Agencja Restrukturyzacji
i Modernizacji Rolnictwa

adres korespondencyjny
Centrala ARiMR
ul. Poleczki 33, 02-822 Warszawa

Specyfikacja Warunków Zamówienia

w postępowaniu o udzielenie zamówienia publicznego
o wartości równej lub przekraczającej progi unijne
prowadzonym w trybie przetargu nieograniczonego

na:

„Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, wdrożeniem i konsultacjami"

numer referencyjny sprawy: DPiZP.2610.17.2021

wszczętym na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.)

Informacje dotyczące prowadzonego postępowania o udzielenie zamówienia publicznego

A. Dane Zamawiającego

1. Zamawiającym jest:

   Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie (adres: Al. Jana Pawła II 70, 00-175 Warszawa); adres do korespondencji: ul. Poleczki 33, 02-822 Warszawa, tel. 22 595 06 11, adres e-mail: zamowieniapubliczne@arimr.gov.pl;

   REGON: 010613083;

   NIP: 526-19-33-940.

2. Adres strony internetowej prowadzonego postępowania o udzielenie zamówienia publicznego (dalej: *„postępowanie"*): https://platformazakupowa.pl/pn/arimr.
3. Niniejsze postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.; dalej: *„ustawa"*).

B. Pozostałe informacje dotyczące prowadzonego postępowania

1. Zmiany i wyjaśnienia treści Specyfikacji Warunków Zamówienia (dalej: *„SWZ"*) oraz inne dokumenty zamówienia bezpośrednio związane z niniejszym postępowaniem będą zamieszczane na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr gdzie należy wybrać zakładkę „postępowania", a następnie przejść na formularz niniejszego postępowania.
2. Postępowanie prowadzone jest w języku polskim. Komunikacja między Zamawiającym a Wykonawcami w niniejszym postępowaniu odbywa się przy użyciu środków komunikacji elektronicznej, tj. Platformy Zakupowej dostępnej pod adresem https://platformazakupowa.pl/pn/arimr (dalej: *„Platforma Zakupowa"*).
3. Poniżej Zamawiający przedstawia wymagania techniczno-organizacyjne związane z udziałem Wykonawców w postępowaniu:
   3.1. Złożenie oferty możliwe jest przez Wykonawców, którzy posiadają konto na Platformie Zakupowej oraz przez Wykonawców nieposiadających konta na Platformie Zakupowej. W celu założenia konta na Platformie Zakupowej należy wybrać zakładkę „Zaloguj się" w kolejnym kroku należy wybrać „Załóż konto", następnie należy wypełnić formularze i postępować zgodnie z poleceniami wyświetlającymi się na ekranie monitora. W przypadku Wykonawców niezalogowanych w celu złożenia oferty niezbędne jest podanie adresu e-mail (na który wysłane będzie potwierdzenie złożenia oferty), nr NIP oraz nazwy firmy i nr telefonu.
   3.2. Złożenie oferty oraz oświadczenia, o którym mowa w art. 125 ustawy, składanych w trakcie toczącego się postępowania wymaga od Wykonawcy posiadania kwalifikowanego podpisu elektronicznego.
   3.3. Wykonawca składa ofertę, która w przypadku prawidłowego złożenia oferty zostaje automatycznie zaszyfrowana przez system. Nie jest możliwe zapoznanie się z treścią złożonej oferty przed upływem terminu otwarcia ofert.
   3.4. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku kwalifikowanym podpisem elektronicznym.
4. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (t.j. Dz. U. z 2020 r. poz. 2452; dalej: *„Rozporządzenie w sprawie środków komunikacji"*), udostępnia informacje na temat specyfikacji połączenia, formatu przesyłanych danych oraz szyfrowania i oznaczania czasu przekazania i odbioru danych umożliwiających pracę na Platformie Zakupowej, tj.:
   4.1. stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   4.2. komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10.4, Linux, lub ich nowsze wersje,
   4.3. zainstalowana dowolna przeglądarka internetowa; w przypadku Internet Explorer minimalnie wersja 10.0.,
   4.4. włączona obsługa JavaScript,
   4.5. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików PDF.
   4.6. Platforma Zakupowa działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
5. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalne formaty przesyłanych danych, tj. plików o wielkości do 150 MB. Zalecany format: PDF.
6. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia w sprawie środków komunikacji, określa informacje na temat szyfrowania oraz czasu przekazania i odbioru danych, tj.:
   6.1. Szyfrowanie na Platformie Zakupowej (platformazakupowa.pl) odbywa się za pomocą protokołu TLS 1.3.
   6.2. Plik załączony przez Wykonawcę na Platformie Zakupowej i zapisany nie jest widoczny dla Zamawiającego, gdyż jest w systemie jako zaszyfrowany. Możliwość otworzenia pliku dostępna jest dopiero po odszyfrowaniu przez system, co następuje po upływie terminu otwarcia ofert,
   6.3. Oznaczenie czasu przekazania i odbioru danych przez Platformę Zakupową stanowi przypiętą do oferty elektronicznej datę oraz dokładny czas (hh:mm:ss), znajdujące się w kolumnie dotyczącej danej oferty, w sekcji - "Data złożenia oferty".
7. Zamawiający określa dopuszczalny format kwalifikowanego podpisu elektronicznego w przypadku:

7.1. dokumentów sporządzonych w formacie PDF zaleca się podpisanie dokumentu podpisem w formacie PAdES;

7.2. dokumentów sporządzonych w formacie innym niż PDF zaleca się podpisanie dokumentu podpisem w formacie XAdES.

8. Wykonawca przystępując do niniejszego postępowania akceptuje warunki korzystania z Platformy Zakupowej, określone w Regulaminie zamieszczonym na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr w zakładce „Regulamin" oraz uznaje go za wiążący.
9. Zamawiający informuje, że instrukcje korzystania z Platformy Zakupowej dotyczące w szczególności logowania, pobrania dokumentacji, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu Platformy Zakupowej znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr.
10. Korzystanie z Platformy Zakupowej jest bezpłatne. W celu ułatwienia Wykonawcom korzystania z Platformy Zakupowej operator platformy uruchomił Centrum Wsparcia Klienta, które służy pomocą techniczną od 8:00 do 17:00 w dni robocze od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mai: **cwk@platformazakupowa.pl.**

Rozdział I. Przedmiot zamówienia

I.1. Opis przedmiotu zamówienia

1. Kod Wspólnego Słownika Zamówień (CPV).
   1.1. Główny kod: 32420000-3 [*Urządzenia sieciowe*].
2. Przedmiotem zamówienia jest wykonanie przez Wykonawcę na rzecz Agencji Restrukturyzacji i Modernizacji Rolnictwa w Warszawie (zwanej dalej „*Zamawiającym*") dostawy, w skład której wchodzą:
   2.1. Zakup wraz z dostarczeniem fabrycznie nowego, nienoszącego śladów uprzedniego używania Sprzętu IT wraz z Oprogramowaniem, zgodnie ze specyfikacją stanowiącą Załącznik nr 1 do projektowanych postanowień Umowy oraz z Formularzem ofertowym, stanowiących Załącznik nr 8 do SWZ.
   2.2. Wykonanie i dostarczenie Projektu Technicznego oraz Dokumentacji Powykonawczej w formie papierowej i elektronicznej oraz wykonanie i przeprowadzenia Wdrożenia zgodnie z Załącznikiem nr 1 A do projektowanych postanowień umowy, stanowiących Załącznik nr 8 do SWZ.
   2.3. Świadczenie Gwarancji dla Sprzętu IT i Oprogramowania przez okres 24 miesięcy oraz zapewnienie świadczenia Gwarancji przez producenta Sprzętu IT i Oprogramowania, poprzez wydanie odpowiedniego dokumentu na rzecz Zamawiającego, potwierdzającego prawo dostępu do Gwarancji producenta Sprzętu IT i Oprogramowania w okresie obowiązywania Gwarancji zgodnie z ogólnymi warunkami producenta Sprzętu IT i Oprogramowania.
   2.4. Zamawiający wymaga, aby dostarczony Sprzęt IT oraz Oprogramowanie były jednego producenta.
3. Zamawiający wymaga, aby przedmiot zamówienia był świadczony przez Wykonawcę posiadającego certyfikat w zakresie zarządzania bezpieczeństwem informacji ISO/IEC 27001 lub równoważny, wystawiony przez jednostkę akredytowaną do certyfikacji systemu zarządzania ISO/IEC 27001 i opatrzonego znakiem akredytacji.
4. Zamawiający wymaga, aby wykonanie przedmiotu zamówienia nastąpiło na warunkach i zasadach określonych w projektowanych postanowieniach umowy wraz z załącznikami, stanowiącymi Załącznik nr 8 do SWZ.

I.2. Szczegółowy opis przedmiotu zamówienia

Przedmiotowe zamówienie dotyczy dostawy Licencji na zasadach subskrypcji, przełączników sieciowych, serwera z Oprogramowaniem oraz punktów dostępowych WLAN, które mają realizować użytkownikom Centrali ARiMR funkcjonalność przewodowego i bezprzewodowego oraz bezpiecznego i niezawodnego dostępu w sieci kampusowej wraz z wdrożeniem urządzeń ze wskazanymi funkcjonalnościami. Przełączniki sieci kampusowej muszą posiadać wbudowane bezpieczeństwo i automatyzację czynności związanych z administracją i utrzymaniem sieci.

Do nowej sieci kampusowej będą podłączone wszystkie obecne urządzenia sieciowe w Centrali ARiMR oraz ośrodku w Lublinie, tj. przełączniki, komputery, drukarki oraz urządzenia mobilne, które będą działać zgodnie z przyjętą polityką bezpieczeństwa zdefiniowaną w ramach dostępu definiowanego programowo. Obecnie wykorzystywana są przełączniki firmy Cisco z wdrożoną architekturą uwierzytelnienia opartej o protokół 802.1X i bezpieczeństwem opartym na Cisco ISE ver. 2.7.

W związku z posiadaniem przez Zamawiającego wsparcia producenta dla Cisco ISE nowe rozwiązanie sieci kampusowej musi pobierać politykę dla klienta z Identity Services Engine (ISE) w oparciu o znaczniki SGT tam zdefiniowane i uwierzytelnienie w oparciu o protokół 802.1X.

Wdrożenie technologii kampusowej musi zapewniać programowalną sieć przewodową i bezprzewodową w obiektach ARiMR, zautomatyzowanym egzekwowaniu polityk oraz micro i macro segmentację sieci. Przedmiotowe działanie dotyczy dostarczenia wszystkich niezbędnych urządzeń, Licencji na zasadach subskrypcji, Oprogramowania oraz serwisu gwarancyjnego producenta oprogramowania. Sprzedawca w ramach realizacji Umowy zobowiązany jest również przeprowadzić warsztaty powdrożeniowe z wdrożonego rozwiązania.

Wdrożenie w technologii Software-Defined Access (SDA) musi zapewnić realizację przewodowego i bezprzewodowego, bezpiecznego dostępu do wszystkich obecnych usług w Centrali ARiMR, poprzez separację grup użytkowników i aplikacji dozwalając tylko na taki ruch sieciowy, który jest dozwolony w zdefiniowanej polityce bezpieczeństwa.

Jeżeli w niniejszej SWZ użyto do opisania przedmiotu zamówienia oznaczeń lub parametrów wskazujących konkretnego producenta, konkretny produkt lub wskazano znaki towarowe, patenty, normy, standardy, aprobaty techniczne lub pochodzenie urządzeń, Zamawiający dopuszcza zastosowanie produktów równoważnych, przez które należy rozumieć produkty o parametrach nie gorszych od przedstawionych w niniejszej SWZ, kompatybilne (współpracujące) z posiadanym przez Zamawiającego systemem zarządzania, w tym samym zakresie, co produkty określone w niniejszej SWZ oraz posiadające równoważne funkcje i parametry co produkt opisany w niniejszej SWZ. W takim wypadku do oferty należy załączyć dokładny opis oferowanych produktów, z którego jasno wynikać będzie zachowanie warunków równoważności.

Wykonawca ma obowiązek dostarczyć niezbędne urządzenia, Licencje oraz skonfigurować Oprogramowanie oraz wszystkie niezbędne komponenty realizujące funkcjonalność sieci kampusowej w technologii *Software-Defined Access* (SD-*Access*) dla dostępu przewodowego i bezprzewodowego w Centrali ARiMR. Zamawiający wymaga wykupienia wsparcia technicznego producenta dla dostarczonego Sprzętu IT i wdrożonego oprogramowania na okres 24 miesięcy. Wykonawca zobowiązany jest dostarczyć pakiety serwisowe dla Oprogramowania będącego przedmiotem niniejszego zamówienia oraz dokonać ich aktywacji. Aktywowane pakiety serwisowe muszą gwarantować:

- możliwość pobierania poprawek i aktualizacji posiadanego Oprogramowania oraz sygnatur w okresie obowiązywania umowy, dostęp do poprawek i aktualizacji musi posiadać Wykonawca i Zamawiający;
- producent musi zapewnić możliwość zgłaszania i obsługi ewentualnych problemów w języku polskim.
- oferowany system musi posiadać oficjalne wsparcie producenta, nie jest akceptowalne wsparcie typu „community support", oferowane przez społeczność jego użytkowników.
- Zamawiający musi mieć możliwość zgłaszania problemów z Oprogramowaniem bezpośrednio do producenta oprogramowania. Pośrednictwo firmy, która wdrażała system nie może być wymagane do skorzystania z przywileju uzyskania wsparcia.

A. <u>Przełącznik szkieletowy typ A – 2 sztuki</u>

1. W ramach zamówienia Kupujący wymaga dostawy przełącznika typu standalone, który musi być wyposażony w min. 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz 4 porty uplink 40/100 Gigabit Ethernet QSFP,

2. Przełącznik musi posiadać porty SFP/SFP+/SFP28 umożliwiające zastosowanie następujących wkładek interfejsowych:

   2.1. Gigabit Ethernet 1000Base-T,

   2.2. Gigabit Ethernet 1000Base-SX,

   2.3. Gigabit Ethernet 1000Base-LX/LH,

   2.4. Gigabit Ethernet 1000Base-EX,

   2.5. Gigabit Ethernet 1000Base-ZX,

   2.6. Gigabit Ethernet 1000Base-BX-D/U,

   2.7. 10Gigabit Ethernet 10GBase-SR,

   2.8. 10Gigabit Ethernet 10GBase-LR,

   2.9. 10Gigabit Ethernet 10GBase-ER,

   2.10. 10Gigabit Ethernet 10GBase-ZR,

   2.11. 10Gigabit Ethernet 10GBase-BX-D/U,

   2.12. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),

   2.13. 25Gigabit Ethernet 25GBASE-SR,

   2.14. 25Gigabit Ethernet typu twinax (SFP28 – SFP28),

   2.15. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),

   2.16. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF);

3. Przełącznik musi posiadać porty QSFP umożliwiające zastosowanie następujących modułów interfejsowych:

   3.1. Dla transmisji 40Gb/s:

      3.1.1. 40G-SR4,

      3.1.2. 40G-LR4,

      3.1.3. 40G-ER4,

      3.1.4. 40G-SR-BD,

      3.1.5. 40G-CSR,

      3.1.6. 40G-CSR4,

      3.1.7. 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652),

      3.1.8. adapter 40G QSFP->10G SFP+,

      3.1.9. 40Gigabit Ethernet typu twinax (QSFP - QSFP);

   3.2. Dla transmisji 100Gb/s:

3.2.1. 100GBASE-SR4,

3.2.2. 100GBASE-LR4,

3.2.3. 100Gigabit Ethernet typu twinax (QSFP - QSFP);

4. Wymagania w zakresie architektury:

4.1. Urządzenie musi być wyposażone w wymienne moduły wentylatorów,

4.2. Urządzenie musi posiadać możliwość użycia zasilacz redundantnego do pracy w trybie 1:1;

5. Wymagania w z zakresie wydajności:

5.1. Urządzenie musi posiadać min. 32MB bufor pamięci,

5.2. Urządzenie musi posiadać min. 6GB pamięci DRAM i 16GB pamięci flash,

5.3. Przepustowość przełącznika (switching capacity) musi wynosić min. 3.2 Tbps,

5.4. Prędkość przesyłania (forwarding rate) musi wynosić min.1 miliard pps (1Bpps),

5.5. Przełącznik musi obsługiwać:

5.5.1. 1000 aktywnych sieci VLAN,

5.5.2. 80 000 adresów MAC,

5.5.3. 212 000 tras IPv4,

5.5.4. 212 000 tras IPv6,

5.5.5. Ilość wpisów w listach kontroli dostępu Security ACL – 27 000,

5.5.6. ilość wpisów w listach kontroli dostępu QoS ACL – 16 000,

5.5.7. 1000 interfejsów SVI L3,

5.5.8. Jumbo frame 9198B,

5.5.9. 128 połączeń zagregowanych typu „port channel",

5.5.10.16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP;

6. Wymagania w zakresie oprogramowania/funkcjonalności.

6.1. Urządzenie musi umożliwiać obsługę protokołu NTP,

6.2. Urządzenie musi umożliwiać obsługę IGMPv1/2/3,

6.3. System operacyjny przełącznika musi umożliwiać wgrywanie poprawek bez konieczności restartowania platformy,

6.4. Urządzenie musi posiadać wsparcie dla protokołu RESTCONF,

6.5. Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

6.5.1. IEEE 802.1w Rapid Spanning Tree,

6.5.2. Per-VLAN Rapid Spanning Tree (PVRST+),

6.5.3. IEEE 802.1s Multi-Instance Spanning Tree,

6.5.4. Obsługa 1000 instancji protokołu STP;

6.6. Urządzenie musi zapewniać obsługę protokołu IEEE 802.1ab LLDP i LLDP-MED,

6.7. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)

6.8. Urządzenie musi umożliwiać realizację funkcji serwera DHCP,

6.9. Urządzenie musi umożliwiać obsługę 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

6.10. Urządzenie musi posiadać funkcjonalność autoryzacji prób logowania urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,

6.11. Urządzenie musi obsługiwać listę kontroli dostępu (ACL) następujących typów:

6.11.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

6.11.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

6.11.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

6.11.4. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

6.12. Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:

6.12.1. Musi umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

6.12.2. Musi umożliwiać implementację algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,

6.12.3. Musi umożliwiać obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

6.12.4. Urządzenie musi posiadać mechanizm klasyfikacji ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

6.12.5. Urządzenie musi posiadać możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

6.12.6. Urządzenie musi posiadać kontrolę sztormów dla ruchu broadcast/multicast/unicast,

6.12.7. Urządzenie musi posiadać możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

6.13. Przełącznik musi posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

6.14. Urządzenie musi umożliwiać realizację funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),

6.15. Urządzenie musi realizować routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:

6.15.1. Routing statyczny dla IPv4 i IPv6,

6.15.2. Routing dynamiczny dla IPv4: BGP, ISIS,

6.15.3. Routing dynamiczny dla IPv4: OSPF, EIGRP (rfc7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA),

6.15.4. Routing dynamiczny dla IPv6: OSPFv3,

6.15.5. Funkcjonalności Policy-based routing,

6.15.6. multicast routing (PIM-SM, PIM-SSM) ,

6.15.7. Obsługi protokołu redundancji bramy (VRRP) z obsługą 255 grup,

6.15.8. Obsługi 200 tuneli GRE (Generic Routing Encapsulation),

6.15.9. Obsługi 1000 wirtualnych instancji routingu (VRF),

6.16. Przełącznik musi obsługiwać protokół BFD (Bidirectional Forwarding Detection) umożliwiający szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

6.17. Przełącznik musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji,

6.18. Urządzenie musi obsługiwać protokół LISP zgodnie z RFC 6830,

6.19. Urządzenie musi umożliwiać enkapsulację ruchu przy pomocy VXLAN'ów,

6.20. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine / border,

6.21. Urządzenie musi zapewniać obsługę mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,

6.22. Urządzenie musi być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze muszą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,

6.23. Przełącznik musi umożliwiać klastrowanie, które wspiera funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami,

6.24. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

6.25. Przełącznik musi posiadać możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

6.26. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,

6.27. Przełącznik musi posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowania plików typu „pcap" do dalszej analizy przy pomocy oprogramowania zewnętrznego,

6.28. Przełącznik musi posiadać możliwość realizacji funkcji kontrolera dla radiowych punktów dostępowych WiFi z obsługą do 200 AP oraz 4000 klientów bezprzewodowych,

6.29. Przełącznik musi posiadać możliwość modyfikacji programowej takich parametrów urządzenia jak: ilości pozycji w tablicy MAC, ilość tras routingowych unicast i multicast, ilości tras w sieci MPLS VPN, ilości obsługiwanych sesji netflow,

7. Wymagania w zakresie zarządzania i konfiguracji:

7.1. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

7.2. Urządzenie musi posiadać możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Przedmiotowa funkcjonalność musi umożliwiać kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

7.3. Urządzenie musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

7.4. Urządzenie musi być wyposażone w port konsoli USB,

7.5. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

7.6. Urządzenie musi umożliwiać obsługę protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,

7.7. Przełącznik musi posidać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

7.8. Przełącznik musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

8. Wymagania w zakresie parametrów fizycznych:

8.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

8.2. Wysokość urządzenia nie może przekraczać 1 RU,

8.3. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi musi być mniejsza niż 50 cm,

9. Wymagania w zakresie wyposażenia urządzenia

9.1. Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,

9.2. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

B. <u>Przełącznik szkieletowy typ B - 2 sztuki</u>

1. W ramach zamówienie Kupujący wymaga dostawy przełącznik typu standalone, który musi być wyposażony w 16 wbudowanych portów 1/10 Gigabit Ethernet SFP/SFP+,

2. Przełącznik musi posiadać porty SFP/SFP+ umożliwiają zastosowanie następujących wkładek interfejsowych:

2.1. Gigabit Ethernet 1000Base-T,

2.2. Gigabit Ethernet 1000Base-SX,

2.3. Gigabit Ethernet 1000Base-LX/LH,

2.4. Gigabit Ethernet 1000Base-EX,

2.5. Gigabit Ethernet 1000Base-ZX,

2.6. Gigabit Ethernet 1000Base-BX-D/U,

2.7. 10Gigabit Ethernet 10GBase-SR,

2.8. 10Gigabit Ethernet 10GBase-LR,

2.9. 10Gigabit Ethernet 10GBase-LRM,

2.10. 10Gigabit Ethernet 10GBase-ER,

2.11. 10Gigabit Ethernet 10GBase-ZR,

2.12. 10Gigabit Ethernet 10GBase-BX-D/U,

2.13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),

3. Wymagania w z zakresie architektury:

3.1. Urządzenie musi być wyposażone w wymienne moduły wentylatorów,

3.2. Urządzenie musi posiadać możliwość użycia zasilacza redundantnego do pracy w trybie 1:1;

4. Wymagania w z zakresie wydajności:

4.1. Urządzenie musi posiadać min. 32MB bufor pamięci,

4.2. Urządzenie musi posiadać min. 16GB pamięci DRAM i 16GB pamięci flash,

4.3. Minimalna przepustowość przełącznika (switching capacity) musi wynosić 480 Gbps,

4.4. Minimalna prędkość przesyłania (forwarding rate) musi wynosić 360 Mpps,

4.5. Przełącznik musi obsługiwać min.

4.5.1. 1000 aktywnych sieci VLAN,

4.5.2. 64 000 adresów MAC,

4.5.3. 64 000 tras IPv4,

4.5.4. 32 000 tras IPv6,

4.5.5. Ilość wpisów w listach kontroli dostępu Security ACL – 18 000,

4.5.6. ilość wpisów w listach kontroli dostępu QoS ACL – 18 000,

4.5.7. 1000 interfejsów SVI L3,

4.5.8. Jumbo frame 9198B,

4.5.9. 64 połączenia zagregowane typu „port channel",

4.5.10.16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP;

5. Wymagania w z zakresie Oprogramowania/funkcjonalności:

5.1. Przełącznik musi umożliwiać obsługę protokołu NTP,

5.2. Przełącznik musi obsługiwać IGMPv1/2/3,

5.3. System operacyjny przełącznika musi umożliwiać wgrywanie poprawek bez konieczności restartowania platformy,

5.4. System operacyjny przełącznika musi umożliwiać wsparcie dla funkcjonalność klasyfikowania ruchu w warstwach 4-7 i na jego podstawie budowanie polityk bezpieczeństwa czy jakości usług,

5.5. System operacyjny przełącznika musi umożliwiać rozpoznawanie i klasyfikacja około 1400 predefiniowanych znanych aplikacji sieciowych oraz około 150 aplikacji szyfrujących ruch,

5.6. System operacyjny przełącznika musi posiadać wsparcie dla protokołu RESTCONF,

5.7. Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

5.7.1. IEEE 802.1w Rapid Spanning Tree,

5.7.2. Per-VLAN Rapid Spanning Tree (PVRST+),

5.7.3. IEEE 802.1s Multi-Instance Spanning Tree,

5.7.4. Obsługa 256 instancji protokołu STP;

5.8. Przełącznik musi umożliwiać obsługę protokołu IEEE 802.1ab LLDP i LLDP-MED,

5.9. Przełącznik musi umożliwiać realizację funkcji 802.1Q tunneling (QinQ),

5.10. Przełącznik musi umożliwiać realizację funkcję serwera DHCP,

5.11. Przełącznik musi umożliwiać obsługę 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

5.12. Urządzenie musi posiadać funkcjonalność autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,

5.13. Urządzenie musi umożliwiać obsługę listy kontroli dostępu (ACL) następujących typów:

5.13.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

5.13.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

5.13.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

5.13.4. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

5.14. Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:

5.14.1. Musi umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

5.14.2. Musi umożliwiać implementację algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,

5.14.3. Musi umożliwiać obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

5.14.4. Musi posiadać mechanizm klasyfikacji ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

5.14.5. Musi umożliwiać ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

5.14.6. Musi posiadać funkcjonalność kontroli sztormów dla ruchu broadcast/multicast/unicast,

5.14.7. Musi umożliwiać zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

5.15. Przełącznik musi posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

5.16. Urządzenie musi umożliwiać realizacja funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),

5.17. Urządzenie musi realizować routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:

5.17.1. Routing statyczny dla IPv4 i IPv6,

5.17.2. Routing dynamiczny dla IPv4: OSPF, BGP, IS-IS,

5.17.3. Routing dynamiczny dla IPv6: OSPFv3,

5.17.4. Funkcjonalności Policy-based routing,

5.17.5. Multicast routing (PIM-SM, PIM-SSM) ,

5.17.6. Obsługi protokołu redundancji bramy (VRRP) z obsługą 255 grup,

5.17.7. Obsługi 256 wirtualnych instancji routingu (VRF),

5.17.8. Obsługi 100 tuneli GRE (Generic Routing Encapsulation),

5.18. Przełącznik musi umożliwiać obsługę protokołu BFD (Bidirectional Forwarding Detection), któryumożliwia szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

5.19. Przełącznik musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 2000 translacji,

5.20. Urządzenie musi umożliwiać enkapsulację ruchu przy pomocy VXLAN'ów,

5.21. Urządzenie musi obsługiwać protokołu LISP zgodnie z RFC 6830,

5.22. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine,

5.23. Urządzenie musi zapewniać obsługę mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,

5.24. Urządzenie musi być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze muszą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,

5.25. Przełącznik musi umożliwiać klastrowanie, które wspiera funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami,

5.26. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

5.27. Przełącznik musi umożliwiać zdalną obserwacjęruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

5.28. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,

5.29. Przełącznik musi posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów

fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

6. Wymagania w zakresie zarządzania i konfiguracji:

   6.1. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

   6.2. Urządzenie musi umożliwiać realizację dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność musi umożliwiać kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

   6.3. Urządzenie musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi posiadać ć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

   6.4. Urządzenie musi być wyposażone w port konsoli USB,

   6.5. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

   6.6. Urządzenie musi umożliwiać obsługę protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,

   6.7. Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

   6.8. Przełącznik musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

7. Wymagania w zakresie parametrów fizycznych:

   7.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

   7.2. Wysokość urządzenia nie może przekraczać 1 RU,

   7.3. Głębokość chassis urządzenia z wentylatorami i zasilaczami musi być mniejsza niż 60 cm;

8. Wymagania w zakresie wyposażenia urządzenia:

   8.1. Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,

   8.2. Przełącznik musi być wyposażony w moduł: 8-portowy moduł 10Gigabit Ethernet SFP+

   8.3. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

C. **<u>Przełącznik dostępowy typ A (z portami uplink 25G) – 34 sztuki</u>**

1. Przełącznik musi posiadać: 48 portów 100M/1G/2.5G/5GBaseT RJ-45 UPoE (do 60W per port)
2. Przełącznik musi posiadać moduł uplinkowy 2x 25G
3. Przełącznik musi zapewnić moc dostępną dla portów PoE:

   3.1. 645W (z jednym zasilaczem o mocy 1100W),

   3.2. 645W (z dwoma zasilaczami o mocy 1100W pracującymi w układzie redundantnym),

   3.3. 1745W (z dwoma zasilaczami o mocy 1100W pracującymi w układzie współdzielenia mocy)

4. Przełącznik musi posiadać slot na moduł rozszerzeń (dający możliwość instalacji/wymiany „na gorąco" – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):

   4.1. 4x1G SFP

   4.2. 8x1/10G SFP/SFP+

   4.3. 2x40G QSFP

   4.4. 2x25G SFP28

   4.5. 4x100M/1G/2.5G/5G/10GBaseT RJ-45

5. Przełącznik musi posiadać porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia następującymi rodzajami wkładek:

5.1. Porty SFP:

5.1.1. Gigabit Ethernet 1000Base-T,

5.1.2. Gigabit Ethernet 1000Base-SX,

5.1.3. Gigabit Ethernet 1000Base-LX/LH,

5.1.4. Gigabit Ethernet 1000Base-EX,

5.1.5. Gigabit Ethernet 1000Base-ZX,

5.1.6. Gigabit Ethernet 1000Base-BX-D/U

5.2. Porty SFP/SFP+:

5.2.1. Gigabit Ethernet 1000Base-T,

5.2.2. Gigabit Ethernet 1000Base-SX,

5.2.3. Gigabit Ethernet 1000Base-LX/LH,

5.2.4. Gigabit Ethernet 1000Base-EX,

5.2.5. Gigabit Ethernet 1000Base-ZX,

5.2.6. Gigabit Ethernet 1000Base-BX-D/U,

5.2.7. 10Gigabit Ethernet 10GBase-SR,

5.2.8. 10Gigabit Ethernet 10GBase-LR,

5.2.9. 10Gigabit Ethernet 10GBase-LRM,

5.2.10. 10Gigabit Ethernet 10GBase-ER,

5.2.11. 10Gigabit Ethernet 10GBase-ZR,

5.2.12. 10Gigabit Ethernet 10GBase-BX-D/U,

5.2.13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

5.3. Porty SFP/SFP+/SFP28:

5.3.1. Gigabit Ethernet 1000Base-T,

5.3.2. Gigabit Ethernet 1000Base-SX,

5.3.3. Gigabit Ethernet 1000Base-LX/LH,

5.3.4. Gigabit Ethernet 1000Base-EX,

5.3.5. Gigabit Ethernet 1000Base-ZX,

5.3.6. Gigabit Ethernet 1000Base-BX-D/U,

5.3.7. 10Gigabit Ethernet 10GBase-SR,

5.3.8. 10Gigabit Ethernet 10GBase-LR,

5.3.9. 10Gigabit Ethernet 10GBase-ER,

5.3.10. 10Gigabit Ethernet 10GBase-ZR,

5.3.11. 10Gigabit Ethernet 10GBase-BX-D/U,

5.3.12. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

5.3.13. 25Gigabit Ethernet 25GBASE-SR,

5.3.14. 25Gigabit Ethernet typu twinax (SFP28 – SFP28)

5.3.15.10/25Gigabit Ethernet 10/25GBASE-CSR (MMF)

5.3.16.10/25Gigabit Ethernet 10/25GBASE-LR (SMF)

5.4. Porty QSFP:

5.4.1. 40G-SR4,

5.4.2. 40G-LR4,

5.4.3. 40G-ER4,

5.4.4. 40G-SR-BD,

5.4.5. adapter 40G QSFP->10G SFP+

5.4.6. kable twinax

6. Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:

6.1. Min. przepustowość w ramach stosu - 480Gb/s,

6.2. Min. 8 urządzeń w stosie,

6.3. Zarządzanie poprzez jeden adres IP,

6.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

6.5. Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),

6.6. Możliwość współdzielenia mocy zasilaczy (grupa do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie),

7. Wymagania w zakresie zasilania i chłodzenia:

7.1. Przełącznik musi posiadać redundantne i wymienne moduły wentylatorów,

7.2. Przełącznik musi posiadać możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze muszą być wymienne (i mieć możliwość instalacji/wymiany „na gorąco" – ang. hot swap),

7.3. Przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia,

7.4. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik musi umożliwiać przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),

7.5. Przełącznik musi wspierać IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

8. Wymagania w zakresie parametrów wydajnościowych:

8.1. Szybkość przełączania musi zapewnić pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):

8.1.1. Przepustowość przełącznika (switching capacity) musi wynosić min.: 640 Gb/s (bez podłączenia do stosu), 1120 Gb/s (z podłączeniem do stosu)

8.1.2. Prędkość przesyłania (forwarding rate) musi wynosić min.: 476.19 Mpps (bez podłączenia do stosu), 833.33 Mpps (z podłączeniem do stosu)

8.2. Pojemność buforu pakietów musi wynosić mi.n. – 32MB

8.3. Min. 8 GB pamięci DRAM

8.4. Pamięć flash – min. 16GB

8.5. Przełącznik musi zapewnić obsługę:

8.5.1. 1000 aktywnych sieci VLAN

8.5.2. 32000 adresów MAC

8.5.3. 8000 tras IPv4

8.5.4. 4000 tras IPv6

8.5.5. 5000 wpisów w listach kontroli dostępu Security ACL

8.5.6. 5000 wpisów w listach kontroli dostępu QoS ACL

8.5.7. 1000 interfejsów SVI L3

8.5.8. 128 interfejsów L3

8.5.9. Jumbo frame 9198B

8.5.10. 128 połączeń zagregowanych typu „port channel"

8.5.11. 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

9. Przełącznik musi umożliwiać obsługę protokołu NTP

10. Przełącznik musi obsługiwać IGMPv1/2/3 i MLDv1/2 Snooping

11. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

11.1. IEEE 802.1w Rapid Spanning Tree

11.2. Per-VLAN Rapid Spanning Tree (PVRST+)

11.3. IEEE 802.1s Multi-Instance Spanning Tree

11.4. Obsługę 128 instancji protokołu STP

11.5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)

11.6. Redundancję połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego

12. Przełącznik musi wspierać obsługę protokołu LLDP (IEEE 802.1ab) i LLDP-MED

13. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)

14. Urządzenie musi umożliwiać realizacje funkcjonalności Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

15. Urządzenie musi obsługiwać funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

16. Urządzenie musi posiadać możliwość uruchomienia funkcji serwera DHCP

17. Urządzenie musi posiadać mechanizmy związane z bezpieczeństwem sieci:

17.1. Wpoziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

17.2. Autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,

17.3. Autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

17.4. Obsługę funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,

17.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,

17.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,

17.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

17.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,

17.9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),

17.10. Obsługę funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,

17.11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),

17.12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,

17.13. Obsługa list kontroli dostępu (ACL) następujących typów:

17.13.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

17.13.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

17.13.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

17.14. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

17.15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

17.16. Musi realizować funkcję Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),

18. Przełącznik musi obsługiwać mechanizmy zapewaniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

18.1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,

18.2. bezpieczną sekwencję uruchamiania,

18.3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

19. Przełącznik musi obsługiwać mechanizmy związane z zapewnieniem jakości usług w sieci:

19.1. Musi umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

19.2. Musi umożliwiać implementację algorytmu Shaped Round Robin dla obsługi kolejek,

19.3. Musi posiadać możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

19.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

19.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

19.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,

19.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

20. Przełącznik musi umożliwiać obsługę min. następujących protokołów i mechanizmów routingu:

20.1. Routing statyczny dla IPv4 i IPv6,

20.2. Routing dynamiczny – RIP, OSPF,

20.3. Routing dynamiczny zaawansowany - IS-IS, BGP dla IPv4 i IPv6,

20.4. Routing multicastów - PIM-SM, PIM-SSM, PIM-Bidir,

20.5. Multicast Source Discovery Protocol (MSDP),

20.6. Policy-based routing (PBR),

20.7. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,

20.8. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

21. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

22. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),

23. Przełącznik musi posiadać funkcjonalność sondy IP SLA Responder,

24. Przełącznik musi wspierać obsługę dla protokołu OpenFlow 1.3,

25. Przełącznik musi posiadać funkcjonalność Time Domain Reflectometer (TDR) umożliwiającą wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,

26. Wymagania w zakresie zarządzania:

26.1. Urządzenie musi być wyposażone w port konsoli,

26.2. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

26.3. Urządzenie musi mieć możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

26.4. Plik konfiguracyjny urządzenia muszą być możliwe do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

26.5. Urządzenie musi zapewniać możliwość obsługi protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

26.6. Urządzenie musi posiadać wsparcie dla protokoły RESTCONF,

26.7. Urządzenie musi posiadać wsparcie dla protokołu gNMI,

26.8. Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

26.9. Urządzenie musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć uruchomienia z nośnika danych umieszczonego w porcie USB;

26.10. Urządzenie musi posiadać możliwość wyposażenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności min. 120GB;

26.11. Urządzenie musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

27. Wymagania w zakresie parametrów fizycznych:

27.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

27.2. Wysokość urządzenia nie może przekraczać 1 RU,

27.3. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi musi być mniejsza niż 57 cm,

28. Urządzenie musi umożliwiać realizację rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

29. Przełącznik musi posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
30. Przełącznik musi posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,
31. Przełącznik musi zapewniać wsparcie dla protokołu LISP zgodnie z RFC 6830,
32. Przełącznik musi umożliwiać obsługę 256 wirtualnych instancji routingu (VRF),
33. Przełącznik musi zapewniać obsługę protokołu BFD (Bidirectional Forwarding Detection), który umożliwia szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,
34. Przełącznik musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,
35. Przełącznik musi posiadać możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256) dla 16 pierwszych portów downlinkowych przełącznika i wszystkich portów uplinkowych przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,
36. Przełącznik musi posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,
37. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności leaf oraz spine,
38. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tc-connect, udp-echo, udp-jitter,
39. Przełącznik musi posiadać wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii,
40. Przełącznik musi posiadać funkcjonalność bramy dla usług mDNS,
41. Przełącznik musi umożliwiać zdalną obserwację ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),
42. Przełącznik musi zapewniać widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),
43. Przełącznik musi umożliwiać eksport dodatkowych pól w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa),
44. Przełącznik musi posiadać wbudowany analizator pakietów,
45. Przełącznik musi posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,
46. Urządzenie musi umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,
47. Urządzenie musi umożliwiać integrację z zewnętrzną usługą bezpieczeństwa polegającą na przechwytywaniu i sprawdzaniu zapytań DNS (DNS Query) przesyłanych przez przełącznik pod kątem bezpieczeństwa i reputacji domen, o które kierowane są zapytania,
48. Urządzenie musi posiadać wsparcie dla Audio Video Bridging (AVB).
49. Wymagania w zakresie wyposażenia urządzenia:
    - 49.1. Przełącznik musi być wyposażony w zasilacz redundantny o mocy 1100W,
    - 49.2. Przełącznik musi być wyposażony jest w moduł do łączenia w stos data wraz z kablem stakującym o długości min. 50 cm,
    - 49.3. Przełącznik musi być wyposażony w kabel o długości min. 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną,
    - 49.4. Przełącznik musi być wyposażony w moduł: 2x25G SFP28
    - 49.5. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

D. <u>Przełącznik dostępowy typ B (BEZ portów uplink) – 36 sztuk</u>

1. Przełącznik musi posiadać 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at)
2. Przełącznik musi zapewniać moc dostępną dla PoE:

2.1. 437W (z jednym zasilaczem o mocy 715W),

2.2. 437W (z dwoma zasilaczami o mocy 715W pracującymi w układzie redundantnym),

2.3. 1152W (z dwoma zasilaczami o mocy 715W pracującymi w układzie współdzielenia mocy)

3. Przełącznik musi być wyposażony w slot na moduł rozszerzeń (który umożliwia instalację/wymianę „na gorąco" – ang. hot swap) z możliwością obsadzenia nw. modułami (zależnie od potrzeb):

3.1. 4x1G SFP

3.2. 8x1/10G SFP/SFP+

3.3. 2x40G QSFP

3.4. 2x25G SFP28

3.5. 4x100M/1G/2.5G/5G/10GBaseT RJ-45

4. Przełącznik musi posiadać porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia następującymi rodzajami wkładek:

4.1. Porty SFP:

4.1.1. Gigabit Ethernet 1000Base-T,

4.1.2. Gigabit Ethernet 1000Base-SX,

4.1.3. Gigabit Ethernet 1000Base-LX/LH,

4.1.4. Gigabit Ethernet 1000Base-EX,

4.1.5. Gigabit Ethernet 1000Base-ZX,

4.1.6. Gigabit Ethernet 1000Base-BX-D/U

4.2. Porty SFP/SFP+:

4.2.1. Gigabit Ethernet 1000Base-T,

4.2.2. Gigabit Ethernet 1000Base-SX,

4.2.3. Gigabit Ethernet 1000Base-LX/LH,

4.2.4. Gigabit Ethernet 1000Base-EX,

4.2.5. Gigabit Ethernet 1000Base-ZX,

4.2.6. Gigabit Ethernet 1000Base-BX-D/U,

4.2.7. 10Gigabit Ethernet 10GBase-SR,

4.2.8. 10Gigabit Ethernet 10GBase-LR,

4.2.9. 10Gigabit Ethernet 10GBase-LRM,

4.2.10. 10Gigabit Ethernet 10GBase-ER,

4.2.11. 10Gigabit Ethernet 10GBase-ZR,

4.2.12. 10Gigabit Ethernet 10GBase-BX-D/U,

4.2.13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

4.3. Porty SFP/SFP+/SFP28:

4.3.1. Gigabit Ethernet 1000Base-T,

4.3.2. Gigabit Ethernet 1000Base-SX,

4.3.3. Gigabit Ethernet 1000Base-LX/LH,

4.3.4. Gigabit Ethernet 1000Base-EX,

4.3.5. Gigabit Ethernet 1000Base-ZX,

4.3.6. Gigabit Ethernet 1000Base-BX-D/U,

4.3.7. 10Gigabit Ethernet 10GBase-SR,

4.3.8. 10Gigabit Ethernet 10GBase-LR,

4.3.9. 10Gigabit Ethernet 10GBase-ER,

4.3.10. 10Gigabit Ethernet 10GBase-ZR,

4.3.11. 10Gigabit Ethernet 10GBase-BX-D/U,

4.3.12. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

4.3.13. 25Gigabit Ethernet 25GBASE-SR,

4.3.14. 25Gigabit Ethernet typu twinax (SFP28 – SFP28)

4.3.15. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF)

4.3.16. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)

4.4. Porty QSFP:

4.4.1. 40G-SR4,

4.4.2. 40G-LR4,

4.4.3. 40G-ER4,

4.4.4. 40G-SR-BD,

4.4.5. adapter 40G QSFP->10G SFP+

4.4.6. kable twinax

5. Przełącznik musi umożliwiać stackowanie przełączników z zapewnieniem następujących funkcjonalności:

5.1. Przepustowość w ramach stosu min. 480Gb/s,

5.2. min. 8 urządzeń w stosie,

5.3. Zarządzanie poprzez jeden adres IP,

5.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

5.5. Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),

5.6. Możliwość współdzielenia mocy zasilaczy (grupa do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie),

6. Wymagania w zakresie zasilania i chłodzenia:

6.1. Przełącznik musi być wyposażony w redundantne i wymienne moduły wentylatorów,

6.2. Przełącznik musi posiadać możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze muszą być wymienne (i posiadać możliwość instalacji/wymiany „na gorąco" – ang. hot swap),

6.3. Przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia,

6.4. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik musi umożliwiać przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),

6.5. Przełącznik musi wspierać IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

7. Wymagania w zakresie parametrów wydajnościowych, przełącznik musi zapewniać

7.1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):

7.1.1. Przepustowość przełącznika (switching capacity): 256 Gb/s (bez podłączenia do stosu), 736 Gb/s (z podłączeniem do stosu)

7.1.2. Prędkość przesyłania (forwarding rate): 190.47 Mpps (bez podłączenia do stosu), 547.62 Mpps (z podłączeniem do stosu)

7.2. Przełącznik musi posiadać min. 16MB bufor pakietów

7.3. Przełącznik musi posiadać min. 8GB pamięci DRAM

7.4. Przełącznik musi posiadać min. 16GB Pamięci flash

7.5. Przełącznik musi umożliwiać obsługę:

7.5.1. 1000 aktywnych sieci VLAN

7.5.2. 32000 adresów MAC

7.5.3. 8000 tras IPv4

7.5.4. 4000 tras IPv6

7.5.5. Ilość wpisów w listach kontroli dostępu Security ACL – 5000

7.5.6. ilość wpisów w listach kontroli dostępu QoS ACL – 5000

7.5.7. 1000 interfejsów SVI L3

7.5.8. 128 interfejsów L3

7.5.9. Jumbo frame 9198B

7.5.10.128 połączeń zagregowanych typu „port channel"

7.5.11.16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

8. Przełącznik musi umożliwiać obsługę protokołu NTP

9. Przełącznik musi umożliwiać obsługę IGMPv1/2/3 i MLDv1/2 Snooping

10. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

10.1. IEEE 802.1w Rapid Spanning Tree

10.2. Per-VLAN Rapid Spanning Tree (PVRST+)

10.3. IEEE 802.1s Multi-Instance Spanning Tree

10.4. Obsługa 128 instancji protokołu STP

10.5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)

10.6. Redundancję połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego

11. Przełącznik musi umożliwiać obsługę protokołu LLDP (IEEE 802.1ab) i LLDP-MED

12. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)

13. Przełącznik musi wspierać funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

14. Przełącznik musi umożliwiać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
15. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
16. Przełącznik musi zapewniać następujące mechanizmy związane z bezpieczeństwem sieci:
    16.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    16.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    16.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    16.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    16.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    16.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    16.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
    16.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
    16.9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
    16.10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
    16.11. Zapewniać podstawowe mechanizmy bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
    16.12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
    16.13. Obsługa list kontroli dostępu (ACL) następujących typów:
        16.13.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
        16.13.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
        16.13.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    16.14. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
    16.15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
    16.16. Realizacja funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),
17. Przełącznik musi zapewniać obsługę mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    17.1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    17.2. bezpieczna sekwencja uruchamiania,
    17.3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
18. Przełącznik musi zapewniać mechanizmy związane z zapewnieniem jakości usług w sieci:
    18.1. Umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    18.2. Umożliwiać implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
    18.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych

(Strict Priority),

18.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

18.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

18.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,

18.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

19. Przełącznik musi umożliwiać obsługę następujących protokołów i mechanizmów routingu:

19.1. Routing statyczny dla IPv4 i IPv6,

19.2. Routing dynamiczny – RIP, OSPF,

19.3. Routing dynamiczny zaawansowany - IS-IS, BGP dla IPv4 i IPv6,

19.4. Routing multicastów - PIM-SM, PIM-SSM, PIM-Bidir,

19.5. Multicast Source Discovery Protocol (MSDP),

19.6. Policy-based routing (PBR),

19.7. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,

19.8. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

20. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

21. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),

22. Przełącznik musi posiadać funkcjonalność sondy IP SLA Responder,

23. Przełącznik musi posiadać wsparcie dla protokołu OpenFlow 1.3,

24. Przełącznik musi posiadać funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,

25. Wymagania w zakresie zarządzania:

25.1. Urządzenie musi być wyposażone w port konsoli,

25.2. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

25.3. Urządzenie musi zapewniać możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

25.4. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej muci być zapewniona możliwość uruchomienia urządzenia z nową konfiguracją,

25.5. Urządzenie musi posiadać możliwość obsługi protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

25.6. Urządzenie musi posiadać wsparcie dla protokoły RESTCONF,

25.7. Urządzenie musi posiadać wsparcie dla protokołu gNMI,

25.8. Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

25.9. Przełącznik musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;

25.10. Urządzenie musi posiadać możliwość wyposażenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności min. 120GB;

25.11. Przełącznik musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

26. Wymagania w zakresie parametrów fizycznych:

    26.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

    26.2. Wysokość urządzenia nie może przekraczać 1 RU,

    26.3. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi musi być mniejsza niż 50 cm,

27. Urządzenie musi umożliwiać realizację rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

28. Urządzenie musi mieć możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

29. Urządzenie musi mieć możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,

30. Urządzenie musi zapewniać wsparcie dla protokołu LISP zgodnie z RFC 6830,

31. Urządzenie musi zapewniać obsługę 256 wirtualnych instancji routingu (VRF),

32. Urządzenie musi zapewniać obsługę protokołu BFD (Bidirectional Forwarding Detection) który umożliwia szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

33. Urządzenie musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,

34. Urządzenie musi posiadać możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256) dla wszystkich portów przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,

35. Urządzenie musi posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,

36. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności leaf oraz spine,

37. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,

38. Przełącznik musi posiadać wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii,

39. Przełącznik musi posiadać funkcjonalność bramy dla usług mDNS,

40. Przełącznik musi umożliwiać zdalną obserwację ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

41. Przełącznik musi zapewniać widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),

42. Przełącznik musi zapewniać możliwość eksportu dodatkowych pólł w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa),

43. Przełącznik musi posiadać wbudowany analizator pakietów,

44. Przełącznik musi posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,

45. Urządzenie musi umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,

46. Integracja z zewnętrzną usługą bezpieczeństwa polegającą na przechwytywaniu i sprawdzaniu zapytań DNS (DNS Query) przesyłanych przez przełącznik pod kątem bezpieczeństwa i reputacji domen, o które kierowane są zapytania,

47. Urządzenie musi posiadać wsparcie dla Audio Video Bridging (AVB).

48. Wymagania w zakresie wyposażenia urządzenia:

48.1. Przełącznik musi być wyposażony w zasilacz redundantny o mocy 715W,

48.2. Przełącznik musi być wyposażony w moduł do łączenia w stos data wraz z kablem stakującym o długości 50 cm,

48.3. Przełącznik musi być wyposażony w kabel o długości 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną,

48.4. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

E. <u>Przełącznik dostępowy typ C – 2 sztuki</u>

1. Przełącznik musi być wyposażony w 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP
2. Przełącznik musi zapewniać moc dostępna dla PoE:
   2.1. 505W (z jednym zasilaczem o mocy 715W),
   2.2. 505W (z dwoma zasilaczami o mocy 715W pracującymi w układzie redundantnym),
   2.3. 1220W (z dwoma zasilaczami o mocy 715W pracującymi w układzie współdzielenia mocy)
   2.4. 1440W (z zasilaczem pierwszym o mocy 715W oraz drugim o mocy 1100W pracującymi w układzie współdzielenia mocy)
3. Przełącznik musi posiadać porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
   3.1. Gigabit Ethernet 1000Base-T,
   3.2. Gigabit Ethernet 1000Base-SX,
   3.3. Gigabit Ethernet 1000Base-LX/LH,
   3.4. Gigabit Ethernet 1000Base-EX,
   3.5. Gigabit Ethernet 1000Base-ZX,
   3.6. Gigabit Ethernet 1000Base-BX-D/U,
   3.7. 10Gigabit Ethernet 10GBase-SR,
   3.8. 10Gigabit Ethernet 10GBase-LR,
   3.9. 10Gigabit Ethernet 10GBase-LRM,
   3.10. 10Gigabit Ethernet 10GBase-ER,
   3.11. 10Gigabit Ethernet 10GBase-ZR,
   3.12. 10Gigabit Ethernet 10GBase-BX-D/U,
   3.13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
4. Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
   4.1. Przepustowość w ramach stosu - 320Gb/s,
   4.2. Min. 8 urządzeń w stosie,
   4.3. Zarządzanie poprzez jeden adres IP,
   4.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
   4.5. Posiadać wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),
5. Wymagania w zakresie zasilania i chłodzenia:

5.1. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów,

5.2. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze musza być wymienne (i posiadać możliwość instalacji/wymiany „na gorąco" – ang. hot swap),

5.3. Przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia,

5.4. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik musi umożliwiać przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),

5.5. Przełącznik musi wspierać IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

6. Wymagania w zakresie parametrów wydajnościowych:

6.1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):

6.1.1. Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 496 Gb/s (z podłączeniem do stosu)

6.1.2. Prędkość przesyłania (forwarding rate): 130.95 Mpps (bez podłączenia do stosu), 369.05 Mpps (z podłączeniem do stosu)

6.2. Pojemność bufora pakietów – min. 16MB

6.3. Przełącznik musi obsługiwać:

6.3.1. 1000 aktywnych sieci VLAN

6.3.2. 32000 adresów MAC

6.3.3. 8000 tras IPv4

6.3.4. 4000 tras IPv6

6.3.5. Ilość wpisów w listach kontroli dostępu Security ACL – 5000

6.3.6. ilość wpisów w listach kontroli dostępu QoS ACL – 5000

6.3.7. 1000 interfejsów SVI L3

6.3.8. 128 interfejsów L3

6.3.9. Jumbo frame 9198B

6.3.10. 128 połączeń zagregowanych typu „port channel"

6.3.11. 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

7. Przełącznik musi zapewniać obsługę protokołu NTP

8. Przełącznik musi zapewniać obsługę IGMPv1/2/3 i MLDv1/2 Snooping

9. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

9.1. IEEE 802.1w Rapid Spanning Tree

9.2. Per-VLAN Rapid Spanning Tree (PVRST+)

9.3. IEEE 802.1s Multi-Instance Spanning Tree

9.4. Obsługa 128 instancji protokołu STP

9.5. Redundancję połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego

10. Przełącznik musi zapewniać obsługę protokołu LLDP (IEEE 802.1ab) i LLDP-MED

11. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)

12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
13. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
14. Możliwość uruchomienia funkcji serwera DHCP
15. Przełącznik musi posiadać mechanizmy związane z bezpieczeństwem sieci:
    - 15.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
    - 15.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    - 15.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    - 15.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    - 15.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    - 15.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    - 15.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
    - 15.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
    - 15.9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
    - 15.10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
    - 15.11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
    - 15.12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
    - 15.13. Obsługa list kontroli dostępu (ACL) następujących typów:
      - 15.13.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
      - 15.13.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
      - 15.13.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
      - 15.13.4. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
    - 15.14. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
    - 15.15. Funkcja Private VLAN;
16. Przełącznik musi zapewnić obsługę mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    - 16.1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    - 16.2. bezpieczna sekwencja uruchamiania,
    - 16.3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
17. Przełącznik musi zapewnić mechanizmy związane z zapewnieniem jakości usług w sieci:
    - 17.1. Możliwość implementacji min. 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    - 17.2. Możliwość implementacji algorytmu Shaped Round Robin dla obsługi kolejek,

17.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

17.4. Możliwość klasyfikacji ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

17.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

17.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,

17.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

18. Przełącznik musi umożliwiać obsługę następujących protokołów i mechanizmów routingu:

18.1. Routing statyczny dla IPv4 i IPv6,

18.2. Routing dynamiczny – RIP, OSPF, IS-IS

18.3. Policy-based routing (PBR),

18.4. Routing multicastów - PIM-SM, PIM-SSM,

18.5. Multicast Source Discovery Protocol (MSDP),

18.6. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,

18.7. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

19. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

20. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),

21. Przełącznik musi posiadać wsparcie dla protokołu OpenFlow 1.3

22. Przełącznik musi posiadać funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,

23. Wymagania w zakresie zarządzania:

23.1. Przełącznik musi mieć wbudowany port konsoli,

23.2. Przełącznik musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

23.3. Przełącznik musi posiadać możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adapteraUSB Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność ta musi umożliwiać kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

23.4. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

23.5. Przełącznik musi zapewniać obsługę protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

23.6. Przełącznik musi posiadać wsparcie dla protokoły RESTCONF,

23.7. Przełącznik musi posiadać wsparcie dla protokołu gNMI,

23.8. Przełącznik musi posiadaća diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

23.9. Przełącznik musi posiadać a wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,

23.10. Przełącznik musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;

23.11. Urządzenie musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i

nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

23.12. Urządzenie musi posiadać wbudowany graficzny interfejs zarządzania przełącznikiem.

24. Przełącznik musi umożliwiać realizację rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

25. Przełącznik musi umożliwiać eksport dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)

26. Przełącznik musi posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

27. Przełącznik musi posiadać możliwość uruchamiania zdefiniowanych w Pythonie skryptów bezpośrednio na urządzeniu

28. Przełącznik musi posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,

29. Przełącznik musi posiadać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów Edge/VTEP,

30. Przełącznik musi posiadać wsparcie dla protokołu LISP zgodnie z RFC 6830,

31. Przełącznik musi zapewniać obsługę min. 256 wirtualnych instancji routingu (VRF),

32. Przełącznik musi posiadać obsługę protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

33. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,

34. Przełącznik musi posiadać wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii,

35. Przełącznik musi posiadać funkcjonalność bramy dla usług mDNS,

36. Przełącznik musi realizować funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,

37. Przełącznik musi posiadać możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

38. Przełącznik musi posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,

39. Przełącznik musi zapewniać widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),

40. Przełącznik musi posiadać wbudowany analizator pakietów umożliwiamy zbieranie ruchu w czasie rzeczywistym, dekodowanie ruchu i zapisywanie ich w formie pliku .pcap lub do pamięci urządzenia (flash, zewnętrzne usb). Wynik dekodowania ruchu może zostać wyświetlony na konsoli urządzenia lub w zewnętrznym oprogramowaniu typu Wireshark.

41. Urządzenie musi umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,

42. Integracja z zewnętrzną usługą bezpieczeństwa polegającą na przechwytywaniu i sprawdzaniu zapytań DNS (DNS Query) przesyłanych przez przełącznik pod kątem bezpieczeństwa i reputacji domen, o które kierowane są zapytania,

43. Wymagania w zakresie parametrów fizycznych:

    43.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

    43.2. Wysokość urządzenia nie może przekraczać 1 RU,

44. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi nie może być mniejsza niż 50 cm,

45. Wymagania w zakresie wyposażenia urządzenia:

    45.1. Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,

    45.2. Przełącznik musi być wyposażony w moduł do łączenia w stos wraz z kablem stakującym o długości 50 cm,

    45.3. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz

wsparcie producenta na okres 24 miesięcy.

F. **Akcesoria do przełączników i kontrolerów muszą być wyposażone w gwarancję oraz wsparcie producenta na okres 24 miesięcy:**

1. W ramach zamówienia Kupujący wymaga dostarczenia następujących akcesoriów do urządzeń dostępowych typu A i B

   1.1. Moduł optyczny interfejsowy SFP28 typu 10/25Gigabit Ethernet 10/25GBASE-CSR do przełączników dostępowych typ A – **36 sztuk** - *Wkładka interfejsowa w standardzie SFP28, pracująca w standardzie 10/25Gigabit Ethernet 10/25GBASE-CSR. Kupujący wymaga aby wkładka była kompatybilna z wyspecyfikowanym przełącznikami dostępowymi typu A.*

   1.2. Kabel do łączenia w stos do przełączników dostępowych typ A i B o dł. 3m – **24 sztuki** - *Kabel połączeniowy o dł. 3 metrów przystosowany do łączenia przełączników dostępowych typ A i B w stos.*

   1.3. Kabel do łączenia w stos zasilający do przełączników dostępowych typ A i B o dł. 1.5m – **24 sztuki** - *Kabel połączeniowy o dł. 1.5 metra przystosowany do łączenia przełączników dostępowych typ A i B w stos zasilający.*

   1.4. Kabel do łączenia w stos do przełączników dostępowych typ A i B o dł. 1m – **6 sztuk** - *Kabel połączeniowy o dł. 1 metr przystosowany do łączenia przełączników dostępowych typ A i B w stos.*

2. W ramach zamówienia Kupujący wymaga dostarczenia następujących akcesoriów do przełącznika szkieletowego typu A i C

   2.1. Moduł optyczny interfejsowy SFP28 typu 10/25Gigabit Ethernet 10/25GBASE-CSR do przełączników szkieletowych typ A – **36 sztuk** - *Wkładka interfejsowa w standardzie SFP28, kompatybilna z przełącznikami szkieletowymi typ A, pracująca w standardzie 10/25Gigabit Ethernet 10/25GBASE-CSR.*

   2.2. Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ A – **4 sztuki** - *Kabel połączeniowy typu twinax o dł. 3 metrów umożliwiający połączenie ze sobą przełączników szkieletowych typu A, przy pomocy interfejsów SFP+ pracujących z prędkością 10 Gb/s.*

   2.3. Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ A i przełączników dostępowych typ C – **4 sztuki** - *Kabel połączeniowy typu twinax o dł. 3 metrów umożliwiający połączenie ze sobą przełączników szkieletowych typu A i przełączników dostępowych typ C w węźle centralnym, przy pomocy interfejsów SFP+ pracujących z prędkością 10 Gb/s.*

   2.4. Kabel połączeniowy typu twinax 40G 3m do przełączników szkieletowych typ A – **4 szt.** - *Kabel połączeniowy typu twinax o dł. 3 metrów umożliwiający połączenie ze sobą przełączników szkieletowych typu A, przy pomocy interfejsów SFP+ pracujących z prędkością 40 Gb/s.*

   2.5. Moduł optyczny SFP+ typu 10G jednomodowy LR do przełączników szkieletowych typ A - **4 sztuki** - *Wkładka interfejsowa w standardzie SFP+ typu LR 10Gigabit Ethernet służąca do podłączenia łącz od operatorów telekomunikacyjnych.*

3. W ramach zamówienia Kupujący wymaga dostarczenia następujących akcesoriów do przełącznika szkieletowego typ B

   3.1. Moduł optyczny interfejsowy SFP typu 10GBASE-LRM do przełączników szkieletowych typ B – **10 sztuk** - *Wkładka interfejsowa w standardzie SFP+, kompatybilna z przełącznikami szkieletowymi typ B, pracująca w standardzie 10GBASE-LRM.*

   3.2. Moduł optyczny interfejsowy SFP typu 10GBASE-SR do przełączników szkieletowych typ B – **10 sztuk** - *Wkładka interfejsowa w standardzie SFP+, kompatybilna z przełącznikami szkieletowymi typ B, pracująca w standardzie 10GBASE-SR.*

   3.3. Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ B – **4 sztuki** - *Kabel połączeniowy typu twinax o dł. 3 metrów umożliwiający połączenie ze sobą przełączników szkieletowych typu B, przy pomocy interfejsów SFP+ pracujących z prędkością 10 Gb/s.*

4. W ramach zamówienia Kupujący wymaga dostarczenia następujących akcesoria do kontrolerów WiFi

   4.1. Kabel połączeniowy typu twinax 10G 7m do kontrolerów sprzętowych WiFi typ A – **4 sztuki** - *Kabel połączeniowy typu twinax o dł. 7 metrów umożliwiający połączenie do przełączników szkieletowych typ A lub przełączników dostępowych typ C sprzętowych kontrolerów WiFi typ A z prędkością 10 Gb/s z wykorzystaniem interfejsów SFP+.*

   4.2. Moduł optyczny SFP+ z oferty producenta urządzenia 10GBase-SR – **8 sztuk** - *Wkładka interfejsowa w standardzie SFP+ służąca do podłączenia kontrolerów do sieci LAN*

G. System zarządzania i monitorowania siecią w lokalizacji Warszawa oraz monitoringu sieci LAN w pozostałych lokalizacjach Zamawiającego (wraz z dedykowanym serwerem, który może zostać zamontowany ww szafie rack 19"- appliance, posiadający wsparcie producenta Oprogramowania) - 1 komplet

1. Przedmiotem zamówienia jest zakup graficznego systemu do zarządzania i monitorowania sieci kampusowej przewodowej oraz bezprzewodowej.

2. Minimalne wymagania w zakresie funkcjonalności podstawowych systemu w zakresie monitoringu sieci. System musi:

   2.1. Zbierać i zapamiętywać do 7 dni wstecz dane telemetryczne o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji z różnych źródeł danych: SNMP, Syslog, NetFlow, sensory bezprzewodowe WiFi;

   2.2. Analizować i korelować dane telemetrycznych o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji na podstawie różnych źródeł danych: SNMP, Syslog, NetFlow, sensory bezprzewodowe WiFi;

   2.3. Umożliwiać wizualizację topologii sieci wraz połączeniami oraz wizualizacją stanu pracy danego monitorowanego obiektu;

   2.4. zbierać i prezentować szczegółową informację o ilości użytkowników przewodowych podłączonych do sieci oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci z podaniem typowych przyczyn braku podłączenia np. problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej. Szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP;

   2.5. zbierać i prezentować szczegółową informację o ilości użytkowników bezprzewodowych podłączonych do sieci z rozbiciem na grupę użytkowników o dobrej jakości i złej jakości pracy oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci bezprzewodowej z podaniem typowych przyczyn braku podłączenia np. problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej. Szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP;

   2.6. Generować automatyczne komunikaty o stwierdzonych nieprawidłowościach w pracy sieci w oparciu o skorelowane informacje zbierane przez system z urządzeń sieciowych wraz z sugestią przyczyny, sposobu rozwiązania problemu oraz dalszych kroków diagnostycznych dla poszczególnych urządzeń sieciowych;

   2.7. Posiadać narzędzie do śledzenia ścieżki sieciowej dla danego ruchu w sieci np. w relacji pomiędzy dwoma hostami wraz podaniem informacji o wszystkich węzłach na ścieżce, ich stanu, topologii fizycznej i logicznej np. zaznaczenie tunelowania ruchu bezprzewodowego, dokładną informacją o interfejsach, przez który płynie ruch;

   2.8. Wyznaczać na postawie analizy danych telemetrycznych dla każdego z urządzeń sieciowych, grupy użytkowników, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji indeksu liczbowego określającego jakość pracy danego monitorowanego obiektu wraz z wizualizacją na skali czasu zmiany wartości indeksów jakości pracy dla grup urządzeń sieciowych, grupy użytkowników przewodowych i bezprzewodowych, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji;

3. Minimalne wymagania w zakresie wykrywania i analizy problemów w sieci. System musi

   3.1. Dokonywać automatycznej analizy zdarzeń w sieci oraz identyfikacja i wyświetlać na tej podstawie problemy w działaniu sieci na poziomie całej sieci lub poszczególnych monitorowanych obiektów np. problemy związane z danym urządzeniem, użytkownikiem lub aplikacją w celu natychmiastowego dostarczenia danych diagnostycznych;

   3.2. Automatycznie priorytetyzować problemy;

4. Minimalne wymagania w zakresie monitoring urządzeń. System musi

   4.1. Zapewniać monitoring dostępności i osiągalności poszczególnych urządzeń sieciowych;

   4.2. W zakresie sieci bezprzewodowej prezentować wykresy:

      4.2.1. Ilości aktywnych i nieaktywnych punktów radiowych z podaniem dokładnej listy urządzeń w każdej z kategorii;

      4.2.2. Listy radiowych punktów dostępowych wg. ilości podłączonych klientów bezprzewodowych;

      4.2.3. Listy radiowych punktów dostępowych wg. poziomu zakłóceń i interferencji w funkcji pasma transmisji 2.4 GHz, 5 GHz;

   4.3. Prezentować pełną listę wszystkich monitorowanych urządzeń sieciowych w całej sieci lub w danej domenie lub

lokalizacji z podaniem modelu urządzenia, wersji systemu operacyjnego, adresu IP, stanu pracy, osiągalności, ilości zidentyfikowanych problemów, lokalizacji geograficznej. Możliwość eksportu danych w postaci pliku CSV;

4.4. Posiadać możliwość łatwego filtrowania listy urządzeń wg. kryteriów:

4.4.1. Typ urządzenia: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, radiowy punkt dostępowy, kontroler WLAN;

4.4.2. Stan pracy urządzenia;

4.4.3. Lokalizacja;

4.4.4. Model urządzenia;

4.4.5. Wersja systemu operacyjnego;

4.4.6. Adres IP;

5. System musi umożliwiać szczegółowy monitoring każdego z urządzeń sieciowych obejmujący:

5.1. Szczegółową informację o następujących parametrach pracy urządzenia w dowolnym momencie pracy urządzenia do 7 dni wstecz. System musi monitorować min. parametry: utylizacja pamięci, utylizacja CPU, dostępność łączy uplinkowych (w górę sieci), poziom błędów na linkach, skojarzone zdarzenia zarejestrowane w systemie;

5.2. Szczegółową listę wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz) problemów skojarzonych z danym urządzeniem;

5.3. Schemat topologii sieci, w której znajduje się dane urządzenie;

5.4. Dostęp do zdarzeń zarejestrowanych w systemie związanych z danym urządzeniem z możliwością filtrowanie wg. ważności;

5.5. Możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia do danego innego miejsca (adresu IP);

5.6. Możliwość bezpośredniego z poziomu konsoli graficznej systemu zarządzania i monitorowania dostępu do konsoli urządzenia lub narzędzia umożliwiającego zdalne wydawanie komend na urządzeniu;

5.7. System musi prezentować szczegółowe informacje o urządzeniu obejmujące:

5.7.1. Wykres czasowy utylizacji CPU;

5.7.2. Wykres czasowy utylizacji pamięci;

5.7.3. Wykres czasowy dostępności urządzenia;

5.7.4. Wykres czasowy temperatury urządzenia;

5.7.5. Informacje o poszczególnych interfejsach urządzeń w uwzględnieniem: stanu interfejsu, typu, numer skonfigurowanej sieci VLAN, MAC adresu podłączonego urządzenia, prędkość linku, FDX/HDX;

5.7.6. Dla każdego z monitorowanych interfejsów informacje o:

5.7.6.1. Wykres czasowy dostępności interfejsu;

5.7.6.2. Wykres czasowy utylizacji interfejsu niezależnie w kierunku nadawczym i odbiorczym;

5.7.6.3. Wykres czasowy poziomu błędów niezależnie w kierunku nadawczym i odbiorczym;

5.7.7. W przypadku urządzeń pracujących jako urządzenia w sieci SDN typu Network Fabric szczegółowe informacje na temat stanu połączenia z siecią podkładową, stanu podłączenia do systemu kontroli dostępu w sieci Network Fabric;

6. Minimalne wymagania w zakresie monitoringu użytkowników:

6.1. System musi monitorować i prezentować szczegółowe informacje o użytkowniku końcowym i urządzeniach na których pracuje takie jak:

6.1.1. identyfikator użytkownika,

6.1.2. nazwa hosta lub hostów, na których pracuje,

6.1.3. adres MAC hosta lub hostów,

6.1.4. adres IPv4 i IPv6 hosta lub hostów,

6.1.5. typ urządzenia,

6.1.6. urządzenie, do którego jest podłączone dane urządzenie końcowe wykorzystywane przez użytkownika,

6.1.7. lokalizacja geograficzna;

6.2. System musi monitorować i prezentować szczegółową informację o następujących parametrach pracy urządzenia końcowego wykorzystywanego przez użytkownika w dowolnym momencie do 7 dni wstecz. System musi monitorować min. następujące parametry: stan podłączenia do sieci, dla urządzeń bezprzewodowych: poziom sygnału RSSI, poziom szumów SNR, przepustowość połączenia, ilość danych otrzymanych i nadawanych, SSID sieci, do której jest podłączone urządzenie końcowe, nazwa radiowego punktu dostępowego, wykorzystywany kanał radiowy i pasmo.

6.3. System musi monitorować i prezentować szczegółową listę wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz) problemów skojarzonych z danym urządzeniem końcowym;

6.4. System musi prezentować schemat topologii sieci z zaznaczeniem urządzenia dostępowego do którego jest podłączony dane urządzenie końcowe;

6.5. Dostęp do zdarzeń zarejestrowanych w systemie związanych z danym użytkownikiem z możliwością filtrowania wg. ważności;

6.6. System musi posiadać możliwość uruchomienia narzędzia do analizy ścieżki od danego użytkownika do danego innego miejsca (adresu IP);

6.7. System musi zbierać, prezentować i monitorować informacje o generowanym ruchu sieciowym przez użytkownika na danym urządzeniu końcowym z podziałem na aplikacje biznesowe oraz niebiznesowe. Szczegółowe informacje dla każdej z aplikacji takie jak: nazwa aplikacji, indeks jakości działania aplikacji w sieci, ilość ruchu (w bajtach), średnia przepustowość (w bps), parametry QoS faktyczne oraz oczekiwane, straty pakietów (maksymalne i średnie), opóźnienie sieciowe (maksymalne i średnie), jitter (maksymalny i średni);

6.8. System musi monitorować szczegółowe informacje o urządzeniu końcowym wykorzystywanym przez użytkownika:

6.8.1. Wykres czasowy ilości danych nadawanych i otrzymywanych;

6.8.2. Wykres czasowy ilości generowanych zapytań DNS i otrzymywanych odpowiedzi;

6.8.3. Dla urządzeń bezprzewodowych wykres czasowy zmian wartości mocy sygnału radiowego RSSI oraz zmian wartości poziomu szumów SNR;

7. Minimalne wymagania w zakresie monitoringu aplikacji:

7.1. System musi prezentować szczegółowe informacje o aplikacjach wykorzystywanych w sieci takie jak: lista wszystkich wykrytych aplikacji z podaniem nazw aplikacji, klas ruchu, ilości ruchu generowanego, średniej przepustowości, straty pakietów, opóźnienia sieciowego oraz wykrytych problemów związanych z daną aplikacją;

7.2. System musi prezentować szczegółowe wykresy czasowe parametrów działania każdej z aplikacji z uwzględnieniem: przepustowości wykorzystywanej przez daną aplikację, strat pakietów, jitter, opóźnienia sieciowego, opóźnienia sieciowego po stronie klienta, opóźnienia sieciowego po stronie serwera, opóźnienia generowanego przez serwer aplikacyjny;

7.3. System musi monitorować i prezentować szczegółową listę wszystkich użytkowników wykorzysujących daną aplikację w sieci z podaniem urządzenia końcowego, który wykorzystuje daną aplikację;

8. Minimalne wymagania w zakresie monitoringu sieci bezprzewodowej.

8.1. System musi umożliwiać wizualizację graficzną rozmieszczenia poszczególnych radiowych punktów dostępowych, sensorów oraz klientów sieci bezprzewodowej na mapie budynku;

8.2. System musi umożliwiać graficzne planowanie i zarządzanie siecią bezprzewodową (hierarchiczne mapy lokalizacji, mapy zasięgu) z wykorzystaniem własnych planów budynków;

8.3. System musi umożliwiać monitorowanie informacji takich jak: poziom szumu, poziom sygnału, interferencje sygnału pochodzących z punktów dostępowych;

8.4. System musi umożliwiać współpracę z systemami lokalizacji urządzeń radiowych (punktów dostępowych, klientów, tagów) z prezentacją graficzną na mapie;

8.5. System musi posiadać narzędzie pozwalające na wykonywanie testów poprawności pracy sieci bezprzewodowej poprzez generowanie syntetycznego ruchu przez punkty dostępowe lub dedykowane sensory bezprzewodowe pozwalające na badanie/wykonanie testu:

8.5.1. czasu podłączania się do sieci: asocjacja, uwierzytelnienie, adresacja z DHCP;

8.5.2. pracy usług: DNS, RADIUS, dostępność bramy, dostępność określonych adresów IP;

8.5.3. pracy aplikacji: POP3, IMAP, Outlook Web Access, FTP, HTTP, HTTPS;

8.6. Możliwość określenia czasu lub częstotliwości wykonywania testów;

9. Minimalne wymagane funkcjonalności z zakresu zarządzania siecią:

9.1. Hierarchizacja zarządzania siecią odzwierciedlająca hierarchię geograficzną tj. możliwość podziału sieci na kilka poziomów geograficznych np. region, kraj, miasto, budynek, piętro;

9.2. Wizualizacja graficzna na mapie lokalizacji poszczególnych urządzeń sieciowych – automatyczne rozmieszczanie urządzeń na postawie adresów pocztowych;

9.3. Możliwość wgrywania własnych planów budynków z dokładnością do poszczególnych pięter;

9.4. Obsługa REST API;

9.5. Integracja z system uwierzytelniania w celu otrzymywania informacji o tym jaki użytkownik jest związany z jakim urządzeniem, szczegółowej informacji o przebiegu procesu uwierzytelniania do sieci. Uwzględnienie tych danych w procesie wyznaczania indeksów jakości pracy użytkowników jak również w procesie diagnostyki problemów w sieci;

9.6. Mechanizm automatycznej aktualizacji wersji systemu bezpośrednio z chmury producenta wtedy, kiedy pojawiają się nowe wersje;

9.7. Wbudowane narzędzia do automatycznego tworzenia polityki QoS dla całej sieci w oparciu o wbudowane wzorce aplikacji, z możliwością tworzenia własnych wzorców. Możliwości dokonywania zmian w polityce i jej szybkiej implementacji oraz możliwość cofania zmian bez konieczności ręcznej rekonfiguracji urządzeń sieciowych;

9.8. Funkcjonalność automatycznego wykrywania urządzeń sieciowych w oparciu o SNMP, CLI, http, SSH;

9.9. Możliwość tworzenia parametryzowanych wzorców konfiguracyjnych dla urządzeń w oparciu o język skryptowy;

9.10. Inwentaryzacja urządzeń oraz oprogramowania;

9.11. Zarządzanie wersjami oprogramowania z możliwością wskazania wersji obowiązujących;

9.12. Narzędzie do bezdotykowej konfiguracji urządzeń sieciowych (Plug and Play lub Zero Touch Deployment);

9.13. Możliwość definiowania profili sieciowych oraz parametrów sieciowych takich jak: serwery TACAS, Radius, NTP, Syslog, NetFlow, DNS, DHCP dla poszczególnych poziomów hierarchii sieciowej niezależnie lub dziedziczenie tych ustawień z poziomu wyższego w dół hierarchii. Centralne zarządzania parametrami dostępowymi do urządzeń wraz z możliwością ich zmiany dla jednego urządzenia, grupy urządzeń lub całej sieci;

10. Minimalne wymagania funkcjonalności z zakresu zarządzania siecią SDA (funkcje kontrolera SDA):

10.1. Zarządzanie i monitorowanie siecią kampusową SDA jako jednolitą siecią typu Network Fabric;

10.2. Graficzny interfejs użytkownika umożliwiający tworzenie segmentacji i polityki bezpieczeństwa w sieci SDA jak również provisioning urządzeń sieciowych tworzących sieć typu Network Fabric;

10.3. Funkcje centralnego kontrolera SDA umożliwiające centralne programowanie urządzeń oraz centralny monitoring i analizę strumieni telemetrycznych z sieci w celu wykrywania nieprawidłowości w jej działaniu;

10.4. Centralne zarządzanie polityką bezpieczeństwa poprzez określenie relacji pomiędzy segmentami logicznymi w sieci SDA (grupami urządzeń, użytkowników lub aplikacji) z możliwością tworzenia kontraktów dla wymiany ruchu pomiędzy tymi grupami;

10.5. Filtracja ruchu niezależna od adresaci IP w oparciu o rolę użytkownika lub urządzenia w sieci i zdefiniowane relacje;

10.6. Zarządzanie pulami adresowymi używanymi w sieci SDA;

10.7. Zarządzanie sposobem uwierzytelniania w sieci Network Fabric na poziomie globalnym oraz na poziomie każdego z portów urządzeń dostępowych niezależnie;

10.8. Logiczny podział sieci na makrosegmenty i mikrosegmenty przy użyciu narzędzia graficznego;

10.9. Logiczny podział użytkowników i urządzeń na grupy i określenie relacji pomiędzy nimi;

10.10. Tworzenie podsieci IP rozciągniętej na dowolne porty dostępowe w ramach Network Fabric;

10.11. Możliwość filtrowania ruchu pomiędzy urządzeniami pracującymi w jednej grupie logicznej i/lub podsieci IP jak również pomiędzy różnymi grupami logicznymi i/lub podsieciami IP bez konieczności stosowania ACL opartych o adresy IP;

10.12. Automatyzacja procesu tworzenia Network Fabric (dodawanie urządzeń, przypisywanie im roli w sieci, określanie poziomów uwierzytelnienia użytkowników i urządzeń na brzegu sieci) bez konieczności używania linii komend (CLI));

10.13. Automatyczne wykrywanie urządzeń sieciowych;

10.14. Narzędzie do automatycznego wykrywania nowo podłączonych urządzeń sieciowych i ich podłączenia do sieci podkładowej (underlay) wraz z konfiguracją urządzeń;

10.15. Jednolite i zunifikowane rozwiązanie dla sieci kampusowej przewodowej oraz bezprzewodowej tj. możliwość tworzenia Network Fabric obejmującej zarówno sieć przewodową jak i bezprzewodową;

11. Pozostałe wymagania

11.1. System musi być dostarczony jako klaster HA składający się minimum z trzech dedykowanych serwerów sieciowych appliance w wersji sprzętowej (fizycznej) umożliwiającej uzyskanie następujących wartości skalowalności:

11.1.1. zarządzanie i monitorowanie 2000 urządzeń sieciowych (przełączniki / routery) w tym dostarczanych modeli

11.1.2. zarządzanie i monitorowanie 6000 radiowych punktów dostępowych WiFi;

11.1.3. monitorowanie 40 000 klientów sieci.

11.2. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

12. Rozwiązanie musi być kompatybilne z posiadanym i użytkowanym przez Zamawiającego systemem kontroli dostępu Cisco ISE w min wersji 2.7.

H. **Kontroler WiFi – 2 sztuki**

1. Urządzenie musi umożliwiać centralną kontrolę punktów dostępu bezprzewodowego w tym:

1.1. zarządzanie politykami bezpieczeństwa

1.2. wykrywanie zagrożeń w sieci bezprzewodowej

1.3. zarządzanie pasmem radiowym

1.4. zarządzanie mobilnością

1.5. zarządzanie jakością transmisji zgodnie z protokołem CAPWAP (RFC 5415)

2. Urządzenie musi obsługiwać 250 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia o kolejne 250 przez dodanie odpowiedniej licencji

3. Urządzenie musi być wyposażone w licencję na obsługę 145 AP wraz ze wsparciem producenta na okres 24 miesięcy.

4. Urządzenie musi posiadać min. 4 interfejsy 2.5G/1G oraz 2 interfejsy 1/10G (SFP/SFP+)

5. Urządzenie musi obsługiwać łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu

6. Urządzenie musi zapewniać obsługę ruchu tunelowanego o przepustowości 5 Gbps

7. Urządzenie musi zapewnić obsługę 5000 klientów sieci bezprzewodowej

8. Urządzenie musi zapewnić zarządzanie pasmem radiowym punktów dostępowych poprzez:

8.1. automatyczną adaptacja do zmian w czasie rzeczywistym

8.2. optymalizację mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)

8.3. dynamiczne przydzielanie kanałów radiowych

8.4. wykrywanie, eliminacja i unikanie interferencji

8.5. równoważenie obciążenia punktów dostępowych

8.6. tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych

8.7. automatyczną dystrybucja klientów pomiędzy punkty dostępowe

8.8. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych

8.9. dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe

9. Urządzenie musi umożliwiać mapowanie SSID do segmentów VLAN w sieci przewodowej:

9.1. 1:1

9.2. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)

9.3. możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)

10. Wymagania w zakresie obsługi sieci kratowych. Urządzenie musi zapewniać:

10.1. komunikację między punktami dostępowymi bez medium kablowego

10.2. separację trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)

10.3. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)

10.4. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)

10.5. autoryzację punktów dostępowych w oparciu o certyfikaty, adresy MAC

11. Urządzenie musi zapewniać obsługę mechanizmów bezpieczeństwa:

11.1. 802.11i, WPA3, WPA2, WPA

11.2. 802.1x z EAP (min. PEAP, EAP-TLS, EAP-FAST)

11.3. obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników

11.4. kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID

11.5. obsługa profilowania użytkowników:

11.5.1.przydział sieci VLAN

11.5.2.przydział list kontroli dostępu (ACL)

11.6. uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w

11.7. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty

11.8. obsługa list kontroli dostępu (ACL)

11.9. obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X

11.10. wykrywanie i dezaktywacja obcych punktów dostępowych

11.11. ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników

11.12. DHCP proxy

11.13. zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową:

11.13.1. kryptograficzne podpisywanie obrazów oprogramowania

11.13.2. bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych

11.13.3. wbudowany moduł sprzętowy unikalnie identyfikujący urządzenie i jego pochodzenie

12. Obsługa ruchu unicast IPv4 i IPv6
13. Obsługa ruchu multicast IPv4 i IPv6
    13.1. IGMP / MLD snooping
    13.2. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)
    13.3. obsługa konwersji ruchu multicast do unicast
14. Obsługa mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami)
15. Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k
16. Wsparcie dla IEEE 802.11u
17. Obsługa mechanizmów QoS
    17.1. 802.1p
    17.2. WMM, TSpec, U-APSD
    17.3. ograniczanie pasma per użytkownik
    17.4. Call Admission Control, SIP CAC, Call Snooping
18. Obsługa sensorów symulujących pracę klientów bezprzewodowych, które pozwalają na badanie działania wybranych usług w sieci (DNS, DHCP, RADIUS, IMAP, Outlook Web Access, inne) i eksportują wyniki testów do dedykowanego zewnętrznego kolektora
19. Obsługa dostępu gościnnego (IPv4 i IPv6)
    19.1. przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony)
    19.2. przekierowanie użytkowników do strony logowania na zewnętrznym serwerze
20. Współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych
21. Obsługa NTP wersji 4 (IPv4 oraz IPv6)
22. Możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania
23. Obsługa Hotspot 2.0
24. Obsługa redundancji rozwiązania (N+1)
25. Obsługa redundancji 1:1 (active/standby) zapewniającej:
    25.1. utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera
    25.2. synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej
26. Dedykowany interfejs 1GE typu RJ45 służący do połączenia dwóch kontrolerów w redundantną parę 1:1
27. Analiza ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu; rozpoznawanie ponad 1000 aplikacji
28. Zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow
29. Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak: VLAN, polityka QoS, lista kontroli dostępu, czas trwania sesji
30. Obsługa protokołu Bonjour poprzez wbudowany mDNS Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów
    30.1. zarządzanie przez HTTPS, SNMP, SSH, NETCONF, port konsoli szeregowej

31. Wbudowana baza najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem

32. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

I. **Radiowy punkt dostępowy WiFi (AP) – 145 sztuk**

1. Urządzenie musi zapewniać obsługę standardów 802.11a/b/g/n/ac/ax
   - 1.1. obsługa OFDMA (uplink/downlink), TWT, BSS Coloring
   - 1.2. obsługa MU-MIMO (uplink/downlink) – min. 8x8:8
   - 1.3. obsługa kanałów 20, 40 MHz dla 802.11n
   - 1.4. obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax
   - 1.5. obsługa prędkości PHY do 3,47 Gbps (ac)
   - 1.6. obsługa prędkości PHY do 5,38 Gbps (ax)
   - 1.7. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
   - 1.8. obsługa beamforming dla klientów 802.11a/g/n/ac/ax
   - 1.9. obsługa MRC (Maximal Ratio Combining)
2. Urządzenie musi osiadać konfigurowalną moc nadajnika
   - 2.1. dla zakresu 2.4 GHz: do 100 mW
   - 2.2. dla zakresu 5GHz: do 400 mW
3. Urządzenie musi praca dwuzakresowo w pasmach: 2,4 GHz oraz 5 GHz
4. Urządzenie musi posiadać możliwość zmiany trybu pracy modułów radiowych (ustawienie konfiguracyjne):
   - 4.1. tryb dwóch modułów radiowych: jeden pracujący w paśmie 2,4GHz (4x4), drugi pracujący w paśmie 5GHz (4x4)
   - 4.2. tryb trzech modułów radiowych: jeden pracujący w paśmie 2,4GHz (4x4), drugi pracujący w paśmie 5GHz (4x4), trzeci pracujący w paśmie 5GHz (4x4) niezależnie od modułu drugiego na innym kanale w celu wytworzenia komórki mikro i makro
5. Urządzenie musi zapewniać zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
   - 5.1. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
   - 5.2. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
   - 5.3. obsługa min. 16 BSSID
   - 5.4. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
   - 5.5. uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w
   - 5.6. obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)
   - 5.7. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników
   - 5.8. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6
   - 5.9. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)
   - 5.10. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
   - 5.11. obsługa IPv6

5.12. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r

5.13. obsługa mechanizmów QoS:

5.13.1. ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik

5.13.2. obsługa WMM, TSPEC, U-APSD

5.14. wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM

5.15. obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting

5.16. wsparcie IEEE 802.11i, WPA3, WPA2, WPA

5.17. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)

5.18. obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS

5.19. obsługa blokowania ruchu Peer-to-Peer

5.20. obsługa polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) za pomocą mechanizmu out-of-band, który przekazuje za pośrednictwem kontrolera do AP mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa

5.21. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)

5.22. obsługa aWIPS (Adaptive Wireless Intrusion Prevention System) polegająca na wykryciu i remediacji zagrożenia. AP będący częścią systemu WIPS pozwala na określenie min. następujących informacji: sygnatura ataku, rodzaj wykrytej anomalii i jej opis, czas zdarzenia

5.22.1. wykrywanie sygnatur DoS: Auth/Deauth Flood, Assoc/Disassoc Flood, CTS/RTS Flood, Broadcast Deauth/Dissassoc Flood, Broadcast Probe Flood, EAPOL Logoff Flood

5.22.2. wykrywanie ataków: EAPOL-Logoff, RTS/CTS Virtual Carrier Sense

5.23. obsługa polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) umożliwiająca dynamiczne nadanie znacznika (w wyniku autoryzacji użytkownika/stacji) przez AP lub kontroler

5.24. uruchamianie aplikacji w kontenerach bezpośrednio na AP

5.25. obsługa VXLAN

6. Urządzenie musi posiadać możliwość pracy jako kontroler sieci bezprzewodowej o następujących funkcjonalnościach: (zmiana trybu pracy -przez wgranie oprogramowania) musi być bezkosztowa w okresie trwania kontraktu serwisowego):

6.1. obsługa do 100 punktów dostępowych

6.2. obsługa do 2000 klientów

6.3. możliwość konfiguracji do 16 sieci bezprzewodowych

6.4. centralna optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)

6.5. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r

6.6. obsługa mechanizmów wsparcia roamingu – IEEE 802.11k, IEEE 802.11v, OKC

6.7. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)

6.8. konfiguracja polityk bezpieczeństwa per SSID

6.9. obsługa WPA2 i WPA3 Personal oraz Enterprise

6.10. współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)

6.11. tworzenie list kontroli dostępu opartych o adresy IPv4 (IPv4 ACL) oraz o nazwy domenowe (DNS ACL)

6.12. obsługa URL Whitelist

6.13. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)

6.14. dwukierunkowe limitowanie transmisji (bidirectional rate-limiting ruchu) per klient, per WLAN

6.15. profilowanie (rozpoznawanie typów) urządzeń podłączających się do sieci bezprzewodowej

6.16. obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC)

6.17. obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym

6.18. obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta

6.19. obsługa protokołu Bonjour poprzez wbudowany mDNS (multicast DNS) Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów

6.20. zarządzanie przez HTTPS

6.21. wsparcie SSH, SNMP, NTP, SYSLOG

6.22. obsługa aktualizacji oprogramowania przez TFTP, SFTP

6.23. wbudowany serwer DHCP

6.24. wbudowany mechanizm redundancji automatycznie wybierający kontroler zapasowy wśród grupy obsługiwanych punktów dostępowych mogących pełnić funkcję kontrolera

7. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:

7.1. sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia

7.2. bezpieczna sekwencja uruchamiania

7.3. sprawdzenie autentyczności urządzenia

8. Interfejs MultiGigabit Ethernet (100/1000/2500/5000) zgodny z IEEE 802.3bz

9. Interfejs konsoli RJ45

10. Port USB 2.0

11. 2 GB RAM, 1 GB Flash

12. Urządzenie musi posiadać zróżnicowane możliwości zasilania:

12.1. pełna funkcjonalność AP przy zasilaniu przez 802.3bt, pobór mocy do 30,5W

12.2. pełna funkcjonalność AP, ale bez obsługi portu USB, przy zasilaniu przez 802.3at

12.3. możliwość uruchomienia AP z wykorzystaniem 802.3af z ograniczonymi funkcjami (min.: redukcja pracy układu radiowego)

13. Anteny zintegrowane o zysku min. 4 dBi dla pasma 2,4 GHz oraz min. 6 dBi dla pasma 5 GHz

14. Obudowa przystosowana do pracy w zakresie temperatur 0 – 50°C

15. Diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji

16. Certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi6, Wi-Fi Enhanced Open, WMM, WMM-PS

17. Wbudowane radio Bluetooth Low Energy (BLE) 5.0

18. IoT ready (Zigbee, Thread)

19. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

J. **W ramach zamówienia Sprzedawca dostarczy licencje do posiadanego i użytkowanego przez Zamawiającego systemu Cisco ISE w wersji 2.7.0.356 na okres 24 miesięcy umożliwiające zestawienie jednocześnie 2000 sesji. Dostarczone**

licencje muszą dawać możliwość wykorzystania wszystkich opisanych w dokumentach przedmiotowego zamówienia funkcjonalności w zakresie SDA.

K. **Świadczenie w okresie 24 miesięcy od dnia podpisania Protokołu odbioru Wdrożenia usług wsparcia w ramach puli godzin inżynierskich (konsultacji) w wymiarze maksymalnie 300 (trzysta) roboczogodzin, w ramach których Sprzedawca wykonywał będzie prace związane z konfiguracją wdrożonej sieci kampusowej oraz rozbudową i zmianami konfiguracyjnymi Oprogramowania zgodnie z oczekiwaniami Zamawiającego.**

L. **W przypadku zaproponowania rozwiązania opartego o producenta Cisco w ramach Umowy Sprzedawca przeprowadzi certyfikowane dwa pięciodniowe warsztaty dla administratorów (6 osób) ARiMR z zakresu:**

1) Cisco SD-Access Workshop v1.3 (CSDAWORK):

- Protokoły LISP oraz VXLAN
- Od data-plane learning do control-plane learning
  - Bezpieczeństwo oparte na grupach: Security Group Tag (SGT) i Group-Based Policy (GBP)
  - Elementy campus fabric
  - Protokół LISP jako control plane
  - Protokół VXLAN jako data plane
  - Integracja typu OTT (Over The Top)
  - Fabric-enabled WLAN
  - Konfiguracja sieci wirtualnych (VN)
  - Polityki bezpieczeństwa: Scalable Group
  - Integracja typu OTT (Over The Top)
  - Fabric-enabled WLAN
  - Konfigurcja węzłów brzegowych
  - Konfiguracja usług wspólnych
  - Cisco ISE jako centrum polityk bezpieczeństwa

1) Cisco Catalyst 9800-CL Wireless LAN Controller and WIFI6 Workshop (C9800WIFI6):

- Podstawowe funkcje i cechy kontrolera bezprzewodowego
- Konfiguracja początkowa WLC, uruchomienie i połączenie z radiowymi punktami dostępu
- Konfigurowanie zabezpieczenia dostępu klienta do sieci WLAN zgodnie ze standardem WPA3
- Podstawowa architektura WLAN
- Wdrożenie centralnej bezprzewodowej sieci LAN z kontrolerami
- Wdrażanie AP w trybie Local, Flexconnect
- Konfigurowanie autentykacji użytkowników (local/central/LWA/CWA) oraz przełączania ich ramek (local/central)
- Podstawowa konserwacja sieci WLAN i rozwiązywanie problemów
- Koncepcje tworzenia kopii zapasowych i odzyskiwania konfiguracji
- Aktualizacje oprogramowania
- Wrażanie nowego standardu WiFi 6 (802.11ax) oraz jego porównanie ze starszymi standardami (802.11abgn / ac)
- Funkcje i cechy WiFi 6 (OFDMA, MU-MIMO, TWT, 1024-QAM, IoT)

W przypadku zastosowania technologii innego producenta Sprzedawca przeprowadzi odpowiednie certyfikowane warsztaty właściwe dla danego producenta zgodne z zakresem przedstawionym powyżej.
Sprzedawca zapewni uczestnikom warsztatów certyfikaty/zaświadczenia potwierdzające uczestnictwo w warsztatach. Podczas warsztatów w każdym dniu warsztatów sporządzona zostanie lista obecności.

Dodatkowe cechy rozwiązania oceniane w ramach kryterium oceny ofert, o którym mowa w rozdz. XI pkt 1.3. SWZ.

Przełączniki szkieletowe i dostępowe:

I. Przełączniki szkieletowe i dostępowe:

Lp.	Część	Wymaganie
1	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C	Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
2	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C, Przełączniki szkieletowe Typ A i B	Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
3	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C	Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow). Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych
4	Przełącznik dostępowy typ A (z portami uplink), przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C, Przełączniki szkieletowe typ A i B	Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników: • Statycznie w oparciu o port do którego podłączona jest stacja, • Statycznie w oparciu o VLAN, w którym pracuje stacja, • Statycznie w oparciu o adres IP stacji, • Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X; Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu, Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa,
5	Przełączniki szkieletowe typ A i typ B	Obsługa standardu IEEE 802.1ae (MACSec) szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,
6	Przełącznik szkieletowy typ A	Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi 98 000. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible

		NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych.
7	Przełącznik szkieletowy typ B	Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi 98 000. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych.
8	Przełączniki szkieletowe typ A i typ B	Eksport dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)
9	Przełączniki szkieletowe typ A i typ B	Wbudowany analizator pakietów umożliwiamy zbieranie ruchu w czasie rzeczywistym, dekodowanie ruchu i zapisywanie ich w formie pliku .pcap lub do pamięci urządzenia (flash, zewnętrzne usb). Wynik dekodowania ruchu może zostać wyświetlony na konsoli urządzenia lub w zewnętrznym oprogramowaniu typu Wireshark.
10	Przełączniki szkieletowe typ A i typ B	Możliwość uruchamiania zdefiniowanych w Pythonie skryptów bezpośrednio na urządzeniu
11	Przełączniki szkieletowe typ A i typ B	Obsługa mechanizmów wysokiej dostępności, takich jak możliwość wgrania łatki oprogramowania bez restartu urządzenia (hot patching). W przypadku kontrolerów sieci bezprzewodowej WiFi obsługa aktualizacji oprogramowania w formie ISSU (in-Service Software upgrade) na parze kontrolerów
12	Przełączniki szkieletowe typ A i typ B	Urządzenie umożliwia uruchamianie dodatkowych aplikacji w kontenerach Docker
13	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C, Przełączniki szkieletowe Typ A i B	Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego
14	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C, Przełączniki szkieletowe Typ A i B	Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą

II. **<u>System zarządzania i monitorowania siecią:</u>**

1. Integracja systemu monitoringu z obecnie wykorzystywanym systemem kontroli Cisco ISE przy pomocy szyny wymiany danych PxGRID, wymiana informacji na temat uwierzytelnienia użytkowników podłączonych do sieci w lokalizacji Warszawa oraz pozostałych lokalizacjach gdzie wykorzystywane jest uwierzytelnianie.

2. Wyznaczenie na postawie analizy danych telemetrycznych dla każdego z urządzeń sieciowych, grupy użytkowników, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji indeksu liczbowego określającego jakość pracy danego monitorowanego obiektu wraz z wizualizacją na skali czasu zmiany wartości indeksów jakości pracy dla grup urządzeń sieciowych, grupy użytkowników przewodowych i bezprzewodowych, pojedynczego użytkownika oraz grupy

aplikacji lub pojedynczej aplikacji;

3. Dla danego problemu, podanie opisu problemu, dostarczenie informacji kontekstowej umożliwiającej identyfikację i rozwiązanie problemu, określenie lokalizacji, urządzeń oraz użytkowników dotkniętych problemem, propozycja sugerowanych działań umożliwiających rozwiązanie problemu wraz z możliwością dostępu do urządzeń sieciowych w celu natychmiastowego dostarczenia danych diagnostycznych;

4. Funkcjonalności monitorowania poprzez zaoferowany system zarządzania dodatkowych urządzeń posiadanych przez Kupującego (wymienionych poniżej):

- przełączników Cisco Catalyst 2960X – 1025 sztuk

- przełączników Cisco Catalyst 4500X – 32 sztuk

1. Monitoring dostępności urządzenia sieciowego
2. Wizualizacja urządzenia na mapie topologii sieci wraz połączeniami oraz wizualizacją stanu pracy urządzenia;
3. Zebranie i prezentacja następujących informacji o urządzeniu: model urządzenia, wersja systemu operacyjnego, adres IP, stan pracy, osiągalność, lokalizacja geograficzna, numer seryjny, czas pracy od ostatniego wyłączenia,
4. Odczyt konfiguracji urządzenia
5. Zarządzanie wersjami oprogramowania z możliwością wskazania wersji obowiązujących dla danego urządzenia
6. Możliwość bezpośredniego z poziomu konsoli graficznej systemu zarządzania i monitorowania dostępu do konsoli urządzenia lub narzędzia umożliwiającego zdalne wydawanie komend na urządzeniu;
7. Szczegółowe informacje o urządzeniu obejmujące:
a. Wykres czasowy utylizacji CPU;
b. Wykres czasowy utylizacji pamięci;
c. Wykres czasowy dostępności urządzenia;
d. Wykres czasowy temperatury urządzenia;
e. Informacje o poszczególnych interfejsach urządzeń w uwzględnieniem: stanu interfejsu, typu, prędkość linku, FDX/HDX;
8. Dla każdego z monitorowanych interfejsów informacje o:
a. Wykres czasowy dostępności interfejsu;
b. Wykres czasowy utylizacji interfejsu niezależnie w kierunku nadawczym i odbiorczym;
c. Wykres czasowy poziomu błędów niezależnie w kierunku nadawczym i odbiorczym;

III. **Kontroler WiFi:**

- możliwość eksportu dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)
- obsługa mechanizmów wysokiej dostępności, takich jak możliwość wgrania łatki oprogramowania bez restartu koncentratora (hot patching), restartu danego procesu, odseparowania systemów operacyjnych punktów dostępowych od systemu kontrolera, sekwencyjnego uaktualniania oprogramowania punktów dostępowych (rolling upgrades)
- zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow
- obsługa wbudowanego interpretera języka PYTHON
- obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020)

IV. **Radiowy punkt dostępowy:**

1. zintegrowany z radiowym punktem dostępowym:
2. moduł analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz):
   a) dokładność analizy (kwant próbkowania) max. 100 kHz
   b) obsługa kanału o szerokości 160MHz
   c) zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych
   d) automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.)
   e) współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego,
3. dedykowany moduł radiowy realizujący skanowanie pod kątem zagrożeń w sieci bezprzewodowej (wIPS) oraz w celach poprawy lokalizacji urządzeń bezprzewodowych pracujący off-channel w pasmach 2,4 oraz 5GHz.

I.3. Opis części zamówienia

1. Zamawiający nie dopuszcza składania przez Wykonawców ofert częściowych w rozumieniu art. 7 pkt 15) ustawy.
2. Wdrożenie przełączników sieciowych LAN oraz sieci WiFi stanowi jednorodną całość, tym samym podział zamówienia na części mógłby spowodować nadmierne trudności techniczne w trakcie realizacji umowy, w szczególności mógłby doprowadzić do rozmycia odpowiedzialności za prawidłowe współdziałanie switchy i sieci WiFi i w konsekwencji przenoszenie odpowiedzialności pomiędzy Wykonawcami poszczególnych części zamówienia. Dodatkowo koniecznym byłoby skoordynowanie działań różnych Wykonawców realizujących poszczególne części zamówienia a współpraca z różnymi Wykonawcami mogłaby zagrozić właściwemu jego wykonaniu i prowadzić do odmiennych i niekompatybilnych działań w okresie wdrożenia i w czasie świadczenia usług gwarancyjnych. Co istotne należy wskazać, że w przypadku podziału zamówienia na części, bez względu na przyjęte kryterium podziału powstaje realne ryzyko niezłożenia przez Wykonawców ofert na wszystkie części zamówienia. Sytuacja, w której jakaś część zamówienia mogłaby być nierozstrzygnięta jest nieakceptowalna z uwagi na konieczność zabezpieczenia realizacji bieżących potrzeb Zamawiającego.

I.4. Powierzenie Podwykonawcy wykonania części zamówienia

1. Zamawiający dopuszcza powierzenie Podwykonawcom wykonania części zamówienia.
2. Wykonawca zobowiązany jest do wskazania w ofercie części zamówienia, której wykonanie zamierza powierzyć Podwykonawcy oraz do podania firm Podwykonawców, jeżeli są już znani.

I.5. Pozostałe istotne elementy związane z zamówieniem

1. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 7 ustawy.
2. Zamawiający nie dopuszcza składania ofert wariantowych w rozumieniu ustawy.
3. Zamawiający nie przewiduje zawarcia umowy ramowej, jak również nie przewiduje przeprowadzenia aukcji elektronicznej.
4. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
5. Wszelkie rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. Zamawiający informuje, że środki finansowe przeznaczone na realizacje niniejszego zamówienia pochodzą z dotacji przyznanej Zamawiającemu, na podstawie Rozporządzenia Rady Ministrów z dnia 21 grudnia w sprawie wydatków budżetu państwa, które w roku 2021 nie wygasają z upływem roku budżetowego. Termin wydatkowania i rozliczenia środków przyznanych w ramach ww. dotacji przypada na dzień 30.11.2022 r. **W przypadku gdy czas trwania postępowania uniemożliwiał będzie zawarcie umowy w terminie umożliwiającym realizację i rozliczenie niniejszego zamówienia zgodnie z postanowieniami określonymi w dokumentach zamówienia do dnia 30.11.2022 r. Zamawiający zastrzega sobie możliwość unieważnienia przedmiotowego postępowania na podstawie art. 257 ustawy**.

Rozdział II. Termin wykonania zamówienia

1. Zamawiający wymaga realizacji zamówienia, tj. dostarczenia Sprzętu IT do wskazanych przez Zamawiającego Lokalizacji wraz z Oprogramowaniem, Dokumentami oraz Wdrożenia w Lokalizacjach nie później niż w terminie do 90 dni kalendarzowych od dnia zawarcia Umowy, jednak niepóźnej niż w terminie do dnia 14.11.2022 r.
2. Szczegółowe terminy realizacji zobowiązań umownych zostały określone przez Zamawiającego w projektowanych postanowieniach umownych stanowiących Załącznik nr 8 do SWZ.

Rozdział III. Podstawy wykluczenia oraz warunki udziału w postępowaniu, jednolity europejski dokument zamówienia

1. O zamówienie objęte niniejszym postępowaniem mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie przesłanek wskazanych w Rozdz. III.1. SWZ oraz spełniają warunki udziału w postępowaniu opisane w Rozdz. III.2. SWZ.
2. Wykonawca jest zobowiązany wykazać, że spełnia warunki udziału w postępowaniu i nie podlega wykluczeniu z postępowania. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia brak podstaw wykluczenia, o których mowa w Rozdz. III.1. SWZ musi wykazać każdy Wykonawca z osobna.
3. Zamawiający informuje, że zgodnie z procedurą wskazaną w art. 139 ust. 1 ustawy, najpierw dokona badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej Wykonawcy, którego oferta została najwyżej oceniona (na podstawie kryteriów oceny ofert określonych w SWZ) w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu.

III.1. Podstawy wykluczenia

1. Z postępowania, na podstawie art. 108 ust. 1 ustawy, Zamawiający wykluczy Wykonawcę:
   1.1. będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      1.1.1. udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      1.1.2. handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
      1.1.3. o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2021 r. poz. 523, 1292, 1559 i 2054),

1.1.4. finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,

1.1.5. o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,

1.1.6. powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej,

1.1.7. przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,

1.1.8. o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

– lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

1.2. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1.1.;

1.3. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

1.4. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

1.5. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

1.6. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z Wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

2. Z postępowania, na podstawie art. 109 ust. 1 ustawy, Zamawiający wykluczy Wykonawcę:

2.1. który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3 ustawy, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

2.2. który naruszył obowiązki w dziedzinie ochrony środowiska, prawa socjalnego lub prawa pracy:

2.2.1. będącego osobą fizyczną skazanego prawomocnie za przestępstwo przeciwko środowisku, o którym mowa w rozdziale XXII Kodeksu karnego lub za przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, o którym mowa w rozdziale XXVIII Kodeksu karnego, lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego,

2.2.2. będącego osobą fizyczną prawomocnie ukaranego za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny,

2.2.3. wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z prawa ochrony środowiska, prawa pracy lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną;

2.3. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo lub ukarano za wykroczenie, o którym mowa w pkt 2.2.1. lub 2.2.2.;

2.4. w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;

2.5. który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów;

2.6. jeżeli występuje konflikt interesów w rozumieniu art. 56 ust. 2 ustawy, którego nie można skutecznie wyeliminować w inny sposób niż przez wykluczenie Wykonawcy;

2.7. który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia

publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady;

2.8. który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;

2.9. który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;

2.10. który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia.

3. Z postępowania, na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 r. poz. 835; dalej *ustawa o szczególnych rozwiązaniach*) Zamawiający wykluczy:

3.1. Wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;

3.2. Wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;

3.3. Wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach.

III.2. Warunki udziału w postępowaniu

1. O niniejsze zamówienie mogą ubiegać się Wykonawcy spełniający warunki udziału w postępowaniu w zakresie:

1.1. **Zdolności technicznej lub zawodowej.** Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że:

1.1.1. wykonał w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, a w przypadku świadczeń powtarzających się lub ciągłych również realizuje: co najmniej:

1.1.1.1. 1 (jedną) dostawę, o wartości nie mniejszej niż 300.000,00 zł brutto (słownie: trzysta tysięcy złotych zero groszy), polegającą na dostawie i wdrożeniu sieci bezprzewodowych; oraz

1.1.1.2. 2 (dwie) dostawy o wartości nie mniejszej niż 700.000,00 zł brutto (słownie: siedemset tysięcy złotych zero groszy) każda, polegające na dostawie i wdrożeniu przełączników sieciowych w technologii Software Defined Networking.

UWAGA 1

Jeżeli wartość dostawy wskazanej w wykazie jest podana w walucie innej niż PLN, Wykonawca zobowiązany jest, na potrzeby niniejszego postępowania, dokonać przeliczenia jej wartości na PLN wg średniego kursu NBP (www.nbp.pl tabela A – tabela kursów średnich walut obcych) z dnia zakończenia dostawy o zakresie jak wyżej wraz z podaniem kursu oraz daty jego obowiązywania (zgodnie z tabelą A – tabela kursów średnich walut obcych) wg których dokonano przeliczenia; w przypadku dostaw nadal realizowanych - wg tabeli kursów średnich walut obcych z dnia rozpoczęcia realizacji danej dostawy.

UWAGA 2

W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają dostawy, do realizacji których te zdolności są wymagane. W takiej sytuacji Wykonawca składa wraz z ofertą oświadczenie w zakresie wskazania, które dostawy wykonają poszczególni Wykonawcy (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 3 do SWZ.

1.1.2. dysponuje następującymi osobami, które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi, wykształceniem i doświadczeniem umożliwiającymi realizację zamówienia na odpowiednim poziomie jakości, tj.: dysponuje co najmniej 1 (jedną) osobą, która posiada łącznie:

1.1.2.1. co najmniej 12 miesięczne doświadczenie przy realizacji zamówień o zakresie jak w pkt 1.1.1. z wyłączeniem wartości zamówień,

1.1.2.2. certyfikat wystawiony przez producenta Sprzętu IT oferowanego w postępowaniu, np. CCIE Enterprise Infrastructure (350-401 ENCOR) (1 osoba) lub równoważny.

UWAGA 3:

Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:

1. *jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:*
   a. *analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,*
   b. *analogiczny stopień poziomu kompetencji,*
   c. *analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,*

2. *potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowe certyfikaty muszą być potwierdzone egzaminem).*
3. *Zamawiający uzna za certyfikaty równoważne do certyfikatów wymienionych powyżej z nazwy m.in. następujące certyfikaty: Juniper Networks Certified Internet Expert (JNCIE-ENT) lub* HP *Master Accredited Systems Engineer (*MASE*) – Network Infrastructure.*

Uwaga 4:

Na mocy art. 5k rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), ***od 9 kwietnia 2022 r. obowiązuje zakaz udzielania*** *lub dalszego wykonywania wszelkich zamówień publicznych lub koncesji objętych zakresem dyrektyw w sprawie zamówień publicznych, a także zakresem art. 10 ust. 1, 3, ust. 6 lit. a)–e), ust. 8, 9 i 10, art. 11, 12, 13 i 14 dyrektywy 2014/23/UE, art. 7 i 8, art. 10 lit. b)–f) i lit. h)–j) dyrektywy 2014/24/UE, art. 18, art. 21 lit. b)–e) i lit. g)–i), art. 29 i 30 dyrektywy 2014/25/UE oraz art. 13 lit. a)–d), lit. f)–h) i lit. j) dyrektywy 2009/81/WE na rzecz lub z udziałem:*

a) obywateli rosyjskich lub osób fizycznych lub prawnych, podmiotów lub organów z siedzibą w Rosji;

b) osób prawnych, podmiotów lub organów, do których prawa własności bezpośrednio lub pośrednio w ponad 50 % należą do podmiotu, o którym mowa w lit. a) (powyżej); lub

c) osób fizycznych lub prawnych, podmiotów lub organów działających w imieniu lub pod kierunkiem podmiotu, o którym mowa w lit. a) lub b) (powyżej),

w tym podwykonawców, dostawców lub podmiotów, na których zdolności polega się w rozumieniu dyrektyw w sprawie zamówień publicznych, w przypadku gdy przypada na nich ponad 10 % wartości zamówienia.

Wykonawcy, których dotyczą wskazane wyżej zakazy, nie mogą ubiegać się o udzielenie przedmiotowego zamówienia publicznego, zaś złożona przez nich oferta będzie podlegać odrzuceniu.

2. Ocena spełniania ww. warunków dokonana zostanie w oparciu o informacje zawarte we właściwych dokumentach wyszczególnionych w Rozdz. IV niniejszej SWZ. Z treści złożonych dokumentów musi wynikać jednoznacznie, iż ww. warunki Wykonawca spełnił.

Rozdział IV. Zawartość ofert, wykaz podmiotowych środków dowodowych

1. W zakresie nieuregulowanym postanowieniami SWZ zastosowanie mają przepisy rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie rodzajów podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od Wykonawcy (Dz. U. z 2020 r. poz. 2415; dalej: *„Rozporządzenie w sprawie rodzajów podmiotowych środków dowodowych"*).
2. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 ustawy, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w terminie przez siebie wskazanym, chyba że:
   2.1. oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub
   2.2. zachodzą przesłanki unieważnienia postępowania.

IV.1. Zawartość ofert

1. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym wg Załącznika nr 1 do SWZ **za pośrednictwem Platformy Zakupowej**.
2. Wykonawca obowiązany jest złożyć wraz z ofertą następujące dokumenty:
   2.1. Odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, w celu potwierdzenia, że osoba działająca w imieniu Wykonawcy jest umocowana do jego reprezentowania.
   2.2. Pełnomocnictwo lub inny dokument potwierdzający umocowanie osoby działającej w imieniu Wykonawcy do jego reprezentowania, jeżeli oferta nie została podpisana przez osoby upoważnione do tych czynności dokumentem rejestracyjnym.
   2.3. Dowód wniesienia wadium. Jeżeli Wykonawca wnosi wadium w formie gwarancji lub poręczenia Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej. W przypadku wniesienia wadium w innej formie niż pieniądz, powinno ono obowiązywać przez cały okres związania ofertą.
   2.4. Zobowiązanie podmiotów udostępniających zasoby do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie będzie dysponował niezbędnymi zasobami, jeżeli Wykonawca powołuje się na zasoby innych podmiotów. Zobowiązanie winno być podpisane przez osobę upoważnioną do reprezentacji podmiotu udostępniającego zasoby. Zapisy pkt 2.1. i 2.2. oraz Rozdz. IV.5 SWZ stosuje się odpowiednio.
   2.5. Aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia (dalej: *„JEDZ"*) sporządzone zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji (UE) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającym standardowy formularz jednolitego europejskiego dokumentu zamówienia (Dz. Urz. UE L 3 z 06.01.2016, str. 16). Dokument JEDZ należy złożyć pod rygorem nieważności w formie elektronicznej. Dokument JEDZ musi być opatrzony kwalifikowanym podpisem elektronicznym.
   2.6. Oświadczenie Wykonawcy, w zakresie braku podstaw wykluczenia na podstawie art. 5k rozporządzenia Rady (UE) nr 833/2014 oraz art. 7 ustawy o szczególnych rozwiązaniach. Wzór oświadczenia stanowi Załącznik nr 2 do SWZ.
   2.7. Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia w zakresie wskazania, które dostawy wykonają poszczególni Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 3 do SWZ.

2.8. Certyfikat w zakresie zarządzania bezpieczeństwem informacji ISO/IEC 27001 lub równoważnego dokumentu wystawianego przez niezależny akredytowany podmiot (jednostka akredytowana) zajmujący się poświadczaniem zgodności ze standardem dotyczącym zarządzania bezpieczeństwem informacji i opatrzony znakiem akredytacji.

2.9. Przedmiotowe środki dowodowe, na potwierdzenie spełniania przez oferowane dostawy określonych przez Zamawiającego cech i wymagań ocenianych w ramach kryterium oceny ofert *dodatkowe parametry techniczne*, tj. dokumentacja techniczna pochodząca od producenta (wraz z tłumaczeniem na język polski, jeśli dokumentacja jest sporządzona w języku obcym), dostępna na stronach internetowych producenta, potwierdzająca spełnienie poszczególnych wymagań. Wymagane jest wskazanie w dokumentacji miejsc określających spełnienie poszczególnych, oferowanych wymagań. (*Zapis ma zastosowanie, jeśli Wykonawca oferuje dostawy spełniające wymagania określone przez Zamawiającego w Załączniku 1B do projektowanych postanowień umowy. Do dokumentacji technicznej stosuje się postanowienia Rozdz. VIII.2 pkt 2 SWZ*).

IV.2 Oświadczenie w formie Jednolitego Europejskiego Dokumentu Zamówienia

1. Wykonawca wypełnia JEDZ, tworząc dokument w postaci elektronicznej. Wykonawca może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu w postaci elektronicznej.
   1.1. Zamawiający udostępnia Wykonawcom plik, w formacie XML, wygenerowany z narzędzia ESPD, który stanowi Załącznik nr 9 do SWZ.
   1.2. Zamawiający informuje, że pod adresem: https://espd.uzp.gov.pl Urząd Zamówień Publicznych udostępnił nieodpłatne narzędzie umożliwiające zamawiającym i wykonawcom utworzenie, wypełnienie i ponowne wykorzystanie standardowego formularza JEDZ (JEDZ/ESPD) w wersji elektronicznej (eESPD).
2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie JEDZ, o którym mowa w Rozdz. IV.1. pkt 2.5. SWZ, składa każdy z Wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
3. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia także oświadczenie JEDZ, o którym mowa w Rozdz. IV.1. pkt 2.5. SWZ podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.
4. Środkiem komunikacji elektronicznej, służącym złożeniu JEDZ przez Wykonawcę, jest Platforma Zakupowa.
5. Dokument elektroniczny JEDZ należy złożyć w formacie PDF.
6. Obowiązek złożenia JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym w sposób określony powyżej dotyczy również JEDZ składanego na wezwanie w trybie art. 128 ust. 1 ustawy.

IV.3. Wykaz podmiotowych środków dowodowych

Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia za pośrednictwem Platformy Zakupowej, w wyznaczonym terminie, nie krótszym niż 10 dni od dnia wezwania, aktualnych na dzień złożenia podmiotowych środków dowodowych, w formie elektronicznej podpisanych kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności, w poniższym zakresie:

1. braku podstaw wykluczenia Wykonawcy z postępowania o udzielenie zamówienia:
   1.1. informacji z Krajowego Rejestru Karnego w zakresie:
      1.1.1. art. 108 ust. 1 pkt 1 i 2 ustawy,
      1.1.2. art. 108 ust. 1 pkt 4 ustawy, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego,
      1.1.3. art. 109 ust. 1 pkt 2 lit. a ustawy,
      1.1.4. art. 109 ust. 1 pkt 2 lit. b ustawy, dotyczącej ukarania za wykroczenie, za które wymierzono karę aresztu,
      1.1.5. art. 109 ust. 1 pkt 3 ustawy, dotyczącej skazania za przestępstwo lub ukarania za wykroczenie, za które wymierzono karę aresztu
      - sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem;
   1.2. zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków i opłat, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem podatków lub opłat wraz z zaświadczeniem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert Wykonawca dokonał płatności należnych podatków lub opłat wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
   1.3. zaświadczenia albo innego dokumentu właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub właściwego oddziału regionalnego lub właściwej placówki terenowej Kasy Rolniczego Ubezpieczenia Społecznego potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne i zdrowotne, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne wraz z zaświadczeniem albo innym dokumentem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert Wykonawca dokonał płatności należnych składek na ubezpieczenia społeczne lub zdrowotne wraz odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;

1.4. odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;

1.5. oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:

1.5.1. art. 108 ust. 1 pkt 3 ustawy,

1.5.2. art. 108 ust. 1 pkt 4 ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,

1.5.3. art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi Wykonawcami porozumienia mającego na celu zakłócenie konkurencji,

1.5.4. art. 108 ust. 1 pkt 6 ustawy,

1.5.5. art. 109 ust. 1 pkt 1 ustawy, odnośnie do naruszenia obowiązków dotyczących płatności podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2019 r. poz. 1170 z późn. zm.),

1.5.6. art. 109 ust. 1 pkt 2 lit. b ustawy, dotyczących ukarania za wykroczenie, za które wymierzono karę ograniczenia wolności lub karę grzywny,

1.5.7. art. 109 ust. 1 pkt 2 lit. c ustawy,

1.5.8. art. 109 ust. 1 pkt 3 ustawy, dotyczących ukarania za wykroczenie, za które wymierzono karę ograniczenia wolności lub karę grzywny,

1.5.9. art. 109 ust. 1 pkt 5-10 ustawy

- sporządzone według wzoru, który stanowi Załącznik nr 4 do SWZ.

1.6. oświadczenia Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej. Wzór oświadczenia stanowi Załącznik nr 5 do SWZ.

2. potwierdzenia spełniania warunków udziału w postępowaniu dotyczących zdolności zawodowej:

2.1. wykazu dostaw wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie Wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy. Wzór oświadczenia stanowi Załącznik nr 6 do SWZ.

2.2. wykazu osób, skierowanych przez wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. Wzór oświadczenia stanowi Załącznik nr 7 do SWZ.

IV.4. Podmiotowe środki dowodowe składane przez Wykonawców mających siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej

1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast:

1.1. informacji z Krajowego Rejestru Karnego, o której mowa w Rozdz. IV.3 pkt 1.1. SWZ – składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, w zakresie, o którym mowa w Rozdz. IV.3 pkt 1.1. SWZ;

1.2. zaświadczenia, o którym mowa w Rozdz. IV.3 pkt 1.2. SWZ, zaświadczenia albo innego dokumentu potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, o których mowa w Rozdz. IV.3 pkt 1.3 SWZ, lub odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa IV.3 pkt 1.4. SWZ – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:

1.2.1. nie naruszył obowiązków dotyczących płatności podatków, opłat, lub składek na ubezpieczenie społeczne lub zdrowotne,

1.2.2. nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.

2. Dokument, o którym mowa w pkt 1.1., powinien być wystawiony nie wcześniej niż 6 miesięcy przed jego złożeniem. Dokumenty, o którym mowa w pkt 1.2., powinny być wystawione nie wcześniej niż 3 miesiące przed ich złożeniem.

3. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt. 1, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4, art.

109 ust. 1 pkt 1, 2 lit. a i b oraz pkt 3 ustawy, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy. Postanowienie pkt. 2 stosuje się.

IV.5. Zasady i warunki korzystania przez Wykonawcę ze zdolności lub sytuacji innych podmiotów

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
2. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających **zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby** do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
3. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w pkt 2, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   1.1. zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
   1.2. sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia.
4. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 118 ustawy, przedstawienia w odniesieniu do tych podmiotów podmiotowych środków dowodowych wymienionych w Rozdz. IV.1 pkt 2.6. oraz Rozdz. IV.3 pkt 1.1. – 1.5. SWZ. Postanowienia Rozdz. IV.3. SWZ stosuje się odpowiednio.

IV.6. Klauzule informacyjne w zakresie danych osobowych

W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2. oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO" Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w toku postępowania jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazanych w pkt 1.
3. Pani/Pana dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   4.1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 2 ustawy,
   4.2. organy kontrolne,
   4.3. osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r. poz. 2176),
   4.4. podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa.
5. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do przeprowadzenia niniejszego postępowania. Ponadto, zgodnie z art. 78 ust. 1 ustawy przechowywane będą przez okres 4 lat od dnia zakończenia niniejszego postępowania. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, a konsekwencje niepodania określonych danych wynikają z ustawy.

Rozdział V. Informacje o sposobie porozumiewania się zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do komunikowania się z Wykonawcami

1. Komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują wyłącznie za pośrednictwem Platformy Zakupowej, z zachowaniem formy albo postaci

elektronicznej, w zależności od rodzaju przekazywanego dokumentu – stosownie do obowiązujących w tym zakresie przepisów prawa. Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się ich datę wczytania do Platformy Zakupowej.

2. Postępowanie prowadzone jest pod numerem referencyjnym sprawy: **DPiZP.2610.17.2021**, Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wskazany numer referencyjny.
3. Wykonawcy powinni kierować do Zamawiającego wszelką korespondencję z zachowaniem zasad opisanych w pkt 1, za pośrednictwem Platformy Zakupowej.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SWZ. Wniosek należy przesłać za pośrednictwem Platformy Zakupowej.
5. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 14 dni przed upływem terminu składania ofert. Treść pytań (bez ujawnienia źródła zapytania) wraz z wyjaśnieniami bądź informacje o dokonaniu zmiany treści SWZ, Zamawiający przekaże (opublikuje) Wykonawcom za pośrednictwem Platformy Zakupowej.
6. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego po upływie terminu, o którym mowa w pkt 5 Zamawiający nie ma obowiązku udzielania wyjaśnień treści SWZ.
7. W uzasadnionym przypadku Zamawiający może przed terminem składania ofert zmienić treść dokumentów składających się na niniejszą SWZ.
8. Zamawiający nie zamierza zwoływać zebrania Wykonawców.
9. Osobami uprawnionymi ze strony Zamawiającego do kontaktów z Wykonawcami są:
   9.1. Pan Zbigniew Antonik, tel.: +48225950062 w godz. 9.00 – 15.00.
   9.2. Pani Kinga Henzel, tel.: +4822259590066 w godz. 9.00 – 15.00.

Rozdział VI. Wymagania dotyczące wadium

1. Wykonawca zobowiązany jest wnieść wadium w wysokości 100.000,00 zł (słownie: sto tysięcy złotych zero groszy).
2. Wadium może być wniesione w:
   2.1. pieniądzu;
   2.2. gwarancjach bankowych;
   2.3. gwarancjach ubezpieczeniowych;
   2.4. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2020 r. poz. 299).
3. Wadium w formie pieniądza należy wnieść przelewem na rachunek bankowy Zamawiającego prowadzony w Banku Gospodarstwa Krajowego III Oddział w Warszawie numer rachunku – 45 1130 1062 8000 0000 0002 8175, z dopiskiem na przelewie: „wadium w postępowaniu na *Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, wdrożeniem i konsultacjami*".
4. W przypadku wnoszenia wadium w formie gwarancji lub poręczenia, o których mowa w pkt. 2.2.-2.4., Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej poprzez wczytanie na Platformie Zakupowej. Wadium powinno być oznaczone w następujący sposób: WADIUM – numer referencyjny sprawy, nazwa postępowania lub w inny sposób umożliwiający identyfikację postępowania, którego dotyczy.
5. Dokument wadialny (gwarancja lub poręczenie) musi wyraźnie wskazywać na wszystkie okoliczności jego utraty określone w art. 98 ust. 6 ustawy.
6. Z treści gwarancji/poręczenia powinno wynikać bezwarunkowe, na każde pisemne żądanie zgłoszone przez Zamawiającego, zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 98 ust. 6 ustawy.
7. Oferta Wykonawcy, który nie wniósł wadium lub wniósł w sposób nieprawidłowy lub nie utrzymywał wadium nieprzerwanie do upływu terminu związania ofertą lub złożył wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 ustawy zostanie odrzucona.
8. W przypadku wniesienia wadium i niezłożenia oferty, Wykonawca jest zobowiązany złożyć do Zamawiającego wniosek o zwrot wadium.

Rozdział VII. Termin związania ofertą

Wykonawcy pozostają związani złożoną ofertą do dnia **07.09.2022 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Rozdział VIII Opis sposobu przygotowywania ofert

VIII.1. Przygotowanie ofert

1. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej. Ofertę należy podpisać kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SWZ).
2. Treść złożonej oferty musi być zgodna z warunkami zamówienia. Wykonawca ma prawo złożyć tylko jedną ofertę. Oferta powinna być sporządzona w języku polskim, w formie elektronicznej pod rygorem nieważności. Ofertę należy podpisać kwalifikowanym podpisem elektronicznym. Ofertę należy złożyć wyłącznie za pośrednictwem Platformy Zakupowej.

3. Oferta powinna zawierać jedną, jednoznacznie opisaną propozycję.
4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Zamawiający informuje, iż zgodnie z art. 74 ust. 1 i 2 ustawy oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu niezwłocznie po otwarciu ofert, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca nie później niż w terminie składania ofert zastrzegł, że nie mogą one być udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji określonych w art. 222 ust. 5 ustawy, tj. nazw albo imion i nazwisk oraz siedzib lub miejsc prowadzonej działalności gospodarczej albo miejsc zamieszkania Wykonawców, których oferty zostały otwarte, cen lub kosztów zawartych w ofertach.

   Uwaga:

   Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), które Wykonawca zamierza zastrzec jako tajemnicę przedsiębiorstwa, muszą zostać odpowiednio oznaczone a następnie załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla Informacji stanowiących tajemnicę przedsiębiorstwa.
6. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia, w takim przypadku:
   6.1. oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie,
   6.2. każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi udokumentować, że nie podlega wykluczeniu z postępowania na podstawie przesłanek określonych w Rozdz. III.1. SWZ,
   6.3. zgodnie z art. 58 ust. 2 ustawy muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego,
   6.4. wszelka korespondencja oraz rozliczenia dokonywane będą wyłącznie z pełnomocnikiem,
   6.5. przed podpisaniem umowy przedłożą pełnomocnictwo do zawarcia umowy w sprawie zamówienia publicznego, jeżeli pełnomocnictwo takie nie zostało dołączone do oferty,
   6.6. w odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają dostawy, do realizacji których te zdolności są wymagane.

VIII.2. Forma dokumentów składanych w postępowaniu

1. Wszystkie dokumenty wchodzące w skład oferty oraz składane w trakcie postępowania należy złożyć na Platformie Zakupowej w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne – podpis elektroniczny spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. – o usługach zaufania oraz identyfikacji elektronicznej (tj. Dz. U. z 2020 r. poz. 1173 z późn. zm.).
2. Dokumenty i oświadczenia wchodzące w skład oferty oraz składane w trakcie postępowania, sporządzone w językach obcych muszą być złożone wraz z tłumaczeniami na język polski.
3. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio Wykonawcy, Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej *„dokumentami potwierdzającymi umocowanie do reprezentowania"*, zostały wystawione przez upoważnione podmioty inne niż Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej *„upoważnionymi podmiotami"*, jako dokument elektroniczny, przekazuje się ten dokument.
4. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
5. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 4, dokonuje w przypadku:
   5.1. podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
   5.2. przedmiotowych środków dowodowych – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
   5.3. innych dokumentów, w tym dokumentów, o których mowa w art. 94 ust. 2 ustawy – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.
6. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.

7. W przypadku gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
8. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 7, dokonuje w przypadku:
   8.1. podmiotowych środków dowodowych – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;
   8.2. przedmiotowego środka dowodowego, dokumentu, o którym mowa w art. 94 ust. 2 ustawy, oświadczenia, o którym mowa w art. 117 ust. 4 ustawy, lub zobowiązania podmiotu udostępniającego zasoby – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
   8.3. pełnomocnictwa – mocodawca.
9. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 4 i 7, może dokonać również notariusz.
10. Przez cyfrowe odwzorowanie, o którym mowa w pkt. 2, 5 oraz pkt. 7-9, należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.
11. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku kwalifikowanym podpisem elektronicznym.

Rozdział IX. Sposób oraz termin składania i otwarcia ofert, warunki zmiany albo wycofania oferty

IX.1. Sposób oraz termin składania ofert i otwarcia ofert

1. Ofertę pod rygorem nieważności należy złożyć w formie elektronicznej. Ofertę musi zostać podpisana kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Ofertę należy złożyć na Platformie Zakupowej udostępnionej przez Zamawiającego na stronie internetowej: https://platformazakupowa.pl/pn/arimr.
2. Termin składania ofert upływa w dniu **10.06.2022 r. o godzinie 10:00.**
3. Otwarcie ofert odbędzie się w dniu **10.06.2022 r. o godzinie 12:00.**
4. Zamawiający nie bierze odpowiedzialności za nieprawidłowe złożenie oferty wynikające z niezastosowania się przez Wykonawcę do wymagań niniejszej SWZ.

IX.2. Warunki zmiany i wycofania złożonej oferty

1. Wykonawca posiadający konto na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić lub wycofać ofertę.
2. Wykonawca nieposiadający konta na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić ofertę. Wykonawca niezalogowany nie może samodzielnie wycofać oferty. W celu wycofania oferty należy skontaktować się z Centrum Wsparcia Klienta uruchomione przez Operatora Platformy Zakupowej, które służy pomocą techniczną od 7:00 do 17:00 od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mail: cwk@platformazakupowa.pl.
3. Na Platformie Zakupowej w zakładce „Instrukcje dla Wykonawców" opisana jest szczegółowa procedura zmiany i wycofania oferty.
4. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty (załączników).

Rozdział X. Opis sposobu obliczenia ceny

1. Wykonawca zobowiązany jest do wyliczenia i podania cen jednostkowych netto, ceny ofertowej netto, należnego podatku od towarów i usług VAT oraz ceny ofertowej brutto, w sposób określony w Formularzu Ofertowym stanowiącym Załącznik nr 1 do SWZ.
2. Ceny określone w Formularzu Ofertowym powinny zawierać wszystkie koszty związane z wykonaniem przedmiotu zamówienia. Podane ceny nie podlegają zmianom przez okres obowiązywania umowy, z zastrzeżeniem postanowień Rozdz. XIV pkt 4 niniejszej SWZ.
3. Ceny określone w formularzu ofertowym muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (wg zasady zaokrąglenia: poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
4. Wszystkie ceny podane w Formularzu Ofertowym powinny być wyrażone w złotych polskich.
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający dla celów zastosowania kryterium ceny lub kosztu doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. Wykonawca, składając ofertę, obowiązany jest do poinformowania Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego

powstania, oraz wskazując ich wartość bez kwoty podatku, wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

Rozdział XI. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze oferty najkorzystniejszej Zamawiający będzie się kierował poniższymi kryteriami:
   1.1. kryterium ***cena*** **(P_C) – waga 73% (73,00 pkt)**, wg poniższego wzoru:

   $$P_C = \frac{C_{min.}}{C_b} \text{ x } 73{,}00 \text{ pkt},$$

   gdzie:
   P_C – liczba punktów oferty badanej w kryterium *cena*
   $C_{min.}$ – cena najniższa spośród ważnych ofert
   C_b – cena oferty badanej

   1.2. kryterium ***dodatkowe parametry techniczne*** **(P_D) – waga 27% (27,00 pkt)**
   Jeżeli Wykonawca zaoferuje spełnienie wszystkich wymagań określonych przez Zamawiającego w Załączniku 1B do projektowanych postanowień umowy, stanowiących Załącznik nr 8 do SWZ, oferta takiego Wykonawcy otrzyma 27 pkt w kryterium dodatkowe parametry techniczne P_D.
   Jeżeli Wykonawca nie zaoferuje spełnienie wszystkich wymagań określonych przez Zamawiającego w Załączniku 1B do projektowanych postanowień umowy, stanowiących Załącznik nr 8 do SWZ, oferta takiego Wykonawcy otrzyma 0 pkt w kryterium dodatkowe parametry techniczne P_D.

2. Za najkorzystniejszą zostanie uznana oferta, która uzyska największą całkowitą liczbę punktów obliczoną z dokładnością do dwóch miejsc po przecinku zgodnie ze wzorem:

   $$P = P_c + P_D$$

   gdzie:
   P – liczba punktów oferty w łącznym kryterium oceny ofert,
   P_c – liczba punktów oferty badanej w kryterium *cena,*
   P_D - liczba punktów oferty badanej w kryterium *dodatkowe parametry techniczne*.

Rozdział XII. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający powiadomi wybranego Wykonawcę o miejscu i terminie podpisania umowy.
2. Wykonawca będzie zobowiązany do niezwłocznego podania Zamawiającemu danych niezbędnych do sporządzenia umowy lub przekazania dokumentów, które okażą się konieczne do zawarcia umowy.

Rozdział XIII. Wymagania dotyczące zabezpieczenia należytego wykonania umowy

1. Zamawiający żąda od Wykonawcy, z którym zostanie podpisana umowa wniesienia zabezpieczenia należytego wykonania umowy w wysokości **2%** ceny całkowitej podanej w ofercie.
2. Zabezpieczenie należytego wykonania umowy może być wniesione w następujących formach:
   2.1. pieniądzu,
   2.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym,
   2.3. gwarancjach bankowych,
   2.4. gwarancjach ubezpieczeniowych,
   2.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
3. W przypadku wniesienia zabezpieczenia w formie pieniężnej Zamawiający przechowuje je na oprocentowanym rachunku bankowym.
4. Zabezpieczenie wnoszone w formie gwarancji bankowej, ubezpieczeniowej, poręczenia bankowego lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej, poręczenia udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, ma być wystawione przez bank, ubezpieczyciela lub poręczyciela. Bank, ubezpieczyciel, poręczyciel zapłaci, na rzecz Zamawiającego w terminie 30 dni od pisemnego żądania kwotę zabezpieczenia, na pierwsze wezwanie Zamawiającego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie Zamawiającego jest uzasadnione czy nie.
5. W przypadku, gdy zabezpieczenie, o którym mowa w niniejszym Rozdz. SWZ będzie wnoszone w formie innej niż pieniądz, Zamawiający zastrzega sobie prawo do akceptacji projektu ww. dokumentów.
6. Zabezpieczenia w innej formie niż pieniądz, Wykonawca złoży u Zamawiającego w Kancelarii Głównej, mieszczącej się w Warszawie przy ul. Poleczki 33, z adnotacją „dla Departamentu Informatyki" a przypadku zabezpieczenia wnoszonego w postaci elektronicznej należy przekazać na adres e-mail uzyskany od Zamawiającego przed podpisaniem umowy.
7. Zabezpieczenie należytego wykonania umowy służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.

8. Zabezpieczenie należytego wykonania Umowy zostanie zwrócone w terminach i na zasadach określonych w projektowanych postanowieniach umowy.

Rozdział XIV. Informacje dotyczące umowy w sprawie zamówienia publicznego

1. Zawarcie umowy nastąpi wg treści projektowanych postanowień umowy w sprawie zamówienia publicznego, stanowiących Załącznik nr 8 do niniejszej SWZ.
2. Postanowienia ustalone w projektowanych postanowieniach umowy nie podlegają negocjacjom.
3. Przyjęcie niniejszych projektowanych postanowień umowy stanowi jeden z istotnych warunków przyjęcia oferty.
4. Zamawiający dopuszcza zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy. Warunki zmian zostały opisane przez Zamawiającego w projektowanych postanowieniach umowy wraz z załącznikami, stanowiących Załącznik nr 8 do SWZ.
5. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza zobowiązany będzie do udzielenia Zamawiającemu wszelkich informacji oraz złożenia oświadczeń i dokumentów niezbędnych do ustalenia czy:
   5.1. udzielenie zamówienia temu Wykonawcy nie będzie stanowić złamania zakazu udzielania lub dalszego wykonywania wszelkich zamówień publicznych na podstawie art. 5k rozporządzenia 2022/576 w sprawie zmiany rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1),
   5.2. aktualne pozostaje niepodleganie wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 7 ustawy o szczególnych rozwiązaniach.

Rozdział XV. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia publicznego

1. Wykonawcom, którzy mają lub mieli interes w uzyskaniu danego zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy przysługują środki ochrony prawnej określone w dziale IX ustawy.
2. Odwołanie przysługuje na:
   2.1. niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   2.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy.
3. Odwołanie winno zawierać informacje określone w art. 516 ust. 1 ustawy, w szczególności wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Pisma w postępowaniu odwoławczym wnosi się w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej, z tym że odwołanie i przystąpienie do postępowania odwoławczego, wniesione w postaci elektronicznej, wymagają opatrzenia podpisem zaufanym.
5. Odwołujący przekazuje Zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Odwołanie wnosi się w terminie:
   6.1 10 (dziesięciu) dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane przy użyciu środków komunikacji elektronicznej;
   6.2 15 (piętnastu) dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przekazana w inny sposób niż określony w pkt. 6.1.;
7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie lub wobec treści dokumentów zamówienia wnosi się w terminie:
   7.1. 10 (dziesięciu) dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej.
8. Odwołanie w przypadkach innych niż określone w pkt. 6 i 7 wnosi się w terminie:
   8.1. 10 (dziesięciu) dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

Załączniki do SWZ:

1. Załącznik nr 1 – Wzór Formularza Ofertowego
2. Załącznik nr 2 – Wzór Oświadczenia o potwierdzeniu braku podstaw wykluczenia – art. 5k rozporządzenia Rady (UE) nr 833/2014 oraz art. 7 ustawy o szczególnych rozwiązaniach
3. Załącznik nr 3 – Wzór Oświadczenia o podziale obowiązków w trakcie realizacji zamówienia
4. Załącznik nr 4 - Wzór Oświadczenia o braku podstaw wykluczenia
5. Załącznik nr 5 - Wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej
6. Załącznik nr 6 - Wzór Oświadczenia – Wykaz dostaw
7. Załącznik nr 7 - Wzór Oświadczenia – Wykaz osób

8. Załącznik nr 8 - projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do umowy w sprawie zamówienia publicznego
9. Załącznik nr 9 - ESPD – plik, w formacie XML, wygenerowany z narzędzia ESPD – do przygotowania formularza jednolitego europejskiego dokumentu zamówienia (JEDZ)

ZASTĘPCA PREZESA

Jacek Paziewski

Zatwierdzam SWZ wraz z Załącznikami: .....

Jacek Paziewski

Zastępca Prezesa ARiMR

Załącznik nr 1 do SWZ – wzór Formularza Ofertowego

Formularz Ofertowy
DPiZP.2610.17.2021

Ja(my) niżej podpisany(-i) .....

Działając w imieniu i na rzecz .....

.....

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na ***„Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, wdrożeniem i konsultacjami"***, zgodnie z wymaganiami określonymi w specyfikacji warunków zamówienia i projektowanych postanowieniach umowy wraz z załącznikami, oferuję(-emy) realizację przedmiotu zamówienia, za cenę:

I. **Tabela nr 1 – Etap I**

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
1.	**Przełącznik szkieletowy typ A**, spełniający wymagania określone w Rozdz. I.2. lit. A SWZ. ***Producent*** ..... ***Model****	**2**					
2.	**Przełącznik dostępowy typ A (z portami uplink 25G)**, spełniający wymagania określone w Rozdz. I.2. lit. C SWZ. ***Producent*** ..... ***Model****	**34**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
	.....						
3.	**Przełącznik dostępowy typ B (bez portów uplink)**, spełniający wymagania określone w Rozdz. I.2. lit. D SWZ. ***Producent*** ..... ***Model****	**36**					
4.	**Przełącznik dostępowy typ C**, spełniający wymagania określone w Rozdz. I.2. lit. E SWZ. ***Producent*** ..... ***Model****	**2**					
5.	**Moduł optyczny interfejsowy SFP28 typu 10/25Gigabit Ethernet 10/25GBASE-CSR do przełączników dostępowych typ A**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 1.1 SWZ. ***Producent*** ..... ***Model****	**36**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
6.	**Kabel do łączenia w stos do przełączników dostępowych typ A i B o dł. 1m**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 1.4 SWZ. ***Producent*** ..... ***Model****	**6**					
7.	**Kabel do łączenia w stos do przełączników dostępowych typ A i B o dł. 3m**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 1.2 SWZ. ***Producent*** ..... ***Model****	**24**					
8.	**Kabel połączeniowy typu twinax 40G 3m do przełączników szkieletowych typ A**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 2.4 SWZ. ***Producent*** ..... ***Model****	**4**					
9.	**Moduł optyczny interfejsowy SFP28 typu 10/25Gigabit Ethernet 10/25GBASE-CSR do**	**36**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
	przełączników szkieletowych typ A, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 2.1 SWZ ***Producent*** ..... ***Model****						
10.	**Moduł optyczny SFP+ typu 10G jednomodowy LR do przełączników szkieletowych typ A,** spełniający wymagania określone w Rozdz. I.2. lit. F pkt 2.5 SWZ. ***Producent*** ..... ***Model****	**4**					
11.	**Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ A,** spełniający wymagania określone w Rozdz. I.2. lit. F pkt 2.2 SWZ. ***Producent*** ..... ***Model****	**4**					
12.	**Kabel do łączenia w stos zasilający do przełączników dostępowych typ A i B o dł.**	**24**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
	1.5m, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 1.3 SWZ. ***Producent*** ..... ***Model****						
13.	**Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ A i przełączników dostępowych typ C,** spełniający wymagania określone w Rozdz. I.2. lit. F pkt 2.3 SWZ. ***Producent*** ..... ***Model****	**4**					
14.	**System zarządzania i monitorowania siecią w lokalizacji Warszawa oraz monitoringu sieci LAN w pozostałych lokalizacjach Zamawiającego,** spełniający wymagania określone w Rozdz. I.2. lit. G SWZ. ***Producent*** ..... ***Nazwa systemu, model serwera****	**1**					
15.	**Licencje do posiadanego i użytkowanego przez Kupującego systemu Cisco ISE w wersji**	**1 komplet**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
	2.7.0.356 na okres 24 miesięcy umożliwiające zestawienie jednocześnie 2000 sesji o których mowa w Rozdz. I.2. lit. J SWZ						
16.	**Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz Dokumentacja wytworzona w ramach Etapu I a także przeprowadzenie warsztatów zgodnie z założeniami w lit. L Załącznika nr 1 do ppu oraz przeprowadzenie instruktażu z obsługi wdrożonego sprzętu zgodnie z Załącznikiem nr 1A do ppu**	**1**					
Razem [∑1÷5]:					**X**		

- wymagane jest podanie oznaczeń part number nadanych przez producenta dla sprzętu i systemu zarządzania i monitorowania siecią oraz wymagany jest wykaz wyposażenia poprzez podanie part number wraz z ilością wchodzącą w skład danego urządzenia

II. **Tabela nr 2 – Etap II**

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
1.	**Przełącznik szkieletowy typ B**, spełniający wymagania określone w Rozdz. I.2. lit. B SWZ. ***Producent*** ..... ***Model****	**2**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
2.	**Moduł optyczny interfejsowy SFP typu 10GBASE-LRM do przełączników szkieletowych typ B**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 3.1 SWZ. ***Producent*** ..... ***Model****	**10**					
3.	**Moduł optyczny interfejsowy SFP typu 10GBASE-SR do przełączników szkieletowych typ B**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 3.2 SWZ. ***Producent*** ..... ***Model****	**10**					
4.	**Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ B**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 3.3 SWZ. ***Producent*** ..... ***Model****	**4**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
5.	**Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz Dokumentacja wytworzona w ramach Etapu II**	**1**					
Razem [∑1÷5]:					**X**		

- wymagane jest podanie oznaczeń part number nadanych przez producenta dla sprzętu i systemu zarządzania i monitorowania siecią oraz wymagany jest wykaz wyposażenia poprzez podanie part number wraz z ilością wchodzącą w skład danego urządzenia

III. **Tabela nr 3 – Etap III**

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
1.	**Kontroler sprzętowy WiFi**, spełniający wymagania określone w Rozdz. I.2. lit. H SWZ. ***Producent*** ..... ***Model****	**2**					
2.	**Kabel połączeniowy typu twinax 10G 7m do kontrolerów sprzętowych WiFi**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 4.1 SWZ. ***Producent*** ..... ***Model****	**4**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
	.....						
3.	**Moduł optyczny SFP+ z oferty producenta urządzenia 10GBase-SR**, spełniający wymagania określone w Rozdz. I.2. lit. F pkt 4.2 SWZ. ***Producent*** ..... ***Model****	8					
4.	**Radiowe punkty dostępowe WiFi**, spełniający wymagania określone w Rozdz. I.2. lit. I SWZ. ***Producent*** ..... ***Model****	50					
5.	**Wdrożenie Sieci Bezprzewodowej WiFi**	1					
6.	**Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz Dokumentacja wytworzona w ramach Etapu III**	1					
Razem [∑1÷6]:					X		

- wymagane jest podanie oznaczeń part number nadanych przez producenta dla sprzętu i systemu zarządzania i monitorowania siecią oraz wymagany jest wykaz wyposażenia poprzez podanie part number wraz z ilością wchodzącą w skład danego urządzenia

IV. Tabela nr 4 – Etap IV

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
1.	**Radiowe punkty dostępowe WiFi**, spełniający wymagania określone w Rozdz. I.2. lit. I SWZ. ***Producent*** ..... ***Model****	**45**					
2.	**Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz Dokumentacja wytworzona w ramach Etapu IV**	**1**					
Razem [∑1÷2]:					**X**		

- wymagane jest podanie oznaczeń part number nadanych przez producenta dla sprzętu i systemu zarządzania i monitorowania siecią oraz wymagany jest wykaz wyposażenia poprzez podanie part number wraz z ilością wchodzącą w skład danego urządzenia

V. **Tabela nr 5 – Etap V**

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
1.	**Radiowe punkty dostępowe WiFi**, spełniający wymagania określone w Rozdz. I.2. lit. I SWZ. ***Producent*** ..... ***Model****	**45**					

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
2.	**Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz Dokumentacja wytworzona w ramach Etapu I**	**1**					
Razem [∑1÷2]:					**X**		

- wymagane jest podanie oznaczeń part number nadanych przez producenta dla sprzętu i systemu zarządzania i monitorowania siecią oraz wymagany jest wykaz wyposażenia poprzez podanie part number wraz z ilością wchodzącą w skład danego urządzenia

VI. Tabela nr 6 – Konsultacje

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
1	**Konsultacje techniczne**, o których mowa w §2 ust. 3 projektowanych postanowień umowy.	**300**					

VII. Tabela nr 7 – Gwarancja

Lp.	Przedmiot zamówienia	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
			%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f] = [c] + [e]*
1	**Gwarancja**, o których mowa w § 6 projektowanych postanowień umowy.				

VIII. Tabela nr 8 – Łączna cena oferty

Lp.	Przedmiot zamówienia:	Łączna cena ofertowa netto (zł) *[w poz. 1-7 należy wpisać sumę cen ofertowych netto odpowiednio z Tabel nr 1-7]*	Podatek VAT		Łączna cena ofertowa brutto (zł)
			%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f] = [c] + [e]*
1	**Tabela nr 1 – Etap I**				
2	**Tabela nr 2 – Etap II**				
3	**Tabela nr 3 – Etap III**				
4	**Tabela nr 4 – Etap IV**				
5	**Tabela nr 5 – Etap V**				
6	**Tabela nr 6 – Konsultacje techniczne**				
7	**Tabela nr 7 - Gwarancja**				
	Razem [∑1÷7]:		X		

Słownie zł łączna cena ofertowa netto: _____

Słownie zł łączna cena ofertowa brutto: _____

IX. Dodatkowe parametry techniczne

1 Zgodnie z kryterium oceny ofert oferujemy Zamawiającemu spełnienie wszystkich wymagań określonych przez Zamawiającego w Załączniku 1B do projektowanych postanowień umowy, stanowiących Załącznik nr 8 do SWZ. W takim przypadku Wykonawca zobowiązany jest do dołączenia od oferty dokumentacji technicznej pochodzącej od producenta (wraz z tłumaczeniem na język polski, jeśli dokumentacja jest sporządzona w języku obcym), dostępnej na stronach internetowych producenta, potwierdzających spełnienie poszczególnych wymagań. Wymagane jest wskazanie w dokumentacji miejsc określających spełnienie poszczególnych, oferowanych wymagań. ..... *)

*) **UWAGA:**

1. *Wykonawca winien wyraz TAK albo NIE, bądź w inny jednoznaczny sposób wyrazić swoją wolę.*
2. *Jeżeli Wykonawca zaoferuje spełnienie wszystkich wymagań określonych przez Zamawiającego w Załączniku 1B do projektowanych postanowień umowy, stanowiących Załącznik nr 8 do SWZ, oferta takiego Wykonawcy otrzyma 27 pkt w kryterium dodatkowe parametry techniczne P_D.*

3. *W przypadku, gdy Wykonawca nie wskaże, czy oferuje spełnienie wszystkich wymagań określonych przez Zamawiającego w Załączniku 1B do projektowanych postanowień umowy, stanowiących Załącznik nr 8 do SWZ (np. nie wypełni pkt VIII Formularza Ofertowego), Zamawiający uzna, że Wykonawca nie oferuje spełniania ww. wymagań.*
4. *W przypadku, gdy Wykonawca wskaże, czy oferuje spełnienie niektórych wymagań określonych przez Zamawiającego w Załączniku 1B do projektowanych postanowień umowy, stanowiących Załącznik nr 8 do SWZ (np. nie wypełni pkt VIII Formularza Ofertowego), Zamawiający nie przyzna ofercie takiego Wykonawcy pkt w ramach tego kryterium oceny ofert.*

Oświadczamy, że:

1. Zapoznaliśmy się z treścią specyfikacji warunków zamówienia (SWZ), w tym projektowanych postanowień umowy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
2. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdz. II SWZ oraz projektowanych postanowieniach umowy.
3. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
4. Uważamy się za związanych niniejszą ofertą do terminu określonego w SWZ.
5. Wadium w wysokości **100.000,00 zł** (słownie: sto tysięcy złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
6. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr .....prowadzony w banku ..... Oświadczenie o zwolnieniu wadium wniesionego w innej formie niż pieniądz należy przekazać gwarantowi/poręczycielowi na następujący adres e-mail.....
7. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **2%** ceny całkowitej podanej w ofercie.
8. W przypadku udzielenia nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
9. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz nazwę Podwykonawcy, jeśli jest już znany):
   9.1. .....[1]
   [1] w przypadku *niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.*
   UWAGA:
   Zamawiający przypomina, że powyższy punkt Formularza Ofertowego należy wypełnić w każdym przypadku, jeśli Wykonawca zamierza powierzyć podwykonawcom wykonanie części zamówienia, a także mając na uwadze treść art. 118 ust. 2 ustawy cyt.: „W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane."
   Udział podmiotu trzeciego w realizacji zamówienia w odniesieniu do warunków winien mieć charakter podwykonawstwa, w związku z czym wypełnieniu podlega pkt 9 Formularza Ofertowego.
10. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres e-mail: ..... Dane kontaktowe: imię i nazwisko ....., nr tel. ....., adres e-mail: .....
11. Dokumenty wymienione od strony ..... do strony ..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913) i nie mogą być ujawnione pozostałym uczestnikom postępowania.
    UWAGA:
    Zamawiający przypomina, że stosownie do treści:
    - *art. 18 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa*
    - *Rozdz. VIII.1. pkt 5 SWZ wszelkie informacje stanowiące tajemnicę przedsiębiorstwa muszą zostać odpowiednio oznaczone a następnie załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla Informacji stanowiących tajemnicę przedsiębiorstwa.*
12. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO)[2] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.[3]

[2] *rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2. oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35).*

[3] *w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie ma obowiązku składać (w takim przypadku Wykonawca może usunąć treści oświadczenia np. przez jego wykreślenie, przekreślenie, itp.).*

13. Jednocześnie, zgodnie z treścią art. 225 ust. 2 ustawy oświadczam, że wybór niniejszej oferty:
    13.1. **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego[4]
    13.2. **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, w związku z tym:[4]
        13.2.1. .....[5]

[4] *Niepotrzebne skreślić. W przypadku nie skreślenia (nie wskazania) żadnej z ww. treści oświadczenia i niewypełnienia powyższego pola oznaczonego: „należy wskazać nazwę (rodzaj) towaru/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz ich wartość bez kwoty podatku od towarów i usług" – Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.*

[5] *W pkt. 13.2.1. należy wskazać: nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego, wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku, stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.*

14. Zgodnie z Rozdz. IV.1. SWZ do oferty zostają załączone dokumenty:
    14.1. .....
    14.2. .....
    14.3. .....
    14.4. .....
    14.5. .....

Świadom odpowiedzialności karnej oświadczam, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień złożenia oferty (art. 297 k.k.).

Załącznik nr 2 do SWZ – wzór Oświadczenia o potwierdzeniu braku podstaw wykluczenia – art. 5k rozporządzenia 2022/576 w sprawie zmiany rozporządzenia Rady (UE) nr 833/2014 oraz art. 7 ustawy o szczególnych rozwiązaniach

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie o braku podstaw wykluczenia – art. 5k rozporządzenia 2022/576 w sprawie zmiany rozporządzenia Rady (UE) nr 833/2014 oraz art. 7 ustawy o szczególnych rozwiązaniach
DPIZP.2610.17.2021

Przystępując do udziału w postępowaniu o zamówienie publiczne na ***„Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, wdrożeniem i konsultacjami"*** oświadczam(-y), że na dzień złożenia niniejszego oświadczenia nie podlegam(-y) wykluczeniu na podstawie na podstawie:

1. art. 5k rozporządzenia 2022/576 w sprawie zmiany rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), oświadczam, nie zachodzą w stosunku do mnie opisane tamże okoliczności skutkujące zakazem udzielania lub dalszego wykonywania zamówień publicznych, w szczególności, że:
   1.1. nie jestem obywatelem rosyjskim, osobą fizyczną lub prawną, podmiotem lub organem z siedzibą w Rosji;
   1.2. nie jestem osobą prawną, podmiotem lub organem, do których prawa własności bezpośrednio lub pośrednio w ponad 50 % należą do podmiotu, o którym mowa w pkt. 14.1. niniejszego oświadczenia;
   1.3. nie jestem osobą fizyczną lub prawną, podmiotem lub organem działającym w imieniu lub pod kierunkiem podmiotu, o którym mowa w pkt. 14.1. lub 14.2. niniejszego oświadczenia;
   1.4. nie zaangażuję podwykonawców, dostawców będących obywatelami rosyjskimi, osobami fizycznymi lub prawnymi, podmiotów lub organów o których mowa w pkt. 14.1.-14.3. niniejszego oświadczenia, w przypadku gdy przypada na nich ponad 10 % wartości zamówienia.
2. art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 r. poz. 835; dalej ustawa o szczególnych rozwiązaniach) tj.:
   2.1. Nie jestem podmiotem wymienionym w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanym na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającą o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;
   2.2. Jestem podmiotem:
      2.2.1. Dla którego nie występuje beneficjent rzeczywisty.[1]
      2.2.2. Którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest:

         2.2.2.1. Imię i Nazwisko - .....[1]
         ww. osoba jest/nie jest[1] wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;

         2.2.2.2. Imię i Nazwisko - .....[1]
         ww. osoba jest/nie jest[1] wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;
   2.3. Jestem podmiotem:
      2.3.1. Dla którego nie występuje jednostka dominująca.1
      2.3.2. Którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106) jest:

         2.3.2.1. Nazwa podmiotu ..... adres ..... [1]
         ww. podmiot jest/nie jest[1] wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na

listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach.

2.3.2.2. Nazwa podmiotu ..... adres ..... [1]
ww. podmiot jest/nie jest[1] wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach.

W przypadku zmiany w trakcie realizacji umowy stanu faktycznego w zakresie objętym niniejszym oświadczeniem zobowiązuję się do niezwłocznego powiadomienia Zamawiającego o zakresie zmian.

[1] Niepotrzebne skreślić

Załącznik nr 3 do SWZ – wzór Oświadczenia o podziale obowiązków w trakcie realizacji zamówienia

Oświadczenie o podziale obowiązków w trakcie realizacji zamówienia
(dotyczy Wykonawców wspólnie ubiegających się o udzielenie zamówienia)

DPIZP.2610.17.2021

Działając w imieniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia: .....[1], przystępując do udziału w postępowaniu o zamówienie publiczne na ***„Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, wdrożeniem i konsultacjami"*** oświadczam(-y), że wyszczególnione poniżej dostawy/usługi zostaną zrealizowane zgodnie z poniższym:

1. Wykonawca .....[2] wykona następujące usługi/dostawy w ramach realizacji zamówienia:
   1.1. .....
   1.2. .....
   1.3. .....
2. Wykonawca .....[2] wykona następujące usługi/dostawy w ramach realizacji zamówienia:
   2.1. .....
   2.2. .....
   2.3. .....
3. Wykonawca .....[2] wykona następujące usługi/dostawy w ramach realizacji zamówienia:
   3.1. .....
   3.2. .....
   3.3. .....

UWAGA:

[1] należy wpisać firmy wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia

[2] należy wpisać firmy i adresy poszczególnych Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

Załącznik nr 4 do SWZ – wzór Oświadczenia o braku podstaw wykluczenia

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie o braku podstaw wykluczenia

DPIZP.2610.17.2021

Przystępując do udziału w postępowaniu o zamówienie publiczne na ***„Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, wdrożeniem i konsultacjami"*** oświadczam(-y), że na dzień złożenia niniejszego oświadczenia aktualne pozostają informacje zawarte w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, tj. nie podlegam(-y) wykluczeniu na podstawie:

1. art. 108 ust. 1 pkt 3 ustawy,
2. art. 108 ust. 1 pkt 4 ustawy dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
3. art. 108 ust. 1 pkt 5 ustawy dotyczących zawarcia z innymi Wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
4. art. 108 ust. 1 pkt 6 ustawy,
5. art. 109 ust. 1 pkt 1 ustawy odnośnie do naruszenia obowiązków dotyczących płatności podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz.U. z 2019 r. poz. 1170 z późn. zm.),
6. art. 109 ust. 1 pkt 2 lit. b ustawy dotyczących ukarania za wykroczenie, za które wymierzono karę ograniczenia wolności lub karę grzywny,
7. art. 109 ust. 1 pkt 2 lit. c ustawy,
8. art. 109 ust. 1 pkt 3 ustawy dotyczących ukarania za wykroczenie, za które wymierzono karę ograniczenia wolności lub karę grzywny,
9. art. 109 ust. 1 pkt 5-10 ustawy.

Załącznik nr 5 do SWZ – wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej
DPIZP.2610.17.2021

Przystępując do udziału w postępowaniu o zamówienie publiczne na ***„Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, i wdrożeniem"*** oświadczam(-y), że:

1. **nie należę(-ymy) do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j.: Dz. U. z 2021 r., poz. 275) **z żadnym z Wykonawców, którzy złożyli odrębną ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego[1].
2. **należę(-ymy) do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j.: Dz. U. z 2021 r., poz. 275) **z następującymi Wykonawcami, którzy złożyli odrębną ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego[1]:

Lp.	Nazwa podmiotu	Siedziba
1		
(...)		

Jednocześnie na potwierdzenie, że nasza oferta została przygotowana niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej składam(-y) następujące informacje i/lub dokumenty:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

UWAGA:

[1] niepotrzebne skreślić

Załącznik nr 6 do SWZ – wzór Oświadczenia – Wykaz dostaw

[warunek udziału w postępowaniu]

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie – Wykaz dostaw

DPIZP.2610.17.2021.

Przystępując do udziału w postępowaniu o zamówienie publiczne na ***„Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, wdrożeniem i konsultacjami"***, składam(-y) wykaz dostaw wykonanych (wykonywanych) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, na potwierdzenie spełniania warunku udziału w postępowaniu, o którym mowa w Rozdz. III.2. pkt 1.1.1. SWZ.

Lp.	Przedmiot wykonanych/wykonywanych dostaw *(wg warunku udziału w postępowaniu)*	Wartość brutto dostawy w zł *(w przypadku gdy zakres dostawy jest szerszy, należy podać wyłącznie wartość dostawy odpowiadającej treści warunku udziału w postępowaniu w badanym zakresie, wg warunku udziału w postępowaniu)*	Podmiot na rzecz którego wykonano dostawę *(nazwa i adres)*	Daty wykonania		Dowody	Informacje uzupełniające	
				Od dd-mm-rrrr	Do dd-mm-rrrr		Zasoby innego podmiotu	Nazwa innego podmiotu
1	2	3	4	5	6	7	8	9
1								
2								
3								

Uwaga do kol. 7:

1. *Do wykazu należy dołączyć dowody potwierdzające, że powyższe dostawy zostały wykonane lub są wykonywane należycie, tj.:*
   - 1.1. *referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane lub są wykonywane należycie, z tym, że w odniesieniu do nadal wykonywanych dostaw powtarzających się lub ciągłych referencje bądź inne dokumenty powinny być wydane nie wcześniej niż 3 m-ce przed upływem terminu składania ofert;*
   - 1.2. *oświadczenie Wykonawcy - jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów, o którym mowa wyżej w pkt 1.1;*
2. *Należy wpisać nazwę dowodu (dokumentu) potwierdzającego, że dostawy zostały wykonane lub są wykonywane należycie (podać numer strony);*

Uwaga do kol. 8:

1. *Zaznaczyć „TAK", tylko w przypadku, gdy Wykonawca polega na zdolnościach podmiotu udostępniającego zasoby dla wykazania spełniania warunku udziału;*
2. *Dla wykazania spełniania warunku udziału w postępowaniu, opisanego w Rozdz. III.2. pkt 1.1.1.SWZ, Wykonawca może polegać na zdolnościach podmiotu udostępniającego zasoby, na zasadach określonych w art. 118 Ustawy. W tym celu Wykonawca składa podmiotowe środki dowodowe zgodnie z zasadami określonymi w Rozdz. IV.5. SWZ.*

Załącznik nr 7 do SWZ – wzór Oświadczenia – Wykaz osób

[warunek udziału w postępowaniu]

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie – Wykaz osób

DPIZP.2610.17.2021.

Przystępując do udziału w postępowaniu o zamówienie publiczne na ***„Zakup przełączników sieciowych LAN oraz sieci WiFi wraz z dodatkowymi elementami (wkładki, kable, oprogramowanie) z gwarancją, wsparciem, wdrożeniem i konsultacjami"***, składam(-y) wykaz osób, które będą uczestniczyć w wykonaniu zamówienia, na potwierdzenie spełniania warunku udziału w postępowaniu, o którym mowa w Rozdz. III.2. pkt 1.1.2. SWZ.

1. ***Jedna osoba, spełniająca poniższe wymagania:***

Wymagania Zamawiającego wskazane w SWZ	**Wypełnia Wykonawca**					
Osoba, która posiada: 1) co najmniej 12 miesięczne doświadczenie przy realizacji zamówień o zakresie jak w Rozdz. III.2. pkt 1.1.1. SWZ z wyłączeniem wartości zamówień; 2) certyfikat wystawiony przez producenta Sprzętu IT oferowanego w postępowaniu, np. CCIE Enterprise Infrastructure (350-401 ENCOR) (1 osoba) lub równoważny 3) *Zamawiający uzna za certyfikaty równoważne do certyfikatów wymienionych powyżej z nazwy m.in. następujące certyfikaty: Juniper Networks Certified Internet Expert (JNCIE-ENT) lub* HP *Master Accredited Systems Engineer* (MASE) *– Network Infrastructure.*	1	1.1	Imię i Nazwisko			
		1.2.	Wskazana osoba spełnia wymagania zdefiniowane w Rozdz. III.2. pkt 1.1.2.SWZ			
		1.3	Posiadany certyfikat	1.3.1	Nazwa certyfikatu	
				1.3.2	Podmiot wydający certyfikat	
				1.3.3	Nr certyfikatu *[o ile dotyczy]*	
				1.3.4	Data ważności certyfikatu [DD-MM-RRRR] *[o ile dotyczy]*	
		1.4		1.4.1	Dysponowanie bezpośrednie	
Uwaga: *Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:* *1) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:* *a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,* *b) analogiczny stopień poziomu kompetencji,*						

c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu, 2) *potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowy certyfikaty muszą być potwierdzone egzaminem).*			Podstawa dysponowania osobą	1.4.2	Dysponowanie osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych	

Uwaga:

1. *Dla wykazania spełniania warunku udziału w postępowaniu opisanego w Rozdz. III.2. pkt 1.1.2. IWZ, Wykonawca może polegać, na zasadach określonych w art. 118 ustawy, na osobach zdolnych do wykonania zamówienia oddanych mu do dyspozycji przez inne podmioty.*
2. *W odniesieniu do podstawy dysponowania osobą Wykonawca wypełnia kolumnę „Dysponowanie bezpośrednie" albo „Dysponowanie osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych".*
3. *W przypadku dysponowania przez Wykonawcę osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych jest obowiązany udowodnić Zamawiającemu, iż będzie dysponował niezbędnymi osobami zdolnymi do wykonania zamówienia, w szczególności przedstawiając w tym celu dokumenty i oświadczenia w zakresie wskazanym w rozdziale IV.5 SWZ*

Załącznik nr 8 do SWZ – projektowane postanowienia umowy

Projektowane postanowienia umowy

Umowa nr _____/DI/2022/2610

zawarta w dniu _____ _____ 2022 r. w Warszawie pomiędzy:

Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie przy al. Jana Pawła II nr 70, 00-175 Warszawa, (adres do korespondencji: ARiMR Departament Informatyki ul. Poleczki 33, 02-822 Warszawa), REGON nr 010613083, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, zwaną dalej "**Kupującym**" lub „**ARiMR**", którą reprezentuje:

_____ –Zastępca Prezesa ARiMR, pełnomocnik;
_____ – Dyrektor Departamentu Księgowości, w ramach zajmowanego stanowiska wykonująca obowiązki Głównego Księgowego, pełnomocnik;

a

_____
_____
_____
_____, zwaną dalej "**Sprzedawcą**", którą reprezentuje:

_____ –
_____;
_____ –
_____;

zwanych łącznie „**Stronami**".

W wyniku wyboru oferty w postępowaniu o udzielenie zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego zgodnie z art. 132 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych dalej zwana „Ustawą" (Dz. U. z 2021 r. poz. 1129 ze zm.), zawarto umowę o następującej treści:

§ 1. Definicje

W niniejszej umowie następujące wyrażenia i określenia będą miały znaczenie zgodnie z podanymi poniżej definicjami, zapisane z dużej litery w celu podkreślenia, że jest to pojęcie zdefiniowane:

1) **Strony** – Sprzedawca i Kupujący wymienieni w komparycji Umowy;
2) **Umowa** – niniejsza umowa wraz z załącznikami regulująca prawa i obowiązki Stron z niej wynikające i związane z jej wykonaniem;
3) **Sprzęt IT** – urządzenia sieciowe do realizacji sieci LAN oraz sieci bezprzewodowej WIFI a także urządzenia informatyczne wraz z systemem zarządzania oraz Oprogramowaniem w Lokalizacjach Kupującego, których ilość i parametry zostały szczegółowo opisane w Załączniku nr 1 do Umowy;
4) **Oprogramowanie** – system zarządzania i monitorowania siecią LAN wraz z oprogramowaniem stanowiącym doposażenie istniejącego systemu NAC (Cisco ISE) o nowe licencje, tj. licencje wyspecyfikowane w Załączniku nr 1 do umowy dostarczone przez Sprzedawcę, z którego Kupujący korzysta na podstawie Licencji udzielonej przez producenta na zasadach subskrypcji obowiązującej do czasu zakończenia Gwarancji, która została opisana w Załączniku nr 1 do Umowy;
5) **Projekt Techniczny** - dokumentacja projektowa, wykonana przez Sprzedawcę i odebrana przez Kupującego, szczegółowo określająca i opisująca wszelkie elementy Sprzętu IT u Kupującego, zakres i opis wykonywanych prac, kontrolę jakości prac i odbiory prac, instalacje i wyposażenie techniczne, zastosowane technologie, rozwiązania techniczne, specyfikacje produktowe, procedury konfiguracyjne oraz procedury testowe dla Sprzętu IT u Kupującego wraz z rysunkami i schematami połączeń elektrycznych i logicznych Sprzętu IT - szczegółowo opisany w Załączniku nr 1 D do Umowy;
6) **Licencja** – prawo do czasowego korzystania z Oprogramowania do czasu zakończenia obowiązywania Gwarancji, zgodnie z warunkami określonymi przez producenta Oprogramowania, potwierdzone dokumentem licencyjnym;
7) **Gwarancja** – opieka serwisowa i wsparcie techniczne dla Sprzętu IT oraz Oprogramowania, wykonywana w zakresie i na zasadach określonych w Umowie oraz zgodnie z warunkami określonymi przez producenta Sprzętu IT i Oprogramowania;
8) **Wdrożenie** – czynności wykonywane przez Sprzedawcę w ramach Etapów, mające na celu instalację i uruchomienie dostarczonego Sprzętu IT w Lokalizacjach, instalację Oprogramowania w CPD oraz uruchomienie sieci bezprzewodowej WIFI w

Lokalizacji Warszawa (dalej zwane „Wdrożenie Sieci Bezprzewodowej WIFI") – szczegółowo opisane w Załączniku nr 1 A do Umowy z zastrzeżeniem, że Wdrożenie nie obejmuje Licencji dostarczonych do systemu NAC (CISCO ISE);

9) **Dokumentacja powykonawcza** - dokumentacja zawierająca schematy fizyczne i logiczne infrastruktury sieci IT u Kupującego, w tym podłączenia Sprzętu IT, konfigurację Sprzętu IT oraz opis zastosowanych rozwiązań i technologii - szczegółowo opisana w Załączniku nr 1 D do Umowy;
10) **Dokumenty** - instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT, dokument licencyjny dla Oprogramowania oraz dokumenty gwarancyjne w tym potwierdzające prawo dostępu do Gwarancji producenta Sprzętu IT i Oprogramowania,
11) **Lokalizacja/Lokalizacje** - Centrala ARiMR, ul. Poleczki 33, Warszawa (dalej zwana „Lokalizacja Warszawa"), Wydział Tworzenia Oprogramowania, ul. Bohdana Dobrzańskiego 7, Lublin (dalej zwana „Lokalizacja Lublin") oraz Centrum Przetwarzania Danych zlokalizowane przy ul. Poleczki 23 w Warszawie (dalej „CPD");
12) **Dni Robocze** – dni w godzinach pracy Kupującego od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych od pracy u Kupującego, o których Kupujący powiadomi Sprzedawcę.
13) **Etap** - wyodrębniona część realizacyjna Umowy, obejmująca wykonanie określonych świadczeń Sprzedawcy opisanych Umową. Etapy podlegają Odbiorom. Zakres dostaw i prac dla poszczególnych Etapów określa Załącznik nr 1A do Umowy.
14) **Odbiór** – potwierdzenie przez Kupującego należytego wykonania Umowy w zakresie wykonania poszczególnych Etapów, Dokumentacji, Wdrożenia. Dowodem dokonania Odbioru jest odpowiedni Protokół Odbioru.
15) **Protokół Odbioru** – dokument stanowiący potwierdzenie dokonanie Odbioru w zakresie poszczególnych Etapów lub Wdrożenia, sporządzony odpowiednio zgodnie z Załącznikiem nr 2 lub Załącznikiem 2 A do Umowy.
16) **Plan Testów Akceptacyjnych** - oznacza dokument opracowany przez Sprzedawcę, opisujący planowane testy akceptacyjne wraz ze scenariuszami testów akceptacyjnych na podstawie, którego Kupujący przeprowadzi weryfikację poprawności wdrożenia danego Etapu - szczegółowo opisany w Załączniku nr 1 D do Umowy;
17) **Dokumentacja** - oznacza dokumentację dostarczaną w ramach realizacji Umowy tj. Projekt Techniczny, Dokumentację powykonawczą, Plan Testów Akceptacyjnych. Wymagania dotyczące dokumentacji zostały zawarte w Załączniku nr 1 D do Umowy.

§ 2. Przedmiot Umowy

1. Na podstawie Umowy Sprzedawca:
   1) sprzedaje i dostarczy fabrycznie nowy, nienoszący śladów uprzedniego używania Sprzęt IT wraz z Oprogramowaniem, zgodnie ze specyfikacją stanowiącą Załącznik nr 1 do Umowy, *Załącznik nr 1B do Umowy (jeżeli Sprzedawca zaoferuje spełnienie wymagań ocenianych w ramach kryterium oceny ofert dodatkowe parametry techniczne)* oraz z Formularzem ofertowym, stanowiącym Załącznik nr 7 do Umowy;
   2) wykona i dostarczy Dokumentację w formie papierowej i elektronicznej oraz wykona i przeprowadzi Wdrożenie w ramach Etapów zgodnie z Załącznikiem nr 1 A do Umowy,
   3) świadczył będzie Gwarancję dla Sprzętu IT i Oprogramowania przez okres 24 miesięcy oraz zapewni świadczenie Gwarancji przez producenta Sprzętu IT i Oprogramowania, poprzez wydanie odpowiedniego dokumentu na rzecz Kupującego, potwierdzającego prawo dostępu do Gwarancji producenta Sprzętu IT i Oprogramowania w ww. okresie zgodnie z ogólnymi warunkami producenta Sprzętu IT i Oprogramowania, a Kupujący kupuje Sprzęt IT i nabywa Licencje na Oprogramowania.
2. Wraz z dostawą Sprzętu IT wraz z Oprogramowaniem Sprzedawca dostarczy Kupującemu Dokumenty.
3. W ramach Umowy Sprzedawca zapewni Kupującemu 300 godzin konsultacji technicznych w okresie 24 miesięcy od dnia podpisania bez zastrzeżeń Protokołu odbioru Wdrożenia, którego wzór stanowi Załącznik nr 2 A do Umowy, jednak nie mniej niż 50 godzin, w zakresie problemów dotyczących Sprzętu IT lub Oprogramowania. Konsultacje będą obejmowały analizy, audyty oraz rekomendację dot. Sprzętu IT lub Oprogramowania, jak również wszelkiego rodzaju prace rekonfiguracyjne Sprzętu IT lub Oprogramowania oraz pomoc przy pracach technicznych przeprowadzanych przez Kupującego w Lokalizacjach. W ramach konsultacji technicznych wymagana będzie również przez Kupującego asysta techniczna w zakresie wszystkich niezbędnych czynności związanych z przeniesieniem Sprzętu IT, jeśli w okresie obowiązywania Umowy zaistnieje konieczność relokacji Sprzętu IT, tak aby utrzymać warunki gwarancji producenta na Sprzęt IT. Konsultacje będą świadczone w języku polskim, drogą elektroniczną .....lub telefoniczną pod numerem telefonu..... lub w siedzibie Kupującego. Czas dojazdu Sprzedawcy nie będzie wliczony jako wykorzystanie dostępnej puli godzin.
4. Sprzedawca będzie przyjmował zgłoszenia konsultacyjne od poniedziałku do piątku, w godzinach od 7:00 -15:00 telefonicznie pod numerem: .....lub na adres poczty elektronicznej ..... Przyjęcie zgłoszenia zostanie przez Sprzedawcę potwierdzone (drogą elektroniczną na adresy e-mail pracowników Kupującego, wskazanych w §3 ust. 2 pkt 1 Umowy) w ciągu 1 godziny od otrzymania zgłoszenia. Niepotwierdzenie zgłoszenia w powyższym terminie Kupujący uznaje za przyjęcie zgłoszenia. O każdej zmianie adresu lub numeru telefonu wskazanego powyżej, Sprzedawca zobowiązany jest niezwłocznie powiadomić na piśmie Kupującego. Zmiana danych, o których mowa w zdaniu poprzedzającym nie wymaga zmiany Umowy w formie pisemnego aneksu, a jedynie poinformowania drugiej Strony o zmianie.

5. Na koniec każdego kwartału Sprzedawca dostarczy Protokół odbioru konsultacji ze zgłoszonych i przeprowadzonych konsultacji, którego wzór został określony w Załączniku nr 4 A do Umowy.

§ 3. Wymagania dotyczące wykonania Umowy

1. Sprzedawca oświadcza, że posiada konieczne doświadczenie i profesjonalne kwalifikacje niezbędne do prawidłowego wykonania Umowy i zobowiązuje się do wykonania Umowy przy zachowaniu należytej staranności określonej w art. 355 § 2 Kodeksu Cywilnego.
2. Osobami upoważnionymi do rozpatrywania bieżących spraw i podpisywania protokołów odbioru związanych z wykonaniem Umowy, przy zachowaniu określonych w niej warunków, w tym terminów:
   1) po stronie Kupującego są:
      Pan(-i) _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl
      Pan(-i) _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl
      Pan(-i) _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl
   2) po stronie Sprzedawcy są:
      Pan(-i) _____ tel.: (XX) _____; e-mail: _____@_____
      Pan(-i) _____ tel.: (XX) _____; e-mail: _____@_____
3. Zmiana osób, o których mowa w ust. 2 powyżej, nie stanowi zmiany Umowy wymagającej sporządzenia aneksu.
4. Sprzedawca oświadcza, że Sprzęt IT i Oprogramowanie posiada wszelkie certyfikaty i homologacje niezbędne do eksploatacji na terytorium Rzeczypospolitej Polskiej oraz gwarantuje, że Sprzęt IT i Oprogramowanie jest zgodny z Polskimi Normami niezawodności i bezpieczeństwa.
5. Sprzedawca oświadcza, że dostarczony Sprzęt IT oraz Oprogramowanie są wolne od oprogramowania szkodliwego i szpiegującego, a także są zabezpieczone przed nieautoryzowanym dostępem. Ponadto wszystkie elementy oprogramowania zarówno firmware (oprogramowanie systemowe) jak i określone w definicji Oprogramowanie muszą być standardowe, dostępne na stronie producenta utworzone min. 3 miesiące przed terminem otwarcia ofert.
6. Do realizacji przedmiotu Umowy Sprzedawca zapewni udział co najmniej jednej osoby wskazanej w wykazie osób (złożonym w postępowaniu) na potwierdzenie spełniania warunku udziału w postępowaniu. W przypadku zmian personalnych Sprzedawca zobowiązany jest do zapewnienia osoby o co najmniej tych samych kwalifikacjach i doświadczeniu, jak wymagana dla wykazania spełniania warunku udziału w postępowaniu. Każdorazowo zmiany personalne, o których mowa w zdaniu poprzednim wymagają zgody Kupującego, z wyjątkiem przypadków, gdy odsunięcie od realizacji Umowy następuje z przyczyn pozostających poza kontrolą Sprzedawcy, np. ustanie stosunku pracy, zdarzenie losowe. W celu uniknięcia wątpliwości Strony potwierdzają, że wszelkie konsekwencje zmian osób uczestniczących w realizacji Umowy po stronie obciążają Sprzedawcę.

§ 4. Terminy i odbiory

1. Umowa zostanie wykonana przez Sprzedawcę w następujących terminach:
   1) Etapy I-V w zakresie opisanym w Załączniku nr 1 A do Umowy, nie później niż w terminie do 90 dni kalendarzowych od dnia zawarcia Umowy, jednak nie później niż w terminie do dnia 14.11.2022 r.
   2) Gwarancja świadczona będzie przez Sprzedawcę przez okres 24 miesięcy od dnia podpisania Protokołu odbioru Wdrożenia, którego wzór stanowi Załącznik nr 2A.
2. Odbiorom podlegają dostawy i rezultaty prac Sprzedawcy w podziale na Etapy. Odbiór poszczególnych Etapów zostanie potwierdzony podpisaniem przez Strony bez żadnych uwag lub zastrzeżeń, odpowiednio dla każdego z Etapów, Protokołu Odbioru Etapu, którego wzór określa Załącznik nr 2 do Umowy. Poniżej opisane zasady odbioru obowiązują dla każdego z Etapów.
3. Sprzedawca powiadomi, w formie pisemnej, Kupującego o terminie dostarczenia Sprzętu IT wraz z Oprogramowaniem, i Dokumentów oraz o terminie rozpoczęcia Wdrożenia w Lokalizacjach, z wyprzedzeniem co najmniej 2 Dni Roboczych. W terminie do 2 Dni Roboczych Kupujący potwierdzi wskazany termin lub wskaże inny, jednak nie później niż 4 Dni Robocze od daty otrzymania przez Kupującego ww. powiadomienia.
4. W terminie do 5 Dni Roboczych od dnia zawarcia Umowy Sprzedawca dostarczy Kupującemu Projekt Techniczny. Odbiór zostanie potwierdzony Protokołem odbioru Projektu Technicznego, którego wzór stanowi Załącznik nr 3. Kupujący zastrzega sobie prawo zgłaszania uwag i zastrzeżeń do Projektu Technicznego w terminie 3 Dni Roboczych, które Sprzedawca zobowiązany jest uwzględnić w terminie 3 Dni Roboczych od dnia ich otrzymania od Kupującego.
5. Dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentów oraz dostarczenie Dokumentacji oraz Wdrożenie odbędzie się na koszt i ryzyko Sprzedawcy. Sprzedawca dostarczy Sprzęt IT wraz z Oprogramowaniem i Dokumenty zgodnie z warunkami Umowy i poniesie pełne ryzyko związane z niebezpieczeństwem utraty albo uszkodzenia Sprzętu IT wraz z Oprogramowaniem do momentu dokonania ich odbioru przez osobę upoważnioną przez Kupującego, zgodnie z ust. 6 - 11.
6. Odbiór Sprzętu IT wraz z Oprogramowaniem i Dokumentów zostanie dokonany komisyjnie z udziałem upoważnionych przedstawicieli Sprzedawcy i Kupującego. Odbiór i zawiadomienia Stron dotyczące odbioru i Wdrożenia będą dokonywane w Dniach Roboczych.

7. Podczas odbioru Sprzętu IT wraz z Oprogramowaniem i Dokumentów Sprzedawca w obecności Kupującego:
   1) rozpakuje dostarczony Sprzęt IT oraz sprawdzi czy nie nosi znamion uszkodzeń mechanicznych oraz czy jest fabrycznie nowy i zgodny z Załącznikiem nr 1 i nr 7 do Umowy oraz Załącznikiem *1 B (Załącznik nr 1 B zostanie wprowadzony do treści umowy, jeżeli Sprzedawca zaoferuje spełnienie wymagań ocenionych w ramach kryterium oceny ofert dodatkowe parametry techniczne);*
   2) podłączy Sprzęt IT do sieci zasilającej i zainstaluje Oprogramowanie;
   3) usunie z miejsca dostarczenia i zutylizuje wszelkie opakowania, pozostałe po dostarczeniu i zainstalowaniu Sprzętu IT.
8. Sprzedawca wykona Wdrożenie odpowiednio dla każdego z Etapów w zakresie zgodnym z zapisami w Załączniku nr 1 A do Umowy. Prawidłowość Wdrożenia każdego z Etapów będzie weryfikowana przez Kupującego na podstawie Planu Testów Akceptacyjnych.
9. Po dokonaniu przez Kupującego bez zastrzeżeń odbioru Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz Wdrożenia w Lokalizacjach oraz Dokumentacji dla danego Etapu Kupujący podpisze Protokół odbioru Etapu, którego wzór stanowi Załącznik nr 2 do Umowy.
10. W przypadku stwierdzenia podczas odbioru, że:
    1) Sprzęt IT lub Oprogramowanie są niezgodne z Załącznikiem nr 1 lub Załącznikiem nr 7 do Umowy oraz Załącznikiem *1 B (Załącznik 1 B zostanie wprowadzony do treści umowy, jeżeli Sprzedawca zaoferuje spełnienie wymagań ocenionych w ramach kryterium oceny ofert dodatkowe parametry techniczne);*
    2) lub posiadają ślady zewnętrznego uszkodzenia lub
    3) nie dostarczono wszystkich wymaganych Dokumentów, o których mowa w ust. 3 lub
    4) Wdrożenie nie zostało wykonane prawidłowo lub
    5) Sprzęt IT wraz z Oprogramowaniem, Dokumenty lub Wdrożenie budzą inne zastrzeżenia niż określone w pkt 1-4,

    Kupujący odmówi podpisania Protokołu odbioru Etapu, jednocześnie przekaże Sprzedawcy protokół przedstawiający powód odmowy odbioru ze wskazaniem terminu dostarczenia Sprzętu IT wraz z Oprogramowaniem lub Dokumentów wolnych od wad lub ponownego wykonania Wdrożenia. Procedura czynności odbioru zostanie przeprowadzona ponownie.
11. W przypadku stwierdzenia podczas powtórnej procedury czynności odbioru którejkolwiek z okoliczności wskazanych w ust. 10, Kupujący odmówi odbioru przedmiotu Umowy i jednocześnie przekaże Sprzedawcy protokół przedstawiający powód odmowy odbioru Sprzętu IT wraz z Oprogramowaniem, Dokumentów wraz z Wdrożeniem. W sytuacji odmowy odbioru Sprzętu IT wraz z Oprogramowaniem i Dokumentów Sprzedawca ma obowiązek odbioru dostarczonego Sprzętu IT wraz z Oprogramowaniem i Dokumentów z miejsca dostarczenia w terminie 5 Dni Roboczych od daty przekazania Sprzedawcy protokołu przedstawiającego powody odmowy odbioru Sprzętu IT.
12. Sprzedawca dostarczy Kupującemu Dokumentację powykonawczą zgodnie z wymaganiami zawartymi w Załączniku nr 1 D do Umowy dla każdego z Etapów. Odbiór zostanie potwierdzony Protokołem odbioru Dokumentacji powykonawczej, którego wzór stanowi Załącznik nr 3 do Umowy. Kupujący zastrzega sobie prawo zgłaszania uwag do Dokumentacji powykonawczej. Sprzedawca zobowiązany jest uwzględnić uwagi Kupującego lub zgłosić zastrzeżenia w terminie 3 Dni Roboczych od dnia otrzymania uwag od Kupującego.
13. Sprzedawca dostarczy Kupującemu Plan Testów Akceptacyjnych na co najmniej 5 Dni Roboczych przed planowanymi testami. Plan Testów Akceptacyjnych musi być zgodny z wymaganiami zawartymi w Załączniku nr 1 D do Umowy i jest sporządzany dla każdego z Etapów. Odbiór zostanie potwierdzony Protokołem odbioru Plan Testów Akceptacyjnych, którego wzór stanowi Załącznik nr 3 do Umowy. Kupujący zastrzega sobie prawo zgłaszania uwag do Plan Testów Akceptacyjnych. Sprzedawca zobowiązany jest uwzględnić uwagi Kupującego lub zgłosić zastrzeżenia w terminie 3 Dni Roboczych od dnia otrzymania uwag od Kupującego. Pozytywny odbiór Planu Testów Akceptacyjnych warunkuje przystąpienie Kupującego do odbioru Etapu.
14. Wszystkie powiadomienia dotyczące odbiorów Sprzętu IT wraz z Oprogramowaniem, Dokumentów, Projektu Technicznego, Dokumentacji powykonawczej, Planu Testów Akceptacyjnych lub wykonania Wdrożenia powinny być dokonywane w Dni Robocze.
15. Na podstawie wszystkich Protokołów odbioru dla Etapów I-V Kupujący stwierdza poprawne zakończenie wszystkich Etapów oraz spełnienie wszystkich wymagań przewidzianych Umową i dokonuje końcowego odbioru Wdrożenia. Odbiór zostanie potwierdzony poprzez podpisanie bez uwag i zastrzeżeń Protokołu Odbioru Wdrożenia, którego wzór stanowi Załącznik nr 2 A do Umowy.

§ 5. Udzielenie Licencji

1. Kupujący, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 Umowy, nabywa Licencję upoważniającą do czasowego korzystania z Oprogramowania do czasu zakończenia okresu Gwarancji w celu zachowania funkcjonalności Sprzętu IT oraz służące do monitorowania i zarządzania Sprzętem IT.
2. Kupujący, w ramach udzielonej Licencji, zgodnie z warunkami producenta Oprogramowania, ma prawo do trwałego lub czasowego zwielokrotnienia Oprogramowania w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie; w zakresie, w którym jest to niezbędne dla wprowadzania, wyświetlania, stosowania, przekazywania, przechowywania Oprogramowania dla własnych potrzeb Kupującego, z uwzględnieniem treści ust. 3, zgodnie z jego charakterem i przeznaczeniem, Dokumentami i warunkami Umowy.

3. Licencja uzyskana zgodnie z zapisami ust. 2, może być wykorzystywana wyłącznie dla celów działalności Kupującego i nie obejmuje prawa do wprowadzania Oprogramowania do obrotu lub przekazywania ani w części ani w całości osobom trzecim zarówno odpłatnie, jak i nieodpłatnie w żadnej formie prawnej.
4. W ramach udzielonej Licencji Kupujący jest upoważniony do korzystania z Dokumentów dostarczonych z Oprogramowaniem, na polach eksploatacji wskazanych w ust. 2.

§ 6. Gwarancja

1. Gwarancja świadczona będzie przez Sprzedawcę przez okres 24 miesięcy od dnia podpisania Protokołu odbioru Wdrożenia, o którym mowa w § 4 ust. 15.
2. Sprzedawca zobowiązuje się, że podczas trwania Gwarancji, po otrzymaniu zgłoszenia serwisowego od Kupującego, na własny koszt i ryzyko, naprawi lub wymieni w terminach określonych w niniejszym paragrafie wadliwy Sprzęt IT na wolny od wad oraz usunie skutki tych wad. Naprawy będą dokonywane bezpośrednio przez Sprzedawcę w Lokalizacji, w której dokonano Wdrożenia Sprzętu IT, którego dotyczy wada.
3. Gwarancja obejmuje dokonanie naprawy, w tym wymianę podzespołów na nowe, a także dojazd serwisanta, transport Sprzętu IT oraz podstawienie urządzeń zastępczych.
4. W ramach Gwarancji Sprzedawca dokona naprawy Sprzętu IT, która nastąpi najpóźniej w najbliższym Dniu Roboczym rozpoczynającym się po Dniu Roboczym przyjęcia zgłoszenia serwisowego , przy czym procedura zgłaszania będzie się odbywać w reżimie 8x5xNBD tj. zgłoszenie serwisowe uznaje się za przyjęte, jeżeli zostało zgłoszone w Dniu Roboczym do godziny 15.00, zgłoszenia serwisowe dokonane po godz. 15.00 będzie traktowane jako dokonane w następnym Dniu Roboczym. Naprawa Sprzętu IT powinna być dokonana przez serwisanta posiadającego właściwe kwalifikacje techniczne.
5. Sprzedawca, w przypadku niemożności dokonania naprawy w terminie wskazanym w ust. 4, zobowiązany jest dokonać w tym terminie wymiany wadliwego Sprzętu IT na fabrycznie nowy, wolny od wad. Obowiązek, o którym mowa w zdaniu poprzednim dotyczy również sytuacji, gdy wada, usterka lub inna nieprawidłowość Sprzętu IT nie zostanie usunięta w wyniku dokonania naprawy po raz trzeci, przy czym dostarczenie Sprzętu IT w takim wypadku nastąpi najpóźniej w najbliższym Dniu Roboczym następującym po Dniu Roboczym przyjęcia przez Sprzedawcę czwartego zgłoszenia serwisowego dotyczącego tego samego Sprzętu IT. W przypadku, gdy dostarczenie takiego samego Sprzętu IT nie będzie możliwe, Sprzedawca dostarczy nowy Sprzęt IT o parametrach technicznych nie gorszych od określonych w Załączniku nr 1 i 7 do Umowy. Dostarczenie zastępcze wymaga zgody Kupującego.
6. Sprzedawca będzie przyjmował zgłoszenia serwisowe Kupującego od osób wskazanych pisemnie przez Kupującego, w trybie 24 godziny na dobę 7 dni w tygodniu (tryb 24/7) telefonicznie pod numerem: (XX) _____, lub na adres poczty elektronicznej: _____@_____. O każdej zmianie adresu lub numerów telefonów wskazanych powyżej, Sprzedawca zobowiązany jest niezwłocznie powiadomić na piśmie Kupującego. Zmiana danych, o których mowa w zdaniu poprzedzającym nie wymaga zmiany Umowy. Usunięcie wady lub wymiana Sprzętu IT zostaną potwierdzone Protokołem odbioru usunięcia wady podpisanym przez upoważnionych przedstawicieli Stron, sporządzonym według wzoru stanowiącego Załącznik nr 4 do Umowy.
7. Dla Sprzętu IT przez naprawę należy rozumieć przywrócenie takiego stanu, w którym Sprzęt IT pracuje poprawnie i spełnia wszystkie funkcjonalności określone w Załączniku nr 1 do Umowy.
8. Wszelkie koszty związane ze świadczeniem Gwarancji obciążają Sprzedawcę.
9. Niezależnie od uprawnień z tytułu Gwarancji Kupującemu przysługują wobec Sprzedawcy uprawnienia z tytułu rękojmi. Jeżeli w ramach rękojmi Kupujący zażąda wykonania przez Sprzedawcę obowiązków, określonych w niniejszym paragrafie, do terminów realizacji poszczególnych obowiązków z tytułu rękojmi mają odpowiednie zastosowanie terminy określone dla tych obowiązków w ust. 4 lub 5. Okres rękojmi za wady zostaje rozszerzony i wygasa z upływem okresu gwarancji.
10. Postanowienie ust. 1-9 stosuje się odpowiednio do realizacji uprawnień Kupującego z tytułu rękojmi i Gwarancji na Oprogramowanie, z uwzględnieniem specyfiki realizacji wskazanych uprawnień w przypadku Oprogramowania.
11. Kupujący zastrzega sobie prawo do zmiany Lokalizacji. Kupujący odinstaluje, przewiezie, dokona instalacji i uruchomi Sprzęt IT i Oprogramowanie w nowej Lokalizacji. Uruchomienie Sprzętu IT odbędzie się w asyście przedstawiciela Sprzedawcy, jeśli Sprzedawca poinformuje Kupującego o zamiarze uczestniczenia w uruchomieniu Sprzętu IT w nowej Lokalizacji. Nieobecność przedstawiciela Sprzedawcy podczas uruchomienia Sprzętu IT w nowej Lokalizacji nie wpływa na uruchomienie przez Kupującego Sprzętu IT oraz nie zwalnia Sprzedawcy z obowiązku świadczenia zobowiązań wynikających z Umowy zgodnie z jej postanowieniami. Zmiana Lokalizacji nie wymaga zmiany Umowy w formie pisemnego aneksu a jedynie poinformowania osób wskazanych przez Sprzedawcę w § 3 ust. 2 Umowy o takiej zmianie na 5 Dni Roboczych przed planowaną zmianą Lokalizacji. Od momentu przekazania informacji o uruchomieniu Sprzętu IT w nowej Lokalizacji, Sprzedawca świadczyć będzie zobowiązania wynikające z Umowy dla zmienionej Lokalizacji.
12. W ramach Gwarancji Kupujący będzie miał prawo dostępu do serwisu producenta Sprzętu IT i Oprogramowania, w tym do:
    1) aktualizacji wersji Oprogramowania (*updates, upgrade, patches*) oraz nowych wersji Oprogramowania i udoskonaleń do wersji bieżących Oprogramowania (nowych edycji Oprogramowania, wydań uzupełniających, poprawek programistycznych); Kupujący, w ramach wynagrodzenia, uzyskuje prawo do zainstalowania, uruchamiania, przechowywania i czasowego (w okresie Gwarancji) korzystania z aktualizacji,

2) monitorowania statusu zgłoszeń serwisowych;
3) samodzielnego oraz za pośrednictwem Sprzedawcy zgłaszania awarii do producenta;
4) samodzielnego oraz za pośrednictwem Sprzedawcy dostępu do bazy Oprogramowania, bazy wiedzy, dokumentacji i forum dyskusyjnego producenta Sprzętu IT, o ile takie istnieją;

§ 7. Wynagrodzenie

1. Łączne wynagrodzenie z tytułu wykonania Umowy wynosi netto ..... zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100), z czego:
   1) Wynagrodzenie za wykonanie Etapu I - w wysokości wynosi netto ..... zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100), w tym wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentami oraz Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz wynagrodzenie za przeniesienie autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu I wraz z prawem do wykonywania praw zależnych, na polach eksploatacji, o których mowa w § 9 ust. 3 Umowy, zgodnie z cenami jednostkowymi wskazanymi w Załączniku nr 7 do Umowy,
   2) Wynagrodzenie za wykonanie Etapu II - w wysokości wynosi netto ..... zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100), w tym wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentami oraz Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz wynagrodzenie za przeniesienie autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu II wraz z prawem do wykonywania praw zależnych, na polach eksploatacji, o których mowa w § 9 ust. 3 Umowy, zgodnie z cenami jednostkowymi wskazanymi w Załączniku nr 7 do Umowy,
   3) Wynagrodzenie za wykonanie Etapu III - w wysokości wynosi netto ..... zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100), w tym wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentami oraz Wdrożenie a także wynagrodzenie za przeniesienie autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu III wraz z prawem do wykonywania praw zależnych, na polach eksploatacji, o których mowa w § 9 ust. 3 w wysokości netto ..... zł (słownie złotych: ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100) oraz wynagrodzenie za Wdrożenie Sieci Bezprzewodowej WIFI w wysokości netto ..... zł (słownie złotych: ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100),
   4) Wynagrodzenie za wykonanie Etapu IV - w wysokości wynosi netto ..... zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100), w tym wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentami oraz Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz wynagrodzenie za przeniesienie autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu IV wraz z prawem do wykonywania praw zależnych, na polach eksploatacji, o których mowa w § 9 ust. 3 Umowy, zgodnie z cenami jednostkowymi wskazanymi w Załączniku nr 7 do Umowy,
   5) Wynagrodzenie za wykonanie Etapu V - w wysokości wynosi netto ..... zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100), w tym wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentami oraz Wdrożenie (z wyłączeniem Wdrożenia Sieci Bezprzewodowej WIFI) oraz wynagrodzenie za przeniesienie autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu V wraz z prawem do wykonywania praw zależnych, na polach eksploatacji, o których mowa w § 9 ust. 3 Umowy, zgodnie z cenami jednostkowymi wskazanymi w Załączniku nr 7 do Umowy,
   6) Wynagrodzenie z tytułu korzystania z Gwarancji wynosi netto .....zł (słownie złotych: .....00/100) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto .....zł (słownie złotych: ..... 00/100),
   7) maksymalne wynagrodzenie z tytułu konsultacji, wynosi netto _____,XX zł (słownie złotych: ..... XX/100) powiększone o należny podatek od towarów i usług, co daje kwotę brutto .....,XX zł (słownie złotych: ..... XX/100),
2. Zapłata wynagrodzenia, o którym mowa w ust. 1 pkt. 1-5, nastąpi w terminie do 28 dni licząc od dnia otrzymania przez Kupującego prawidłowo wystawionych faktur VAT odpowiednio dla każdego z Etapów przy czym podstawę do wystawienia faktur stanowić będzie podpisany bez zastrzeżeń przez upoważnionych przedstawicieli Stron Protokół odbioru Etapu odpowiednio dla każdego z Etapów, o którym mowa w § 4 ust. 2 Umowy. Zapłata wynagrodzenia, o którym mowa w ust. 1 pkt 6 nastąpi w terminie 28 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionych faktur VAT, w dwóch równych częściach, przy czym Sprzedawca uprawniony jest wystawić fakturę obejmującą pierwszą cześć wynagrodzenia w dniu podpisania bez zastrzeżeń Protokołu odbioru Wdrożenia, o którym mowa w § 4 ust. 15 Umowy zaś fakturę obejmującą drugą cześć wynagrodzenia po upływie roku od wystawienia pierwszej faktury, jednak nie później niż 30.11.2023 r. Wynagrodzenie, o którym mowa w ust. 1 pkt 7 płatne będzie każdorazowo w terminie do 28 dni licząc od daty otrzymania przez Kupującego prawidłowo wystawionej faktury oraz podpisanego bez zastrzeżeń przez upoważnionych przedstawicieli Stron Protokołu odbioru konsultacji, o którym mowa w § 2 ust. 5 Umowy. Wynagrodzenie o którym mowa w zdaniu poprzednim (za konsultacje), rozliczane jest kwartalnie i wyliczane jako iloczyn ilości godzin konsultacji odebranych w danym kwartale i ceny za jedną godzinę

konsultacji określoną zgodnie z ofertą Sprzedawcy na kwotę netto .....,XX zł (słownie złotych: .... XX/100) powiększoną o należny podatek VAT, co daje kwotę brutto .....,XX zł (słownie złotych: ..... XX/100). W przypadku niewykorzystania minimalnej ilości godzin konsultacji, o której mowa w § 2 ust. 3 Umowy, rozliczenie minimalnego zakresu zostanie uwzględnione w Protokole odbioru konsultacji za ostatni kwartał realizacji Umowy.

3. Wynagrodzenie, o którym mowa w ust. 1, wyczerpuje wszelkie roszczenia finansowe Sprzedawcy z tytułu wykonania Umowy.
4. Za termin wykonania płatności uznaje się dzień obciążenia rachunku bankowego Kupującego.
5. Błędnie wystawiona faktura VAT lub brak podpisanego przez umocowanych przedstawicieli Stron Protokołu Odbioru Etapu, o którym mowa w § 4 ust. 9, Protokołu odbioru Wdrożenia, o którym mowa w § 4 ust. 15 Umowy lub Protokołu odbioru konsultacji, o którym mowa w § 2 ust. 5 Umowy spowodują naliczenie ponownego, 28-dniowego terminu płatności od dostarczenia prawidłowo wystawionej faktury VAT lub podpisanego Protokołu odbioru Dokumentacji powykonawczej lub Protokołu odbioru konsultacji.
6. Jeżeli w trakcie realizacji Umowy nastąpi:
   1) zmiana stawki podatku od towarów i usług oraz podatku akcyzowego,
   2) zmiana wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę,
   3) zmiana zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub ubezpieczenie zdrowotne,
   4) zmiana zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych,

   a zmiany te będą miały wpływ na koszty wykonania Umowy – zastosowanie mają zasady wprowadzania zmian wysokości wynagrodzenia należnego Sprzedawcy określone w ust. 8-14 poniżej.
7. Zmiana wysokości wynagrodzenia wymaga zmiany Umowy w drodze aneksu.
8. Sprzedawca najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany o których mowa w ust. 6 uprawniony jest do wystąpienia do Kupującego z pisemnym wnioskiem o dokonanie zmiany Umowy w zakresie wysokości wynagrodzenia wraz z jej uzasadnieniem oraz dokumentami niezbędnymi do oceny przez Kupującego, czy zmiany, o których mowa w ust. 6, mają wpływ na koszty wykonania Umowy przez Sprzedawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia Sprzedawcy o którym mowa w niniejszej Umowie, a w szczególności:
   1) szczegółową kalkulację proponowanej zmienionej wysokości wynagrodzenia Sprzedawcy oraz wykazanie adekwatności propozycji do zmiany wysokości kosztów wykonania Umowy przez Sprzedawcę.
   2) przyjęte przez Sprzedawcę zasady kalkulacji wysokości kosztów wykonania Umowy oraz założenia co do wysokości dotychczasowych oraz przyszłych kosztów wykonania Umowy, wraz z dokumentami potwierdzającymi prawidłowość przyjętych założeń - takimi jak np. umowy o pracę, dokumenty potwierdzające zgłoszenie pracowników do ubezpieczeń.
9. W terminie 30 dni od otrzymania wniosku, o którym mowa w ust. 8, Kupujący może zwrócić się do Sprzedawcy o jego uzupełnienie lub przekazanie dodatkowych wyjaśnień lub dokumentów (np. zażądać: oryginałów do wglądu, przekazania kopii dokumentów potwierdzonych za zgodność z oryginałami).
10. Kupujący w terminie 30 dni od dnia otrzymania kompletnego wniosku zajmie w stosunku do niego pisemne stanowisko. Za dzień przekazania stanowiska uznaje się dzień jego wysłania na adres właściwy dla doręczeń pism dla Sprzedawcy.
11. Kupujący najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany, o których mowa w ust. 6 może przekazać Sprzedawcy pisemny wniosek o dokonanie zmiany Umowy. Wniosek powinien zawierać co najmniej propozycję zmiany Umowy w zakresie wysokości wynagrodzenia oraz powołanie zmian przepisów.
12. Przed przekazaniem wniosku, o którym mowa w ust. 11, Kupujący może zwrócić się do Sprzedawcy o złożenie wyjaśnień lub dokumentów (oryginałów do wglądu lub kopii potwierdzonych za zgodność z oryginałem) niezbędnych do oceny przez Kupującego, czy zmiany, o których mowa w ust. 6 mają wpływ na koszty wykonania Umowy przez Sprzedawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia. Rodzaj i zakres tych informacji określi Kupujący. Postanowienia ust. 9-10stosuje się odpowiednio, z tym, że Sprzedawca jest zobowiązany w każdym przypadku do zajęcia pisemnego stanowiska w terminie 30 dni od dnia otrzymania wniosku od Kupującego.
13. W przypadku niewykonania lub nienależytego wykonania przez Sprzedawcę zobowiązania o którym mowa w ust. 12 w terminie określonym w ust. 12, Sprzedawca zapłaci na rzecz Kupującego karę umowną w wysokości 0,01 % wynagrodzenia brutto o którym mowa w ust. 1 za każdy rozpoczęty dzień kalendarzowy zwłoki. Jeżeli w terminie określonym w ust. 12 Sprzedawca nie przedłoży wyjaśnień lub dokumentów, o których mowa w ust. 12 lub przedłożone przez Sprzedawcę wyjaśnienia lub dokumenty będą niewystarczające do dokonania przez Kupującego oceny, o której mowa w ust. 12 – Kupujący wyznaczy Sprzedawcy dodatkowy termin, nie dłuższy niż 10 dni, na dostarczenie lub uzupełnienie wyjaśnień lub dokumentów. W przypadku bezskutecznego upływu terminu wyznaczonego zgodnie ze zdaniem drugim, Kupujący uprawniony będzie do wypowiedzenia Umowy z zachowaniem miesięcznego terminu wypowiedzenia.
14. Jeżeli w trakcie procedury opisanej w ust. 8-13 zostanie wykazane, że zmiany, o których mowa w ust. 6 uzasadniają zmianę wysokości wynagrodzenia, Strony uzgodnią treść aneksu do Umowy oraz podpiszą aneks, z zachowaniem zasady zmiany

wysokości wynagrodzenia w kwocie odpowiadającej zmianie kosztów wykonania Umowy wywołanych przyczynami określonymi w ust. 6.

15. W przypadku niezgodności, w dniu realizacji płatności, numeru rachunku bankowego wskazanego przez Sprzedawcę na fakturze z numerem rachunku bankowego zamieszczonym w wykazie podmiotów, o których mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, Strony ustalają, że realizacja płatności nastąpi w trybie art. 108a ww. ustawy.
16. Zasady zmiany wynagrodzenia określone w ust. 7 – 14 powyżej mają odpowiednie zastosowanie do zmiany wysokości wynagrodzenia w przypadku zmiany średniorocznego wskaźnika cen towarów i usług konsumpcyjnych ogółem ogłaszanego w komunikacie Prezesa Głównego Urzędu Statystycznego na podstawie przepisów ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (dalej „wskaźnik"), z zastrzeżeniem następujących zasad:
    1) zmiana wynagrodzenia jest możliwa, gdy wskaźnik w stosunku do roku poprzedniego będzie wyższy niż 101,5 albo będzie niższy niż 98,5 (tj. wzrost poziomu cen o 1,5% albo spadek poziomu cen o 1,5%);
    2) zmiana wynagrodzenia obowiązuje w stosunku do wynagrodzenia, które stanie się należne dopiero po dniu podpisania aneksu do Umowy (w formie pisemnej pod rygorem nieważności), tym samym zmiana nie dotyczy wynagrodzenia ustalonego (wystawienie faktury) lub rozliczonego przed dokonaniem zmiany Umowy;
    3) zmiana wynagrodzenia możliwa jest najwcześniej po upływie 12 miesięcy od zawarcia Umowy (tzn., jeżeli Umowa została zawarta w październiku 2022 roku, to pierwsza zmiana będzie możliwa po publikacji wskaźnika w 2024 roku), chyba że data zawarcia Umowy przypada 180 dni od daty złożenia oferty przez Sprzedawcę, wówczas:
        a) zmiana wynagrodzenia możliwa jest po upływie 12 miesięcy od dnia otwarcia oferty Sprzedawcy,
        b) wartość zmiany wskaźnika zostanie ustalona nie względem roku poprzedniego, a względem roku, w którym doszło do otwarcia oferty Sprzedawcy;
    4) z zastrzeżeniem limitu ustalonego w pkt 5, w przypadku zmiany wskaźnika, każdorazowa wartość zmiany wynagrodzenia jednostkowego z tytułu jednej godziny świadczenia konsultacji, o którym mowa w ust. 2 będzie ustalana w następujący sposób:
        a) jeśli zmiana wskaźnika będzie na poziomie powyżej 101,5 do 103 (wzrost poziomu cen od 1,5% do 3%) - wynagrodzenie z tytułu jednej godziny świadczenia konsultacji określone w ust. 2 wzrośnie o 1% względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 98,5 do 97 (spadek poziomu cen od 1,5% do 3%) - wynagrodzenie z tytułu jednej godziny świadczenia konsultacji określone w ust. 2 zmaleje o 1% względem wynagrodzenia, które w chwili zmiany wynika z Umowy,
        b) jeśli zmiana wskaźnika będzie na poziomie powyżej 103 do 105 (wzrost poziomu cen od 3 % do 5 %) - wynagrodzenie z tytułu jednej godziny świadczenia konsultacji określone w ust. 2 wzrośnie o 2 % względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 97 do 95 (spadek poziomu cen od 3% do 5%) - wynagrodzenie z tytułu jednej godziny świadczenia konsultacji określone w ust. 2 zmaleje o 2% względem wynagrodzenia, które w chwili zmiany wynika z Umowy,
        c) jeśli zmiana wskaźnika będzie na poziomie powyżej 105 (wzrost poziomu cen ponad 5%) - wynagrodzenie z tytułu jednej godziny świadczenia konsultacji określone w ust. 2 zmieni się o 3,5% względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 5 (spadek poziomu cen o ponad 5%) - wynagrodzenie z tytułu jednej godziny świadczenia konsultacji określone w ust. 2 zmaleje o 3,5% względem wynagrodzenia, które w chwili zmiany wynika z Umowy;
    5) zmiany wskaźnika skutkować mogą w całym okresie obowiązywania Umowy zmianą ceny z tytułu jednej godziny świadczenia konsultacji, określonej w ust. 2 łącznie nie więcej niż o 10 % w stosunku do wartości wskazanej w ofercie;
    6) zmiany wynagrodzenia zgodnie z zasadami określonymi w niniejszym ustępie są możliwe do wysokości nieprzekraczającej łącznie 5% maksymalnego łącznego wynagrodzenie o którym mowa w ust. 1;
    7) uprawnienie do wnioskowania o waloryzację wynagrodzenia zastrzeżone jest dla obu Stron umowy.
17. Sprzedawca, którego wynagrodzenie zostało zmienione w związku ze zmianą wskaźnika, o którym mowa w ust. 16, zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom cen materiałów lub kosztów dotyczących zobowiązania podwykonawcy.

§ 8. Kary umowne i roszczenia odszkodowawcze

1. W przypadku zwłoki Sprzedawcy w dostarczeniu Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz w realizacji Wdrożenia w terminie wskazanym w § 4 ust. 1 pkt 1 Umowy Kupującemu przysługuje kara umowna w wysokości 10.000,00 zł (słownie złotych: dziesięć tysięcy złotych 00/100) za każdy rozpoczęty dzień zwłoki.
2. Jeśli zwłoka, o której mowa w ust. 1 trwała będzie dłużej niż 14 dni, Kupujący może, bez wyznaczenia dodatkowego terminu, odstąpić od Umowy (w terminie 14 dni od wystąpienia przesłanki uprawniającej do odstąpienia) oraz zażądać kary umownej w wysokości 10 % kwoty łącznego wynagrodzenia brutto o którym mowa w § 7 ust. 1 Umowy.
3. W przypadku zwłoki Sprzedawcy w naprawie lub wymianie Sprzętu IT lub Oprogramowania na fabrycznie nowe, wolne od wad w okresie Gwarancji lub rękojmi, w stosunku do terminów, o którym mowa w § 6 ust. 4, 5 lub 9 Umowy, Kupującemu przysługuje kara umowna w wysokości 2 000,00 zł (słownie: dwa tysiące 00/100) za każdy rozpoczęty Dzień Roboczy zwłoki.

4. Jeżeli zwłoka, o której mowa w ust. 3 trwała będzie dłużej niż 2 Dni Robocze, Kupujący, w terminie 14 dni od upływu terminu powyższej zwłoki, ma prawo, według własnego wyboru:
   1) odstąpić od Umowy bez konieczności wyznaczania dodatkowego terminu na usunięcie wad oraz żądać kary umownej w wysokości 10 % kwoty sumy łącznego wynagrodzenia brutto o którym mowa w § 7 ust. 1 pkt 1 - 6 Umowy,
   2) dokonać zastępczej wymiany Sprzętu IT wraz z Oprogramowaniem na koszt Sprzedawcy,
   3) naliczyć 2-krotność kary umownej określonej w ust. 3, począwszy odpowiednio od 3 Dnia Roboczego zwłoki, do terminu, w którym zostanie naprawiony lub wymieniony Sprzęt IT, z zachowaniem prawa do kary umownej określonej w ust.3.
5. W przypadku zwłoki Sprzedawcy w dostarczeniu Sprzętu IT wraz z Oprogramowaniem lub Dokumentów wolnych od wad lub ponownego wykonania Wdrożenia, w stosunku do terminu, o którym mowa w § 4 ust. 11 Sprzedawca zapłaci karę umowną w wysokości 10.000,00 zł (słownie złotych: dziesięć tysięcy złotych 00/100) za każdy rozpoczęty Dzień Roboczy zwłoki.
6. W przypadku zwłoki Sprzedawcy w odbiorze Sprzętu IT wraz z Oprogramowaniem i Dokumentów z miejsca dostarczenia, w stosunku do terminu, o którym mowa w § 4 ust. 11, Sprzedawca zapłaci karę umowną w wysokości 10.000,00 zł (słownie złotych: dziesięć tysięcy złotych 00/100) za każdy rozpoczęty Dzień Roboczy zwłoki. W przypadku ponownej odmowy odbioru Sprzętu IT, o której mowa w § 4 ust. 11Umowy, Kupujący ma prawo odstąpić od Umowy w terminie 30 dni od daty przekazania Sprzedawcy protokołu odmowy odbioru Sprzętu IT i żądać kary umownej w wysokości 10% kwoty łącznego wynagrodzenia brutto o którym mowa w § 7 ust. 1 Umowy, z zachowaniem prawa do kary umownej określonej w zdaniu poprzednim, naliczonej do dnia odstąpienia.
7. W przypadku zwłoki Sprzedawcy w dostarczeniu Kupującemu Projektu Technicznego lub Dokumentacji powykonawczej w stosunku do terminów, o którym mowa odpowiednio w § 4 ust. 4 i 12 Sprzedawca zapłaci karę umowną w wysokości 1.000,00 zł (słownie złotych: jeden tysiąc złotych 00/100) za każdy rozpoczęty Dzień Roboczy zwłoki.
8. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy powstanie szkoda przewyższająca zastrzeżoną karę umowną, bądź szkoda powstanie z innych przyczyn niż te, dla których zastrzeżono karę, Kupującemu przysługuje prawo do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.
9. W przypadku braku zapłaty lub nieterminowej zapłaty wynagrodzenia należnego podwykonawcom z tytułu zmiany wysokości wynagrodzenia, odpowiadającego zmianie wskaźnika, o którym mowa w § 7 ust. 17, Zamawiającemu przysługiwać będzie od Sprzedawcy kara umowna w wysokości 1 000,00 zł za każdy stwierdzony przypadek.
10. Kary umowne płatne są w terminie 14 dni od daty otrzymania wezwania. Niezależnie od powyższego kary umowne mogą być potrącane z wynagrodzenia należnego Sprzedawcy lub z zabezpieczenia należytego wykonania Umowy.
11. Łączna wysokość kar umownych z wszystkich tytułów wynikających z Umowy, zastrzeżonych na rzecz Kupującego jest ograniczona do 100 % łącznej sumy wartości wynagrodzenia brutto, określonej w § 7 ust. 1 pkt. 1-6 Umowy,

§ 9. Prawa autorskie

1. Sprzedawca zapewnia, że korzystanie przez Kupującego z Dokumentacji nie będzie naruszało praw osób trzecich. Na podstawie Umowy Sprzedawca przeniesie na Kupującego autorskie prawa majątkowe w zakresie i w sposób opisany poniżej.
2. Z dniem podpisania Protokołu odbioru Projektu Technicznego, Dokumentacji powykonawczej, Planu Testów Akceptacyjnych dla poszczególnych Etapów o którym mowa w § 4 ust. 4, 12 i 13 Umowy, Sprzedawca przenosi na Kupującego autorskie prawa majątkowe do Dokumentacji, na polach eksploatacji wskazanych w ust. 3, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 Umowy.
3. Przeniesienie autorskich praw majątkowych do utworów, o których mowa w niniejszym paragrafie, obejmuje następujące pola eksploatacji:
   1) w zakresie utrwalania i zwielokrotniania utworu – wytwarzanie każdą techniką egzemplarzy utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
   2) w zakresie obrotu oryginałem oraz egzemplarzami, na których utwory utrwalono – wprowadzanie do obrotu, użyczanie oraz najem oryginału oraz egzemplarzy;
   3) w zakresie rozpowszechniania utworów w sposób inny niż określony w pkt. 2 – publiczne wykonanie, wystawienie, wyświetlanie, odtwarzanie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym;
   4) dowolne przetwarzanie utworów, w tym łączenie z innymi utworami;
   5) zezwalanie na wykonywanie zależnych praw autorskich poprzez rozporządzanie i korzystanie na wszystkich polach eksploatacji wymienionych w pkt. 1-4.
4. Z dniem dokonania przez Kupującego odbioru Dokumentacji Kupujący nabywa na własność nośniki, na których utwory te utrwalono, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 Umowy.

§ 10. Wady prawne

1. Sprzedawca gwarantuje, że Sprzęt IT, Oprogramowanie, Dokumenty oraz Dokumentacja nie naruszają praw własności intelektualnej ani innych praw osób trzecich.

2. W przypadku wystąpienia osób trzecich wobec Kupującego z roszczeniami opartymi na twierdzeniu, iż używany przez Kupującego Sprzęt IT, Oprogramowanie, Dokumenty, Dokumentacja naruszają jakiekolwiek prawa, o których mowa w ust. 1, Kupującemu przysługują wszystkie niżej wymienione uprawnienia, które ma prawo zrealizować według swojego wyboru (łącznie lub osobno):
   1) prawo odstąpienia od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach z wyłączeniem zapłaty na rzecz Sprzedawcy jakichkolwiek kosztów, odszkodowań itp.,
   2) prawo żądania zapłaty przez Sprzedawcę kary umownej w wysokości 5 % łącznego wynagrodzenia brutto o którym mowa w § 7 ust. 1 Umowy oraz prawo żądania odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.
3. W przypadku wytoczenia przeciwko Kupującemu powództwa opartego na twierdzeniu opisanym w ust. 2, Sprzedawca zobowiązuje się zapewnić Kupującemu na swój koszt ochronę sądową oraz ponieść konsekwencje zapadłego wyroku sądowego.

§ 11. Zabezpieczenie należytego wykonania Umowy (dalej: „**ZNWU**")

1. Sprzedawca złożył u Kupującego ZNWU w jednej z form, o których mowa w art. 450 Ustawy w wysokości .....,XX zł (słownie złotych: ..... XX/100.
2. ZNWU dotyczy pokrycia ewentualnych roszczeń wynikających z niewykonania lub nienależytego wykonania Umowy.
3. ZNWU zostanie zwolnione (zwrócone):
   1) w wysokości 70% zabezpieczenia w terminie 30 dni od dnia podpisania bez zastrzeżeń Protokołu odbioru, o którym mowa w § 4 ust. 15 Umowy,
   2) w wysokości 30 % zabezpieczenia w terminie 15 dni po upływie okresu Gwarancji lub rękojmi za wady.
4. W przypadku zmiany formy ZNWU w trakcie trwania Umowy obowiązywać będą poniższe zasady.
5. ZNWU w formie pieniężnej Sprzedawca wpłaca przelewem na rachunek bankowy wskazany przez Kupującego.
6. ZNWU wnoszone w formie gwarancji bankowej lub ubezpieczeniowej może być wystawione przez bank albo ubezpieczyciela. Bank lub ubezpieczyciel zapłaci, na rzecz Kupującego w terminie 30 dni od pisemnego żądania kwotę .....,XX zł (słownie złotych: ..... XX/100), na pierwsze wezwanie Kupującego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Sprzedawcy i bez dochodzenia czy wezwanie Kupującego jest uzasadnione czy nie.
7. ZNWU wnoszone w formie poręczenia ma być wystawione przez bank, spółdzielczą kasę oszczędnościowo-kredytową lub podmiot, o którym mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, który poręczy należyte wykonanie Umowy do wysokości .....,XX zł (słownie złotych: ..... XX/100).
8. W przypadku, gdy ZNWU, o którym mowa w ust.1 będzie wnoszone w formie: poręczenia, bankowej lub ubezpieczeniowej gwarancji, Kupujący zastrzega sobie prawo do akceptacji projektu tych dokumentów.
9. ZNWU wniesione w formie pieniężnej podlega zwrotowi wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek Sprzedawcy.
10. ZNWU w formie innej niż pieniężna Sprzedawca złoży u Kupującego w Kancelarii Głównej, Warszawa ul. Poleczki 33, 02-822 Warszawa, z dopiskiem *„Dla Departamentu Informatyki"* lub w formie dokutemu elektronicznego na adres poczty e-mail: zamowieniapubliczne@arimr.gov.pl.

§ 12. Odstąpienie od Umowy

1. Strony mogą odstąpić od Umowy w przypadkach przewidzianych obowiązującymi przepisami, a także w przypadku zaistnienia okoliczności, o których mowa w Umowie.
2. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Kupujący może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim wypadku Sprzedawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy.
3. Przy wykonaniu Umowy Sprzedawca bez zgody Kupującego nie ma prawa do korzystania w jakimkolwiek charakterze z osób zatrudnionych u Kupującego, pod rygorem odstąpienia od Umowy przez Kupującego z winy Sprzedawcy w terminie 30 dni od powzięcia wiadomości o zaistnieniu takiego faktu oraz żądania zapłaty kary umownej, o której mowa w ust. 4.
4. W wyniku wystąpienia okoliczności, o której mowa w ust. 3 Sprzedawca jest zobowiązany do zapłaty w terminie 14 dni od wezwania przez Kupującego kary umownej w wysokości 20.000,00 zł (słownie złotych: dwadzieścia tysięcy złotych 00/100). Jeżeli szkoda poniesiona przez Kupującego jest wyższa od zastrzeżonej wyżej kary umownej, Kupujący może dochodzić odszkodowania uzupełniającego od Sprzedawcy na zasadach ogólnych Kodeksu cywilnego.

§ 13. Zawiadomienia

1. Wszelkie zawiadomienia wymienione w Umowie, niezależnie od nazwy, pod którą występują, dla swojej skuteczności Strony muszą przekazać osobiście za potwierdzeniem odbioru lub pocztą poleconą za zwrotnym poświadczeniem ich odbioru i będą uważane za skutecznie doręczone w dniu ich odbioru, chyba, że postanowienia niniejszej umowy stanowią inaczej.
2. Zawiadomienia, zapytania, informacje nie wymienione w postanowieniach Umowy mogą być doręczane osobiście, przesyłane kurierem lub listem, pod warunkiem ich potwierdzenia przez drugą Stronę.

3. Zawiadomienia będą wysyłane na adresy Stron wskazane w komparycji Umowy. Każda ze Stron zobowiązana jest do informowania drugiej Strony o każdej zmianie adresu. Jeżeli Strona nie powiadomiła o zmianie adresu, zawiadomienia wysłane na ostatni znany adres Strony uznają za doręczone. Powiadomienie o powyższych zmianach nie stanowi zmiany Umowy wymagającej sporządzenia aneksu.

§ 14. Poufność, bezpieczeństwo informacji i zasady przetwarzania danych osobowych

1. Wszelkie informacje, w tym dokumentacja, w których posiadanie weszła druga Strona przy zawieraniu i wykonywaniu Umowy mają charakter poufny. Każda ze Stron zobowiązuje się nie ujawniać ich osobom trzecim, także po zakończeniu Umowy, wyjąwszy przypadki przewidziane prawem.
2. Sprzedawca zobowiązuje się do zapoznania się i przestrzegania przyjętych u Kupującego zasad bezpieczeństwa informacji, których treść została określona w Załączniku nr 5 (Regulamin użytkownika), 6 (Regulamin bezpieczeństwa fizycznego i środowiskowego) i nr 12 (Regulamin eksploatacji systemów teleinformatycznych) do Zarządzenia nr 78/2019 w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR, które stanowią Załącznik nr 5 do Umowy.
3. Sprzedawca zobowiązuje się do przestrzegania przy wykonywaniu Umowy przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1; sprost.: Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz sprost.: Dz. Urz. UE L 74 z 04.03.2021, str. 35), oraz przepisów krajowych wydanych w związku z ogólnym rozporządzeniem o ochronie danych, zwanym dalej: „RODO".
4. Sprzedawca pisemnie zobowiąże pracowników realizujących zobowiązania określone w Umowie do przestrzegania przepisów, o których mowa w ust. 2 i 3.
5. Sprzedawca oświadcza, że zapoznał się z klauzulą informacyjną w zakresie przetwarzania danych osobowych, stanowiącą Załącznik nr 6a, 6b i 6c do Umowy, o ile znajduje zastosowanie.
6. Kupujący informuje, że staje się administratorem danych osobowych osoby lub osób fizycznych, pozyskanych od Sprzedawcy, które to dane osobowe Kupujący bezpośrednio lub pośrednio pozyskał w celu wykonania Umowy. Sprzedawca oświadcza, że dane osobowe, o których mowa w zdaniu pierwszym przetwarza zgodnie z obowiązującymi w tym zakresie regulacjami prawnymi i jest uprawniony do ich przekazania Kupującemu oraz uczynił zadość wszelkim obowiązkom związanym z ich przekazaniem, a w szczególności poinformował osobę lub osoby fizyczne, których dane przekazuje, o fakcie i celu ich przekazania, jak również przekazał tym osobom w imieniu Kupującego informację o treści zamieszczonej w Załączniku nr 6d do Umowy.

§ 15. Zmiany Umowy

1. Kupujący dopuszcza zmiany Umowy, w szczególności stosownie do art. 455 ust. 1 pkt 1 Ustawy, Kupujący przewiduje możliwość wprowadzenia do Umowy zmian opisanych poniżej:
    1) niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest korzystna dla Kupującego lub konieczna w celu prawidłowego wykonania umowy i nie spowoduje podwyższenia ceny umowy;
    2) w przypadku wprowadzenia nowej wersji Oprogramowania lub innych nowych elementów Sprzętu IT lub Oprogramowania przez producenta, która to wersja lub elementy nie były dostępne na rynku w chwili upływu terminu składania ofert, z zastrzeżeniem, że wskutek zmiany wszystkie wymagania określone w dokumentach zamówienia oraz w ofercie Sprzedającego zostaną zachowane, a wynagrodzenie Sprzedającego nie ulegnie podwyższeniu;
    3) powstała możliwość zastosowania nowszych lub korzystniejszych dla Zamawiającego rozwiązań w zakresie modelu/typu Sprzętu IT lub Oprogramowania w przypadku zakończenia produkcji lub braku dostępności na rynku pod warunkiem ze Sprzęt IT/Oprogramowanie będzie posiadał parametry nie gorsze od oferowanego modelu/typu oprogramowania i nie spowoduje podwyższenia wynagrodzenia Sprzedawcy,
    4) zachodzi konieczność zmiany terminu wskazanego w § 4 ust. 1 pkt 1 Umowy, w przypadku przedłużającej się procedury udzielania zamówienia publicznego na skutek korzystania przez wykonawców ze środków ochrony prawnej, w takim przypadku Kupujący zastrzega sobie możliwość wydłużenia terminu wskazanego w § 4 ust. 1 pkt 1 Umowy o czas trwania procedury odwoławczej.

§ 16.
Postanowienia końcowe

1. W sprawach nieuregulowanych Umową mają zastosowanie przepisy Kodeksu cywilnego, Ustawy oraz ustawy o prawie autorskim i prawach pokrewnych.
2. Wszelkie zmiany treści Umowy wymagają formy pisemnej pod rygorem nieważności, za wyjątkiem tych, dla których w Umowie zastrzeżono inną formę
3. Ewentualne spory mogące wyniknąć na tle wykonania Umowy rozstrzygać będzie sąd powszechny właściwy dla siedziby Kupującego.
4. Sprzedawca nie może bez zgody Kupującego przenieść praw wynikających z Umowy na osoby trzecie.
5. Załączniki wymienione w Umowie stanowią jej integralną część.

Poniżej przedstawiono spis załączników:

1) Załącznik nr 1 – Specyfikacja Sprzętu IT i Oprogramowania;
2) Załącznik nr 1 A – Etapy realizacji Umowy;
3) *Załącznik nr 1B – dodatkowe cechy rozwiązania (załącznik zostanie wprowadzony do treści Umowy, jeżeli Sprzedawca zaoferuje spełnienie wymagań ocenianych w ramach kryterium oceny ofert jako dodatkowe parametry techniczne);*
4) Załącznik nr 1 C – Zestawienie ilościowe;
5) Załącznik nr 1 D – Wymagania w zakresie Dokumentacji;
6) Załącznik nr 2 – Protokół odbioru Etapu I/II/III/IV/V (wzór);
7) Załącznik nr 2 A – Protokół Odbioru Wdrożenia (wzór);
8) Załącznik nr 3 – Protokół odbioru Projektu Technicznego/Dokumentacji powykonawczej/Planu Testów Akceptacyjnych (wzór);
9) Załącznik nr 4 – Protokół odbioru usunięcia wady (wzór);
10) Załącznik nr 4 A – Protokół odbioru konsultacji (wzór);
11) Załącznik nr 5 – Treść Załączników nr 5, 6 i 12 do Zarządzenia Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR (ze zmianami);
12) Załącznik nr 6a – Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku bezpośredniego pozyskiwania danych osobowych osób fizycznych będących drugą Stroną umowy oraz pełnomocników osób fizycznych będących drugą Stroną umowy;
13) Załącznik nr 6b – Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku pośredniego pozyskiwania danych osobowych pełnomocników, prokurenta oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego;
14) Załącznik nr 6c – Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku bezpośredniego pozyskiwania danych osobowych pełnomocnika, prokurenta oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego;
15) Załącznik nr 6d – Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku pośredniego pozyskiwania danych osobowych w szczególności podwykonawców, pracowników podwykonawców, osób wyznaczonych do kontaktów roboczych oraz odpowiedzialnych za koordynację i realizację umowy;
16) Załącznik nr 7 – Formularz ofertowy.

6. Umowę sporządzono w 4 jednobrzmiących egzemplarzach, w tym jeden dla Sprzedawcy i trzy dla Kupującego.
/Umowę sporządzono w formie elektronicznej i opatrzono kwalifikowanymi podpisami elektronicznymi przez upoważnionych przedstawicieli Stron/.

Sprzedawca	**Kupujący**
.....	.....
.....	.....

Załącznik nr 1 do Umowy nr _____/DI/2022/2610

Specyfikacja Sprzętu IT i Oprogramowania

Przedmiotowe zamówienie dotyczy dostawy Licencji na zasadach subskrypcji, przełączników sieciowych, serwera z Oprogramowaniem oraz punktów dostępowych WLAN, które mają realizować użytkownikom Centrali ARiMR funkcjonalność przewodowego i bezprzewodowego oraz bezpiecznego i niezawodnego dostępu w sieci kampusowej wraz z wdrożeniem urządzeń ze wskazanymi funkcjonalnościami. Przełączniki sieci kampusowej muszą posiadać wbudowane bezpieczeństwo i automatyzację czynności związanych z administracją i utrzymaniem sieci.

Do nowej sieci kampusowej będą podłączone wszystkie obecne urządzenia sieciowe w Centrali ARiMR oraz ośrodku w Lublinie, tj. przełączniki, komputery, drukarki oraz urządzenia mobilne, które będą działać zgodnie z przyjętą polityką bezpieczeństwa zdefiniowaną w ramach dostępu definiowanego programowo. Obecnie wykorzystywana są przełączniki firmy Cisco z wdrożoną architekturą uwierzytelnienia opartej o protokół 802.1X i bezpieczeństwem opartym na Cisco ISE ver. 2.7.

W związku z posiadaniem przez Kupującego wsparcia producenta dla Cisco ISE nowe rozwiązanie sieci kampusowej musi pobierać politykę dla klienta z Identity Services Engine (ISE) w oparciu o znaczniki SGT tam zdefiniowane i uwierzytelnienie w oparciu o protokół 802.1X.

Wdrożenie technologii kampusowej musi zapewniać programowalną sieć przewodową i bezprzewodową w obiektach ARiMR, zautomatyzowanym egzekwowaniu polityk oraz micro i macro segmentację sieci. Przedmiotowe działanie dotyczy dostarczenia wszystkich niezbędnych urządzeń, Licencji na zasadach subskrypcji, Oprogramowania oraz serwisu gwarancyjnego producenta oprogramowania. Sprzedawca w ramach realizacji Umowy zobowiązany jest również przeprowadzić warsztaty powdrożeniowe z wdrożonego rozwiązania.

Wdrożenie w technologii Software-Defined Access (SDA) musi zapewnić realizację przewodowego i bezprzewodowego, bezpiecznego dostępu do wszystkich obecnych usług w Centrali ARiMR, poprzez separację grup użytkowników i aplikacji dozwalając tylko na taki ruch sieciowy, który jest dozwolony w zdefiniowanej polityce bezpieczeństwa.

Jeżeli w niniejszym załączniku użyto do opisania przedmiotu zamówienia oznaczeń lub parametrów wskazujących konkretnego producenta, konkretny produkt lub wskazano znaki towarowe, patenty, normy, standardy, aprobaty techniczne lub pochodzenie urządzeń, Kupujący dopuszcza zastosowanie produktów równoważnych, przez które należy rozumieć produkty o parametrach nie gorszych od przedstawionych w niniejszym załączniku, kompatybilne (współpracujące) z posiadanym przez Zamawiającego systemem zarządzania, w tym samym zakresie, co produkty określone w niniejszym załączniku oraz posiadające równoważne funkcje i parametry co produkt opisany w niniejszym załączniku. W takim wypadku do oferty należy załączyć dokładny opis oferowanych produktów, z którego jasno wynikać będzie zachowanie warunków równoważności.

Sprzedawca ma obowiązek dostarczyć niezbędne urządzenia, Licencje oraz skonfigurować Oprogramowanie oraz wszystkie niezbędne komponenty realizujące funkcjonalność sieci kampusowej w technologii *Software-Defined Access* (SD-*Access*) dla dostępu przewodowego i bezprzewodowego w Centrali ARiMR. Kupujący wymaga wykupienia wsparcia technicznego producenta dla dostarczonego Sprzętu IT i wdrożonego oprogramowania na okres 24 miesięcy. Sprzedawca zobowiązany jest dostarczyć pakiety serwisowe dla Oprogramowania będącego przedmiotem niniejszego zamówienia oraz dokonać ich aktywacji. Aktywowane pakiety serwisowe muszą gwarantować:

- możliwość pobierania poprawek i aktualizacji posiadanego Oprogramowania oraz sygnatur w okresie obowiązywania umowy, dostęp do poprawek i aktualizacji musi posiadać Sprzedawca i Kupujący;
- producent musi zapewnić możliwość zgłaszania i obsługi ewentualnych problemów w języku polskim.
- oferowany system musi posiadać oficjalne wsparcie producenta, nie jest akceptowalne wsparcie typu „community support", oferowane przez społeczność jego użytkowników.
- Kupujący musi mieć możliwość zgłaszania problemów z Oprogramowaniem bezpośrednio do producenta oprogramowania. Pośrednictwo firmy, która wdrażała system nie może być wymagane do skorzystania z przywileju uzyskania wsparcia.

A. <u>Przełącznik szkieletowy typ A – 2 sztuki</u>

1. W ramach zamówienia Kupujący wymaga dostawy przełącznika typu standalone, który musi być wyposażony w min. 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz 4 porty uplink 40/100 Gigabit Ethernet QSFP,
2. Przełącznik musi posiadać porty SFP/SFP+/SFP28 umożliwiające zastosowanie następujących wkładek interfejsowych:
   - 2.1. Gigabit Ethernet 1000Base-T,
   - 2.2. Gigabit Ethernet 1000Base-SX,
   - 2.3. Gigabit Ethernet 1000Base-LX/LH,
   - 2.4. Gigabit Ethernet 1000Base-EX,

2.5. Gigabit Ethernet 1000Base-ZX,

2.6. Gigabit Ethernet 1000Base-BX-D/U,

2.7. 10Gigabit Ethernet 10GBase-SR,

2.8. 10Gigabit Ethernet 10GBase-LR,

2.9. 10Gigabit Ethernet 10GBase-ER,

2.10. 10Gigabit Ethernet 10GBase-ZR,

2.11. 10Gigabit Ethernet 10GBase-BX-D/U,

2.12. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),

2.13. 25Gigabit Ethernet 25GBASE-SR,

2.14. 25Gigabit Ethernet typu twinax (SFP28 – SFP28),

2.15. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),

2.16. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF);

3. Przełącznik musi posiadać porty QSFP umożliwiające zastosowanie następujących modułów interfejsowych:

3.1. Dla transmisji 40Gb/s:

3.1.1. 40G-SR4,

3.1.2. 40G-LR4,

3.1.3. 40G-ER4,

3.1.4. 40G-SR-BD,

3.1.5. 40G-CSR,

3.1.6. 40G-CSR4,

3.1.7. 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652),

3.1.8. adapter 40G QSFP->10G SFP+,

3.1.9. 40Gigabit Ethernet typu twinax (QSFP - QSFP);

3.2. Dla transmisji 100Gb/s:

3.2.1. 100GBASE-SR4,

3.2.2. 100GBASE-LR4,

3.2.3. 100Gigabit Ethernet typu twinax (QSFP - QSFP);

4. Wymagania w zakresie architektury:

4.1. Urządzenie musi być wyposażone w wymienne moduły wentylatorów,

4.2. Urządzenie musi posiadać możliwość użycia zasilacz redundantnego do pracy w trybie 1:1;

5. Wymagania w z zakresie wydajności:

5.1. Urządzenie musi posiadać min. 32MB bufor pamięci,

5.2. Urządzenie musi posiadać min. 6GB pamięci DRAM i 16GB pamięci flash,

5.3. Przepustowość przełącznika (switching capacity) musi wynosić min. 3.2 Tbps,

5.4. Prędkość przesyłania (forwarding rate) musi wynosić min.1 miliard pps (1Bpps),

5.5. Przełącznik musi obsługiwać:

5.5.1. 1000 aktywnych sieci VLAN,

5.5.2. 80 000 adresów MAC,

5.5.3. 212 000 tras IPv4,

5.5.4. 212 000 tras IPv6,

5.5.5. Ilość wpisów w listach kontroli dostępu Security ACL – 27 000,

5.5.6. ilość wpisów w listach kontroli dostępu QoS ACL – 16 000,

5.5.7. 1000 interfejsów SVI L3,

5.5.8. Jumbo frame 9198B,

5.5.9. 128 połączeń zagregowanych typu „port channel",

5.5.10.16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP;

6. Wymagania w zakresie oprogramowania/funkcjonalności.

6.1. Urządzenie musi umożliwiać obsługę protokołu NTP,

6.2. Urządzenie musi umożliwiać obsługę IGMPv1/2/3,

6.3. System operacyjny przełącznika musi umożliwiać wgrywanie poprawek bez konieczności restartowania platformy,

6.4. Urządzenie musi posiadać wsparcie dla protokołu RESTCONF,

6.5. Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

6.5.1. IEEE 802.1w Rapid Spanning Tree,

6.5.2. Per-VLAN Rapid Spanning Tree (PVRST+),

6.5.3. IEEE 802.1s Multi-Instance Spanning Tree,

6.5.4. Obsługa 1000 instancji protokołu STP;

6.6. Urządzenie musi zapewniać obsługę protokołu IEEE 802.1ab LLDP i LLDP-MED,

6.7. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)

6.8. Urządzenie musi umożliwiać realizację funkcji serwera DHCP,

6.9. Urządzenie musi umożliwiać obsługę 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

6.10. Urządzenie musi posiadać funkcjonalność autoryzacji prób logowania urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,

6.11. Urządzenie musi obsługiwać listę kontroli dostępu (ACL) następujących typów:

6.11.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

6.11.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

6.11.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

6.11.4. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

6.12. Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:

6.12.1. Musi umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

6.12.2. Musi umożliwiać implementację algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,

6.12.3. Musi umożliwiać obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

6.12.4. Urządzenie musi posiadać mechanizm klasyfikacji ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

6.12.5. Urządzenie musi posiadać możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

6.12.6. Urządzenie musi posiadać kontrolę sztormów dla ruchu broadcast/multicast/unicast,

6.12.7. Urządzenie musi posiadać możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

6.13. Przełącznik musi posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

6.14. Urządzenie musi umożliwiać realizację funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),

6.15. Urządzenie musi realizować routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:

6.15.1. Routing statyczny dla IPv4 i IPv6,

6.15.2. Routing dynamiczny dla IPv4: BGP, ISIS,

6.15.3. Routing dynamiczny dla IPv4: OSPF, EIGRP (rfc7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA),

6.15.4. Routing dynamiczny dla IPv6: OSPFv3,

6.15.5. Funkcjonalności Policy-based routing,

6.15.6. multicast routing (PIM-SM, PIM-SSM) ,

6.15.7. Obsługi protokołu redundancji bramy (VRRP) z obsługą 255 grup,

6.15.8. Obsługi 200 tuneli GRE (Generic Routing Encapsulation),

6.15.9. Obsługi 1000 wirtualnych instancji routingu (VRF),

6.16. Przełącznik musi obsługiwać protokół BFD (Bidirectional Forwarding Detection) umożliwiający szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

6.17. Przełącznik musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji,

6.18. Urządzenie musi obsługiwać protokół LISP zgodnie z RFC 6830,

6.19. Urządzenie musi umożliwiać enkapsulację ruchu przy pomocy VXLAN'ów,

6.20. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine / border,

6.21. Urządzenie musi zapewniać obsługę mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,

6.22. Urządzenie musi być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze muszą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,

6.23. Przełącznik musi umożliwiać klastrowanie, które wspiera funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami,

6.24. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu

pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

6.25. Przełącznik musi posiadać możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

6.26. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,

6.27. Przełącznik musi posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowania plików typu „pcap" do dalszej analizy przy pomocy oprogramowania zewnętrznego,

6.28. Przełącznik musi posiadać możliwość realizacji funkcji kontrolera dla radiowych punktów dostępowych WiFi z obsługą do 200 AP oraz 4000 klientów bezprzewodowych,

6.29. Przełącznik musi posiadać możliwość modyfikacji programowej takich parametrów urządzenia jak: ilości pozycji w tablicy MAC, ilość tras routingowych unicast i multicast, ilości tras w sieci MPLS VPN, ilości obsługiwanych sesji netflow,

7. Wymagania w zakresie zarządzania i konfiguracji::

7.1. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

7.2. Urządzenie musi posiadać możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Przedmiotowa funkcjonalność musi umożliwiać kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

7.3. Urządzenie musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

7.4. Urządzenie musi być wyposażone w port konsoli USB,

7.5. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

7.6. Urządzenie musi umożliwiać obsługę protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,

7.7. Przełącznik musi posidać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

7.8. Przełącznik musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

8. Wymagania w zakresie parametrów fizycznych:

8.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

8.2. Wysokość urządzenia nie może przekraczać 1 RU,

8.3. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi musi być mniejsza niż 50 cm,

9. Wymagania w zakresie wyposażenia urządzenia

9.1. Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,

9.2. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

B. <u>Przełącznik szkieletowy typ B - 2 sztuki</u>

1. W ramach zamówienie Kupujący wymaga dostawy przełącznik typu standalone, który musi być wyposażony w 16 wbudowanych portów 1/10 Gigabit Ethernet SFP/SFP+,

2. Przełącznik musi posiadać porty SFP/SFP+ umożliwiają zastosowanie następujących wkładek interfejsowych:

2.1. Gigabit Ethernet 1000Base-T,

2.2. Gigabit Ethernet 1000Base-SX,

2.3. Gigabit Ethernet 1000Base-LX/LH,

2.4. Gigabit Ethernet 1000Base-EX,

2.5. Gigabit Ethernet 1000Base-ZX,

2.6. Gigabit Ethernet 1000Base-BX-D/U,

2.7. 10Gigabit Ethernet 10GBase-SR,

2.8. 10Gigabit Ethernet 10GBase-LR,

2.9. 10Gigabit Ethernet 10GBase-LRM,

2.10. 10Gigabit Ethernet 10GBase-ER,

2.11. 10Gigabit Ethernet 10GBase-ZR,

2.12. 10Gigabit Ethernet 10GBase-BX-D/U,

2.13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),

3. Wymagania w z zakresie architektury:

3.1. Urządzenie musi być wyposażone w wymienne moduły wentylatorów,

3.2. Urządzenie musi posiadać możliwość użycia zasilacza redundantnego do pracy w trybie 1:1;

4. Wymagania w z zakresie wydajności:

4.1. Urządzenie musi posiadać min. 32MB bufor pamięci,

4.2. Urządzenie musi posiadać min. 16GB pamięci DRAM i 16GB pamięci flash,

4.3. Minimalna przepustowość przełącznika (switching capacity) musi wynosić 480 Gbps,

4.4. Minimalna prędkość przesyłania (forwarding rate) musi wynosić 360 Mpps,

4.5. Przełącznik musi obsługiwać min.

4.5.1. 1000 aktywnych sieci VLAN,

4.5.2. 64 000 adresów MAC,

4.5.3. 64 000 tras IPv4,

4.5.4. 32 000 tras IPv6,

4.5.5. Ilość wpisów w listach kontroli dostępu Security ACL – 18 000,

4.5.6. ilość wpisów w listach kontroli dostępu QoS ACL – 18 000,

4.5.7. 1000 interfejsów SVI L3,

4.5.8. Jumbo frame 9198B,

4.5.9. 64 połączenia zagregowane typu „port channel",

4.5.10.16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP;

5. Wymagania w z zakresie Oprogramowania/funkcjonalności:

5.1. Przełącznik musi umożliwiać obsługęprotokołu NTP,

5.2. Przełącznik musi obsługiwać IGMPv1/2/3,

5.3. System operacyjny przełącznika musi umożliwiać wgrywanie poprawek bez konieczności restartowania platformy,

5.4. System operacyjny przełącznika musi umożliwiać wsparcie dla funkcjonalność klasyfikowania ruchu w warstwach 4-7

i na jego podstawie budowanie polityk bezpieczeństwa czy jakości usług,

5.5. System operacyjny przełącznika musi umożliwiać rozpoznawanie i klasyfikacja około 1400 predefiniowanych znanych aplikacji sieciowych oraz około 150 aplikacji szyfrujących ruch,

5.6. System operacyjny przełącznika musi posiadać wsparcie dla protokołu RESTCONF,

5.7. Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

5.7.1. IEEE 802.1w Rapid Spanning Tree,

5.7.2. Per-VLAN Rapid Spanning Tree (PVRST+),

5.7.3. IEEE 802.1s Multi-Instance Spanning Tree,

5.7.4. Obsługa 256 instancji protokołu STP;

5.8. Przełącznik musi umożliwiać obsługę protokołu IEEE 802.1ab LLDP i LLDP-MED,

5.9. Przełącznik musi umożliwiać realizację funkcji 802.1Q tunneling (QinQ),

5.10. Przełącznik musi umożliwiać realizację funkcję serwera DHCP,

5.11. Przełącznik musi umożliwiać obsługę 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

5.12. Urządzenie musi posiadać funkcjonalność autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,

5.13. Urządzenie musi umożliwiać obsługę listy kontroli dostępu (ACL) następujących typów:

5.13.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

5.13.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

5.13.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

5.13.4. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

5.14. Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:

5.14.1. Musi umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

5.14.2. Musi umożliwiać implementacjęalgorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,

5.14.3. Musi umożliwiać obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

5.14.4. Musi posiadać mechanizm klasyfikacji ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

5.14.5. Musi umożliwiać ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

5.14.6. Musi posiadać funkcjonalność kontroli sztormów dla ruchu broadcast/multicast/unicast,

5.14.7. Musi umożliwiać zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

5.15. Przełącznik musi posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

5.16. Urządzenie musi umożliwiać realizacja funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),

5.17. Urządzenie musi realizować routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:

5.17.1. Routing statyczny dla IPv4 i IPv6,

5.17.2. Routing dynamiczny dla IPv4: OSPF, BGP, IS-IS,

5.17.3. Routing dynamiczny dla IPv6: OSPFv3,

5.17.4. Funkcjonalności Policy-based routing,

5.17.5. Multicast routing (PIM-SM, PIM-SSM) ,

5.17.6. Obsługi protokołu redundancji bramy (VRRP) z obsługą 255 grup,

5.17.7. Obsługi 256 wirtualnych instancji routingu (VRF),

5.17.8. Obsługi 100 tuneli GRE (Generic Routing Encapsulation),

5.18. Przełącznik musi umożliwiać obsługę protokołu BFD (Bidirectional Forwarding Detection), któryumożliwia szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

5.19. Przełącznik musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 2000 translacji,

5.20. Urządzenie musi umożliwiać enkapsulację ruchu przy pomocy VXLAN'ów,

5.21. Urządzenie musi obsługiwać protokołu LISP zgodnie z RFC 6830,

5.22. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine,

5.23. Urządzenie musi zapewniać obsługę mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,

5.24. Urządzenie musi być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze muszą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,

5.25. Przełącznik musi umożliwiać klastrowanie, które wspiera funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami,

5.26. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

5.27. Przełącznik musi umożliwiać zdalną obserwacjęruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

5.28. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,

5.29. Przełącznik musi posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

6. Wymagania w zakresie zarządzania i konfiguracji:

6.1. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

6.2. Urządzenie musi umożliwiać realizację dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność musi umożliwiać kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

6.3. Urządzenie musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi posiadać ć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

6.4. Urządzenie musi być wyposażone w port konsoli USB,

6.5. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

6.6. Urządzenie musi umożliwiać obsługę protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,

6.7. Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

6.8. Przełącznik musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

7. Wymagania w zakresie parametrów fizycznych:

7.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

7.2. Wysokość urządzenia nie może przekraczać 1 RU,

7.3. Głębokość chassis urządzenia z wentylatorami i zasilaczami musi być mniejsza niż 60 cm;

8. Wymagania w zakresie wyposażenia urządzenia:

8.1. Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,

8.2. Przełącznik musi być wyposażony w moduł: 8-portowy moduł 10Gigabit Ethernet SFP+

8.3. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

C. <u>Przełącznik dostępowy typ A (z portami uplink 25G) – 34 sztuki</u>

1. Przełącznik musi posiadać: 48 portów 100M/1G/2.5G/5GBaseT RJ-45 UPoE (do 60W per port)

2. Przełącznik musi posiadać moduł uplinkowy 2x 25G

3. Przełącznik musi zapewnić moc dostępną dla portów PoE:

3.1. 645W (z jednym zasilaczem o mocy 1100W),

3.2. 645W (z dwoma zasilaczami o mocy 1100W pracującymi w układzie redundantnym),

3.3. 1745W (z dwoma zasilaczami o mocy 1100W pracującymi w układzie współdzielenia mocy)

4. Przełącznik musi posiadać slot na moduł rozszerzeń (dający możliwość instalacji/wymiany „na gorąco" – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):

4.1. 4x1G SFP

4.2. 8x1/10G SFP/SFP+

4.3. 2x40G QSFP

4.4. 2x25G SFP28

4.5. 4x100M/1G/2.5G/5G/10GBaseT RJ-45

5. Przełącznik musi posiadać porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia następującymi rodzajami wkładek:

5.1. Porty SFP:

5.1.1. Gigabit Ethernet 1000Base-T,

5.1.2. Gigabit Ethernet 1000Base-SX,

5.1.3. Gigabit Ethernet 1000Base-LX/LH,

5.1.4. Gigabit Ethernet 1000Base-EX,

5.1.5. Gigabit Ethernet 1000Base-ZX,

5.1.6. Gigabit Ethernet 1000Base-BX-D/U

5.2. Porty SFP/SFP+:

5.2.1. Gigabit Ethernet 1000Base-T,

5.2.2. Gigabit Ethernet 1000Base-SX,

5.2.3. Gigabit Ethernet 1000Base-LX/LH,

5.2.4. Gigabit Ethernet 1000Base-EX,

5.2.5. Gigabit Ethernet 1000Base-ZX,

5.2.6. Gigabit Ethernet 1000Base-BX-D/U,

5.2.7. 10Gigabit Ethernet 10GBase-SR,

5.2.8. 10Gigabit Ethernet 10GBase-LR,

5.2.9. 10Gigabit Ethernet 10GBase-LRM,

5.2.10. 10Gigabit Ethernet 10GBase-ER,

5.2.11. 10Gigabit Ethernet 10GBase-ZR,

5.2.12. 10Gigabit Ethernet 10GBase-BX-D/U,

5.2.13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

5.3. Porty SFP/SFP+/SFP28:

5.3.1. Gigabit Ethernet 1000Base-T,

5.3.2. Gigabit Ethernet 1000Base-SX,

5.3.3. Gigabit Ethernet 1000Base-LX/LH,

5.3.4. Gigabit Ethernet 1000Base-EX,

5.3.5. Gigabit Ethernet 1000Base-ZX,

5.3.6. Gigabit Ethernet 1000Base-BX-D/U,

5.3.7. 10Gigabit Ethernet 10GBase-SR,

5.3.8. 10Gigabit Ethernet 10GBase-LR,

5.3.9. 10Gigabit Ethernet 10GBase-ER,

5.3.10. 10Gigabit Ethernet 10GBase-ZR,

5.3.11. 10Gigabit Ethernet 10GBase-BX-D/U,

5.3.12. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

5.3.13. 25Gigabit Ethernet 25GBASE-SR,

5.3.14. 25Gigabit Ethernet typu twinax (SFP28 – SFP28)

5.3.15. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF)

5.3.16. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)

5.4. Porty QSFP:

5.4.1. 40G-SR4,

5.4.2. 40G-LR4,

5.4.3. 40G-ER4,

5.4.4. 40G-SR-BD,

5.4.5. adapter 40G QSFP->10G SFP+

5.4.6. kable twinax

6. Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:

6.1. Min. przepustowość w ramach stosu - 480Gb/s,

6.2. Min. 8 urządzeń w stosie,

6.3. Zarządzanie poprzez jeden adres IP,

6.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

6.5. Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),

6.6. Możliwość współdzielenia mocy zasilaczy (grupa do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie),

7. Wymagania w zakresie zasilania i chłodzenia:

7.1. Przełącznik musi posiadać redundantne i wymienne moduły wentylatorów,

7.2. Przełącznik musi posiadać możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze muszą być wymienne (i mieć możliwość instalacji/wymiany „na gorąco" – ang. hot swap),

7.3. Przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia,

7.4. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik musi umożliwiać przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),

7.5. Przełącznik musi wspierać IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

8. Wymagania w zakresie parametrów wydajnościowych:

8.1. Szybkość przełączania musi zapewnić pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):

8.1.1. Przepustowość przełącznika (switching capacity) musi wynosić min.: 640 Gb/s (bez podłączenia do stosu), 1120 Gb/s (z podłączeniem do stosu)

8.1.2. Prędkość przesyłania (forwarding rate) musi wynosić min.: 476.19 Mpps (bez podłączenia do stosu), 833.33 Mpps (z podłączeniem do stosu)

8.2. Pojemność buforu pakietów musi wynosić mi.n. – 32MB

8.3. Min. 8 GB pamięci DRAM

8.4. Pamięć flash – min. 16GB

8.5. Przełącznik musi zapewnić obsługę:

8.5.1. 1000 aktywnych sieci VLAN

8.5.2. 32000 adresów MAC

8.5.3. 8000 tras IPv4

8.5.4. 4000 tras IPv6

8.5.5. 5000 wpisów w listach kontroli dostępu Security ACL –

8.5.6. 5000 wpisów w listach kontroli dostępu QoS ACL –

8.5.7. 1000 interfejsów SVI L3

8.5.8. 128 interfejsów L3

8.5.9. Jumbo frame 9198B

8.5.10. 128 połączeń zagregowanych typu „port channel"

8.5.11. 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

9. Przełącznik musi umożliwiać obsługę protokołu NTP

10. Przełącznik musi obsługiwać IGMPv1/2/3 i MLDv1/2 Snooping

11. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

11.1. IEEE 802.1w Rapid Spanning Tree

11.2. Per-VLAN Rapid Spanning Tree (PVRST+)

11.3. IEEE 802.1s Multi-Instance Spanning Tree

11.4. Obsługę 128 instancji protokołu STP

11.5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)

11.6. Redundancję połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego

12. Przełącznik musi wspierać obsługę protokołu LLDP (IEEE 802.1ab) i LLDP-MED

13. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)

14. Urządzenie musi umożliwiać realizacje funkcjonalności Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

15. Urządzenie musi obsługiwać funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

16. Urządzenie musi posiadać możliwość uruchomienia funkcji serwera DHCP

17. Urządzenie musi posiadać mechanizmy związane z bezpieczeństwem sieci:

17.1. Wpoziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

17.2. Autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,

17.3. Autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

17.4. Obsługę funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,

17.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,

17.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,

17.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

17.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,

17.9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w

oparciu o MAC adres/uwierzytelnianie oparciu o portal www),

17.10. Obsługę funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,

17.11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),

17.12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,

17.13. Obsługa list kontroli dostępu (ACL) następujących typów:

17.13.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

17.13.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

17.13.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

17.14. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

17.15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

17.16. Musi realizować funkcję Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),

18. Przełącznik musi obsługiwać mechanizmy zapewaniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

18.1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,

18.2. bezpieczną sekwencję uruchamiania,

18.3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

19. Przełącznik musi obsługiwać mechanizmy związane z zapewnieniem jakości usług w sieci:

19.1. Musi umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

19.2. Musi umożliwiać implementację algorytmu Shaped Round Robin dla obsługi kolejek,

19.3. Musi posiadać możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

19.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

19.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

19.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,

19.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

20. Przełącznik musi umożliwiać obsługę min. następujących protokołów i mechanizmów routingu:

20.1. Routing statyczny dla IPv4 i IPv6,

20.2. Routing dynamiczny – RIP, OSPF,

20.3. Routing dynamiczny zaawansowany - IS-IS, BGP dla IPv4 i IPv6,

20.4. Routing multicastów - PIM-SM, PIM-SSM, PIM-Bidir,

20.5. Multicast Source Discovery Protocol (MSDP),

20.6. Policy-based routing (PBR),

20.7. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,

20.8. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

21. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

22. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),

23. Przełącznik musi posiadać funkcjonalność sondy IP SLA Responder,

24. Przełącznik musi wspierać obsługę dla protokołu OpenFlow 1.3,

25. Przełącznik musi posiadać funkcjonalność Time Domain Reflectometer (TDR) umożliwiającą wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,

26. Wymagania w zakresie zarządzania:

26.1. Urządzenie musi być wyposażone w port konsoli,

26.2. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

26.3. Urządzenie musi mieć możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

26.4. Plik konfiguracyjny urządzenia muszą być możliwe do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

26.5. Urządzenie musi zapewniać możliwość obsługi protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

26.6. Urządzenie musi posiadać wsparcie dla protokoły RESTCONF,

26.7. Urządzenie musi posiadać wsparcie dla protokołu gNMI,

26.8. Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

26.9. Urządzenie musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć uruchomienia z nośnika danych umieszczonego w porcie USB;

26.10. Urządzenie musi posiadać możliwość wyposażenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności min. 120GB;

26.11. Urządzenie musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

27. Wymagania w zakresie parametrów fizycznych:

27.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

27.2. Wysokość urządzenia nie może przekraczać 1 RU,

27.3. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi musi być mniejsza niż 57 cm,

28. Urządzenie musi umożliwiać realizację rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

29. Przełącznik musi posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

30. Przełącznik musi posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,
31. Przełącznik musi zapewniać wsparcie dla protokołu LISP zgodnie z RFC 6830,
32. Przełącznik musi umożliwiać obsługę 256 wirtualnych instancji routingu (VRF),
33. Przełącznik musi zapewniać obsługę protokołu BFD (Bidirectional Forwarding Detection), który umożliwia szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,
34. Przełącznik musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,
35. Przełącznik musi posiadać możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256) dla 16 pierwszych portów downlinkowych przełącznika i wszystkich portów uplinkowych przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,
36. Przełącznik musi posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,
37. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności leaf oraz spine,
38. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tc-connect, udp-echo, udp-jitter,
39. Przełącznik musi posiadać wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii,
40. Przełącznik musi posiadać funkcjonalność bramy dla usług mDNS,
41. Przełącznik musi umożliwiać zdalną obserwację ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),
42. Przełącznik musi zapewniać widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),
43. Przełącznik musi umożliwiać eksport dodatkowych pól w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa),
44. Przełącznik musi posiadać wbudowany analizator pakietów,
45. Przełącznik musi posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,
46. Urządzenie musi umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,
47. Urządzenie musi umożliwiać integrację z zewnętrzną usługą bezpieczeństwa polegającą na przechwytywaniu i sprawdzaniu zapytań DNS (DNS Query) przesyłanych przez przełącznik pod kątem bezpieczeństwa i reputacji domen, o które kierowane są zapytania,
48. Urządzenie musi posiadać wsparcie dla Audio Video Bridging (AVB).
49. Wymagania w zakresie wyposażenia urządzenia:
    - 49.1. Przełącznik musi być wyposażony w zasilacz redundantny o mocy 1100W,
    - 49.2. Przełącznik musi być wyposażony jest w moduł do łączenia w stos data wraz z kablem stakującym o długości min. 50 cm,
    - 49.3. Przełącznik musi być wyposażony w kabel o długości min. 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną,
    - 49.4. Przełącznik musi być wyposażony w moduł: 2x25G SFP28
    - 49.5. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

D. <u>Przełącznik dostępowy typ B (BEZ portów uplink) – 36 sztuk</u>

1. Przełącznik musi posiadać 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at)

2. Przełącznik musi zapewniać moc dostępną dla PoE:
   - 2.1. 437W (z jednym zasilaczem o mocy 715W),
   - 2.2. 437W (z dwoma zasilaczami o mocy 715W pracującymi w układzie redundantnym),
   - 2.3. 1152W (z dwoma zasilaczami o mocy 715W pracującymi w układzie współdzielenia mocy)
3. Przełącznik musi być wyposażony w slot na moduł rozszerzeń (który umożliwia instalację/wymianę „na gorąco" – ang. hot swap) z możliwością obsadzenia nw. modułami (zależnie od potrzeb):
   - 3.1. 4x1G SFP
   - 3.2. 8x1/10G SFP/SFP+
   - 3.3. 2x40G QSFP
   - 3.4. 2x25G SFP28
   - 3.5. 4x100M/1G/2.5G/5G/10GBaseT RJ-45
4. Przełącznik musi posiadać porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia następującymi rodzajami wkładek:
   - 4.1. Porty SFP:
     - 4.1.1. Gigabit Ethernet 1000Base-T,
     - 4.1.2. Gigabit Ethernet 1000Base-SX,
     - 4.1.3. Gigabit Ethernet 1000Base-LX/LH,
     - 4.1.4. Gigabit Ethernet 1000Base-EX,
     - 4.1.5. Gigabit Ethernet 1000Base-ZX,
     - 4.1.6. Gigabit Ethernet 1000Base-BX-D/U
   - 4.2. Porty SFP/SFP+:
     - 4.2.1. Gigabit Ethernet 1000Base-T,
     - 4.2.2. Gigabit Ethernet 1000Base-SX,
     - 4.2.3. Gigabit Ethernet 1000Base-LX/LH,
     - 4.2.4. Gigabit Ethernet 1000Base-EX,
     - 4.2.5. Gigabit Ethernet 1000Base-ZX,
     - 4.2.6. Gigabit Ethernet 1000Base-BX-D/U,
     - 4.2.7. 10Gigabit Ethernet 10GBase-SR,
     - 4.2.8. 10Gigabit Ethernet 10GBase-LR,
     - 4.2.9. 10Gigabit Ethernet 10GBase-LRM,
     - 4.2.10. 10Gigabit Ethernet 10GBase-ER,
     - 4.2.11. 10Gigabit Ethernet 10GBase-ZR,
     - 4.2.12. 10Gigabit Ethernet 10GBase-BX-D/U,
     - 4.2.13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
   - 4.3. Porty SFP/SFP+/SFP28:
     - 4.3.1. Gigabit Ethernet 1000Base-T,
     - 4.3.2. Gigabit Ethernet 1000Base-SX,

4.3.3. Gigabit Ethernet 1000Base-LX/LH,

4.3.4. Gigabit Ethernet 1000Base-EX,

4.3.5. Gigabit Ethernet 1000Base-ZX,

4.3.6. Gigabit Ethernet 1000Base-BX-D/U,

4.3.7. 10Gigabit Ethernet 10GBase-SR,

4.3.8. 10Gigabit Ethernet 10GBase-LR,

4.3.9. 10Gigabit Ethernet 10GBase-ER,

4.3.10. 10Gigabit Ethernet 10GBase-ZR,

4.3.11. 10Gigabit Ethernet 10GBase-BX-D/U,

4.3.12. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

4.3.13. 25Gigabit Ethernet 25GBASE-SR,

4.3.14. 25Gigabit Ethernet typu twinax (SFP28 – SFP28)

4.3.15. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF)

4.3.16. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)

4.4. Porty QSFP:

4.4.1. 40G-SR4,

4.4.2. 40G-LR4,

4.4.3. 40G-ER4,

4.4.4. 40G-SR-BD,

4.4.5. adapter 40G QSFP->10G SFP+

4.4.6. kable twinax

5. Przełącznik musi umożliwiać stackowanie przełączników z zapewnieniem następujących funkcjonalności:

5.1. Przepustowość w ramach stosu min. 480Gb/s,

5.2. min. 8 urządzeń w stosie,

5.3. Zarządzanie poprzez jeden adres IP,

5.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

5.5. Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),

5.6. Możliwość współdzielenia mocy zasilaczy (grupa do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie),

6. Wymagania w zakresie zasilania i chłodzenia:

6.1. Przełącznik musi być wyposażony w redundantne i wymienne moduły wentylatorów,

6.2. Przełącznik musi posiadać możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze muszą być wymienne (i posiadać możliwość instalacji/wymiany „na gorąco" – ang. hot swap),

6.3. Przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia,

6.4. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik musi umożliwiać przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),

6.5. Przełącznik musi wspierać IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

7. Wymagania w zakresie parametrów wydajnościowych, przełącznik musi zapewniać

7.1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):

7.1.1. Przepustowość przełącznika (switching capacity): 256 Gb/s (bez podłączenia do stosu), 736 Gb/s (z podłączeniem do stosu)

7.1.2. Prędkość przesyłania (forwarding rate): 190.47 Mpps (bez podłączenia do stosu), 547.62 Mpps (z podłączeniem do stosu)

7.2. Przełącznik musi posiadać min. 16MB bufor pakietów

7.3. Przełącznik musi posiadać min. 8GB pamięci DRAM

7.4. Przełącznik musi posiadać min. 16GB Pamięci flash

7.5. Przełącznik musi umożliwiać obsługę:

7.5.1. 1000 aktywnych sieci VLAN

7.5.2. 32000 adresów MAC

7.5.3. 8000 tras IPv4

7.5.4. 4000 tras IPv6

7.5.5. Ilość wpisów w listach kontroli dostępu Security ACL – 5000

7.5.6. ilość wpisów w listach kontroli dostępu QoS ACL – 5000

7.5.7. 1000 interfejsów SVI L3

7.5.8. 128 interfejsów L3

7.5.9. Jumbo frame 9198B

7.5.10.128 połączeń zagregowanych typu „port channel"

7.5.11.16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

8. Przełącznik musi umożliwiać obsługę protokołu NTP

9. Przełącznik musi umożliwiać obsługę IGMPv1/2/3 i MLDv1/2 Snooping

10. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

10.1. IEEE 802.1w Rapid Spanning Tree

10.2. Per-VLAN Rapid Spanning Tree (PVRST+)

10.3. IEEE 802.1s Multi-Instance Spanning Tree

10.4. Obsługa 128 instancji protokołu STP

10.5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)

10.6. Redundancję połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego

11. Przełącznik musi umożliwiać obsługę protokołu LLDP (IEEE 802.1ab) i LLDP-MED
12. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)
13. Przełącznik musi wspierać funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
14. Przełącznik musi umożliwiać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
15. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
16. Przełącznik musi zapewniać następujące mechanizmy związane z bezpieczeństwem sieci:
    - 16.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    - 16.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    - 16.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    - 16.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    - 16.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    - 16.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    - 16.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
    - 16.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
    - 16.9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
    - 16.10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
    - 16.11. Zapewniać podstawowe mechanizmy bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
    - 16.12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
    - 16.13. Obsługa list kontroli dostępu (ACL) następujących typów:
        - 16.13.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
        - 16.13.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
        - 16.13.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    - 16.14. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
    - 16.15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
    - 16.16. Realizacja funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),
17. Przełącznik musi zapewniać obsługę mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    - 17.1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    - 17.2. bezpieczna sekwencja uruchamiania,
    - 17.3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

18. Przełącznik musi zapewniać mechanizmy związane z zapewnieniem jakości usług w sieci:
    18.1. Umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    18.2. Umożliwiać implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
    18.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    18.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    18.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
    18.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
    18.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
19. Przełącznik musi umożliwiać obsługę następujących protokołów i mechanizmów routingu:
    19.1. Routing statyczny dla IPv4 i IPv6,
    19.2. Routing dynamiczny – RIP, OSPF,
    19.3. Routing dynamiczny zaawansowany - IS-IS, BGP dla IPv4 i IPv6,
    19.4. Routing multicastów - PIM-SM, PIM-SSM, PIM-Bidir,
    19.5. Multicast Source Discovery Protocol (MSDP),
    19.6. Policy-based routing (PBR),
    19.7. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,
    19.8. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
20. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
21. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
22. Przełącznik musi posiadać funkcjonalność sondy IP SLA Responder,
23. Przełącznik musi posiadać wsparcie dla protokołu OpenFlow 1.3,
24. Przełącznik musi posiadać funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,
25. Wymagania w zakresie zarządzania:
    25.1. Urządzenie musi być wyposażone w port konsoli,
    25.2. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,
    25.3. Urządzenie musi zapewniać możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
    25.4. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej muci być zapewniona możliwość uruchomienia urządzenia z nową konfiguracją,
    25.5. Urządzenie musi posiadać możliwość obsługi protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

25.6. Urządzenie musi posiadać wsparcie dla protokoły RESTCONF,

25.7. Urządzenie musi posiadać wsparcie dla protokołu gNMI,

25.8. Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

25.9. Przełącznik musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;

25.10. Urządzenie musi posiadać możliwość wyposażenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności min. 120GB;

25.11. Przełącznik musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

26. Wymagania w zakresie parametrów fizycznych:

26.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

26.2. Wysokość urządzenia nie może przekraczać 1 RU,

26.3. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi musi być mniejsza niż 50 cm,

27. Urządzenie musi umożliwiać realizację rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

28. Urządzenie musi mieć możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

29. Urządzenie musi mieć możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,

30. Urządzenie musi zapewniać wsparcie dla protokołu LISP zgodnie z RFC 6830,

31. Urządzenie musi zapewniać obsługę 256 wirtualnych instancji routingu (VRF),

32. Urządzenie musi zapewniać obsługę protokołu BFD (Bidirectional Forwarding Detection) który umożliwia szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

33. Urządzenie musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,

34. Urządzenie musi posiadać możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256) dla wszystkich portów przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,

35. Urządzenie musi posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,

36. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności leaf oraz spine,

37. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,

38. Przełącznik musi posiadać wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii,

39. Przełącznik musi posiadać funkcjonalność bramy dla usług mDNS,

40. Przełącznik musi umożliwiać zdalną obserwację ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

41. Przełącznik musi zapewniać widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),

42. Przełącznik musi zapewniać możliwość eksportu dodatkowych pólł w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa),

43. Przełącznik musi posiadać wbudowany analizator pakietów,
44. Przełącznik musi posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,
45. Urządzenie musi umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,
46. Integracja z zewnętrzną usługą bezpieczeństwa polegającą na przechwytywaniu i sprawdzaniu zapytań DNS (DNS Query) przesyłanych przez przełącznik pod kątem bezpieczeństwa i reputacji domen, o które kierowane są zapytania,
47. Urządzenie musi posiadać wsparcie dla Audio Video Bridging (AVB).
48. Wymagania w zakresie wyposażenia urządzenia:
    - 48.1. Przełącznik musi być wyposażony w zasilacz redundantny o mocy 715W,
    - 48.2. Przełącznik musi być wyposażony w moduł do łączenia w stos data wraz z kablem stakującym o długości 50 cm,
    - 48.3. Przełącznik musi być wyposażony w kabel o długości 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną,
    - 48.4. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

E. **Przełącznik dostępowy typ C – 2 sztuki**

1. Przełącznik musi być wyposażony w 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP
2. Przełącznik musi zapewniać moc dostępna dla PoE:
    - 2.1. 505W (z jednym zasilaczem o mocy 715W),
    - 2.2. 505W (z dwoma zasilaczami o mocy 715W pracującymi w układzie redundantnym),
    - 2.3. 1220W (z dwoma zasilaczami o mocy 715W pracującymi w układzie współdzielenia mocy)
    - 2.4. 1440W (z zasilaczem pierwszym o mocy 715W oraz drugim o mocy 1100W pracującymi w układzie współdzielenia mocy)
3. Przełącznik musi posiadać porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
    - 3.1. Gigabit Ethernet 1000Base-T,
    - 3.2. Gigabit Ethernet 1000Base-SX,
    - 3.3. Gigabit Ethernet 1000Base-LX/LH,
    - 3.4. Gigabit Ethernet 1000Base-EX,
    - 3.5. Gigabit Ethernet 1000Base-ZX,
    - 3.6. Gigabit Ethernet 1000Base-BX-D/U,
    - 3.7. 10Gigabit Ethernet 10GBase-SR,
    - 3.8. 10Gigabit Ethernet 10GBase-LR,
    - 3.9. 10Gigabit Ethernet 10GBase-LRM,
    - 3.10. 10Gigabit Ethernet 10GBase-ER,
    - 3.11. 10Gigabit Ethernet 10GBase-ZR,
    - 3.12. 10Gigabit Ethernet 10GBase-BX-D/U,
    - 3.13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
4. Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
    - 4.1. Przepustowość w ramach stosu - 320Gb/s,

4.2. Min. 8 urządzeń w stosie,

4.3. Zarządzanie poprzez jeden adres IP,

4.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

4.5. Posiadać wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),

5. Wymagania w zakresie zasilania i chłodzenia:

5.1. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów,

5.2. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze musza być wymienne (i posiadać możliwość instalacji/wymiany „na gorąco" – ang. hot swap),

5.3. Przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia,

5.4. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik musi umożliwiać przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),

5.5. Przełącznik musi wspierać IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

6. Wymagania w zakresie parametrów wydajnościowych:

6.1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):

6.1.1. Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 496 Gb/s (z podłączeniem do stosu)

6.1.2. Prędkość przesyłania (forwarding rate): 130.95 Mpps (bez podłączenia do stosu), 369.05 Mpps (z podłączeniem do stosu)

6.2. Pojemność bufora pakietów – min. 16MB

6.3. Przełącznik musi obsługiwać:

6.3.1. 1000 aktywnych sieci VLAN

6.3.2. 32000 adresów MAC

6.3.3. 8000 tras IPv4

6.3.4. 4000 tras IPv6

6.3.5. Ilość wpisów w listach kontroli dostępu Security ACL – 5000

6.3.6. ilość wpisów w listach kontroli dostępu QoS ACL – 5000

6.3.7. 1000 interfejsów SVI L3

6.3.8. 128 interfejsów L3

6.3.9. Jumbo frame 9198B

6.3.10. 128 połączeń zagregowanych typu „port channel"

6.3.11. 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

7. Przełącznik musi zapewniać obsługę protokołu NTP

8. Przełącznik musi zapewniać obsługę IGMPv1/2/3 i MLDv1/2 Snooping

9. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

9.1. IEEE 802.1w Rapid Spanning Tree

9.2. Per-VLAN Rapid Spanning Tree (PVRST+)

9.3. IEEE 802.1s Multi-Instance Spanning Tree

9.4. Obsługa 128 instancji protokołu STP

9.5. Redundancję połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego

10. Przełącznik musi zapewniać obsługę protokołu LLDP (IEEE 802.1ab) i LLDP-MED

11. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)

12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

13. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

14. Możliwość uruchomienia funkcji serwera DHCP

15. Przełącznik musi posiadać mechanizmy związane z bezpieczeństwem sieci:

15.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),

15.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,

15.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

15.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,

15.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adreś MAC,

15.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,

15.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

15.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,

15.9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),

15.10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,

15.11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),

15.12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,

15.13. Obsługa list kontroli dostępu (ACL) następujących typów:

15.13.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

15.13.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

15.13.3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

15.13.4. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

15.14. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

15.15. Funkcja Private VLAN;

16. Przełącznik musi zapewnić obsługę mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

16.1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,

16.2. bezpieczna sekwencja uruchamiania,

16.3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

17. Przełącznik musi zapewnić mechanizmy związane z zapewnieniem jakości usług w sieci:

17.1. Możliwość implementacji min. 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

17.2. Możliwość implementacji algorytmu Shaped Round Robin dla obsługi kolejek,

17.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

17.4. Możliwość klasyfikacji ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

17.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

17.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,

17.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

18. Przełącznik musi umożliwiać obsługę następujących protokołów i mechanizmów routingu:

18.1. Routing statyczny dla IPv4 i IPv6,

18.2. Routing dynamiczny – RIP, OSPF, IS-IS

18.3. Policy-based routing (PBR),

18.4. Routing multicastów - PIM-SM, PIM-SSM,

18.5. Multicast Source Discovery Protocol (MSDP),

18.6. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,

18.7. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

19. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

20. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),

21. Przełącznik musi posiadać wsparcie dla protokołu OpenFlow 1.3

22. Przełącznik musi posiadać funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,

23. Wymagania w zakresie zarządzania:

23.1. Przełącznik musi mieć wbudowany port konsoli,

23.2. Przełącznik musi posiadać dedykowany port Ethernet do zarządzania out-of-band,

23.3. Przełącznik musi posiadać możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność ta musi umożliwiać kontrolę dostępu do konsoli poprzez

mechanizm lokalnego konta logowania lub mechanizm AAA,

23.4. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

23.5. Przełącznik musi zapewniać obsługę protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

23.6. Przełącznik musi posiadać wsparcie dla protokoły RESTCONF,

23.7. Przełącznik musi posiadać wsparcie dla protokołu gNMI,

23.8. Przełącznik musi posiadaća diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

23.9. Przełącznik musi posiadać a wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,

23.10. Przełącznik musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;

23.11. Urządzenie musi posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

23.12. Urządzenie musi posiadać wbudowany graficzny interfejs zarządzania przełącznikiem.

24. Przełącznik musi umożliwiać realizację rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

25. Przełącznik musi umożliwiać eksport dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)

26. Przełącznik musi posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

27. Przełącznik musi posiadać możliwość uruchamiania zdefiniowanych w Pythonie skryptów bezpośrednio na urządzeniu

28. Przełącznik musi posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,

29. Przełącznik musi posiadać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów Edge/VTEP,

30. Przełącznik musi posiadać wsparcie dla protokołu LISP zgodnie z RFC 6830,

31. Przełącznik musi zapewniać obsługę min. 256 wirtualnych instancji routingu (VRF),

32. Przełącznik musi posiadać obsługę protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

33. Przełącznik musi posiadać funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,

34. Przełącznik musi posiadać wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii,

35. Przełącznik musi posiadać funkcjonalność bramy dla usług mDNS,

36. Przełącznik musi realizować funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,

37. Przełącznik musi posiadać możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

38. Przełącznik musi posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,

39. Przełącznik musi zapewniać widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),

40. Przełącznik musi posiadać wbudowany analizator pakietów umożliwiamy zbieranie ruchu w czasie rzeczywistym, dekodowanie ruchu i zapisywanie ich w formie pliku .pcap lub do pamięci urządzenia (flash, zewnętrzne usb). Wynik dekodowania ruchu może

zostać wyświetlony na konsoli urządzenia lub w zewnętrznym oprogramowaniu typu Wireshark.

41. Urządzenie musi umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,

42. Integracja z zewnętrzną usługą bezpieczeństwa polegającą na przechwytywaniu i sprawdzaniu zapytań DNS (DNS Query) przesyłanych przez przełącznik pod kątem bezpieczeństwa i reputacji domen, o które kierowane są zapytania,

43. Wymagania w zakresie parametrów fizycznych:

    43.1. Urządzenie musi być możliwe do zamontowania w szafie rack 19",

    43.2. Wysokość urządzenia nie może przekraczać 1 RU,

44. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi nie może być mniejsza niż 50 cm,

45. Wymagania w zakresie wyposażenia urządzenia:

    45.1. Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,

    45.2. Przełącznik musi być wyposażony w moduł do łączenia w stos wraz z kablem stakującym o długości 50 cm,

    45.3. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

F. **Akcesoria do przełączników i kontrolerów muszą być wyposażone w gwarancję oraz wsparcie producenta na okres 24 miesięcy:**

1. W ramach zamówienia Kupujący wymaga dostarczenia następujących akcesoriów do urządzeń dostępowych typu A i B

    1.1. Moduł optyczny interfejsowy SFP28 typu 10/25Gigabit Ethernet 10/25GBASE-CSR do przełączników dostępowych typ A – **36 sztuk** - *Wkładka interfejsowa w standardzie SFP28, pracująca w standardzie 10/25Gigabit Ethernet 10/25GBASE-CSR. Kupujący wymaga aby wkładka była kompatybilna z wyspecyfikowanym przełącznikami dostępowymi typu A.*

    1.2. Kabel do łączenia w stos do przełączników dostępowych typ A i B o dł. 3m – **24 sztuki** - *Kabel połączeniowy o dł. 3 metrów przystosowany do łączenia przełączników dostępowych typ A i B w stos.*

    1.3. Kabel do łączenia w stos zasilający do przełączników dostępowych typ A i B o dł. 1.5m – **24 sztuki** - *Kabel połączeniowy o dł. 1.5 metra przystosowany do łączenia przełączników dostępowych typ A i B w stos zasilający.*

    1.4. Kabel do łączenia w stos do przełączników dostępowych typ A i B o dł. 1m – **6 sztuk** - *Kabel połączeniowy o dł. 1 metr przystosowany do łączenia przełączników dostępowych typ A i B w stos.*

2. W ramach zamówienia Kupujący wymaga dostarczenia następujących akcesoriów do przełącznika szkieletowego typu A i C

    2.1. Moduł optyczny interfejsowy SFP28 typu 10/25Gigabit Ethernet 10/25GBASE-CSR do przełączników szkieletowych typ A – **36 sztuk** - *Wkładka interfejsowa w standardzie SFP28, kompatybilna z przełącznikami szkieletowymi typ A, pracująca w standardzie 10/25Gigabit Ethernet 10/25GBASE-CSR.*

    2.2. Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ A – **4 sztuki** - *Kabel połączeniowy typu twinax o dł. 3 metrów umożliwiający połączenie ze sobą przełączników szkieletowych typu A, przy pomocy interfejsów SFP+ pracujących z prędkością 10 Gb/s.*

    2.3. Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ A i przełączników dostępowych typ C – **4 sztuki** - *Kabel połączeniowy typu twinax o dł. 3 metrów umożliwiający połączenie ze sobą przełączników szkieletowych typu A i przełączników dostępowych typ C w węźle centralnym, przy pomocy interfejsów SFP+ pracujących z prędkością 10 Gb/s.*

    2.4. Kabel połączeniowy typu twinax 40G 3m do przełączników szkieletowych typ A – **4 szt.** - *Kabel połączeniowy typu twinax o dł. 3 metrów umożliwiający połączenie ze sobą przełączników szkieletowych typu A, przy pomocy interfejsów SFP+ pracujących z prędkością 40 Gb/s.*

    2.5. Moduł optyczny SFP+ typu 10G jednomodowy LR do przełączników szkieletowych typ A - **4 sztuki** - *Wkładka interfejsowa w standardzie SFP+ typu LR 10Gigabit Ethernet służąca do podłączenia łącz od operatorów telekomunikacyjnych.*

3. W ramach zamówienia Kupujący wymaga dostarczenia następujących akcesoriów do przełącznika szkieletowego typ B

   3.1. Moduł optyczny interfejsowy SFP typu 10GBASE-LRM do przełączników szkieletowych typ B – **10 sztuk** - *Wkładka interfejsowa w standardzie SFP+, kompatybilna z przełącznikami szkieletowymi typ B, pracująca w standardzie 10GBASE-LRM.*

   3.2. Moduł optyczny interfejsowy SFP typu 10GBASE-SR do przełączników szkieletowych typ B – **10 sztuk** - *Wkładka interfejsowa w standardzie SFP+, kompatybilna z przełącznikami szkieletowymi typ B, pracująca w standardzie 10GBASE-SR.*

   3.3. Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ B – **4 sztuki** - *Kabel połączeniowy typu twinax o dł. 3 metrów umożliwiający połączenie ze sobą przełączników szkieletowych typu B, przy pomocy interfejsów SFP+ pracujących z prędkością 10 Gb/s.*

4. W ramach zamówienia Kupujący wymaga dostarczenia następujących akcesoria do kontrolerów WiFi

   4.1. Kabel połączeniowy typu twinax 10G 7m do kontrolerów sprzętowych WiFi typ A – **4 sztuki** - *Kabel połączeniowy typu twinax o dł. 7 metrów umożliwiający połączenie do przełączników szkieletowych typ A lub przełączników dostępowych typ C sprzętowych kontrolerów WiFi typ A z prędkością 10 Gb/s z wykorzystaniem interfejsów SFP+.*

   4.2. Moduł optyczny SFP+ z oferty producenta urządzenia 10GBase-SR – **8 sztuk** - *Wkładka interfejsowa w standardzie SFP+ służąca do podłączenia kontrolerów do sieci LAN*

G. **System zarządzania i monitorowania siecią w lokalizacji Warszawa oraz monitoringu sieci LAN w pozostałych lokalizacjach Zamawiającego (wraz z dedykowanym serwerem, który może zostać zamontowany ww szafie rack 19"- appliance, posiadający wsparcie producenta Oprogramowania) - 1 komplet**

1. Przedmiotem zamówienia jest zakup graficznego system do zarządzania i monitorowania sieci kampusowej przewodowej oraz bezprzewodowej.

2. Minimalne wymagania w zakresie funkcjonalności podstawowych systemu w zakresie monitoringu sieci. System musi:

   2.1. Zbierać i zapamiętywać do 7 dni wstecz dane telemetryczne o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji z różnych źródeł danych: SNMP, Syslog, NetFlow, sensory bezprzewodowe WiFi;

   2.2. Analizować i korelować dane telemetrycznych o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji na podstawie różnych źródeł danych: SNMP, Syslog, NetFlow, sensory bezprzewodowe WiFi;

   2.3. Umożliwiać wizualizację topologii sieci wraz połączeniami oraz wizualizacją stanu pracy danego monitorowanego obiektu;

   2.4. zbierać i prezentować szczegółową informację o ilości użytkowników przewodowych podłączonych do sieci oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci z podaniem typowych przyczyn braku podłączenia np. problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej. Szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP;

   2.5. zbierać i prezentować szczegółową informację o ilości użytkowników bezprzewodowych podłączonych do sieci z rozbiciem na grupę użytkowników o dobrej jakości i złej jakości pracy oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci bezprzewodowej z podaniem typowych przyczyn braku podłączenia np. problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej. Szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP;

   2.6. Generować automatyczne komunikaty o stwierdzonych nieprawidłowościach w pracy sieci w oparciu o skorelowane informacje zbierane przez system z urządzeń sieciowych wraz z sugestią przyczyny, sposobu rozwiązania problemu oraz dalszych kroków diagnostycznych dla poszczególnych urządzeń sieciowych;

   2.7. Posiadać narzędzie do śledzenia ścieżki sieciowej dla danego ruchu w sieci np. w relacji pomiędzy dwoma hostami wraz podaniem informacji o wszystkich węzłach na ścieżce, ich stanu, topologii fizycznej i logicznej np. zaznaczenie tunelowania ruchu bezprzewodowego, dokładną informacją o interfejsach, przez który płynie ruch;

   2.8. Wyznaczać na postawie analizy danych telemetrycznych dla każdego z urządzeń sieciowych, grupy użytkowników, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji indeksu liczbowego określającego jakość pracy danego monitorowanego obiektu wraz z wizualizacją na skali czasu zmiany wartości indeksów jakości pracy dla grup urządzeń sieciowych, grupy użytkowników przewodowych i bezprzewodowych, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji;

3. Minimalne wymagania w zakresie wykrywania i analizy problemów w sieci. System musi

3.1. Dokonywać automatycznej analizy zdarzeń w sieci oraz identyfikacja i wyświetlać na tej podstawie problemy w działaniu sieci na poziomie całej sieci lub poszczególnych monitorowanych obiektów np. problemy związane z danym urządzeniem, użytkownikiem lub aplikacją w celu natychmiastowego dostarczenia danych diagnostycznych;

3.2. Automatycznie priorytetyzować problemy;

4. Minimalne wymagania w zakresie monitoring urządzeń. System musi

4.1. Zapewniać monitoring dostępności i osiągalności poszczególnych urządzeń sieciowych;

4.2. W zakresie sieci bezprzewodowej prezentować wykresy:

4.2.1. Ilości aktywnych i nieaktywnych punktów radiowych z podaniem dokładnej listy urządzeń w każdej z kategorii;

4.2.2. Listy radiowych punktów dostępowych wg. ilości podłączonych klientów bezprzewodowych;

4.2.3. Listy radiowych punktów dostępowych wg. poziomu zakłóceń i interferencji w funkcji pasma transmisji 2.4 GHz, 5 GHz;

4.3. Prezentować pełną listę wszystkich monitorowanych urządzeń sieciowych w całej sieci lub w danej domenie lub lokalizacji z podaniem modelu urządzenia, wersji systemu operacyjnego, adresu IP, stanu pracy, osiągalności, ilości zidentyfikowanych problemów, lokalizacji geograficznej. Możliwość eksportu danych w postaci pliku CSV;

4.4. Posiadać możliwość łatwego filtrowania listy urządzeń wg. kryteriów:

4.4.1. Typ urządzenia: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, radiowy punkt dostępowy, kontroler WLAN;

4.4.2. Stan pracy urządzenia;

4.4.3. Lokalizacja;

4.4.4. Model urządzenia;

4.4.5. Wersja systemu operacyjnego;

4.4.6. Adres IP;

5. System musi umożliwiać szczegółowy monitoring każdego z urządzeń sieciowych obejmujący:

5.1. Szczegółową informację o następujących parametrach pracy urządzenia w dowolnym momencie pracy urządzenia do 7 dni wstecz. System musi monitorować min. parametry: utylizacja pamięci, utylizacja CPU, dostępność łączy uplinkowych (w górę sieci), poziom błędów na linkach, skojarzone zdarzenia zarejestrowane w systemie;

5.2. Szczegółową listę wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz) problemów skojarzonych z danym urządzeniem;

5.3. Schemat topologii sieci, w której znajduje się dane urządzenie;

5.4. Dostęp do zdarzeń zarejestrowanych w systemie związanych z danym urządzeniem z możliwością filtrowanie wg. ważności;

5.5. Możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia do danego innego miejsca (adresu IP);

5.6. Możliwość bezpośredniego z poziomu konsoli graficznej systemu zarządzania i monitorowania dostępu do konsoli urządzenia lub narzędzia umożliwiającego zdalne wydawanie komend na urządzeniu;

5.7. System musi prezentować szczegółowe informacje o urządzeniu obejmujące:

5.7.1. Wykres czasowy utylizacji CPU;

5.7.2. Wykres czasowy utylizacji pamięci;

5.7.3. Wykres czasowy dostępności urządzenia;

5.7.4. Wykres czasowy temperatury urządzenia;

5.7.5. Informacje o poszczególnych interfejsach urządzeń w uwzględnieniem: stanu interfejsu, typu, numer skonfigurowanej sieci VLAN, MAC adresu podłączonego urządzenia, prędkość linku, FDX/HDX;

5.7.6. Dla każdego z monitorowanych interfejsów informacje o:

5.7.6.1. Wykres czasowy dostępności interfejsu;

5.7.6.2. Wykres czasowy utylizacji interfejsu niezależnie w kierunku nadawczym i odbiorczym;

5.7.6.3. Wykres czasowy poziomu błędów niezależnie w kierunku nadawczym i odbiorczym;

5.7.7. W przypadku urządzeń pracujących jako urządzenia w sieci SDN typu Network Fabric szczegółowe informacje na temat stanu połączenia z siecią podkładową, stanu podłączenia do systemu kontroli dostępu w sieci Network Fabric;

6. Minimalne wymagania w zakresie monitoringu użytkowników:

6.1. System musi monitorować i prezentować szczegółowe informacje o użytkowniku końcowym i urządzeniach na których pracuje takie jak:

6.1.1. identyfikator użytkownika,

6.1.2. nazwa hosta lub hostów, na których pracuje,

6.1.3. adres MAC hosta lub hostów,

6.1.4. adres IPv4 i IPv6 hosta lub hostów,

6.1.5. typ urządzenia,

6.1.6. urządzenie, do którego jest podłączone dane urządzenie końcowe wykorzystywane przez użytkownika,

6.1.7. lokalizacja geograficzna;

6.2. System musi monitorować i prezentować szczegółową informację o następujących parametrach pracy urządzenia końcowego wykorzystywanego przez użytkownika w dowolnym momencie do 7 dni wstecz. System musi monitorować min. następujące parametry: stan podłączenia do sieci, dla urządzeń bezprzewodowych: poziom sygnału RSSI, poziom szumów SNR, przepustowość połączenia, ilość danych otrzymanych i nadawanych, SSID sieci, do której jest podłączone urządzenie końcowe, nazwa radiowego punktu dostępowego, wykorzystywany kanał radiowy i pasmo.

6.3. System musi monitorować i prezentować szczegółową listę wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz) problemów skojarzonych z danym urządzeniem końcowym;

6.4. System musi prezentować schemat topologii sieci z zaznaczeniem urządzenia dostępowego do którego jest podłączony dane urządzenie końcowe;

6.5. Dostęp do zdarzeń zarejestrowanych w systemie związanych z danym użytkownikiem z możliwością filtrowania wg. ważności;

6.6. System musi posiadać możliwość uruchomienia narzędzia do analizy ścieżki od danego użytkownika do danego innego miejsca (adresu IP);

6.7. System musi zbierać, prezentować i monitorować informacje o generowanym ruchu sieciowym przez użytkownika na danym urządzeniu końcowym z podziałem na aplikacje biznesowe oraz niebiznesowe. Szczegółowe informacje dla każdej z aplikacji takie jak: nazwa aplikacji, indeks jakości działania aplikacji w sieci, ilość ruchu (w bajtach), średnia przepustowość (w bps), parametry QoS faktyczne oraz oczekiwane, straty pakietów (maksymalne i średnie), opóźnienie sieciowe (maksymalne i średnie), jitter (maksymalny i średni);

6.8. System musi monitorować szczegółowe informacje o urządzeniu końcowym wykorzystywanym przez użytkownika:

6.8.1. Wykres czasowy ilości danych nadawanych i otrzymywanych;

6.8.2. Wykres czasowy ilości generowanych zapytań DNS i otrzymywanych odpowiedzi;

6.8.3. Dla urządzeń bezprzewodowych wykres czasowy zmian wartości mocy sygnału radiowego RSSI oraz zmian wartości poziomu szumów SNR;

7. Minimalne wymagania w zakresie monitoringu aplikacji:

7.1. System musi prezentować szczegółowe informacje o aplikacjach wykorzystywanych w sieci takie jak: lista wszystkich wykrytych aplikacji z podaniem nazw aplikacji, klas ruchu, ilości ruchu generowanego, średniej przepustowości, straty pakietów, opóźnienia sieciowego oraz wykrytych problemów związanych z daną aplikacją;

7.2. System musi prezentować szczegółowe wykresy czasowe parametrów działania każdej z aplikacji z uwzględnieniem: przepustowości wykorzystywanej przez daną aplikację, strat pakietów, jitter, opóźnienia sieciowego, opóźnienia sieciowego po stronie klienta, opóźnienia sieciowego po stronie serwera, opóźnienia generowanego przez serwer aplikacyjny;

7.3. System musi monitorować i prezentować szczegółową listę wszystkich użytkowników wykorzysujących daną aplikację w sieci z podaniem urządzenia końcowego, który wykorzystuje daną aplikację;

8. Minimalne wymagania w zakresie monitoringu sieci bezprzewodowej.

8.1. System musi umożliwiać wizualizację graficzną rozmieszczenia poszczególnych radiowych punktów dostępowych, sensorów oraz klientów sieci bezprzewodowej na mapie budynku;

8.2. System musi umożliwiać graficzne planowanie i zarządzanie siecią bezprzewodową (hierarchiczne mapy lokalizacji, mapy zasięgu) z wykorzystaniem własnych planów budynków;

8.3. System musi umożliwiać monitorowanie informacji takich jak: poziom szumu, poziom sygnału, interferencje sygnału pochodzących z punktów dostępowych;

8.4. System musi umożliwiać współpracę z systemami lokalizacji urządzeń radiowych (punktów dostępowych, klientów, tagów) z prezentacją graficzną na mapie;

8.5. System musi posiadać narzędzie pozwalające na wykonywanie testów poprawności pracy sieci bezprzewodowej poprzez generowanie syntetycznego ruchu przez punkty dostępowe lub dedykowane sensory bezprzewodowe pozwalające na badanie/wykonanie testu:

8.5.1. czasu podłączania się do sieci: asocjacja, uwierzytelnienie, adresacja z DHCP;

8.5.2. pracy usług: DNS, RADIUS, dostępność bramy, dostępność określonych adresów IP;

8.5.3. pracy aplikacji: POP3, IMAP, Outlook Web Access, FTP, HTTP, HTTPS;

8.6. Możliwość określenia czasu lub częstotliwości wykonywania testów;

9. Minimalne wymagane funkcjonalności z zakresu zarządzania siecią:

9.1. Hierarchizacja zarządzania siecią odzwierciedlająca hierarchię geograficzną tj. możliwość podziału sieci na kilka poziomów geograficznych np. region, kraj, miasto, budynek, piętro;

9.2. Wizualizacja graficzna na mapie lokalizacji poszczególnych urządzeń sieciowych – automatyczne rozmieszczanie urządzeń na postawie adresów pocztowych;

9.3. Możliwość wgrywania własnych planów budynków z dokładnością do poszczególnych pięter;

9.4. Obsługa REST API;

9.5. Integracja z system uwierzytelniania w celu otrzymywania informacji o tym jaki użytkownik jest związany z jakim urządzeniem, szczegółowej informacji o przebiegu procesu uwierzytelniania do sieci. Uwzględnienie tych danych w procesie wyznaczania indeksów jakości pracy użytkowników jak również w procesie diagnostyki problemów w sieci;

9.6. Mechanizm automatycznej aktualizacji wersji systemu bezpośrednio z chmury producenta wtedy, kiedy pojawiają się nowe wersje;

9.7. Wbudowane narzędzia do automatycznego tworzenia polityki QoS dla całej sieci w oparciu o wbudowane wzorce aplikacji, z możliwością tworzenia własnych wzorców. Możliwości dokonywania zmian w polityce i jej szybkiej implementacji oraz możliwość cofania zmian bez konieczności ręcznej rekonfiguracji urządzeń sieciowych;

9.8. Funkcjonalność automatycznego wykrywania urządzeń sieciowych w oparciu o SNMP, CLI, http, SSH;

9.9. Możliwość tworzenia parametryzowanych wzorców konfiguracyjnych dla urządzeń w oparciu o język skryptowy;

9.10. Inwentaryzacja urządzeń oraz oprogramowania;

9.11. Zarządzanie wersjami oprogramowania z możliwością wskazania wersji obowiązujących;

9.12. Narzędzie do bezdotykowej konfiguracji urządzeń sieciowych (Plug and Play lub Zero Touch Deployment);

9.13. Możliwość definiowania profili sieciowych oraz parametrów sieciowych takich jak: serwery TACAS, Radius, NTP, Syslog, NetFlow, DNS, DHCP dla poszczególnych poziomów hierarchii sieciowej niezależnie lub dziedziczenie tych ustawień z poziomu wyższego w dół hierarchii. Centralne zarządzania parametrami dostępowymi do urządzeń wraz z możliwością ich zmiany dla jednego urządzenia, grupy urządzeń lub całej sieci;

10. Minimalne wymagania funkcjonalności z zakresu zarządzania siecią SDA (funkcje kontrolera SDA):

10.1. Zarządzanie i monitorowanie siecią kampusową SDA jako jednolitą siecią typu Network Fabric;

10.2. Graficzny interfejs użytkownika umożliwiający tworzenie segmentacji i polityki bezpieczeństwa w sieci SDA jak również provisioning urządzeń sieciowych tworzących sieć typu Network Fabric;

10.3. Funkcje centralnego kontrolera SDA umożliwiające centralne programowanie urządzeń oraz centralny monitoring i analizę strumieni telemetrycznych z sieci w celu wykrywania nieprawidłowości w jej działaniu;

10.4. Centralne zarządzanie polityką bezpieczeństwa poprzez określenie relacji pomiędzy segmentami logicznymi w sieci SDA (grupami urządzeń, użytkowników lub aplikacji) z możliwością tworzenia kontraktów dla wymiany ruchu pomiędzy tymi grupami;

10.5. Filtracja ruchu niezależna od adresaci IP w oparciu o rolę użytkownika lub urządzenia w sieci i zdefiniowane relacje;

10.6. Zarządzanie pulami adresowymi używanymi w sieci SDA;

10.7. Zarządzanie sposobem uwierzytelniania w sieci Network Fabric na poziomie globalnym oraz na poziomie każdego z portów urządzeń dostępowych niezależnie;

10.8. Logiczny podział sieci na makrosegmenty i mikrosegmenty przy użyciu narzędzia graficznego;

10.9. Logiczny podział użytkowników i urządzeń na grupy i określenie relacji pomiędzy nimi;

10.10. Tworzenie podsieci IP rozciągniętej na dowolne porty dostępowe w ramach Network Fabric;

10.11. Możliwość filtrowania ruchu pomiędzy urządzeniami pracującymi w jednej grupie logicznej i/lub podsieci IP jak również pomiędzy różnymi grupami logicznymi i/lub podsieciami IP bez konieczności stosowania ACL opartych o adresy IP;

10.12. Automatyzacja procesu tworzenia Network Fabric (dodawanie urządzeń, przypisywanie im roli w sieci, określanie poziomów uwierzytelnienia użytkowników i urządzeń na brzegu sieci) bez konieczności używania linii komend (CLI));

10.13. Automatyczne wykrywanie urządzeń sieciowych;

10.14. Narzędzie do automatycznego wykrywania nowo podłączonych urządzeń sieciowych i ich podłączenia do sieci podkładowej (underlay) wraz z konfiguracją urządzeń;

10.15. Jednolite i zunifikowane rozwiązanie dla sieci kampusowej przewodowej oraz bezprzewodowej tj. możliwość tworzenia Network Fabric obejmującej zarówno sieć przewodową jak i bezprzewodową;

11. Pozostałe wymagania

11.1. System musi być dostarczony jako klaster HA składający się minimum z trzech dedykowanych serwerów sieciowych appliance w wersji sprzętowej (fizycznej) umożliwiającej uzyskanie następujących wartości skalowalności:

11.1.1. zarządzanie i monitorowanie 2000 urządzeń sieciowych (przełączniki / routery) w tym dostarczanych modeli

11.1.2. zarządzanie i monitorowanie 6000 radiowych punktów dostępowych WiFi;

11.1.3. monitorowanie 40 000 klientów sieci.

11.2. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

12. Rozwiązanie musi być kompatybilne z posiadanym i użytkowanym przez Zamawiającego systemem kontroli dostępu Cisco ISE w min wersji 2.7.

H. **Kontroler WiFi – 2 sztuki**

1. Urządzenie musi umożliwiać centralną kontrolę punktów dostępu bezprzewodowego w tym:
    1.1. zarządzanie politykami bezpieczeństwa
    1.2. wykrywanie zagrożeń w sieci bezprzewodowej
    1.3. zarządzanie pasmem radiowym
    1.4. zarządzanie mobilnością
    1.5. zarządzanie jakością transmisji zgodnie z protokołem CAPWAP (RFC 5415)
2. Urządzenie musi obsługiwać 250 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia o kolejne 250 przez dodanie odpowiedniej licencji
3. Urządzenie musi być wyposażone w licencję na obsługę 145 AP wraz ze wsparciem producenta na okres 24 miesięcy .
4. Urządzenie musi posiadać min. 4 interfejsy 2.5G/1G oraz 2 interfejsy 1/10G (SFP/SFP+)
5. Urządzenie musi obsługiwać łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
6. Urządzenie musi zapewniać obsługę ruchu tunelowanego o przepustowości 5 Gbps
7. Urządzenie musi zapewnić obsługę 5000 klientów sieci bezprzewodowej
8. Urządzenie musi zapewnić zarządzanie pasmem radiowym punktów dostępowych poprzez:
    8.1. automatyczną adaptacja do zmian w czasie rzeczywistym
    8.2. optymalizację mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
    8.3. dynamiczne przydzielanie kanałów radiowych
    8.4. wykrywanie, eliminacja i unikanie interferencji
    8.5. równoważenie obciążenia punktów dostępowych
    8.6. tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
    8.7. automatyczną dystrybucja klientów pomiędzy punkty dostępowe
    8.8. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
    8.9. dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
9. Urządzenie musi umożliwiać mapowanie SSID do segmentów VLAN w sieci przewodowej:
    9.1. 1:1
    9.2. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
    9.3. możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
10. Wymagania w zakresie obsługi sieci kratowych. Urządzenie musi zapewniać::
    10.1. komunikację między punktami dostępowymi bez medium kablowego
    10.2. separację trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)
    10.3. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)
    10.4. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
    10.5. autoryzację punktów dostępowych w oparciu o certyfikaty, adresy MAC

11. Urządzenie musi zapewniać obsługę mechanizmów bezpieczeństwa:
    - 11.1. 802.11i, WPA3, WPA2, WPA
    - 11.2. 802.1x z EAP (min. PEAP, EAP-TLS, EAP-FAST)
    - 11.3. obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
    - 11.4. kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
    - 11.5. obsługa profilowania użytkowników:
        - 11.5.1. przydział sieci VLAN
        - 11.5.2. przydział list kontroli dostępu (ACL)
    - 11.6. uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w
    - 11.7. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty
    - 11.8. obsługa list kontroli dostępu (ACL)
    - 11.9. obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X
    - 11.10. wykrywanie i dezaktywacja obcych punktów dostępowych
    - 11.11. ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników
    - 11.12. DHCP proxy
    - 11.13. zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową:
        - 11.13.1. kryptograficzne podpisywanie obrazów oprogramowania
        - 11.13.2. bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych
        - 11.13.3. wbudowany moduł sprzętowy unikalnie identyfikujący urządzenie i jego pochodzenie
12. Obsługa ruchu unicast IPv4 i IPv6
13. Obsługa ruchu multicast IPv4 i IPv6
    - 13.1. IGMP / MLD snooping
    - 13.2. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)
    - 13.3. obsługa konwersji ruchu multicast do unicast
14. Obsługa mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami)
15. Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k
16. Wsparcie dla IEEE 802.11u
17. Obsługa mechanizmów QoS
    - 17.1. 802.1p
    - 17.2. WMM, TSpec, U-APSD
    - 17.3. ograniczanie pasma per użytkownik
    - 17.4. Call Admission Control, SIP CAC, Call Snooping
18. Obsługa sensorów symulujących pracę klientów bezprzewodowych, które pozwalają na badanie działania wybranych usług w sieci (DNS, DHCP, RADIUS, IMAP, Outlook Web Access, inne) i eksportują wyniki testów do dedykowanego zewnętrznego kolektora
19. Obsługa dostępu gościnnego (IPv4 i IPv6)
    - 19.1. przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony)

19.2. przekierowanie użytkowników do strony logowania na zewnętrznym serwerze

20. Współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych
21. Obsługa NTP wersji 4 (IPv4 oraz IPv6)
22. Możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania
23. Obsługa Hotspot 2.0
24. Obsługa redundancji rozwiązania (N+1)
25. Obsługa redundancji 1:1 (active/standby) zapewniającej:
    25.1. utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera
    25.2. synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej
26. Dedykowany interfejs 1GE typu RJ45 służący do połączenia dwóch kontrolerów w redundantną parę 1:1
27. Analiza ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu; rozpoznawanie ponad 1000 aplikacji
28. Zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow
29. Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak: VLAN, polityka QoS, lista kontroli dostępu, czas trwania sesji
30. Obsługa protokołu Bonjour poprzez wbudowany mDNS Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów
    30.1. zarządzanie przez HTTPS, SNMP, SSH, NETCONF, port konsoli szeregowej
31. Wbudowana baza najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem
32. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

I. **Radiowy punkt dostępowy WiFi (AP) – 145 sztuk**

1. Urządzenie musi zapewniać obsługę standardów 802.11a/b/g/n/ac/ax
    1.1. obsługa OFDMA (uplink/downlink), TWT, BSS Coloring
    1.2. obsługa MU-MIMO (uplink/downlink) – min. 8x8:8
    1.3. obsługa kanałów 20, 40 MHz dla 802.11n
    1.4. obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax
    1.5. obsługa prędkości PHY do 3,47 Gbps (ac)
    1.6. obsługa prędkości PHY do 5,38 Gbps (ax)
    1.7. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
    1.8. obsługa beamforming dla klientów 802.11a/g/n/ac/ax
    1.9. obsługa MRC (Maximal Ratio Combining)
2. Urządzenie musi osiadać konfigurowalną moc nadajnika
    2.1. dla zakresu 2.4 GHz: do 100 mW
    2.2. dla zakresu 5GHz: do 400 mW
3. Urządzenie musi praca dwuzakresowo w pasmach: 2,4 GHz oraz 5 GHz
4. Urządzenie musi posiadać możliwość zmiany trybu pracy modułów radiowych (ustawienie konfiguracyjne):

4.1. tryb dwóch modułów radiowych: jeden pracujący w paśmie 2,4GHz (4x4), drugi pracujący w paśmie 5GHz (4x4)

4.2. tryb trzech modułów radiowych: jeden pracujący w paśmie 2,4GHz (4x4), drugi pracujący w paśmie 5GHz (4x4), trzeci pracujący w paśmie 5GHz (4x4) niezależnie od modułu drugiego na innym kanale w celu wytworzenia komórki mikro i makro

5. Urządzenie musi zapewniać zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:

5.1. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN

5.2. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)

5.3. obsługa min. 16 BSSID

5.4. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID

5.5. uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w

5.6. obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)

5.7. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników

5.8. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6

5.9. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)

5.10. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h

5.11. obsługa IPv6

5.12. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r

5.13. obsługa mechanizmów QoS:

5.13.1. ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik

5.13.2. obsługa WMM, TSPEC, U-APSD

5.14. wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM

5.15. obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting

5.16. wsparcie IEEE 802.11i, WPA3, WPA2, WPA

5.17. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)

5.18. obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS

5.19. obsługa blokowania ruchu Peer-to-Peer

5.20. obsługa polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) za pomocą mechanizmu out-of-band, który przekazuje za pośrednictwem kontrolera do AP mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa

5.21. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)

5.22. obsługa aWIPS (Adaptive Wireless Intrusion Prevention System) polegająca na wykryciu i remediacji zagrożenia. AP będący częścią systemu WIPS pozwala na określenie min. następujących informacji: sygnatura ataku, rodzaj wykrytej anomalii i jej opis, czas zdarzenia

5.22.1. wykrywanie sygnatur DoS: Auth/Deauth Flood, Assoc/Disassoc Flood, CTS/RTS Flood, Broadcast Deauth/Dissassoc Flood, Broadcast Probe Flood, EAPOL Logoff Flood

5.22.2. wykrywanie ataków: EAPOL-Logoff, RTS/CTS Virtual Carrier Sense

5.23. obsługa polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) umożliwiająca dynamiczne nadanie znacznika (w wyniku autoryzacji użytkownika/stacji) przez AP lub kontroler

5.24. uruchamianie aplikacji w kontenerach bezpośrednio na AP

5.25. obsługa VXLAN

6. Urządzenie musi posiadać możliwość pracy jako kontroler sieci bezprzewodowej o następujących funkcjonalnościach: (zmiana trybu pracy -przez wgranie oprogramowania) musi być bezkosztowa w okresie trwania kontraktu serwisowego):

6.1. obsługa do 100 punktów dostępowych

6.2. obsługa do 2000 klientów

6.3. możliwość konfiguracji do 16 sieci bezprzewodowych

6.4. centralna optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)

6.5. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r

6.6. obsługa mechanizmów wsparcia roamingu – IEEE 802.11k, IEEE 802.11v, OKC

6.7. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)

6.8. konfiguracja polityk bezpieczeństwa per SSID

6.9. obsługa WPA2 i WPA3 Personal oraz Enterprise

6.10. współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)

6.11. tworzenie list kontroli dostępu opartych o adresy IPv4 (IPv4 ACL) oraz o nazwy domenowe (DNS ACL)

6.12. obsługa URL Whitelist

6.13. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)

6.14. dwukierunkowe limitowanie transmisji (bidirectional rate-limiting ruchu) per klient, per WLAN

6.15. profilowanie (rozpoznawanie typów) urządzeń podłączających się do sieci bezprzewodowej

6.16. obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC)

6.17. obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym

6.18. obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta

6.19. obsługa protokołu Bonjour poprzez wbudowany mDNS (multicast DNS) Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów

6.20. zarządzanie przez HTTPS

6.21. wsparcie SSH, SNMP, NTP, SYSLOG

6.22. obsługa aktualizacji oprogramowania przez TFTP, SFTP

6.23. wbudowany serwer DHCP

6.24. wbudowany mechanizm redundancji automatycznie wybierający kontroler zapasowy wśród grupy obsługiwanych punktów dostępowych mogących pełnić funkcję kontrolera

7. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:

7.1. sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia

7.2. bezpieczna sekwencja uruchamiania

7.3. sprawdzenie autentyczności urządzenia

8. Interfejs MultiGigabit Ethernet (100/1000/2500/5000) zgodny z IEEE 802.3bz
9. Interfejs konsoli RJ45
10. Port USB 2.0
11. 2 GB RAM, 1 GB Flash
12. Urządzenie musi posiadać zróżnicowane możliwości zasilania:

12.1. pełna funkcjonalność AP przy zasilaniu przez 802.3bt, pobór mocy do 30,5W

12.2. pełna funkcjonalność AP, ale bez obsługi portu USB, przy zasilaniu przez 802.3at

12.3. możliwość uruchomienia AP z wykorzystaniem 802.3af z ograniczonymi funkcjami (min.: redukcja pracy układu radiowego)

13. Anteny zintegrowane o zysku min. 4 dBi dla pasma 2,4 GHz oraz min. 6 dBi dla pasma 5 GHz
14. Obudowa przystosowana do pracy w zakresie temperatur 0 – 50oC
15. Diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji
16. Certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi6, Wi-Fi Enhanced Open, WMM, WMM-PS
17. Wbudowane radio Bluetooth Low Energy (BLE) 5.0
18. IoT ready (Zigbee, Thread)
19. Urządzenie musi być wyposażone w licencję subskrypcyjną na wymagane funkcjonalności, gwarancję oraz wsparcie producenta na okres 24 miesięcy.

J. **W ramach zamówienia Sprzedawca dostarczy licencje do posiadanego i użytkowanego przez Zamawiającego systemu Cisco ISE w wersji 2.7.0.356 na okres 24 miesięcy umożliwiające zestawienie jednocześnie 2000 sesji. Dostarczone licencje muszą dawać możliwość wykorzystania wszystkich opisanych w dokumentach przedmiotowego zamówienia funkcjonalności w zakresie SDA.**

K. **Świadczenie w okresie 24 miesięcy od dnia podpisania Protokołu odbioru Wdrożenia usług wsparcia w ramach puli godzin inżynierskich (konsultacji) w wymiarze maksymalnie 300 (trzysta) roboczogodzin, w ramach których Sprzedawca wykonywał będzie prace związane z konfiguracją wdrożonej sieci kampusowej oraz rozbudową i zmianami konfiguracyjnymi Oprogramowania zgodnie z oczekiwaniami Zamawiającego.**

L. **W przypadku zaproponowania rozwiązania opartego o producenta Cisco w ramach Umowy Sprzedawca przeprowadzi certyfikowane dwa pięciodniowe warsztaty dla administratorów (6 osób) ARiMR z zakresu:**

1) Cisco SD-Access Workshop v1.3 (CSDAWORK):

- Protokoły LISP oraz VXLAN
- Od data-plane learning do control-plane learning
  - Bezpieczeństwo oparte na grupach: Security Group Tag (SGT) i Group-Based Policy (GBP)
  - Elementy campus fabric
  - Protokół LISP jako control plane
  - Protokół VXLAN jako data plane
  - Integracja typu OTT (Over The Top)
  - Fabric-enabled WLAN
  - Konfiguracja sieci wirtualnych (VN)
  - Polityki bezpieczeństwa: Scalable Group
  - Integracja typu OTT (Over The Top)
  - Fabric-enabled WLAN
  - Konfigurcja węzłów brzegowych

- Konfiguracja usług wspólnych
- Cisco ISE jako centrum polityk bezpieczeństwa

2) Cisco Catalyst 9800-CL Wireless LAN Controller and WIFI6 Workshop (C9800WIFI6) :

- Podstawowe funkcje i cechy kontrolera bezprzewodowego
- Konfiguracja początkowa WLC, uruchomienie i połączenie z radiowymi punktami dostępu
- Konfigurowanie zabezpieczenia dostępu klienta do sieci WLAN zgodnie ze standardem WPA3
- Podstawowa architektura WLAN
- Wdrożenie centralnej bezprzewodowej sieci LAN z kontrolerami
- Wdrażanie AP w trybie Local, Flexconnect
- Konfigurowanie autentykacji użytkowników (local/central/LWA/CWA) oraz przełączania ich ramek (local/central)
- Podstawowa konserwacja sieci WLAN i rozwiązywanie problemów
- Koncepcje tworzenia kopii zapasowych i odzyskiwania konfiguracji
- Aktualizacje oprogramowania
- Wrażanie nowego standardu WiFi 6 (802.11ax) oraz jego porównanie ze starszymi standardami (802.11abgn / ac)
- Funkcje i cechy WiFi 6 (OFDMA, MU-MIMO, TWT, 1024-QAM, IoT)

W przypadku zastosowania technologii innego producenta Sprzedawca przeprowadzi odpowiednie certyfikowane warsztaty właściwe dla danego producenta zgodne z zakresem przedstawionym powyżej.
Sprzedawca zapewni uczestnikom warsztatów certyfikaty/zaświadczenia potwierdzające uczestnictwo w warsztatach. Podczas warsztatów w każdym dniu warsztatów sporządzona zostanie lista obecności.

Załącznik nr 1A do Umowy nr _____/DI/___1/2610

Etapy realizacji Umowy

I. **W ramach Etapu I**

1) Sprzedawca opracuje i dostarczy Projekt Techniczny, który musi zostać odebrany przez Kupującego przed rozpoczęciem prac wdrożeniowych wchodzących w zakres Etapu I. Projekt Techniczny musi obejmować zakres wszystkich Etapów Umowy oraz cechować się spójnością i koordynacją we wszystkich dziedzinach wiążących się z realizacją przedmiotu zamówienia oraz taką formą i szczegółowością, aby możliwe było dokonanie jej oceny przez Kupującego oraz musi zawierać opis konfiguracji komponentów wdrażanego Oprogramowania i opis integracji ze środowiskiem produkcyjnym Kupującego.
2) Sprzedawca dostarczy Sprzęt IT i Oprogramowanie o którym mowa w Załączniku nr 1 C do Umowy, w tabeli „Zestawienie ilościowe" pkt 1, pkt 3 oraz pkt 5 spełniający wymagania opisane w Załączniku nr 1 do Umowy.
3) Sprzedawca skonfiguruje i zainstaluje Sprzęt IT, Oprogramowanie wraz ze sprzętem (dedykowany serwer możliwy do zamontowania w szafie rack 19", posiadający wsparcie producenta Oprogramowania appliance) do monitorowania i zarządzania siecią LAN przełączników dostarczonych w ramach niniejszej umowy o których mowa w pkt 2) a jeżeli Sprzedawca zaoferuje spełnienie wymagań ocenianych w ramach kryterium oceny ofert dodatkowe parametry techniczne także przełączników posiadanych przez Kupującego Cisco Catalyst 2960X – 1025 sztuk oraz przełączników Cisco Catalyst 4500X – 32 sztuk.
4) Sprzedawca skonfiguruje i zainstaluje dwa przełączniki szkieletowe typ A (pracujące jako jeden przełącznik logiczny), 34 przełączniki dostępowe typ A i 36 przełączników dostępowych typ B, 2 przełączników dostępowych typ C. Przełączniki dostępowe będą pracowały w stosach, złożonych z przełączników dostępowych typu A i B, natomiast przełączniki typ C będą pełniły rolę wspomagającą podłączone do przełączników szkieletowych. W ramach prac Sprzedawca dokona migracji konfiguracji do docelowej architektury w oparciu o technologię SDA (Software-Defined Access - utworzenie (dystrybucja) vlanów oraz routingu, kanałów etherchannel pomiędzy przełącznikami szkieletowymi i dostępowymi, konfiguracja portów dostępowych przełączników dostępowych, konfiguracja uwierzytelniania urządzeń końcowych z Cisco ISE oraz AAA oraz dokona integracji z posiadanym systemem Cisco ISE, przeniesienie list dostępu ACL, synchronizacja NTP) z obecnie użytkowanych przełączników szkieletowych (Cisco 6509) i dostępowych (Cisco 2960X-48FPD-L) na dostarczony sprzęt, zdeinstaluje obecnie używane przełączniki szkieletowe i dostępowe oraz dokona przełączenia użytkowników końcowych. Sprzedawca skonfiguruje mechanizmy bezpieczeństwa oparte na grupach: Security Group Tag (SGT) i Group-Based Policy (GBP) Sprzedawca dostarczy niezbędne do wykonania instalacji patchcordy światłowodowe.
5) Sprzedawca dokona wgrania na serwery dostarczonych w ramach Etapu I Licencji, w tym dla posiadanego i użytkowanego przez Kupującego systemu CISCO ISE o którym mowa w Załączniku nr 1 C do Umowy, w tabeli „Zestawienie ilościowe" pkt 5.
6) Sprzedawca opracuje i dostarczy Plan Testów Akceptacyjnych zawierający scenariusze testów akceptacyjnych dla Etapu I.
7) Sprzedawca opracuje i dostarczy Dokumentację powykonawczą dla Etapu I.
8) Sprzedawca przeprowadzi warsztaty zgodnie z założeniami określonymi w lit. L Załącznika nr 1 do Umowy.

9) Sprzedawca dokona instruktażu z obsługi wdrożonego Sprzętu IT, czas trwania instruktażu wyniesie 5 Dni Roboczych i będzie przeprowadzony w wymiarze 6 godzin dziennie. W instruktażu po stronie Kupującego będzie uczestniczyć do 10 osób.

10) Instalacja Sprzętu IT oraz Oprogramowania nastąpi w Lokalizacji Warszawa i CPD.

II. W ramach Etapu II

1) Sprzedawca dostarczy Sprzęt IT o którym mowa w Załączniku nr 1 C do Umowy, w tabeli „Zestawienie ilościowe" pkt 2 spełniający wymagania opisane w Załączniku nr 1 do Umowy.

2) Sprzedawca skonfiguruje i zainstaluje dwa przełączniki szkieletowe typ B (pracujące jako jeden przełącznik logiczny). W ramach prac Sprzedawca dokona migracji konfiguracji (utworzenie (dystrybucja) vlanów oraz routingu, kanałów etherchannel pomiędzy przełącznikami szkieletowymi i dostępowymi, konfiguracja portów dostępowych przełączników dostępowych, konfiguracja uwierzytelniania urządzeń końcowych z Cisco ISE oraz AAA, przeniesienie list dostępu ACL, synchronizacja NTP) z obecnie użytkowanych przełączników szkieletowych (Cisco 6509) na dostarczony sprzęt, zdeinstaluje obecnie używane przełączniki szkieletowe oraz podłączy do dostarczonych przełączników szkieletowych dwa obecnie użytkowane stosy przełączników dostępowych (Cisco 2960X-48FPD-L). Sprzedawca dostarczy niezbędne do wykonania instalacji patchcordy światłowodowe.

3) Sprzedawca dokona wgrania na serwery dostarczonych w ramach Etapu II Licencji

4) Sprzedawca opracuje i dostarczy Plan Testów Akceptacyjnych zawierający scenariusze testów akceptacyjnych dla Etapu II.

5) Sprzedawca opracuje i dostarczy Dokumentację powykonawczą dla Etapu II.

6) Instalacja Sprzętu IT/ Oprogramowania odbędzie się w Lokalizacja Lublin.

III. W ramach Etapu III

1) Sprzedawca dostarczy Sprzęt IT o którym mowa w Załączniku nr 1 C do Umowy, w tabeli „Zestawienie ilościowe" pkt 4 lit. A, B oraz C spełniający wymagania opisane w Załączniku nr 1 do Umowy.

2) Sprzedawca dostarczy Sprzęt IT o którym mowa w Załączniku nr 1 C do Umowy, w tabeli „Zestawienie ilościowe" pkt 4 lit. D w ilości 50 szt. spełniający wymagania opisane w Załączniku nr 1 do Umowy.

3) Sprzedawca dokona wgrania na serwery dostarczonych w ramach Etapu III Licencji.

4) Sprzedawca wykona Wdrożenia Sieci Bezprzewodowej WIFI.

5) Sprzedawca skonfiguruje i zainstaluje dwa kontrolery sprzętowe sieci WiFi oraz 50 Radiowych Punktów Dostępowych WiFi. Kontrolery Sprzętowe i Punkty Dostępowe WiFi muszą zostać zintegrowane z dostarczaną w ramach postepowania i istniejącą infrastrukturą sieciową Zamawiającego z wykorzystaniem technologii SDA (prawidłowa współpraca z dostarczonymi przełącznikami szkieletowymi typ A i dostępowymi typu A i B oraz z system zarządzania Cisco ISE, wykorzystywanym w ARiMR). Punkty Dostępowe WiFi muszą być tak skonfigurowane, aby ruch od użytkowników końcowych przechodził bezpośrednio z Radiowego Punktu Dostępowego do przełącznika dostępowego, a nie przez Kontrolery Sprzętowe. Dostarczone rozwiązanie musi zapewniać możliwość dostępu do różnych segmentów (VLAN'ów) sieci LAN w lokalizacji Centrala Biuro, użytkownik musi mieć zapewniony roaming między punktami dostępu. Stacje robocze i użytkownicy w procesie logowania się do sieci muszą być prawidłowo uwierzytelniani z wykorzystaniem mechanizmów zaimplementowanych w systemie ISE (certyfikaty, konta domenowe, adresy MAC). Punkty dostępowe zostaną zainstalowane w płytach sufitu podwieszanego, wymagane będzie również wykonanie zabezpieczenia sprzętowego przed kradzieżą (linka mocowana do sufitu lub inne, podobne rozwiązanie). Miejsca instalacji Punktów Dostępowych WiFi zostaną wskazane przez Zamawiającego, na podstawie dokumentacji z przeprowadzonego badania pomieszczeń biurowych pod kątem ilości i miejsca instalacji urządzeń typu Access Point sieci bezprzewodowej WiFi 2,4 GHz oraz 5 GHz. Wdrożenie sieci (dotyczy lokalizacji Warszawa ul. Poleczki

33) w oparciu o SDA musi zapewnić realizację przewodowego i bezprzewodowego, bezpiecznego dostępu do wszystkich obecnych usług w centrali ARiMR, poprzez separację grup użytkowników i aplikacji dozwalając tylko na taki ruch sieciowy, który jest dozwolony w zdefiniowanej polityce bezpieczeństwa.

6) Sprzedawca opracuje i dostarczy Plan Testów Akceptacyjnych zawierający scenariusze testów akceptacyjnych dla Etapu III.
7) Sprzedawca opracuje i dostarczy Dokumentację powykonawczą dla Etapu III.
8) Instalacja Sprzętu IT/Oprogramowania odbędzie się w Lokalizacji Warszawa.

IV. W ramach Etapu IV

1) Dostawa Sprzętu IT o którym mowa w Załączniku nr 1 C do Umowy, w tabeli „Zestawienie ilościowe" pkt 4 lit. D w ilości 50 szt.
2) Sprzedawca skonfiguruje i zainstaluje 50 Radiowych Punktów Dostępowych WiFi. Punkty Dostępowe WiFi muszą zostać zintegrowane z dostarczaną w ramach postepowania i istniejącą infrastrukturą sieciową Zamawiającego z wykorzystaniem technologii SDA (Software-Defined Access) (prawidłowa współpraca z dostarczonymi przełącznikami szkieletowymi typ A i dostępowymi typu A i B oraz z system zarządzania Cisco ISE, wykorzystywanym w ARiMR). Punkty Dostępowe WiFi muszą być tak skonfigurowane, aby ruch od użytkowników końcowych przechodził bezpośrednio z Radiowego Punktu Dostępowego do przełącznika dostępowego, a nie przez Kontrolery Sprzętowe. Dostarczone rozwiązanie musi zapewniać możliwość dostępu do różnych segmentów (VLAN'ów) sieci LAN w lokalizacji Centrala Biuro, użytkownik musi mieć zapewniony roaming między punktami dostępu. Stacje robocze i użytkownicy w procesie logowania się do sieci muszą być prawidłowo uwierzytelniani z wykorzystaniem mechanizmów zaimplementowanych w systemie ISE (certyfikaty, konta domenowe, adresy MAC). Punkty dostępowe zostaną zainstalowane w płytach sufitu podwieszanego, wymagane będzie również wykonanie zabezpieczenia sprzętowego przed kradzieżą (linka mocowana do sufitu lub inne, podobne rozwiązanie). Miejsca instalacji Punktów Dostępowych WiFi zostaną wskazane przez Zamawiającego, na podstawie dokumentacji z przeprowadzonego badania pomieszczeń biurowych pod kątem ilości i miejsca instalacji urządzeń typu Access Point sieci bezprzewodowej WiFi 2,4 GHz oraz 5 GHz. Wdrożenie sieci (dotyczy lokalizacji Warszawa ul. Poleczki 33) w oparciu o SDA musi zapewnić realizację przewodowego i bezprzewodowego, bezpiecznego dostępu do wszystkich obecnych usług w centrali ARiMR, poprzez separację grup użytkowników i aplikacji dozwalając tylko na taki ruch sieciowy, który jest dozwolony w zdefiniowanej polityce bezpieczeństwa.
3) Sprzedawca opracuje i dostarczy Plan Testów Akceptacyjnych zawierający scenariusze testów akceptacyjnych dla Etapu IV.
4) Sprzedawca opracuje i dostarczy Dokumentację powykonawczą dla Etapu IV.
5) Instalacja Sprzętu IT/Oprogramowania odbędzie się w Lokalizacji Warszawa

V. W ramach Etapu V

1) Sprzedawca dostarczy Sprzęt IT o którym mowa w Załączniku nr 1 C do Umowy, w tabeli „Zestawienie ilościowe" pkt 4 lit. D w ilości 45 szt.
2) Sprzedawca skonfiguruje i zainstaluje 45 Radiowych Punktów Dostępowych WiFi. Punkty Dostępowe WiFi muszą zostać zintegrowane z dostarczaną w ramach postepowania i istniejącą infrastrukturą sieciową Zamawiającego z wykorzystaniem technologii SDA (prawidłowa współpraca z dostarczonymi przełącznikami szkieletowymi typ A i dostępowymi typu A i B oraz z system zarządzania Cisco ISE, wykorzystywanym w ARiMR). Punkty Dostępowe WiFi muszą być tak skonfigurowane, aby ruch od użytkowników końcowych przechodził bezpośrednio z Radiowego Punktu Dostępowego do przełącznika dostępowego, a nie przez Kontrolery Sprzętowe. Dostarczone rozwiązanie musi zapewniać możliwość dostępu do różnych segmentów (VLAN'ów) sieci LAN w lokalizacji Centrala Biuro, użytkownik

musi mieć zapewniony roaming między punktami dostępu. Stacje robocze i użytkownicy w procesie logowania się do sieci muszą być prawidłowo uwierzytelniani z wykorzystaniem mechanizmów zaimplementowanych w systemie ISE (certyfikaty, konta domenowe, adresy MAC). Punkty dostępowe zostaną zainstalowane w płytach sufitu podwieszanego, wymagane będzie również wykonanie zabezpieczenia sprzętowego przed kradzieżą (linka mocowana do sufitu lub inne, podobne rozwiązanie). Miejsca instalacji Punktów Dostępowych WiFi zostaną wskazane przez Zamawiającego, na podstawie dokumentacji z przeprowadzonego badania pomieszczeń biurowych pod kątem ilości i miejsca instalacji urządzeń typu Access Point sieci bezprzewodowej WiFi 2,4 GHz oraz 5 GHz. Wdrożenie sieci (dotyczy lokalizacji Warszawa ul. Poleczki 33) w oparciu o SDA musi zapewnić realizację przewodowego i bezprzewodowego, bezpiecznego dostępu do wszystkich obecnych usług w centrali ARiMR, poprzez separację grup użytkowników i aplikacji dozwalając tylko na taki ruch sieciowy, który jest dozwolony w zdefiniowanej polityce bezpieczeństwa.

3) Sprzedawca opracuje i dostarczy Plan Testów Akceptacyjnych zawierający scenariusze testów akceptacyjnych dla Etapów V.
4) Sprzedawca opracuje i dostarczy Dokumentację powykonawczą dla Etapu V.
5) Instalacja Sprzętu IT/Oprogramowania odbędzie się w Lokalizacji Warszawa.

Załącznik nr 1B do Umowy nr _____/DI/__/2610

[UWAGA: *załącznik zostanie wprowadzony do treści umowy, jeżeli Sprzedawca zaoferuje spełnienie wymagań ocenianych w ramach kryterium oceny ofert dodatkowe parametry techniczne*]

Dodatkowe cechy rozwiązania:

V. Przełączniki szkieletowe i dostępowe:

Lp.	Część	Wymaganie
1	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C	Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
2	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C, Przełączniki szkieletowe Typ A i B	Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
3	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C	Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow). Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych
4	Przełącznik dostępowy typ A (z portami uplink), przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C, Przełączniki szkieletowe typ A i B	Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników: • Statycznie w oparciu o port do którego podłączona jest stacja, • Statycznie w oparciu o VLAN, w którym pracuje stacja, • Statycznie w oparciu o adres IP stacji, • Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X; Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu, Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa,
5	Przełączniki szkieletowe typ A i typ B	Obsługa standardu IEEE 802.1ae (MACSec) szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,
6	Przełącznik szkieletowy typ A	Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o

		pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi 98 000. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych.
7	Przełącznik szkieletowy typ B	Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi 98 000. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych.
8	Przełączniki szkieletowe typ A i typ B	Eksport dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)
9	Przełączniki szkieletowe typ A i typ B	Wbudowany analizator pakietów umożliwiamy zbieranie ruchu w czasie rzeczywistym, dekodowanie ruchu i zapisywanie ich w formie pliku .pcap lub do pamięci urządzenia (flash, zewnętrzne usb). Wynik dekodowania ruchu może zostać wyświetlony na konsoli urządzenia lub w zewnętrznym oprogramowaniu typu Wireshark.
10	Przełączniki szkieletowe typ A i typ B	Możliwość uruchamiania zdefiniowanych w Pythonie skryptów bezpośrednio na urządzeniu
11	Przełączniki szkieletowe typ A i typ B	Obsługa mechanizmów wysokiej dostępności, takich jak możliwość wgrania łatki oprogramowania bez restartu urządzenia (hot patching). W przypadku kontrolerów sieci bezprzewodowej WiFi obsługa aktualizacji oprogramowania w formie ISSU (in-Service Software upgrade) na parze kontrolerów
12	Przełączniki szkieletowe typ A i typ B	Urządzenie umożliwia uruchamianie dodatkowych aplikacji w kontenerach Docker
13	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C, Przełączniki szkieletowe Typ A i B	Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego
14	Przełącznik dostępowy typ A (z portami uplink), Przełącznik dostępowy typ B (bez portów uplink), Przełącznik dostępowy typ C, Przełączniki szkieletowe Typ A i B	Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą

VI. <u>System zarządzania i monitorowania siecią:</u>

5. Integracja systemu monitoringu z obecnie wykorzystywanym systemem kontroli Cisco ISE przy pomocy szyny wymiany danych

PxGRID, wymiana informacji na temat uwierzytelnienia użytkowników podłączonych do sieci w lokalizacji Warszawa oraz pozostałych lokalizacjach gdzie wykorzystywane jest uwierzytelnianie.

6. Wyznaczenie na postawie analizy danych telemetrycznych dla każdego z urządzeń sieciowych, grupy użytkowników, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji indeksu liczbowego określającego jakość pracy danego monitorowanego obiektu wraz z wizualizacją na skali czasu zmiany wartości indeksów jakości pracy dla grup urządzeń sieciowych, grupy użytkowników przewodowych i bezprzewodowych, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji;

7. Dla danego problemu, podanie opisu problemu, dostarczenie informacji kontekstowej umożliwiającej identyfikację i rozwiązanie problemu, określenie lokalizacji, urządzeń oraz użytkowników dotkniętych problemem, propozycja sugerowanych działań umożliwiających rozwiązanie problemu wraz z możliwością dostępu do urządzeń sieciowych w celu natychmiastowego dostarczenia danych diagnostycznych;

8. Funkcjonalności monitorowania poprzez zaoferowany system zarządzania dodatkowych urządzeń posiadanych przez Kupującego (wymienionych poniżej):

- przełączników Cisco Catalyst 2960X – 1025 sztuk

- przełączników Cisco Catalyst 4500X – 32 sztuk

1. Monitoring dostępności urządzenia sieciowego
2. Wizualizacja urządzenia na mapie topologii sieci wraz połączeniami oraz wizualizacją stanu pracy urządzenia;
3. Zebranie i prezentacja następujących informacji o urządzeniu: model urządzenia, wersja systemu operacyjnego, adres IP, stan pracy, osiągalność, lokalizacja geograficzna, numer seryjny, czas pracy od ostatniego wyłączenia,
4. Odczyt konfiguracji urządzenia
5. Zarządzanie wersjami oprogramowania z możliwością wskazania wersji obowiązujących dla danego urządzenia
6. Możliwość bezpośredniego z poziomu konsoli graficznej systemu zarządzania i monitorowania dostępu do konsoli urządzenia lub narzędzia umożliwiającego zdalne wydawanie komend na urządzeniu;
7. Szczegółowe informacje o urządzeniu obejmujące:
a. Wykres czasowy utylizacji CPU;
b. Wykres czasowy utylizacji pamięci;
c. Wykres czasowy dostępności urządzenia;
d. Wykres czasowy temperatury urządzenia;
e. Informacje o poszczególnych interfejsach urządzeń w uwzględnieniem: stanu interfejsu, typu, prędkość linku, FDX/HDX;
8. Dla każdego z monitorowanych interfejsów informacje o:
a. Wykres czasowy dostępności interfejsu;
b. Wykres czasowy utylizacji interfejsu niezależnie w kierunku nadawczym i odbiorczym;
c. Wykres czasowy poziomu błędów niezależnie w kierunku nadawczym i odbiorczym;

VII. <u>Kontroler WiFi:</u>

- możliwość eksportu dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)
- obsługa mechanizmów wysokiej dostępności, takich jak możliwość wgrania łatki oprogramowania bez restartu koncentratora (hot patching), restartu danego procesu, odseparowania systemów operacyjnych punktów dostępowych od systemu kontrolera, sekwencyjnego uaktualniania oprogramowania punktów dostępowych (rolling upgrades)
- zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow
- obsługa wbudowanego interpretera języka PYTHON
- obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020)

VIII. <u>Radiowy punkt dostępowy:</u>

4. zintegrowany z radiowym punktem dostępowym:
5. moduł analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz):
   f) dokładność analizy (kwant próbkowania) max. 100 kHz
   g) obsługa kanału o szerokości 160MHz
   h) zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych
   i) automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.)
   j) współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego,
6. dedykowany moduł radiowy realizujący skanowanie pod kątem zagrożeń w sieci bezprzewodowej (wIPS) oraz w celach poprawy lokalizacji urządzeń bezprzewodowych pracujący off-channel w pasmach 2,4 oraz 5GHz.

Załącznik nr 1C do Umowy nr _____/DI/__/2610

Zestawienie ilościowe

Pkt/ lit.	Nazwa	Ilość
1.	Sprzęt sieciowy do realizacji sieci LAN dla Lokalizacji Warszawa	
A.	Przełącznik dostępowy typ A (z portami uplink 25G)	34
B.	Przełącznik dostępowy typ B (bez portów uplink)	36
C.	Przełącznik dostępowy typ C	2
D	Kabel do łączenia w stos do przełączników dostępowych typ A i B o dł. 1m	6
E.	Kabel do łączenia w stos do przełączników dostępowych typ A i B o dł. 3m	24
F.	Kabel do łączenia w stos zasilający do przełączników dostępowych typ A i B o dł. 1.5m	24
G	Przełącznik szkieletowy typ A	2
H	Moduł optyczny interfejsowy SFP28 typu 10/25Gigabit Ethernet 10/25GBASE-CSR do przełączników szkieletowych typ A	36
I.	Moduł optyczny interfejsowy SFP28 typu 10/25Gigabit Ethernet 10/25GBASE-CSR do przełączników dostępowych typ A	36
J.	Kabel połączeniowy typu twinax 40G 3m do przełączników szkieletowych typ A	4
K.	Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ A i przełączników dostępowych typ C	4
L.	Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ A	4
M	Moduł optyczny SFP+ typu 10G jednomodowy LR do przełączników szkieletowych typ A	4
2.	Sprzęt sieciowy do realizacji sieci LAN CORE w Lokalizacji Lublin	
A.	Przełącznik szkieletowy typ B	2
B.	Moduł optyczny interfejsowy SFP typu 10GBASE-LRM do przełączników szkieletowych typ B	10
C.	Moduł optyczny interfejsowy SFP typu 10GBASE-SR do przełączników szkieletowych typ B	10
D	Kabel połączeniowy typu twinax 10G 3m do przełączników szkieletowych typ B	4

3.	Oprogramowanie **(wraz z dedykowanym serwerem montowanym w szafie rack 19" - appliance, posiadający wsparcie producenta Oprogramowania)** monitorowania i zarządzania siecią LAN	
A.	System zarządzania i monitorowania siecią w lokalizacji Warszawa oraz monitoringu sieci LAN w pozostałych lokalizacjach Zamawiającego	1
4.	Sieć bezprzewodowa WiFi w lokalizacji Warszawa	
A.	Kontroler sprzętowy WiFi	2
B.	Kabel połączeniowy typu twinax 10G 7m do kontrolerów sprzętowych WiFi	4
C.	Moduł optyczny SFP+ z oferty producenta urządzenia 10GBase-SR	8
D	Radiowe punkty dostępowe WiFi	145
5.	**Licencje do posiadanego i użytkowanego przez Kupującego systemu Cisco ISE w wersji 2.7.0.356 na okres 24 miesięcy umożliwiające zestawienie jednocześnie 2000 sesji.**	1 komplet
6.	Świadczenie w okresie 24 miesięcy od dnia podpisania Protokołu odbioru Wdrożenia usług wsparcia w ramach puli godzin inżynierskich (konsultacji) w wymiarze maksymalnie 300 (trzysta) roboczogodzin, w ramach których Sprzedawca wykonywał będzie prace związane z konfiguracją wdrożonej sieci kampusowej oraz rozbudową i zmianami konfiguracyjnymi oprogramowania zgodnie z oczekiwaniami Zamawiającego	
7.	Certyfikowane dwa pięciodniowe warsztaty dla administratorów (6 osób) ARiMR z zakresu SDA oraz WiFi	

Załącznik nr 1D do Umowy nr_____/DI/__/2610

Wymagania w zakresie Dokumentacji

1. **Projekt Techniczny musi** cechować się:
   a) spójnością i koordynacją we wszystkich dziedzinach wiążących się z realizacją przedmiotu zamówienia oraz taką formą i szczegółowością, która umożliwi Kupującemu weryfikację dokumentu.
   b) odzwierciedleniem architektury i wszystkich funkcji przewidzianych do realizowania przez administratorów i użytkowników,kompletnym i szczegółowym opisem przyjętych rozwiązań funkcjonalnych wraz z informacjami o parametrach i sposobie konfiguracji, konstrukcyjnych, użytkowych i sprzętowych oraz z wyspecyfikowaniem asortymentowym i ilościowym wszystkich elementów składowych i oprogramowania,
   c) określeniem zasad i planu instalacji oraz Wdrożenia.
   d) Projekt techniczny musi obejmować zakresem wszystkie Etapy realizacji Umowy.
2. Plan Testów Akceptacyjnych musi zawierać scenariusze testów akceptacyjnych oraz spełniać następujące wymagania:
   a) opisać w sposób wyczerpujący wszystkie możliwe przypadki użycia,
   b) dla każdego scenariusza testowego wskazywać na oczekiwane wyniki testu stanowiące warunek pozytywnego zakończenia danego testu,
   c) określać harmonogram testów oraz wskazać na warunki i osoby niezbędne do przeprowadzenia testów, w tym personel Kupującego.
   d) Sprzedawca przygotuje Plan Testów Akceptacyjnych dla każdego z Etapów.
3. Dokumentacja powykonawcza zawierać będzie co najmniej:
   a) opis zainstalowanego (rejestr konfiguracji) Sprzętu IT, Oprogramowania wraz z informacjami o parametrach i sposobie konfiguracji,
   b) instrukcje obsługi Sprzętu IT i Oprogramowania,
   c) wskazanie punktów krytycznych i zagrożeń mających wpływ na niezawodne działanie Oprogramowania.
   d) Sprzedawca przygotuje Dokumentację powykonawczą dla każdego z Etapów.

Załącznik nr 2 do Umowy nr _____/DI/___/2610

Protokół odbioru Etapu I/II/III/IV/V*
(wzór)

Zgodnie z Umową nr ...../DI/___/2610 zawartą w dniu ..... r. pomiędzy Agencją Restrukturyzacji i Modernizacji Rolnictwa (Kupujący) a ....., Kupujący potwierdza, że Sprzedawca dostarczył Sprzęt IT/Oprogramowanie, Dokumenty i wykonał Wdrożenie Etapu .... zgodnie z Umową:

Lp.	Nazwa Sprzętu IT/Oprogramowania/Dokumentu	Liczba	Numer seryjny/wersja**

Upoważnieni przedstawiciele Kupującego i Sprzedawcy złożonymi pod niniejszym protokołem podpisami zgodnie oświadczają, że:

1. Dostarczony Sprzęt IT wraz z Oprogramowaniem jest fabrycznie nowy i nie nosi śladów uszkodzeń zewnętrznych oraz uprzedniego używania. Ilość oraz rodzaj dostarczonego Sprzętu IT wraz z Oprogramowaniem jest zgodny z Umową.
2. Dostarczony Sprzęt IT oraz Oprogramowanie są wolne od oprogramowania szkodliwego i szpiegującego, a także są zabezpieczone przed nieautoryzowanym dostępem.
3. Wraz ze Sprzętem IT dostarczono wszystkie wymagane Dokumenty (instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT oraz dokumenty licencyjne dla Oprogramowania).
4. Dokonano usunięcia i utylizacji wszelkich opakowań pozostałych po rozpakowaniu Sprzętu IT.
5. Dostarczono wymaganą w ramach Etapu Dokumentację.
6. Wykonano Wdrożenie prawidłowo, zgodnie z Umową.

Uwagi i zastrzeżenia:

Kupujący (upoważniony przedstawiciel)			**Sprzedawca** (upoważniony przedstawiciel)
.....			.....
.....			.....

....., dnia ..... roku

* - niepotrzebne skreślić

** - dopuszcza, żeby wykaz dostarczonego Sprzętu IT/Oprogramowania/Dokumentów stanowił załącznik do przedmiotowego Protokołu

Załącznik nr 2 A do Umowy nr _____/DI/___/2610

Protokół odbioru Wdrożenia
(wzór)

Zgodnie z Umową nr ...../DI/___/2610 zawartą w dniu ..... r. pomiędzy Agencją Restrukturyzacji i Modernizacji Rolnictwa (Kupujący) a .....(Sprzedawca), Kupujący potwierdza, że Sprzedawca dostarczył Sprzęt IT/Oprogramowanie, Dokumenty i wykonał Wdrożenie Etapów I-V zgodnie z Umową.

Kupujący (upoważniony przedstawiciel)			**Sprzedawca** (upoważniony przedstawiciel)
.....			.....
.....			.....
....., dnia ..... roku			

* - niepotrzebne skreślić

Załącznik nr 3 do Umowy nr _____/DI/___/2610

Protokół odbioru Projektu Technicznego /Dokumentacji powykonawczej/Planu Testów Akceptacyjnych
(wzór)

Dane dokumentu

Nazwa dokumentu + **Lokalizacja** **Kierownik Sprzedawcy:**	**Numer wersji dokumentu:** **Data wersji dokumentu:**

UWAGI:

1. .....
2. .....
3. .....
4. .....
5. .....
6. .....
7. .....

Kupujący odbiera / nie odbiera*
Projekt Techniczny / Dokumentację powykonawczą/Plan Testów Akceptacyjnych *

Kupujący (upoważniony przedstawiciel)		**Sprzedawca** (upoważniony przedstawiciel)	
Imię i nazwisko:		**Imię i nazwisko:**	
Stanowisko:		**Stanowisko:**	
Data:		**Data:**	
Podpis:		**Podpis:**	

Załącznik nr 4 do Umowy nr _____/DI/___/2610

Protokół odbioru usunięcia wady
(wzór)

1. Imiona i nazwiska osób dokonujących czynności odbioru:

2. Wyszczególnienie odbieranych czynności w ramach usuniętych wad:

3. Data podpisania protokołu: ..... r.

4. Podpisy

.....	.....
Kupujący	Sprzedawca
(upoważniony przedstawiciel)	(upoważniony przedstawiciel)

Załącznik nr 4a do umowy nr _____/DI/____/2610

Protokół odbioru konsultacji
(wzór)

1. Opis konsultacji w kwartale _____

   _____
   _____
   _____

2. Ilość wykorzystanych godzin _____

3. Uwagi/zastrzeżenia

   _____
   _____

4. Podpisy

Sprzedawca	**Kupujący**
(upoważniony przedstawiciel)	*(upoważniony przedstawiciel)*
.....	.....
.....	.....

Warszawa, dnia _____ r.

Załącznik nr 5 do Umowy nr _____/DI/____/2610

Treść Załączników nr 5, 6 i 12 do Zarządzenia Prezesa ARiMR nr 78/2019
z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR
(stanowią odrębny plik)

Załącznik nr 6a do umowy nr _____/DI/___/2610

Klauzula informacyjna w zakresie przetwarzania danych osobowych[1]

W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1; Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO", Kupujący informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II nr 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. b i c RODO w zw. z art. 431 i nast. ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.), tj. w celu zawarcia oraz wykonania niniejszej umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176 z późn. zm.),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych zostanie każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych zostanie przedłużony o okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia, prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych oraz prawo do przenoszenia danych, w przypadkach określonych w RODO.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia umowy.

[1] Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych drugiej strony umowy będącej osobą fizyczną.

Załącznik nr 6b do Umowy nr _____/DI/___/2610

Klauzula informacyjna w zakresie przetwarzania danych osobowych[2]

W związku z treścią z art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO", Kupujący informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w zw. z art. 431 i nast. ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.) w zw. z art. 98 i nast. ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2020 r. poz. 1740 z późn. zm.) oraz w zw. z ustawą z 15 września 2000 r. Kodeks spółek handlowych (Dz. U. z 2020 r. poz. 1526 z późn. zm.), tj. w celu zawarcia oraz wykonania niniejszej umowy.
4. Administrator będzie przetwarzał następujące kategorie Pani/Pana danych: dane identyfikacyjne oraz dane kontaktowe.
5. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176 z późn. zm.),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
6. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych zostanie każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych zostanie przedłużony o okres 5 lat, na potrzeby archiwizacji.
7. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
8. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
9. Pani/Pana dane Administrator uzyskał od ..... *

*należy wskazać źródło pozyskania danych [np. firmę przedsiębiorcy, od którego Administrator pozyskał dane].

[2] Niniejsza klauzula znajdzie zastosowanie w przypadku pośredniego pozyskania danych: pełnomocników, prokurenta oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego.

Załącznik nr 6c do Umowy nr _____/DI/___/2610

Klauzula informacyjna w zakresie przetwarzania danych osobowych[3]

W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO", Kupujący informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w zw. z art. 431 i nast. ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.) w zw. z art. 98 i nast. ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2020 r. poz. 1740 z późn. zm.) oraz w zw. z ustawą z 15 września 2000 r. Kodeks spółek handlowych (Dz. U. z 2020 r. poz. 1526 z późn. zm.), tj. w celu zawarcia oraz wykonania niniejszej umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176 z późn. zm.),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych zostanie każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych zostanie przedłużony o okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia umowy.

[3] Niniejsza klauzula znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych: pełnomocnika, prokurenta oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego.

Załącznik nr 6d do Umowy nr _____/DI/___/2610

Klauzula informacyjna w zakresie przetwarzania danych osobowych[4]

W związku z treścią z art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO", Kupujący informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w zw. z art. 431 i nast. ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.), tj. w celu zawarcia oraz wykonania niniejszej umowy.
4. Administrator będzie przetwarzał następujące kategorie Pani/Pana danych: dane identyfikacyjne, dane kontaktowe oraz dane związane z zatrudnieniem.
5. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176 z późn. zm.),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
6. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych zostanie każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych zostanie przedłużony o okres 5 lat, na potrzeby archiwizacji.
7. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
8. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
9. Pani/Pana dane Administrator uzyskał od ..... *

*należy wskazać źródło pozyskania danych [np. firmę przedsiębiorcy, od którego Administrator pozyskał dane].

[4] Niniejsza klauzula dotyczy osób, których dane Administrator pozyskuje w sposób pośredni, w szczególności podwykonawców, pracowników podwykonawców, osób wyznaczonych do kontaktów roboczych oraz odpowiedzialnych za koordynację i realizację umowy.

Załącznik nr 7 do Umowy nr _____/DI/___/2610

Formularz ofertowy

Załącznik nr 9 do SWZ – plik, w formacie XML, wygenerowany z narzędzia ESPD

Plik, w formacie XML, wygenerowany z narzędzia ESPD („*ESPD*") znajduje się w odrębnym pliku o nazwie „Załącznik nr 9 do SWZ_ESPD". Plik należy pobrać i zapisać na dysk komputera oraz wypełnić przy pomocy narzędzia udostępnionego przez Urząd Zamówień Publicznych pod adresem https://espd.uzp.gov.pl.

Po uruchomieniu wyżej wymienionej strony internetowej Urzędu, należy wybrać „pl Polski", a w dalszej kolejności zaznaczyć „Jestem wykonawcą". Następnie należy zaimportować „ESPD" wczytując plik w formacie XML będący Załącznikiem nr 9 do SWZ. Po sporządzeniu oświadczenia w formie jednolitego europejskiego dokumentu zamówienia („*JEDZ*") należy je podpisać przez osobę lub osoby uprawnione.

Aktualne na dzień składania ofert oświadczenie w formie JEDZ należy złożyć w formie elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym, za pomocą środka komunikacji elektronicznej, tj. Platformę Zakupową.
Szczegółowy zakres wymagań określony został w Rozdz. IV.2 SWZ.