



LOTNICZE POGOTOWIE RATUNKOWE

CENTRALA

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

Załącznik nr 2d do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Budowa zapasowego ośrodka LPR – urządzenia sieciowe

Spis treści

SŁOWNIKI I SKRÓTY	3
CEL ZAMÓWIENIA	4
PRZEDMIOT ZAMÓWIENIA	4
1) WYMAGANIA DLA URZĄDZENIA ROUTER – 2 SZT.	4
2) WYMAGANIA DLA URZĄDZENIA SWITCH ETHERNET – 2 SZT.	9
3) WYMAGANIA GWARANCYJNE I SERWISOWE	11
4) ZASADY OGÓLNE	13

SŁOWNIKI I SKRÓTY

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

Skrót/pojęcie	Definicja
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.
Informacje	Należy przez to rozumieć informacje, o których mowa w art. 78 ust. 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576).
Oprogramowanie	Oprogramowanie standardowe i oprogramowanie aplikacyjne.
Oprogramowanie standardowe	Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące przedmiotem dostaw w ramach realizacji niniejszego przedmiotu zamówienia, którego producentem jest Wykonawca lub podmiot trzeci. Zamawiający dopuszcza zastosowanie oprogramowania standardowego w poniższych obszarach: 1) system operacyjny; 2) oprogramowanie bazodanowe; 3) oprogramowanie do tworzenia raportów; 4) oprogramowanie do archiwizacji i tworzenia kopii bezpieczeństwa; 5) oprogramowanie antywirusowe; 6) oprogramowanie ETL (ang. Extract, Transform and Load); 7) komunikator (np. oparty o protokół XMPP); 8) oprogramowanie do wirtualizacji; 9) oprogramowanie serwera pocztowego; 10) oprogramowanie serwera aplikacyjnego, kontener aplikacji (z wyłączeniem kodu aplikacji udostępnianej użytkownikowi), serwera WWW; 11) oprogramowanie narzędziowe do monitorowania i diagnozy Systemu; 12) oprogramowanie sterujące i zarządzające centralami telefonicznymi. Zamawiający dopuszcza zastosowanie oprogramowania standardowego, którego producentem jest Wykonawca lub podmiot trzeci również w innych obszarach pod warunkiem, że zastosowanie takiego oprogramowania nie ograniczy kompatybilności z innymi dostępnymi na rynku rozwiązaniami technicznymi oraz dalszej rozbudowy Systemu i świadczenia serwisu gwarancyjnego przez inne podmioty niż Wykonawca i podmiot trzeci, co wymaga przekazania kodów źródłowych oprogramowania standardowego oraz udzielenia licencji dla oprogramowania standardowego na polach eksploatacji określonych w umowie, którego producentem jest Wykonawca lub podmiot trzeci wraz z prawem do modyfikacji kodu źródłowego przez Zamawiającego i osoby trzecie oraz udzielenia zezwolenia na wykonywanie praw zależnych do dokonanych w ten sposób modyfikacji oprogramowania standardowego i jego aktualizacji.

Skrót/pojęcie	Definicja
	Każde oprogramowanie standardowe musi uzyskać akceptację Zamawiającego.
SLA	Service Level Agreement, poziom dostępności usług.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Urządzenia	Sprzęt teleinformatyczny wraz z niezbędnym wyposażeniem i odnoszącą się do nich dokumentacją techniczną producenta, w tym również okablowanie strukturalne i szafy rackowe oraz ich wyposażenie, będące przedmiotem niniejszego zamówienia.
Usługa serwisu gwarancyjnego	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania dostarczonych urządzeń i oprogramowania, w szczególności usuwanie błędów.
Wykonawca/Dostawca	Podmiot realizujący zamówienie.
Zamawiający	Lotnicze Pogotowie Ratunkowe.

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

CEL ZAMÓWIENIA

Celem Zamówienia jest dostawa 2 szt. urządzeń typu router oraz 2 szt. przełączników sieciowych dla ośrodka zapasowego Lotniczego Pogotowia Ratunkowego. Będą one pełniły rolę centralnych punktów routujących dla uruchomionych tam sieci, wraz z realizacją punktów styku z siecią Internet.

PRZEDMIOT ZAMÓWIENIA

Zamawiający wymaga dostarczenia dwóch routerów oraz dwóch przełączników sieciowych spełniających poniżej opisane wymagania. Zamawiający wymaga również dostarczenia wszystkich wymaganych w opisie licencji oraz pakietów rozszerzonego wsparcia producenta na okres i zakres zgodnie z wymaganiami opisanymi w pkt. 3 dotyczącym gwarancji i serwisu.

Ilekoć w dokumentacji użyto nazw własnych, znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych – dopuszcza się rozwiązania równoważne.

1) WYMAGANIA DLA URZĄDZENIA ROUTER – 2 SZT.

Nr	Wymagania minimalne
Wymagania na architekturę urządzenia	
1.	Musi być urządzeniem pełniącym rolę wielousługowego routera modułowego.
2.	Musi pozwalać na instalację: a. co najmniej 3 modułów usługowych z interfejsami, przy czym moduły usługowe muszą mieć możliwość wyłączenia w celu oszczędzania energii elektrycznej,

	b. wewnętrznego modułu DSP (architektura urządzenia powinna dopuszczać możliwość stosowania kart rozszerzeń z dodatkowymi, wbudowanymi modułami DSP).
3.	Musi posiadać zainstalowany wewnętrzny sprzętowy moduł akceleracji szyfrowania.
4.	Musi posiadać możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora.
5.	Musi posiadać wszystkie interfejsy „aktywne”. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
6.	Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł usługowy muszą mieć możliwość obsadzenia modułami: • z co najmniej dwoma portami Gigabit Ethernet (z interfejsami miedzianymi i możliwością instalacji wkładek optycznych SFP).
7.	Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartę sieciową muszą mieć możliwość obsadzenia kartami: • z portami szeregowymi o gęstości co najmniej 4 porty na moduł, • z interfejsem ISDN PRI o gęstości 1 portu per moduł, 2 portów per moduł, 4 portów per moduł oraz 8 portów per moduł, • umożliwiającymi instalację dysków SSD (ten wymóg dotyczy jednego slotu).
8.	Slot urządzenia przewidziany pod rozbudowę o moduł z układami DSP musi mieć możliwość obsadzenia modułem: • o gęstości nie mniejszej niż 256 kanałów, • pozwalającym na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing).
9.	Urządzenie musi oferować wydajność co najmniej 500 Mbps, musi posiadać możliwość zwiększenia przepustowości do 1Gbps poprzez zakup licencji, nie dopuszcza się by było konieczne doposażenie urządzenia w dodatkowe komponenty.
Wymagania na oprogramowanie/funkcjonalności	
10.	Oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji.
11.	Musi posiadać obsługę protokołów routingu IPv4 takich, jak RIPv2, OSPF, BGPv4, OSPF, ISIS, EIGRP, a także routingu statycznego.
12.	Musi posiadać obsługę protokołów routingu IPv6 takich, jak RIPng, OSPFv3, BGPv4, ISIS, EIGRP, a także routingu statycznego.
13.	Musi posiadać obsługę protokołów routingu multicastowego PIM Sparse oraz PIM SSM, a także routingu statycznego.
14.	Protokół BGP musi posiadać obsługę 4 bajtowych ASN.
15.	Musi posiadać wsparcie dla funkcjonalności Policy Based Routing.
16.	Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF).
17.	Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q.
18.	Musi obsługiwać IPv6 w tym ICMP dla IPv6 oraz protokoły routingu IPv6 takie jak EIGRP, RIP, OSPFv3, IS-IS.

19.	Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL.
20.	Musi umożliwiać obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast.
21.	Musi posiadać obsługę mechanizmu DiffServ.
22.	Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
23.	Musi zapewniać obsługę mechanizmów kolejowania ruchu: • z obsługą kolejki absolutnego priorytetu, • ze statyczną alokacją pasma dla typu ruchu, • WFQ.
24.	Musi obsługiwać mechanizm WRED.
25.	Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precedence dla ruchu tunelowanego.
26.	Musi obsługiwać protokół NTP.
27.	Musi obsługiwać DHCP w zakresie Client, Server.
28.	Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika).
29.	Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+.
30.	Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (tzw. Embedded Event Monitor – EEM, lub odpowiednik).
31.	Funkcjonalność EEM musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych.
32.	Funkcjonalność EEM musi pozwalać na generowanie akcji takich jak: • wykonanie komendy z poziomu linii poleceń urządzenia, • wykonanie skryptu, • wygenerowanie SNMP trap, • ustawienie lub modyfikacja określonego licznika systemowego.
33.	Musi posiadać funkcjonalność automatycznej optymalizacji routingu dla połączeń typu multihomed (funkcjonalność Optimized Edge Routing lub odpowiednik).
34.	Funkcjonalność OER (lub odpowiednik) musi posiadać wsparcie dla: • optymalizacji ruchu przychodzącego z wykorzystaniem rozgłaszania informacji BGP do zewnętrznych routerów (BGP external peers), • optymalizacji ruchu głosowego, • optymalizacji ruchu dla tuneli VPN IPSec/GRE.
35.	Musi posiadać wsparcie dla Layer-2 Tunneling Protocol Version 3.
36.	Umożliwia wsparcie dla następujących funkcjonalności bezpieczeństwa sieciowego: • funkcjonalność szyfrowania połączeń z wykorzystaniem algorytmów DES/3DES/AES, • algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności: i. Elliptic Curve Diffie-Hellman (ECDH), ii. Galois Counter Mode Advanced Encryption Standard (GCM-AES) 128/256 bitów,

	iii. Galois Message Authentication Code (GMAC-AES) 128/256 bitów, iv. Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2, • możliwość konfiguracji tuneli IPsec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2). Wsparcie dla IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych, dla ruchu IPv4 oraz IPv6, z obsługą ruchu szyfrowanego z wydajnością co najmniej 85Mbps, • funkcjonalność VPN musi wspierać tworzenie niezależnych VPN (w tym różnego typu: site-2-site, dynamicznych), • technologia umożliwiająca szyfrowanie IPsec ruchu unicast IPv4 bez konieczności tworzenia tuneli, z wykorzystaniem z użyciem protokołu Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547, w tym: i. mechanizm pasywnego IPsec SA, w którym urządzenie akceptuje zaszyfrowany i niezaszyfrowany ruch przychodzący, ale wysyła zawsze ruch zaszyfrowany, ii. mechanizm fail-close, w którym urządzenie nie wysyła ruchu, w sytuacji, kiedy miałby on pozostać niezaszyfrowany w przypadku kiedy urządzenie jest niezarejestrowane w sieci VPN, iii. mechanizm współdzielenia kluczy przez redundantne serwery kluczy, iv. mechanizm zmiany podstawowego serwera kluczy (Key Server) w scenariuszu z wysoką dostępnością serwerów kluczy, • funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall), • funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall), • możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, w tym: i. przesyłu, który jest poddawany inspekcji, ii. przesyłu, który jest odrzucany, iii. przesyłu, który jest przenoszony bez inspekcji, • ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU, • możliwość logowania pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU, • możliwość wymuszenia reguł złożoności haseł tworzonych na urządzeniu, • w przypadku modułu przełącznika, działającego jako urządzenie dostępowe RADIUS (NAD - Network Access Devices), wsparcie funkcjonalności 802.1x.
37.	Musi posiadać możliwość rozbudowy do następujących funkcjonalności poprzez zakup odpowiednich licencji i opcji sprzętowych: • funkcjonalność procesowania połączeń telefonii IP (funkcja serwera zestawiającego połączenia), • funkcje pozwalające na automatyzację konfiguracji ustawień QoS (w szczególności dla usług VoIP) w postaci automatycznego tworzenia wzorców konfiguracyjnych na potrzeby implementacji QoS, • funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia "tam i z powrotem" (roundtrip, jitter i utraty pakietów), • możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych, przy czym brama taka musi mieć możliwość pracy w sposób niezależny lub być sterowana przez system centralny procesowania połączeń.

Wymagania na zarządzanie i konfigurację	
38.	Musi być zarządzane za pomocą SNMPv1, SNMPv2, SNMPv3, Telnet, SSH.
39.	Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow/JFlow lub odpowiednika.
40.	Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI).
41.	Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
Wymagania na obudowę	
42.	Musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
43.	Musi mieć możliwość montażu w szafie 19”.
Wymagania na zasilanie	
44.	Urządzenie musi być wyposażone w minimum 1 zasilacz zmiennie-prądowy AC 230V.
45.	Urządzenie musi umożliwiać doprowadzenie zasilania do portów Ethernet (tzw. inline-power) - w modułach sieciowych dostępnych do urządzenia (funkcja wymagana).
Wymagania na wyposażenie	
46.	Urządzenie musi być wyposażone w minimum 4 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN. Wszystkie interfejsy muszą mieć możliwość pracy z gigabitowym portem światłowodowym definiowanym przez wkładki GBIC, SFP lub równoważne.
47.	Urządzenie musi być wyposażone w minimum 16GB pamięci Flash.
48.	Urządzenie musi być wyposażone w minimum 16GB pamięci RAM.
49.	Urządzenie musi być wyposażone w minimum dwa porty USB. Porty muszą pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.
50.	Wszystkie karty i moduły muszą być objęte wspólnym serwisem producenta.

2) WYMAGANIA DLA URZĄDZENIA SWITCH ETHERNET – 2 SZT.

Działanie obejmuje dostawę 2 urządzeń sieciowych z wymaganymi licencjami oraz gwarancją producenta na okres 36 miesięcy w poniższym uкомплекtowaniu:

Produkt	Opis	Ilość
C9300-24T-E	Catalyst 9300 24-port data only, Network Essentials.	1
CON-SSSNT-C93002TE	SOLN SUPP 8X5XNBD Catalyst 9300 24-port data only, Network.	1
C9300-NW-E-24	C9300 Network Essentials, 24-port license.	1
S9300UK9-166	CAT9300 Universal image.	1
PWR-C1-350WAC	350W AC Config 1 Power Supply.	1
PWR-C1-350WAC/2	350W AC Config 1 SecondaryPower Supply.	1
C9300-NM-8X	Catalyst 9300 8 x 10GE Network Module.	1
CAB-TA-EU	Europe AC Type A Power Cable.	2
STACK-T1-50CM	50CM Type 1 Stacking Cable.	1
C9300-DNA-E-24	C9300 DNA Essentials, 24-Port Term Licenses.	1
C9300-DNA-E-24-3Y	C9300 DNA Essentials, 24-Port, 3 Year Term License.	1

Zamawiający dopuszcza rozwiązanie równoważne, pod warunkiem spełnienia przez nie następujących minimalnych wymagań:

Kod wymagania	Opis wymagania
SW.01	Przełącznik musi być wyposażony w min. 24 porty 10/100/1000 oraz min. 8 portów SFP/SFP+.
SW.02	Porty SFP/SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR.
SW.03	Urządzenie musi obsługiwać minimum 4000 sieci VLAN i 32000 adresów MAC.
SW.04	Urządzenie musi mieć możliwość montażu w szafie 19”, a jego wysokość nie może być większa niż 1RU.
SW.05	Wydajność przełączania musi wynosić minimum 100 Gbps.

SW.06	Urządzenie musi posiadać możliwość łączenia w stosy z zachowaniem następującej funkcjonalności: 1) Obsługa min. 4 jednostek w stosie, 2) Magistrala stakująca o wydajności co najmniej 480 Gb/s, 3) Możliwość przeniesienia zasilania za pomocą magistrali stakującej.
SW.07	W celu uzyskania tej funkcjonalności dopuszcza się konieczność doposażenia urządzenia w dodatkowy, opcjonalny moduł.
SW.08	Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości 9198 bajtów.
SW.09	Obsługa protokołu NTP.
SW.10	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree.
SW.11	Wsparcie dla protokołu IEEE 802.1ad Q-in-Q.
SW.12	Funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
SW.13	Obsługa protokołów BGP, OSPF, EIGRP, IS-IS, RIP, HSRP, VRRP, IGMPv3.
SW.14	Wsparcie dla VPN Routing and Forwarding (VRF), MPLS VPN – Layer 3 VPN, Ethernet over MPLS (EoMPLS), VPLS.
SW.15	Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa: 1) wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level); 2) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL; 3) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC; 4) możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X (bez konieczności stosowania zewnętrznego serwera www).
SW.16	Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www.
SW.17	Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie.
SW.18	Wsparcie dla standardu IEEE 802.1ae (MACsec).
SW.19	Wsparcie dla mechanizmów zabezpieczenia CoPP.
SW.20	Możliwość uzyskania dostępu do urządzenia przez SNMPv2 oraz SNMPv3, SSHv2 z obsługą certyfikatów typu self-signed.

SW.21	Obsługa list kontroli dostępu (ACL), mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard. Wymagane jest, aby listy ACL posiadały domyślny wpis "blokuj" dla ostatniego, niewidocznego wpisu w ACL.
SW.22	Funkcjonalność Protected Port.
SW.23	Przełącznik musi wspierać mechanizmy QoS związane z zapewnieniem jakości usług w sieci.
SW.24	Wsparcie dla automatyzacji zadań, np. Embedded Event Manager (EEM), Python.
SW.25	Obsługa protokołu CDP lub LLDP.
SW.26	Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli.
SW.27	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).
SW.28	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. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 4 plików konfiguracyjnych.
SW.29	Redundantne zasilanie 230V AC.
SW.30	Zaoferowane przełączniki muszą być dostarczone z serwisem 36 miesięcznym liczonym od dnia następnego po dacie podpisania bez uwag protokołu odbioru urządzeń, działającym w trybie 8x5xNBD oraz z możliwością bezpośredniego pobrania z serwisu producenta wszystkich aktualizacji oprogramowania.

3) WYMAGANIA GWARANCYJNE I SERWISOWE

- Wykonawca wraz z dostawą urządzeń przekaże warunki gwarancyjne i serwisowe, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta.
- Wymagania gwarancyjne:
 - Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu:
 - prawo do pobierania nowych wersji i aktualizacji oprogramowania przez okres minimum 36 miesięcy od dnia podpisania protokołu odbioru produktu,
 - przyjmowanie zgłoszeń Zamawiającego przez Wykonawcę 24 godziny na dobę (dla sprzętu objętego serwisem NBD, zgłoszenia zamawiającego dokonane po godz. 15:35 i w dni wolne od pracy będą traktowane jako zgłoszenia dokonane następnego dnia roboczego),
 - wymianę sprzętu na sprawny w przypadku zdiagnozowania awarii urządzenia,

- d) dostarczenie sprawnego urządzenia lub jego elementu podlegającego wymianie do miejsca zainstalowania urządzenia uszkodzonego,
 - e) możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania,
 - f) dostęp do pomocy technicznej producenta,
 - g) dostęp do poprawek i nowych wersji oprogramowania;
- 2) gwarancją producenta muszą zostać objęte wszystkie dostarczone urządzenia przez okres minimum 36 miesięcy, przy czym bieg okresu gwarancji rozpocznie się w dniu następnym po dacie podpisania bez zastrzeżeń protokołu zdawczo-odbiorczego. Do dostarczonych urządzeń będą dołączone karty gwarancyjne zawierające numery seryjne produktu, numery seryjne oprogramowania, termin i warunki ważności gwarancji (zgodnie z umową), adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
3. Do przedmiotu zamówienia muszą zostać dostarczone procedury zgłaszania awarii w formie edytowalnych dokumentów w wersji elektronicznej.
5. Wykonawca zobowiązuje się do świadczenia usług gwarancyjnych w trybie NBD (następny dzień roboczy).
6. Ileć w treści niniejszego dokumentu jest mowa o awarii rozumie się taki stan sprzętu i oprogramowania, który uniemożliwia korzystanie z dostarczonego sprzętu.
7. Zamawiający wymaga, aby awaria została usunięta następnego dnia roboczego od chwili jej zgłoszenia, dotyczy serwisu NBD.
8. W przypadku braku możliwości wykonania naprawy w terminie podanym wyżej, Wykonawca na okres przedłużającej się naprawy bądź usuwania awarii, dostarczy Zamawiającemu sprzęt zastępczy, równoważny funkcjonalnie. Po zakończeniu naprawy sprzęt zastępczy zostanie zwrócony Wykonawcy z wyłączeniem nośników danych.
9. Uszkodzone elementy sprzętu będą wymienione przez Wykonawcę na nowe, wolne od wad i o parametrach nie gorszych od uszkodzonych.
10. 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.
11. Przez usunięcie awarii należy rozumieć przywrócenie pierwotnej funkcjonalności sprzętu i systemu operacyjnego sprzed wystąpienia awarii.
12. Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.
13. Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.
14. Dla oprogramowania obowiązują prawa gwarancyjne producenta.
15. 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.
16. Zamawiający zastrzega sobie prawo do dodawania nowych modułów dowolnych producentów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą.

4) ZASADY OGÓLNE

1. Wykonawca zobowiązany jest wykonać przedmiot zamówienia wraz z dostarczeniem wszystkich wymaganych dokumentów nie później niż w terminie 90 dni od podpisania umowy.
2. Odbiór przedmiotu Umowy zostanie przeprowadzony w 72-100 Goleniów, Główny Lotnisko Szczecin Goleniów.
3. Odbiór przedmiotu Umowy zostanie potwierdzony podpisaniem przez wyznaczonych przedstawicieli Zamawiającego i Wykonawcy protokołu zdawczo-odbiorczego.
4. Protokół zostanie sporządzony w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
5. Wszelkie pozostałe kwestie i szczegółowe postanowienia w zakresie realizacji przedmiotu zamówienia regulować będzie umowa zawarta pomiędzy Zamawiającym a Wykonawcą.