

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na dostawę Systemu typu SDN (Software Defined Network) dla dwóch ośrodków przetwarzania.

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany poprzez następujące działania:

1. Dostawę sprzętu oraz licencji Systemu typu SDN na który składają się:
 - a) dostawa klastra 4 sztuk kontrolerów;
 - b) dostawa 4 sztuk przełączników typu Spine;
 - c) dostawa 2 przełączników typu Leaf;
2. Dostawę licencji w formie subskrypcji na okres 36 miesięcy dla 4 sztuk przełączników typu Leaf posiadanych przez Zamawiającego.
3. Wykonanie migracji obecnej architektury sieciowej do rozwiązania SDN.
4. Usługi asysty technicznej do dostarczanego Systemu typu SDN.

W ramach punktu I.1. należy zapewnić gwarancję oraz wsparcie producenta dla dostarczanego sprzętu na okres minimum 36 miesięcy, niezbędne licencje do prawidłowego działania zgodnie z wymaganiami OPZ oraz niezbędne okablowanie. Dostarczony sprzęt musi zostać zainstalowany i wstępnie skonfigurowany.

W ramach punktu I.2. 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 dla dostarczanego Systemu typu SDN.

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

W ramach punktu I.3. Należy wykonać migrację obecnej architektury sieciowej do rozwiązania SDN.

Ministerstwo posiada aktualnie pracującą sieć w dwóch ośrodkach przetwarzania. Dostarczone rozwiązanie 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.

W ramach punktu I.4. Wykonawca będzie świadczył usługi asysty technicznej do dostarczonego systemu typu SDN na podstawie wystawianych przez Zamawiającego zleceń. Maksymalna liczba roboczogodzin w ramach usługi asysty technicznej to 720.

W okresie obowiązywania umowy wymagane jest świadczenie usług asysty technicznej na podstawie dodatkowych zleceń Ministerstwa w tym m.in:

- a. Wykonywanie aktualizacji komponentów sieci SDN
- b. Wykonywanie zmian w konfiguracji np. podłączanie nowych urządzeń do sieci SDN
- c. Przeglądy i optymalizacja konfiguracji sieci SDN
- d. Tworzenie i aktualizacja dokumentacji oraz procedur sieci SDN

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie maksymalnie **do 40 dni** od daty podpisania przez strony umowy **(termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym)**.

Realizacja przedmiotu zamówienia obejmować będzie dostawę zakup klastra serwerów baz danych wraz z niezbędnymi licencjami technologicznymi dla Ministerstwa Rozwoju i Technologii do centrum przetwarzania na terenie Polski wskazanego przez Zamawiającego.

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Zaoferowane urządzenia oraz oprogramowanie nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
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 dostarczony System pochodził 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.
4. Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.

IV. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE W ZAKRESIE KONTROLERÓW SIECI SDN

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 rozwiązanie 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 udostępnić 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 połączenia 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 Sieć 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.

V. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE PRZEŁĄCZNIKA SPINE

1. Przełącznik, niezależnie od opisanej poniżej wymaganej standardowej funkcjonalności, musi mieć możliwość pracy jako element istniejącego opisanego powyżej sieciowego rozwiązania klasy 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 (pasma) 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 wiązkę;
 - 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. kolejkovanie na wyjściu w oparciu o CoS 802.1p
 - d. bezwzględne (strict-priority) kolejkovanie na wyjściu
 - e. kolejkovanie 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 Port-Channel, 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 modułowego dopuszcza się większy rozmiar urządzenia.

VI. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE DLA PRZEŁĄCZNIKA TYPU LEAF

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. Obsługa 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 IP
 - 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-XPB. Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie.
 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. Kolejowanie w oparciu o CoS 802.1p na wyjściu
 - d. Kolejowanie z bezwzględnym priorytetem (Strict-Priority) na wyjściu
 - e. Kolejowanie 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 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. Obsługa 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 rozwiązania SDN musi być możliwe z wykorzystaniem jego istniejącego oprogramowania, bądź po jego wymianie na odpowiednie oprogramowanie, bez żadnych ingerencji czy modyfikacji sprzętowych. Jeśli funkcjonalność SDN wymaga dostarczenia dodatkowej licencji to jest ona wymagana na tym etapie.
15. Przełącznik musi posiadać narzędzia programowania i zarządzania:
- 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 upublicznonym 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 deklarację 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.

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

1. Sprzęt będący przedmiotem niniejszego zamówienia zostanie dostarczony do dwóch lokalizacji wskazanych przez Zamawiającego znajdujących się na terenie Polski.
2. Dostawa obejmuje dostawę wszelkich wymaganych do działania Systemu oprogramowania oraz licencji/subskrypcji.
3. Wszelkie prace konfiguracyjne muszą uwzględniać dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczonej infrastruktury sprzętowej oraz programowej.
4. Zamawiający zapewni przestrzeń w szafie RACK 19", zasilanie gwarantowane wraz z niezbędną ilością gniazd w listwach zasilających dla obydwu lokalizacji.
5. Sprzęt musi zostać dostarczony z przewodami zasilającymi kompatybilnymi z infrastrukturą Zamawiającego. Zamawiający w udostępnionej przestrzeni szaf rack posiada złącza C13 i C19.
6. 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.
7. 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 warsztaty, min. 3 dni po 6 godzin, na których Wykonawca przeszkoli Zamawiającego z podstawowej obsługi wdrożonej infrastruktury.

VIII. MINIMALNE WYMAGANIA W ZAKRESIE ASYSTY TECHNICZNEJ

1. Wykonawca przez cały okres trwania umowy 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:
 - a. Zapewnieniu Zamawiającemu pomocy w rozwiązaniu problemów i incydentów wynikłych w trakcie obsługi dostarczonego sprzętu oraz oprogramowania tj.:
 - i. analiza problemów zgłaszanych przez Zamawiającego,
 - ii. asysta przy określaniu i usuwaniu przyczyn oraz skutków zgłaszanych incydentów,
 - iii. dostarczanie, instalacja (po uzyskaniu zgody Zamawiającego) i konfiguracja uaktualnień i nowych wersji oprogramowania lub jego komponentów, oraz związana z tym aktualizacja dostarczonej dokumentacji,
 - iv. przeprowadzanie analiz oraz udzielanie konsultacji Zamawiającemu,
 - v. dokonywanie zmian konfiguracji oprogramowania,
 - vi. opracowywanie i dostarczanie dokumentacji, w tym aktualizacji dokumentacji oraz dostarczanie dokumentacji wprowadzanych zmian.
 - vii. implementację nowych funkcjonalności lub modyfikację już skonfigurowanych.
 - b. Wsparcie w przypadku wystąpienia incydentu bezpieczeństwa.
 - i. Wsparcie w zakresie wykonania analizy wykorzystanych podatności.
 - ii. Kontakt z ekspertem w zakresie bezpieczeństwa dostarczonego systemu.
 - iii. Analizy zakresu kompromitacji systemu.
 - iv. Wsparcia w konfiguracji/rekomendacji w celu zabezpieczenia systemu,
 - v. Wsparcia w zakresie usunięcia skutków oraz rozwiązania incydentu bezpieczeństwa,
 - c. Wsparcie w planowanych pracach serwisowych:
 - i. Przeprowadzenia standardowych prac serwisowych,
 - ii. Przeprowadzania aktualizacji komponentów systemu,
 - iii. Weryfikacji poprawności konfiguracji,
 - iv. Zmiany w topologii sieci,
 - v. Wsparcia w okresie podwyższonej czujności (np. Monitoring środowiska w czasie biznesowo krytycznych wydarzeń),
 - d. Dokonywanie okresowych (nie rzadziej niż co 6 m-cy) przeglądów gwarancyjnych dostarczonego oprogramowania. W ramach przeprowadzanych okresowych przeglądów gwarancyjnych muszą być wykonane co najmniej następujące czynności:
 - i. weryfikacja poprawności działania oraz optymalizacja konfiguracji wszystkich komponentów wchodzących w skład dostarczonego rozwiązania,
 - ii. analiza logów i podjęcie działań naprawczych w razie potrzeby,
 - iii. aktualizacja (w razie potrzeby i po uzyskaniu uprzedniej zgody Zamawiającego) wersji poszczególnych komponentów wchodzących w skład dostarczonego rozwiązania.
 - e. Wsparcie on-site w przypadku braku możliwości rozwiązania problemu zdalnie.
 - f. usługi asysty technicznej muszą być realizowane przez inżyniera posiadającego Certyfikat z oficjalnej ścieżki producenta dostarczonego systemu na poziomie eksperckim.
4. Usługi asysty technicznej Wykonawca zobowiązuje się realizować w dwóch formach:
 - a. w siedzibie Zamawiającego przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez liczbę godzin wskazanych w zleceniu,
 - b. zdalnie przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez określoną liczbę godzin w danym dniu. Wykonawca udostępni narzędzie umożliwiające zdalną komunikację, które w uzgodnieniu z Zamawiającym zostanie uruchomione na stacji roboczej pracownika Zamawiającego.
5. Po wykonaniu usług Wykonawca przedłoży Zamawiającemu protokół z wykonania usług asysty zawierający ich rodzaj, zakres oraz termin.
6. Maksymalna liczba roboczogodzin w trakcie trwania umowy wskazana jest w Formularzu Ofertowym.

7. Zamawiający zastrzega sobie prawo do nie udzielania zleceń na usługi asysty technicznej.
8. Proces realizacji asysty technicznej będzie przebiegał następująco:
 - a. Zamawiający przekaze Wykonawcy drogą mailową zlecenie wykonania asysty technicznej. Zgłoszenie zawierać będzie co najmniej:
 - i. zakres prac do wykonania lub opis problemu do rozwiązania,
 - ii. określenie proponowanego terminu realizacji (opcjonalnie).
 - b. W terminie nie dłuższym niż 3 dni robocze od dnia otrzymania zgłoszenia o asystę techniczną Wykonawca skontaktuje się z Zamawiającym w celu ustalenia szczegółowego zakresu prac, terminu realizacji i szacowanego wymiaru godzin realizacji asysty technicznej.

IX. MINIMALNE WYMAGANIA W ZAKRESIE GWARANCJI

Gwarancja dla oferowanych urządzeń i oprogramowania musi spełniać niżej opisane wymagania:

1. Minimalny okres gwarancji na urządzenia i oprogramowanie wskazany w Formularzu Ofertowym
2. Zamawiający wymaga, aby usługa gwarancyjna na wszystkie dostarczone w ramach zamówienia sprzęt była, przez cały okres jej trwania, świadczona na podstawie wykupionego wsparcia producenta dostarczonych urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczanych urządzeń i 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 rozwiązania. Serwis gwarancyjny świadczony ma być w miejscu instalacji Sprzętów.
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 tożsamy 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 rękomią 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 kalendarzowe 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-Business 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 gwarancyjne.
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.