Poznań, 5.09.2025 r.

Zapytanie ofertowe
5/2025

Zamawiający:

Roltec sp. z o.o.
Ul. Św. Marcin 29/8
Poznań, 61-806
NIP: 8952026494

Roltec sp. z o.o.
Ul. Św. Marcin 29/8, 61-806 Poznań
NIP: 8952026494, REGON: 022321514
realizując projekt:
„Budowa inteligentnej fabryki cienkowarstwowych paneli fotowoltaicznych wraz z inwestycją w technologie cyfryzacji i automatyzacji procesów produkcyjno-zarządczych w oparciu o koncepcję Przemysłu 4.0."

w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO),
Komponent A „Odporność i konkurencyjność gospodarki",
Cel szczegółowy: *A2. Rozwój narodowego systemu innowacji: wzmocnienie koordynacji, stymulowanie potencjału innowacyjnego oraz współpracy pomiędzy przedsiębiorstwami i organizacjami badawczymi, w tym w zakresie technologii środowiskowych*
Reforma: A2.1. *Przyśpieszenie procesów robotyzacji i cyfryzacji i innowacji*
Inwestycja: *A2.1.1. Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach*

ZAPRASZA DO SKŁADANIA OFERT

Zapytanie ofertowe prowadzone jest na podstawie zasady konkurencyjności w ramach inwestycji A 2.1.1, o której mowa w załączniku nr 10 do Umowy o objęcie wsparciem bezzwrotnym z planu rozwojowego.

I. Informacje o Projekcie

Celem Projektu, w ramach którego ogłaszane jest niniejsze Zapytanie ofertowe, jest wybudowanie na terenie Wrocławia pierwszej w Polsce fabryki cienkowarstwowych paneli fotowoltaicznych (w technologii CIGS), w której możliwe będzie uruchomienie automatycznej i zintegrowanej linii technologicznej wg. technologii opracowanej przez Wnioskodawcę, umożliwiającej wysokowydajną produkcję ogniw fotowoltaicznych CIGS. W ramach przedsięwzięcia zostanie przeprowadzona inwestycja wybudowania zakładu dostosowanego i umożliwiającego wdrożenie kompleksowych rozwiązań z zakresu cyfryzacji oraz technologii Przemysłu 4.0, które pozwolą w pełni zautomatyzować proces produkcji (m.in poprzez komunikację Machine to Machine), wykorzystać AI do zarządzania procesami biznesowymi, zintegrować procesy biznesowe (zarządcze, operacyjne, pomocnicze) oraz zapewnić wymagany poziom bezpieczeństwa w ramach systemu zarządzania budynkiem.

Powierzchnia zabudowy hali produkcyjnej fabryki to ponad 13,8 tysiąca m^2. Powierzchnia ta będzie podzielona na tj. linię produkcyjną, magazyn, część socjalną i aneks technologiczny. Infrastruktura fabryki ma zapewnić produkcję cienkowarstwowych paneli fotowoltaicznych o szacowanej wielkości ok. 333 tysięcy sztuk pojedynczych modułów PV w skali roku. Szacowane jest, że w fabryce będzie pracować około 220 osób, odpowiedzialnych za realizację zadań, które ma wspierać sieć LAN, będąca przedmiotem niniejszego Zapytania.

II. Przedmiot zamówienia:

Przedmiotem zapytania ofertowego jest dostawa, montaż i instalacja sieci LAN – 1 komplet, niezbędnej do osiągnięcia celów Projektu. Przedmiot zamówienia obejmuje dostawę infrastruktury (sieć LAN) obejmującej następujące części:

1. CORE + DC
2. WAN + FireWall
3. WiFi
4. Przełączniki LAN
5. Zestawienie wkładek SFP/SFP+

Zamawiający nie dopuszcza składania ofert częściowych. Zamawiający wskazuje, że z powodów organizacyjnych, technicznych i ekonomicznych przedmiot zamówienia tworzy nierozerwalną całość. Przedmiotem zamówienia są przedmioty mające stanowić integralną sieć LAN, spełniającą wymagania techniczne określone w treści Zapytania ofertowego. Z tego powodu Zamawiający wskazuje, że dostarczone przedmioty mają być ze sobą kompatybilne i zostaną zamontowane i zainstalowane w budowanej fabryce na terenie Wrocławia jako infrastruktura sieci LAN – 1 komplet.
Podział zamówienia na części generowałby niemożliwe do ograniczenia ryzyko niekompatybilności, braku integracji i nieprawidłowego funkcjonowania infrastruktury, co podważałoby możliwość osiągnięcia gospodarczego celu zamówienia. Zamawiający wymaga, aby jeden wykonawca odpowiadał za dostawę, montaż i instalację sieci LAN, jak również za wykonywanie świadczeń z tytułu gwarancji oraz rękojmi.

Zamawiający nie dopuszcza dostawy przedmiotu zamówienia, które nie są dopuszczone do obrotu na obszarze Unii Europejskiej.

Cel zamówienia

Celem jest dostawa, montaż i instalacja sieci LAN – 1 komplet, obejmującej:

1. CORE + DC
2. WAN + FireWall
3. WiFI
4. Przełączniki LAN
5. Zestawienie wkładek SFP/SFP+

Przedmiotem zamówienia są przedmioty mające stanowić integralną sieć LAN, która będzie częścią infrastruktury w budowanej fabryce cienkowarstwowych paneli fotowoltaicznych (w technologii CIGS).

Kody CPV:

32420000-3 – Urządzenia sieciowe
48200000-0 - Pakiety oprogramowania dla sieci, internetu i intranetu
48821000-9 - Serwery sieciowe
48822000-6 - Serwery komputerowe
48900000-7 - Różne pakiety oprogramowania i systemy komputerowe

Szczegółowy opis przedmiotu zamówienia:

Szczegółowy opis przedmiotu zamówienia znajduje się w tabeli poniżej i jest zgodny z wnioskiem o dofinansowanie projektu: „Budowa inteligentnej fabryki cienkowarstwowych paneli fotowoltaicznych wraz z inwestycją w technologie cyfryzacji i automatyzacji procesów produkcyjno-zarządczych w oparciu o koncepcję Przemysłu 4.0."

Szczegółowy opis przedmiotu zamówienia		
L.p	**Oznaczenie przedmiotu zamówienia**	**Wymagane minimalne parametry techniczne:**
		Sieć LAN – 1 komplet:
1	CORE + DC	Przełącznik CORE L3 wyposażony w 48-port x 1/10/25G + 4-port 40/100G, dwa zasilacze – 2 szt.
		Minimalne wymagania techniczne i funkcjonalne urządzenia: ▪ Przełącznik typu standalone wyposażony w 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz 4 porty uplink 40/100 Gigabit Ethernet QSFP, ▪ Porty SFP/SFP+/SFP28 umożliwiają zastosowanie następujących wkładek interfejsowych: o Gigabit Ethernet 1000Base-T, o Gigabit Ethernet 1000Base-SX, o Gigabit Ethernet 1000Base-LX/LH, o Gigabit Ethernet 1000Base-EX, o Gigabit Ethernet 1000Base-ZX, o Gigabit Ethernet 1000Base-BX-D/U, o 10Gigabit Ethernet 10GBase-SR, o 10Gigabit Ethernet 10GBase-LR, o 10Gigabit Ethernet 10GBase-ER, o 10Gigabit Ethernet 10GBase-ZR, o 10Gigabit Ethernet 10GBase-BX-D/U, o 10Gigabit Ethernet typu twinax (SFP+ - SFP+), o 25Gigabit Ethernet 25GBASE-SR, o 25Gigabit Ethernet typu twinax (SFP28 – SFP28), o 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),10/25Gigabit Ethernet 10/25GBASE-LR (SMF); ▪ Porty QSFP umożliwiają zastosowanie następujących modułów interfejsowych: Dla transmisji 40Gb/s: o 40G-SR4, o 40G-LR4, o 40G-ER4, o 40G-SR-BD, o 40G-CSR, o 40G-CSR4,40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652), o adapter 40G QSFP->10G SFP+, o 40Gigabit Ethernet typu twinax (QSFP - QSFP); Dla transmisji 100Gb/s: o 100GBASE-SR4, o 100GBASE-LR4,100Gigabit Ethernet typu twinax (QSFP - QSFP); **Architektura:** ▪ Urządzenie wyposażone w wymienne moduły wentylatorów, ▪ Urządzenie posiadające możliwość wyposażenia w zasilacz redundantny do pracy w trybie 1:1. Wykonawca nie ma obowiązku dostarczenia zasilacza. **Wydajność:** ▪ Urządzenie posiadające min. 32MB bufor pamięci, ▪ 16GB pamięci DRAM i 16GB pamięci flash, ▪ Przepustowość przełącznika (switching capacity) wynosi min. 3.2 Tbps, ▪ Prędkość przesyłania (forwarding rate) wynosi 1 miliard pps (1Bpps), Obsługa min: ▪ 1000 aktywnych sieci VLAN, ▪ 80 000 adresów MAC, ▪ 212 000 tras IPv4, ▪ 212 000 tras IPv6, ▪ Ilość wpisów w listach kontroli dostępu Security ACL – 27 000, ▪ ilość wpisów w listach kontroli dostępu QoS ACL – 16 000, ▪ 1000 interfejsów SVI L3, ▪ Jumbo frame 9198B,

- 128 połączeń zagregowanych typu „port channel”,
- 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP;

Oprogramowanie/funkcjonalność:

- Obsługa protokołu NTP,
- Obsługa IGMPv1/2/3,
- 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 zagregowane L2 i L3,
- System operacyjny przełącznika umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,
- System operacyjny przełącznika konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwiający eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów,
- Wsparcie dla protokołu RESTCONF,
- Możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia,
- Przełącznik realizujący następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
  - IEEE 802.1w Rapid Spanning Tree,
  - Per-VLAN Rapid Spanning Tree (PVRST+),
  - IEEE 802.1s Multi-Instance Spanning Tree,
  - Obsługa 1000 instancji protokołu STP;
- Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED,
  - Realizacja funkcji 802.1Q tunneling (QinQ)
- Funkcja serwera DHCP,
- Obsługa 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwiający zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
- Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
- Obsługa list kontroli dostępu (ACL) następujących typów:
  - Port ACL umożliwiający kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
  - VLAN ACL umożliwiający kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
  - Routed ACL umożliwiający kontrolę ruchu routowanego pomiędzy sieciami VLAN,
  - Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
- Przełącznik realizujący następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:
  - 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
  - Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,
  - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
  - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
  - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
  - Kontrola sztormów dla ruchu broadcast/multicast/unicast,
  - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
- Przełącznik posiada wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
- 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),
- Urządzenie realizujące routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:
  - Routing statyczny dla IPv4 i IPv6,
  - Routing dynamiczny dla IPv4: BGP, ISIS,
  - Routing dynamiczny dla IPv4: OSPF, EIGRP (rfc7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA),
  - Routing dynamiczny dla IPv6: OSPFv3,
  - Funkcjonalności Policy-based routing,
  - multicast routing (PIM-SM, PIM-SSM) ,
  - Obsługa protokołu redundancji bramy (VRRP) z obsługą 255 grup,
  - Obsługa 200 tuneli GRE (Generic Routing Encapsulation),
  - Obsługa 1000 wirtualnych instancji routingu (VRF),
- Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,
- Realizacja funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji,
- Urządzenie realizujące protokół LISP zgodnie z RFC 6830,
- Urządzenie umożliwiające enkapsulację ruchu przy pomocy VXLAN’ów,
- Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine / border,
- Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,

- Urządzenie przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze będą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,
- Klastrowanie wspierające funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami,
- Przełącznik umożliwiający 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,
- 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),
- 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,
- Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
- Wbudowany analizator pakietów,
- 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,
- Urządzenie umożliwiające uruchamianie dodatkowych aplikacji w kontenerach Docker,
- Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku M2 SATA o pojemności 240/480/960GB,
- 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,

Funkcjonalności z zakresu MPLS:

- Urządzenie realizuje następujące funkcjonalności z zakresu MPLS:
  - L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC,
  - L2VPN - Virtual Private LAN Services (VPLS) - obsługa 1000 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji,
  - L3 VPN - MPLS Virtual Private Network (VPN),
  - Multicast VPN (MVPN);
  - Inter AS Option A i B,
  - EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS),
  - MPLS over GRE,

Zarządzanie i konfiguracja:

- Urządzenie realizujące sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosząca 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,
- Urządzenie posiadające dedykowany port Ethernet do zarządzania out-of-band,
- 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,
- Urządzenie posiadające port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
- Urządzenie wyposażone w port konsoli USB,
- Urządzenie umożliwiające tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
- Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
- Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia,
- Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
- Funkcja 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,

Obudowa:

		▪ Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU. Głębokość chassis urządzenia z wentylatorami, i zasilaczami mniejsza niż 50 cm, **Wyposażenie urządzenia** ▪ Przełącznik wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy, ▪ Urządzenie wyposażone w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat. ▪ Urządzenie wyposażone jest w dodatkowy, 4-punktowy system mocujący do szafy rack
		Przełącznik DC wyposażony w 48p 1/10/25G, 6p 40/100G, dwa zasilacze – 4 szt.
		Minimalne wymagania techniczne i funkcjonalne urządzenia: **Przełącznik musi posiadać:** ▪ Min. 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+/SFP28 ▪ Min. 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiadający możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m). **Parametry wydajnościowe:** ▪ Prędkość przełączania 1.8Tbps full duplex ▪ Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 **Przełącznik posiadający następującą funkcjonalność dla warstwy L2:** ▪ Trunking IEEE 802.1Q VLAN; ▪ Wsparcie dla 3000 sieci VLAN; ▪ Wsparcie sprzętowe dla 90 tysięcy adresów MAC ▪ IEEE 802.1w Rapid Spanning Tree (RST) ▪ IEEE 802.1s Multiple Spanning Tree (MST) ▪ Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU) ▪ Internet Group Management Protocol (IGMP) Versions 2, 3; ▪ Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach ▪ Link Aggregation Control Protocol (LACP): IEEE 802.3ad ▪ Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów); ▪ Funkcjonalność izolowania portów znajdujących się w tym samym VLAN **Przełącznik posiadający następującą funkcjonalność dla warstwy L3:** ▪ Sprzętowe przełączanie pakietów w warstwie L3 ▪ Routing w oparciu o trasy statyczne ▪ Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. ▪ Policy Based Routing (PBR) ▪ VRRP ▪ Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6 ▪ Wsparcie sprzętowe dla minimum 750 tyś prefixów LPM/ wpisów hosta w tablicy routingu IP ▪ Wsparcie dla min. 32 VRF ▪ Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP) ▪ Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast) ▪ Wsparcie dla IGMPv3 oraz MSDP ▪ Wsparcie sprzętowe dla minimum 32,000 tras multicastowych ▪ Obsługa minimum 5000 wpisów dla ACL (access control list) **Przełącznik wspierający następujące mechanizmy związane z funkcjonalnością VXLAN:** ▪ Zintegrowany, sprzętowy VXLAN Bridging/Routing ▪ Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) ▪ Implementacja VXLAN BGP EVPN (Ethernet VPN) ▪ Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN) **Przełącznik wspierający następujące mechanizmy związane z zapewnieniem jakości usług w sieci:** ▪ Layer 2 IEEE 802.1p (CoS) oraz DSCP ▪ Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6) ▪ Kolejkowanie bezwzględne (strict-priority) ▪ Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection) ▪ Ograniczanie ruchu (policing) do zadanej przepływności ▪ Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych

- Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
- Protokół RDMA/RoCE oraz ECN

Przełącznik wspierający następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:

- Obsługa list kontroli dostępu (ACL)
  - ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
  - ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
  - ACL oparte o porty (PACL);
- DHCP Snooping
- ARP Inspection
- IP Source Guard
- Unicast reverse path forwarding (uRPF)
- Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast

Przełącznik wspierający następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:

- Port zarządzający 100/1000 Mbps;
- Port konsoli CLI;
- Zarządzanie In-band;
- SSHv2;
- Authentication, authorization, and accounting (AAA);
- RADIUS;
- TACACS+
- Syslog;
- SNMP v1, v2c, v3;
- Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. <1s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB.
- Role-Based Access Control RBAC;
- IEEE 802.1ab LLDP
- Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
- 802.1x
- Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
- Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)
- Network Time Protocol (NTP);
- Precision Time Protocol IEEE 1588
- Diagnostyka procesu BOOT;
- Ping
- Traceroute
- Netflow

Narzędzia programowania i zarządzania przełącznikiem:

- Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
- Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika
- Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika.
- Interfejs programistyczny REST API wraz z upublicznionym SDK
- Możliwość zainstalowania klienta Chef
- Możliwość zainstalowania agenta Puppet

Inne wymagania techniczne:

- Przełącznik wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych;
- Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
- Urządzenie umożliwiające pracę samodzielną (realizując opisane powyżej funkcjonalności).

Wyposażenie przełącznika obejmuje:

- wkładki QSFP 100/40GE umożliwiające połączenie 100GE lub 40GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional)
- wkładki SFP+ typu 10GBASE-SR

		▪ Kable DAC twinax 25G 3 metrowe (pasywne)
2.	WAN + FireWall	Router brzegowy do agregacji łączy internetowych 200M(Aggr,400M) – 2 szt.

Minimalne wymagania techniczne i funkcjonalne urządzenia:

Typ i liczba portów:

- Router wyposażony jest w 6 aktywnych interfejsów 1 GE L3 (4 interfejsy miedziane 1GE RJ45 oraz 2 interfejsy 1GE w standardzie SFP);
- Router wyposażony jest w port USB typ A oraz USB typ C;
- Router wyposażony jest w port konsolowy RJ45 oraz micro USB;

Sloty na moduły rozszerzeń:

- Router wyposażony w jeden dedykowany slot przeznaczony do instalacji modułów łączności radiowej w standardzie 4G/5G SA;
- Router wyposażony w jeden slot przeznaczony do instalacji modułów następujących typów:
  - Moduł wyposażony w 1 port 2.5/1Gbps RJ-45 WAN (L3) wraz z realizacją 90W Poe 802.3;
  - Moduł wyposażony w 2 porty 100Mbps/1Gbps dual-mode RJ45/SFP WAN (L3) wraz z realizacją szyfrowanie na warstwie L2 modelu ISO/OSI (MACSEC IEEE 802.1AE);
  - Moduł przełącznika LAN z 4 portami 1GE;
  - Moduł przełącznika LAN z 8 portami 1GE;
  - Moduł przełącznika LAN z 8 portami 1GE oraz z realizacją PoE 802.3 af/at;
  - Moduł wyposażony w 2 porty telefonii analogowej FXO;
  - Moduł wyposażony w 4 porty telefonii analogowej FXO;
  - Moduł wyposażony w 2 porty telefonii analogowej FXS służące do podłączenie telefonów analogowych;
  - Moduł wyposażony w 4 porty telefonii analogowej FXS służące do podłączenie telefonów analogowych;
  - Moduł wyposażony w 2 porty telefonii analogowej FXO oraz 4 porty telefonii analogowej FXS służące do podłączenie telefonów analogowych;
  - Moduł wyposażony w 2 porty telefonii cyfrowej BRI (NT/TE);
  - Moduł wyposażony w 4 porty telefonii cyfrowej BRI (NT/TE);
  - Moduł wyposażony w układy DSP z obsługą 32 kanałów głosowych;
  - Moduł wyposażony w układy DSP z obsługą 64 kanałów głosowych;
  - Moduł wyposażony w układy DSP z obsługą 128 kanałów głosowych;
  - Moduł wyposażony w układy DSP z obsługą 256 kanałów głosowych;
  - Moduł wyposażony w 1 port uniwersalny T1/E1 do zastosowań jako port telefonii cyfrowej lub port transmisji danych typu „clear channel”;
  - Moduł wyposażony w 2 porty uniwersalne T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych;
  - Moduł wyposażony w 4 porty uniwersalne T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych;
  - Moduł wyposażony w 8 portów uniwersalnych T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych;
  - Moduł wyposażony w port VDSL2/ADSL/2/2+ Annex A;
  - Moduł wyposażony w port VDSL2/ADSL/2/2+ Annex B;
  - Moduł wyposażony w port VDSL2/ADSL/2/2+ Annex M;
  - Moduł wyposażony w 1 port uniwersalny T1/E1 do zastosowań jako port telefonii cyfrowej lub port transmisji danych typu „channelized”;
  - Moduł wyposażony w 2 porty uniwersalne T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych typu „channelized”;
  - Moduł wyposażony w 8 portów uniwersalnych T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych typu „channelized”;
  - Moduł wyposażony w 2 porty do transmisji danych WAN ISDN BRI;
  - Moduł wyposażony w 4 porty do transmisji danych WAN ISDN BRI;
  - Moduł wyposażony w 1 port WAN szeregowej transmisji danych;
  - Moduł wyposażony w 2 porty WAN szeregowej transmisji danych;
  - Moduł wyposażony w 4 porty WAN szeregowej transmisji danych;
  - Moduł umożliwiający uzyskanie 16 asynchronicznych portów szeregowych;
  - Moduł umożliwiający uzyskanie 24 asynchronicznych portów szeregowych;

- Router wyposażony w jeden slot przeznaczony do instalacji modułów następujących typów:
  - Moduł wyposażony w 12 portów telefonii analogowej FXO oraz 8 portów telefonii analogowej FXS służące do podłączenia telefonów analogowych;
  - Moduł wyposażony w 2 porty telefonii analogowej FXO oraz 16 portów telefonii analogowej FXS służące do podłączenia telefonów analogowych;
  - Moduł wyposażony w 4 porty telefonii analogowej FXO oraz 24 portów telefonii analogowej FXS służące do podłączenia telefonów analogowych;
  - Moduł wyposażony w układy DSP z obsługą 768 kanałów głosowych;
  - Moduł wyposażony w układy DSP z obsługą 1024 kanałów głosowych;
  - Moduł wyposażony w układy DSP z obsługą 2048 kanałów głosowych;
  - Moduł wyposażony w układy DSP z obsługą 3080 kanałów głosowych;

- Moduł przełącznika sieciowego wyposażonego w 20 portów 1GE RJ45 oraz 2 porty 10GE SFP+;
- Moduł adaptera umożliwiający instalacje dwóch modułów spośród modułów następujących typów:
  - Moduł wyposażony w 1 port 2.5/1Gbps RJ-45 WAN (L3) wraz z realizacją 90W Poe 802.3;
  - Moduł wyposażony w 2 porty 100Mbps/1Gbps dual-mode RJ45/SFP WAN (L3) wraz z realizacją szyfrowania na warstwie L2 modelu ISO/OSI (MACSEC IEEE 802.1AE);
  - Moduł przełącznika LAN z 4 portami 1GE;
  - Moduł przełącznika LAN z 8 portami 1GE;
  - Moduł przełącznika LAN z 8 portami 1GE oraz z realizacją PoE 802.3 af/at;
  - Moduł wyposażony w 2 porty telefonii analogowej FXO;
  - Moduł wyposażony w 4 porty telefonii analogowej FXO;
  - Moduł wyposażony w 2 porty telefonii analogowej FXS służące do podłączenie telefonów analogowych;
  - Moduł wyposażony w 4 porty telefonii analogowej FXS służące do podłączenie telefonów analogowych;
  - Moduł wyposażony w 2 porty telefonii analogowej FXO oraz 4 porty telefonii analogowej FXS służące do podłączenie telefonów analogowych;
  - Moduł wyposażony w 2 porty telefonii cyfrowej BRI (NT/TE);
  - Moduł wyposażony w 4 porty telefonii cyfrowej BRI (NT/TE);
  - Moduł wyposażony w 1 port uniwersalny T1/E1 do zastosowań jako port telefonii cyfrowej lub port transmisji danych typu „clear channel”;
  - Moduł wyposażony w 2 porty uniwersalne T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych;
  - Moduł wyposażony w 4 porty uniwersalne T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych;
  - Moduł wyposażony w 8 portów uniwersalnych T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych;
  - Moduł wyposażony w port VDSL2/ADSL/2/2+ Annex A;
  - Moduł wyposażony w port VDSL2/ADSL/2/2+ Annex B;
  - Moduł wyposażony w port VDSL2/ADSL/2/2+ Annex M;
  - Moduł wyposażony w 1 port uniwersalny T1/E1 do zastosowań jako port telefonii cyfrowej lub port transmisji danych typu „channelized”;
  - Moduł wyposażony w 2 porty uniwersalne T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych typu „channelized”;
  - Moduł wyposażony w 8 portów uniwersalnych T1/E1 do zastosowań jako porty telefonii cyfrowej lub porty transmisji danych typu „channelized”;
  - Moduł wyposażony w 2 porty do transmisji danych WAN ISDN BRI;
  - Moduł wyposażony w 4 porty do transmisji danych WAN ISDN BRI;
  - Moduł wyposażony w 1 port WAN szeregowej transmisji danych;
  - Moduł wyposażony w 2 porty WAN szeregowej transmisji danych;
  - Moduł wyposażony w 4 porty WAN szeregowej transmisji danych;
  - Moduł umożliwiający uzyskanie 16 asynchronicznych portów szeregowych;
  - Moduł umożliwiający uzyskanie 24 asynchronicznych portów szeregowych;

Typ i wykonanie urządzenia, parametry fizyczne:

- Router o rozmiarze 1RU przystosowany jest do montażu w szafie rack 19”, posiada obudowę wykonaną z metalu oraz niezbędne uchwyty;
- Router wyposażony w identyfikator RFID;
- Router posiadający 8 GB pamięci RAM, którą można rozszerzyć do 32GB;
- Router wyposażony w 8GB wbudowanej pamięci FLASH;
- Router wyposażony w dodatkowe 16 GB pamięci M.2 USB do przechowywania obrazów systemu operacyjnego, konfiguracji oraz logów systemowych, którą można rozbudować do 32GB M.2 USB oraz do 600GB M.2 NVMe SSD;
- Router posiadający redundantne zasilacze przystosowane do zasilania prądem naprzemiennym 230V;
- Router pobierający maksymalnie 250W;
- Router posiadający komponent sprzętowy zawierający certyfikat X.509v3 oraz łańcuch zaufania, pozwalający realizować bezpieczne uwierzytelnienie urządzenia – w tym również proces automatycznego i bezpiecznie uwierzytelnionego dodania urządzenia do sieci bez konieczności wpisywania haseł jednorazowych, ani logowania się do urządzenia za pomocą sieci bezprzewodowej, czy linii poleceń;
- Urządzenie posiadające następujące certyfikacje: Common Criteria, Evaluation Assurance (EAL), FIPS 140-2 Level 1;
- Router posiadający redundantne wentylatory, które w przypadku awarii można wymienić nie wyłączając routera;
- Router pracujący w zakresie temperatury od 0 do 40°C;

Parametry wydajnościowe – minimalne wymagania:

- 1600000 prefiksów w tablicach routingu IPv4/IPv6 i umożliwiający rozszerzenie do 4000000 prefiksów IPv4/IPv6 poprzez zwiększenie pamięci RAM do 32GB;
- Wydajność 19.7 Gbps dla sumarycznego ruchu IPv4 dla pakietów o długości 1400B;
- Wydajność 1.9 Gbps dla sumarycznego ruchu IPv4 dla pakietów o długości 1400B szyfrowanych protokołem IPSec;
- Wydajność SD-WAN 1.8 Gbps dla sumarycznego ruchu IPv4 dla ruchu IMIX (dla pakietów o średniej długości 352

bajtów) szyfrowanych protokołem IPSec;
- Wydajność 1.9 Gbps dla sumarycznego ruchu IPv4 dla IPv4 dla ruchu IMIX (dla pakietów o średniej długości 352 bajtów) szyfrowanych protokołem IPSec;
- Obsługa 4000 tuneli szyfrowanych IPSec;
- Obsługa 4000 instancji VRF (Virtual Route Forwarding);
- Obsługa 4000 ACL (Access Control Lists) oraz 72 000 wpisów ACE (Access Control Entries);
- Obsługa QoS z 8 000 kolejkami oraz 4000 polityk per system;
- Obsługa 1200000 sesji NAT, które można rozszerzyć do 2000000 poprzez zwiększenie pamięci RAM do 32GB;
- Obsługa 512000 sesji firewalla;

Funkcjonalności urządzenia:
- Routing dynamiczny: RIP, OSPF, EIGRP, IS-IS, BGP dla protokołów IPv4 i IPv6;
- Obsługa PPP, Multi-link PPP, PPP over Ethernet (PPPoE);
- Obsługa Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC) oraz obsługa interfejsów szeregowych WAN (RS-232, RS-449, X.21, V.35);
- Obsługa BFD, GRE, VLAN, PBR, NetFlow, IPFIX, NTP;
- Funkcjonalność BFD posiadająca wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego oraz HSRP;
- Obsługa routingu między sieciami VLAN w oparciu o trunking 802.1Q;
- Obsługa LACP, PAgP, EtherChannel, LLDP;
- Realizacja ochrony warstwy zarządzającej (Control Plane Policing - CoPP);
- Obsługa ruchu multicastowego, realizacja protokołów: PIM Sparse/Dense, PIM-SSM, IGMPv3; Bi-Di PIM, MLD (v1, v2), MSDP;
- Obsługa Unicast Reverse Path Forwarding (uRPF);
- Zarzadzanie poprzez: CLI (SSHv2, port konsoli), graficzny interfejs webowy (GUI) oraz programistyczny interfejs (API);
- Obsługa: SNMPv3, serwer NTP, serwer DHCP (serwer i klient),
- Wsparcie dla systemów AAA (RADIUS, TACACS+);
- Realizacja uwierzytelniania w standardzie IEEE 802.1X;
- Obsługa list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL;
- Obsługa NAT dla ruchu IP unicast oraz PAT dla ruchu IP unicast;
- Możliwość tworzenia klas ruchu oraz oznaczanie (marking), klasyfikowanie i obsługę ruchu (policing, Shaping) w oparciu o klasę ruchu;
- Obsługa mechanizmów kolejkowania ruchu:
  - z obsługą kolejki absolutnego priorytetu;
  - ze statyczną alokacją pasma dla typu ruchu;
  - WFQ;
- Obsługa mechanizmu WRED;
- Obsługa Traffic Shaping;
- Obsługa mechanizmu ograniczania pasma dla określonego typu ruchu (policing);
- Obsluga HQoS;
- Obsługa tunelowania GRE wraz z zapewnienieniem mechnizmu honorowania IP Precendence dla ruchu tunelowanego;
- Obsługa tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP);
- Obsluga NetFlow oraz Flexible NetFlow (FnF);
- Obsługa wirtualnych instancji routingu (VRF);
- Obsługa 802.1P;
- Obsługa NETCONF/YANG, RESTCONF, GNMI, gRPC;
- Realizacja funkcji:
  - Zapory ogniowej (zone-based firewall);
  - IPS;
- Szyfrowanie ruchu przy pomocy IPSec z wykorzystaniem:
  - Szyfrowania za pomocą AES-256 w trybie CBC lub GCM, Internet Key Exchange (IKE);
  - Mechanizmów autentykacji RSA (1024/2048 bitów) lub ECDSA (256/384 bitów);
- Realizacja szyfrowania WAN MACSec (125-/256-bit) dla wbudowanych portów 1G oraz portów znajdujących się na modułach rozszerzeń wspierających funkcje MACSEC;
- Wsparcie dla sieci VPN w technologii:
  - DMVPN (Obsługa dynamicznego zestawianie VPN z wykorzystaniem protokołu NHRP w relacji spoke to spoke w celu optymalizacji transmisji danych pomiędzy oddziałami);
  - GET VPN (bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast);
  - FlexVPN;
- Funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia „tam i z powrotem" (roundtrip), jitter i utraty pakietów);
- Funkcjonalność bramki IP-to-IP dla ruchu głosowego;
- Funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (tzw. Embedded Event Manager – EEM);
- Funkcjonalność EEM pozwala na monitorowanie zdarzenia związanego z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych;

		▪ Funkcjonalność EEM pozwala na generowanie akcji: o Wykonanie komendy z poziomu linii poleceń urządzenia; o Wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej; o Wykonanie skryptu; o Wygenerowanie SNMP trap; o Ustawienie lub modyfikacja określonego licznika systemowego; ▪ Urządzenie posiadające możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do Urządzenia i uruchomiona; ▪ Funkcja wyszukiwania oraz filtrowania fragmentów konfiguracji z linii poleceń, dzięki stosowaniu wyrażeń regularnych tzw. Regex; ▪ Urządzenie może zostać zastosowanie jako urządzenie w sieci SD-WAN poprzez zmianę trybu pracy urządzenia i zakup odpowiedniej licencji; ▪ Musi obsługiwać zarzadzanie ruchem (QoS): o Hierarchiczne polityki QoS; o 3 poziomy hierarchii; ▪ Urządzenie posiadające możliwość integracji i współpracy z centralnym systemem zarządzania, monitorowania, konfiguracji jak również troubleshootingu sieci; ▪ Urządzenie umożliwiające obsługę przez zcentralizowany system zarządzania w celu zmiany wersji systemu operacyjnego; ▪ Urządzenie umożliwiające współpracę ż centralnym systemem zarządzania w celu automatycznego podłączenia i konfiguracji urządzenia do sieci (Plug and Play); ▪ Urządzenie umożliwiające uruchomienie jako router brzegowy w sieci SD-WAN; **Wyposażenie:** ▪ Urządzenie wyposażone w zasilacz redundantny identyczny jak zasilacz podstawowy; ▪ Urządzenie wyposażone w 16 GB pamięci RAM oraz 16 GB pamięci Flash; ▪ Urządzenie wyposażone w następujący moduł / następujące moduły: o moduł z dwoma portami combo z dwoma miedzianymi portami liniowymi RJ-45 i dwoma portami światłowodowymi SFP ▪ Urządzenie wyposażone w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat ▪ Urządzenie dostarczone z licencją umożliwiającą szyfrowanie ruchu na poziomie: o 250/250Mbps (sumarycznie 500Mbps) dla ruchu szyfrowanego; ▪ Router dostarczany z licencją umożliwiającą wykorzystanie wszystkich opisanych powyżej funkcjonalności; ▪ Urządzenie dostarczone z licencja umożlwiającą podłączenie i zarządzenie urządzeniem przez system zarządzania i monitorowania w zakresie podstawowym obejmującym inwentaryzację urządzenia, wyświetlenie na mapie topologii, zarządzanie i aktualizację oprogramowania urządzanie, konfigurację podstawową urządzenia, monitoring podstawowych parametrów pracy urządzenia; ▪ Router nie ogranicza i nie licencjonuje ruchu nieszyfrowanego;
		Firewall wraz z oprogramowaniem do antywirus oraz filtrowaniem URL – 2 szt.
		System NGFW składa się z dwóch urządzeń NGFW dostarczonych jako dedykowane urządzenia wraz ze wszystkimi usługami subskrypcyjnymi na okres 3 lat oraz redundantnymi zasilaczami **Opis techniczny – Minimalne wymagania techniczne i funkcjonalne urządzenia:** **NGFW** ▪ Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia ▪ Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall) ▪ Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band ▪ Urządzenie jest zasilanie prądem przemiennym 230V ▪ Możliwość montażu w szafie rack 19” (dołączone niezbędne elementy montażowe) ▪ Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1 000 sieci VLAN ▪ Urządzenie wyposażone w port USB 3.0 ▪ Wysokość urządzenia 1RU ▪ Urządzenie wyposażone jest w redundantny zasilacz. Zasilacze mogą być wymieniane podczas pracy urządzenia („na gorąco”) ▪ Urządzenia zapewniające możliwość połączenia w klaster wydajnościowy o następujących właściwościach: o Obsługa do 16 urządzeń fizycznych w jednym klastrze o Wszystkie urządzenia w klastrze biorą aktywny udział w procesowaniu ruchu o Zachowanie symetrii ruchu - stany sesji są zachowane również, gdy ruch wyjściowy i powrotny będzie odbywał się przez inne fizyczne urządzenia o Klaster pozwala na bezprzerwowy upgrade lub wymianę całego urządzenia o Klaster może zostać utworzony w ramach jednej lokalizacji oraz może być rozproszony na dwie geograficznie rozdzielone lokalizacje działające zarówno w trybie active-standby jak i active-active o Klastrowanie można stosować w przypadku interfejsów routowanych (L3), bridge’owanych (L2) oraz

typowych interfejsów IPS inline

- Platforma umożliwiająca tworzenie instancji w ramach jednego urządzenia
  - Każda instancja to oddzielne wirtualne urządzenie w ramach jednego urządzenia fizycznego.
  - Każda instancja ma przydzielone dedykowane zasoby pamięci, procesora oraz dysku, które nie są współdzielone z innymi.
  - Instancje można restartować niezależnie od siebie. Restart jednej instancji nie powoduje przerwy działania innej instancji
  - Instancje w ramach jednego urządzenia mogą posiadać różne wersje oprogramowania udostępnianego przez producenta rozwiązania
  - Każda z instancji w ramach jednego fizycznego urządzenia może być zarządzana przez różne systemy do zarządzania producenta rozwiązania
  - Interfejsy mogą być dołączone do instancji na dwa sposoby:
    - Interfejs dedykowany dla jednej instancji, wyizolowany i niedostępny dla innych instancji
    - Interfejs współdzielony między instancjami
  - Podział urządzenia fizycznego na instancje nie powoduje potrzeby dokupowania dodatkowych licencji na jakiekolwiek używane funkcjonalności
- Urządzenie wyposażone w 8 portów 100/1000 Mbps RJ45, 8 portów 1/10 Gbps SFP+ oraz jeden slot na moduł rozszerzeń umożliwiający dalszą rozbudowę o 8 interfejsów 1/10 Gbps
- Przepustowość urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 17 Gbps dla pakietów wielkości 1024B
- Urządzenie osiągające powyższe parametry wydajnościowe wraz z uruchomionym silnikiem IPS.
- 2 000 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 130 000 nowych połączeń na sekundę
- Możliwość połączenia VPN do 3 000 urządzeń z maksymalną sumaryczną przepustowością 8 Gbps dla pakietów 1024B
- Przepustowość deskrypcji ruchu szyfrowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048B) wynosi przynajmniej 4,8 Gbps
- Urządzenie pozwalające na utworzenie 15 osobnych tablic routingu dla odseparowania ruchu na poziomie warstwy L3 dla grup interfejsów
- Maksymalna ilość instancji: 3

Opis funkcjonalny

- Urządzenie nie posiadające ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
- Możliwość uruchomienia urządzenia w trybie firewall'a L2 oraz L3
- Urządzenie obsługuje routing statyczny oraz dynamiczny: RIP, OSPF, OSPFv3, BGP
- Możliwość monitorowania dostępności „next hop" w trasach statycznych i automatycznego wyłączania trasy, gdy jest niedostępny.
- Urządzenie obsługuje ruch multicastowy oraz protokoły IGMP, PIM-SM oraz bidirectional PIM
- Urządzenie posiadające możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory i aktywne uwierzytelnienie.
- System IPS zapewniający pasywną identyfikację użytkowników (przezroczystą dla użytkowników) dzięki integracji z dedykowanym agentem, który wysyła dane o sesjach z Microsoft Active Directory do firewalla przez system zarządzania. Agent nie musi być instalowany bezpośrednio na serwerze AD lub kontrolerze domeny, ale może też działać na komputerze podłączonym do monitorowanej domeny.
- System IPS posiadający możliwość współdzielenia sesji wraz z innymi urządzeniami, dzięki czemu użytkownik logujący się poprzez captive-portal na jednym firewall nie musi się logować ponownie, jeżeli ruch jego przejdzie przez inny firewall
- Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT)
- Urządzenie może pracować jako serwer DHCP lub DHCP relay oraz zapewnia usługę DDNS
- Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby
- Urządzanie zapewnia możliwość obsługi użytkowników zdalnych VPN (RA VPN)
- Dla RA VPN urządzenie zapewnia integrację z systemami Multi-Factor Authentication MFA
- Urządzenie zapewnia możliwość zestawienia dostępu ZTNA dla aplikacji HTTPS do sieci wewnętrznych poprzez wykorzystanie zewnętrznego SAML Identity Provider (IdP), umożliwiając w ten sposób osobną autoryzację do każdej z aplikacji. System współpracuje co najmniej z takimi IdP jak Azure AD, Octa, Duo.
- Urządzenie zapewniające możliwość konfiguracji połączeń VPN typu Site-to-Site w następujących topologiach:
  - Point to Point
  - Hub and Spoke
  - Full Mesh
- Urządzenie zapewniające możliwość konfiguracji połączeń VPN typu Site-to-Site za pomocą interfejsów tunelowych (VTI) zarówno statycznych jak i dynamicznych dla zapewnienia metody route-based w topologii hub and spoke.
- Urządzenia pozwalające na tworzenie klastra VPN dla zdalnego dostępu. W klastrze takim każde urządzenie lub układ HA pracuje niezależnie od siebie, a połączenia są kierowane do odpowiedniego urządzenia przez wybrany na początku węzeł zarządzający, którym jest jedno z działających urządzeń VPN. Węzeł zarządzający przydziela do poszczególnych urządzeń ilość sesji VPN w zależności od ich mocy przerobowej dzięki czemu urządzenia w klastrze nie muszą być takie same (np. w jednym klastrze może pracować słabe urządzenie, duże klasy enterprise oraz urządzenie wirtualne).
- Urządzenie pozwalające na sterowanie ruchem poprzez Policy Based Routing w zależności od takich parametrów jak RTT, Jitter, utrata pakietów oraz MOS (Mean Opinion Score).

		▪ Urządzenie pozwalające na utworzenie interfejsu logicznego (software'owego) loopback, których stan nie jest powiązany z żadnym interfejsem logicznym. Interfejs taki można wykorzystać m.in. do: statycznych i dynamicznych tuneli VTI, BGP, SSH, Syslog, AAA, ICMP. ▪ Urządzenie pozwalające na uruchomienie dynamicznych następujących protokołów routingu na tunelach VTI: o BGP o OSPFv3/v3 o EIGRP ▪ Urządzenie zapewniające możliwość ograniczenia pasma w konkretnym kierunku – upload i download dla: o Źródłowych i docelowych stref NGFW o Źródłowych i docelowych adresów IP oraz portów o Aplikacji o Użytkowników o URLi zdefiniowanych przez administratora o Kategorii URL (jeżeli jest licencja URL filtering) o Źródłowego i docelowego kraju lub kontynentu (geolokacja) ▪ System posiadający możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System może stworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów: o Wiedza o użytkownikach – uwierzytelenienie o Wiedza o urządzeniach – pasywne skanowanie ruchu o Wiedza o urządzeniach mobilnych, load balancerach, urządzeniach NAT o Wiedza o aplikacjach wykorzystywanych po stronie klienta o Wiedza o podatnościach o Wiedza o bieżących zagrożeniach o Baza danych URL ▪ System posiadający otwarte API dla współpracy z systemami zewnętrznymi ▪ Rozwiązanie współpracujące z systemami SIEM ▪ System umożliwiający wykrycie co najmniej 7000 aplikacji ▪ System posiadający wbudowany moduł wykrywania aplikacji AVC na podstawie sygnatur, który współpracuje z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach ▪ Rozwiązanie umożliwiające integrację z chmurową konsolą korelacji informacji o zagrożeniach z różnych rozwiązań bezpieczeństwa tego samego producenta. ▪ Urządzenie może być zarządzane lokalnie lub przez scentralizowaną konsolę zarządzającą ▪ System umożliwia zdefiniowanie różnych wartości czasu wygaśnięcia sesji dla takich protokołów jak: ARP, SIP, H.323, H225, ICMP, UDP oraz dla sesji translacji PAT i sesji półotwartych. ▪ System umożliwiające zdefiniowanie następujących podstawowych zabezpieczeń dla połączeń: o Randomizacja TCP sequence numer o Ograniczenie ilości wszystkich połączeń globalnie oraz do jednego hosta o Ograniczenie ilości połączeń półotwartych globalnie oraz do jednego hosta o Detekcja wygasłych połączeń, poprzez sprawdzanie czy dwie strony sesji są nadal aktywne ▪ Urządzenie umożliwiające wybór następujących metod kompilacji reguł polityki dostępu w przypadku użycia obiektów (np. grupy adresów IP, portów): o Rozłożenie jednej skonfigurowanej reguły na reguły szczegółowe będące wszystkimi możliwymi kombinacjami wszystkich elementów zawartych w obiektach w celu monitorowania każdej z tych reguł z osobna (np. ilość dopasowani połączeń hit-counts) kosztem większego wykorzystania pamięci o Dopasowanie ruchu do głównej reguły na podstawie zdefiniowanych obiektów bez tworzenia wszytkich możliwych kombinacji obiektów w celu zmniejszenia wykorzystania pamięci przez szczegółowe reguły. ▪ Urządzenie zapewniające możliwość przypisania do reguł czasu jej aktywności. Istnieje możliwość zdefiniowania czasu całkowitego oraz zaplanowania interwałów czasowych. ▪ System pozwalający na przypisanie różnego profilu wydajnościowego do control plane i data plane tak, by administrator miał możliwość przypisania większej ilości zasobów do data plane w przypadku, gdy najbardziej obciążającą funkcjonalnością firewalla jest obsługa VPN ▪ System IPS zapewniający: o możliwość pracy w trybie in-line o możliwość pracy w trybie pasywnym (IDS) o możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym: • złośliwe oprogramowanie • skanowanie sieci • ataki na usługę VoIP • próby przepełnienia bufora • ataki na aplikacje P2P • zagrożenia dnia zerowego, itp. ▪ możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna) ▪ wiele sposobów wykrywania zagrożeń w tym: o sygnatury ataków opartych na exploitach o reguły oparte na zagrożeniach o mechanizm wykrywania anomalii w protokołach o mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego

		▪ możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu ▪ mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives) ▪ możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń ▪ wiele możliwości reakcji na zdarzenia w tym takie, jak: o tylko monitorowanie o blokowanie ruchu zawierającego zagrożenia o zapisywanie pakietów ▪ IP, CIP, DCE, DNP3, IEC104, modbus, s7commplus ▪ możliwość detekcji ataków i zagrożeń opartych na protokole IPv6 ▪ możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o: o systemach operacyjnych o serwisach o otwartych portach, aplikacjach o zagrożeniach ▪ możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych ▪ możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp. ▪ możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji ▪ możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego ▪ mechanizm aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne ▪ możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie ▪ obsługę reguł Snort3 ▪ możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS ▪ mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise) ▪ mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa, na podstawie danych kontekstowych ▪ Urządzenie zapewniające możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym: o pliki systemowe o pliki graficzne o pliki PDF o pliki wykonywalne o pliki multimedialne o pliki pakietu Office o pliki skompresowane ▪ Urządzenie posiadające możliwość monitorowania i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download ▪ System umożliwiający zdefiniowanie osobnej polityki IPS dla ruchu klasyfikowanego na podstawie aplikacji i wymagającego wymiany kilku pakietów w celu poprawnego wykrycia aplikacji. ▪ System pozwalający na budowanie polityk w oparciu o nazwy DNS z możliwością przekierowania zapytań do tzw. „sinkhole”. ▪ System pozwalający na przypisanie innych polityk IPS do różnych reguł polityki dostępu ▪ System zbierający dane kontekstowe, na podstawie których buduje profil każdego hosta. Profil taki zawiera informacje o systemie operacyjnym i jego wersji, aplikacjach i ich wersjach, protokołach. ▪ Wyżej wymienione dane kontekstowe są mapowane do wbudowanej bazy podatności na zagrożenia. Mapowanie pozwala na trafne określenie wpływu zagrożenia na zaatakowany system (jeżeli jest podatność system jest skompromitowany, jeżeli nie było podatności to system nie został skompromitowany). ▪ System pozwala na wstrzykiwanie tagów usług Azure i AWS, tagów z Vmware oraz atrybutów Office365 i użycie ich w polityce bezpieczeństwa. System automatycznie reaguje na zmianę tych tagów i atrybutów bez konieczności aktualizowania polityki. Wymagania te wynikają z rozwiązań stosowanych przez Zamawiającego w jego przedsiębiorstwie. ▪ System pozwalający na odszyfrowywanie i analizę ruchu w protokole TLS 1.3 natywnie, tzn. bez wymuszenia obniżenia sesji TLS do wersji 1.2 ▪ System pozwala na odszyfrowanie i analizę ruchu w protokole QUIC ▪ System posiadający wbudowany moduł wykrywania aplikacji oraz zagrożeń w ruchu zaszyfrowanym bez jego deszyfracji na podstawie analizy co najmniej trzech parametrów: o fingerprinty generowane na podstawie TLS handshake oraz porównanie ich z bazą danych znanych fingerprintów aplikacji i zagrożeń dostarczonych przez producenta rozwiązania o docelowy adres IP o nazwy domeny z SNI ▪ System umożliwiający kontrolę co najmniej 100 aplikacji typu GenAI

		▪ System zapewniający możliwość detekcji zagrożeń zero-day oparty na silniku, który bazuje nie na sygnaturach IPS, ale na wytrenowanych modelach uczenia maszynowego na znanych wzorcach ataków i grupach podatności. ▪ System ma możliwość wykrycia przepływów typu „elephant flows" i obsługi ich poprzez: o Bypass przepływu z ominięciem silnika detekcji zagrożeń o Ograniczenie przepływu poprzez „rate-limit" i kontynuację jego inspekcji ▪ Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez: o sprawdzenie reputacji plików w systemie globalnym o sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze) o statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu ▪ Urządzenie zapewniające możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach: o pliki wolne od złośliwego kodu o pliki zawierające złośliwy kod o pliki podejrzane o pliki o własnej, zdefiniowanej przez użytkownika kategorii ▪ Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna) ▪ System filtracji URL zapewniający: o kategoryzację stron – w co najmniej 80 kategoriach o bazę URL o wielkości nie mniejszej niż 280 mln URL o bazę URL producenta rozwiązania ▪ System umożliwiający określenie kategorii URL w ruchu zaszyfrowanym TLS 1.3 bez uruchamiania procesu deszyfracji poprzez próbę otworzenia nowego połączenia TLS w wersji 1.2 i analizy pakietu Server Hello. Jeżeli ruch kwalifikuje się do deszyfracji jest on rozszyfrowywany do analizy i następnie szyfrowany wersją. ▪ System nie dopuszcza kategoryzowania URL poprzez analizę SNI z pakietu TLS Client Hello, ze względu na łatwość spoofingu tej wartości. ▪ System umożliwiający określenie kategorii URL na podstawie analizy nazwy domenowej uprzedniego zapytania DNS o adres IP danego URL.
		Przełącznik do DMZ wyposażony w 24-port data only,4 x 10G, dwa zasilacze – 2 szt.
		Minimalne wymagania techniczne i funkcjonalne urządzenia: Typ i liczba portów: 24 porty 10/100/1000BaseT RJ-45 + uplink 4x10G SFP ▪ Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek: o Gigabit Ethernet 1000Base-T, o Gigabit Ethernet 1000Base-SX, o Gigabit Ethernet 1000Base-LX/LH, o Gigabit Ethernet 1000Base-EX, o Gigabit Ethernet 1000Base-ZX, o Gigabit Ethernet 1000Base-BX-D/U, o 10Gigabit Ethernet 10GBase-SR, o 10Gigabit Ethernet 10GBase-LR, o 10Gigabit Ethernet 10GBase-ER, o 10Gigabit Ethernet 10GBase-ZR, o 10Gigabit Ethernet typu twinax (SFP+ - SFP+) ▪ Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: o Przepustowość w ramach stosu - 80Gb/s, o 8 urządzeń w stosie, o Zarządzanie poprzez jeden adres IP, o Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, ▪ Zasilanie i chłodzenie: o Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap), o Redundantne wentylatory, **Parametry wydajnościowe:** ▪ Przepustowość przełącznika (switching capacity): 128 Gb/s (bez podłączenia do stosu), 208 Gb/s (z podłączeniem do stosu) ▪ Prędkość przesyłania (forwarding rate): 95.23 Mpps ▪ Bufor pakietów – 6MB ▪ Pamięć DRAM – 2GB ▪ Pamięć flash – 4GB ▪ Obsługa: o 500 aktywnych sieci VLAN o 16000 adresów MAC o 3000 tras IPv4

		○ 1500 tras IPv6 ○ Ilość wpisów w listach kontroli dostępu Security ACL – 1000 ○ ilość wpisów w listach kontroli dostępu QoS ACL – 1000 ○ 512 interfejsów SVI L3 ○ Jumbo frame 9198B ○ 48 połączeń zagregowanych typu „port channel” ○ 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP ▪ Obsługa protokołu NTP ▪ Obsługa IGMPv1/2/3 i MLDv1/2 Snooping ▪ Przełącznik wspierający następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: ○ IEEE 802.1w Rapid Spanning Tree ○ Per-VLAN Rapid Spanning Tree (PVRST+) ○ IEEE 802.1s Multi-Instance Spanning Tree ○ Obsługa 64 instancji protokołu STP ○ Wsparcie dla protokołu REP (Resilient Ethernet Protocol) ○ Redundancja 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 liku podstawowego ▪ Obsługa protokołu LLDP i LLDP-MED. ▪ Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ) ▪ Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC ▪ Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego ▪ Możliwość uruchomienia funkcji serwera DHCP ▪ Mechanizmy związane z bezpieczeństwem sieci: ○ Możliwość ustanawiania wielu poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), ○ Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, ○ Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, ○ Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, ○ Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, ○ Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, ○ Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, ○ Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, ○ Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), ○ Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, ○ Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), ○ Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, ○ Obsługa list kontroli dostępu (ACL) następujących typów: • Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, • VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, • Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, • Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); ○ Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA), ○ Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), ○ Funkcja Private VLAN z obsługą dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS, ○ Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci, ▪ Obsługa mechanizmów zapewaniających 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.

		▪ Mechanizmy związane z zapewnieniem jakości usług w sieci: ○ Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, ○ Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, ○ Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), ○ Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, ○ Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), ○ Kontrola sztormów dla ruchu broadcast/multicast/unicast, ○ Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP; ▪ Obsługa protokołów i mechanizmów routingu: ○ Routing statyczny dla IPv4 i IPv6, ○ Routing dynamiczny – RIP, OSPF do 1000 routes PIM Stub do 1000 routes Policy-based routing (PBR), ○ Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup, ○ Obsługa 10 tuneli GRE (Generic Routing Encapsulation); ▪ Przełącznik umożliwiający lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN, ▪ Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego, ▪ Przełącznik posiadający 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.), ▪ Funkcjonalność sondy IP SLA Responder, **Zarządzanie** ▪ Port konsoli, ▪ Dedykowany port Ethernet do zarządzania out-of-band, ▪ 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, ▪ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, ▪ Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog, ▪ Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, ▪ Wsparcie dla protokoły RESTCONF, ▪ Wsparcie dla protokołu gNMI, ▪ Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych, ▪ Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą, ▪ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB, ▪ Funkcja 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, ▪ Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: ○ Monitoring pracy przełącznika w zakresie: • Użycie CPU, użycie pamięci, temperatura pracy, • Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny, • Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, • Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router) • Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, • Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, • Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik, • Protokół REP (Resilient Ethernet Protocol), • Protokół STP (Spanning Tree Protocol), • Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy), ○ Konfigurację przełącznika w zakresie: ▪ Konfiguracja interfejsów Fizycznych:

		○ opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, ○ w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP), ○ w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x, ○ przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) ▪ Logicznych typu „port channel": ○ opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, ○ w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, ○ w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ○ przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) ▪ Wirtualnych typu SVI: ○ opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP) ▪ Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN, ▪ Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), ▪ Konfiguracja mechanizmów SPAN i RSPAN, ▪ Konfiguracja protokołu STP, ▪ Konfiguracja protokołu REP, ▪ Konfiguracja routingu statycznego i dynamicznego, ▪ Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów, ▪ Tworzenie i przypisanie list kontroli dostępu ACL, ▪ Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, ▪ Konfiguracja i uruchomienie NetFlow, ▪ Konfiguracja polityk QoS, ▪ Administracja przełącznika w zakresie: ▪ Zdalne uruchamianie komend linii poleceń, ▪ Nazwa przełącznika, ▪ Tryb pracy L2/L3, ▪ Adres IP przełącznika do celów zarządzania zdalnego, ▪ Konfiguracja serwera DHCP, ▪ Konfiguracja DNS, ▪ Czas systemowy w tym protokół NTP, ▪ Konta administracyjne, ▪ Upgrade oprogramowania, ▪ Backup konfiguracji, ▪ Zdalny restart urządzenia, ▪ Konfiguracja i dostęp przez SNMP, ▪ Diagnostyka urządzenia: ▪ Narzędzie PING i TRACEROUTE, ▪ Przeglądanie logów systemowych, ▪ Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego, **Parametry fizyczne:** ▪ Możliwość montażu w szafie rack 19", ▪ Wysokość urządzenia 1 RU, ▪ Głębokość chassis urządzenia bez wentylatorów i zasilaczy mniejsza niż 30 cm ▪ Głębokość chassis urządzenia z wentylatorami i zasilaczami mniejsza niż 33 cm **Inne wymagania:** ▪ 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, ▪ Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, ▪ Wyposażenie urządzenia ▪ Przełącznik wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego, ▪ Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat,

3.	WiFI	Kontroler sieci WiFi z obsługą min. 250 AP – 2 szt.

Minimalne wymagania techniczne i funkcjonalne urządzenia:

- Kontroler sieci bezprzewodowej - urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
  - zarządzanie politykami bezpieczeństwa
  - wykrywanie zagrożeń w sieci bezprzewodowej
  - zarządzanie pasmem radiowym
  - zarządzanie mobilnością
  - zarządzanie jakością transmisji
  - zgodnie z protokołem CAPWAP (RFC 5415)
- obsługa 250 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia do 500 przez dodanie odpowiedniej licencji
- 4 interfejsy 2.5G/1G oraz 2 interfejsy 1/10G (SFP/SFP+)
- obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
- obsługa ruchu tunelowanego o przepustowości 5 Gbps z możliwością rozszerzenia do 10Gbps przez dodanie odpowiedniej licencji
- obsługa 5000 klientów sieci bezprzewodowej
- zarządzanie pasmem radiowym punktów dostępowych:
  - automatyczna adaptacja do zmian w czasie rzeczywistym
  - optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
  - dynamiczne przydzielanie kanałów radiowych
  - wykrywanie, eliminacja i unikanie interferencji
  - równoważenie obciążenia punktów dostępowych
  - tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
  - automatyczna dystrybucja klientów pomiędzy punkty dostępowe
  - mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
  - dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
- mapowanie SSID do segmentów VLAN w sieci przewodowej
  - 1:1
  - 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
  - możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
- obsługa sieci kratowych
  - komunikacja między punktami dostępowymi bez medium kablowego
  - separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)
  - automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)
  - automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
  - autoryzacja punktów dostępowych w oparciu o certyfikaty, adresy MAC
- obsługa mechanizmów bezpieczeństwa:
  - 802.11i, WPA3, WPA2, WPA
  - 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)
  - obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
  - kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
  - obsługa profilowania użytkowników:
    - przydział sieci VLAN
    - przydział list kontroli dostępu (ACL)
  - uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w
  - uwierzytelnianie punktów dostępowych w oparciu o certyfikaty
  - obsługa list kontroli dostępu (ACL)
  - obsługa list kontroli dostępu opartych o nazwy domenowe
  - obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X
  - wykrywanie i dezaktywacja obcych punktów dostępowych
  - możliwość budowania reguł klasyfikacji obcych punktów dostępowych w oparciu o nazwę SSID, wybrany ciąg znaków w SSID, siłę sygnału RSSI, minimalną ilość podłączonych urządzeń
  - ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP
  - DHCP proxy, wsparcie dla DHCP Option 82
  - obsługa polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa z wykorzystaniem mechanizmu out-of-band, który przekazuje mapowania aktualnych adresów IP stacji i znacznika
- zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową:
  - kryptograficzne podpisywanie obrazów oprogramowania
  - bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych
  - wbudowany moduł sprzętowy unikalnie identyfikujący urządzenie i jego pochodzenie

		▪ 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 ▪ obsługa ruchu unicast IPv4 i IPv6 ▪ zgodność z funkcjonalnościami IPv6 pod kątem RFC: 4191, 6980, 8200, 8201 ▪ obsługa ruchu multicast IPv4 i IPv6: o IGMP / MLD snooping o optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym) o obsługa konwersji ruchu multicast do unicast ▪ obsługa mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami) ▪ obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k ▪ obsługa mechanizmów QoS: o 802.1p o WMM, TSpec, U-APSD o Ograniczanie pasma per użytkownik o Call Admission Control, SIP CAC, Call Snooping o równomierna obsługa klientów sieci bezprzewodowej w oparciu o utylizację czasu antenowego o kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID o zbiór wbudowanych profili do automatycznej konfiguracji ustawień QoS ▪ 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; współpraca z serwerami autoryzacyjnymi w celu przypisania odpowiednich polityk kontroli ruchu aplikacji per użytkownik/grupa użytkowników ▪ obsługa protokołu Bonjour poprzez wbudowany mDNS (multicast DNS) Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów ▪ obsługa dostępu gościnnego (IPv4 i IPv6): o przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony) o przekierowanie użytkowników do strony logowania na zewnętrznym serwerze o obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta o obsługa konfiguracji jako dedykowany kontroler do obsługi ruchu gości – całość ruchu z SSID dostępu gościnnego zebranego na pozostałych kontrolerach musi być przesyłana do tego kontrolera w sposób zapewniający logiczną separację od ruchu wewnętrznego ▪ obsługa NTP (IPv4 oraz IPv6), możliwość ustawienia różnych serwerów NTP dla wybranych grup AP ▪ możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania (dni tygodnia, godziny) ▪ obsługa EoGRE w celu tunelowania ruchu z kontrolera do dedykowanego koncentratora (np. na routerze) ▪ wsparcie dla IEEE 802.11u ▪ obsługa Hotspot 2.0 ▪ obsługa redundancji rozwiązania (N+1) ▪ obsługa redundancji 1:1 (active/standby) zapewniającej: o utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera o synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej ▪ dedykowany interfejs 1GE typu RJ45 służący do połączenia dwóch kontrolerów w redundantną parę 1:1 ▪ dedykowany interfejs 1GE typu RJ45 do zarządzania ▪ port konsoli RJ45 ▪ zarządzanie przez HTTPS, SNMP, SSH, NETCONF, port konsoli szeregowej ▪ obsługa logowania Syslog, wsparcie dla IPSec w celu zabezpieczenia Syslog ▪ obsługa wbudowanego interpretera języka PYTHON ▪ obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020) ▪ wbudowana baza najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow, w tym również informacji zawartych w pakiecie od warstw 2 do 7 (w szczególności informacji o aplikacjach)
		Punkt dostępowy z antenami wewnętrznymi (tri-band 4x4) z obsługą W6E – 18 szt.
		Minimalne wymagania techniczne i funkcjonalne urządzenia: Punkt dostępu bezprzewodowego WiFi6E: ▪ obsługa standardów 802.11a/b/g/n/ac/ax o obsługa OFDMA (uplink/downlink), TWT, BSS Coloring o obsługa MU-MIMO (uplink/downlink) – min. 4x4:4 (5GHz oraz 6GHz) o obsługa MU-MIMO (uplink/downlink) – min. 2x2:2 (2,4GHz) o obsługa kanałów 20, 40, 80 MHz dla 802.11ac o obsługa kanałów 20, 40, 80, 160 MHz dla 6GHz oraz 20, 40, 80 MHz dla 5GHz dla 802.11ax o obsługa prędkości PHY do 1,7 Gbps (ac) (przy parametrach: 4x4, 80 MHz, 5GHz) o obsługa prędkośći PHY do 7,4 Gbps (ax) (przy parametrach: 4x4 160 MHz 6GHz oraz 4x4 80 MHz 5GHz oraz 2x2 20 MHz 2,4GHz)

		○ obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) ○ obsługa beamforming dla klientów 802.11ac/ax ○ obsługa MRC (Maximal Ratio Combining) ▪ konfigurowalna moc nadajnika ○ dla zakresu 2.4GHz: do 100 mW ○ dla zakresu 5GHz: do 200 mW ○ dla zakresu 6GHz: do 200 mW ▪ praca trójzakresowa w pasmach: 2,4GHz oraz 5GHz oraz 6GHz ▪ zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ 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) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników ○ obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6 ○ jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN) ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: • ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik • obsługa WMM, TSPEC, U-APSD ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ 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 ○ wsparcie IEEE 802.11i, WPA2, WPA3, WPA3-OWE (Enhanced Open) ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) ○ obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS ○ obsługa blokowania ruchu Peer-to-Peer ○ analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie) ▪ obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym: ○ sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia ○ bezpieczna sekwencja uruchamiania ○ sprawdzenie autentyczności urządzenia ▪ moduł radiowy pełniący funkcję analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz, 5GHz, 6GHz): ○ zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych ○ automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.) ○ umożliwia skanowanie off-channel (funkcjonuje niezależnie od pracy modułów radiowych transmitujących do klientów) zapewniając dodatkową analizę pasma radiowego pod kątem, m.in.: wykrywania sygnałów DFS, zarządzania ustawieniami parametrów radiowych, zbierania pakietów do lokalizacji urządzeń mobilnych ▪ interfejs MultiGigabit Ethernet (100/1000/2500) ▪ interfejs konsoli RJ45 ▪ port USB 2.0 ▪ 2 GB RAM, 1 GB Flash ▪ zróżnicowane możliwości zasilania: ○ przy zasilaniu przez 802.3bt: pełna funkcjonalność AP ○ przy zasilaniu przez 802.3at: praca z wyłączonym portem USB ○ przy zasilaniu przez 802.3af: możliwość uruchomienia AP w celach diagnostycznych bez pracujących modułów radiowych ▪ anteny zintegrowane o zysku: ○ min. 3 dBi dla pasma 2,4GHz ○ min. 5 dBi dla pasma 5GHz ○ min. 4 dBi dla pasma 6GHz ▪ obudowa przystosowana do pracy w zakresie temperatur 0 – 50oC ▪ certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi6, Wi-Fi Enhanced Open, WMM, WMM-PS ▪ wbudowane radio Bluetooth Low Energy (BLE) 5.1 ▪ Urządzenie wyposażone jest w licencję subskrypcyjną na wymagane funkcjonalności na okres 3 lat
		Punkt dostępowy z antenami zewnętrznymi z obsługą W6 – 28 szt.

		Minimalne wymagania techniczne i funkcjonalne urządzenia: Punkt dostępu bezprzewodowego: ▪ obsługa standardów 802.11a/b/g/n/ac/ax ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 4x4:4 (w 2,4 GHz oraz 5 GHz) ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa prędkości PHY do 3,4 Gbps (ac) ○ obsługa prędkośći PHY do 5,3 Gbps (ax) ○ obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) ○ obsługa beamforming dla klientów 802.11ac/ax ○ obsługa MRC (Maximal Ratio Combining) ▪ konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz: do 200 mW ▪ praca dwuzakresowa w pasmach: 2,4 GHz oraz 5 GHz ▪ możliwość zmiany trybu pracy modułów radiowych (elastyczna praca drugiego modułu) ○ jeden moduł pracujący w paśmie 2,4GHz, drugi moduł pracujący w paśmie 5GHz ○ oba moduły pracujące w paśmie 5GHz na różnych kanałach pozwalając na podłączenie dwóch zestawów anten obejmujących zasięgiem różne obszary ▪ zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ 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) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników ○ obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6 ○ jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN) ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: • ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik • obsługa WMM, TSPEC, U-APSD ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ 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 ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) ○ obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS ○ obsługa blokowania ruchu Peer-to-Peer ○ analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie) ▪ możliwość pracy jako kontroler sieci bezprzewodowej o następujących funkcjonalnościach: (zmiana trybu pracy (przez wgranie oprogramowania) musi być bez kosztowa w okresie trwania kontraktu serwisowego): ○ obsługa do 100 punktów dostępowych ○ obsługa do 2000 klientów ○ możliwość konfiguracji do 16 sieci bezprzewodowych ○ centralna optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów wsparcia roamingu – IEEE 802.11k, IEEE 802.11v, OKC ○ jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN) ○ konfiguracja polityk bezpieczeństwa per SSID ○ obsługa WPA2 i WPA3 Personal oraz Enterprise ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 (IPv4 ACL) oraz o nazwy domenowe (DNS ACL) ○ obsługa URL Whitelist ○ analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)

		○ dwukierunkowe limitowanie transmisji (bidirectional rate-limiting ruchu) per klient, per WLAN ○ profilowanie (rozpoznawanie typów) urządzeń podłączających się do sieci bezprzewodowej ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta ○ obsługa protokołu Bonjour poprzez wbudowany mDNS (multicast DNS) Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów ○ zarządzanie przez HTTPS ○ wsparcie SSH, SNMP, NTP, SYSLOG ○ obsługa aktualizacji oprogramowania przez TFTP, SFTP ○ wbudowany serwer DHCP ○ wbudowany mechanizm redundancji automatycznie wybierający kontroler zapasowy wśród grupy obsługiwanych punktów dostępowych mogących pełnić funkcję kontrolera ▪ obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym: ○ sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia ○ bezpieczna sekwencja uruchamiania ○ sprawdzenie autentyczności urządzenia ▪ zintegrowany moduł radiowy pełniący funkcję analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz): ○ dokładność analizy (kwant próbkowania) max. 200 kHz ○ zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych ○ automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.) ○ współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego w celu szybkiej reakcji w wyniku wykrycia ○ umożliwiający skanowanie off-channel (funkcjonuje niezależnie od pracy modułów radiowych transmitujących do klientów) zapewniając dodatkową analizę pasma radiowego pod kątem, m.in.: wykrywania sygnałów DFS, zarządzania ustawieniami parametrów radiowych, zbierania pakietów do lokalizacji urządzeń mobilnych ▪ interfejs MultiGigabit Ethernet (100/1000/2500) zgodny z IEEE 802.3bz ▪ interfejs konsoli RJ45 ▪ port USB 2.0 ▪ 2 GB RAM, 1 GB Flash ▪ pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at), możliwość uruchomienia AP z wykorzystaniem PoE (802.3af) z ograniczonymi funkcjami (m.in.: redukcja pracy układu radiowego lub wyłączenie jednego z modułów radiowych) ▪ wyposażony w złącza dla anten zewnętrznych oraz w funkcję wykrywania rodzaju dołączanych anten i w ten sposób obliczający maksymalny dopuszczalny poziom EIRP ▪ obudowa przystosowana do pracy w zakresie temperatur -20 – 50oC ▪ diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji ▪ certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi6, Wi-Fi Enhanced Open, WMM, WMM-PS ▪ wbudowane radio Bluetooth Low Energy (BLE) 5.0 ▪ IoT ready (Zigbee, Thread) Wyposażenie dodatkowe ▪ zestaw 4 anten dwuzakresowych per AP dookólnych o zysku 2dBi w paśmie 2,4GHz oraz 4dBi w paśmie 5 GHz w kolorze białym zgodnych z zaleceniami producenta ▪ Urządzenie wyposażone w licencję subskrypcyjną na wymagane funkcjonalności na okres 3 lat
4.	Przełączniki LAN	Przełącznik L3 wyposażony w 48-port 100/1000Mbit PoE+, 8 portów 10GB SFP+, dwa zasilacze – 2 szt.
		Minimalne wymagania techniczne i funkcjonalne urządzenia: ▪ Typ i liczba portów: 48 portów 10/100/1000BaseT RJ-45 ▪ Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami: ○ 4x1G SFP ○ 8x1/10G SFP/SFP+ ○ 2x40G QSFP ○ 2x25G SFP28 ○ 4x100M/1G/2.5G/5G/10GBaseT RJ-45 ▪ Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: ○ Przepustowość w ramach stosu - 480Gb/s, ○ 8 urządzeń w stosie, ○ Zarządzanie poprzez jeden adres IP, ○ Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, ○ Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na

		ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2) o 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), **Zasilanie i chłodzenie:** ▪ Redundantne i wymienne moduły wentylatorów, ▪ Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap), ▪ Przełącznik wspierający IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności), **Parametry wydajnościowe:** ▪ Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate): o Przepustowość przełącznika (switching capacity): 256 Gb/s (bez podłączenia do stosu), 736 Gb/s (z podłączeniem do stosu) o Prędkość przesyłania (forwarding rate): 190.47 Mpps (bez podłączenia do stosu), 547.62 Mpps (z podłączeniem do stosu) o Bufor pakietów – 16MB ▪ Pamięć DRAM – 8GB ▪ Pamięć flash – 16GB ▪ Obsługa: o 1000 aktywnych sieci VLAN o 32000 adresów MAC o 8000 tras IPv4 o 4000 tras IPv6 o Ilość wpisów w listach kontroli dostępu Security ACL – 5000 o ilość wpisów w listach kontroli dostępu QoS ACL – 5000 o 1000 interfejsów SVI L3 o 128 interfejsów L3 o Jumbo frame 9198B o 128 połączeń zagregowanych typu „port channel" o 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP ▪ Obsługa protokołu NTP ▪ Obsługa IGMPv1/2/3 i MLDv1/2 Snooping ▪ Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: o IEEE 802.1w Rapid Spanning Tree o Per-VLAN Rapid Spanning Tree (PVRST+) o IEEE 802.1s Multi-Instance Spanning Tree o Obsługa 128 instancji protokołu STP o Wsparcie dla protokołu REP (Resilient Ethernet Protocol) o Redundancja 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 liku podstawowego ▪ Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED. ▪ Realizacja funkcji 802.1Q tunneling (QinQ ▪ Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC ▪ Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego ▪ Możliwość uruchomienia funkcji serwera DHCP ▪ Mechanizmy związane z bezpieczeństwem sieci: o Możliwość ustanawiania wielu poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwiający zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), o Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, o Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL o Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, o Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, o Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, o Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, o Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, o Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), o Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, o Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym

		minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), ○ Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, ○ Obsługa list kontroli dostępu (ACL) następujących typów: • Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, • VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, • Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, • Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); ○ Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128), ○ Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), ○ 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), ▪ Obsługa mechanizmów zapewaniających 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. ▪ Mechanizmy związane z zapewnieniem jakości usług w sieci: ○ Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, ○ Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, ○ Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), ○ Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, ○ Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), ○ Kontrola sztormów dla ruchu broadcast/multicast/unicast, ○ Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP; ▪ Obsługa protokołów i mechanizmów routingu: ○ Routing statyczny dla IPv4 i IPv6, ○ Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes ○ Policy-based routing (PBR), ○ Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup, ○ Obsługa 10 tuneli GRE (Generic Routing Encapsulation); ▪ Przełącznik umożliwiający lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN, ▪ Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego, ▪ Przełącznik posiadający 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.), ▪ Funkcjonalność sondy IP SLA Responder, ▪ Wsparcie dla protokołu OpenFlow 1.3 ▪ Funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary, **Zarządzanie** ▪ Port konsoli, ▪ Dedykowany port Ethernet do zarządzania out-of-band, ▪ 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, ▪ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, ▪ Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog, ▪ Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, ▪ Wsparcie dla protokoły RESTCONF, ▪ Wsparcie dla protokołu gNMI, ▪ Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

		▪ Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą, ▪ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB; ▪ Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności 120GB; ▪ Funkcja 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, ▪ Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: ○ Monitoring pracy przełącznika w zakresie: • Użycie CPU, użycie pamięci, temperatura pracy, • Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny, • Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, • Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router) • Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, • Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, • Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik, • Protokół REP (Resilient Ethernet Protocol), • Protokół STP (Spanning Tree Protocol), • Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy), ▪ Konfiguracja przełącznika w zakresie: ○ Konfiguracja interfejsów Fizycznych: • opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, • w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP), • w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x, • przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) ○ Logicznych typu „port channel”: • opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, • w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, • w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, • przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) ○ Wirtualnych typu SVI: • opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do” oraz „z”, parametry protokołu DHCP Relay (adres IP serwera DHCP) ▪ Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN, ▪ Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), ▪ Konfiguracja mechanizmów SPAN i RSPAN, ▪ Konfiguracja protokołu STP, ▪ Konfiguracja protokołu REP, ▪ Konfiguracja routingu statycznego i dynamicznego, ▪ Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja ▪ Uwierzytelnienia dla poszczególnych portów ▪ Tworzenie i przypisanie list kontroli dostępu ACL, ▪ Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, ▪ Konfiguracja i uruchomienie NetFlow, ▪ Konfiguracja polityk QoS, ▪ Administracja przełącznika w zakresie: ○ Zdalne uruchamianie komend linii poleceń, ○ Nazwa przełącznika, ○ Tryb pracy L2/L3,

		○ Adres IP przełącznika do celów zarządzania zdalnego, ○ Konfiguracja serwera DHCP, ○ Konfiguracja DNS, ○ Czas systemowy w tym protokół NTP, ○ Konta administracyjne, ○ Upgrade oprogramowania, ○ Backup konfiguracji, ○ Zdalny restart urządzenia, ○ Konfiguracja i dostęp przez SNMP, ▪ Diagnostyka urządzenia: ○ Narzędzie PING i TRACEROUTE, ○ Przeglądanie logów systemowych, ○ Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego, **Parametry fizyczne:** ▪ Możliwość montażu w szafie rack 19", ▪ Wysokość urządzenia 1 RU, ▪ Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi mniejsza niż 50 cm, **Inne Wymagania:** ▪ Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 64000 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, ▪ Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, ▪ Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku, **Wyposażenie urządzenia** ▪ Przełącznik wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy, ▪ Przełącznik wyposażony jest w moduł do łączenia w stos data wraz z kablem stakującym o długości 1m, ▪ Przełącznik wyposażony jest w kabel o długości 150 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną, ▪ Przełącznik wyposażony jest w moduł: 8x1/10G SFP/SFP+, możliwy do obsadzenia następującymi rodzajami wkładek: ○ Gigabit Ethernet 1000Base-T, ○ Gigabit Ethernet 1000Base-SX, ○ Gigabit Ethernet 1000Base-LX/LH, ○ Gigabit Ethernet 1000Base-EX, ○ Gigabit Ethernet 1000Base-ZX, ○ Gigabit Ethernet 1000Base-BX-D/U, ○ 10Gigabit Ethernet 10GBase-SR, ○ 10Gigabit Ethernet 10GBase-LR, ○ 10Gigabit Ethernet 10GBase-LRM, ○ 10Gigabit Ethernet 10GBase-ER, ○ 10Gigabit Ethernet 10GBase-ZR, ○ 10Gigabit Ethernet 10GBase-BX-D/U, ○ 10Gigabit Ethernet typu twinax (SFP+ - SFP+) ○ kable twinax ▪ Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat,
		Przełącznik L3 wyposażony w 48-port 100/1000Mbit – 3 szt.
		Minimalne wymagania techniczne i funkcjonalne urządzenia: ▪ Typ i liczba portów: 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) ▪ Moc dostępna dla PoE: ○ 437W (z jednym zasilaczem o mocy 715W), ○ 437W (z dwoma zasilaczami o mocy 715W pracującymi w układzie redundantnym), ○ 1152W (z dwoma zasilaczami o mocy 715W pracującymi w układzie współdzielenia mocy) ▪ Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco" – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb): ○ 4x1G SFP ○ 8x1/10G SFP/SFP+ ○ 2x40G QSFP ○ 2x25G SFP28 ○ 4x100M/1G/2.5G/5G/10GBaseT RJ-45 ▪ Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: ○ Przepustowość w ramach stosu - 480Gb/s, ○ 8 urządzeń w stosie, ○ Zarządzanie poprzez jeden adres IP,

- Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
- Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),
- 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),

Zasilanie i chłodzenie:

- Redundantne i wymienne moduły wentylatorów,
- Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap),
- Przełącznik umożliwiający podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
- W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),
- Przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

Parametry wydajnościowe:

- Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):
  - Przepustowość przełącznika (switching capacity): 256 Gb/s (bez podłączenia do stosu), 736 Gb/s (z podłączeniem do stosu)
  - Prędkość przesyłania (forwarding rate): 190.47 Mpps (bez podłączenia do stosu), 547.62 Mpps (z podłączeniem do stosu)
  - Bufor pakietów – 16MB
  - Pamięć DRAM – 8GB
  - Pamięć flash – 16GB

Obsługa:

- Obsługa:
  - 1000 aktywnych sieci VLAN
  - 32000 adresów MAC
  - 8000 tras IPv4
  - 4000 tras IPv6
  - Ilość wpisów w listach kontroli dostępu Security ACL – 5000
  - ilość wpisów w listach kontroli dostępu QoS ACL – 5000
  - 1000 interfejsów SVI L3
  - 128 interfejsów L3
  - Jumbo frame 9198B
  - 128 połączeń zagregowanych typu „port channel"
  - 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
- Obsługa protokołu NTP
- Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
- Przełącznik wspierający następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
  - IEEE 802.1w Rapid Spanning Tree
  - Per-VLAN Rapid Spanning Tree (PVRST+)
  - IEEE 802.1s Multi-Instance Spanning Tree
  - Obsługa 128 instancji protokołu STP
  - Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
  - Redundancja 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 liku podstawowego
- Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED.
- Realizacja funkcji 802.1Q tunneling (QinQ
- Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
- Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
- Możliwość uruchomienia funkcji serwera DHCP
- Mechanizmy związane z bezpieczeństwem sieci:
  - Możliwość ustanawiania wielu poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
  - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
  - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL

		○ Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, ○ Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, ○ Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, ○ Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, ○ Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, ○ Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), ○ Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, ○ Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), ○ Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, ○ Obsługa list kontroli dostępu (ACL) następujących typów: • Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, • VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, • Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, • Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); ○ Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128), ○ Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), ○ 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), ▪ Obsługa mechanizmów zapewaniających 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. ▪ Mechanizmy związane z zapewnieniem jakości usług w sieci: ○ Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, ○ Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, ○ Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), ○ Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, ○ Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), ○ Kontrola sztormów dla ruchu broadcast/multicast/unicast, ○ Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP; ▪ Obsługa protokołów i mechanizmów routingu: ○ Routing statyczny dla IPv4 i IPv6, ○ Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes ○ Policy-based routing (PBR), ○ Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup, ○ Obsługa 10 tuneli GRE (Generic Routing Encapsulation); ▪ Przełącznik umożliwiający lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN, ▪ Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego, ▪ Przełącznik posiadający 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.), ▪ Funkcjonalność sondy IP SLA Responder, ▪ Wsparcie dla protokołu OpenFlow 1.3 ▪ Funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary, **Zarządzanie** ▪ Port konsoli, ▪ Dedykowany port Ethernet do zarządzania out-of-band, ▪ Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzajacego

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,

- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
- Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
- Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
- Wsparcie dla protokoły RESTCONF,
- Wsparcie dla protokołu gNMI,
- Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
- Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
- Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności 120GB;
- Funkcja 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,
- Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
  - Monitoring pracy przełącznika w zakresie:
    - Użycie CPU, użycie pamięci, temperatura pracy,
    - Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
    - Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
    - Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)
    - Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    - Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    - Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
    - Protokół REP (Resilient Ethernet Protocol),
    - Protokół STP (Spanning Tree Protocol),
    - Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),
- Konfiguracja przełącznika w zakresie:
  - Konfiguracja interfejsów Fizycznych:
    - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
    - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),
    - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,
    - przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
  - Logicznych typu „port channel”:
    - opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
    - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,
    - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,
    - przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
  - Wirtualnych typu SVI:
    - opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do” oraz „z”, parametry protokołu DHCP Relay (adres IP serwera DHCP)
- Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
- Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
- Konfiguracja mechanizmów SPAN i RSPAN,
- Konfiguracja protokołu STP,

		▪ Konfiguracja protokołu REP, ▪ Konfiguracja routingu statycznego i dynamicznego, ▪ Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja ▪ Tworzenie i przypisanie list kontroli dostępu ACL, ▪ Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, ▪ Konfiguracja i uruchomienie NetFlow, ▪ Konfiguracja polityk QoS, ▪ Administracja przełącznika w zakresie: o Zdalne uruchamianie komend linii poleceń, o Nazwa przełącznika, o Tryb pracy L2/L3, o Adres IP przełącznika do celów zarządzania zdalnego, o Konfiguracja serwera DHCP, o Konfiguracja DNS, o Czas systemowy w tym protokół NTP, o Konta administracyjne, o Upgrade oprogramowania, o Backup konfiguracji, o Zdalny restart urządzenia, o Konfiguracja i dostęp przez SNMP, ▪ Diagnostyka urządzenia: o Narzędzie PING i TRACEROUTE, o Przeglądanie logów systemowych, o Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego, **Parametry fizyczne:** ▪ Możliwość montażu w szafie rack 19”, ▪ Wysokość urządzenia 1 RU, ▪ Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi mniejsza niż 50 cm, **Inne Wymagania** ▪ Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 64000 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, ▪ Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, ▪ Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku, **Wyposażenie urządzenia** ▪ Przełącznik wyposażony jest w moduł do łączenia w stos data wraz z kablem stakującym o długości 50 cm, ▪ Przełącznik wyposażony jest w kabel o długości 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną, ▪ Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat,
		Przełącznik L3 wyposażony w 48-port 5Gbps PoE+, dwa zasilacze – 2 szt.
		Minimalne wymagania techniczne i funkcjonalne urządzenia: ▪ Typ i liczba portów: 48 portów 100M/1G/2.5G/5GBaseT RJ-45 UPoE (do 60W per port) ▪ Moc dostępna dla PoE: o 645W (z jednym zasilaczem o mocy 1100W), o 645W (z dwoma zasilaczami o mocy 1100W pracującymi w układzie redundantnym), o 1745W (z dwoma zasilaczami o mocy 1100W pracującymi w układzie współdzielenia mocy) ▪ Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb): o 4x1G SFP o 8x1/10G SFP/SFP+ o 2x40G QSFP o 2x25G SFP28 o 4x100M/1G/2.5G/5G/10GBaseT RJ-45 ▪ Porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia następującymi rodzajami wkładek: o Porty SFP: • Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U o Porty SFP/SFP+: • Gigabit Ethernet 1000Base-T,

- Gigabit Ethernet 1000Base-SX,
- Gigabit Ethernet 1000Base-LX/LH,
- Gigabit Ethernet 1000Base-EX,
- Gigabit Ethernet 1000Base-ZX,
- Gigabit Ethernet 1000Base-BX-D/U,
- 10Gigabit Ethernet 10GBase-SR,
- 10Gigabit Ethernet 10GBase-LR,
- 10Gigabit Ethernet 10GBase-LRM,
- 10Gigabit Ethernet 10GBase-ER,
- 10Gigabit Ethernet 10GBase-ZR,
- 10Gigabit Ethernet 10GBase-BX-D/U,
- 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

○ Porty SFP/SFP+/SFP28:

- Gigabit Ethernet 1000Base-T,
- Gigabit Ethernet 1000Base-SX,
- Gigabit Ethernet 1000Base-LX/LH,
- Gigabit Ethernet 1000Base-EX,
- Gigabit Ethernet 1000Base-ZX,
- Gigabit Ethernet 1000Base-BX-D/U,
- 10Gigabit Ethernet 10GBase-SR,
- 10Gigabit Ethernet 10GBase-LR,
  10Gigabit Ethernet 10GBase-ER,
  10Gigabit Ethernet 10GBase-ZR,
  10Gigabit Ethernet 10GBase-BX-D/U,
  10Gigabit Ethernet typu twinax (SFP+ - SFP+)
  25Gigabit Ethernet 25GBASE-SR,
  25Gigabit Ethernet typu twinax (SFP28 – SFP28)
  10/25Gigabit Ethernet 10/25GBASE-CSR (MMF)
  10/25Gigabit Ethernet 10/25GBASE-LR (SMF)

○ Porty QSFP:

- 40G-SR4,
- 40G-LR4,
- 40G-ER4,
- 40G-SR-BD,
- adapter 40G QSFP->10G SFP+
- kable twinax

▪ Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
○ Przepustowość w ramach stosu - 480Gb/s,
○ 8 urządzeń w stosie
○ Zarządzanie poprzez jeden adres IP,
○ Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
○ Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),
○ 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),

Zasilanie i chłodzenie:

▪ Redundantne i wymienne moduły wentylatorów,
▪ Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap),
▪ Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
▪ W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),
▪ Przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

Parametry wydajnościowe:

▪ Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):
  ○ Przepustowość przełącznika (switching capacity): 640 Gb/s (bez podłączenia do stosu), 1120 Gb/s (z podłączeniem do stosu)
  ○ Prędkość przesyłania (forwarding rate): 476.19 Mpps (bez podłączenia do stosu), 833.33 Mpps (z podłączeniem do stosu)
▪ Bufor pakietów – 32MB
▪ Pamięć DRAM – 8GB

- Pamięć flash – 16GB

Obsługa:

- Obsługa:
  - 1000 aktywnych sieci VLAN
  - 32000 adresów MAC
  - 8000 tras IPv4
  - 4000 tras IPv6
  - Ilość wpisów w listach kontroli dostępu Security ACL – 5000
  - ilość wpisów w listach kontroli dostępu QoS ACL – 5000
  - 1000 interfejsów SVI L3
  - 128 interfejsów L3
  - Jumbo frame 9198B
  - 128 połączeń zagregowanych typu „port channel”
  - 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
- Obsługa protokołu NTP
- Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
- Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
  - IEEE 802.1w Rapid Spanning Tree
  - Per-VLAN Rapid Spanning Tree (PVRST+)
  - IEEE 802.1s Multi-Instance Spanning Tree
  - Obsługa 128 instancji protokołu STP
  - Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
  - Redundancja 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 liku podstawowego
- Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED.
- Realizacja funkcji 802.1Q tunneling (QinQ
- Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
- Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
- Możliwość uruchomienia funkcji serwera DHCP
- Mechanizmy związane z bezpieczeństwem sieci:
  - Możliwość ustanawiania wielu poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
  - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
  - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
  - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
  - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
  - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
  - Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
  - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
  - Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
  - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
  - Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
  - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
  - Obsługa list kontroli dostępu (ACL) następujących typów:
    - Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    - VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
    - Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    - Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
  - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128),
  - Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
  - 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),
- Obsługa mechanizmów zapewaniających 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.
- Mechanizmy związane z zapewnieniem jakości usług w sieci:
  - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
  - Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
  - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
  - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
  - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
  - Kontrola sztormów dla ruchu broadcast/multicast/unicast,
  - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
- Obsługa protokołów i mechanizmów routingu:
  - Routing statyczny dla IPv4 i IPv6,
  - Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes
  - Policy-based routing (PBR),
  - Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,
  - Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
- Przełącznik umożliwiający lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
- Przełącznik umożliwiający lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
- Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
- Przełącznik posiadający 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.),
- Funkcjonalność sondy IP SLA Responder,
- Wsparcie dla protokołu OpenFlow 1.3
- Funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,

Zarządzanie

- Port konsoli,
- Dedykowany port Ethernet do zarządzania out-of-band,
- Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzajacego 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,
- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
- Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
- Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
- Wsparcie dla protokoły RESTCONF,
- Wsparcie dla protokołu gNMI,
- Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
- Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
- Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności 120GB;
- Funkcja 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,
- Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
  - Monitoring pracy przełącznika w zakresie:
    - Użycie CPU, użycie pamięci, temperatura pracy,
    - Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
    - Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
    - Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny

port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)
- Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
- Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
- Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
- Protokół REP (Resilient Ethernet Protocol),
- Protokół STP (Spanning Tree Protocol),
- Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),

▪ Konfigurację przełącznika w zakresie:
  ○ Konfiguracja interfejsów Fizycznych:
    - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
    - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),
    - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,
    - przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
  ○ Logicznych typu „port channel":
    - opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
    - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,
    - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,
    - przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
  ○ Wirtualnych typu SVI:
    - opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP)
▪ Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
▪ Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
▪ Konfiguracja mechanizmów SPAN i RSPAN,
▪ Konfiguracja protokołu STP,
▪ Konfiguracja protokołu REP,
▪ Konfiguracja routingu statycznego i dynamicznego,
▪ Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja
▪ Tworzenie i przypisanie list kontroli dostępu ACL,
▪ Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
▪ Konfiguracja i uruchomienie NetFlow,
▪ Konfiguracja polityk QoS,
▪ Administracja przełącznika w zakresie:
  ○ Zdalne uruchamianie komend linii poleceń,
  ○ Nazwa przełącznika,
  ○ Tryb pracy L2/L3,
  ○ Adres IP przełącznika do celów zarządzania zdalnego,
  ○ Konfiguracja serwera DHCP,
  ○ Konfiguracja DNS,
  ○ Czas systemowy w tym protokół NTP,
  ○ Konta administracyjne,
  ○ Upgrade oprogramowania,
  ○ Backup konfiguracji,
  ○ Zdalny restart urządzenia,
  ○ Konfiguracja i dostęp przez SNMP,
▪ Diagnostyka urządzenia:
  ○ Narzędzie PING i TRACEROUTE,
  ○ Przeglądanie logów systemowych,
  ○ Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego

Parametry fizyczne:
▪ Możliwość montażu w szafie rack 19",

		▪ Wysokość urządzenia 1 RU, ▪ Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi mniejsza niż 57 cm **Inne Wymagania** ▪ Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 128 000 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, ▪ Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, ▪ Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku, **Wyposażenie urządzenia** ▪ Przełącznik wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy, ▪ Przełącznik wyposażony w moduł do łączenia w stos data wraz z kablem stakującym o długości 50 cm ▪ Przełącznik wyposażony w kabel o długości 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną, ▪ Przełącznik wyposażony w moduł: o 2x25G SFP28
		Przełącznik L2 wyposażony w 48-port 100/1000Mbit PoE+, 4portów 10GB SFP+, dwa zasilacze – 4 szt.
		Minimalne wymagania techniczne i funkcjonalne urządzenia: ▪ Typ i liczba portów: 48 porty 10/100/1000 BaseT RJ45 PoE+ (zgodne z IEEE 802.3at) ▪ Moc dostępna dla PoE: o 740W (z jednym zasilaczem o mocy 1KW), o 740W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie redundantnym), o 1440W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie współdzielenia mocy), ▪ Urządzenie wyposażone jest w slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia następującymi modułami: o 4x1G SFP gdzie porty SFP możliwe do obsadzenia następującymi rodzajami wkładek interfejsowych: • Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U o 4x1G/10G SFP/SFP+ gdzie porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek interfejsowych: • Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-LRM, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet typu twinax (SFP+ - SFP+) ▪ Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: o Przepustowość w ramach stosu - 160Gb/s, o 8 urządzeń w stosie, o Zarządzanie poprzez jeden adres IP, o Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, **Zasilanie i chłodzenie:** ▪ Redundantne i wymienne moduły wentylatorów, ▪ Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), ▪ Przełącznik umożliwiający podtrzymanie zasilania z portów PoE podczas restartu urządzenia, ▪ W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika), **Parametry wydajnościowe:** ▪ Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 336 Gb/s (z podłączeniem do stosu)

- Prędkość przesyłania (forwarding rate): 130.95 Mpps
- Bufor pakietów – 6MB
- Pamięć DRAM – 4GB
- Pamięć flash – 4GB

Obsługa:

- 1000 aktywnych sieci VLAN
- 32000 adresów MAC
- 4000 tras IPv4
- 2000 tras IPv6
- Ilość wpisów w listach kontroli dostępu Security ACL – 1000
- ilość wpisów w listach kontroli dostępu QoS ACL – 1000
- 1000 interfejsów SVI L3
- Jumbo frame 9198B
- 48 połączeń zagregowanych typu „port channel"
- 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
- Obsługa protokołu NTP
- Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
- Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
  - IEEE 802.1w Rapid Spanning Tree
  - Per-VLAN Rapid Spanning Tree (PVRST+)
  - IEEE 802.1s Multi-Instance Spanning Tree
  - Obsługa 64 instancji protokołu STP
  - Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
  - Redundancja 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 liku podstawowego
- Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED.
- Realizacja funkcji 802.1Q tunneling (QinQ)
- Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
- Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
- Możliwość uruchomienia funkcji serwera DHCP
- Mechanizmy związane z bezpieczeństwem sieci:
  - Możliwość ustawiania wielu poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
  - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
  - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
  - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
  - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
  - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
  - Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
  - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
  - Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
  - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
  - Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
  - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
  - Obsługa list kontroli dostępu (ACL) następujących typów:
    - Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    - VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
    - Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    - Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
  - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
  - Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
  - Funkcja Private VLAN;
- Obsługa mechanizmów zapewaniających 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.

- Mechanizmy związane z zapewnieniem jakości usług w sieci:
  - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
  - Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
  - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
  - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
  - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
  - Kontrola sztormów dla ruchu broadcast/multicast/unicast,
  - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
- Obsługa protokołów i mechanizmów routingu:
  - Routing statyczny dla IPv4 i IPv6,
  - Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes,
  - Policy-based routing (PBR),
  - Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
  - Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
- Przełącznik umożliwiający lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
- Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
- Przełącznik posiadający 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.),
- Funkcjonalność sondy IP SLA Responder,

Zarządzanie

- Port konsoli,
- Dedykowany port Ethernet do zarządzania out-of-band,
- Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzajacego 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,
- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
- Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
- Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
- Wsparcie dla protokoły RESTCONF,
- Wsparcie dla protokołu gNMI,
- Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
- Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
- Funkcja 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,
- Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
  - Monitoring pracy przełącznika w zakresie:
    - Użycie CPU, użycie pamięci, temperatura pracy,
    - Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
    - Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
    - Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)
    - Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    - Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,

- Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
- Protokół REP (Resilient Ethernet Protocol),
- Protokół STP (Spanning Tree Protocol),
- Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),

▪ Konfiguracja przełącznika w zakresie:
  - Konfiguracja interfejsów Fizycznych:
    - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
    - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),
    - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,
    - przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
  - Logicznych typu „port channel":
    - opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
    - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,
    - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,
    - przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
  - Wirtualnych typu SVI:
    - opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP)

▪ Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
▪ Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
▪ Konfiguracja mechanizmów SPAN i RSPAN,
▪ Konfiguracja protokołu STP,
▪ Konfiguracja protokołu REP,
▪ Konfiguracja routingu statycznego i dynamicznego,
▪ Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
▪ Tworzenie i przypisanie list kontroli dostępu ACL,
▪ Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
▪ Konfiguracja i uruchomienie NetFlow,
▪ Konfiguracja polityk QoS,
▪ Administracja przełącznika w zakresie:
  - Zdalne uruchamianie komend linii poleceń,
  - Nazwa przełącznika,
  - Tryb pracy L2/L3,
  - Adres IP przełącznika do celów zarządzania zdalnego,
  - Konfiguracja serwera DHCP,
  - Konfiguracja DNS,
  - Czas systemowy w tym protokół NTP,
  - Konta administracyjne,
  - Upgrade oprogramowania,
  - Backup konfiguracji,
  - Zdalny restart urządzenia,
  - Konfiguracja i dostęp przez SNMP,
▪ Diagnostyka urządzenia:
  - Narzędzie PING i TRACEROUTE,
  - Przeglądanie logów systemowych,
  - Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

Parametry fizyczne:
- Możliwość montażu w szafie rack 19",
- Wysokość urządzenia 1 RU,
- Głębokość chassis urządzenia bez wentylatorów i kabli zasilających mniejsza niż 36 cm,
- Głębokość chassis urządzenia z wentylatorami i kablami zasilającymi mniejsza niż 40 cm,

Inne Wymagania:
- 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,
- Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

Wyposażenie urządzenia
- Przełącznik wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego,
- Przełącznik wyposażony w moduł rozszerzeń typu 4x1G/10G SFP/SFP+ wraz z następującymi wkładkami interfejsowymi:
- Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat,

Przełącznik L2 wyposażony w 24-port 100/1000Mbit PoE+, 4portów 10GB SFP+, dwa zasilacze – 17 szt.

Minimalne wymagania techniczne i funkcjonalne urządzenia:

- Typ i liczba portów: 24 porty 10/100/1000 BaseT RJ45 PoE+ (zgodne z IEEE 802.3at)
- Moc dostępna dla PoE:
  - 370W (z jednym zasilaczem o mocy 600W),
  - 370W (z dwoma zasilaczami o mocy 600W pracującymi w układzie redundantnym),
  - 740W (z dwoma zasilaczami o mocy 600W pracującymi w układzie współdzielenia mocy),
- Urządzenie wyposażone w slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco" – ang. hot swap) z możliwością obsadzenia następującymi modułami:
  - 4x1G SFP gdzie porty SFP możliwe do obsadzenia następującymi rodzajami wkładek interfejsowych:
    - Gigabit Ethernet 1000Base-T,
    - Gigabit Ethernet 1000Base-SX,
    - Gigabit Ethernet 1000Base-LX/LH,
    - Gigabit Ethernet 1000Base-EX,
    - Gigabit Ethernet 1000Base-ZX,
    - Gigabit Ethernet 1000Base-BX-D/U
  - 4x1G/10G SFP/SFP+ gdzie porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek interfejsowych:
    - Gigabit Ethernet 1000Base-T,
    - Gigabit Ethernet 1000Base-SX,
    - Gigabit Ethernet 1000Base-LX/LH,
    - Gigabit Ethernet 1000Base-EX,
    - Gigabit Ethernet 1000Base-ZX,
    - Gigabit Ethernet 1000Base-BX-D/U,
    - 10Gigabit Ethernet 10GBase-SR,
    - 10Gigabit Ethernet 10GBase-LR,
      10Gigabit Ethernet 10GBase-LRM,
      10Gigabit Ethernet 10GBase-ER,
      10Gigabit Ethernet 10GBase-ZR,
      10Gigabit Ethernet typu twinax (SFP+ - SFP+)
- Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
  - Przepustowość w ramach stosu - 160Gb/s,
  - 8 urządzeń w stosie,
  - Zarządzanie poprzez jeden adres IP,
  - Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

Zasilanie i chłodzenie:
- Redundantne i wymienne moduły wentylatorów,
- Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap),
- Przełącznik umożliwiający podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
- W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),

Parametry wydajnościowe:
- Przepustowość przełącznika (switching capacity): 128 Gb/s (bez podłączenia do stosu), 288 Gb/s (z podłączeniem do stosu)
- Prędkość przesyłania (forwarding rate): 95.23 Mpps
- Bufor pakietów – 6MB
- Pamięć DRAM – 4GB
- Pamięć flash – 4GB

Obsługa:
- 1000 aktywnych sieci VLAN
- 32000 adresów MAC

- 4000 tras IPv4
- 2000 tras IPv6
- Ilość wpisów w listach kontroli dostępu Security ACL – 1000
- ilość wpisów w listach kontroli dostępu QoS ACL – 1000
- 1000 interfejsów SVI L3
- Jumbo frame 9198B
- 48 połączeń zagregowanych typu „port channel”
- 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
- Obsługa protokołu NTP
- Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
- Przełącznik wspierający następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
  - IEEE 802.1w Rapid Spanning Tree
  - Per-VLAN Rapid Spanning Tree (PVRST+)
  - IEEE 802.1s Multi-Instance Spanning Tree
  - Obsługa 64 instancji protokołu STP
  - Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
  - Redundancja 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 liku podstawowego
- Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED.
- Realizacja funkcji 802.1Q tunneling (QinQ)
- Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
- Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
- Możliwość uruchomienia funkcji serwera DHCP
- Mechanizmy związane z bezpieczeństwem sieci:
  - Możliwość ustawiania wielu poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
  - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
  - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
  - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
  - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
  - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
  - Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
  - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
  - Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
  - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
  - Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
  - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
  - Obsługa list kontroli dostępu (ACL) następujących typów:
    - Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    - VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
    - Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    - Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
  - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
  - Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
  - Funkcja Private VLAN;
- Obsługa mechanizmów zapewaniających 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.
- Mechanizmy związane z zapewnieniem jakości usług w sieci:
  - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
  - Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,

- Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
- Kontrola sztormów dla ruchu broadcast/multicast/unicast,
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

- Obsługa protokołów i mechanizmów routingu:
  - Routing statyczny dla IPv4 i IPv6,
  - Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes,
  - Policy-based routing (PBR),
  - Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
  - Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
- Przełącznik umożliwiający lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
- Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
- Przełącznik posiadający 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.),
- Funkcjonalność sondy IP SLA Responder,

Zarządzanie

- Port konsoli,
- Dedykowany port Ethernet do zarządzania out-of-band,
- Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzajacego 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,
- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
- Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
- Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
- Wsparcie dla protokoły RESTCONF,
- Wsparcie dla protokołu gNMI,
- Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
- Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
- Funkcja 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,
- Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
  - Monitoring pracy przełącznika w zakresie:
    - Użycie CPU, użycie pamięci, temperatura pracy,
    - Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
    - Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
    - Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)
    - Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    - Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    - Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
    - Protokół REP (Resilient Ethernet Protocol),
    - Protokół STP (Spanning Tree Protocol),
    - Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),
- Konfiguracja przełącznika w zakresie:
  - Konfiguracja interfejsów Fizycznych:
    - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony),

włączenie lub wyłączenie trybu L2/L3,
- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),
- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,
- przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

- Logicznych typu „port channel":
  - opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
  - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,
  - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,
  - przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
- Wirtualnych typu SVI:
  - opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP)

- Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
- Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
- Konfiguracja mechanizmów SPAN i RSPAN,
- Konfiguracja protokołu STP,
- Konfiguracja protokołu REP,
- Konfiguracja routingu statycznego i dynamicznego,
- Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
- Tworzenie i przypisanie list kontroli dostępu ACL,
- Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
- Konfiguracja i uruchomienie NetFlow,
- Konfiguracja polityk QoS,
- Administracja przełącznika w zakresie:
  - Zdalne uruchamianie komend linii poleceń,
  - Nazwa przełącznika,
  - Tryb pracy L2/L3,
  - Adres IP przełącznika do celów zarządzania zdalnego,
  - Konfiguracja serwera DHCP,
  - Konfiguracja DNS,
  - Czas systemowy w tym protokół NTP,
  - Konta administracyjne,
  - Upgrade oprogramowania,
  - Backup konfiguracji,
  - Zdalny restart urządzenia,
  - Konfiguracja i dostęp przez SNMP,
- Diagnostyka urządzenia:
  - Narzędzie PING i TRACEROUTE,
  - Przeglądanie logów systemowych,
  - Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

Parametry fizyczne:
- Możliwość montażu w szafie rack 19",
- Wysokość urządzenia 1 RU,
- Głębokość chassis urządzenia bez wentylatorów i kabli zasilających mniejsza niż 36 cm,
- Głębokość chassis urządzenia z wentylatorami i kablami zasilającymi mniejsza niż 40 cm,

Inne Wymagania:
- 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,
- Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

Wyposażenie urządzenia
- Przełącznik wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy

<table>
<tr><td></td><td></td><td>zasilacza podstawowego,
▪ Przełącznik wyposażony w moduł rozszerzeń typu 4x1G/10G SFP/SFP+ wraz z następującymi wkładkami interfejsowymi:
▪ Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat,</td></tr>
<tr><td>5.</td><td>Zestawienie wkładek SFP/SFP+</td><td>Wymagane jest dostarczenie modułów SFP / SFP+ oraz kabli w minimalnej ilości jak w tabeli.

Wszystkie dostarczone moduły mają być tego samego producenta jak dostarczony sprzęt aktywny

<table>
<tr><th>LP</th><th>Opis</th><th>Szt.</th></tr>
<tr><td>1</td><td>10GBASE-LR SFP Module, Enterprise-Class</td><td>96</td></tr>
<tr><td>2</td><td>1000BASE-T SFP transceiver module for Category 5 copper wire</td><td>2</td></tr>
<tr><td>3</td><td>1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM</td><td>16</td></tr>
<tr><td>4</td><td>Active Twinax cable assembly, 7m</td><td>4</td></tr>
<tr><td>5</td><td>100G QSFP28 Transceiver 100G-FR, 2km SMF, duplex, LC</td><td>8</td></tr>
<tr><td>6</td><td>100GBASE QSFP Active Optical Cable, 7m</td><td>2</td></tr>
<tr><td>7</td><td>25GBASE Active Optical SFP28 Cable, 7M</td><td>1</td></tr>
<tr><td>8</td><td>Dual Rate 10/25GBASE-CSR SFP Module</td><td>2</td></tr>
<tr><td>10</td><td>100GBASE QSFP Active Optical Cable, 7m</td><td>4</td></tr>
<tr><td>11</td><td>100G QSFP28 Transceiver 100G-FR, 2km SMF, duplex, LC</td><td>8</td></tr>
<tr><td>12</td><td>10GBASE Active Optical SFP+ Cable, 7M</td><td>2</td></tr>
</table>
</td></tr>
<tr><td colspan="3">Opis wymagań</td></tr>
<tr><td colspan="3">Dostarczone przełączniki L3, L2, punkty dostępowe WiFi oraz kontrolery Wifi muszą być w pełni zarządzane przez oprogramowanie dostarczone przez wykonawcę oprogramowania tj. Cisco Catalyst Center
Dostarczone przełączniki L3, L2, punkty dostępowe WiFi oraz kontrolery Wifi muszą w pełni współpracować z systemem bezpieczeństwa Cisco Identity Service dostarczonego przez Generalnego Wykonawcę.
Całość dostarczonego sprzętu oraz oprogramowania musi pochodzić od jednego producenta
Dostarczony sprzęt musi pochodzić z produkcji nie starszej niż 3 miesięcy od daty złożenia oferty
Zamawiający musi skierować do wykonania zamówienia co najmniej dwóch specjalistów, legitymujących wykształceniem wyższym (co najmniej pierwszego stopnia) w zakresie nauk inżynieryjno-technicznych lub nauk ścisłych i przyrodniczych, posiadających doświadczenie w – w ostatnich trzech latach przed dniem złożenia oferty - w montażu co najmniej 3 (trzech) sieci LAN.
Jeżeli producent oferowanych sprzętów sieciowych wymaga, aby instalacja, montaż, uruchomienie lub utrzymanie (serwisowanie) realizowały osoby posiadające wydawany przez niego certyfikat, to Wykonawca ma zapewnić skierowanie do realizacji zamówienia oraz wykonywania świadczeń w okresie gwarancji personel spełniający takie wymaganie.
Oferent zapewni w ramach całości dostarczonego rozwiązania dostęp do serwisu-wsparcia inżynierskiego na okres 3 lat. Okno zgłoszeń: 8x5xNBD, serwis dostępny w godzinach 8-16 pon-pt (bez świąt). Ilość bezpłatnych godzin inżynierskich w miesiącu minimum 25.

1) Wykonawca wykona wdrożenie, instalację oraz konfigurację dostarczonych urządzeń w następującym zakresie:
• Dostarczenie sprzętu do serwerowni;
• Wykonanie projektu wdrożeniowego oraz dokumentacji powykonawczej;
• Montaż sprzętu w głównej serwerowni oraz w pośrednich punktach dystrybucyjnych, w tym montaż kabli LAN oraz kabli zasilających;
• Podłączenie sprzętu do sieci zasilającej;
2) W ramach wdrożenia Wykonawca zobowiązany jest do:
a. instalacji fizycznej urządzeń,
b. podłączenia kabli,
c. konfiguracji urządzeń niezbędnej do uruchomienia (adresacja interfejsów, konfiguracja uwierzytelniania, konfiguracja usług NTP, DNS, SNMP, Syslog, dodanie do systemu monitorowania Cisco Catalyst Center, ISE),
d. instalacji i konfiguracji systemu do zarządzania urządzeniami posiadanymi przez Zamawiającego oraz dostarczonymi w ramach zamówienia (w tym dodanie urządzeń do systemu zarządzania siecią LAN).

Opis usług wdrożeniowych infrastruktury sieciowej
W ramach realizacji projektu wdrożenia infrastruktury sieciowej wymagane jest wykonanie kompleksowej usługi instalacji, konfiguracji oraz uruchomienia urządzeń klasy Enterprise. Zakres prac obejmuje następujące elementy:</td></tr>
</table>

1. Klaster zapór sieciowych – NGFW

W ramach wdrożenia klastra wysokiej dostępności (HA) Next Generation Firewalli wymagane jest:

- Przygotowanie planu wdrożenia wraz z konfiguracją oprogramowania
- Fizyczna instalacja i montaż urządzeń w środowisku Data Center,
- Konfiguracja klastra HA (active/standby),
- Wdrożenie polityk bezpieczeństwa dla infrastruktury sieci LAN,
- Aktywację i konfiguracja funkcjonalności: Threat, Malware, URL Filtering,
- testy poprawności działania klastra oraz mechanizmów failover.
- Dokumentacja powykonawcza:

Schemat sieci
Raport końcowy testów powdrożeniowych
Protokół odbioru

2. Klaster routerów brzegowych

Dla zapewnienia niezawodności i wysokiej dostępności usług WAN, wymagana jest:

- Instalacja fizyczna urządzeń brzegowych - router,
- Konfiguracja routingu statycznego i dynamicznego (np. OSPF/BGP),
- Zestawienie klastra urządzeń z odpowiednią redundancją i przełączaniem awaryjnym,
- Testy wydajnościowe i funkcjonalne.
- Dokumentacja powykonawcza:

Schemat sieci
Raport końcowy testów powdrożeniowych
Protokół odbioru

3. Przełączniki Data Center – przełączniki dostępowe dla serwerów (4 sztuki)

W obszarze rdzenia centrum danych wymagane jest:

- Fizyczna instalacja czterech przełączników DC,
- Wstępna konfiguracja urządzeń,
- Aktualizacja oprogramowania do najnowszej zalecanej wersji,
- Konfiguracja interfejsów sieciowych,
- Konfiguracja sieci warstwy 2/3 (VLAN, vPC, VXLAN, EVPN – zgodnie z wymaganiami),
- Optymalizację pod kątem wysokiej wydajności, niskich opóźnień i niezawodności,
- Testy wydajnościowe i połączeniowe
- Dokumentacja powykonawcza:

Schemat sieci
Raport końcowy testów powdrożeniowych
Protokół odbioru

4. Przełączniki szkieletowe CORE – 2 sztuki

Dla zapewnienia wydajnego i stabilnego szkieletu sieci LAN wymagane jest:

- Montaż oraz konfiguracja dwóch przełączników CORE (48x 25G, 4x 100G),
- Konfiguracja routingu, agregacji łączy (LAG), VRF,
- Zabezpieczenia warstwy dostępowej (ACL, DHCP snooping, BPDU Guard),
- Konfiguracja wirtualnego klastra przełączników
- Dokumentacja powykonawcza:

Schemat sieci
Raport końcowy testów powdrożeniowych
Protokół odbioru

5. Przełączniki dostępowe

Zakres działań:

- Fizyczna instalacja i montaż przełączników w lokalizacjach końcowych.
- Konfiguracja warstwy 2 (VLAN, porty dostępu/trunk).
- Konfiguracja warstwy 3 (jeśli wymagane, np. SVI, routing statyczny).
- Konfiguracja zabezpieczeń dostępowych:
    - Port Security
    - BPDU Guard
    - Storm Control
    - DHCP Snooping
- Dynamic ARP Inspection (DAI)Wdrożenie funkcji automatyzacji i zarządzania portami (np. Auto Smartports, Profilowanie urządzeń).
- Testy działania oraz weryfikacja komunikacji sieciowej.
- Dokumentacja powykonawcza:

Schemat sieci
Raport końcowy testów powdrożeniowych
Protokół odbioru

6. Przełączniki DMZ

Zakres działań:

- Instalacja przełączników w strefie DMZ zgodnie z założeniami projektu wdrożeniowego.
- Fizyczne podłączenie do zapór sieciowych (NGFW) oraz odpowiednich serwerów i systemów końcowych.

- Konfiguracja VLAN i segmentacja ruchu zgodnie z politykami bezpieczeństwa (np. strefy serwerowe, monitoring, zarządzanie).
- Wdrożenie mechanizmów zabezpieczeń na poziomie warstwy 2/3
- Wdrożenie redundancji i agregacji połączeń (LAG, STP/VPC).
- Testy zgodności działania z zaporami sieciowymi oraz politykami ruchu DMZ.
- Dokumentacja powykonawcza:

Schemat sieci
Raport końcowy testów powdrożeniowych
Protokół odbioru

7. Instalacja i konfiguracja klastra kontrolerów sieci Wi-Fi

Dla zapewnienia wydajnego i stabilnego działania sieci Wifi wymagane jest:

- Projekt logiczny i fizyczny rozplanowania kontrolerów
- Instalacja urządzeń w szafie RACK lub wskazanym miejscu.
- Konfiguracja redundancji (klaster HA – high availability).
- Konfiguracja polityk dostępu, SSID, zabezpieczeń (WPA2/WPA3, VLAN, RADIUS/802.1x, itp.).
- Dokumentacja powykonawcza:

Schemat sieci
Raport końcowy testów powdrożeniowych
Protokół odbioru

8. Instalacja i konfiguracja Punktów dostępowych sieci Wi-Fi

Dla zapewnienia wydajnego i stabilnego działania sieci Wifi wymagane jest:
17 sztuk – przestrzeń hala 2:

- Rozmieszczenie urządzeń zgodnie z projektem radiowym.
- Montaż sufitowy/ścienny.
- Konfiguracja parametrów transmisji (kanały, moc, roaming).

28 sztuk – przestrzeń hala 1:

- Rozmieszczenie urządzeń zgodnie z projektem radiowym
- Dobór lokalizacji z uwzględnieniem zakłóceń i przeszkód konstrukcyjnych.
- Zastosowanie AP o zwiększonej odporności.
- Montaż sufitowy/ścienny.
- Konfiguracja parametrów transmisji (kanały, moc, roaming).

9. Dodatkowe wymagane usługi:

- przygotowanie dokumentacji technicznej powdrożeniowej (topologia fizyczna, logiczna, konfiguracje, instrukcje operacyjne),
- testy integracyjne i odbiorowe (UAT),
- szkolenie administratorów z obsługi nowej infrastruktury,
- wsparcie techniczne w okresie stabilizacji po uruchomieniu systemu.
- Testy zasięgu i pokrycia.
- Przed- i powdrożeniowe pomiary sieci bezprzewodowej
- Integracja dostarczonych urządzeń z system bezpieczeństwa NAC, który kontroluje dostęp do sieci komputerowej, sprawdzając tożsamość i stan bezpieczeństwa urządzeń podłączających się do sieci oraz środowiskiem do zarządzania i monitorowania sieci Cisco Catalyst Center posiadanych przez Zamawiającego
- Oferent zapewni w ramach całości dostarczonego rozwiązania dostęp do serwisu-wsparcia inżynierskiego na okres 3 lat. Okno zgłoszeń: 8x5xNBD, serwis dostępny w godzinach 8-16 pon-pt (bez świąt). Ilość bezpłatnych godzin inżynierskich w miesiącu minimum 25

10. Opis usług wdrożeniowych infrastruktury niskoprądowej

W ramach dostawy sprzętu aktywnego należy zapewnić wykonanie okablowania LAN oraz wyposażenia serwerowni. Zakres wymaganych prac został przedstawiony poniżej.

Zakres wymaganych prac

- Wykonanie okablowania strukturalnego pionowego (FO),
- Wykonanie okablowania strukturalnego między-szafowego w serwerowni w hali 1 oraz hali 2,
- Wykonanie sieci bezprzewodowej WLAN,
- Montaż szaf RACK.
- Montaż UPSów wraz z BYPASSem,
- Pomiary certyfikacyjne wykonanej infrastruktury światłowodowej
- Pomiary elektryczne wykonanej infrastruktury elektrycznej
- Częściowe pomiary dynamiczne infrastruktury miedzianej wykonanej przez generalnego wykonawcę (5% okablowania)
- Dostarczenie kompletnej dokumentacji powykonawczej

Opis techniczny

Branża telekomunikacyjna

W ramach niniejszego zadania Zamawiający wymaga zbudowanie okablowania strukturalnego pionowego kablem SM 9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 w celu skomunikowania szaf RACK.

LP	Relacja	Kabel	Długość [m]
1	Serwerownia Hala 1 – Serwerownia Hala 2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 48J	125
2	Serwerownia Hala 1 – LPD-0.1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	60
3	Serwerownia Hala 1 – LPD-0.2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	200
4	Serwerownia Hala 1 – LPD-R0.1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	195
5	Serwerownia Hala 1 – LPD-R0.2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	130
6	Serwerownia Hala 1 – LPD-R0.3	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	149
7	Serwerownia Hala 1 – LPD-R0.4	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	93
8	Serwerownia Hala 1 – LPD-R0.5	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	80
9	Serwerownia Hala 1 – LPD-R0.6	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	190
10	Serwerownia Hala 1 – LPD-R0.7	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	220
11	Serwerownia Hala 1 – LPD-R0.8	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	42
12	Serwerownia Hala 1 – LPD-R0.9	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	62
13	Serwerownia Hala 1 – LPD-R_Spr	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	20
14	Serwerownia Hala 1 – LPD-RW2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	40
15	Serwerownia Hala 1 – LPD-RW3	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	50
16	Serwerownia Hala 1 – LPD-1.1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	155
17	Serwerownia Hala 1 – LPD-1.2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	120
18	Serwerownia Hala 1 – LPD-1.3	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	210
19	Serwerownia Hala 1 – LPD-2.1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	200
20	Serwerownia Hala 1 – PD-P1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	220
21	Serwerownia Hala 1– PD-P2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	136
22	Serwerownia Hala 2 - LPD-0.1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	140
23	Serwerownia Hala 2 - LPD-0.2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	125
24	Serwerownia Hala 2- LPD-R0.1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	265
25	Serwerownia Hala 2- LPD-R0.2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	225
26	Serwerownia Hala 2- LPD-R0.3	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	220
27	Serwerownia Hala 2- LPD-R0.4	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	145
28	Serwerownia Hala 2- LPD-R0.5	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	115
29	Serwerownia Hala 2- LPD-R0.6	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	175
30	Serwerownia Hala 2- LPD-R0.7	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	145
31	Serwerownia Hala 2- LPD-R0.8	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	100
32	Serwerownia Hala 2- LPD-R0.9	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	70
33	Serwerownia Hala 2- LPD-R_Spr	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	105
34	Serwerownia Hala 2- LPD-RW2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	115
35	Serwerownia Hala 2- LPD-RW3	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	65
36	Serwerownia Hala 2- LPD-1.1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	205
37	Serwerownia Hala 2 - LPD-1.2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	175
38	Serwerownia Hala 2- LPD-1.3	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	25
39	Serwerownia Hala 2- LPD-2.1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	270
40	Serwerownia Hala 2- PD-P1	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	117
41	Serwerownia Hala 2- PD-P2	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J	35

- ***Architektura***
- Projektuje się dwie główne serwerownie zlokalizowane na Hali 1 (pomieszczenie H0.17) i w Hali 2 połączone kablem światłowodowym SM 9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 wg. 13501-6 48J.
- Połączenie między szafą CPD a lokalnymi puntami dystrybucyjnymi (LPD) należy zrealizować przy pomocy kabla światłowodowego SM 9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 wg. 13501-6 12J, zakończonego złączami LC w topologii podwójnej gwiazdy.
- W celu zakończenia okablowani w szafie należy zainstalować w każdej szafie przełącznicę światłowodową 48 portów OS2 1U 19". wyposażoną w płytę czołową z adapterami LC, zakłada się zakończenie czterech lokalnych punktów dystrybucyjnych (LPD) na jednej przełącznicy. W każdej szafie należy pozostawić 10mb zapasu kabla.

Instalacja WLAN:

W projektowanym systemie medium transmisyjnym które będzie realizować komunikację pomiędzy punktami dostępowymi sieci bezprzewodowej (AP), a projektowanymi przełącznikami sieciowymi będzie kabel S/FTP kategorii 6A, klasa B2ca.

Okablowanie należy zakończyć po stronie urządzenia gniazdem natynkowym 1xRJ-45 ekranowanym kat. 6A, po stronie szafy LPD zakończyć na panelu krosowym, a następnie połączyć z wolnym portem w przełączniku kablem krosowym ekranowanym kat. 6A.

W celu eliminacji konieczności stosowania osobnych przewodów do zasilania i transmisji danych projektowane przełączniki sieciowe realizować będą zasilanie poprzez PoE/PoE+.

Wdrożenie sieci bezprzewodowej WLAN dzielimy na 4 etapy:

- Symulacja.
- Pomiary przedwdrożeniowe.
- Wdrożenie.
- Pomiary powdrożeniowe.
- Przedstawiony zakres zawiera miejsca montażu punktów dostępowych (AP), jedynie na podstawie symulacji. W związku z tym, należy mieć świadomość, że jest to swego rodzaju przybliżenie, które powinno zostać poddane weryfikacji pomiarowej po postawieniu budynku. Dzięki pomiarom przedwdrożeniowym, uzyskujemy pełny obraz wdrażanego środowiska tj. wpływ różnego rodzaju obiektów (ściany, maszyny, regały itd.) na propagacje sygnału. Ponadto, na podstawie samego planu budynku, nie jesteśmy w wstanie w 100% ustalić miejsca dokładnego montażu punktów dostępowych- w tej kwestii jest konieczność weryfikacji miejsc montażu. Należy pamiętać, że punkty dostępowe powinny być opuszczone poniżej poziomu przeszkód, które negatywnie wpływają na propagacje sygnału.
- Pomiary powdrożeniowe należy wykonać na już w pełni pracującym środowisku produkcyjnym. Pozwala to na weryfikacje wdrożonego rozwiązania i wychwycenie ewentualnych braków w zasięgu sieci bezprzewodowej.
- W celu łatwego zarządzania okablowaniem strukturalnym każdy moduł RJ45 w punkcie logicznym musi posiadać oznaczanie jednoznacznie je identyfikujące. Projektuje się numerację gniazd logicznych sieci komputerowej wg poniższego schematu:

A / B / C, gdzie:
A – oznaczenie szafy dystrybucyjnej,
B – numer panelu w szafie,
C – numer portu w panelu.
Przykład: LPD/4/15-16

Branża elektryczna

W celu zasilenia projektowanych szaf RACK należy zabudować w serwerowni rozdzielnice typu Legrand XL³6x24M:

- Hala 2 (RUPS1, RUPS2),
- Hala 1 (RUPS1),
- W celu zapewniania nieprzerwanej pracy urządzeń IT należy zainstalować w szafach: MDF-1, MDF-3, MDF-5 UPS 15kVA z modułami akumulatorów 4x6Ah i BYPASSem. Połączenia wykonać zgodnie z wytycznymi producenta.
- Projektuje się zasilanie dwutorowe do każdej szafy RACK kablem 5x6mm² H07RN-F. W tym celu należy zainstalować dwie listwy PDU 32A, 230/400V, wejście IEC 60309, (36)C13/C19 w każdej z szaf. Kable wprowadzać od góry, połączenia wykonać wtykiem CEEkon.
- Dla projektowanej instalacji zakłada się montaż przeciwpożarowego wyłącznika prądu (PWP), z szybką ochronną przed przypadkowym użyciem. PWP zamontować przed wejściem do serwerowni na wysokości 140cm. Nad przyciskiem zamocować znak informacyjny „przeciwpożarowy wyłącznik prądu". Połączenia wykonać kablem HDGs 3x1,5mm².
- Należy dodatkowo uziemić każdą szafę RACK, po wykonaniu niezbędnych połączeń należy wykonać pomiarów ciągłości połączeń wyrównawczych.
- Szafa powinna być indywidualnie podłączona do szyny uziemiającej oraz wszystkie punkty uziemień powinny zostać połączone razem w celu zredukowania różnic potencjałów.

Zestawienie materiałów

Instalacja teletechniczna				
LP	Materiał	Model	Kod produktu	Ilość
1	Kabel światłowodowy	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 12J		6000mb
2	Kabel światłowodowy	9/125 OS2 G657.A2 LS0H klasa B2ca-s1a-d,a1 48JJ		200mb
3	Puszki przyłączeniowe dla AP			46 szt.
4	Koryto perforowane	D200H60		Wg. potrzeb
5	Kabel skrętka	S/FTP kat 6A B2ca		1500mb

6	Szafa RACK	Szafa Rack 48U 2265 mm (96,16")wys. x 800 mm (31,50")szer. x 1215 mm (47,83")gł. z (1) perforowanymi drzwiami przednimi z zamkiem 77%, (2) perforowanymi drzwiami tylnymi z dzielonym zamkiem 77%, kolor szary RAL 7021, bez prawych paneli bocznych	VR3357-005	3 szt.
7	Szafa RACK	Szafa Rack 48U 2265 mm (96.16")wys. x 800 mm (31.50")szer. x 1215 mm (47.83")gł. z (1) perforowanymi drzwiami przednimi z blokadą 77%, (2) perforowanymi drzwiami tylnymi z dzieloną blokadą 77%, kolor RAL 7021 czarny szary, bez lewych paneli bocznych	VR3357-006	3 szt.
8	Panel dolny szafy	800 x 1200, kolor RAL 7021	VRA6040	6 szt.
9	Zestaw akcesoriów do szaf	Zestaw osprzętu do łączenia w rząd	VRA5002	3 szt.
10	Zestaw akcesoriów do szaf	Zestaw uszczelek pomiędzy szafami w rzędzie	VRA5003	3 szt.
11	Panel zaślepiający	czarny plastikowy panel zaślepiający beznarzędziowy 1U 19”	VRA2001	1 szt.
12	Poziomy menedżer kabli	2U o głębokości 6", jednostronny z pokrywą	VRA1022	18szt.
13	Poziomy menedżer kabli	1U o głębokości 6", jednostronny z pokrywą	VRA1023	6 szt.
14	Pionowy menedżer kabli	do szafy 48U o szerokości 800 mm	VRA1017	6 szt.
15	Osłony na zawiasach	pionowy menedżer kabli do 48U o szerokości 800 mm	VRA1020	6 szt.
16	Koryto kablowe VR	800 mm	VRA8571	6 szt.
17	Koryto kablowe VR,	zaślepki	VRA8567	3 szt.
18	Pokrywa koryta kablowego	800 mm,	VRA8575	6 szt.
19	Koryto kablowe VR, zestaw złącz		VRA8502	2 szt.
20	UPS	Liebert ITA2 15kVA Rack-UPS z POD i zestawem szyn 8MIN autonomii przy 0,8PF z modułami akumulatorów 2x 6Ah LIB	ITA2151H1000A00	3 szt.
21	Listwa PDU	32A, 230/400V, wejście IEC 60309, (36)C13/C19	VP5G9006	12 szt.
22	Uniwersalny zasilacz	Z monitoringiem parametrów środowiskowych	WATCHDOG 100-UN	2 szt.
23	Karta komunikacyjna	SNMP/Web, Modbus, BACnet i LIFE.	IS-UNITY-DP	3 szt.
24	Zdalny czujnik środowiskowy	temperatura/wilgotność/punkt rosy + 2 dodatkowe sondy temperatury	GT3HD	6 szt.
Instalacja elektryczna				
25	Rozdzielnice elektryczne	Legrand $XL^3$6x24M	3 szt.	
26	Wyłącznik nadprądowy	C63A	6 szt.	
27	Wyłącznik nadprądowy	C32A	12 szt.	
28	Sygnalizacja napięcia	L400	3 szt.	
29	Wyłącznik przeciwpożarowy	PWP1-W01-A-11-2LED7\M	2 szt.	
30	Kabel do wyłącznika przeciwpożarowego	HDGs3x1,5mm²	30mb	
31	Kabel	N2XH-J 5x6 mm²	40mb	
32	Kabel	H07RN-F 5x6mm²	60mb	

Wymagania minimalne dla urządzeń

Monitoring środowiska serwerowni

- Czynniki środowiskowe, takie jak temperatura i wilgotność stwarzają poważne zagrożenie dla infrastruktury krytycznej. W celu zminimalizowania ryzyka projektuje się wdrażenie rozwiązania monitorowania środowiska, które gromadzą dane oraz ostrzegają użytkowników przed potencjalnymi zagrożeniami.
- Projektuje się zastosowanie czujników środowiska takich jak np. Vertiv Geist pozwalających użytkownikom śledzić warunki pracy i otrzymywać alerty w momencie przekroczenia limitów skonfigurowanych przez użytkownika.

System powinien posiadać możliwości:

- Wyświetlania danych czujnika w czasie rzeczywistym w bezpiecznym interfejsie sieciowym i otrzymywania powiadomienia za pośrednictwem poczty e-mail, SNMP lub bramki Email-to-SMS.
- System powinien wysyłać alerty w momentach przekroczenia parametrów skrajnych skonfigurowanych przez użytkownika co umożliwi rozwiązuj problemów zanim spowodują przestój.
- System kontroli środowiska serwerowni nie powinien wymagać instalowania specjalnego oprogramowania poza standardową przeglądarką internetową.

Wymagane monitorowane parametry w ramach systemu:

- temperatura
- wilgotność
- punkt rosy

Wymagane parametry fizyczne:

- wysokość 1U
- możliwość rozszerzenia o dodatkowe czujniki minimum 8

Wymagane certyfikacje/Aprobaty

- zgodność z dyrektywą RoHS
- zgodność z FCC część 15, klasa A
- zgodność z normą EN 55032 i EN 55024
- oznaczenie CE

Wymagania odnośnie gwarancji:

- Co najmniej 5 lat

Okablowanie strukturalne

Instalacja okablowania strukturalnego zostanie wykonana kablem S/FTP kategorii 6A. Wymagane jest wsparcie transmisji danych 10 Gigabit Ethernet (10GBASE-T). Kabel musi posiadać 4 pary i oznaczone kolorami: niebieskim, pomarańczowym, zielonym i brązowym. W obrębie pary pierwszy przewodnik jest w kolorze pary np. niebieskim, a drugi w kolorze pary i białym więc np. biało-niebieskim.
Kabel musi być ekranowany i posiadać konstrukcję S/FTP.
Powłoka kabla musi być w wykonaniu LSZH i w kolorze innym niż biały, szary i czerwony w celu odróżnienia kabli logicznych okablowania strukturalnego od kabli innych instalacji.
Projektowane systemy mają być zgodne z Klasyfikacją odporności ogniowej Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 305/2011 (CPR), EN 50575:2014+A:2016 oraz z polską normą SEP-E-007:2017-09, a co za tym idzie dedykowaną klasą odporności dla instalacji przebiegającej przez przejścia ewakuacyjne jest klasa B2ca -s1a d1 a1.

Wymagania dla systemów ekranowanych:

- wszystkie elementy systemu muszą być ekranowane,
- podłączenie ekranów kabli w panelach i gniazdach musi gwarantować ciągłość ekranu,
- należy zwrócić uwagę na montaż elementów połączeniowych, kontakt ekranu powinien występować na całym obwodzie zgodnie z zasadą klatki Faradaya,

Punkty przyłączeniowe logiczne:

Punkty Logiczne (gniazda przyłączeniowe punktów dostępowych AP WLAN) będą zaprojektowane w postaci modułów RJ45 keystone kat. 6A montowanych w adapterach z tworzywa sztucznego. osadzonych w ramkach i puszkach natynkowych. Zasilanie projektowanych AP będzie się odbywało po PoE(PoE+) z przełączników sieciowych zainstalowanych w szafach RACK.
Poszczególne moduły w Punkcie Logicznym należy oznakować w sposób trwały.

Standardy branżowe:

- ANSI/TIA-568.2-D dla kategorii 6_(A).
- ISO/IEC 11801-1
- PN-EN 50173
- IEC 60332-1 (pojedynczy kabel pionowy)
- IEC 60754 (halogenki i kwasy)
- IEC 61034 (brak gęstego dymu)
- Zgodność z dyrektywą RoHS

Klasyfikacja odporności ogniowej:

- Regulacja Unii Europejskiej rr. 305/2011 (CPR)
- EN 50575:2014+A:2016
- Klasa B2ca -s1a d1 a1

Parametry mechaniczne

- Rozmiar przewodnika: 23 AWG (0,57 mm ±}0,005)
- Średnica przewodnika w osłonie [mm]: 1.35 ±}0,05

- Ilość par: 4
- Zewnętrzna średnica kabla [mm]: 7,4 ±} 0,5
- Ekranowanie pary: Folia aluminiowa zapewniająca ekranowanie w 100%
- Drut uziemienia: Tak
- Ekran zewnętrzny: Brak

Dopuszczalne promienie zagięć:

- Podczas instalacji: 8 x średnica kabla
- Podczas pracy: 4 x średnica kabla
- Siła wciągania: max 100N
- Powłoka: LS0H
- Waga transportowa [kg]: 28,5
- Tolerancja długości kabla: +/- 5%

Panel miedziany

Kable należy zakończyć na ekranowych panelach kat. 6A. Panel musi posiadać 24 porty i wysokość 1U.

Okablowanie światłowodowe

Połączenia światłowodowe należy wykonać kablami światłowodowymi OS2 o konstrukcji luźnej tuby, która ma umożliwiać instalowanie wewnątrz jak i na zewnątrz pomieszczeń, włącznie z bezpośrednim układaniem w gruncie (w otoczeniu piasku). Projektowany kabel musi posiadać zabezpieczenie przed gryzoniami w postaci karbowanej stalowej taśmy oraz dodatkowe włókna szklane, jako element wzmacniający. Powłoka ma być wykonana w technologii LS0H która jest odporna na promieniowanie UV oraz ma być zgodna z Europejską Klasą B2ca-s1a,d1,a1. Kabel musi zawierać 12 włókna OS2 G657A2 ułożone w centralnej tubie wypełnionej żelem.

Standardy branżowe:

Włókna:

- IEC 60793-2-50 Kategoria B.1.3
- ISO/IEC 11801:2002, Kategoria OS2 oraz OS1
- ISO/IEC 24702: 2006, Kategoria OS2 oraz OS1
- IEEE 802.3 – 2012
- EN 50173-1:2007, Kategoria OS2 oraz OS1

Kabel:

- ISO 11801-1,
- EN 187 000,
- IEC 60794-2,
- EN 50173,
- IEC 60794-2-20
- Zgodność z dyrektywą ROSH

Testy palności:

- Regulacja EU 305/2011 (CPR)
- EN 50575:2014+A:2016
- Europejska Klasa: B2ca-s1a,d1,a1

Parametry transmisyjne

Tłumienie kabla zgodne ze standardem IEC 60793-1-40:

- 1310 nm – 1625 nm: ≤ 0,3 dB/km
- 1550 nm: ≤ 0,25 dB/km

Współczynnik załamania fali optycznej zgodny ze standardem IEC 60793-1-22:

- Dla fali 1310 nm: 1,467
- Dla fali 1550 nm: 1,468
- Dla fali 1625 nm: 1,468

- ***Szafy RACK***

Projektuje się szafy o wysokości 48U

- Wysokość: 2265 mm
- Szerokość: 800 mm
- Głębokość: 1215 mm

W szafach należy zainstalować UPS wraz z modułem akumulatorów (całkowita przestrzeń 9U). Szafy należy wyposażyć w monitor środowiska z wbudowanymi czujnikami wilgotności i punktu rosy. Każda szafę należy wyposażyć w 2 listwy PDU 32A 230/400V z gniazdami C13/C19 (36) wraz z czujnikiem monitorowania środowiska zewnętrznego.

Wymagania dla prowadzenia prac

Trasy kablowe:

Tory kablowe powinny być prowadzone równolegle lub prostopadle do krawędzi ścian w sposób niekolidujący z elementami stałymi i infrastrukturą znajdującą się w pomieszczeniach. Całe okablowanie powinno być ciągłe na całej długości toru bez złączy (okablowanie miedziane) Wszystkie kable powinny być poprawnie umieszczone w korytach w sposób uporządkowany. Przy układaniu okablowania należy przestrzegać dopuszczalnych promieni gięcia określonych przez producenta okablowania. W miejscach, gdzie znajduje się duża ilość istniejących kabli dla lepszej identyfikacji należy oznaczać przywieszkami, zgodnie ze standardem Zamawiającego.

Okablowanie należy prowadzić w istniejących kanałach/korytach kablowych w przypadku braku technicznych możliwości (brak ciągłości istniejących tras kablowych lub zajętości kanałów/koryt kablowych) należy ułożyć nowe koryta dostosowane do warunków środowiskowych i ująć je w dokumentacji powykonawczej.

Parametry nowych koryt kablowych:

- Szerokość: 200 mm
- Wysokość: 60 mm
- Grubość materiału: 1,2 mm
- Materiał: Stal ocynkowana zgodnie z PN-EN 10346:2011
- Maksymalne obciążenie: 20kg/m,

Ponadto wymaga się:

- Kable powinny krzyżować się pod kątem prostym.
- Metalowe konstrukcje wykorzystywane do prowadzenia kabli powinny być „uziemiane” na obu końcach. Jeżeli ich długość przekracza 50 m należy zastosować dodatkowe połączenia z systemem uziemiającym.
- Połączenia uziemiające powinny być możliwie najkrótsze.
- Pokrycia metalowych korytek i korytka powinny spełniać te same wymagania.
- Przy wprowadzaniu kabli do urządzenia, gdy mogą wystąpić trudności z zachowaniem wymaganych odstępów pomiędzy kablami. W takich przypadkach kable mogą być ułożone obok siebie na możliwie najkrótszym odcinku.
- Należy unikać równoległego układania kabli sygnałowych i zasilających względem zwodów i przewodów odprowadzających lub przewodzących elementów konstrukcyjnych wykorzystywanych do odprowadzania prądu piorunowego.
- Między kondygnacjami kable należy układać w biegnących pionowo ekranowanych kanałach, szybach, traktach itp.

Przy równoległym prowadzeniu kabli niskoprądowych i kabli energetycznych, dla uniknięcia tworzenia z przewodów pętli, w których mogłyby indukować się przepięcia, należy zachować pomiędzy nimi odległości uniemożliwiające występowanie przeników.

Przejścia przez ściany wewnętrzne:

Przejścia poprzez stropy należy wykonać wiertłem o odpowiedniej średnicy z zabezpieczeniem wykonanego otworu poprzez umieszczenie krótkiego odcinka rury w jego wnętrzu o średnicy min. 25 mm. Po wykonaniu przejścia należy dokonać wypełnienia ubytków w stropie powstałych na skutek przewiertu. Rury używane na przepusty powinny być dostatecznie wytrzymałe na działanie sił ściskających, z jakimi należy liczyć się w miejscu ich ułożenia. Wnętrza ścianek powinny być gładkie lub powleczone warstwą wygładzającą ich powierzchnie. Przepusty instalacyjne powinny mieć klasę odporności ogniowej (EI) ścian i stropów tego pomieszczenia. Przepust instalacyjny należy rozumieć miejsce przejścia instalacji użytkowych stosowanych w budynku przez przegrody. Wymóg zapewnienia odpowiedniej klasy odporności ogniowej dotyczy zarówno wypełnienia przestrzeni pomiędzy

elementem konstrukcji, a przechodzącą instalacją, jak i samej instalacji. Do izolacji stosować materiał niepalny np. wełna mineralna o gęstości minimum 150 kg/m3. Uszczelnianie należy wykonywać przy zastosowaniu zapraw ogniochronnych lub masy ogniochronnej. Po wykonaniu przepustu należy zastosować tabliczkę (firma wykonującą, data wykonania, typ masy uszczelniającej, identyfikator przejścia). Niedopuszczalne jest prowadzenie kabli przez niezabezpieczony otwór. Niedopuszczalne jest zastosowanie (w celu zabezpieczenia powłoką ognioodporną zapory ogniowej) masy uszczelniającej innego typu niż wcześniej zastosowana (dotyczy przejść przez istniejące zapory ogniowe).

Pomiary

Po zakończeniu prac należy wykonać pomiary które należy udokumentować protokołami. Pomiary powinny zostać wykonane zgodnie z normą PN-EN 50346:2004/A1+A2:2009. Pomiary należy wykonać dla wszystkich interfejsów okablowania. W przypadku sieci miedzianej pomiary należy wykonać w konfiguracji pomiarowej łącza stałego (ang. „Permanent Link") – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego.

Wymagane parametry testu dla kabli miedzianych:

- Wire Map – mapa połączeń,
- Length – długość,
- Propagation delay – opóźnienie propagacji,
- Resistance - Rezystancja
- Delay skew – opóźnienie skrośne,
- NEXT (near end cross-talk) – przesłuch zbliżny,
- PSNEXT – Power sum next,
- ACR – attenuation to crosstalk ratio,
- PSACR – Power sum ACR,
- ELFEXT,
- PSELFEXT,
- Insertion loss – straty wtrąceniowe,
- Return loss – straty odbiciowe.

Wymagania odnośnie pomiarów linii miedzianych:

- Wymaga się, aby urządzenia pomiarowe były okresowo kalibrowane według wytycznych producenta oraz posiadały możliwe najnowsze oprogramowanie,
- Pomiary muszą być wykonane zgodnie z zaprojektowaną wydajnością - klasą lub kategorią,
- Każdy pomiar musi zawierać wartości takich parametrów jak: mapa połączeń, długości par, tłumienność, opóźnienie propagacji, różnica opóźnień, rezystancja, NEXT, PS NEXT, ACR-N, PS ACR-N, ACR-F, PS ACR-F, RL
- Nie należy akceptować żadnych marginalnych wyników

Dla zapewnienia odpowiednich parametrów POE należy:
Podczas pomiarów należy włączyć testy DC Loop Resistance i DC Resistance Unbalance (między parami i w parze).

Okablowanie światłowodowe:
Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą PN-EN 14763- 3:2009/A1:2010. Wykonać pomiary tłumienia wtrąceniowego dla każdego łącza/włókna światłowodowego. Pomiary tłumienności i parametru Return loss (straty odbiciowe) wykonać dwukrotnie, włączając źródło światła z obu stron łącza.

Wymagania odnośnie pomiarów linii światłowodowych:
Wymaga się, aby dostarczyć pomiary wykonane w obu kierunkach w dwóch adekwatnych do rodzaju światłowodu oknach pomiarowych.

Oznaczenia okablowania

Należy stosować w celu lepszej identyfikacji okablowania trwałe przywieszki identyfikacyjne. Przywieszki muszą zawierać dane: Relacja, Typ okablowania, Data, Wykonawca, System.

Miejsca stosowania:

- Na końcach i łukach kabli,
- W miejscach charakterystycznych (skrzyżowania, przepusty, zbliżenia, odcinki proste co 15m).

Zamawiający wymaga, aby minimalny czas gwarancji udzielonej na przedmiot zamówienia wynosił nie mniej niż 36 miesięcy. Kryterium ustanowione dla Zapytania premiuje oferty odwołujące się do

dłuższego okresu gwarancji. Serwis w okresie gwarancji świadczony w trybie 24 godziny przez 7 dni w tygodniu na wszystkie elementy infrastruktury z gwarantowanym czasem naprawy awarii w ciągu 24 godzin. Dostawca ma zapewnić, aby usługi serwisowe świadczone były przez producenta oferowanego przedmiotu zamówienia.

Z tytułu dostawy przedmiotu zamówienia, wyłoniony Wykonawca otrzyma wynagrodzenie ryczałtowe, w rozumieniu art. 632 ustawy Kodeks cywilny.

Wynagrodzenie wskazane przez Wykonawcę musi obejmować wszystkie koszty związane dostawą i instalacją przedmiotu zamówienia. Wykonawca ponosi wyłącznie ryzyko oszacowania ceny.

Wysokość wynagrodzenia ryczałtowego, ustalonego w umowie zawartej z wyłonionym Wykonawcą wynikać będzie ze złożonej przez niego oferty, stanowiącej odpowiedź na niniejsze zapytanie ofertowe. Zapytanie ofertowe oraz oferta będą załącznikiem do umowy zawartej z wyłonionym Wykonawcą. Ze względu na zasady udzielania pomocy ze środków publicznych Zamawiający wyklucza negocjowanie oferty.

Oferta Wykonawcy musi uwzględniać koszty dostawy, montażu i uruchomienia przedmiotu zamówienia na adres: ul. Piołunowa, Wrocław. *Hala produkcyjna będzie zlokalizowana na działkach nr 7 i 8, AM-4, dz. Nr.: 39, AM-5, dz. Nr 15, AM-6, obręb 0030 Jerzmanowo, jedn. ewid. 026401_1 Wrocław przy ul. Piołunowej we Wrocławiu.*

III. Dodatkowe przedmioty zamówienia:

Nie dotyczy.

Uwaga! Warunkiem ważności oferty jest wypełnienie załączonego formularza ofertowego.

Zamawiający nie dopuszcza składania ofert wariantowych.

Zamawiający nie dopuszcza składanie ofert częściowych.

Każdy oferent może złożyć tylko jedną ofertę. Każda kolejna oferta złożona przez tego samego oferenta podlega odrzuceniu.

Wymaga się, aby oferty były ważne co najmniej 30 dni od daty zakończenia naboru ofert.

Planowany termin zawarcia umowy z dostawcą: do 31 października 2025 r.

IV. Sposób obliczania ceny:

Cena zakupu obejmuje cenę jednostkową zamówienia, czyli cenę netto, podatek VAT oraz cenę brutto.

Dopuszcza się składanie ofert w walutach innych niż złoty (PLN). Waluty obce zostaną przeliczone na złote (PLN) wg kursu średniego NBP z ostatniego dnia składania ofert.

Cena dla przedmiotu zamówienia może być tylko jedna, nie dopuszcza się wariantowości cen. Wszelkie upusty, rabaty, winny być od razu ujęte w obliczaniu ceny, tak by wyliczona cena za

realizację przedmiotu zamówienia była ceną ostateczną, bez konieczności dokonywania przez Zamawiającego przeliczeń i innych działań w celu jej określenia.

Cena musi uwzględniać wszystkie wymagania niniejszego Zapytania ofertowego oraz obejmować wszelkie koszty związane z terminowym i prawidłowym dostarczeniem przedmiotu zamówienia. Dostawca ponosi wyłączne ryzyko oszacowania ceny.

Uwaga: umowa zawarta z Dostawcą będzie zawierała postanowienia dotyczące zasad zmian tej umowy (wskazanych w pkt XIX niniejszego Zapytania) oraz możliwości zmiany terminu obowiązywania tej umowy.

V. Zasady płatności:

Zamawiający przewiduje następujące płatności częściowe:
- 30% ceny, w formie zaliczki, płatnej w terminie do 30 dni od dnia podpisania umowy; Zamawiający dopuszcza skrócenie terminu zapłaty zaliczki;
- 50% ceny w terminie do 30 dni przed wysyłką przedmiotu zamówienia do Zamawiającego potwierdzoną informacją pisemną od dostawcy zweryfikowaną przez Zamawiającego;
- 20% ceny w terminie do 30 dni od dnia dostarczenia, zakończenia instalacji przedmiotu zamówienia, potwierdzonego protokołem odbioru, opatrzonym przez Strony klauzulą „bez zastrzeżeń”.

VI. Termin składania ofert:

Termin składania ofert rozpoczyna się z dniem 5.09.2025 r. i będą one przyjmowane do dnia 8.10.2025 r. do godz. 10:00

Oferty będą rozpatrywane po 8.10.2025 r.

Na pytania dotyczące przedmiotu zamówienia oraz zasad niniejszego postępowania odpowiedzi udziela Adam Żelazny. Pytania należy składać poprzez adres e-mail: fabryka.piolunowa@roltec.pl. Wykonawcy będą mogli zadawać pytania wyłącznie za pośrednictwem poczty e-mail i tylko na tak zadane pytania Zamawiający udzieli odpowiedzi. Zamawiający będzie publikował pytania zadane przez wykonawców oraz udzielone odpowiedzi na swojej stronie internetowej. Mechanizm ten wprowadzany jest w celu zapewnienia wszystkim wykonawcom tożsamego zbioru informacji o warunkach postępowania.

VII. Planowany termin i miejsce realizacji zamówienia:

Całość zamówienia zostanie zrealizowana do 30 kwietnia 2026 r. Maksymalny termin realizacji zamówienia – uwzględniający zasady zmian w Umowie określone w niniejszym Zapytaniu - nie może przekroczyć 31 maja 2026 r.

Zamawiający dopuszcza możliwość zmiany terminu realizacji zamówienia na zasadach określonych w niniejszym Zapytaniu.

Miejsce wykonania zamówienia:

ul. Piołunowa, Wrocław. *Hala produkcyjna będzie zlokalizowana na działkach nr 7 i 8, AM-4, dz. Nr.: 39, AM-5, dz. Nr 15, AM-6, obręb 0030 Jerzmanowo, jedn. ewid. 026401_1 Wrocław przy ul. Piołunowej we Wrocławiu.*

Uwaga: prawidłowe wykonanie przedmiotu zamówienia w terminach określonych powyżej, będzie zabezpieczone zastrzeżeniem w umowie kar umownych o wartości 0,2% wynagrodzenia Dostawcy za każdy dzień zwłoki; kara umowna będzie naliczana do wartości 5% wartości zamówienia, przy

czym umowa będzie zakładała także możliwość dochodzenia przez Zamawiającego naprawienia szkody na zasadach ogólnych, jeśli wartość szkody będzie przekraczała wartość naliczonych kar umownych.

VIII. Miejsce, sposób i termin składania ofert:

1.Wykonawca może złożyć jedną ofertę. Złożenie więcej niż jednej oferty spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.

2. Oferta składana jest wyłącznie w formie elektronicznej, na adres e-mail Zamawiającego: fabryka.piolunowa@roltec.pl. Wykonawca może zabezpieczyć formularz ofertowym hasłem zabezpieczającym plik przed otworzeniem przez osobę nieuprawnioną, które przekaże Zamawiającemu w dniu 9.10.2025 r. przed godziną 12.00, tj. przed ustaloną godziną otwarcia ofert. Przekazanie hasła zabezpieczającego następuje wyłącznie w formie elektronicznej na adres e-mail Zamawiającego: fabryka.piolunowa@roltec.pl.

Uwaga: jeżeli Wykonawca zabezpieczy formularz ofertowy hasłem, a nie przekaże go do Zamawiającego przed wyznaczonym terminem lub przekazane hasło nie będzie pozwalało otworzyć pliku, Zamawiający ofertę odrzuci bez wzywania do poprawy.

3.Do upływu terminu składania ofert, Wykonawca może wycofać lub zmienić ofertę – składające Zamawiającemu jednoznaczne oświadczenie o zmianie lub wycofaniu Oferty.

4. Oferta musi być złożona na formularzu opublikowanym przez Zamawiającego oraz zawierać wszystkie wymagane załączniki.

5. Oferta musi być podpisana przez Wykonawcę, tj. osobę (osoby) reprezentującą Wykonawcę, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub osobę (osoby) upoważnioną do reprezentowania Wykonawcy.

6. Jeżeli osoba (osoby) podpisująca ofertę (reprezentująca Wykonawcę) działa na podstawie pełnomocnictwa, pełnomocnictwo to w formie oryginału (w formie elektronicznej, zgodnie z art. 78^1 Kodeksu cywilnego) musi zostać dołączone do oferty.

7.Oferta wraz z załącznikami musi być sporządzona w języku polskim. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

8.Oferta musi zawierać:
a) Formularz ofertowy (Załącznik nr 1 do Zapytania ofertowego) wraz z załącznikami: dokumentami potwierdzającymi spełnienie minimalnego wymagania sytuacji ekonomicznej i finansowej.
b) Dokumenty, z których wynika prawo do złożenia oferty w imieniu Wykonawcy (oryginał w formie elektronicznej w rozumieniu art. 78^1 Kodeksu cywilnego lub kopia), chyba że Zamawiający może je uzyskać w szczególności za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 poz. 340). W przypadku, gdy oferta podpisywana jest zgodnie z zasadami reprezentacji określonymi w publicznym rejestrze (np. rejestrze przedsiębiorców KRS), zapewniającym bezpłatny dostęp do danych, Wykonawca nie jest obowiązany składać dodatkowych dokumentów.

W przypadku ofert składanych w formie elektronicznej, na adres e-mail wskazany w Zapytaniu, obowiązkiem Wykonawcy jest w formie załączników przesłać pliki zawierające wszystkie wymagane dokumenty.

9. Termin związania ofertą wynosi co najmniej 30 dni. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

10. Wykonawca samodzielnie lub na wniosek zamawiającego może przedłużyć termin związania ofertą, z tym, że zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 30 dni.

11.Termin składania ofert upływa 8.10.2025 r. o godzinie 10:00. Oferty złożone po tak określonym terminie nie będą podlegały ocenie. Przez złożenie oferty należy rozumieć sytuację, w której wpływa ona na serwer pocztowy Zamawiającego. Otwarcie ofert nastąpi w dniu 9.10.2025 r. o godzinie 12.00.

12. Wybór wykonawcy nastąpi do dnia: 17.10.2025 r. Zamawiający dopuszcza zmianę tego terminu.

13. Zamawiający odrzuci ofertę, jeśli nie zawiera wszystkich stron lub załączników, lub gdy Wykonawca nie przedstawi w ofercie lub załącznikach wszystkich wymaganych informacji.

14. Zamawiający poprawi w ofercie oczywiste omyłki pisarskie – niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.

15.Zamawiający zastrzega sobie prawo do odwołania postępowania w każdym czasie bez podania przyczyn. Zastrzega sobie również prawo do zwrócenia się do oferentów z prośbą o wydłużenie terminu związania z ofertą.

IX. Uprawnienia do wykonywania określonej działalności lub czynności:

Zamawiający nie precyzuje szczególnych wymagań w tym zakresie.

X. Wiedza i doświadczenie:

Zamawiający nie precyzuje szczególnych wymagań w tym zakresie

XI. Potencjał techniczny:

Zamawiający nie precyzuje szczególnych wymagań w tym zakresie.

XII. Osoby zdolne do wykonania zamówienia:

Zgodnie z opisem zamówienia (por. str. 44), Wykonawca ma skierować do wykonania zamówienia personel o kompetencjach wymaganych przez Zamawiającego.

XIII. Sytuacja ekonomiczna i finansowa:

Zamawiający wskazuje, że o udzielenie zamówienia może ubiegać się Wykonawca, którego przychody w ostatnim zamkniętym roku obrachunkowym wyniosły minimum 3.000,000,00 PLN (słownie: trzech milionów złotych).

Warunek zostanie spełniony na podstawie oświadczenia złożonego w formularzu oferty oraz dokumentów złożonych przez Wykonawcę wraz z ofertą, potwierdzających prawidłowość oświadczenia. W przypadku Wykonawców rozpoczynających działalność (działających krócej niż rok lub takich, który nie zamykali jeszcze roku obrotowego), składają oni oświadczenie w dobrej wierze oraz potwierdzające je dokumenty. Dokumenty składane wraz z ofertą muszą jednoznacznie potwierdzać treść oświadczenia. Brak złożenia takich dokumentów albo złożenie dokumentów niepotwierdzających jednoznacznie treści oświadczenia spowoduje odrzucenie oferty, bez wzywania Wykonawcy do jej poprawy lub uzupełnienia.

XIV. Dodatkowe warunki:

Nie dotyczy**.**

XV. Rodzaje i opis kryteriów mających wpływ na wybór oferty:

Przy rozpatrzeniu nadesłanych ofert będziemy kierować się następującymi kryteriami (odrębnie dla każdego elementu przedmiotu zamówienia):

L. P.	KRYTERIUM	WAGA	JEDNOSTKA MIARY
1.	Cena	70%	waluta PLN lub inna
2.	Gwarancja	20%	miesiące
3.	Czas reakcji serwisu (liczony od momentu zgłoszenia usterki przez Zamawiającego do momentu rozpoczęcia naprawy przez Dostawcę)	10%	godziny

Zamawiający dokona oceny ofert na podstawie wyniku osiągniętej liczby punktów wyliczonych w oparciu o następujące kryteria i ustaloną punktację do 100 pkt. (100% = 100 pkt.):

1. Punkty za kryterium „cena netto” zostaną obliczone wg następującego wzoru:

$$\frac{\text{Cena netto oferty najtańszej}}{\text{Cena netto oferty badanej}} \times 70 = \text{ilość punktów}$$

Przez cenę netto Zamawiający rozumie cenę bez podatku od towarów i usług (VAT).

Na potrzeby oceny kryterium, Zamawiający dokona przeliczenia ofert złożonych w walutach innych, niż PLN, według średniego kursu danej waluty w złotych ustalonego przez Narodowy Bank Polski, obowiązującego w dniu zakończenia naboru ofert.

Cena dla przedmiotu zamówienia może być tylko jedna, nie dopuszcza się wariantowości cen. Wszelkie upusty, rabaty, winny być od razu ujęte w obliczaniu ceny, tak by wyliczona cena za realizację przedmiotu zamówienia była ceną ostateczną, bez konieczności dokonywania przez Zamawiającego przeliczeń i innych działań w celu jej określenia.

Ze względu na zasady udzielania pomocy ze środków europejskich Zamawiający wyklucza negocjowanie oferty.

Cena musi uwzględniać wszystkie wymagania niniejszego zapytania ofertowego oraz obejmować wszelkie koszty związane z terminowym i prawidłowym wykonaniem przedmiotu zamówienia oraz warunkami i wytycznymi stawianymi przez Zamawiającego, odnoszącymi się do przedmiotu zamówienia. Dostawca ponosi wyłączne ryzyko oszacowania ceny.

Jeżeli zaoferowana cena lub koszt będą wydawać się rażąco niskie w stosunku do przedmiotu zamówienia, tj. będą różnić się o więcej niż 30% od średniej arytmetycznej cen wszystkich ważnych ofert niepodlegających odrzuceniu, lub będą budzić wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w Zapytaniu ofertowym lub wynikającymi z odrębnych przepisów, Zamawiający zażąda od Dostawcy złożenia w wyznaczonym terminie wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu. Zamawiający oceni te wyjaśnienia w konsultacji z Dostawcą i może odrzucić tę ofertę wyłącznie w przypadku, gdy złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej ceny lub kosztu w tej ofercie.

W powołanych przypadkach Zamawiający wezwie Dostawcę do szczegółowego określenia podstaw oszacowania oczekiwanej ceny. Dostawca będzie zobligowany do złożenia wyjaśnień w terminie 3 dni od daty otrzymania przez niego wezwania Zamawiającego.

Wezwanie będzie kierowane na adres e-mail, wskazany w formularzu oferty.

W przypadku, gdy Dostawca nie przedstawi wyjaśnień w wyznaczonym terminie lub wyjaśnienia Dostawcy wykażą, iż zamierzał wykonać przedmiot zamówienia odwołując się do rażąco niskiej ceny, Zamawiający odrzuci ofertę. W takim przypadku, Dostawca otrzyma informację o odrzuceniu jego oferty, wraz ze szczegółowym uzasadnieniem.

W przypadku, gdyby Dostawca wezwany do określenia podstaw oszacowania ceny dokonał zmiany swojej oferty w aspektach podlegających ocenie na podstawie ustanowionych kryteriów – oferta ta zostanie odrzucona.

2. Punkty za kryterium „gwarancja” zostaną obliczone wg następującego wzoru:

$$\frac{\text{Gwarancja w ofercie badanej}}{\text{Gwarancja najdłuższa spośród wszystkich ofert}} \text{ x 20 = ilość punktów}$$

Gwarancja liczona od daty odbioru urządzenia przez Zamawiającego, potwierdzonego protokołem z klauzulą „bez zastrzeżeń”. Nie krótsza niż 36 miesięcy na wykonany przedmiot zamówienia.
Oferta, która będzie odwoływała się do krótszego, niż 36 miesięcy, terminu gwarancji, zostanie odrzucona jako niespełniająca warunków postępowania.

Zamawiający określa minimalną oraz maksymalną długość okresu gwarancji, w przedziale od 36 miesięcy do 60 miesięcy.

W przypadku, gdy Dostawca w ogóle nie wskaże w ofercie oferowanego okresu gwarancji, Zamawiający przyjmie, że Dostawca nie oferuje gwarancji, i ofertę odrzuci.

Dostawca może zaproponować długość okresu gwarancji dłuższy niż wyznaczony maksymalny 60 miesięcy, jednak w tym przypadku Zamawiający przyjmie do obliczeń wartość 60 m-cy - najdłuższy przyjęty w kryterium oceny ofert. Dostawcy zobowiązani są oferować długości okresu gwarancji w pełnych miesiącach w przedziale od 36 do 60 miesięcy.

3. Punkty za kryterium „czas reakcji serwisu” zostaną obliczone wg następującego wzoru:

$$\frac{\text{Czas reakcji serwisu najkrótszy spośród wszystkich ofert}}{\text{Czas reakcji serwisu w ofercie badanej}} \text{ x 10 = ilość punktów}$$

Zamawiający wymaga, by Dostawca, w okresie gwarancji, zapewniał serwis (rozpoczęcie działań serwisowych) w czasie nie dłuższym niż 24 godzin od zgłoszenia przez Zamawiającego awarii lub usterki danego środka trwałego (czas reakcji serwisu).

Oferta odwołująca się do czasu reakcji serwisu dłuższego niż 24 godziny zostanie odrzucona jako niespełniająca warunków postępowania.

Czas reakcji serwisu liczony jest jako czas przyjazdu do Zamawiającego przedstawicieli Dostawcy lub producenta danego środka trwałego, odpowiedzialnych za prowadzenie prac naprawczych lub serwisowych przedmiotu zamówienia.

Czas reakcji liczony jest w pełnych godzinach, od momentu zgłoszenia takiej potrzeby (w formie elektronicznej: e mail wysłany na adres oznaczony w umowie zawartej z Dostawcą) w przypadku, gdy takie wezwanie zostanie zgłoszone w dniach roboczych (dniach innych niż soboty lub dni ustawowo wolne od pracy), w godzinach od 8.00 do 16.00.

Na potrzeby oceny kryterium oraz przyznania punktacji, Zamawiający wskazuje, że najkrótszy czas reakcji serwisu wynosi 16 godzin. Dostawca może zaoferować krótszy czas, jednak w tym przypadku Zamawiający przyjmie do obliczeń wartość 16 godzin.

Uwaga – ze względu na to, że oświadczenie o czasie reakcji serwisu może decydować o wyborze oferty, zobowiązanie Dostawcy będzie przeniesione do umowy oraz będzie zabezpieczone karami umownymi. Zamawiający wskazuje, że za każdą godzinę spóźnienia, względem oświadczenia złożonego w ofercie, Dostawca zapłaci karę umowną w wysokości 200,00 złotych. W przypadku, gdy wartość szkody będzie wyższa od wartości kar umownych, Zamawiający będzie uprawniony dochodzić odszkodowania na zasadach ogólnych.

Ocena końcowa danej oferty będzie liczona jako suma punktów uzyskanych w poszczególnych kryteriach, tj.: ilość punktów uzyskanych w kryterium 1 „cena netto” + ilość punktów uzyskanych w kryterium 2 „gwarancja” + ilość punktów uzyskanych w kryterium 3 „czas reakcji serwisu”.

Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą końcową ocenę.

Zobowiązania Dostawcy, wskazane w ofercie w zakresie: ceny, terminu gwarancji, czasu reakcji serwisu zostaną przeniesione do umowy z Dostawcą i będą uznawane za postanowienia istotne.

XVII. Informacje na temat zakresu wykluczenia:

W celu uniknięcia konfliktu interesów zamówienie nie może być udzielone podmiotom powiązanym z Zamawiającym osobowo lub kapitałowo (OFERTY WYKLUCZONE). Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między firmą Roltec sp. z o.o. lub osobami upoważnionymi do zaciągania zobowiązań w imieniu firmy Roltec sp. z o.o. lub osobami wykonującymi w imieniu firmy Roltec sp. z o.o. czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru Dostawcy a dostawcą, polegające w szczególności na:
a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej, posiadaniu co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa), pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,

b) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związaniu z tytułu przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z dostawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych dostawców ubiegających się o udzielenie zamówienia,

c) pozostawaniu z dostawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

Oferty niespełniające tego kryterium nie będą podlegać ocenie (oferty wykluczone).
Zamawiający wskazuje, że do zaciągania zobowiązań w jego imieniu jest:

- Adam Woźniak

Zamawiający wskazuje, że czynności związane z wyborem Dostawcy będą wykonywać:

- Adam Woźniak
- Artur Żelazny

XVIII. Udzielanie informacji:

Każdy podmiot zainteresowany ofertą ma prawo zwrócić się do Zamawiającego o wyjaśnienie treści zawartych w zapytaniu ofertowym oraz jego załącznikach.

Pytania muszą być złożone poprzez adres e-mail: fabryka.piolunowa@roltec.pl. W będą mogli zadawać pytania wyłącznie za pośrednictwem poczty e-mail i tylko na tak zadane pytania Zamawiający udzieli odpowiedzi. Zamawiający będzie publikował pytania i odpowiedzi na swojej stronie internetowej.

W imieniu Zamawiającego informacji o zasadach wyboru Wykonawcy oraz przedmiocie zamówienia udziela: Artur Żelazny.

Jeżeli w wyniku zmiany treści zapytania ofertowego niezbędny będzie dodatkowy czas na wprowadzenie zmian w ofertach, Zamawiający przedłuży termin składania ofert, zamieści taką informację na swojej stronie internetowej.

XIX. Warunki zmiany umowy:

Umowa zawarta w wyniku postępowania wszczętego na skutek niniejszego zapytania ofertowego, może zostać zmieniona w drodze aneksu do umowy, w formie pisemnej pod rygorem nieważności, w następującym zakresie i przypadkach:
1) Umowa może zostać zmieniona w sytuacji wystąpienia niemożliwych do przewidzenia okoliczności. Pojęcie to Zamawiający będzie interpretował w sposób odpowiadający postanowieniu pkt. 109 preambuły Dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE.
W świetle tego postanowienia, „Pojęcie niemożliwych do przewidzenia okoliczności odnosi się do okoliczności, których nie można było przewidzieć pomimo odpowiednio starannego przygotowania pierwotnego postępowania o udzielenie zamówienia przez instytucję zamawiającą, z uwzględnieniem dostępnych jej środków, charakteru i cech tego konkretnego projektu, dobrych praktyk w danej dziedzinie oraz konieczności zagwarantowania odpowiedniej relacji pomiędzy zasobami wykorzystanymi na przygotowanie postępowania jego przewidywalną wartością. Nie może to jednak mieć zastosowania w sytuacjach, w których modyfikacja powoduje zmianę charakteru całego zamówienia, na przykład przez zastąpienie zamawianych robót budowlanych, dostaw lub usług innym przedmiotem zamówienia lub przez całkowitą zmianę rodzaju zamówienia (…)”.
W takim przypadku, umowa zostanie zmieniona w ten sposób, by możliwe było odwrócenie lub naprawienie skutków wystąpienia niemożliwych do przewidzenia okoliczności.
W przypadku wystąpienia niemożliwych do przewidzenia okoliczności, możliwa jest także zmiana terminu dostaw y oraz terminu realizacji umowy.

2) Umowa może zostać zmieniona w przypadku zmiany Dostawcy, gdy wynika ona z sukcesji uniwersalnej lub częściowej w prawa i obowiązki pierwotnego dostawcy, w wyniku restrukturyzacji, w tym przejęcia, połączenia, nabycia lub upadłości, przez innego dostawcę, który spełnia pierwotnie ustalone kryteria kwalifikacji podmiotowej, pod warunkiem, że nie pociąga to za sobą innych istotnych modyfikacji umowy i nie ma na celu obejścia zasad, wynikających z niniejszego zapytania ofertowego, umowy o dofinansowanie zawartej z Ministerstwem Aktywów Państwowych.

3) Umowa może zostać zmieniona w przypadku, gdy zachodzi konieczność przedłużenia terminu wykonania zamówienia lub terminu wykonania obowiązku wynikającego z umowy z powodu wystąpienia siły wyższej. Przez siłę wyższą Zamawiający będzie rozumiał nieprzewidywalną, wyjątkową sytuację lub takie zdarzenie będące poza kontrolą stron niniejszej Umowy, które uniemożliwiają którejkolwiek z nich wywiązanie się ze swoich obowiązków na podstawie niniejszej Umowy, i które nie były wynikiem błędu lub zaniedbania po ich stronie lub po stronie ich poddostawców, i których nie można było uniknąć przez postępowa nie z odpowiednią i uzasadnioną należytą starannością. W takim wypadku, umowa zostanie wydłużona o czas trwania siły wyższej lub czas niezbędny do odwrócenia skutków wystąpienia siły wyższej lub zostanie zmieniony termin

wykonania obowiązku wynikającego z umowy, o czas trwania siły wyższej lub czas niezbędny do odwrócenia skutków wystąpienia siły wyższej.
W przypadku wystąpienia siły wyższej możliwa jest także zmiana terminu dostawy oraz terminu realizacji umowy.
W takim przypadku możliwa jest także zmiana terminu dostawy oraz terminu realizacji umowy.

4) Umowa może zostać zmieniona w sytuacji, gdy dojdzie do zmiany powszechnie obowiązujących przepisów prawa lub wprowadzenia nowych regulacji prawnych, mających wpływ na wykonanie niniejszej Umowy. W takim przypadku, umowa zostanie zmieniona w ten sposób, by opowiadała obowiązującym regulacjom prawnym.

5) Możliwa jest zmiana umowy z Dostawcą, gdy zmiany dotyczą realizacji dodatkowych dostaw lub usług od dotychczasowego Dostawcy, nieobjętych zamówieniem podstawowym, o ile stały się niezbędne i zostały spełnione łącznie następujące warunki:
• zmiana dostawcy nie może zostać dokonana z powodów ekonomicznych lub technicznych, w szczególności dotyczących zamienności lub interoperacyjności sprzętu, usług lub instalacji, zamówionych w ramach zamówienia podstawowego,
• zmiana dostawcy spowodowałaby istotną niedogodność lub znaczne zwiększenie kosztów dla zamawiającego,
• wartość każdej kolejnej zmiany nie przekracza 50% wartości zamówienia określonej pierwotnie w umowie.

6) Zmiana umowy możliwa jest także w przypadku, gdy nie prowadzi do zmiany ogólnego charakteru umowy i zostały spełnione łącznie następujące warunki:
i) konieczność zmiany umowy spowodowana jest okolicznościami, których zamawiający, działając z należytą starannością, nie mógł przewidzieć,
ii) wartość zmian nie przekracza 50% wartości zamówienia określonej pierwotnie w umowie,

7) Zmiana umowy możliwa jest także w przypadku, gdy zmiana nie prowadzi do zmiany ogólnego charakteru umowy, a łączna wartość zmian jest mniejsza niż 140 000 EUR w przypadku dostaw i usług i jednocześnie jest mniejsza od 10% wartości zamówienia określonej pierwotnie w umowie.

Nie stanowi zmiany umowy, w rozumieniu punktu 1. powyżej:
1) zmiana danych związanych z obsługą administracyjno-organizacyjną umowy (np. zmiana nr rachunku bankowego);
2) zmiana nazw stron lub ich formy prawnej (przy zachowaniu ciągłości podmiotowości prawnej) teleadresowych, zmiana osób wskazanych do kontaktów między Stronami.

XX. Klauzula RODO

Zgodnie z art. 13 ust. 1 i 2 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), dalej „RODO", informuję, że: Roltec sp. z o.o. ul. Św. Marcin 29/8, 61-806 Poznań
• Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia w ramach Projektu, objętego wsparciem w ramach Programu Operacyjnego Inteligentny Rozwój 2014- 2020.
• Pani/Pana dane osobowe będą udostępnione podmiotom uprawnionym do kontroli realizacji Projektu.
• Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do wywiązania się przez Zamawiającego z obowiązków, wynikających z umowy o dofinansowanie projektu. Zamawiający wskazuje, że ma obowiązek przechowywać dokumenty związane z realizacją Projektu nie krócej, niż przez 10 lat od daty płatności końcowej, o ile przepisy prawa dotyczące pomocy publicznej nie stanowią inaczej.

• w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
• posiada Pani/Pan:
- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO; wnioski takie będą oceniane przez Zamawiającego w świetle przepisów RODO;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
• nie przysługuje Pani/Panu:
- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

XXI. Informacja dotycząca umowy:

1. Zamawiający – występując jako wierzyciel, zobowiązuje się do współdziałania z Dostawcą celem wykonania zobowiązań Dostawcy (art. 354 § 2 Kodeksu Cywilnego).

XXII. Załączniki do zapytania ofertowego:

1. Formularz ofertowy.