OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa infrastruktury sieciowej

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia jest rozbudowa infrastruktury sieciowej. Składająca się z następujących elementów:

1. dostawa systemu typu SDN;
2. dostawę 20 sztuk przełączników sieciowych typu access wraz z gwarancją na okres 60 miesięcy;
3. dostawę 8 przełączników typu datacenter wraz z gwarancją na okres 36 miesięcy.

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w następujących terminach:

1. W zakresie przedmiotu zamówienia dotyczącego dostawy systemu typu SDN:
   a) dostawa sprzętu oraz oprogramowania Systemu typu SDN oraz subskrypcji oprogramowania dla 6 przełączników typu Leaf - **w terminie maksymalnie do 35 dni od daty podpisania przez strony umowy** (termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym);
   b) wykonanie migracji obecnej architektury sieciowej do Systemu SDN - **w terminie do 30 dni od dnia odbioru wykonania dostawy określonej w ppkt 1;**
   c) **36 miesięcy od dnia realizacji zadania określonego w ppkt 2**, w zakresie świadczenie usługi asysty technicznej do dostarczonego Systemu SDN;
   d) **36 miesięcy od dnia wykonania zadań opisanych w pkt 1** w zakresie świadczenia usług gwarancyjnych.
2. W zakresie dostawy 20 sztuk przełączników sieciowych typu access wraz z gwarancją na okres 60 miesięcy – **w terminie maksymalnie do 60 dni od daty podpisania przez strony umowy** (termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym).
3. W zakresie dostaw 8 przełączników typu datacenter wraz z gwarancją na okres 36 miesięcy - w terminie **maksymalnie do 60 dni od daty podpisania przez strony umowy** (termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym).

Realizacja przedmiotu zamówienia, w tym dostawa urządzeń wraz z wdrożeniem dla Ministerstwa Rozwoju i Technologii nastąpi do siedziby Zamawiającego, przy Placu Trzech Krzyży 3/5 w Warszawie oraz do centrum przetwarzania na terenie Polski wskazanego przez Zamawiającego.

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Zaoferowane urządzenia oraz oprogramowanie nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.
2. Wszystkie elementy dostarczone z urządzeniami, będą pochodziły od jednego producenta. Stosowane elementy muszą być wspierane przez producenta urządzeń i być objęte możliwością analizy potencjalnych błędów w trakcie potencjalnych zgłoszeń serwisowych. Muszą pochodzić z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej.
3. Zaoferowane urządzenia muszą być fabrycznie nowe przeznaczone do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz.U. z 2004 r., nr 204, poz. 2087 j.t. z późn. zm.) i z wydanymi na jej podstawie rozporządzeniami), wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz objęte wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów „odnawianych" (ang. Refurbished). Zaoferowane urządzenia, oprogramowanie sterujące połączeniami oraz aplikacje zarządzające muszą pochodzić od tego samego producenta. Zamawiający wymaga, aby dostarczone urządzenia pochodziły z oficjalnego kanału dystrybucyjnego danego producenta, a serwis gwarancyjny był autoryzowany przez producenta urządzeń i oprogramowania oraz świadczony przez producenta lub autoryzowanych partnerów w centrach serwisowych na terenie Unii Europejskiej.

IV. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE W ZAKRESIE SYSTEMU SDN

Dostawa systemu typu SDN zostanie zrealizowana poprzez dostawę sprzętu klasy datacenter oraz oprogramowania Systemu typu SDN na który składają się:

1. 4 sztuki kontrolerów wraz z gwarancją na okres 36 miesięcy;
2. 4 sztuki przełączników typu Spine wraz z gwarancją na okres 36 miesięcy;
3. 4 sztuki przełączników typu Leaf wraz z gwarancją na okres 36 miesięcy;
4. dostawę subskrypcji oprogramowania na okres 36 miesięcy dla 4 sztuk przełączników typu Leaf posiadanych przez Zamawiającego.
5. wykonanie migracji obecnej architektury sieciowej do Systemu SDN.
6. usługi asysty technicznej do dostarczanego Systemu typu SDN.

Warunki techniczne:

1. **Kontroler SDN – klaster 4 sztuk kontrolerów**

Dostarczany system typu SDN musi składać się z klastra czterech węzłów sprzętowych (4 kontrolery) dla zapewnienia redundancji.

1. Kontroler SDN musi być zrealizowany w oparciu o dedykowaną warstwę sprzętową i programową.
2. Kontroler SDN musi być zrealizowany redundantnie zarówno w warstwie sprzętowej, jak i programowej tak, aby zapewnić spójne działanie środowiska i możliwość modyfikacji konfiguracji po ewentualnej utracie jednej z instancji.
3. Utrata wszystkich instancji kontrolera SDN nie może wpływać na działanie infrastruktury sieciowej w zakresie istniejącej konfiguracji (nie dotyczy to zmian lub np. podłączania nowych urządzeń).
4. Kontroler SDN musi posiadać możliwość jednoczesnej implementacji w dwóch lokalizacjach dla odległości co najmniej 150 km (np. w formie klastra złożonego z kilku instancji). W przypadku utraty komunikacji między lokalizacjami musi być możliwość dalszej modyfikacji konfiguracji przynajmniej dla jednej z lokalizacji (np. pierwszego ośrodka przetwarzania danych).
5. Możliwość modyfikacji konfiguracji musi być zapewniona także w scenariuszu całkowitej utraty dowolnej z dwóch lokalizacji. Wymagane jest w tym celu zapewnienie odpowiednich zasobów sprzętowych i mechanizmów software kontrolera SDN.
6. Komunikacja między kontrolerem SDN i elementami infrastruktury sieciowej (fabric) musi być prowadzona w trybie in-band, nie wymagającym użycia dedykowanych interfejsów na przełącznikach wchodzących w skład architektury.
7. Kontroler SDN musi obsługiwać wyłącznie ruch związany z zarządzaniem i monitorowaniem infrastruktury sieciowej (control plane), nie zajmuje się przełączaniem ruchu (data plane).
8. Kontroler SDN musi umożliwiać zarządzanie infrastrukturą sieciową dołączającą co najmniej 1200 portów fizycznych dla dołączania serwerów i innych usług.
9. Kontroler SDN musi umożliwiać zarządzanie infrastrukturą wirtualną złożoną z co najmniej 2000 maszyn wirtualnych VM.
10. Musi umożliwiać automatyzację konfigurowania zarządzanej sieci w oparciu o model sieciowych polityk grupowych powiązanych z aplikacjami.
11. Polityka definiowana na kontrolerze musi opisywać model działania aplikacji w oparciu o relacje pomiędzy punktami styku elementów aplikacji z siecią. W przykładowym modelu trójwarstwowym aplikacji oznacza to:
    a. zdefiniowanie segmentów (warstw aplikacji) takich jak np. web, aplikacyjna i bazodanowa (Web, App, DB), złożonych z grup fizycznych i wirtualnych serwerów oraz kontenerów Docker;
    b. określenie punktów styku takich jak VLAN, interfejsy serwerów (fizyczne lub wirtualna port-grupa), adresy IP – dla danego segmentu;
    c. zdefiniowanie przydziału serwera wirtualnego do danego segmentu na bazie jego atrybutów – nazwa maszyny VM, id maszyny VM, nazwa i wersja systemu operacyjnego, typ hypervisora, znacznik (tag);
    d. zdefiniowanie przydziału grupy kontenerów Docker do segmentu poprzez mechanizm adnotacji;
    e. zdefiniowanie usług zewnętrznych realizowanych dla warstw 4-7 takich jak np. load-balancing, content switch, firewall, itp. Istnieje możliwość dołączenia powyższych fizycznych oraz wirtualnych urządzeń usługowych do portu brzegowego matrycy sieciowej (fabric). Mechanizm przekierowania ruchu do tych urządzeń jest integralną częścią polityki sieciowej (aplikacyjnej) w ramach matrycy;
    f. możliwość zdefiniowania relacji pomiędzy segmentami (warstwami aplikacyjnymi) jako wzajemnie udostępnianych i konsumowanych zasobów, definicja segmentów (grup serwerów) opiera się o fizyczne i wirtualne punkty styku a sama relacja obejmuje usługi L4-7 (firewall/balansowanie ruchu itp);
    g. możliwość wprowadzenia izolacji między fizycznymi i wirtualnymi serwerami wchodzącymi w skład segmentu (warstwy aplikacji) z jednoczesną możliwością ich określonej komunikacji z innymi segmentami.
12. Musi umożliwiać zintegrowanie usług zewnętrznych poprzez zapewnienie konfiguracji mechanizmu przekierowania ruchu dla warstw 4-7 dla następujących wspieranych przez system SDN urządzeń:

a. firewall Palo Alto;
b. firewall FortiGate.

13. Kierowanie ruchu do usług zewnętrznych musi być możliwe bezpośrednio w warstwie L2 oraz w warstwie L3 przez mechanizm PBR (Policy Based Redirect), a także z wykorzystaniem protokołów routingu OSPF, BGP.
14. Musi umożliwiać monitorowanie dostępności usługi zewnętrznej poprzez HTTP URI.
15. Musi umożliwiać wydzielanie izolowanych wirtualnych środowisk sieciowych SDN wraz z dedykowanymi zespołami administratorów i prawami dostępu dla 100 takich środowisk (multitenant).
16. Dla izolowanych środowisk sieciowych musi umożliwiać implementację funkcjonalności dedykowanej bramy wyjściowej L2/L3 oraz dedykowanych usług zewnętrznych realizowanych dla warstw 4-7.
17. Musi umożliwiać tworzenie segmentów sieci L2 w oparciu o technologię VXLAN.
18. Musi umożliwiać jednoczesne konfigurowanie sieci dla środowisk złożonych z:
    a. serwerów fizycznych;
    b. serwerów wirtualnych realizowanych w oparciu o VMWare vSphere i VMware vCenter;
    c. serwerów wirtualnych realizowanych w oparciu o RedHat KVM i OVS (Open vSwitch) w środowisku OpenStack;
    d. kontenerów Docker opartych o orkiestratory Kubernetes i OpenShift.
19. Dla środowisk serwerów wirtualnych (hypervisor) musi umożliwiać integrację z rozproszonym przełącznikiem wirtualnym zapewniając automatyczne mapowanie kreowanych w kontrolerze SDN segmentów (warstw aplikacji) na segmenty przełącznika wirtualnego. Całość ruchu w przełączniku wirtualnym, zarówno na lokalnym serwerze jak i między różnymi serwerami kontrolowana jest przez matrycę SDN.
20. Musi umożliwiać monitorowanie i diagnostykę sieciową dla uruchamianych środowisk w oparciu o następujące mechanizmy:
    a. prezentację sprawności środowiska w formie SLA dla danego środowiska sieciowego oraz modelu polityk aplikacyjnych w skali bezwzględnej (np. 1-100);
    b. prezentowanie bieżącej i historycznej statystyki ruchu dla danego środowiska sieciowego, zdefiniowanych segmentów (warstw aplikacji) oraz interfejsów fizycznych;
    c. prezentację historycznych danych nt. sprawności (SLA) środowiska;
    d. pomiar ruchu na portach wejściowych i wyjściowych infrastruktury sieciowej (fabric) dla środowisk uruchamianych w oparciu o model polityk aplikacyjnych;
    e. diagnostykę ścieżki (traceroute) między dowolną parą portów fizycznych bądź wirtualnych wchodzących w skład infrastruktury;
    f. monitorowanie i raportowanie ilości wykorzystanych i dostępnych zasobów wchodzących w skład infrastruktury.
21. Musi umożliwiać zbieranie, agregowanie i interpretowanie zdarzeń (events) i problemów (faults) w ramach infrastruktury sieciowej (fabric).
22. Musi umożliwiać monitorowanie ruchu poprzez kopiowanie (mirroring) ruchu dla wybranych segmentów (warstw aplikacyjnych).
23. Musi umożliwiać automatyczną detekcję topologii oraz inwentarza infrastruktury sieciowej (fabric).
24. Musi implementować centralne repozytorium oprogramowania (firmware) dla infrastruktury sieciowej (fabric).
25. Musi implementować centralny mechanizm aktualizacji oprogramowania (firmware) dla infrastruktury sieciowej (fabric).
26. Musi umożliwiać zachowywanie (snapshot) i odtwarzanie (rollback) dla całości konfiguracji infrastruktury sieciowej (fabric).
27. Musi udostępnić następujące interfejsy zarządzające:
    a. GUI (http/https);
    b. CLI (linia komend konsoli);
    c. Plugin dla OpenStack umożliwiający integrację na poziomie Neutron ML2.
28. Musi udostępniać następujące mechanizmy programowania:
    a. REST API ze wsparciem dla formatów JSON lub XML. Możliwość konfiguracji infrastruktury bezpośrednio poprzez HTTP (np. z wykorzystaniem Postman REST Client);
    b. Python lub JavaScript SDK;
    c. powszechnie dostępny model obiektowy dla struktur logicznych i sprzętowych wchodzących w skład infrastruktury sieciowej (fabric).
29. Musi udostępniać następujące mechanizmy bezpieczeństwa:
    a. uwierzytelnienie dostępu użytkowników w oparciu o podstawowe mechanizmy: lokalną definicję, RADIUS, TACACS+, LDAP;
    b. dwustopniowe uwierzytelnienie dostępu użytkowników w oparciu o mechanizm podstawowy oraz następujące dodatkowe mechanizmy: powiadomienie na smartfon z odpowiednią

aplikacją, oddzwonienie na zarejestrowany numer telefonu, dodatkowe hasło (passcode) generowane z aplikacji na smartfonie;
   c. uwierzytelnienie dołączenia hosta (serwera) do matrycy poprzez 802.1X;
   d. ograniczanie liczby dołączanych do portu matrycy hostów (serwerów) w oparciu o zdefiniowaną maksymalną liczbę adresów MAC dla portu;
   e. ograniczanie ruchu kierowanego do warstwy sterowania (control plane);
   f. ograniczanie ruchu wejściowego i wyjściowego (policing) na portach matrycy w oparciu o zdefiniowany próg przepustowości.
30. Musi umożliwiać zdefiniowanie i obsługę w ramach jednej matrycy (fabric) co najmniej dwóch fizycznie odrębnych lokalizacji połączonych przez zewnętrzną, niezależną sieć IP (tzw. Siecią Połączeniową), z wykorzystaniem wbudowanego mechanizmu łączenia lokalizacji opartego o tunelowanie przez zewnętrzną Siecią Połączeniową. Wszystkie wymienione w poprzedzających punktach funkcjonalności są w ten sam, jednolity sposób dostępne dla obu wspomnianych lokalizacji, zarządzanie całością topologii prowadzone jest z jednego punktu (kontrolera SDN).
31. Sprzęt musi zostać dostarczony z przewodami zasilającymi kompatybilnymi z infrastrukturą Zamawiającego. Zamawiający w udostępnionej przestrzeni szaf rack posiada złącza C13 i C19.

2. **Przełącznik Spine – 4 sztuki**

1. Przełącznik, niezależnie od opisanej poniżej wymaganej standardowej funkcjonalności, musi mieć możliwość pracy jako element istniejącego opisanego powyżej sieciowego systemu typu SDN i w takim trybie zapewniać realizację opisanej powyżej funkcjonalności SDN.
2. Przełącznik musi posiadać:
   a. minimum 28 portów QSFP28 bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40 Gbps oraz w trybie 100 Gbps;
   b. minimum 8 portów QSFP-DD bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 100 Gbps oraz w trybie 400 Gbps;
   c. pamięć operacyjna minimum 32 GB;
   d. pamięć flash minimum 128 GB;
   e. bufor do obsługi pakietów minimum 80 MB.
3. Parametry wydajnościowe:
   a. prędkość przełączania „wirespeed” dla każdego portu przełącznika;
   b. urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3;
   c. obsługiwana łączna przepływność (pasmo) min. 12 Tbps;
   d. obsługiwana łączna przepustowość pakietowa przełącznika min. 4 bpps.
4. Przełącznik musi posiadać następującą funkcjonalność warstwy L2:
   a. trunking IEEE 802.1Q VLAN;
   b. wsparcie dla min 3000 sieci VLAN;
   c. funkcjonalność izolowania portów znajdujących się w tym samym VLAN;
   d. wsparcie sprzętowe dla minimum 256 tysięcy adresów MAC;
   e. IEEE 802.1w Rapid Spanning Tree (RST);
   f. IEEE 802.1s Multiple Spanning Tree (MST);
   g. wsparcie sprzętowe dla tunelowania QinQ;
   h. statyczny i dynamiczny NAT;
   i. zabezpieczenie przeciwko incydentom w topologii Spanning Tree;
   j. Internet Group Management Protocol (IGMP) Versions 2, 3;
   k. terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;
   l. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce;
   m. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów).
5. Przełącznik musi posiadać następującą funkcjonalność warstwy L3:
   a. sprzętowe przełączanie pakietów w warstwie L3;
   b. routing w oparciu o trasy statyczne;
   c. routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6;
   d. Policy Based Routing (PBR) dla IPv4 i IPv6;
   e. VRRP v3;
   f. wsparcie dla BFDv6 (Bidirectional Forwarding Protocol);
   g. wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM / wpisów hosta w tablicy routingu IP;
   h. wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast);

i. wsparcie dla IGMPv3 oraz MSDP;
j. wsparcie sprzętowe dla minimum 32,000 tras multicastowych;
k. wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking);
l. wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);
m. minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list.

6. Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN:
   a. sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway);
   b. wymiana ruchu z co najmniej 256 VTEP (VXLAN Tunnel Endpoint);
   c. obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM i Anycast RP;
   d. obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);
   e. implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol);
   f. obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN);
   g. VXLAN Multihoming dla dołączania urządzeń do pary przełączników w oparciu o zagregowane połączenie LACP.
7. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   a. Layer 2 IEEE 802.1p (CoS);
   b. klasyfikacja QoS w oparciu o listy ACL (access control list) – w warstwach 2, 3, 4;
   c. kolejkowanie na wyjściu w oparciu o CoS 802.1p
   d. bezwzględne (strict-priority) kolejkowanie na wyjściu
   e. kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych
   f. dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   g. protokół PFC (Priority Flow Control) IEEE 802.1Qbb
8. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   a. wejściowe ACL (standardowe oraz rozszerzone)
   b. standardowe oraz rozszerzone ACL dla warstwy 2, w oparciu o adresy MAC, typ protokołu
   c. standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP)
   d. ACL oparte o VLAN-y (VACL)
   e. ACL oparte o porty (PACL)
   f. DHCP Snooping; ARP Inspection; IP Source Guard
   g. prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
9. Musi zapewniać funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
   a. port zarządzający 100/1000 Mbps
   b. port konsoli CLI
   c. zarządzanie In-band
   d. SSHv2
   e. Authentication, authorization, and accounting (AAA)
   f. RADIUS
   g. TACACS+
   h. Syslog
   i. SNMP v1, v2, v3
   j. IEEE 802.1ab LLDP
   k. 802.1x i dynamiczny przydział VLAN do portu
   l. możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   m. Role-Based Access Control RBAC
   n. ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   o. kopiowanie ruchu ze Źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror)
   p. Network Time Protocol (NTP)
   q. Precision Time Protocol IEEE 1588
   r. diagnostyka procesu BOOT

s. ping
t. traceroute

10. Musi zapewniać narzędzia programowania i zarządzania przełącznikiem:
    a. interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
    b. wbudowana powłoka bash do zarządzania systemem Linux przełącznika
    c. wsparcie dla kontenerów Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych
    d. interfejs programistyczny REST API wraz z upublicznionym SDK
    e. możliwość zainstalowania klienta Chef
    f. możliwość zainstalowania agenta Puppet
    g. wsparcie dla NETCONF i zarządzania poprzez XML
    h. wsparcie dla OpenStack Neutron plugin
    i. wsparcie dla kontenerów Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych
11. Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony zasilaczy.
12. Musi zostać dostarczony z przewodami zasilającymi kompatybilnymi z infrastrukturą Zamawiającego. Zamawiający w udostępnionej przestrzeni szaf rack posiada złącza C13 i C19.
13. Musi posiadać obudowę o rozmiarach maksymalnie 1RU (rack unit), przeznaczoną do montażu w szafie rackowej 19”. W wypadku zastosowania przełącznika modularnego dopuszcza się większy rozmiar urządzenia.

3. **Przełącznik Leaf – 4 sztuki**

1. Przełącznik musi posiadać:
    a. 48 portów 1/10/25GE SFP/SFP+/SFP28.
    b. 6 portów definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi mieć możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps,
2. Porty SFP/SFP+/SFP28 muszą umożliwiać zastosowanie następujących modułów:
    a. Gigabit Ethernet 1000Base-T,
    b. Gigabit Ethernet 1000Base-SX,
    c. 10Gigabit Ethernet 10GBase-SR,
    d. 10Gigabit Ethernet 10GBase-SR-S,
    e. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),
    f. 10Gigabit Ethernet 10GBase-LR,
    g. 10Gigabit Ethernet typu twinax (SFP+ - SFP+ DAC),
    h. 25Gigabit Ethernet 25GBASE-SR,
    i. 25Gigabit Ethernet typu twinax (SFP28 – SFP28 DAC),
    j. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF).
3. Porty QSFP muszą umożliwiać zastosowanie następujących modułów:
    a. 40G-SR4,
    b. 40G-CSR,
    c. 40G-CSR4,
    d. 40G-LR4,
    e. 40G-SR-BD,
    f. Adaptera 40G QSFP->10G SFP+,
    g. 40Gigabit Ethernet typu twinax (QSFP – QSFP DAC),
    h. 100GBASE-SR4,
    i. 100Gigabit Ethernet typu twinax (QSFP – QSFP DAC).
4. Przełącznik musi spełniać następujące wymagania w zakresie parametrów wydajnościowych:
    a. Urządzenie musi posiadać bufor pamięci o wielkości minimum 40MB,
    b. Urządzenie musi posiadać min. 16GB pamięci DRAM i 64GB pamięci Flash,
    c. Przepustowość łączna przełącznika (switching capacity) nie może być mniejsza niż 3 Tbps,
    d. Prędkość przesyłania (forwarding rate) nie mniejsza niż 1 miliard pps,
    e. Wymagana jest prędkość przełączania „wirespeed” dla każdego portu przełącznika,
    f. Opóźnienie przełączania pakietów nie większe niż 2 µs,
5. Przełącznik musi posiadać następującą funkcjonalność warstwy L2 OSI:
    a. Trunking IEEE 802.1Q VLAN,
    b. Możliwość izolowania portów znajdujących się w tym samym segmencie VLAN,

c. Wsparcie sprzętowe dla minimum 90 000 adresów MAC,
d. IEEE 802.1w Rapid Spanning Tree (RST),
e. IEEE 802.1s Multiple Spanning Tree (MST),
f. Wsparcie sprzętowe dla tunelowania QinQ (802.1Q Tunneling),
g. Funkcja statycznej i dynamicznej translacji adresów IP NAT (Network Address Translation),
h. Obsluga IGMP v2/3,
i. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach,
j. Wsparcie dla Link Aggregation Control Protocol (LACP): IEEE 802.3ad,
k. 32 interfejsów fizycznych w ramach jednego połączenia zagregowanego typu „Port Channel" LACP.
l. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów).

6. Przełącznik musi posiadać następującą funkcjonalność warstwy L3 OSI:
   a. Routing statyczny dla protokołów IPv4 oraz IPv6,
   b. Routing dynamiczny w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6,
   c. Policy Based Routing (PBR) dla IPv4 i IPv6,,
   d. Wsparcie sprzętowe dla minimum 768 000 prefixów LPM/wpisów hosta w tablicy routingu I,
   e. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast),
   f. Wsparcie dla IGMPv2/v3 oraz MSDP,
   g. Wsparcie sprzętowe dla minimum 100 000 tras multicast,
   h. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking),
   i. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP),
   j. Obsługa protokołu BFD (Bidirectional Forwarding Detection) dla protokołów IPv4 i IPv6, umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu,
   k. Wsparcie dla protokołu VRRP v3,
   l. Wsparcie dla Microsoft NLB,
   m. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list,
   n. Jeśli funkcjonalność warstwy L3 OSI opisana w powyższym punkcie wymaga dostarczenia dodatkowej licencji, to jest ona wymagana na tym etapie.
7. Przełącznik musi posiadać możliwość uruchomienia sprzętowego load-balancera dla protokołów IPv4 i IPv6 ze wsparciem dla tworzenia grup serwerów i adresów VIP, próbkowania serwerów, wyboru ruchu na podstawie protokołu/portu L4 i poprzez filtra ACL.
8. Przełącznik musi posiadać możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet:
   a. dołączenie modułów lub przełączników nie może być realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3, a jedynie w ramach domeny fizycznej bądź stosu urządzeń;
   b. porty modułu wyniesionego muszą być udostępniane do zarządzania i monitorowania z poziomu przełącznika macierzystego;
   c. przełącznik musi umożliwiać programową konwersję własnego trybu pracy do trybu modułu wyniesionego, zarządzanego z innego przełącznika macierzystego.
9. Przełącznik musi posiadać sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad na blokach 128 bit oraz 256 bit oraz wykorzystaniem trybu GCM-AES-XPN.
10. Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN
    a. Sprzętowa implementacja VTEP (VXLAN Tunnel Endpoint),
    b. Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway),
    c. Wymiana ruchu z co najmniej 255 innymi sprzętowymi VTEP,
    d. Obsługa ruchu rozgłoszeniowego BUM (broadcast, multicast, unknown-unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP,
    e. Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol),
    f. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN),
    g. Jeśli funkcjonalność VXLAN opisana powyżej wymaga dostarczenia dodatkowej licencji to jest ona wymagana na tym etapie,
11. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Obsługa Layer 2 IEEE 802.1p (CoS),
    b. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2-4 OSI. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki

Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP,
   c. Kolejkowanie w oparciu o CoS 802.1p na wyjściu,
   d. Kolejkowanie z bezwzględnym priorytetem (Strict-Priority) na wyjściu,
   e. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny,
   f. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych,
   g. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych,
   h. Obsługa protokołu PFC (Priority Flow Control) IEEE 802.1Qbb,
   i. Urządzenie musi posiadać architekturę pamięci przystosowaną dla obsługi buforów, QoS oraz ruchu typu microburst (chwilowe wzrosty ruchu), zapewniając skuteczną obsługę zarówno małych jak i bardzo dużych przepływów danych. Urządzenie musi potrafić monitorować wykorzystanie buforów i sygnalizować przekraczanie zdefiniowanych przez użytkownika progów wielkości przepływu w przypadku zaistnienia zjawiska microburst.
12. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa i stabilności w sieci:
   a. Wejściowe ACL (standardowe oraz rozszerzone),
   b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC,
   c. Standardowe oraz rozszerzone ACL dla warstw 3-4 OSI w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP),
   d. ACL oparte o VLAN-y (VACL) i porty (PACL),
   e. Funkcja zabezpieczenia przed niekontrolowanym wzrostem ilości ruchu (storm control) dla ruchu unicast, multicast i broadcast,
   f. Mechanizmy DHCP Snooping, ARP Inspection i IP Source Guard,
   g. Funkcja zabezpieczenia przed niekontrolowanym wzrostem ilości ruchu (storm control) dla ruchu unicast, multicast i broadcast.
13. Przełącznik musi wspierać funkcjonalności z obszaru zarządzania i zabezpieczenia przełącznika:
   a. Port konsoli CLI,
   b. Zarządzanie In-band - obsługa protokołów SSHv2, SNMPv3, HTTPS, Syslog,
   c. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
   d. 802.1x i dynamiczny przydział VLAN do portu,
   e. Wsparcie dla protokołów sFlow lub NetFlow,
   f. Wsparcie sprzętowe dla telemetrii przepływów z możliwością eksportu z wykorzystaniem protokołu gRPC,
   g. Wsparcie dla IEEE 802.1ab LLDP,
   h. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback),
   i. Obsluga Role-Based Access Control RBAC,
   j. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (Control Plane Policing),
   k. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror, SPAN),
   l. Obsługa Network Time Protocol (NTP) i Precision Time Protocol IEEE 1588,
   m. Diagnostyka procesu BOOT;
14. Przełącznik musi posiadać sprzętowe i programowe wsparcie dla architektury SDN dedykowanej przez jego producenta dla infrastruktury Data Center. Dodanie przełącznika do systemu SDN musi być możliwe z wykorzystaniem jego istniejącego oprogramowania, bądź po jego wymianie na odpowiednie oprogramowanie, bez żadnych ingerencji czy modyfikacji sprzętowych.
15. Przełącznik musi posiadać narzędzia programowania i zarzadzania:
   a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API,
   b. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika,
   c. Wsparcie dla kontenerów Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych,
   d. Interfejs programistyczny REST API wraz z upublicznionym SDK,
   e. Wsparcie dla NETCONF i zarządzania poprzez XML.
16. Przełącznik musi spełniać następujące wymagania sprzętowe:

a. Musi być wyposażony w dwa zasilacze zmiennoprądowe, pracujące w konfiguracji redundantnej,
b. Musi posiadać wymienne moduły wentylatorów, w konfiguracji zapewniającej wyrzut ciepłego powietrza od strony portów liniowych,
c. Musi umożliwiać montaż w szafie rack 19".
d. Sprzęt musi zostać dostarczony z przewodami zasilającymi kompatybilnymi z infrastrukturą Zamawiającego. Zamawiający w udostępnionej przestrzeni szaf rack posiada złącza C13 i C19.
e. Wysokość obudowy nie może przekraczać 1 RU.

17. Przełącznik musi posiadać deklaracja CE lub równoważną.
18. Przełącznik musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną.
19. Przełącznik musi być zgodny z normami UE i przeznaczony na rynek UE, musi posiadać certyfikat CE lub równoważny.
20. Z każdym przełącznikiem musi zostać dostarczony zestaw kabli i modułów optycznych pochodzących od Producenta przełącznika:
    a. Kabel typu 25Gb AOC SFP28, min. 3m – min. 12 szt.
    b. Kabel typu 10Gb AOC SFP+, min. 3m – min. 12 szt.
    c. Kabel typu 100 Gb AOC QSFP28 min. 1m – min. 1 szt.
    d. Moduł optyczny typu 25Gb SFP-25G-SR – min. 10 szt.
    e. Moduł optyczny typu 10Gb SFP-10G-SR – min. 10 szt.
    f. Kabel typu 100Gb AOC QSFP28 min. 10m – min. 1 szt.

V. MINIMALNE WYMAGANIA DOTYCZĄCE OPROGRAMOWANIA DO PRZEŁĄCZNIKÓW TYPU LEAF POSIADANYCH PRZEZ ZAMAWIAJĄCEGO

Dla każdego z wymienionych przełączników posiadanych przez Zamawiającego należy dostarczyć przedłużenie gwarancji, wsparcia producenta oraz subskrypcję Cisco DCN Essentials na tożsamy okres 36 miesięcy zgodny terminem wsparcia i gwarancji dla 2 przełączników typu Leaf dostarczanych zaoferowanego Systemu typu SDN. Łącznie należy dostarczyć gwarancję, wsparcie oraz opisana wyżej subskrypcję dla 4 przełączników typu Leaf.

Ministerstwo posiada następujące 4 przełączniki typu Leaf:

1. Cisco Nexus9000 C93180YC-FX3 Chassis – SN: FDO26020BAX
2. Cisco Nexus9000 C93180YC-FX3 Chassis – SN: FDO26020BCB
3. Cisco Nexus9000 C93180YC-FX3 Chassis – SN: FDO2752094Q
4. Cisco Nexus9000 C93180YC-FX3 Chassis – SN: FDO275208XG

VI. MINIMALNE WYMAGANIA W ZAKRESIE USŁUGI MIGRACJI OBECNEJ ARCHITEKTURY SIECIOWEJ DO DOSTARCZONEGO SYSTEMU TYPU SDN

Ministerstwo posiada aktualnie pracującą sieć w dwóch ośrodkach przetwarzania. Dostarczony System należy zintegrować z pracującymi urządzeniami firewall oraz klastrami VMware, następnie wykonać migrację obecnie działających usług sieciowych na sieć typu SDN w sposób minimalizujący niedostępność usług produkcyjnych dla systemów informatycznych opartych o aktualne rozwiązania sieciowe.

1. W ramach przedmiotu zamówienia musi zostać wykonana migracja obecnej architektury sieciowej do Systemu SDN.
2. Wszelkie prace konfiguracyjne muszą uwzględniać dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczonej infrastruktury sprzętowej oraz programowej.
3. W ramach przygotowania do wdrożenia Wykonawca:
    a. Przeprowadzi analizę zastanej infrastruktury sieciowej, w zakresie niezbędnym do przygotowania projektu technicznego.
    b. Opracuje projekt techniczny, który musi zawierać co najmniej:
        i. opis techniczny i funkcjonalny zaoferowanych urządzeń;
        ii. specyfikację parametrów fizycznych i środowiskowych, tj. wagę, rozmiar, parametry zasilania, emitowane ciepło;
        iii. rozmieszczenie urządzeń w szafach RACK;
        iv. koncepcję podłączenia dostarczanych urządzeń do istniejącej infrastruktury Zamawiającego – schemat podłączenia fizycznego i logicznego, z uwzględnieniem m.in. posiadanych firewalli;
        v. zakres prac dot. konwersji przełączników Nexus do roli Leaf;
        vi. zakres prac i zmian konfiguracyjnych;

vii. opis sposobu migracji dotychczasowej konfiguracji sieci na nowe urządzenia;
viii. procedurę i harmonogram przełączenia sieci na dostarczone urządzenia z uwzględnieniem wymogu prowadzenia prac w dniu ustawowo wolnym od pracy lub w nocy ze względu, że prace wykonywane będą na produkcyjnie działającej infrastrukturze. Zamawiający dopuszcza przerwę techniczną w działaniu infrastruktury IT (powodującą niedostępność usług IT) wynoszącą 2 godziny, w czasie którego Wykonawca dokona przełączenia ruchu sieciowego na dostarczone urządzenia.

c. Zamawiający w terminie 7 dni roboczych od otrzymania projektu technicznego dokona jego akceptacji lub zgłosi uwagi. Warunkiem rozpoczęcia prac wdrożeniowych jest zaakceptowanie przez Zamawiającego projektu technicznego.

4. W ramach wdrożenia urządzeń Wykonawca zgodnie z zaakceptowanym projektem technicznym:
   a. zainstaluje dostarczane urządzenia w szafach RACK, podłączy do sieci: elektrycznej i LAN, skonfiguruje zarządzanie urządzeniami;
   b. wykona połączenia światłowodowe pomiędzy szafami RACK (dostarczenie kabli światłowodowych leży po stronie Wykonawcy);
   c. uruchomi urządzenia oraz dokona aktualizacji oprogramowania zgodnie z przyjętą rekomendowaną obowiązującą wersją stabilną;
   d. dostosuje konfigurację istniejących urządzeń, aby umożliwić podłączenie dostarczonych urządzeń;
   e. wykona dołączenie środowiska SDN do posiadanej przez Zamawiającego sieci i przepięcie posiadanych usług na nowe środowisko. Następnie rozciągnięcie środowiska SDN na drugą lokalizację geograficznie odległą.
   f. wykona testy akceptacyjne, w tym testy redundancji środowiska (plan testów Wykonawca przedstawi Zamawiającemu do akceptacji);
   g. wykonana dokumentację powykonawczą i procedury eksploatacyjne;
   h. przeprowadzi instruktaż, min. 3 dni po 6 godzin z podstawowej obsługi wdrożonego systemu.

VII. MINIMALNE WYMAGANIA W ZAKRESIE ASYSTY TECHNICZNEJ

1. Wykonawca przez 36 miesięcy zobowiązany będzie do świadczenia usługi asysty technicznej na każde żądanie Zamawiającego, tj. każdorazowo na podstawie pisemnego zlecenia asysty technicznej, wystawianego przez Zamawiającego.
2. Zakres, sposób oraz termin realizacji zostanie uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie.
3. Zlecenia będą obejmować w szczególności wsparcie administratorów Zamawiającego w użytkowaniu Systemu, zarówno techniczne jak i merytoryczne.
4. Szczegółowy zakres usługi asysty technicznej uwzględniać będzie każdorazowo zlecenie.
5. Usługi asysty technicznej muszą być realizowane przez inżyniera posiadającego Certyfikat z oficjalnej ścieżki producenta dostarczonego systemu na poziomie eksperckim.
6. Usługi asysty technicznej Wykonawca zobowiązuje się realizować w dwóch formach:
   a) w siedzibie Zamawiającego;
   b) zdalnie.
7. Wykonawca udostępni narzędzie umożliwiające zdalną komunikację, które w uzgodnieniu z Zamawiającym zostanie uruchomione na stacji roboczej pracownika Zamawiającego.
8. Po wykonaniu usług Wykonawca przedłoży Zamawiającemu protokół z wykonania usług asysty zawierający ich rodzaj, zakres oraz termin.
9. Maksymalna liczba roboczogodzin w trakcie trwania umowy wskazana jest w Formularzu Ofertowym.
10. Zamawiający zastrzega sobie prawo do nie udzielania zleceń na usługi asysty technicznej.

VIII. MINIMALNE WYMAGANIA TECHNICZNE ORAZ DOTYCZĄCE OPROGRAMOWANIA DO PRZEŁĄCZNIKÓW TYPU ACCESS – 20 SZTUK

1. Przełącznik typu standalone, minimalne wyposażenie:
   a) 48 portów 10/100/1000BaseT RJ-45 POE+;
   b) uplink 4x10G SFP+;

2. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
   a) Gigabit Ethernet 1000Base-T,
   b) Gigabit Ethernet 1000Base-SX,
   c) Gigabit Ethernet 1000Base-LX/LH,
   d) Gigabit Ethernet 1000Base-BX-D/U,
   e) 10Gigabit Ethernet 10GBase-SR,
   f) 10Gigabit Ethernet 10GBase-LR,
3. Musi być możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
   a) Przepustowość w ramach stosu - 80Gb/s;
   b) 8 urządzeń w stosie;
   c) zarządzanie poprzez jeden adres IP;
   d) możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad;

   W przypadku gdy wymagane są dodatkowe moduły do zapewnienia funkcjonalności stacka, urządzenie musi być w nie wyposażone na obecnym etapie zamówienia, wraz z kablem stackującym o długości 50 cm.
4. Zasilanie:
   a) urządzenie musi posiadać możliwość instalacji zasilacza redundantnego AC 230V
   b) możliwość instalacji/wymiany zasilaczy „na gorąco” (ang. hot swap),
   c) urządzenie musi być wyposażone w pojedynczy zasilacz podstawowy i redundantne wentylatory,
   d) dodatkowo urządzenie powinno być doposażone w zapasowy zasilacz umożliwiający samodzielną wymianę w przypadku awarii zasilacza podstawowego
5. Przełącznik musi spełniać następujące wymagania w zakresie parametrów wydajnościowych:
   a) Przepustowość przełącznika (switching capacity) nie mniej-sza niż 170 Gb/s (bez podłączenia do stosu), 250 Gb/s (z podłączeniem do stosu),
   b) Prędkość przesyłania (forwarding rate) nie mniejsza niż 125 Mpps,
   c) Bufor pakietów nie mniejszy niż 5MB.
   d) Pamięć DRAM minimum 2GB,
   e) Pamięć flash minimum 4GB,
   f) Obsługa:
      i. Minimum 500 aktywnych sieci VLAN jak i interfejsów SVI L3,
      ii. Nie mniej niż 15000 adresów MAC,
      iii. Minimum 2500 tras IPv4,
      iv. Nie mniej niż 900 wpisów w listach kontroli dostępu Security ACL,
      v. Nie mniej niż 900 wpisów w listach kontroli dostępu QoS ACL,
      vi. Wparcie dla jumbo frame o wielkości 9198B,
      vii. Minimum 40 połączeń zagregowanych typu „port chan-nel” ,
      viii. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
6. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   a) IEEE 802.1w Rapid Spanning Tree,
   b) Per-VLAN Rapid Spanning Tree (PVRST+),
   c) IEEE 802.1s Multi-Instance Spanning Tree,
   d) Wsparcie dla protokołu REP (Resilient Ethernet Protocol),
   e) Redundancja połączeń uplink bez używania protokołu Span-ning-Tree lub funkcji „portchannel” umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego, wraz z możliwością wskazania uplinku podstawowego i zapasowego dla poszczególnych sieci VLAN. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (funkcja preempt) po przywrócenia aktywności linku podstawowego.
7. Przełącznik musi zapewniać obsługę następujących protokołów:
   a) IGMPv1/2/3 i MLDv1/2 Snooping,
   b) LLDP i LLDP-MED
8. Urządzenie musi realizować funkcje:
   a) 802.1Q tunneling (QinQ),

b) Layer 2 traceroute umożliwiającej śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC,
c) Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,
d) Możliwość uruchomienia serwera DHCP

9. Przełącznik musi wspierać mechanizmy związane z bezpieczeństwem sieci:
   a) Wiele poziomów dostępu administracyjnego poprzez konsolę, możliwość zalogowania się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
   b) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
   c) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
   d) Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
   e) Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
   f) Możliwość uwierzytelniania użytkowników w oparciu o por-tal web dla klientów bez suplikanta 802.1X,
   g) Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
   h) Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
   i) Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
   j) Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
   k) 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),
   l) Możliwość autoryzacji prób logowania do urządzenia (do-stęp administracyjny) do serwerów RADIUS i TACACS+,
   m) Obsługa list kontroli dostępu (ACL) następujących typów:
      i. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
      ii. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
      iii. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
      iv. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
   n) 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),
   o) Wbudowane mechanizmy ochrony warstwy kontrolnej prze-łącznika (CoPP – Control Plane Policing),
   p) Funkcja Private VLAN;
10. Przełącznik musi wspierać mechanizmy zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
   a) sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
   b) bezpieczna sekwencja uruchamiania,
   c) sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
11. Przełącznik musi obsługiwać następujące funkcje związane z zapewnieniem jakości usług w sieci:
   d) Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
   e) Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
   f) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

g) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) po-przez wykorzystanie następujących parametrów: źródło-wy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
h) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
i) Kontrola sztormów dla ruchu broadcast/multicast/unicast,
j) Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

12. Przełącznik musi zapewnić obsługę następujących protokołów i mechanizmów routingu:
    a) Routing statyczny dla IPv4 i IPv6,
    b) Routing dynamiczny – RIP, OSPF nie mniej niż 900 wpisów, PIM Stub nie mniej niż 900 wpisów,
    c) Policy-based routing (PBR),
    d) Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
    e) Obsługa minimum 10 tuneli GRE (Generic Routing Encap-sulation);
13. Przełącznik musi:
    a) umożliwiać 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,
    b) posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
    c) posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane za-leżnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
    d) urządzenie powinno posiadać funkcjonalność sondy IP SLA Responder,
14. Przełącznik musi wspierać następujące mechanizmy i narzędzia zarządzania:
    a) Port konsoli,
    b) Dedykowany port Ethernet do zarządzania out-of-band,
    c) 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. Kontrola dostępu dla tej funkcjonalności musi być realizowana poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
    d) 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,
    e) Obsługa protokołów SNMPv3, SSHv2, SCP, SFTP (SSH Fi-le Transfer Protocol), HTTPS, Syslog,
    f) Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
    g) Wsparcie dla protokołów RESTCON i gNMI,
    h) Wbudowana dioda umożliwiająca identyfikację konkretnego urządzenia podczas akcji serwisowych,
    i) Wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
    j) Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
    k) 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,
    l) Wbudowany graficzny interfejs zarządzania przełącznikiem.
15. Urządzenie musi spełniać następujące parametry fizyczne:
    a) Możliwość montażu w szafie rack 19”,
    b) Wysokość urządzenia 1 RU,

c) Głębokość chassis urządzenia bez wentylatorów i kabli zasilających mniejsza niż 30 cm'
d) Głębokość chassis urządzenia z wentylatorami i kablami zasilającymi mniejsza niż 33 cm.

16. Przełącznik musi wspierać funkcjonalność NetFlow w zakresie:
    a) możliwości próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow i obsługą 16000 strumieni (flow),
    b) realizacji rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7 OSI, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
17. Certyfikaty:
    a) Switch musi posiadać deklaracja CE lub równoważną.
    b) Switch musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną.
    c) Switch musi być zgodny z normami UE i przeznaczony na rynek UE, musi posiadać certyfikat CE lub równoważny.

1. Dodatkowe wyposażenie - moduły i kable światłowodowe, dodatkowe zasilacze

1. 20 modułów SFP 1G -RJ45
    a) Wkładka umożliwiająca rozszerzenie funkcjonalności prze-łączników z portem SFP o interfejs kablowy 1 Gbps LC , pracujący z wykorzystaniem kabla skrętkowego UTP z wtykiem RJ45
    b) Typ i liczba portów: 1 x 1 Gbps LC
    c) Zamawiający wymaga, aby wkładki były kompatybilne z dostarczonymi przełącznikami.
    d) Zamawiający dopuszcza wkładki innego producenta (zamienniki) pod warunkiem pełnej kompatybilności i braku utraty gwarancji w przypadku użycia.
2. 20 modułów SFP+ 10G -RJ45
    a) Wkładka umożliwiająca rozszerzenie funkcjonalności prze-łączników z portem SFP o interfejs kablowy 10 Gbps LC , pracujący z wykorzystaniem kabla skrętkowego UTP z wtykiem RJ45
    b) Typ i liczba portów: 1 x 10 Gbps LC
    c) Zamawiający wymaga, aby wkładki były kompatybilne z dostarczonymi przełącznikami.
    d) Zamawiający dopuszcza wkładki innego producenta (zamienniki) pod warunkiem pełnej kompatybilności i braku utraty gwarancji w przypadku użycia.
3. 10 kabli światłowodowych MM LC-LC – 15 M:
    a) Patchcord światłowodowy MuliMode z wtykiem LC o długo-ści 15 metrów, min OM-4
4. 300 kabli UTP Cat min 5c 0,5m:
    a) Patchcord skrętkowy kategorii min 5c z wtykiem RJ45 o długości 0.5 m kolor biały/szary.
5. 200 kabli UTP Cat min 5c 1m:
    a) Patchcord skrętkowy kategorii min 5c z wtykiem RJ45 o długości 1 m kolor biały/szary.
6. 5 kabli stackujący o długości 1m:
    a) Dedykowany dla oferowanych urządzeń kabel stackujący o długości 1m
7. 5 kabli stackujący o długości 3m:
    a) Dedykowany dla oferowanych urządzeń kabel stackujący o długości 3m

IX. MINIMALNE WYMAGANIA TECHNICZNE ORAZ DOTYCZĄCE OPROGRAMOWANIA DO PRZEŁĄCZNIKÓW TYPU DATACENTER - 8 SZTUK

1. Przełącznik musi posiadać:
    a. 48 portów 1/10 Base-T
    g. 6 portów definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi mieć możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps,
2. Przełącznik musi spełniać następujące wymagania w zakresie parametrów wydajnościowych:
    a. Urządzenie musi posiadać bufor pamięci o wielkości minimum 40MB,
    b. Urządzenie musi posiadać min. 16GB pamięci DRAM i 64GB pamięci Flash,
    c. Przepustowość łączna przełącznika (switching capacity) nie może być mniejsza niż 2 Tbps,
    d. Prędkość przesyłania (forwarding rate) nie mniejsza niż 1 miliard pps,
    e. Wymagana jest prędkość przełączania „wirespeed" dla każdego portu przełącznika,
    f. Opóźnienie przełączania pakietów nie większe niż 2 µs,

3. Przełącznik musi posiadać następującą funkcjonalność warstwy L2 OSI:
   a. Trunking IEEE 802.1Q VLAN,
   b. Możliwość izolowania portów znajdujących się w tym samym segmencie VLAN,
   c. Wsparcie sprzętowe dla minimum 90 000 adresów MAC,
   d. IEEE 802.1w Rapid Spanning Tree (RST),
   e. IEEE 802.1s Multiple Spanning Tree (MST),
   f. Wsparcie sprzętowe dla tunelowania QinQ (802.1Q Tunneling),
   g. Funkcja statycznej i dynamicznej translacji adresów IP NAT (Network Address Translation),
   h. Obsluga IGMP v2/3,
   i. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach,
   j. Wsparcie dla Link Aggregation Control Protocol (LACP): IEEE 802.3ad,
   k. 32 interfejsów fizycznych w ramach jednego połączenia zagregowanego typu „Port Channel" LACP.
   l. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów).
4. Przełącznik musi posiadać następującą funkcjonalność warstwy L3 OSI:
   a. Routing statyczny dla protokołów IPv4 oraz IPv6,
   b. Routing dynamiczny w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6,
   c. Policy Based Routing (PBR) dla IPv4 i IPv6,,
   d. Wsparcie sprzętowe dla minimum 768 000 prefixów LPM/wpisów hosta w tablicy routingu I,
   e. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast),
   f. Wsparcie dla IGMPv2/v3 oraz MSDP,
   g. Wsparcie sprzętowe dla minimum 100 000 tras multicast,
   h. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking),
   i. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP),
   j. Obsługa protokołu BFD (Bidirectional Forwarding Detection) dla protokołów IPv4 i IPv6, umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu,
   k. Wsparcie dla protokołu VRRP v3,
   l. Wsparcie dla Microsoft NLB,
   m. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list,
   n. Jeśli funkcjonalność warstwy L3 OSI opisana w powyższym punkcie wymaga dostarczenia dodatkowej licencji, to jest ona wymagana na tym etapie.
5. Przełącznik musi posiadać możliwość uruchomienia sprzętowego load-balancera dla protokołów IPv4 i IPv6 ze wsparciem dla tworzenia grup serwerów i adresów VIP, próbkowania serwerów, wyboru ruchu na podstawie protokołu/portu L4 i poprzez filtra ACL.
6. Przełącznik musi posiadać możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet:
   a. dołączenie modułów lub przełączników nie może być realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3, a jedynie w ramach domeny fizycznej bądź stosu urządzeń;
   b. porty modułu wyniesionego muszą być udostępniane do zarządzania i monitorowania z poziomu przełącznika macierzystego;
   c. przełącznik musi umożliwiać programową konwersję własnego trybu pracy do trybu modułu wyniesionego, zarządzanego z innego przełącznika macierzystego.
7. Przełącznik musi posiadać sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad na blokach 128 bit oraz 256 bit oraz wykorzystaniem trybu GCM-AES-XPN.
8. Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN
   a. Sprzętowa implementacja VTEP (VXLAN Tunnel Endpoint),
   b. Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway),
   c. Wymiana ruchu z co najmniej 255 innymi sprzętowymi VTEP,
   d. Obsługa ruchu rozgłoszeniowego BUM (broadcast, multicast, unknown-unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP,
   e. Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol),
   f. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN),
   g. Jeśli funkcjonalność VXLAN opisana powyżej wymaga dostarczenia dodatkowej licencji to jest ona wymagana na tym etapie,
9. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   a. Obsługa Layer 2 IEEE 802.1p (CoS),

b. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2-4 OSI. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP,
c. Kolejkowanie w oparciu o CoS 802.1p na wyjściu,
d. Kolejkowanie z bezwzględnym priorytetem (Strict-Priority) na wyjściu,
e. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny,
f. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych,
g. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych,
h. Obsługa protokołu PFC (Priority Flow Control) IEEE 802.1Qbb,
i. Urządzenie musi posiadać architekturę pamięci przystosowaną dla obsługi buforów, QoS oraz ruchu typu microburst (chwilowe wzrosty ruchu), zapewniając skuteczną obsługę zarówno małych jak i bardzo dużych przepływów danych. Urządzenie musi potrafić monitorować wykorzystanie buforów i sygnalizować przekraczanie zdefiniowanych przez użytkownika progów wielkości przepływu w przypadku zaistnienia zjawiska microburst.

10. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa i stabilności w sieci:
    a. Wejściowe ACL (standardowe oraz rozszerzone),
    b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC,
    c. Standardowe oraz rozszerzone ACL dla warstw 3-4 OSI w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP),
    d. ACL oparte o VLAN-y (VACL) i porty (PACL),
    e. Funkcja zabezpieczenia przed niekontrolowanym wzrostem ilości ruchu (storm control) dla ruchu unicast, multicast i broadcast,
    f. Mechanizmy DHCP Snooping, ARP Inspection i IP Source Guard,
    g. Funkcja zabezpieczenia przed niekontrolowanym wzrostem ilości ruchu (storm control) dla ruchu unicast, multicast i broadcast.
11. Przełącznik musi wspierać funkcjonalności z obszaru zarządzania i zabezpieczenia przełącznika:
    a. Port konsoli CLI,
    b. Zarządzanie In-band - obsługa protokołów SSHv2, SNMPv3, HTTPS, Syslog,
    c. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
    d. 802.1x i dynamiczny przydział VLAN do portu,
    e. Wsparcie dla protokołów sFlow lub NetFlow,
    f. Wsparcie sprzętowe dla telemetrii przepływów z możliwością eksportu z wykorzystaniem protokołu gRPC,
    g. Wsparcie dla IEEE 802.1ab LLDP,
    h. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback),
    i. Obsluga Role-Based Access Control RBAC,
    j. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (Control Plane Policing),
    k. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror, SPAN),
    l. Obsługa Network Time Protocol (NTP) i Precision Time Protocol IEEE 1588,
    m. Diagnostyka procesu BOOT;
12. Przełącznik musi posiadać sprzętowe i programowe wsparcie dla architektury SDN dedykowanej przez jego producenta dla infrastruktury Data Center. Dodanie przełącznika do systemu SDN musi być możliwe z wykorzystaniem jego istniejącego oprogramowania, bądź po jego wymianie na odpowiednie oprogramowanie, bez żadnych ingerencji czy modyfikacji sprzętowych.
13. Przełącznik musi posiadać narzędzia programowania i zarzadzania:
    a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API,
    b. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika,
    c. Wsparcie dla kontenerów Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych,
    d. Interfejs programistyczny REST API wraz z upublicznionym SDK,

e. Wsparcie dla NETCONF i zarządzania poprzez XML.

14. Przełącznik musi spełniać następujące wymagania sprzętowe:
    a. Musi być wyposażony w dwa zasilacze zmiennoprądowe, pracujące w konfiguracji redundantnej,
    b. Musi posiadać wymienne moduły wentylatorów, w konfiguracji zapewniającej wyrzut ciepłego powietrza od strony portów liniowych,
    c. Musi umożliwiać montaż w szafie rack 19".
    d. Sprzęt musi zostać dostarczony z przewodami zasilającymi kompatybilnymi z infrastrukturą Zamawiającego. Zamawiający w udostępnionej przestrzeni szaf rack posiada złącza C13 i C19.
    e. Wysokość obudowy nie może przekraczać 1 RU.
15. Przełącznik musi posiadać deklaracja CE lub równoważną.
16. Przełącznik musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną.
17. Przełącznik musi być zgodny z normami UE i przeznaczony na rynek UE, musi posiadać certyfikat CE lub równoważny.
18. Z każdym przełącznikiem musi zostać dostarczony zestaw kabli i modułów optycznych pochodzących od Producenta przełącznika:
    a. Kabel typu 100 Gb AOC QSFP28 min. 1m – min. 1 szt.
    b. Kabel typu 100Gb AOC QSFP28 min. 10m – min. 1 szt.

X. MINIMALNE WYMAGANIA W ZAKRESIE GWARANCJI

Gwarancja dla oferowanych urządzeń musi spełniać niżej opisane wymagania:

1. Minimalny okres gwarancji na urządzenia wynosi **36 miesięcy** natomiast w przypadku przełączników sieciowych typu access minimalny okres gwarancji na urządzenia wynosi **60 miesięcy**.
2. Zamawiający wymaga, aby usługa gwarancyjna na wszystkie dostarczone w ramach zamówienia urządzenia, przez cały okres jej trwania, zapewniała naprawę lub wymianę urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczanych urządzeń i Wykonawca był jego autoryzowanym dostawcą.
3. Wszystkie urządzenia dostarczone i zastosowane przez Wykonawcę będą pochodziły z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej. Spełnienie powyższego wymogu zostanie potwierdzone oświadczeniem producenta Urządzeń lub jego polskiego przedstawicielstwa, które Wykonawca zobowiązuje się dostarczyć Zamawiającemu najpóźniej w dniu dostawy oferowanych Urządzeń.
4. Gwarancja będzie liczona od daty odbioru przedmiotu umowy i oparta na gwarancji producentów urządzeń. Serwis gwarancyjny świadczony ma być w miejscu instalacji urządzeń.
5. Gwarancja ma być świadczona w reżimie 8x5xNBD. Czas naprawy Awarii liczony jest od czasu przesłania zgłoszenia o awarii do Wykonawcy zgodnie z procedurą przyjmowania zgłoszeń serwisowych.
6. Zamawiający dopuszcza świadczenie serwisu dla dostarczonych urządzeń poprzez zastosowanie zamienników wskazanych przez producenta tylko i wyłącznie w przypadku, gdy takiego wsparcia u producenta nie da się wykupić (np. produkty zostały wycofane przez producenta bez możliwości świadczenia serwisu).
7. W przypadku, gdy w okresie gwarancyjnym nastąpi trzykrotna naprawa wadliwego podzespołu Wykonawca niezwłocznie tj. w terminie nie dłuższym niż 14 dni liczonych od dnia zgłoszenia awarii, dokona jego wymiany na sprzęt nowy, wolny od wad. Na czas potrzebny do wymiany podzespołu wykonawca dostarczy element zastępczy o parametrach tożsamych z podzespołem uszkodzonym. Zamawiający oczekuje, iż w wypadku konieczności wymiany urządzenia, dyski na których zapisane są dane nieulotne wymienianego urządzenia pozostaną w siedzibie Zamawiającego.
8. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub www) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń w godzinach pracy Zamawiającego.

9. Zamawiający zastrzega sobie prawo do dodawania nowych modułów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą. W przypadku nieprawidłowego lub niezgodnego z zaleceniami Wykonawcy i producenta Urządzenia dodania modułów lub wymiany zainstalowanych modułów przez Zamawiającego Wykonawca nie jest obciążony gwarancją i rękojmią w tym zakresie.
10. W okresie gwarancji Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania do najnowszych wersji oferowanych przez producenta (włączając tzw. firmware) oraz patche i programy korekcji błędów, a także dostęp do usług wsparcia technicznego producenta właściwy dla danego Urządzenia lub Oprogramowania. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu ww. przed podpisaniem protokołu odbioru Urządzeń.
11. W przypadku konieczności naprawy Urządzenia lub Oprogramowania poza Lokalizacją, Wykonawca pokrywa koszty transportu i ponosi ryzyko uszkodzenia lub przypadkowej utraty urządzenia lub oprogramowania Standardowego w przypadku konieczności naprawy poza siedzibą Zamawiającego.
12. Na okres przedłużającej się naprawy Wykonawca może stosować procedury zastępcze. Czas trwania procedur zastępczych nie może być dłuższy niż 45 dni kalendarzowych od chwili zgłoszenia awarii.
13. Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Systemu we wszystkich modułach i zaprzestanie stosowania w bieżącej prac rezerwowego Urządzenia i/lub procedur zastępczych.
14. Po usunięciu każdej Awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.
15. W ramach gwarancji Zamawiający będzie miał prawo przez okres wskazany w formularzu ofertowym do:
    a) pobierania i instalowania nowych wersji oprogramowania dla każdego elementu wchodzącego w skład oferty
    b) Dostępu do bazy wiedzy oraz dokumentacji dostarczonych elementów
    c) Dostępu do powiadomień/ogłoszeń/alarmów w zakresie dostarczonych elementów
    d) Zgłaszania nieograniczonej liczby awarii systemu w trybie 24x365x7 za pomocą dedykowanego portalu i/lub zgłoszenia telefonicznego,
    e) Wymiany uszkodzonych/wadliwych dostarczonych elementów w trybie NDB (Next-Bussines Day),
16. Czasy reakcji/naprawy na zgłoszenie będą na poziomie:
    a) 1 godzina/8 godzin - błąd krytyczny – tj. przerwa w działaniu usług w środowisku produkcyjnym, brak dostępnego obejścia problemu,
    b) 2 godziny/2 dni - błędy wysokie – tj. problem z poprawnym działaniem usługi znacząco utrudniający realizację procesów biznesowych, brak dostępnego obejścia problemu,
    c) 4 godziny/7 dni - błędy średnie - tj. problem z poprawnym działaniem usługi, utrudnienie realizacji procesów biznesowych, dostępne obejście problemu,
    d) 8 godzin/14 dni - błędy niskie – tj. problem z poprawnym działaniem usługi, brak wpływu na realizację procesów biznesowych.
17. Wykonawca do dostarczonych urządzeń, będących przedmiotem zamówienia, dołączy karty gwarancyjne zawierające numer seryjny, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjnej.
18. Wykonawca w terminie 7 dni od zawarcia Umowy dostarczy Zamawiającemu procedury zgłaszania i obsługi Awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej i nr telefonów.

19. Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób uprawnionych do wykonywania czynności serwisowych.
20. W okresie gwarancji Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie urządzeń i oprogramowania stanowiącego przedmiot zamówienia, z zastrzeżeniem, że Wykonawca nie ponosi odpowiedzialności za uszkodzenia urządzeń i oprogramowania powstałych z wyłącznej winy Zamawiającego lub osób trzecich działających w jego imieniu.
21. Wymagany tryb zgłaszania wszelkich awarii, wad i błędów. Zgłoszenie następuje w drodze pisemnej mailem na adres podany przez Wykonawcę lub za pośrednictwem telefonicznego zgłaszania awarii, wad i błędów dotyczących sprzętu i oprogramowania w dni robocze w godzinach 8:00-17:00.
22. Zamawiający wymaga obsługi zgłoszeń w języku polskim.