1. Bezprzewodowe punkty dostępowe 22szt

Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac/ax, 2.4GHz b/g/n/ax, 6GHz ax (musi być możliwe wybranie pasma dla każdego interfejsu radiowego – czyli praca w trybach: 2,4GHz i 5GHz; 5GHz i 6GHz; 2,4GHz i 6GHz)

1. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej

2. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj bez nadzoru centralnego kontrolera:

a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https

b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki

c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.

3. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:

a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako kontroler a pozostałych punktów dostępowych w klastrze kontrolerów zapasowych

b. W przypadku awarii punktu dostępowego pełniącego rolę głównego kontrolera, kolejny punkt dostępowy musi przejąć jego rolę w sposób automatyczny, przełączanie takie występuje aż do momentu awarii ostatniego punkt dostępowego pracującego w kastrze

c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe

d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję

e. Tworzenie klastra złożonego z co najmniej 120 urządzeń

4. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP

5. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa

6. W system musi być wbudowany serwer DHCP

7. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów

8. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:

a. EAP-TLS

b. PEAP-MSCHAPv2

c. PEAP-GTC

d. TTLS-MSCHAPv2

9. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP

10. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID dla częstotliwości 2.4 i 5 GHz, nie mniej niż 4 niezależne SSID dla częstotliwości 6GHz oraz do 512 urządzeń klienckich per radio

11. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN

12. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:

a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania

b. Zewnętrzny portal WWW

13. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT

14. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne

15. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:

a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe

b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu

c. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma

d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału

e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz

f. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g)

g. Wsparcie dla 802.11d oraz 802.11h

h. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane

16. Minimalizacja interferencji związanych z sieciami 3G/4G LTE

17. Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrz budynkowej oraz jako dostęp do konsoli urządzenia

18. Obsługa roamingu klientów w warstwie 2

19. Obsługa monitoringu przez SNMP

20. Obsługa logowania na zewnętrznym serwerze SYSLOG

21. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci

22. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:

a. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością

b. Wykorzystanie pasma

c. Ilość klientów korzystających z systemu/interferujących

d. Ilość ramek wejściowych/wyjściowych dla każdego radia

e. Ilość odrzuconych/błędnych ramek/s dla każdego radia

f. Szum tła dla każdego radia

g. Wyświetlanie logów systemowych

23. Punkt dostępowy musi wbudowane anteny dookólne do pracy w trybie 2x2: MU-MIMO. Uzyska anten nie powinien być mniejszy niż

a. 2,7 dBi dla 2,4 GHz

b. 4,4 dBi dla 5 Ghz

c. 4,4 dBi dla 6 Ghz

24. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2, 802.11ax

25. Praca w trybie MIMO 2X2:2

26. Specyfikacja wspieranych standardów:

a. 802.11b: DSSS

b. 802.11a/g/n/ac: OFDM

c. 802.11ax: OFDMA z 8 Resource units

27. Specyfikacja wpieranych modulacji:

a. 802.11b: BPSK, QPSK, CCK

b. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

c. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM

d. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

28. Specyfikacja wspieranych szerokości kanałów pracy:

a. 802.11n high-throughput (HT) wspiera MT20/40

b. 802.11ac very high-throughput (VHT) wspiera VHT20/40/80

c. 802.11ax high efficiency (HE) wspiera HE20/40/80/160

29. Obsługiwane częstotliwości:

- 2.400 ~ 2.4835 GHz (ISM)

- 5.150 ~ 5.250 GHz (low band)

- 5.250 ~ 5.350 GHz (mid band)

- 5.470 ~ 5.725 GHz (Europa)

- 5.725 ~ 5.850 GHz (high band)

- 5.925 ~ 6.425 GHz (U-NII-6)

- 6.525 ~ 6.875 GHz (U-NII-7)

- 6.875 ~ 7.125 GHz (U-NII-8)

30. Wspierane prędkości przesyłania danych (Mbps)

a. 802.11b: 1,2,5.5,11

b. 802.11a/g 6,9,12,18,24,36,48,54

c. 802.11n: od 6.5 do 300 (MCS0 do MCS15, HT20 do HT40) 400 z 256-QAM

d. 802.11ac: od 6.5 do 867 (MCS0 do MCS9, NSS= 1 do 2, HE20 do HE40)

e. 802.11ax (2,4 GHz) od 3.6 do 574 (MCS0 do MCS11, NSS=1 do 2, HE20 do HE40)

f. 802.11ax (5GHz) 3.6 do 1201 (MCS0 do MCS11, NSS = 1 do 2, HE20 do HE80)

g. 802.11ax (6GHz) 3.6 do 2402 (MCS0 do MCS11, NSS = 1 do 2, HE20 do HE160)

31. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm

a. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz

b. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac

c. Wsparcie dla:

• MRC (Maximal ratio combining)

• CDD/CSD (Cyclic delay/shift diversity)

• STBC (Space-time block coding)

• LDPC (Low-density parity check)

• Technologia TxBF

• TWT (Target Wait Time)

32. Punkt dostępowy musi posiadać co najmniej

a. 1 interfejs 100/1000/2500 Base-T

• z funkcją PoE 802.3at/bt

• zgodny ze standardem 802.3az Energy Effcient Ethernet EEE

b. 1 interfejs konsoli szeregowej (micro USB)

c. Zasilanie PoE zgodne z 802.3at/802.3.bt

• maksymalny pobór mocy 21W PoE

d. przycisk przywracający konfigurację fabryczną

e. Kontrolka LED do określania statusu systemu i interfejsów radiowych

f. slot zabezpieczający Keningston

g. Zigbee (802.15.4)

h. Bluetooth 5.0 Low Energy (BLE5.0)

i. USB 2.0 (host) (Type A)

j. Port zasilania DC 12VDC

33. Parametry pracy urządzenia:

a. Temperatura otoczenia: 0°C- +50°C

b. Wilgotność 5% - 95% nie skondensowana

c. Znak CE

d. EN 300 019

34. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac wave 2/ ax

35. Wszystkie dostępne na urządzeniu funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji, o ile nie wyspecyfikowano inaczej.

36. Producent sprzętu musi być sklasyfikowany co najmniej 5 ostatnich (w tym bieżącym) w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” lub równoważnym i znajdować się w kwadracie liderów (Leaders). Za ranking równoważny Zamawiający uzna ranking klasyfikujący rozwiązania klasy enterprise przewodowych i bezprzewodowych sieci LAN, prowadzony i publikowany przez podmiot niezależny od producentów tych rozwiązań. Zamawiający wymaga, aby ranking taki był aktualizowany w okresach nie dłuższych niż 1 rok i publikowany był od co najmniej 10 lat. Podstawą do sporządzenia raportów muszą być badania polegające na sprawdzeniu jakości oferowanych usług i rozwiązań. Ocena jest prowadzona według kryteriów dotyczących kompletności wizji oferowanych usług, rozwiązań oraz prognoz na przyszłość w tym segmencie rynku oraz zdolności ich realizacji do wdrożenia, są to możliwości finansowe, biznesowe i organizacyjne. Wynik oceny wyznacza miejsce w rankingu, w którym znajduje się konkretny dostawca i jego rozwiązanie. Ranking musi uwzględniać co najmniej 4 kategorie, każda z nich ma określać jaką rolę na rynku spełnia dane rozwiązanie/dostawca. Liderzy – najwyższa kategoria, gdzie znajdują się liderzy/producenci danego rozwiązania. Kandydaci – pretendenci pozostający bardzo wysoko w rankingu ze względu na swoje działania i potencjał do dominacji na rynku, w którym działa. Wizjonerzy - firmy rozwiązania posiadający wizję możliwości rynkowych, jednak poprzez realizowane działania nie są oni skuteczni na rynku. Niszowi gracze – rozwiązania skupiające się na niewielkiej części rynku lub nie mających możliwości innowacyjnych do osiągnięcia większych sukcesów rynkowych. Ranking równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy

37. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni

38. Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.

1. Kontroler nadrzędny sieci bezprzewodowej – klaster wysoko niezawodnościowy

1. Kontroler ma być dostępny w formie maszyny wirtualnej uruchamianej w środowisku VMware ESXi lub KVM hypervisor.

2. Kontroler musi zarządzać siecią bezprzewodową złożoną z minimum 50 punktów dostępowych i kontrolerów podrzędnych, w szczególności punktów dostępowych i kontrolerów opisanych w tym dokumencie

3. Kontroler musi umożliwiać stworzenie spójnej, centralnie zarządzanej i sterowanej struktury hierarchicznej złożonej co najmniej z 5 kontrolerów podrzędnych.

4. Kontroler musi mieć możliwość rozbudowy do co najmniej 1000 punktów dostępowych. Dopuszcza się rozbudowę poprzez dodanie odpowiednich licencji i zmianę parametrów maszyn wirtualnych.

5. Kontroler musi obsługiwać co najmniej 5000 użytkowników

6. Kontroler musi zapewniać redundancję, realizowaną poprzez dostarczenie licencji umożliwiającej instalację kilku maszyn wirtualnych w ramach pojedynczej licencji lub dostarczenie licencji na co najmniej dwa kontrolery lub dostarczenie licencji typu HA, pozwalającej na instalację dodatkowej maszyny wirtualnej.

7. Kontroler musi wspierać jako kontrolery podrzędne kontrolery opisane w tym dokumencie

8. Kontroler ma umożliwić konfigurację klastrów kontrolerów podrzędnych w celu zapewnienia wysokie dostępności oraz rozkładania obciążenia.

9. Kontroler musi zapewnić centralny punkt dystrybucji licencji dla kontrolerów podrzędnych.

10. Kontroler musi umożliwiać tworzenie centralnego planu rozłożenia kanałów sieci bezprzewodowej oraz mocy jej nadawania dla całej sieci bezprzewodowej uwzględniając wszystkie kontrolery podrzędne.

11. Kontroler musi umożliwiać aktualizacje w locie klastra kontrolerów podrzędnych bez przerywana pracy sieci bezprzewodowej.

12. Kontroler musi umożliwiać tworzenie odseparowanej sieci gościnnej poprzez podłączenie osobnego kontrolera w sieci DMZ i udostępnienie zasobów punktów dostępowych zarządzanych poprzez kontroler podrzędny. (terminowanie ruchy z AP na dwóch niezależnych kontrolerach).

13. Kontroler musi umożliwiać bezstratny roaming pomiędzy kontrolerami podrzędnymi.

14. Producent sprzętu musi być sklasyfikowany co najmniej 5 ostatnich (w tym bieżącym) w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” lub równoważnym i znajdować się w kwadracie liderów (Leaders). Za ranking równoważny Zamawiający uzna ranking klasyfikujący rozwiązania klasy enterprise przewodowych i bezprzewodowych sieci LAN, prowadzony i publikowany przez podmiot niezależny od producentów tych rozwiązań. Zamawiający wymaga, aby ranking taki był aktualizowany w okresach nie dłuższych niż 1 rok i publikowany był od co najmniej 10 lat. Podstawą do sporządzenia raportów muszą być badania polegające na sprawdzeniu jakości oferowanych usług i rozwiązań. Ocena jest prowadzona według kryteriów dotyczących kompletności wizji oferowanych usług, rozwiązań oraz prognoz na przyszłość w tym segmencie rynku oraz zdolności ich realizacji do wdrożenia, są to możliwości finansowe, biznesowe i organizacyjne. Wynik oceny wyznacza miejsce w rankingu, w którym znajduje się konkretny dostawca i jego rozwiązanie. Ranking musi uwzględniać co najmniej 4 kategorie, każda z nich ma określać jaką rolę na rynku spełnia dane rozwiązanie/dostawca. Liderzy – najwyższa kategoria, gdzie znajdują się liderzy/producenci danego rozwiązania. Kandydaci – pretendenci pozostający bardzo wysoko w rankingu ze względu na swoje działania i potencjał do dominacji na rynku, w którym działa. Wizjonerzy - firmy rozwiązania posiadający wizję możliwości rynkowych, jednak poprzez realizowane działania nie są oni skuteczni na rynku. Niszowi gracze – rozwiązania skupiające się na niewielkiej części rynku lub nie mających możliwości innowacyjnych do osiągnięcia większych sukcesów rynkowych. Ranking równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy

15. Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

16. Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji czasowych o ile nie wyspecyfikowano inaczej

1. Kontroler podrzędny sieci bezprzewodowej - klaster wysoko niezawodnościowy

1. Dwa, pracujące w klastrze HA kontrolery muszą w pełni obsługiwać punkty dostępowe, opisane w tym dokumencie

2. Kontrolery muszą zarządzać siecią bezprzewodową złożoną z co najmniej 22 punktów dostępowych z możliwością rozbudowy do co najmniej 1000 punktów dostępowych. Dopuszcza się rozbudowę poprzez dodanie odpowiednich licencji i zmianę parametrów maszyn wirtualnych. Wartości łączne, dla klastra kontrolerów pracujących w HA.

3. Kontrolery muszą posiadać możliwość obsługi łącznie co najmniej 1500 użytkowników

4. Każdy z wymaganych kontrolerów musi posiadać wyspecyfikowane w tym dokumencie funkcje:

a. Musi posiadać funkcje VPN Gateway

b. Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym.

c. Kontroler musi mieć możliwość pracy w klastrze w celu zapewnienia zwiększenia pojemności, zapewnienia nieprzerwanej pracy, balansowania obciążenia. Przełączanie użytkowników w obrębie klastra ma się odbywać niezauważalnie z poziomu klienta tzn. żadne sesje klienta nie mogą być przerwane. Dotyczy to przełączanie związanego tak z roamingiem jak i awarią kontrolera

d. Kontroler musi posiadać mechanizm automatyzacji doboru kanałów pracy, mocy nadawania. Mechanizm musi mieć możliwość wymiany informacji pomiędzy wszystkimi kontrolerami w sieci a centralnym punktem zarządzania.

e. Kontroler musi mieć możliwość przeprowadzenia Live update polegającego na aktualizacji klastra kontrolerów oraz punktów dostępowych bez przerwania obsługi urządzeń klienckich

f. Kontroler ma mieć możliwość współdzielenia zasobów punktów dostępowych innemu kontrolerowi. Główny kontroler zezwala na zarzadzanie danym wirtualnym punktem dostępowym innemu kontrolerowi, na którym ten ruch jest terminowany. Kontroler ten może samodzielnie konfigurować wszystkie polityki w ramach udostępnionego wirtualnego punktu dostępowego. Funkcjonalność ta umożliwia stworzenie bezpiecznej sieci ruchu obcego np. ruch gościnny lub IoT.

g. Kontroler musi mieć możliwość udostępniania informacji na temat stanu sieci poprzez API

h. Kontroler musi mieć możliwość uaktualniania poszczególnych modułów np. odpowiedzialnego na dynamiczny dobór kanałów, analizę aplikacji itp. bez konieczności uaktualniana całego systemu operacyjnego.

i. Kontroler musi mieć możliwość terminowania ruchu z przełączników tego samego producenta w celu ujednolicenia polityk bezpieczeństwa dla sieci przewodowej i bez przewodowej.

j. Wspieranie wieli wersji oprogramowania. Funkcja ta umożliwia administratorowi przetestowanie nowych funkcjonalności na wybranym obszarze sieci bez konieczności aktualizowania całego środowiska

k. Kontroler musi być wyposażony w technologię, która umożliwi optymalizację rozłożenia klientów pomiędzy dostępnymi punktami dostępowymi oraz pasmami (2,4 GHz oraz 5 GHz). Mechanizm musi zapewnić wykluczenie problemy tzw. Sticky clients.

l. Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall) (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie)

m. Kontroler musi być wyposażony w funkcjonalność umożliwiającą rozpoznawanie aplikacji. Liczba domyślnie rozpoznawanych aplikacji minimum 2000 (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie)

n. Kontroler musi wspierać protokoły wykorzystywane przez urządzenia Apple TV oraz Google chromcast

o. Kontroler musi wspierać mechanizmy ochrony sieci bezprzewodowej przed atakami hackerskimi. (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie)

p. Kontroler musi mieć możliwości jako koncentrator VPN i umożliwiać dostęp zdalny dla użytkowników dzięki wykorzystaniu darmowej aplikacji dla urządzeń mobilnych. (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie)

q. Kontroler musi mieć możliwość integracji z systemami centralnego zarządzania siecią przewodową i bezprzewodową

r. Kontroler musi mieć możliwość wprowadzenia klasyfikacji treści przeglądanych przez użytkowników stron www (np. przemoc, hazard itp.) oraz określenia ich reputacji. (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie, dostęp do bazy treści może być oferowany w formie subskrypcji, o ile dostępna jest ona na co najmniej 10 lat bez konieczności jej odnawiania)

s. Kontroler musi mieć możliwość automatycznej klasyfikacji i monitoringu jakości połączenia dla aplikacji komunikacyjnych (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie) takich jak:

i. Apple FaceTime

ii. Alcatel Lucent New Office Environment (NOE)

iii. Microsoft Lync/Skype for Business

iv. Cisco Jabber

v. Cisco Skinny Call Control Protocol (SCCP)

vi. Spectralink Voice Priority (SVP)

vii. SIP

viii. H.323

ix. Vocera

x. Cellular Wi-Fi Calling

5. Kontroler ma być dostępny w formie maszyny wirtualnej uruchamianej w środowisku VMware ESXi lub KVM hypervisor.

6. Kontroler musi wspierać poniższe formy uwierzytelniania:

a. IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP, EAP-GTC, EAP-TLV, EAP-AKA, EAP-Experimental, EAP-MD5)

b. RFC 2548 Microsoft vendor-specifc RADIUS attributes

c. RFC 2716 PPP EAP-TLS

d. RFC 2865 RADIUS authentication

e. RFC 3579 RADIUS support for EAP

f. RFC 3580 IEEE 802.1X RADIUS guidelines

g. RFC 3748 extensible authentication protocol

h. MAC address authentication

i. Web-based captive portal authentication

7. Kontroler musi wspierać poniższe serwery autoryzacji:

a. Internal database

b. LDAP/SSL secure LDAP

c. RADIUS

d. TACACS+

8. Kontroler musi wspierać następujące protokoły szyfrowania:

a. CCMP/AES

b. WEP 64- and 128-bit

c. TKIP

d. SSL and TLS:

i. RC4 128-bit

ii. RSA 1024-bit

iii. RSA 2048-bit

e. L2TP/IPsec (RFC 3193)

f. XAUTH/IPsec

g. PPTP (RFC 2637)

9. Kontroler musi wspierać Site-to-site VPN dla sposobów autentykacji X.509 PKI, IKEv2, IKE PSK, IKE aggressive mode.

10. Producent sprzętu musi być sklasyfikowany co najmniej 5 ostatnich (w tym bieżącym) w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” lub równoważnym i znajdować się w kwadracie liderów (Leaders). Za ranking równoważny Zamawiający uzna ranking klasyfikujący rozwiązania klasy enterprise przewodowych i bezprzewodowych sieci LAN, prowadzony i publikowany przez podmiot niezależny od producentów tych rozwiązań. Zamawiający wymaga, aby ranking taki był aktualizowany w okresach nie dłuższych niż 1 rok i publikowany był od co najmniej 10 lat. Podstawą do sporządzenia raportów muszą być badania polegające na sprawdzeniu jakości oferowanych usług i rozwiązań. Ocena jest prowadzona według kryteriów dotyczących kompletności wizji oferowanych usług, rozwiązań oraz prognoz na przyszłość w tym segmencie rynku oraz zdolności ich realizacji do wdrożenia, są to możliwości finansowe, biznesowe i organizacyjne. Wynik oceny wyznacza miejsce w rankingu, w którym znajduje się konkretny dostawca i jego rozwiązanie. Ranking musi uwzględniać co najmniej 4 kategorie, każda z nich ma określać jaką rolę na rynku spełnia dane rozwiązanie/dostawca. Liderzy – najwyższa kategoria, gdzie znajdują się liderzy/producenci danego rozwiązania. Kandydaci – pretendenci pozostający bardzo wysoko w rankingu ze względu na swoje działania i potencjał do dominacji na rynku, w którym działa. Wizjonerzy - firmy rozwiązania posiadający wizję możliwości rynkowych, jednak poprzez realizowane działania nie są oni skuteczni na rynku. Niszowi gracze – rozwiązania skupiające się na niewielkiej części rynku lub nie mających możliwości innowacyjnych do osiągnięcia większych sukcesów rynkowych. Ranking równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy

11. Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

12. Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji czasowych, o ile nie wyspecyfikowano inaczej.