

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zakup usługi wsparcia i serwisu producenta lub autoryzowanego przedstawiciela producenta wraz ze wsparciem i serwisem oprogramowania dla posiadanych przez Zamawiającego routerów CISCO C8300-2N2S-4T2X oraz CISCO C8200-1N-4T na okres 36 miesięcy, poczynając od dnia podpisania umowy (nie wcześniej niż od dnia 27 grudnia 2025 roku).

Wykonawca w terminie nie dłuższym niż 5 dni kalendarzowych od dnia zawarcia umowy, zobowiązuje się zapewnić na profilu Zamawiającego, na stronie <https://cisco.com> – zarejestrowany elektronicznie kontrakt SmartNet potwierdzający zakup usługi wsparcia i serwisu producenta lub autoryzowanego przedstawiciela producenta wraz ze wsparciem i serwisem oprogramowania, dla posiadanych przez Zamawiającego routerów CISCO C8300-2N2S-4T2X oraz CISCO C8200-1N-4T na okres 36 miesięcy, poczynając od dnia podpisania umowy (nie wcześniej niż od dnia 27 grudnia 2025 roku).

Specyfikacja 1.1.

Lista routerów posiadanych przez Zamawiającego:

L.p.	Model/Producent	nr seryjny
1	Router CISCO C8300-2N2S-4T2X	JAE17110BC2
2	Router CISCO C8300-2N2S-4T2X	JAE12110BCR
3	Router CISCO C8200-1N-4T	SFGL2646LFKY
4	Router CISCO C8200-1N-4T	SFGL2646LF7Q
5	Router CISCO C8200-1N-4T	SFGL2646LFC0
6	Router CISCO C8200-1N-4T	SFGL2646LFH3

Wyżej wymienione urządzenia oraz oprogramowanie muszą zostać objęte na okres 36 miesięcy wsparciem serwisem technicznym opartym o świadczenia serwisowe producenta lub autoryzowanego przedstawiciela producenta, niezależne od statusu partnerskiego Wykonawcy.

I. Oferowane wsparcie techniczne musi zapewnić Zamawiającemu przez cały okres trwania wsparcia:

1. możliwość zgłoszenia awarii urządzenia bezpośrednio producentowi urządzenia lub autoryzowanemu przedstawicielowi producenta (a nie tylko Wykonawcy zamówienia) wraz z możliwością otrzymania „z góry” urządzenia zamiennego, wolnego od uszkodzeń, bez dodatkowych opłat, a jedynie pod warunkiem zwrotu wadliwego urządzenia,
2. bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta przez telefon, e-mail oraz WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją urządzeń,

3. dostęp do producenckiej bazy aktualizacji subskrypcji pozwalających aktualizowanie funkcji bezpieczeństwa, zgodnie z zapotrzebowaniem Zamawiającego, jednakże w ramach ogólnie dostępnej oferty producenta, a także w ramach wykupionego zestawu funkcjonalności oprogramowania i wykupionej konfiguracji urządzeń, wraz z wolnym od dodatkowych opłat prawem (tj. licencją) do korzystania z pobranego oprogramowania, na zasadach określonych w warunkach licencyjnych dla użytkownika końcowego,
4. czas naprawy lub wymiany urządzeń nie może przekroczyć 48 godzin zegarowych liczonych w oknie 7:30 -15:30, 5 dni roboczych w tygodniu - od chwili zgłoszenia awarii,
5. serwis świadczony w miejscu instalacji. Zamawiający dopuszcza świadczenie usługi on-site przez Wykonawcę oraz zdalną diagnozę uszkodzenia.

II. Oferowane wsparcie dla oprogramowania systemowego musi zapewnić

Zamawiającemu przez cały okres trwania wsparcia producenta następujące możliwości w zakresie oprogramowania:

1. Możliwość zgłoszenia awarii oprogramowania bezpośrednio producentowi oprogramowania lub autoryzowanemu przedstawicielowi producenta (a nie tylko Wykonawcy zamówienia),
2. Bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta lub autoryzowanego przedstawiciela producenta przez telefon, e-mail oraz WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją oprogramowania,
3. Dostęp do producenckiej bazy aktualizacji oprogramowania, subskrypcji pozwalających aktualizowanie funkcji bezpieczeństwa, zgodnie z zapotrzebowaniem Zamawiającego, jednakże w ramach ogólnie dostępnej oferty producenta, a także w ramach wykupionego zestawu funkcjonalności oprogramowania i wykupionej konfiguracji urządzeń, wraz z wolnym od dodatkowych opłat prawem (tj. licencją) do korzystania z pobranego oprogramowania, na zasadach określonych w warunkach licencyjnych dla użytkownika końcowego,

Dla routerów CISCO C8300-2N2S-4T2X zapewni funkcjonalności w zakresie:

1. Szyfrowanie wszystkich łączy WAN z centralnym, redundantnym kontrolerem zarządzającym i monitorującym całą sieć, z możliwością ustalania polityk związanych z jakością obsługi aplikacji i ew. przełączeniem ruchu aplikacji na łącza spełniające wymagania aplikacji zdefiniowane w polityce:
 - a) bezpieczne połączenie WAN lokalizacji, wykorzystując w tym celu dowolną kombinację połączeń przez sieć transportową (IP VPN), jak też opcjonalnie sieci publiczne (Internet);
 - b) aktywne wykorzystanie wszystkich dostępnych połączeń pomiędzy lokalizacjami, odpowiednio sterując ruchem zależnie od aktualnych warunków;
 - c) elastyczne tworzenie topologii (gwiazda, częściowa lub pełna kratę, punkt-punkt) per segment;
 - d) monitorowanie wydajności wszystkich łączy systemu;
 - e) równoważenie obciążenia poszczególnych łączy (per sesja):
 - statyczne (active/standby i active/active równoważne i ważone)
 - dynamiczne oparte o monitorowanie jakości w danym czasie;
 - f) redundancja active-active urządzeń na poziomie zakończenia usługi w każdej lokalizacji (jedno urządzenie CE obsługujące łącze podstawowe, drugie urządzenie CE obsługujące łącza podstawowe i zapasowe).
2. Funkcjonalności z zakresu bezpieczeństwa:
 - a) szyfrowanie wszystkich połączeń co najmniej AES256;
 - b) funkcja skrótu co najmniej SHA-2;
 - c) uwierzytelnienie urządzeń na bazie certyfikatów X.509 podpisanych zaufanymi kluczami prywatnymi – zintegrowane w systemie CA z mechanizmem automatycznej dystrybucji kluczy (bez wykorzystania kluczy typu pre-shared);

- d) obsługa list kontroli dostępu (ACL);
 - e) segmentacja sieci, np. w oparciu o osobne tablice routingu (obsługa nakładających się przestrzeni adresowych); możliwość definicji topologii sieciowej per segment; obsługa co najmniej 4-ech segmentów;
 - f) obsługa translacji adresów NAT/PAT i NAT Traversal - wsparcie dla lokalnego wyjścia do Internetu z pominięciem komunikacji przez sieć WAN dla zdefiniowanych aplikacji – ruch taki powinien być translowany i lokalnie wychodzić do Internetu;
 - g) możliwość segmentacji routera na 4 odseparowane na warstwie IP podsieci – poprzez funkcjonalność VPN;
 - h) funkcjonalność zapory sieciowej dla protokołu opartej o definicję stref bezpieczeństwa (zone-based firewall);
 - i) funkcjonalność IPS;
 - j) funkcjonalność filtracji URL;
 - k) funkcjonalność analizy ruchu pod kątem występowania w nim malware'u.
3. Polityki jakości obsługi aplikacji:
- a) wykrywanie aplikacji na bazie głębokiej inspekcji ruchu (DPI);
 - b) możliwość definicji polityki systemu określającej maksymalne tolerowane przez określoną aplikację parametry sieci: opóźnienie, zmienność opóźnień, straty w pakietach - w przypadku przekroczenia zdefiniowanych progów ruch aplikacyjny powinien zostać przekierowany na inne łącze WAN, jeśli spełnia ono wymogi aplikacji wg polityki;
 - c) monitorowanie jakości dostępu do usług chmurowych typu SaaS (co najmniej Google Apps, Office365, Dropbox) i IaaS (co najmniej AWS, Azure) z możliwością optymalizacji dostępu do nich - system musi umożliwiać przekierowanie ruchu do usług przez każdy węzeł dysponujący wyjściem do Internetu, zapewniający w danym czasie najlepszą jakość dostępu do usługi.
4. Mechanizmy zapewnienia jakości ruchu (QoS):
- a) obsługa kształtowania (shaping), ograniczania (policing) ruchu, gwarancje pasma;
 - b) kolejkowanie z kolejką priorytetową i model WFQ (Weighted Fair Queuing) dla pozostałych klas ruchu;
 - c) mechanizm tail-drop i RED (Random Early Detect);
 - d) oznaczanie i zmiana oznaczeń DSCP na bazie przekroczeń ograniczeń ruchu.
5. Obsługa protokołów routingu dynamicznego:
- a) BFD;
 - b) OSPFv2 (także na portach LAN);
 - c) BGP.
6. Obsługa protokołów i funkcjonalności sieciowych:
- a) 802.1q;
 - b) SSHv2;
 - c) SNMP v2c, v3;
 - d) NTP z uwierzytelnieniem;
 - e) Syslog
7. Mechanizmy konfiguracji „zero touch” – możliwość skonfigurowania urządzenia brzegowego w sposób automatyczny z wykorzystaniem centralnego kontrolera bez konieczności prekonfiguracji samego urządzenia brzegowego (bez wpisywania kodów, tokenów, czy wspólnych haseł).
8. Rozwiązanie ma opierać się o centralny kontroler, routery CE uwierzytelniające się z innymi komponentami rozwiązania poprzez certyfikaty X.509 podpisane kluczami prywatnymi.
9. Interfejs kontrolera musi zapewniać:

- a) graficzny interfejs konfiguracyjny;
 - b) obsługę API umożliwiającego konfigurację wszystkich możliwości oferowanych przez kontroler; dopuszczalne standardy API to: Python, Ansible, REST, RESTConf, NETConf/Yang, XML;
 - c) obsługę RBAC (możliwość zróżnicowania ról administratorów w zakresie brak dostępu / tylko odczyt / pełen dostęp dla poszczególnych funkcjonalności systemu zarządzania – co najmniej alarmów, logów, monitorowania urządzeń, aktualizacji oprogramowania, interfejsów, polityk, routingu, bezpieczeństwa);
 - d) zarządzanie routerami ma odbywać się całkowicie z poziomu kontrolerów centralnych;
 - e) wymaga się zarządzania aktualizacją oprogramowania z centralnego systemu;
 - f) zarządzanie oraz diagnostyka z poziomu GUI oraz CLI;
 - g) konfiguracja urządzeń oparta o wzorce konfiguracyjne.
10. Przepustowość routera dla szyfrowania 20 Gb/s (10 Gb/s w każdym z kierunków przepływu ruchu);
11. Pozostała funkcjonalność:
- a) obsługa ruchu multicastowego, realizacja protokołów: PIM Sparse/Dense, PIM-SSM, IGMPv3; Bi-Di PIM, MLD (v1, v2), MSDP;
 - b) obsługa ruchu multicastowego w sieci overlay z obsługą replikacji w poszczególnych węzłach sieciowych (w celu uniknięcia replikacji u źródła);
 - c) możliwość tworzenia polityk QoS per sieć VPN oraz możliwość zestawiania dynamicznych tuneli w relacji pomiędzy routerami brzegowymi;
 - d) możliwość definiowania polityki określającej maksymalne tolerowane przez określoną aplikację parametry sieci: opóźnienie, zmienność opóźnień, straty w pakietach - w przypadku przekroczenia zdefiniowanych progów ruch aplikacyjny powinien zostać przekierowany na inne łącze WAN, jeśli spełnia ono wymogi aplikacji wg polityki;
 - e) obsługa mechanizmów podnoszących niezawodność dostarczania pakietów na łączach stratnych: poprzez dostarczanie pakietów nadmiarowych z wyliczoną sumą kontrolną z kilku pakietów pozwalającej na odtworzenie zagubionego pakietu; poprzez duplikowanie pakietów dla określonego ruchu i wysyłanie ich na więcej niż jedno łącze transportowe (tunel). Pakiety duplikowane powinny być automatycznie rozpoznawane po stronie docelowej i tylko pierwszy dostarczony pakiet powinien zostać przesyłany dalej, a kopie odrzucone na urządzeniu brzegowym.

Dla routerów CISCO C8200-1N-4T zapewni funkcjonalności w zakresie:

1. Szyfrowanie wszystkich łączy WAN z centralnym, redundantnym kontrolerem zarządzającym i monitorującym całą sieć, z możliwością ustalania polityk związanych z jakością obsługi aplikacji i ew. przełączeniem ruchu aplikacji na łącza spełniające wymagania aplikacji zdefiniowane w polityce:
 - a) bezpieczne połączenie WAN lokalizacji, wykorzystując w tym celu dowolną kombinację połączeń przez sieć transportową (IP VPN), jak też opcjonalnie sieci publiczne (Internet);
 - b) aktywne wykorzystanie wszystkich dostępnych połączeń pomiędzy lokalizacjami, odpowiednio sterując ruchem zależnie od aktualnych warunków;
 - c) elastyczne tworzenie topologii (gwiazda, częściowa lub pełna kratę, punkt-punkt) per segment;
 - d) monitorowanie wydajności wszystkich łączy systemu;
 - e) równoważenie obciążenia poszczególnych łączy (per sesja):
 - statyczne (active/standby i active/active równoważne i ważone)
 - dynamiczne oparte o monitorowanie jakości w danym czasie

- f) redundancja active-active urządzeń na poziomie zakończenia usługi w każdej lokalizacji (jedno urządzenie CE obsługujące łącze podstawowe, drugie urządzenie CE obsługujące łącza podstawowe i zapasowe).
2. Funkcjonalności z zakresu bezpieczeństwa:
- a) szyfrowanie wszystkich połączeń co najmniej AES256;
 - b) funkcja skrótu co najmniej SHA-2;
 - c) uwierzytelnienie urządzeń na bazie certyfikatów X.509 podpisanych zaufanymi kluczami prywatnymi – zintegrowane w systemie CA z mechanizmem automatycznej dystrybucji kluczy (bez wykorzystania kluczy typu pre-shared);
 - d) obsługa list kontroli dostępu (ACL);
 - e) segmentacja sieci, np. w oparciu o osobne tablice routingu (obsługa nakładających się przestrzeni adresowych); możliwość definicji topologii sieciowej per segment; obsługa co najmniej 4-ech segmentów;
 - f) obsługa translacji adresów NAT/PAT i NAT Traversal - wsparcie dla lokalnego wyjścia do Internetu z pominięciem komunikacji przez sieć WAN dla zdefiniowanych aplikacji – ruch taki powinien być translowany i lokalnie wychodzić do Internetu;
 - g) możliwość segmentacji routera na 4 odseparowane na warstwie IP podsieci – poprzez funkcjonalność VPN;
 - h) funkcjonalność zapory sieciowej dla protokołu opartej o definicję stref bezpieczeństwa (zone-based firewall);
 - i) funkcjonalność IPS;
 - j) funkcjonalność filtracji URL;
 - k) funkcjonalność analizy ruchu pod kątem występowania w nim malware'u.
3. Polityki jakości obsługi aplikacji:
- a) wykrywanie aplikacji na bazie głębokiej inspekcji ruchu (DPI);
 - b) możliwość definicji polityki systemu określającej maksymalne tolerowane przez określoną aplikację parametry sieci: opóźnienie, zmienność opóźnień, straty w pakietach - w przypadku przekroczenia zdefiniowanych progów ruch aplikacyjny powinien zostać przekierowany na inne łącze WAN, jeśli spełnia ono wymogi aplikacji wg polityki;
 - c) monitorowanie jakości dostępu do usług chmurowych typu SaaS (co najmniej Google Apps, Office365, Dropbox) i IaaS (co najmniej AWS, Azure) z możliwością optymalizacji dostępu do nich - system musi umożliwiać przekierowanie ruchu do usług przez każdy węzeł dysponujący wyjściem do Internetu, zapewniający w danym czasie najlepszą jakość dostępu do usługi.
4. Mechanizmy zapewnienia jakości ruchu (QoS):
- a) obsługa kształtowania (shaping), ograniczania (policing) ruchu, gwarancje pasma;
 - b) kolejkowanie z kolejką priorytetową i model WFQ (Weighted Fair Queuing) dla pozostałych klas ruchu;
 - c) mechanizm tail-drop i RED (Random Early Detect);
 - d) oznaczanie i zmiana oznaczeń DSCP na bazie przekroczeń ograniczeń ruchu.
5. Obsługa protokołów routingu dynamicznego:
- a) BFD;
 - b) OSPFv2 (także na portach LAN);
 - c) BGP.
6. Obsługa protokołów i funkcjonalności sieciowych:
- a) 802.1q;
 - b) SSHv2;
 - c) SNMP v2c, v3;
 - d) NTP z uwierzytelnieniem;

- e) Syslog
- 7. Mechanizmy konfiguracji „zero touch” – możliwość skonfigurowania urządzenia brzegowego w sposób automatyczny z wykorzystaniem centralnego kontrolera bez konieczności prekonfiguracji samego urządzenia brzegowego (bez wpisywania kodów, tokenów, czy wspólnych haseł).
- 8. Rozwiązanie ma opierać się o centralny kontroler, routery CE uwierzytelniające się z innymi komponentami rozwiązania poprzez certyfikaty X.509 podpisane kluczami prywatnymi.
- 9. Interfejs kontrolera musi zapewniać:
 - a) graficzny interfejs konfiguracyjny;
 - b) obsługę API umożliwiającego konfigurację wszystkich możliwości oferowanych przez kontroler; dopuszczalne standardy API to: Python, Ansible, REST, RESTConf, NETConf/Yang, XML;
 - c) obsługę RBAC (możliwość zróżnicowania ról administratorów w zakresie brak dostępu/tylko odczyt/pełen dostęp dla poszczególnych funkcjonalności systemu zarządzania – co najmniej alarmów, logów, monitorowania urządzeń, aktualizacji oprogramowania, interfejsów, polityk, routingu, bezpieczeństwa);
 - d) zarządzanie routerami ma odbywać się całkowicie z poziomu kontrolerów centralnych;
 - e) wymaga się zarządzania aktualizacją oprogramowania z centralnego systemu;
 - f) zarządzanie oraz diagnostyka z poziomu GUI oraz CLI;
 - g) konfiguracja urządzeń oparta o wzorce konfiguracyjne.
- 10. Zagregowana przepustowość routera dla szyfrowania 500 Mb/s (250 Mb/s w każdym z kierunków przepływu ruchu).
- 11. Pozostała funkcjonalność:
 - a) obsługa ruchu multicastowego, realizacja protokołów: PIM Sparse/Dense, PIM-SSM, IGMPv3; Bi-Di PIM, MLD (v1, v2), MSDP;
 - b) obsługa ruchu multicastowego w sieci overlay z obsługą replikacji w poszczególnych węzłach sieciowych (w celu uniknięcia replikacji u źródła);
 - c) możliwość tworzenia polityk QoS per sieć VPN oraz możliwość zestawiania dynamicznych tuneli w relacji pomiędzy routerami brzegowymi;
 - d) możliwość definiowania polityki określającej maksymalne tolerowane przez określoną aplikację parametry sieci: opóźnienie, zmienność opóźnień, straty w pakietach - w przypadku przekroczenia zdefiniowanych progów ruch aplikacyjny powinien zostać przekierowany na inne łącze WAN, jeśli spełnia ono wymogi aplikacji wg polityki;
 - e) obsługa mechanizmów podnoszących niezawodność dostarczania pakietów na łączach stratnych: poprzez dostarczanie pakietów nadmiarowych z wyliczoną sumą kontrolną z kilku pakietów pozwalającej na odtworzenie zagubionego pakietu; poprzez duplikowanie pakietów dla określonego ruchu i wysyłanie ich na więcej niż jedno łącze transportowe (tunel). Pakiety duplikowane powinny być automatycznie rozpoznawane po stronie docelowej i tylko pierwszy dostarczony pakiet powinien zostać przesyłany dalej a kopie odrzucone na urządzeniu brzegowym.

Opis rozwiązania równoważnego:

- I. W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego Zamawiający wymaga, aby Wykonawca:
 - 1) zapewnił warunki i zakres usługi wsparcia producenta dla produktów równoważnych nie gorsze niż usługa określona dla produktów producenta Cisco,
 - 2) zapewnił warunki wsparcia dla oprogramowania w każdym aspekcie nie gorsze niż warunki wsparcia oprogramowania dla urządzeń Cisco w momencie ich zakupu,

- 3) umożliwił implementację oprogramowania równoważnego uruchamianego na istniejących konfiguracjach urządzeń Cisco,
 - 4) zapewnił, że dostarczane subskrypcje, licencji oprogramowania równoważnego pozwalają na legalne używanie posiadanych przez Zamawiającego licencji oprogramowania Cisco,
 - 5) wykazał, że funkcjonalność produktów oprogramowania równoważnego nie jest gorsza od funkcjonalności przewidzianych dla produktów producenta Cisco,
 - 6) zapewnił, że wsparcie i serwis dla urządzeń Cisco pozwoli w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem systemowym, aplikacyjnym i użytkowym, eksploatowanym przez Zamawiającego. Powyższe wsparcie i serwis dla urządzeń oraz oprogramowania musi umożliwiać korzystanie ze wszystkich funkcjonalności dostępnych w urządzeniach i oprogramowaniu Cisco posiadanych przez Zamawiającego,
 - 7) zapewnił, że warunki i zakres usługi asysty technicznej i konserwacji dla produktów równoważnych nie są gorsze, niż usługi oferowane przez producenta Cisco,
 - 8) zapewni w ramach ceny ofertowej przeszkolenie min 5 użytkowników Zamawiającego z funkcjonalności i sposobu działania zaoferowanych produktów równoważnych.
- II. Wykonawca, który powoła się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać w ofercie, że oferowane przez niego rozwiązania spełniają wymagania określone przez Zamawiającego. Na Wykonawcy spoczywa ciężar dowodu - dowody powinny zawierać informacje umożliwiające Zamawiającemu weryfikację spełniania przez oferowane rozwiązania równoważne poszczególnych kryteriów równoważności.
- III. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie sprzętowej ani w warstwie oprogramowania.

Inne warunki dotyczące zamówienia - podsumowanie:

Wykonawca zobligowany jest do zapewnienie wsparcia i serwisu technicznego producenta lub autoryzowanego przedstawiciela producenta z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych. Wykonawca wraz ze wsparciem i serwisem producenta zobowiązany jest w terminie nie dłuższym niż 5 dni kalendarzowych od dnia zawarcia umowy, dostarczyć na adres e-mail wskazany przez Zamawiającego: zakupy-it@lublin.sa.gov.pl poświadczony za zgodność z oryginałem przez Wykonawcę (kwalifikowanym podpisem elektronicznym) dokument potwierdzający zarejestrowanie kontraktu SmartNet oraz potwierdzający bezpośredni dostęp Zamawiającego do wsparcia producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem, wystawiony przez producenta urządzeń lub jego oficjalnego przedstawiciela. Wykupiona usługa musi zapewnić wsparcie techniczne w ramach kontraktu SmartNet, min. w trybie 8x5xNBD.