ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Nazwa zamówienia**
   Dostawa, montaż i konfiguracja Programowalnej Sieci Komputerowej (ang. SDN).

2. **Oznaczenie przedmiotu zamówienia wg Kod CPV:**
   32420000-3 Urządzenia sieciowe
   48000000-8 Pakiety oprogramowania i systemy informatyczne
   72263000-6 Usługi wdrażania oprogramowania
   72611000-6 Usługi w zakresie wsparcia technicznego

3. **Termin realizacji przedmiotu zamówienia**
   Maksymalny czas dostawy, o której mowa w pkt 4.1.1. – 45 dni od dnia zawarcia umowy, w tym:
   3.1. maksymalny czas dostawy – 30 dni od dnia podpisania Umowy;
   3.2. czas montażu i konfiguracji, o których mowa w pkt 4.1.2. – 15 dni od dnia podpisania Protokołu Odbioru Dostawy ostatniej z Lokalizacji;
   3.3. dostawa voucherów, o których mowa w 4.1.3., w terminie 30 dni od dni zawarcia umowy.

4. **Przedmiot zamówienia**
   4.1. Przedmiotem zamówienia jest:
   4.1.1. dostawa, montaż i konfiguracja Programowalnej Sieci Komputerowej (SDN), obejmująca:
   4.1.1.1. sprzedaż i dostarczenie przez Wykonawcę do lokalizacji urządzeń wraz z dokumentacją i oprogramowaniem;
   4.1.1.2. dostawę licencji na oprogramowanie;
   4.1.2. montaż i konfiguracja SDN;
   4.1.3. dostawa voucherów pozwalających zrealizować szkolenia z obsługi SDN:
   4.1.3.1. szkolenie z konfiguracji i administracji urządzeniami;
   4.1.3.2. szkolenie z integracji z aplikacjami i systemami;
   4.1.3.3. szkolenie z zakresu wsparcia operacyjnego w obszarze utrzymania.
   4.1.4. udzielenie przez Wykonawcę gwarancji i wsparcia technicznego na urządzenia i oprogramowanie oraz zapewnienie gwarancji i wsparcia technicznego producenta dla urządzeń i oprogramowania na okres 60 miesięcy od dnia podpisania protokołu odbioru dostawy.

5. **Wymagania ogólne**
   5.1. 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.
   5.2. Wykonawca wykona montaż urządzeń w miejscach wskazanych przez Zamawiającego oraz dokona konfiguracji w uzgodnieniu z Zamawiającym. Zamawiający wymaga, aby instalacja

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

została dokonana przez osobę posiadającą odpowiednie uprawnienia, w szczególności posiadającą certyfikat producenta urządzeń uprawniający do wykonywanych prac.

5.3. Na potwierdzenie wykonania konfiguracji zostanie wykonana dokumentacja, obejmująca w szczególności wykaz wszystkich urządzeń i modułów, połączeń sieciowych, wykonanej konfiguracji w zakresie zaimplementowanej logiki SDN.

5.4. Urządzenia mają być fabrycznie nowe, nie używane wcześniej, mają być objęte opieką serwisową producenta oraz posiadać najnowszą dostępną stabilną wersję oprogramowania.

5.5. Zamawiający wymaga, aby Wykonawca posiadał najwyższy status partnerstwa przyznawany przez producenta oprogramowania i sprzętu potwierdzony poświadczeniem producenta. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa w zdaniu poprzednim.

5.6. Programowalna sieć komputerowa (SDN) 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 bezpieczeństwa (tj. Dz. U z 2018 r. poz. 1560), 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, Programowalna sieć komputerowa (SDN) musi być zgodna z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.

6. Warunki dotyczące gwarancji i świadczenia wsparcia:

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

6.1.1. 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;

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

6.1.3. Lokalizacja – miejsca na terenie miasta stołecznego Warszawy, do których ma nastąpić dostawa SDN. Dokładne adresy zostaną podane do wiadomości Wykonawcy niezwłocznie po podpisaniu umowy.

6.2. Dostarczone rozwiązanie objęte będzie 60-miesięcznym wsparciem technicznym i serwisem gwarancyjnym.

6.3. Do obowiązków Wykonawcy należy usuwanie Awarii najpóźniej w ciągu 24 godzin (w systemie 24/7 przez cały rok kalendarzowy) od chwili zgłoszenia Awarii.

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

6.5. W razie nieusunięcia Awarii urządzenia w terminie, Wykonawca dostarczył 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.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

6.6. W ramach wsparcia technicznego Zamawiającemu przysługuje m.in. uprawnienie do naprawy lub wymiany uszkodzonego Urządzenia.

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

6.7.1. 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;

6.7.2. wsparcia technicznego realizowanego w miejscu instalacji urządzeń;

6.7.3. obsługi świadczonej w języku polskim;

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

6.7.5. dostępności inżyniera serwisu w szczególności na wypadek zaistnienia konieczności konsultacji, rozwiania wątpliwości lub rozwiązania bieżących problemów Zamawiającego z obsługą SDN: w dni robocze (tj. od poniedziałku do piątku, poza dniami ustawowo wolnymi od pracy), w godzinach 8:00 – 16:00.

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

7. Szkolenia

7.1. Należy zrealizować certyfikowane szkolenia z dostarczonego rozwiązania dla maksymalnie 20 wskazanych pracowników Zamawiającego:

7.1.1. szkolenie z konfiguracji i administracji urządzeniami (dla maksimum 7 osób, minimum 2 dni szkolenia),

7.1.2. szkolenie z integracji z aplikacjami i systemami (dla maksimum 7 osób, minimum 2 dni szkolenia),

7.1.3. szkolenie z zakresu wsparcia operacyjnego w obszarze utrzymania (dla maksimum 6 osób, minimum 2 dni szkolenia).

7.2. Wykonawca przedstawi zakres szkolenia w uzgodnieniu z Zamawiającym.

7.3. Szkolenia należy zrealizować:

7.3.1. szkolenie, o którym mowa w punkcie 7.1.1. - w siedzibie Zamawiającego, w terminie do 90 dni od daty podpisania Umowy,

7.3.2. szkolenie, o którym mowa w punkcie 7.1.2. – w siedzibie Zamawiającego, w terminie do 120 dni od dnia podpisania Umowy,

7.3.3. szkolenie, o którym mowa w punkcie 7.1.3. – w miejscu uzgodnionym z Zamawiającym na terenie m.st. Warszawy, w terminie do 12 miesięcy od dnia podpisania Umowy.

7.4. Zamawiający zapewnia w swojej siedzibie salę szkoleniową wyposażoną w rzutnik lub monitor o dużej przekątnej.

7.5. Dla celów dokonania przez Wykonawcę wyceny Zamawiający oświadcza, że planowana minimalna liczba osób, które wezmą udział w szkoleniach, to 10, w tym minimum 4 na

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

szkolenie, o którym mowa w punkcie 7.1.1. i po minimum 3 osoby na szkolenia, o których mowa w punkcie 7.1.2. i 7.1.3.

8. Szczegółowe wymagania techniczne dla Systemu Software Defined Networking (SDN)

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

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

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

8.1.3. **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):

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

8.2.2. 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;

8.2.3. utrata wszystkich instancji kontrolera SDN nie może wpływać na działanie infrastruktury sieciowej w zakresie istniejącej konfiguracji (nie dotyczy to zmian konfiguracji);

8.2.4. Kontroler SDN musi posiadać 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) musi istnieć możliwość dalszej modyfikacji konfiguracji przynajmniej dla jednej z lokalizacji (podstawowego DC). 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;

8.2.5. komunikacja między kontrolerem SDN i elementami infrastruktury sieciowej (tzw. „IP fabric") musi być możliwa w trybie in-band, niewymagającym użycia dedykowanych interfejsów na przełącznikach wchodzących w skład architektury;

8.2.6. Kontroler SDN musi obsługiwać wyłącznie ruch związany z zarządzaniem i monitorowaniem infrastruktury sieciowej (tzw. „control plane"), nie zajmuje się przełączaniem ruchu (tzw. „data plane");

8.2.7. Kontroler SDN musi umożliwiać zarządzanie infrastrukturą sieciową złożoną z 2000 portów i dołączającą co najmniej 500 fizycznych serwerów dwuprocesorowych

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

(odpowiednie licencje, jeśli wymagane, muszą być dostarczone na docelową pojemność platformy);

8.2.8. Kontroler SDN musi umożliwiać 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):

8.3.1. musi umożliwiać automatyzację konfiguracji zarządzanej sieci w oparciu o model sieciowych polityk powiązanych z aplikacjami;

8.3.2. 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:

8.3.2.1. zdefiniowanie warstw aplikacji takich jak web, aplikacyjna i bazodanowa (Web, App, DB);

8.3.2.2. zdefiniowanie przydziału serwera wirtualnego do danej warstwy aplikacyjnej/segmentu na bazie jego atrybutów – nazwa maszyny VM, id maszyny VM, nazwa systemu operacyjnego, tagi itp.;

8.3.2.3. zdefiniowanie relacji pomiędzy warstwami aplikacyjnymi, jako wzajemnie udostępnianych i konsumowanych zasobów opisanych przez polityki bezpieczeństwa (filtracji oraz przekierowania na zewnętrzne urządzenia bezpieczeństwa);

8.3.3. musi umożliwiać zintegrowanie usług zewnętrznych poprzez zapewnienie mechanizmu przekierowania ruchu dla warstw 4-7 dla funkcjonalności Next Generation Firewall;

8.3.4. dla izolowanych środowisk sieciowych SDN musi umożliwiać implementację funkcjonalności dedykowanej bramy wyjściowej L3 oraz dedykowanych usług zewnętrznych realizowanych dla warstw 4-7;

8.3.5. musi realizować tworzenie segmentów sieci L2 i L3 w oparciu o technologię VXLAN;

8.3.6. musi realizować sprzętowy VTEP;

8.3.7. musi umożliwiać monitorowanie i diagnostykę sieciową dla uruchamianych środowisk w oparciu o następujące mechanizmy:

8.3.7.1. prezentację sprawności środowiska/aplikacji w formie wskaźnika stanu zdrowia;

8.3.7.2. prezentowanie bieżącej i historycznej statystyki ruchu dla danego środowiska sieciowego;

8.3.7.3. diagnostykę ścieżki (traceroute) między dowolną parą portów fizycznych bądź wirtualnych wchodzących w skład infrastruktury;

8.3.7.4. monitorowanie i raportowanie ilości wykorzystanych i dostępnych zasobów wchodzących w skład infrastruktury;

8.3.7.5. monitorowanie ruchu poprzez kopiowanie (mirroring) ruchu dla wybranych warstw aplikacyjnych lub interfejsów sieciowych.

8.3.8. musi umożliwiać automatyczną detekcję topologii oraz inwentarza infrastruktury sieciowej. Dopuszcza się realizację na innym komponencie zarządzania pod warunkiem zapewnienia dedykowanej, redundantnej platformy sprzętowej.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

8.3.9. musi implementować centralne repozytorium oprogramowania (firmware) dla infrastruktury sieciowej. Dopuszcza się realizację na innym komponencie zarządzania pod warunkiem zapewnienia dedykowanej, redundantnej platformy sprzętowej.
8.3.10. musi implementować centralny mechanizm aktualizacji oprogramowania (firmware) dla infrastruktury sieciowej. Dopuszcza się realizację na innym komponencie zarządzania pod warunkiem zapewnienia dedykowanej, redundatnej platformy sprzętowej.
8.3.11. musi udostępniać interfejs zarządzania poprzez GUI.
8.3.12. musi zapewniać integrację z Active Directory.
8.3.13. musi udostępniać następujące mechanizmy programowania (alternatywa do GUI):
8.3.13.1. REST API ze wsparciem dla formatu XML;
8.3.13.2. możliwość konfiguracji infrastruktury bezpośrednio poprzez HTTP (np. z wykorzystaniem Postman REST Client);
8.3.13.3. Python SDK;
8.3.13.4. powszechnie dostępna dokumentacja dla REST API;
8.3.14. musi udostępniać autoryzację dostępu użytkowników w oparciu o mechanizmy LDAP lub lokalne definicje;
8.3.15. musi umożliwiać synchronizację całej infrastruktury sieciowej w oparciu o protokół NTP.

8.4. Funkcjonalność centralnego systemu analizy środowisk aplikacyjnych i zarządzania politykami segmentacji:
8.4.1. Centralny system analizy środowisk aplikacyjnych musi dostarczać zautomatyzowane mechanizmy modelowania aplikacji w Data Center i w chmurach publicznych, generowania polityk bezpieczeństwa, ich testowania, audytowania i ochrony serwerów.
8.4.2. System musi składać się z następujących elementów:
8.4.2.1. oprogramowania centralnego systemu analizy środowisk aplikacyjnych i zarządzania politykami segmentacji;
8.4.2.2. systemu serwerów hiperkonwergentnych zapewniających odpowiednie zasoby CPU i dyskowe na potrzeby oprogramowania (nie licząc zasobów związanych z realizacją zadań samej platformy hiperkonwergentnej). Minimalnie jest to (z uwzględnieniem awarii jednego węzła – n+1):
8.4.2.2.1. 2TB RAM;
8.4.2.2.2. 20TB storage (min. 2 repliki danych) o parametrach wydajności co najmniej 5000IOPS;
8.4.2.2.3. 128vCPU;
8.4.2.3. system serwerów hiperkonwergentnych musi posiadać oficjalne wsparcie producenta oprogramowania i zawierać wszystkie niezbędne licencje i subskrybcje niezbędne do poprawnego działania;
8.4.2.4. Agenci programowi, zainstalowani na końcowych systemach operacyjnych przekazujący dane o stacjach końcowych oraz wymuszający polityki bezpieczeństwa.
8.4.2.5. zewnętrzne źródła danych, przekazujące lub pobierające dane poprzez API.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

8.4.3. System musi umożliwiać import danych z systemów CMDB/IPAM celem wzbogacenia analizy metadanych o dodatkowe informacje typu nazwa hosta, aplikacji, środowiska, projektu itp.

8.4.4. System musi umożliwiać 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).

8.4.5. Funkcje modelowanie aplikacji i budowy polityk na potrzeby segmentacji:

8.4.5.1. na bazie zebranych danych z różnych źródeł system musi rekomendować politykę segmentacji opartą o tzw. „white-listing", czyli otwarcie do komunikacji tylko wymaganych i wykorzystywanych portów wymaganych do działania aplikacji;

8.4.5.2. system musi umożliwiać testowanie polityki a następnie jej wymuszenie;

8.4.5.3. system musi wizualizować topologię aplikacji w danym obszarze (podział na warstwy/segmenty);

8.4.5.4. system musi wizualizować mapę polityki (przepływy pomiędzy segmentami/workload z dokładnością do L4).

8.4.6. Funkcje ochrony systemów końcowych i wymuszania polityk:

8.4.6.1. system musi gromadzić dane z agentów na stacjach końcowych (OS) i wykorzystuje je w korelacji z innymi źródłami;

8.4.6.2. gromadzone dane obejmują informacje o portach, protokołach i procesach;

8.4.6.3. system potrafi wizualizować informację o procesach uruchomionych na stacji końcowej (drzewo lub lista procesów);

8.4.6.4. oprogramowanie agentów musi działać zarówno w środowiskach zwirtualizowanych jak na i serwerach fizycznych;

8.4.6.5. oprogramowanie agentów powinno wspierać systemy Linux i Windows;

8.4.6.6. oprogramowanie agentów powinno wspierać hosty dla środowisk kontenerów;

8.4.6.7. platforma koreluje dane ze stacji końcowych (workload) z informacjami o znanych lukach lub ekspozycji w zabezpieczeniach, np. importowanych z bazy podatności CVE;

8.4.6.8. platforma pokazuje ocenę/rating poziomu zagrożeń dla danej aplikacji lub workload w postaci wskaźnika (np. typu procent, kolor itp.);

8.4.6.9. platforma musi być w stanie wymusić politykę opisującą aplikację poprzez konfigurację firewall właściwego dla stacji końcowej (ip tables dla Unix lub Windows Firewall).

8.4.7. Centralny system analizy środowisk aplikacyjnych musi wspierać minimum 1000 urządzeń końcowych (serwery fizyczne lub maszyny wirtualne).

8.4.8. 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. 60 miesięcy.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

8.5. Funkcjonalność sprzętowa dla infrastruktury sieciowej („IP fabric") pozostającej pod nadzorem komponentu zarządzającego (kontrolera SDN):
  8.5.1. 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";
  8.5.2. przełączniki muszą być wspierane i zarządzane przez komponent zarządzający (kontroler SDN) opisany powyżej;
  8.5.3. Jeśli do współpracy z komponentem zarządzającym (kontrolerem) konieczna jest dla przełącznika licencja to wymaga się jej dostarczenia. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 60 miesięcy.
  8.5.4. Zarządzana jako całość poprzez centralny komponent zarządzający (kontroler).
  8.5.5. 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.
  8.5.6. Implementuje następujące protokoły i mechanizmy L2:
    8.5.6.1. sprzętowe wsparcie dla VXLAN Bridging i VXLAN Routing w oparciu o sprzętowy VTEP;
    8.5.6.2. dołączanie urządzeń zewnętrznych (serwerów, modułów, przełączników) poprzez zagregowaną wiązkę połączeń LACP 802.3ad do dwóch przełączników brzegowych (multi link aggregation, virtual port channel, itp.);
    8.5.6.3. pełna mobilność serwera fizycznego i wirtualnego w domenie L2, również pomiędzy kilkoma DC;
    8.5.6.4. definiowanie zewnętrznych połączeń w domenie L2;
    8.5.6.5. mechanizm eliminacji pętli na przełącznikach brzegowych w IP Fabric.
  8.5.7. Implementuje następujące protokoły i mechanizmy L3:
    8.5.7.1. IPv4 Unicast i Multicast;
    8.5.7.2. przesyłanie IPv6 Unicast;
    8.5.7.3. niezależne sieci prywatne (VRF) z duplikacją adresacji IP;
    8.5.7.4. protokoły routingu eBGP, iBGP, OSPF dla IPv4 i IPv6;
    8.5.7.5. routing statyczny dla IPv4 i IPv6;
    8.5.7.6. 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;
    8.5.7.7. pełna mobilność serwera fizycznego i wirtualnego w domenie L3;
    8.5.7.8. interfejsy i subinterfejsy L3 (per VLAN) na portach fizycznych przełączników brzegowych;
    8.5.7.9. definiowanie zewnętrznych połączeń w domenie L3 opartych o protokoły routingu statycznego lub dynamicznego (OSPF lub BGP);
  8.5.8. Implementuje następujące mechanizmy optymalizacji ruchu:
    8.5.8.1. Load-balancing pakietów dostosowany się do różnych warunków przesyłania (natłoku) w ramach środowiska opartego o ECMP;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

8.5.8.2. priorytetyzacja połączeń.

8.6. Wymagana jest pełna kompatybilność pomiędzy kontrolerem SDN a urządzeniami sieciowymi potwierdzona dokumentacją producenta.

8.7. Wymaga się dostarczenia następującej liczby urządzeń sieciowych i ich typów:

8.7.1. urządzenie typu leaf z portami dostępowymi 48x 10/25G dla wkładek SFP+: 16 szt.;

8.7.2. urządzenie typu leaf z portami dostępowymi 48x 100M/1/10GBASE-T: 4szt.;

8.7.3. urządzenie typu spine z portami 32x 40/100G QSFP: 4 szt.;

8.7.4. urządzenie typu IPN z portami 36x 40/100G QSFP: 4 szt.

9. Wymagania dotyczące urządzeń:

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

9.1.1. Przełącznik musi posiadać:

9.1.1.1. minimum 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+;

9.1.1.2. minimum 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps oraz w trybie100Gbps na pojedynczej parze okablowania multi-mode (do 100m).

9.1.2. Parametry wydajnościowe:

9.1.2.1. prędkość przełączania minimum 1.8Tbps full duplex;

9.1.2.2. urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.

9.1.3. Przełącznik musi posiadać następującą funkcjonalność dla warstwy L2:

9.1.3.1. trunking IEEE 802.1Q VLAN;

9.1.3.2. wsparcie dla 3000 sieci VLAN;

9.1.3.3. wsparcie sprzętowe dla 250 tysięcy adresów MAC;

9.1.3.4. IEEE 802.1w Rapid Spanning Tree (RST);

9.1.3.5. IEEE 802.1s Multiple Spanning Tree (MST);

9.1.3.6. zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU);

9.1.3.7. Internet Group Management Protocol (IGMP) Versions 2, 3;

9.1.3.8. terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;

9.1.3.9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad;

9.1.3.10. ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);

9.1.3.11. funkcjonalność izolowania portów znajdujących się w tym samym VLAN;

9.1.3.12. wsparcie sprzętowe dla tunelowania QinQ i QinVNI.

9.1.4. Przełącznik musi posiadać następującą funkcjonalność dla warstwy L3:

9.1.4.1. sprzętowe przełączanie pakietów w warstwie L3;

9.1.4.2. routing w oparciu o trasy statyczne;

9.1.4.3. routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6;

9.1.4.4. Policy Based Routing (PBR);

9.1.4.5. VRRP;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.1.4.6. wsparcie dla BFD (Bidirectional Forwarding Protocol), w tym zarówno dla IPv4 jak i IPv6;
9.1.4.7. tunele GRE;
9.1.4.8. wsparcie sprzętowe dla minimum 800 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;
9.1.4.9. wsparcie dla VRF;
9.1.4.10. wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);
9.1.4.11. wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast);
9.1.4.12. wsparcie dla IGMPv3 oraz MSDP;
9.1.4.13. wsparcie sprzętowe dla minimum 32,000 tras multicastowych;
9.1.4.14. obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (access control list).

9.1.5. Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN:
9.1.5.1. zintegrowany, sprzętowy VXLAN Bridging/Routing;
9.1.5.2. obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);
9.1.5.3. implementacja VXLAN BGP EVPN (Ethernet VPN);
9.1.5.4. obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).

9.1.6. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
9.1.6.1. Layer 2 IEEE 802.1p (CoS) oraz DSCP;
9.1.6.2. klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6);
9.1.6.3. kolejkowanie bezwzględne (strict-priority);
9.1.6.4. kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection);
9.1.6.5. ograniczanie ruchu (policing) do zadanej przepływności;
9.1.6.6. dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
9.1.6.7. protokół PFC (Priority Flow Control) IEEE 802.1Qbb.

9.1.7. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
9.1.7.1. obsługa list kontroli dostępu (ACL):
9.1.7.1.1. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
9.1.7.1.2. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
9.1.7.1.3. ACL oparte o porty (PACL);
9.1.7.2. DHCP Snooping;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.1.7.3. ARP Inspection;
9.1.7.4. IP Source Guard;
9.1.7.5. Unicast reverse path forwarding (uRPF);
9.1.7.6. prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.

9.1.8. Przełącznik musi wspierać następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
9.1.8.1. port zarządzający 100/1000 Mbps;
9.1.8.2. port konsoli CLI;
9.1.8.3. zarządzanie In-band;
9.1.8.4. SSHv2;
9.1.8.5. Authentication, authorization, and accounting (AAA);
9.1.8.6. RADIUS;
9.1.8.7. TACACS+;
9.1.8.8. Syslog;
9.1.8.9. SNMP v1, v2c, v3;
9.1.8.10. 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;
9.1.8.11. Role-Based Access Control RBAC;
9.1.8.12. IEEE 802.1ab LLDP;
9.1.8.13. możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback);
9.1.8.14. 802.1x;
9.1.8.15. ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
9.1.8.16. kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring);
9.1.8.17. Network Time Protocol (NTP);
9.1.8.18. Precision Time Protocol IEEE 1588;
9.1.8.19. Diagnostyka procesu BOOT;
9.1.8.20. Ping;
9.1.8.21. Traceroute.

9.1.9. Narzędzia programowania i zarządzania przełącznikiem, tj:
9.1.9.1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API;
9.1.9.2. wbudowana powłoka Bash do zarządzania systemem Linux przełącznika;
9.1.9.3. wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.1.9.4. interfejs programistyczny REST API wraz z upublicznionym SDK;
9.1.9.5. możliwość zainstalowania klienta Chef;
9.1.9.6. możliwość zainstalowania agenta Puppet;
9.1.9.7. wsparcie dla OpenStack Neutron plugin.

9.1.10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.

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

9.1.12. Wyposażenia przełącznika:

9.1.12.1. 2 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional);

9.1.12.2. 48 wkładek SFP+ typu 10GBASE-SR;

9.1.13. 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. 60 miesięcy.

9.2. Urządzenie typu leaf z portami dostępowymi 48x 100M/1/10GBASE-T

9.2.1. Przełącznik musi posiadać:

9.2.1.1. minimum 48 portów 100M/1/10GBASE-T;

9.2.1.2. 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 trybie100Gbps na pojedynczej parze okablowania multi-mode (do 100m).

9.2.2. Parametry wydajnościowe:

9.2.2.1. prędkość przełączania 1.8Tbps full duplex;

9.2.2.2. urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.

9.2.3. Przełącznik musi posiadać następującą funkcjonalność dla warstwy L2:

9.2.3.1. trunking IEEE 802.1Q VLAN;

9.2.3.2. wsparcie dla 3000 sieci VLAN;

9.2.3.3. wsparcie sprzętowe dla 250 tysięcy adresów MAC;

9.2.3.4. IEEE 802.1w Rapid Spanning Tree (RST);

9.2.3.5. IEEE 802.1s Multiple Spanning Tree (MST);

9.2.3.6. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU);

9.2.3.7. Internet Group Management Protocol (IGMP) Versions 2, 3;

9.2.3.8. terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.2.3.9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad;
9.2.3.10. ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
9.2.3.11. funkcjonalność izolowania portów znajdujących się w tym samym VLAN;
9.2.3.12. wsparcie sprzętowe dla tunelowania QinQ i QinVNI.

9.2.4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:
9.2.4.1. sprzętowe przełączanie pakietów w warstwie L3;
9.2.4.2. routing w oparciu o trasy statyczne;
9.2.4.3. routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6;
9.2.4.4. Policy Based Routing (PBR);
9.2.4.5. VRRP;
9.2.4.6. wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6;
9.2.4.7. tunele GRE;
9.2.4.8. wsparcie sprzętowe dla minimum 800 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;
9.2.4.9. wsparcie dla VRF;
9.2.4.10. wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);
9.2.4.11. wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast);
9.2.4.12. wsparcie dla IGMPv3 oraz MSDP;
9.2.4.13. wsparcie sprzętowe dla minimum 32,000 tras multicastowych;
9.2.4.14. obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (access control list).

9.2.5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
9.2.5.1. zintegrowany, sprzętowy VXLAN Bridging/Routing;
9.2.5.2. obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);
9.2.5.3. implementacja VXLAN BGP EVPN (Ethernet VPN);
9.2.5.4. obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).

9.2.6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
9.2.6.1. Layer 2 IEEE 802.1p (CoS) oraz DSCP;
9.2.6.2. klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6);
9.2.6.3. kolejkowanie bezwzględne (strict-priority);
9.2.6.4. kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection);
9.2.6.5. ograniczanie ruchu (policing) do zadanej przepływności;
9.2.6.6. dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.2.6.7. protokół PFC (Priority Flow Control) IEEE 802.1Qbb.

9.2.7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:

9.2.7.1. obsługa list kontroli dostępu (ACL):

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

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

9.2.7.1.3. ACL oparte o porty (PACL);

9.2.7.2. DHCP Snooping;

9.2.7.3. ARP Inspection;

9.2.7.4. IP Source Guard;

9.2.7.5. Unicast reverse path forwarding (uRPF);

9.2.7.6. prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.

9.2.8. Przełącznik musi wspierać następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:

9.2.8.1. Port zarządzający 100/1000 Mbps;

9.2.8.2. Port konsoli CLI;

9.2.8.3. Zarządzanie In-band;

9.2.8.4. SSHv2;

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

9.2.8.6. RADIUS;

9.2.8.7. TACACS+

9.2.8.8. Syslog;

9.2.8.9. SNMP v1, v2c, v3;

9.2.8.10. Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB;

9.2.8.11. Role-Based Access Control RBAC;

9.2.8.12. IEEE 802.1ab LLDP;

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

9.2.8.14. 802.1x;

9.2.8.15. ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);

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

9.2.8.17. Network Time Protocol (NTP);

9.2.8.18. Precision Time Protocol IEEE 1588;

9.2.8.19. Diagnostyka procesu BOOT;

9.2.8.20. Ping;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.2.8.21. Traceroute.

9.2.9. Narzędzia programowania i zarządzania przełącznikiem:

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

9.2.9.2. wbudowana powłoka Bash do zarządzania systemem Linux przełącznika;

9.2.9.3. wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika;

9.2.9.4. Interfejs programistyczny REST API wraz z upublicznionym SDK;

9.2.9.5. możliwość zainstalowania klienta Chef;

9.2.9.6. możliwość zainstalowania agenta Puppet;

9.2.9.7. wsparcie dla OpenStack Neutron plugin.

9.2.10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.

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

9.2.12. Wyposażenia przełącznika - 2 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional).

9.2.13. 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 60 miesięcy.

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

9.3.1. Przełącznik musi posiadać 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).

9.3.2. Parametry wydajnościowe:

9.3.2.1. prędkość przełączania 3.2Tbps full duplex;

9.3.2.2. urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.

9.3.3. Przełącznik musi posiadać następującą funkcjonalność dla warstwy L2:

9.3.3.1. Trunking IEEE 802.1Q VLAN;

9.3.3.2. wsparcie dla 3000 sieci VLAN;

9.3.3.3. wsparcie sprzętowe dla 90 tysięcy adresów MAC;

9.3.3.4. IEEE 802.1w Rapid Spanning Tree (RST);

9.3.3.5. IEEE 802.1s Multiple Spanning Tree (MST);

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.3.3.6. zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU);
9.3.3.7. Internet Group Management Protocol (IGMP) Versions 2, 3;
9.3.3.8. terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;
9.3.3.9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad;
9.3.3.10. ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
9.3.3.11. funkcjonalność izolowania portów znajdujących się w tym samym VLAN;
9.3.3.12. wsparcie sprzętowe dla tunelowania QinQ i QinVNI.

9.3.4. Przełącznik musi posiadać następującą funkcjonalność dla warstwy L3:
9.3.4.1. sprzętowe przełączanie pakietów w warstwie L3;
9.3.4.2. routing w oparciu o trasy statyczne;
9.3.4.3. umożliwia rozbudowę poprzez licencje o funkcjonalności warstwy L3 – OSPF, BGP, IS-IS dla protokołów IPv4 oraz IPv6;
9.3.4.4. Policy Based Routing (PBR);
9.3.4.5. VRRP;
9.3.4.6. wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6;
9.3.4.7. tunele GRE;
9.3.4.8. wsparcie sprzętowe dla minimum 60 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;
9.3.4.9. wsparcie dla VRF;
9.3.4.10. wybór do 16-tu jednoczesnych ścieżek o równej metryce (ECMP);
9.3.4.11. wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast);
9.3.4.12. wsparcie dla IGMPv3 oraz MSDP;
9.3.4.13. wsparcie sprzętowe dla minimum 12,000 tras multicast;
9.3.4.14. obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (access control list).

9.3.5. Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN:
9.3.5.1. zintegrowany, sprzętowy VXLAN Bridging/Routing;
9.3.5.2. obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);
9.3.5.3. implementacja VXLAN BGP EVPN (Ethernet VPN);
9.3.5.4. obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN.

9.3.6. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
9.3.6.1. Layer 2 IEEE 802.1p (CoS) oraz DSCP;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.3.6.2. klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6);
9.3.6.3. kolejkowanie bezwzględne (strict-priority);
9.3.6.4. kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection);
9.3.6.5. ograniczanie ruchu (policing) do zadanej przepływności;
9.3.6.6. dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
9.3.6.7. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.

9.3.7. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
9.3.7.1. obsługa list kontroli dostępu (ACL)
9.3.7.1.1. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
9.3.7.1.2. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
9.3.7.1.3. ACL oparte o porty (PACL);
9.3.7.2. DHCP Snooping;
9.3.7.3. ARP Inspection;
9.3.7.4. IP Source Guard;
9.3.7.5. Unicast reverse path forwarding (uRPF);
9.3.7.6. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.

9.3.8. Urządzenie musi realizować następujące funkcjonalności dotyczące zarządzania i zabezpieczenia:
9.3.8.1. Port zarządzający 100/1000 Mbps;
9.3.8.2. Port konsoli CLI;
9.3.8.3. Zarządzanie In-band;
9.3.8.4. SSHv2;
9.3.8.5. Authentication, authorization, and accounting (AAA);
9.3.8.6. RADIUS;
9.3.8.7. TACACS
9.3.8.8. Syslog;
9.3.8.9. SNMP v1, v2, v3;
9.3.8.10. telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB;
9.3.8.11. Role-Based Access Control RBAC;
9.3.8.12. IEEE 802.1ab LLDP;
9.3.8.13. możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback);
9.3.8.14. 802.1x;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.3.8.15. ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
9.3.8.16. kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring);
9.3.8.17. Network Time Protocol (NTP);
9.3.8.18. Precision Time Protocol IEEE 1588;
9.3.8.19. Diagnostyka procesu BOOT;
9.3.8.20. Ping;
9.3.8.21. Traceroute.

9.3.9. Narzędzia programowania i zarzadzania przełącznikiem:
9.3.9.1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API;
9.3.9.2. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika;
9.3.9.3. Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika;
9.3.9.4. Interfejs programistyczny REST API wraz z upublicznionym SDK;
9.3.9.5. możliwość zainstalowania klienta Chef;
9.3.9.6. możliwość zainstalowania agenta Puppet.

9.3.10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych.
9.3.11. Obudowa o rozmiarach maksymalnie 2RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
9.3.12. Wyposażenia przełącznika 10 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional);
9.3.13. 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 60 miesięcy.

9.4. Urządzenie typu IPN z portami 36x 40/100G QSFP

9.4.1. 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).

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.4.2. Parametry wydajnościowe:
- 9.4.2.1. Prędkość przełączania 3.6Tbps full duplex;
- 9.4.2.2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.

9.4.3. Przełącznik musi posiadać następujące funkcjonalności dla warstwy L2:
- 9.4.3.1. Trunking IEEE 802.1Q VLAN;
- 9.4.3.2. wsparcie dla 3000 sieci VLAN;
- 9.4.3.3. wsparcie sprzętowe dla 256 tysięcy adresów MAC;
- 9.4.3.4. IEEE 802.1w Rapid Spanning Tree (RST);
- 9.4.3.5. IEEE 802.1s Multiple Spanning Tree (MST);
- 9.4.3.6. zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU);
- 9.4.3.7. Internet Group Management Protocol (IGMP) Versions 2, 3;
- 9.4.3.8. terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;
- 9.4.3.9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad;
- 9.4.3.10. ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
- 9.4.3.11. funkcjonalność izolowania portów znajdujących się w tym samym VLAN;
- 9.4.3.12. wsparcie sprzętowe dla tunelowania QinQ i QinVNI.

9.4.4. Przełącznik musi posiada następującą funkcjonalność dla warstwy L3:
- 9.4.4.1. sprzętowe przełączanie pakietów w warstwie L3;
- 9.4.4.2. routing w oparciu o trasy statyczne;
- 9.4.4.3. umożliwia rozbudowę poprzez licencje o funkcjonalności warstwy L3 – OSPF, BGP, IS-IS dla protokołów IPv4 oraz IPv6;
- 9.4.4.4. Policy Based Routing (PBR);
- 9.4.4.5. VRRP;
- 9.4.4.6. wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6;
- 9.4.4.7. tunele GRE;
- 9.4.4.8. wsparcie sprzętowe dla minimum 800 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;
- 9.4.4.9. wsparcie dla VRF;
- 9.4.4.10. wybór do 16-tu jednoczesnych ścieżek o równej metryce (ECMP);
- 9.4.4.11. wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast);
- 9.4.4.12. wsparcie dla IGMPv3 oraz MSDP;
- 9.4.4.13. wsparcie sprzętowe dla minimum 32,000 tras multicast;
- 9.4.4.14. obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (access control list).

9.4.5. Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN:
- 9.4.5.1. zintegrowany, sprzętowy VXLAN Bridging/Routing;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.4.5.2. obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);
9.4.5.3. implementacja VXLAN BGP EVPN (Ethernet VPN);
9.4.5.4. obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN.

9.4.6. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
9.4.6.1. Layer 2 IEEE 802.1p (CoS) oraz DSCP;
9.4.6.2. klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6);
9.4.6.3. kolejkowanie bezwzględne (strict-priority);
9.4.6.4. kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection);
9.4.6.5. ograniczanie ruchu (policing) do zadanej przepływności;
9.4.6.6. dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
9.4.6.7. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.

9.4.7. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
9.4.7.1. obsługę list kontroli dostępu (ACL)
9.4.7.1.1. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
9.4.7.1.2. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
9.4.7.1.3. ACL oparte o porty (PACL);
9.4.7.2. DHCP Snooping;
9.4.7.3. ARP Inspection;
9.4.7.4. IP Source Guard;
9.4.7.5. Unicast reverse path forwarding (uRPF);
9.4.7.6. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.

9.4.8. Urządzenie musi realizować następujące funkcjonalności dotyczące zarządzania i zabezpieczenia:
9.4.8.1. port zarządzający 100/1000 Mbps;
9.4.8.2. port konsoli CLI;
9.4.8.3. zarządzanie In-band;
9.4.8.4. SSHv2;
9.4.8.5. Authentication, authorization, and accounting (AAA);
9.4.8.6. RADIUS;
9.4.8.7. TACACS
9.4.8.8. Syslog;
9.4.8.9. SNMP v1, v2, v3;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.4.8.10. telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB;
9.4.8.11. Role-Based Access Control RBAC;
9.4.8.12. IEEE 802.1ab LLDP;
9.4.8.13. możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback);
9.4.8.14. 802.1x;
9.4.8.15. ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
9.4.8.16. kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring);
9.4.8.17. Network Time Protocol (NTP);
9.4.8.18. Precision Time Protocol IEEE 1588;
9.4.8.19. Diagnostyka procesu BOOT;
9.4.8.20. Ping;
9.4.8.21. Traceroute.

9.4.9. Narzędzia programowania i zarzadzania przełącznikiem:
9.4.9.1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API;
9.4.9.2. wbudowana powłoka Bash do zarządzania systemem Linux przełącznika;
9.4.9.3. wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika;
9.4.9.4. Interfejs programistyczny REST API wraz z upublicznionym SDK;
9.4.9.5. możliwość zainstalowania klienta Chef;
9.4.9.6. możliwość zainstalowania agenta Puppet.

9.4.10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych.
9.4.11. Obudowa o rozmiarach maksymalnie 2RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
9.4.12. Wyposażenia przełącznika 10 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional).
9.4.13. 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

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

wymaga się jej dostarczenia. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 60 miesięcy.

9.5. Przełączniki zarządzające – szt. 12, o następujących parametrach:

9.5.1. powinny pochodzić od tego samego producenta co przełączniki dla SDN;
9.5.2. minimum 48 fizycznych portów 10/100/1000 (RJ-45);
9.5.3. minimum 2 porty 10GBASE-SR;
9.5.4. przepustowość minimum 105Gbps;
9.5.5. szybkość przełączania 120 Mpps;
9.5.6. przełącznik musi posiadać dedykowany port konsoli (RS-232) oraz dedykowany port typu out-of-band management (Ethernet RJ-45);
9.5.7. możliwość budowania stosu z innymi przełącznikami tego samego typu – minimum 8 przełączników w jednym stosie;
9.5.8. urządzenie musi obsługiwać min. 12000 adresów MAC oraz min. 1000 sieci VLAN;
9.5.9. urządzenie musi umożliwiać agregację łączy, minimum 8 portów
9.5.10. Wsparcie dla protokołów dynamicznego routingu – RIP, OSPF stub oraz routingu statycznego
9.5.11. urządzenie musi mieć możliwość pobrania konfiguracji w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona;
9.5.12. urządzenie musi posiadać redundantne zasilacze;
9.5.13. przystosowane do montażu w 19” szafie rack (zestaw montażowy dostarczony z urządzeniem).

9.6. LoadBalancer – szt. 4, o następujących parametrach:

9.6.1. przepustowość szyfrowania (sprzętowa) minimum 18Gbps, 15000 TPS (algorytm oparty o krzywe eliptyczne z kluczem 256bit);
9.6.2. przepustowość minimum 40Gbps L4/L7;
9.6.3. obsługa minimum 1000000 żądań na sekundę L7;
9.6.4. obsługa minimum 600000 połączeń na sekundę L4;
9.6.5. musi posiadać wbudowany język skryptowy pozwalający na zmianę oraz zastępowanie parametrów w nagłówku HTTP oraz w zawartości pakietów w skali całego ruchu obsługiwanego przez urządzenie;
9.6.6. w budowanych skryptach można analizować, zmieniać oraz zastępować parametry w nagłówkach protokołów: HTTP, TCP, RTSP, SIP;
9.6.7. musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego;
9.6.8. rozwiązanie na dedykowanej platformie sprzętowej (appliance);
9.6.9. architektura oprogramowania 64-bitowa;
9.6.10. minimum 4 porty 10GBASE-SR
9.6.11. musi umożliwiać agregację łączy Ethernet statycznie lub w oparciu o protokół LACP;
9.6.12. musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band;

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

9.6.13. management (Ethernet RJ-45);
9.6.14. posiada możliwość kreowania minimum 5 partycji wirtualnych (osobne tablice routingu);
9.6.15. urządzenie musi mieć możliwość pobrania konfiguracji w formie tekstowej. Konfiguracja;
9.6.16. po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona.
9.6.17. urządzenie musi posiadać redundantne zasilacze;
9.6.18. przystosowane do montażu w 19” szafie rack (zestaw montażowy dostarczony z urządzeniem).

10. Pozostałe wymagania opisane zostały w Istotnych postanowieaniach umowy (zawartych w rozdziale III SIWZ).

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl