OPIS PRZEDMIOTU ZAMÓWIENIA

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest:

1) Dostawy i instalacji 8 szt. przełączników sieciowych LAN szkieletowych;
2) Dostawy i instalacji 80 szt. przełączników sieciowych dostępowych LAN TYP 1;
3) Dostawy i instalacji 20 szt. przełączników sieciowych dostępowych LAN TYP 2;
4) Dostawa systemu zarządzania siecią LAN;
5) Dostawa 100 szt. modułów SFP+ 10/25GE standardu CSR;
6) Dostawa 24 szt. modułów SFP+ 10/25GE standardu LR;
7) Dostawa 24 szt. modułów SFP 1GE standardu 1000Base-T;
8) Dostawy i instalacji 1 szt. przełącznika sieciowego, szkieletowego centrum danych DC;
9) Dostawy i instalacji 12 szt. przełączników sieciowych dostępowych centrum danych DC;
10) Dostawy i instalacji 12 szt. przełączników sieciowych 1G centrum danych DC;
11) wdrożenie i instalacja dostarczonego sprzętu na podstawie przyjętego projektu technicznego;
12) Wykonanie i dostarczenie projektu wdrożenia oraz dokumentacji powykonawczej;
13) świadczenie przez Wykonawcę, usług serwisu gwarancyjnego;
14) świadczenie wsparcia technicznego (asysty technicznej) w liczbie 1000 roboczogodzin;,
15) udzielenie lub zapewnienie udzielenia niezbędnych licencji na oprogramowanie wskazane w niniejszym Załączniku.
16) przeprowadzenie warsztatów powdrożeniowych.

2. TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1) w zakresie wymienionym w pkt 1 ppkt 1)-10) i 15- w terminie do 200 dni od dnia zawarcia umowy. Wykonanie tej części przedmiotu zamówienia zostanie potwierdzone podpisaniem przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Ilościowego Urządzeń i Licencji;
2) w zakresie wymienionym w pkt 1 ppkt 11), 12) - w terminie do 90 dni od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Ilościowego Urządzeń i Licencji. Wykonanie tej części przedmiotu zamówienia zostanie potwierdzone podpisaniem przez Zamawiającego bez zastrzeżeń odpowiednio Protokołu Odbioru Jakościowego Urządzeń i Licencji i Protokołu Odbioru Projektu Wdrożenia Dokumentacji Powykonawczej ;
3) w zakresie wymienionym w pkt 1 ppkt 13) - przez okres 40 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji;
4) w zakresie wymienionym w pkt 1 ppkt 14) - przez okres 40 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji albo do wyczerpania puli roboczogodzin, w zależności które zdarzenie nastąpi wcześniej;
5) w zakresie wymienionym w pkt 1 ppkt 16) - przez okres 24 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji.

3. MIEJSCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1) Miejscem realizacji przedmiotu zamówienia jest budynek Ministerstwa Sprawiedliwości przy ul. Czerniakowskiej 100 w Warszawie lub inna lokalizacja wynikająca z punktu 2.
2) Zamawiający zastrzega sobie prawo do zmiany lokalizacji urządzeń w trakcie trwania umowy, wynikającą ze zmian organizacyjnych Zamawiającego, w tym m.in. w związku ze zmianą siedziby Zamawiającego lub zmianą miejsca realizacji przedmiotu zamówienia w obrębie województwa mazowieckiego, po pisemnym zawiadomieniu Wykonawcy, na co najmniej 5 dni przed terminem zmiany.
3) Koszt transportu sprzętu do nowej siedziby Zamawiającego pokrywa Wykonawca. Wykonawca zapewni transport do nowej siedziby Zamawiającego. Zamawiający gwarantuje, że maksymalna ilość zmian lokalizacji nie przekroczy ilości 2 w trakcie trwania umowy.
4) Zamawiający zastrzega sobie prawo do zmiany miejsca umieszczenia urządzeń będącego przedmiotem zamówienia – bez utraty prawa do gwarancji.
5) Zamawiający wymaga realizacji zgłoszeń w miejscu określonym w pkt. 1 i 2.
6) Zamawiający nie dopuszcza napraw sprzętowych poza miejscem realizacji przedmiotu zamówienia.
7) Komunikacja oraz wszelka korespondencja pomiędzy Stronami będzie odbywała się w języku polskim.

4. ZAMÓWIENIE OBEJMUJE:

Rozbudowę posiadanej sieci LAN poprzez dostawę oraz instalację i wdrożenie urządzeń wraz z gwarancją, oraz oprogramowaniem zarządzającym.

5. OPIS SYSTEMU

1) Zamawiający posiada sieć LAN składającą się z:
    a. 4 przełączników Cisco Catalyst 6880-X;
    b. 3 przełączniki Cisco Nexus C9508;
    c. 12 przełączników Cisco Nexus C93180YC-FX;
    d. 10 przełączników Cisco Nexus C9348GC-FXP;
    e. 25 Cisco Catalyst 3650;
    f. system do uwierzytelniania użytkowników Cisco ISE;
    g. system do monitorowania sieci firmy Solarwinds.

6. WYMAGANIA OGÓLNE

1) W ramach postępowania Wykonawca dostarczy i zainstaluje przełączniki LAN oraz oprogramowanie do zarządzania przełącznikami sieci LAN
2) Dostarczone przełączniki muszą współpracować z obecnym w sieci Zamawiającego systemem uwierzytelniania Cisco ISE w następującym zakresie:

a. Uwierzytelnianie użytkowników za pomocą protokołu 802.1X;
b. Uwierzytelnianie użytkowników na podstawie adresu MAC;
c. Uwierzytelnianie użytkowników za pomocą portalu wystawionego przez system Cisco ISE, przełączniki muszą obsługiwać odpowiednie atrybuty, które przekierują użytkownika na portal wystawiony na Cisco ISE i umożliwią uwierzytelnianie.
d. Automatyczne przypisanie VLAN;
e. Protokół Radius CoA;

3) Dostarczone przełączniki muszą współpracować z obecnym w sieci Zamawiającego systemem monitorowania sieci Solrawinds w następującym zakresie:
   a. Monitorowanie z wykorzystaniem protokołu SNMPv2 i SNMPv3;
   b. Muszą posiadać zestaw MIB do systemu Solarwinds.
4) Dostarczony system do zarządzania urządzeniami musi współpracować z posiadanymi przez Zamawiającego przełącznikami Cisco Catalyst6880-X, Cisco Catalyst 3650 oraz z przełącznikami, które zostaną dostarczone w ramach postępowania.

7. WDROŻENIE

1) Wykonawca wykona wdrożenie i instalację dostarczonych urządzeń w następującym zakresie:
   - Dostarczenie sprzętu do serwerowni;
   - Wykonanie projektu wdrożeniowego oraz dokumentacji powykonawczej;
   - Demontaż urządzeń wskazanych przez Zamawiającego;
   - Montaż sprzętu, w tym montaż kabli LAN oraz kabli zasilających;
   - Podłączenie sprzętu do sieci zasilającej;
   - Migracja konfiguracji z urządzeń posiadanych przez Zamawiającego.
2) W ramach wdrożenia Wykonawca zobowiązany jest do:
   a. instalacji fizycznej urządzeń,
   b. podłączenia kabli,
   c. konfiguracji urządzeń niezbędnej do uruchomienia (adresacja interfejsów, konfiguracja uwierzytelniania, konfiguracja usług NTP, DNS, SNMP, Syslog, dodanie do systemu monitorowania Solarwinds, ISE),
   d. instalacji i konfiguracji systemu do zarządzania urządzeniami posiadanymi przez Zamawiającego oraz dostarczonymi w ramach zamówienia (w tym dodanie urządzeń do systemu zarządzania siecią LAN).

3) Wykonawca dostarczy wszystkie niezbędne kable, wkładki światłowodowe zarówno do oferowanych urządzeń jak również do przełączników posiadanych przez Zamawiającego do prawidłowego uruchomienia sprzętu zgodnie z przyjętym i zaakceptowanym projektem wdrożeniowym. Wkładki muszą pochodzić od producenta sprzętu.

8. DOKUMENTACJA WDROŻENIOWA I POWYKONAWCZA

1) Wykonawca opracuje projekt wdrożeniowy oraz dokumentację powykonawczą co najmniej:
   a. Dla projektu wdrożeniowego:
      i. diagramy połączeniowe dla wszystkich komponentów sieci zamawiającego powiązanych z dostarczonymi urządzeniami,
      ii. konfigurację przewidzianą dla wszystkich urządzeń oraz propozycje zmian dla istniejących urządzeń połączonych z przedmiotem zamówienia,
      iii. harmonogram wdrożenia uwzględniający wdrożenie wyłącznie w dni wolne od pracy tj. piątek od godz. 17:00 do niedzieli godz. 17:00,
      iv. koncepcję testów następujących po wszystkich etapach wdrożenia,
      v. plan awaryjny „backout" dla każdego kroku wdrożenia,
      vi. koncepcję testów redundancji wykonywanych po zakończeniu wdrożenia.
   b. 2. Dla dokumentacji powykonawczej:
      i. diagramy połączeń,
      ii. opis wszystkich funkcjonalności wdrożonych podczas uruchamiania systemu,
      iii. pełne konfiguracje urządzeń,
      iv. wyniki testów redundancji.

9. WYMAGANIA DOTYCZĄCE PRZEŁACZNIKÓW LAN SZKIELETOWYCH – 8 szt.

Identyfikator wymagania	*Opis wymagania*
LAN-01	**Rodzaj urządzenia:**
LAN-01.01	Przełącznik musi być wyposażony w minimum 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28
LAN-01.02	Przełącznik musi być wyposażony w co najmniej 4 porty uplink 40/100 Gigabit Ethernet QSFP
LAN-01.03	Porty SFP muszą umożliwiać zastosowanie następujących wkładek: • Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, Porty SFP+ muszą umożliwiać zastosowanie następujących wkładek: • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet 10GBase-BX-D/U, • 10Gigabit Ethernet typu twinax (SFP+ - SFP+), Porty SFP28 muszą umożliwiać zastosowanie następujących wkładek: • 25Gigabit Ethernet 25GBASE-SR, • 25Gigabit Ethernet typu twinax (SFP28 – SFP28), • 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF), • 10/25Gigabit Ethernet 10/25GBASE-LR (SMF);
LAN-01.04	Porty QSFP muszą umożliwiać zastosowanie następujących modułów: Dla transmisji 40Gb/s: • 40G-SR4, • 40G-LR4, • 40G-ER4, • 40G-SR-BD, • 40G-CSR, • 40G-CSR4, • 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652), • adapter 40G QSFP->10G SFP+, • 40Gigabit Ethernet typu twinax (QSFP - QSFP); Dla transmisji 100Gb/s: • 100GBASE-SR4, • 100GBASE-LR4, • 100Gigabit Ethernet typu twinax (QSFP - QSFP);
LAN-01.05	Musi być możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU. Głębokość urządzenia z wentylatorami, i zasilaczami nie większa niż 50 cm,
LAN-02	**Architektura:**
LAN-02.01	Urządzenie musi być wyposażone w wymienne moduły wentylatorów
LAN-02.02	Urządzenie musi zostać wyposażone w zasilacz redundantny do pracy w trybie 1:1

LAN-03	**Wydajność:**
LAN-03.01	Urządzenie musi posiadać bufor pamięci 32MB
LAN-03.02	Urządzenie musi posiadać 16GB pamięci DRAM i 16GB pamięci flash,
LAN-03.03	Przepustowość przełącznika (switching capacity) musi wynosić co najmniej 3.2 Tbps,
LAN-03.04	Prędkość przesyłania (forwarding rate) musi wynosić 1 miliard pps (1Bpps),
LAN-03.05	Urządzenie musi obsługiwać co najmniej 1000 aktywnych sieci VLAN,
LAN-03.06	Urządzenie musi obsługiwać co najmniej 80 000 adresów MAC,
LAN-03.07	Urządzenie musi obsługiwać co najmniej 212 000 tras IPv4,
LAN-03.08	Urządzenie musi obsługiwać co najmniej 212 000 tras IPv6,
LAN-03.09	Ilość wpisów w listach kontroli dostępu Security ACL co najmniej 27 000,
LAN-03.10	Ilość wpisów w listach kontroli dostępu QoS ACL co najmniej 16 000,
LAN-03.11	Urządzenie musi obsługiwać co najmniej 1000 interfejsów SVI L3,
LAN-03.12	Jumbo frame 9198B,
LAN-03.13	Urządzenie musi obsługiwać co najmniej 128 połączeń zagregowanych typu „port channel”,
LAN-03.14	Urządzenie musi obsługiwać co najmniej 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP;
LAN-04	**Oprogramowanie/funkcjonalność:**
LAN-04.01	Urządzenie musi obsługiwać protokołu NTP,
LAN-04.02	Urządzenie musi obsługiwać IGMPv1/2/3,
LAN-04.03	Urządzenie musi obsługiwać standard IEEE 802.1ae (MACSec) szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika. Urządzenie musi umożliwiać uruchomienie MACsec na portach tworzących połączenia zaagregowane L2 i L3,
LAN-04.04	System operacyjny przełącznika musi umożliwiać wgrywanie poprawek bez konieczności restartowania platformy,
LAN-04.05	System operacyjny przełącznika musi być konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwiać eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów,
LAN-04.06	Urządzenie musi obsługiwać protokoł RESTCONF,
LAN-04.07	Urządzenie musi umożliwiać uruchamianie zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia,
LAN-04.08	Przełącznik musi posiadąć następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: • IEEE 802.1w Rapid Spanning Tree, • Per-VLAN Rapid Spanning Tree (PVRST+), • IEEE 802.1s Multi-Instance Spanning Tree, • Obsługa 1000 instancji protokołu STP;
LAN-04.09	Urządzenie musi obsługiwać protokoł IEEE 802.1ab LLDP i LLDP-MED,
LAN-04.10	Urządzenie musi obsługiwać 802.1Q tunneling (QinQ)
LAN-04.11	Urządzenie musi posiadać funkcję serwera DHCP,

LAN-04.12	Urządzenie musi obsługiwać 5 poziomów dostępu administracyjnego poprzez konsolę. Urządzenie musi obsługiwać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
LAN-04.13	Urządzenie musi obsługiwać autoryzację prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
LAN-04.14	Urządzenie musi obsługiwać listy kontroli dostępu (ACL) następujących typów: • Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, • VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, • Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, • tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
LAN-04.15	Przełącznik musi realizować następujące mechanizmy związane z zapewnieniem, jakości usług w sieci: • 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, • Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek, • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), • Kontrola sztormów dla ruchu broadcast/multicast/unicast, • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
LAN-04.16	Przełącznik musi posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), Urządzenie musi obsługiwać funkcje 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),
LAN-04.17	Urządzenie musi realizować routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie: • Routing statyczny dla IPv4 i IPv6, • Routing dynamiczny dla IPv4: BGP, ISIS, • Routing dynamiczny dla IPv4: OSPF, EIGRP (rfc7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA), • Routing dynamiczny dla IPv6: OSPFv3, • Funkcjonalności Policy-based routing, • multicast routing (PIM-SM, PIM-SSM) , • Obsługa protokołu redundancji bramy (VRRP) z obsługą 255 grup, • Obsługa 200 tuneli GRE (Generic Routing Encapsulation), • Obsługa 1000 wirtualnych instancji routingu (VRF),
LAN-04.18	Urządzenie musi obsługiwać protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii

	połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,
LAN-04.19	Urządzenie musi obsługiwać funkcjonalność translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji,
LAN-04.20	Urządzenie musi obsługiwać protokołu LISP zgodnie z RFC 6830,
LAN-04.21	Urządzenie musi obsługiwać enkapsulację ruchu przy pomocy VXLAN'ów,
LAN-04.22	Urządzenie musi obsługiwać BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine / border,
LAN-04.23	Urządzenie musi obsługiwać mechanizmy zapewniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,
LAN-04.24	Urządzenie musi być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze będą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,
LAN-04.25	Klastrowanie musi wspierać funkcję eliminacji przesyłania ruchu Broadcast, unknown-unicast i multicast poprzez połączenie realizujące klaster pomiędzy przełącznikami,
LAN-04.26	Urządzenie musi obsługiwać 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,
LAN-04.27	Urządzenie musi obsługiwać zdalną obserwację 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),
LAN-04.28	Urządzenie musi posiadać 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,
LAN-04.29	Urządzenie musi posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
LAN-04.30	Urządzenie musi posiadać wbudowany analizator pakietów,
LAN-04.31	Urządzenie musi umożliwiać tworzenia bezpośrednio na nim polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników: • Statycznie w oparciu o port, do którego podłączona jest stacja, • Statycznie w oparciu o VLAN, w którym pracuje stacja, • Statycznie w oparciu o adres IP stacji, • Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;
LAN-04.32	Musi być możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
LAN-04.33	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,
LAN-04.34	Urządzenie musi umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,
LAN-04.35	Urządzenie musi mieć możliwość wyposażenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku M2 SATA o pojemności 240/480/960GB,
LAN-04.36	Urządzenie musi mieć możliwość modyfikacji programowej takich parametrów urządzenia jak: ilości pozycji w tablicy MAC, ilość tras routingowych unicast i multicast, ilości tras w sieci MPLS VPN, ilości obsługiwanych sesji netflow,
LAN-05	**Funkcjonalności z zakresu MPLS:**
LAN-05.01	Urządzenie musi obsługiwać L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC,
LAN-05.02	Urządzenie musi obsługiwać L2VPN - Virtual Private LAN Services (VPLS) - obsługa 1000 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji,
LAN-05.03	Urządzenie musi obsługiwać L3 VPN - MPLS Virtual Private Network (VPN),
LAN-05.04	Urządzenie musi obsługiwać Multicast VPN (MVPN);
LAN-05.05	Urządzenie musi obsługiwać Inter AS Option A i B,
LAN-05.06	Urządzenie musi obsługiwać EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS),
LAN-05.07	Urządzenie musi obsługiwać MPLS over GRE,
LAN-06	**Zarządzanie i konfiguracja:**
LAN-06.01	Urządzenie musi realizować sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow lub równoważny (bez próbkowania), wielkość tablicy monitorowanych strumieni musi wynosić co najmniej 98 000,
LAN-06.02	Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,
LAN-06.03	Urządzenie musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
LAN-06.04	Urządzenie musi być wyposażone w port konsoli,
LAN-06.05	Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
LAN-06.06	Urządzenie musi obsługiwać protokoły SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
LAN-06.07	Przełącznik musi posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia,
LAN-06.08	Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
LAN-06.09	Urządzenie musi posiadać funkcje 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,
LAN-07	**Wyposażenie urządzenia:**
LAN-07.01	Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,

LAN-07.02	Urządzenie musi zostać wyposażone w licencje subskrypcyjną na wymagane funkcjonalności na okres 48 miesięcy
LAN-07.03	Urządzenie musi w pełni współpracować z dostarczanym systemem do zarządzania siecią LAN, jeżeli wymaga dostarczenia dodatkowych licencji to należy je dostarczyć na okres 48 miesięcy.
LAN-07.04	Jeżeli przełącznik wyposażony jest w moduł do łączenia w stos musi być dostarczony wraz z kablem stakującym o długości 50 cm,

10. WYMAGANIA DOTYCZĄCE PRZEŁACZNIKÓW LAN DOSTĘPOWYCH TYP 1 – 80 szt.

Identyfikator wymagania	*Opis wymagania*
LAN-01	**Rodzaj urządzenia:**
LAN-01.01	Przełącznik musi być wyposażony w minimum 8 portów mGIG 100M/1G/2.5G/5G/10GBaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + 40 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at)
LAN-01.02	Moc dostępna dla PoE: 740W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie redundantnym),
LAN-01.03	Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb): • 4x10G SFP/SFP+ • 2x40G QSFP • 2x25G SFP28
LAN-01.04	Porty SFP muszą umożliwiać zastosowanie następujących wkładek: • Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U • Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, Porty SFP+ muszą umożliwiać zastosowanie następujących wkładek: • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-LRM, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet 10GBase-BX-D/U, • 10Gigabit Ethernet typu twinax (SFP+ - SFP+) • Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet 10GBase-BX-D/U,

	• 10Gigabit Ethernet typu twinax (SFP+ - SFP+) Porty SFP28 muszą umożliwiać zastosowanie następujących wkładek: • 25Gigabit Ethernet 25GBASE-SR, • 25Gigabit Ethernet typu twinax (SFP28 – SFP28) • 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF) • 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)
LAN-01.05	Porty QSFP muszą umożliwiać zastosowanie następujących modułów: • 40G-SR4, • 40G-LR4, • 40G-ER4, • 40G-SR-BD, • adapter 40G QSFP->10G SFP+, • 40Gigabit Ethernet typu twinax (QSFP - QSFP);
LAN-01.06	Możliwość montażu w szafie rack 19”,
LAN-01.07	Wysokość urządzenia 1 RU,
LAN-01.08	Głębokość chassis urządzenia bez wentylatorów i kabli zasilających mniejsza niż 36 cm,
LAN-01.09	Głębokość chassis urządzenia z wentylatorami i kablami zasilającymi mniejsza niż 40 cm,
LAN-02	**Architektura:**
LAN-02.01	Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: • Przepustowość w ramach stosu - 160Gb/s, • 8 urządzeń w stosie, • Zarządzanie poprzez jeden adres IP, • Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
LAN-02.02	Zasilanie i chłodzenie: • Redundantne i wymienne moduły wentylatorów, • Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), • Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia, • 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),
LAN-03	**Wydajność:**
LAN-03.01	Przepustowość przełącznika (switching capacity): 400 Gb/s (bez podłączenia do stosu), 580 Gb/s (z podłączeniem do stosu)
LAN-03.02	Prędkość przesyłania (forwarding rate):297.61 Mpps
LAN-03.03	Bufor pakietów – 6MB
LAN-03.04	Pamięć DRAM – 4GB
LAN-03.05	Pamięć flash – 4GB
LAN-03.06	1000 aktywnych sieci VLAN
LAN-03.07	32000 adresów MAC
LAN-03.08	4000 tras IPv4
LAN-03.09	2000 tras IPv6

LAN-03.10	Ilość wpisów w listach kontroli dostępu Security ACL – 1000
LAN-03.11	ilość wpisów w listach kontroli dostępu QoS ACL – 1000
LAN-03.12	1000 interfejsów SVI L3
LAN-03.13	Jumbo frame 9198B
LAN-03.14	48 połączeń zagregowanych typu „port channel”
LAN-03.15	16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
LAN-04	**Oprogramowanie/funkcjonalność:**
LAN-04.01	Obsługa protokołu NTP
LAN-04.02	IEEE 802.1w Rapid Spanning Tree
LAN-04.03	Per-VLAN Rapid Spanning Tree (PVRST+)
LAN-04.04	IEEE 802.1s Multi-Instance Spanning Tree
LAN-04.05	Obsługa 64 instancji protokołu STP
LAN-04.06	Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
LAN-04.07	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 liku podstawowego
LAN-04.08	Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED
LAN-04.09	Realizacja funkcji 802.1Q tunneling (QinQ)
LAN-04.10	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
LAN-04.11	Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
LAN-04.12	Możliwość uruchomienia funkcji serwera DHCP
LAN-04.13	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,
LAN-04.14	Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
LAN-04.15	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.),
LAN-04.16	Funkcjonalność sondy IP SLA Responder,
LAN-05	**Mechanizmy związane z bezpieczeństwem sieci:**
LAN-05.01	Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
LAN-05.02	Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
LAN-05.03	Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

LAN-05.04	Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
LAN-05.05	Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
LAN-05.06	Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
LAN-05.07	Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
LAN-05.08	Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
LAN-05.09	Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
LAN-05.10	Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
LAN-05.11	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),
LAN-05.12	Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
LAN-05.13	Obsługa list kontroli dostępu (ACL) następujących typów: • Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, • VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, • Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, • Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
LAN-05.14	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) z mechanizmem MACsec Key Agreement (MKA),
LAN-05.15	Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
LAN-05.16	Funkcja Private VLAN;
LAN-05.17	sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
LAN-05.18	bezpieczna sekwencja uruchamiania,
LAN-05.19	sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
LAN-05.20	Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow),
LAN-05.21	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,
LAN-05.22	Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

LAN-05.23	Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,
LAN-06	**Mechanizmy związane z zapewnieniem jakości usług w sieci:**
LAN-06.01	Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
LAN-06.02	Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
LAN-06.03	Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
LAN-06.04	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
LAN-06.05	Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
LAN-06.06	Kontrola sztormów dla ruchu broadcast/multicast/unicast,
LAN-06.07	Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
LAN-07	**Obsługa protokołów i mechanizmów routingu:**
LAN-07.01	Routing statyczny dla IPv4 i IPv6,
LAN-07.02	Routing dynamiczny – RIP, OSPF do 1000 PIM Stub do 1000 routes
LAN-07.03	Policy-based routing (PBR),
LAN-07.04	Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
LAN-07.05	Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
LAN-07.06	Wsparcie dla protokołu LISP zgodnie z RFC 6830,
LAN-07.07	Obsługa 4 wirtualnych instancji routingu (VRF),
LAN-07.08	Obsługa zaawansowanych protokołów routingu • IS-IS dla IPv4 i IPv6, • OSPF, • EIGRP (rfc7868), • Routing multicastów - PIM-SM, PIM-SSM, • Multicast Source Discovery Protocol (MSDP),
LAN-07.09	Możliwość enkapsulacji ruchu w pakiety VXLAN,
LAN-08	**Zarządzanie i konfiguracja:**
LAN-08.01	Port konsoli,
LAN-08.02	Dedykowany port Ethernet do zarządzania out-of-band,
LAN-08.03	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,
LAN-08.04	Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
LAN-08.05	Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
LAN-08.06	Wsparcie dla protokoły RESTCONF,
LAN-08.07	Wsparcie dla protokołu gNMI,
LAN-08.08	Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

LAN-08.09	Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
LAN-08.10	Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
LAN-08.11	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,
LAN-08.12	Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
LAN-07	**Wyposażenie urządzenia:**
LAN-07.01	Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,
LAN-07.02	Przełącznik wyposażony jest w moduł do łączenia w stos wraz z kablem stakującym o długości 50 cm,
LAN-07.03	Przełącznik musi być wyposażony jest w moduł rozszerzeń 2x25G.
LAN-07.04	Urządzenie musi zostać wyposażone w licencje subskrypcyjną na wymagane funkcjonalności na okres 48 miesięcy
LAN-07.05	Urządzenie musi w pełni współpracować z dostarczanym systemem do zarządzania siecią LAN, jeżeli wymaga dostarczenia dodatkowych licencji to należy je dostarczyć

11. WYMAGANIA DOTYCZĄCE PRZEŁACZNIKÓW LAN DOSTĘPOWYCH TYP 2 – 20 szt.

Identyfikator wymagania	*Opis wymagania*
LAN-01	**Rodzaj urządzenia:**
LAN-01.01	Przełącznik musi być wyposażony w minimum 12 porty 10/100/1000BaseT POE+ oraz 2 porty 10G SFP+
LAN-01.02	Musi być możliwość montażu w szafie rack 19”. Wysokość maksimum 1RU, głębokość nie większa niż 24cm. Szerokość nie większa niż 28cm. Obudowa bezwiatrakowa.
LAN-02	**Wydajność:**
LAN-02.01	Przełącznik musi zapewniać obsługę wszystkich portów z pełną wydajnością (wirespeed). Szybkość przełączania minimum 50 Mpps dla pakietów 64-bajtowych
LAN-02.02	Minimum 512MB pamięci DRAM i 128MB pamięci Flash
LAN-02.03	Obsługa minimum 1000 sieci VLAN
LAN-02.04	Obsługa minimum 16.000 adresów MAC
LAN-03	**Oprogramowanie/funkcjonalność:**
LAN-03.01	Obsługa protokołu NTP
LAN-03.02	Obsługa IGMPv3 i MLDv1/2 Snooping
LAN-03.03	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu STP
LAN-03.04	Obsługa protokołu LLDP i LLDP-MED
LAN-03.05	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

LAN-03.06	Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów bezpieczeństa typu Port Security i IP Source Guard na interfejsach link aggregation
LAN-03.07	Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
LAN-03.08	Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
LAN-04	Mechanizmy bezpieczeństwa Sieci:
LAN-04.01	Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
LAN-04.02	Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
LAN-04.02	Obsługa funkcji Guest VLAN
LAN-04.03	Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
LAN-04.05	Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X (bez konieczności stosowania zewnętrznego serwera www)
LAN-04.06	Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
LAN-04.07	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
LAN-04.08	Możliwość wdrożenia uwierzytelniania w oparciu o 802.1X w trybie monitor (niezależnie od tego czy uwierzytelnianie się powiedzie, czy nie użytkownik ma prawo dostępu do sieci) – jako element sprawdzenia gotowości instalacji na pełne wdrożenie 802.1X
LAN-04.09	Przełącznik musi posiadać funkcję supplicanta 802.1X (możliwość podłączenia przełącznika do innego switcha z uruchomionym mechanizmem uwierzytelniania 802.1X)
LAN-04.10	Obsługa funkcji bezpieczeństwa sieci LAN: Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
LAN-04.11	Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
LAN-04.12	Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
LAN-04.13	Obsługa list kontroli dostępu (ACL)
LAN-04.14	Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard) oraz ochronę przed fałszowaniem źródłowych adresów IPv6 (IPv6 Source Guard)
LAN-04.15	Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6
LAN-04.16	Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)

LAN-04.17	Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
LAN-04.18	Obsługa funkcji Guest VLAN
LAN-04.19	Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
LAN-04.20	Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X (bez konieczności stosowania zewnętrznego serwera www)
LAN-04.21	Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
LAN-04.22	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
LAN-04.23	Możliwość wdrożenia uwierzytelniania w oparciu o 802.1X w trybie monitor (niezależnie od tego czy uwierzytelnianie się powiedzie, czy nie użytkownik ma prawo dostępu do sieci) – jako element sprawdzenia gotowości instalacji na pełne wdrożenie 802.1X
LAN-04.24	Przełącznik musi posiadać funkcję supplicanta 802.1X (możliwość podłączenia przełącznika do innego switcha z uruchomionym mechanizmem uwierzytelniania 802.1X)
LAN-04.25	Obsługa funkcji bezpieczeństwa sieci LAN: Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
LAN-04.26	Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
LAN-04.27	Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
LAN-04.28	Obsługa list kontroli dostępu (ACL)
LAN-04.29	Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard) oraz ochronę przed fałszowaniem źródłowych adresów IPv6 (IPv6 Source Guard)
LAN-04.30	Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6
LAN-04.31	Możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym
LAN-04.32	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)
LAN-05	**Funkcjonalności z zakresu zapewnienia jakości usług:**
LAN-05.01	Implementacja co najmniej czterech kolejek sprzętowych dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek
LAN-05.02	Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
LAN-05.03	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP

LAN-05.04	Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Wymagana jest możliwość skonfigurowania minimum 64 różnych ograniczeń per port, każde odpowiednio dla różnej klasy obsługi ruchu
LAN-05.05	Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
LAN-06	**Zarządzanie i konfiguracja:**
LAN-06.01	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.)
LAN-06.02	Wbudowane reflektometry (TDR) dla portów 10/100/1000
LAN-06.03	Dedykowany port Ethernet do zarządzania out-of-band
LAN-06.04	Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
LAN-06.05	Urządzenie musi być wyposażone w port konsoli
LAN-06.06	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 5 plików konfiguracyjnych

a) Z przełącznikami, Wykonawca zobowiązany jest dostarczyć następujące okablowanie i akcesoria:
- 20x rura peszel z 4 szt. kabla światłowodowego LC-LC MM OM4 duplex 5m;
- 20x rura peszel z 4 szt. kabla światłowodowego LC-LC MM OM4 duplex 10m;
- 20x rura peszel z 4 szt. kabla światłowodowego LC-LC MM OM4 duplex 15m;
- 5x rura peszel z 4 szt. kabla światłowodowego LC-LC MM OM4 duplex 20m;
- 200x kabel miedziany RJ45 kat 6a 0,5m;
- 200x kabel miedziany RJ45 kat 6a 1,5m;
- 200x kabel miedziany RJ45 kat 6a 3m;
- 200x kabel miedziany RJ45 kat 6a 7m;
- 10x taśma/opaska rzep do kabli szerokość 10mm, długość 5m;
- 200x opaski zaciskowe 2,5 x 100 mm;
- 200x opaski zaciskowe 3,5 x 150 mm;
- 200x opaski zaciskowe 3,5 x 250 mm;
- 200x śruby montażowe M6 do szafy RACK 19" (zestaw – śruba, nakrętka, podkładka);
- 30x organizer kablowy 19", 1U, min. 5 uchwytów, metalowy;
- 30x listwa zasilająca do szaf RACK 19”, pozioma, 1U, 8 gniazd zasilających, podświetlany wyłącznik sieciowy, bezpiecznik, długość przewodu min. 1,5 m, wtyczka/gniazda UNI-SCHUKO min.16A;
- 30x listwa zasilająca do szaf RACK 19”, pozioma, 1U, 8 gniazd zasilających, podświetlany wyłącznik sieciowy, bezpiecznik, długość przewodu min. 3 m, wtyczka/gniazda UNI-SCHUKO min.16A.
- 30x listwa zasilająca do szaf RACK 19”, pozioma, 1U, 8 gniazd zasilających, podświetlany wyłącznik sieciowy, bezpiecznik, długość przewodu min. 5 m, wtyczka/gniazda UNI-SCHUKO min.16A.

12. WYMAGANIA DOTYCZĄCE SYSTEMU ZARZĄDZANIA SIECIĄ LAN

Identyfikator wymagania	*Opis wymagania*
MGMT-01	**System musi posiadać:**
MGMT-01.01	Graficzny interfejs użytkownika
MGMT-01.02	Hierarchizacja zarządzania siecią odzwierciedlająca hierarchię geograficzną tj. możliwość podziału sieci na kilka poziomów geograficznych np. region, kraj, miasto, budynek, piętro;
MGMT-01.03	Wizualizacja graficzna na mapie lokalizacji poszczególnych urządzeń sieciowych – automatyczne rozmieszczanie urządzeń na postawie adresów pocztowych;
MGMT-01.04	Obsługa REST API;
MGMT-01.05	Integracja z system uwierzytelniania w celu otrzymywania informacji o tym jaki użytkownik jest związany z jakim urządzeniem, szczegółowej informacji o przebiegu procesu uwierzytelniania do sieci. Uwzględnienie tych danych w procesie wyznaczania indeksów jakości pracy użytkowników jak również w procesie diagnostyki problemów w sieci;
MGMT-01.06	Mechanizm automatycznej aktualizacji wersji systemu bezpośrednio z chmury producenta wtedy, kiedy pojawiają się nowe wersje;
MGMT-01.07	Wbudowane narzędzia do automatycznego tworzenia polityki QoS dla całej sieci w oparciu o wbudowane wzorce aplikacji, z możliwością tworzenia własnych wzorców. Możliwości dokonywania zmian w polityce i jej szybkiej implementacji oraz możliwość cofania zmian bez konieczności ręcznej rekonfiguracji urządzeń sieciowych;
MGMT-01.08	Funkcjonalność automatycznego wykrywania urządzeń sieciowych w oparciu o SNMP, CLI, http, SSH;
MGMT-01.09	Możliwość tworzenia parametryzowanych wzorców konfiguracyjnych dla urządzeń w oparciu o język skryptowy;
MGMT-01.10	Inwentaryzacja urządzeń oraz oprogramowania;
MGMT-01.11	Zarządzanie wersjami oprogramowania z możliwością wskazania wersji obowiązujących;
MGMT-01.12	Narzędzie do bezdotykowej konfiguracji urządzeń sieciowych (Plug and Play lub Zero Touch Deployment);
MGMT-01.13	Narzędzie do zdalnego uruchamiania aplikacji i zarządzania nimi na urządzeniach sieciowych wyposażonych w taką funkcjonalność;
MGMT-01.14	Możliwość definiowania profili sieciowych oraz parametrów sieciowych takich jak: serwery TACAS, Radius, NTP, Syslog, NetFlow, DNS, DHCP dla poszczególnych poziomów hierarchii sieciowej niezależnie lub dziedziczenie tych ustawień z poziomu wyższego w dół hierarchii. Centralne zarządzania parametrami dostępowymi do urządzeń wraz z możliwością ich zmiany dla jednego urządzenia, grupy urządzeń lub całej sieci;
MGMT-01.15	System dostarczany jest jako appliance sieciowy w wersji sprzętowej umożliwiającej zarządzanie co najmniej 300 urządzeniami
MGMT-01.16	System musi współpracować z posiadanymi przez Zamawiającego przełącznikami Cisco Catalyst 6880-X oraz Cisco Catalyst 3650. Urządzenia te muszą znajdować się na liście kompatybilności oferowanego systemu.
MGMT-01.17	Jeżeli zarządzenie urządzeniami posiadanymi przez Zamawiającego (Cisco Catalyst C6880-X-LE oraz Cisco Catalyst WS-C3650-48FD-S) wymaga dodatkowej licencji na te urządzenia to należy ją dostarczyć w ilościach: • 4x C6880-X-LE

	• 25x WS-C3650-48FD-S
MGMT-02	**Monitoring aplikacji:**
MGMT-02.01	Szczegółowe informacje o aplikacjach wykorzystywanych w sieci takie jak: lista wszystkich wykrytych aplikacji z podaniem nazw aplikacji, klas ruchu, ilości ruchu generowanego, średniej przepustowości, straty pakietów, opóźnienia sieciowego oraz wykrytych problemów związanych z daną aplikacją;
MGMT-02.02	Szczegółowe wykresy czasowe parametrów działania każdej z aplikacji z uwzględnieniem: przepustowości wykorzystywanej przez daną aplikację, strat pakietów, jitter, opóźnienia sieciowego, opóźnienia sieciowego po stronie klienta, opóźnienia sieciowego po stronie serwera, opóźnienia generowanego przez serwer aplikacyjny;
MGMT-02.03	Szczegółowa lista wszystkich użytkowników wykorzysujących daną aplikację w sieci z podaniem urządzenia końcowego, który wykorzystuje daną aplikację;
MGMT-03	**Monitoring użytkowników:**
MGMT-03.01	Szczegółowe informacje o użytkowniku końcowym i urządzeniach na których pracuje takie jak: • identyfikator użytkownika, • nazwa hosta lub hostów, na których pracuje, • adres MAC hosta lub hostów, • adres IPv4 i IPv6 hosta lub hostów, • typ urządzenia, • urządzenie, do którego jest podłączone dane urządzenie końcowe wykorzystywane przez użytkownika, • lokalizacja geograficzna;
MGMT-03.02	Wykres zmian indeksu jakości pracy użytkownika i urządzenia, urządzenia, które wykorzystuje w zadanym okresie czasu do 7 dni wstecz;
MGMT-03.03	Szczegółowa lista wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz) problemów skojarzonych z danym urządzeniem końcowym;
MGMT-03.04	Schemat topologii sieci z zaznaczeniem urządzenia dostępowego do którego jest podłączony dane urządzenie końcowe;
MGMT-03.05	Dostęp do zdarzeń zarejestrowanych w systemie związanych z danym urządzenie z możliwością filtrowanie wg. ważności;
MGMT-03.06	Możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia do danego innego miejsca (adresu IP);
MGMT-03.07	Informacje o generowanym ruchu sieciowym przez użytkownika na danym urządzeniu końcowym z podziałem na aplikacje biznesowe oraz niebiznesowe. Szczegółowe informacje dla każdej z aplikacji takie jak: nazwa aplikacji, indeks jakości działania aplikacji w sieci, ilość ruchu (w bajtach), średnia przepustowość (w bps), parametry QoS faktyczne oraz oczekiwane, straty pakietów (maksymalne i średnie), opóźnienie sieciowe (maksymalne i średnie), jitter (maksymalny i średni);
MGMT-03.08	Szczegółowe informacje o urządzeniu końcowym wykorzystywanym przez użytkownika: • Wykres czasowy ilości danych nadawanych i otrzymywanych; • Wykres czasowy ilości generowanych zapytań DNS i otrzymywanych odpowiedzi; • Dla urządzeń bezprzewodowych wykres czasowy zmian wartości mocy sygnału radiowego RSSI oraz zmian wartości poziomu szumów SNR; • Dodatkowe dane analityczne dla użytkowników urządzeń końcowych wyposażonych w system operacyjny Apple iOS;
MGMT-04	**Wykrywanie i analiza problemów w sieci:**

MGMT-04.01	Automatyczna analiza zdarzeń w sieci oraz identyfikacja i wyświetlanie na tej podstawie problemów w działaniu sieci na poziomie całej sieci lub poszczególnych monitorowanych obiektów np. problemy związane z danym urządzeniem, użytkownikiem lub aplikacją;
MGMT-04.02	Automatyczna priorytetyzacja problemów;
MGMT-05	**Monitoring urządzeń:**
MGMT-05.01	Monitoring dostępności i osiągalności poszczególnych urządzeń sieciowych;
MGMT-05.02	Pełna lista wszystkich monitorowanych urządzeń sieciowych w całej sieci lub w danej domenie lub lokalizacji z podaniem modelu urządzenia, wersji systemu operacyjnego, adresu IP, indeksu jakości pracy, osiągalności, ilości zidentyfikowanych problemów, lokalizacji geograficznej. Możliwość eksportu danych w postaci pliku CSV;
MGMT-05.03	• Możliwość łatwego filtrowania listy urządzeń wg. kryteriów: • Typ urządzenia: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, • Stan jakości pracy urządzenia: jakość niska, średnia, wysoka; • Lokalizacja; • Model urządzenia; • Wersja systemu operacyjnego; • Adres IP;

13. MODUŁ SFP+ 10/25GE STANDARDU CSR – 100 sztuk

Identyfikator wymagania	*Opis wymagania*
SFP-01	Kompatybilność z oferowanymi przełącznikami LAN
SFP-02	Zgodność ze standardem SFP+ 10/25GBase-CSR

14. MODUŁ SFP+ 10/25GE STANDARDU LR – 24 sztuk

Identyfikator wymagania	*Opis wymagania*
SFP-01	Kompatybilność z oferowanymi przełącznikami LAN
SFP-02	Zgodność ze standardem SFP+ 10/25GBase-LR

15. MODUŁ SFP 1GE STANDARDU 1000Base-T – 24 sztuki

Identyfikator wymagania	*Opis wymagania*
SFP-01	Kompatybilność z oferowanymi przełącznikami LAN
SFP-02	Zgodność ze standardem SFP 1000Base-T

16. **WYKONAWCA ZOBOWIĄZANY JEST DOSTARCZYĆ I ZAINSTALOWAĆ 1 szt. PRZEŁĄCZNIKA SIECIOWEGO, SZKIELETOWEGO CENTRUM DANYCH DC: CISCO NEXUS C9508, W PEŁNI WSPÓŁPRACUJĄCY Z POSIADANYMI PRZEZ ZAMAWIAJĄCEGO, tj: CISCO NEXUS C9508 LUB PRODUKT RÓWNOWAŻNY.**

UWAGA: Dostarczony przełącznik musi być zgodny z parametrami i wyposażeniem opisanym dla produktu równoważnego.

Produkt równoważny musi spełniać następujące wymagania:

a) Urządzenie o architekturze modularnej, pozwalającej na instalację kart liniowych, redundantnych modułów kontrolno-zarządzających (supervisorów) oraz modułów przełączających (fabryk), nie mniej niż 8 gniazd na karty liniowe.

b) Urządzenie musi być oparte o w pełni rozdzielną i niezależną od warstwy przesyłania danych warstwę kontrolno-zarządzającą. Moduły kontrolno-zarządzające (supervisory) nie mogą pośredniczyć w przesyłaniu ramek/pakietów między modułami liniowymi;

c) Urządzenie musi posiadać zainstalowany jeden moduł kontrolno-zarządzający;

d) Wydajność urządzenia:
   a. Moduły przełączające zapewniające przepływność co najmniej 3 Tbps (jednokierunkowo) per gniazdo na kartę liniową.
   b. głębokość buforów min. 40 MB
   c. pamięć RAM min. 24 GB
   d. Pamięć SSD/FLASH 256GB

b) Wyposażenie w porty:
   a. Urządzenie musi być wyposażone w 76 gniazd QSFP28 40/100 GigabitEthernet umożliwiających instalację wkładek QSFP28 następującego typu: 40G-Twinax (DAC) 1/3/5/10 metrów, 40G-AOC 1/3/5/10 metrów, 40G-SR4, 100G-SR4, 100G-LR4, 100GBASE-SR BiDi LC. Wszystkie porty 40/100GE SFP+ muszą mieć możliwość jednoczesnej pracy w trybie wirespeed (linerate), zarówno dla prędkości 40G jak i 100G.
   b. Urządzenie musi być wyposażone w 96 gniazd SFP+ 1/10/25 GigabitEthernet umożliwiające instalację wkładek SFP następującego typu: 1000BaseT, 1000BaseSX, 10G-SR, 10G-LR, 10G-Twinax (DAC) 1/3/5/10 metrów, 10G-AOC 1/3/5/10 metrów, 25G-SR, 25G-Twinax (DAC) 1/3/5 metrów, 25G-AOC 1/3/5/10 metrów. Wszystkie porty 10GE SFP+ muszą mieć możliwość jednoczesnej pracy w trybie wirespeed (linerate), zarówno dla prędkości 10G jak i 25G.

c) Urządzenie musi być dostarczone razem z następującymi wkładkami:
   a. 40 wkładek światłowodowych typu 100GBASE-SR BiDi LC umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional);
   b. 1 kabel Twinax 100G o długości 3 metrów;
   c. 8 wkładek światłowodowych typu 40GBase-SR4 QSFP.

d) Przełącznik musi posiadć sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit. Wymagane jest wsparcie technologii MacSec przynajmniej na 72 portach QSFP28 40/100.

e) Wymagana funkcjonalność Ethernet dla warstwy 2:
   a. Trunking IEEE 802.1Q VLAN;
   b. Wsparcie dla min. 4000 VLAN;
   c. Wsparcie dla 88,000 adresów MAC ;
   d. Rapid Per-VLAN Spanning Tree Plus (PVRST+) (IEEE 802.1w);
   e. Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s);
   f. Internet Group Management Protocol (IGMP) Versions 1, 2, 3 snooping;
   g. Grupowanie EtherChannel (do 32 portów per wiązka EtherChannel);
   h. Link Aggregation Control Protocol (LACP): IEEE 802.3ad;
   i. Grupowanie typu MCEC/MLAG/virtual PortChannel polegające na terminowaniu pojedynczej wiązki EtherChannel (LACP) na 2 niezależnych urządzeniach;
   j. Ramki Jumbo dla wszystkich portów (min. 9216 bajtów);
   k. Wsparcie sprzętowe dla tunelowania QinQ;
   l. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu multicast, broadcast;
   m. BFDv6;

f) Wymagana funkcjonalność dla warstwy 3:
   a. IPv4;
   b. IPv6;
   c. Protokoły routingu dla IPv4: RIPv2, OSPFv2, IS-IS, BGP;
   d. Protokoły routingu dla IPv6: OSPFv3, IS-IS, BGP;
   e. Wsparcie dla minimum 512 tysięcy tras w tablicy routingu IPv4;
   f. Wsparcie dla minimum 172 tysięcy tras w tablicy routingu IPv6;
   g. Policy Based Routing dla IPv4 oraz IPv6;
   h. Wirtualizacja warstwy 3 (VRF) dla IPv4 oraz IPv6;
   i. HSRP lub VRRP lub odpowiednik;
   j. Multicast: IGMPv3, MSDP, PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
   k. 32,000 prefiksów multicast;
   l. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking);
   m. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);
   n. Minimum 3000 wejściowych oraz 1500 wyjściowych wpisów dla ACL - access control list dla IPv4;

g) Przełącznik musi posiadać możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet. Dołączenie modułów lub przełączników nie jest realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3 a jedynie w ramach domeny fizycznej bądź stosu urządzeń. Porty modułu wyniesionego udostępniane do zarządzania i monitorowania z poziomu przełącznika centralnego.

h) Przełącznik powinien mieć możliwość podłączenia do obecnych w sieci Zamawiającego przełączników Cisco Nexus 2248TP (16 sztuk) oraz Nexus 2232PP (18 sztuk). W przypadku braku możliwości współpracy z tymi przełącznikami, należy dostarczyć przełączniki równoważne w ilościach takich jak posiadane przez Zamawiającego. Opis równoważności znajduje się na końcu Rozdziału II pkt 1.

i) Wymagane funkcje bezpieczeństwa:
   a. Wejściowe ACL (standardowe oraz rozszerzone);
   b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC addresses, typ protokołu, itd.;
   c. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i v6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP), itd.;

d. ACL oparte o VLAN-y (VACL);
e. ACL oparte o porty (PACL);
f. Logowanie i statystyka dla ACL;
g. DHCP Snooping;
h. ARP Inspection;
i. IP Source Guard;
j. Wsparcie dla protokołu autentykacji 802.1X łącznie ze wsparciem dla wielokrotnej autentykacji na tym samym porcie oraz dynamicznym przydziałem VLAN;
k. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast;
l. Ograniczanie ruchu kierowanego do warstwy kontrolno-sterującej (control plane policing);

j) Wymagane funkcje jakości usług QoS:
a. Layer 2 IEEE 802.1p (CoS);
b. Klasyfikacja ruchu w oparciu o: 802.1Q CoS, IP precedence, IP DSCP, rozmiar pakietu;
c. Znakowanie (marking) ruchu w oparciu o: 802.1Q CoS, IP precedence, IP DSCP;
d. Dławienie (policing) ruchu wejściowego i wyjściowego;
e. Kolejkowanie na wyjściu w oparciu o CoS 802.1p;
f. Flow control w oparciu o ramki Pause IEEE 802.3x;

k) Wymagane podstawowe funkcje zarządzania:
a. Port zarządzający 10/100 /1000 Mbps;
b. Port konsoli CLI;
c. Port USB;
d. Zarządzanie In-band;
e. SSHv2;
f. Telnet;
g. Authentication, authorization, and accounting (AAA);
h. RADIUS;
i. TACACS+;
j. LDAP;
k. Syslog;
l. PTP (Precision Time Protocol) IEEE 1588;
m. SNMP v1, v2, v3;
n. Remote monitoring (RMON), przynajmniej grupy Alarms, Events;
o. sFlow lub NetFlow;
p. IEEE 802.1ab LLDP;
q. Role-Based Access Control RBAC;
r. Wsparcie sprzętowe dla gromadzenia i strumieniowania danych telemetrycznych w formatach GPB oraz JSON obejmujących szczegółowe dane na temat przepływów sieciowych;
s. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu;
t. Możliwość wykonywania shapshotów konfiguracji (checkpoint) i przywracania jej w dowolnym momencie bez potrzeby restartu urządzenia (rollback);
u. Wysyłanie powiadomień e-mail w razie wystąpienia błędu;
v. Liczniki pakietów wchodzących/wychodzących per każdy port;
w. Network Time Protocol (NTP);
x. Ping;
y. Traceroute;

l) Wymagane funkcje programowania i automatyzacji:
a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
b. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika
c. Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener posiada możliwość wykorzystywania portów fizycznych przełącznika.
d. Wsparcie dla wbudowanego środowiska konteneryzacji Docker wraz z możliwością uruchamiania usług opartych o kontenery Docker
e. Interfejs programistyczny REST API wraz z upublicznionym SDK do budowy aplikacji przeznaczonych do uruchomienia na urządzeniu
f. Możliwość uruchomienia klienta Chef
g. Możliwość uruchomienia agenta Puppet
h. Możliwość uruchomienia agenta gRPC i konfigurowania poprzez GBP API
i. Możliwość konfiguracji poprzez Ansible z dostępnymi na stronach Ansible modułami
j. Wsparcie dls NETCONF i zarządzania poprzez XML
k. Wsparcie dla OpenStack Neutron plugin

m) Wymagania środowiskowe:
a. Obudowa o wysokości nie większej niż 13 RU (rack units)
b. Obudowa, zasilacze i wentylatory oryginalnie zaprojektowane przez producenta do chłodzenia przepływem powietrza przód - tył
c. Nie mniej niż 3 zasilacze pracujące w trybie redundantnym, zasilane prądem naprzemiennym 230 V i zapewniające razem nie mniej niż 9 kW nominalnej mocy.
d. Redundantne wentylatory
e. Wymiana wszystkich modułów i kart liniowych bez wyłączania zasilania (tzw. Hot-Swap)
f. Obudowa wykonana z metalu, przystosowana do montażu w szafie 19’’.

17. **WYKONAWCA ZOBOWIĄZANY JEST DOSTARCZYĆ I ZAINSTALOWAĆ 12 szt. PRZEŁĄCZNIKÓW SIECIOWYCH DOSTĘPOWYCH CENTRUM DANYCH DC: Cisco Nexus C93180YC-FX, W PEŁNI WSPÓŁPRACUJĄCY Z POSIADANYMI PRZEZ ZAMAWIAJĄCEGO, tj: Cisco Nexus C93180YC-FX LUB PRODUKT RÓWNOWAŻNY.**
UWAGA: Dostarczone przełączniki muszą być zgodne z parametrami i wyposażeniem opisanym dla produktu równoważnego.

Produkt równoważny musi spełniać następujące wymagania:

b) Przełącznik posiada:
   a. 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+ bezpośrednio w obudowie przełącznika lub na karcie liniowej
   b. 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps

c) Parametry wydajnościowe:
   a. Prędkość przełączania „wirespeed" dla każdego portu przełącznika
   b. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
   c. Obsługiwana łączna przepływność (pasmo) min. 3,6 Tbps
   d. Obsługiwana łączna przepustowość pakietowa przełącznika min. 2,000 mpps
   e. opóźnienie przełączania pakietów poniżej 2 µs
   f. głębokość buforów min. 40 MB
   g. pamięć RAM min. 24 GB
   h. Pamięć SSD/FLASH 128GB

d) Przełącznik posiada następującą funkcjonalność warstwy L2:
   a. Trunking IEEE 802.1Q VLAN;
   b. Wsparcie dla 3900 sieci VLAN;
   c. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   d. Wsparcie sprzętowe dla minimum 250 tysięcy adresów MAC
   e. IEEE 802.1w Rapid Spanning Tree (RST)
   f. IEEE 802.1s Multiple Spanning Tree (MST)
   g. Wsparcie sprzętowe dla tunelowania QinQ
   h. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree
   i. Internet Group Management Protocol (IGMP) Versions 2, 3;
   j. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   k. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce
   l. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);

e) Przełącznik posiada następująca funkcjonalność warstwy L3
   a. Sprzętowe przełączanie pakietów w warstwie L3
   b. Routing w oparciu o trasy statyczne
   c. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
   d. Policy Based Routing (PBR) dla IPv4
   e. VRRP v3
   f. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol)
   g. Wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP
   h. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast)
   i. Wsparcie dla IGMPv3 oraz MSDP
   j. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych
   k. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking)
   l. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP)
   m. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list
   n. Jeśli funkcjonalność powyższa wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie

f) Przełącznik posiada sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit. Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie

g) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   a. Layer 2 IEEE 802.1p (CoS);
   b. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4;
   c. Kolejkowanie na wyjściu w oparciu o CoS 802.1p;
   d. Bezwzględne (strict-priority) kolejkowanie na wyjściu;
   e. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający
   f. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych
   g. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   h. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb

h) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   a. Wejściowe ACL (standardowe oraz rozszerzone);
   b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
   c. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
   d. ACL oparte o VLAN-y (VACL);
   e. ACL oparte o porty (PACL);
   f. DHCP Snooping
   g. ARP Inspection
   h. IP Source Guard
   i. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast

i) Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
   a. Port zarządzający 100/1000 Mbps;
   b. Port konsoli CLI;

c. Zarządzanie In-band;
d. SSHv2;
e. Authentication, authorization, and accounting (AAA);
f. RADIUS;
g. TACACS+
h. Syslog;
i. SNMP v1, v2, v3;
j. RMON (przynajmniej grupy Events, Alarms)
k. sFlow lub netFlow
l. IEEE 802.1ab LLDP
m. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
n. Role-Based Access Control RBAC;
o. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
p. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror)
q. Network Time Protocol (NTP);
r. Precision Time Protocol IEEE 1588
s. Diagnostyka procesu BOOT;
t. Ping
u. Traceroute

j) Narzędzia programowania i zarzadzania przełącznikiem:
   a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
   b. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika
   c. Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener posiada możliwość wykorzystywania portów fizycznych przełącznika.
   d. Interfejs programistyczny REST API wraz z upublicznionym SDK
   e. Możliwość zainstalowania klienta Chef
   f. Możliwosć zainstalowania agenta Puppet
   g. Wsparcie dls NETCONF i zarządzania poprzez XML
   h. Wsparcie dla OpenStack Neutron plugin
k) Urządzenie musi być dostarczone razem z następującymi wkładkami:
   a. 2 wkładki 100GBASE-SR BiDi LC umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional)
   b. 1 kabel Twinax 100G QSFP28 o długości 1 m
   c. 16 wkładek 10G SFP+ SR LC
l) Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych lub połączeń zasilających urządzenia
m) Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”,

18. WYKONAWCA ZOBOWIĄZANY JEST DOSTARCZYĆ I ZAINSTALOWAĆ 12 szt. PRZEŁĄCZNIKÓW SIECIOWYCH 1G CENTRUM DANYCH DC: Cisco Nexus C9348GC-FXP, W PEŁNI WSPÓŁPRACUJĄCY Z POSIADANYMI PRZEZ ZAMAWIAJĄCEGO, tj: Cisco Nexus C9348GC-FXP LUB PRODUKT RÓWNOWAŻNY.
UWAGA: Dostarczone przełączniki muszą być zgodne z parametrami i wyposażeniem opisanym dla produktu równoważnego.

Produkt równoważny musi spełniać następujące wymagania:

a) Przełącznik posiada:
   a. 48 portów 100Mb/1GBaseT
   b. 4 porty SFP+ 1/10/25 Gbpsb
   c. 2 porty definiowane za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps
b) Parametry wydajnościowe:
   a. Prędkość przełączania „wirespeed” dla każdego portu przełącznika
   b. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
   c. Obsługiwana łączna przepływność (pasmo) min. 600 Gbps
   d. Obsługiwana łączna przepustowość pakietowa przełącznika min. 250 mpps
   e. opóźnienie przełączania pakietów nie większe niż 3 µs
   f. głębokość buforów min. 40 MB
   g. pamięć RAM min. 24 GB
   h. Pamięć SSD/FLASH 128GB
c) Przełącznik posiada następującą funkcjonalność warstwy L2:
   a. Trunking IEEE 802.1Q VLAN;
   b. Wsparcie dla 3900 sieci VLAN;
   c. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   d. Wsparcie sprzętowe dla minimum 250 tysięcy adresów MAC
   e. IEEE 802.1w Rapid Spanning Tree (RST)
   f. IEEE 802.1s Multiple Spanning Tree (MST)
   g. Wsparcie sprzętowe dla tunelowania QinQ
   h. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree
   i. Internet Group Management Protocol (IGMP) Versions 2, 3;
   j. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   k. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce
   l. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
d) Przełącznik posiada następująca funkcjonalność warstwy L3

   a. Sprzętowe przełączanie pakietów w warstwie L3
   b. Routing w oparciu o trasy statyczne
   c. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
   d. Policy Based Routing (PBR) dla IPv4
   e. VRRP v3
   f. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol)
   g. Wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP
   h. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast)
   i. Wsparcie dla IGMPv3 oraz MSDP
   j. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych
   k. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking)
   l. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP)
   m. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list
   n. Jeśli funkcjonalność powyższa wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie
e) Przełącznik posiada sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit. Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie
f) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   a. Layer 2 IEEE 802.1p (CoS);
   b. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4;
   c. Kolejkowanie na wyjściu w oparciu o CoS 802.1p;
   d. Bezwzględne (strict-priority) kolejkowanie na wyjściu;
   e. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający
   f. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych
   g. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   h. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
g) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   a. Wejściowe ACL (standardowe oraz rozszerzone);
   b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
   c. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
   d. ACL oparte o VLAN-y (VACL);
   e. ACL oparte o porty (PACL);
   f. DHCP Snooping
   g. ARP Inspection
   h. IP Source Guard
   i. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
h) Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
   a. Port zarządzający 100/1000 Mbps;
   b. Port konsoli CLI;
   c. Zarządzanie In-band;
   d. SSHv2;
   e. Authentication, authorization, and accounting (AAA);
   f. RADIUS;
   g. TACACS+
   h. Syslog;
   i. SNMP v1, v2, v3;
   j. RMON (przynajmniej grupy Events, Alarms)
   k. sFlow lub netFlow
   l. IEEE 802.1ab LLDP
   m. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   n. Role-Based Access Control RBAC;
   o. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   p. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror)
   q. Network Time Protocol (NTP);
   r. Precision Time Protocol IEEE 1588
   s. Diagnostyka procesu BOOT;
   t. Ping
   u. Traceroute
i) Narzędzia programowania i zarzadzania przełącznikiem:
   a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
   b. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika
   c. Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener posiada możliwość wykorzystywania portów fizycznych przełącznika.
   d. Interfejs programistyczny REST API wraz z upublicznionym SDK
   e. Możliwość zainstalowania klienta Chef
   f. Możliwosć zainstalowania agenta Puppet
   g. Wsparcie dls NETCONF i zarządzania poprzez XML
   h. Wsparcie dla OpenStack Neutron plugin
j) Przełącznik musi być wyposażony w:
   a. 2 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional)
k) Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych lub połączeń zasilających urządzenia
l) Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.

19. GWARANCJA

1) Wykonawca zobowiązuje się świadczyć usługi gwarancyjne w miejscu użytkowania sprzętu, z możliwością naprawy w serwisie Wykonawcy, jeżeli naprawa sprzętu w miejscu użytkowania okaże się niemożliwa. W przypadku braku możliwości dokonania naprawy w miejscu użytkowania sprzętu i konieczności jego dostarczenia do punktu serwisowego wskazanego przez Wykonawcę, koszty dostarczenia uszkodzonego sprzętu do punktu serwisowego oraz z punktu serwisowego do miejsca użytkowania pokrywa Wykonawca.
2) Wykonawca zobowiązuje się do ponoszenia wszelkich kosztów naprawy sprzętu, w tym kosztów części zamiennych i podzespołów, transportu, instalacji, konfiguracji i uruchomienia sprzętu.
3) Wykonawca zobowiązuje się do świadczenia usług serwisu z należytą starannością z uwzględnieniem ogólnie przyjętych i stosowanych standardów i procedur przy tego rodzaju usługach, a także zaleceń lub procedur określonych przez producentów sprzętu.
4) Nośniki informacji takie jak np. dyski twarde, pamięci flash, mogą być naprawiane jedynie w miejscu ich użytkowania, a w przypadku konieczności wymiany uszkodzonych nośników na nowe, wolne od wad, nośniki informacji pozostają u Zamawiającego. W przypadku konieczności dokonania naprawy sprzętu wyposażonego w nośniki informacji poza miejscem użytkowania, nośniki te pozostają w siedzibie Zamawiającego.
5) Wykonawca zobowiązany jest w terminie do 90 dni od daty podpisania bez zastrzeżeń Protokołu Odbioru Ilościowego Urządzeń i Licencji do dostarczenia Zamawiającemu niezbędnych danych do autoryzacji na stronie www producenta w celu pobierania nowych wersji oprogramowania sprzętu, poprawek, korzystania z bazy wiedzy, instrukcji obsługi itp.
6) Wykonawca zobowiązuje się przyjmować zgłoszenia gwarancyjne poprzez stronę www Wykonawcy dostępną przez całą dobę, 365 dni w roku. Wykonawca dostarczy dane niezbędne do autoryzacji na stronie www Wykonawcy w celu dokonywania zgłoszeń serwisowych przez Zamawiającego. Zamawiający wymaga również zapewnienia możliwości dokonywania zgłoszeń serwisowych poprzez e-mail na adres .....@..... w przypadku braku możliwości dokonania zgłoszenia serwisowego przez stronę www (np. w przypadku braku dostępności dedykowanej strony www). Wzór formularza zgłoszenia serwisowego będzie stanowił załącznik do Umowy. Wykonawca potwierdzi otrzymanie zgłoszenia serwisowego poprzez wysłanie wiadomości e-mail na adres .....@..... .Wszelkie wykonane przez Wykonawcę lub jego przedstawicieli czynności serwisowe wymagają dokumentowania w formie pisemnej.
7) W przypadku, gdy realizacja zgłoszenia gwarancyjnego wymaga wymiany urządzenia Zamawiający wymaga, aby Wykonawca każdorazowo w takiej sytuacji przedstawił informacje w tym zakresie przedstawicielowi Zamawiającego do akceptacji. Zamawiający zobowiązany jest do udzielenia odpowiedzi w terminie nie dłuższym niż 30 minut na adres email skazany w pkt. 6powyżej. Brak odpowiedzi w wyżej wymienionym terminie oznacza akceptację.
8) Wykonawca zobowiązuje się, że nie będzie dokonywał żadnych modyfikacji sprzętu bez wcześniejszego uzgodnienia ich z Zamawiającym. Zamawiający zobowiązany jest do udzielenia odpowiedzi w terminie nie dłuższym niż 30 minut. Brak odpowiedzi w wyżej wymienionym terminie oznacza akceptację. Zamawiający zastrzega sobie prawo do samodzielnej rozbudowy sprzętu i dokonywania zmian w konfiguracji..
9) Wykonawca zobowiązany jest do świadczenia serwisu gwarancyjnego na każde zgłoszenie serwisowe Zamawiającego.
10) Czas usunięcia awarii lub usterki liczony jest w godzinach od momentu wysłania przez Zamawiającego do Wykonawcy formularza „zgłoszenia serwisowego".
11) Wykonawca podejmie działania serwisowe w trybie 24x7x365- zgłoszenie awarii lub usterki przez wszystkie dni tygodnia, 365 dni w roku, naprawa urządzeń (z wyłączeniem awarii oprogramowania) w ciągu 4 godzin od przesłania zgłoszenia przez Zamawiającego w przypadku awarii oraz naprawa urządzeń (z wyłączeniem usterek oprogramowania) w ciągu 8 godzin od przesłania zgłoszenia przez Zamawiającego w przypadku usterki. Przez **awarię** należy rozumieć stan niesprawności sprzętu uniemożliwiający jego funkcjonowanie, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie. Przez **usterkę** należy rozumieć stan, w którym następuje obniżenie sprawności urządzenia jednak nie wpływającą na jego funkcjonowanie (np. awaria jednego z dwóch redundantnych zasilaczy).
12) Zamawiający dopuszcza możliwość usunięcia awarii lub usterki poprzez dostarczenie i uruchomienie sprzętu zastępczego z zachowaniem terminów określonych w ust. 11. Wykonawca zobowiązany jest do dostarczenia w tym terminie Zamawiającemu kompatybilnego sprzętu zastępczego, wolnego od wad, o parametrach wydajnościowych i funkcjonalnych nie gorszych niż sprzęt podlegający naprawie. Wykonawca zobowiązuje się jednocześnie do naprawy uszkodzonego sprzętu i jego konfiguracji, instalacji i uruchomienia (zamiast sprzętu zastępczego) w terminie nie dłuższym niż 30 dni od przesłania zgłoszenia serwisowego.
13) Wykonawca zobowiązany jest w dniu wykonania naprawy do potwierdzenia wykonania naprawy w protokole „zgłoszenia serwisowego", wskazując datę i godzinę naprawy.. Data i godzina wykonania usługi naprawy zostanie potwierdzona przez przedstawiciela Zamawiającego jest. Ww. dokument musi zostać podpisany (data, godzina i podpis) przez przedstawiciela Zamawiającego.
14) W przypadku wystąpienia awarii tego samego elementu po wykonaniu 3 napraw w okresie obowiązywania Umowy, Wykonawca zobowiązuje się na pisemne wezwanie Zamawiającego do wymiany tego elementu na fabrycznie nowy, nieużywany i wolny od wad, na sprawny, tego samego producenta i tego samego typu o parametrach wydajnościowych i funkcjonalnych nie gorszych niż element wymieniany w terminie 30 dni od dnia otrzymania wezwania do wymiany. Nowe elementy muszą być wyprodukowane nie wcześniej niż sześć miesięcy przed planowanym terminem składania ofert.
15) W przypadku, gdy Wykonawca nie wykona obowiązku wynikającego z ust. 11 Zamawiający na koszt Wykonawcy ma prawo wypożyczyć od dowolnego Wykonawcy sprzęt zastępczy o nie gorszych parametrach od sprzętu ulegającego awarii, zachowując jednocześnie prawo do naliczenia kary umownej i odszkodowania. Jednocześnie Zamawiający ma prawo zlecić dowolnej firmie naprawę uszkodzonego sprzętu, a kosztami naprawy obciążyć Wykonawcę, zachowując jednocześnie prawo do naliczenia kary umownej i odszkodowania, nie tracąc gwarancji Wykonawcy.
16) W przypadku dokonania naprawy przez Wykonawcę poprzez wymianę elementów, zostaną zainstalowane fabrycznie nowe elementy o parametrach wydajnościowych i funkcjonalnych nie gorszych niż elementy wymieniane. Wykonawca udzieli gwarancji na prawidłowe działanie wymienionych Urządzeń na okres 40 miesięcy od ich wymiany.
17) Po usunięciu awarii lub usterki, dostarczeniu sprzętu zastępczego lub wymianie na sprzęt nowy, wolny od wad, obowiązkiem Wykonawcy będzie również uruchomienie i odtworzenie konfiguracji sprzętu wraz z oprogramowaniem w miejscu użytkowania. Odtworzenie konfiguracji jest zależne od dostarczenia przez Zamawiającego kopi konfiguracji. Przekazanie kopi konfiguracji sprzętu do Wykonawcy nastąpi niezwłocznie.
18) Strony zobowiązują się do wzajemnego przekazywania sobie niezwłocznie wszelkich informacji mogących mieć wpływ na realizację zamówienia. Wykonawca niezwłocznie udzieli odpowiedzi w formie pisemnej na zgłaszane przez Zamawiającego uwagi dotyczące realizacji zamówienia, w terminie nie dłuższym niż 2 dni robocze.
19) Osoby wskazane przez Wykonawcę do realizacji Umowy zobowiązane są do przestrzegania postanowień regulaminów wewnętrznych i stosowania odpowiednich procedur obowiązujących w Ministerstwie Sprawiedliwości. Osoby skierowane przez Wykonawcę do realizacji Umowy zobowiązane są do zapoznania się i stosowania się do zapisów polityki bezpieczeństwa Ministerstwa Sprawiedliwości. Powyższe zostanie potwierdzone pisemnym oświadczeniem każdej z osób wyznaczonych do realizacji Umowy.

20) Wykonawca zobowiązany jest do dostarczenia wszelkich części zamiennych, podzespołów i materiałów, które są niezbędne do utrzymania sprzętu sieciowego i oprogramowania sprzętu sieciowego objętego umową w należytym stanie technicznym. Części zamienne, podzespoły i materiały muszą być fabrycznie nowe, nieużywane i wolne od wad.
21) Wykonawca zobowiązany jest do zapewnienia niezbędnych części, podzespołów i materiałów w ramach wynagrodzenia za wykonanie przedmiotu umowy.
22) W ramach serwisu pogwarancyjnego Wykonawca wykona aktualizację oprogramowania sprzętu objętego serwisem, nie rzadziej niż raz na 180 dni za pomocą aktualnych narzędzi aktualizujących do wersji uzgodnionej z Zamawiającym.
23) Harmonogram wykonania wszystkich aktualizacji oprogramowania sprzętu objętego serwisem pogwarancyjnym zostanie uzgodniony z Zamawiającym
w terminie do 30 dni przed przystąpieniem do ww. prac.
24) Przed przystąpieniem do prac związanych z aktualizacją oprogramowania sprzętu Wykonawca przeprowadzi analizę wpływu dokonywanej aktualizacji na sprzęt podłączony do innego sprzętu i pozostałych urządzeń podłączonych do sprzętu.
25) W przypadku wystąpienia problemów, ze sprzętem (lub wersją oprogramowania), a objętym serwisem pogwarancyjnym, wynikających z przeprowadzonej aktualizacji oprogramowania sprzętu sieciowego (lub brakiem komunikacji sieciowej z/do urządzeń podłączonych do sprzętu sieciowego), Wykonawca niezwłocznie wykona powrót do poprzednich wersji i na własny koszt zapewni rozwiązanie problemów z urządzeniami, których prawidłową prace zakłóciły działania prowadzone przez Wykonawcę.
26) Wykonawca:
    a. przeprowadzi, nie rzadziej niż jeden raz na 180 dni analizę w zakresie uaktualnień poziomu oprogramowania sprzętu, poziomu firmware'u (mikrokodów);
    b. przeprowadzi na żądanie Zamawiającego, nie częściej niż jeden raz na 60 dni aktualizację poziomu oprogramowania sprzętu wynikającą z wykrytych podatności
    c. przedstawi Zamawiającemu raport po wykonanej obsłudze serwisowej;
    d. opracuje harmonogram prac optymalizacji instalacji uaktualnień;
    e. zweryfikuje poprawność działania sprzętu i oprogramowania sprzętu po wykonaniu obsługi serwisowej.
27) Wykonawca zobowiązany jest do zapewnienia dla Zamawiającego dostępu do dedykowanego portalu www producenta dla urządzeń, na którym będzie możliwe co najmniej pobieranie i instalacji nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do baz wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp.
28) Zamawiający wymaga zapewnienia dostępu do pomocy technicznej Wykonawcy i producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem. Wykonawca musi zapewnić dostęp Zamawiającemu do najnowszego oprogramowania do sprzętu objętego serwisem pogwarancyjnym. Wykonawca jest zobligowany do instalowania najnowszego oprogramowania na sprzęcie oraz zapewnienia ciągłości działania sprzętu.

20. ASYSTA TECHNICZNA

1) Wykonawca zapewni świadczenie asysty technicznej inżyniera zgodnie z potrzebami Zamawiającego, przez minimum jednego inżyniera, który będzie posiadał certyfikat na poziomie minimum F5-CSE Security, PaloAlto PCNSE, CISCO CCIE – Sec, CISCO CCIE – Routing and Switching, Juniper JNCIP-ENT, Juniper JNCIP – SEC, HPE MASE lub równoważne. Osoby skierowane do realizacji zamówienia muszą posiadać aktualne certyfikaty w całym okresie obowiązywania Umowy. Usługi asysty technicznej inżyniera będą świadczone w wymiarze do 1000 roboczogodzin (w roboczogodzinę wsparcia nie wlicza się czasu dojazdu oraz ilości osób świadczących usługę, tzn. nie ma znaczenia ile osób jednocześnie będzie świadczyło usługę w ramach jednej roboczogodziny). Usługa będzie świadczona dla infrastruktury Zamawiającego (sprzętu i oprogramowania). Równoważność certyfikatów została opisana w SIWZ.
2) Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym serwisem pogwarancyjnym. W przypadku, gdy Zamawiający zleci Wykonawcy prace, które powinny być zrealizowane w ramach serwisu pogwarancyjnego, Wykonawca ma obowiązek poinformowania o tym fakcie Zamawiającego.
3) Zlecenia w ramach asysty technicznej będą dotyczyły w szczególności rozwoju i modyfikacji sprzętu, zaawansowanej konfiguracji sprzętu, wsparciu w zakresie utrzymania sprzętu.
4) Zamawiający będzie przekazywać Wykonawcy, na adres mailowy wskazany w § 4 umowy, zlecenia w ramach asysty technicznej, w których określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
5) Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą w szczególności proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia wraz z rozbiciem na poszczególne czynności.
6) Zamawiający może zaakceptować propozycję wykonania zlecenia albo odrzucić propozycję, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, w wyznaczonym terminie, dodatkowych wyjaśnień, informacji do przedstawionej propozycji wykonania zlecenia.
7) W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, termin wykonania prac.
8) Rozliczenie wsparcia technicznego inżyniera odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Wykonawcę i Zamawiającego, Miesięcznych Protokołów odbioru usługi raz na miesiąc.
9) Zamawiający wymaga, aby inżynier na wezwanie Zamawiającego przybył do wskazanego miejsca/siedziby na terenie Warszawy i tam realizował zgłoszenie. Zamawiający nie dopuszcza zdalnej realizacji zgłoszenia w tym zakresie.

21. WARSZTATY POWDROŻENIOWE

1) Warsztat 1 – Minimalny czas trwania - 5 dni. Warsztat dla 4 osób . W zakresie urządzeń dostarczonych w przedmiotowym postępowaniu.
    a. Poznawanie funkcji sieci komputerowych
    b. Wprowadzenie do modelu komunikacji pomiędzy komputerami
    c. Działanie oprogramowania przełącznika
    d. Wprowadzenie do sieci LAN
    e. Opis warstwy łącza modelu TCP/IP
    f. Rozpoczęcie pracy na przełączniku
    g. Wprowadzenie do warstwy internetu modelu TCP/IP , adresacji IPv4, podsieci
    h. Opis warstwy transportowej i aplikacyjnej modelu TCP/IP
    i. Poznanie funkcji routingu
    j. Podstawowa konfiguracja routera
    k. Opis procesu dostarczania pakietów

l. Diagnozowanie i rozwiązywanie podstawowych problemów w sieciach
m. Opis głównych funkcji IPv6, adresy oraz konfiguracja i weryfikacja podstawowej łączności IPv6
n. Konfigurowanie routingu statycznego
o. Wdrażanie VLAN-ów i trunk-ów
p. Routing pomiędzy VLAN-ami
q. Wprowadzenie do protokołu routingu dynamicznego typu OSPF
r. Poprawa redundancji sieci przełączanych za pomocą rozwiązania typu EtherChannel
s. Wyjaśnienie podstaw działania ACL
t. Konfiguracja dostępu do sieci Internet, protokół DHCP oraz wyjaśnienie i konfiguracja translacji adresów sieciowych (NAT) na routerach
u. Opis koncepcji sieci bezprzewodowych, typy sieci bezprzewodowych oraz wykorzystanie kontrolerów sieci bezprzewodowych LAN (WLC)*
v. Wprowadzenie do różnych architektur sieci i wirtualizacji
w. Wprowadzenie do ewolucji sieci inteligentnych, do koncepcji programowalności sieci, SDN oraz opis inteligentnych rozwiązań do zarządzania siecią, takich jak DNA Center, SD-Access i SD-WAN
x. Konfiguracja podstawowych narzędzi do monitorowania systemu IOS
y. Zarządzanie urządzeniami sieciowymi
z. Zabezpieczanie dostępu administracyjnego do urządzeń
aa. Wdrażanie rozwiązań typu Device Hardening.

2) Warsztat 2 – Minimalny czas trwania - 3 dni. Warsztat dla 4 osób. W zakresie urządzeń dostarczonych w przedmiotowym postępowaniu
   a. Wprowadzenie do przełączników;
   b. Pozycjonowanie przełączników;
   c. Analiza możliwości zarządzania przełącznikami;
   d. Wdrażanie przełączników;
   e. Opis nowych funkcji przełączników;
   f. Opis funkcji skalowania i wydajności przełączników;
   g. Opis funkcji zabezpieczeń, QoS i IoT Convergence w przełącznikach;
   h. Opis rozwiązań chmurowych i automatyzacji zadań w przełącznikach;
   i. Zarządzanie oprogramowaniem przełączników za pomocą interfejsu GUI i komend CLI w programie systemie do zarządzania siecią LAN dostarczonym w ramach zamówienia.

3) Wykonawca zobowiązany jest do przeprowadzenia warsztatów w ośrodku szkoleniowym na terenie Warszawy. Za zgodą Zamawiającego, szkolenia mogą zostać przeprowadzone na odległość, w trybie zdalnym uzgodnionym roboczo przez Strony.
4) Każdy uczestnik otrzyma certyfikat jego ukończenia.
5) Warsztaty muszą być prowadzone w języku polskim.
6) Wykonawca musi dysponować odpowiednio wykwalifikowaną kadrą, której powierzy realizację przedmiotu zamówienia w zakresie warsztatówa. Wymagane jest, aby trenerzy posiadali udokumentowane co najmniej 2- letnie doświadczenie w przedmiocie szkolenia z zakresu oferowanego rozwiązania.
7) Wykonawca zobowiązuje się dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazą szkoleniową z odpowiednimi pomieszczeniami wraz z zapleczem do przeprowadzenia warsztatów dla osób dorosłych tj. sale dostosowane do prowadzenia zajęć, dobrze oświetlone (światło dzienne i sztuczne), wentylowane (z dostępem do świeżego powietrza), posiadające odpowiednie warunki sanitarne, bezpieczeństwa i higieny pracy, wyposażone w akustyczne i jakościowe narzędzia i urządzenia, a także oprogramowania i pomoce dydaktyczne niezbędne do wykonania zamówienia.
8) Wykonawca w terminie do 30 dni, od dnia podpisania bez zastrzeżeń Protokołu Odbioru Ilościowego Urządzeń i Licencji, przedstawi Zamawiającemu do akceptacji Program warsztatów. Program musi zawierać informacje dotyczące tematyki prowadzonych warsztatów z podziałem na zajęcia teoretyczne i praktyczne. Program powinien zawierać również informacje dotyczące wiedzy i umiejętności jakie zdobędą uczestnicy po zakończeniu warsztatów.
9) Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy warsztatów – z rozpisaniem na dni i godziny i dostarczy je do 30 dni, od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu.
10) Zajęcia odbywać się będą w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin zegarowych dziennie. Harmonogram i program powinny zostać wydrukowane i rozdane uczestnikom szkolenia na pierwszym spotkaniu.
11) Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika do danego rodzaju warsztatu, pozwalające na samodzielną edukację z zakresu tematyki warsztatów (opracowania, wydruku materiałów szkoleniowych).
12) Komplet materiałów szkoleniowych dla każdego uczestnika warsztatu obejmuje:
    a. papierową wersję materiałów szkoleniowych. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych;
    b. materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne niezbędne do realizacji szkolenia.
13) Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć.
14) Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.
15) Wykonawca zapewni: na potrzeby wyżywienia uczestników szkoleń odpowiednie pomieszczenie oraz niezbędną liczbę stołów i krzeseł. Zamawiający nie dopuszcza serwowania posiłków w tej samej sali, w której odbywają się szkolenia. Miejsce posiłku nie powinno być oddalone dalej niż 10 minut drogi pieszo od miejsca szkolenia; obiady powinny być zróżnicowane, dany zestaw obiadowy nie powinien powtarzać się częściej niż raz na 3 dni szkoleniowe; Wykonawca zapewni 2 przerwy kawowe podczas jednego dnia szkoleniowego.
    a. W zakresie wyżywienia uczestników szkoleń Wykonawca zapewni:
        i. obiad dwudaniowy dla wszystkich uczestników szkolenia - (z opcją wegetariańską) obejmujące: zupę, gorące danie główne (mięsne lub rybne) z dodatkami skrobiowymi oraz surówką/sałatkami, deser (wyroby cukiernicze lub owoce sezonowe), kawę i herbatę wraz z dodatkami, wodę mineralną gazowaną i niegazowaną.
        ii. Wykonawca zapewni następujące gramatury wymienionych powyżej posiłków:
            1. zupa – co najmniej 0,25 l na uczestnika szkolenia,
            2. danie gorące (mięsne lub rybne, opcja wegetariańska - warzywne) – co najmniej 150 g na uczestnika szkolenia,
            3. zestaw surówek/sałatek – co najmniej 150 g na uczestnika szkolenia,
            4. dodatki skrobiowe - porcja ziemniaków lub frytek / makaronu / ryżu / kaszy – co najmniej 200 g na uczestnika szkolenia,

5. kawa, herbata, woda mineralna gazowana i niegazowana - co najmniej 0,5 l na uczestnika szkolenia.

iii. Przerwa kawowa dla wszystkich uczestników szkolenia podczas jego trwania:
1. serwis będzie dostępny przy sali szkoleniowej;
2. naczynia, w których serwowany jest serwis kawowy powinny być szklane lub ceramiczne;
3. Serwis kawowy dla każdego uczestnika szkolenia obejmuje:
4. butelkowaną wodę mineralną gazowaną i niegazowaną (0,5 l);
5. świeżo parzoną, gorącą kawę z ekspresu lub zaparzacza oraz kawę sypaną i rozpuszczalną;
6. herbatę – co najmniej 3 rodzaje herbat w torebkach;
7. dodatki – cukier, mleko do kawy, cytrynę;
8. dodatki - np. ciastka / wafelki i inne słodycze oraz ciasto.

b. W zakresie wyżywienia Wykonawca zobowiązany jest do:
i. terminowego przygotowania i podania posiłków, zgodnie z ramowym programem warsztatu,
ii. zachowania zasad higieny i obowiązujących przepisów sanitarnych przy przygotowaniu posiłków i ich podawaniu,
iii. przygotowania posiłków zgodnie z zasadami racjonalnego wyżywienia, urozmaiconych z pełnowartościowych, świeżych produktów z ważnymi terminami przydatności do spożycia,
iv. przestrzegania w trakcie realizacji usług wchodzących w zakres przedmiotu umowy obowiązujących przepisów sanitarnych, w tym ustawy z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia. (Dz.U.2015.594 j.t. z późn. zm.).

c. czas na przerwy kawowe i obiadowe należy doliczyć do założonej liczby godzin zegarowych szkolenia.

16) Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.

17) Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru szkolenia – wraz z dołączonymi załącznikami, tj. oryginalną listą obecności, harmonogramem i programem warsztatu oraz ankiety oceny warsztatu przeprowadzonej wśród uczestników warsztatu.