

Szczegółowy opis przedmiotu umowy

I. Przełącznik LAN - 2 urządzenia

Sprzedawca dostarczy i wdroży dwie sztuki fizycznych przełączników (urządzeń) o identycznej konfiguracji (wymagania szczegółowe poniżej). Dostarczone przełączniki po wdrożeniu stanowiącą będą warstwę rdzenia sieci i docelowo zastąpią obecnie eksploatowany pojedynczy przełącznik Cisco Nexus7000. Sprzedawca wraz z przełącznikami dostarczy vouchery na autoryzowane szkolenie w ośrodku szkoleniowym na terenie Warszawy dla 2 osób, ważne przez okres co najmniej 6 miesięcy, licząc od dnia sporządzenia protokołu odbioru. Szkolenie musi trwać co najmniej 2 dni, być prowadzone w języku polskim i obejmować podstawowe zagadnienia z zakresu instalacji, konfiguracji i zarządzania dostarczonymi urządzeniami.

Lp.	Wymagania minimalne
1	<p>Przełącznik musi zapewniać:</p> <ul style="list-style-type: none"> a) minimum 48 portów 1/10GE definiowanych za pomocą wkładek SFP/SFP+ bezpośrednio w obudowie przełącznika lub na karcie liniowej b) minimum 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP powinien mieć możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps
2	<p>Parametry wydajnościowe:</p> <ul style="list-style-type: none"> a) Wymagana jest prędkość przełączania „wirespeed” dla każdego portu przełącznika b) Urządzenie musi sprzętowo przełączać pakiety w warstwie L2 i L3 c) Obsługiwana łączna przepływność (pasmo) min. 3 Tbps (terabits per second) d) Obsługiwana łączna przepustowość pakietowa przełącznika min. 2 bpps (billion packets per second) e) opóźnienie przełączania pakietów nie większe niż 2 μs
3	<p>Przełącznik musi spełniać następujące wymagania dla warstwy L2:</p> <ul style="list-style-type: none"> a) Trunking IEEE 802.1Q VLAN b) Wsparcie dla 4094 sieci VLAN c) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN d) Wsparcie sprzętowe dla minimum 200 tysięcy adresów MAC e) IEEE 802.1w f) IEEE 802.1s g) Wsparcie sprzętowe dla tunelowania QinQ h) Spanning Tree Guard lub odpowiadający i) Internet Group Management Protocol (IGMP) j) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach (MCEC, vPC lub odpowiadający mechanizm) k) Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 16 interfejsów fizycznych w wiązce l) Ramki Jumbo dla wszystkich portów do 9216 bajtów
4	<p>Przełącznik musi spełniać następujące wymagania dla warstwy L3:</p> <ul style="list-style-type: none"> a) Sprzętowe przełączanie pakietów w warstwie L3 b) Routing w oparciu o trasy statyczne c) Routing w oparciu o OSPF, BGP dla protokołów IPv4 d) Policy Based Routing (PBR) dla IPv4 e) VRRP w wersji 3 lub równoważna f) Wsparcie sprzętowe dla minimum 800 tysięcy prefixów (Longest Prefix Match)/ wpisów hosta w tablicy routingu IP

	<ul style="list-style-type: none"> g) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast) h) Wsparcie dla IGMPv3 oraz MSDP a) Wsparcie dla minimum 16,000 tras multicastowych b) Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) c) Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) d) Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla list kontroli dostępu (ACL)
5	<p>Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN:</p> <ul style="list-style-type: none"> a) Obsługa co najmniej 256 sprzętowych VTEP (VXLAN Tunnel Endpoint) b) Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) c) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP d) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) e) Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol) f) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN)
6	<p>Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:</p> <ul style="list-style-type: none"> a) Layer 2 IEEE 802.1p (CoS) b) Klasyfikacja QoS w oparciu o listy kontroli dostępu (ACL) – w warstwach 2, 3, 4 c) Bezwzględne (strict-priority) kolejkowanie na wyjściu d) Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający e) Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych f) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych g) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
7	<p>Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:</p> <ul style="list-style-type: none"> a) Standardowe i rozszerzone listy kontroli dostępu (ACL) b) ACL oparte o adresy MAC, adresy IP, VLAN-y; porty TCP/UDP c) Obsługa co najmniej następujących mechanizmów: Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard d) mechanizmy ochrony przed sztormami ruchu rozgłoszeniowego i multicast (broadcast/multicast storm) e) ochrona warstwy kontrolnej urządzenia przed atakami kierowanymi do niego (ograniczanie ruchu kierowanego do urządzenia)
8	<p>Wymagania dotyczące zarządzania i zabezpieczenia przełącznika:</p> <ul style="list-style-type: none"> a) Port zarządzający, zarządzanie In-band b) Port konsoli CLI c) SSHv2 d) Authentication, authorization and accounting (AAA) e) RADIUS lub TACACS+ f) Syslog g) SNMP v3 h) RMON (przynajmniej grupy Events, Alarms) i) OpenFlow 1.3 lub nowszy j) sFlow k) IEEE 802.1ab LLDP l) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)

	<ul style="list-style-type: none"> m) Role-Based Access Control (RBAC) n) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, o) sieci VLAN na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror) p) Network Time Protocol (NTP); q) Precision Time Protocol IEEE 1588
9	<p>Wymagania dotyczące narzędzi programowania i zarządzania przełącznikiem:</p> <ul style="list-style-type: none"> a) Interpreter języka skryptowego (np. Python) z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API b) Wbudowana powłoka linii komend do zarządzania systemem. c) Wsparcie dla konteneryzacji (np. Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie dystrybucji oprogramowania (np. yum i paczki rpm), niezależnie od systemu operacyjnego przełącznika. Kontener musi mieć możliwość wykorzystywania portów fizycznych przełącznika. d) Interfejs programistyczny REST API wraz z upublicznonym SDK e) Wsparcie dla NETCONF i zarządzania poprzez XML f) Wsparcie dla OpenStack Neutron plugin
10	Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej
11	Obudowa o rozmiarze maksymalnie 1 RU. Z przełącznikiem należy dostarczyć elementy do montażu w szafie RACK 19”
12	<p>Z przełącznikiem należy dostarczyć wkładki:</p> <ul style="list-style-type: none"> a) QSFP40G BiDi Short-reach Transceiver - 3 sztuki b) 10GBASE-SR SFP - 8 sztuk c) 1000BASE-T SFP - 30 sztuk d) 10GBASE-LR SFP – 1 sztuka <p>Dostarczone wkładki muszą być na liście sprzętu kompatybilnego z dostarczonym przełącznikiem i objęte oficjalnym wsparciem serwisowym.</p>
13	<p>Z przełącznikiem należy dostarczyć patchcordsy:</p> <ul style="list-style-type: none"> a) Patchcord UTP; dł. 0,5m; cat6; 10/100/1000Mbit/s Ethernet; kolor zielony -10 szt. b) Patchcord UTP; dł. 1m; cat6; 10/100/1000Mbit/s Ethernet; kolor zielony – 10 szt. c) Patchcord UTP; dł. 0,5m; cat6; 10/100/1000Mbit/s Ethernet; kolor żółty – 10 szt. d) Patchcord UTP; dł. 1m; cat6; 10/100/1000Mbit/s Ethernet; kolor żółty – 10 szt. e) Patchcord UTP; dł. 1m; cat6; 10/100/1000Mbit/s Ethernet; kolor szary – 10 szt. f) Patchcord UTP; dł. 2m; cat6; 10/100/1000Mbit/s Ethernet; kolor szary – 10 szt. g) Patchcord światłowodowy OM3 (fiber optic OM3); dł.=2m, wielomodowy 50/125um ze złączami LC na LC; duplex – 5 szt. h) Patchcord światłowodowy OM3 (fiber optic OM3); dł.=1m, wielomodowy 50/125um ze złączami LC na LC; duplex – 5 szt.

II. Router VPN - 1 urządzenie

Kupujący dla zapewnienia bezpiecznej komunikacji dla 490 lokalizacji zdalnych wykorzystuje sieć rozległą (WAN) zbudowaną w oparciu o wirtualne sieci prywatne (VPN). Do routerów IP VPN (CE) stanowiących punkt styku z siecią operatora telekomunikacyjnego, podłączone zostały routery dostępne (CPE) Kupującego. Sieć operatora telekomunikacyjnego zapewnia usługę transportową dla routerów CPE. Na routerach Kupującego wykorzystywana jest technologia DMVPN (Dynamic Multipoint Virtual Private Network), dzięki której ruch pomiędzy lokalizacjami Kupującego jest szyfrowany. W Data Center Kupującego dostęp do sieci rozległej zrealizowany jest za pomocą 2 routerów dostępowych Cisco ASR 1002. Routery te mają dedykowane oddzielne połączenia do sieci operatora i zostały skonfigurowane w sposób redundantny. Rolę koncentratora VPN zapewnia pojedynczy router CISCO ASR 1004. Router CISCO ASR 1004 agreguje połączenia IPSEC VPN z 490 lokalizacji na terenie kraju, gdzie zamontowane są routery CPE (Cisco serii 2900), na których uruchomiono protokół DMVPN. Na routerach

wykorzystywane są następujące funkcjonalności: tunelowanie GRE oraz IP, protokół NHRP (Next Hop Resolution Protocol), szyfrowanie ruchu, QoS.

Przedmiotem umowy jest dostarczenie i wdrożenie zapasowego routera, który w sposób automatyczny, w przypadku awarii routera CISCO ASR 1004, przejmie jego rolę i będzie pełnił rolę koncentratora VPN.

Lp.	Wymagania minimalne
1	6 portów Gigabit Ethernet typu SFP
2	2 porty 10 Gigabit Ethernet typu SFP+
3	Wydajność szyfrowania 2 Gbps dla ruchu VPN (AES256) z możliwością podniesienia wydajności do 8 Gbps przez zakup licencji
4	Obsługa co najmniej 1 000 000 tras IPv4, co najmniej 100 000 tras multicast i 3000 grup multicast
5	Liczba tuneli IPsec: 6 000
6	Router musi posiadać funkcjonalność dynamicznych tuneli VPN (hub-to-spoke oraz spoke-to-spoke); funkcjonalność ta musi być kompatybilna z analogiczną Wykorzystywaną przez Zamawiającego na obecnie eksploatowanym routerze Cisco ASR 1004 i routerach Cisco serii 2900 na terenie kraju
7	Router musi obsługiwać protokół NHRP (ang. Next Hop Resolution Protocol)
8	Router musi obsługiwać routing dla IPv4: RIP, OSPF, BGP
9	Router musi obsługiwać MPLS: MPLS VPN
10	Router musi pozwalać na stworzenie co najmniej 1000 instancji VRF (ang. Virtual Routingu Forwarding)
11	Router musi obsługiwać protokół VRRP (ang. Virtual Router Redundancy Protocol)
12	Router musi obsługiwać multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN
13	<p>Router musi obsługiwać następujące funkcje i elementy bezpieczeństwa:</p> <ul style="list-style-type: none"> a) ochrona warstwy kontrolnej urządzenia przed atakami kierowanymi do niego (ograniczanie ruchu kierowanego do urządzenia) b) Unicast RPF (Reverse Path Forwarding) c) listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL d) 4.000 ACL (Access Control Lists) e) dostęp administracyjny oparty o role z przypisanymi uprawnieniami f) zapewnia konfigurację polityk per wirtualna tablica routingu (VRF)
14	<p>Router musi obsługiwać następujące mechanizmy jakości usług (QoS):</p> <ul style="list-style-type: none"> a) klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN b) hierarchiczny QoS (H-QoS) - 3 poziomy c) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, 802.1p (CoS), IP ToS/DSCP d) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
15	Wymiana modułów w trakcie pracy (hot swap)
16	Zarządzanie poprzez CLI (Telnet, SSHv2, port konsoli), SNMPv3
17	Porty umożliwiające zarządzanie: port konsoli, port Ethernet, port AUX

18	Router musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania z wykorzystaniem protokołów RADIUS lub TACACS+
19	Router musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej; konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona
20	Router musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów
21	Wraz z routerem należy dostarczyć elementy do montażu w szafie RACK 19"
22	Router musi posiadać zainstalowane 2 zasilacze w układzie redundantnym o mocy pozwalającej na obsługę w pełni obsadzonego urządzenia; awaria jednego z nich, albo jednego z obwodów zasilających nie może powodować przerwy oraz spadku funkcjonalności w pracy urządzenia, zasilanie z sieci 230V/50Hz
23	Z routerem należy dostarczyć wkładki: 1000BASE-T SFP - 4 sztuki Dostarczone wkładki muszą być na liście sprzętu kompatybilnego z dostarczonym routerem i objęte oficjalnym wsparciem serwisowym

III. Zakres prac wdrożeniowych

1. Wykonanie analizy obecnej konfiguracji przełącznika rdzeniowego i routera VPN będącego w posiadaniu Kupującego.
2. Wykonanie harmonogramu wdrożenia (z uwzględnieniem wymogu prowadzenia prac instalacyjnych i konfiguracyjnych w dni ustawowo wolne od pracy lub w nocy).
3. Wykonanie projektu wdrożenia (w tym diagramów połączeń) dla wszystkich dostarczanych komponentów sieci z uwzględnieniem obecnej infrastruktury Kupującego.
4. Instalacja dostarczonych urządzeń w szafach RACK.
5. Wykonanie konfiguracji nowych urządzeń sieciowych oraz w razie konieczności dokonanie zmian dla istniejących urządzeń, mających związek z przedmiotem zamówienia.
6. Przełączenie okablowania z dotychczasowego przełącznika rdzeniowego do nowych przełączników i oznaczenie patchcordów.
7. Wykonanie testów redundancji po zakończeniu wdrożenia.
8. Przeprowadzenie w siedzibie Kupującego 1 dniowego warsztatu powdrożeniowego dla administratorów Kupującego, podczas których omówiona zostanie konfiguracja dostarczonego sprzętu i wykonane zmiany w infrastrukturze Kupującego.
9. Wykonanie aktualizacji istniejącej dokumentacji sieci.

IV. Szczegółowe warunki serwisu gwarancyjnego i wsparcia technicznego:

1. Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach. Nie dopuszcza się urządzeń typu refurbished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).
2. Wszystkie karty oraz interfejsy dokładane do urządzeń muszą pochodzić od tego samego producenta sprzętu.
3. Sprzedawca zapewnia bezpłatny serwis gwarancyjny w okresie obowiązywania gwarancji.
4. Serwis gwarancyjny musi być świadczony w oparciu o świadczenia gwarancyjne producenta sprzętu i zapewniać prawo do aktualizacji oprogramowania zainstalowanego na urządzeniach.
5. Gwarancji podlegają stwierdzone w dostarczonych urządzeniach wady materiałowe i konstrukcyjne, a także niespełnianie deklarowanych przez producenta funkcji użytkowych.

6. Sprzedawca przystąpi do naprawy urządzeń nie później niż następnego dnia roboczego od zgłoszenia awarii.
7. Serwisowanie sprzętu odbywać się będzie w dni robocze w godzinach pracy Kupującego, tj. od godz. 8:15 do godz. 16:15.
8. Naprawa urządzeń odbywać się będzie w miejscu wskazanym przez Kupującego. Naprawa może odbyć się w serwisie, jeżeli Sprzedawca uzna to za konieczne, przy czym Sprzedawca transportuje uszkodzony sprzęt do serwisu, a po naprawie z serwisu, na własny koszt i ryzyko.
9. Po wykonaniu napraw urządzeń poza siedzibą Kupującego, Sprzedawca zobowiązuje się dokonać ponownej instalacji sprzętu w środowisku Kupującego.
10. Termin naprawy urządzeń sieciowych wynosi maksymalnie 1 dzień roboczy od daty otrzymania zgłoszenia awarii przez Sprzedawcę. Dla zgłoszeń po godz. 16:15 lub w dni ustawowo wolne od pracy, jako datę zgłoszenia przyjmuje się datę pierwszego dnia roboczego.
11. W przypadku, gdy czas usunięcia awarii przekracza 2 dni robocze, Sprzedawca zobowiązuje się do dostarczenia sprzętu zastępczego o parametrach nie gorszych od sprzętu uszkodzonego oraz do jego instalacji.
12. Okres gwarancji zostanie przedłużony o łączną liczbę dni, podczas których sprzęt był wyłączony z eksploatacji z powodu naprawy w okresie objętym gwarancją, o ile nie dostarczono sprzętu zastępczego. Liczbę tę określa się jako liczbę dni, która upłynęła pomiędzy datą zgłoszenia awarii przez Kupującego, a datą naprawy lub dostarczenia naprawionego sprzętu przez Sprzedawcę.
13. W razie odrzucenia reklamacji przez Sprzedawcę, Kupujący może zlecić przeprowadzenie niezależnej ekspertyzy.
14. Jeżeli reklamacja Kupującego okaże się uzasadniona, koszty związane z przeprowadzeniem ekspertyzy ponosi Sprzedawca.
15. Podczas usuwania awarii urządzeń Sprzedawca zobowiązuje się przestrzegać wymagań wynikających m.in. z polityki bezpieczeństwa lub procedur stosowanych u Kupującego, z którymi Kupujący zapozna Sprzedawcę niezwłocznie po zawarciu umowy.
16. Uprawnienia wynikające z udzielonej gwarancji nie wyłączają możliwości dochodzenia przez Kupującego uprawnień z tytułu rękojmi za wady.
17. Sprzedawca zapewni ... godzin (*liczba godzin zostanie uzupełniona na podstawie oferty Sprzedawcy*) wsparcia technicznego inżyniera Sprzedawcy przez okres 12 miesięcy od daty odbioru przedmiotu dostawy. Wsparcie inżynierskie musi być świadczone przez osobę posiadającą kompetencje inżynierskie w zakresie zaoferowanych produktów. Wsparcie techniczne świadczone będzie w dni robocze w godzinach 8-16. W przypadku konieczności świadczenia wsparcia technicznego po godz. 16 lub w dniach wolnych od pracy - termin zostanie uzgodniony ze Sprzedawcą z 3 dniowym wyprzedzeniem.