LOTNICZE POGOTOWIE RATUNKOWE

CENTRALA

ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933

Załącznik nr 2 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

„Zakup systemów ochrony infrastruktury informatycznej Lotniczego Pogotowia Ratunkowego – 2 zadania”

ZADANIE NR 1: Urządzenia sieciowe - router w ilości 2 szt.
ZADANIE NR 2: Urządzenia sieciowe - switch w ilości 4 szt.

Spis treści

1. Słownik i skróty (dotyczy Zadania nr 1 i 2).

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Awaria	Oznacza Awaria Krytyczna i/lub Awaria Niekrytyczna i/lub Awaria Zwykła.
Awaria Krytyczna	Oznacza brak działania środowiska produkcyjnego Systemu, praca nie może być kontynuowana, operacja krytyczna dla procesu biznesowego jest niemożliwa. Awarie Krytyczne mają jedną lub więcej z poniższych cech: 1) dane biznesowe zostały uszkodzone; 2) funkcjonalność Krytyczna udokumentowana w Projekcie Technicznym nie działa; 3) System w zakresie Funkcjonalności Krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę, tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji; 4) wszelkie błędy związane z bezpieczeństwem przechowywania i przetwarzania danych, które mogą wpłynąć na: a) uwierzytelnianie, b) niezaprzeczalność, c) poufność, d) integralność, e) dostępność, f) rozliczalność; wszelkie awarie związane z bezpieczeństwem dostępu do Systemu (w tym nieautoryzowanym dostępem do danych).
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 15:35.
Dokumentacja	Wytworzone przez Wykonawcę w ramach realizacji Umowy i podlegające zatwierdzeniu przez Zamawiającego materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych, w szczególności wykaz ilościowo-cenowy.
HA	High Availability - System wysokiej niezawodności (SWN), system wysokiej dostępności − systemy informatyczne charakteryzujące się odpowiednio dostosowywaną: niezawodnością, dostępnością, wydajnością do specyficznych, zwykle krytycznych, zastosowań danego systemu
Incydent serwisowy	Oznacza zgłoszenie do Wykonawcy przez Zamawiającego lub osoby wskazane przez Zamawiającego, w trybie 24/7/365 nieprawidłowości w działaniu urządzenia lub Oprogramowania. Wykonawca zobowiązany jest do rejestracji zgłoszenia oraz usuwania błędów i usterek lub dostarczenia procedur obejścia, powodujących przywrócenie działania urządzenia lub Oprogramowania i rozwiązania zgłoszenia pod warunkiem, że na przedstawioną przez Wykonawcę propozycję obejścia Zamawiający wyrazi pisemną zgodę.
Lokalizacje	Oznacza wskazane przez Zamawiającego lokalizacje na terenie Rzeczpospolitej Polskiej, w których Wykonawca będzie świadczył usługę serwisu, dla urządzeń będących przedmiotem niniejszego zamówienia.
Oprogramowanie Standardowe	Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące w użytkowaniu Zamawiającego, na które Wykonawca udziela Zamawiającemu licencji lub sublicencji na czas nieokreślony
SLA	Poziom dostępności usług (*Service Level Agreement).*
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.

Skrót/pojęcie	Definicja
Usługa Serwisu	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania urządzenia i Oprogramowania oraz jego poszczególnych komponentów.
Użytkownik	Zamawiający oraz jego pracownicy.
Wykonawca/Dostawca	Podmiot realizujący zamówienie.
Zamawiający/LPR	Lotnicze Pogotowie Ratunkowe.

2. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup systemu ochrony infrastruktury LPR, który składa się z następujących części:

I **ZADANIE NR 1: Urządzenia sieciowe - router w ilości 2 szt.**
Urządzenia będą objęte gwarancją i wsparciem technicznym na Oprogramowanie przez okres co najmniej 36 miesięcy od dnia podpisania protokołu odbioru dostawy**.**

II **ZADANIE NR 2: Urządzenia sieciowe - switch w ilości 4 szt.**
Urządzenia będą objęte gwarancją i wsparciem technicznym na Oprogramowanie przez okres co najmniej 36 miesięcy od dnia podpisania protokołu odbioru dostawy**.**

3. ZADANIE NR 1

3.1. Urządzenie sieciowe - router (2 szt.)

1 Wykonawca wraz z Urządzeniami dostarczy zestaw montażowy RACK.
2 Urządzenia muszą być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end- of-sale", „end-of-life" oraz „end-of-support" producenta.
3 Urządzenia muszą posiadać najnowszą dostępną stabilną wersję Oprogramowania.
4 Nie dopuszcza się oferowania urządzeń, dla których producent nie udostępnia już najnowszej wersji oprogramowania / systemu operacyjnego.
5 Szczegółowe wymagania dla każdego z Urządzeń

Kod wymagania	Opis wymagania
WUSR.01	Musi posiadać co najmniej 4 interfejsy 1GE RJ45 lub co najmniej 2 interfejsy 1GE / 10GE SFP+.
WUSR.02	Urządzenie musi pozwalać na rozszerzenie o co najmniej 1 dodatkowy moduł z portem 10GE, wspierającym standard szyfrowania MACSec. W przypadku braku możliwości rozszerzenia, router powinien mieć 4 porty 1 GE RJ45 i 3 porty 10GE SFP/SFP+.
WUSR.03	Urządzenie musi umożliwiać rozszerzenie o wbudowany moduł łączności poprzez sieć komórkową przynajmniej w standardzie LTE kategorii 6. Wbudowany moduł powinien pozwalać na przełączania między co najmniej dwoma różnymi operatorami sieci komórkowej.
WUSR.04	Urządzenie musi umożliwiać rozszerzenie o platformę serwerową bądź mieć możliwość uruchomienia oprogramowania „hypervisora", na którym można instalować maszyny wirtualne.
WUSR.05	Urządzenie musi wspierać porty telefonii analogowej FXS do podłączania telefonów jako wbudowane w urządzenie lub w ramach modułów rozszerzenia. Oczekuje się możliwości rozszerzenia o minimum 24 portów FXS.
WUSR.06	Urządzenie musi obsługiwać transkodowanie strumieni głosowych przynajmniej dla 256 kanałów.
WUSR.07	Musi być wyposażone w identyfikator RFID i mieć możliwość umieszczenia etykiety z kodem QR.
WUSR.08	Musi być wyposażone w co najmniej 16 GB pamięci RAM.
WUSR.09	Musi być wyposażone w pamięć o pojemności co najmniej 16 GB do przechowywania obrazów systemu operacyjnego, konfiguracji oraz logów systemowych.
WUSR.10	Musi mieć możliwość redundancji zasilania. Należy dostarczyć urządzenie z min. dwoma zasilaczami.
WUSR.11	Musi obsługiwać co najmniej 2 000 000 prefiksów w tablicach routingu IPv4/IPv6.
WUSR.12	Musi obsługiwać co najmniej 50 000 prefiksów w tablicach routingu multicast i co najmniej 1000 grup.

WUSR.13	Musi oferować wydajność przesyłania pakietów co najmniej 19 Gbps dla pakietów 1400 bajtów.
WUSR.14	Musi być przystosowane do montażu w szafie 19”, obudowa wykonana z metalu, wysokość max 1RU.
WUSR.15	Musi posiadać redundantne zasilacze przystosowane do zasilania prądem naprzemiennym 230V.

6 Funkcje Oprogramowania

Kod wymagania	Opis wymagania
WFOR.01	Musi obsługiwać routing dynamiczny: RIP, OSPF, ISIS, BGP dla IPv4 i IPv6.
WFOR.02	Musi posiadać możliwość rozszerzenia funkcjonalności dla MPLS i MPLS VPN (L2: VPLS, VPWS i L3: VPNv4, VPNv6, mVPN) poprzez wykupienie licencji.
WFOR.03	Musi być w stanie obsłużyć co najmniej 4000 instancji VRF (Virtual Route Forwarding);
WFOR.04	Musi posiadać ochronę warstwy zarządzającej (Control Plane Policing);
WFOR.05	Musi obsługiwać co najmniej 4000 ACL (Access Control Lists) z 40 000 wpisów ACE (Access Control Entries);
WFOR.06	Musi wspierać multicast w szczególności: PIM sparse/SSM/Bi-directional, IGMP, MLDv2;
WFOR.07	Musi obsługiwać RPF (Reverse Path Forwarding);
WFOR.08	Musi obsługiwać zarządzanie ruchem (QoS): 1) minimum 16000 kolejek per system; 2) hierarchiczne polityki QoS; 3) 3 poziomy hierarchii; 4) dwie kolejki priorytetowe LLQ per polityka; 5) opóźnienie dla ruchu priorytetowego na poziomie nie większym niż 200 mikrosekund.
WFOR.09	Musi obsługiwać funkcjonalność sFlow lub odpowiednik (J-Flow, NetFlow) przy wydajności co najmniej 4Gbps dla pakietów typu IMIX;
WFOR.10	Musi posiadać funkcjonalność VRRP lub odpowiednika;
WFOR.11	Musi umożliwiać zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3;
WFOR.12	Musi posiadać wsparcie dla systemów AAA (RADIUS, TACACS);
WFOR.13	Urządzenie musi posiadać 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.
WFOR.14	Urządzenie musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń Urządzenia, dzięki stosowaniu wyrażeń – filtrów.
WFOR.15	Urządzenie powinno wspierać standardy szyfrowania ruchu – IPSec z wykorzystaniem co najmniej AES-256 w trybie CBC lub GCM, HMAC-SHA1, ECDSA (256/384 bit), SHA-1 i SHA-2 z prędkością min 50 Mbps full-duplex.

4. ZADANIE NR 2

4.1. Urządzenie sieciowe – switch core (2 szt.)

Kod wymagania	Opis wymagania
WUSS.01	Urządzenie o architekturze modularnej – 7-slotowe (w tym 5 slotów przeznaczonych na karty liniowe), pozwalające na instalację kart liniowych i redundantnych kart zarządzająco-przełączających.
WUSS.02	Chassis urządzenia umożliwia uzyskanie przepustowości 480 Gbps na slot urządzenia.
WUSS.03	Urządzenie umożliwia instalację następujących kart liniowych oraz kart zarządzająco-przełączających: 1) Karta liniowa wyposażona w 48 portów Gigabit Ethernet 10/100/1000 (RJ45); 2) Karta liniowa wyposażona w 48 portów Gigabit Ethernet 10/100/1000 (RJ45) PoE+ (zgodność z IEEE 802.3at);

	3) Karta liniowa wyposażona w 48 portów Gigabit Ethernet 10/100/1000BaseT RJ-45 UPoE IEEE 802.3at, IEEE 802.3af (do 60W per port); 4) Karta liniowa wyposażona w 48 portów Gigabit Ethernet 10/100/1000BaseT RJ-45 UPoE+ IEEE 802.3bt, IEEE 802.3at, IEEE 802.3af (do 90W per port); 5) Karta liniowa wyposażona w: a) 24 porty mGIG 100M/1G/2.5G/5G RJ-45 UPoE IEEE 802.3at, IEEE 802.3af (do 60W per port) oraz b) 24 porty Gigabit Ethernet 10/100/1000BaseT RJ-45 UPoE IEEE 802.3at, IEEE 802.3af (do 60W per port); 6) Karta liniowa wyposażona w 48 portów Gigabit Ethernet 10/100/1000 (RJ45) UPoE+ (zgodność z IEEE 802.3bt); 7) Karta liniowa wyposażone w 24 porty 10GigabitEthernet SFP/SFP+; 8) Karta liniowa wyposażone w 24 porty 1GigabitEthernet SFP; 9) Karta liniowa wyposażone w 48 portów 1GigabitEthernet SFP; 10) Karta zarządzająco-przełączająca wyposażona w 8 portów 10GigabitEthernet SFP/SFP+ i 2 porty 40GiabitEthernet QSFP (maksymalna ilość jednocześnie wykorzystanych portów na jednej lub na dwóch kartach zarządzająco-przełączających jednocześnie zainstalowanych w urządzeniu nie może przekraczać 80 Gb/s).
WUSS.04	Urządzenie posiada następujące parametry wydajnościowe: 1) Pasmo minimum 120Gb/s per slot, 2) Zagregowana przepustowość urządzenia 1.44 Tb/s, 3) Szybkość przełączania/routingu 900 Mpps dla IPv4 i 780 Mpps dla IPv6 (dla pakietów 95B), 4) Bufor pakietów – 96MB (32MB per ASIC), 5) Pamięć DRAM – 16GB, 6) Pamięć FLASH – 10GB, 7) Obsługa: a) 64 000 adresów MAC, b) 64 000 tras IPv4, c) 32 000 tras IPv6, d) 1000 aktywnych sieci VLAN, e) 1000 interfejsów SVI L3, f) 1000 interfejsów L3, g) 128 połączeń zagregowanych typu „port channel”, h) 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP, i) 18 000 – ilość wpisów w listach kontroli dostępu Security ACL, j) 18 000 – ilość wpisów w listach kontroli dostępu QoS ACL;
WUSS.05	Urządzenie umożliwia instalację maksymalnie 8 zasilaczy pracujących w trybie redundantnym N+1 (np. 4+1, 3+1, 2+1) lub N+N (np. 4+4, 3+3, 2+2, 1+1) o mocy: 3200W AC, 2100W AC lub 3200W DC;
WUSS.06	Zasilanie i chłodzenie: 1) Redundantne i wymienne moduły wentylatorów; 2) Możliwość wymiany modułów interfejsowych „na gorąco” – ang. hot swap; 3) 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); 4) Przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności).
WUSS.07	Obudowa przystosowana do montażu w szafie 19”. Wysokość 10RU. Głębokość chassis urządzenia mniejsza niż 42 cm.

WUSS.08	Obsługa protokołu NTP.
WUSS.09	Obsługa IGMPv1/2/3 i MLDv1/2 Snooping.
WUSS.10	Przełącznik wspiera 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 128 instancji protokołu STP; 5) Wsparcie dla protokołu REP (Resilient Ethernet Protocol); 6) 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 linku podstawowego.
WUSS.11	Obsługa protokołu LLDP i LLDP-MED,.
WUSS.12	Realizacja funkcji 802.1Q tunneling (QinQ).
WUSS.13	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
WUSS.14	Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
WUSS.15	Możliwość uruchomienia funkcji serwera DHCP.
WUSS.16	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 w 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) 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); 14) Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing); 15) Obsługa list kontroli dostępu (ACL) następujących typów:

	a) Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, b) 16.15.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, c) Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, d) Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); 16) 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),
WUSS.17	Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: 1) sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia; 2) bezpieczna sekwencja uruchamiania; 3) sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
WUSS.18	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) Implementacja algorytmu Shaped Round Robin dla obsługi kolejek; 3) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority); 4) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP; 5) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting); 6) Kontrola sztormów dla ruchu broadcast/multicast/unicast; 7) Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
WUSS.19	Obsługa protokołów i mechanizmów routingu: 1) Routing statyczny dla IPv4 i IPv6; 2) Routing dynamiczny – RIP, OSPF, BGP, IS-IS; 3) Policy-based routing (PBR); 4) Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup; 5) Obsługa 100 tuneli GRE (Generic Routing Encapsulation).
WUSS.20	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.
WUSS.21	Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowania zewnętrznego.
WUSS.22	Przełącznik posiada 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.).
WUSS.23	Funkcjonalność sondy IP SLA Responder.
WUSS.24	Wsparcie dla protokołu OpenFlow 1.3.
WUSS.25	Wymagania na zarządzanie urządzeniem: 1) Urządzenie musi posiadać port konsoli; 2) Urządzenie musi posiadać 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, SFTP (SSH File Transfer Protocol), https, syslog; 5) Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANG'a (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów; 6) Wsparcie dla protokołu RESTCONF; 7) Wsparcie dla protokołu gNMI; 8) Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych; 9) Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą; 10) Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB; 11) Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku M2 SATA o pojemności 240GB; 12) 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.
WUSS.26	Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: 1) Monitoring pracy przełącznika w zakresie; 2) Użycie CPU, użycie pamięci, temperatura pracy; 3) Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny; 4) Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy; 5) 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); 6) 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; 7) Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast; 8) Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik; 9) Protokół REP (Resilient Ethernet Protocol); 10) Protokół STP (Spanning Tree Protocol); 11) 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).
WUSS.27	Konfiguracja przełącznika w zakresie - konfiguracja interfejsów: 1) Fizycznych: a) Opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, b) w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP), c) 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, d) przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych); 2) Logicznych typu „port channel”: a) opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, b) w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, c) w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, d) przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych); 3) Wirtualnych typu SVI: a) 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) b) Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN, c) 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.); 4) Konfiguracja mechanizmów SPAN i RSPAN; 5) Konfiguracja protokołu STP; 6) Konfiguracja protokołu REP; 7) Konfiguracja routingu statycznego i dynamicznego; 8) Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów, a) Tworzenie i przypisanie list kontroli dostępu ACL, b) Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, c) Konfiguracja i uruchomienie NetFlow, d) Konfiguracja polityk QoS; 9) Administracja przełącznika w zakresie: a) Zdalne uruchamianie komend linii poleceń, b) Nazwa przełącznika, c) Tryb pracy L2/L3, d) Adres IP przełącznika do celów zarządzania zdalnego, e) Konfiguracja serwera DHCP, f) Konfiguracja DNS, g) Czas systemowy w tym protokół NTP, h) Konta administracyjne, i) Upgrade oprogramowania, j) Backup konfiguracji, k) Zdalny restart urządzenia, l) Konfiguracja i dostęp przez SNMP; 10) Diagnostyka urządzenia: a) Narzędzie PING i TRACEROUTE, b) Przeglądanie logów systemowych,

	c) Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego.
WUSS.28	Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 128 000 strumieni (flow).
WUSS.29	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.
WUSS.30	Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
WUSS.31	Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku.
WUSS.32	Wsparcie dla protokołu LISP zgodnie z RFC 6830.
WUSS.33	Urządzenie realizuje następujące funkcjonalności z zakresu MPLS: 1) L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC; 2) L2VPN - Virtual Private LAN Services (VPLS) - obsługa 128 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji; 3) L3 VPN - MPLS Virtual Private Network (VPN); 4) Multicast VPN (MVPN); 5) Inter AS Option A i B; 6) EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS); 7) MPLS over GRE.
WUSS.34	Obsługa 256 wirtualnych instancji routingu (VRF).
WUSS.35	Obsługa zaawansowanych protokołów routingu 1) IS-IS i BGP dla IPv4 i IPv6; 2) OSPF, EIGRP (RFC 7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA); 3) Routing multicastów - PIM-SM, PIM-SSM, PIM-Bidir; 4) Multicast Source Discovery Protocol (MSDP).
WUSS.36	Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD.
WUSS.37	Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256). Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zagregowane L2 i L3.
WUSS.38	Możliwość enkapsulacji ruchu w pakiety VXLAN.
WUSS.39	Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności LEAF oraz SPINE.
WUSS.40	Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (Secure Tag) z możliwością przypisywania znaczników: 1) Statycznie w oparciu o port, do którego podłączona jest stacja; 2) Statycznie w oparciu o VLAN, w którym pracuje stacja; 3) Statycznie w oparciu o adres IP stacji; 4) Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X.
WUSS.41	Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu.
WUSS.42	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.
WUSS.43	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.

WUSS.44	Wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii.
WUSS.45	Urządzenie wyposażone w jedną kartę zarządzająco-przełączającą jest przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze będą zachowywać się jak jedno urządzenie z punktu widzenia protokołów L2 i L3. Klastrowanie wspiera funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami.
WUSS.46	Funkcjonalność bramy dla usług mDNS.
WUSS.47	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).
WUSS.48	Przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7).
WUSS.49	Możliwość eksportu dodatkowych pól w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa).
WUSS.50	Wbudowany analizator pakietów.
WUSS.51	System operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy.
WUSS.52	Urządzenie umożliwia uruchamianie dodatkowych aplikacji w kontenerach Docker.
WUSS.53	Wyposażenie urządzenia: 1) Przełącznik wyposażony w 2 zasilacze o mocy, 2100W AC; 2) Zasilacze mają pracować w układzie redundancyjnym; 3) Przełącznik wyposażony jest w pojedynczą kartę zarządzająco-przełączającą typu: Karta zarządzająco-przełączająca wyposażona w 8 portów 10GigabitEthernet SFP/SFP+ i 2 porty 40GiabitEthernet QSFP (maksymalna ilość jednocześnie wykorzystanych portów na jednej lub na dwóch kartach zarządzająco-przełączających jednocześnie zainstalowanych w urządzeniu nie może przekraczać 80 Gb/s); 4) Przełącznik wyposażony jest w następujące karty liniowe: a) 4szt. Karta liniowa wyposażona w 48 portów Gigabit Ethernet 10/100/1000 (RJ45), b) 1szt. Karta liniowa wyposażone w 24 porty 10GigabitEthernet SFP/SFP+.
WUSS.54	Przełącznik wyposażony jest w następujące moduły interfejsowe SFP / SFP+ pochodzące z oferty producenta przełącznika: 1) Porty SFP: a) 10szt. 10Gigabit Ethernet 10GBase-SR, b) 10szt. 10Gigabit Ethernet typu twinax (SFP+ - SFP+) o długości 7 metrów; 2) Przełącznik wyposażony jest w następujące moduły QSFP pochodzące z oferty producenta przełącznika: 2szt. kable typu twinax QSFP = QSFP o długości 2 metrów.
WUSS.55	Urządzenie wyposażone jest w licencje na wymagane funkcjonalności na okres 3 lat.

4.2. Urządzenie sieciowe – przełączniki dodatkowe (2 szt.)

Kod wymagania	Opis wymagań
WOA.01	1) Parametry wydajnościowe: 2) Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate): a) Przepustowość przełącznika (switching capacity): i. 256 Gb/s (bez podłączenia do stosu), 736 Gb/s (z podłączeniem do stosu)

Kod wymagania	Opis wymagań
	b) Prędkość przesyłania (forwarding rate): i. 190.47 Mpps (bez podłączenia do stosu), 547.62 Mpps (z podłączeniem do stosu) 3) Bufor pakietów – 16MB 4) Pamięć DRAM – 8GB 5) Pamięć flash – 16GB 6) Obsługa: a) 1000 aktywnych sieci VLAN b) 32000 adresów MAC c) 8000 tras IPv4 d) 4000 tras IPv6 e) Ilość wpisów w listach kontroli dostępu Security ACL – 5000 f) ilość wpisów w listach kontroli dostępu QoS ACL – 5000 g) 1000 interfejsów SVI L3 h) 128 interfejsów L3 i) Jumbo frame 9198B j) 128 połączeń zagregowanych typu „port channel” k) 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
WOA.02	Zasilanie i chłodzenie: 1) Redundantne i wymienne moduły wentylatorów, 2) Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), 3) Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia, 4) Przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),
WOA.03	Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
WOA.04	Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: 1) Przepustowość w ramach stosu – 480Gb/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), 6) 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),
WOA.05	Przełącznik wspiera 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 128 instancji protokołu STP
WOA.06	Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED
WOA.07	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
WOA.08	Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
WOA.09	Możliwość uruchomienia funkcji serwera DHCP
WOA.10	Mechanizmy związane z bezpieczeństwem sieci: 1) Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia

Kod wymagania	Opis wymagań
	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 w 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) z wykorzystaniem protokołów RADIUS i TACACS+, 13) Obsługa list kontroli dostępu (ACL) następujących typów: a) Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, b) VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, c) Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, d) 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;
WOA.11	Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: 1) sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, 2) bezpieczna sekwencja uruchamiania, 3) sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
WOA.12	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) Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, 3) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), 4) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, 5) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), 6) Kontrola sztormów dla ruchu broadcast/multicast/unicast, 7) Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

Kod wymagania	Opis wymagań
WOA.13	Obsługa protokołów i mechanizmów routingu: 1) Routing statyczny dla IPv4 i IPv6, 2) Routing dynamiczny – RIP, OSPF do 1000 routes [Uwaga! w przypadku większej ilości routów jest wymagana licencja Network Advantage / DNA Advantage], PIM Stub do 1000 routes [Uwaga! w przypadku większej ilości routów jest wymagana licencja Network Advantage / DNA Advantage], 3) Policy-based routing (PBR), 4) Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup, 5) Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
WOA.14	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,
WOA.15	Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),
WOA.16	Funkcjonalność sondy IP SLA Responder,
WOA.17	Funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,
WOA.18	Zarządzanie 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, sftp (SSH File Transfer Protocol), https, syslog, 5) Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, 6) Wsparcie dla protokołu RESTCONF, 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: a) Monitoring pracy przełącznika w zakresie: i. Użycie CPU, ii. Użycie pamięci, iii. Temperatura pracy, iv. Podstawowe informacje systemowe: rodzaj sprzętu, czas pracy, czas systemowy, oprogramowanie, data i czas ostatniej zmiany konfiguracji, v. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, wykorzystanie PoE, vi. Informacji o urządzeniach sąsiednich podłączonych do przełącznika, vii. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, viii. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3, ix. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik, b) Konfigurację przełącznika w zakresie: i. Konfiguracja interfejsów L2: ii. Konfiguracja interfejsów L3, iii. Tworzenie i konfiguracja sieci VLAN, iv. Konfiguracja protokołu STP, v. Tworzenie i konfiguracja wirtualnych instancji routingu (VRF), vi. Konfiguracja routingu statycznego, vii. Uruchamianie i konfiguracja protokołów RADIUS i TACACS+ oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,

Kod wymagania	Opis wymagań
	viii. Tworzenie i przypisanie list kontroli dostępu ACL, ix. Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, x. Konfiguracja i uruchomienie NetFlow, c) Administracja przełącznika w zakresie: i. Zdalne uruchamianie komend linii poleceń, ii. Czas systemowy w tym protokół NTP, iii. Konta administracyjne, iv. Upgrade oprogramowania, v. Backup konfiguracji, vi. Zdalny restart urządzenia, vii. Konfiguracja i dostęp przez SNMP, viii. Narzędzie PING i TRACEROUTE, ix. Przeglądanie logów systemowych.
WOA.19	Obsługa protokołu NTP
WOA.20	Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU,
WOA.21	Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 64000 strumieni (flow),
WOA.22	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,
WOA.23	Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
WOA.24	Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,
WOA.25	Wyposażenie urządzenia 1) Przełącznik wyposażony w zasilacz redundantny o mocy identyczny jak zasilacz podstawowy, 2) Przełącznik wyposażony jest w moduł do łączenia w stos data wraz z kablem stakującym o długości 1m, 3) Przełącznik wyposażony jest w kabel o długości 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną, 4) Przełącznik wyposażony jest w moduł: a) 8x1/10G SFP/SFP+ 5) Przełącznik wyposażony jest w następujące moduły interfejsowe SFP / SFP+ pochodzące z oferty producenta przełącznika: b) 10Gigabit Ethernet 10GBase-SR,
WOA.26	Typ i liczba portów: 1) 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at)
WOA.27	Moc dostępna dla PoE: 1) 437W (z jednym zasilaczem o mocy 715W), 2) 437W (z dwoma zasilaczami o mocy 715W pracującymi w układzie redundantnym), 3) 1152W (z dwoma zasilaczami o mocy 715W pracującymi w układzie współdzielenia mocy)
WOA.28	Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb): 1) 4x1G SFP 2) 8x1/10G SFP/SFP+ 3) 2x40G QSFP 4) 2x25G SFP28 5) 4x100M/1G/2.5G/5G/10GBaseT RJ-45

5. Wymagania dodatkowe (dotyczy Zadania nr 1 i 2)

Wykonawca musi zapewnić Zamawiającemu możliwość odnowienia, po wygaśnięciu zawartej umowy serwisowej, usługi wsparcia producenta bez konieczności uiszczania dodatkowych opłat wznowieniowych, z wyjątkiem sytuacji, kiedy producent w okresie trwania usługi zakończy świadczenie usług wsparcia technicznego dla urządzeń sieciowych, będących przedmiotem zamówienia.

6. Świadczenie serwisu gwarancyjnego i gwarancji (dotyczy Zadania nr 1 i 2) .

Kod wymagania	Opis funkcjonalności
WUS.01	Na dostarczone Urządzenia/oprogramowanie wykonawca zapewni serwis gwarancyjny liczony od daty podpisania protokołu odbioru produktu na okres co najmniej 36 miesięcy opartego na świadczeniach serwisowych producenta.
WUS.02	Usługa wsparcia technicznego musi być realizowana w trybie 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, naprawa lub wymiana uszkodzonego urządzenia w ciągu 8 godzin od momentu zgłoszenia – w sytuacji wystąpienia Awarii Krytycznej.
WUS.03	Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu przez okres minimum 36 miesięcy od podpisania protokołu odbioru produktu: 1) prawo do pobierania nowych wersji i aktualizacji;; 2) wymianę Urządzenia w przypadku zdiagnozowania awarii; 3) dostarczenie sprawnego urządzenia lub jego elementu podlegającego wymianie do miejsca zainstalowania urządzenia uszkodzonego w uzgodnieniu z Zamawiającym; 4) możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania; 5) dostęp do pomocy technicznej producenta; 6) nieograniczona ilość zgłoszeń serwisowych; 7) dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta oprogramowania/urządzeń; 8) dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia oraz nowych wersji; 9) dostęp do portalu www. producenta oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji oprogramowania; 10) dostęp do rejestru licencji (dostępnego przez portal www producenta oprogramowania/urządzeń).
WUS.04	Wykonawca wraz z dostawą urządzeń przekaże warunki gwarancyjne i serwisowe Sprzętu, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta. Do zamówienia muszą zostać dostarczone procedury zgłaszania awarii w formie elektronicznej edytowalnej.
WUS.05	Do kontaktów/zgłoszeń Wykonawca udostępnia: 1) numer telefonu – _____ (infolinia bezpłatna), _____ (dla telefonów komórkowych i z zagranicy); 2) e-mail - _____. Do kontaktów/zgłoszeń Zamawiający udostępnia: 1) numer telefonu – _____; 2) e-mail - _____.
WUS.06	Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone przez Wykonawcę, zwrotnie na adres e-mail zgłaszającego.
WUS.07	Za moment zgłoszenia przyjmuje się datę i godzinę zarejestrowania przez system elektroniczny Wykonawcy, w szczególności odebrania przesyłki e-mail przez system pocztowy lub zarejestrowanie zdarzenia przez Zamawiającego w udostępnionym przez Wykonawcę systemie zgłoszeniowym. W przypadku zgłoszenia telefonicznego moment zgłoszenia zostanie ustalony z Zamawiającym w trakcie tego zgłoszenia i potwierdzony w e-mailu, o którym mowa w wymaganiu WUS.04.

WUS.08	Przez usunięcie awarii należy rozumieć przywrócenie pierwotnej funkcjonalności sprzętu i systemu operacyjnego sprzed wystąpienia awarii albo zaproponowanie procedury obejścia zaistniałych awarii bez rozwiązania problemu, pod warunkiem, że na przedstawioną przez Wykonawcę propozycję Zamawiający wyrazi zgodę.
WUS.09	Wykonawca dokona usunięcia Awarii Krytycznej w terminie nie dłuższym niż 8 godzin od momentu zgłoszenia.
WUS.10	Wykonawca dokona usunięcia Awarii Niekrytycznej w terminie nie dłuższym niż 24 godziny od momentu zgłoszenia.
WUS.11	Wykonawca dokona usunięcia Awarii Zwykłej w terminie nie dłuższym niż 72 godziny od momentu zgłoszenia.
WUS.12	Po wymianie Urządzenia lub modułu będącego wyposażeniem tego Urządzenia lub Oprogramowania zostanie on objęty serwisem na takich samych zasadach jak wymienione Urządzenie lub moduł będący wyposażeniem tego Urządzenia lub Oprogramowania.
WUS.13	Wykonawca najpóźniej w 1 Dzień Roboczy, po rozwiązaniu każdego Incydentu serwisowego przedstawi raport z tego Incydentu serwisowego (prezentujący, co najmniej czasy przyjęcia zgłoszenia o Incydencie serwisowym oraz rozwiązania Incydentu serwisowego, a także przyczyny, sposoby rozwiązania i działania zapobiegające występowaniu Incydentu serwisowego).
WUS.14	Do każdego dostarczonego Urządzenia i Oprogramowania Wykonawca zobowiązuje się dostarczyć kartę gwarancyjną producenta, zawierającą numer seryjny, termin i warunki ważności gwarancji. Jeśli dla danego dostarczonego Urządzenia lub Oprogramowania producent nie przewiduje wystawiania własnych kart gwarancyjnych, kartę taką wystawi Wykonawca. W celu ułatwienia Zamawiającemu zarządzania kartami gwarancyjnymi dopuszcza się wystawianie zbiorczych kart gwarancyjnych Wykonawcy, jednakże każdorazowo z podaniem nr seryjnych lub innych danych umożliwiających jednoznaczną identyfikację Urządzenia lub Oprogramowania, którego dotyczy gwarancja Wykonawcy. W wypadku, jeżeli postanowienia gwarancji producenta są mniej korzystne od warunków zapisanych w Umowie, stosuje się zapisy Umowy.
WUS.16	W przypadku, gdy wadliwe urządzenie uniemożliwia wykorzystanie funkcjonalności lub uniemożliwia pracę jakiegokolwiek jego podsystemu Wykonawca na czas naprawy zobowiązany jest dostarczyć, skonfigurować i uruchomić urządzenie zastępcze, o takich samych lub zbliżonych parametrach technicznych i funkcjonalnych, w sposób, który pozwoli na przywrócenie utraconych funkcjonalności Systemu lub podsystemu.
WUS.17	Usługi serwisowe, będą świadczone w miejscu użytkowania Urządzeń, z możliwością naprawy w serwisie Wykonawcy, jeśli naprawa u użytkownika okaże się niemożliwa. Jeżeli naprawa odbywać się będzie poza miejscem użytkowania Urządzeń, przed zabraniem urządzenia Wykonawca zobowiązany jest wymontować i pozostawić u Zamawiającego dyski i wymienne pamięci flash. Wykonawca pokryje koszty transportu oraz koszty ewentualnego ubezpieczenia przedmiotu zamówienia do miejsca naprawy oraz jego zwrotu do Lokalizacji. W przypadku Urządzeń, dla których jest wymagany dłuższy czas na naprawę lub wymianę Zamawiający dopuszcza możliwość dostarczenia Urządzenia zastępczego na czas naprawy o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia awarii. Po usunięciu awarii, dyski wymienne i/lub pamięci flash z urządzenia zastępczego pozostają u Zamawiającego.
WUS.18	Uszkodzone elementy Urządzeń będą wymienione przez Wykonawcę na nowe, wolne od wad i o parametrach nie gorszych od uszkodzonych.
WUS.19	Wykonawca jest zobowiązany do samodzielnego dokonania naprawy/wymiany Urządzenia w Lokalizacji. Jednakże, o ile Zamawiający wyrazi uprzednią zgodę, dopuszcza się realizację świadczenia gwarancyjnego w ten sposób, że na podstawie informacji diagnostycznych przekazanych przez Zamawiającego do Wykonawcy podczas zgłoszenia Błędów, Wykonawca prześle na swój koszt zamiennik uszkodzonego Urządzenia, natomiast fizycznej wymiany uszkodzonego Urządzenia dokona odpowiednio przeszkolony przez Wykonawcę pracownik Zamawiającego, czyniąc to na ryzyko Wykonawcy. Jednakże taki tryb realizacji naprawy nie zwalnia Wykonawcy z obowiązku zapewnienia przywrócenia pierwotnego stanu pracy Systemu.
WUS.20	Gwarancja obejmuje między innymi: 1) wady materiałowe i konstrukcyjne, a także nie spełnienie deklarowanych przez producenta parametrów i/lub funkcji użytkowych Urządzeń i Oprogramowania; 2) naprawę wykrytych uszkodzeń, w tym wymianę uszkodzonych modułów na nowe; 3) usuwanie wykrytych usterek i Awarii w działaniu Urządzeń lub Oprogramowania.
WUS.19	W okresie gwarancji, w przypadku awarii dysku twardego lub innego nośnika danych, będzie on wymieniony przez gwaranta na nowy bez konieczności zwrotu uszkodzonego dysku twardego lub

	innego nośnika danych przez Zamawiającego i dokonywania ekspertyzy dysku poza siedzibą Zamawiającego.
WUS.20	Dwukrotne uszkodzenie tego samego Urządzenia lub modułu, będącego wyposażeniem tego Urządzenia w okresie gwarancji, obliguje Wykonawcę do jego wymiany na fabrycznie nowy, wolny od wad, spełniający co najmniej te same parametry i zgodny funkcjonalnie z naprawianym Urządzeniem, w terminie 14 dni od chwili ostatniego zgłoszenia o uszkodzeniu. Okres gwarancji na wymienione Urządzenie biegł będzie od daty protokołu stwierdzającego tę wymianę, przez okres standardowo udzielany przez producenta, lecz nie krócej niż do dnia Gwarancji udzielanej przez Wykonawcę na Uzupełnienia, na warunkach określonych w Umowie.
WUS.21	Wszystkie części zamienne muszą pochodzić z oficjalnego kanału dystrybucji, z terenu Polski lub UE.
WUS.22	Wszystkie naprawy urządzeń oraz aktualizacje muszą być wykonywane przez autoryzowany serwis producenta urządzeń.
WUS.24	Zamawiający uprawniony jest do opóźnienia terminu rozpoczęcia usuwania awarii przez Wykonawcę, w takim przypadku gwarantowany czas naprawy ulegnie odpowiedniemu wydłużeniu i będzie liczony względem wskazanego przez Zamawiającego terminu.
WUS.25	W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji oprogramowania urządzeń posiadających wsparcie producenta, pozwalających na usunięcie tych błędów. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej aktualizacji, Wykonawca dokona eskalacji zgłoszenia do producenta. Wykonawca zapewnia i zobowiązuje się, że zgodnie z niniejszą specyfikacją korzystanie przez Zamawiającego z oprogramowania w ramach wsparcia technicznego nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
WUS.26	Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.
WUS.27	Zamawiający wymaga elastyczności w rozbudowie, aby była możliwość bez konieczności uzyskania zgody Wykonawcy czy Producenta, rozbudowy posiadanych urządzeń o kolejne moduły rozszerzeń. Rozbudowa nie może powodować utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego urządzenia.
WUS.28	Dla oprogramowania obowiązują prawa gwarancyjne producenta.
WUS.29	Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.

7. Zasady odbioru przedmiotu zamówienia (dotyczy Zadania nr 1 i 2).

I.Zasady Ogólne

1. Przedmiot Umowy należy dostarczyć zgodnie z zasadami i terminami wskazanymi w Umowie.
2. Odbiór zostanie przeprowadzony w biurze Zamawiającego przy ul. Księżycowej 5, w Warszawie, w obecności przedstawicieli Wykonawcy i Zamawiającego w godz. 8:00 – 15:35.
3. Przedmiot Umowy podlegać będzie odbiorowi ilościowo - jakościowemu.
4. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy protokołu – zdawczo-odbiorczego, którego wzór stanowi załącznik nr 3 do Umowy.

II.Odbiór ilościowo – jakościowy

1. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowo – jakościowego jest sprawdzenie kompletności dostarczonego przedmiotu umowy i potwierdzenie zgodności z ilością określoną w umowie oraz sprawdzenie wszystkich wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu zamówienia i umową.
2. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego przedmiotu umowy.
3. Podstawą dokonania odbioru ilościowo – jakościowego jest przeprowadzenie z pozytywnym skutkiem sprawdzeń kompletności oraz poprawności działania Oprogramowania dostarczonego w ramach umowy wraz z wymaganymi licencjami.
4. Pozytywny wynik odbioru ilościowo – jakościowego zostanie potwierdzony podpisaniem protokołu odbioru zdawczo-odbiorczego.