

Załącznik nr 3 do zapytania ofertowego

Popielów, 29.10.2024 r.

Opis przedmiotu zamówienia

Przedmiot zamówienia obejmuje dostawę nowego urządzenia FortiAP 231G lub „równoważnego” oraz wymianę posiadanego urządzenia FortiGate 61E na nowe FortiGate 90G z licencją i wsparciem serwisowym na 2 lata, pakietem wsparcia HEZO Assistance AHR 24x7xNBD 2 Years oraz przeniesieniem obecnej konfiguracji na nowe urządzenie łącznie z posiadanymi 10 tokenami dla połączeń VPN lub urządzenie „równoważne”, zgodnie z poniższymi wymaganiami. Zamawiający dopuszcza, przedłużenie licencji dla obecnego urządzenia FortiGate 61E do planowanego terminu wymiany, jednak nie dłużej niż na 1 miesiąc.

I. Wymagania dla urządzenia UTM¹

System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi zapewnić pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System musi umożliwić budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.

System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewnić funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwić agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

¹ Wszystkie wymagania dotyczą urządzenia FortiGate 90G lub „równoważnego”

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:
 - 8 portami Gigabit Ethernet RJ-45.
 - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall powinien pozwolić skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. Urządzenie musi być wyposażone w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 124 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6,5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4,4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2,1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.3 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekami poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

13. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wystanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall musi umożliwić filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.
 - Kubernetes.

Połączenia VPN

1. System musi umożliwić konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewnić:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwić konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnić:
- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie musi zapewnić obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System musi umożliwić wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall musi umożliwić zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System musi umożliwić określanie pasma dla poszczególnych aplikacji.
3. System musi pozwolić zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System musi zapewnić możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwić skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 21).

2. Silnik antywirusowy musi zapewnić skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System musi umożliwić skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System musi umożliwić blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System musi zapewnić usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Musi posiadać możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Musi posiadać możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewnić wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. System musi zapewnić mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. System musi mieć możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Musi umożliwić wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. System musi mieć możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji musi umożliwić kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
6. Musi istnieć możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System musi dać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorie stron zabronionych prawem np.: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW musi umożliwić statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwolić definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW musi dać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System musi pozwolić określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwić weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System musi dać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System musi umożliwić budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwić przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System musi dać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall musi umożliwić wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Musi być możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Musi być możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze lub przez zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall musi zapewnić przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnić możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Umożliwić włączenie logowania per reguła w polityce firewall.
5. System powinien zapewnić możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów musi być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent musi zapewnić dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania na poziomie specjalista.

Urządzenie musi być objęte rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wymagania powinny być potwierdzone dokumentami:

- Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

II. Wymagania dla urządzenia dostępowego Access Point²

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. Zaproponowane urządzenie musi być wyposażone w oryginalny zasilacz oraz wszystkie niezbędne przewody umożliwiające pracę po podłączeniu do instalacji elektrycznej 230V.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w temperaturze 0–50°C,
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
 - a. 2.4 GHz 802.11b/g/n,
 - b. 5 GHz 802.11a/n/ac/ax,

² Wszystkie wymagania dotyczą urządzenia FortiAP 231G lub „równoważnego”

- c. 2.4/5/6 GHz 802.11a/b/g/n/ac/ax
- 4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
- 5. Urządzenie musi być wyposażone w moduł BLE.
- 6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet: 10/100/1000 Base-TX oraz 100/1000/2500 Base-TX,
- 7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
- 8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - a. Tunnel,
 - b. Bridge,
 - c. Mesh.
- 9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
- 10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
- 11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
 - a. MIMO – 2x2,
 - b. Maksymalna przepustowość dla poszczególnych modułów radiowych:
 - i. 574 Mbps;
 - ii. 1201 Mbps;
 - iii. 2401 Mbps;
 - c. Wymagana moc nadawania:
 - i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - ii. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - iii. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - d. Wsparcie dla 802.11n 20/40Mhz HT,
 - e. Wsparcie dla kanałów 80 i 160MHz,
 - f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz.
 - g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
- 12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512;
- 13. Funkcje dodatkowe:
 - a. OFDMA UL i DL
 - b. Spatial Reuse (BSS Coloring)
 - c. UL-MU-MIMO
 - d. DL-MU-MIMO
 - e. Enhanced Target Wake Time (TWT)
 - f. Wbudowany analizator widma
 - g. Wbudowane mechanizmy WIPS/WIDS

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną licencję i wsparcie techniczne przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.