POLITECHNIKA GDAŃSKA

Kanclerz

Gdańsk, 01.06.2020r.

dot. przetargu nieograniczonego na dostawę wraz z uruchomieniem i wdrożeniem zestawu do transmisji bezprzewodowej wifi na potrzeby Centrum Usług Informatycznych Politechniki Gdańskiej ZP/98/055/D/20

ODPOWIEDŹ NA ZAPYTANIA OD WYKONAWCÓW ORAZ ZMIANA SIWZ

Na podstawie art. 38 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych Zamawiający (t.j. Dz. U. z 2019 r., poz. 1843 z późn. zm.) Politechnika Gdańska udziela odpowiedzi na zapytania od Wykonawców dotyczące treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ) oraz dokonuje zmiany (SIWZ).

Pytanie 1.
Zamawiający pisze o w SIWZ i Załącznikach o 150 szt. AP i kolejnych 150 szt. AP jako opcja. Jednocześnie Zamawiający wymaga 2 000 licencji dostępowych dla AP(Zał. nr 3 do SIWZ, tabela poz. 5).
1A. Czy ilość 2 000 licencji dostępowych dla AP jest prawidłowa i z czego wynika skoro AP maksymalnie będzie 300 szt. ?
1B. Do czego Zamawiający planuje użyć dodatkowe 1 700 licencji dostępowych dla AP (z 2 000 lic), które będą dostarczone w aktualnym przetargu (Nr postępowania: ZP/98/055/D/20) ?

Odpowiedź nr 1:

Zamawiający wymaga 2000 licencji dostępowych dla użytkowników systemu UA.
Zamawiający dokonał zmian w SIWZ opublikowanym w dniu 28.05.2020, w którym uszczegółowił wymagania. Poprawiony został również odpowiednio formularz rzeczowo cenowy.

Pytanie 2
Prośba od Zamawianego o przekazanie planów, rzutów pomieszczeń, budynków, które mają być pokryte sygnałem i zasięgiem sieci WIFI o formie pliku .PDF, .dwg lub ostatecznie .jpeg.
2A. Czy Zamawiający wskaże miejsca, obiekty (pomieszczenia), obszary kampusu PG gdzie bezwzględnie musi być zasięg sieci WIFI , a gdzie może być jako np. opcja ?
2B. Czy Zamawiający udzieli wskazówek dla projektowania zasięgu, pokrycie sygnałem WIFI obiektów, pomieszczeń itp.
2C. Czy Zamawiający udzieli wskazówek dot. pomieszczeń nt rodzaju sufitu (np. tzw. podwieszany), rodzaju ścian (materiał z którego są wykonane), które mogą być pomocne przy projektowaniu zasięgu WIFI w budynkach , pomieszczeniach ?
2D. Czy zasięgiem mają być objęte także pomieszczenia toalet w budynkach ?

Odpowiedź nr 2:

Zamawiający na obecnym etapie postępowania nie przekaże planów budynków. Pogląd na skalę i zakres prac związanych z planowaniem rozmieszczenia AP Wykonawca może sobie wyrobić na podstawie dostępnych obecnie planów kampusu na stronie https://campus.pg.edu.pl/.
2A. Tak, na etapie wdrożenia.

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.edu.pl

2B. Tak, na etapie wdrożenia.
2C. Tak, jeśli będzie posiadał na ten temat wiedzę.
2D. Tak, jeśli będzie to możliwe ze względu na posiadaną przez Zamawiającego infrastrukturę.

Pytanie 3
3A. Czy Wykonawca ma dokonać fizycznej instalacji punktów dostępowych AP w budynkach, obszarach pokrycia sygnałem WIFI obiektów, terenu Zamawiającego ?
3B. Czy Zamawiający zapewni we własnym zakresie okablowanie Ethernet i zasilanie 230V do punktów instalacji AP ?
3C. Czy Zamawiający zapewni we własnym zakresie zasilanie PoE (w jakim dokładnie standardzie) dla instalowanych AP ?

Odpowiedź nr 3:

3A. Nie
3B. Tak. Zamawiający zapewni zasilanie 230V lub PoE+ (802.3at)
3C. patrz pkt. 3B

Pytanie 4.
Czy Zamawiający posiada aktualnie jakąś sieć WIFI w swoich obiektach lub ich części, a które (obiekty, pomieszczania)są przedmiotem obecnego postępowania przetargowego (i planowanego zasięgu WIFI) ?
4A. Jakiego producenta sprzęt AP i kontroler są użyte w tej sieci WIFI ?
4B. Kiedy został uruchomiona ?
4C. Której kategorii kable miedziane są używane przez obecny system sieci WIFI ?
4D. Czy na obiektach (kampus PG) są rozmieszczone punkty dystrybucyjne z okablowaniem światłowodowym, jeżeli tak to czy można prosić o przesłanie schematu sieci ?

Odpowiedź nr 4:

Tak, Zamawiający posiada aktualnie sieć WIFI w swoich obiektach lub ich częściach.
4A. Meru/Fortinet
4B. Sieć funkcjonuje od ok. 10 lat.
4C. 5e/6A
4D. Na obiektach kampusu PG są rozmieszczone również punkty dystrybucyjne z okablowaniem światłowodowym. Zamawiający nie udostępni schematu sieci, gdyż nie ma to związku z postępowaniem – prace związane z okablowaniem leżą po stronie Zamawiającego.

Pytanie 5
Czy Zamawiający może podać listę obiektów, pomieszczeń, obszarów, które mają zostać pokryte sygnałem WIFI ?
5A. Czy Zamawiający może jednocześnie wskazać jak dokładne ma być to pokrycie sygnałem WIFI w zależności od miejsca?

Odpowiedź nr 5:

Tak, na etapie wdrożenia.
5A. Tak, na etapie wdrożenia

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

Pytanie 6
Czy aktualne postępowanie przetargowe na „dostawę wraz z uruchomieniem i wdrożeniem zestawu do transmisji bezprzewodowej wifi na potrzeby Centrum Usług Informatycznych Politechniki Gdańskie", ma zastąpić obecną sieć EDUROAM czy może ją uzupełnić, albo rozszerzyć ?

Odpowiedź nr 6:

Przedmiotem postępowania jest system wifi, który sukcesywnie, w miarę jego rozbudowy, będzie zastępował użytkowane aktualnie rozwiązanie, które udostępnia sieć EDUROAM.

Pytanie 7
Czy Zamawiający planuje zainstalować nowe AP (z obecnego przetargu) w miejsce obecnych ? Dzięki temu okablowanie i zasilanie byłoby już przygotowane (wymiany AP w miejscu instalacji).

Odpowiedź nr 7:

Część AP zostanie zapewne zainstalowane w miejscach aktualnie używanych przez dotychczasowe AP. Jeśli jednak z pomiarów wyniknie, iż ze względu na zapewnienie zasięgu należy dołożyć nowe punkty dostępowe Zamawiający zainstaluje AP w nowych lokalizacjach.

Pytanie 8
Czy Zamawiający sam we własnym zakresie wykona instalację i zasilanie punktów dostępowych AP w oparciu o wykonaną mapę zasięgu i rozmieszczenia AP (Wykonawca) na terenie kampusu PG ?

Odpowiedź nr 8:

Tak.

Pytanie 9
Czy Zamawiający sam we własnym zakresie wybierze miejsca (na podstawie wykonanej mapy zasięgu i rozmieszczenia AP przez Wykonawcę) i sam wykona instalację i zasilanie punktów dostępowych AP ?

Odpowiedź nr 9:

Tak.

Pytanie 10
W pkt II zamawiający opisuje minimalne wymagania dotyczące kontrolera sieci bezprzewodowej. Czy Zamawiający dopuszcza zaoferowanie jako kontroler sieci bezprzewodowej serwera wraz z oprogramowaniem do wirtualizacji oraz dedykowanym oprogramowaniem pełniącym funkcjonalności kontrolera sieci bezprzewodowej (tzw. wirtualny kontroler)?

Odpowiedź nr 10:

Zamawiający dokonał zmian w SIWZ opublikowanym w dniu 28.05.2020, w którym uszczegółowił wymagania.

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

Pytanie 11
W pkt IV.12 „Analiza stacji końcowej (Posture Assessment)" zamawiający opisuje funkcjonalność serwera UA dotyczącą głębokiej analizy stacji końcowej. W pkt. IV.8.3 w którym mowa o funkcjonalnościach, które musi zapewnić serwer UA wyszczególnione zostało tylko uwierzytelnienie 802.1X oraz profilowanie. Czy należy przyjąć, że oferta powinna zawierać odpowiednie licencje nie tylko na uwierzytelnianie 802.1X oraz profilowanie, a także na funkcjonalność analizy stacji końcowej (posture assessment) dla 2000 urządzeń?

Odpowiedź nr 11:

Tak, licencja powinna zawierać odpowiednie licencje na funkcjonalność analizy stacji końcowej (posture assessment) dla 2000 urządzeń.

Pytanie 12
W pkt II.1.42.2 oraz IV.7.2 („zachowaj dysk") Zamawiający wymaga od producenta realizacji gwarancji w taki sposób, że w przypadku uszkodzenia urządzenia, dysk twardy pozostanie u Zamawiającego. Czy Zamawiający wyraża zgodę aby obowiązek wynikający z pkt II.1.4.2 oraz IV.7.2 był realizowany przez Wykonawcę, a nie bezpośrednio przez producenta?

Odpowiedź nr 12:

Tak.

Pytanie 13
Nawiązując do pkt III, czy należy przyjąć, że Zamawiający w ramach postępowania wymaga dostarczenia wyłącznie licencji uprawniającej do zainstalowania Systemu w formie maszyny wirtualnej? Oznacza to, że oferent nie ma obowiązku dostarczenia serwera sprzętowego oraz oprogramowania do wirtualizacji, gdzie zostanie zainstalowania maszyna wirtualna z opisanym systemem. Prosimy o potwierdzenie.

Odpowiedź nr 13:

Tak. Zamawiający dokonał zmian w SIWZ opublikowanym w dniu 28.05.2020, w którym uszczegółowił wymagania.

Pytanie 14
Nawiązując do pkt III.2.22, czy należy przyjąć, że Zamawiający w ramach postępowania wymaga dostarczenia licencji uprawniającej do zainstalowania systemu jednocześnie na dwóch maszynach wirtualnych z możliwością skonfigurowania trybu wysokiej dostępności (tzw. HA w trybie Active-Standby)?

Odpowiedź nr 14:

Nie, nie wymagana jest taka licencja. Zamawiający dokonał zmian w SIWZ opublikowanym w dniu 28.05.2020, w którym uszczegółowił wymagania.

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

Pytanie 15
Dotyczy załącznika nr 6 do SIWZ:

Czy zamawiający dopuszcza całościowo alternatywne rozwiązanie o poniższych parametrach:

I. Punkt dostępowy – 150 szt. w zamówieniu podstawowym plus 150 szt. w opcji

1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2/ax, oraz 2.4GHz b/g/n/ax.
2. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej, w szczególności z kontrolerem opisanym w punkcie II.
3. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:
   3.1. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https
   3.2. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki
   3.3. 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.
4. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:
   4.1. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego
   4.2. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny
   4.3. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe
   4.4. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję
   4.5. Tworzenie klastra do 130 urządzeń
5. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP
6. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa
7. W system musi być wbudowany serwer DHCP
8. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów
9. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
   9.1. EAP-TLS
   9.2. PEAP-MSCHAPv2
   9.3. PEAP-GTC
   9.4. TTLS-MSCHAPv2
10. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP
11. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID
12. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN
13. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
    13.1. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania
    13.2. Zewnętrzny portal WWW

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

14. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT
15. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne
16. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
    16.1. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe
    16.2. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu
    16.3. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma
    16.4. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
    16.5. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz
    16.6. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g)
    16.7. Wsparcie dla 802.11d oraz 802.11h
    16.8. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane
17. Minimalizacja interferencji związanych z sieciami 3G/4G LTE
18. Punkt dostępowy musi mieć wbudowany moduł Bluetooth Low Energy (BLE5.0) (co najmniej 7dBm) wykorzystywany w systemie nawigacji wewnątrzbudynkowej
19. Punkt dostępowy musi mieć wbudowany moduł Zigbee (802.15.4) (co najmniej 7dBm)
20. Obsługa roamingu klientów w warstwie 2
21. Obsługa monitoringu przez SNMP
22. Obsługa logowania na zewnętrznym serwerze SYSLOG
23. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
24. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
25. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
    25.1. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością
    25.2. Wykorzystanie pasma
    25.3. Ilość klientów korzystających z systemu/interferujących
    25.4. Ilość ramek wejściowych/wyjściowych dla każdego radia
    25.5. Ilość odrzuconych/błędnych ramek/s dla każdego radia
    25.6. Szum tła dla każdego radia
    25.7. Wyświetlanie logów systemowych
26. Punkt dostępowy musi posiadać 4 wbudowane anteny pracujące w trybie 4x4 MIMO, z parametrami co najmniej: 4 dBi dla 2,4GHz, 7.5 dBi dla 5 GHz
27. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave, 802.11ac 2 Wave, 802.11ax
28. Praca w trybie SU MIMO 4X4:4 dla 5GHz
29. Specyfikacja radia 802.11a/n/ac/ax:
    29.1. Obsługiwana technologia OFDM oraz OFDMA
    29.2. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
    29.3. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm
    29.4. Prędkości transmisji:
        29.4.1. 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a,
        29.4.2. MCS0-MCS23 (6,5Mbps do 450Mbps) dla 802.11n
        29.4.3. MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11ac

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

29.4.4. MCS0 do MCS11, NSS = 1-2 (3.6 Mbps do 574 Mbps) dla 802.11ax (2,4GHz)
29.4.5. MCS0 do MCS11, NSS = 1-4 (3.6 Mbps do 4803 Mbps) dla 802.11ax (5GHz)
29.5. Obsługa HT – kanały 20/40MHz dla 802.11n
29.6. Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac
29.7. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax
29.8. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz
29.9. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac
29.10. Wsparcie dla:
29.10.1. MRC (Maximal ratio combining)
29.10.2. CDD/CSD (Cyclic delay/shift diversity)
29.10.3. STBC (Space-time block coding)
29.10.4. LDPC (Low-density parity check)
29.10.5. Technologia TxBF
30. Specyfikacja radia 802.11b/g/n/ax:
30.1. Częstotliwość 2,400 ~2,4835
30.2. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA
30.3. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256-QAM, 1024-QAM
30.4. Moc transmisji konfigurowalna przez administratora
31. Punkt dostępowy musi posiadać co najmniej:
31.1. 1 interfejs 100/1000 BaseT
31.1.1. z funkcją auto-sensing link oraz MDI/MDX
31.1.2. obsługa równoważenie obciążenia „load balancing"
31.2. 1 interfejs 100/1000/2.5G BaseT (zgodny z 802.3bz)
31.2.1. z funkcją auto-sensing link oraz MDI/MDX
31.2.2. z funkcją PoE/PoE+
31.2.3. obsługa równoważenie obciążenia „load balancing"
31.3. interfejs konsoli RS-232 (RJ-45) lub USB
31.4. interfejs USB 2.0 (Typ-A, niezależny od portu konsoli)
31.5. przycisk przywracający konfigurację fabryczną
31.6. slot zabezpieczający Keningston
32. Parametry pracy urządzenia:
32.1. Temperatura otoczenia (zakres minimalny): 0-50 º C
32.2. Wilgotność (zakres minimalny): 5% - 92%
32.3. Obsługiwane standardy:
33. Ethernet IEEE 802.3 / IEEE 802.3u
34. Power-over-Ethernet IEEE 802.3af
35. Wireless IEEE 802.11a/b/g/n/ac/ax
35.1. Znak CE
35.2. EN 300 328
35.3. EN 301 489
35.4. EN 301 893
35.5. EN 60601-1-1, EN60601-1-2
36. Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE.
37. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac
38. Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

39. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na powierzchni płaskiej (sufit, ściana)
40. 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.

II. Kontroler sieci bezprzewodowej zwany dalej kontrolerem – 1 szt.

1. Musi w pełni obsługiwać punkty dostępowe, opisane w pkt. I.
2. Kontroler musi zarządzać siecią bezprzewodową złożoną z 150 punktów dostępowych z możliwością rozbudowy do 2000 punktów dostępowych (min. 1000 na pojedynczym kontrolerze, dalsza rozbudowa poprzez kolejne kontrolery w klastrze)
3. Każdy z wymaganych kontrolerów musi posiadać wyspecyfikowane funkcje:
   3.1. Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall)
   3.2. Musi posiadać funkcje VPN Gateway
   3.3. Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym.
   3.4. Kontroler musi mieć możliwość pracy w klastrze HA 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
   3.5. 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.
   3.6. Kontroler musi mieć możliwość przeprowadzenia Live update polegającego na aktualizacji klastra kontrolerów oraz punktów dostępowych bez przerwania obsługi urządzeń klienckich
   3.7. 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.
   3.8. Kontroler musi mieć możliwość uaktualniania poszczególnych modułów np. odpowiedzialnego na dynamiczny dobór kanałów, analizę aplikacji itp. bez konieczności uaktualniana całego systemu operacyjnego.
   3.9. Kontroler musi mieć możliwość terminowania ruchu z obsługujących tą funkcję przełączników w celu ujednolicenia polityk bezpieczeństwa dla sieci przewodowej i bezprzewodowej.
   3.10. Wspieranie wieli wersji oprogramowania. Funkcja ta umożliwia administratorowi przetestowanie nowych funkcjonalności na wybranym obszarze sieci bez konieczności aktualizowania całego środowiska
   3.11. Komunikacja pomiędzy kontrolerami musi wykorzystywać protokoły sieciowe niewymagające instalacji dodatkowych urządzeń sieciowych.

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

3.12. Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania

3.13. Kontroler musi zapewniać centralne zarządzenia licencjami, tzn. w architekturze sieci, w której występuję więcej niż jedne kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom.

3.14. Kontroler musi posiadać następujące parametry sieciowe:

3.14.1. możliwość wdrożenia w warstwie 2 i 3 ISO/OSI,

3.14.2. wsparcie dla sieci VLAN w tym również trunk 802.1q

3.14.3. wbudowany serwer DHCP

3.14.4. obsługa SNMPv2, SNMPv3

3.14.5. routing dynamiczny OSPF

3.15. Kontroler sieci WLAN musi obsługiwać co najmniej:

3.15.1. Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST, DES, 3DES, AES-CBC

3.15.2. Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze

3.15.3. Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit

3.15.4. Autoryzację dostępu użytkowników:

3.15.4.1. Typy uwierzytelnienia: IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS,EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal", 802.1X i MAC

3.15.4.2. Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia

3.15.4.3. Wsparcie dla autoryzacji, minumum: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba NAC

3.15.4.4. Musi umożliwiać utworzenie nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal"

3.15.4.5. Musi umożliwiać wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES)

3.15.4.6. Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym

3.15.4.7. Uwierzytelnienie oraz autoryzacja muszą być możliwe przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius.

3.16. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających.

3.17. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu

3.18. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia

3.19. Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci:

3.19.1. Integracja jednoczesnej transmisji danych i głosu

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

3.19.2. Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejkowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p

3.19.3. Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming)

3.19.4. Ograniczanie pasma dla użytkownika oraz dla roli użytkownika

3.19.5. Ograniczenie pasma dla poszczególnych aplikacji

3.19.6. Ograniczenie pasma dla poszczególnych SSID

3.20. Kontroler musi umożliwiać integrację ze środowiskiem Microsoft Lync poprzez SDN API.

3.21. Kontroler musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal)

3.22. Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni)

3.23. Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym:

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

3.24.1.1. Stałe monitorowanie pasma oraz usług

3.24.2. Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi

3.24.3. Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma

3.24.4. Przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie

3.24.5. Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b)

3.24.6. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału

3.24.7. Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w

3.24.8. Integracja z systemami RFID - wymagane jest wbudowane stosowne API

3.25. Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej co najmniej następujące własności:

3.25.1. Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia

3.25.2. Kopiowanie (mirroring) sesji

3.25.3. Szczegółowe logi (per pakiet) do późniejszej analizy

3.25.4. ALG (Application Layer gateway) co najmniej dla protokołów: FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera, PPTP

3.25.5. Translacja źródłowa, docelowa adresów IP

3.25.6. Identyfikacja i blokowanie ataków DoS

3.25.7. Obsługa protokołu GRE

3.25.8. Deep packet inspection (DPI)

3.25.9. Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci wifi

3.26. Kontroler musi posiadać funkcję systemu WIDS/ WIPS (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie). Moduł WIPS musi posiadać co najmniej następujące funkcje:

3.26.1. Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

3.26.2. Identyfikacja i możliwość blokowania sieci Adhoc
3.26.3. Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging
3.26.4. Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler
3.26.5. Identyfikacja błędów konfiguracji klientów WLAN
3.26.6. Identyfikacja podszywania się pod autoryzowane punkty dostępowe

3.27. Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w zamawianych dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie).

3.28. Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli.

3.29. Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA

3.30. Kontroler musi być zgodny z następującymi parametrami ilościowymi/wydajnościowymi:
3.30.1. Możliwa liczba obsługiwanych punktów dostępowych nie mniej niż 1000
3.30.2. Liczba jednocześnie obsługiwanych adresów MAC nie mniej niż 16000
3.30.3. Liczba aktywnych sesji zapory sieciowej nie mniej niż 2000000
3.30.4. Przepustowość co najmniej 40Gbps
Przepustowość zapory sieciowej co najmniej 40Gbps
Liczba obsługiwanych BSSID nie mniej niż 8192
3.30.5. Liczba jednoczesnych sesji IPSEC nie mniej niż 24000
3.30.6. Minimum 4 porty 10GBASE-X ze stykiem definiowanym przez SFP+
3.30.7. Minimum 2 porty gigabitowe w standardzie 10/100/1000BaseT
3.30.8. Minimum 2 porty 1000BaseX ze stykiem definiowanym przez SFP (dopuszcza się porty typu Combo, współdzielone z portami 10/100/1000BaseT)
3.30.9. 1 interfejs konsoli (mini USB/RJ-45)
3.30.10. Minimum 1 port USB 2.0
3.30.11. Zużycie energii nie większe niż 120W
3.30.12. Pełna obsługa standardu 802.1Q – 4094 tagów sieci VLAN
3.30.13. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.

4. Dla kontrolera wymagana zgodność z normami CE
5. Minimum 3 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy urządzenia (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie co najmniej 8x5 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.
6. Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji czasowych

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

III. System zarządzania siecią przewodową i bezprzewodową

1. Dedykowane oprogramowanie służące do zarządzania i monitorowania pracy kontrolerem i punktami dostępowymi opisanymi w pkt. I, II. Oprogramowanie musi być wyposażone w licencję pozwalającą na zarządzaniem minimum 155 urządzeniami sieciowymi każdego typu (licencja nie może być ograniczona do jednego typu urządzeń, jeżeli dany typ urządzeń wymaga oddzielnego licencjonowania, muszą być one zaoferowane ponad wymagane minimum).
2. System Zarządzania i Monitoringu tego samego producenta co urządzania zainstalowane w sieci WLAN i LAN
3. Oprogramowanie umożliwiające instalacje w środowisku wirtualnym VMware
4. Obsługa poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW
5. Zarządzanie wszystkimi punktami dostępowymi AP oraz kontrolerami Sieci Radiowej będących przedmiotem tego samego postępowania
6. System musi posiadać odpowiednią ilość licencji do obsługi wszystkich niezbędnych urządzeń.
7. Wsparcie środowisk heterogenicznych, czyli możliwość zarządzania z wykorzystaniem SNMP urządzeniami sieciowymi różnych producentów
8. Automatyczne wykrywanie urządzeń
9. Bieżące monitorowanie stanu wszystkich podłączonych urządzeń
10. Funkcja automatycznej konfiguracji urządzeń sieci radiowej po podłączeniu się ich do sieci
11. Funkcja zbierania i wyświetlania informacji dotyczących pracujących w sieci urządzeń klienckich oraz możliwość ich wyszukania przy użyciu różnych parametrów takich jak:
    11.1. system operacyjny
    11.2. typ urządzenia
    11.3. użytkowanego urządzenia sieci WLAN oraz danego SSID
12. Funkcja pełnej wizualizacji położenia urządzeń znajdujących się w sieci
13. Funkcja archiwizacji konfiguracji urządzeń
14. Konfiguracja zadań dla podłączonych urządzeń, w szczególności
    14.1. automatyczna zmiana wersji oprogramowania urządzeń
    14.2. ponowne uruchomienie urządzenia
    14.3. definiowanie przedziałów czasowych, w których dane SSID ma być rozgłaszane
15. Narzędzie ułatwiające planowanie radiowe dla sieci posiadające możliwość wizualizacji pokrycia radiowego
16. Funkcja tworzenia map pokrycia (tzw. Heat Map)
17. Panel zarządzający GUI umożliwiający wyświetlanie przynajmniej
    17.1. Wykresu liczby zasocjowanych urządzeń klienckich
    17.2. Wykresu potencjalnej przepustowości urządzeń klienckich
    17.3. Wykresu stosunku sygnał do szumu (SNR) urządzeń klienckich
18. Funkcja automatycznego wykrycia urządzeń fałszywych, jego lokalizacji oraz ich ograniczenie np. poprzez rozłączenie urządzeń podłączonych do AP
19. Funkcja generowania ostrzeżeń i logów dotyczących wykrytych ataków w sieci bezprzewodowej
20. Funkcja generowania wiadomości email dla administratorów sieci (alerty, ostrzeżenia)
21. Funkcja definiowania poziomu dostępu dla administratorów z przypisanymi:
    21.1. Rolami
    21.2. Segmentami sieci, do których uzyskuje się dostęp
22. Obsługa XMP API
23. Funkcja monitorowania jakości oraz ilości połączeń Unified Communication and Collaboration

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

24. Minimum 3 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.
25. Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji czasowych

IV. Serwer uwierzytelniania i autoryzacji sieci przewodowej i bezprzewodowej – 2 szt.

1. Serwer UA musi charakteryzować się następującymi cechami:
   1.1. Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
   1.2. Serwer UA musi odsługiwać minimum 2000 urządzeń klienckich (w tym gości) w trybie HA – klaster dwóch fizycznych, wyposażonych w redundantne, modularne zasilacze, maszyn pracujący w trybie wysokiej dostępności (redundancja). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
   1.3. Każda z dostarczonych maszyn musi być tak wyskalowana, aby zapewnić obsługę minimum 10000 jednoczesnych sesji.
   1.4. Musi posiadać wbudowany serwer Radius oraz TACACS +
   1.5. Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:
      1.5.1.Cisco Systems
      1.5.2.Fortinet
      1.5.3.Microsoft
      1.5.4.Alcatel-lucent Enterprise
      1.5.5.Aruba Networks
      1.5.6.Huawei
      1.5.7.Extreme Networks
      1.5.8.PaloAlto
   1.6. Serwer UA musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera. W szczególności, musi współpracować w tym zakresie z kontrolerem opisanym w punkcie II.
   1.7. Serwer UA musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego. W szczególności, musi współpracować w tym zakresie z kontrolerem opisanym w punkcie II.
   1.8. Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
   1.9. Musi posiadać panel informacyjny który można dostosować do potrzeb użytkownika poprzez wyświetlania widget-ów prezentujących co najmniej poniższe informacje:
      1.9.1.Status pracy klastra urządzeń
      1.9.2.Utylizacje CPU
      1.9.3.Czas procesowania zapytań trafiających do systemu
      1.9.4.Informacje o ilości zapytań trafiających do systemu
      1.9.5.Skróty do innych elementów systemu (np. systemu obsługi ruchy gościnnego etc.)
      1.9.6.Skróty do uruchomiana aplikacji pracujących w ramach rozwiązania
      1.9.7.Statusu autoryzacji (poprawne, błędne)
      1.9.8.Kategorii podłączonych urządzeń (komputery, smartdevice, drukarki etc.)
      1.9.9.Rodziny urządzeń

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

1.9.10. Podsumowania profilowania urządzeń końcowych
1.9.11. Informacja o błędnych autoryzacjach (nazwa użytkownika czas oraz przez jaki serwis została autoryzacja procesowana)
1.9.12. Informacja o ostatnich autoryzacjach (nazwa użytkownika czas oraz przez jaki serwis została autoryzacja procesowana)
1.9.13. Informacja o poprawnych autoryzacjach (nazwa użytkownika czas oraz przez jaki serwis została autoryzacja procesowana)
1.9.14. Informacja o wykorzystaniu licencji przez system
1.9.15. Informacje o urządzeniach MDM
1.9.16. Informacje z systemu monitorowania końcówek (liczba klientów w rozbiciu na systemy operacyjne)
1.9.17. Statystyki systemu (takie jak, główna pamięć, pamięć wymiany, dysk, dysk wymiany)
1.10. Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
1.10.1. Microsoft Active Directory
1.10.2. Radius
1.10.3. Kerberos
1.10.4. LDAP
1.10.5. ODBC
1.10.6. Współpraca z serwerami tokenów
1.11. Musi obsługiwać metody profilowania
1.11.1. DHCP
1.11.2. TCP
1.11.3. MAC OUI
1.11.4. SNMP
1.11.5. Cisco device sensor
1.12. Wspierać protokoły
1.12.1. Radius, Radius CoA, TACACS +, web authentication, SAML v2.0
1.12.2. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
1.12.3. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
1.12.4. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
1.12.5. EAP-TLS
1.12.6. PAP, CHAP, MSCHAPv1 i v2, EAP-MD5
1.12.7. NAC, Microsoft NAP
1.12.8. Windows machine authentication
1.12.9. MAC Auth
1.12.10. Audit (role oparte na porcie oraz skanowanie podatności)
1.12.11. OCSP (Online Certificate Status Protocol) SNMP generic MIB, SNMP private MIB
1.12.12. CEF (Common Event Format), LEEF (Log Event Extended Format)
1.12.13. TLS 1.2
1.13. Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami
1.14. Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:
1.14.1. Co najmniej ESX 4.0, ESXi 4.1 do 6.0
1.14.2. Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

2. Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (2000). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.

3. System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności
   3.1. Samodzielna rejestracja klientów gościnnych w oparciu o:
      3.1.1. Adres e-mail
      3.1.2. Numer telefonu (wiadomość SMS)
      3.1.3. Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
   3.2. Logowanie w oparciu o portale społecznościowe
   3.3. Funkcja integracji z systemami trzecimi poprzez API
   3.4. Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową
   3.5. Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.
   3.6. Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
   3.7. Funkcja personalizacji strony gościnnej

4. Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.
   4.1. Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT
   4.2. System musi wspierać obsługę następujących systemów operacyjnych
      4.2.1. MS Windows
      4.2.2. Mac OS X
      4.2.3. iOS
      4.2.4. Android
      4.2.5. Chromebook
      4.2.6. Ubuntu
   4.3. Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
   4.4. Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej
   4.5. Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
   4.6. Funkcja tworzenia unikalnych certyfikatów dla urządzeń.
   4.7. Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń
   4.8. Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID

5. Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

6. System kontroli końcówek klienckich musi mieć następujące funkcjonalności

   6.1. System musi wspierać następujące systemy operacyjne
      6.1.1. Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)
      6.1.2. Apple Mac OS X 10.7 i nowsze
      6.1.3. Red HAT Enterprise Linux 4 i nowsze

6.1.4.CentOS 4 (Community Enterprise Operating System) i nowsze
6.1.5.Fedora Core 5 i nowsze
6.1.6.SUSE linux 10.x i nowsze
6.2. Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall
6.3. Wyświetlanie informacji on-line o statusie monitorowanych końcówek
6.4. System powinien obsługiwać agenta w formie
6.4.1.Stałej (Presistent Agent)
6.4.2.Tymczasowej (Dissolvabe Agent)
6.4.3.Agenta NAP

7. Minimum 3 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy urządzenia (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie co najmniej 8x5 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.

8. Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.

Odpowiedź nr 15:

Zamawiający, w oparciu o przedstawiony opis, nie jest w stanie zweryfikować czy zaproponowane rozwiązanie spełnia SIWZ opisany przez Zamawiającego. Zamawiający dokonał zmian w SIWZ opublikowanym w dniu 28.05.2020, w którym dodatkowo uszczegółowił swoje wymagania.

Powyższe odpowiedzi i zmiany stają się integralną część SIWZ i są wiążące dla wszystkich Wykonawców.
W związku z udzieloną odpowiedzią termin składania i otwarcia ofert nie ulega zmianie.

Kanclerz
Politechniki Gdańskiej
mgr inż. Mariusz Miller

.....
(podpis kierownika zamawiającego
lub osoby upoważnionej)

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl