**Załącznik nr 2 do SIWZ**

**Zarządzalne przełączniki dostępowe – 2 szt.**

1. **Wymagania ogólne dla dostarczanych urządzeń:**
2. Zamawiający wymaga, by dostarczony sprzęt był nowy oraz nieużywany (przy czym Zamawiający dopuszcza, by sprzęt był rozpakowany i uruchomiony przed jego dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania sprzętu, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem),
3. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonego przedmiotu zamówienia nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich, w szczególności Zamawiającemu nie mogą być zaoferowane sprzęt i oprogramowanie, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego.
4. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej w dniu poprzedzającym dzień składania ofert,
5. Wymagane jest, aby dostarczone urządzenia były sprzętem zakupionym w oficjalnym kanale sprzedaży producenta na terenie Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji powyższego wymogu u przedstawiciela producenta oferowanego rozwiązania.
6. Wymagane jest, aby data produkcji dostarczonych urządzeń nie była wcześniejsza niż 6 miesięcy.
7. **Warunki gwarancji, serwisu i wsparcia technicznego:**
8. Na dostarczany sprzęt musi być udzielona min. 36-miesięczna gwarancja liczona od dnia podpisania protokołu odbioru przez Zamawiającego; Zamawiający wymaga by zapewniona była naprawa lub wymiana urządzeń lub ich części, zgodnie z metodyką i zaleceniami producenta i Zamawiającego,
9. Wykonawca przejmuje na siebie wszelkie obowiązki związane z obsługą serwisu gwarancyjnego oferowanego sprzętu w okresie gwarancji,
10. Serwis gwarancyjny będzie świadczony w siedzibie Zamawiającego (miejscu instalacji i użytkowania sprzętu), w języku polskim (przyjmowanie zgłoszeń i realizacja świadczeń).
11. Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego (tj. poniedziałek – piątek, godz. 07:00-15:00),
12. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu trzech dni roboczych od momentu zdiagnozowania usterki,
13. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), faks, e-mail lub WWW (przez całą dobę),
14. Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla całości sprzętu i oprogramowania dostarczonego w ramach przedmiotu zamówienia,
15. Zamawiający otrzyma bezpośredni dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją całości sprzętu i oprogramowania dostarczonego w ramach przedmiotu zamówienia w godzinach pracy Zamawiającego,
16. Zamawiający uzyska bezpośredni dostęp do części chronionych stron internetowych producentów rozwiązań, umożliwiający:
	1. pobieranie nowych wersji oprogramowania,
	2. dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
	3. dostęp do pomocy technicznej producentów.
17. **Instalacja urządzeń:**
18. Wykonawca zobowiązany jest w szczególności dostarczyć, zainstalować, skonfigurować i uruchomić urządzenia zgodnie z wytycznymi Zamawiającego.
19. Instalacja i konfiguracja urządzeń obejmuje połączenie ich w stos, a następnie podłączenie stosu do głównego przełącznika sieci LAN Zamawiającego dwoma łączami agregowanymi, z których każde wyprowadzone jest z innego elementu stosu.
20. Urządzenia, które Wykonawca dostarcza Zamawiającemu muszą posiadać stosowne certyfikaty, oraz spełniać wszelkie wymogi i normy zastrzeżone przez obowiązujące w Polsce przepisy.
21. Do czasu przetestowania urządzenia i podpisania protokołu odbioru końcowego, Wykonawca ponosi ryzyko ich niesprawności lub wystąpienia innych wad, chyba że niesprawność lub wada powstały z winy Zamawiającego.
22. **Parametry techniczne:**
23. Przełącznik wyposażony 48 portów 10/100/1000BaseT RJ-45 wspierających standard IEEE 802.3at PoE+
24. Budżet mocy przeznaczony na funkcje PoE nie mniejszy niż 740W
25. Przełączniki muszą być dostarczone ze wszystkimi komponentami do instalacji w szafie rack 19''
26. Przełączniki muszą posiadać redundantne wentylatory
27. Każdy przełącznik musi posiadać minimum jeden zasilacz
28. Każdy przełącznik musi umożliwiać zastosowanie dwóch zasilaczy i redundancji zasilania (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
29. Pobór mocy nie więcej jak 1000W.
30. Wysokość przełącznika nie więcej jak 1RU
31. Każdy przełącznik musi posiadać porty typu UPLINK z możliwością obsadzenia wkładami (w zależnie od potrzeb):
	1. 4x10G SFP+
	2. 4x1G SFP
	3. 4x 1G i 10G SFP i SFP+
	4. porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
		1. Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U
		2. Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
32. Jeżeli którakolwiek z opisanych funkcjonalności wymaga licencji wymaga się jej dostarczenie na okres 3 lat,
33. Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
	1. Przepustowość w ramach stosu - 80Gb/s,
	2. 8 urządzeń w stosie,
	3. Zarządzanie poprzez jeden adres IP,
	4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
	5. Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),
34. Przełącznik musi posiadać minimalne parametry wydajnościowe:
	1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych i większych (przełącznik line-rate): 175Gbps
	2. Przepustowość przełącznika (switching capacity): 130Mpps
		1. Bufor pakietów – 6MB
		2. Pamięć DRAM – 2GB
		3. Pamięć flash – 4GB
	3. Obsługa:
		1. 1000 sieci VLAN, 500 interfejsów SVI
		2. 16000 adresów MAC
		3. 4000 tras IPv4
		4. 1500 tras IPv6
		5. 1000 tras multicast
		6. Ilość wpisów ACE dla list ACL –1500 wpisów
		7. musi posiadać sprzętową realizowane tworzenie statystyk ruchu w oparciu o NetFlow, wielkość tablicy monitorowanych strumieni wynosi minimum 16 000.
35. Przełącznik musi zapewnić obsługę protokołu NTP
36. Przełącznik musi zapewnić obsługę IGMPv1/2/3 i MLDv1/2 Snooping
37. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
	1. IEEE 802.1w Rapid Spanning Tree
	2. Per-VLAN Rapid Spanning Tree (PVRST+)
	3. IEEE 802.1s Multi-Instance Spanning Tree
	4. Obsługa minimum 64 instancji protokołu STP
38. Przełącznik musi zapewnić obsługę protokołu IEEE CDP, LLDP i LLDP-MED.
39. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
40. Przełącznik musi zapewnić obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
41. Przełącznik musi zapewnić możliwość uruchomienia funkcji serwera DHCP
42. Przełącznik musi zapewnić mechanizmy związane z bezpieczeństwem sieci:
	1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
	2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
	3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
	4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
	5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
	6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
	7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
	8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
	9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
	10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
	11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
	12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
	13. Obsługa list kontroli dostępu (ACL) następujących typów:
		1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
		2. możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
	14. 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),
	15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
	16. Funkcja Private VLAN;
43. Przełącznik musi zapewniać mechanizmy związane z zapewnieniem jakości usług w sieci:
	1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
	2. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
	3. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
	4. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting) w kierunku wejściowych i wyjściowym dla portu Ethernet
	5. Kontrola sztormów dla ruchu broadcast/multicast/unicast
	6. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP na wejściu i wyjściu z portu Ethernet
44. Przełącznik musi zapewniać obsługę protokołów i mechanizmów routingu (jeżeli funkcjonalność wymaga specjalnej licencji, Zamawiający nie wymaga takiej licencji) :
	1. Routing statyczny dla IPv4 i IPv6,
	2. Routing dynamiczny – RIP, OSPF, ISIS
	3. Policy-based routing (PBR),
	4. Routing multicastów - PIM-SM, PIM-SSM
	5. Multicast Source Discovery Protocol (MSDP)
	6. Obsługa protokołu redundancji bramy (VRRP)
	7. musi umożliwiać enkapsulację ruchu przy pomocy VXLAN’ów
	8. Realizacja protokołu LISP zgodnie z RFC 6830
45. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
46. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),
47. Przełącznik musi zapewnić zarządzanie poprzez:
	1. Port konsoli,
	2. Dedykowany port Ethernet do zarządzania out-of-band,
	3. 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,
	4. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
	5. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANG (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
	6. Obsługa protokołu gRPC Dial-Out
	7. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
	8. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
	9. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
	10. Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
		1. Monitoring pracy przełącznika w zakresie:
			1. Użycie CPU,
			2. Użycie pamięci,
			3. Temperatura pracy,
			4. Podstawowe informacje systemowe: rodzaj sprzętu, czas pracy, czas systemowy, oprogramowanie, data i czas ostatniej zmiany konfiguracji,
			5. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, wykorzystanie PoE,
			6. Informacji o urządzeniach sąsiednich podłączonych do przełącznika,
			7. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN,
			8. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3,
			9. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
		2. Konfigurację przełącznika w zakresie:
			1. Konfiguracja interfejsów L2:
			2. Konfiguracja interfejsów L3,
			3. Tworzenie i konfiguracja sieci VLAN,
			4. Konfiguracja protokołu STP,
			5. Tworzenie i konfiguracja wirtualnych instancji routingu (VRF),
			6. Konfiguracja routingu statycznego,
			7. Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
			8. Tworzenie i przypisanie list kontroli dostępu ACL,
			9. Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
			10. Konfiguracja i uruchomienie NetFlow,
		3. Administracja przełącznika w zakresie:
			1. Zdalne uruchamianie komend linii poleceń,
			2. Czas systemowy w tym protokół NTP,
			3. Konta administracyjne,
			4. Upgrade oprogramowania,
			5. Backup konfiguracji,
			6. Zdalny restart urządzenia,
			7. Konfiguracja i dostęp przez SNMP,
			8. Narzędzie PING i TRACEROUTE,
			9. Przeglądanie logów systemowych
48. Przełącznik musi mieć możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
49. Przełącznik musi mieć możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,
50. Wymagana jest możliwość stackowania przełącznika z będącymi w posiadaniu Zamawiającego przełącznikami serii Cisco 9200L.

**Moduły i kable stackujące – 2 szt.**

1. Wraz z przełącznikami muszą być dostarczone moduły i kable stackujące umożliwiające połączenie dostarczonych przełączników ze sobą.
2. Na dostarczany sprzęt musi być udzielona min. 36-miesięczna gwarancja liczona od dnia podpisania protokołu odbioru przez Zamawiającego.

**Wkładki SFP+ – 4 szt. oraz SFP – 1szt.**

1. Wraz z przełącznikami muszą być dostarczone cztery wkładki SFP+ 10Gb/s. Transceivery muszą zapewnić komunikację typu duplex, w technologii SingleMode i zapewnić wtyk LC.
2. Wraz z przełącznikami musi być dostarczona jedna wkładka SFP 1Gb/s. Transceiver musi zapewnić komunikację typu duplex, w technologii SingleMode i zapewnić wtyk LC.
3. Na dostarczany sprzęt musi być udzielona min. 36-miesięczna gwarancja liczona od dnia podpisania protokołu odbioru przez Zamawiającego.

**Zarządzane punkty dostępowe – 7 szt.**

1. Punkt dostępowy musi być urządzeniem posiadającym dwa moduły radiowe standardu IEEE 802.11b/g/n (2,4GHz) oraz 802.11a/n/ac (5GHz).
2. Punkt musi wspierać standardy IEEE 802.11a/b/g, 802.11n, 802.11ac, 802.11i.
3. Punkt dostępowy musi posiadać anteny zintegrowane.
4. Punkt powinien być wyposażone minimum jeden interfejs Ethernet 10/100/1000BASE-T
z możliwością zasilania z przełącznika sieciowego / PoE w standardzie IEEE 802.3af.
5. Punkt musi mieć posiadać zestaw montażowy umożliwiający zamontowanie go na ścianie wewnątrz budynku.
6. Punkt dostępowy musi umożliwiać zarządzanie nim z poziomu kontrolera Cisco 5500 Series Wireless Controller.
7. Automatycznego wykrywania i konfiguracji punktu dostępowego poprzez sieć LAN.
8. Możliwość konfiguracji różnych polityk bezpieczeństwa per SSID.
9. Możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID.
10. Uwierzytelnianie i autoryzacja za pomocą serwerów RADIUS lub za pomocą lokalnej bazy danych.
11. Filtrowanie MAC za pomocą serwerów RADIUS lub za pomocą lokalnej bazy danych.
12. Tworzenie list kontroli dostępu (ACL).
13. Możliwość profilowania użytkowników z przypisaniem im polityki QoS, ACL oraz VLAN.
14. Wykrywanie „nieprzyjaznych/obcych” punktów dostępowych oraz ataków typu DoS.
15. Punkt musi umożliwiać zasilanie go poprzez interfejs sieciowy PoE w standardzie 802.3af
16. Diodowa sygnalizacja stanu urządzenia.
17. Punkt powinien wspierać standardy bezpieczeństwa 802.11i, WPA, WPA2, 802.1X, AES
18. Punkt powinien wspierać standard EAP wraz z jego rozszerzeniami: EAP-FAST, EAP-GTC, PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, EAP-SIM.
19. Gwarancja minimum 24 miesiące w miejscu użytkowania sprzętu.

Złożenie podpisu jest równoznaczne z potwierdzeniem spełnienia warunków technicznych wymaganych powyżej.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 podpis osoby(osób) uprawnionej(ych)

 do reprezentowania wykonawcy