

Fundusze Europejskie
dla MazowszaRzeczpospolita
PolskaDofinansowane przez
Unię Europejską**Mazowsze.**
serce Polski

Opis Przedmiotu Zamówienia na zakup licencji na kontroler sieci bezprzewodowej.

1. Kontroler sieci bezprzewodowej musi spełniać następujące parametry:

- Kontroler wirtualny uruchamialny jako wirtualna maszyna (VM) w środowisku Microsoft Hyper-V,
- Kontroler wirtualny musi potrafić współpracować z drugim kontrolerem wirtualnym aby stworzyć klaster wysokiej dostępności (HA) Active-Active. W ramach redundancji ma się odbywać pełna synchronizacja pomiędzy kontrolerami,
- Rozwiązanie musi być w pełni zgodne (pełna obsługa) urządzeń AP które posiada Zamawiający:
- 30 szt. Ruckus R510
- Wymagania dla licencji dla Access-Point'ów:
 - a) Rozwiązanie musi być dostarczone z pulą licencji obsługującą minimum 30 urządzeń Access-Point (AP)
 - b) Musi być możliwość przypisania licencji AP do danego kontrolera wirtualnego, oraz późniejszej zmiany za pomocą systemu licencji producenta lub poprzez otwarcie zgłoszenia serwisowego.
 - c) W przypadku gdy dwa kontrolery wirtualne tworzą klaster wysokiej dostępności (HA) licencje muszą się sumować dla wszystkich kontrolerów – tak aby nie trzeba było dwukrotnie kupować/alokować licencji dla zapewnienia redundancji.
- Pojedyncza instancja kontrolera musi obsługiwać minimum 100 urządzeń AP oraz minimum 5000 podłączonych jednocześnie klientów WiFi. Rozbudowa nie może wymagać zakupu dodatkowych licencji na maszyny wirtualne – rozbudowa ma być wykonana poprzez dokupienie licencji dla obsługi nowych urządzeń AP.
- Provisioning nowych urządzeń AP dodawanych do kontrolera:
 - a) Wymagane jest automatyczne wykrywanie nowych punktów dostępowych poprzez opcje protokołu DHCP lub odpowiednie wpisy w DNS w porozumieniu z parametrem domain-name skonfigurowanym na serwerze DHCP,
 - b) Wymagana jest możliwość konfiguracji jak kontroler ma się zachować dla nowego, dodanego urządzenia AP – automatyczne dodanie go do środowiska lub umiejscowienie go w grupie przeznaczonej do akceptacji przez Administratorów,
- Kontroler musi wspierać punkty dostępowe (AP) z radiami pracującymi w standardach IEEE 802.11a/b/g/n/ac Wave 1/ac Wave 2/ax/WiFi-7,
- Zarządzanie kontrolerem musi odbywać się poprzez Web GUI (HTTPS://) oraz wiersz poleceń – CLI (SSH),
- Kontroler musi obsługiwać nie mniej niż 500 skonfigurowanych SSID jednocześnie,
- Kontroler musi centralnie zarządzać oprogramowaniem (firmware) dołączonych urządzeń Access-Point - pozwalać na aktualizację oprogramowania urządzeń AP po aktualizacji oprogramowania kontrolera,
- Automatyczne równoważenie obciążenia pomiędzy wieloma punktami dostępowymi.
- Centralne zarządzanie siecią MESH stworzoną z punktów dostępowych w celu zwiększenia zasięgu pracy systemu,
- Funkcjonalność chroniąca sieci kratowe MESH przed nadmiernym ruchem broadcast generowanym przez znanych klientów, poprzez jego konwersję do typu unicast,

- Możliwość dobierania optymalnych kanałów transmisyjnych za pomocą mechanizmów statystycznych bez konieczności przerywania transmisji danych,
- Możliwość dobierania optymalnych kanałów transmisyjnych za pomocą skanowania pasma RF,
- Równoważenie obciążenia pomiędzy częstotliwością 2,4GHz a 5GHz - zachęcanie klientów do łączenia się na częstotliwości 5GHz w celu wykorzystania większej liczby kanałów dostępnych w tym paśmie,
- Możliwość konfiguracji izolacji klientów w warstwie 2 ISO/OSI – konfiguracja per SSID,
- Możliwość konfiguracji VLAN per SSID oraz dynamicznych VLAN w porozumieniu z rozwiązaniem klasy Radius / NAC 802.1x,
- Możliwość konfiguracji ograniczenia pasma (upstream oraz downstream) per SSID,
- Optymalizacja wydajności sieci przy podłączonych klientach WLAN obsługujących różną przepustowość (sterowanie czasem dostępu do access pointa w celu unikania spowalniania wszystkich klientów przez najwolniejsze jednostki),
- Praca w trybie rozproszonego przetwarzania ruchu w trybie gdzie ścieżka danych nie wymaga przechodzenia przez kontroler, czyli bez konieczności tunelowania ruchu z punktu dostępowego do kontrolera, a jednocześnie z zachowaniem wszystkich funkcjonalności systemu zarządzanego kontrolerem. Wymagana konfiguracja per SSID,
- Praca w trybie tunelowania klienckiego ruchu (per SSID) przez kontroler lub dedykowany Dataplane (osobna maszyna VM lub appliance). Rozwiązanie musi wspierać możliwość szyfrowania tunelowego ruchu dla wybranych SSID. Jeśli wymagana jest dodatkowa licencja dla Dataplane to należy ją zapewnić razem z licencją na kontroler,
- Obsługa funkcjonalności BYOD (Bring Your Own Device) – auto-provisioning oraz automatyczna konfiguracja klientów mobilnych, tj. automatyczne dostarczenie konfiguracji do urządzeń typu: smartfon, tablet, obsługa minimum 10000 użytkowników BYOD w ramach dostarczonej licencji. Obsługa systemów operacyjnych, nie mniej niż Apple iOS, Android, Microsoft Windows. Funkcja może być realizowana na zewnętrznym komponencie programowo-sprzętowym pochodzącym od tego samego producenta, co kontroler. Dopuszczalna realizacja poprzez protokoły klasy IEEE 802.1x lub inne rozwiązania typu unikatowe klucze PSK per klient w ramach jednego SSID,
- Wbudowany serwer DHCP,
- Lokalna baza klientów sieci WLAN, obsługująca nie mniej niż 2000 użytkowników,
- Możliwość integracji z Active Directory, LDAP, Radius oraz TACACS,
- Oprogramowanie działające na urządzeniach AP działające z kontrolerem musi wspierać możliwość pełnej pracy urządzeń AP przy utracie kontrolera lub braku połączenia do kontrolerów WiFi. Nie dopuszczalna jest sytuacja, gdzie urządzenia AP przestają asocjować nowych klientów, gdy kontrolery nie działają,
- Rozwiązanie musi wspierać dwa tryby komunikacji z serwerami Radius:
 - a) Proxy przez kontroler,
 - b) Bezpośrednia komunikacja z urządzeniami AP,
- Dedykowany interfejs do generowania tymczasowych kont dla gości oraz wsparcie dla funkcji Captive Portal,
- Wbudowany analizator spektrum radiowego,
- Monitorowanie na bieżąco kanałów radiowych, na których aktualnie nie pracują AP w celu czasowego pominięcia ich jako potencjalnych kanałów, na których AP mogą pracować w przyszłości, gdyby zaszła konieczność zmiany obecnie wykorzystywanego kanału. Mechanizm powinien sprawdzać dostępne, aktualnie nie wykorzystywane kanały, pod kątem

ewentualnego wykrycia aktywności radiowej mogącej powodować konieczność czasowego opuszczenia tego kanału przez AP i klientów (tzw. DFS pre-scanning),

- Wsparcie mechanizmu 802.11r Fast BSS Transition,
- Możliwość wyłączenia diod sygnalizacyjnych LED na wybranych urządzeniach AP,
- Definiowanie parametrów sieciowych jak typ portu (access, trunk) przenoszone VLAN id oraz dynamiczne przypisywanie VLAN dla portów fizycznych AP,
- Funkcjonalność diagnostyki problemów w oparciu o poniższe kategorie z możliwością zawężenia procesu do wskazanego MAC AP lub klienta oraz eksportu wyniku działania w postaci pliku poprzez WebUI:
 - a) 802.11
 - b) 802.1x
 - c) Radius
 - d) Proces asocjacji/podłączania klientów do sieci WLAN
 - e) Środowisko RF
 - f) Zarządzanie
- System ochrony (WIDS) sieci WLAN:
 - a) Wykrywanie obcych punktów dostępowych oraz przedstawienie ich w systemie,
 - b) Ochrona przed atakami DoS,
 - c) Ochrona przed próbami nieautoryzowanego dostępu przez zgadywanie haseł (password guessing),
 - d) Limitowanie pasma (rate limiting),
 - e) Jeśli system WIDS wymaga licencji – należy je dostarczyć dla wszystkich AP,
- Obsługa następujących protokołów / standardów:
 - a) WEP, WPA-TKIP, WPA2-AES, WPA3, 802.11i,
 - b) 802.1x,
 - c) 802.1q,
 - d) 802.11e, VoIP Tunneling,
 - e) SNMP v2/v3,
 - f) IPv4 i IPv6,
 - g) 802.11u i HotSpot 2.0 lub PassPoint.
- Licencje na instancje kontrolera wirtualnego oraz obsługę Access-Point muszą być licencjami dożywotnimi, nie dopuszczalne są tutaj subskrypcje,
- Funkcjonalność importu planów obiektu, nanoszenia punktów dostępowych wraz z podglądem ich statusu, wydajności, parametrów zdrowotnych oraz wyświetlenia map przybliżonej siły sygnału (heatmap),
- Możliwość wzbudzania powiadomień w interfejsie kontrolera dla wybranych grup punktów dostępowych na podstawie poniższych kryteriów z możliwością określenia ich progów:
 - a) Opóźnienia dla pasma 2.4GHz i 5GHz.
 - b) Wysycenia pasma radiowego dla 2.4GHz i 5GHz.
 - c) Ilości podłączonych klientów.
- Funkcjonalność wskazania niepowodzeń w podłączeniu się klientów do sieci w podziale na:
 - a) Niepowodzenia na etapie 802.11 open system authentication.
 - b) Niepowodzenia na etapie 802.11 association.
 - c) Niepowodzenia związanych z EAP i RADIUS.
 - d) Niepowodzenia przydzielenia adresów ip z DHCP.
- Funkcjonalność wskazania parametrów wydajnościowych sieci w ujęciu min/max i średniej z podziałem na:

- a) Opóźnienia w dostarczaniu ramek do klientów bezprzewodowych.
- b) Wyczerpanie pasma radiowego.
- c) Potencjalnej pojemności sieci w danej jednostce czasu.
- System musi być objęty gwarancją i pełnym wsparciem producenta na okres 60 miesięcy,
- W ramach wdrożenia należy zapewnić usługę migracji z obecnego kontrolera ZoneDirector ZD1200 posiadanego przez Zamawiającego.