Opis Przedmiotu Zamówienia

-

Modernizacja Sieci LAN

SPIS TREŚCI

Rozdział 1
Informacje wstępne

I
Słownik pojęć i skrótów

1. **PAŻP –** Polska Agencja Żeglugi Powietrznej;
2. **Wykonawca / Usługodawca –** Podmiot, wyłoniony w postępowaniu przetargowym, świadczący usługę na rzecz Zamawiającego;
3. **OPZ** – Opis Przedmiotu Zamówienia;
4. **Przedmiot Zamówienia / Przedmiot Umowy** – Dostawa urządzeń (w ramach Części I, Części II i Części III), Usługa Serwisowa (w ramach Części I, Części II i Części III) i Usługa Wsparcia Wykonawcy (w ramach Części I, Części II i Części III) na rzecz Zamawiającego na warunkach i w okresie opisanym w Umowie;
5. **Awaria –** nieprzewidziane, nagłe zakłócenie (uszkodzenie) w eksploatowanym urządzeniu, systemie, oprogramowaniu, które powoduje utratę funkcjonalności lub zmniejszenie zdolności użytkowej urządzenia;
6. **Czas reakcji –** podjęcie działań diagnostycznych i kontakt ze zgłaszającym, w odpowiedzi na zgłoszoną przez przedstawiciela Zamawiającego usterkę/awarię urządzenia;
7. **Inżynier Wykonawcy –** Wykwalifikowany personel Wykonawcy lub pracujący na jego zlecenie, posiadający umiejętności, kwalifikacje i kompetencje (np. aktualne certyfikaty (wystawione przez producenta urządzeń) CCNP, PCNSA, CCIE, PCNSE) niezbędne do świadczenia Usługi na rzecz Zamawiającego;
8. **Inżynier CCIE –** pracownik posiadający aktualny certyfikat „Cisco Certified Internetworking Expert";
9. **Inżynier CCNP –** pracownik posiadający aktualny certyfikat „Cisco Certified Network Professional";
10. **Inżynier PCNSE –** pracownik posiadający aktualny certyfikat „PaloAlto Networks Certified Network Security"
11. **Dni robocze –** wszystkie dni od poniedziałku do piątku, oprócz dni ustawowo wolnych od pracy;
12. **Cisco TAC –** Cisco Technical Assistance Center;
13. **Cisco CCO –** Cisco Connection Online;
14. **PaloAlto ASC –** PaloAlto Authorized Support;
15. **Data –** oznaczenie punktu czasu zdefiniowane za pośrednictwem: godziny (godzina, minuty – gg:mm) i dnia tygodnia (dzień, miesiąc, rok – dd.mm.rrrr);
16. **Infrastruktura Teleinformatyczna** – elementy aktywne i pasywne tworzące sieć telekomunikacyjną/teletechniczną oraz całokształt rozwiązań sprzętowo-programowych stanowiących podstawę funkcjonowania systemów informatycznych Zamawiającego;
17. **Usługa –** świadczona przez Wykonawcę **Usługa Wsparcia** oraz usługa wynikająca z wykupionego przez Wykonawcę (na rzecz Zamawiającego): **Kontraktu Serwisowego**, dla urządzeń dostarczonych Zamawiającemu (w ramach Części I, Części II i Części III),

18. **Kontrakt Serwisowy –** usługa zapewniona przez producenta urządzeń - odpowiednio Usługa np. dla urządzeń CISCO - SMARTnet Total Care Next Business Day (NBD) lub dla urządzeń PaloAlto - Premium Support, itp.
19. **Usługa Wsparcia –** Usługa wsparcia technicznego i serwisowego, dla urządzeń sieciowych oferowana bezpośrednio przez Wykonawcę w związku z realizacją Umowy;
20. **NBD –** Next Business Day, kolejny dzień roboczy liczony od daty zgłoszenia;
21. **Tryb (24/7/365) –** tryb pracy 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku;
22. **Próba Usunięcia Awarii Urządzenia –** pierwsza próba usunięcia awarii, liczona od daty, kiedy zdiagnozowano prawdopodobną przyczynę awarii urządzenia;
23. **Wsparcie techniczne i serwisowe dla urządzeń [WTiSU] –** wsparcie w eksploatacji urządzeń wskazanych w OPZ, – diagnostyka, nieodpłatna naprawa, wymiana, wymiana niezbędnego do ich funkcjonowania oprogramowania (w tym np. aktualizacja, itp.) – z uwzględnieniem warunków zdefiniowanych w Kontrakcie Serwisowym producenta oraz wynikające z Usługi Wsparcia;

Nie wymienione w pkt. I definicje i pojęcia, a wykorzystane w niniejszym dokumencie, należy rozumieć i stosować zgodnie ogólnie przyjętą nomenklaturą i standardami obowiązującymi na świecie (w tym tymi obowiązującymi w branży telekomunikacyjnej i sieciach komputerowych). W przypadku wątpliwości, należy je zgłosić do Zamawiającego, który określi ich interpretację

Ilekroć w dokumencie posłużono się pojęciami: „należy", „powinny" lub podobnymi uznaje się, iż pojęcia te są tożsame i używane zamiennie, a zwroty, w których zostały użyte, uznaje się za stanowiące zobowiązanie Wykonawcy.

II
Ogólny Opis Zamówienia

Przedmiotem zamówienia jest zakup, dostawa oraz usługa wsparcia technicznego, dla:

A. Przełączników Sieciowych, wraz z kontraktami serwisowymi, oraz wsparciem technym Wykonawcy, zwanych dalej „Przełączniki Sieciowe LAN 1" – **Część I**

B. Przełączników Sieciowych, wraz z kontraktami serwisowymi, oraz wsparciem technym Wykonawcy zwanych dalej „Przełączniki Sieciowe LAN 2" – **Część II**

C. Urządzeń bezpieczeństwa sieci, wraz z kontraktami serwisowymi, oraz wsparciem technym wykonawcy, zwanych dalej „Urządzenia odpowiedzialne za bezpieczeństwo sieci LAN" – **Część III**

1. Cały zakres zamówienia podzielony zostaje na 3 Części – Tabela 1

Tabela 1

Nr	Zakres Zamówienia	
I	Przełączniki Sieciowe LAN 1	
	Urządzenia:	Kontrakty Serwisowe + Usługa Wsparcia Technicznego Wykonawcy
	1. Przełącznik sieciowy modularny, typ 1A	
	2. Przełącznik sieciowy modularny, typ 1B	
	3. Przełącznik sieciowy modularny, typ 2A	
	4. Przełącznik sieciowy modularny, typ 3	
	5. Przełącznik sieciowy QSFP, typ 1	
	6. Przełącznik sieciowy QSFP/SFP28/SFP+, typ 1	
	7. Przełącznik sieciowy rozszerzony	
	8. Przełącznik sieciowy z chłodzeniem pasywnym	
II	Przełączniki Sieciowe LAN 2	
	Urządzenia:	Kontrakty Serwisowe + Usługa Wsparcia Technicznego Wykonawcy
	1. Przełącznik sieciowy modularny, typ 1C	
	2. Przełącznik sieciowy modularny, typ 2B	
	3. Przełącznik sieciowy serwerowy, typ 1	
III	Urządzenia odpowiedzialne za bezpieczeństwo sieci LAN	
	Urządzenia:	Kontrakty Serwisowe + Usługa wsparcia Technicznego Wykonawcy
	1. Urządzenie odpowiedzialne za bezpieczeństwo sieci core LAN	
	2. Urządzenie odpowiedzialne za bezpieczeństwo sieci core LAN na styku z siecią Internet	

2. W Tabeli 2 wskazano zestawienie ilościowe elementów zamówienia wchodzących w skład Części I, Części II i Części III

Tabela 2

Nr Części	Zakres Zamówienia	Ilość
I	Przełączniki Sieciowe LAN 1	
	1. Przełącznik sieciowy modularny, typ 1A	4 szt.
	2. Przełącznik sieciowy modularny, typ 1B	1 szt.
	3. Przełącznik sieciowy modularny, typ 2A	1 szt.
	4. Przełącznik sieciowy modularny, typ 3	1 szt.
	5. Przełącznik sieciowy QSFP, typ 1	2 szt.
	6. Przełącznik sieciowy QSFP/SFP28/SFP+, typ 1	4 szt.
	7. Przełącznik sieciowy rozszerzony	8 szt.
	8. Przełącznik sieciowy z chłodzeniem pasywnym	10 szt.
II	Przełączniki Sieciowe LAN 2	
	1. Przełącznik sieciowy modularny, typ 1C	1 szt.
	2. Przełącznik sieciowy modularny, typ 2B	1 szt.
	3. Przełącznik sieciowy serwerowy, typ 1	4 szt.
III	Urządzenia odpowiedzialne za bezpieczeństwo sieci LAN	
	1. Urządzenie odpowiedzialne za bezpieczeństwo sieci core LAN	1 kpl.
	2. Urządzenie odpowiedzialne za bezpieczeństwo sieci core LAN na styku z siecią Internet	1 kpl.

III
Miejsce dostawy

1. Miejsce dostawy urządzeń wskazanych w Części I, Części II i Części III wyszczególniono w Tabeli 3

Tabela 3

Nr Części	Zakres Zamówienia
I	Przełączniki Sieciowe LAN 1
II	Przełączniki Sieciowe LAN 2
	Polska Agencja Żeglugi Powietrznej 02-147 Warszawa ul. Wieżowa 8 Osoby do kontaktu: 1.
III	Urządzenia odpowiedzialne za bezpieczeństwo sieci LAN
	Polska Agencja Żeglugi Powietrznej 62-081 Wysogotowo ul. Radarowa 1 Osoby do kontaktu: 1.

Rozdział 2
Szczegółowy Opis Przedmiotu Zamówienia – Część I

I
Przełącznik sieciowy modularny typ 1A

1. **Wymagania Ogólne**

1.1. Przełącznik modularny posiadający 10 slotów na karty w tym 2 na karty zarządzająco-przełączające oraz 8 kart liniowych.

1.2. Przełącznik musi posiadać możliwość montażu w szafie rack 19 cali

1.3. Obudowa urządzenia musi zapewniać przepustowość minimum 480Gbps na slot urządzenia.

1.4. Przełącznik musi być wyposażony w dwa redundantne moduły supervisora, każdy supervisor wyposażony w co najmniej 4 porty 40/100GE oraz co najmniej 4 porty 10/25GE.

1.5. Wraz z przełącznikiem muszą zostać dostarczone 4 (cztery) moduły 10/25GBASE, do realizacji połączeń 25G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) z możliwością pracy z prędkością 10G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) oraz dostarczone 4 (cztery) moduły 10/25G do realizacji połączeń do 10 kilometrów z wykorzystaniem światłowodów jedno-modowych.

1.6. Przełącznik musi posiadać możliwość zainstalowania do 8 kart rozszerzeń – kart liniowych.

1.7. Zamawiający wymaga dostarczenia przełącznika z 8 kartami liniowymi, każda 48 portów multigig 100M/1G/2.5G/5G/10GBASE-T RJ-45 UPOE+

1.8. Każdy moduł przełączająco-zarządzający (supervisor) musi być wyposażony w dysk SSD o pojemność co najmniej 240GB

1.9. Karta zarządzająca musi posiadać wydajność minimum 240Gbps na każdy slot

1.10. Karta zarządzająca musi posiadać wydajność przełączania/routingu co najmniej 3000Mpps dla pakietów IPv4 oraz IPv6

1.11. Przełącznik musi być wyposażony w co najmniej 8 zasilaczy AC 230V, każdy o mocy co najmniej 3200W

1.12. Przełącznik musi być wyposażony w demontowalny moduł wentylatorów, z możliwością wyciągania z tyłu urządzenia

1.13. Przełącznik musi posiadać agregowaną przepustowość co najmniej 9Tbps (4 Tbps w trybie fullduplex)

2. **Oczekiwana funkcjonalność urządzenia**

2.1. Przełącznik musi:

2.1.1. Obsługiwać do 64 000 adresów MAC

2.1.2. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv4 unicast

2.1.3. Obsługiwać co najmniej 16 000 wpisów w tablicy IPv4 multicast

2.1.4. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv6 unicast

2.1.5. Posiadać co najmniej 16 GB pamięci DRAM

2.1.6. Posiadać co najmniej 10 GB pamięci flash

2.1.7. Obsługiwać co najmniej 16 000 wpisów QoS ACE

2.1.8. obsługiwać co najmniej 16 000 wpisów security ACE

2.1.9. Posiadać bufor pakietów o wielkości co najmniej 108MB

2.1.10. Obsługiwać co najmniej 1000 unikalnych vlanów

2.1.11. Obsługiwać co najmniej 1000 interfejsów SVI

2.1.12. Obsługiwać ramki Jumbo o wielkości 9216 Bajtów

2.1.13. Posiadać wparcie dla protokołów BGP, MPLS, CDP, EIGRP, PIM, VXLAN

2.1.14. Posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping

2.1.15. Posiadać obsługę protokołu NTP

2.1.16. Posiadać wsparcie dla NETFLOW, EEM (lub równoważne), ERSPAN

2.1.17. Posiadać wsparcie dla ETA (Encrypted Traffic Analysys) (lub równoważne)

2.1.18. posiadać wsparcie dla SDACCESS lub równoważne

2.1.19. Posiadać wsparcie dla NSF, NSR, GIR, ISSU

2.1.20. Posiadać obsługę protokołu LLDP i LLDP-MED,

2.1.21. Posiadać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC,

2.1.22. Posiadać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,

2.1.23. Posiadać możliwość uruchomienia funkcji serwera DHCP

2.1.24. Posiadać możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow (lub równoważnego)– wymagana obsługa co najmniej 144 000 strumieni (flow),

2.1.25. Posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

2.1.26. Posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,

2.1.27. Posiadać wsparcie dla protokołu LISP zgodnie z RFC 6830 lub równoważnego

2.1.28. Realizować następującą funkcjonalność w zakresie MPLS: L2VPN, L3VPN, mVPN, InterAS option A i B, EoMPLS wraz z obsługą MACSec, MPLS over GRE

2.1.29. Posiadać obsługę protokołu BFD dla co najmniej 100 sesji

2.1.30. Posiadać obsługę protokołu MACSec w tym również na portach zagregowanych

2.1.31. Posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,

2.1.32. Posiadać możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu

2.1.33. Posiadać obsługę funkcjonalności bramy dla usług mDNS

2.1.34. Posiadać wbudowany analizator pakietów

2.1.35. Posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy

2.1.36. Posiadać obsługę co najmniej 256 wirtualnych instancji routingu (VRF),

2.2. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

II
Przełącznik sieciowy modularny typ 1B

1. **Wymagane ogólne:**

1.1. Przełącznik modularny posiadający 10 slotów na karty w tym 2 na karty zarządzająco-przełączające oraz 8 kart liniowych.

1.2. Przełącznik musi posiadać możliwość montażu w szafie rack 19 cali

1.3. Obudowa urządzenia musi zapewniać przepustowość minimum 480Gbps na slot urządzenia.

1.4. Przełącznik musi być wyposażony w dwa redundantne moduły supervisora, każdy supervisor wyposażony w co najmniej 4 porty 40/100GE oraz co najmniej 4 porty 10/25GE.

1.5. Wraz z przełącznikiem muszą zostać dostarczone: 4 (cztery) moduły 10/25G, do realizacji połączeń 25G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) z możliwością pracy z prędkością 10G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) oraz 4 (cztery) moduły 10/25G

do realizacji połączeń do 10 kilometrów z wykorzystaniem światłowodów jedno-modowych.

1.6. Przełącznik musi posiadać możliwość zainstalowania do 8 kart rozszerzeń – kart liniowych.

1.7. Zamawiający wymaga dostarczenia przełącznika z 8 kartami liniowymi, każda 48 portów multigig 100M/1G/2.5G/5G/10GBASE-T RJ-45 UPOE+

1.8. Każdy moduł przełączająco-zarządzający (supervisor) musi być wyposażony w dysk SSD o pojemność co najmniej 240GB

1.9. Karta zarządzająca musi posiadać wydajność minimum 240Gbps na każdy slot

1.10. Karta zarządzająca musi posiadać wydajność przełączania/routingu co najmniej 3000Mpps dla pakietów IPv4 oraz IPv6

1.11. Przełącznik musi być wyposażony w co najmniej 6 zasilaczy AC 230V, każdy o mocy co najmniej 3200W

1.12. Przełącznik musi być wyposażony w demontowalny moduł wentylatorów, z możliwością wyciągania z tyłu urządzenia

1.13. Przełącznik musi posiadać agregowaną przepustowość co najmniej 9Tbps (4 Tbps w trybie fullduplex)

2. **Oczekiwana funkcjonalność urządzenia**

2.1. Przełącznik musi:

2.1.1. Obsługiwać do 64 000 adresów MAC;

2.1.2. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv4 unicast;

2.1.3. Obsługiwać co najmniej 16 000 wpisów w tablicy IPv4 multicast;

2.1.4. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv6 unicast;

2.1.5. Posiadać co najmniej 16 GB pamięci DRAM;

2.1.6. Posiadać co najmniej 10 GB pamięci flash;

2.1.7. Obsługiwać co najmniej 16 000 wpisów QoS ACE;

2.1.8. Obsługiwać co najmniej 16 000 wpisów security ACE;

2.1.9. Posiadać bufor pakietów o wielkości co najmniej 108MB;

2.1.10. Obsługiwać co najmniej 1000 unikalnych vlanów;

2.1.11. Obsługiwać co najmniej 1000 interfejsów SVI;

2.1.12. Obsługiwać ramki Jumbo o wielkości 9216 Bajtów;

2.1.13. Posiadać wparcie dla protokołów BGP, MPLS, CDP, EIGRP, PIM, VXLAN;

2.1.14. Posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping;

2.1.15. Posiadać obsługę protokołu NTP;

2.1.16. Posiadać wsparcie dla NETFLOW, EEM (lub równoważne), ERSPAN;

2.1.17. Posiadać wsparcie dla ETA (Encrypted Traffic Analysys) (lub równoważne);

2.1.18. Posiadać wsparcie dla SDACCESS lub równoważne;

2.1.19. Posiadać wsparcie dla NSF, NSR, GIR, ISSU;

2.1.20. Posiadać obsługę protokołu LLDP i LLDP-MED;

2.1.21. Posiadać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC;

2.1.22. Posiadać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego;

2.1.23. Posiadać możliwość uruchomienia funkcji serwera DHCP;

2.1.24. Posiadać możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow (lub równoważnego)– wymagana obsługa co najmniej 144 000 strumieni (flow);

2.1.25. Posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie;

2.1.26. Posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku;

2.1.27. Posiadać wsparcie dla protokołu LISP zgodnie z RFC 6830 lub równoważnego;

2.1.28. Realizować następującą funkcjonalność w zakresie MPLS: L2VPN, L3VPN, mVPN, InterAS option A i B, EoMPLS wraz z obsługą MACSec, MPLS over GRE;

2.1.29. Posiadać obsługę protokołu BFD dla co najmniej 100 sesji;

2.1.30. Posiadać obsługę protokołu MACSec w tym również na portach zagregowanych;

2.1.31. Posiadać możliwość enkapsulacji ruchu w pakiety VXLAN;

2.1.32. Posiadać możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu;

2.1.33. Posiadać obsługę funkcjonalności bramy dla usług mDNS;

2.1.34. Posiadać wbudowany analizator pakietów;

2.1.35. Posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy;

2.1.36. Posiadać obsługę co najmniej 256 wirtualnych instancji routingu (VRF);

2.2. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

III
Przełącznik sieciowy modularny typ 1B

1. **Wymagane ogólne:**

1.1. Przełącznik modularny posiadający 7 slotów na karty w tym 2 na karty zarządzająco-przełączające oraz 5 kart liniowych;

1.2. Przełącznik musi posiadać możliwość montażu w szafie rack 19 cali;

1.3. Obudowa urządzenia musi zapewniać przepustowość minimum 480Gbps na slot urządzenia;

1.4. Przełącznik musi być wyposażony w dwa redundantne moduły supervisora, każdy supervisor wyposażony w co najmniej 4 porty 40/100GE oraz co najmniej 4 porty 10/25GE;

1.5. Wraz z przełącznikiem musi zostać dostarczone 8 (osiem) modułów 10/25GBASE, do realizacji połączeń 25G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) z możliwością pracy z prędkością 10G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4);

1.6. Przełącznik musi posiadać możliwość zainstalowania do 5 kart rozszerzeń – kart liniowych;

1.7. Zamawiający wymaga dostarczenia przełącznika z 5 kartami liniowymi, każda 48 portów multigig 100M/1G/2.5G/5G/10GBASE-T RJ-45 UPOE+;

1.8. Każdy moduł przełączająco-zarządzający (supervisor) musi być wyposażony w dysk SSD o pojemność co najmniej 240GB;

1.9. Karta zarządzająca musi posiadać wydajność minimum 240Gbps na każdy slot;

1.10. Karta zarządzająca musi posiadać wydajność przełączania/routingu co najmniej 3000Mpps dla pakietów IPv4 oraz IPv6;

1.11. Przełącznik musi być wyposażony w co najmniej 6 zasilaczy AC 230V, każdy o mocy co najmniej 3200W;

1.12. Przełącznik musi być wyposażony w demontowalny moduł wentylatorów, z możliwością wyciągania z tyłu urządzenia;

1.13. Przełącznik musi posiadać agregowaną przepustowość co najmniej 9Tbps (4 Tbps w trybie fullduplex);

2. **Oczekiwana funkcjonalność urządzenia**

2.1. Przełącznik musi:

2.1.1. Obsługiwać do 64 000 adresów MAC;

2.1.2. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv4 unicast;

2.1.3. Obsługiwać co najmniej 16 000 wpisów w tablicy IPv4 multicast;

2.1.4. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv6 unicast;

2.1.5. Posiadać co najmniej 16 GB pamięci DRAM;

2.1.6. Posiadać co najmniej 10 GB pamięci flash;

2.1.7. Obsługiwać co najmniej 16 000 wpisów QoS ACE;

2.1.8. Obsługiwać co najmniej 16 000 wpisów security ACE;

2.1.9. Posiadać bufor pakietów o wielkości co najmniej 108 MB;

2.1.10. Obsługiwać co najmniej 1000 unikalnych vlanów;

2.1.11. Obsługiwać co najmniej 1000 interfejsów SVI;

2.1.12. Obsługiwać ramki Jumbo o wielkości 9216 Bajtów;

2.1.13. Posiadać wparcie dla protokołów BGP, MPLS, CDP, EIGRP, PIM, VXLAN;

2.1.14. Posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping;

2.1.15. Posiadać obsługę protokołu NTP;

2.1.16. Posiadać wsparcie dla NETFLOW, EEM (lub równoważne), ERSPAN;

2.1.17. Posiadać wsparcie dla ETA (Encrypted Traffic Analysys) (lub równoważne);

2.1.18. Posiadać wsparcie dla SDACCESS lub równoważne;

2.1.19. Posiadać wsparcie dla NSF, NSR, GIR, ISSU;

2.1.20. Posiadać obsługę protokołu LLDP i LLDP-MED.;

2.1.21. Posiadać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC;

2.1.22. Posiadać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego;

2.1.23. Posiadać możliwość uruchomienia funkcji serwera DHCP;

2.1.24. Posiadać możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow (lub równoważnego)– wymagana obsługa co najmniej 144 000 strumieni (flow);

2.1.25. Posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie;

2.1.26. Posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku;

2.1.27. Posiadać wsparcie dla protokołu LISP zgodnie z RFC 6830 lub równoważnego;

2.1.28. Realizować następującą funkcjonalność w zakresie MPLS: L2VPN, L3VPN, mVPN, InterAS option A i B, EoMPLS wraz z obsługą MACSec, MPLS over GRE;

2.1.29. posiadać obsługę protokołu BFD dla co najmniej 100 sesji;

2.1.30. Posiadać obsługę protokołu MACSec w tym również na portach zagregowanych;

2.1.31. Posiadać możliwość enkapsulacji ruchu w pakiety VXLAN;

2.1.32. Posiadać możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu;

2.1.33. Posiadać obsługę funkcjonalności bramy dla usług mDNS;

2.1.34. Posiadać wbudowany analizator pakietów;

2.1.35. Posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy;

2.1.36. Posiadać obsługę co najmniej 256 wirtualnych instancji routingu (VRF);

2.2. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

IV
Przełącznik sieciowy modularny typ 3

1. **Wymagane ogólne:**

1.1. Przełącznik modularny posiadający 4 sloty na karty, w tym 2 na karty zarządzająco-przełączające, oraz 2 dla kart liniowych;

1.2. Przełącznik musi posiadać możliwość montażu w szafie rack 19 cali;

1.3. Obudowa urządzenia musi zapewniać przepustowość minimum 480Gbps na slot urządzenia;

1.4. Przełącznik musi być wyposażony w moduł supervisora, posiadający co najmniej 4 porty 40/100GE oraz co najmniej 4 porty 10/25GE;

1.5. Wraz z przełącznikiem muszą zostać dostarczone 4 (cztery) moduły QSFP, posiadające możliwość pracy zarówno w trybie 40Gbps jak i 100Gbps na pojedynczej parze okablowania multi-mode(OM4) do 100metrów. Moduły muszą posiadać konektory LC;

1.6. Wraz z przełącznikiem muszą zostać dostarczone 32(trzydzieści dwa) moduły SFP 1G do pracy z wykorzystaniem pojedynczej pary światłowodów wielo-modowych oraz

10(dziesięć) modułów optycznych SFP 1G do pracy z wykorzystaniem pojedynczej pary światłowodów jedno-modowych (SM) o zasięgu pracy 10 Km SMF (G.652);

1.7. Przełącznik musi posiadać możliwość zainstalowania do 2 kart rozszerzeń – kart liniowych;

1.8. Zamawiający wymaga dostarczenia przełącznika z 2 kartami liniowymi:

1.8.1. 1x 48 portów multigig 100M/1G/2.5G/5G/10GBASE-T RJ-45 UPOE+

1.8.2. 1x 48 portów SFP/SFP+ 1/10G

1.9. Każdy moduł przełączająco-zarządzający (supervisor) musi być wyposażony w dysk SSD o pojemność co najmniej 240GB;

1.10. Karta zarządzająca musi posiadać wydajność minimum 240Gbps na każdy slot;

1.11. Karta zarządzająca musi posiadać wydajność przełączania/routingu co najmniej 3000Mpps dla pakietów IPv4 oraz IPv6;

1.12. Przełącznik musi być wyposażony w co najmniej 4 zasilacze AC 230V, każdy o mocy co najmniej 3200 W;

1.13. Przełącznik musi być wyposażony w demontowalny moduł wentylatorów, z możliwością wyciągania z tyłu urządzenia;

1.14. Przełącznik musi posiadać agregowaną przepustowość co najmniej 9Tbps (4 Tbps w trybie fullduplex).

2. **Oczekiwana funkcjonalność urządzenia**

2.1. Przełącznik musi:

2.1.1. Obsługiwać do 64 000 adresów MAC

2.1.2. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv4 unicast

2.1.3. Obsługiwać co najmniej 16 000 wpisów w tablicy IPv4 multicast

2.1.4. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv6 unicast

2.1.5. Posiadać co najmniej 16 GB pamięci DRAM

2.1.6. Posiadać co najmniej 10 GB pamięci flash

2.1.7. Obsługiwać co najmniej 16 000 wpisów QoS ACE

2.1.8. Obsługiwać co najmniej 16 000 wpisów security ACE

2.1.9. Posiadać bufor pakietów o wielkości co najmniej 108MB

2.1.10. Obsługiwać co najmniej 1000 unikalnych vlanów

2.1.11. Obsługiwać co najmniej 1000 interfejsów SVI

2.1.12. Obsługiwać ramki Jumbo o wielkości 9216 Bajtów

2.1.13. Posiadać wparcie dla protokołów BGP, MPLS, CDP, EIGRP, PIM, VXLAN

2.1.14. Posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping

2.1.15. Posiadać obsługę protokołu NTP

2.1.16. Posiadać wsparcie dla NETFLOW, EEM (lub równoważne), ERSPAN

2.1.17. musi Posiadać wsparcie dla ETA (Encrypted Traffic Analysys) (lub równoważne)

2.1.18. Posiadać wsparcie dla SDACCESS lub równoważne

2.1.19. Posiadać wsparcie dla NSF, NSR, GIR, ISSU

2.1.20. Posiadać obsługę protokołu LLDP i LLDP-MED,

2.1.21. Posiadać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC,

2.1.22. Posiadać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,

2.1.23. Posiadać możliwość uruchomienia funkcji serwera DHCP

2.1.24. Posiadać możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow (lub równoważnego)– wymagana obsługa co najmniej 144 000 strumieni (flow),

2.1.25. Posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

2.1.26. Posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,

2.1.27. Posiadać wsparcie dla protokołu LISP zgodnie z RFC 6830 lub równoważnego

2.1.28. Realizować następującą funkcjonalność w zakresie MPLS: L2VPN, L3VPN, mVPN, InterAS option A i B, EoMPLS wraz z obsługą MACSec, MPLS over GRE

2.1.29. Przełącznik musi Posiadać obsługę protokołu BFD dla co najmniej 100 sesji

2.1.30. Posiadać obsługę protokołu MACSec w tym również na portach zagregowanych

2.1.31. Posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,

2.1.32. Posiadać możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu

2.1.33. Posiadać obsługę funkcjonalności bramy dla usług mDNS

2.1.34. Posiadać wbudowany analizator pakietów

2.1.35. Posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy

2.1.36. Posiadać obsługę co najmniej 256 wirtualnych instancji routingu (VRF),

2.2. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

V
Przełącznik sieciowy QSFP typ 1

1. **Wymagane ogólne:**

1.1. Przełącznik typu „standalone" wyposażony w 32 porty 40/100GE definiowane za pomocą modułów optycznych QSFP28, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps jak i 100Gbps na pojedynczej parze okablowania multi-mode lub single mode

2. **Architektura urządzenia:**

2.1. Urządzenie jest wyposażone w:

2.1.1. Wymienne moduły wentylatorów

2.1.2. Wymienne zasilacze

2.1.3. Zasilacz redundantny do pracy w trybie 1:1

3. **Wydajność urządzenia:**

3.1. Urządzenie posiadana:

3.1.1. Minimum 32MB bufor pamięci per ASIC

3.1.2. Minimum 16GB pamięci DRAM i 16GB pamięci flash

3.2. Wydajność przesyłania minimum: 2 Miliardy pps

3.3. Wydajność przełączania minimum: 6,2 Tbps,

4. **Obsługa przez urządenie:**

4.1. Urządzenie obsługujące minimum:

4.1.1. 1000 sieci VLAN

4.1.2. 80 000 adresów MAC

4.1.3. 212 000 tras IPv4

4.1.4. 212 000 tras IPv6

4.1.5. liczba wpisów w listach kontroli dostępu Security ACL – 27 000

4.1.6. liczba wpisów w listach kontroli dostępu QoS ACL – 16 000

5. **Oprogramowanie i funkcjonalność urządzenia:**

5.1. Obsługa protokołu NTP

5.2. Obsługa IGMPv1/2/3

5.3. Obsługa standardu 802.1AE (szyfrowanie ruchu) 256-bit z prędkością linerate dla każdego z interfejsów

5.4. System operacyjny przełącznika umożliwia wgrywanie poprawek bez konieczności restartowania platformy

5.5. System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.

5.6. Możliwość uruchamiania zdefiniowanych w języku Python, skryptów w chwili zaistnienia określonego zdarzenia.

6. **Mechanizmy zaimplementowane w urządzeniu – ciągłość pracy sieci:**

6.1. IEEE 802.1w Rapid Spanning Tree

6.2. Per-VLAN Rapid Spanning Tree (PVRST+)

6.3. IEEE 802.1s Multi-Instance Spanning Tree

6.4. Obsługa minimum 128 instancji protokołu STP

6.5. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED

6.6. Funkcja serwera DHCP

6.7. Obsługa minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)

6.8. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+

7. **Mechanizmy zaimplementowane w urządzeniu – jakość usług sieci:**

7.1. Minimum 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi

7.2. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek

7.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)

7.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP

7.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 1000 ograniczeń per przełącznik

7.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast

7.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

8. **Realizacja routingu statycznego i dynamicznego dla IPv4 i IPv6 w zakresie:**
   - 8.1. dla IPv4: OSPF, BGP, ISIS
   - 8.2. dla IPv6: OPSFv3,
9. **Wymagania dodatkowe wobec funckjonalności urządzenia:**
   - 9.1. Funkcjonalności Policy-based routing, multicast routing (PIM-SM, PIM-SSM)
   - 9.2. Realizacja protokołu LISP lub równoważny zgodnie z RFC 6830
   - 9.3. Enkapsulacja ruchu przy pomocy VXLAN'ów
   - 9.4. Obsługa mechanizmów zapewniających 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.
   - 9.5. Obsługa mechanizmów segmentacji logicznej opartej o znaczniki bezpieczeństwa (security group tags) z możliwością egzekwowania polityk bezpieczeństwa zbudowanych na bazie takich znaczników oraz propagacji znaczników do innych przełączników w systemie.
   - 9.6. Urządzenie jest 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.
   - 9.7. Urządzenie realizuje następujące funkcjonalności z zakresu MPLS:
     - 9.7.1. L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC
     - 9.7.2. L2VPN - Virtual Private LAN Services (VPLS) - obsługa minimum 128 wirtualnych instancji (VFI) i 32 sąsiadów w ramach jednej instancji
     - 9.7.3. L3 VPN - MPLS Virtual Private Network (VPN)
     - 9.7.4. Multicast VPN (MVPN)
10. **Zarządzanie i konfiguracja urządzenia:**
    - 10.1. Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o NetFlow, wielkość tablicy monitorowanych strumieni wynosi co najmniej 98000
    - 10.2. Urządzenie realizuje rozszerzenie 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 pół kluczowych
    - 10.3. Urządzenie posiada dedykowany port Ethernet do zarządzania out-of-band
    - 10.4. Urządzenie posiada port USB umożliwiający podłączenie zewnętrznego nośnika danych.

10.4.1. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB

10.5. Urządzenie jest wyposażone w port konsoli USB

10.6. Urządzenie umożliwia tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie

10.7. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6

10.8. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia

10.9. Przełącznik posiada diodę LED umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych

10.10. Urządzenie wyposażone jest w system operacyjny urządzenia umożliwiający uruchamianie własnych aplikacji (application hosting) z wykorzystaniem mechanizmu kontenerów LXC

11. **Obudowa urządzenia i jego właściwości fizyczne:**

11.1. Możliwość montażu w szafie rack 19".

11.2. Wysokość urządzenia 1 RU

12. **Licencjonowanie funkcjonalności urzadzenia:**

12.1. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

13. **Wymagane wyposażenie urządzenia**

13.1. Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy

13.2. Wraz z przełącznikiem muszą zostać dostarczone:

13.2.1. 20 (dwadzieścia) modułów QSFP, posiadających możliwość pracy zarówno w trybie 40Gbps jak i 100Gbps na pojedynczej parze okablowania multi-mode (OM4) do 100 metrów

13.2.2. 8 (osiem) modułów QSFP 40G do pracy na pojedynczej parze okablowania multi-mode (OM4) do 100 metrów.

13.2.3. 4(cztery) moduły optyczne QSFP28 100Gb umożliwiających połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów jedno-modowych (SM) o zasięgu pracy 10Km SMF (G.652) zakończony konektorem LC

13.2.3.1. Moduły muszą posiadać konektory LC.

13.3. Moduły SPF/SFP+/SFP28/QSFP+/ QSFP28 oferowane wraz z urządzeniem muszą pochodzić od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem.

VI
Przełącznik sieciowy QSFP/SFP28/SFP+ typ 1

1. **Wymagane ogólne:**
   - 1.1. Przełącznik typu „standalone" wyposażony w 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz 4 porty 40/100G QSFP+/QSFP28
   - 1.2. Porty SFP/SFP+ umożliwiają zastosowanie następujących modułów interfejsowych:
     - 1.2.1. Dla transmisji 1Gb/s (SFP): 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX
     - 1.2.2. Dla transmisji 10Gb/s (SFP+): 10GBase-SR, 10GBase-LR, 10GBase-ZR, 10GBase-ER
     - 1.2.3. Do łączenia urządzeń na krótkie odległości typu: SFP+ twinax copper, SFP+ active optical
     - 1.2.4. Dla transmisji 25Gb/s (SFP28): 10/25G do realizacji połączeń 25G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) z możliwością pracy z prędkością 10G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4)
     - 1.2.5. Do łączenia urządzeń na krótkie odległości typu: SFP28 do SFP28 25G copper direct-attach cables, SFP28 do SFP28 25G active optical cables
2. **Architektura urządzenia:**
   - 2.1. Urządzenie jest wyposażone w:
     - 2.1.1. Wymienne moduły wentylatorów
     - 2.1.2. Wymienne zasilacze
     - 2.1.3. Zasilacz redundantny do pracy w trybie 1:1
3. **Wydajność urządzenia:**
   - 3.1. Urządzenie posiadana:
     - 3.1.1. Minimum 32MB bufor pamięci per ASIC
     - 3.1.2. Minimum 16GB pamięci DRAM i 16GB pamięci flash
   - 3.2. Wydajność przełączania minimum: 3 Tbps,
   - 3.3. Wydajność przesyłania minimum: 1 Miliard pps
4. **Obsługa przez urządenie:**
   - 4.1. Urządzenie obsługujące minimum:
     - 4.1.1. 1000 sieci VLAN
     - 4.1.2. 80 000 adresów MAC

4.1.3. 212 000 tras IPv4

4.1.4. 212 000 tras IPv6

4.1.5. Liczba wpisów w listach kontroli dostępu Security ACL – 27 000

4.1.6. Lliczba wpisów w listach kontroli dostępu QoS ACL – 16 000

5. **Oprogramowanie i funkcjonalność urządzenia:**

5.1. Obsługa protokołu NTP

5.2. Obsługa IGMPv1/2/3

5.3. Obsługa standardu 802.1AE (szyfrowanie ruchu) 256-bit z prędkością linerate dla każdego z interfejsów

5.4. System operacyjny przełącznika umożliwia wgrywanie poprawek bez konieczności restartowania platformy

5.5. System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.

5.6. Możliwość uruchamiania zdefiniowanych w języku Python, skryptów w chwili zaistnienia określonego zdarzenia.

6. **Mechanizmy zaimplementowane w urządzeniu – ciągłość pracy sieci:**

6.1. IEEE 802.1w Rapid Spanning Tree

6.2. Per-VLAN Rapid Spanning Tree (PVRST+)

6.3. IEEE 802.1s Multi-Instance Spanning Tree

6.4. Obsługa minimum 128 instancji protokołu STP

6.5. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED

6.6. Funkcja serwera DHCP

6.7. Obsługa minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)

6.8. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+

7. **Mechanizmy zaimplementowane w urządzeniu – jakość usług sieci:**

7.1. Obsługa minimum 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi

7.2. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek

7.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)

7.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP

7.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 1000 ograniczeń per przełącznik

7.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast

7.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

8. **Realizacja routingu statycznego i dynamicznego dla IPv4 i IPv6 w zakresie:**

8.1. dla IPv4: OSPF, BGP, ISIS

8.2. dla IPv6: OPSFv3,

9. **Wymagania dodatkowe wobec funckjonalności urządzenia:**

9.1. Funkcjonalności Policy-based routing, multicast routing (PIM-SM, PIM-SSM)

9.2. Urządzenie realizuje protokołu LISP lub równoważny zgodnie z RFC 6830

9.3. Urządzenie umożliwia enkapsulację ruchu przy pomocy VXLAN'ów

9.4. Obsługa mechanizmów zapewniających 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.

9.5. Obsługa mechanizmów segmentacji logicznej opartej o znaczniki bezpieczeństwa (security group tags) z możliwością egzekwowania polityk bezpieczeństwa zbudowanych na bazie takich znaczników oraz propagacji znaczników do innych przełączników w systemie.

9.6. Urządzenie jest 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.

9.7. Urządzenie realizuje następujące funkcjonalności z zakresu MPLS:

9.7.1. L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC

9.7.2. L2VPN - Virtual Private LAN Services (VPLS) - obsługa minimum 128 wirtualnych instancji (VFI) i 32 sąsiadów w ramach jednej instancji

9.7.3. L3 VPN - MPLS Virtual Private Network (VPN)

9.7.4. Multicast VPN (MVPN)

10. **Zarządzanie i konfiguracja urządzenia:**

    10.1. Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o NetFlow, wielkość tablicy monitorowanych strumieni wynosi co najmniej 98000

    10.2. Urządzenie realizuje rozszerzenie 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 pół kluczowych

    10.3. Urządzenie posiada dedykowany port Ethernet do zarządzania out-of-band

    10.4. Urządzenie posiada port USB umożliwiający podłączenie zewnętrznego nośnika danych.

    10.5. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB

    10.6. Urządzenie jest wyposażone w port konsoli USB

    10.7. Urządzenie umożliwia tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie

    10.8. Urządzenie obsługuje protokoły SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6

    10.9. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia

    10.10. Przełącznik posiada diodę LED umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych

    10.11. Urządzenie wyposażone jest w system operacyjny urządzenia umożliwiający uruchamianie własnych aplikacji (application hosting) z wykorzystaniem mechanizmu kontenerów LXC

11. **Obudowa urządzenia i jego właściwości fizyczne:**

    11.1. Możliwość montażu w szafie rack 19".

    11.2. Wysokość urządzenia 1 RU

12. **Licencjonowanie funkcjonalności urzadzenia:**

    12.1. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

13. **Wymagane wyposażenie urządzenia**

    13.1. Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy

    13.2. Wraz z przełącznikiem muszą zostać dostarczone:

        13.2.1. 4 (cztery) moduły QSFP, posiadające możliwość pracy zarówno w trybie 40Gbps jak i 100Gbps na pojedynczej parze okablowania multi-mode (OM4) do 100 metrów

13.2.2. 38 (trzydzieści osiem) modułów 10/25GBASE, do realizacji połączeń 25G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) z możliwością pracy z prędkością 10G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4)

13.2.3. 10 (dziesięć) modułów 10/25G do realizacji połączeń do 10 kilometrów z wykorzystaniem światłowodów jedno-modowych

13.2.3.1. Moduły muszą posiadać konektory LC.

13.3. Moduły SPF/SFP+/SFP28/QSFP+/ QSFP28 oferowane wraz z urządzeniem muszą pochodzić od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem.

VII
Przełącznik sieciowy rozszerzony

1. **Wymagane ogólne:**

1.1. Typ i liczba portów:

1.1.1. 48 portów 5G/2.5G/1G/100M RJ-45 UPOE

1.2. Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami) – minimum 645W / 2545W

1.3. Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco" – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):

1.3.1. 4x1G SFP

1.3.2. 8x1/10G SFP+

1.3.3. 2x40G QSFP

1.3.4. 2x25G SFP+

1.3.5. 4x100M/1G/2.5G/5G/10GBaseT RJ-45

1.4. Porty SFP/SFP+/QSFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb, tj.:

1.4.1. Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U

1.4.2. Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR,

1.4.3. Porty QSFP - wkładki 40Gigabit Ethernet w tym 40G-SR4, 40G-LR4, 40G-ER4, 40G-SR-BD, adapter 40G QSFP->10G SFP+

1.5. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:

1.5.1. Przepustowość w ramach stosu – minimum 480Gb/s

1.5.2. Minimum 8 urządzeń w stosie

1.5.3. Zarządzanie poprzez jeden adres IP

1.5.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad

1.5.5. Możliwość współdzielenia mocy zasilaczy tzn. zasilacze stanowią zasób wspólny dla wszystkich przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie)

2. **Zasilanie i chłodzenie**

2.1. Redundantne i wymienne moduły wentylatorów

2.2. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap)

2.3. Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia

3. **Parametry wydajnościowe urządzenia**

3.1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)

3.2. Pamięć DRAM – minimum 8GB

3.3. Pamięć flash – minimum 16GB

3.4. Obsługa minimum:

3.4.1. 4.000 sieci VLAN

3.4.2. 32.000 adresów MAC

3.4.3. 24.000 tras IPv4

3.4.4. 16.000 tras IPv6

4. **Mechanizmy zaimplementowane w urządzeniu – ciągłość pracy sieci:**

4.1. IEEE 802.1w Rapid Spanning Tree

4.2. Per-VLAN Rapid Spanning Tree (PVRST+)

4.3. IEEE 802.1s Multi-Instance Spanning Tree

4.4. Obsługa minimum 128 instancji protokołu STP

5. **Mechanizmy zaimplementowane w urządzeniu – bezpieczeństwo sieci:**

5.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)

5.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN

5.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL

5.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X

5.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

5.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X

5.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem

5.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176

5.9. Minimum 5000 wpisów dla list kontroli dostępu (Security ACE)

5.10. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)

5.11. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard

5.12. 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)

5.13. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+

5.14. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)

5.15. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch)

5.16. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)

5.17. Funkcja Private VLAN

6. **Mechanizmy zaimplementowane w urządzeniu – jakość usług w sieci:**

6.1. Implementacja minimum 8 kolejek dla ruchu wyjściowego, na każdym porcie dla obsługi ruchu o różnej klasie obsługi

6.2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek

6.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)

6.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP

6.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting)

6.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast

6.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

7. **Obsługa protokołów routingu:**

7.1. Routing statyczny dla IPv4 i IPv6

7.2. Routing dynamiczny – RIP, OSPF

7.3. Policy-based routing (PBR)

7.4. Obsługa protokołu redundancji bramy (VRRP)

8. **Obsługa zaawansowanych protokołów routingu**

8.1. IS-IS dla IPv4

8.2. BGP dla IPv4 i IPv6

8.3. Routing multicastów - PIM-SM, PIM-SSM

8.4. Multicast Source Discovery Protocol (MSDP)

8.5. VRF-Lite

9. **Obsługa dodatkowych protokołów**

9.1. Obsługa protokołu NTP

9.2. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

9.3. LLDP i LLDP-MED.

9.4. Wsparcie dla protokołu LISP zgodnie z RFC 6830

10. **Zarządzanie urzadzeniem**

10.1. Port konsoli

10.2. Dedykowany port Ethernet do zarządzania out-of-band

10.3. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją

10.4. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6

10.5. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów

10.6. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych

10.7. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą

10.8. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB

11. **Wyposażenie urządzenia**

11.1. Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy

11.2. Moduł uplink: 8x1/10G SFP+

11.3. 4(cztery) moduły SFP+ 10G do obsługi połączeń z wykorzystaniem światłowodu wielomodowego(MMF OM4)

11.4. Kabel i moduły stack o długości 1 m

12. **Obudowa urządzenia i jego właściwości fizyczne:**

12.1. Możliwość montażu w szafie rack 19".

12.2. Wysokość urządzenia 1 RU

13. **Wymagania dodatkowe wobec urzadzenia**

13.1. Obsługa MPLS – w tym L3 VPN i Multicast VPN (mVPN)

13.2. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE kluczami o długości 256-bitów (gcm-aes-256)

13.3. System operacyjny przełącznika umożliwia wgrywanie poprawek bez konieczności restartowania platformy

13.4. Możliwość enkapsulacji ruchu w pakiety VXLAN

13.5. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 64.000 strumieni

13.6. Wbudowany analizator pakietów

13.7. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie

13.8. Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku

13.9. Funkcjonalność bramy dla usług mDNS

13.10. Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN)

13.11. Przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7)

13.12. Możliwość eksportu dodatkowych pół w ramach statystyk NetFlow – w tym IDP (Initial Data Pacekt) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)

13.13. 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

13.14. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)

13.15. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

13.16. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

13.17. Możliwość uruchomienia funkcji serwera DHCP

14. **Licencjonowanie funkcjonalności urzadzenia:**

14.1. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

VIII
Przełącznik sieciowy z chłodzeniem pasywnym

1. **Wymagane ogólne:**

1.1. Przełącznik musi być wyposażony w 12 portów 10/100/1000 BaseT RJ45 PoE+ (zgodne z IEEE 802.3at) + 2 porty uplinkowe 1000BaseT RJ45 + 2 porty uplinkowe 10G SFP+

1.2. Moc dostępna dla PoE: 240W

1.2.1. 48 portów 5G/2.5G/1G/100M RJ-45 UPOE

2. **Zasilanie i chłodzenie urządzenia:**

2.1. Brak wentylatorów (urządzenie typu fanless),

2.2. Możliwość zasilenia urządzenia poprzez wbudowany zasilacz o mocy co najmniej 310W

2.3. Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia,

2.4. 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),

3. **Minimalne parametry wydajnościowe urządzenia:**

3.1. Przepustowość przełącznika (switching capacity): 68 Gb/s

3.2. Prędkość przesyłania (forwarding rate): 50 Mp/s

3.3. Bufor pakietów – 6MB

3.4. Pamięć DRAM – 4GB

3.5. Pamięć flash – 8GB

3.6. Możliwość obsługi 512 aktywnych sieci VLAN

3.7. Możliwość obsługi 32000 adresów MAC

3.8. Możliwość obsługi 4000 tras IPv4

3.9. Możliwość obsługi 2000 tras IPv6

3.10. Ilość wpisów w listach kontroli dostępu Security ACL – 1000

3.11. ilość wpisów w listach kontroli dostępu QoS ACL – 1000

3.12. Możliwość obsługi 512 interfejsów SVI L3

3.13. Możliwość obsługi Jumbo frame 9198 B

3.14. Możliwość obsługi 48 połączeń zagregowanych typu „port channel"

3.15. Możliwość obsługi 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

4. **Mechanizmy zaimplementowane w urządzeniu – ciągłość pracy sieci:**

4.1. IEEE 802.1w Rapid Spanning Tree

4.2. Per-VLAN Rapid Spanning Tree (PVRST+)

4.3. IEEE 802.1s Multi-Instance Spanning Tree

4.4. Obsługa 64 instancji protokołu STP

4.5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)

4.6. Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji port-channel 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 (pre-empt) po przywrócenia aktywności liku podstawowego

5. **Mechanizmy zaimplementowane w urządzeniu – bezpieczeństwo sieci:**

5.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

5.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,

5.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

5.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,

5.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,

5.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,

5.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

5.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,

5.9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),

5.10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,

5.11. 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),

5.12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,

5.13. Obsługa list kontroli dostępu (ACL) następujących typów:

5.14. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

5.15. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

5.16. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

5.17. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

5.18. 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),

5.19. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

5.20. Funkcja Private VLAN z obsługą dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS,

5.21. Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci

6. **Mechanizmy zaimplementowane w urządzeniu – weryfikacja autentyczności software i hardware**

6.1. Weryfikacja uruchamianego oprogramowania oraz hardware urządzenia w tym:

6.1.1. Sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,

6.1.2. Bezpieczna sekwencja uruchamiania,

6.1.3. Sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia

7. **Mechanizmy zaimplementowane w urządzeniu – jakość usług w sieci:**

7.1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

7.2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,

7.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

7.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

7.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

7.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,

7.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

8. **Obsługa protokołów i mechanizmów routingu:**

8.1. Routing statyczny dla IPv4 i IPv6,

8.2. Routing dynamiczny – RIP, OSPF do 1000 routes PIM Stub do 1000 routes

8.3. Policy-based routing (PBR),

8.4. Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,

8.5. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

9. **Obsługa zaawansowanych protokołów routingu**
   - 9.1. IS-IS dla IPv4 i IPv6,
   - 9.2. OSPF,
   - 9.3. EIGRP (rfc7868),
   - 9.4. Routing multicastów - PIM-SM, PIM-SSM,
   - 9.5. Multicast Source Discovery Protocol (MSDP),
10. **Obsługa dodatkowych protokołów**
   - 10.1. Obsługa protokołu NTP
   - 10.2. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
   - 10.3. LLDP (IEEE 802.1ab) i LLDP-MED.
   - 10.4. Wsparcie dla protokołu LISP zgodnie z RFC 6830 lub równoważny
   - 10.5. Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
   - 10.6. Wsparcie dla protokoły RESTCONF,
   - 10.7. Wsparcie dla protokołu gNMI,

11. **Zarządzenie urządzeniem:**
   - 11.1. Port konsoli,
   - 11.2. Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
   - 11.3. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
   - 11.4. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
   - 11.5. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

11.6. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,

11.7. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

11.8. Przełącznik posiada slot na kartę pamięci SD,

11.9. 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,

11.10. Wbudowany graficzny interfejs zarządzania przełącznikiem

12. **Parametry fizyczne urządzenia**

12.1. Obudowa kompaktowa umożliwiająca używanie / instalacje urządzenia na biurku oraz w szafie rack

12.2. Rozmiary (wartości nie więcej):

12.2.1. głębokość urządzenia: 24.4 cm,

12.2.2. szerokość urządzenia 26.9 cm,

12.2.3. wysokość urządzenia 4.4 cm

13. **Wyposażenie urządzenia:**

13.1. Urządzenie wyposażone jest w zestaw do montażu w szafie rack 19'',

13.2. zamawiający wymaga dostarczenia do każdego przełącznika dwóch wkładek 10Gb SFP+ Multimode.

14. **Wymagania dodatkowe:**

14.1. Możliwość enkapsulacji ruchu w pakiety VXLAN,

14.2. Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,

14.3. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:

14.3.1. Statycznie w oparciu o port do którego podłączona jest stacja,

14.3.2. Statycznie w oparciu o VLAN, w którym pracuje stacja,

14.3.3. Statycznie w oparciu o adres IP stacji,

14.3.4. Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;

14.4. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,

14.5. 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,

14.6. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 256-bitów (gcm-aes-256) z mechanizmem MACsec Key Agreement (MKA),

14.7. Współpraca z systemem ochrony opartym o filtrację zapytań DNS (DNS query). Przechwytywanie zapytań DNS i skierowanie ich do systemu analizy danej domeny (FQDN) pod kątem reputacji i bezpieczeństwa,

14.8. Przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),

14.9. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow),

14.10. 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,

14.11. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

14.12. Izolowane środowisko oparte o Linuxa (GuestShell) dostępne bezpośrednio na przełączniku z możliwością tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,

14.13. Obsługa 16 wirtualnych instancji routingu (VRF),

14.14. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

14.15. Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

14.16. 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.),

14.17. Funkcjonalność sondy IP SLA Responder

14.18. Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ)

14.19. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

14.20. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

14.21. Możliwość uruchomienia funkcji serwera DHCP

15. **Licencjonowanie funkcjonalności urzadzenia:**

15.1. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

Rozdział 3
Szczegółowy Opis Przedmiotu Zamówienia – Część II

I
Przełącznik sieciowy modularny typ 1C

1. **Wymagania podstawowe:**

1.1. Przełącznik modularny posiadający 10 slotów na karty w tym 2 na karty zarządzająco-przełączające oraz 8 kart liniowych.

1.2. Przełącznik musi posiadać możliwość montażu w szafie rack 19 cali

1.3. Obudowa urządzenia musi zapewniać przepustowość minimum 480Gbps na slot urządzenia.

1.4. Przełącznik musi być wyposażony w dwa redundantne moduły supervisora, każdy supervisor wyposażony w co najmniej 4 porty 40/100GE oraz co najmniej 4 porty 10/25GE.

1.5. Wraz z przełącznikiem muszą zostać dostarczone: 4 (cztery) moduły 10/25G do realizacji połączeń do 10 kilometrów z wykorzystaniem światłowodów jedno-modowych.

1.6. Przełącznik musi posiadać możliwość zainstalowania do 8 kart rozszerzeń – kart liniowych.

1.7. Każdy moduł przełączająco-zarządzający (supervisor) musi być wyposażony w dysk SSD o pojemność co najmniej 240GB

1.8. Karta zarządzająca musi posiadać wydajność minimum 240Gbps na każdy slot

1.9. Karta zarządzająca musi posiadać wydajność przełączania/routingu co najmniej 3000Mpps dla pakietów IPv4 oraz IPv6

1.10. Przełącznik musi być wyposażony w co najmniej 4 zasilacze AC 230V, każdy o mocy co najmniej 3200W

1.11. Przełącznik musi być wyposażony w demontowalny moduł wentylatorów, z możliwością wyciągania z tyłu urządzenia

1.12. Przełącznik musi posiadać agregowaną przepustowość co najmniej 9Tbps (4 Tbps w trybie fullduplex)

1.13. Przełącznik musi posiadać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC,

1.14. Przełącznik musi posiadać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,

1.15. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP

1.16. Przełącznik musi posiadać możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow (lub równoważnego)– wymagana obsługa co najmniej 144 000 strumieni (flow),

1.17. Przełącznik musi posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

1.18. Przełącznik musi posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,

1.19. Przełącznik musi posiadać wsparcie dla protokołu LISP zgodnie z RFC 6830 lub równoważnego

1.20. Przełącznik musi realizować następującą funkcjonalność w zakresie MPLS: L2VPN, L3VPN, mVPN, InterAS option A i B, EoMPLS wraz z obsługą MACSec, MPLS over GRE

1.21. Przełącznik musi posiadać obsługę protokołu BFD dla co najmniej 100 sesji

1.22. Przełącznik musi posiadać obsługę protokołu MACSec w tym również na portach zagregowanych

1.23. Przełącznik musi posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,

1.24. Przełącznik musi posiadać możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu

1.25. Przełącznik musi posiadać obsługę funkcjonalności bramy dla usług mDNS

1.26. Przełącznik musi posiadać wbudowany analizator pakietów

1.27. Przełącznik musi posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy

1.28. Przełącznik musi posiadać obsługę co najmniej 256 wirtualnych instancji routingu (VRF),

1.29. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

2. **Przełącznik musi:**

2.1.1. Obsługiwać do 64 000 adresów MAC

2.1.2. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv4 unicast

2.1.3. Obsługiwać co najmniej 16 000 wpisów w tablicy IPv4 multicast

2.1.4. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv6 unicast

2.1.5. Posiadać co najmniej 16 GB pamięci DRAM

2.1.6. Posiadać co najmniej 10 GB pamięci flash

2.1.7. Obsługiwać co najmniej 16 000 wpisów QoS ACE

2.1.8. Obsługiwać co najmniej 16 000 wpisów security ACE

2.1.9. Oosiadać bufor pakietów o wielkości co najmniej 108MB

2.1.10. Obsługiwać co najmniej 1000 unikalnych vlanów

2.1.11. Obsługiwać co najmniej 1000 interfejsów SVI

2.1.12. Obsługiwać ramki Jumbo o wielkości 9216 Bajtów

2.1.13. Posiadać wparcie dla protokołów BGP, MPLS, CDP, EIGRP, PIM, VXLAN

2.1.14. Posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping

2.1.15. Posiadać obsługę protokołu NTP

2.1.16. Posiadać wsparcie dla NETFLOW, EEM (lub równoważne), ERSPAN

2.1.17. Posiadać wsparcie dla ETA (Encrypted Traffic Analysys) (lub równoważne)

2.1.18. Posiadać wsparcie dla SDACCESS lub równoważne

2.1.19. Posiadać wsparcie dla NSF, NSR, GIR, ISSU

2.1.20. Posiadać obsługę protokołu LLDP i LLDP-MED,

3. **Wyposażenie dodatkowe urządzenia**:

3.1. Zamawiający wymaga dostarczenia przełącznika z 5 kartami liniowymi:

3.1.1. 4x 48 portów multigig 100M/1G/2.5G/5G/10GBASE-T RJ-45 UPOE+

3.1.2. 1x 48 portów SFP/SFP+ 1/10G

II
Przełącznik sieciowy modularny typ 2B

1. **Wymagania podstawowe:**

1.1. Przełącznik modularny posiadający 7 slotów na karty w tym 2 na karty zarządzająco-przełączające oraz 5 kart liniowych.

1.2. Przełącznik musi posiadać możliwość montażu w szafie rack 19 cali

1.3. Obudowa urządzenia musi zapewniać przepustowość minimum 480Gbps na slot urządzenia.

1.4. Przełącznik musi być wyposażony w dwa redundantne moduły supervisora, każdy supervisor wyposażony w co najmniej 4 porty 40/100GE oraz co najmniej 4 porty 10/25GE.

1.5. Wraz z przełącznikiem muszą zostać dostarczone: 4 (cztery) moduły 10/25G do realizacji połączeń do 10 kilometrów z wykorzystaniem światłowodów jedno-modowych

1.6. Przełącznik musi posiadać możliwość zainstalowania do 5 kart rozszerzeń – kart liniowych.

1.7. Każdy moduł przełączająco-zarządzający (supervisor) musi być wyposażony w dysk SSD o pojemność co najmniej 240GB

1.8. Karta zarządzająca musi posiadać wydajność minimum 240Gbps na każdy slot

1.9. Karta zarządzająca musi posiadać wydajność przełączania/routingu co najmniej 3000Mpps dla pakietów IPv4 oraz IPv6

1.10. Przełącznik musi być wyposażony w co najmniej 2 zasilacze AC 230V, każdy o mocy co najmniej 3200W

1.11. Przełącznik musi być wyposażony w demontowalny moduł wentylatorów, z możliwością wyciągania z tyłu urządzenia

2. **Przełącznik musi:**

2.1. Posiadać agregowaną przepustowość co najmniej 9Tbps (4 Tbps w trybie fullduplex)

2.2. Obsługiwać do 64 000 adresów MAC

2.3. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv4 unicast

2.4. Obsługiwać co najmniej 16 000 wpisów w tablicy IPv4 multicast

2.5. Obsługiwać co najmniej 112 000 wpisów w tablicy IPv6 unicast

2.6. Posiadać co najmniej 10 GB pamięci flash

2.7. Obsługiwać co najmniej 16 000 wpisów QoS ACE

2.8. Obsługiwać co najmniej 16 000 wpisów security ACE

2.9. Posiadać bufor pakietów o wielkości co najmniej 108MB

2.10. Obsługiwać co najmniej 1000 unikalnych vlanów

2.11. Obsługiwać co najmniej 1000 interfejsów SVI

2.12. Obsługiwać ramki Jumbo o wielkości 9216 Bajtów

2.13. Posiadać wparcie dla protokołów BGP, MPLS, CDP, EIGRP, PIM, VXLAN

2.14. Posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping

2.15. Posiadać obsługę protokołu NTP

2.16. Posiadać wsparcie dla NETFLOW, EEM (lub równoważne), ERSPAN

2.17. Posiadać wsparcie dla ETA (Encrypted Traffic Analysys) (lub równoważne)

2.18. Posiadać wsparcie dla SDACCESS lub równoważne

2.19. Posiadać wsparcie dla NSF, NSR, GIR, ISSU

2.20. Posiadać obsługę protokołu LLDP i LLDP-MED,

2.21. Posiadać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC,

2.22. Posiadać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,

2.23. Posiadać możliwość uruchomienia funkcji serwera DHCP

2.24. Posiadać możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow (lub równoważnego)– wymagana obsługa co najmniej 144 000 strumieni (flow),

2.25. Posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

2.26. Posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,

2.27. Posiadać wsparcie dla protokołu LISP zgodnie z RFC 6830 lub równoważnego

2.28. Realizować następującą funkcjonalność w zakresie MPLS: L2VPN, L3VPN, mVPN, InterAS option A i B, EoMPLS wraz z obsługą MACSec, MPLS over GRE

2.29. Posiadać obsługę protokołu BFD dla co najmniej 100 sesji

2.30. Posiadać obsługę protokołu MACSec w tym również na portach zagregowanych

2.31. Posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,

2.32. Posiadać możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu

2.33. 5 Posiadać obsługę funkcjonalności bramy dla usług mDNS

2.34. Posiadać wbudowany analizator pakietów

2.35. Posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy

2.36. Posiadać obsługę co najmniej 256 wirtualnych instancji routingu (VRF),

3. **Wyposażenie dodatkowe urządzenia**:

3.1. Zamawiający wymaga dostarczenia przełącznika z 5 kartami liniowymi:

3.1.1. 2x 48 portów multigig 100M/1G/2.5G/5G/10GBASE-T RJ-45 UPOE+

3.1.2. 1x 48 portów SFP/SFP+ 1/10G

4. **Licencjonowanie funkcjonalności urzadzenia:**

4.1. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

III
Przełącznik sieciowy serwerowy, typ 1

1. **Wymagania podstawowe:**
   - 1.1. Przełącznik musi posiadać:
     - 1.1.1. 48 portów 1/10/25G definiowanych za pomocą wkładek SFP/SFP+
     - 1.1.2. 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m).
2. **Parametry wydajnościowe:**
   - 2.1. Prędkość przełączania wirespeed dla wszystkich portów
   - 2.2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3. **Funkcjonalność urzadzenia dla warstwy L2**
   - 3.1. Trunking IEEE 802.1Q VLAN;
   - 3.2. Wsparcie dla minimum 3000 sieci VLAN;
   - 3.3. Wsparcie sprzętowe dla 90 tysięcy adresów MAC
   - 3.4. IEEE 802.1w Rapid Spanning Tree (RST)
   - 3.5. IEEE 802.1s Multiple Spanning Tree (MST)
   - 3.6. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
   - 3.7. Internet Group Management Protocol (IGMP) Versions 2, 3;
   - 3.8. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   - 3.9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad
   - 3.10. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
   - 3.11. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   - 3.12. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4. **Funkcjonalność urzadzenia dla warstwy L3**
   - 4.1. Sprzętowe przełączanie pakietów w warstwie L3
   - 4.2. Routing w oparciu o trasy statyczne
   - 4.3. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
   - 4.4. Policy Based Routing (PBR)
   - 4.5. VRRP lub HSRP
   - 4.6. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6

4.7. Wsparcie sprzętowe dla minimum 750 tyś prefixów LPM/ wpisów hosta w tablicy routingu IP

4.8. Wsparcie dla min. 32 VRF

4.9. Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP)

4.10. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)

4.11. Wsparcie dla IGMPv3 oraz MSDP

4.12. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych

4.13. Obsługa minimum 5000 wpisów dla ACL (access control list)

5. **Mechanizmy związane z funkcjonalnością VXLAN urządzenia**

5.1. Zintegrowany, sprzętowy VXLAN Bridging/Routing

5.2. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)

5.3. Implementacja VXLAN BGP EVPN (Ethernet VPN)

5.4. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN)

5.5. Mechanizm wykrywania i zapobiegania efektom pętli w podłączone infrastrukturze L2 poprzez mechanizm VXLAN OAM

6. **Mechanizmy zaimplementowane w urządzeniu – jakość usług w sieci:**

6.1. Layer 2 IEEE 802.1p (CoS) oraz DSCP

6.2. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6)

6.3. Kolejkowanie bezwzględne (strict-priority)

6.4. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection)

6.5. Ograniczanie ruchu (policing) do zadanej przepływności

6.6. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych

6.7. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb

6.8. Protokół RDMA/RoCE oraz ECN

7. **Mechanizmy zaimplementowane w urządzeniu – bezpieczeństwo w sieci:**

7.1. Obsługa list kontroli dostępu (ACL)

7.1.1. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;

7.1.2. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);

7.1.3. ACL oparte o porty (PACL)

7.1.4. DHCP Snooping

7.1.5. ARP Inspection

7.1.6. IP Source Guard

7.1.7. Unicast reverse path forwarding (uRPF)

7.2. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast

7.3. Możliwość wsparcie dla MACSEC na wszystkich portach. Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie.

7.4. Wsparcie dla szyfrowania AES 256 w warstwie overlay (VTEP do VTEP - tunel VXLAN). Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie

8. **Wymagana funkcjonalność urządzenia w zakresie zarządzania i zabezpieczenia przełącznika**

8.1. Port zarządzający 100/1000 Mbps;

8.2. Port konsoli CLI;

8.3. Zarządzanie In-band;

8.4. SSHv2;

8.5. Authentication, authorization, and accounting (AAA);

8.6. RADIUS;

8.7. TACACS+

8.8. Syslog;

8.9. SNMP v1, v2c, v3;

8.10. Role-Based Access Control RBAC;

8.11. IEEE 802.1ab LLDP

8.12. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)

8.13. 802.1x

8.14. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)

8.15. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)

8.16. Pełen Netflow v9

8.17. Network Time Protocol (NTP);

8.18. Precision Time Protocol IEEE 1588

8.19. Diagnostyka procesu BOOT;

8.20. Ping

8.21. Traceroute

9. **Wymagana narzędzia do programowania i zarządzania przełącznikiem**

9.1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API

9.2. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika

9.3. Wsparcie dla kontenera LXC (Linux Container) lub runC 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.

9.4. Interfejs programistyczny REST API wraz z upublicznionym SDK

9.5. Możliwość zainstalowania klienta Chef

9.6. Możliwość zainstalowania agenta Puppet

10. **Wymagane wyposażenie dodatkowe urzadzenia:**

10.1. 10 (dziewięć) modułów optycznych QSFP28 100Gb umożliwiających połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów jedno-modowych (SM) o zasięgu pracy 500m SMF (G.652) zakończony konektorem LC

10.2. 5 (pięć) modułów optycznych QSFP28 100Gb umożliwiających połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów jedno-modowych (SM) o zasięgu pracy 10Km SMF (G.652) zakończony konektorem LC

10.3. 3(trzy) moduły optyczne SFP 1G do pracy z wykorzystaniem pojedynczej pary światłowodów jedno-modowych (SM) o zasięgu pracy 10 Km SMF (G.652)

10.4. 10(dziesięć) modułów optycznych SFP+ 10G do pracy z wykorzystaniem pojedynczej pary światłowodów jedno-modowych (SM) o zasięgu pracy 10 Km SMF (G.652)

10.5. 30(trzydzieści) modułów 10/25G, do realizacji połączeń 25G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) z możliwością pracy z prędkością 10G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) zakończony konektorem LC

10.6. 2(dwa) moduły QSFP, posiadające możliwość pracy zarówno w trybie 40Gbps jak i 100Gbps na pojedynczej parze okablowania multi-mode (OM4) do 100 metrów

10.7. 10(dziesięć) modułów SFP+ 10G do pracy z wykorzystaniem kabli Cat6A/Cat7 o zasięgu pracy 30 metrów

10.8. Moduły SPF/SFP+/SFP28/QSFP+/ QSFP28 oferowane wraz z urządzeniem muszą pochodzić od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem.

11. **Wymagania dodatkowe:**

11.1. Przełącznik jest wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wlot powietrza od strony portów liniowych

11.2. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19".

11.3. Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) lub współpracy z komponentem zarządzającym (kontrolerem sieci SDN, Cisco ACI posiadanym przez Zamawiającego).

11.4. Telemetria z control/data plane eksportowana w interwałach co najmniej 100 milisekund bezpośrednio z układu ASIC przełącznika. Wsparcie dla narzędzi programistycznych w standardzie „OpenTelemetry". Eksportowane dane w formacie gRPC lub GPB dostarczają następujące informacje (dla każdego przepływu/flow):

11.4.1. Informacji o przepływie (flow), zawierają dane o adresach IP, protokołach, portach, kiedy przepływ się rozpoczął, jak długo przepływ był aktywny , ile było w nim sumarycznie danych itp.

11.4.2. Zmienność między pakietami, daje wgląd w zmiany pomiędzy pakietami w danym przepływie. Przykłady obejmują zmiany czasu życia (TTL), flagi IP i TCP, długość payload itp.

11.4.3. Szczegóły kontekstu przepływu, informacje te są uzyskiwane poza nagłówkiem pakietu, w tym zmiany w wykorzystaniu bufora kolejki, powód odrzucania pakietów w przepływie (bufor, routing, ACL), powiązanie z końcami tunelu VXLAN (VTEP) itp.

11.4.4. Dodatkowo funkcjonalność telemetrii pozwalająca na pozyskanie metadanych o każdym przepływie, który spełnia określone kryteria (np. odrzucenie, opóźnienie, microburst) z dodatkowymi informacjami identyfikującymi przyczynę (np. ACL/routing/bufor drop, opóźnienie dla scieżki, wystąpienie microburst itp.)

12. **Licencjonowanie funkcjonalności urzadzenia:**

12.1. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

Rozdział 4
Szczegółowy Opis Przedmiotu Zamówienia – Część III

I
Urządzenie odpowiedzialne za bezpieczeństwo sieci core LAN

1. **Wymagania podstawowe:**

1.1. Urządzenia muszą być wyspecjalizowanymi urządzeniami sieciowymi (tzw. appliance) mogącymi pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby i Active/Active.

1.2. Całość dostarczonych urzadzeń i oprogramowania musi umożliwiać zapewnienie wsparcia serwisowego przez jednego, tego samego, producenta.

1.3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:

1.3.1. routera (tzn. w warstwie 3 modelu ISO OSI),

1.3.2. mostu (tzn. w warstwie 2 modelu ISO OSI),

1.3.3. w trybie pasywnego nasłuchu (tzw. sniffer/tap).

1.3.4. System zainstalowany w urzadzeniu musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie, na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.

1.4. Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 4000 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

1.5. Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia lub z użyciem zewnętrznej konsoli zarządzającej GUI dostarczonej przez producenta.

1.6. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików wybranego typu, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.

1.7. Urządzenia muszą umożliwiać zarządzanie za pomocą interfejsu webowego bez konieczności instalowania dedykowanego oprogramowania na stacji końcowej.

1.8. Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia. Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy przewidzieć odpowiednie licencje dla minimum 30 administratorów na wszystkie oferowane urządzenia.

1.9. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

1.10. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH.

1.11. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:

1.11.1. Microsoft Active Directory,

1.11.2. Terminal Services,

1.11.3. Syslog,

1.11.4. Cisco ISE.

1.12. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.

1.13. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL, połączeniach VPN.

1.14. Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego zakresu czasu.

1.15. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników.

1.16. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESXi i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.

1.17. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.

1.18. Urządzenia firewall muszą obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

1.19. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

1.20. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami informacji o NAT.

1.21. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.

1.22. Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia NGFW, w celu jego dalszego przetwarzania. Urządzenie NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Nie dopuszcza się rozwiązania przesyłającego do zewnętrznych systemów bezpieczeństwa jedynie kopii ruchu, jak również rozwiązań działających na bazie protokołu ICAP. Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem NGFW przy spełnieniu poniższych wymagań:

1.22.1. realizuje wymaganą funkcjonalność dla wydajności przetwarzania minimum 3 Gbps inspekcji TLS dla sesji http 64K,

1.22.2. jest wyposażone w co najmniej 2 interfejsy 10 Gigabit Ethernet SFP+,

1.22.3. zapewnia redundancję zasilaczy analogicznie do urządzeń firewall,

1.22.4. musi być dostarczone w modelu redundancji 1:1 (analogicznie do urządzeń firewall) z potrzebnymi licencjami i gwarancją/wsparciem zgodnym z długością wsparcia firewalla,

1.22.5. musi być dostarczone z potrzebnymi licencjami i gwarancją zgodną z długością wsparcia firewalla,

1.22.6. w przypadku zewnętrznego urządzenia lub urządzeń innych niż NGFW wymagane jest dostarczenie opisu współpracy proponowanej integracji z NGFW wykonującym inspekcję wykrywania i zapobiegania włamaniom na rozszyfrowanym ruchu przez zewnętrzne urządzenia.

1.23. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.

1.24. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takim przypadku urządzenie musi umożliwiać blokadę takiej sesji użytkownika.

1.25. Wykonywanie operacji deszyfrowania ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji.

1.26. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL (w przypadku, gdy jest wymagane jego dostarczenie) albo możliwość wykorzystania własnej utworzonej na urządzeniu listy URL które mają podlegać deszyfracji albo być z niej wykluczone (tzw. wyjątek).

1.27. Urządzenie firewall musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.

1.28. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.

1.29. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.

1.30. Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).

1.31. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.

1.32. Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla min. 1500 użytkowników jednocześnie (tzw. Remote Access VPN) bez łamania warunków licencyjnych. Funkcja zdalnego dostępu VPN musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowanie klienta Remote Access VPN wymaga licencji – należy tę licencję dostarczyć.

1.33. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.

1.34. Oprogramowanie klienta VPN musi być zapewnione dla minimum 5000 urządzeń.

1.35. Producent oferowanego rozwiązania musi być obecny w najnowszym rynkowym raporcie Gartner Magic Quadrant for Enterprise Network Firewalls w części (tzw. ćwiartce) Leaders.

1.36. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

1.37. Bezpośrednio w GUI urządzenia lub w zewnętrznej konsoli zarządzającej GUI dostarczonej przez producenta musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.

1.38. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.

1.39. Urządzenie musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny (nie rzadziej niż raz na 48h) i pochodzić od tego samego producenta co firewall.

1.40. Urządzenie musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.

1.41. Urządzenie musi posiadać funkcję filtrowania URL, nie jest wymagane dostarczenie licencji jeśli jest wymagana do uruchomienia funkcjonalności.

1.42. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.

1.43. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa.

1.44. Urządzenia firewall muszą posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach, pozwalając jednocześnie znacznie zmniejszyć okres ryzyka tzw. pacjenta typu ZERO.

1.45. Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port Ethernet 10/100/1000 lub jako port SFP z wkładką 1000BASE-T.

1.46. Urządzenia muszą być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie.

1.47. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.

1.48. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane). Akceptowana jest separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU cores) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.

1.49. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.

1.50. Urządzenia firewall muszą wspierać protokół LACP.

1.51. Urządzenia firewall muszą, zgodnie z ustaloną polityką, prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).

1.52. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.

2. **Wymagania dodatkowe:**

2.1. Należy dostarczyć 2 szt. urządzeń, które będą pracowały jako 1 para w układzie HA.

2.2. Urządzenie musi być wyposażone w minimum:

2.2.1. 8 portów Ethernet RJ45 wspierających 1G/2.5G/5G/10G

2.2.2. 8 portów Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP),

2.2.3. 4 porty 25G.

2.2.4. 40G/100G QSFP/QSFP28

2.3. Urządzenie musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 480 GB na potrzeby systemu operacyjnego i logów.

3. **Wymagania wydajnosciowe:**

3.1. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:

3.1.1. 24 Gbps dla rozpoznawania i kontroli aplikacji,

3.1.2. 8,5 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia,

3.1.3. 11 Gbps wydajności IPSec VPN,

3.1.4. 210 000 nowych sesji na sekundę,

3.1.5. 2,1 M równoległych sesji.

3.2. Wymagania podczas pracy w trybach router/most muszą być zapewnione z włączonymi pełnymi zakresami ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w urządzeniu dla silników antywirus i antyspyware/antymalware. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez urządzenie. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez urządzenie – jeżeli urządzenie pozwala na pracę w wielu trybach to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.

3.3. Wszystkie parametry dotyczące wydajności (w trybie pracy router/most) pod kątem przepustowości (ang. throughput), zakładają, iż będą to parametry wskazane przez producentów w kartach katalogowych jako HTTP 64KB (lub HTTP dla mniejszych sesji np. HTTP 44KB, HTTP 40KB).

3.4. W przypadku gdy Wykonawca zaproponuje urządzenie, którego producent nie publikuje wyników testów wydajnościowych dla HTTP 64KB lub mniejszych sesji, wówczas jest on zobowiązany do dodatkowego potwierdzenia spełnienia wymagań wydajnościowych. Zamawiający wymaga aby potwierdzenie zostało dostarczone w postaci wyników testów przeprowadzonych przez publiczny ośrodek badawczo-rozwojowy w Polsce z wykorzystaniem dedykowanych testerów ruchu – IXIA lub Spirent lub Agilent.

4. **Obudowa urządzenia i jego właściwości fizyczne:**

4.1. Możliwość montażu w szafie rack 19".

5. **Polityka zabezpieczeń firewall musi uwzględniać**

5.1. adresy IP źródłowe i docelowe,

5.2. protokoły i usługi sieciowe,

5.3. aplikacje,

5.4. kategorie URL,

5.5. użytkowników aplikacji i grupy,

5.6. reakcje zabezpieczeń,

5.7. logowanie zdarzeń (początek i koniec sesji),

5.8. strefa wejściowa i wyjściowa.

6. **Licencjonowanie funkcjonalności urzadzenia:**

6.1. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

7. **Wyposażenie dodatkowe:**

7.1. Wraz z urządzeniem muszą zostać dostarczone:

7.1.1. 2 (dwa) moduły QSFP 40G do pracy na pojedynczej parze okablowania multimode (OM4) do 100 metrów.

7.1.2. 4 (cztery) moduły 10/25G, do realizacji połączeń 25G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) z możliwością pracy z prędkością 10G dla połączenia światłowodowego MMF na odległość 300m (OM3) lub 400m (OM4) zakończony konektorem LC

7.1.3. 8 (osiem) modułów optycznych SFP+ 10G do pracy z wykorzystaniem pojedynczej pary światłowodów wielo-modowych (MMF) o zasięgu pracy 400 metrów(dla OM4)

7.2. Moduły SPF/SFP+/SFP28/QSFP+/ QSFP28 oferowane wraz z urządzeniem muszą pochodzić od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem

II
Urządzenie odpowiedzialne za bezpieczeństwo sieci core LAN na styku z siecią Internet

1. **Wymagania podstawowe:**

1.1. Urządzenie musi być wyspspecjalizowanym urządzeniem sieciowym (tzw. appliance) mogącym pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby i Active/Active.

1.2. Należy dostarczyć 2 szt. urządzeń, które będą pracowały jako 1 para w układzie HA.

1.3. Każde z urządzeń musi (poza wymaganiami ogólnymi), spełniać dodatkowo wymagania:

1.4. Urządzenie musi być wyposażone w minimum:

1.4.1. minimum 8 portów Ethernet RJ45 wspierających 1G/2.5G/5G

1.4.2. minimum 8 portów Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP).

1.5. Urządzenie musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 240 GB na potrzeby systemu operacyjnego i logów.

1.6. Urządzenie muszą umożliwiać działanie w następujących trybach pracy:

1.6.1. rutera (tzn. w warstwie 3 modelu ISO OSI),

1.6.2. mostu (tzn. w warstwie 2 modelu ISO OSI),

1.6.3. w trybie pasywnego nasłuchu (tzw. sniffer/tap).

1.7. Systemzainstalowany w urzadzeniu musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.

1.8. Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port Ethernet 10/100/1000 lub jako port SFP z wkładką 1000BASE-T.

1.9. Urządzenia muszą być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie.

1.10. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.

1.11. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw.

management plane). Akceptowana jest separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU cores) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.

1.12. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.

1.13. Urządzenia firewall muszą wspierać protokół LACP.

1.14. Urządzenia muszą umożliwiać zarządzanie za pomocą interfejsu webowego bez konieczności

1.15. Urzędzenie musi umożliwiać instalowanie dedykowanego oprogramowania na stacji końcowej.

1.16. Urządzenia firewall musi, zgodnie z ustaloną polityką, prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).

1.17. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.

2. **Polityka zabezpieczeń:**

2.1. Urządzenie, w swojej polityce zabezpieczeń, musi uwzględniać:

2.1.1. adresy IP źródłowe i docelowe,

2.1.2. protokoły i usługi sieciowe,

2.1.3. aplikacje,

2.1.4. kategorie URL,

2.1.5. użytkowników aplikacji i grupy,

2.1.6. reakcje zabezpieczeń,

2.1.7. logowanie zdarzeń (początek i koniec sesji),

2.1.8. strefa wejściowa i wyjściowa.

3. **Wymagania dodatkowe:**

3.1. Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 4000 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

3.2. Urządzenia firewall muszą posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach oraz kategoriach URL, pozwalając jednocześnie znacznie zmniejszyć okres ryzyka tzw. pacjenta typu ZERO.

3.3. Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia lub z użyciem zewnętrznej konsoli zarządzającej GUI dostarczonej przez producenta.

3.4. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików wybranego typu, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.

3.5. Urządzenia firewall muszą być zarządzane z linii poleceń (CLI) oraz interfejsu GUI lub z użyciem zewnętrznej konsoli zarządzającej GUI dostarczonej przez producenta.

3.6. Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia. Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy przewidzieć odpowiednie licencje dla minimum 30 administratorów na wszystkie oferowane urządzenia.

3.7. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

3.8. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH.

3.9. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:

3.9.1. Microsoft Active Directory,

3.9.2. Terminal Services,

3.9.3. Syslog,

3.9.4. Cisco ISE.

3.10. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.

3.11. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL, połączeniach VPN.

3.12. Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego zakresu czasu.

3.13. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników.

3.14. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESXi i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.

3.15. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.

3.16. Urządzenia firewall muszą obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

3.17. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

3.18. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami informacji o NAT.

3.19. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.

3.20. Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia NGFW, w celu jego dalszego przetwarzania. Urządzenie NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Nie dopuszcza się rozwiązania przesyłającego do zewnętrznych systemów bezpieczeństwa jedynie kopii ruchu, jak również rozwiązań działających na bazie protokołu ICAP. Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem NGFW przy spełnieniu poniższych wymagań:

3.20.1. realizuje wymaganą funkcjonalność dla wydajności przetwarzania minimum 1 Gbps inspekcji TLS dla sesji http 64K,

3.20.2. jest wyposażone w co najmniej 2 interfejsy 1 Gigabit Ethernet SFP+,

3.20.3. zapewnia redundancję zasilaczy analogicznie do urządzeń firewall,

3.20.4. musi być dostarczone w modelu redundancji 1:1 (analogicznie do urządzeń firewall) z potrzebnymi licencjami i gwarancją/wsparciem zgodnym z długością wsparcia firewalla,

3.20.5. musi być dostarczone z potrzebnymi licencjami i gwarancją zgodną z długością wsparcia firewalla,

3.20.6. w przypadku zewnętrznego urządzenia lub urządzeń innych niż NGFW wymagane jest dostarczenie opisu współpracy proponowanej integracji z NGFW wykonującym inspekcję wykrywania i zapobiegania włamaniom na rozszyfrowanym ruchu przez zewnętrzne urządzenia.

3.21. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.

3.22. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takim przypadku urządzenie musi umożliwiać blokadę takiej sesji użytkownika.

3.23. Wykonywanie operacji deszyfrowania ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji.

3.24. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL (w przypadku, gdy jest wymagane jego dostarczenie) albo możliwość wykorzystania własnej utworzonej na urządzeniu listy URL które mają podlegać deszyfracji albo być z niej wykluczone (tzw. wyjątek).

3.25. Urządzenie firewall musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.

3.26. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.

3.27. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.

3.28. Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).

3.29. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.

3.30. Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla min. 1000 użytkowników jednocześnie (tzw. Remote Access VPN) bez łamania warunków licencyjnych. Funkcja zdalnego dostępu VPN musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowanie klienta Remote Access VPN wymaga licencji – należy tę licencję dostarczyć.

3.31. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.

3.32. Oprogramowanie klienta VPN musi być zapewnione dla minimum 5000 urządzeń.

3.33. Producent oferowanego rozwiązania musi być obecny w najnowszym rynkowym raporcie Gartner Magic Quadrant for Enterprise Network Firewalls w części (tzw. ćwiartce) Leaders.

4. **Wymagania wydajnościowe:**

4.1. Urzadzenie musi spełniać co najmniej następujące parametry wydajnościowe:

4.1.1. 9 Gbps dla rozpoznawania i kontroli aplikacji,

4.1.2. 4 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia,

4.1.3. 6 Gbps wydajności IPSec VPN,

4.1.4. 120 000 nowych sesji na sekundę,

4.1.5. 1,2 M równoległych sesji.

4.2. Wymagania podczas pracy w trybach router/most muszą być zapewnione z włączonymi pełnymi zakresami ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w urządzeniu dla silników antywirus i antyspyware/antymalware. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez urządzenie. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez urządzenie – jeżeli urządzenie pozwala na pracę w wielu trybach to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.

4.3. Wszystkie parametry dotyczące wydajności (w trybie pracy router/most) pod kątem przepustowości (ang. throughput), zakładają, iż będą to parametry wskazane przez producentów w kartach katalogowych jako HTTP 64KB (lub HTTP dla mniejszych sesji np. HTTP 44KB, HTTP 40KB).

4.4. W przypadku gdy Wykonawca zaproponuje urządzenie, którego producent nie publikuje wyników testów wydajnościowych dla HTTP 64KB lub mniejszych sesji, wówczas jest on zobowiązany do dodatkowego potwierdzenia spełnienia wymagań wydajnościowych. Zamawiający wymaga aby potwierdzenie zostało dostarczone w postaci wyników testów przeprowadzonych przez publiczny ośrodek badawczo-rozwojowy w Polsce z wykorzystaniem dedykowanych testerów ruchu – IXIA lub Spirent lub Agilent.

5. **Wymagane funckje zabezpieczeń**

5.1. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

5.2. Bezpośrednio w GUI urządzenia lub w zewnętrznej konsoli zarządzającej GUI dostarczonej przez producenta musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.

5.3. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.

5.4. Urządzenie musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny (nie rzadziej niż raz na 48h) i pochodzić od tego samego producenta co firewall.

5.5. Urządzenie musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.

5.6. Urządzenie musi posiadać funkcję filtrowania URL. Filtrowanie ruchu URL musi odbywać się w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron dostarczoną przez producenta urządzeń. Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp) oraz określenie ryzyka do niej przypisanego (co najmniej wysokie-średnie-niskie).

5.7. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.

5.8. Urządzenie musi posiadać funkcję filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa.

5.9. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania kategorii URL.

5.10. Urządzenie musi umożliwiać wysyłanie plików przesyłanych przez urządzenie do lokalnego lub chmurowego systemu Sandbox (który należy zapewnić w ofercie bądź w postaci fizycznego urządzenia bądź usługi subskrypcji):

5.10.1. Urządzenie firewall musi pozwalać na przesyłanie do systemu Sandbox plików zdefiniowanych przez administratora – co najmniej exe, dll, java, MS Office,

5.10.2. Urządzenie firewall musi być aktualizowane o nowo wykryte (w Sandbox zagrożenia),

5.10.3. Administrator musi posiadać dostęp do raportów z Sandbox'a dotyczących plików wysłanych przez urządzenie firewall oraz posiadać możliwość manualnego wysłania pliku do Sandbox (np. poprzez upload poprzez stronę www),

5.10.3.1. dopuszcza się zaoferowanie lokalnego rozwiązania Sandbox (zapewnianego przez producenta firewall'i) – należy wówczas przewidzieć urządzenie pozwalające na jednoczesną analizę co najmniej 30 próbek/plików (VM Sandboxing),

5.10.3.2. dopuszcza się zaoferowanie chmurowego rozwiązania Sandbox (realizowanego przez producenta firewall'i). W przypadku, jeżeli producent licencjonuje dostęp do chmurowego Sandbox'a należy przewidzieć licencję pozwalającą na jednoczesną analizę minimum 30 próbek/plików (VM Sandboxing),

5.11. Urządzenie musi mieć możliwość analizy co najmniej 30 próbek/plików jednocześnie bez względu na to czy pliki te wysłane będą automatycznie czy manualnie przez administratora, czy też będzie to „mix" plików pochodzących zarówno bezpośrednio z firewall'a i od administratorów.

5.12. Urządzenia muszą posiadać funkcjonalność ochrony zapytań DNS w czasie rzeczywistym. Zamawiający zastrzega, że nie dopuszcza rozwiązania funkcjonującego tylko i wyłącznie o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę domenową, która jeszcze nie znajduje się w bazie. Dla każdego zapytania DNS przetwarzanego przez firewall musi zostać wykonana pełna analiza co najmniej w zakresie jak poniżej:

5.12.1. Wykrywanie zapytań do domen złośliwych (baza domen musi mieć co najmniej 30 milionów wpisów),

5.12.2. Wykrywanie domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA),

5.12.3. Wykrywanie domen dynamicznych Dynamic DNS,

5.12.4. Wykrywanie nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych (tunelowanie DNS),

5.12.5. Wykrywanie domen typu fast-flux.

5.13. Urządzenia muszą umożliwiać skonfigurowanie fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing).

5.14. Urządzenia firewall muszą posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach, pozwalając jednocześnie znacznie zmniejszyć okres ryzyka tzw. pacjenta typu ZERO.

6. **Wymagane wyposażenie dodatkowe**

6.1. Wraz z urządzeniem muszą zostać dostarczone:

6.2. 4 (cztery) moduły optyczne SFP 1G do pracy z wykorzystaniem pojedynczej pary światłowodów jedno-modowych (SM) o zasięgu pracy 10 Km SMF (G.652)

6.3. 4 (cztery) moduły optyczne SFP+ 10G do pracy z wykorzystaniem pojedynczej pary światłowodów jedno-modowych (SM) o zasięgu pracy 10 Km SMF (G.652)

6.4. Moduły SPF/SFP+/SFP28/QSFP+/ QSFP28 oferowane wraz z urządzeniem muszą pochodzić od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem

7. **Licencjonowanie funkcjonalności urzadzenia:**

7.1. Wszelkie licencje, niezbędne do zapewnienia opisanej wyżej funkcjonalności, muszą być dostarczane bezterminowo lub na okres co najmniej równy długości wsparcia technicznego dla danego urządzenia.

Rozdział 5
Warunki Świadczenia Gwarancji i Serwis na dostarczone urządzenia

I
Wymagania dla Części I
- Przełączniki Sieciowe LAN 1

A. Wymagania podstawowe

1. Zamawiajacy wymaga aby dostarczone do niego urządzenia objęte były opieką serwisową w ramach:
   1.1. **Kontraktu Serwisowego,** dedykowanych przez producenta urządzeń (dotyczy każdego dostarczonego w ramach Umowy urządzenia) – usługa świadczona bezpośrednio przez Producenta lub pośrednio przez jego oficjalnego przedstawciela (zgodnie z warunkami określonymi przez producenta urządzeń w Kontrakcie Serwisowym)
   1.2. **Usługi wsparcia Wykonawcy dla** urządzeń dostarczonych w ramach Umowy – usługa świadczona bezpośrednio przez Wykonawcę
2. Okres trwania Usługi
   2.1. Kontrakt Serwisowy – 48 mc.
      2.1.1. Okres obowiązywania Kontraktów Serwisowych liczony będzie od dnia Podpisania Protokołów Zdawczo – Odbiorczych przez Zamawiajacego,
   2.2. Sparcie Techniczne Wykonawcy - 48 mc.
      2.2.1. Okres obowiązywania Wsparcia Wykonawcy liczony będzie od dnia Podpisania Protokołów Zdawczo – Odbiorczych przez Zamawiajacego,
3. W przypadku awarii urządzeń objętych jednocześnie Usługą Wsparcia i Kontraktem Serwisowym, nadrzędnym sposobem naprawy urządzeń Zamawiającego jest ten określony w Kontrakcie Serwisowym producenta. Tym samym, sposób (gdzie jako, „sposób naprawy", należy rozumieć wymianę uszkodzonego urządzenia lub jego naprawę) naprawy usterki/awarii urządzeń Zamawiającego, zdefiniowany w Kontrakcie Serwisowym, ma pierwszeństwo w zastosowaniu przed zobowiązaniami nałożonymi na Wykonawcę.
4. Zamawiający zastrzega, że wybór drogi obsługi serwisowej urządzenia nie zwalnia Wykonawcy ze zobowiązań terminowych wskazanych w OPZ (Rozdział 5). Tym samym zobowiązania terminowe wskazane w OPZ (Rozdział 5) mają pierwszeństwo nad tymi określonymi w Kontrakcie Serwisowym producenta.

B. Wymagania wobec Usługi Wsparcia realizowanej przez Wykonawcę

1. Zamawiający wymaga, aby Usługa Wsparcia ze strony Wykonawcy realizowane było przez wyznaczonych przez niego Inżynierów, którzy posiadają akredytację/certyfikację producenta, dostarczonych przez Wykonawcę urządzeń, do pracy z tymi urządzeniami, np. Inżyniera CCNP, CCNE (w przypadku dostarczenie przez Wykponawcę urządzeń marki CISCO)

    1.1. Zamawiający wymaga, aby Inżynierowie Wykonawcy (wytypowani do wsparcia Zamawiajacego) posiadali certyfikację producenta urządzeń na 2 poziomach:

        1.1.1. Najwyższą dostępną certyfikację przewidzianą przez producenta, a niezbędną do obsługi urządzeń sieciowych

        1.1.2. Certyfikację na poziomie o jeden stopień niższy (wg producenta urządzeń) niż najwyższy stopień certyfikacji, o którym mowa w ust. 1.1.1. powyżej, a niezbędną do obsługi urządzeń sieciowych

2. W przypadku przekazania przez Zamawiającego informacji o wystąpieniu awarii urządzeń, Wykonawca zapewni wsparcie swojego Inżyniera, którego zadaniem będzie: diagnoza zgłoszonej awarii, określenie sposobu usunięcia awarii, a następnie usunięcie awarii.

    2.1. Wykonawca zobowiązany jest zapewnić wsparcie Inżyniera, którego zakres wiedzy (potwierdzony stosownym certyfikatem producenta urządzeń) okaże się wystarczający, do usunięcia awarii (diagnostyka, zidentyfikowanie przyczyny awarii, usunięcia awarii).

        2.1.1. Jeżeli poziom certyfikacji danego Inżyniera będzie nie wystarczający do usunięcia ustarki i rozwiązania problemu, Wykonawca zapewni Zamawiającemy wsparcie techniczne innego Inżyniera, którego poziom certyfikacji będzie uznawany przez producenta urządzenia, jako wyższy

3. Czas reakcji Wykonawcy na zgłoszoną przez Zamawiającego awarię/usterkę nie może przekroczyć 1 godziny

    3.1. Działania serwisowe i wsparcia technicznego Wykonawcy muszą zostać podjęte w terminie nieprzekraczającym 1 godziny, od momentu zgłoszenia awarii przez Zamawiającego – z zastrzeżeniem, że w przypadku awarii zgłoszonych przez Zamawiającego po godzinie 15:00, do świadczenia Usług Wykonawca przystąpi o godz. 8:00 następnego dnia roboczego;

    3.2. W przypadku zgłoszeń wykonanych przez Zamawiajacego w dni ustatowo wolne od pracy, do świadczenia Usług Wsparcia Wykonawca przystąpi o godz. 8:00 w pierwszym dniu roboczym, jaki nastąpi po dniu wolnym od pracy;

4. Wymagana przez Zamawiającego Usługa Wsparcia, musi mieć formę wsparcia „8x5xNBD", czyli:

    4.1. Obsługa zgłoszeń serwisowych w dni robocze (w godz. 8:00 – 15:00);

    4.2. Czas reakcji na zgłoszenie Zamawiajacego - maksymalnie 1 godzina;

    4.3. Usunięcie awarii (przywrócenie pełnej sprawności urządzenia lub oprogramowania)

5. Zamawiający wymaga, aby w przypadku awarii urządzenia:

5.1. Wykonawca naprawił urządzenie Zamawiającego własnymi staraniami i przywrócił je do pełnej sprawności technicznej i funkcjonalnej (przywrócenie sprawności elementów hardware i software).

5.2. Na czas naprawy urządzenia, które uległo awarii, Wykonawca dostarczy Zamawiającemu zamienne, sprawne urządzenie o parametrach i funkcjonalności nie gorszej niż urządzenie które uległo awarii.

5.3. Po naprawie urządzenia Zamawiającego Wykonawca zainstaluje naprawione urządzenie w lokalizacji wskazanej przez Zmawiającego.

5.4. W przypadku kiedy naprawa urządzenia Zamawiającego, przez Wykonawcę będzie niemożliwa, Wykonawca przekaże nieodpłatnie na rzecz i do dyspozycji Zamawiającego fabrycznie nowe urządzenie tej samej klasy (urządzenie o parametrach i funkcjonalności nie gorszej niż urządzenie które uległo awarii – urządzenie tego samego producenta). Urządzenie zostanie wpisane na stan środków trwałych Zamawiającego i będzie stanowiło jego własność (zamiennie za urządzenie które uległo awarii).

5.5. Urządzenie zastępcze przekazane przez Wykonawcę Zamawiającemu – o którym mowa w ust. 2.4 powyżej, musi być objęte Usługą Wsparcia do czasu zakończenia obowiązywania Umowy i jednocześnie wykupiony na to urządzenie musi zostać Kontrakt Serwisowy (na warunkach nie gorszych niż te wskazane w OPZ).

6. Zamawiający przewiduje możliwość świadczenia Usługi Wsparcia zdalnie lub telefoniczne, jednak jeżeli taka forma kontaktu okaże się niewystarczające do: stwierdzenia przyczyn awarii, określenia sposobu usunięcia awarii i usunięcia awarii, inżynier Wykonawcy zobowiązany jest do niezwłocznego przyjazdu na miejsce wystąpienia awarii i wymiany urządzenia. Decyzję o konieczności przyjazdu Wykonawcy na miejsce, w którym wystąpiła awaria urządzenia, podejmuje uprawniony pracownik Zamawiającego, wskazany w Umowie;

7. W przypadku konieczności realizacji Usługi w obiektach technicznych Zamawiającego, koniecznym jest umówienie takiej wizyty - daty i godziny przyjazdu przedstawiciela Wykonawcy, z uprawnionym pracownikiem Zamawiającego;

8. Diagnostyka uszkodzonego i/lub nie w pełni funkcjonalnego urządzenia przez Wykonawcę nie może trwać dłużej niż 24 godziny, liczonych od daty kiedy wysłano przez Zamawiającego zgłoszenie z informacją o uszkodzonym i/lub nie w pełni funkcjonalnym urządzeniu. W tym przedziale czasowym (w ciągu 24 godziny od wysłania zgłoszenia) Wykonawca zobowiązany jest do poinformowania Zamawiającego o sposobie usunięcia awarii urządzenia. Jeżeli w ciągu 24 godzin, od daty zgłoszenia awarii przez Zamawiającego, nie uda się zidentyfikować przyczyny awarii i jej usunąć, Wykonawca zobowiązany jest do wymiany urządzenia na zastępcze wolne od wad (w ramach Usługi Wsparcia lub Kontraktu Serwisowego);

9. Jeżeli usunięcie awarii będzie wymagało wymiany urządzenia, Wykonawca zobowiązany jest do przekazania Zamawiającemu informacji o konieczności wymiany urządzenia (na zastępcze) nie później niż ciągu 5 godzin po zakończonej diagnostyce urządzenia – z zastrzeżeniem o którym mowa w pkt. 5 powyżej;

10. Jeżeli usunięcie awarii możliwe będzie do zrealizowania bez konieczności wymiany urządzenia wadliwego na zastępcze, Wykonawca zobowiązany będzie usunąć awarię nie później niż ciągu

10 godzin po zakończonej diagnostyce urządzenia – z zastrzeżeniem, o którym mowa w pkt. 5 powyżej;

11. Jeżeli Póba Usunięcia Awarii Urządzenia nie przyniesie oczekiwanych rezultatów, Wykonawca zobowiązany jest w ciągu 8 godzin – liczonych od Daty wykonania pierwszej Próby usunięcia awarii urządzenia, wymienić urządzenie na zastępcze (w ramach Usługi Wsparcia lub Kontraktu Serwisowego);
12. Wykonawca gwarantuje, iż w przypadku konieczności wymiany wadliwego urządzenia na zastępcze (wolne od wad) zostanie to dokonane nie później niż w ciągu 24 godzin od daty zakończenia procedury diagnostycznej lub do godziny 17:00 kolejnego dnia roboczego (w zależności który z tych terminów wystąpi później).
13. Wymiany urządzenia wadliwego, w ramach Usługi Wsparcia, dokona Inżynier Wykonawcy;
14. Wymiana urządzenia, jego uruchomienie zapewniające przywrócenie pierwotnej funkcjonalności sieci teleinformatycznej Zamawiającego - sprzed awarii, dokonane zostanie nie później niż do godziny 24:00 trzeciego dnia roboczego liczonego od dnia, w którym Zamawiający zgłosił Wykonawcy awarię.
15. Serwis i wsparcie techniczne dla urządzenia, dostarczonego w miejsce urządzenia wadliwego, świadczone będzie na warunkach określonych w ramach Usługi Wsparcia do końca obowiązywania Umowy.
16. Termin rozpoczęcia usuwania awarii (w ramach Usługi Wsparcia) wymaga każdorazowego uzgodnienia z Zamawiającym. Termin ten może zostać przesunięty przez Zamawiającego z przyczyn operacyjnych związanych z bezpieczeństwem ruchu lotniczego. W takim przypadku termin usunięcia awarii ulegnie odpowiedniemu wydłużeniu, o czym Zamawiający powiadomi Wykonawcę telefonicznie (potwierdzając niezwłocznie e-mailem), lub pocztą elektroniczną;
17. Realizacja Przedmiotu Zamówienia musi być świadczona w taki sposób, aby nie zostały utracone gwarancje udzielone przez producentów innych urządzeń na: powiązane podzespoły urządzeń, inne urządzenia pracujące w sieci Zamawiającego, inne elementy aktywne i pasywne tworzące infrastrukturę teleinformatyczną Zamawiającego, w trakcie świadczenia Usługi przez Wykonawcę;
18. W ramach Usługi Wsparcia, Zamawiający zastrzega sobie prawo do kontaktu z Wykonawcą w celu obsługi bieżących problemów z funkcjonowaniem dostarczonych urządzeń, jak również w przypadku konieczności zwiększenia ich funkcjonalności i tym samym zmianą ich konfiuracji

C. Minimalne wymagania wobec warunków Kontraktów Serwisowych

1. Zakres Kontraktów Serwisowych musi wynikać z oferty serwisowej producenta dostarczonych urządzeń
2. Kontrakt Serwisowy musi zapewniać Zamawiajacemu:
   - 2.1. Dostęp do technicznego centrum wsparcia producenta dostarczonych urządzeń, np. tyu: Cisco Technical TAC, przez dwadzieścia cztery (24) godziny na dobę, siedem (7) dni w tygodniu.
     - 2.1.1. Czasy odpowiedzi dla połączeń o poziomach ważności 1 i 2 nie może przekraczać (1) godziny.
     - 2.1.2. Czasy reakcji dla połączeń o poziomach ważności 3 i 4: W godzinach pracy centrum wsparcia techncicznego - w ciągu jednej (1) godziny.
     - 2.1.3. W dni wolne od pracy - w ciągu następnego dnia roboczego w godzinach pracy
   - 2.2. Dostęp do portalu, który zapewni Zamawiającemu wgląd w informacje techniczne na temat dostarczonych w ramach zamówienia urządzeń, w tym aktualnego oprogramowania i poprawek dla tych urządzeń,
   - 2.3. Dostęp do portalu, który zapewni Zamawiającemu możliwość wymiany informacji z grupą użytkowników produktów producenta dostarczonych urządzeń.
   - 2.4. Dostęp do portalu samoobsługowego, który zapewni Zamawiającemu wgląd w informacje nt. raportów z funkcjonowania urządzeń, aplikacji (w celu zarządzania uprawnieniami do usług i innymi funkcjami) oraz innego oprogramowania (w celu zbierania informacji dotyczących konfiguracji i inwentaryzacji zainstalowanych produktów producenta dostarczonych urządzeń)
   - 2.5. Możliwość aktualizacji systemu operacyjnego urządzeń, obejście problemu lub dostęp do poprawki dla zgłoszonych problemów z oprogramowaniem
   - 2.6. Możliwość aktualizacji oprogramowania urządzeń, która to konieczność może wyniknąć z kontaktu z centrum wsparcia technicznego producenta i np. po zgłoszenia producentowi problemów
   - 2.7. Dostęp do dokumentacji i każdej wersji oprogramowania dedykowanego dla danego urządzenia objętego Kontraktem Serwisowym
   - 2.8. Dostęp do narzędzia, którym producent urządzenia zbiera informacje nt. funkcjonowania swoich urządzeń (poprawności lub awarii urządzeń)
   - 2.9. Wymianę części i modułów w dostarczonych urządzeniach Zamawiającemu
3. Usługi serwisowe w ramach Kontraktu Serwisowego muszą być świadczone w miejscu zainstalowanai urządzeń Zamawiajacego,
4. Kontrakt Serwisowy musi zapewniać wymiane uszkodzonych i nie właściwie funkcjonujących urządzeń ew. ich modułów na nowe

5. Kontrakty Serwisowe muszą mieć formę wsparcia „8x5xNBD", czyli:
   5.1. Obsługa zgłoszeń serwisowych w dni robocze (w godz. 8:00 – 15:00);
   5.2. Czas reakcji na zgłoszenie Zamawiajacego - maksymalnie 1 godzina;
   5.3. Usunięcie awarii (przywrócenie pełnej sprawności urządzenia lub oprogramowania)

II
Wymagania dla Części II
- Przełączniki Scieciowe LAN2

A. Wymagania podstawowe

1. Zamawiajacy wymaga aby dostarczone do niego urządzenia objęte były opieką serwisową w ramach:
   1.1. **Kontraktu serwisowego,** dedykowanych przez producenta urządzeń (dotyczy każdego dostarczonego w ramach Umowy urządzenia) – usługa świadczona bezpośrednio przez Producenta lub pośrednio przez jego oficjalnego przedstawiciela (zgodnie z warunkami określonymi przez producenta urządzeń w Kontrakcie Serwisowym)
   1.2. **Usługi wsparcia Wykonawcy dla** urządzeń dostarczonych w ramach Umowy – usługa świadczona bezpośrednio przez Wykonawcę
2. Okres trwania Usługi
   2.1. Kontrakt Serwisowy – 48 mc.
      2.1.1. Okres obowiązywania Kontraktów Serwisowych liczony będzie od dnia Podpisania Protokołów Zdawczo – Odbiorczych przez Zamawiajacego
   2.2. Sparcie Techniczne Wykonawcy - 48 mc.
      2.2.1. Okres obowiązywania Wsparcia Wykonawcy liczony będzie od dnia Podpisania Protokołów Zdawczo – Odbiorczych przez Zamawiajacego,
3. W przypadku awarii urządzeń objętych jednocześnie Usługą Wsparcia i Kontraktem Serwisowym, nadrzędnym sposobem naprawy urządzeń Zamawiającego jest ten określony w Kontrakcie Serwisowym producenta. Tym samym, sposób (gdzie jako, „sposób naprawy", należy rozumieć wymianę uszkodzonego urządzenia lub jego naprawę) naprawy usterki/awarii urządzeń Zamawiającego, zdefiniowany w Kontrakcie Serwisowym, ma pierwszeństwo w zastosowaniu przed zobowiązaniami nałożonymi na Wykonawcę.
4. Zamawiający zastrzega, że wybór drogi obsługi serwisowej urządzenia nie zwalnia Wykonawcy ze zobowiązań terminowych wskazanych w OPZ (Rozdział 5). Tym samym zobowiązania terminowe wskazane w OPZ (Rozdział 5) mają pierwszeństwo nad tymi określonymi w Kontrakcie Serwisowym producenta.

B. Wymagania wobec Usługi Wsparcia realizowanej przez Wykonawcę

1. Zamawiający wymaga, aby Usługa Wsparcia ze strony Wykonawcy realizowane było przez wyznaczonych przez niego Inżynierów, którzy posiadają akredytację/certyfikację producenta, dostarczonych przez Wykonawcę urządzeń, do pracy z tymi urządzeniami, np. Inżyniera CCNP, CCNE (w przypadku dostarczenie przez Wykponawcę urządzeń marki CISCO)

1.1. Zamawiający wymaga, aby Inżynierowie Wykonawcy (wytypowani do wsparcia Zamawiajacego) posiadali certyfikację producenta urządzeń na 2 poziomach:

1.1.1. Najwyższą dostępną certyfikację przewidzianą przez producenta, a niezbędną do obsługi urządzeń sieciowych

1.1.2. Certyfikację na poziomie o jeden stopień niższy (wg producenta urządzeń) niż najwyższy stopień certyfikacji, o którym mowa w ust. 1.1.1. powyżej, a niezbędną do obsługi urządzeń sieciowych

2. W przypadku przekazania przez Zamawiającego informacji o wystąpieniu awarii urządzeń, Wykonawca zapewni wsparcie swojego Inżyniera, którego zadaniem będzie: diagnoza zgłoszonej awarii, określenie sposobu usunięcia awarii, a następnie usunięcie awarii.

2.1. Wykonawca zobowiązany jest zapewnić wsparcie Inżyniera, którego zakres wiedzy (potwierdzony stosownym certyfikatem producenta urządzeń) okaże się wystarczający, do usunięcia awarii (diagnostyka, zidentyfikowanie przyczyny awarii, usunięcia awarii).

2.1.1. Jeżeli poziom certyfikacji danego Inżyniera będzie nie wystarczający do usunięcia ustarki i rozwiązania problemu, Wykonawca zapewni Zamawiającemy wsparcie techniczne innego Inżyniera, którego poziom certyfikacji będzie uznawany przez producenta urządzenia, jako wyższy

3. Czas reakcji Wykonawcy na zgłoszoną przez Zamawiającego awarię/usterkę nie może przekroczyć 1 godziny

3.1. Działania serwisowe i wsparcia technicznego Wykonawcy muszą zostać podjęte w terminie nieprzekraczającym 1 godziny, od momentu zgłoszenia awarii przez Zamawiającego – z zastrzeżeniem, że w przypadku awarii zgłoszonych przez Zamawiającego po godzinie 15:00, do świadczenia Usług Wykonawca przystąpi o godz. 8:00 następnego dnia roboczego;

3.2. W przypadku zgłoszeń wykonanych przez Zamawiajacego w dni ustatowo wolne od pracy, do świadczenia Usług Wsparcia Wykonawca przystąpi o godz. 8:00 w pierwszym dniu roboczym, jaki nastąpi po dniu wolnym od pracy;

4. Wymagana przez Zamawiającego Usługa Wsparcia, musi mieć formę wsparcia „8x5xNBD", czyli:

4.1. Obsługa zgłoszeń serwisowych w dni robocze (w godz. 8:00 – 15:00);

4.2. Czas reakcji na zgłoszenie Zamawiajacego - maksymalnie 1 godzina;

4.3. Usunięcie awarii (przywrócenie pełnej sprawności urządzenia lub oprogramowania)

5. Zamawiający wymaga, aby w przypadku awarii urządzenia:

5.1. Wykonawca naprawił urządzenie Zamawiającego własnymi staraniami i przywrócił je do pełnej sprawności technicznej i funkcjonalnej (przywrócenie sprawności elementów hardware i software).

5.2. Na czas naprawy urządzenia, które uległo awarii, Wykonawca dostarczy Zamawiającemu zamienne, sprawne urządzenie o parametrach i funkcjonalności nie gorszej niż urządzenie które uległo awarii.

5.3. Po naprawie urządzenia Zamawiającego Wykonawca zainstaluje naprawione urządzenie w lokalizacji wskazanej przez Zmawiającego.

5.4. W przypadku kiedy naprawa urządzenia Zamawiającego, przez Wykonawcę będzie niemożliwa, Wykonawca przekaże nieodpłatnie na rzecz i do dyspozycji Zamawiającego fabrycznie nowe urządzenie tej samej klasy (urządzenie o parametrach i funkcjonalności nie gorszej niż urządzenie które uległo awarii – urządzenie tego samego producenta). Urządzenie zostanie wpisane na stan środków trwałych Zamawiającego i będzie stanowiło jego własność (zamiennie za urządzenie które uległo awarii).

5.5. Urządzenie zastępcze przekazane przez Wykonawcę Zamawiającemu – o którym mowa w ust. 2.4 powyżej, musi być objęte Usługą Wsparcia do czasu zakończenia obowiązywania Umowy i jednocześnie wykupiony na to urządzenie musi zostać Kontrakt Serwisowy (na warunkach nie gorszych niż te wskazane w OPZ).

6. Zamawiający przewiduje możliwość świadczenia Usługi Wsparcia zdalnie lub telefoniczne, jednak jeżeli taka forma kontaktu okaże się niewystarczające do: stwierdzenia przyczyn awarii, określenia sposobu usunięcia awarii i usunięcia awarii, inżynier Wykonawcy zobowiązany jest do niezwłocznego przyjazdu na miejsce wystąpienia awarii i wymiany urządzenia. Decyzję o konieczności przyjazdu Wykonawcy na miejsce, w którym wystąpiła awaria urządzenia, podejmuje uprawniony pracownik Zamawiającego, wskazany w Umowie;

7. W przypadku konieczności realizacji Usługi w obiektach technicznych Zamawiającego, koniecznym jest umówienie takiej wizyty - daty i godziny przyjazdu przedstawiciela Wykonawcy, z uprawnionym pracownikiem Zamawiającego;

8. Diagnostyka uszkodzonego i/lub nie w pełni funkcjonalnego urządzenia przez Wykonawcę nie może trwać dłużej niż 24 godziny, liczonych od daty kiedy wysłano przez Zamawiającego zgłoszenie z informacją o uszkodzonym i/lub nie w pełni funkcjonalnym urządzeniu. W tym przedziale czasowym (w ciągu 24 godziny od wysłania zgłoszenia) Wykonawca zobowiązany jest do poinformowania Zamawiającego o sposobie usunięcia awarii urządzenia. Jeżeli w ciągu 24 godzin, od daty zgłoszenia awarii przez Zamawiającego, nie uda się zidentyfikować przyczyny awarii i jej usunąć, Wykonawca zobowiązany jest do wymiany urządzenia na zastępcze wolne od wad (w ramach Usługi Wsparcia lub Kontraktu Serwisowego);

9. Jeżeli usunięcie awarii będzie wymagało wymiany urządzenia, Wykonawca zobowiązany jest do przekazania Zamawiającemu informacji o konieczności wymiany urządzenia (na zastępcze) nie później niż ciągu 5 godzin po zakończonej diagnostyce urządzenia – z zastrzeżeniem o którym mowa w pkt. 5 powyżej;

10. Jeżeli usunięcie awarii możliwe będzie do zrealizowania bez konieczności wymiany urządzenia wadliwego na zastępcze, Wykonawca zobowiązany będzie usunąć awarię nie później niż ciągu 10 godzin po zakończonej diagnostyce urządzenia – z zastrzeżeniem, o którym mowa w pkt. 5 powyżej;

11. Jeżeli Póba Usunięcia Awarii Urządzenia nie przyniesie oczekiwanych rezultatów, Wykonawca zobowiązany jest w ciągu 8 godzin – liczonych od Daty wykonania pierwszej Próby usunięcia awarii urządzenia, wymienić urządzenie na zastępcze (w ramach Usługi Wsparcia lub Kontraktu Serwisowego);

12. Wykonawca gwarantuje, iż w przypadku konieczności wymiany wadliwego urządzenia na zastępcze (wolne od wad) zostanie to dokonane nie później niż w ciągu 24 godzin od daty zakończenia procedury diagnostycznej lub do godziny 17:00 kolejnego dnia roboczego (w zależności który z tych terminów wystąpi później).
13. Wymiany urządzenia wadliwego, w ramach Usługi Wsparcia, dokona Inżynier Wykonawcy;
14. Wymiana urządzenia, jego uruchomienie zapewniające przywrócenie pierwotnej funkcjonalności sieci teleinformatycznej Zamawiającego - sprzed awarii, dokonane zostanie nie później niż do godziny 24:00 trzeciego dnia roboczego liczonego od dnia, w którym Zamawiający zgłosił Wykonawcy awarię.
15. Serwis i wsparcie techniczne dla urządzenia, dostarczonego w miejsce urządzenia wadliwego, świadczone będzie na warunkach określonych w ramach Usługi Wsparcia do końca obowiązywania Umowy.
16. Termin rozpoczęcia usuwania awarii (w ramach Usługi Wsparcia) wymaga każdorazowego uzgodnienia z Zamawiającym. Termin ten może zostać przesunięty przez Zamawiającego z przyczyn operacyjnych związanych z bezpieczeństwem ruchu lotniczego. W takim przypadku termin usunięcia awarii ulegnie odpowiedniemu wydłużeniu, o czym Zamawiający powiadomi Wykonawcę telefonicznie (potwierdzając niezwłocznie e-mailem), lub pocztą elektroniczną;
17. Realizacja Przedmiotu Zamówienia musi być świadczona w taki sposób, aby nie zostały utracone gwarancje udzielone przez producentów innych urządzeń na: powiązane podzespoły urządzeń, inne urządzenia pracujące w sieci Zamawiającego, inne elementy aktywne i pasywne tworzące infrastrukturę teleinformatyczną Zamawiającego, w trakcie świadczenia Usługi przez Wykonawcę;
18. W ramach Usługi Wsparcia, Zamawiający zastrzega sobie prawo do kontaktu z Wykonawcą w celu obsługi bieżących problemów z funkcjonowaniem dostarczonych urządzeń, jak również w przypadku konieczności zwiększenia ich funkcjonalności i tym samym zmianą ich konfiuracji

C. Minimalne wymagania wobec warunków Kontraktów Serwisowych

1. Zakres Kontraktów Serwisowych musi wynikać z oferty serwisowej producenta dostarczonych urządzeń
2. Kontrakty Serwisowe muszą przewidywać min. 48 miesięcy obsługi urządzeń, dla których kontrakt został zawarty
3. Kontrakt Serwisowy musi zapewniać Zamawiajacemu:
   - 3.1. Dostęp do technicznego centrum wsparcia producenta dostarczonych urządzeń, np. tyu: Cisco Technical TAC, przez dwadzieścia cztery (24) godziny na dobę, siedem (7) dni w tygodniu.
     - 3.1.1. Czasy odpowiedzi dla połączeń o poziomach ważności 1 i 2 nie może przekraczać (1) godziny.
     - 3.1.2. Czasy reakcji dla połączeń o poziomach ważności 3 i 4: W godzinach pracy centrum wsparcia techniciznego - w ciągu jednej (1) godziny.
     - 3.1.3. W dni wolne od pracy - w ciągu następnego dnia roboczego w godzinach pracy
   - 3.2. Dostęp do portalu, który zapewni Zamawiającemu wgląd w informacje techniczne na temat dostarczonych w ramach zamówienia urządzeń, w tym aktualnego oprogramowania i poprawek dla tych urządzeń,
   - 3.3. Dostęp do portalu, który zapewni Zamawiającemu możliwość wymiany informacji z grupą użytkowników produktów producenta dostarczonych urządzeń.
   - 3.4. Dostęp do portalu samoobsługowego, który zapewni Zamawiającemu wgląd w informacje nt. raportów z funkcjonowania urządzeń, aplikacji (w celu zarządzania uprawnieniami do usług i innymi funkcjami) oraz innego oprogramowania (w celu zbierania informacji dotyczących konfiguracji i inwentaryzacji zainstalowanych produktów producenta dostarczonych urządzeń)
   - 3.5. Możliwość aktualizacji systemu operacyjnego urządzeń, obejście problemu lub dostęp do poprawki dla zgłoszonych problemów z oprogramowaniem
   - 3.6. Możliwość aktualizacji oprogramowania urządzeń, która to konieczność może wyniknąć z kontaktu z centrum wsparcia technicznego producenta i np. po zgłoszenia producentowi problemów
   - 3.7. Dostęp do dokumentacji i każdej wersji oprogramowania dedykowanego dla danego urządzenia objętego Kontraktem Serwisowym
   - 3.8. Dostęp do narzędzia, którym producent urządzenia zbiera informacje nt. funkcjonowania swoich urządzeń (poprawności lub awarii urządzeń)
   - 3.9. Wymianę części i modułów w dostarczonych urządzeniach Zamawiającemu
4. Usługi serwisowe w ramach Kontraktu Serwisowego muszą być świadczone w miejscu zainstalowanai urządzeń Zamawiajacego,

5. Kontrakt Serwisowy musi zapewniać wymiane uszkodzonych i nie właściwie funkcjonujących urządzeń ew. ich modułów na nowe

6. Kontrakty Serwisowe muszą mieć formę wsparcia „8x5xNBD", czyli:
   6.1. Obsługa zgłoszeń serwisowych w dni robocze (w godz. 8:00 – 15:00);
   6.2. Czas reakcji na zgłoszenie Zamawiajacego - maksymalnie 1 godzina;
   6.3. Usunięcie awarii (przywrócenie pełnej sprawności urządzenia lub oprogramowania)

III
Wymagania dla Części III
- Urządzenia odpowiedzialne za bezpieczeństwo sieci LAN

A. Wymagania podstawowe

1. Zamawiajacy wymaga aby dostarczone do niego urządzenia objęte były opieką serwisową w ramach:
   1.1. **Kontraktu serwisowego,** dedykowanych przez producenta urządzeń (dotyczy każdego dostarczonego w ramach Umowy urządzenia) – usługa świadczona bezpośrednio przez Producenta lub pośrednio przez jego oficjalnego przedstawiciela (zgodnie z warunkami określonymi przez producenta urządzeń w Kontrakcie Serwisowym)
   1.2. **Usługi wsparcia Wykonawcy dla** urządzeń dostarczonych w ramach Umowy – usługa świadczona bezpośrednio przez Wykonawcę
2. Okres trwania Usługi
   2.1. Kontrakt Serwisowy – 48 mc.
      2.1.1. Okres obowiązywania Kontraktów Serwisowych liczony będzie od dnia Podpisania Protokołów Zdawczo – Odbiorczych przez Zamawiajacego, dedykowanego dla konkretnej dostawy urządzeń (zgodnie z wymaganiami OPZ Rozdział 7 ust. 4.3)
   2.2. Sparcie Techniczne Wykonawcy - 48 mc.
      2.2.1. Okres obowiązywania Wsparcia Wykonawcy liczony będzie od dnia Podpisania Protokołów Zdawczo – Odbiorczych przez Zamawiajacego, dla pierwszej partii dostarczonych urządzeń (niezależnie od terminu dostawy kolejnej partii urządzeń wskazanej w OPZ Rozdział 7 ust. 4.3)
3. W przypadku awarii urządzeń objętych jednocześnie Usługą Wsparcia i Kontraktem Serwisowym, nadrzędnym sposobem naprawy urządzeń Zamawiającego jest ten określony w Kontrakcie Serwisowym producenta. Tym samym, sposób (gdzie jako, „sposób naprawy", należy rozumieć wymianę uszkodzonego urządzenia lub jego naprawę) naprawy usterki/awarii urządzeń Zamawiającego, zdefiniowany w Kontrakcie Serwisowym, ma pierwszeństwo w zastosowaniu przed zobowiązaniami nałożonymi na Wykonawcę.
4. Zamawiający zastrzega, że wybór drogi obsługi serwisowej urządzenia nie zwalnia Wykonawcy ze zobowiązań terminowych wskazanych w OPZ (Rozdział 5). Tym samym zobowiązania terminowe wskazane w OPZ (Rozdział 5) mają pierwszeństwo nad tymi określonymi w Kontrakcie Serwisowym producenta.

B. Wymagania wobec Usługi Wsparcia realizowanej przez Wykonawcę

1. Zamawiający wymaga, aby Usługa Wsparcia ze strony Wykonawcy realizowane było przez wyznaczonych przez niego Inżynierów, którzy posiadają akredytację/certyfikację producenta, dostarczonych przez Wykonawcę urządzeń, do pracy z tymi urządzeniami, np. Inżyniera CCNP, CCNE (w przypadku dostarczenie przez Wykponawcę urządzeń marki CISCO)

    1.1. Zamawiający wymaga, aby Inżynierowie Wykonawcy (wytypowani do wsparcia Zamawiajacego) posiadali certyfikację producenta urządzeń na 2 poziomach:

        1.1.1. Najwyższą dostępną certyfikację przewidzianą przez producenta, a niezbędną do obsługi urządzeń sieciowych

        1.1.2. Certyfikację na poziomie o jeden stopień niższy (wg producenta urządzeń) niż najwyższy stopień certyfikacji, o którym mowa w ust. 1.1.1. powyżej, a niezbędną do obsługi urządzeń sieciowych

2. W przypadku przekazania przez Zamawiającego informacji o wystąpieniu awarii urządzeń, Wykonawca zapewni wsparcie swojego Inżyniera, którego zadaniem będzie: diagnoza zgłoszonej awarii, określenie sposobu usunięcia awarii, a następnie usunięcie awarii.

    2.1. Wykonawca zobowiązany jest zapewnić wsparcie Inżyniera, którego zakres wiedzy (potwierdzony stosownym certyfikatem producenta urządzeń) okaże się wystarczający, do usunięcia awarii (diagnostyka, zidentyfikowanie przyczyny awarii, usunięcia awarii).

        2.1.1. Jeżeli poziom certyfikacji danego Inżyniera będzie nie wystarczający do usunięcia ustarki i rozwiązania problemu, Wykonawca zapewni Zamawiającemy wsparcie techniczne innego Inżyniera, którego poziom certyfikacji będzie uznawany przez producenta urządzenia, jako wyższy

3. Czas reakcji Wykonawcy na zgłoszoną przez Zamawiającego awarię/usterkę nie może przekroczyć 1 godziny

    3.1. Działania serwisowe i wsparcia technicznego Wykonawcy muszą zostać podjęte w terminie nieprzekraczającym 1 godziny, od momentu zgłoszenia awarii przez Zamawiającego – z zastrzeżeniem, że w przypadku awarii zgłoszonych przez Zamawiającego po godzinie 15:00, do świadczenia Usług Wykonawca przystąpi o godz. 8:00 następnego dnia roboczego;

    3.2. W przypadku zgłoszeń wykonanych przez Zamawiajacego w dni ustatowo wolne od pracy, do świadczenia Usług Wsparcia Wykonawca przystąpi o godz. 8:00 w pierwszym dniu roboczym, jaki nastąpi po dniu wolnym od pracy;

4. Wymagana przez Zamawiającego Usługa Wsparcia, musi mieć formę wsparcia „8x5xNBD", czyli:

    4.1. Obsługa zgłoszeń serwisowych w dni robocze (w godz. 8:00 – 15:00);

    4.2. Czas reakcji na zgłoszenie Zamawiajacego - maksymalnie 1 godzina;

    4.3. Usunięcie awarii (przywrócenie pełnej sprawności urządzenia lub oprogramowania)

5. Zamawiający wymaga, aby w przypadku awarii urządzenia:

   5.1. Wykonawca naprawił urządzenie Zamawiającego własnymi staraniami i przywrócił je do pełnej sprawności technicznej i funkcjonalnej (przywrócenie sprawności elementów hardware i software).

   5.2. Na czas naprawy urządzenia, które uległo awarii, Wykonawca dostarczy Zamawiającemu zamienne, sprawne urządzenie o parametrach i funkcjonalności nie gorszej niż urządzenie które uległo awarii.

   5.3. Po naprawie urządzenia Zamawiającego Wykonawca zainstaluje naprawione urządzenie w lokalizacji wskazanej przez Zmawiającego.

   5.4. W przypadku kiedy naprawa urządzenia Zamawiającego, przez Wykonawcę będzie niemożliwa, Wykonawca przekaże nieodpłatnie na rzecz i do dyspozycji Zamawiającego fabrycznie nowe urządzenie tej samej klasy (urządzenie o parametrach i funkcjonalności nie gorszej niż urządzenie które uległo awarii – urządzenie tego samego producenta). Urządzenie zostanie wpisane na stan środków trwałych Zamawiającego i będzie stanowiło jego własność (zamiennie za urządzenie które uległo awarii).

   5.5. Urządzenie zastępcze przekazane przez Wykonawcę Zamawiającemu – o którym mowa w ust. 2.4 powyżej, musi być objęte Usługą Wsparcia do czasu zakończenia obowiązywania Umowy i jednocześnie wykupiony na to urządzenie musi zostać Kontrakt Serwisowy (na warunkach nie gorszych niż te wskazane w OPZ).

6. Zamawiający przewiduje możliwość świadczenia Usługi Wsparcia zdalnie lub telefoniczne, jednak jeżeli taka forma kontaktu okaże się niewystarczające do: stwierdzenia przyczyn awarii, określenia sposobu usunięcia awarii i usunięcia awarii, inżynier Wykonawcy zobowiązany jest do niezwłocznego przyjazdu na miejsce wystąpienia awarii i wymiany urządzenia. Decyzję o konieczności przyjazdu Wykonawcy na miejsce, w którym wystąpiła awaria urządzenia, podejmuje uprawniony pracownik Zamawiającego, wskazany w Umowie;

7. W przypadku konieczności realizacji Usługi w obiektach technicznych Zamawiającego, koniecznym jest umówienie takiej wizyty - daty i godziny przyjazdu przedstawiciela Wykonawcy, z uprawnionym pracownikiem Zamawiającego;

8. Diagnostyka uszkodzonego i/lub nie w pełni funkcjonalnego urządzenia przez Wykonawcę nie może trwać dłużej niż 24 godziny, liczonych od daty kiedy wysłano przez Zamawiającego zgłoszenie z informacją o uszkodzonym i/lub nie w pełni funkcjonalnym urządzeniu. W tym przedziale czasowym (w ciągu 24 godziny od wysłania zgłoszenia) Wykonawca zobowiązany jest do poinformowania Zamawiającego o sposobie usunięcia awarii urządzenia. Jeżeli w ciągu 24 godzin, od daty zgłoszenia awarii przez Zamawiającego, nie uda się zidentyfikować przyczyny awarii i jej usunąć, Wykonawca zobowiązany jest do wymiany urządzenia na zastępcze wolne od wad (w ramach Usługi Wsparcia lub Kontraktu Serwisowego);

9. Jeżeli usunięcie awarii będzie wymagało wymiany urządzenia, Wykonawca zobowiązany jest do przekazania Zamawiającemu informacji o konieczności wymiany urządzenia (na zastępcze) nie później niż ciągu 5 godzin po zakończonej diagnostyce urządzenia – z zastrzeżeniem o którym mowa w pkt. 5 powyżej;

10. Jeżeli usunięcie awarii możliwe będzie do zrealizowania bez konieczności wymiany urządzenia wadliwego na zastępcze, Wykonawca zobowiązany będzie usunąć awarię nie później niż ciągu 10 godzin po zakończonej diagnostyce urządzenia – z zastrzeżeniem, o którym mowa w pkt. 5 powyżej;
11. Jeżeli Póba Usunięcia Awarii Urządzenia nie przyniesie oczekiwanych rezultatów, Wykonawca zobowiązany jest w ciągu 8 godzin – liczonych od Daty wykonania pierwszej Próby usunięcia awarii urządzenia, wymienić urządzenie na zastępcze (w ramach Usługi Wsparcia lub Kontraktu Serwisowego);
12. Wykonawca gwarantuje, iż w przypadku konieczności wymiany wadliwego urządzenia na zastępcze (wolne od wad) zostanie to dokonane nie później niż w ciągu 24 godzin od daty zakończenia procedury diagnostycznej lub do godziny 17:00 kolejnego dnia roboczego (w zależności który z tych terminów wystąpi później).
13. Wymiany urządzenia wadliwego, w ramach Usługi Wsparcia, dokona Inżynier Wykonawcy;
14. Wymiana urządzenia, jego uruchomienie zapewniające przywrócenie pierwotnej funkcjonalności sieci teleinformatycznej Zamawiającego - sprzed awarii, dokonane zostanie nie później niż do godziny 24:00 trzeciego dnia roboczego liczonego od dnia, w którym Zamawiający zgłosił Wykonawcy awarię.
15. Serwis i wsparcie techniczne dla urządzenia, dostarczonego w miejsce urządzenia wadliwego, świadczone będzie na warunkach określonych w ramach Usługi Wsparcia do końca obowiązywania Umowy.
16. Termin rozpoczęcia usuwania awarii (w ramach Usługi Wsparcia) wymaga każdorazowego uzgodnienia z Zamawiającym. Termin ten może zostać przesunięty przez Zamawiającego z przyczyn operacyjnych związanych z bezpieczeństwem ruchu lotniczego. W takim przypadku termin usunięcia awarii ulegnie odpowiedniemu wydłużeniu, o czym Zamawiający powiadomi Wykonawcę telefonicznie (potwierdzając niezwłocznie e-mailem), lub pocztą elektroniczną;
17. Realizacja Przedmiotu Zamówienia musi być świadczona w taki sposób, aby nie zostały utracone gwarancje udzielone przez producentów innych urządzeń na: powiązane podzespoły urządzeń, inne urządzenia pracujące w sieci Zamawiającego, inne elementy aktywne i pasywne tworzące infrastrukturę teleinformatyczną Zamawiającego, w trakcie świadczenia Usługi przez Wykonawcę;
18. W ramach Usługi Wsparcia, Zamawiający zastrzega sobie prawo do kontaktu z Wykonawcą w celu obsługi bieżących problemów z funkcjonowaniem dostarczonych urządzeń, jak również w przypadku konieczności zwiększenia ich funkcjonalności i tym samym zmianą ich konfiuracji

C. Minimalne wymagania wobec warunków Kontraktów Serwisowych

1. Zakres Kontraktów Serwisowych musi wynikać z oferty serwisowej producenta dostarczonych urządzeń
2. Kontrakty Serwisowe muszą przewidywać min. 48 miesięcy obsługi urządzeń, dla których kontrakt został zawarty
3. Kontrakt Serwisowy musi zapewniać Zamawiajacemu:
   - 3.1. Dostęp do wsparcia producenta urządzeń w trybie 24h 7 dni w tygodniu 365 dni w roku
   - 3.2. Reakcja producenta na zgłoszoną przez Zamawiajaćego awarię lub problem:
     - 3.2.1. Poniżej 1h (z aktualizacją zgłoszenia co 4h, aż do rozwiązania zgłoszenia) – dla zgłoszeń dotyczących urządzeń niezdolnych do całkowitego działania oraz kiedy środowisko produkcyjne jest krytycznie dotknięte awarią.
     - 3.2.2. Do 2h (z aktualizacją zgłoszenia co 1 dzień roboczy, aż do rozwiązania zgłoszenia) - dla zgłoszeń dotyczących urządzeń częściowo uszkodzony oraz kiedyśrodowisko produkcyjne jest częściowo dotknięte problemem.
     - 3.2.3. Do 4h (z aktualizacją zgłoszenia co 3 dni robocze, aż do rozwiązania zgłoszenia) - dla zgłoszeń dotyczących urządzeń kiedy jedna z funkcji urządzenia nie działa, ale środowisko produkcyjne nie jest dotknięte problemem. Support producenta jest świadomy problemu i zostało zaproponowane/wdrożonerozwiązanie zastępcze
     - 3.2.4. Do 8h (z aktualizacją zgłoszenia raz na tydzień, aż do rozwiązania zgłoszenia) – dla zdarzenie niskiej krytyczności, kiedy awaria nie dotyka środowiska produkcyjnego. Zapytanie Zmawiajacego dotyczy dokumentacji, opisu funkcji, przewodnika konfiguracyjny, zalecanej wersji oprogramowania
   - 3.3. Pomoc producenta urządzenia przy tzw. „śledztwach bezpieczeństwa”
   - 3.4. Zaawansowanej analizie logów oraz IOC
   - 3.5. Rekomendacji dot. zastosowania procedur i rozwiązań zwiększających bezpieczeństo środowiska sieciowego
   - 3.6. Dostęp do najnowszej wersji oprogramowania oraz poraweg dla urzdzeń Zamawiajacego
   - 3.7. Dostęp do portalu online do zgłaszania problemów, który pozwala zakładać, prowadzić oraz eskalować zgłoszenia serwisowe
   - 3.8. Zarządzania zgłoszeniami: zakładanie, aktualizacja, sprawdznie statusu i zarządzanie zgłoszeniami poprzez portal online
   - 3.9. Dostęp do do przewodników konfiguracyjnych, wytycznych technicznych, informacji o nowych wersjach oprogramowania wraz ze zmianami, które wprowadzają (release notes) oraz do FAQ aby przyśpieszyć i ułatwić rozwiązywanie problemów

Rozdział 6
Wymagania dla Urządzeń Sieciowych względem Cyberbezpieczeństwa

I
Wymagania z zakresu Cyberbezpieczeństwa dla Części I

Wymagania bezpieczeństwa dla urządzeń		
Kategoria wymagania	Szczegóły wymagania	Uwagi
Monitoring bezpieczeństwa	System operacyjny urządzenia musi spełniać minimalny zestaw wymaganych zdarzeń rejestrowania i monitorowania zgodnie ze standardem klienta: - Zdarzenia logowania i wylogowania są logowane, - Błędy uwierzytelniania są logowane, - Nadawanie i odbieranie uprawnień jest logowane, - Zmiany poziomów logowania komponentów aplikacji oraz systemów zależnych są logowane, - Włączenie lub wyłączenie logowania jest logowane, - usunięcie zawartości dziennika logów jest logowane, - Dziennik audytu powinien być chroniony przed nieautoryzowaną modyfikacją i usunięciem, - Dziennik audytu może dostarczać logi w czasie rzeczywistym do zewnętrznego systemu SIEM lub systemu zarządzania dziennikami.	
Mechanizmy enkrypcji	Wszelkie hasła przechowywane w tabelach bazy danych, plikach konfiguracyjnych, skryptach automatycznego logowania, plikach wsadowych i makrach oprogramowania są szyfrowane lub haszowane (szyfrowanie jednokierunkowe).	
Mechanizmy enkrypcji	Szyfrowanie jest używane do przesyłania wszystkich haseł.	
Mechanizmy enkrypcji	System przechowuje dane zaszyfrowane.	
Mechanizmy enkrypcji	Wszelka komunikacja między aplikacją a użytkownikiem końcowym jest szyfrowana.	
Proces logowania	Każdy proces logowania zawiera specjalną informację. Powiadomienie to musi określać: (1) system ma być używany wyłącznie przez autoryzowanych użytkowników oraz (2) kontynuując korzystanie z systemu użytkownik oświadcza, że jest autoryzowanym użytkownikiem (3) wszystkie działania użytkownika są zarejestrowane i ewentualnie monitorowane.	
Proces logowania	W przypadku braku aktywności użytkownika przez okres piętnastu (15) minut system operacyjny urządzenia musi automatycznie wylogować użytkownika. Ponowne nawiązanie sesji musi nastąpić dopiero po ponownym uwierzytelnieniu użytkownika.	

II
Wymagania z zakresu Cyberbezpieczeństwa dla Części II

Wymagania bezpieczeństwa dla urządzeń		
Kategoria wymagania	Szczegóły wymagania	Uwagi
Monitoring bezpieczeństwa	System operacyjny urządzenia musi spełniać minimalny zestaw wymaganych zdarzeń rejestrowania i monitorowania zgodnie ze standardem klienta: - Zdarzenia logowania i wylogowania są logowane, - Błędy uwierzytelniania są logowane, - Nadawanie i odbieranie uprawnień jest logowane, - Zmiany poziomów logowania komponentów aplikacji oraz systemów zależnych są logowane, - Włączenie lub wyłączenie logowania jest logowane, - usunięcie zawartości dziennika logów jest logowane, - Dziennik audytu powinien być chroniony przed nieautoryzowaną modyfikacją i usunięciem, - Dziennik audytu może dostarczać logi w czasie rzeczywistym do zewnętrznego systemu SIEM lub systemu zarządzania dziennikami.	
Mechanizmy enkrypcji	Wszelkie hasła przechowywane w tabelach bazy danych, plikach konfiguracyjnych, skryptach automatycznego logowania, plikach wsadowych i makrach oprogramowania są szyfrowane lub haszowane (szyfrowanie jednokierunkowe).	
Mechanizmy enkrypcji	Szyfrowanie jest używane do przesyłania wszystkich haseł.	
Mechanizmy enkrypcji	System przechowuje dane zaszyfrowane.	
Mechanizmy enkrypcji	Wszelka komunikacja między aplikacją a użytkownikiem końcowym jest szyfrowana.	
Proces logowania	Każdy proces logowania zawiera specjalną informację. Powiadomienie to musi określać: (1) system ma być używany wyłącznie przez autoryzowanych użytkowników oraz (2) kontynuując korzystanie z systemu użytkownik oświadcza, że jest autoryzowanym użytkownikiem (3) wszystkie działania użytkownika są zarejestrowane i ewentualnie monitorowane.	
Proces logowania	W przypadku braku aktywności użytkownika przez okres piętnastu (15) minut system operacyjny urządzenia musi automatycznie wylogować użytkownika. Ponowne nawiązanie sesji musi nastąpić dopiero po ponownym uwierzytelnieniu użytkownika.	

III
Wymagania z zakresu Cyberbezpieczeństwa dla Części III

Wymagania bezpieczeństwa dla urządzeń		
Kategoria wymagania	Szczegóły wymagania	Uwagi
Monitoring bezpieczeństwa	System operacyjny urządzenia musi spełniać minimalny zestaw wymaganych zdarzeń rejestrowania i monitorowania zgodnie ze standardem klienta: - Zdarzenia logowania i wylogowania są logowane, - Błędy uwierzytelniania są logowane, - Nadawanie i odbieranie uprawnień jest logowane, - Zmiany poziomów logowania komponentów aplikacji oraz systemów zależnych są logowane, - Włączenie lub wyłączenie logowania jest logowane, - usunięcie zawartości dziennika logów jest logowane, - Dziennik audytu powinien być chroniony przed nieautoryzowaną modyfikacją i usunięciem, - Dziennik audytu może dostarczać logi w czasie rzeczywistym do zewnętrznego systemu SIEM lub systemu zarządzania dziennikami.	
Mechanizmy enkrypcji	Wszelkie hasła przechowywane w tabelach bazy danych, plikach konfiguracyjnych, skryptach automatycznego logowania, plikach wsadowych i makrach oprogramowania są szyfrowane lub haszowane (szyfrowanie jednokierunkowe).	
Mechanizmy enkrypcji	Szyfrowanie jest używane do przesyłania wszystkich haseł.	
Mechanizmy enkrypcji	System przechowuje dane zaszyfrowane.	
Mechanizmy enkrypcji	Wszelka komunikacja między aplikacją a użytkownikiem końcowym jest szyfrowana.	
Proces logowania	Każdy proces logowania zawiera specjalną informację. Powiadomienie to musi określać: (1) system ma być używany wyłącznie przez autoryzowanych użytkowników oraz (2) kontynuując korzystanie z systemu użytkownik oświadcza, że jest autoryzowanym użytkownikiem (3) wszystkie działania użytkownika są zarejestrowane i ewentualnie monitorowane.	
Proces logowania	W przypadku braku aktywności użytkownika przez okres piętnastu (15) minut system operacyjny urządzenia musi automatycznie wylogować użytkownika. Ponowne nawiązanie sesji musi nastąpić dopiero po ponownym uwierzytelnieniu użytkownika.	

Rozdział 7
Fakturowanie i rozliczenie

1. Urządzenia należy dostarczyć do:
   - 1.1. Dotyczy Części I
     - 1.1.1. Do 01.12.2024
   - 1.2. Dotyczy Części II
     - 1.2.1. Do 01.03.2025
   - 1.3. Dotyczy Części III
     - 1.3.1. Do 01.12.2024
     - 1.3.2. Do 01.03.2025
   - 1.4. Zamawiający zastrzega, że za dostarczone urządzenia będzie można uznać stan, kiedy Zamawiający zweryfikuję dostarczone urządzenia pod kątem ich zgodności z ofertą oraz podpisze Protokół Zdawczo – Odbiorczy
     - 1.4.1. Zamawiający rezerwuje dla siebie 10 dni roboczych na weryfikację przekazanych urządzeń na zgodność z ofertą, liczonych od dnia przekazania ostatniego urządzenia wymaganego OPZ
2. Potwierdzenia zawarcia Kontraktów Serwisowych (wystawione przez producenta urządzeń) na dostarczone Zamawiającemu urządzenia (w ramach Części I, Części II, Części III) należy dostarczyć Zamawiajacemu nie później niż 10 dni kalendarzowych od podpisania Protokołów Zdawczo-Odbiorczych, o których mowa w ust. 1 powyżej
3. W Zamawiający wymaga, aby oferta przekazana przez Wykonawcę obejmowała następujące pozycje wraz z ich wartością/wyceną:
   - 3.1. Dotyczy Części I
     - 3.1.1. Urządzenia
     - 3.1.2. Usługa Wsparcia Wykonawcy
     - 3.1.3. Kontrakt Serwisowy
   - 3.2. Dotyczy Części II
     - 3.2.1. Urządzenia
     - 3.2.2. Usługa Wsparcia Wykonawcy
     - 3.2.3. Kontrakt Serwisowy

3.3. Dotyczy Części III

3.3.1. Urządzenia

3.3.2. Usługa Wsparcia Wykonawcy

3.3.3. Kontrakt Serwisowy

4. Faktury za dostarczone urządzenia i przypisane do nich urządzenia rozliczna będą w następujący sposób:

4.1. **Dotyczy Części I,**

4.1.1. Rok 2024:

4.1.1.1. Dostarczone Urzadzenia – 100% wartości oferty

4.1.1.2. Kontrakt Serwisowy – 25% wartości oferty

4.1.1.3. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.1.2. Rok 2025:

4.1.2.1. Kontrakt Serwisowy – 25% wartości oferty

4.1.2.2. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.1.3. Rok 2026:

4.1.3.1. Kontrakt Serwisowy – 25% wartości oferty

4.1.3.2. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.1.4. Rok 2027:

4.1.4.1. Kontrakt Serwisowy – 25% wartości oferty

4.1.4.2. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.2. **Dotyczy Części II,**

4.2.1. Rok 2025:

4.2.1.1. Dostarczone Urzadzenia – 100% wartości oferty

4.2.1.2. Kontrakt Serwisowy – 25% wartości oferty

4.2.1.3. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.2.2. Rok 2026:

4.2.2.1. Kontrakt Serwisowy – 25% wartości oferty

4.2.2.2. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.2.3. Rok 2027:

4.2.3.1. Kontrakt Serwisowy – 25% wartości oferty

4.2.3.2. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.2.4. Rok 2028:

4.2.4.1. Kontrakt Serwisowy – 25% wartości oferty

4.2.4.2. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.3. **Dotyczy Części III,**

4.3.1. Rok 2024:

4.3.1.1. Dostarczone Urzadzenia – 60% wartości oferty

4.3.1.2. Kontrakt Serwisowy – 25% wartości oferty

4.3.1.3. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.3.2. Rok 2025:

4.3.2.1. Dostarczone Urzadzenia – 40% wartości oferty

4.3.2.2. Kontrakt Serwisowy – 25% wartości oferty

4.3.2.3. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.3.3. Rok 2026:

4.3.3.1. Kontrakt Serwisowy – 25% wartości oferty

4.3.3.2. Usługa Wsparcia Wykonawcy – 25% wartości oferty

4.3.4. Rok 2027:

4.3.4.1. Kontrakt Serwisowy – 25% wartości oferty

4.3.4.2. Usługa Wsparcia Wykonawcy – 25% wartości oferty