**<u>Załącznik nr 2 do Zaproszenia</u>**
**<u>Załącznik nr 2 do Umowy</u>**
**<u>Nr postępowania: Adm.262.50.2025</u>**

***Opis Przedmiotu Zamówienia dla usługi serwisu i wsparcia technicznego dla Przełączników i Routerów SD-WAN na potrzeby Sądu Rejonowego w Węgrowie w okresie od 27 grudnia 2025 roku do 26 grudnia 2028 roku***

Przedmiotem zamówienia jest dostawa wsparcia i serwisu producenta wraz ze wsparciem i serwisem oprogramowania systemowego dla posiadanych przez Zamawiającego przełączników oraz urządzeń SD-WAN na okres 36 miesięcy, poczynając od dnia 27 grudnia 2025 roku:

| | Nazwa | Model/Producent | Nr seryjny |
|---|---|---|---|
| 1 | Przełącznik | C9200-48P-E/Cisco | JAE254105VV |
| 2 | Przełącznik | C9200-48P-E/Cisco | JAE25420Z5Y |
| 3 | Router SD-WAN | C8200-1N-4T/Cisco | SFGL2646LFAW |
| 4 | Router SD-WAN | C8200-1N-4T/Cisco | SFGL2646LFKR |

Wykonawca w terminie nie dłuższym niż 5 dni kalendarzowych od dnia zawarcia umowy, zobowiązuje się zapewnić na profilu Zamawiającego, na stronie producenta pod adresem: https://cisco.com – zarejestrowany elektronicznie kontrakt SmartNet potwierdzający dostawę wsparcia i serwisu producenta wraz ze wsparciem i serwisem oprogramowania systemowego, dla posiadanych przez Zamawiającego przełączników i urządzeń SD-WAN na okres 36 miesięcy, począwszy od dnia 27 grudnia 2025 roku. Przełączniki i urządzenia SD-WAN wymienione w tabeli powyżej, muszą zostać objęte na okres 36 miesięcy (poczynając od dnia 27 grudnia 2025 roku) wsparciem technicznym opartym o świadczenia serwisowe 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 (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. możliwość pobierania bezpośrednio od producenta nowych wydań oprogramowania systemowego, 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.

Oprogramowanie musi pochodzić od producenta urządzeń i być objęte 36 miesięcznym wsparciem opartym o świadczenia serwisowe producenta, niezależne od statusu partnerskiego Wykonawcy.

**II. Oferowane wsparcie dla oprogramowania systemowego musi zapewnić Zamawiającemu przez cały okres trwania wsparcia producenta następujące możliwości w zakresie oprogramowania:**

1. możliwość zgłoszenia awarii bezpośrednio producentowi oprogramowania (a nie tylko Wykonawcy zamówienia),
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. możliwość pobierania bezpośrednio od producenta nowych wydań oprogramowania, zgodnie z zapotrzebowaniem Zamawiającego, jednakże w ramach ogólnie dostępnej oferty producenta, a także w ramach wykupionego zestawu funkcjonalności oprogramowania, wraz z wolnym od dodatkowych opłat prawem (tj. licencją) do korzystania z pobranego oprogramowania na zasadach określonych w warunkach licencyjnych dla użytkownika końcowego.

## Dla Cisco C8200-1N-4T 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 łącz (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 dostarczania 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 CISCO C9200-48P-E:

1. możliwość zgłoszenia awarii bezpośrednio producentowi oprogramowania (a nie tylko Wykonawcy zamówienia);
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. możliwość pobierania bezpośrednio od producenta nowych wydań oprogramowania, zgodnie z zapotrzebowaniem Zamawiającego, jednakże w ramach ogólnie dostępnej oferty producenta, a także w ramach wykupionego zestawu funkcjonalności oprogramowania, wraz z wolnym od dodatkowych opłat prawem (tj. licencją) do korzystania z pobranego oprogramowania na zasadach określonych w warunkach licencyjnych dla użytkownika końcowego;
4. graficzny system do zarządzania i monitorowania sieci kampusowej przewodowej oraz bezprzewodowej;
5. funkcjonalności z zakresu zarządzania i konfiguracji sieci:
   1) hierarchizacja zarządzania siecią odzwierciedlająca hierarchię geograficzną tj. możliwość podziału sieci na kilka poziomów geograficznych np. region, kraj, miasto, budynek, piętro;
   2) wizualizacja poszczególnych budynków na mapie świata – automatyczne rozmieszczanie budynków w odpowiednich miejscach na podstawie adresów pocztowych;
   3) wgrywanie własnych planów budynków z dokładnością do poszczególnych pięter;
   4) funkcjonalność automatycznego wykrywania urządzeń sieciowych w oparciu o SNMP, CLI, HTTP, SSH;
   5) inwentaryzacja urządzeń oraz oprogramowania w zakresie minimum:
      a) nazwa urządzenia;
      b) adres IP oraz adres MAC urządzenia;
      c) typ urządzenia;
      d) lokalizacja;
      e) osiągalność oraz czas „uptime”;
      f) numer seryjny;
      g) wersja oprogramowania oraz zgodność oprogramowania z obowiązującą wersją.
   6) indeks jakości pracy;
   7) współczynnik zgodności z przyjętymi kryteriami (compliance);
   8) narzędzie do definiowania profili sieciowych oraz parametrów sieciowych takich jak: serwery TACACS+, RADIUS, NTP, Syslog, NetFlow, DNS, DHCP dla poszczególnych poziomów hierarchii sieciowej niezależnie lub dziedziczenie tych ustawień z poziomu wyższego w dół hierarchii; Centralne zarządzanie parametrami dostępowymi do urządzeń wraz z możliwością ich zmiany dla jednego urządzenia, grupy urządzeń lub całej sieci;

9) tworzenie sparametryzowanych wzorców konfiguracyjnych dla urządzeń w oparciu o język skryptowy;
10) konfiguracja indywidualnych przełączników pod kątem następujących ustawień, takich jak: obsługiwane VLANy, ustawienia STP, ustawienia DHCP Snooping, IGMP Snooping, MLD Snooping, konfiguracja ustawień indywidualnych portów takich jak: tryb pracy portu, przypisany VLAN, status portu, uwierzytelnianie 802.1X;
11) narzędzie do aktualizacji oprogramowania na urządzeniach umożliwiające:
    a) zarządzanie wersjami oprogramowania z możliwością wskazania wersji obowiązujących;
    b) weryfikację warunków technicznych i software'owych do wykonania aktualizacji (ilość wolnego miejsca, weryfikacja ustawień konfiguracji startowej, warunki do wykonania aktualizacji bezprzerwowej ISSU – In Service Software Upgrade);
    c) przeprowadzenie aktualizacji na wybranych urządzeniach lub grupie urządzeń, w tym bezprzerwowej aktualizacji ISSU dla urządzeń, które wspierają taką funkcję;
    d) wykonanie predefiniowanych i możliwość dodania własnych komend kontrolnych (sprawdzeń) przed i po wykonaniu aktualizacji;
    e) funkcja zaprogramowania daty i czasu wykonania aktualizacji;
    f) funkcja usunięcia z pamięci Flash urządzenia nieaktualnych wersji oprogramowania po aktualizacji;
    g) raport z aktualizacji obejmujący wynik aktualizacji i jej przebieg, status wykonania komend kontrolnych oraz raport niezgodności;
12) narzędzie do archiwizacji konfiguracji urządzeń umożliwiające:
    a) stworzenie kopii zapasowej konfiguracji;
    b) ustalenie dnia i godziny automatycznego stworzenia kopii zapasowej;
    c) wyświetlanie na osi czasu punktów, w których została dokonania kopia konfiguracji razem z wyświetleniem różnic między wersjami;
    d) zapisywanie do 50 kopii konfiguracji danego urządzenia;
    e) zapisywanie konfiguracji lokalnie lub na zewnętrznym serwerze SFTP z opcją ustalenia archiwizacji co określona ilość dni lub tygodni oraz datą zakończenia archiwizacji;
13) narzędzie do bezdotykowej konfiguracji urządzeń sieciowych (Plug and Play lub Zero Touch Deployment);
14) narzędzie do automatyzacji procesu wymiany urządzenia uszkodzonego na urządzenie serwisowe obejmujące odtworzenie parametrów takich jak: wersja systemu operacyjnego, konfiguracja, licencje oraz aktualizacja danych w bazie systemu zarządzania (numer seryjny);
15) wbudowane narzędzia do automatycznego tworzenia polityki QoS dla całej sieci w oparciu o wbudowane wzorce aplikacji, z możliwością tworzenia własnych wzorców. Możliwości dokonywania zmian w polityce i jej szybkiej implementacji oraz możliwość cofania zmian bez konieczności ręcznej rekonfiguracji urządzeń sieciowych;
16) narzędzie do zdalnego uruchamiania aplikacji w kontenerach Dockerowych i zarządzania nimi na urządzeniach sieciowych wyposażonych w taką funkcjonalność;
17) analiza zgodności zarządzanego urządzenia (routera, przełącznika, kontrolera WLAN) pod kątem:

a) status na podstawie informacji publikowanej przez producenta, o końcu wsparcia urządzenia pod kątem sprzętowym i software'owym;
b) zgodność konfiguracji urządzenia z przyjętym wzorcem konfiguracji/ustawieniami systemowymi;
c) zgodność bieżącego oprogramowania urządzenia z ustaloną przez administratora wersją oprogramowania;

6. Monitoring urządzeń:
1) monitoring dostępności i osiągalności poszczególnych urządzeń sieciowych;
2) pełna lista wszystkich monitorowanych urządzeń sieciowych w całej sieci lub w danej domenie lub lokalizacji z podaniem modelu urządzenia, wersji systemu operacyjnego, adresu IP, indeksu jakości pracy, osiągalności, ilości zidentyfikowanych problemów, lokalizacji geograficznej. Możliwość eksportu danych w postaci pliku CSV;
3) możliwość łatwego filtrowania listy urządzeń wg. kryteriów:
   a) typ urządzenia: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, radiowy punkt dostępowy, kontroler WLAN;
   b) stan jakości pracy urządzenia: jakość niska, średnia, wysoka;
   c) lokalizacja;
   d) model urządzenia;
   e) wersja systemu operacyjnego;
   f) adres IP;
   g) adres MAC;
4) W zakresie sieci bezprzewodowej wykresy:
   a) ilości aktywnych i nieaktywnych punktów radiowych z podaniem dokładnej listy urządzeń w każdej z kategorii;
   b) lista radiowych punktów dostępowych wg. ilości podłączonych klientów bezprzewodowych;
   c) lista radiowych punktów dostępowych wg. poziomu zakłóceń i interferencji w funkcji pasma transmisji 2.4 GHz, 5 GHz;
5) Narzędzie do analizy wykorzystania energii elektrycznej dostarczanej przez Power over Ethernet (PoE), w szczególności dostarczanie takich informacji jak:
   a) całkowita energia PoE z podziałem na alokowaną i konsumowaną przez odbiorniki PoE wraz z wizualizacją trendu zmiany zużycia energii na przestrzeni czasu;
   b) ilość urządzeń pobierających PoE z rozbiciem na: prawidłowo zasilane, urządzenia do których PoE nie zostało dostarczone, uszkodzone, wyłączone wraz z wizualizacją trendu zmiany tych wartości na przestrzeni czasu oraz możliwością wyświetlenia informacji o indywidualnych urządzeniach w danym zakresie;
   c) ilość urządzeń pobierających PoE z podziałem na zakresy alokowanej ilości energii: do 4W, do 15,4W, do 30W, do 60W, do 90W i powyżej 90W wraz z wizualizacją trendu zmiany tych wartości na przestrzeni czasu oraz możliwością wyświetlenia informacji o indywidualnych urządzeniach w danym zakresie;
6) Szczegółowy monitoring każdego z urządzeń sieciowych obejmujący:
   a) wykres zmian indeksu jakości pracy urządzenia w zadanym okresie czasu do 30 dni wstecz;

b) szczegółowa informacja o następujących parametrach pracy urządzenia w dowolnym momencie pracy urządzenia do 30 dni wstecz. Monitorowane parametry: utylizacja pamięci, utylizacja CPU, dostępność łączy uplinkowych (w górę sieci), poziom błędów na linkach, skojarzone zdarzenia zarejestrowane w systemie;
c) szczegółowa lista wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 30 dni wstecz) o problemach skojarzonych z danym urządzeniem;
d) schemat topologii sieci, w której znajduje się dane urządzenie;
e) dostęp do zdarzeń zarejestrowanych w systemie związanych z danym urządzeniem z możliwością filtrowanie wg. ważności;
f) możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia do danego innego miejsca (adresu IP);
g) możliwość bezpośredniego z poziomu konsoli graficznej systemu zarządzania i monitorowania dostępu do konsoli urządzenia lub narzędzia umożliwiającego zdalne wydawanie komend na urządzeniu;
h) szczegółowe informacje o urządzeniu obejmujące:
   - wykres czasowy utylizacji CPU;
   - wykres czasowy utylizacji pamięci;
   - wykres czasowy dostępności urządzenia;
   - wykres czasowy temperatury urządzenia;
   - informacje o poszczególnych interfejsach urządzeń w uwzględnieniem: stanu interfejsu, typu, numer skonfigurowanej sieci VLAN, MAC adresu podłączonego urządzenia, prędkość linku, FDX/HDX;
i) dla każdego z monitorowanych interfejsów informacje o:
   - wykres czasowy dostępności interfejsu;
   - wykres czasowy utylizacji interfejsu niezależnie w kierunku nadawczym i odbiorczym;
   - wykres czasowy poziomu błędów niezależnie w kierunku nadawczym i odbiorczym;

7) w przypadku urządzeń pracujących jako urządzenia w sieci SDN typu Network Fabric szczegółowe informacje na temat stanu połączenia z siecią podkładową, stanu podłączenia do systemu kontroli dostępu w sieci Network Fabric;

7. Monitoring użytkowników:

1) szczegółowe informacje o użytkowniku końcowym i urządzeniach na których pracuje takie jak:
   a) identyfikator użytkownika,
   b) nazwa hosta lub hostów, na których pracuje,
   c) adres MAC hosta lub hostów,
   d) adres IPv4 i IPv6 hosta lub hostów,
   e) typ urządzenia,
   f) urządzenie, do którego jest podłączone dane urządzenie końcowe wykorzystywane przez użytkownika,

g) lokalizacja geograficzna;
2) wykres zmian indeksu jakości pracy użytkownika i urządzenia, urządzenia, które wykorzystuje w zadanym okresie czasu do 30 dni wstecz;
3) szczegółowa informacja o następujących parametrach pracy urządzenia końcowego wykorzystywanego przez użytkownika w dowolnym momencie do 30 dni wstecz. Monitorowane parametry: stan podłączenia do sieci, dla urządzeń bezprzewodowych: poziom sygnału RSSI, poziom szumów SNR, przepustowość połączenia, ilość danych otrzymanych i nadawanych, SSID sieci, do której jest podłączone urządzenie końcowe, nazwa radiowego punktu dostępowego, wykorzystywany kanał radiowy i pasmo;
4) szczegółowa lista wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz) problemów skojarzonych z danym urządzeniem końcowym;
5) schemat topologii sieci z zaznaczeniem urządzenia dostępowego do którego jest podłączone dane urządzenie końcowe;
6) dostęp do zdarzeń zarejestrowanych w systemie związanych z danym urządzeniem z możliwością filtrowanie wg. ważności;
7) możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia do danego innego miejsca (adresu IP);
8) informacje o generowanym ruchu sieciowym przez użytkownika na danym urządzeniu końcowym z podziałem na aplikacje biznesowe oraz niebiznesowe. Szczegółowe informacje dla każdej z aplikacji takie jak: nazwa aplikacji, indeks jakości działania aplikacji w sieci, ilość ruchu (w bajtach), średnia przepustowość (w bps), parametry QoS faktyczne oraz oczekiwane, straty pakietów (maksymalne i średnie), opóźnienie sieciowe (maksymalne i średnie), jitter (maksymalny i średni);
9) szczegółowe informacje o urządzeniu końcowym wykorzystywanym przez użytkownika:
   a) wykres czasowy ilości danych nadawanych i otrzymywanych;
   b) wykres czasowy ilości generowanych zapytań DNS i otrzymywanych odpowiedzi;
   c) dla urządzeń bezprzewodowych wykres czasowy zmian wartości mocy sygnału radiowego RSSI oraz zmian wartości poziomu szumów SNR;
   d) dodatkowe dane analityczne dla użytkowników urządzeń końcowych wyposażonych w system operacyjny Apple iOS;

8. <u>Monitoring aplikacji:</u>
   1) szczegółowe informacje o aplikacjach wykorzystywanych w sieci takie jak: lista wszystkich wykrytych aplikacji z podaniem nazw aplikacji, klas ruchu, ilości ruchu generowanego, średniej przepustowości, straty pakietów, opóźnienia sieciowego oraz wykrytych problemów związanych z daną aplikacją;
   2) szczegółowe wykresy czasowe parametrów działania każdej z aplikacji z uwzględnieniem: przepustowości wykorzystywanej przez daną aplikację, strat pakietów, jitter, opóźnienia sieciowego, opóźnienia sieciowego po stronie klienta, opóźnienia sieciowego po stronie serwera, opóźnienia generowanego przez serwer aplikacyjny;
   3) szczegółowa lista wszystkich użytkowników wykorzysujących daną aplikację w sieci z podaniem urządzenia końcowego, który wykorzystuje daną aplikację;

9. Monitoring i zarządzanie siecią bezprzewodową:
   1) Wizualizacja graficzna rozmieszczenia poszczególnych radiowych punktów dostępowych oraz klientów sieci bezprzewodowej na mapie budynku:
      a) graficzne planowanie i zarządzanie siecią bezprzewodową (hierarchiczne mapy lokalizacji, mapy zasięgu) z wykorzystaniem własnych planów budynków;
      b) tworzenie i wyświetlanie dwuwymiarowych (2D) oraz trójwymiarowych (3D) map teoretycznego zasięgu sieci bezprzewodowej dla częstotliwości dostępnych w monitorowanej sieci bezprzewodowej, wizualizacja dla RSSI, SNR oraz interferencji;
      c) narzędzie do wizualizacji zmiany teoretycznego zasięgu sieci bezprzewodowej (planowanie) przy dołożeniu dodatkowych (wirtualnych) punktów dostępowych na mapie;
      d) narzędzie do weryfikacji rozmieszczenia punktów dostępowych pod względem zadanych wartości SLA: oczekiwana wartość RSSI, SNR na zadanej wysokości dla częstotliwości 2,4;5;6 GHz, pokazujące w jakim stopniu aktualne rozmieszczenie spełnia te kryteria SLA oraz narzędzie optymalizujące to rozmieszczenie przez dołożenie lub przesunięcie punktów dostępowych
      e) monitorowanie informacji takich jak: poziom szumu, poziom sygnału, interferencje sygnału pochodzących z punktów dostępowych;
      f) narzędzie pozwalające określić gotowość sieci bezprzewodowej na standard WiFi6 oraz WiFi6E dostarczające następujących informacji:
         - Ilość klientów (urządzeń mobilnych/użytkowników) wspierających standard: 11abg, 11n, 11ac, WiFi6, WiFi6E wraz z wizualizacją trendu zmiany tej wartości na przestrzeni czasu oraz możliwością wyświetlenia informacji o indywidualnych klientach w danej grupie;
         - Ilość punktów dostępowych obsługujących standard: WiFi6E, WiFi6 starszy oraz tych które mają standard WiFi6E włączony wraz możliwością wyświetlenia informacji o indywidualnych punktach dostępowych w danej grupie;
         - Średnie opóźnienie (ms) wprowadzane przez klientów pracujących w standardach WiFi6E, WiFi6, starszych w określonych kategoriach ruchu: Voice, Video, Best Effort oraz Background wraz z wizualizacją trendu zmiany tej wartości na przestrzeni czasu oraz możliwością wyświetlenia informacji o indywidualnych klientach w danej grupie;
         - Efektywność wykorzystania pasma radiowego (MB/s) przez klientów pracujących w standardach WiFi6E, WiFi6, starszych w określonych kategoriach ruchu: Voice, Video, Best Effort oraz Background wraz z wizualizacją trendu zmiany tej wartości na przestrzeni czasu oraz możliwością wyświetlenia informacji o indywidualnych klientach w danej grupie;
      g) współpraca z systemami lokalizacji urządzeń radiowych (punktów dostępowych, klientów, tagów) z prezentacją graficzną na mapie;
   2) monitoring usług sieciowych takich jak: usługi uwierzytelniania i kontroli dostępu (AAA), DHCP, DNS w zakresie:
      a) ilość udanych i nieudanych transakcji;
      b) średnie opóźnienie;

c) lista lokalizacji o największym opóźnieniu oraz największej ilości nieudanych transakcji łącznie lub per serwer;

3) narzędzie pozwalające na zbieranie od wybranych urządzeń bezprzewodowych Apple, Samsung, Intel informacji o:
   a) typie urządzenia i wersji oprogramowania;
   b) parametrach pracy sieci bezprzewodowej z perspektywy urządzenia (słyszane punkty bezprzewodowe oraz ich parametry pracy);
   c) przyczynie ostatniego rozłączenia/przełączenia z siecią bezprzewodową;
4) narzędzie pozwalające na monitoring i zarządzanie zagrożeniami w sieci bezprzewodowej uwzględniające wrogie punkty dostępowe (Rogue AP) oraz ataki identyfikowane przez sygnatury Wireless IPS/IDS:
   a) wyświetlanie zdarzeń bezpieczeństwa w zadanym oknie czasowym: ostatnich 3 godzin, 24 godzin lub 7 dni do 14 dni wstecz;
   b) wyświetlanie szczegółowej listy indywidualnych zagrożeń wraz z informacją o ich: szkodliwości, typie, lokalizacji, czasie wykrycia oraz nazwie AP który je wykrył;
   c) konfiguracja profili WIPS, które pozwalają na: określenie typów obsługiwanych sygnatur, wartości progów liczbowych wyzwalających daną sygnaturę oraz czy ma zostać zebrany materiał dowodowy (plik pcap) z danego zdarzenia;
   d) konfiguracja reguł klasyfikacji wrogich punktów dostępowych (Rogue AP) w oparciu o: nazwę SSID, siłę sygnału RSSI (Received Signal Stength Indicator), to czy dane SSID jest szyfrowane czy nie, minimalną liczbę podłączonych urządzeń;
   e) generowanie raportów z informacjami o zdarzeniach bezpieczeństwa w formie pliku CSV lub JSON
5) narzędzie do tworzenia konfiguracji na kontrolerach i punktach dostępowych w zakresie:
   a) tworzenie sieci WLAN (SSID) typu: sieć oparta o 802.1X oraz sieć gościnna;
   b) tworzenie profili ustawień radiowych uwzględniających takie parametry jak: obsługiwane kanały radiowe, wspierane prędkości radiowe, parametry wykrywania dziur w pokryciu, itp.;
   c) tworzenie list kontroli dostępu;
   d) konfiguracja tunelowania ruchu w sieci bezprzewodowej;

10. <u>Wykrywanie problemów w sieci i zaawansowana analityka systemu:</u>
    1) narzędzie do śledzenia ścieżki sieciowej dla danego ruchu w sieci np. w relacji pomiędzy dwoma hostami wraz podaniem informacji o wszystkich węzłach na ścieżce, ich indeksie jakości pracy, topologii fizycznej i logicznej np. zaznaczenie tunelowania ruchu bezprzewodowego, dokładną informacją o interfejsach, przez który płynie ruch, z zaznaczeniem lokalizacji list ACL, które dokonują filtracji danego ruchu;
    2) analiza problemów w sieci:
       a) automatyczna analiza zdarzeń w sieci oraz identyfikacja i wyświetlanie na tej podstawie problemów w działaniu sieci na poziomie całej sieci lub poszczególnych monitorowanych obiektów np. problemy związane z danym urządzeniem, użytkownikiem lub aplikacją;
       b) automatyczna priorytetyzacja problemów;

c) dla danego problemu, podanie opisu problemu, dostarczenie informacji kontekstowej umożliwiającej identyfikację i rozwiązanie problemu, określenie lokalizacji, urządzeń oraz użytkowników dotkniętych problemem, propozycja sugerowanych działań umożliwiających rozwiązanie problemu wraz z możliwością dostępu do urządzeń sieciowych w celu natychmiastowego dostarczenia danych diagnostycznych;

3) analiza parametrów pracy punktów dostępowych w zakresie:
   a) zbieranie, per punkt dostępowy, danych takich jak: ilość podłączonych klientów, ilość zmian kanału radiowego, utylizacja kanału radiowego, RSSI klienta, SNR klienta, Data Rate (przepustowość), ilość nieudanych roamingów, poziom interferencji, poziom strat pakietów, ilość resetów modułu radiowego, ilość podłączeń klienckich;
   b) wyznaczanie dla danego obszaru geograficznego (lokalizacja, budynek, piętro) oraz przedziału czasu (określony miesiąc) oraz zakresu częstotliwości radiowych (2,4; 5; 6 GHz) dla zbieranych danych, wartości średniej miesięcznej oraz średniej dziennej oraz dla wybranych danych również wartości minimalnej oraz maksymalnej, z wizualizacją tych informacji w formie graficznej;
4) analiza pracy sieci bezprzewodowej pod kątem jej użytkowania:
   a) zbieranie danych takich jak: czas podłączenia się do sieci, czas otrzymania adresu IP z serwera DHCP, czas uwierzytelnienia, czas asocjacji do sieci bezprzewodowej;
   b) wyznaczanie dla danego obszaru geograficznego (lokalizacja, budynek, piętro) oraz przedziału czasu (do tygodnia wstecz) oraz danego SSID – oczekiwanego przedziału badanej wartości wraz ze wskazaniem momentów w czasie, gdy pojawiały się odstępstwa;
   c) wykorzystanie informacji o tych odstępstwach do generowania alarmów o problemach w sieci;
   d) wyświetlanie zbieranych danych per dany punkt dostępowy;
5) narzędzie do analizy ustawień parametrów radiowych sieci bezprzewodowej:
   a) analiza parametrów radiowych sieci bezprzewodowej, dla danego okresu czasu, takich jak:
      - ilość wprowadzonych przez kontroler zmian w ustawieniach pracy AP, takich jak: kanał pracy, szerokość kanału, moc nadawania;
      - ilość modułów radiowych obsługujących klientów oraz dedykowanych do monitorowania pasma radiowego;
      - jakość pracy modułów radiowych pod kątem wydajności ustawień radiowych (poziom niski, średni, dobry) per punkt dostępowy;
      - poziom interferencji międzykanałowych (poziom niski, średni, dobry) per punkt dostępowy;
   b) analiza zbieranych danych pod kątem możliwości optymalizacji pracy sieci radiowej oraz wyświetlanie rekomendacji konfiguracyjnych wraz z możliwością przeprowadzenia symulacji działania sieci po wprowadzeniu sugerowanych rekomendacji;
   c) symulacja umożliwia zobrazowanie poprawy analizowanych parametrów sieci bezprzewodowej;
6) analiza jakości pracy sieci per lokalizacja pod kątem skuteczności i jakości podłączania użytkowników do sieci:

a) monitoring takich parametrów jak: ilość podłączeń do sieci, czas podłączeń do sieci, prędkość podłączenia do sieci, ilość przełączeń użytkownika między radiowymi punktami dostępowymi (roaming), czas trwania roamingu, pokrycie użytkowników sygnałem bezprzewodowym;
b) graficzna reprezentacja wybranego parametru na wykresie czasowym;

11. Funkcjonalności systemowe oraz integracja z innymi systemami:
1) mechanizm automatycznej aktualizacji wersji systemu bezpośrednio z chmury producenta;
2) obsługa REST API;
3) interfejs graficzny GUI działający w przeglądarkach Mozilla Firefox oraz Google Chrome;
4) integracja z systemem uwierzytelniania w celu otrzymywania informacji o tym jaki użytkownik jest związany z jakim urządzeniem, szczegółowej informacji o przebiegu procesu uwierzytelniania do sieci; uwzględnienie tych danych w procesie wyznaczania indeksów jakości pracy użytkowników jak również w procesie diagnostyki problemów w sieci;
5) integracja z systemem do proaktywnego monitoringu sieci, usług i aplikacji, który wykorzystuje do tego celu agentów (kontener Dockerowy) instalowanych na przełącznikach i realizacja przez tych agentów syntetycznych testów:
6) zarządzanie instalacją, deinstalacją, aktualizacją agentów na przełącznikach umożliwiających taką funkcję
7) konfiguracja i weryfikacja parametrów pracy agentów (adresacja IP, ustawienia proxy, dedykowane zasoby przełącznika)
8) wyświetlanie informacji o przeprowadzonych testach bezpośrednio w oknie systemie zarządzania z informacjami o: nazwa agenta, typ testu, monitorowany obiekt, wyniki testu: straty pakietów, jitter, opóźnienie
9) integracja z systemem Microsoft Teams oraz Cisco Webex w zakresie monitorowania połączeń audio/wideo z wyświetlaniem informacji o:
a) dacie początku i końca połączenia, długości trwania oraz statusie
b) parametrach połączenia takich jak: straty pakietów, jitter, bitrate, niezależnie dla części audio, wideo oraz współdzielenia treści (sharing).

12. Funkcjonalności z zakresu zarządzania siecią SDN (funkcje kontrolera SDN):
1) zarządzanie i monitorowanie siecią kampusową SDN jako jednolitą siecią typu Network Fabric;
2) graficzny interfejs użytkownika umożliwiający tworzenie segmentacji i polityki bezpieczeństwa w sieci SDN jak również provisioning urządzeń sieciowych tworzących sieć typu Network Fabric;
3) funkcje centralnego kontrolera SDN umożliwiające centralne programowanie urządzeń oraz centralny monitoring i analizę strumieni telemetrycznych z sieci w celu wykrywania nieprawidłowości w jej działaniu;

4) centralne zarządzanie polityką bezpieczeństwa poprzez określenie relacji pomiędzy segmentami logicznymi w sieci SDN (grupami urządzeń, użytkowników lub aplikacji) z możliwością tworzenia kontraktów dla wymiany ruchu pomiędzy tymi grupami;
5) filtracja ruchu niezależna od adresaci IP w oparciu o rolę użytkownika lub urządzenia w sieci i zdefiniowane relacje;
6) zarządzanie pulami adresowymi używanymi w sieci SDN;
7) zarządzanie sposobem uwierzytelniania w sieci Network Fabric na poziomie globalnym oraz na poziomie każdego z portów urządzeń dostępowych niezależnie;
8) logiczny podział sieci na wiele sieci wirtualnych (VN);
9) logiczny podział użytkowników i urządzeń na grupy i określenie relacji pomiędzy nimi;
10) tworzenie podsieci IP rozciągniętej na dowolne porty dostępowe w ramach Network Fabric;
11) możliwość filtrowania ruchu pomiędzy urządzeniami pracującymi w jednej grupie logicznej i/lub podsieci IP jak również pomiędzy różnymi grupami logicznymi i/lub podsieciami IP bez konieczności stosowania ACL opartych o adresy IP;
12) automatyzacja procesu tworzenia Network Fabric (dodawanie urządzeń, przypisywanie im roli w sieci, określanie poziomów uwierzytelnienia użytkowników i urządzeń na brzegu sieci) bez konieczności używania linii komend (CLI);
13) automatyczne wykrywanie urządzeń sieciowych;
14) narzędzie do automatycznego wykrywania nowo podłączonych urządzeń sieciowych i ich podłączenia do sieci podkładowej (underlay) wraz z konfiguracją urządzeń;
15) jednolite i zunifikowane rozwiązanie dla sieci kampusowej przewodowej oraz bezprzewodowej tj. możliwość tworzenia Network Fabric obejmującej zarówno sieć przewodową jak i bezprzewodową;

13. Parametry techniczne :
1) system w formie wirtualnego appliance sieciowego działający pod obsługą hypervisora VMware ESXi umożliwiający uzyskanie następujących wartości skalowalności:
2) zarządzanie i monitorowanie 1000 urządzeń sieciowych (przełączniki / routery);
3) zarządzanie i monitorowanie do 4000 radiowych punktów dostępowych WiFi;
4) monitorowanie do 25 000 klientów sieci;

14. W zakresie monitoringu sieci:
1) zbieranie i zapamiętywanie do 30 dni wstecz danych telemetrycznych o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji z różnych źródeł danych: SNMP, Syslog, NetFlow;
2) analiza i korelacja danych telemetrycznych o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji na podstawie różnych źródeł danych: SNMP, Syslog, NetFlow;
3) wyznaczenie na postawie analizy danych telemetrycznych dla każdego z urządzeń sieciowych, grupy użytkowników, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji indeksu liczbowego określającego jakość pracy danego monitorowanego obiektu, monitorowanych obiektów;
4) wizualizacja topologii sieci z przedstawieniem następujących informacji:

a) połączenia sieciowe z podaniem przepustowości, ilości fizycznych linków tworzących dane połączenie oraz szczegółowymi informacjami o adresach IP oraz nazwach interfejsów na końcach linków;
b) status połączenia sieciowego z zaznaczeniem braku łączności;
c) indeks jakości pracy danego obiektu;
d) filtrowanie urządzeń w topologii wykorzystujących dany VRF, VLAN, protokół routingu, tag.
e) wyświetlanie graficzne frontu przełączników wraz z portami na topologii uwzględniające stan portu, tryb pracy portu oraz fizyczne połączenia między danym portem a portem na innym przełączniku.

5) wyznaczenie i wizualizacja indeksów jakości pracy dla grup urządzeń sieciowych wg.:
a) typów urządzeń: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, kontroler WLAN, radiowy punkt dostępowy - w przedziałach czasowych za ostatnie 7 dni, ostatnie 24h, ostatnie 3h, zadany przedział czasowy w okresie ostatnich 30 dni;
b) lokalizacji geograficznych.

6) wizualizacja na skali czasu zmiany wartości indeksów jakości pracy dla grup urządzeń sieciowych.
7) wyznaczenie i wizualizacja indeksów jakości pracy dla grup użytkowników z rozbiciem na użytkowników przewodowych oraz bezprzewodowych wraz z wizualizacją na skali czasu zmiany wartości indeksów jakości pracy dla grup użytkowników.
8) dla użytkowników przewodowych szczegółowa informacja o ilości użytkowników podłączonych do sieci oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci z podaniem typowych przyczyn braku podłączenia np.: problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej. Szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP.
9) dla użytkowników bezprzewodowych szczegółowa informacja o ilości użytkowników podłączonych do sieci z rozbiciem na grupę użytkowników o dobrej jakości i złej jakości pracy oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci bezprzewodowej z podaniem typowych przyczyn braku podłączenia np. problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej. Szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP.
10) generowanie automatycznych komunikatów o stwierdzonych nieprawidłowościach w pracy sieci w oparciu o skorelowane informacje zbierane przez system z urządzeń sieciowych wraz z sugestią przyczyny, sposobu rozwiązania problemu oraz dalszych krokach diagnostycznych dla poszczególnych urządzeń sieciowych.

**III. Inne warunki dotyczące zamówienia - podsumowanie:**

Wykonawca zobligowany jest do dostarczenia wsparcia i serwisu technicznego 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: **zamowienia@wegrow.sr.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.

**Zatwierdzam:**
***Kierownik Zamawiającego***

**Dyrektor**
**Sądu Rejonowego w Węgrowie**
**Joanna Żółkowska**
*/podpisano elektronicznie/*