**Opis Przedmiotu Zamówienia (OPZ)**

Przedmiotem zamówienia, jest dostawa i wdrożenie przełączników sieci LAN z usługami instalacji, konfiguracji, wsparcia technicznego, systemem do zarządzania infrastrukturą sieciową, wykonanie dokumentacji i przeprowadzenie warsztatu szkoleniowego. Zadaniem Wykonawcy będzie dostawa oraz wdrożenie rozwiązania sieciowego w istniejącej infrastrukturze sieci LAN Zamawiającego.

Celem dostawy przełączników do infrastruktury zamawiającego jest modernizacja środowiska sieci LAN KG PSP w obszarze zapewnienia bezpieczeństwa, niezawodności i dostępności usług świadczonych w sieci LAN, jak również wyższych wydajności i przepływności, przy zachowaniu zgodności z istniejącymi elementami oraz w oparciu  
o kierunki i zasady budowy wydajnych i bezpiecznych sieci.

Przedmiotem zamówienia jest w szczególności dostawa urządzeń oraz usług wymienionych poniżej:

1. **Przedmioty zamówienia:**
   1. Przełącznik sieciowy typu I – 3 szt.
   2. Przełącznik sieciowy typu II – 8 szt.
   3. Wkładki, połączenia i kable:
      1. Moduł Dual Rate 10/25GBASE-CSR SFP – 8 szt.
      2. Patchcord LC-LC MM OM4 50/125 duplex 2m – 15 szt.

oraz

* 1. Dostawa wraz z przełącznikami niezbędnego oprogramowania i licencji, modułów optycznych oraz kabli.
  2. Wykonanie audytu sieci LAN KGPSP i na tej podstawie przygotowanie projektu wymiany przełączników, z uwzględnieniem zmiany architektury połączeń, integracją  
     z pozostałą siecią i planem przełączeń oraz testami odbiorowymi. Projekt, plan przełączeń i testy odbioru musi być zatwierdzony przez Zamawiającego.
  3. Instalacja i konfiguracja dostarczonych urządzeń, a także innych przełączników posiadanych przez Zamawiającego zgodnie z projektem. Instalacja obejmuje też wymianę wszystkich patchcordów światłowodowych i miedzianych.
  4. Integracja Systemu z istniejącą infrastrukturą Zamawiającego, szczególnie systemem zarządzania Cisco Prime Infrastructure, systemem Cisco Application Control Interface i telefonią IP.
  5. Wykonanie dokumentacji powykonawczej Systemu.
  6. Wykonanie testów odbiorowych zgodnych z Projektem.
  7. Zapewnienie serwisu sprzętu w okresie trwania gwarancji.
  8. Zapewnienie dodatkowych godzin wsparcia technicznego sieci LAN w formie konsultacji.
  9. Zapewnienie co najmniej 60 miesięcznego okresu gwarancji i serwisu.
  10. Przeprowadzenie instruktażu i szkolenia dla wskazanych pracowników Zamawiającego w formie warsztatów – min. 2 dni.

Obecnie sieć LAN KG PSP zbudowana jest w oparciu o przełączniki firmy Cisco System. Rdzeń sieci stanowią dwa przełączniki C9500-24Y4C do których podłączone jest łączami 25 Mbps 7 sztuk przełączników C9300-48P w sześciu różnych węzłach sieci KG PSP oraz starsza część sieci obejmująca 30 przełączników rodzin Catalyst 2690X, 3560, 3750, 3850. Przełączniki zarządzane są przy pomocy oprogramowania Cisco Prime Infrastructure ver 3.10. Sieć LAN połączona jest z Data Center opartą na Cisco Application Centric Infrastructure (Cisco ACI) i przełącznikach Cisco Nexus. W sieci LAN pracuje telefonia IP oparta o rozwiązania Cisco Systems. KG PSP zamierza wymienić starsze przełączniki na nowe urządzenia i jednocześnie dokonać modernizacji sieci LAN podnosząc jej parametry: większa wydajność połączeń szkieletowych i połączeń dostępowych, możliwość zapewnienia zasilania UPoE (60W).

1. **Wymagania ogólne wspólne dla urządzeń wyszczególnionych w pkt. 1.1.-1.2.**

|  |  |  |
| --- | --- | --- |
| **CECHA** | | **WYMAGANIA OGÓLNE** |
| 2.1. | **OZNAKOWANIE** | Urządzenia muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu (nazwa, nr seryjny) jak i producenta. |
| 2.2. | **OZNAKOWANIE CE** | Wszystkie urządzenia muszą posiadać oznakowanie CE produktu albo spełniać normy równoważne. |
| 2.3. | **OPAKOWANIE** | Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych. |
| 2.4 | **DOKUMENTACJA** | Na żądanie Zamawiającego wymagane jest dostarczenie, wraz z dostawą urządzeń, szczegółowej dokumentacji technicznej producenta oferowanych produktów potwierdzającej spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia (Zamawiający dopuszcza w tym przypadku możliwość złożenia dokumentacji w języku angielskim). Dostarczane urządzenia będą nowe i będą pochodzić z bieżącej produkcji, a jednocześnie nie będą urządzeniami, które mogły być używane w innych projektach i poddane procesowi odnowienia. Wymagane jest dostarczenie wraz ze sprzętem pisemnego potwierdzenia wydanego przez producenta lub przedstawicielstwo producenta sprzętu, poświadczającego datę produkcji sprzętu. Sprzęt musi być wyprodukowany nie wcześniej niż w roku 2021. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający, że oprogramowanie zawarte w dostarczonym sprzęcie jest licencjonowane na Zamawiającego. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający zarejestrowanie kontraktu serwisowego na dostarczone urządzenia i oprogramowanie. |
| 2.5. | **KABLE ZASILAJĄCE** | Wszystkie urządzenia muszą być wyposażone w kable zasilające w standardzie kontynentalnym, typu C. |
| 2.6. | **KOMPATYBILNOŚĆ** | Ze względu na fakt, że wymiana obejmuje tylko część przełączników, zarządzanie będzie realizowane przez posiadane przez Zamawiającego oprogramowanie Cisco Prime Infrastructure oraz Cisco Application Centric Infrastructure (Cisco ACI). Nowe przełączniki muszą znajdować się na liście urządzeń zarządzanych przez Cisco Prime Infrastructure „Cisco Prime Infrastructure 3.9 Supported Devices”. Urządzenia muszą być podłączone i skonfigurowane do pracy w infrastrukturze sieciowej Zamawiającego oraz będzie można je podłączyć do pracy w infrastrukturze sieciowej Zamawiającego, która oprócz części LAN składa się także z Data Center opartego na kontrolerach Cisco Application Centric Infrastructure (Cisco ACI) ( w technologii „spine-leaf”) zarządzanej przez klaster trzech serwerów APIC-SERVER.  Ze względu na pożądaną pełną kompatybilność oraz zabezpieczenie uprawnień gwarancyjnych Zamawiającego, dostarczane w ramach Zamówienia rozwiązania (urządzenia oraz karty i moduły do nich) powinny pochodzić od jednego producenta, chyba że wymagania szczegółowe stanowią inaczej. W przypadku oferowania urządzeń różnych producentów, należy dostarczyć oświadczenia ich producentów o pełnej wzajemnej kompatybilności oraz oświadczenia o współpracy autoryzowanych placówek serwisowych producentów w zakresie usuwania problemów powstających na styku rozwiązań. |
| 2.7. | **GWARANCJA** | * minimum 60 miesięczna gwarancja świadczona na miejscu u klienta; * czas reakcji serwisu - do końca następnego dnia roboczego; * wykonawca zapewnia w okresie trwania gwarancji: * usługi serwisowe świadczone w miejscu instalacji urządzenia- zgłaszania usterek przez portal internetowy, telefonicznie lub mailowo * dostępność wsparcia technicznego w godzinach pracy zamawiającego (815 — 1615) * Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich * Serwis gwarancyjny musi obejmować prawo do aktualizacji wersji oprogramowania systemowego urządzeń oraz zapewniać Zamawiającemu bezpośredni dostęp do: nowych wersji oprogramowania; narzędzi konfiguracyjnych i dokumentacji technicznej; pomocy technicznej producentów, w tym możliwość samodzielnego otwierania zgłoszeń serwisowych u producenta * Dostarczane urządzenia muszą być objęte serwisem gwarancyjnym na okres 60 miesięcy, opartym na bezpośrednim serwisie producenta świadczonym w trybie 8x5xNBD (8 godzin dziennie, 5 dni w tygodniu, naprawa w następnym dniu roboczym); Serwis musi umożliwiać Zamawiającemu bezpośredni dostęp do stron producenta w celu pobrania najnowszego oprogramowania lub poprawek (ang. patch) do dostarczonych urządzeń, zgłaszania problemów serwisowych oraz bezpośredni dostęp Zamawiającego do TAC (Technical Assistance Center) producenta urządzenia |

1. **Wymagania dla przełącznika sieciowego typu I – 3 szt. (pkt.1.1.)**

|  |
| --- |
| **PARAMETRY I WYMAGANIA MINIMALNE** |
| * 1. Typ i liczba portów: * 48 portów 10/100/1000BaseT RJ-45 zgodnych z IEEE 802.3at (30W per port) * budżet mocy dla POE 437W * przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia |
| * 1. 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) |
| * 1. Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb): * 8x1/10G SFP+ * 2x40G QSFP * 4x100M/1G/2.5G/5G/10GBaseT RJ-45 * 2x25G SFP28 |
| * 1. Możliwość łączenia w stos 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 zgodnie z IEEE 802.3ad * Możliwość współdzielenia mocy zasilaczy dla grup liczących 4 przełączniki - tzn. zasilacze stanowią zasób wspólny dla wszystkich przełączników w grupie (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) |
| * 1. Parametry fizyczne * Urządzenia wyposażone w wymienny zasilacz AC 230V * Możliwość instalacji zasilacza redundantnego AC 230V * Możliwość instalacji zasilacza prądu stałego, jak również jednoczesnej instalacji zasilacza prądu zmiennego i stałego * Urządzenie wyposażone w redundantne i wymienne moduły wentylatorów * Wysokość przełącznika 1RU * Możliwość montażu w szafie 19” |
| * 1. Obsługa IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności |
| * 1. Parametry wydajnościowe: * Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) * Bufor pakietów –16MB * Pamięć DRAM – 8GB * Pamięć flash – 16GB * Obsługa * 1000 sieci VLAN/interfejsów SVI * 32.000 adresów MAC * 8.000 tras IPv4 * 4.000 tras IPv6 |
| * 1. Obsługa protokołu NTP |
| * 1. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping |
| * 1. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: * IEEE 802.1w Rapid Spanning Tree * IEEE 802.1s Multi-Instance Spanning Tree * Obsługa 128 instancji protokołu STP |
| * 1. Obsługa protokołu LLDP i LLDP-MED |
| * 1. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC |
| * 1. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego |
| * 1. Mechanizmy związane z bezpieczeństwem sieci: * Wiele 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 * 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 * Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www) * Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 * 5000 wpisów dla list kontroli dostępu (Security ACE) * 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 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) * Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing) * Funkcja Private VLAN * Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 64.000 strumieni |
| * 1. Zestaw narzędzi pozwalających na kontrolę pochodzenia przełączników i działającego na nich oprogramowania oraz wykluczenie możliwości ich modyfikacji podczas procesów produkcyjnych lub logistycznych obejmujące:   + podpisywanie cyfrowe i weryfikację podpisu wszystkich komponentów programowych przełącznika (BIOS, firmware itp.)   + wyposażenie przełączników w bezpieczne, odporne na manipulacje układy kryptograficzne, gwarantujące uwierzytelnienie oryginalności sprzętu i jego jednoznaczną identyfikację   + bezpieczne uruchamianie (secure boot), zapewniające sprzętową weryfikację sekwencji startowej i uniemożliwiające uruchomienie nielegalnie zmodyfikowanego oprogramowania systemowego |
| * 1. Możliwość uruchomienia funkcji serwera DHCP |
| * 1. Mechanizmy związane z zapewnieniem jakości usług w sieci: * Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi * 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 (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 |
| * 1. Obsługa protokołów routingu: * Routing statyczny dla IPv4 i IPv6 * Routing dynamiczny IPv4/IPv6 – RIP, OSPF (1000 tras) * Policy-based routing (PBR) * Obsługa protokołu redundancji bramy – VRRP |
| * 1. Przełącznik umożliwia 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 |
| * 1. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.) |
| * 1. Zarządzanie * Port konsoli * Dedykowany port Ethernet do zarządzania out-of-band * 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, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 * Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB * Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów * Obsługa protokołu gRPC Dial-Out i RESTCONF * Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych * Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą * Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku |
| * 1. Możliwość rozszerzenia funkcjonalności przełącznika poprzez zakup i aktywację odpowiedniej licencji (bez konieczności modyfikacji sprzętowych) o: * Obsługę zaawansowanych protokołów routingu IPv4 i IPv6 – IS-IS i BGP * Routing multicastów - PIM-SM, PIM-SSM * Multicast Source Discovery Protocol (MSDP) * VRF-Lite * Obsługę MPLS – w tym L3 VPN, Multicast VPN (mVPN), EoMPLS, VPLS * Wsparcie dla protokołu LISP zgodnie z RFC 6830 * Możliwość enkapsulacji ruchu w pakiety VXLAN * Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) kluczami o długości 256-bitów (gcm-aes-256) * 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) * Widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7) * Wbudowany analizator pakietów |
| * 1. Ukompletowanie urządzenia: * Licencje wymagane do zarządzaniem przełącznikiem z poziomu systemu Prime Infrastructure na okres taki jak gwarancja na sprzęt * Komplet kabli stakujących dla danych i zasilania, o długości co najmniej 1 m każdy * Zasilacz redundantny o parametrach identycznych jak podstawowy |

1. **Wymagania dla przełącznika sieciowego typu II – 8 szt. (pkt.1.2.)**

|  |
| --- |
| **PARAMETRY I WYMAGANIA MINIMALNE** |
| * 1. Typ i liczba portów: * 36 portów 100M/1G/2.5GBaseT RJ-45 zgodnych z IEEE 802.3bt type 3 (60W per port) * 12 portów mGIG 100M/1G/2.5G/5G/10GBaseT RJ-45 zgodnych z IEEE 802.3bt type 3 (60W per port) * budżet mocy dla POE 490W * przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia |
| * 1. 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) |
| * 1. Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb): * 8x1/10G SFP+ * 2x40G QSFP * 4x100M/1G/2.5G/5G/10GBaseT RJ-45 * 2x25G SFP28 |
| * 1. Możliwość łączenia w stos 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 zgodnie z IEEE 802.3ad * Możliwość współdzielenia mocy zasilaczy dla grup liczących 4 przełączniki - tzn. zasilacze stanowią zasób wspólny dla wszystkich przełączników w grupie (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) |
| * 1. Parametry fizyczne * Urządzenia wyposażone w wymienny zasilacz AC 230V * Możliwość instalacji zasilacza redundantnego AC 230V * Możliwość instalacji zasilacza prądu stałego, jak również jednoczesnej instalacji zasilacza prądu zmiennego i stałego * Urządzenie wyposażone w redundantne i wymienne moduły wentylatorów * Wysokość przełącznika 1RU * Możliwość montażu w szafie 19” |
| * 1. Obsługa IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności |
| * 1. Parametry wydajnościowe: * Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) * Bufor pakietów –16MB * Pamięć DRAM – 8GB * Pamięć flash – 16GB * Obsługa * 1000 sieci VLAN/interfejsów SVI * 32.000 adresów MAC * 8.000 tras IPv4 * 4.000 tras IPv6 |
| * 1. Obsługa protokołu NTP |
| * 1. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping |
| * 1. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: * IEEE 802.1w Rapid Spanning Tree * IEEE 802.1s Multi-Instance Spanning Tree * Obsługa 128 instancji protokołu STP |
| * 1. Obsługa protokołu LLDP i LLDP-MED. |
| * 1. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC |
| * 1. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego |
| * 1. Mechanizmy związane z bezpieczeństwem sieci: * Wiele 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 * 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 * Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www) * Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 * 5000 wpisów dla list kontroli dostępu (Security ACE) * 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 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) * Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing) * Funkcja Private VLAN * Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 64.000 strumieni |
| * 1. Zestaw narzędzi pozwalających na kontrolę pochodzenia przełączników i działającego na nich oprogramowania oraz wykluczenie możliwości ich modyfikacji podczas procesów produkcyjnych lub logistycznych obejmujące:   + podpisywanie cyfrowe i weryfikację podpisu wszystkich komponentów programowych przełącznika (BIOS, firmware itp.)   + wyposażenie przełączników w bezpieczne, odporne na manipulacje układy kryptograficzne, gwarantujące uwierzytelnienie oryginalności sprzętu i jego jednoznaczną identyfikację   + bezpieczne uruchamianie (secure boot), zapewniające sprzętową weryfikację sekwencji startowej i uniemożliwiające uruchomienie nielegalnie zmodyfikowanego oprogramowania systemowego |
| * 1. Możliwość uruchomienia funkcji serwera DHCP |
| * 1. Mechanizmy związane z zapewnieniem jakości usług w sieci: * Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi * 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 (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 |
| * 1. Obsługa protokołów routingu: * Routing statyczny dla IPv4 i IPv6 * Routing dynamiczny IPv4/IPv6 – RIP, OSPF (1000 tras) * Policy-based routing (PBR) * Obsługa protokołu redundancji bramy – VRRP |
| * 1. Przełącznik umożliwia 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 |
| * 1. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.) |
| * 1. Zarządzanie * Port konsoli * Dedykowany port Ethernet do zarządzania out-of-band * 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, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 * Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB * Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów * Obsługa protokołu gRPC Dial-Out i RESTCONF * Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych * Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą * Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku |
| * 1. Możliwość rozszerzenia funkcjonalności przełącznika poprzez zakup i aktywację odpowiedniej licencji (bez konieczności modyfikacji sprzętowych) o: * Obsługę zaawansowanych protokołów routingu IPv4 i IPv6 – IS-IS i BGP * Routing multicastów - PIM-SM, PIM-SSM * Multicast Source Discovery Protocol (MSDP) * VRF-Lite * Obsługę MPLS – w tym L3 VPN, Multicast VPN (mVPN), EoMPLS, VPLS * Wsparcie dla protokołu LISP zgodnie z RFC 6830 * Możliwość enkapsulacji ruchu w pakiety VXLAN * Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) kluczami o długości 256-bitów (gcm-aes-256) * 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) * Widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7) * Wbudowany analizator pakietów |
| * 1. Ukompletowanie urządzenia: * Licencje wymagane do zarządzaniem przełącznikiem z poziomu systemu Prime Infrastructure na okres taki jak gwarancja na sprzęt * Komplet kabli stakujących dla danych i zasilania * Zasilacz redundantny o parametrach identycznych jak podstawowy * 6 przełączników typ II musi zostać dostarczone z modułami uplink 2x10/25G SFP28 |

1. **Wymagania dla wkładek optycznych (pkt.1.3.1.) -**

|  |
| --- |
| **PARAMETRY I WYMAGANIA MINIMALNE** |
| * 1. Dual Rate 10/25GBASE-CSR SFP. Wkładki muszą być tego samego producenta co przełączniki i znajdować się na liście sprzętu kompatybilnego z dostarczonymi przełącznikami |

1. **Instalacja i konfiguracja**
   1. Przygotowanie Projektu oraz opracowanie planu wdrożenia dostarczanych urządzeń  
      i wymiany przełączników, z uwzględnieniem zmiany architektury połączeń, integracją  
      z pozostałą siecią, planem przełączeń oraz testami odbiorowymi. Projekt, plan przełączeń  
      i testów odbiorowych muszą być zatwierdzone przez ZAMAWIAJĄCEGO.
   2. Montaż urządzeń w szafach serwerowych ZAMAWIAJĄCEGO.
   3. Wykonanie połączeń fizycznych pomiędzy urządzeniami.
   4. Skonfigurowanie dostarczonych urządzeń do pracy w środowisku sieciowym Zamawiającego obejmujące integrację z istniejącą infrastrukturą Zamawiającego, szczególnie systemem zarządzania Cisco Prime Infrastructure, systemem Cisco Application Centric Infrastructure (Cisco ACI) i telefonią IP.
   5. Wykonanie dokumentacji powykonawczej oraz testów odbiorowych zgodnych z Projektem.
   6. Przeprowadzenie warsztatów z administrowania dostarczonymi urządzeniami w zakresie eksploatacji Systemu wraz z instruktażem na dostarczonych urządzeniach i oprogramowaniu. Program instruktażu zostanie uzgodniony z Zamawiającym. Liczbę osób biorących udział  
      w poszczególnych instruktażach oraz czas ich trwania zostanie uzgodniony z Zamawiającym. Dla oferty należy przyjąć dwa szkolenia jednodniowe ośmiogodzinne, każde dla co najmniej 4 osób prowadzonych na konfiguracjach sieci LAN KGPSP, dotyczące w szczególności administracji dostarczonymi urządzeniami aktywnymi w zakresie podstawowym oraz  
      z wykorzystaniem Systemu Monitoringu Cisco Prime Infrastructure.
   7. Zapewnienie serwisu sprzętu w okresie trwania gwarancji.
   8. Zapewnienie dodatkowego wsparcia technicznego sieci LAN w formie konsultacji przez inżyniera posiadającego certyfikat co najmniej CCIE- Enterprise Infrastructure – 30 godzin rocznie w okresie gwarancji.