ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI I

1. Nazwa zamówienia

Dostawa, montaż i konfiguracja Infrastruktury Sieci Podkładowej wraz ze wsparciem technicznym i gwarancją.

2. Definicje:

2.1. Na potrzeby niniejszego dokumentu, określenia poniższe będą miały następujące znaczenie:

2.1.1. **Awaria** – nieprawidłowe działanie Urządzeń lub oprogramowania, w szczególności brak możliwości używania Urządzeń lub oprogramowania w sposób zgodny z ich przeznaczeniem lub z dokumentacją producenta i dokumentacją powykonawczą;

2.1.2. **Dni robocze** – dni od poniedziałku do piątku, oprócz dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej;

2.1.3. **Lokalizacje** – dwa miejsca na terenie miasta stołecznego Warszawy, do których ma nastąpić dostawa przedmiotu zamówienia, a także montaż i konfiguracja. Dokładne adresy zostaną podane do wiadomości Wykonawcy niezwłocznie po podpisaniu umowy;

2.1.4. **SDN** - Programowalna Sieć Komputerowa (ang. Software Defined Networking), której wymagania techniczne opisane są w pkt 8 OPZ;

2.1.5. **Portal Użytkownika i Orkiestrator** – produkty , których wymagania techniczne opisane są w pkt 11 OPZ;

2.1.6. **Montaż i konfiguracja** – w ramach tych prac Zamawiający wymaga w szczególności: instalacji i uruchomienia dostarczonego rozwiązania - adresowania oraz konfiguracji urządzeń sieciowych, zestawienie topologii SDN w obu ośrodkach i pomiędzy nimi, uruchomienia kontrolera SDN, aktualizacji do wersji rekomendowanej przez producenta oprogramowania, jeżeli wymagana, instalację oprogramowania SDN na zwirtualizowanych serwerach, skonfigurowania wyjść L2 i L3 środowiska SDN, uruchomienia centralnego systemu analizy środowisk aplikacyjnych i zarządzania politykami segmentacji na dedykowanej platformie oraz Portalu Użytkownika;

2.1.7. **Wezwanie** - zawiadomienie w przedmiocie realizacji Umowy w zakresie wskazanym w pkt 4 OPZ skierowane do Wykonawcy przez Zamawiającego w terminie do 90 dni od dnia zawarcia Umowy, z zastrzeżeniem że Zamawiający bez konieczności zawarcia aneksu ma możliwość jednokrotnego przedłużenia tego 90-dniowego terminu o nie dłużej niż kolejne 90 dni, o czym poinformuje Wykonawcę, przesyłając informację na adres e-mail wskazany w § 13 ust. 2 Umowy nie później niż 30 dni przed upływem 90-dniowego terminu, o którym mowa w tym zdaniu.

3. Oznaczenie przedmiotu zamówienia wg Kod CPV:

32420000-3 Urządzenia sieciowe;
48000000-8 Pakiety oprogramowania i systemy informatyczne;
48820000-2 Serwery;
72263000-6 Usługi wdrażania oprogramowania;
72611000-6 Usługi w zakresie wsparcia technicznego.

4. Termin realizacji przedmiotu zamówienia:

Maksymalny czas dostawy, Montażu i konfiguracji SDN, Portalu Użytkownika i Orkiestratora oraz przełączników zarządzających, o których mowa w pkt 5.1.1. – 80 dni od Wezwania Zamawiającego, w tym:

4.1. maksymalny czas dostawy – w terminie do 45 dni od dnia Wezwania Zamawiającego;

4.2. maksymalny czas Montażu i konfiguracji, o których mowa w pkt 5.1.2. – w terminie do 35 dni, od dnia podpisania Protokołu Odbioru Dostawy dla danej Lokalizacji.

5. Przedmiot zamówienia:

5.1. Przedmiotem zamówienia jest:

5.1.1. Dostawa SDN oraz Portalu Użytkownika i Orkiestratora, a także przełączników zarządzających obejmująca:

5.1.1.1. sprzedaż i dostarczenie przez Wykonawcę do dwóch Lokalizacji urządzeń wraz z dokumentacją i oprogramowaniem;

5.1.1.2. udzielenie licencji na oprogramowanie oraz dokumentację na warunkach wskazanych w umowie;

5.1.2. Montaż i konfiguracja SDN, Portalu Użytkownika i Orkiestratora oraz przełączników zarządzających wraz z dostarczeniem dokumentacji powykonawczej;

5.1.3. udzielenie przez Wykonawcę gwarancji i wsparcia technicznego na urządzenia i oprogramowanie oraz zapewnienie gwarancji i wsparcia technicznego producenta dla urządzeń i oprogramowania na okres 36 miesięcy od dnia podpisania Protokołu Odbioru Końcowego (może wykonywać autoryzowany partner producenta).

5.1.4. świadczenie usługi tzw. godzin eksperckich w ramach prawa opcji na warunkach określonych poniżej;

[Świadczenie usługi tzw. godzin eksperckich w ramach prawa opcji]

5.1.5. Zamawiający jest uprawniony do zlecenia Wykonawcy w ramach prawa opcji świadczenia usługi tzw. godzin eksperckich przez certyfikowanego przez producenta inżyniera na poziomie eksperta dotyczącej m.in. konsultacji, rozwiania wątpliwości lub rozwiązania bieżących problemów Zamawiającego z obsługi Urządzeń lub oprogramowania w miejscu zainstalowania Urządzeń lub zdalnie, w liczbie do 736 roboczogodzin, realizowanej w Dni Robocze, w godzinach od 9:00 do 17:00.

5.1.6. W zakresie przedmiotu prawa opcji, o którym mowa w pkt 5.1.4. powyżej, rozliczenie wynagrodzenia Wykonawcy będzie następować w oparciu o stawkę godzinową pracy konsultanta, w ramach puli 736 roboczogodzin na zasadach określonych w Umowie, w terminie do 31 grudnia 2022 roku.

5.1.7. Zlecenie w zakresie skorzystania z prawa opcji następować będzie na zasadach określonych w Umowie.

5.1.8. Do praw i obowiązków Wykonawcy oraz Zamawiającego oraz zasad rozliczania Zleceń w ramach skorzystania przez Zamawiającego z prawa opcji zastosowanie mają w całości postanowienia Umowy.

5.1.9. Skorzystanie z prawa opcji jest uprawnieniem Zamawiającego. Zamawiający nie zobowiązuje się w żaden sposób do skorzystania z prawa opcji. Nieskorzystanie przez Zamawiającego z prawa opcji nie rodzi po stronie Wykonawcy jakichkolwiek roszczeń w stosunku do Zamawiającego.

5.1.10. Na wniosek Zamawiającego, usługa tzw. godzin eksperckich zostanie przeprowadzona w trybie online. Wykonawca zobowiązany jest zapewnić wszelkie niezbędne narzędzia do przeprowadzenia usługi online, w tym odpowiednią platformę. Do czasu trwania usługi online nie wlicza się czasu, kiedy nie mogła być prowadzona z przyczyn leżących po stronie

Wykonawcy lub z powodów technicznych, np. zakłócenia połączenia, awaria sprzętu lub oprogramowania.

6. Wymagania ogólne:

6.1. Wykonawca wraz z urządzeniami dokona dostawy wszystkich niezbędnych elementów koniecznych do ich montażu i uruchomiania w Lokalizacjach Zamawiającego takie jak: śrubki, nakrętki, kable zasilające, konieczne patchcordy (kable krosowe) itp.

6.2. Wykonawca wykona montaż urządzeń w miejscach wskazanych przez Zamawiającego oraz dokona konfiguracji w uzgodnieniu z Zamawiającym. Zamawiający wymaga, aby Montaż i konfiguracja została dokonana przez osobę posiadającą odpowiednie uprawnienia, w szczególności posiadającą certyfikat producenta urządzeń, uprawniający do wykonywanych prac.

6.3. Na potwierdzenie wykonania Montażu i konfiguracji zostanie wykonana dokumentacja powykonawcza, obejmująca w szczególności wykaz wszystkich urządzeń i modułów, połączeń sieciowych, opis wykonanego Montażu i konfiguracji w zakresie zaimplementowanej logiki przedmiotu zamówienia. Wykonawca przeniesie na Zamawiającego majątkowe prawa autorskie do dokumentacji powykonawczej na warunkach opisanych w umowie.

6.4. Urządzenia mają być fabrycznie nowe, nieużywane wcześniej, mają być objęte serwisem gwarancyjnym producenta oraz posiadać najnowszą dostępną stabilną wersję oprogramowania.

6.5. Wykonawca powinien posiadać status partnera producenta urządzeń albo oprogramowania, w zależności którego komponentu (urządzenia albo oprogramowanie) wartościowy udział w zamówieniu jest najwyższy (wykaz urządzeń oraz oprogramowania znajduje się w pkt 6 formularza oferty), z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby wykonawca posiadał nie niższy niż drugi w kolejności poziom partnerstwa licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu poprzedzającym.

6.6. Przedmiot zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy o Krajowym systemie cyberbezpieczeństwa, dalej: „Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, przedmiot zamówienia musi być zgodny z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.

6.7. Wykonawca oświadcza, że jest świadomy, iż z uwagi na wymogi bezpieczeństwa obowiązujące w Lokalizacjach, osoby wyznaczone przez Wykonawcę do realizacji prac mogą być zobowiązane do okazania służbom ochrony obiektów, przed rozpoczęciem świadczenia prac w danej Lokalizacji, aktualnego zaświadczenia o niekaralności (informacja z Krajowego Rejestru Karnego).

6.8. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji ul. Królewska 27, 00-060 Warszawa.

6.9. Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z oprogramowania w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją chmury prywatnej na rzecz Ministra Cyfryzacji.

7. Warunki dotyczące gwarancji i świadczenia wsparcia technicznego:

7.1. Dostarczone urządzenia i oprogramowanie objęte będą 36-miesięcznym wsparciem technicznym i serwisem gwarancyjnym.

7.2. W ramach gwarancji do obowiązków Wykonawcy należy usuwanie Awarii najpóźniej do końca Dnia roboczego, następującego po dniu zgłoszenia Awarii, z zastrzeżeniem, że niniejszy termin nie obowiązuje w zakresie Awarii oprogramowania, które mogą zostać usunięte wyłącznie przez producenta. W przypadku gdy Awaria oprogramowania może zostać usunięta wyłącznie przez producenta Wykonawca zawiadomi Zamawiającego o tym fakcie co najmniej w formie dokumentowej na adres e-mail podany przez Wykonawcę, w ciągu 24 godzin od momentu dokonania zgłoszenia Awarii.

7.3. Za chwilę zgłoszenia Awarii Strony uznają chwilę przesłania zgłoszenia do Wykonawcy.

7.4. W razie nieusunięcia Awarii urządzenia w terminie, Wykonawca dostarczy na czas naprawy urządzenie zastępcze o parametrach technicznych nie gorszych od parametrów technicznych urządzenia naprawianego oraz zapewniających nie gorszy poziom bezpieczeństwa do Lokalizacji, w której znajduje się urządzenie.

7.5. W ramach wsparcia technicznego Zamawiający ma prawo w szczególności do:

7.5.1. dostępu do nowych wersji fabrycznie zainstalowanego oprogramowania, sterowników i firmware'u w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z tego oprogramowania;

7.5.2. obsługi świadczonej w języku polskim;

7.5.3. godziny i dni tygodnia przyjmowania zgłoszeń Awarii: 24 godziny na dobę, przez 7 dni w tygodniu.

7.6. Wykonawca zobowiązuje się podać Zamawiającemu, najpóźniej w dniu podpisania Protokołu odbioru dostawy dla każdej Lokalizacji, a także później przy każdej zmianie tych danych, wszelkie dane niezbędne do skorzystania przez Zamawiającego z zakresu gwarancji i wsparcia technicznego, w tym: numerów telefonicznych, adresów e-mail, a także dane dostępowe do: konta w serwisie producenta umożliwiające samodzielne pobieranie oprogramowania w ramach posiadanej licencji.

8. Szczegółowe wymagania techniczne dla SDN:

8.1. Rozwiązanie SDN składa się z uzupełniających się komponentów sprzętowych i programowych tworzących wspólną całość:

a. **Centralnego kontrolera SDN** zarządzającego siecią fizyczną, wirtualną, kontenerową oraz warstwą logiczną i zapewniającego uruchamianie usług w oparciu o modelowanie polityk dla aplikacji.

b. **Centralnego systemu analizy środowisk aplikacyjnych** oraz definiowania, testowania i wymuszania polityk bezpieczeństwa dla aplikacji.

c. **Infrastruktury sieciowej** w postaci przełączników 10/25/40/100 Gigabit Ethernet tworzących sieć o architekturze „IP fabric" (spine/leaf) i znajdujących się pod wyłączną kontrolą komponentu zarządzającego SDN.

8.2. Funkcjonalność architektury systemu SDN i komponentu zarządzającego (kontrolera SDN):

a. Kontroler SDN musi być zrealizowany w oparciu o dedykowaną redundantną warstwę sprzętową i programową. Zasoby sprzętowe (CPU, pamięć, dyski, porty sieciowe) są w pełni dedykowane dla oprogramowania kontrolera SDN.

b. Kontroler SDN musi być zrealizowany redundantnie (np. w formie klastra kilku instancji) zarówno w warstwie sprzętowej jak i programowej tak, aby zapewnić spójne działanie

środowiska i możliwość modyfikacji konfiguracji po ewentualnej utracie jednej z instancji. Minimalna ilość instancji musi zapewnić zarządzanie po utracie jednego z ośrodków.

c. Utrata wszystkich instancji kontrolera SDN nie wpływa na działanie infrastruktury sieciowej w zakresie istniejącej konfiguracji (nie dotyczy to zmian konfiguracji).
d. Kontroler SDN posiada możliwość implementacji w postaci redundantnej w dwóch lokalizacjach dla odległości, co najmniej 500 km (np. w formie klastra złożonego z kilku instancji). W przypadku utraty komunikacji między lokalizacjami (np. split brain) istnieje możliwość dalszej modyfikacji konfiguracji przynajmniej dla jednej z lokalizacji (podstawowego DataCenter). W przypadku utraty podstawowego ośrodka DC musi istnieć mechanizm (inicjowany przez administratora) przywrócenia możliwości zmian w konfiguracji w ośrodku zapasowym i potem poprawna synchronizacja po przywróceniu ośrodka podstawowego.
e. Komunikacja między kontrolerem SDN i elementami infrastruktury sieciowej (tzw. „IP fabric") musi być realizowana w trybie in-band, niewymagającym użycia dedykowanych interfejsów na przełącznikach wchodzących w skład architektury.
f. Kontroler SDN obsługuje wyłącznie ruch związany z zarządzaniem i monitorowaniem infrastruktury sieciowej (tzw. „control plane"), nie zajmuje się przełączaniem ruchu (tzw. „data plane").
g. Kontroler SDN umożliwia zarządzanie infrastrukturą sieciową złożoną z 2000 portów i dołączającą co najmniej 500 fizycznych serwerów dwuprocesorowych (odpowiednie licencje, jeśli wymagane, muszą być dostarczone na docelową pojemność platformy).
h. Kontroler SDN umożliwia zarządzanie infrastrukturą wirtualną złożoną z co najmniej 2000 maszyn wirtualnych VM (odpowiednie licencje, jeśli wymagane, muszą być dostarczone na docelową pojemność platformy).

8.3. Funkcjonalność SDN dla oprogramowania komponentu zarządzającego (kontrolera SDN):

a. Umożliwia automatyzację konfiguracji zarządzanej sieci w oparciu o model sieciowych polityk powiązanych z aplikacjami.
b. Polityka definiowana na kontrolerze opisuje model działania aplikacji w oparciu o relacje pomiędzy punktami styku elementów aplikacji z siecią. W przykładowym modelu trójwarstwowym aplikacji oznacza to:
    i. Zdefiniowanie warstw aplikacji takich jak web, aplikacyjna i bazodanowa (Web, App, DB)
    ii. Zdefiniowanie przydziału serwera wirtualnego do danej warstwy aplikacyjnej/segmentu na bazie jego atrybutów – nazwa maszyny VM, id maszyny VM, nazwa systemu operacyjnego, tagi itp.
    iii. Zdefiniowanie relacji pomiędzy warstwami aplikacyjnymi, jako wzajemnie udostępnianych i konsumowanych zasobów opisanych przez polityki bezpieczeństwa (filtracji oraz przekierowania na zewnętrzne urządzenia bezpieczeństwa).
c. Umożliwia zintegrowanie usług zewnętrznych poprzez zapewnienie mechanizmu przekierowania ruchu dla warstw 4-7 dla funkcjonalności Next Generation Firewall.
d. Dla izolowanych środowisk sieciowych SDN umożliwia implementację funkcjonalności dedykowanej bramy wyjściowej L3 oraz dedykowanych usług zewnętrznych realizowanych dla warstw 4-7.
e. Realizuje tworzenie segmentów sieci L2 i L3 w oparciu o technologię VXLAN.
f. Realizuje sprzętowy VTEP.
g. Umożliwia monitorowanie i diagnostykę sieciową dla uruchamianych środowisk w oparciu o następujące mechanizmy:
    i. Prezentację sprawności środowiska/aplikacji w formie wskaźnika stanu zdrowia

ii. Prezentowanie bieżącej i historycznej statystyki ruchu dla danego środowiska sieciowego
iii. Diagnostykę ścieżki (traceroute) między dowolną parą portów fizycznych bądź wirtualnych wchodzących w skład infrastruktury
iv. Monitorowanie i raportowanie ilości wykorzystanych i dostępnych zasobów wchodzących w skład infrastruktury
v. Monitorowanie ruchu poprzez kopiowanie (mirroring) ruchu dla wybranych warstw aplikacyjnych lub interfejsów sieciowych

h. Umożliwia automatyczną detekcję topologii oraz inwentarza infrastruktury sieciowej. Dopuszcza się realizację na innym komponencie zarządzania pod warunkiem zapewnienia dedykowanej, redundantnej platformy sprzętowej.
i. Implementuje centralne repozytorium oprogramowania (firmware) dla infrastruktury sieciowej. Dopuszcza się realizację na innym komponencie zarządzania pod warunkiem zapewnienia dedykowanej, redundantnej platformy sprzętowej.
j. Implementuje centralny mechanizm aktualizacji oprogramowania (firmware) dla infrastruktury sieciowej. Dopuszcza się realizację na innym komponencie zarządzania pod warunkiem zapewnienia dedykowanej, redundantnej platformy sprzętowej.
k. Udostępnia interfejs zarządzania poprzez GUI.
l. Integracja z Active Directory.
m. Udostępnia następujące mechanizmy programowania (alternatywa do GUI):
    i. REST API ze wsparciem dla formatu XML;
    ii. Możliwość konfiguracji infrastruktury bezpośrednio poprzez HTTP (np. z wykorzystaniem Postman REST Client);
    iii. Python SDK;
    iv. Powszechnie dostępna dokumentacja dla REST API.

i. Udostępnia autoryzację dostępu użytkowników w oparciu o mechanizmy LDAP lub lokalne definicje.
j. Umożliwia synchronizację całej infrastruktury sieciowej w oparciu o protokół NTP.

8.4. Funkcjonalność centralnego systemu analizy środowisk aplikacyjnych i zarządzania politykami segmentacji

a. Centralny system analizy środowisk aplikacyjnych dostarcza zautomatyzowane mechanizmy modelowania aplikacji w Data Center i w chmurach publicznych, generowania polityk bezpieczeństwa, ich testowania, audytowania i ochrony serwerów.
b. System składa się z następujących elementów:
    i. Oprogramowanie centralnego systemu analizy środowisk aplikacyjnych i zarządzania politykami segmentacji.
    ii. Platformy sprzętowej zapewniającej odpowiednie zasoby CPU, pamięci i dyskowe na potrzeby oprogramowania. Minimalnie jest to:
        a. 6TB RAM
        b. 288 vCPU

    Platforma sprzętowa musi posiadać oficjalne wsparcie producenta oprogramowania i zawierać wszystkie licencje i subskrybcje niezbędne do poprawnego działania.
    iii. Agenci programowi, zainstalowani na końcowych systemach operacyjnych przekazujący dane o stacjach końcowych oraz wymuszający polityki bezpieczeństwa.
    iv. Zewnętrzne źródła danych, przekazujące lub pobierające dane poprzez API.
c. System umożliwia import danych z systemów CMDB/IPAM celem wzbogacenia analizy metadanych o dodatkowe informacje typu nazwa hosta, aplikacji, środowiska, projektu itp.

d. System umożliwia wprowadzanie własnych etykiet/tagów, które można następnie wykorzystać w budowaniu opartych o nie polityk (typu zakaz ruchu pomiędzy stacjami końcowymi oznaczonymi etykietą DEV a tymi oznaczonymi PROD).
e. Funkcje modelowanie aplikacji i budowy polityk na potrzeby segmentacji:
   i. Na bazie zebranych danych z różnych źródeł system rekomenduje politykę segmentacji opartą o tzw. „white-listing", czyli otwarcie do komunikacji tylko wymaganych i wykorzystywanych portów wymaganych do działania aplikacji.
   ii. System umożliwia testowanie polityki a następnie jej wymuszenie.
   iii. System wizualizuje topologię aplikacji w danym obszarze (podział na warstwy/segmenty).
   iv. System wizualizuje mapę polityki (przepływy pomiędzy segmentami/workload z dokładnością do L4).
f. Funkcje ochrony systemów końcowych i wymuszania polityk:
   i. System gromadzi dane z agentów na stacjach końcowych (OS) i wykorzystuje je w korelacji z innymi źródłami.
   ii. Gromadzone dane obejmują informacje o portach, protokołach i procesach.
   iii. System potrafi wizualizować informację o procesach uruchomionych na stacji końcowej (drzewo lub lista procesów).
   iv. Oprogramowanie agentów działa zarówno w środowiskach zwirtualizowanych jak i na serwerach fizycznych.
   v. Oprogramowanie agentów wspiera systemy Linux i Windows.
   vi. Oprogramowanie agentów wspiera hosty dla środowisk kontenerów.
   vii. Platforma koreluje dane ze stacji końcowych (workload) z informacjami o znanych lukach lub ekspozycji w zabezpieczeniach np. importowanych z bazy podatności CVE bezpośrednio lub poprzez dodatkowo integrowane narzędzie.
   viii. Platforma pokazuje ocenę/rating poziomu zagrożeń dla danej aplikacji (workload) bezpośrednio lub poprzez dodatkowo integrowane narzędzie.
   ix. Platforma jest w stanie wymusić politykę opisującą aplikację poprzez konfigurację firewall właściwego dla stacji końcowej (ip tables dla Unix lub Windows Firewall).
g. Centralny system analizy środowisk aplikacyjnych wspiera minimum 2000 urządzeń końcowych (serwery fizyczne lub maszyny wirtualne) z możliwością podwojenia tej liczby.
h. Jeśli dla celów realizacji opisanych powyżej funkcjonalności konieczna jest dostarczenie licencji na komponenty sprzętowe, programowe lub inne to wymaga się jej dostarczenia. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 36 miesięcy.

8.5. Funkcjonalność sprzętowa dla infrastruktury sieciowej („IP fabric") pozostającej pod nadzorem komponentu zarządzającego (kontrolera SDN):
a) Złożona z przełączników 10/25/40/100 GigabitEthernet, opisanych w oddzielnych punktach, zorganizowanych w dwustopniowej, nieblokowalnej architekturze rdzeń-brzeg (spine-leaf) określanej jako „IP fabric".
b) Przełączniki są wspierane i zarządzane przez komponent zarządzający (kontroler SDN) opisany powyżej.
c) Jeśli do współpracy z komponentem zarządzającym (kontrolerem) konieczna jest dla przełącznika licencja to wymagane jest jej dostarczenie. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 36 miesięcy.
d) Zarządzana jako całość poprzez centralny komponent zarządzający (kontroler).

e) Wszystkie połączenia między warstwą brzegową i rdzeniową w ramach fabric implementowane są jako 100GE o pełnej wydajności (wirespeed) z wykorzystaniem interfejsów QSFP i połączeń 100GE opartych o jednoparowe okablowanie multimodowe LC.
f) Implementuje następujące protokoły i mechanizmy L2:
    i. Sprzętowe wsparcie dla VXLAN Bridging i VXLAN Routing w oparciu o sprzętowy VTEP
    ii. Dołączanie urządzeń zewnętrznych (serwerów, modułów, przełączników) poprzez zagregowaną wiązkę połączeń LACP 802.3ad do dwóch przełączników brzegowych (multi link aggregation, virtual port channel, itp.)
    iii. Pełna mobilność serwera fizycznego i wirtualnego w domenie L2, również pomiędzy kilkoma DC
    iv. Definiowanie zewnętrznych połączeń w domenie L2
    v. Mechanizm eliminacji pętli na przełącznikach brzegowych w IP Fabric
g) Implementuje następujące protokoły i mechanizmy L3:
    i. IPv4 Unicast i Multicast
    ii. Przesyłanie IPv6 Unicast
    iii. Niezależne sieci prywatne (VRF) z duplikacją adresacji IP
    iv. Protokoły routingu eBGP, iBGP, OSPF dla IPv4 i IPv6
    v. Routing statyczny dla IPv4 i IPv6
    vi. Przełączanie ruchu pomiędzy parą podsieci IP (SVI) realizowane sprzętowo w modelu IP Anycast w ramach fabric tj. na każdym przełączniku brzegowym, niezależnie od ilości przełączników brzegowych w fabric
    vii. Pełna mobilność serwera fizycznego i wirtualnego w domenie L3
    viii. Interfejsy i subinterfejsy L3 (per VLAN) na portach fizycznych przełączników brzegowych
    ix. Definiowanie zewnętrznych połączeń w domenie L3 opartych o protokoły routingu statycznego lub dynamicznego (OSPF lub BGP)
h) Implementuje następujące mechanizmy optymalizacji ruchu:
    i. Load-balancing pakietów dostosowany się do różnych warunków przesyłania (natłoku) w ramach środowiska opartego o ECMP
    ii. Priorytetyzacja połączeń

8.6. Wymagana jest pełna kompatybilność pomiędzy kontrolerem SDN a urządzeniami sieciowymi.
8.7. Wymaga się dostarczenia następującej liczby urządzeń sieciowych i ich typów:

d. Urządzenie typu leaf z portami dostępowymi 48x 10/25G dla wkładek SFP+: 32 sztuki;
e. Urządzenie typu spine z portami 32x 40/100G QSFP: 4 sztuki;
f. Urządzenie typu przełącznik tranzytowy z portami 36x 40/100G QSFP: 4 sztuki.

8.8. Wszystkie urządzenia sieciowe muszą pochodzić od jednego producenta.

9. Szczegółowe wymagania dla urządzeń sieciowych:

9.1. Urządzenie typu leaf z portami dostępowymi 48x 10/25G dla wkładek SFP+

1. Przełącznik posiada:
    a. Minimum 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+
    b. Minimum 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m).
2. Parametry wydajnościowe:
    a. Prędkość przełączania minimum 1.8Tbps full duplex
    b. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:
    a. Trunking IEEE 802.1Q VLAN;
    b. Wsparcie dla 3000 sieci VLAN;
    c. Wsparcie sprzętowe dla 250 tysięcy adresów MAC
    d. IEEE 802.1w Rapid Spanning Tree (RST)
    e. IEEE 802.1s Multiple Spanning Tree (MST)
    f. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
    g. Internet Group Management Protocol (IGMP) Versions 2, 3;
    h. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
    i. Link Aggregation Control Protocol (LACP): IEEE 802.3ad
    j. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
    k. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
    l. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4. Przełącznik posiada następującą funkcjonalność dla 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)
    e. VRRP
    f. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6
    g. Tunele GRE
    h. Wsparcie sprzętowe dla minimum 800 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP
    i. Wsparcie dla VRF
    j. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP)
    k. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
    l. Wsparcie dla IGMPv3 oraz MSDP
    m. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych
    n. Obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (access control list)
5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
    a. Zintegrowany, sprzętowy VXLAN Bridging/Routing
    b. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
    c. Implementacja VXLAN BGP EVPN (Ethernet VPN)

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

6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   a. Layer 2 IEEE 802.1p (CoS) oraz DSCP
   b. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6)
   c. Kolejkowanie bezwzględne (strict-priority)
   d. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection)
   e. Ograniczanie ruchu (policing) do zadanej przepływności
   f. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   g. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   a. Obsługa list kontroli dostępu (ACL)
      i. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
      ii. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
      iii. ACL oparte o porty (PACL);
   b. DHCP Snooping
   c. ARP Inspection
   d. IP Source Guard
   e. Unicast reverse path forwarding (uRPF)
   f. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
8. Przełącznik wspiera następujące 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, v2c, v3;
   j. Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB.
   k. Role-Based Access Control RBAC;
   l. IEEE 802.1ab LLDP
   m. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   n. 802.1x
   o. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   p. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)

q. Network Time Protocol (NTP);
r. Precision Time Protocol IEEE 1588
s. Diagnostyka procesu BOOT;
t. Ping
u. Traceroute

9. 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 kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika.
   d. Interfejs programistyczny REST API wraz z upublicznionym SDK
   e. Możliwość zainstalowania klienta Chef
   f. Możliwość zainstalowania agenta Puppet
   g. Wsparcie dla OpenStack Neutron plugin
10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.
11. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”,
12. Wyposażenia przełącznika:
    a. 2 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional)
    b. 48 wkładek SFP+ typu 10/25GBASE-SR
13. Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym (kontrolerem opisanym w odpowiednim punkcie). Istnieje możliwość zmiany trybu pracy (np. poprzez wymianę oprogramowania lub wgranie odpowiedniej licencji jeśli potrzebne), nie dopuszcza się konieczności modyfikacji sprzętowej urządzeń. Jeśli dla celów realizacji tych funkcjonalności konieczna jest dla przełącznika licencja to wymaga się jej dostarczenia. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 36 miesięcy.

9.2. Urządzenie typu spine z portami 32x 40/100G QSFP

1. Przełącznik posiada min. 32 porty 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m).
2. Parametry wydajnościowe:
   a. Prędkość przełączania 3.2Tbps full duplex
   b. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:
   a. Trunking IEEE 802.1Q VLAN;
   b. Wsparcie dla 3000 sieci VLAN;
   c. Wsparcie sprzętowe dla 90 tysięcy adresów MAC
   d. IEEE 802.1w Rapid Spanning Tree (RST)
   e. IEEE 802.1s Multiple Spanning Tree (MST)
   f. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
   g. Internet Group Management Protocol (IGMP) Versions 2, 3;
   h. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach

i. Link Aggregation Control Protocol (LACP): IEEE 802.3ad;
j. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
k. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
l. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI

4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:
   a. Sprzętowe przełączanie pakietów w warstwie L3
   b. Routing w oparciu o trasy statyczne
   c. Umożliwia rozbudowę poprzez licencje o funkcjonalności warstwy L3 – OSPF, BGP, IS-IS dla protokołów IPv4 oraz IPv6
   d. Policy Based Routing (PBR)
   e. VRRP
   f. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6
   g. Tunele GRE
   h. Wsparcie sprzętowe dla minimum 60 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP
   i. Wsparcie dla VRF
   j. Wybór do 16-tu jednoczesnych ścieżek o równej metryce (ECMP)
   k. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
   l. Wsparcie dla IGMPv3 oraz MSDP
   m. Wsparcie sprzętowe dla minimum 12,000 tras multicast
   n. Obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (access control list)
5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   a. Zintegrowany, sprzętowy VXLAN Bridging/Routing
   b. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
   c. Implementacja VXLAN BGP EVPN (Ethernet VPN)
   d. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN
6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   a. Layer 2 IEEE 802.1p (CoS) oraz DSCP
   b. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6)
   c. Kolejkowanie bezwzględne (strict-priority)
   d. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection)
   e. Ograniczanie ruchu (policing) do zadanej przepływności
   f. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   g. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   a. Obsługa list kontroli dostępu (ACL)
      i. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
      ii. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
      iii. ACL oparte o porty (PACL);
   b. DHCP Snooping

   c. ARP Inspection
   d. IP Source Guard
   e. Unicast reverse path forwarding (uRPF)
   f. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
8. Urządzenie realizuje następujące funkcjonalności dotyczące zarządzania i zabezpieczenia:
   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. Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB.
   k. Role-Based Access Control RBAC;
   l. IEEE 802.1ab LLDP
   m. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   n. 802.1x
   o. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   p. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)
   q. Network Time Protocol (NTP);
   r. Precision Time Protocol IEEE 1588
   s. Diagnostyka procesu BOOT;
   t. Ping
   u. Traceroute
9. Narzędzia programowania i zarzadzania przełącznikiem:
   a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
   b. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika
   c. Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika.
   d. Interfejs programistyczny REST API wraz z upublicznionym SDK
   e. Możliwość zainstalowania klienta Chef
   f. Możliwość zainstalowania agenta Puppet
10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych;
11. Obudowa o rozmiarach maksymalnie 2RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
12. Wyposażenia przełącznika:
   a. 16 wkładek QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional).

13. Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym (kontrolerem opisanym w odpowiednim punkcie). Istnieje możliwość zmiany trybu pracy (np. poprzez wymianę oprogramowania lub wgranie odpowiedniej licencji jeśli potrzebne), nie dopuszcza się konieczności modyfikacji sprzętowej urządzeń. Jeśli dla celów realizacji tych funkcjonalności konieczna jest dla przełącznika licencja to wymaga się jej dostarczenia. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 36 miesięcy.

9.3. Urządzenie typu przełącznik tranzytowy z portami 36x 40/100G QSFP

1. Przełącznik posiada min. 36 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m) lub jednomodowej o zasięgu minimum 25km.
2. Parametry wydajnościowe:
    a. Prędkość przełączania 3.6Tbps full duplex
    b. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:
    a. Trunking IEEE 802.1Q VLAN;
    b. Wsparcie dla 3000 sieci VLAN;
    c. Wsparcie sprzętowe dla 256 tysięcy adresów MAC
    d. IEEE 802.1w Rapid Spanning Tree (RST)
    e. IEEE 802.1s Multiple Spanning Tree (MST)
    f. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
    g. Internet Group Management Protocol (IGMP) Versions 2, 3;
    h. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
    i. Link Aggregation Control Protocol (LACP): IEEE 802.3ad;
    j. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
    k. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
    l. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:
    a. Sprzętowe przełączanie pakietów w warstwie L3
    b. Routing w oparciu o trasy statyczne
    c. Umożliwia rozbudowę poprzez licencje o funkcjonalności warstwy L3 – OSPF, BGP, IS-IS dla protokołów IPv4 oraz IPv6
    d. Policy Based Routing (PBR)
    e. VRRP
    f. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6
    g. Tunele GRE
    h. Wsparcie sprzętowe dla minimum 800 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP
    i. Wsparcie dla VRF
    j. Wybór do 16-tu jednoczesnych ścieżek o równej metryce (ECMP)
    k. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
    l. Wsparcie dla IGMPv3 oraz MSDP
    m. Wsparcie sprzętowe dla minimum 32,000 tras multicast
    n. Obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (access control list)

5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
    e. Zintegrowany, sprzętowy VXLAN Bridging/Routing
    f. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
    g. Implementacja VXLAN BGP EVPN (Ethernet VPN)
    h. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN
6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Layer 2 IEEE 802.1p (CoS) oraz DSCP
    b. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6)
    c. Kolejkowanie bezwzględne (strict-priority)
    d. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection)
    e. Ograniczanie ruchu (policing) do zadanej przepływności
    f. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
    g. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
    a. Obsługa list kontroli dostępu (ACL)
        i. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
        ii. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
        iii. ACL oparte o porty (PACL);
    b. DHCP Snooping
    c. ARP Inspection
    d. IP Source Guard
    e. Unicast reverse path forwarding (uRPF)
    f. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
8. Urządzenie realizuje następujące funkcjonalności dotyczące zarządzania i zabezpieczenia:
    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. Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB.
    k. Role-Based Access Control RBAC;
    l. IEEE 802.1ab LLDP
    m. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
    n. 802.1x

   o. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   p. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)
   q. Network Time Protocol (NTP);
   r. Precision Time Protocol IEEE 1588
   s. Diagnostyka procesu BOOT;
   t. Ping
   u. Traceroute
9. Narzędzia programowania i zarzadzania przełącznikiem:
   a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
   b. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika
   c. Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika.
   d. Interfejs programistyczny REST API wraz z upublicznionym SDK
   e. Możliwość zainstalowania klienta Chef
   f. Możliwość zainstalowania agenta Puppet
10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych;
11. Obudowa o rozmiarach maksymalnie 2RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
12. Wyposażenia przełącznika:
   a. 6 wkładek QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional)
   b. 2 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów jednomodowych o zasięgu minimum 25km
13. Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym (kontrolerem opisanym w odpowiednim punkcie). Istnieje możliwość zmiany trybu pracy (np. poprzez wymianę oprogramowania lub wgranie odpowiedniej licencji jeśli potrzebne), nie dopuszcza się konieczności modyfikacji sprzętowej urządzeń. Jeśli dla celów realizacji tych funkcjonalności konieczna jest dla przełącznika licencja to wymaga się jej dostarczenia. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 36 miesięcy.

10. Szczegółowe wymagania techniczne dla przełączników zarządzających – sztuk 16

1. Muszą pochodzić od tego samego producenta co przełączniki dla Infrastruktury Sieciowej, o której mowa w pkt 8 OPZ;
2. Minimum 48 fizycznych portów 10/100/1000 (RJ-45);
3. Minimum 2 porty 10GBASE-SR;
4. Przepustowość minimum 105Gbps;
5. Szybkość przełączania 120 Mpps;
6. Przełącznik musi posiadać dedykowany port konsoli (RS-232) oraz dedykowany port typu out-of-band management (Ethernet RJ-45);
7. Możliwość budowania stosu z innymi przełącznikami tego samego typu – minimum 8 przełączników w jednym stosie;
8. Urządzenie musi obsługiwać min. 12000 adresów MAC oraz min. 1000 sieci VLAN;
9. Urządzenie musi umożliwiać agregację łączy, minimum 8 portów;

10. Wsparcie dla protokołów dynamicznego routingu – RIP, OSPF stub oraz routingu statycznego;
11. Urządzenie musi mieć możliwość pobrania konfiguracji w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona;
12. Urządzenie musi posiadać redundantne zasilacze;
13. Przystosowane do montażu w 19” szafie rack (zestaw montażowy dostarczony z urządzeniem).

11. Szczegółowe wymagania techniczne dla Portalu Użytkownika i Orkiestratora:

11.1. Zapewnienie funkcjonalności - Katalog usług:

- interfejs pozwalający na prezentację i samodzielnie zamawianie przez użytkowników zdefiniowanych wcześniej komponentów SaaS, PaaS oraz IaaS z dostępnego katalogu usług;
- interfejs pozwalający na pozyskiwanie, edycję oraz przechowywanie zdefiniowanych usług w katalogu usług;
- tworzenie pozycji w katalogu usług przez dedykowanych administratorów;
- interfejsy dostępne poprzez przeglądarkę, bez konieczności instalowania komponentów trzecich lub plug-in;
- interfejs użytkownika dopasowany do wymagań wizualnych i szaty graficznej Zamawiającego, spersonalizowany, w języku polskim, pozwalający wyświetlać komunikaty, filmy video i usługi w formie portletów;
- prezentacja cen usług w katalogu usług oraz kosztów posiadanych przez użytkownika usług;
- różne modele wyceny usług z katalogu usług – stałe ceny jednostkowe oraz dynamiczne ceny usługi zależne od definiowanych przez użytkownika parametrów (np. zależne od wybranej ilości pamięci serwera lub procesorów);
- śledzenie stanu zamówionych usług przez administratorów i użytkowników;
- mechanizm generowania raportów zamawiania i wykorzystywania posiadanych usług;
- wydzielone role administratora usług, administratora systemu, osoby akceptującej zgłoszenia oraz użytkownika tworzącego i zarządzającego usługi w katalogu usług;
- wbudowana obsługa jednoczesnych wielu różnych środowisk odbiorców (multi-tenant). Całkowite oddzielenie administratorów, użytkowników, usług, raportów etc. W zależności od tego, z którego środowiska loguje się użytkownik;
- mechanizm Role-Based Access Control (RBAC) w celu definiowania poziomu uprawnień dostępu do usług katalogu usług;
- mechanizmy akceptacji, przeglądania, eskalacji oraz kolejkowania zgłoszeń wspólnie przez wydzielone grupy administratorów;
- wsparcie dla wielotorowego i wielopoziomowego procesu akceptacji zamawianych usług.

11.2. Zapewnienie funkcjonalności - Zamawianie:

- mechanizmy prezentacji ograniczonej części katalogu usług bazując na źródłowej organizacji, roli użytkownika, dające dostęp jedynie do wydzielonej puli usług i zadań;
- konfiguracja uprawnień użytkowników do zamawiania usług na podstawie przynależności do określonej grupy lub roli;
- mechanizm wyszukiwania usług z katalogu za pomocą nazwy, kategorii, opisu;
- możliwość wyboru języka dla użytkownika zamawiającego usługi z katalogu usług;
- możliwość oceny poziomu zadowolenia/przydatności produktów zamawianych z katalogu usług przez użytkowników;
- informacja o końcowej cenie usługi dla użytkownika;
- zamawianie
    - za pomocą uproszczonego mechanizmu wyboru (one-click order),
    - zamawianie usług w oparciu o mechanizm shopping-cart,

  - zamawianie usług w imieniu innego użytkownika;
- mechanizm automatycznego wstępnego wypełniania formatek danymi z profilu użytkownika oraz wcześniej pobranymi informacjami;
- możliwość wykonywania samodzielnych akcji na zamówionych przez użytkownika usługach odpowiednich dla typu zamówionej usługi. Użytkownik musi mieć możliwość dokonywania zmian zamówionych usług takich jak kasowanie usługi, zmiana rozmiaru, ilości, etc.;
- obsługa proaktywnej komunikacji z użytkownikiem, podpowiadanie odpowiedzi w formatkach, wstępne proponowanie wypełnienia formatki, dane dynamicznie wymieniane w formatkach na podstawie wyborów i odpowiedzi użytkownika we wcześniejszym polu;
- funkcja samodzielnego kasowania zamówionej usługi przez użytkownika;
- definicja punktu w procesie dostarczania usługi, powyżej którego zgłoszenie nie może być anulowane przez zamawiającego;
- śledzenie wielu różnych zamówień użytkownika na podstawie wyboru ich stanu;
- mechanizm powiadamiania o zamówieniu za pomocą email;
- dynamiczne adresy URL w wiadomościach email wysyłanych jako potwierdzenia i zadania do użytkowników i administratorów;
- mechanizm prezentujący ilość oraz rodzaje usług posiadanych zbiorczo przez użytkowników danego działu;
- mechanizm automatycznego tworzenia zgłoszenia w katalogu jako wynik zewnętrznego zdarzenia;
- łatwy sposób akceptacji przez administratora zamówień użytkownika oraz prezentacji ile i jakich usług oczekuje na akceptację;
- mechanizm warunkowego zatwierdzenia zgłoszenia na podstawie typu zgłoszenia, rodzaju usługi, ilości zamówionych elementów z katalogu usług;
- obsługa akceptacji zamawianych usług na zasadzie kolejek. Kolejki muszą dodatkowo posiadać swojego super użytkownika, zarządzającego zadaniami i nadzorującego pracę osób akceptujących.

11.3. Zapewnienie funkcjonalności - Projektowanie usług:

- nieprogramistyczny interfejs na potrzeby tworzenia i modyfikowania pozycji z katalogu usług;
- praca na formatkach modularnych wielokrotnego wykorzystania;
- możliwość modułowego budowania formularza, który umożliwia współdzielenie pól i formularzy w ramach różnych usług;
- możliwość wielokrotnego użycia całości lub części skonfigurowanych procesów dostarczania usług;
- mechanizm centralnego przechowywania i wykorzystywania atrybutów i zestawów danych komponentów do wielokrotnego wykorzystywania w formatkach;
- interfejs niebazujący na programowaniu dla pokazywania i ukrywania pól formularza na podstawie roli użytkownika, zamawianych usług, itp.;
- mechanizm rozbicia formatek na różne strony;
- definicja reguł biznesowych dyktujących dynamiczne zależności między polami formularza, np. gdy użytkownik wybierze „Desktop” na zamówienie sprzętu, następne pole zapełnia się listą typów komputerów stacjonarnych. Te reguły biznesowe nie mogą wymagać programowania;
- nieprogramistyczny mechanizm pokazywania dodatkowych pól lub ukrywania ich w zależności od interakcji użytkownika z formatką;
- nieprogramistyczny sposób dostępu do baz danych i wykorzystania danych w formularzach i usługach;
- szeregowanie zadań (workflow) z możliwością wielokrotnego wykorzystania;

- dynamiczne zmiany przepływu zadań (workflow) na podstawie informacji zebranych od użytkownika;
- szeregowe i równoległe przetwarzanie zadań (workflow);
- mechanizm obsługi zamówień/realizacji usług z katalogu usług przez podmioty trzecie, zewnętrzne będące poza kontrolą organizacji;
- możliwość przekazania użytkownikowi informacji pomocniczych w postaci tekstu oraz łączy w celu instruowania podania poprawnych danych wejściowych dla usług;
- podejrzenie stanu poszczególnych usług – otwarty, zamknięty, odrzucony;
- dodawanie grafik dla usług umieszczanych w katalogu usług.

11.4. Zapewnienie funkcjonalności - Łącznik chmurowy:

- mechanizm samodzielnego projektowania i umieszczenia w katalogu potrzebnych usług PaaS, IaaS. Graficzne projektowanie szablonu aplikacji (ilość warstw aplikacji, sposób połączenia komponentów), następnie wypełnienie komponentów szablonu wg pełnionej roli i wymaganej aplikacji (serwer www apache, baza sql, loadbalancer etc.), sparametryzowanie ich, a w finalnym kroku umieszczenie w katalogu usług;
- środowisko pozwala na samodzielne opisanie tworzonych usług, przydzielanie praw dostępu, umieszczanie grafik i wskazywanie katalogów, w jakich ma się docelowo znaleźć usługa;
- obsługiwane szablony pozwalają na tworzenie aplikacji złożonych co najmniej z 3 poziomów serwerów z możliwością umieszczenia wielu wirtualnych maszyn oraz kontenerów na każdym z poziomów aplikacji;
- możliwość uruchamiania przez użytkownika w dowolnym obsługiwanym środowisku chmurowym prywatnym oraz publicznym aplikacji wg zdefiniowanego szablonu. Rozwiązanie tłumaczy schemat aplikacji na język/API obsługiwanych chmur;
- dostarczanie zgodnie ze wzorcem zawartym w szablonie, odpowiednio do wybranego środowiska chmurowego przez użytkownika, instalowanie komponentów aplikacji, ładowanie poprawek, skryptów, personalizacja, konfiguracja zabezpieczeń a w końcowym kroku przekazanie użytkownikowi danych do logowania do gotowej aplikacji;
- dla każdej aplikacji definicja parametrów takich jak: nazwa aplikacji, obraz bazowy, ilość zamawianych kopii, rodzaj paczki z aplikacją, miejsce położenia aplikacji, tagi, wskazanie opcjonalnych skryptów do uruchomienia przed/po dostarczeniu aplikacji, przed/po usunięciu aplikacji, reguły komunikacji - adresy, porty, protokoły na których komunikują się komponenty aplikacji, parametry wydajnościowe aplikacji - ilość wymaganych rdzeni, pamięci RAM, przestrzeni na dysku, parametry dodatkowe do wykorzystania w skryptach. Funkcjonalność dostępna w sposób nieprogramistyczny i integralny z interfejsu graficznego. Środowisko umożliwia administratorom definicję aplikacji wg wskazanych wyżej parametrów w sposób graficzny z zasadami przeciągnij i upuść;
- wbudowana obsługa wielu różnych środowisk odbiorców (multi-tenant). Całkowite oddzielenie administratorów, użytkowników, usług, raportów etc. w zależności od tego z którego środowiska loguje się użytkownik;
- mechanizm Role-Based Access Control (RBAC) w celu definiowania poziomu uprawnień dostępu do usług;
- powołanie zasobów obliczeniowych, maszyn wirtualnych i kontenerów w środowiskach chmur publicznych oraz prywatnych;
- możliwość powoływania aplikacji z zasobami w różnych środowiskach chmurowych;
- powołanie, edycja oraz usuwanie gotowych aplikacji w wybranych przez użytkownika środowiskach chmurowych prywatnych oraz publicznych. Zmiana parametrów działania, przypisanie dodatkowych zasobów (np. cpu), przesuwanie aplikacji pomiędzy obsługiwanymi

środowiskami np. z chmury publicznej na prywatną lub odwrotnie, wdrażanie nowej wersji oprogramowania;

- konsola zarządzająca z interfejsem Web dostarcza w sposób graficzny:
  - portal administratora i użytkownika z katalogiem aplikacji do samodzielnego zamawiania przez użytkowników we wskazanych chmurach,
  - instrumenty raportowania stanu zasobów fizycznych i wirtualnych, czas wykorzystania, ilość posiadanych aplikacji, właścicieli aplikacji,
  - mechanizm pozwalający na określenie kosztów aplikacji, definiowanie i przydzielanie budżetu dla każdej z chmur,
  - mechanizm testowania wydajności aplikacji w wybranym przez użytkownika środowisku, raportowanie wydajności względem kosztów,
  - mechanizm porównujący wydajność w kilku wybranych środowiskach do ceny powołania w nich aplikacji,
  - mechanizm pozwalający w sposób graficzny podglądać architekturę wybranej z katalogu aplikacji i powiązania między komponentami,
  - interfejs pozwalający konfigurować komponenty aplikacji znajdujące się w katalogu usług. Interfejs pozwala na konfigurację zależności między komponentami w sposób graficzny, za pomocą mechanizmu przeciągnij i upuść,
  - mechanizm oznaczania aplikacji za pomocą zdefiniowanych tagów;
- otwarte API do integracji z narzędziami orkiestracji chmury;
- zgodność definicji polityki bezpieczeństwa między chmurami prywatnymi i publicznymi;
- oficjalne wsparcie producenta do łączenia z co najmniej następującymi chmurami prywatnymi (obsługa musi być gotowa, tzn. bez konieczności dodatkowej integracji,
  - VMware VSphere
  - Microsoft Azure
  - OpenStack
- obsługa co najmniej 2700 maszyn wirtualnych dla jednej w powyższych chmurach prywatnych oraz na platformach wirtualizacyjnych (łącznie) przez 36 miesięcy;
- gotowość oprogramowania do rozszerzenia o obsługę co najmniej dwóch spośród poniższych chmur prywatnych:
  - Kubernetes
  - Cisco UCS Director
  - VMware vCloud Director
- gotowość oprogramowania do rozszerzenia o obsługę co najmniej trzech spośród poniższych chmur publicznych:
  - Amazon
  - Microsoft Azure
  - Google Compute Platform
  - IBM SoftLayer
- repozytorium obrazów wykorzystywanych do dostarczania zamawianych aplikacji, obsługa wersji obrazów;
- mechanizmy ujednoliconego zabezpieczania ruchu w chmurze prywatnej i w chmurze publicznej zadawane z poziomu konsoli zarządzania umieszczonej w chmurze prywatnej:
  - definiowanie filtrowania ruchu pomiędzy komponentami aplikacji,
  - obsługa klasyfikacji ruchu w oparciu o adresację IP oraz atrybuty maszyn wirtualnych,
  - obsługa maszyn należących do kilku stref bezpieczeństwa,
  - obsługa rozwiązań multi-tenant,
  - konfiguracja polityk w oparciu o szablony i pliki konfiguracyjne,

  - przydzielanie aplikacji/maszyn do różnych stref/chmur w zależności od sposobu tagowania aplikacji. Np. aplikacja oznaczona jako testowa nie może być umieszczona w chmurze infrastruktury produkcyjnej,
  - integracja z sieciami wirtualnymi dostarczanymi w ramach rozwiązania;
- mechanizm raportowania i liczenia kosztów wykorzystanej infrastruktury w obsługiwanych środowiskach publicznych i prywatnych. Zestawienie wydatków za moc obliczeniową, powierzchnię dyskową, sieci oraz usługi w środowiskach. Analiza wykorzystania rozwiązania w zadanym okresie. Podpowiedzi dotyczące wymiarowania maszyn do powierzonego zadania celem optymalizacji kosztów.

Pozostałe wymagania zostały opisane w Projektowanych postanowieniach Umowy, które zawarte są w rozdziale III SWZ.