**ZAŁĄCZNIK NR 1**

**Przedmiot zamówienia oraz wytyczne.**

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 dostarczane urządzenia musi być udzielona minimum 36-miesięczna gwarancja liczona od dnia podpisania protokołu odbioru przedmiotu zamówienia przez Zamawiającego.
9. Zamawiający wymaga by zapewniona była naprawa lub wymiana urządzeń lub ich części, zgodnie z metodyką i zaleceniami producenta i Zamawiającego.
10. Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta.
11. Usługi wsparcia technicznego w zakresie obsługi zgłoszeń gwarancyjnych będą świadczone przez inżynierów Wykonawcy posiadających ważne certyfikaty producenta urządzeń na poziomie profesjonalisty.
12. Wykonawca przejmuje na siebie wszelkie obowiązki związane z obsługą serwisu gwarancyjnego oferowanego sprzętu w okresie gwarancji.
13. Serwis gwarancyjny będzie świadczony w siedzibie Zamawiającego (miejscu instalacji i użytkowania urządzeń), w języku polskim (przyjmowanie zgłoszeń i realizacja świadczeń).
14. Wykonawca udostępni pojedynczy punkt przyjmowania zgłoszeń dla całości sprzętu i oprogramowania dostarczonego w ramach przedmiotu zamówienia.
15. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego tj. poniedziałek – piątek, godz. 07:00-13:00), e-mail lub WWW (przez całą dobę).
16. 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.
17. 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).
18. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu jednego dnia roboczego od momentu zdiagnozowania usterki.
19. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę, Zamawiający dopuszcza podstawienie na czas naprawy urządzenia o nie gorszych parametrach funkcjonalnych; naprawa w takim przypadku nie może przekroczyć 14 dni od momentu zgłoszenia usterki a wymiana urządzenia nastąpi w miejscu jego instalacji i w czasie nie dłuższym niż następny dzień roboczy.
20. W okresie gwarancji koszty serwisu wbudowanych urządzeń są po stronie Wykonawcy. Wykonawca gwarantuje Zamawiającemu pełny zakres obsługi gwarancyjnej nieodpłatnie (z wyjątkiem uszkodzeń z winy użytkownika).
21. Wykonawca zobowiązuje się przenieść na Zamawiającego wszelkie uprawnienia z tytułu gwarancji na sprzedawany sprzęt wydając mu w tym celu odpowiednie dokumenty, najpóźniej w chwili podpisywania protokołu uruchomienia przedmiotu umowy, w tym instrukcje obsługi, karty gwarancyjne.
22. Zamawiający uzyska bezpośredni dostęp do części chronionych stron internetowych producentów rozwiązań, umożliwiający:
23. pobieranie nowych wersji oprogramowania,
24. dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
25. dostęp do pomocy technicznej producentów.
26. **Instalacja urządzeń:**
27. Wykonawca zobowiązany jest w szczególności dostarczyć, zainstalować, skonfigurować i uruchomić urządzenia zgodnie z wytycznymi Zamawiającego.
28. 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.
29. Urządzenia, które Wykonawca dostarcza Zamawiającemu muszą posiadać stosowne certyfikaty, oraz spełniać wszelkie wymogi i normy zastrzeżone przez obowiązujące w Polsce przepisy.
30. 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.
31. **Parametry techniczne:**
32. **Przełącznik sieciowy 48 portów – 1 szt.**

Wymagane parametry:

1. Przełącznik wolnostojący wyposażony w 48 portów 10/100/1000BaseT oraz 4 porty uplink SFP+ 1/10Gbps (łącznie przełącznik ma posiadać 52 porty LAN).
2. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 1000Base-T, 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-BX10, DWDM SFP, CWDM SFP oraz oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, DWDM SFP+.
3. Wymagana możliwość rozbudowy o funkcjonalność łączenia w stosy (stackowanie) z posiadanymi przez Zamawiającego przełącznikami Cisco serii 9200L poprzez dokupienie modułów i kabli stackujących z zapewnieniem następujących funkcjonalności:
4. Przepustowość magistrali stackującej – min. 80Gb/s,
5. Minimum 8 urządzeń w stosie,
6. Zarządzanie poprzez jeden adres IP,
7. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad.
8. Zasilanie i chłodzenie:
9. Przełącznik musi posiadać możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap).
10. Parametry wydajnościowe (co najmniej):
11. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate): 176Gbps oraz 130Mpps,
12. Bufor pakietów – 6MB,
13. Pamięć DRAM – 2GB,
14. Pamięć flash – 4GB,
15. Obsługa( co najmniej):
* 512 sieci VLAN,
* 16000 adresów MAC,
* 3000 tras IPv4,
* 1500 tras IPv6,
* 512 interfejsów L3,
* Ramek jumbo o wielkości 9198 bajtów,
* 1000 tras typu multicast,
* 1000 wpisów w polityce QoS,
* 1500 wpisów ACL.
1. Obsługa protokołu NTP.
2. Obsługa protokołu Cisco VTP i współpraca w tym zakresie z posiadanymi przez Zamawiającego przełącznikami Cisco 2960x oraz 9200L.
3. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping.
4. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
5. IEEE 802.1w Rapid Spanning Tree,
6. Per-VLAN Rapid Spanning Tree (PVRST+),
7. IEEE 802.1s Multi-Instance Spanning Tree,
8. Obsługa 128 instancji protokołu STP,
9. Obsługa protokołu LLDP i LLDP-MED.
10. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
11. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
12. Możliwość uruchomienia funkcji serwera DHCP.
13. Mechanizmy związane z bezpieczeństwem sieci:
14. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik ma umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
15. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
16. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
17. Obsługa funkcji Guest VLAN umożliwiającej uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
18. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
19. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
20. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
21. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
22. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
23. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
24. 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),
25. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
26. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia),
27. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch),
28. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing).
29. Funkcja Private VLAN.
30. Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania
31. Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne, jednoukładowe rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny,
32. Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego,
33. Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności.
34. Mechanizmy związane z zapewnieniem jakości usług w sieci:
35. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
36. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
37. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych,
38. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
39. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
40. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
41. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
42. Obsługa protokołów routingu:
43. Routing statyczny dla IPv4 i IPv6,
44. Routing dynamiczny – RIP, OSPF, EIGRP Stub,
45. Policy-based routing (PBR),
46. Obsługa protokołu redundancji bramy (VRRP).
47. Przełącznik ma 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.
48. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
49. Zarządzanie:
50. Port konsoli,
51. Dedykowany port Ethernet do zarządzania out-of-band pracujący w oddzielnej instancji routingu (VRF),
52. 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,
53. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
54. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
55. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
56. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
57. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
58. Możliwość montażu w szafie rack 19” (dołączone uchwyty montażowe). Wysokość urządzenia 1 RU.
59. **Moduł i kable stackujące – 1 kpl.**
60. Wraz z przełącznikiem musi być dostarczony moduł i kable stackujące umożliwiające dołączenie dostarczonego przełącznika do stosu.
61. **Wkładki SFP – 4 szt.**
62. Wraz z przełącznikiem muszą być dostarczone cztery wkładki SFP+, 10Gb/s kompatybilne z przełącznikem. Transceivery muszą zapewnić komunikację typu duplex, w technologii SingleMode i zapewnić wtyk LC.

Data ……………….. Podpis uprawnionego Wykonawcy …………………………