Załącznik nr 1 do SIWZ

**Opis przedmiotu zamówienia**

**Przełącznik I ( jedna sztuka )**

**I. Rodzaj urządzenia:**

1. Przełącznik stakowalny wyposażony w minimum 48 portów 10/100/1000BaseT.
2. Przełącznik musi dysponować mocą 1440W dostępnych dla PoE/PoE+.
3. Przełącznik musi zasilić 48 portów z mocą PoE+.
4. Przełącznik musi posiadać minimum 4-portowy moduł 10Gigabit Ethernet SFP+.

Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH).

**II. Architektura**

1. Przełącznik musi zapewniać możliwość stakowania z zapewnieniem następujących parametrów:
	1. Przepustowość w ramach stosu min. 80Gb/s;
	2. Min. 8 urządzeń w stosie;
	3. Stos widoczny jako jeden node dla procesu spanning-tree;
	4. Zarządzanie poprzez jeden adres IP;
	5. Możliwość tworzenia połączeń cross-stack link aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad;
	6. Przełączniki muszą umożliwiać współdzielenie mocy zasilaczy tzn. zasilacze muszą stanowić zasób wspólny dla wszystkich przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania” mocy dla innych jednostek w stosie).
2. Urządzenie musi posiadać możliwość instalacji podtrzymania zasilania pomimo restartu urządzenia (następuję tylko programowy reset).

**III. Oczekiwana wydajność**

1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate).
2. Urządzenie posiada 6MB bufor pamięci współdzielony przez wszystkie porty.
3. Minimum 2GB pamięci DRAM i 4GB pamięci flash.
4. Urządzenie musi zapewniać przepustowość nie mniejszą niż 176 Gbps.
5. Szybkość przełączania urządzenia musi wynosić minimum 260 Mpps.
6. Obsługa minimum:
7. 1024 sieci VLAN;
8. 16.000 adresów MAC;
9. 8.000 tras IPv4;
10. 1.500 tras IPv6.

**IV. Oprogramowanie/funkcjonalność**

1. Obsługa protokołu NTP.
2. Obsługa IGMPv1/2/3.
3. Wszystkie porty na przełączniku muszą obsługiwać standard 802.1AE (szyfrowanie ruchu) 128-bit
z prędkością linerate dla każdego z interfejsów.
4. System operacyjny przełącznika umożliwia wgrywanie poprawek bez konieczności restartowania platformy.
5. System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.
6. Przełącznik zapewnia widoczność aplikacyjną, klasyfikowanie ruchu w warstwach 4-7 i na jego podstawie budowanie polityk bezpieczeństwa czy jakości usług.
7. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
8. IEEE 802.1w Rapid Spanning Tree;
9. Per-VLAN Rapid Spanning Tree (PVRST+);
10. IEEE 802.1s Multi-Instance Spanning Tree;
11. Obsługa minimum 128 instancji protokołu STP.
12. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED.
13. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
14. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
15. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
16. Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level);
17. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN;
18. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL;
19. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X;
20. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC;
21. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X;
22. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem;
23. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176;
24. Minimum 1000 wpisów dla list kontroli dostępu (ACE);
25. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania
– 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www);
26. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard;
27. 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);
28. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+;
29. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych
w określonych godzinach i dniach tygodnia).
30. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
31. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
32. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek.
33. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem
w stosunku do innych (Strict Priority).
34. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
35. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 1000 ograniczeń per przełącznik.
36. Kontrola sztormów dla ruchu broadcast/multicast/unicast.
37. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
38. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4(OSPF) oraz funkcjonalności Policy-based routingu. Urządzenie musi mieć możliwość zapewnienia wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, ISIS) i IPv6 (OPSFv3), routingu multicast (PIM-SM, PIM-SSM) poprzez wgranie odpowiedniej licencji.
39. Możliwość wsparcia dla protokołu LISP zgodnie z RFC 6830.

**V. Zarządzanie i konfiguracja**

1. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)
2. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 16.000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow.
3. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
4. Dedykowany port Ethernet do zarządzania out-of-band.
5. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.
6. Urządzenie musi być wyposażone w port konsoli USB.
7. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.
8. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się
w systemie.
9. Urządzenie musi posiadać wbudowany analizator pakietów.
10. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
11. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą.
12. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.

**VI. Obudowa**

1. Możliwość montażu w szafie rack 19”. Wysokość urządzenia nie może przekraczać 1 RU.

**VII. Wyposażenie**

1. Oferowany przełącznik musi być wyposażony w zasilacz podstawowy i redundantny, każdy o mocy minimum 1KW.
2. Razem z urządzeniem wymaga się dostarczenia świadczonego przez producenta rocznego serwisu 8X5XNBD.
3. Wraz z urządzeniem muszą być dostarczone licencje umożliwiające uruchomienie Flexible NetFlow, WIreshark.

**Przełącznik II ( dwie sztuki )**

**I. Rodzaj urządzenia**

1. Przełącznik stakowalny wyposażony w minimum 24 portów 10/100/1000BaseT.
2. Przełącznik musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń z możliwością jego wymiany „na gorąco” (ang. hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły:
	1. Minimum 4-portowy moduł Gigabit Ethernet z gniazdami SFP;
	2. Minimum 8-portowy moduł 10Gigabit Ethernet SFP+;
	3. Minimum 2- portowy moduł 40Gigabit Ethernet QSFP;
	4. Minimum 4- portowy moduł miedziany IEEE 802.3bz.
3. Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-BX zależnie od potrzeb Zamawiającego. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH). Porty QSFP muszą umożliwiać obsadzenie modułami 40G-SR, 40G-LR oraz 40G-ER.

**II. Architektura**

1. Przełącznik musi zapewniać możliwość stakowania z zapewnieniem następujących parametrów:
	1. Przepustowość w ramach stosu min. 480Gb/s;
	2. Min. 8 urządzeń w stosie;
	3. Stos widoczny jako jeden node dla procesu spanning-tree;
	4. Zarządzanie poprzez jeden adres IP;
	5. Możliwość tworzenia połączeń cross-stack link aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad;
	6. Przełączniki muszą umożliwiać współdzielenie mocy zasilaczy tzn. zasilacze muszą stanowić zasób wspólny dla wszystkich przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania” mocy dla innych jednostek w stosie).
2. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów.
3. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne.

**III. Oczekiwana wydajność**

1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate).
2. Urządzenie posiadana 16MB bufor pamięci współdzielony przez wszystkie porty.
3. Minimum 8GB pamięci DRAM i 16GB pamięci flash.
4. Urządzenie musi zapewniać przepustowość nie mniejszą niż 208 Gbps.
5. Szybkość przełączania urządzenia musi wynosić minimum 150 Mpps.
6. Obsługa minimum:
7. 4000 sieci VLAN;
8. 32.000 adresów MAC;
9. 24.000 tras IPv4;
10. 16.00 tras IPv6;

**IV. Oprogramowanie/funkcjonalność**

1. Obsługa protokołu NTP
2. Obsługa IGMPv1/2/3
3. Wszystkie porty na przełączniku muszą obsługiwać standard 802.1AE (szyfrowanie ruchu) 256-bit
z prędkością linerate dla każdego z interfejsów.
4. System operacyjny przełącznika umożliwia wgrywanie poprawek bez konieczności restartowania platformy.
5. System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.
6. Przełącznik zapewnia widoczność aplikacyjną, klasyfikowanie ruchu w warstwach 4-7 i na jego podstawie budowanie polityk bezpieczeństwa czy jakości usług.
7. Możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia.
8. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
9. IEEE 802.1w Rapid Spanning Tree;
10. Per-VLAN Rapid Spanning Tree (PVRST+);
11. IEEE 802.1s Multi-Instance Spanning Tree;
12. Obsługa minimum 128 instancji protokołu STP.
13. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED.
14. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
15. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
16. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
17. Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level);
18. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN;
19. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL;
20. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X;
21. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC;
22. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X;
23. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem;
24. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176;
25. Minimum 5000 wpisów dla list kontroli dostępu (ACE);
26. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania
– 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www);
27. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard;
28. 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);
29. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+;
30. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych
w określonych godzinach i dniach tygodnia).
31. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
32. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi;
33. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek
34. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem
w stosunku do innych (Strict Priority);
35. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP;
36. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik;
37. Kontrola sztormów dla ruchu broadcast/multicast/unicast;
38. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
39. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4(OSPF) oraz funkcjonalności Policy-based routingu. Urządzenie musi mieć możliwość zapewnienia wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP, ISIS) i IPv6 (OPSFv3), routingu multicast (PIM-SM, PIM-SSM) poprzez wgranie odpowiedniej licencji.
40. Możliwość wsparcia dla protokołu LISP zgodnie z RFC 6830.

**V. Zarządzanie i konfiguracja**

1. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN).
2. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 64.000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow.
3. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
4. Dedykowany port Ethernet do zarządzania out-of-band.
5. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.
6. Urządzenie musi być wyposażone w port konsoli USB.
7. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.
8. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się
w systemie.
9. Urządzenie musi posiadać wbudowany analizator pakietów.
10. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
11. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą.
12. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.

**VI. Obudowa**

1. Możliwość montażu w szafie rack 19”. Wysokość urządzenia nie może przekraczać 1 RU.

**VII. Wyposażenie**

1. Oferowany przełącznik musi być wyposażony w zasilacz podstawowy i redundantny, każdy o mocy minimum 350W.
2. Razem z urządzeniem wymaga się dostarczenia świadczonego przez producenta rocznego serwisu 8X5XNBD.
3. Razem z urządzeniem wymaga się dostarczenia 8-portowy moduł 10Gigabit Ethernet SFP+.
4. Wraz z urządzeniem muszą być dostarczone licencje umożliwiacie uruchomienie Flexible NetFlow, WIreshark.

**Wymagania dotyczące w.w przełączników:**

1. **Gwarancja:**

Wszystkie zaproponowane urządzenia, licencje i oprogramowania powinny:

* być objęte min. 12-miesięcznym (1 rok) serwisem producenta urządzenia, zapewniającym wymianę uszkodzonego sprzętu najpóźniej w następnym dniu roboczym po dniu zgłoszenia awarii, jeżeli zgłoszenie wpłynęło w dniu roboczym do godziny 12:00, lub kolejnego dnia w pozostałych przypadkach. Producent zapewni w tym okresie możliwość bezpłatnej aktualizacji oprogramowania do nowych wersji i dostępu do wsparcia technicznego producenta (zapis ten nie dotyczy przestrzeni dyskowej),
* sprzęt dostarczony w ramach realizacji umowy będzie sprzętem nowym, nieużywanym oraz dostarczanym wcześniej w innych projektach,
* sprzęt dostarczony w ramach realizacji umowy będzie posiadał gwarancję świadczoną bezpośrednio przez producenta sprzętu,
* Wykonawca ma obowiązek przedstawić oficjalny dokument producenta, który będzie poświadczał, że sprzęt dostarczony w ramach realizacji Umowy jest sprzętem zakupionym w oficjalnym kanale sprzedaży. Wykonawca ma obowiązek zarejestrować sprzęt na użytkownika końcowego, którym jest Zamawiający.
* Zamawiający zastrzega sobie prawo sprawdzenia poprzez numery seryjne czy dostarczony sprzęt spełnia wszystkie wyżej wymienione warunki.
* w przypadku niespełnienia przez sprzęt któregokolwiek z wyżej wymienionych warunków Zamawiający zastrzega sobie prawo zwrotu całego dostarczonego sprzętu (na koszt dostawcy) jak również obciążenia dostawcy karą umowną za niedotrzymanie warunków umowy.

W ramach składanej oferty, Wykonawca zobowiązany jest do wyszczególnienia wszystkich numerów produktów (licencje, sprzęt i oprogramowanie). Lista ta będzie podlegała weryfikacji przez Zamawiającego lub niezależną firmę zewnętrzną, wskazaną przez Zamawiającego, w celu weryfikacji z wymaganiami
i zgodnością z SIWZ. W przypadku jakichkolwiek wątpliwości, Zamawiający zastrzega sobie możliwość powołania zewnętrznej, niezależnej firmy, wskazanej przez Zamawiającego w celu przeprowadzenia potrzebnych testów sprzętowych. Do tego celu, Wykonawca zobowiązany jest dostarczyć wskazany sprzęt, licencje i oprogramowanie do 60 dni od daty podpisania umowy. W razie nieprzejścia testów oferta zostanie odrzucona i Oferent zobowiązany będzie do pokrycia kosztów zewnętrznej firmy, weryfikującej zgodność sprzętu. W przypadku przejścia testów, Zamawiający pokrywa ich koszty.

1. **WDROŻENIE:**

Przed rozpoczęciem prac Wykonawca powinien przeprowadzić audyt i analizę stanu sieci (w zakresie jaki będzie wymagany do uruchomienia funkcji w ramach przetargu) oraz ustalić harmonogram prac, plan adresacji, plan sieci fizycznej i politykę obsługi ruchu grupowego (multicast), reguł ACL. Ustalenia te będą prowadzone z wyznaczonym do tego celu pracownikiem/pracownikami Zamawiającego. Zamawiający dostarczy checklistę, zawierającą wszystkie krytyczne punkty/usługi, jakie powinny zostać zweryfikowane po wykonaniu prac.

Zamawiający wymaga wykonania poniższych usług związanych z montażem i uruchomieniem obu dostarczonych urządzeń:

1. Montaż urządzeń w szafie/w urządzeniu.
2. Uruchomienie i inicjalizacja urządzeń.
3. W ramach wdrożenia, należy przeprowadzić instalację przełącznika warstwy trzeciej (przeprowadzić konfigurację stack) oraz konfigurację przełącznika warstwy drugiej, które są przedmiotem dostawy). Należy przeprowadzić uruchomienie mechanizmów L2 Security:
* IP DHCP Snooping,
* IP Source Guard,
* Dynamic ARP Inspection,
* Port Security,
* BPDU Filter, BPDU Guard i RootGuard.

Należy przeprowadzić konfigurację 802.1X na zamówionych przełącznikach. W tym celu należy również dostosować konfigurację Cisco ISE do zmian zaistniałych w sieci.

W ramach prac należy przeprowadzić konfiguracje przełączników z zakresem, który będzie obejmować między innymi technologie/protokoły: Archive, EtherChannel, MSTP, VLAN, Trunk, VTPv3, DTP, CDP/LLDP, ACL, Role-Based CLI Access.

1. Należy przeprowadzić rekonfigurację serwera, która w swoim zakresem będzie obejmować:
* rekonfigurację środowiska GNU/Linux Debian/RedHat/CentOS,
* konfigurację mechanizmów iproute2 (traffic control) i iptables,
* rekonfigurację serwera z uruchomionymi usługami FTP/TFTP do zbierania konfiguracji
i przetrzymywania plików do aktualizacji urządzeń sieciowych,
* rekonfigurację serwera z uruchomioną usługą Syslog do zbierania logów z urządzeń sieciowych/serwerowych.
1. Oprócz konfiguracji nowo zakupionego sprzętu, Wykonawca zobowiązany jest przeprowadzić także rekonfigurację obecnych urządzeń sieciowych w lokalizacjach Zamawiającego, gdzie będą przeprowadzane prace tak, aby wszystkie one w pełni ze sobą współdziałały.
2. Wykonawca zapewni 4-dniowe wsparcie po dacie podpisania protokołu odbioru, w celu rozwiązania problemów związanych z dostosowaniem konfiguracji do wymagań środowiska pracy.

W związku z tym, że obecnie większą ilość sprzętu, z którym będzie musiało zostać zintegrowane rozwiązanie jest firmy Cisco Systems, od Wykonawcy wymaga się przedstawienia certyfikatów potwierdzających kompetencje:

* + CCDP (Cisco Certified Design Professional),
	+ CCNP R&S (Cisco Certified Network Professional Routing&Switching),
	+ CCNP-S (CCNP Security, formerly known as CCSP),
	+ RHCE oraz RHCSA.

Listę osób jaka zostanie wydelegowana do projektu, wraz z listą posiadanych przez nich certyfikatach należy załączyć razem z ofertą.

1. **SZKOLENIE/DOKUMENTACJA:**

Zamawiający wyznaczy minimum jedną osobę, która zajmie się weryfikacją działania urządzeń końcowych. Prawidłowe funkcjonowanie sieci potwierdzone zostanie stosownym protokołem.

Na tydzień po zakończeniu instalacji urządzeń, Wykonawca zobowiązany jest przeprowadzić krótki instruktaż (nie trwający dłużej niż 6 godzin). Swoim zakresem będzie obejmować: zmiany zaistniałe w sieci, wykorzystane technologie, sposób działania nowego systemu, metodykę diagnozy i rozwiązywania problemów. Instruktaż odbędzie się w siedzibie Zamawiającego.

Na zakończenie prac, wykonawca zobowiązany jest dostarczyć dokumentację powdrożeniową, zawierającą schemat aktualnej sieci, adresację IP, numerację VLAN, podział podsieci i rozłożenie urządzeń.