 60950-1-07 2nd; IEC-62368-1: 2nd Edition; EN 60825-1:2014 / IEC 60825-1:2014 Class 1* Wymagane normy środowiskowe: EN 55032:2012/CISPR 32 Class A; FCC CFR 47 Part 15 Class A; VCCI Class A; ICES-003 Class A; CNS 13438
* Inne wymagane normy i standardy: EN 55024:2010/CISPR 24, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-11, IEC/EN 61000-3-2, IEC/EN 61000-3-3
* Gwarancja producenta minimum 15 lat od daty zakupu, realizowana poprzez wymianę urządzenia. Producent jest zobowiązany po zgłoszeniu gwarancyjnym przysłać urządzenie jako pierwszy a po jego otrzymaniu Zamawiający odsyła uszkodzony produkt na koszt producenta.

Przykładowy produkt spełniający wymogi specyfikacji: HP Aruba 2930F 48G 4SFP+ (JL254A) lub równoważny. |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Produkt | Przełącznik |
| Ilość sztuk/kompletów produktu | 4 |
| Lokalizacja | Piotrków Trybunalski |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | Switch zarządzalny POE+ warstwy 3* Sprzęt fabrycznie nowy
* Urządzenie przeznaczone do montażu w szafie telekomunikacyjnej 19” ze standardowymi stelażami Rack o wysokości obudowy 1U i maksymalnej głębokości 310 mm)
* Urządzenie przystosowane do zasilania bezpośrednio z sieci 230V, 50 Hz, bez dodatkowego zewnętrznego zasilacza niskonapięciowego
* Gniazdo zasilające typu C14 zlokalizowane z tyłu obudowy
* Uchwyt do mocowania linki uziemiającej z tyłu obudowy
* Maksymalny pobór mocy poniżej 460W
* Łączna moc gwarantowana dla urządzeń POE minimum 370W
* Maksymalna moc POE dla jednego portu minimum 30W
* Maksymalny hałas wytwarzany przez urządzenie poniżej 56 dB
* Wewnętrzny system chłodzenia musi zapewniać przepływ powietrza w układzie lewo-prawo z otworami wentylacyjnymi po bokach urządzenia
* Minimum 48 portów RJ-45 POE+ 10/100/1000 Mbit, pracujących z prędkościami 10 i 100 Mbit w trybach half-duplex oraz full-duplex i w trybie 1000 Mbit full-duplex zlokalizowanych z przodu urządzenia
* Minimum 4 porty SFP+ o przepustowości 1/10 Gbit każdy zlokalizowanych z przodu urządzenia
* Minimum 1 port konsolowy do zarządzania urządzeniem z wiersza poleceń (CLI) zlokalizowany z przodu urządzenia z wejściami RJ45-serial oraz USB Micro-B
* Obsługa następujących protokołów i funkcjonalności: IEEE 802.1AX-2008, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, 802.1s, IEEE 802.1v, IEEE 802.1w, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3az, IEEE 802.3x, IEEE 802.1ad, IEEE 802.1p, RFC 768, RFC 783, RFC 792, RFC 793, RFC 826, RFC 854, RFC 868, RFC 951, RFC 1058, RFC 1256, RFC 1350, RFC 1519, RFC 1542, RFC 1918, RFC 2030, RFC 2131, RFC 2236, RFC 2453, RFC 2865, RFC 2866, RFC 3046, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418, RFC 3575, RFC 3576, RFC 4541, RFC 4675, RFC 4861, RFC 4862, RFC 5905, RFC 1981, RFC 2080, RFC 2081, RFC 2082, RFC 2460, RFC 2464, RFC 2710, RFC 2925, RFC 3019, RFC 3315, RFC 3484, RFC 3513, RFC 3596, RFC 3810, RFC 4022, RFC 4113, RFC 4251, RFC 4252, RFC 4253, RFC 4254, RFC 4291, RFC 4293, RFC 4419, RFC 4443, RFC 5095, RFC 6620, RFC 1155, RFC 1157, RFC 1591, RFC 1901-1907, RFC 1908, RFC 2576, RFC 2578-2580, RFC 2579, RFC 2819, RFC 1112, RFC 3376, RFC 2474, RFC 2475, RFC 2597, RFC 2598, UDLD, IEEE 802.3at
* Łączna przepustowość (throughput) na minimalnym poziomie 110 Mpps
* Opóźnienie w trybie pracy 1Gbit poniżej 4 µs dla 64 bajtowych pakietów, w trybie pracy 10Gbit poniżej 3 µs dla 64 bajtowych pakietów
* Przepustowość całkowita urządzenia (switching capacity) minimum 175 Gbps
* Rozmiar sprzętowej tablicy routingu minimum 2000 wpisów IPv4 i 1000 wpisów IPv6, minimum 256 statycznych tras, minimum 200 tras OSPF, minimum 10000 tras RIP
* Rozmiar tablicy adresów MAC minimum 32000 pozycji
* Producent urządzenia musi posiadać usługę, umożliwiającą zarządzanie urządzeniem przez chmurę.
* Obsługa następujących funkcjonalności: VxLAN, obsługa ramek Jumbo powyżej 9000 bajtów, RPVST+, IEEE 802.1Q z obsługą powyżej 4000 identyfikatorów VLAN, IEEE 802.1v, IEEE 802.1ad, GVRP, MVRP, wbudowany serwer DHCP, OSPFv2, OSPFv3, RIPv1, RIPv2,RIPng, routing statyczny, routing według zadanych reguł, blokada wybranych adresów MAC, RADIUS/TACACS+, Radius over TLS (RadSec), blokada pakietów DHCP z nieautoryzowanych serwerów, blokada ARP z nieautoryzowanych serwerów, MAC-pinning, listy kontroli dostępu ACLs, możliwość przypisania uprawnionych adresów MAC do korzystania z danego portu urządzenia, ochrona DoS,
* Zarządzanie urządzeniem z wiersza poleceń (CLI) poprzez port konsolowy oraz sieć IP z protokołem SSHv1/v2
* Zarządzanie poprzez HTTP z protokołem SSL
* Możliwość wymiany danych z urządzeniem za pomocą protokołu SFTP
* Możliwość personalizacji informacji powitalnej wyświetlanej podczas logowania się użytkowników do urządzenia
* Możliwość nadawania poszczególnym portom urządzenia własnych nazw
* Możliwość monitorowania ruchu typu „voip”
* Urządzenie musi posiadać dwa obrazy systemu, zapewniające możliwość przywrócenia wersji poprzedniej po aktualizacji firmware
* Urządzenie musi obsługiwać wiele plików konfiguracji systemu i przechowywać je w nieulotnej pamięci Flash
* Sprzęt musi prawidłowo współpracować z już posiadanym przez zamawiającego sprzętem sieciowym HP Procurve serii 2600 i 2800 oraz Cisco Catalyst serii 2960 w zakresie obsługi VLANów (zwłaszcza typu „voice”) oraz łącz agregowanych
* Wymagane normy bezpieczeństwa: UL 60950-1, 2nd Edition; UL 62368-1: 2nd Edition; EN 60950-1:2006 +A11:2009 +A1:2010

+A12:2011+A2:2013; IEC 60950-1:2005 +A1:2009 +A2:2013; EN 62368-1: 2nd Edition; CSA 22.2 No. 60950-1-07 2nd; IEC-62368-1: 2nd Edition; EN 60825-1:2014 / IEC 60825-1:2014 Class 1* Wymagane normy środowiskowe: EN 55032:2012/CISPR 32 Class A; FCC CFR 47 Part 15 Class A; VCCI Class A; ICES-003 Class A; CNS 13438
* Inne wymagane normy i standardy: EN 55024:2010/CISPR 24, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-11, IEC/EN 61000-3-2, IEC/EN 61000-3-3
* Gwarancja producenta minimum 15 lat od daty zakupu, realizowana poprzez wymianę urządzenia. Producent jest zobowiązany po zgłoszeniu gwarancyjnym przysłać urządzenie jako pierwszy a po jego otrzymaniu Zamawiający odsyła uszkodzony produkt na koszt producenta.

Przykładowy produkt spełniający wymogi specyfikacji: HP Aruba 2930F 48G PoE+ 4SFP+ (JL256A) lub równoważny |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Produkt | Przełącznik |
| Ilość sztuk/kompletów produktu | 1 |
| Lokalizacja | Sandomierz |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | Switch 24 port POE RACK 19**Porty:** minimum24 porty RJ45 10/100/1000Mb/s**Porty PoE+ (RJ45):** 24**Wydajność przełączania**: min. 56Gb/s**Szybkość przekierowań pakietów:** min. 41,7Mp/s**Tablica adresów MAC:** min. 16k**Sieci VLAN:** Do 4K VLAN jednocześnie (z 4K VLAN ID) 802.1Q/MAC/Protocol/Private VLAN GARP/GVRP**Zarządzanie:** Interfejs przeglądarki internetowej GUI, interfejs linii poleceń CLI SNMP v1/v2c/v3**Funkcje L2 i L2+:** Routing statyczny DHCP Relay Serwer DHCP IGMP Snooping V1/V2/V3 802.3ad LACP (Do 8 grup agregacji, 8 portów na grupę) STP/RSTP/MSTP BPDU Filtering/Guard TC/Root Protect Wykrywanie pętli zwrotnych Kontrola przepływu 802.3x L2PT**Bezpieczeństwo transmisji:** Wiązanie IP-MAC-Port AAA Uwierzytelnianie oparte o standard IEEE 802.1X oraz Radius Ochrona przed atakami DoS Dynamiczna ochrona przed atakami ARP (DAI) SSH v1/v2 SSL v2/v3/TLSv1 Zabezpieczenia portów Broadcast/Multicast/Unknown-unicast Storm Control**Maksymalna łączna moc podłączonych urządzeń:** minimum 384W**Wymiary (S x G x W)**: 440\*330\*44 mm (17,3\*13\*1,7 cala) RACK 19 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Produkt | Przełącznik |
| Ilość sztuk/kompletów produktu | 2 |
| Lokalizacja | Sandomierz |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | Switch 16 port RACK 10 **Rodzaj urządzenia:** niezarządzalny**Ilość portów RJ-45 1GbE:** minimum 16 szt.**Bufor pamięci:** minimum 256 KB**Szybkość przekierowań (Mpps):** minimum 23,8**Ilość portów** minimum 16**Obsługiwane protokoły / Zgodność z normami:** IEEE 802.3 10 Base-T (RJ45),IEEE 802.3u 100 Base-T (RJ45),IEEE 802.3ab 1000 Base-T (RJ45),IEEE 802.3x Flow control,IEEE 802.3az Green Ethernet / Energy-Efficient Ethernet (EEE),IEEE 802.3z Gigabit Ethernet,IEEE 802.1p Priorytetyzacja ruchu,IEEE 802.3af **Przepustowość (Gbps)**: 32.0**Wymiary [G x S x W] (mm**): 215 x 133 x 42 **RACK 10’** |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Centralne zapory sieciowe [I\_NET-FW\_CORE]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | Fortinet |
| Model | Fortigate |
| Numer katalogowy | FG-1500D |
| Numery seryjne | FG1K5D3I17803385, FG1K5D3I17803424 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Przedłużenie gwarancji i serwisu producenta do 36 miesięcy od daty podpisania umowy |
|  | Dostarczenie licencji na :- Intrusion Prevention- Outbreak Prevention - AntyVirus- Web Filtering- FortiCare Support- Firmware and General Updates |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Zapory sieciowe [I\_NET-FW]

Specyfikacja urządzeń

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Produkt | Firewall |
| Ilość sztuk/kompletów produktu | 1 |
| Lokalizacja | Piotrków Trybunalski |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | Wymagania dla zapory sieciowej:* Kompleksowa i wydajna platforma bezpieczeństwa realizowana w oparciu o dedykowany procesor ASIC SOC3
* Dwa złącza typu WAN oraz siedem przełączanych portów LAN GE, które mogą zapewnić dwie strefy służące do wymuszania zastosowania zasad bezpieczeństwa dla wszystkich urządzeń końcowych
* Nieograniczona ilość licencji na jedno urządzenie
* Wielofunkcyjna zapora UTM, która powinna zawierać kontrolę aplikacji, IPS, VPN, web filtering oraz firewall
* Dostęp do usług, które zapewniają automatyczną ochronę przed wszelkimi zagrożeniami, realizowana powinna być w czasie rzeczywistym. Wszelkie urządzenia na bieżąco powinny być ochraniane przed szkodliwymi programami typu exploit, które mogą nawet umożliwić atakującemu przejęcie kontroli nad komputerem
* Możliwość bezpiecznego przeglądania Internetu poprzez filtrowanie wszystkich potencjalnie szkodliwych stron, a także usuwaniu zagrożeń (również z aplikacji). Ochrona przed spamem oraz wirusami. Powinna istnieć możliwość zablokowania stron zawierających niepokojącą treść, między innymi sceny przemocy i pornografię
* Centralny interfejs służący do zarządzania bezpieczeństwem - zintegrowane centrum zabezpieczeń, które pozwala na spełnienie wszystkich potrzeb związanych z zapewnieniem bezpieczeństwa, jednocześnie wykluczając konieczność zarządzania wieloma procesami przy użyciu wielu urządzeń
* Brak konieczności zakupu dodatkowych licencji; wszystkie funkcje produktu powinny być dostępne po zakupie, bez potrzeby inwestowania w kolejne funkcjonalności, które trzeba dopiero aktywować
* Możliwość bezpiecznego połączenia się z biurem dzięki zastosowaniu nowoczesnego rozwiązania Site to Site IPSec VPN
* Certyfikacja ICSA UTM
* Możliwość zdalnego połączenia z biurem poprzez Remote VPN, dostęp do plików bez ryzyka przechwycenia ich przez osoby nieuprawnione.
* Autentykacja przy wykorzystaniu dwóch składników hasła i tokenu
* Realizacja połączeń 3G i 4G poprzez wbudowany, zintegrowany port USB, który może stanowić zarówno główne, jak i zapasowe połączenie.
* Obsługa funkcji loadbalancing (równoważenie obciążenia) oraz automatyczne przekierowywanie połączenia na sprawne łącze
* Centralne sterowanie oprogramowaniem - zarządzanie wszelkimi aktualizacjami oraz konfiguracjami z jednego miejsca.
* Możliwość autentykacji użytkowników sieci - możliwość nadania im unikatowych loginów oraz haseł.
* Centralne raportowanie.
* Urządzenia powinno być wyposażone w kontroler sieci bezprzewodowej mogący współpracować z Access Pointami które będą również kompatybilne z posiadanym przez zamawiającego kontrolerem FG-1500D.

**Specyfikacja szczegółowa**

|  |  |
| --- | --- |
| Porty | 2 x WAN 10/100/1000 + 12 x LAN 10/100/1000Base-T + 4 SFP + 2 SFP+(10G) + 4 Combo RJ45/SFP |
| Przepustowość IPS | 1.6 Gb/s |
| Przepustowość NGFW | 800 Mb/s |
| Przepustowość Threat Protection | 700 Mb/s |
| Przepustowość Firewalla (1518/ 512/ 64 bajty pakiety UDP) | 20/ 18/ 10 Gb/s |
| Opóźnienie zapory (64 bajtowe pakiety) | 5 μs |
| Przepustowość zapory (liczba pakietów na sekundę) | 15 Mpps |
| Sesje równoległe (TCP) | 1 500 000 |
| Nowe sesje na sekundę (TCP) | 56 000 |
| Firewall Policies | 10 000 |
| Przepustowość IPsec VPN (512 bajtów) | 11.5 Gb/s |
| Tunele IPsec typu Brama-Brama | 2 500 |
| Tunele IPsec typu Klient-Brama     | 16 000 |
| Przepustowość SSL-VPN | 750 Mb/s |
| Liczba użytkowników SSL-VPN (zalecana) | 500 |
| SSL Inspection Throughput (IPS, avg. HTTPS)  | 1 Gb/s |
| SSL Inspection CPS (IPS, avg. HTTPS) | 1 800 |
| Ilość sesji SSL Inspectio (IPS, avg. HTTPS) | 135 000 |
| Przepustowość kontroli aplikacji (HTTP 64K) | 2.2 Gb/s |
| Przepustowość CAPWAP (HTTP 64 KB) | 15 Gb/s |
| Domeny wirtualne (domyślne / maksymalne) | 10/10 |
| Maksymlana liczba obsługiwanych przełączników FortiSwitches | 24 |
| Maksymalna liczba FortiAP (łącznie/tunel) | 64/32 |
| Maksymalna liczba FortiTokens | 5 000 |
| Maksymalna liczba zarejestrowanych FortiClients | 600 |
| Konfiguracje wysokiej dostępności | Active/Active, Active/Passive, Clustering |
| Lokalna dysk do zapisu logów | min. 480 GB |
|  |  |
|  |  |

 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Produkt | Firewall |
| Ilość sztuk/kompletów produktu | 1 |
| Lokalizacja | Sandomierz |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | Wymagania dla zapory sieciowej:* Kompleksowa i wydajna platforma bezpieczeństwa realizowana w oparciu o dedykowany procesor ASIC SOC3
* Dwa złącza typu WAN oraz siedem przełączanych portów LAN GE, które mogą zapewnić dwie strefy służące do wymuszania zastosowania zasad bezpieczeństwa dla wszystkich urządzeń końcowych
* Nieograniczona ilość licencji na jedno urządzenie
* Wysoka wydajność, oraz krótki czas odpowiedzi sieci oraz przepustowości firewalla - aż do 20 Gbps
* Wielofunkcyjna zapora UTM, która powinna zawierać kontrolę aplikacji, IPS, VPN, web filtering oraz firewall
* Dostęp do usług, które zapewniają automatyczną ochronę przed wszelkimi zagrożeniami, realizowana powinna być w czasie rzeczywistym. Wszelkie urządzenia na bieżąco powinny być ochraniane przed szkodliwymi programami typu exploit, które mogą nawet umożliwić atakującemu przejęcie kontroli nad komputerem
* Możliwość bezpiecznego przeglądania Internetu poprzez filtrowanie wszystkich potencjalnie szkodliwych stron, a także usuwaniu zagrożeń (również z aplikacji). Ochrona przed spamem oraz wirusami. Powinna istnieć możliwość zablokowania stron zawierających niepokojącą treść, między innymi sceny przemocy i pornografię
* Centralny interfejs służący do zarządzania bezpieczeństwem - zintegrowane centrum zabezpieczeń, które pozwala na spełnienie wszystkich potrzeb związanych z zapewnieniem bezpieczeństwa, jednocześnie wykluczając konieczność zarządzania wieloma procesami przy użyciu wielu urządzeń
* Brak konieczności zakupu dodatkowych licencji; wszystkie funkcje produktu powinny być dostępne po zakupie, bez potrzeby inwestowania w kolejne funkcjonalności, które trzeba dopiero aktywować
* Możliwość bezpiecznego połączenia się z biurem dzięki zastosowaniu nowoczesnego rozwiązania Site to Site IPSec VPN
* Certyfikacja ICSA UTM
* Możliwość zdalnego połączenia z biurem poprzez Remote VPN, dostęp do plików bez ryzyka przechwycenia ich przez osoby nieuprawnione.
* Autentykacja przy wykorzystaniu dwóch składników hasła i tokenu
* Realizacja połączeń 3G i 4G poprzez wbudowany, zintegrowany port USB, który może stanowić zarówno główne, jak i zapasowe połączenie.
* Obsługa funkcji loadbalancing (równoważenie obciążenia) oraz automatyczne przekierowywanie połączenia na sprawne łącze
* Centralne sterowanie oprogramowaniem - zarządzanie wszelkimi aktualizacjami oraz konfiguracjami z jednego miejsca.
* Możliwość autentykacji użytkowników sieci - możliwość nadania im unikatowych loginów oraz haseł.
* Centralne raportowanie.
* Urządzenia powinno być wyposażone w kontroler sieci bezprzewodowej mogący współpracować z Access Pointami które będą również kompatybilne z posiadanym przez zamawiającego kontrolerem FG-1500D.

**Specyfikacja szczegółowa**

|  |  |
| --- | --- |
| Porty | 8 x 10/100/1000Base-T + 2 x Combo RJ45/SFP + RJ45 console |
| Przepustowość IPS | 1.4 Gb/s |
| Przepustowość NGFW | 1 Gb/s |
| Przepusutść Threat Protection | 900 Mb/s |
| Przepustowość Firewalla (1518/ 512/ 64 bajty pakiety UDP) | 10/ 10/ 7 Gb/s |
| Opóźnienie zapory (64 bajtowe pakiety) | 3.23 μs |
| Przepustowośc zapory (liczba pakietów na sekundę) | 10.5 Mpps |
| Sesje równoległe (TCP) | 1 500 000 |
| Nowe sesje na sekundę (TCP) | 45 000 |
| Firewall Policies | 5 000 |
| Przepustowość IPsec VPN (512 bajtów) | 6.5 Gb/s |
| Tunele IPsec typu Brama-Brama | 200 |
| Tunele IPsec typu Klient-Brama     | 2 500 |
| Przepustowość SSL-VPN | 950 Mb/s |
| Liczba użytkowników SSL-VPN (zalecana) | 200 |
| SSL Inspection Throughput (IPS, avg. HTTPS)  | 715 Mb/s |
| SSL Inspection CPS (IPS, avg. HTTPS) | 700 |
| Ilość Sesji SSL Inspectio (IPS, avg. HTTPS) | 100 000 |
| Przepustowość kontroli aplikacji (HTTP 64K) | 1.8 Gb/s |
| Przepustowość CAPWAP (HTTP 64 KB) | 9 Gb/s |
| Domeny wirtualne (domyślne / maksymalne) | 10/10 |
| Maksymlana liczba obsługiwanych przełączników FortiSwitches | 16 |
| Maksymalna liczba FortiAP (łącznie/tunel) | 32/16 |
| Maksymalna liczba FortiTokens | 500 |
| Konfiguracje wysokiej dostępności | Active/Active, Active/Passive, Clustering |
| Lokalny dysk do zapisu logów | Min. 128 GB SSD |
|  |  |
|  |  |

 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Szkolenia
			1. Szkolenia autoryzowane

Wymagane jest zapewnienie szkoleń autoryzowanych o tematyce:

|  |  |
| --- | --- |
| **Tematyka** | **Liczba osób – pracowników Zamawiającego** |
| **I\_NET** |
| Centralne zapory sieciowe [I\_NET-FW\_CORE]1. Wstęp do UTM
2. Logowanie i monitoring
3. Konfiguracja polityk firewalla
4. NAT – Translacja adresów sieciowych
5. Lokalne uwierzytelnianie użytkowników
6. SSL VPN
7. Wstęp do IPSec-VPN
8. Explicit Proxy
9. Skanowanie antywirusowe
10. Filtr stron WWW
11. Kontrola aplikacji
12. Konfiguracja Routingu
13. Wirtualne domeny (VDOM)
14. Transparentny tryb pracy
15. High Availability
16. Zaawansowana konfiguracja IPSec VPN
17. Intrusion Prevention System – IPS
18. Operacje oparte na certyfikatach
19. Ochrona przed wyciekiem danych – DLP
20. Diagnostyka
21. Przyspieszenie sprzętowe – chipy ASIC
22. Ipv6
 | 5 |

* + - 1. Szkolenia autorskie

Wymagane jest zapewnienie szkoleń autorskich dla następujących podsystemów/podobszarów:

|  |  |  |
| --- | --- | --- |
| **Kod / mnemonik** | **Podsystem / podobszar** | **Czas trwania [dni]** |
| **I\_NET** |
| I\_NET-FW\_CORE | Zapory sieciowe | 2 |

Zakres szkolenia powinien obejmować funkcje i konfiguracje zastosowane we wdrożonym u Zamawiającego Podsystemie.

* 1. Sieć bezprzewodowa [I\_WIFI]

Wymagana jest aktualizacja rozwiązań sieci WIFI posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta na 36 miesięcy od daty podpisania umowy lub protokolarnego odbioru w przypadku dostawy nowych rozwiązań.

* + 1. System zarządzania siecią WIFI [I\_WIFI-CTRL]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | Fortinet |
| Model | Forti-WLC500D |
| Numer katalogowy |  |
| Numery seryjne | FWC5HD3A16000300, FWC5HD3A17000014 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Przedłużenie gwarancji i serwisu producenta do 36 miesięcy od daty podpisania umowy. |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Nowe urządzenia

Specyfikacja urządzeń

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Produkt | Access Point |
| Ilość sztuk/kompletów produktu | 55 |
| Lokalizacja | Piotrków Trybunalski (45)/Sandomierz (10) |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | * 2x2 MIMO
* 802.11ac Wave 1
* Do zastosowań wewnątrz budynku
* Dwa radia WiFi
* 2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM),
* 5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
* jedno radio BLE
* 4 anteny WiF (3 dBi dla 2.4 GHz, 4 dBi dla 5 GHz), 1 antena BLE
* Zakres częstotliwości [GHz] 2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850
* Maksymalna szybkość transmisji danych 867 Mbps
* Interfejsy: 1x 10/100/1000 Base-T RJ45, 1x Type A USB
* PoE IEEE 802.3af, 802.3.at
* Ilość jednocześnie używanych SSID: 16
* Urządzenie musi wspierać EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST, WPA, WPA2, WPA3 z 802.1x albo Preshared key, WEP, Web Captive Portal, MAC - lista blokowanych i akceptowanych adresów, 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1Q, 802.1X, 802.3af, 802.3at, 802.3az
* Kensington Lock
* Wspierane typy SSID: Local-Bridge, Tunnel & Mesh
* Przycisk reset, możliwość wyłączenia diod LED na urządzeniu
* Wbudowany moduł Sniffera pakietów i spectrum analyzer
* W zestawie zestaw montażowy do sufitu
* Maksymalny pobór mocy 12.5 W
* Zakres temperatury pracy 0–50°C
* AP musi w pełni współpracować z kontrolerami opisanymi w punkcie 7.3.1 i 7.2.6
 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Szkolenia
			1. Szkolenia autoryzowane

Wymagane jest zapewnienie szkoleń autoryzowanych o tematyce:

|  |  |  |
| --- | --- | --- |
| **Kod / mnemonik** | **Podsystem / podobszar** | **Czas trwania [dni]** |
| **I\_WIFI** |
| I\_WIFI | Sieć bezprzewodowa w oparciu kontroler wbudowany w firewall  | 2 |

* + - 1. Szkolenia autorskie

Wymagane jest zapewnienie szkoleń autorskich dla następujących podsystemów/podobszarów:

|  |  |  |
| --- | --- | --- |
| **Kod / mnemonik** | **Podsystem / podobszar** | **Czas trwania [dni]** |
| **I\_WIFI** |
| I\_WIFI | Sieć bezprzewodowa w oparciu kontroler wbudowany w firewall | 2 |

Zakres szkolenia powinien obejmować funkcje i konfiguracje zastosowane we wdrożonym u Zamawiającego Podsystemie.

* 1. Bezpieczeństwo informacji [I\_SEC]

Wymagana jest aktualizacja rozwiązań z zakresu bezpieczeństwa informacji posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta na 36 miesięcy od daty podpisania umowy lub protokolarnego odbioru w przypadku dostawy nowych rozwiązań.

* + 1. System zdalnego dostępu VPN SSL [I\_SEC-VPN\_SSL]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | Fortinet |
| Model | Realizacja funkcjonalności spełnianej przez Podsystem w ramach I\_NET-FW-CORE |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Przedłużenie gwarancji i serwisu producenta do 36 miesięcy od daty podpisania umowy |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Zewnętrzne zapory sieciowe [I\_SEC-FW\_EXT]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | PaloAlto Networks |
| Model | PA-5050 |
| Numer katalogowy | PAN-PA-5050 |
| Numery seryjne | 0009C102218, 0009C102196 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  | Next Generation Firewall – klaster (2 urządzenia)* Wbudowany mechanizm ML (machine learning) wspomagający wykrywanie ataków typu phishing
* Automatyczne rekomendacje dotyczące polityk i reguł minimalizujące ryzyko błędów ludzkich.
* Inspekcja i możliwość tworzenia polityk dla ruchu wejściowego i wyjściowego szyfrowanego TLS/SSL włącznie z TLS 1.3 i HTTP/2
* Możliwość tworzenia kopii odszyfrowanego ruchu z firewalla (decrytion mirroring) i przesłania go do zewnętrznego urządzenia analizującego
* Threat Prevention, z możliwością automatycznego sprawdzania całego ruchu i blokowania znanych podatności, złośliwego oprogramowania, exploitów
* Malware prevention – ochrona przed złośliwym oprogramowaniem z analizą w chmurze
* URL Filtering z możliwością tworzenia polityk dla adresów URL
* DNS Security z możliwością wykrywania i blokowania zagrożeń (w tym data exfiltration via DNS tunneling)
* Identyfikacja i kategoryzacja aplikacji na wszystkich portach z pełną inspekcją warstwy 7, możliwość tworzenia niestandardowych identyfikatorów aplikacji.
* Parametry wydajnościowe:

Firewall throughput (HTTP/appmix) 8.3/9.2 GbpsThreat Prevention throughput (HTTP/appmix) 4.1/5.0 GbpsIPsec VPN throughput 5.0 GbpsMax sessions 3MNew sessions per second 105,000* Możliwość pracy w klastrze HA active/active, active/passive
* Obsługa: 802.1Q VLAN tags per device/per interface: 4,094/4,094 Aggregate interfaces (802.3ad), LACP, NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation) NAT64, NPTv6 Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription, OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE) Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3, IPsec VPN Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication) Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
* 12 portów 10/100/1000, 8 porów 1G/10G SFP/SFP+, 4 porty 40G QSFP+,1 port 10/100/1000 out-of-band management port, 2 porty 10/100/1000 high availability, 1 port 10G SFP+ high availability, 1 port consoli RJ-45, 1 port Micro USB.
* Pamięć przechowywania 240 GB SSD
* Zasilacz Redundantny
* Wymiary urządzenia 2U, 19’’
* Urządzenie musi zapewniać przeniesienie wszystkich funkcjonalności wykorzystywane przez Zamawiającego na obecnym urządzeniu PA-5050
* **Urządzenie musi być wyposażone w ilość wkładek (min. 10 Gb) niezbędną do pracy klastra HA.**
 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. System filtrowania treści i ochrony ruchu SMTP [I\_SEC-CF\_MAIL]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | Fortinet |
| Model | Fortimail |
| Numer katalogowy | FML-200E |
| Numery seryjne | FE200E3A17000649, FE200E3A17000677 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Przedłużenie gwarancji i serwisu producenta do 36 miesięcy od daty podpisania umowy |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem [I\_SEC-SIEM]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | kpl |
| Producent | Splunk Enterprise |
| Model | Splunk |
| Hardware | System x 3650 M5 MT: 8871 M:AC3 s/n J339H4K J339H4L (Lenovo) |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Przedłużenie gwarancji i serwisu producenta do 36 miesięcy od daty podpisania umowy –. Wymagane jest dostarczę licencji, która pozwoli zwiększyć wolumen ruchu o 25% |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. System uwierzytelniania administratorów [I\_SEC-ADM\_AUTH]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 1 kpl |
| Producent | Fortinet |
| Model | Fortiauthenticator |
| Numer katalogowy | FAC-VM-BASE |
| Numery seryjne | FAC-VM0A17001239, FAC-VM0A17001252 |

Działania Wykonawcy w ramach podsytemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Przedłużenie gwarancji i serwisu producenta do 36 miesięcy od daty podpisania umowy |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Szkolenia
			1. Szkolenie przez certyfikowanych inżynierów wykonawcy

Wymagane jest zapewnienie warsztatów o tematyce:

|  |  |
| --- | --- |
| **Tematyka** | **Liczba osób – pracowników Zamawiającego** |
| **I\_SEC** |
| I\_SEC- SIEM | 5 |

* + - 1. Szkolenia autorskie

Wymagane jest zapewnienie szkoleń autorskich dla następujących podsystemów/podobszarów:

|  |  |  |
| --- | --- | --- |
| **Kod / mnemonik** | **Podsystem / podobszar** | **Czas trwania [dni]** |
| **I\_SEC** |
| I\_SEC-SIEM | System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem | 2 |

Zakres szkolenia powinien obejmować funkcje i konfiguracje zastosowane we wdrożonym u Zamawiającego Podsystemie.

* 1. Zintegrowany system łączności [I\_UC]

Wymagana jest aktualizacja rozwiązań z zakresu zintegrowanego systemu łączności posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta na 36 miesięcy od daty podpisania umowy.

* + 1. Bramy głosowe [I\_UC-VG]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | Cisco |
| Model | 2951 Integrated Services Router |
| Numer katalogowy | C2951-VSEC/K9 |
| Numery seryjne | FGL164513RF, FGL164513RE |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Przedłużenie gwarancji i serwisu producenta do 31.12.2022 r. |
|  | Udzielenie Wsparcia technicznego wykonawcy do 31.12.2022 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* 1. Środowisko przetwarzania danych [I\_CPD]

Wymagana jest aktualizacja rozwiązań z obszaru środowiska przetwarzania danych posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcia producenta na 36 miesięcy od daty podpisania umowy lub protokolarnego odbioru w przypadku dostawy nowych rozwiązań.

* + 1. Obudowy serwerów kasetowych - chassis [I\_CPD-BLD\_CHASS]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | IBM |
| Model | BladeCenter H |
| Numer katalogowy | 88524TG |
| Numery seryjne | 88524TGKD3L64A, 88524TGKD4P53Y |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie 3 sztuk serwerów, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  |

|  |  |
| --- | --- |
| **Obudowa** | Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – 205W. Minimalna ilość rdzeni dla procesora – 24. Wynik wydajności procesora instalowanego w oferowanym serwerze nie powinien być niższy niż 278 punków base w teście SPEC CPU 2017 / SPECrate 2017 Integer, opublikowanym przez SPEC.org ([www.spec.org](http://www.spec.org)) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów. |
| **Liczba procesorów**  | Min. 2 |
| **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) |
| **Pamięć operacyjna** | Zainstalowane minimum 16x32GB pamięci RAM łącznie 512Gb o częstotliwości 2933MHz TruDDR4 w kościach 32GB. Minimum 24 sloty na pamięć. Możliwość rozbudowy do 7,5TB RAM.  |
| **Zabezpieczenie pamięci** | memory mirroring, demand scrubing, patrol scrubing, memory rank sparing, ECC, SDDC, ADDDC |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.1 port VGA na tylnym panelu serwera. Wymagana możliwość instalacji portu VGA na panelu przednim. |
| **Rozbudowa dysków** | W chwili dostawy serwer musi posiadać zainstalowane minimum 2 dyski 2.5” SSD o pojemności nie mniejszej niż 960GB. Wymaga się, aby serwer posiadał możliwość instalacji dysków SED. Możliwość instalacji 24 dysków. |
| **Kontroler dyskowy** | Sprzętowy bez pamięci cache, pozwalający na utworzenie RAID 0/1. Możliwość zainstalowania kontrolera dyskowego posiadającego dodatkową pamięć cache z zabezpieczeniem na nieulotnej pamięci. Kontroler musi obsługiwać wymagane systemy operacyjne w wymaganych poziomach RAID.. |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 1600W z certyfikatem minimum Platinum. |
| **Interfejsy sieciowe** | Zintegrowane 2 porty 1Gb Base-T (w interfejsie dedykowanym do wyprowadzenia portów z płyty głównej). 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, wsparcie dla DCB, obsługa ramek Jumbo do 9.5Kb, Możliwość wymiany interfejsów karty rozszerzeń na min. cztery porty 10Gb SFP+. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. 1 karta sieciowa czteroportowa z portami 10Gb Ethernet SFP+ wraz z wkładkami 10Gb SR1 karta sieciowa dwuportowa typu SAN FC, o prędkości 32Gb wraz z wkładkami 32Gb.Do każdego typu portu należy dostarczyć odpowiedni patchcord długości 3m. |
| **Dodatkowe sloty I/O** | Serwer powinien umożliwiać instalacje min 5 kart PCIe. |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.0, , Możliwość instalacji portu VGA.
* z tyłu obudowy: 2x USB 3.0, , 1x VGA . Możliwość instalacji portu DB9
 |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |
| **Zasilanie** | Dwa redundantne hotswapowe zasilacze o mocy min 1600W każdy |
| **Zarządzanie** | Możliwość zdalnego zarządzania serwerem, udostępniania zdalnej konsoli graficznej i podłączania zdalnych napędów. Możliwość podstawowego monitoringu serwera za pomocą telefonu z dedykowaną aplikacją producenta serwera działającą w systemie Android lub iOS podłączonego do portu USB |
| **Funkcje zabezpieczeń** | Hasło włączania, hasło administratora, moduł TPM min 1.2. Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz. |
| **Urządzenia hot swap** | Dyski twarde, zasilacze, wentylatory. |
| **Obsługa** | Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane’y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych. |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAIDMożliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. |
| **Systemy operacyjne** | Microsoft Windows Server 2016, 2019, Red Hat Enterprise Linux 7 oraz 8, SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6.7 oraz 7.0 |
| **Waga** | maximum: 33kg |
| **Wymagania środowiskowe** | Serwer musi umożliwiać pracę w zakresie temperatur 5-45 st C. |

 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Przełączniki Fibre Channel sieci SAN [I\_CPD-SW\_FC]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | IBM |
| Model | Express IBM System Storage SAN24B-4 |
| Numer katalogowy | 249824E |
| Numery seryjne | 249824E10222HT, 249824E10222LB |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie 2-sztuk przełączników FC, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach:. |
|  |

|  |  |
| --- | --- |
| **1.** | Obudowa musi być dostosowana do montażu w szafie 19”. Wysokość co najwyżej 1U |
| **2.** | Przełącznik FC musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8 Gb/s w zależności od rodzaju zastosowanych wkładek SFP |
| **3.** | Przełącznik musi posiadać minimum 24 porty FC 16Gb, aktywne 24 porty, obsługiwane typy portów: F\_Port, E\_Port, M\_Port, D\_Port |
| **4.** | Przełącznik musi być w pełni obsadzony wkładkami SFP 16Gb |
| **5.** | Przełącznik musi umożliwić obsługę standardów i protokołów: Monitoring and Alerting Policy Suite (MAPS) Flow Vision Adaptive Networking (Traffic Isolation, quality of service) Fabric Performance Impact (FPI) Monitoring Slow Drain Device Quarantine (SDDQ) Advanced Zoning (default zoning, port/WWN zoning, broadcast zoning, peer zoning, target-driven zoning) Dynamic Fabric Provisioning (DFP) Dynamic Path Selection (DPS) Extended Fabrics Enhanced BB credit recovery FDMI Frame Redirection Frame-based Trunking FSPF ISL Trunking Management Server NPIV NTP v3 Registered State Change Notification (RSCN) Reliable Commit Service (RCS) Simple Name Server (SNS) Read Diagnostics Parameter (RDP) VM Insight |
| **6.** | Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 8Gb/s lub 16Gb/s |
|  |  |
| **8** | Oferowany przełącznik musi posiadać licencję Full Fabric.  |
| **9.** | Oferowany przełącznik musi posiadać interfejs administracyjny 10/100/1000 Mbps Ethernet (RJ-45), in-band over Fibre Channel, serial port (RJ-45), and one USB port |

 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Macierz dyskowa [I\_CPD-DA]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 2 |
| Producent | IBM |
| Model | Storwize V5030 Disk Control EnclosureStorwize V5030 Disk Expansion Enclosure |
| Numery seryjne | 7812V30, 7813F24, 7812V23, 78ZZ3L2 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
| 1. | Przedłużenie gwarancji i serwisu producenta do 36 miesięcy od daty podpisania umowy |
| 2. | Dostarczenie dysków do każdej macierzy w ilości: - 8 sztuk o pojemności 1.8Tb 2.5” 10krpm,- 4 dysków o pojemności 6Tb NLSAS 7200rpm, dyski muszą być kompatybilne z macierzami posiadanymi przez zamawiającego |
| 3. | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. Biblioteka taśmowa [I\_CPD-TL]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 1 |
| Producent | IBM |
| Model | TS3200 Tape Library Model L4U Driveless |
| Numer katalogowy | 35734UL |
| Numery seryjne | 78T1521 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  |

|  |  |
| --- | --- |
| **1.** | Biblioteka musi mieć możliwość instalacji w szafie Rack 19", wysokość nie więcej niż 3U, z zestawem szyn do mocowania w szafie. |
| **2.** | Biblioteka musi posiadać możliwość instalacji 3 napędów taśmowych. Biblioteka musi być wyposażona w 2 napędy taśmowe LTO 8 generacji z interfejsem FC minimum 8 Gbit/s. |
| **3.** | Biblioteka taśmowa musi mieć możliwość rozbudowy do min. 20 napędów taśmowych. |
| **4.** | Biblioteka musi być wyposażona w nie mniej niż 40 slotów na taśmy. |
| **5.** | Biblioteka musi być wyposażona w czytnik kodów kreskowych. |
| **6.** | Biblioteka musi być wyposażona w przynajmniej 4 sloty wejścia/wyjścia, umożliwiający wymianę taśm bez konieczności wyłączania urządzenia. |
| **7.** | Biblioteka musi posiadać interfejs webowy do zarządzania. |
| **8.** | Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów. |
| **9.** | Biblioteka musi być wyposażona w taśmę czyszczącą dla każdego napędu (2 szt.) |
| **10.** | Biblioteka musi być wyposażona w dwa zasilacze |
| **11.** | Do biblioteki należy dostarczyć 55 szt. taśm LTO 8. |

 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. System kopii zapasowych - oprogramowanie [I\_CPD-BKP\_SRV]

Obecnie posiadane urządzenia

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 1 |
| Producent | IBM |
| Model | System x3650M3 |
| Numer katalogowy | 7945H4G |
| Numery seryjne | 7945H4GKD3L64H |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie serwera oraz oprogramowania , uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  |

|  |  |
| --- | --- |
|  | **Serwer sytemu kopii zapasowych** |
| **Obudowa** | Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – 90W. Minimalna ilość rdzeni dla procesora – 12. Wynik wydajności procesora instalowanego w oferowanym serwerze nie powinien być niższy niż 130 punków base w teście SPEC CPU 2017 / SPECrate 2017 Integer, opublikowanym przez SPEC.org ([www.spec.org](http://www.spec.org)) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów. |
| **Liczba procesorów**  | Min. 2 |
| **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) |
| **Pamięć operacyjna** | Zainstalowane minimum 64GB pamięci RAM o częstotliwości 2666MHz w kościach 32GB. Minimum 24 sloty na pamięć. Możliwość rozbudowy do 3TB RAM.  |
| **Zabezpieczenie pamięci** | memory mirroring, demand scrubing, patrol scrubing, memory rank sparing, ECC, SDDC, ADDDC |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.1 port VGA na tylnym panelu serwera. Wymagana możliwość instalacji portu VGA na panelu przednim. |
| **Rozbudowa dysków** | W chwili dostawy serwer musi posiadać zainstalowane minimum 2 dyski SSD o pojemności nie mniejszej niż 1,2TB. Oraz 12 dysków 2.5” o pojemności 2TB Wymaga się, aby serwer posiadał możliwość instalacji dysków SED. Możliwość instalacji 24 dysków. |
| **Kontroler dyskowy** | Sprzętowy z pamięcią Flash 2 GB, pozwalający na utworzenie RAID 0/1/10/5/50/6/60 |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Platinum. |
| **Interfejsy sieciowe** | Zintegrowane 2 porty 1Gb Base-T (w interfejsie dedykowanym do wyprowadzenia portów z płyty głównej). 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, wsparcie dla DCB, obsługa ramek Jumbo do 9.5Kb, Możliwość wymiany interfejsów karty rozszerzeń na min. cztery porty 10Gb SFP+. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. 1 karta sieciowa dwuportowa z portami 10Gb Ethernet SFP+ wraz z wkładkami 10Gb SR1 karta sieciowa dwuportowa typu SAN FC, o prędkości 16Gb wraz z wkładkami 16Gb.Do każdego typu portu należy dostarczyć odpowiedni patchcord długości 3m.  |
| **Dodatkowe sloty I/O** | Serwer powinien umożliwiać instalacje min 5 kart PCIe.  |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.0, 1x USB 2.0, Możliwość instalacji portu VGA.
* z tyłu obudowy: 2x USB 3.0, , 1x VGA . Możliwość instalacji portu DB9
 |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |
| **Zasilanie** | Dwa redundantne hotswapowe zasilacze o mocy min 750W każdy |
| **Zarządzanie** | Możliwość zdalnego zarządzania serwerem, udostępniania zdalnej konsoli graficznej i podłączania zdalnych napędów. Możliwość podstawowego monitoringu serwera za pomocą telefonu z dedykowaną aplikacją producenta serwera działającą w systemie Android lub iOS podłączonego do portu USB |
| **Funkcje zabezpieczeń** | Hasło włączania, hasło administratora, moduł TPM min 1.2. Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz. |
| **Urządzenia hot swap** | Dyski twarde, zasilacze, wentylatory. |
| **Obsługa** | Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane’y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych. |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAIDMożliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. |
| **Obsługiwane systemy operacyjne** | Microsoft Windows Server 2016, 2019, Red Hat Enterprise Linux 7 oraz 8, SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6.7 oraz 7.0 |
| **Waga** | maximum: 33kg |
| **Wymagania środowiskowe** | Serwer musi umożliwiać pracę w zakresie temperatur 5-45 st C. |
| **System operacyjny** | **System operacyjny musi obsłużyć wszystkie rdzenie procesorów, oraz obsługiwać obrogramowanie systemu kopii zapasowych.** System nie posiadający ograniczenia ilości użytkowników które posiada możliwość domeny Active Directory, pozwalający na uruchomienie dowolnej aplikacji stworzonej dla systemów Windows. Oprogramowanie dostarczone musi być w aktualnej najnowszej wersji dostępnej na rynku. System musi posiadać poniższe parametry:-obsługę 64 fizycznych procesorów-awaryjne węzły klastra w ilości 64 obsługe pamięci RAM 4TB-działanie na procesorach opartych na architekturze x64. System musi posiadać następujące opcje: Network Policy and Access Services limits, Remonte Desktop Sevices limits, Virtualizations rights, DHCP role, DNS server role, Fax server role, UDDI Services, Print and Dokuments Management Services, Aplication server role, Server Manager, Active Directory Domain Services, Active Directory Certificate Services, Active Directory Fereration Services, Tryb Server Core, Hyper-V. Licencja dożywotnia |

 |
|  |

|  |  |
| --- | --- |
|  | **Oprogramowanie sytemu kopii zapasowych** |
| **1.** | Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5 |
| **2.** | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
| **3.** | Oprogramowanie musi umożliwić wykonywanie kopi zapasowych maszyn wirtualnych |
|  | Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej |
| **4.** | Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. |
| **5.** | Oprogramowanie musi umożliwić odzyskiwanie całej maszyny wirtualnej, określonych plików takich jak: dyski wirtualne, pliki konfiguracyjne. |
| **6.** | Oprogramowanie musi umożliwić przywracanie plików systemu gościa maszyn wirtualnych z wielu różnych systemów plików, w tym Linux, BSD macOS, Novell NetWare i Solaris |
| **7.** | Oprogramowanie musi posiadać scentralizowany system zarządzania kopiami zapasowymi |
| **8.** | Oprogramowanie musi posiadać możliwość łatwej rozbudowy w miarę rozrastania się infrastruktury teleinformatycznej. |
| **9.** | Oprogramowanie musi posiadać możliwość stałego monitorowania sytemu backapu jego kontroli i sporządzania raportów. |
| **10.** | Oprogramowanie musi umożliwić zorganizowanie skalowalnego repozytorium kopii zapasowych na podstawie zbioru heterogenicznych urządzeń magazynujących |
| **11.** | System musi umożliwić tworzenie kopii zapasowych, które można przechowywać lokalnie, przenosić do zewnętrznych repozytoriów za pośrednictwem sieci WAN, zapisywać na nośnikach taśmowych w celu długoterminowego przechowywania lub przesyłać do pamięci masowej w chmurze. |
| **12.** | System musi pozwalać na tworzenie automatyczne kopii według ustalonego harmonogramu. |
| **13.** | System może być niezależny od pamięci masowej, ale musi oferować również integracje pamięciami masowymi, takimi jak: Lenovo Storage V, IBM, EMC VNX, EMC VNXe, HP 3PAR, HP StoreVirtual, 9 |
|  | Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |
| **14.** | System musi wykorzystywać migawki systemu pamięci masowej jako źródło do tworzenia kopii zapasowych i odzyskiwania maszyn wirtualnych VMware z dysków znajdujących się na woluminach pamięci masowej. |
| **15.** | System musi umożliwić granularne odzyskiwanie elementów z Microsoft Exchange Server, Microsoft SharePoint, Microsoft Active Directory, Microsoft SQL Server i baz danych Oracle, a także odzyskiwanie pojedynczych plików i maszyn wirtualnych z migawek pamięci masowej dla istniejących partnerów pamięci masowej. |
| **16.** | System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 |
| **17.** | System musi być dostarczony z licencją wieczystą pozwalającą wykonywać kopie 30 maszyn wirtualnych. |

 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + 1. System wirtualizacji [I\_CPD-VRT]

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 1 |
| Producent | IBM |
| System | VMWare 5.5 Enterprise Plus |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, uruchomienie, konfiguracja, migracja maszyn do nowe środowiska wirtualnego, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach: |
|  |

|  |  |
| --- | --- |
| 1. | Warstwa wirtualizacji musi być zainstalowana bezpośrednio na .sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych . |
| 2. | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. |
| 3. | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w maksymalnie dwanaście rdzeni. |
| 4. | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-8 procesorowych . |
| 5. |  Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia minimum 255GB pamięci operacyjnej RAM. |
| 6. | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych , z których każda może mieć 1-10 wirtualnych kart sieciowych . |
| 7. | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych , z których każda może mieć 1-10 wirtualnych kart sieciowych . |
| 8. | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. |
| 9. | Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. |
| 10. | Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM. |
| 11. | Rozwiązanie musi wspierać następujące systemy operacyjne : , Windows 2000 , Windows Server 2003 , Windows Server 2008, Windows 7, Windows 10 , SLES 1O, SLES9 , SLES8 , Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris 1O, Solaris 9, Solaris 8, OS/2Warp 4.0, NetWare |
| 12. | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. |
| 13. | Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. |
| 14. | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. |
| 15. | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. |
| 16. | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. |
| 17. | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. |
| 18. | Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. |
| 19. | Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn. |
| 20. | Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi na których pracują. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie . |
| 21. | Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny które na nim pracowały były bezprzerwowe były dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. |
| 22. | System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej . Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. |
| 23. | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). |
| 24. | Rozwiązanie musi mieć możliwość zastosowania wirtualnych rozproszonych przełączników innych firm. Przełączniki te powinny posiadać możliwość ścisłej integracji z oprogramowaniem do wirtualizacji i być zaimplementowana jako wirtualne moduły liniowe na każdym hoście (serwerze) oraz redundantny moduł zarządzający . Implementacja stałego wirtualnego portu dołączającego maszynę wirtualną niezależnie od fizycznych serwerów (hostów) miedzy którymi maszyna jest miarowalna. |
| 25 | Wirtualny przełącznik wbudowany w rozwiązanie lub firmy trzeciej musi posiadać następujące możliwości:* Agregacja portów: Możliwość agregacji indywidualnych portów na danym hoście (serwerze) do pojedynczej wiązki logicznej, zgodnie z protokołem LACP
* QoS: Markowanie ruchu DSCP per wirtualny port; Dławienie (policing) ruchu per wirtualny port
* Zarządzanie : Zarządzanie wirtualnym przełącznikiem złożonym z wirtualnych modułów liniowych znajdujących się w hostach (serwerach) z wykorzystaniem redundantnego wirtualnego modułu typu Supervisor ;' Implementacja Netflow

lub podobnego mechanizmu dla statystyki ruchu; SNMP v3; Syslog* Bezpieczeństwo : Wymagane mechanizmy bezpieczeństwa: bezpieczny dostęp w oparciu o SSH; Port Security dla wirtualnych portów dołączających wirtualne maszyny; listy kontroli dostępu (ACL) na poziomie wirtualnych portów

filtracja na poziomie warstw L2/L3/L4; możliwość kopiowania ruchu z wybranego wirtualnego portu na inny określony wirtualny port na tym samym hoście (port monitorujący SPAN lub podobna funkcjonalność). Możliwość kopiowania ruchu z wybranego wirtualnego portu i tunelowania go poprzez zewnętrzną sieć do urządzenia monitorującego (port ERSPAN lub podobna funkcjonalność)Prywatne sieci VLAN; Wsparcie dla RADIUS/TACACS+ . |
| 26 | Licencja musi by dostarczona na 6 procesorów fizycznych w raz z systemem zarządzania platformą wirtualizacjiW raz platformą wirtualizacji należy dostarczyć licencję na serwerowy system operacyjny Microsoft Windows Server Standard w wersji edukacyjnej w ilości 32 sztuk licencji dwu rdzeniowych, lub równoważny. |

 |
|  | Udzielenie Wsparcia technicznego wykonawcy do 36 miesięcy od daty podpisania umowy – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE. |

* + - 1. Szkolenia autorskie

Wymagane jest zapewnienie szkoleń autorskich dla następujących podsystemów/podobszarów:

|  |  |  |
| --- | --- | --- |
| **Kod / mnemonik** | **Podsystem / podobszar** | **Czas trwania [dni]** |
| **I\_CPD** |
| I\_CPD-BLD\_ | Serwery kasetowe | 1 |
| I\_CPD-SW\_FC | Przełączniki Fibre Channel sieci SAN | 0,5 |
| I\_CPD-DA | Macierz dyskowa | 2 |
| I\_CPD-TL | Biblioteka taśmowa | 0,5 |
| I\_CPD-VRT | Platforma wirtualizacji | 1 |
| I\_CPD-BKP\_ | System kopii zapasowych | 1 |

* 1. Zarządzanie infrastrukturą teleinformatyczną [I\_MGMT]

Wymagane jest dostarczenie poniższych urządzeń:

* + 1. Konsole administratorskie do zdalnego zarządzania podsystemami infrastruktury teleinformatycznej [I\_MGMT-NMS]

Dostarczenie nowych urządzeń

|  |  |
| --- | --- |
| **Produkt** | **Opis** |
| Ilość sztuk/kompletów produktu | 10 |

Działania Wykonawcy w ramach podsystemu:

|  |  |
| --- | --- |
| **Lp.** | **Wymagania minimalne Zamawiającego** |
|  | Dostarczenie, urządzeń o następujących parametrach: |
|  | * Akumulator 3-komorowy, litowo-jonowy
* Wyświetlacz, rozdzielczość 1920 x 1080 (Full HD) pikseli, jasność 250 nitów, powłoka anyrefleksyjna, IPS -Level, przekątna 15.6 cali
* Procesor 2.0 GHz, 4.1 GHz Turbo, 8 MB Cache, 8 rdzeni, wydajność w CPU benchmark: PassMark minimum 13 000 (CPU Mark)
* Pamięć RAM 16 GB
* Dysk twardy SSD, format M.2, pojemność 512 GB
* Rodzaj karty graficznej zintegrowana, z wyjściem na HDMI
* Interfejsy: 1 x USB 3.2 1 x USB 3.2 typ C 2 x USB
* Komunikacja Bluetooth
* Wi-Fi 6 (802.11a/b/g/n/ac/ax)
* Czytnik kart pamięci MicroSD
* Dźwięk stereo
* Materiał obudowy: aluminium
* Klawiatura podświetlana z wydzieloną klawiaturą numeryczną
* Waga do 2 kg
* Czytnik linii papilarnych
* Kamera HD
* Wbudowany mikrofon
* Szyfrowanie TPM
* Wielodotykowy touchpad
* Zewnętrzna karta sieciowa USB 3.0 ze złączem RJ-45
* System operacyjny Windows 10, lub równoważny
* Torba umożliwiająca przenoszenie urządzenia
 |