Warszawa, dnia 30 sierpnia 2019 r.

Znak sprawy: ZAMPUB/PRZETARG/2019/04

Specyfikacja Istotnych Warunków Zamówienia

1. Informacje ogólne.

1.1. Tryb postępowania: przetarg nieograniczony. Postępowanie prowadzone jest w procedurze, o której mowa w art. 24 aa. ust. 1 ustawy pzp. Zamawiający najpierw dokona oceny ofert, a następnie zbada, czy wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

1.2. Nazwa zamówienia: **dostawa, montaż oraz konfiguracja sieciowych urządzeń aktywnych dla Centrum Sztuki Współczesnej - Zamek Ujazdowski**.

1.3. Zamawiający: Centrum Sztuki Współczesnej - Zamek Ujazdowski

Adres zamawiającego: ul. Jazdów 2, 00-467 Warszawa; Podstawa prawna: ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.J. Dz. U. z 2018 r. poz. 1986, z późn. zm) dalej zwana „pzp".

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO" Zamawiający, informuję, że:

1. Administratorem danych osobowych Wykonawcy jest Centrum Sztuki Współczesnej Zamek Ujazdowski, ul. Jazdów 2, 00-467 Warszawa;
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się pod adresem email: iod@u-jazdowski.pl
3. Dane osobowe Wykonawcy będą przetwarzane na podstawie art. 6 ust. 1 lit. c RODO oraz na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 z późn zm.), „ustawa Pzp"; w celu związanym z postępowaniem o udzielenie zamówienia publicznego, zawarciem umowy oraz jej realizacją oraz na podstawie art. 6 ust. 1 lit. f RODO zgodnie z pkt. 5 /dane identyfikujące postępowanie, np. nazwa, numer/ prowadzonym w trybie przetargu nieograniczonego W przypadku przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO za prawnie uzasadniony interes Administratora uznaje się:
   1) ustalenie lub dochodzenie przez Administratora roszczeń cywilnoprawnych wynikających z realizacji niniejszej Umowy, a także obrona przed takimi roszczeniami;
   2) weryfikacja danych osobowych w publicznych rejestrach.

4. Odbiorcami danych osobowych Wykonawcy będą osoby lub podmioty upoważnione zgodnie z przepisami prawa powszechnie obowiązującego, którym udostępniona zostanie dokumentacja postępowania, w tym w szczególności w oparciu o art. 8 oraz art. 96 ust. 3 ustawy Pzp. Odbiorcami państwa danych będą: podmioty i organy, którym Administrator jest zobowiązany lub upoważniony udostępnić dane osobowe na podstawie powszechnie obowiązujących przepisów prawa, oraz podmioty, które na podstawie stosownych umów przetwarzają dane osobowe powierzone do przetwarzania przez Administratora w związku z realizacją usług gwarantujących należyte wykonanie niniejszej Umowy;
5. Dane osobowe Wykonawcy będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy. W przypadku zawarcia i realizacji umowy obejmuje również okres niezbędny do zabezpieczenia ewentualnych roszczeń wynikających z umowy, chyba, że przepisy szczegółowe stanowią inaczej;
6. Obowiązek podania przez Wykonawcę danych osobowych bezpośrednio dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp w związku z art. 6 ust. 1 lit. c RODO związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
7. W odniesieniu do danych osobowych Wykonawcy decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8. Wykonawca posiada:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących Wykonawcy;
   - na podstawie art. 16 RODO prawo do sprostowania danych osobowych Wykonawcy;
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy Wykonawca uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
   - prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych, który administrator przetwarza na podstawie art. 6 ust. 1 lit. f RODO w związku z treścią pkt 3 i 5;
9. Wykonawcy nie przysługuje:
   - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

na podstawie art. 21 RODO, prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych Wykonawcy jest art. 6 ust. 1 lit. c RODO.

10. Wzór oświadczenia wymaganego od wykonawcy w zakresie wypełnienia przez niego obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO został uwzględniony we wzorze formularza ofertowego.

2. Opis przedmiotu zamówienia.

2.1. Przedmiot zamówienia stanowi dostawa, montaż oraz konfiguracja sieciowych urządzeń aktywnych:

1) Przełącznik dostępowy 7 sztuk
2) Kontroler sieci WLAN 1 sztuka (klaster)
3) Radiowy punkt dostępowy wewnętrzny 43 sztuki
4) Radiowy punkt dostępowy zewnętrzny 3 sztuki
5) Zapora sieciowa UTM 1 sztuka
6) Przełącznik dystrybucyjny 1 sztuka

W ramach realizacji przedmiotu umowy Wykonawca jest zobowiązany do:

- Dostarczenia, zainstalowania oraz skonfigurowania urządzeń określonych w przedmiocie zmówienia;
- Wdrożenia wraz z uruchomieniem urządzeń określonych w przedmiocie zmówienia;
- Przeprowadzenia testów potwierdzających poprawność działania wdrożonej infrastruktury zakończonych pisemnym potwierdzeniem Zamawiającego;
- Przeprowadzenie szkolenia instruktażowego obejmującego zakres możliwości dostarczonych urządzeń i oprogramowania. Szkolenie będzie odbywało się w siedzibie Zmawiającego. Szkolenie przeznaczone dla 2 pracowników Zamawiającego.

Szczegółowy opis przedmiotu zamówienia określony został w załączniku nr 1 oraz 1a do SIWZ. W przypadku gdy w opisie przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, należy rozumieć, zgodnie z art. 29 ust. 3 ustawy Pzp, że jest to uzasadnione specyfiką przedmiotu zamówienia i Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń. W takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania (funkcjonalności) nie gorsze od parametrów (funkcjonalności) wskazanych w opisie przedmiotu zamówienia.

2.2. Kody CPV:
32420000-3 Urządzenia sieciowe,
72700000-7 Usługi w zakresie sieci komputerowej.

2.3. Oferty częściowe. Czy dopuszcza się składanie ofert częściowych: Nie.
2.4. Oferty wariantowe. Czy dopuszcza się składanie ofert wariantowych: Nie.
2.5. Zamówienia uzupełniające. Zamawiający nie przewiduje możliwości udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt 7 ustawy pzp.

3. Podwykonawcy.

W przypadku gdy wykonawca przy realizacji przedmiotu umowy będzie korzystał z pomocy podwykonawców wówczas zobowiązany jest do wskazania w ofercie części zamówienia, które powierzy im do wykonania oraz ich firm jeżeli są znane wykonawcy na dzień złożenia oferty.

4. Terminy realizacji zamówienia

Wykonawca zobowiązany jest do realizacji przedmiotu umowy maksymalnie w terminie 75 dni licząc od dnia podpisania umowy, z zastrzeżeniem, iż dostawa urządzeń musi zostać zrealizowana w terminie: 30 dni licząc od dnia podpisania umowy.

5. Informacje dotyczące warunków składania ofert.

5.1. Niniejsza specyfikacja oraz wszystkie dokumenty do niej dołączone mogą być użyte jedynie w celu sporządzenia oferty.
5.2. Wykonawca przedstawia ofertę zgodnie z wymaganiami określonymi w niniejszej specyfikacji.
5.3. Wykonawca ponosi wszystkie koszty związane z przygotowaniem i złożeniem oferty.
5.4. Dodatkowe wyjaśnienia i informacje dotyczące zamówienia można otrzymać w godz. od 09:00 do 15:00 przesyłając zapytanie pocztą lub na adres e-mailowy: m.gonda@u-jazdowski.pl
5.5. Osobą uprawnioną do kontaktowania się z wykonawcami jest:
Małgorzata Gońda, e-mail: m.gonda@u-jazdowski.pl

6. Sposób porozumiewania się Zamawiającego z wykonawcami oraz przekazywania oświadczeń i dokumentów.

6.1. Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i wykonawcy przekazują pisemnie lub pocztą elektroniczną na adres: m.gonda@u-jazdowski.pl przy jednoczesnym niezwłocznym przesłaniu wersji pisemnej (pocztą lub kurierem).
6.2. Każda ze stron na żądanie drugiej ma obowiązek niezwłocznie potwierdzić fakt otrzymania jakiegokolwiek oświadczenia, wniosku, zawiadomienia lub informacji.

7. Termin związania ofertą.

7.1.Termin związania ofertą wynosi 30 dni i rozpoczyna swój bieg wraz z upływem terminu składania ofert.
7.2. W uzasadnionych przypadkach, co najmniej na 3 dni przed upływem terminu związania ofertą Zamawiający może tylko raz zwrócić się do wykonawców o wyrażenie

zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.8. Opis warunków udziału w postępowaniu.

8.1. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

a) nie podlegają wykluczeniu;

b) spełniają warunki udziału w postępowaniu, o ile zostały one określone przez zamawiającego w ogłoszeniu o zamówieniu.

8.2. O udzielenie zamówienie mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące:

a) posiadania kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów;

b) sytuacji ekonomicznej i finansowej;

c) zdolności technicznej lub zawodowej.

8.3. Opis sposobu dokonania oceny spełnienia warunków o których mowa w pkt 8.2.

a) Ad 8.2 lit. a) i b) Zamawiający nie wprowadza szczególnego warunku w tym zakresie;

b) Ad 8.2 lit. c) Zamawiający uzna, iż Wykonawca posiada zdolność techniczną lub zawodową jeżeli wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie wykonał, co najmniej dwie dostawy polegające na dostawie urządzeń aktywnych LAN o łącznej wartości wykonanych dostaw co najmniej 300.000,00 zł brutto.

8.4. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia zgodnie z art. 23 ust. 1 ustawy. W takim przypadku, wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.

8.5. Jeżeli oferta wykonawców, o której mowa w ust. 2, została wybrana, Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego, umowy regulującej współpracę tych wykonawców.

8.6. Zamawiający najpierw dokona oceny ofert, a następnie zbada, czy wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

8.7. Ocena spełniania warunków udziału w postępowaniu będzie prowadzona na podstawie treści złożonych oświadczeń lub dokumentów wymaganych zgodnie z art. 25a pzp i rozporządzeniem Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r., poz. 1126).

8.8. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

8.9. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.

9. Wykaz oświadczeń i dokumentów, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu, niepodleganiu wykluczeniu oraz spełnienia przez oferowane dostawy parametrów technicznych określonych przez Zamawiającego.

9.1. W celu wstępnego potwierdzenia, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu do oferty należy załączyć oświadczenie o niepodleganiu wykluczeniu według wzoru stanowiącego załącznik nr 3 do niniejszej SIWZ oraz oświadczenie o spełnianiu warunków udziału w postępowaniu według wzoru stanowiącego załącznik nr 4 do niniejszej SIWZ.
9.2. Zamawiający przed udzieleniem zamówienia, wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów, o których mowa w rozdziale 9 pkt 9.3. i 9.4. SIWZ.
9.3. W celu potwierdzenia spełniania przez wykonawcę warunku udziału w postępowaniu dotyczącego zdolności technicznej lub zawodowej wykonawcy, na wezwanie o którym mowa w pkt. 9.2 złożą:
- wykaz dostaw wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy lub usługi zostały wykonane, oraz załączeniem dowodów określających czy te dostawy lub usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postepowaniu – zgodnie ze wzorem stanowiącym załącznik nr 5 do SIWZ.
9.4. W celu potwierdzenia braku podstaw do wykluczenia wykonawcy z udziału w postępowaniu, o których mowa w art. 24 ust 1 Zamawiający żąda na wezwanie, o którym mowa w pkt 9.2 powyżej:
- oświadczenia wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku wydania takiego wyroku lub

decyzji – dokumenty potwierdzające dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności;
- oświadczenia wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne;

9.5. W przypadku wątpliwości co do treści dokumentu złożonego przez wykonawcę, zamawiający może zwrócić się do właściwych organów odpowiednio kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.
9.6. W przypadku oferty składanej przez Wykonawców ubiegających się wspólnie o udzielenie zamówienia publicznego, dokumenty potwierdzające, że Wykonawca nie podlega wykluczeniu składa każdy z Wykonawców oddzielnie.
9.7. Zamawiający żąda od wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w pkt 9.4.
9.8. Oświadczenia, o których mowa w niniejszym rozdziale dotyczące wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 22a ustawy oraz dotyczące podwykonawców, składane są w oryginale. Inne dokumenty niż oświadczenia, o których mowa zdaniu pierwszym, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poświadczenie za zgodność z oryginałem następuje w formie pisemnej lub w formie elektronicznej.
9.9. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
9.10. Zgodnie z art. 24 ust. 11 ustawy wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji określonych w art. 86 ust 5 przekazuje zamawiającemu oświadczenie o przynależności albo braku przynależności do tej samej grupy kapitałowej; w przypadku przynależności do tej samej grupy kapitałowej wykonawca może złożyć wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu.
9.11. W celu potwierdzenia, że oferowane dostawy, odpowiadają wymaganiom określonym przez zamawiającego, zamawiający żąda załączenia do oferty następujących dokumentów: opisów technicznych, folderów lub katalogów oferowanych urządzeń wyspecyfikowanych w formularzu cenowym zawierające zestawienie parametrów technicznych potwierdzających spełnienie minimalnych parametrów określonych przez Zamawiającego.

10. Wymagania dotyczące wadium.

10.1. Zamawiający nie wymaga wniesienia wadium.

11. Opis sposobu przygotowywania ofert.

11.1. Wymagania podstawowe.

11.1.1. Każdy Wykonawca może złożyć tylko jedną ofertę.

11.1.2. Ofertę należy przygotować ściśle według wymagań określonych w niniejszej SIWZ.

11.1.3. Oferta musi być podpisana przez osoby upoważnione do reprezentowania Wykonawcy (Wykonawców wspólnie ubiegających się o udzielenie zamówienia). Oznacza to, iż jeżeli z dokumentu(ów) określającego(ych) status prawny Wykonawcy(ów) lub pełnomocnictwa (pełnomocnictw) wynika, iż do reprezentowania Wykonawcy(ów) upoważnionych jest łącznie kilka osób dokumenty wchodzące w skład oferty muszą być podpisane przez wszystkie te osoby.

11.1.4. Upoważnienie osób podpisujących ofertę do jej podpisania musi bezpośrednio wynikać z dokumentów dołączonych do oferty. Oznacza to, że jeżeli upoważnienie takie nie wynika wprost z dokumentu stwierdzającego status prawny Wykonawcy (odpisu z właściwego rejestru) to do oferty należy dołączyć oryginał lub poświadczoną notarialnie kopię stosownego pełnomocnictwa wystawionego przez osoby do tego upoważnione.

11.1.5. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

11.2. Forma oferty.

11.2.1. Oferta musi być sporządzona w języku polskim, mieć formę pisemną i format nie większy niż A4. Arkusze o większych formatach należy złożyć do formatu A4. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski poświadczonym przez wykonawcę.

11.2.2. Stosowne wypełnienia we wzorach dokumentów stanowiących załączniki do SIWZ i wchodzących następnie w skład oferty mogą być dokonane komputerowo, maszynowo lub ręcznie.

11.2.3. Dokumenty przygotowywane samodzielnie przez Wykonawcę na podstawie wzorów stanowiących załączniki do SIWZ powinny mieć formę wydruku komputerowego lub maszynopisu.

11.2.4. Całość oferty powinna być złożona w formie uniemożliwiającej jej przypadkowe zdekompletowanie.

11.2.5. Wszelkie miejsca w ofercie, w których Wykonawca naniósł poprawki lub zmiany wpisywanej przez siebie treści, (czyli wyłącznie w miejscach, w których jest to dopuszczone przez Zamawiającego) muszą być parafowane przez osobę (osoby) podpisującą (podpisujące) ofertę. Wszelkie skreślenia i zmiany naniesione przez Wykonawcę w uprzednio wpisany przez niego tekst muszą być parafowane i datowane.

11.3. Zawartość oferty.

Kompletna oferta musi zawierać:

a) formularz oferty - sporządzony na podstawie wzoru stanowiącego załącznik nr 2 do SIWZ,
b) formularz cenowy - sporządzony na podstawie wzoru stanowiącego załącznik nr 2a do SIWZ.
c) Dokumenty i oświadczenia określone przez Zamawiającego w pkt 9.1 oraz 9.11 SIWZ,
d) Stosowne Pełnomocnictwo(a) - w przypadku, gdy upoważnienie do podpisania oferty nie wynika bezpośrednio ze złożonego w ofercie odpisu z właściwego rejestru,

e) W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokument ustanawiający Pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie niniejszego zamówienia publicznego.

11.4. Informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Wykonawca, nie później niż w terminie składania ofert może zastrzec w ofercie (oświadczeniem zawartym w Formularzu Oferty), iż Zamawiający nie będzie mógł ujawnić informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

11.5. Ofertę należy złożyć w zamkniętej kopercie oznakowanej w sposób następujący:
<NAZWA ZAMAWIAJĄCEGO I JEGO ADRES> oferta w <TRYB POSTĘPOWANIA> na <NAZWA (TYTUŁ) POSTĘPOWANIA> nie otwierać przed <DATA I GODZINA OTWARCIA OFERT> Koperta powinna być zapieczętowana w sposób gwarantujący zachowanie poufności jej treści oraz zabezpieczająca jej nienaruszalność do terminu otwarcia ofert.

12. Opis sposobu udzielania wyjaśnień dotyczących treści niniejszej SIWZ oraz oświadczenie, czy Zamawiający zamierza zwołać zebranie Wykonawców.

12.1. Wykonawca może zwrócić się do Zamawiającego z pisemną prośbą o wyjaśnienie treści SIWZ. Zamawiający niezwłocznie udzieli wyjaśnień, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem że wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu składania wniosku, o którym mowa powyżej, lub dotyczy udzielonych wyjaśnień, zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa zdaniu pierwszym.

12.2. Pytania należy kierować na adres Zamawiającego: ul. Jazdów 2, 00-467 Warszawa lub pocztą elektroniczną na adres: m.gonda@u-jazdowski.pl.

12.3. Zamawiający nie zamierza zwoływać zebrania wykonawców.

12.4. W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ, a treścią udzielonych odpowiedzi jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

12.5. W uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu do składania ofert, zmienić treść niniejszej SIWZ. Zmiana może wynikać z pytań zadanych przez Wykonawców, jak i z własnej inicjatywy Zamawiającego. Zmiana treści SIWZ będzie wiążąca przy składaniu ofert. Dokonana zmiana SIWZ zostanie niezwłocznie przekazana wszystkim wykonawcom, którym przekazano SIWZ oraz zamieszczona na stronie internetowej Zamawiającego.

12.6. Zamawiający przedłuży termin składania ofert, jeżeli w wyniku zmiany treści SIWZ nie prowadzącej do zmiany treści ogłoszenia o zamówieniu, niezbędny będzie dodatkowy czas na wprowadzenie zmian w ofertach. O przedłużeniu terminu składania ofert Zamawiający

poinformuje Wykonawców, którym przekazano SIWZ oraz zamieści tę informację na swojej stronie internetowej.

13. Miejsce oraz termin składania i otwarcia ofert.

13.1. Oferty można składać w siedzibie Zamawiającego – w Sekretariacie, II piętro, w terminie do dnia **12 września 2019 r. do godz. 12.00.**

13.2. Oferta złożona po terminie zostanie zwrócona bez otwierania.

13.3. Oferty zostaną otwarte w siedzibie Zamawiającego, w dniu **12 września 2019 r. o godz. 12.10.**

13.4. Wykonawcy mogą uczestniczyć w publicznej sesji otwarcia ofert.

14. Sposób obliczenia ceny oferty.

14.1. Ceną oferty jest cena brutto podana w Formularzu ofertowym.

14.2. Cena musi być podana w złotych polskich, cyfrowo, z zaokrągleniami do dwóch miejsc po przecinku.

14.3. Cena - należy przez to rozumieć cenę w rozumieniu ustawy z dnia 5 maja 2014 r. o informowaniu o cenach towarów i usług (Dz. U. z 2014 r. poz. 915)

14.4. Cena oferty, to wartość wyrażona w złotych, jaką Zamawiający będzie obowiązany zapłacić Wykonawcy za wykonanie przedmiotu zamówienia, z uwzględnieniem podatku VAT oraz podatku akcyzowego, jeżeli na podstawie odrębnych przepisów sprzedaż towaru podlega obciążeniu podatkiem od towarów i usług oraz podatkiem akcyzowym.

14.5. Cena całkowita oferty musi obejmować w kalkulacji wszystkie koszty i składniki, niezbędne do wykonania przedmiotu zamówienia.

14.6. Stawkę VAT należy określić wg obowiązujących przepisów i stanu faktycznego na dzień złożenia oferty.

15. Wycofanie oferty lub jej zmiany.

15.1. Wykonawca może wprowadzać zmiany, poprawki i uzupełnienia do złożonych ofert pod warunkiem, że zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmian przed upływem terminu składania ofert.

15.2. Powiadomienie o wprowadzeniu zmian musi być złożone według takich samych wymagań, jak składana oferta tj. w dwóch kopertach (wewnętrznej i zewnętrznej) odpowiednio oznakowanych dodatkowo dopiskiem „ZMIANA".

15.3. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie pisemnego powiadomienia (według takich samych zasad, jak wprowadzenie zmian i poprawek) z napisem na zewnętrznej kopercie „WYCOFANIE".

15.4. Koperty oznaczone napisem „WYCOFANIE" będą otwierane w pierwszej kolejności i po stwierdzeniu poprawności postępowania wykonawcy oraz zgodności ze złożonymi ofertami, koperty wewnętrzne ofert wycofanych nie będą otwierane.

15.5. Koperty oznaczone dopiskiem „ZMIANA" zostaną otwarte przy otwieraniu oferty wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian zostaną dołączone do oferty.

16. Ocena ofert.

16.1. W odniesieniu do wykonawców, którzy spełnili postawione warunki Zamawiający dokona oceny ofert na podstawie następujących kryteriów:

l.p.	Opis kryteriów oceny	Znaczenie
1.	CENA	60 %
2.	TERMIN REALIZACJI	40 %

16.2. Zamawiający porówna i oceni oferty w następujący sposób:

a) w zakresie kryterium cena ocena kryterium nastąpi w skali punktowej od 0 do 60 pkt, według wzoru:

najniższa cena brutto spośród złożonych ofert/ wartość brutto w ofercie badanej x 60 pkt.

b) w zakresie kryterium terminu realizacji ocena kryterium nastąpi w skali punktowej od 0 do 40 pkt. Zamawiający przyzna pkt w sposób następujący:

- zaoferowanie terminu realizacji przedmiotu umowy licząc od dnia podpisania umowy:
  - 55 dni – 40 pkt,
  - 65 dni – 20 pkt,
  - 75 dni – 0 pkt.

Oferta wykonawcy, który zaoferuje termin realizacji przedmiotu umowy dłuższy niż 75 dni lub nie złoży oświadczenia w zakresie oferowanego terminu realizacji zostanie odrzucona.

16.3. Za najkorzystniejszą ofertę zostanie uznana oferta, która uzyska najwyższą sumę punktów z wszystkich kryteriów.

16.4. Zamawiający udzieli zamówienia wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w niniejszej specyfikacji i została oceniona jako najkorzystniejsza w oparciu o podane kryteria wyboru, tj. uzyskała najwyższa liczbę punktów.

16.5. Zamawiający poinformuje niezwłocznie wszystkich wykonawców o wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres, jeżeli jest miejscem wykonywania działalności wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy, jeżeli są miejscami wykonywania działalności wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację.

16.6. Zamawiający udostępnia informacje, o których mowa w pkt 1 na stronie internetowej.

17. Wykluczenie Wykonawcy.

17.1. Z postępowania o udzielenie zamówienia wyklucza się:

a) wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie został zaproszony do negocjacji lub złożenia ofert wstępnych albo ofert, lub nie wykazał braku podstaw wykluczenia;

b) wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
- o którym mowa w art. 165a, art. 181–188, art. 189a, art. 218–221, art. 228–230a, art. 250a, art. 258 lub art. 270–309 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. poz. 553, z późn. zm.[5])) lub art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2016 r. poz. 176),
- o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny,
- skarbowe,
- o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769);

c) wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 13;

d) wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

e) wykonawcę, który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawieniu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub obiektywne i niedyskryminacyjne kryteria, zwane dalej „kryteriami selekcji", lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów;

f) wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia;

g) wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;

h) wykonawcę, który brał udział w przygotowaniu postępowania o udzielenie zamówienia lub którego pracownik, a także osoba wykonująca pracę na podstawie umowy zlecenia, o dzieło, agencyjnej lub innej umowy o świadczenie usług, brał udział w przygotowaniu takiego postępowania, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;

i) wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;

j) wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. z 2015 r. poz. 1212, 1844 i 1855 oraz z 2016 r. poz. 437 i 544);

k) wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne;

l) wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że istniejące między nimi powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

17.2. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.

18. Wzór umowy.

18.1. Wzór umowy stanowi załącznik nr 6 do SIWZ.

19. Zmiana umowy.

19.1. Zamawiający przewiduje możliwość zmiany umowy o udzielenie zamówienia publicznego w przypadku zaistnienia okoliczności określonych w § 10 ust. 2 wzoru umowy.

20. Zabezpieczenie należytego wykonania umowy.

20.1. Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

21. Informacje o formalnościach jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.

21.1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z zastrzeżeniem art. 183 ustawy PZP, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni – jeżeli zostało przesłane w inny sposób.

21.2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminów, o których mowa w ust. 1, jeżeli:

1) w postępowaniu o udzielenie zamówienia:

- złożono tylko jedną ofertę,

- upłynął termin do wniesienia odwołania na czynności zamawiającego wymienione w art. 180 ust. 2 lub w następstwie jego wniesienia Izba ogłosiła wyrok lub postanowienie kończące postępowanie odwoławcze.

21.3. Jeżeli wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych

ofert bez przeprowadzania ich ponownego badania i oceny, chyba że zachodzą przesłanki unieważnienia postępowania, o których mowa w art. 93 ust. 1 ustawy.

22. Środki ochrony prawnej.

22.1. Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy.

22.2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz specyfikacji istotnych warunków zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy.

22.3. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy czynności zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której zamawiający jest zobowiązany na podstawie ustawy.

22.4. Odwołanie przysługuje wyłącznie wobec czynności:

a) określenia warunków udziału w postępowaniu;

b) wykluczenia odwołującego z postępowania o udzielenie zamówienia;

c) odrzucenia oferty odwołującego;

d) opisu przedmiotu zamówienia;

e) wyboru najkorzystniejszej oferty.

22.5. Odwołanie wnosi się do Prezesa Izby w formie pisemnej lub w postaci elektronicznej, podpisane bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub równoważnego środka, spełniającego wymagania dla tego rodzaju podpisu.

22.6. Odwołanie powinno wskazywać czynności lub zaniechanie czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.

22.7. Odwołujący przesyła kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.

22.8. Odwołanie wnosi się: w terminie 5 dni od dnia przesłania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane w sposób określony w art. 180 ust. 5 zdanie drugie albo w terminie 10 dni – jeżeli zostały przesłane w inny sposób.

22.9. Odwołanie wobec treści ogłoszenia o zamówieniu oraz wobec postanowień specyfikacji istotnych warunków zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub specyfikacji istotnych warunków zamówienia na stronie internetowej - jeżeli wartość zamówienia jest mniejsza niż kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8.
22.10. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Izbę orzeczenia.
22.11. Pozostałe kwestie związane ze środkami ochrony prawnej określone są w dziale VI „Środki ochrony prawnej" ustawy.

Załączniki do SIWZ:
- nr 1 – szczegółowy opis przedmiotu zamówienia;
- nr 1a – koncepcja rozmieszczenia AP w Centrum Sztuki Współczesnej w Zamku Ujazdowskim
- nr 2 - formularz oferty;
- nr 2 a – formularz cenowy;
- nr 3 – oświadczenie o niepodleganiu wykluczeniu;
- nr 4 – oświadczenie – spełnianiu warunków udziału w postępowaniu;
- nr 5 – wzór wykazu wykonanych dostaw;
- nr 6 – wzór umowy.

Z A T W I E R D Z A M:

.....
(podpis)

Załącznik nr 1 do SIWZ – szczegółowy opis przedmiotu zamówienia

Dostawa, montaż oraz konfiguracja sieciowych urządzeń aktywnych dla Centrum Sztuki Współczesnej - Zamek Ujazdowski.

Zestawienie urządzeń aktywnych:

Przełącznik dostępowy	7 sztuk
Kontroler sieci WLAN	1 szt. (klaster)
Radiowy punkt dostępowy wewnętrzny	43 sztuki
Radiowy punkt dostępowy zewnętrzny	3 sztuki
Zapora sieciowa UTM	1 sztuka
Przełączniki dystrybucyjny	1 sztuka

Przełącznik dostępowy – 7 sztuk

1. Przełącznik powinien posiadać następującą konfigurację portów:
    a. 24 porty RJ-45 z autonegocjacja 10/100/1000 (IEEE 802.3 typu 10Base-T, IEEE 802.3u typu 100Base-TX, IEEE 802.3ab typu 1000Base-T); duplex 10Base-T/100Base-TX: pół lub pełny duplex; 1000Base-T - tylko pełny; wsparcie dla IEEE 802.3at PoE+
    b. 4 porty 10Gigabit Ethernet SFP+
    c. 1 port szeregowy konsoli RJ45 lub USB
2. Obudowa wieżowa Rack o wysokości 1U umożliwiająca instalację w szafie 19"
3. Zarządzanie:
    a. CLI
    b. WWW
    c. telnet
    d. pozapasmowe konsolowe (port szeregowy RS-232C -RJ45),
    e. możliwość scentralizowanego zarządzania zarówno przez dedykowane oprogramowanie producenta jak i chmurowo
4. Warstwa przełączania – Layer 3
5. Rozmiar tablicy adresów MAC- minimum 16000
6. Tablica routingu:
    a. 2000 wpisów dla IPv4
    b. 1000 wpisów dla IPv6
7. Prędkość magistrali: 128 Gbps
8. Przepustowość: 95,2 Mpps
9. Parametry jednostki centralnej przełącznika:
    a. Taktowanie procesora minimum 1000MHz
    b. Pamięć flash minimum 4GB
    c. Pamięć RAM minimum 1GB
10. Opóźnienie poniżej 3.8 µs dla 1000 Mbit
11. Bufor pakietów minimum 12 MB
12. VLAN
    a. Pełna zgodność z IEEE 802.1Q
    b. 4094 VLAN IDs

    c. Do 512 VLANów jednocześnie
13. Funkcje wysokiej dostępności:
    a. Spanning Tree (802.1d)
    b. Rapid Convergence Spanning Tree (802.1w)
    c. Muliple Spanning Tree (802.1s)
    d. Rapid Per-VLAN Spanning Tree (RPVST+)
    e. GVRP and MVRP
14. Agregacja portów zgodna z 802.3ad LACP
15. Funkje QoS:
    a. priorytetyzacja zgodna z 802.1p,
    b. Class of Service (CoS) priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port and DiffServ ToS
    c. Layer 4 prioritization TCP/UDP
    d. wsparcie dla 4 kolejek,
    e. rate-limiting
    f. Voice VLAN
    g. IP SLA for voice
16. Monitorowanie:
    a. RMON 4 grupy statistics, history, alarm, events,
    b. SFLOW
    c. XRMON
17. Inne funkcje i funkcjonalności:
    a. LLDP
    b. LLDP-MED
    c. dual flash images
    d. obsługa ramek typu Jumbo
    e. iSCSI
    f. DHCP snooping
    g. DHCP Server
    h. BPDU Guard
    i. BPDU Protection
    j. port isolation
    k. wsparcie dla IPv4 i Ipv6
    l. Tunneled node dla ruchu z AP
    m. Zero Touch Provisioning
    n. Access control lists (ACL)
    o. Dynamic ARP protection
18. Autentyfikacja użytkowników:
    a. IEEE 802.1X
    b. Web-based authentication
    c. Supports MAC-based authentication
    d. RADIUS/TACACS+ support
19. Budżet mocy PoE 370W
20. Moc pobierana maksymalna 445W
21. Zasilanie z wbudowanego zasilacza 100 - 127 / 200 - 240 VAC, zasilacz z certyfikacją co najmniej 80Plus Silver
22. Przełącznik musi być przystosowany do środowiska pracy od 0°C do 45°C

23. Każdy przełącznik musi być wyposażony w dwie wkładki SFP+ dla standardu 10G Base-SR. Wkładki musza być dedykowanym rozwiązaniem producenta i objęte tą samą gwarancją co przełącznik.
24. Gwarancja i wsparcie techniczne zapewniające dostęp do poprawek i aktualizacji przez okres 60 miesięcy licząc od dnia podpisania protokołu odbioru.
    W ramach Gwarancji Zamawiający wymaga naprawy wadliwego urządzenia w terminie 3 dni licząc od dnia zgłoszenia wady lub usterki, a w przypadku braku możliwości naprawy wymiany urządzenia na nowe w terminie 7 dni licząc od dnia zgłoszenia.

Kontroler sieci WLAN – 1 szt. (klaster)

Wymagane funkcjonalności i parametry dla kontrolera sieci bezprzewodowej

1. Kontroler sieci WLAN musi w pełni obsługiwać wszystkie punkty dostępowe będą przedmiotem postępowania.
2. Kontroler musi obsługiwać minimum 64 punktów dostępowych.
3. Kontroler musi być dostarczony razem z oprogramowaniem do obsługi wszystkich punktów dostępowych będących przedmiotem postępowania.
4. Musi istnieć możliwość rozbudowy kontrolera o nie mniej niż poniższe funkcje:
    a. Kryptograficzny moduł ochrony xSec zabezpieczający transmisję w warstwie 2 ISO/OSI (uwierzytelnienie 802.1X, 256-bit AES-CBC)
    b. Szyfrowanie z wykorzystaniem "Suite-B Cryptography" – AES128-GCM/AES256-GCM
    c. Zdalny dostęp VPN za pomocą klienta Windows/MAC/iOS/Android
5. Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości, pracując w systemie hierarchicznym (w przypadku rozbudowy w przyszłości).
6. Kontroler musi mieć możliwość pracy w klastrze (praca w konfiguracji active-active oraz active-standby).
7. W ramach postępowania należy dostarczyć drugi identyczny kontroler bez oprogramowania przygotowany do pracy w trybie active-standby.
8. Komunikacja pomiędzy kontrolerami musi wykorzystywać protokoły sieciowe niewymagające instalacji dodatkowych urządzeń sieciowych.
9. Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania.
10. Kontroler musi zapewniać centralne zarządzenia oprogramowaniem czyli pełnić funkcję serwera, który automatycznie będzie przydzielał prawa pozostałym kontrolerom dla AP terminującym na innych kontrolerach.
11. Kontroler musi posiadać następujące parametry sieciowe:
    a. możliwość wdrożenia w warstwie 2 i 3 modelu ISO/OSI,
    b. routing dynamiczny OSPF
    c. wsparcie dla sieci VLAN w tym również trunk 802.1q
    d. wbudowany serwer DHCP
    e. obsługa SNMPv2, SNMPv3
12. Kontroler sieci WLAN musi obsługiwać co najmniej:
    a. Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST , DES, 3DES, AES-CBC

b. Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze
c. Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit
d. Autoryzację dostępu użytkowników:
    i. 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
    ii. Możliwość wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia
    iii. Wsparcie dla autoryzacji: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba NAC
    iv. Możliwość utworzenia 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"
    v. Możliwość wykorzystania mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES)
    vi. Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym
    vii. Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających.
    viii. 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.
e. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę użytkowników w przypadku awarii serwerów uwierzytelniających.
f. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu (rozbudowa poprzez dokupienie stosownej funkcji oprogramowania)
g. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia

13. Kontroler sieci WLAN musi posiadać obsługę transmisji różnego typu danych w jednej sieci: (rozbudowa poprzez dokupienie stosownej funkcji oprogramowania)
    a. Integracja jednoczesnej transmisji danych i głosu
    b. 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
    c. Obsługa fast roaming
    d. Ograniczanie pasma dla użytkownika oraz dla roli użytkownika
    e. Ograniczenie pasma dla poszczególnych aplikacji
    f. Ograniczenie pasma dla poszczególnych kategorii stron internetowych bądź też poziomu zaufania
    g. Ograniczenie pasma dla poszczególnych SSID
14. Kontroler musi umożliwiać integrację w innymi platformami poprzez SDN API (wymagane co najmniej dla Microsoft Lync).

15. Kontroler sieci WLAN musi umożliwiać stworzenie strony logowania dla gości (Captive Portal)
16. Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości przez co umożliwi zarządzanie przez osoby spoza działu IT (bez wiedzy specjalistycznej).
17. Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym:
    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
    c. Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi
    d. Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma
    e. Wykrywanie urządzeń obsługujących MU-MIMO i podłączenie ich do punktów dostępowych obsługujących tą technologię (pracujących w standardzie 802.11ac Wave 2)
    f. Możliwość wymuszania przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie
    g. Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie kolejnymi generacjami standardu Wifi (802.11ac, 11n, 11g, 11a, 11b)
    h. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
    i. Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w
    j. Integracja z systemami RFID - wymagane jest wbudowane stosowne API
18. Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej co najmniej następujące własności:
    a. Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia
    b. Mirroring sesji
    c. Obsługa protokołu GRE
    d. Szczegółowe logi (per packet) do późniejszej analizy
    e. ALG (Application Layer gateway) dla protokołów FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera, PPTP
    f. Translacja adresów IP (źródłowa i docelowa)
    g. Identyfikacja i blokowanie ataków DoS

Jeśli powyższe funkcjonalności wymagają dodatkowych funkcji oprogramowania– należy je dostarczyć razem z kontrolerem w ramach tego postępowania.

19. Kontroler musi posiadać funkcję systemu WIDS/ WIPS. Moduł WIPS musi posiadać co najmniej następujące funkcje(rozbudowa poprzez dokupienie stosownej funkcji oprogramowania):
    a. Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.
    b. Identyfikacja i możliwość blokowania sieci Ad-hoc
    c. Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging

d. Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler
e. Identyfikacja błędów konfiguracji klientów WLAN
f. Identyfikacja podszywania się pod autoryzowane punkty dostępowe

20. 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.
21. Kontroler musi mieć wbudowany serwer VPN, charakteryzujący się następującymi parametrami, nie mniej niż(rozbudowa poprzez dokupienie stosownej funkcji oprogramowania):
    a. Site-to-site oraz client-site VPN
    b. Terminacja ruchu L2TP/IPSEC VPN, XAUTH/IPSEC, PPTP
    c. Obsługa tokenów
    d. Wsparcie dla serwerów Radius i LDAP w celu uwierzytelnienia sesji VPN przy użyciu: PAP CHAP, MS-CHAP, MS-CHAP2
    e. Wsparcie dla algorytmów kryptograficznych: DES, 3DES, AES przy wykorzystaniu dedykowanych układów scalonych kontrolera (akceleracja sprzętowa).
22. Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody:
    a. interfejs przeglądarki Web (https)
    b. linia komend przez SSH
    c. dedykowany port konsoli.
23. Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA
24. Kontroler musi spełniać następujące parametry wydajnościowe i ilościowe:
    a. Ilość obsługiwanych punktów dostępowych nie mniej niż 64
    b. Ilość jednocześnie obsługiwanych użytkowników (urządzeń końcowych) 4000
    c. Ilość aktywnych sesji zapory sieciowej nie mniej niż 65000,
    d. przepustowość zapory sieciowej nie mniej niż 8 Gbps
    e. Ilość jednoczesnych tuneli IPSEC nie mniej niż 2000
    f. Przepustowość ruchu szyfrowanego nie mniejsza niż 2 Gbps dla algorytmu 3DES, 4Gbps dla algorytmu AES-CCM
    g. 8 portów „combo” (1000Base-T lub 1000BASE-X)
    h. 1 interfejs konsoli (mini USB/RJ-45)
    i. 1 port USB 2.0
    j. Zużycie energii nie większe niż 60W
    k. Szum akustyczny max 58dBA
25. Dla kontrolera wymagana zgodność z normami:
    a. FCC Part 15 Class B
    b. EN 55022 Class A
    c. EN 55024
    d. IEC/EN 60950
    e. CE Marking
    f. cTUVus Marked

26. Gwarancja i wsparcie techniczne zapewniające dostęp do poprawek i aktualizacji przez okres 60 miesięcy licząc od dnia podpisania protokołu odbioru. W ramach Gwarancji Zamawiający wymaga naprawy wadliwego urządzenia w terminie 3 dni licząc od dnia

zgłoszenia wady lub usterki, a w przypadku braku możliwości naprawy wymiany urządzenia na nowe w terminie 7 dni licząc od dnia zgłoszenia.

Radiowy punkt dostępowy wewnętrzny – 43 sztuki

1. Punkt dostępowy musi umożliwiać pracę w jednym z poniższych trybów:
    a. Autonomicznym
    b. Pod kontrolą kontrolera
    c. Pod kontrolą wirtualnego kontrolera (rezydującego na AP)
    d. Remote AP (praca w odległych oddziałach)
    e. Air monitor
    f. Spectrum analyzer
2. W ramach tego postępowania AP będą wdrożone w trybie kontrolerowym z możliwością automatycznej, okresowej konwersji do Air monitor. AP nie może blokować/uniemożliwiać obsługi żadnej z wymienionych funkcjonalności środowiska Wifi opisanej w sekcji dotyczącej kontrolera.
3. Architektura radiowa i obsługa standardów:
    a. Moduł radiowy 802.11 b/g/n
    b. Moduł radiowy 802.11 a/n/ac/ax
    c. Obsługa MIMO 2x2:2 dla 2,4 GHz i 4x4:4 dla 5Ghz
    d. Dwupasmowy moduł radiowy do zastosowań WIDS/WIPS
    e. Moduł BLE (Bluetooth Low Energy)
    f. Moduł Zigbee (dla rozwiązań IoT)
    g. Obsługa prędkości PHY dla 5GHz do 4800 Mbps
    h. Obsługa prędkości PHY dla 2,4GHz do 575 Mbps
    i. Maksymalna sumaryczna prędkość do 5.4Gbps
    j. Obsługa kanałów 20,40,80 i 160 MHz dla 802.11ax oraz 20,40 MHz dla 802.11n
    k. Obsługa MRC i ACC
    l. Obsługa agregacji ramek
4. Obsługa zakresów częstotliwości:
    a. 2.400 – 2.4835 GHz
    b. 5.150 – 5.250 GHz (UNII-1)
    c. 5.250 - 5.350GHz
    d. 5.470 - 5.725GHz
    e. 5.725 - 5.850GHz

Możliwość ograniczania zakresów zgodnie z restrykcjami kraju zastosowania.

5. Konfigurowalna moc nadajnika (agregowalna) :
    a. Dla pasma 2,4 GHz: do 21 dBm
    b. Dla pasma 5 GHz: do 24 dBm

Regulacja z dokładnością do 0,5 dBm

6. Zasilanie:
    a. PoE (IEEE 802.3af/at) na złączu RJ45, zużycie energii: max 21W
    b. Dedykowany port 12V, zużycie energii: max 17W.

7. Parametry fizyczne i anteny:
    a. Budowa niskoprofilowa (poniżej 5 cm)

b. Zabezpieczenie przed kradzieżą (Kensington)
c. Temperatura pracy: 0 – 50 ^{0}C
d. Zintegrowane anteny dookólne o zysku minimum 3.5 dBi dla 2.4 GHz oraz 4.9 dBi dla 5 GHz
e. Sygnalizacyjne diody LED

8. Interfejsy:
    a. Dwa porty Ethernet RJ45
    b. Jeden port zdolny do pracy w trybie Smart Rate do 2,5Gbps (100/1000/2500BASE-T)
    c. Drugi port zdolny do pracy w trybie 10/100/1000 Base-T
    d. port USB, możliwość zasilania podpiętego urządzenia prądem 1A (5W)
    e. port konsoli
    f. przycisk Resetu urządzenia (ustawienia fabryczne)

9. Mechanizmy bezpieczeństwa:
    a. WEP, WPA, WPA2 Personal I Enterprise (802.1X), WPA3
    b. Szyfrowanie TKIP oraz AES
    c. Szyfrowanie IPSec w celu tunelowania danych do koncentratora VPN
    d. Tagowanie VLAN (IEEE 802.1q)
    e. Blokowanie ruchu między klientami bezprzewodowymi
    f. Wbudowany firewall warstwy 3-7
    g. Firewall warstwy 7 umożliwia wykrywanie i blokowanie lub limitowanie pojedynczych aplikacji oraz grup aplikacji danego typu: blogi, email, współdzielenie plików, wiadomości, gry, p2p, portale społecznościowe i współdzielenie zdjęć, aktualizacja oprogramowania, sport, wideo i muzyka, konferencje audio i wideo
    h. Firewall warstwy 7 umożliwia blokowanie określonych stron http, zakresów adresów IP/portów
    i. Zintegrowany system wykrywania włamań, wrogich AP i reagowania na nie (wIPS/wIDS)

10. Funkcje modułu WIPS/WIDS:
    a. Skanowanie pasma 2,4 GHz oraz 5 GHz w czasie rzeczywistym
    b. Detekcja wrogich AP
    c. Wykrywanie podłączenia wrogiego AP do sieci LAN
    d. Klasyfikacja ataków w zależności od stopnia zagrożenia
    e. Klasyfikacja ataków w oparciu o sygnatury bazujące na typie i profilu zachowania (podstawowe ataki to: spoofing, DoS, packet flood)
    f. Konfiguracja polityki reagowania na ataki
    Prowadzenie logu zdarzeń
11. Mechanizmy QoS:
    a. DSCP
    b. 802.1p
    c. Advanced Power Save (U-APSD)
    d. IEEE 802.11e oraz WMM
    e. Limitowanie ruchu per klient oraz per SSID
    f. Rozpoznawanie aplikacji w warstwie 7

g. Limitowanie wybranego typu ruchu aplikacyjnego per klient oraz per SSID z możliwością markowania ruchu
h. Mechanizm preferowania pasma 5 GHz dla klientów dwuzakresowych
i. Mechanizm analizy widma częstotliwości z możliwością graficznej prezentacji pracujący w obu zakresach częstotliwości

12. Mechanizmy mobilności:
    a. 802.11k oraz 802.11r
    b. PMK oraz OKC dla szybkiego roamingu L2
    c. Roaming L3

13. Mechanizmy analityczne:
    a. Zbieranie informacji o urządzeniach w zasięgu sieci radiowej z podziałem na urządzenia/klientów podłączonych do sieci, będących w jej zasięgu oraz przemieszczających się w jej zasięgu
    b. Zbieranie informacji o długości czasu wizyty urządzeń/klientów w zasięgu sieci radiowej
    c. Zbieranie informacji o powtarzalności wizyt urządzeń/klientów
    d. Prezentacja graficzna zebranych informacji
    e. Export danych analitycznych w formie pliku CSV

14. Obsługa dostępu gościnnego:
    a. Przekierowanie użytkowników danego SSID na portal logowania
    b. Personalizacja wyglądu portalu logowania
    c. Kreowanie i zarządzanie kontami gościnnymi przez interfejs webowy
    d. Uwierzytelnianie do sieci za pośrednictwem: akceptacji portalu, uwierzytelniania SMSem, serwera LDAP, serwera RADIUS, serwera Active Directory, kont z portalu Facebook

15. Funkcje ogólne:
    a. Automatyczne budowanie sieci kratowej (formowanie połączeń do innych punktów dostępowych w oparciu o radio 2,4GHz lub 5 GHz bez podłączenia do sieci kablowej)
    b. Konfiguracja do 16 SSID
    c. Konfiguracja dostępności danego SSID w zależności od danego zakresu godzin w danym dniu tygodnia
    d. Zarządzanie przez interfejs webowy
    e. Logowanie zdarzeń systemowych
    f. Logowanie zmian w konfiguracji
    g. Obsługa SYSLOG
    h. Monitoring urządzenia i wyświetlanie następujących parametrów: adres MAC, numer seryjny, uruchomione sieci SSID, adres IP, DNS, transmisja danych oraz ilości klientów z ostatniego dnia
    i. Narzędzia wspomagające diagnostykę problemów: ping, traceroute, wyświetlenie tablicy ARP, test przepustowości, mruganie diodami urządzenia
    j. Narzędzie do przechwytywania ruchu do pliku pcap w celu szczegółowej analizy z możliwością ignorowania pakietów broadcast, multicast oraz tworzeniem wyrażeń filtrujących (np., po adresie IP, MAC, itp.)

k. Monitoring urządzeń podłączających się do sieci w zakresie: parametrów radiowych połączenia (siła sygnału, kanał), parametrach IP (adres IPv4, IPv6, MAC, VLAN), parametrach urządzenia (typ/model urządzenia, wspierane standardy radiowe, maksymalna przepustowość, wspierana ilość
l. strumieni przestrzennych), ilości przetransmitowanych danych z podziałem na aplikacje

16. Regulacje i certyfikacje:
    a. Zgodność z dyrektywą RoHS
    b. CE Marked
    c. RED Directive 2014/53/EU
    d. EMC Directive 2014/30/EU
    e. Low Voltage Directive 2014/35/EU
    f. UL/IEC/EN 60950
    g. EN 60601-1-1, EN60601-1-2
    h. Zgodność z UL2043
    i. Certyfikacja Wi-Fi Alliance (WFA):

- Wi-Fi CERTIFIED a, b, g, n, ac
- Wi-Fi CERTIFIED ax
- WPA, WPA2 and WPA3 - Enterprise, Personal
- WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband
- Wi-Fi Location

    j. Bluetooth SIG
    k. Ethernet Alliance (POE, PD device, class 4)

17. Gwarancja i wsparcie techniczne zapewniające dostęp do poprawek i aktualizacji przez okres 60 miesięcy licząc od dnia podpisania protokołu odbioru. W ramach Gwarancji Zamawiający wymaga naprawy wadliwego urządzenia w terminie 3 dni licząc od dnia zgłoszenia wady lub usterki, a w przypadku braku możliwości naprawy wymiany urządzenia na nowe w terminie 7 dni licząc od dnia zgłoszenia.
18. Urządzenia należy dostarczyć z kompletem dedykowanych mocowań producenta umożliwiających montaż AP na płaskich powierzchniach (ściana/sufit)
19. Urządzenia będą zasilane z przełączników PoE będących częścią postępowania (zasilacze DC nie są wymagane).

Radiowy punkt dostępowy zewnętrzny – 3 sztuki

1. Punkt dostępowy musi umożliwiać pracę w jednym z poniższych trybów:
    a. Autonomicznym
    b. Pod kontrolą kontrolera
    c. Pod kontrolą wirtualnego kontrolera (rezydującego na AP)
    d. Remote AP (praca w odległych oddziałach)
    e. Air monitor
    f. Spectrum analyzer
2. W ramach tego postępowania AP będą wdrożone w trybie kontrolerowym z możliwością automatycznej, okresowej konwersji do Air monitor. AP nie może blokować/uniemożliwiać obsługi żadnej z wymienionych funkcjonalności środowiska Wifi opisanej w sekcji dotyczącej kontrolera.
3. Architektura radiowa i obsługa standardów:
    a. Moduł radiowy 802.11 b/g/n

b. Moduł radiowy 802.11 a/n/ac
c. Obsługa MIMO 2x2:2 dla 2,4 GHz i 2x2:2 dla 5Ghz
d. Dwupasmowy moduł radiowy do zastosowań WIDS/WIPS
e. Moduł BLE (Bluetooth Low Energy)
f. Obsługa prędkości PHY dla 5GHz do 866 Mbps
g. Obsługa prędkości PHY dla 2,4GHz do 400 Mbps
h. Maksymalna sumaryczna prędkość do 1.266 Gbps
i. Obsługa kanałów 20,40,80 MHz dla 802.11ac oraz 20,40 MHz dla 802.11n
j. Obsługa MRC i ACC
k. Obsługa agregacji ramek

4. Obsługa zakresów częstotliwości:
   a. 2.400 – 2.4835 GHz
   b. 5.150 – 5.250 GHz (UNII-1)
   c. 5.250 - 5.350GHz
   d. 5.470 - 5.725GHz
   e. 5.725 - 5.875GHz

Możliwość ograniczania zakresów zgodnie z restrykcjami kraju zastosowania.

5. Konfigurowalna moc nadajnika (agregowalna) :
   a. Dla pasma 2,4 GHz: do 21 dBm
   b. Dla pasma 5 GHz: do 25 dBm

Regulacja z dokładnością do 0,5 dBm

6. Zasilanie:
   a. PoE (IEEE 802.3af) na złączu RJ45, zużycie energii: max 12,5 W

7. Parametry fizyczne i anteny:
   a. Obudowa metalowa, wodoodporna i wiatroodporna, praca w pełnym słońcu spełniające wszelkie wymagania standardów:

- IP66/67
- ASTM B117-07A
- EN 300 019

Potwierdzona certyfikacją na zgodność z wymaganiami

   b. Praca w trudnych warunkach atmosferycznych
   c. Odporność na wibracje i trzęsienia ziemi (zgodność z IEC 60068-2-64/-27/-6)
   d. Temperatura pracy: -40 do +55 ^{0}C
   e. Zintegrowane wewnętrzne anteny dookólne o zysku minimum 2.7 dBi dla 2.4 GHz oraz 4.3 dBi dla 5 GHz
   f. Sygnalizacyjne diody LED

8. Interfejsy:
   a. Port Ethernet RJ45 zdolny do pracy w trybie 10/100/1000 Base-T
   b. port konsoli
   c. przycisk Resetu urządzenia (ustawienia fabryczne)

9. Mechanizmy bezpieczeństwa:
   a. WEP, WPA, WPA2 Personal i Enterprise (802.1X)
   b. Szyfrowanie TKIP oraz AES

c. Szyfrowanie IPSec w celu tunelowania danych do koncentratora VPN
d. Tagowanie VLAN (IEEE 802.1q)
e. Blokowanie ruchu między klientami bezprzewodowymi
f. Wbudowany firewall warstwy 3-7
g. Firewall warstwy 7 umożliwia wykrywanie i blokowanie lub limitowanie pojedynczych aplikacji oraz grup aplikacji danego typu: blogi, email, współdzielenie plików, wiadomości, gry, p2p, portale społecznościowe i współdzielenie zdjęć, aktualizacja oprogramowania, sport, wideo i muzyka, konferencje audio i wideo
h. Firewall warstwy 7 umożliwia blokowanie określonych stron http, zakresów adresów IP/portów
i. Zintegrowany system wykrywania włamań, wrogich AP i reagowania na nie (wIPS/wIDS)

10. Funkcje modułu WIPS/WIDS:
    a. Skanowanie pasma 2,4 GHz oraz 5 GHz w czasie rzeczywistym
    b. Detekcja wrogich AP
    c. Wykrywanie podłączenia wrogiego AP do sieci LAN
    d. Klasyfikacja ataków w zależności od stopnia zagrożenia
    e. Klasyfikacja ataków w oparciu o sygnatury bazujące na typie i profilu zachowania (podstawowe ataki to: spoofing, DoS, packet flood)
    f. Konfiguracja polityki reagowania na ataki
    g. Prowadzenie logu zdarzeń

11. Mechanizmy QoS:
    a. DSCP
    b. 802.1p
    c. Advanced Power Save (U-APSD)
    d. IEEE 802.11e oraz WMM
    e. Limitowanie ruchu per klient oraz per SSID
    f. Rozpoznawanie aplikacji w warstwie 7
    g. Limitowanie wybranego typu ruchu aplikacyjnego per klient oraz per SSID z możliwością markowania ruchu
    h. Mechanizm preferowania pasma 5 GHz dla klientów dwuzakresowych
    i. Mechanizm analizy widma częstotliwości z możliwością graficznej prezentacji pracujący w obu zakresach częstotliwości

12. Mechanizmy mobilności:
    a. 802.11k oraz 802.11r
    b. PMK oraz OKC dla szybkiego roamingu L2
    c. Roaming L3

13. Mechanizmy analityczne:
    a. Zbieranie informacji o urządzeniach w zasięgu sieci radiowej z podziałem na urządzenia/klientów podłączonych do sieci, będących w jej zasięgu oraz przemieszczających się w jej zasięgu

b. Zbieranie informacji o długości czasu wizyty urządzeń/klientów w zasięgu sieci radiowej
c. Zbieranie informacji o powtarzalności wizyt urządzeń/klientów
d. Prezentacja graficzna zebranych informacji
e. Export danych analitycznych w formie pliku CSV

14. Obsługa dostępu gościnnego:
    a. Przekierowanie użytkowników danego SSID na portal logowania
    b. Personalizacja wyglądu portalu logowania
    c. Kreowanie i zarządzanie kontami gościnnymi przez interfejs webowy
    d. Uwierzytelnianie do sieci za pośrednictwem: akceptacji portalu, uwierzytelniania SMSem, serwera LDAP, serwera RADIUS, serwera Active Directory, kont z portalu Facebook

15. Funkcje ogólne:
    a. Automatyczne budowanie sieci kratowej (formowanie połączeń do innych punktów dostępowych w oparciu o radio 2,4GHz lub 5 GHz bez podłączenia do sieci kablowej)
    b. Konfiguracja do 16 SSID
    c. Konfiguracja dostępności danego SSID w zależności od danego zakresu godzin w danym dniu tygodnia
    d. Zarządzanie przez interfejs webowy
    e. Logowanie zdarzeń systemowych
    f. Logowanie zmian w konfiguracji
    g. Obsługa SYSLOG
    h. Monitoring urządzenia i wyświetlanie następujących parametrów: adres MAC, numer seryjny, uruchomione sieci SSID, adres IP, DNS, transmisja danych oraz ilości klientów z ostatniego dnia
    i. Narzędzia wspomagające diagnostykę problemów: ping, traceroute, wyświetlenie tablicy ARP, test przepustowości, mruganie diodami urządzenia
    j. Narzędzie do przechwytywania ruchu do pliku pcap w celu szczegółowej analizy z możliwością ignorowania pakietów broadcast, multicast oraz tworzeniem wyrażeń filtrujących (np., po adresie IP, MAC, itp.)
    k. Monitoring urządzeń podłączających się do sieci w zakresie: parametrów radiowych połączenia (siła sygnału, kanał), parametrach IP (adres IPv4, IPv6, MAC, VLAN), parametrach urządzenia (typ/model urządzenia, wspierane standardy radiowe, maksymalna przepustowość, wspierana ilość
    l. strumieni przestrzennych), ilości przetransmitowanych danych z podziałem na aplikacje

16. Regulacje i certyfikacje:
    a. Zgodność z dyrektywą RoHS
    b. CE Marked
    c. EN 300 328
    d. EN 301 489
    e. EN 301 893
    f. Low Voltage Directive 72/23/EEC
    g. UL/IEC/EN 60950

h. EN 60601-1-1, EN60601-1-2
i. Certyfikacja Wi-Fi Alliance (WFA):

- Wi-Fi CERTIFIED a, b, g, n, ac
- WPA, WPA2 - Enterprise, Personal
- WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband

j. Bluetooth SIG

17. Gwarancja i wsparcie techniczne zapewniające dostęp do poprawek i aktualizacji przez okres 60 miesięcy licząc od dnia podpisania protokołu odbioru. W ramach Gwarancji Zamawiający wymaga naprawy wadliwego urządzenia w terminie 3 dni licząc od dnia zgłoszenia wady lub usterki, a w przypadku braku możliwości naprawy wymiany urządzenia na nowe w terminie 7 dni licząc od dnia zgłoszenia .
18. Urządzenia należy dostarczyć z kompletem dedykowanych mocowań producenta umożliwiających montaż AP na długim ramieniu, ramię mocowane do ściany lub masztu.
19. Urządzenia będą zasilane z przełączników PoE będących częścią postępowania (zasilacze DC nie są wymagane).

UTM – 1 szt.

Typ systemu ochrony:

1. System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.
2. Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).
3. Wymagania systemowe:

System ochrony powinien spełniać wymagania w niżej wymienionym zakresie.

- Obsługa nielimitowanej ilości hostów w sieci chronionej
- Metalowa obudowa o wysokości 1U przeznaczona do montażu w szafie RACK
- Minimalna liczba i typ interfejsów fizycznych:

8 x 1GbE RJ45 (IEEE 1000Base-T)
2 x 1GbE SFP
2 x 10GbE SFP+

- Minimalnie dodatkowe porty: 3x USB 3.0 , 1x Konsola szeregowa (RJ-45 lub DB9), 1x HDMI
- Wyświetlacz LCD na przednim panelu z podstawowymi informacjami statusowymi

i konfiguracyjnymi
- Minimalna liczba i typ interfejsów wirtualnych: 100 (IEEE 802.1Q)
- Minimalna liczba nowych połączeń na sekundę: 200 000
- Minimalna liczba jednoczesnych połączeń: 17 000 000
- Minimalna przepustowość Firewall: 28 Gbps
- Minimalna przepustowość IPS: 5,5 Gbps
- Minimalna przepustowość NGFW (IPS+ App control + Web Filter): 4,5 Gbps
- Minimalna przepustowość VPN: 2,75 Gbps
- Ilość użytkowników nielimitowana
- Zintegrowany dysk SSD do przechowywania oprogramowania, logowania i raportowania o pojemności nie mniejszej niż 180 GB
- wolny slot do rozbudowy o dodatkowe moduły interfejsów sieciowych z możliwością rozbudowy miedzy innymi o:
8 x port GbE copper 8 x port
GbE SFP
2 x port 10 GbE SFP+
4 x port 10 GbE SFP+
2 x port 40 GbE QSFP+ 4 x port
GbE PoE
8 x port GbE PoE

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY
Zarządzanie i utrzymanie:
1. Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI). Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup. Interfejs
graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.
2. Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.
3. dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
4. System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.
5. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
6. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.
7. System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.
8. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.

9. Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.
10. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.
11. Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3.
12. System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych).
13. System powinien oferować możliwość integracji z centralnym systemem do zarządzania.
14. Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego lub via email.
15. Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.
16. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.
17. Zarządzanie subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud
18. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).
19. System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.
20. W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej funkcji oprogramowania (w tym na drugie urządzenie).

Zapora sieciowa, konfiguracja sieciowa oraz routing:

1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.
2. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas.
3. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
4. Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług.
5. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.
6. System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN.
7. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.
8. Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.
9. System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
10. System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking).
11. System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).

12. Rozwiązanie powinno zapewniać obsługę routingu statycznego.
13. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).
14. System powinien oferować wsparcie dla IGMP snooping.
15. Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy).
16. Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.
17. System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.
18. System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP.
19. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
20. Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.
21. Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules.
22. Wymagane jest by rozwiązanie zapewniało obsługę modemów USB 3G/LTE/UMTS.
23. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
24. System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP.
25. System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania.
26. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).

Podstawowe kształtowanie pasma oraz limity ilości danych:

1. System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.
2. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.
3. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.

Bezpieczna sieć bezprzewodowa:

1. System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania.
2. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater.
3. Wdrożenie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play , gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu.
4. Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej.
5. Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej.
6. Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej.
7. Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise.
8. Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication).
9. Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition).
10. System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów.
11. Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła

dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości.
12. System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden.
13. System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy
czasowe.
14. Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów
sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych.

Autoryzacja użytkowników:

1. Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.
2. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.
3. System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i
TACACS+.
4. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.
5. Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time
Password).
6. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie
Single Sign On (SSO) w środowisku opartym o Windows Terminal Server.
7. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania
(klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.
8. Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.
9. Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal.

Samoobsługowy portal dla użytkowników:

1. Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci.
2. Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).
3. Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows.
4. Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android.
5. Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła.
6. Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika.
7. Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.

Podstawowe opcje VPN:

1. System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:
- Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK),
- Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).

Klient IPSec VPN (dostępny osobno):

1. Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH.
2. Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512.
3. Wsparcie dla split-tunneling.
4. Wsparcie dla NAT-traversal.
5. Monitorowanie stanu połączenia.

OCHRONA SIECI

IPS:

1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 7000 sygnatur. Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów. System powinien generować alerty w przypadku wykrycia ataku.

ATP:

1. System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.

Synchronizacja z endpoint:

1. System powinien mieć możliwość rozbudowy uruchomienia synchronizacji stanu bezpieczeństwa komputerów w sieci LAN z Firewallem. Możliwość automatycznego odcięcia komputera/ów zainfekowanych. (wymagane dodatkowe oprogramowanie nie będące częścią tego postępowania).

Clientless VPN:

1. Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5.

OCHRONA I KONTORLA WEB ORAZ APLIKACJI

Ochrona i kontrola Web:

1. Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.
2. Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).
3. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.
4. System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego.
5. Rozwiązanie powinno automatyczne odpytywać bazy producenta w trybie rzeczywistym.
6. Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch).
7. Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów.
8. System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma.
9. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
10. Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , cookies.
11. System powinien zapewniać możliwość emulacji skryptów JavaScript.
12. Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
13. Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.

14. Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.
15. Rozwiązanie powinno umożliwiać blokadę stron HTTPS.
16. Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS.
17. Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do Internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.
18. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji.

Ochrona i kontrola aplikacji:
1. Rozwiązanie powinno oferować bazę danych opisująca, co najmniej 2 500 aplikacji.
2. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.
3. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.
4. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
5. Rozwiązanie powinno umożliwiać blokowanie:
- aplikacji, które pozwalają na transfer plików (np. P2P).
- komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.
- proxy uruchamianych poprzez przeglądarki internetowe.
- streaming media (radio internetowe, Youtube, Vimeo).
6. Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo.

Kształtowanie pasma dla Web i Aplikacji:
1. Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie.
2. Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.
3. Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym oraz współdzielonym.

OCHRONA I KONTROLA EMAIL

Ochrona i kontrola Email:
1. Rozwiązanie powinno oferować możliwość wyboru trybu pracy: Transparent Email Proxy lub Mail Transfer Agent.
2. System powinien umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS.
3. Rozwiązanie powinno zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
4. System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.
5. Rozwiązanie powinno automatyczne odpytywać bazy producenta w trybie rzeczywistym.
6. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur zagrożeń.
7. System powinien zapewniać wykrywanie, blokowanie i skanowanie załączników.
8. Rozwiązanie musi umożliwiać akceptowanie lub odrzucanie wiadomości przekraczających określony przez administratora rozmiar.
9. System powinien wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści wiadomości.
10. Rozwiązanie powinno oferować ochronę przed wyciekiem danych (DLP) na podstawie predefiniowanych wzorców lub kryteriów zdefiniowanych przez administratora.
11. System powinien oferować mechanizm analizy ruchu szyfrowanego TLS dla SMTP, POP oraz IMAP.
12. Rozwiązanie powinno umożliwiać dodanie stopki do każdej wiadomości wychodzącej.
13. Rozwiązanie powinno umożliwiać archiwizowanie wiadomości email.

14. Rozwiązanie powinno współpracować, z co najmniej dwoma bazami RBL.
15. Rozwiązanie powinno umożliwiać tworzenie białych i czarnych list adresów IP i email.
16. Rozwiązanie powinno zapewniać wykrywanie spamu niezależnie od stosowanego języka.
17. Rozwiązanie powinno blokować spam w postaci plików graficznych np. wiadomości z tekstem osadzonym w obrazku.

Kwarantanna Email:
1. System powinien zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako spam z opcją powiadamiania użytkownika.
2. System powinien zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako zainfekowane przez malware.
3. Rozwiązanie powinno zapewniać możliwość przeglądania kwarantanny z opcją wyszukiwania wiadomości i opcjami filtrowania po dacie, nadawcy, odbiorcy, temacie wraz z opcją zwalniania lub usuwania wiadomości z kwarantanny (przez samoobsługowy portal użytkownika).

OCHRONA SERWERÓW APLIKACYJNYCH WEB
WAF:
1. Dodatkowy moduł ochrony klasy Web Application Firewall.
2. Funkcjonalność oparta o mechanizm Reverse Proxy.
3. Rozwiązanie powinno oferować mechanizm URL hardening with deep-linking and directory traversal prevention.
4. Rozwiązanie powinno oferować mechanizm Form hardening.
5. Rozwiązanie powinno oferować ochronę przed SQL injection.
6. Rozwiązanie powinno oferować ochronę przed Cross-site scripting.
7. System powinien zapewniać inspekcję ruchu HTTP oraz HTTPS (SSL).
8. System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.
9. System powinien pozwalać na podpisywanie plików cookies.
10. Rozwiązanie powinno oferować wsparcie dla Path-based routing.
11. Rozwiązanie powinno oferować wsparcie dla Outlook Anywhere.
12. Mechanizm Reverse authentication z automatycznym dodawaniem prefixu lub suffixu w trakcie autoryzacji użytkownika.
13. Rozwiązanie umożliwiające publikowanie aplikacji web w Internecie na zasadzie wirtualnych serwerów aplikacyjnych.
14. Rozwiązanie powinno oferować mechanizm rozkładający ruch odwiedzających między rzeczywiste serwery aplikacyjne (Load Balancing).
15. System powinien umożliwiać stosowania masek typu wildcard dla ścieżek dostępowych.
16. System powinien umożliwiać stosowanie operatorów logicznych AND/OR.

OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY
On-cloud Sandboxing:
1. Rozwiązanie powinno posiadać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox umożliwiający dodatkową inspekcję plików wykonywalnych w tym .exe, .com, .dll.
2. Rozwiązanie umożliwiające dodatkową inspekcję plików dokumentów w tym .doc, .docx, .docm, .rtf.
3. Rozwiązanie umożliwiające dodatkową inspekcję plików .pdf.
4. Rozwiązanie umożliwiające dodatkową inspekcję plików archiwów w tym: .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.
5. System zapewniający dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows i MacOS.
6. System ochrony ze średnim realnym czasem analizy kodu poniżej 120 sekund.
7. System powinien oferować szczegółowe raporty wyników analizy.

LOGOWANIE I RAPORTOWANIE

1. System powinien umożliwiać składowanie oraz archiwizację logów.
2. System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych

aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.

3. System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.
4. System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
5. System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
6. Rozwiązanie powinno umożliwiać wysyłanie raportów via email.
7. Rozwiązanie powinno generować raporty w PDF, HTML i XLS.
8. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych, do co najmniej 3 serwerów syslog.
9. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.
10. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.
11. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.
12. System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora.
13. System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.

POZOSTAŁE

Certyfikaty: CE, FCC Class A, CB, VCCI, C-Tick, UL, CCC.

1. Oferowane rozwiązanie powinno być objęte serwisem gwarancyjnym przez okres 60 Miesięcy. W przypadku wady lub usterki Wykonawca zobowiązany jest do naprawy , lub wymiany urządzenia na nowe niewadliwe.

.

Serwis powinien być realizowany przez podmiot posiadający autoryzację producenta w zakresie serwisu gwarancyjnego (oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu

gwarancyjnego).

2. Obsługa gwarancyjna na sprzęt powinna być prowadzona w trybie 24 godziny przez 7 dni w tygodniu. W przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od stwierdzenia awarii. W przypadku wymiany urządzenie musi mieć możliwość usunięcia dysku SSD przed jego odesłaniem do wykonawcy bez utraty gwarancji.
3. Wsparcie techniczne do oprogramowania powinno być prowadzone przez wykonawcę w trybie 24 godziny przez 7 dni w tygodniu. W ramach wsparcia technicznego wykonawca zobowiązany jest do dostarczania aktualizacji i poprawek oprogramowania dla wszystkich dostarczonych modułów.
4. Urządzenie oraz wszystkie podzespoły muszą być dostarczone w stanie fabrycznie nowym, wolnym od wad technicznych, prawnych i formalnych wraz z zainstalowanym oprogramowaniem systemowym.
5. Urządzanie musi być dostarczone wraz z oprogramowniem umożliwiającymi aktywację niżej wymienionych funkcjonalności na okres minimum 12 miesięcy od daty uruchomienia systemu i są one integralnym elementem całego postępowania:

- Zapora sieciowa oraz routing;
- Ochrona sieci bezprzewodowej;
- Autentykacja użytkowników;
- Ochrona sieci realizowana poprzez technologie IPS, ATP oraz Sandboxing;
- Ochrona i kontrola ruchu webowego;
- Ochrona i kontrola aplikacji;
- Logowanie i raportowanie;

6. Pozostałe funkcjonaliści systemu mogą zostać odblokowane przez Zamawiającego w dowolnym momencie po zakupieniu i instalacji dodatkowych funkcjonalności systemowych, nie będących jednak częścią obecnego postepowania, ale bez konieczności wymiany urządzania na nowe.

Przełącznik dystrybucyjny – 1 sztuka

1. Przełącznik powinien mieć budowę modułową umożliwiającą dostosowanie ilości i typu portów do potrzeb zamawiającego oraz przyszłą rozbudowę poprzez dołożenia lub zmianę modułów.
   Przełącznik powinien umożliwiać posiadanie portów:
   a. 144 portów gigabitowych miedzianych
   b. 144 portów gigabitowych miedzianych PoE+
   c. 144 portów SFP
   d. 48 portów 10-gigabitowych SFP+,
   e. 48 portów miedzianych 1/2,5/5/10-gigabitowych z negocjacją prędkości oraz obsługą standardu PoE+,
   f. 12 portów 40-gigabitowych
   g. lub kombinacji powyższych typów portów
2. Obudowa wieżowa Rack o wysokości maksymalnie 4U umożliwiająca instalację w szafie 19", głębokość urządzenia nie większa jak 46 cm
3. Przełącznik należy wyposażyć w stosowne moduły tak aby sumarycznie posiadał następującą konfigurację portów:
   a. 100 portów RJ-45 z autonegocjacja 10/100/1000 (IEEE 802.3 typu 10Base-T, IEEE 802.3u typu 100Base-TX, IEEE 802.3ab typu 1000Base-T); duplex 10Base-T/100Base-TX: pół lub pełny duplex; 1000Base-T - tylko pełny; wsparcie dla IEEE 802.3at PoE+ (30W per port)
   b. 16 portów 10Gigabit Ethernet SFP+
   c. 4 porty miedziane 1/2,5/5/10Gigabit z negocjacją prędkości oraz obsługą standardu PoE+,
   d. 1 port szeregowy konsoli RJ45 lub USB
   e. 1 port zarządzający RJ45 ethernet OOBM
   f. Przynajmniej jeden wolny slot na dodatkowy moduł
4. Przełącznik musi posiadać moduł zarządzający pełniący funkcję kontrolera całości oraz architekturę nie blokującą zdolną obsłużyć ruch ze wszystkich portów jednocześnie w obu kierunkach.
5. Moduł zarządzający musi umożliwiać redundancję i jego wymianę w przypadku uszkodzenia w trybie hot-swap. Przełącznik należy dostarczyć wraz z drugim redundantnym modułem zarządzającym (co powoduje zdublowanie portów konsolowego i OOBM).
6. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 2 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster).

7. Zarządzanie:
    a. CLI
    b. WWW
    c. telnet/ssh
    d. pozapasmowe konsolowe (port szeregowy RS-232C - RJ45),
    e. dedykowany port Ethernet do zarządzania OOBM
    f. możliwość scentralizowanego zarządzania zarówno przez dedykowane oprogramowanie producenta jak i chmurowo
8. Warstwa przełączania – Layer 3
9. Rozmiar tablicy adresów MAC- minimum 64000
10. Tablica routingu:
    a. 10000 wpisów dla IPv4
    b. 5000 wpisów dla IPv6
11. Obsługa protokołów routingu:
    a. routing statyczny,
    b. RIP v1,
    c. RIP v2,
    d. OSPF,
    e. OSPFv3,
    f. VRRP,
    g. PIM-SM,
    h. PIM-DM,
    i. BGP
    j. Virtual Router Redundancy Protocol (VRRP)
12. Prędkość magistrali: 960 Gbps
13. Przepustowość: 570 Mpps
14. Parametry jednostki centralnej przełącznika:
    a. Dual Core, taktowanie procesora minimum 1200MHz
    b. Pamięć flash minimum 16MB
    c. Pamięć SD minimum 1GB
    d. Pamięć RAM minimum 4GB DDR3
15. Opóźnienie poniżej 2.8 µs dla 1000 Mbit
16. Bufor pakietów minimum 13 MB na moduł
17. VLAN
    a. Pełna zgodność z IEEE 802.1Q
    b. 4094 VLAN IDs
    c. Do 4094 VLANów jednocześnie
    d. Obsługa MAC forwarding table per vlan
    e. Wsparcie dla IEEE 802.1ad Q-in-Q
    f. Wsparcie dla VxLAN
18. Funkcje wysokiej dostępności:
    a. Spanning Tree (802.1d)
    b. Rapid Convergence Spanning Tree (802.1w)
    c. Muliple Spanning Tree (802.1s)
    d. Rapid Per-VLAN Spanning Tree (RPVST+)
    e. GVRP and MVRP
19. Agregacja portów zgodna z 802.3ad LACP
    Obsługa dystrybuowanych łączy agregowanych LACP – łączy agregowanych wychodzących z dwóch, różnych, niezależnych i oddzielnie zarządzanych (nie połączonych w stos) przełączników (tzw. Multi-chassis Link Aggregation, MLAG, MC-LAG, Distributed Trunking).
20. Funkje QoS:
    a. priorytetyzacja zgodna z 802.1p,
    b. Class of Service (CoS) priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port and DiffServ ToS

    c. Layer 4 prioritization TCP/UDP
    d. wsparcie dla 4 kolejek,
    e. rate-limiting
    f. Voice VLAN
    g. IP SLA for voice
21. Monitorowanie:
    a. RMON 4 grupy statistics, history, alarm, events,
    b. SFLOW
    c. XRMON
22. Inne funkcje i funkcjonalności:
    a. LLDP
    b. LLDP-MED
    c. dual flash images
    d. obsługa ramek typu Jumbo
    e. iSCSI
    f. DHCP snooping
    g. DHCP Server
    h. BPDU Guard
    i. BPDU Protection
    j. port isolation
    k. wsparcie dla IPv4 i Ipv6
    l. Tunneled node dla ruchu z AP
    m. Zero Touch Provisioning
    n. Access control lists (ACL)
    o. Dynamic ARP protection
    p. Bidirectional Forwarding Detection (BFD)
    q. Unidirectional link detection (UDLD)
    r. 802.1AE MACsec.
23. Autentyfikacja użytkowników:
    a. IEEE 802.1X
    b. Web-based authentication
    c. Supports MAC-based authentication
    d. RADIUS/TACACS+ support
24. Zasilanie z zasilaczy hot-swap. Przełącznik powinien posiadać dwa sloty na zasilacze i umożliwiać instalację zasilaczy o różnych mocach w zależności od zapotrzebowania na moc PoE. Przełącznik należy dostarczyć z dwoma redundantnymi zasilaczami minimum 1100W każdy. Zasilacze powinny spełniać normę 80Plus Gold.
25. Chłodzenie aktywne z przepływem powietrza w kierunku przód-tył obudowy. Wentylatory na wymiennym module hot-swap.
26. Przełącznik musi być przystosowany do środowiska pracy od 0°C do 45°C
27. Przełącznik należy dostarczyć wraz z wkładkami SFP+ dla standardu 10G Base-SR w ilości sztuk 14. Wkładki musza być dedykowanym rozwiązaniem producenta i objęte tą samą gwarancją co przełącznik.
28. Gwarancja i wsparcie techniczne min 60 miesięcy zapewniające dostęp do poprawek i aktualizacji Gwarancja wymiany wadliwego urządzenia w trybie NBD (następny dzień roboczy) z wysyłką urządzenia na wymianę następnego dnia roboczego od zgłoszenia.

Załącznik 1a do SIWZ – koncepcja rozmieszczenia AP w Centrum Sztuki Współczesnej w Zamku Ujazdowskim

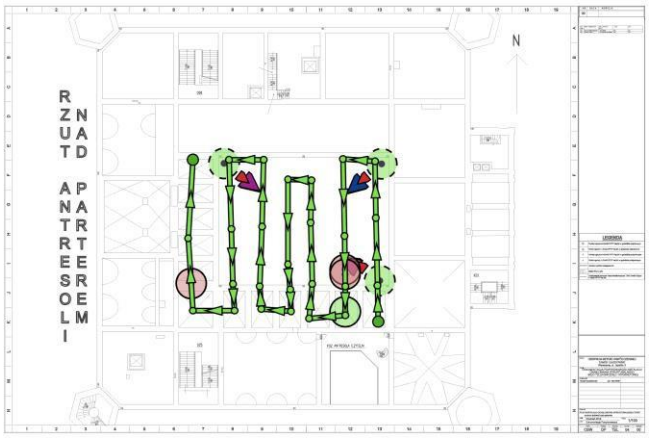
Centrum Sztuki Współczesnej Zamek Ujazdowski koncepcja rozmieszczenia AP

Raport składa się z trzech części:

1. Wyniki pomiaru oraz nałożone na nie teoretyczne pokrycie zasięgiem części antresola – centrum dziedzińca
2. Wyniki teoretycznej koncepcji rozmieszczenia AP na wybranych ściśle określonych częściach elektroniczna tj.:
   - Piwnica (sala wystawowa: P02, P03, P04, P06)
   - Parter (kino: 024, czytelnia: 023, sala edukacyjna: 021, hala główny: 001, księgarnia: 002, sala wystawowa: 005, 013, 015, 019, 032)
   - Piętro I (Sala wystawowa: 101, 102, 103, 108, 110, 112, 114, 116, 117, 120, 121)
   - Piętro II (Pokoje biurowe: 209, 225, 272, 242, korytarze: 204, 261, 249, 230, 215)
3. Wyniki pomiaru w problematycznych miejscach elektroniczna z punktu widzenia propagacji fal Integrator

1. wyniki pomiaru oraz nałożone na nie teoretyczne pokrycie zasięgiem części antresola – centrum dziedzińca

Trasy pomiarowe i punkty Dostępowowe do Centrum Sztuki Współczesnej Zamek Ujazdowski



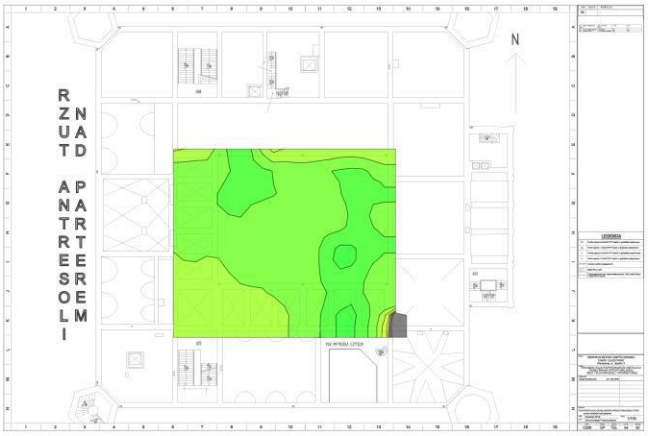
Zapotrzebowanie na pokrycie: **głos + dane**	Siła sygnału min	**-67,0 DBM**
	Stosunek sygnałudoszumu min	**20,0 w DB**
	Szybkość transmisji danych min	**20 MB/s**
	Liczba punktów Dostępowych min	**2 at min.-75,0 DBM**
	Nakładanie kanałów maks .	**2 at min.-85,0 DBM**
	Czas błądzenia (RTT) maks .	**200ms**
	Utrata pakietów Max	**2,0%**

Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia i niskie dane przepływności.

Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepustowość.



Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek ujazdowski w paśmie 2,4 GHz

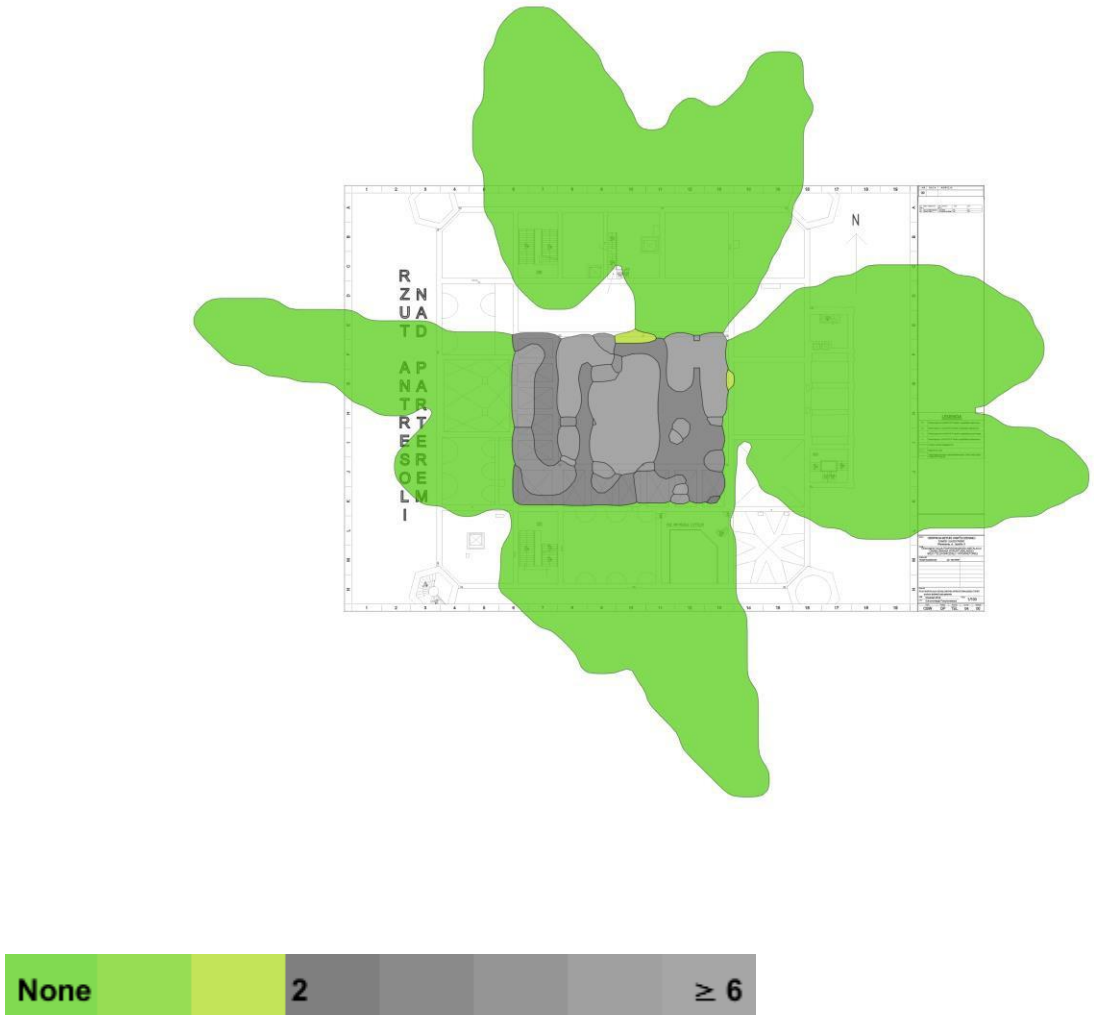
Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR grEater niż zero), aby możliwe było przesyłanie danych

Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR greaTer niż zero), aby możliwe było przesyłanie danych

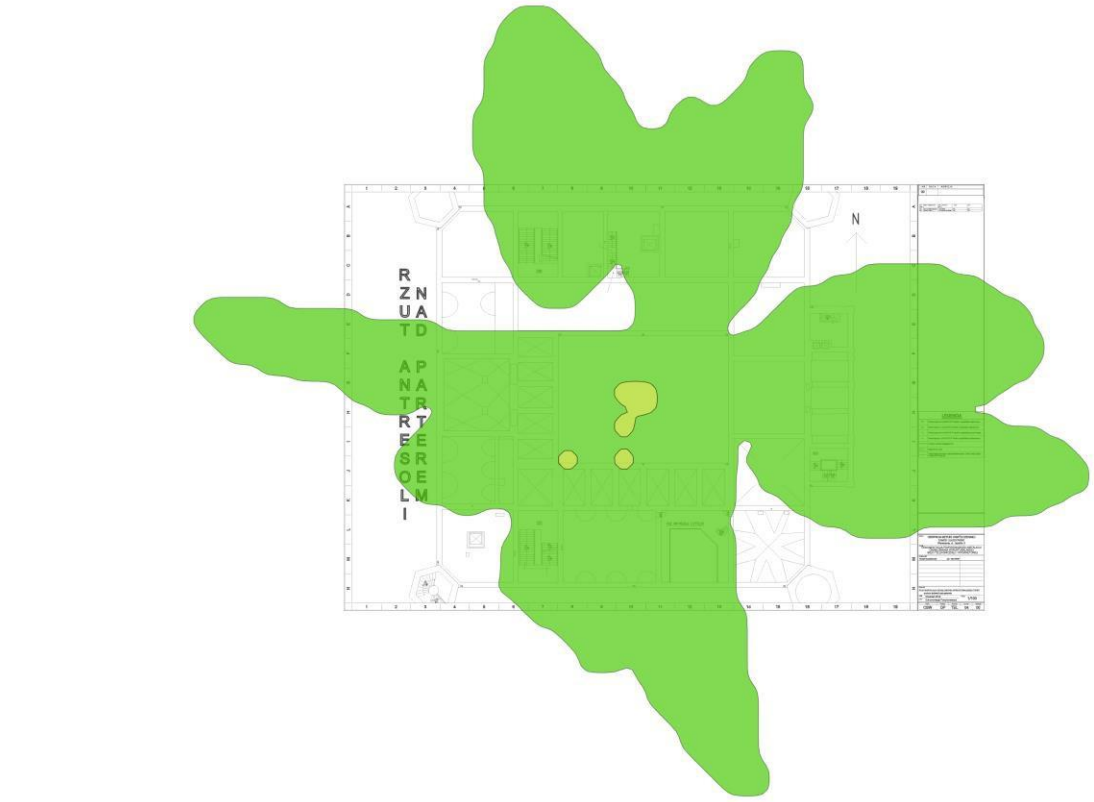
Kanał nakładania dla Centrum Sztuki Współczesnej Zamek Ujazdowski na 2.4 Pasmo GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



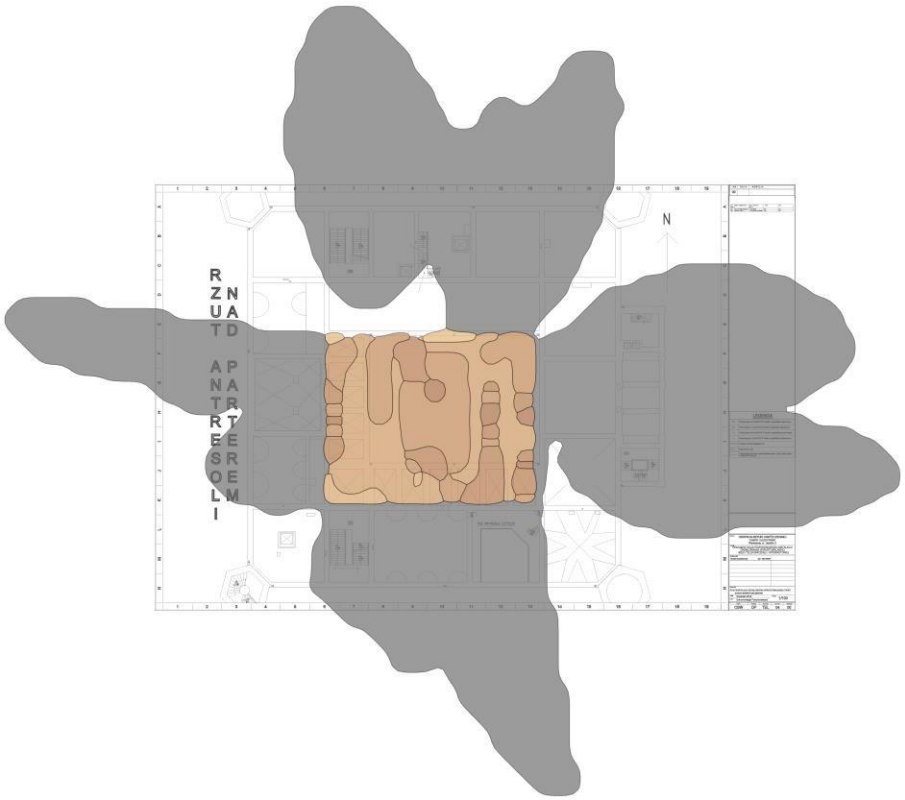
Nakładanie kanałów dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



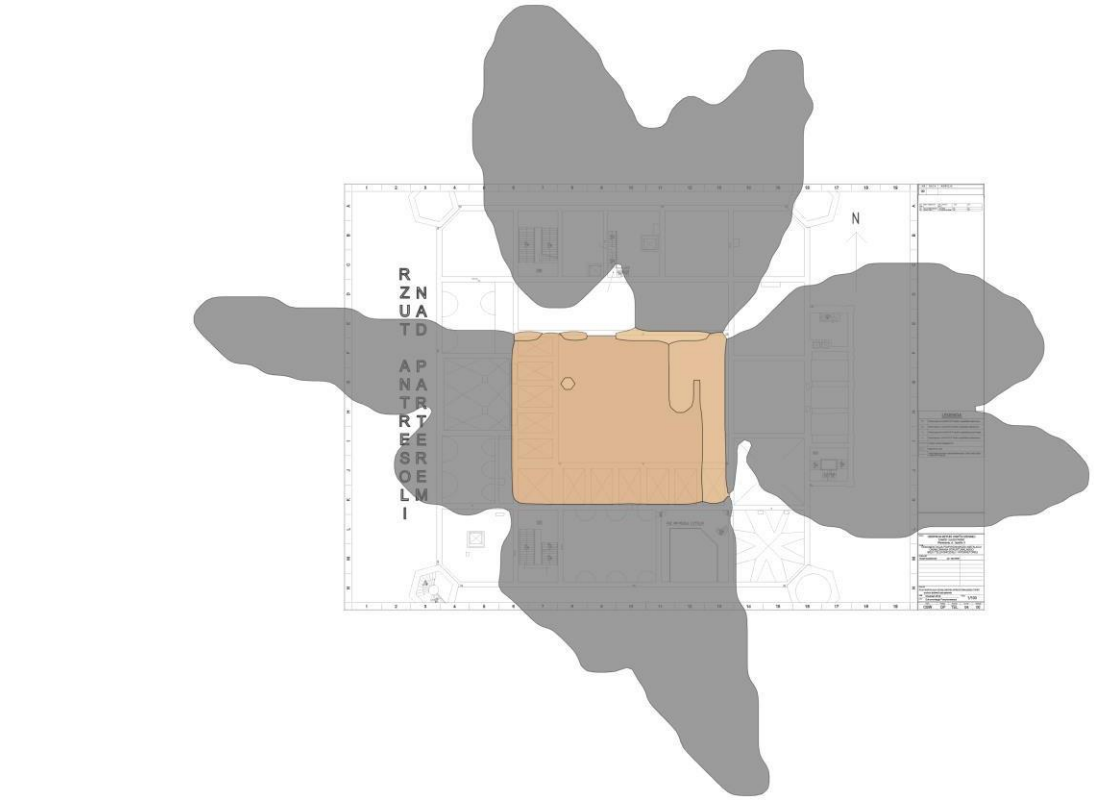
Ilość punktów dla centrum sztuki współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



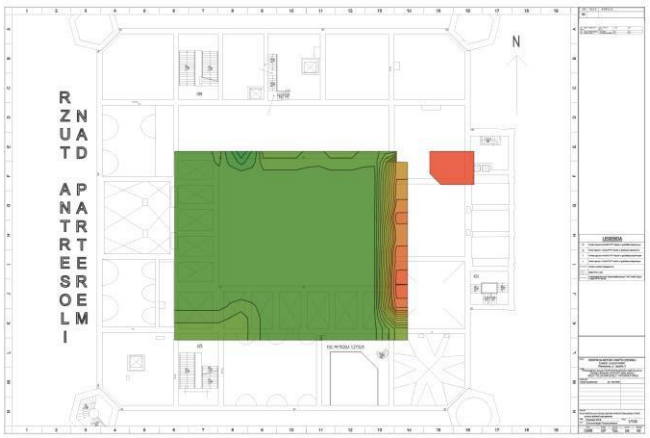
Liczba punktów dostępowy dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



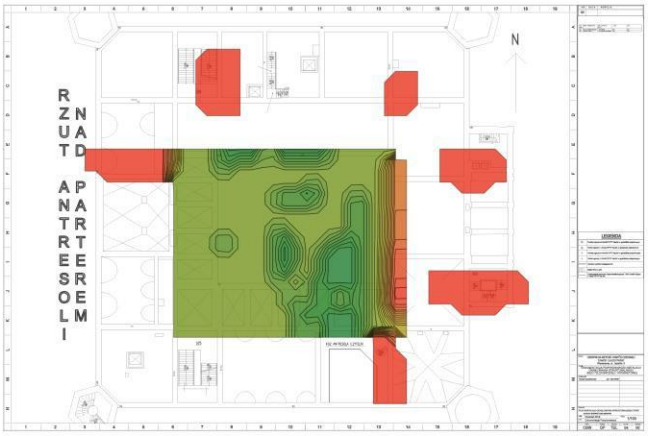
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski na paśmie 2,4 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)



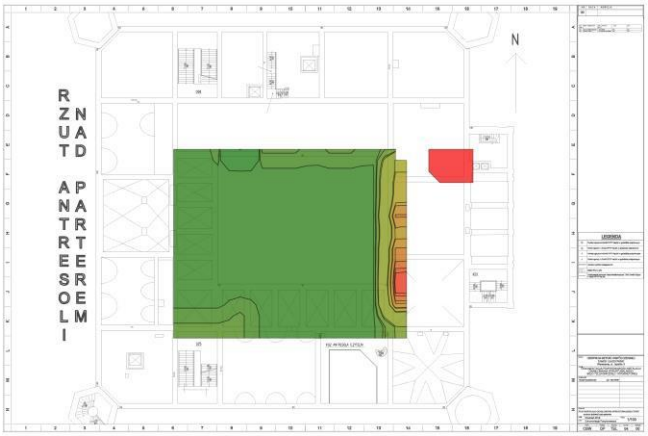
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)
,



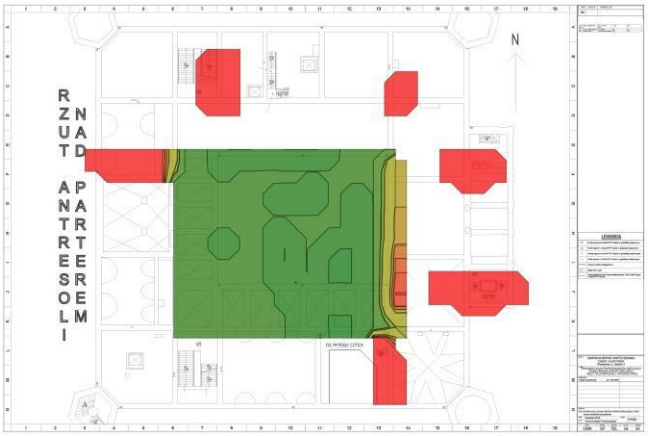
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Wyświetla zmierzoną przepustowość.



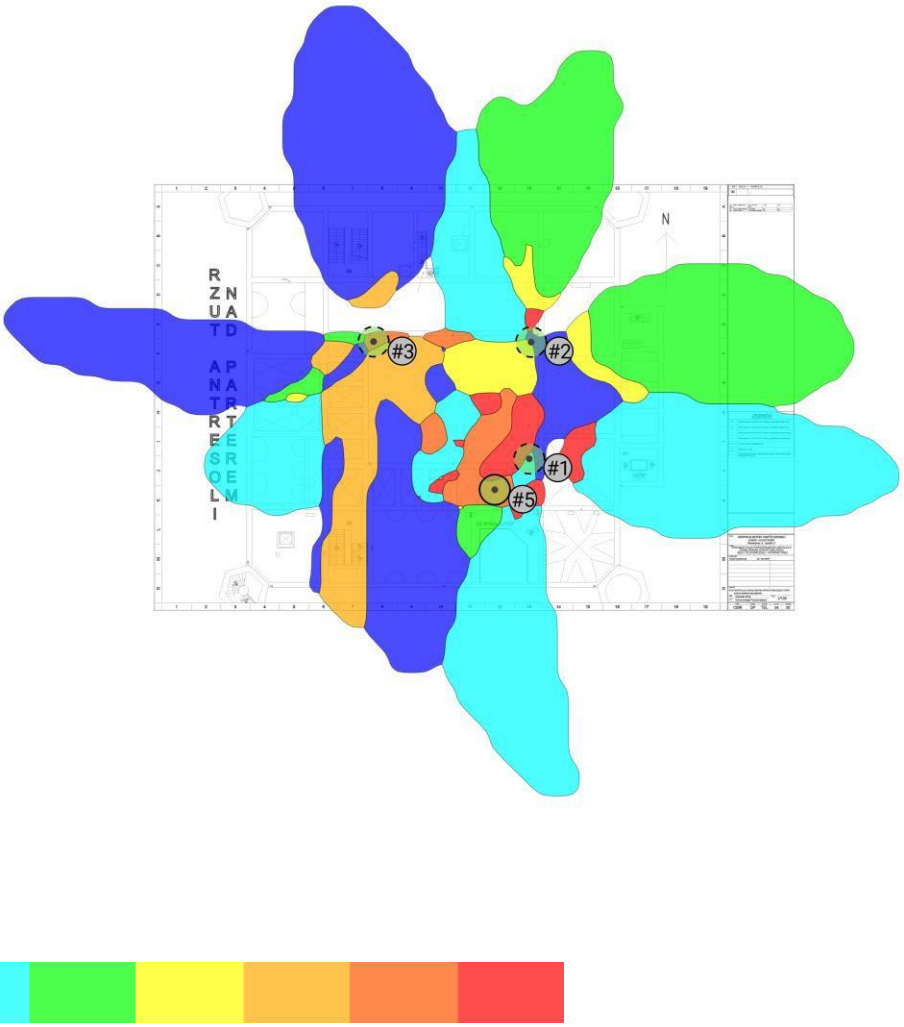
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Wyświetla zmierzoną przepustowość.



Powiązany punkt dostępowy dla centrum sztuki współczesnej zamek Ujazdowski

Wyświetla punkt dostępu , z którym jest skojarzone urządzenie klienckie . Obraz pokazuje przewidywane siły sygnału skojarzenia

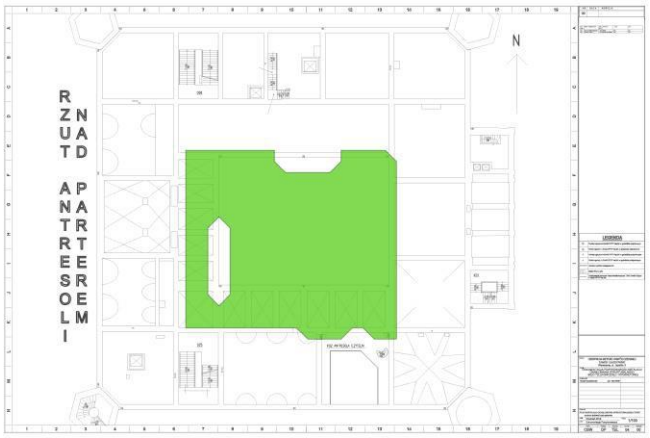


AP	Punkt dostępowy			
1	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	52	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

2	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standard u 802.11 AC	136	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
3	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standard u 802.11 AC	60	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
5	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: B4:2C: C0 C8: B5: AD: B4:2C: C0	IAP22 8 IAP22 8
	standardu 802.11 AC standardu 802.11 AC	100 100	C8: B5: AD: B4:2C: d0 C8: B5: AD: B4:2C: d0	IAP22 8 IAP22 8

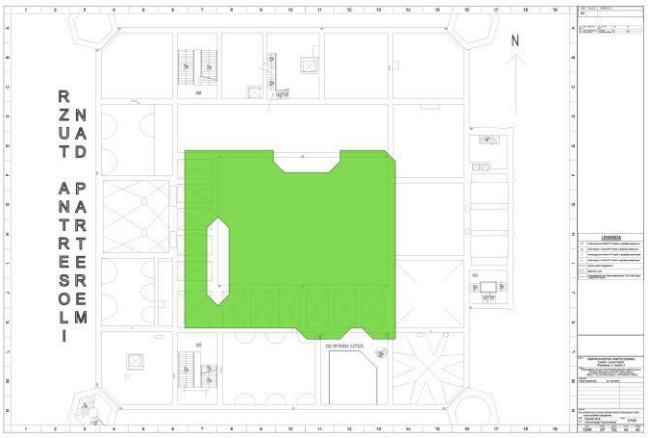
Wykorzystanie widma dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Wykorzystanie widma pokazuje czas , w którym moc widma mierzona przez Analizator widma jest na tyle wysoka , że kanał można znaczą zajęte.

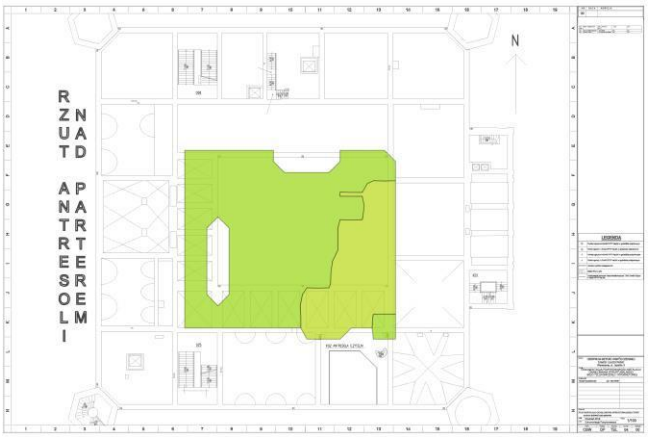


Wykorzystanie widma dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

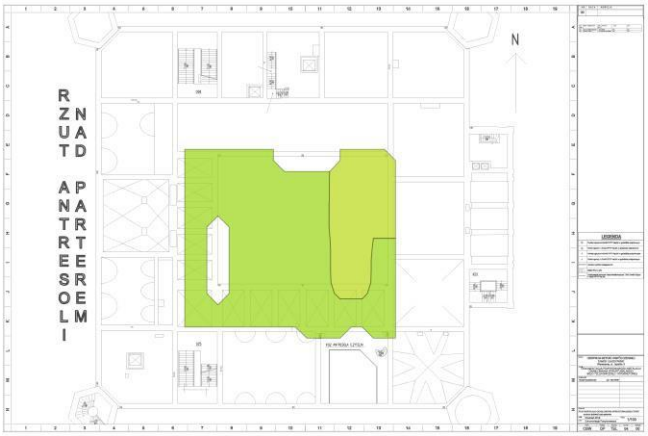
Wykorzystanie widma pokazuje czas , w którym moc widma mierzona przez Analizator widma jest na tyle wysoka , że kanał można znaczą zajęte.



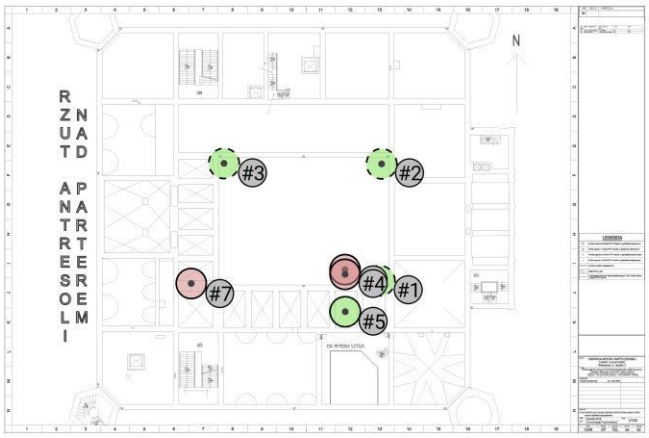
Moc kanału widma dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz



Moc kanału widma **dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz**



Punkty dostępowowe do centrum sztuki współczesnej Zamek Ujazdowski



Moje punkty dostępu do centrum sztuki współczesnej Zamek Ujazdowski

Symulowane punkty dostępowe do centrum sztuki współczesnej zamek Ujazdowski

AP	Punkt dostępowy			
1	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	52	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
2	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	136	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
3	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	60	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

Zmierzone punkty dostępu dla centrum sztuki współczesnej zamek Ujazdowski

AP	Punkt dostępowy			
5	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: B4:2C: C0 C8: B5: AD: B4:2C: C0	IAP22 8 IAP22 8
	standardu 802.11 AC standardu 802.11 AC	100 100	C8: B5: AD: B4:2C: d0 C8: B5: AD: B4:2C: d0	IAP22 8 IAP22 8

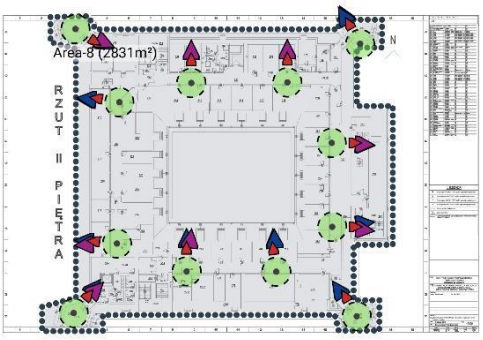
Centrum Sztuki Współczesnej Zamek Ujazdowski

Wyniki teoretycznej koncepcji rozmieszczenia AP na wybranych ściśle określonych częściach elektroniczna tj.:

- Piętro II (Pokoje biurowe: 209, 225, 272, 242, korytarze: 204, 261, 249, 230, 215)
- Piętro I (Sala wystawowa: 101, 102, 103, 108, 110, 112, 114, 116, 117, 120, 121)
- Parter (kino: 024, czytelnia: 023, sala edukacyjna: 021, hala główny: 001, księgarnia: 002, sala wystawowa: 005, 013, 015, 019, 032)
- Piwnica (sala wystawowa: P02, P03, P04, P06)

Centrum Sztuki Współczesnej Zamek Ujazdowski

Pomiaryi punkty dostępowowe do centrum sztuki współczesnej Zamek Ujazdowski



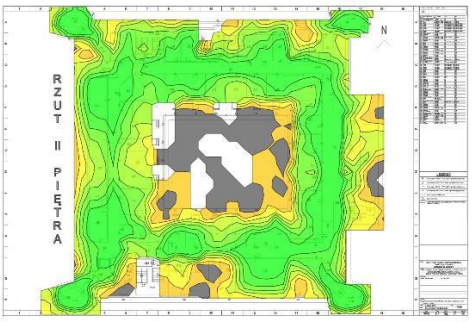
Powierzchnia-8 (2 831 m²)

Zapotrzebowanie na pokrycie: **podstawowa łączność**	Siła sygnału min	**-75,0 DBM**
	Stosunek sygnałudoszumu min	**16,0 w DB**
	Szybkość transmisji danych min	**11 MB/s**
	Liczba punktów Dostępowych min	**2 at min.-80,0 DBM**
	Nakładanie kanałów maks .	**3 at min.-80,0 DBM**
	Czas błądzenia (RTT) maks .	**500ms**
	Utrata pakietów Max	**10,0%**

Zapotrzebowanie na zdolności produkcyjne	**100** Generic smartphone [normalny SLA (2 Mbps)] **10** rodzajowy laptop [normalny SLA (2 Mbps)] **Kwota całkowita: 110 (220 MB/s)**
Notatki	

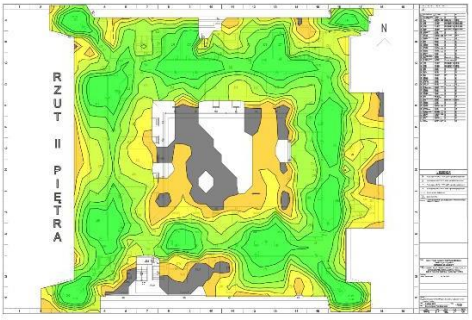
Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepustowość.



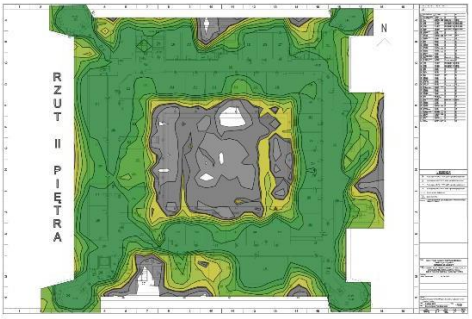
Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepustowość.



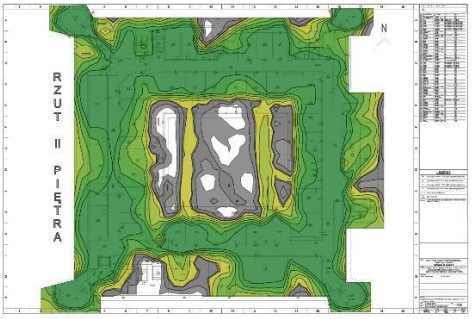
Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy od szumu (SNR Greater niż zero), aby możliwe było przesyłanie danych



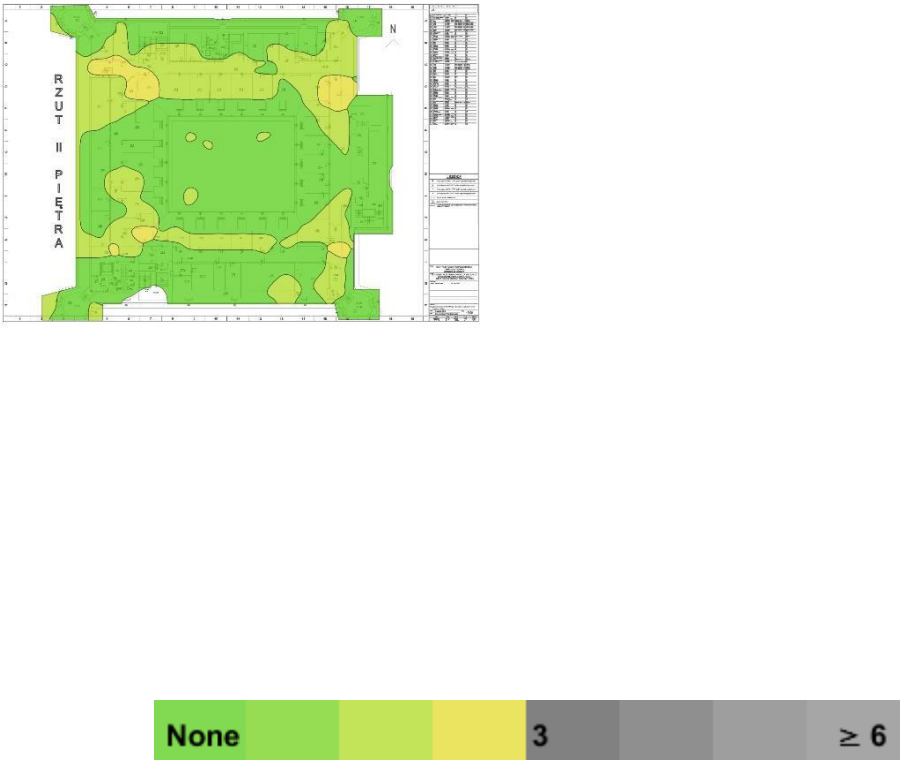
Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR większy od zera), aby możliwe było przesyłanie danych



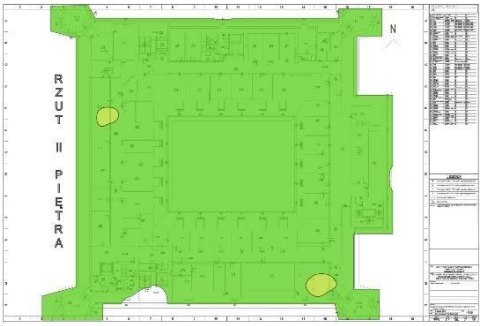
Nakładanie kanałów na centrum sztuki współczesnej Zamek Ujazdowski na paśmie 2,4 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



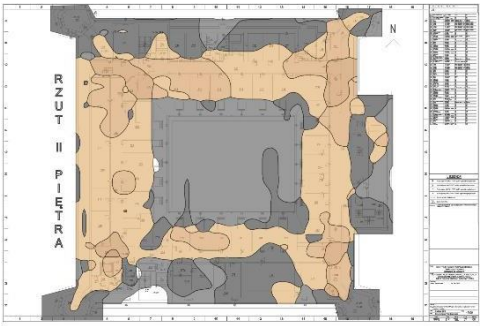
Nakładanie kanałów na centrum sztuki współczesnej Zamek Ujazdowski w paśmie 5 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



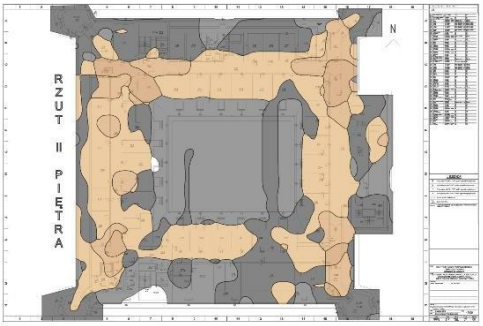
Liczba punktów dostępowy do centrum sztuki współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



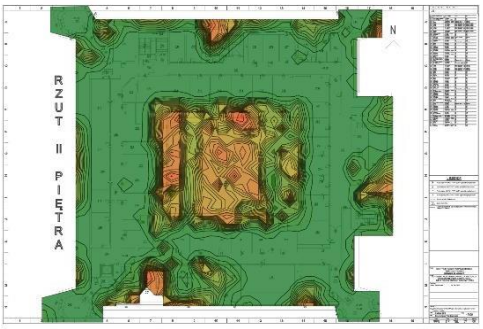
Liczba punktów dostępowy dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



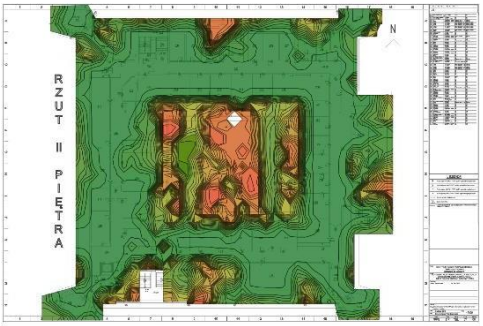
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę) , urządzeńbędziebyćprzekazywaniadanych.Typowotenprawdziwymidanychprzepływnościjestopoło wadanychstawkalubmniej.



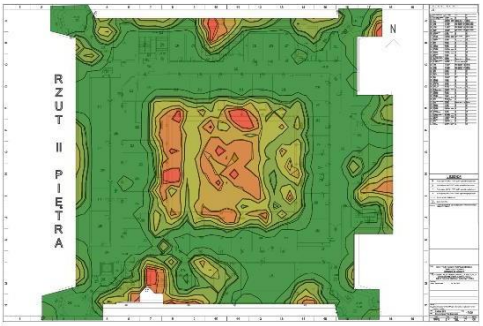
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)
,



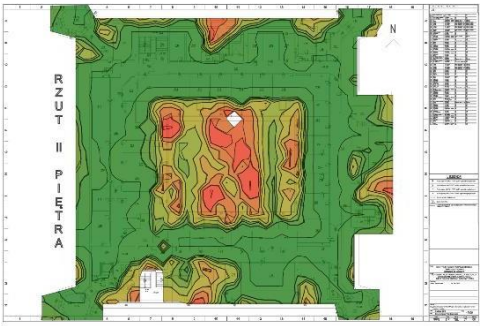
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Wyświetla zmierzoną przepustowość.



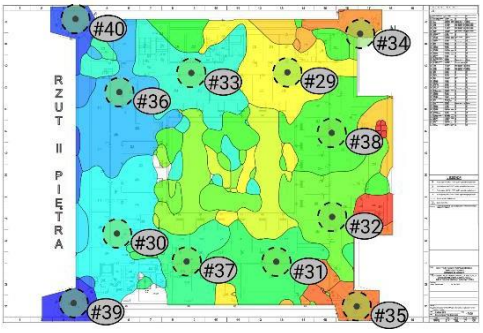
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Wyświetla zmierzoną przepustowość.



Powiązany punkt dostępowy Centrum Sztuki Współczesnej Zamek Ujazdowski

Wyświetla punkt dostępu , z którym jest skojarzone urządzenie klienckie . Obraz pokazuje przewidywane siły sygnału skojarzenia



AP	Punkt dostępowy			
29	AP 2,4/5 GHz			
	802.11 n	6	35 MW	2,4 GHz
	standardu 802.11 AC	108	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble

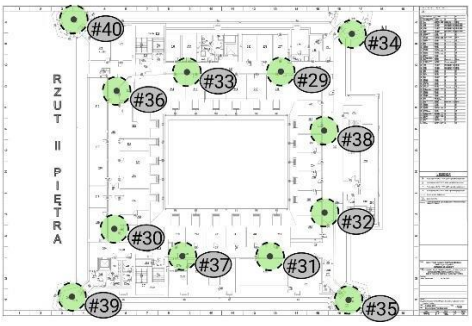
30	AP 2,4/5 GHz			
	802.11 n	11	35 MW	2,4 GHz

	standardu 802.11 AC	140	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
31	AP 2,4/5 GHz			
	802.11 n	11	35 MW	2,4 GHz
	standardu 802.11 AC	40	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
32	AP 2,4/5 GHz			
	802.11 n	6	35 MW	2,4 GHz
	standardu 802.11 AC	60	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
33	AP 2,4/5 GHz			
	802.11 n	11	35 MW	2,4 GHz
	standardu 802.11 AC	56	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
34	AP 2,4/5 GHz			
	802.11 n	1	35 MW	2,4 GHz
	standardu 802.11 AC	120	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
35	AP 2,4/5 GHz			
	802.11 n	1	35 MW	2,4 GHz
	standardu 802.11 AC	136	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
36	AP 2,4/5 GHz			
	802.11 n	6	35 MW	2,4 GHz
	standardu	120	35 MW	5 GHz

	802.11 AC			
	Bluetooth	-	35 MW	Ble
37	AP 2,4/5 GHz			
	802.11 n	6	35 MW	2,4 GHz
	standardu 802.11 AC	116	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble

38	AP 2,4/5 GHz			
	802.11 n	11	35 MW	2,4 GHz
	standardu 802.11 AC	140	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
39	AP 2,4/5 GHz			
	802.11 n	1	35 MW	2,4 GHz
	standardu 802.11 AC	36	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
40	AP 2,4/5 GHz			
	802.11 n	1	35 MW	2,4 GHz
	standardu 802.11 AC	116	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble

Punkty dostępowowe na centrum sztuki współczesnej Zamek Ujazdowski



Moje punkty dostępu na centrum sztuki współczesnej Zamek Ujazdowski

Symulowane punkty dostępowe na centrum sztuki współczesnej Zamek Ujazdowski

AP	Punkt dostępowy			
29	AP 2,4/5 GHz			
	802.11 n	6	35 MW	2,4 GHz
	standardu 802.11 AC	108	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
30	AP 2,4/5 GHz			
	802.11 n	11	35 MW	2,4 GHz
	standardu 802.11 AC	140	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
31	AP 2,4/5 GHz			
	802.11 n	11	35 MW	2,4 GHz
	standardu 802.11 AC	40	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
32	AP 2,4/5 GHz			
	802.11 n	6	35 MW	2,4 GHz
	standardu 802.11 AC	60	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
33	AP 2,4/5 GHz			
	802.11 n	11	35 MW	2,4 GHz
	standardu 802.11 AC	56	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
34	AP 2,4/5 GHz			
	802.11 n	1	35 MW	2,4 GHz
	standardu 802.11 AC	120	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
35	AP 2,4/5 GHz			
	802.11 n	1	35 MW	2,4 GHz

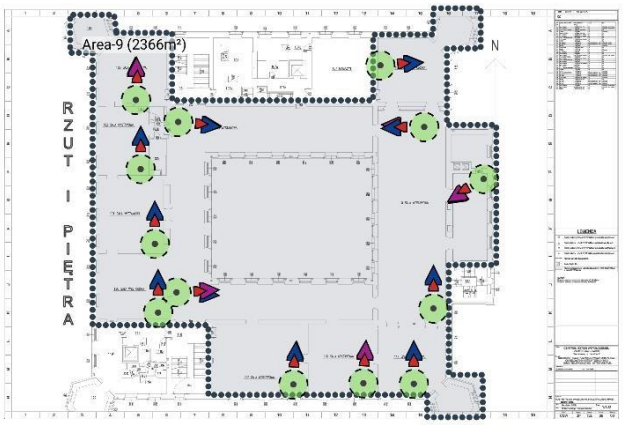
	standardu 802.11 AC	136	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
36	AP 2,4/5 GHz			
	802.11 n	6	35 MW	2,4 GHz
	standardu 802.11 AC	120	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
37	AP 2,4/5 GHz			
	802.11 n	6	35 MW	2,4 GHz
	standardu 802.11 AC	116	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
38	AP 2,4/5 GHz			
	802.11 n	11	35 MW	2,4 GHz
	standardu 802.11 AC	140	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
39	AP 2,4/5 GHz			
	802.11 n	1	35 MW	2,4 GHz
	standardu 802.11 AC	36	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble
40	AP 2,4/5 GHz			
	802.11 n	1	35 MW	2,4 GHz
	standardu 802.11 AC	116	35 MW	5 GHz
	Bluetooth	-	35 MW	Ble

Zmierzone punkty dostępowy na centrum sztuki współczesnej Zamek Ujazdowski

Brak.

Centrum Sztuki Współczesnej Zamek Ujazdowski

Trasy pomiarowe i punkty Dostępowowe do centrum sztuki współczesnej Zamek Ujazdowski



Powierzchnia-9 (2 366 m²)

Zapotrzebowanie na pokrycie: **podstawowa łączność**	Siła sygnału min	**-75,0 DBM**
	Stosunek sygnałudoszumu min	**16,0 w DB**
	Szybkość transmisji danych min	**11 MB/s**
	Liczba punktów Dostępowych min	**2 at min.-80,0 DBM**
	Nakładanie kanałów maks .	**3 at min.-80,0 DBM**
	Czas błądzenia (RTT) maks .	**500ms**
	Utrata pakietów Max	**10,0%**
Zapotrzebowanie na zdolności produkcyjne		

	10 Rodzajowy laptop [normalny SLA (2 Mbps)] **100** Generic smartphone [normalny SLA (2 Mbps)] **Kwota całkowita: 110 (220 MB/s)**
Notatki	

Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia i niskie dane przepływności.

Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepustowość.

Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy od szumu (SNR Greater niż zero), aby możliwe było przesyłanie danych

Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

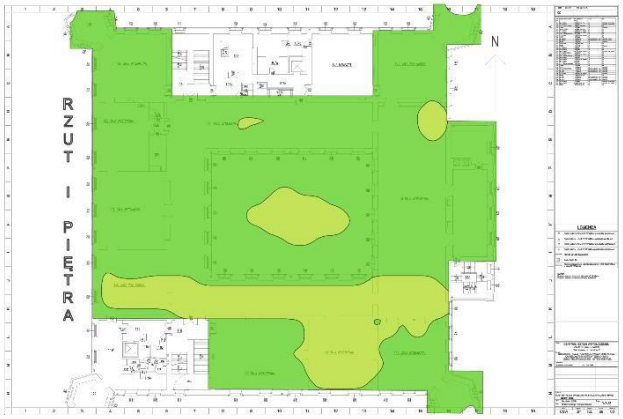
Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR większy od zera)

Nakładanie kanałów na centrum sztuki współczesnej Zamek Ujazdowski na paśmie 2,4 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.

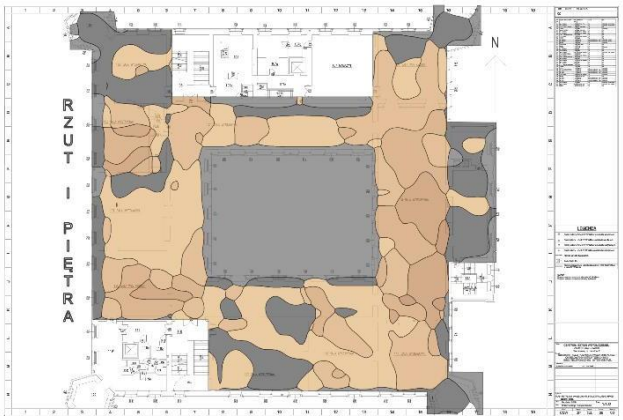
Nakładanie kanałów na centrum sztuki współczesnej Zamek Ujazdowski w paśmie 5 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



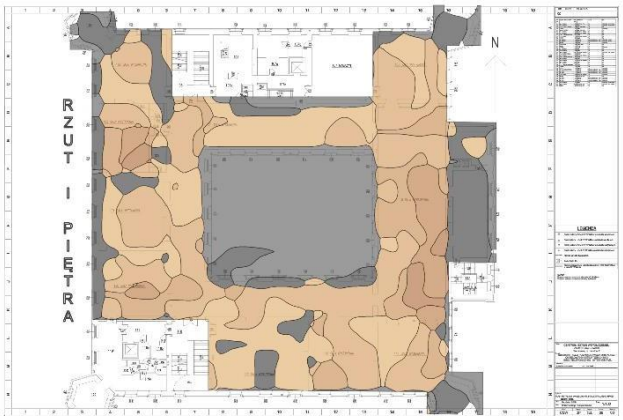
Liczba punktów dostępowy do centrum sztuki współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



Liczba punktów dostępowy dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.

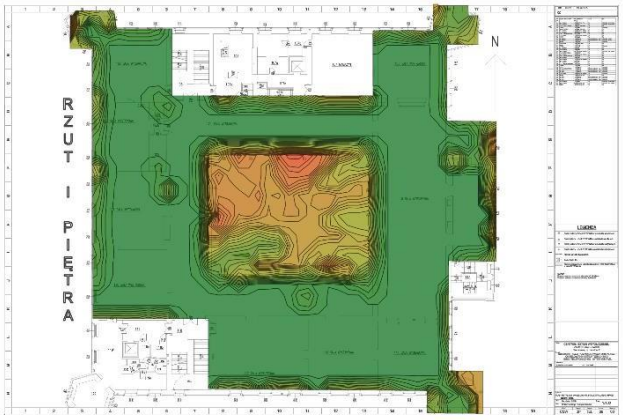


Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)
,

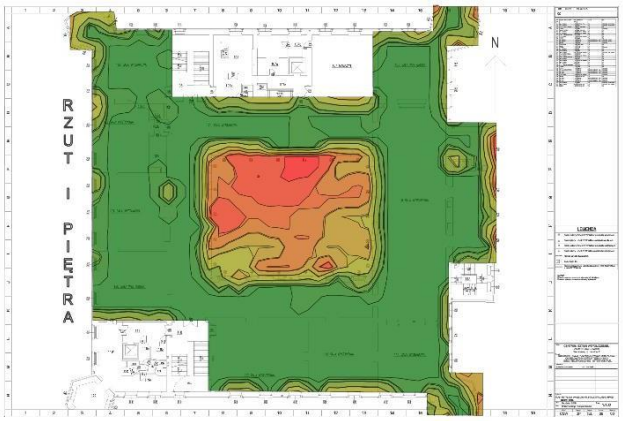
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)
,



Throughput dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Wyświetla zmierzoną przepustowość.

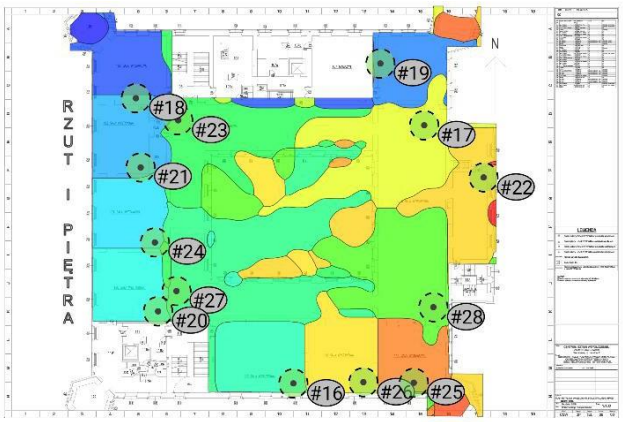


Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Wyświetla zmierzoną przepustowość.

Powiązany punkt dostępowy Centrum Sztuki Współczesnej Zamek Ujazdowski

Wyświetla punkt dostępu , z którym jest skojarzone urządzenie klienckie . Obraz pokazuje przewidywane siły sygnału skojarzenia



AP	Punkt dostępowy			
16	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	104	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

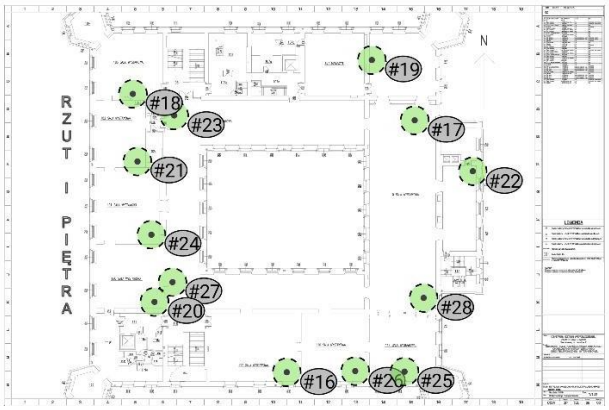
17	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz

	standardu 802.11 AC	44	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
18	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	100	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
19	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	36	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
20	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	112	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
21	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	56	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
22	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	56	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
23	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu	64	25 MW	5 GHz

	802.11 AC			
	Bluetooth	-	1 MW	Ble
24	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	128	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

25	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	40	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
26	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	132	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
27	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	52	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
28	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	52	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

Punkty dostępowowe na centrum sztuki współczesnej Zamek Ujazdowski



Moje punkty dostępu na centrum sztuki współczesnej Zamek Ujazdowski

Symulowane punkty dostępowe na centrum sztuki współczesnej Zamek Ujazdowski

AP	Punkt dostępowy			
16	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	104	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
17	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	44	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
18	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	100	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
19	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	36	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
20	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	112	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
21	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	56	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
22	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz

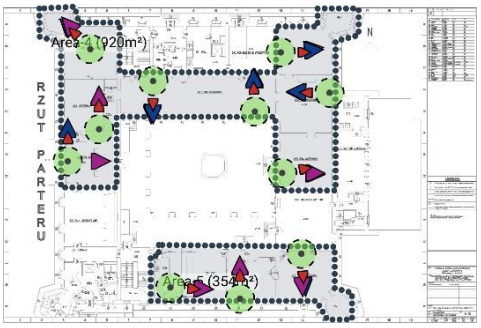
	standardu 802.11 AC	56	25 MW	AP 2,4/5 GHz
	Bluetooth	-	1 MW	AP 2,4/5 GHz
23	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	64	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
24	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	128	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
25	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	40	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
26	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	132	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
27	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	52	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
28	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	52	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

Zmierzone punkty dostępowy na centrum sztuki współczesnej Zamek Ujazdowski

Brak.

Centrum Sztuki Współczesnej Zamek Ujazdowski

Trasy pomiarowe i punkty Dostępowowe do centrum sztuki współczesnej Zamek Ujazdowski



Powierzchnia-4 (920 m²)

Zapotrzebowanie na pokrycie: **podstawowa łączność**	Siła sygnału min	**-75,0 DBM**
	Stosunek sygnałudoszumu min	**16,0 w DB**
	Szybkość transmisji danych min	**11 MB/s**
	Liczba punktów Dostępowych min	**2 at min.-80,0 DBM**
	Nakładanie kanałów maks .	**3 at min.-80,0 DBM**
	Czas błądzenia (RTT) maks .	**500ms**
	Utrata pakietów Max	**10,0%**
Zapotrzebowanie na zdolności produkcyjne		

	100 Generic smartphone [normalny SLA (2 Mbps)] **10** Rodzajowy laptop [normalny SLA (2 Mbps)] **Kwota całkowita: 110 (220 MB/s)**
Notatki	

Powierzchnia-5 (354 m²)

Zapotrzebowanie na pokrycie: **podstawowa łączność**	Siła sygnału min	**-75,0 DBM**
	Stosunek sygnałudoszumu min	**16,0 w DB**
	Szybkość transmisji danych min	**11 MB/s**
	Liczba punktów Dostępowych min	**2 at min.-80,0 DBM**
	Nakładanie kanałów maks .	**3 at min.-80,0 DBM**
	Czas błądzenia (RTT) maks .	**500ms**
	Utrata pakietów Max	**10,0%**
Zapotrzebowanie na zdolności produkcyjne	**100** Generic smartphone [normalny SLA (2 Mbps)] **10** rodzajowy laptop [normalny SLA (2 Mbps)] **Kwota całkowita: 110 (220 MB/s)**	
Notatki		

Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

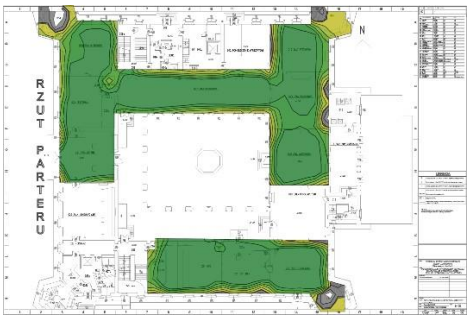
Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia i niskie dane przepływności.

Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepustowość.

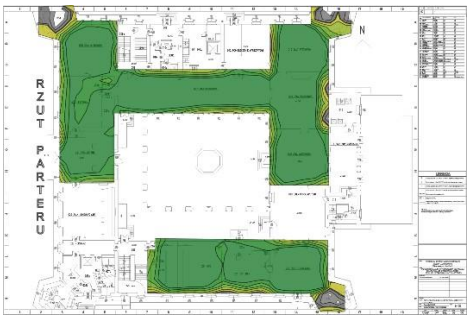
Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek ujazdowski w paśmie 2,4 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR większy od zera) dla danych transfer być



Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR większy od zera



Nakładanie kanałów na centrum sztuki współczesnej Zamek Ujazdowski na paśmie 2,4 GHz

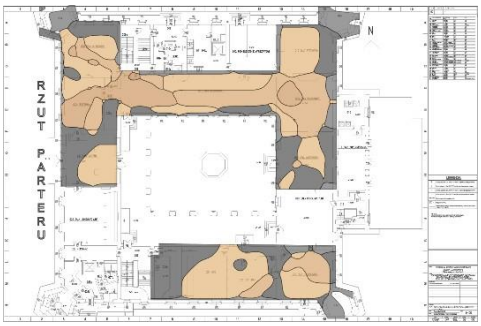
Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.

Nakładanie kanałów na centrum sztuki współczesnej Zamek Ujazdowski w paśmie 5 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.

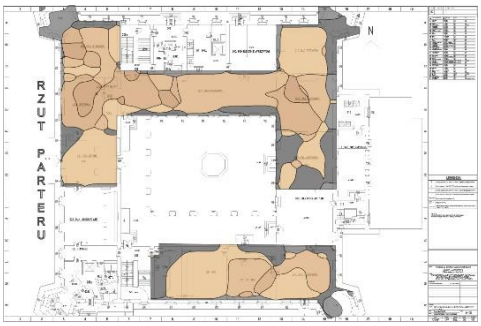
Liczba punktów dostępowy do centrum sztuki współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



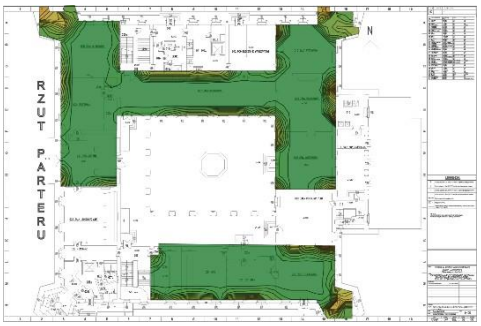
Liczba punktów dostępowy dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



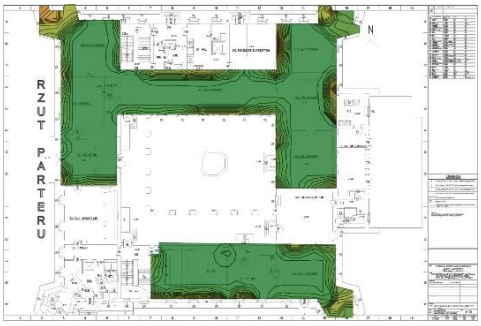
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)
,



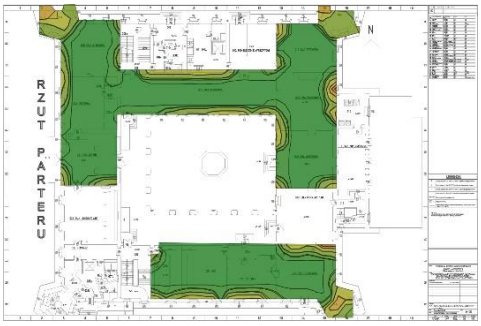
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)
,



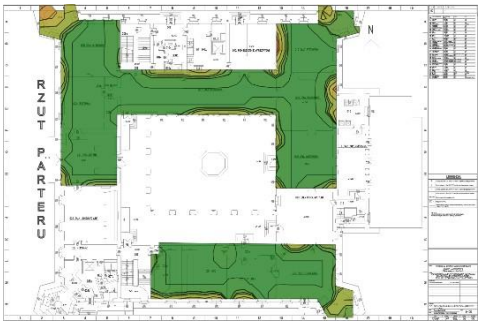
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Wyświetla zmierzoną przepustowość.



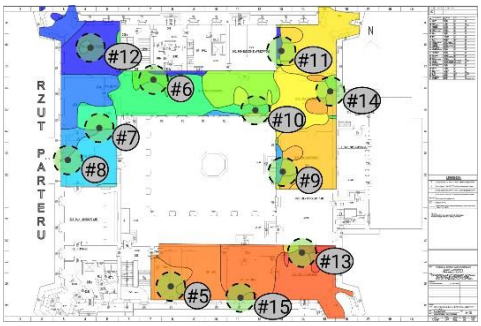
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Wyświetla zmierzoną przepustowość.



Powiązany punkt dostępowy Centrum Sztuki Współczesnej Zamek Ujazdowski

Wyświetla punkt dostępu , z którym jest skojarzone urządzenie klienckie . Obraz pokazuje przewidywane siły sygnału skojarzenia



AP	Punkt dostępowy			
5	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	108	25 MW	5 GHz

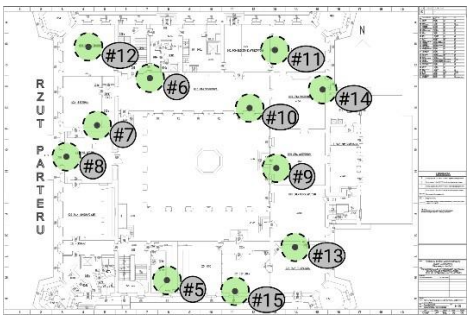
	Bluetooth	-	1 MW	Ble
6	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz

	standardu 802.11 AC	48	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
7	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	132	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
8	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	132	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
9	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	100	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
10	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	100	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
11	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	64	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
12	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu	60	25 MW	5 GHz

	802.11 AC			
	Bluetooth	-	1 MW	Ble
13	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	56	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

14	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	40	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
15	AP 2,4/5 GHz			
	802.11 n	1	25 MW	2,4 GHz
	standardu 802.11 AC	124	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

Punkty dostępowowe na centrum sztuki współczesnej Zamek Ujazdowski



Moje punkty dostępu na centrum sztuki współczesnej Zamek Ujazdowski

Symulowane punkty dostępowe na centrum sztuki współczesnej Zamek Ujazdowski

AP	Punkt dostępowy			
5	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	108	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
6	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	48	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
7	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	132	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
8	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	132	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
9	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	100	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
10	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	100	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
11	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz

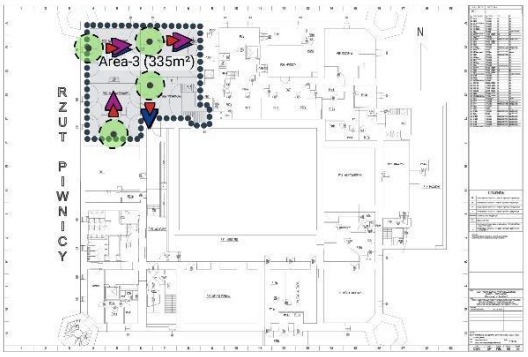
	standardu 802.11 AC	64	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
12	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	60	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
13	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	56	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
14	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	40	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
15	AP 2,4/5 GHz			
	802.11 n	1	25 MW	2,4 GHz
	standardu 802.11 AC	124	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

Zmierzone punkty dostępowy na centrum sztuki współczesnej Zamek Ujazdowski

Brak.

Centrum Sztuki Współczesnej Zamek Ujazdowski

Trasy pomiarowe i punkty Dostępowowe do centrum sztuki współczesnej Zamek Ujazdowski



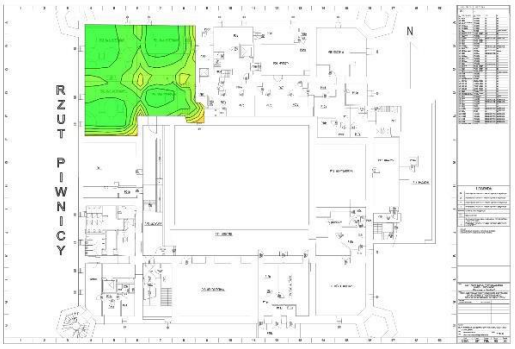
Powierzchnia-3 (335 m²)

Zapotrzebowanie na pokrycie: **podstawowa łączność**	Siła sygnału min	**-75,0 DBM**
	Stosunek sygnałudoszumu min	**16,0 w DB**
	Szybkość transmisji danych min	**11 MB/s**
	Liczba punktów Dostępowych min	**2 at min.-80,0 DBM**
	Nakładanie kanałów maks .	**3 at min.-80,0 DBM**
	Czas błądzenia (RTT) maks .	**500ms**
	Utrata pakietów Max	**10,0%**
Zapotrzebowanie na zdolności produkcyjne		

	100 Generic smartphone [normalny SLA (2 Mbps)] **10** Rodzajowy laptop [normalny SLA (2 Mbps)] **Kwota całkowita: 110 (220 MB/s)**
Notatki	

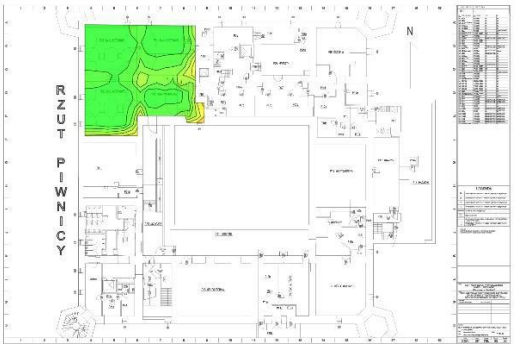
Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia i niskie dane przepływności.



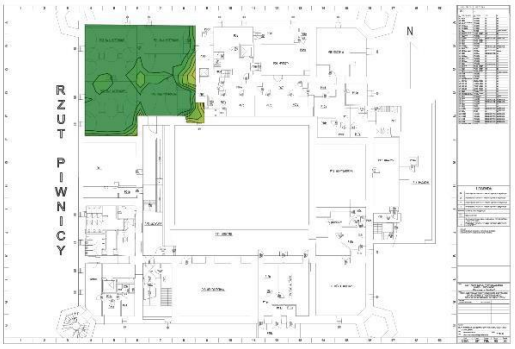
Siła sygnału dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepustowość.



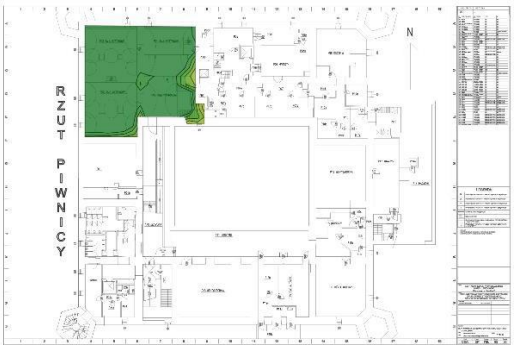
Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy od szumu (SNR Greater niż zero), aby możliwe było przesyłanie danych



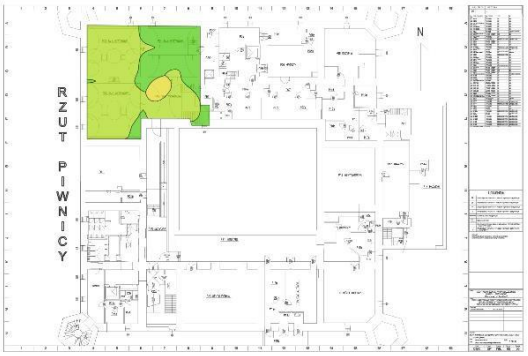
Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR większy od zera), aby możliwe



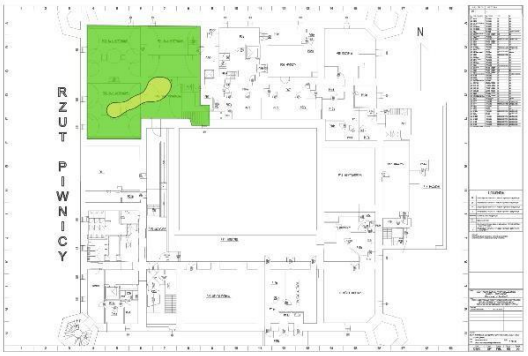
Nakładanie kanałów na centrum sztuki współczesnej Zamek Ujazdowski on 2,4 GHz Band

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



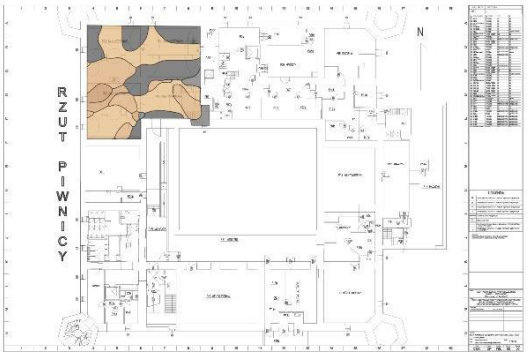
Nakładanie kanałów na centrum sztuki współczesnej Zamek Ujazdowski w paśmie 5 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



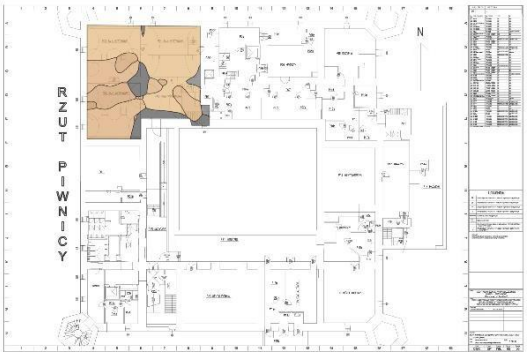
Liczba punktów dostępowy do centrum sztuki współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



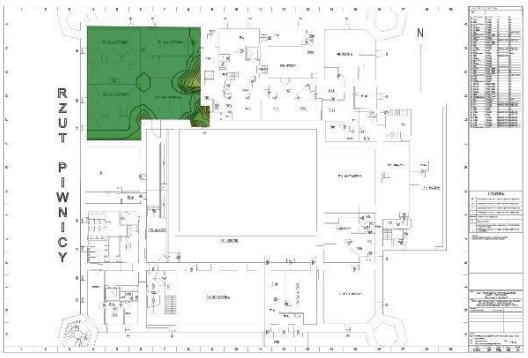
Liczba punktów dostępowy dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



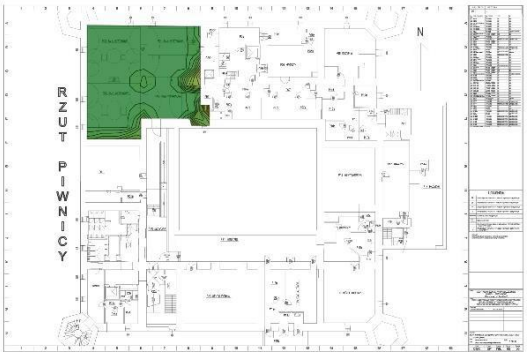
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę) , urządzeńbędziebyćprzekazywaniadanych.Typowotenprawdziwymidanychprzepływnościjestopoło wadanychstawkalubmniej.



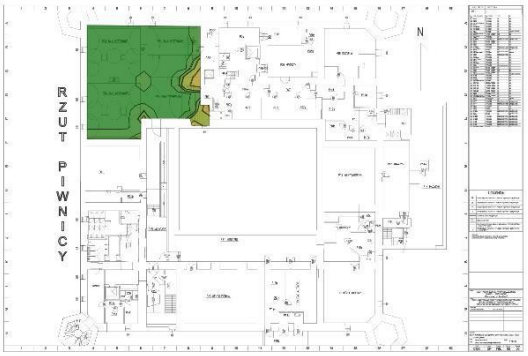
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)
,



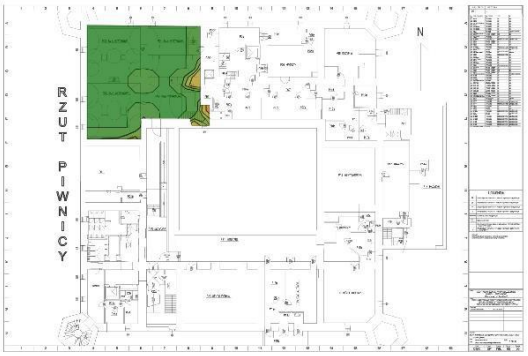
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 2,4 GHz

Wyświetla zmierzoną przepustowość.



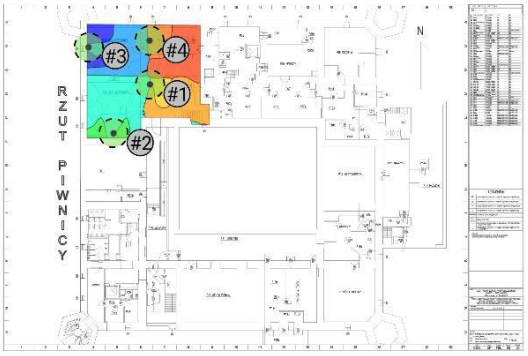
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski w paśmie 5 GHz

Wyświetla zmierzoną przepustowość.



Powiązany punkt dostępowy Centrum Sztuki Współczesnej Zamek Ujazdowski

Wyświetla punkt dostępu , z którym jest skojarzone urządzenie klienckie . Obraz pokazuje przewidywane siły sygnału skojarzenia

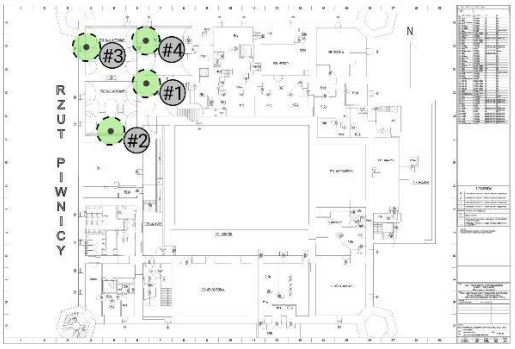


AP	Punkt dostępowy			
1	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	124	25 MW	5 GHz

	Bluetooth	-	1 MW	Ble
2	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz

	standardu 802.11 AC	48	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
3	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	104	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
4	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	136	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

Punkty dostępowowe na centrum sztuki współczesnej Zamek Ujazdowski



Moje punkty dostępu na centrum sztuki współczesnej Zamek Ujazdowski

Symulowane punkty dostępowe na centrum sztuki współczesnej zamek Ujazdowski

AP	Punkt dostępowy			
1	AP 2,4/5 GHz			
	802.11 n	6	6 MW	2,4 GHz
	standardu 802.11 AC	124	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
2	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	48	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
3	AP 2,4/5 GHz			
	802.11 n	11	6 MW	2,4 GHz
	standardu 802.11 AC	104	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble
4	AP 2,4/5 GHz			
	802.11 n	1	6 MW	2,4 GHz
	standardu 802.11 AC	136	25 MW	5 GHz
	Bluetooth	-	1 MW	Ble

Zmierzone punkty dostępowy na centrum sztuki współczesnej zamek Ujazdowski

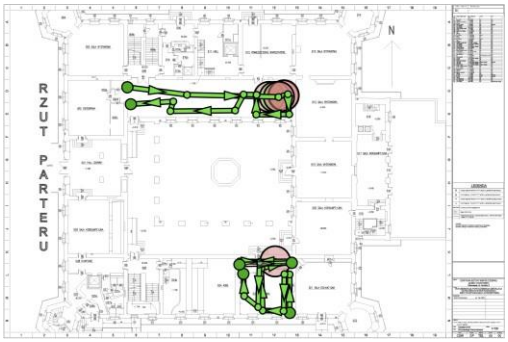
Brak.

Centrum Sztuki Współczesnej Zamek Ujazdowski

Trasy pomiarowe i punkty Dostępowowe do centrum sztuki współczesnej Zamek Ujazdowski

Wyniki pomiaruw problematycznychmiejscach elektroniczna z punktu widzenia propagacji fal Integrator

1. Pomiar parter
   a) Czytelnia 023
   b) SaLa wystawowa 032



Zapotrzebowanie na pokrycie: **głos + dane**	Siła sygnału min	**-67,0 DBM**
	Stosunek sygnałudoszumu min	**20,0 w DB**
	Szybkość transmisji danych min	**20 MB/s**

	Liczba punktów Dostępowych min	**2 at min.-75,0 DBM**

	Nakładanie kanałów maks .	**2 at min.-85,0 DBM**
	Czas błądzenia (RTT) maks .	**200ms**
	Utrata pakietów Max	**2,0%**

Siła sygnału dla Centrum Sztuki Współczesnej pasmo 2,4 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepływności.

Siła sygnału dla Centrum Sztuki Współczesnej Zamek ujazdowskiego pasmo 5 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepustowość.

Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek ujazdowskiego pasmo 2,4 GHz

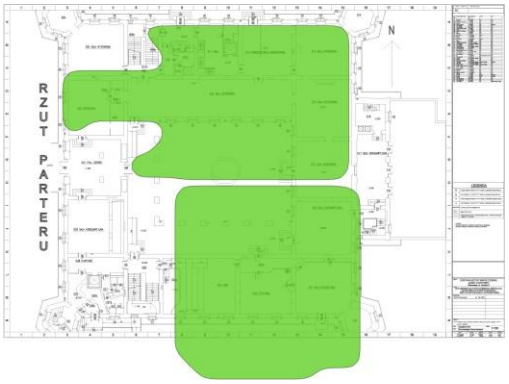
Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR większy od zera), aby możliwe było przesyłanie danych

Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek ujazdowskiego pasmo 5 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy od szumu (SNR Greater tHan zero), aby możliwe było przesyłanie danych

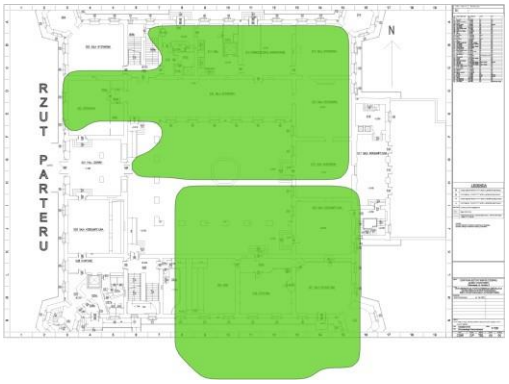
Nakładanie kanałów na centrum sztuki współczesnej zamek ujazdowskiego pasmo 2,4 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



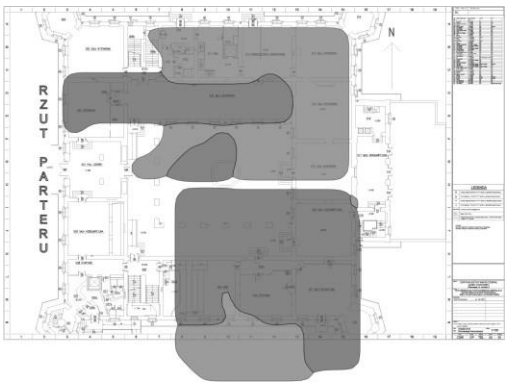
Nakładanie kanałów na centrum sztuki współczesnej zamek ujazdowskiego pasmo 5 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



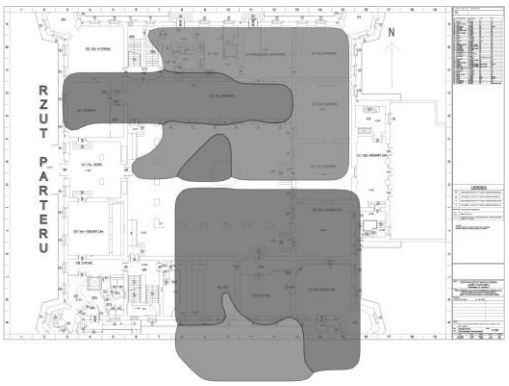
Liczba punktów dostępowy do centrum sztuki współczesnej zamek Ujazdowskio pasmo 2,4 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



Liczba punktów dostępowy do centrum sztuki współczesnej zamek ujazdowskiego pasmo 5 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 2,4 GHz

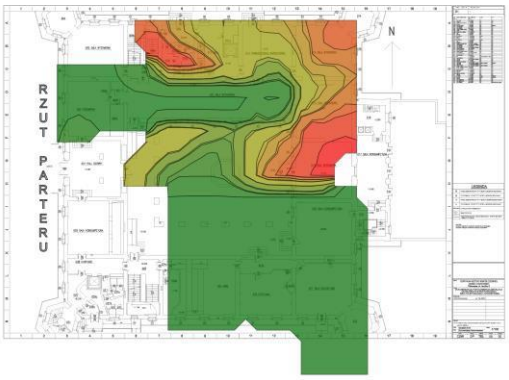
Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę) , urządzeńbędziebyćprzekazywaniadanych.Typowotenprawdziwymidanychprzepływnościjestopoło wadanychstawkalubmniej.

Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 5 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę)
,

Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 2,4 GHz

Wyświetla zmierzoną przepustowość.



Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 5 GHz

Wyświetla zmierzoną przepustowość.

Powiązany punkt dostępowy Centrum Sztuki Współczesnej Zamek Ujazdowski

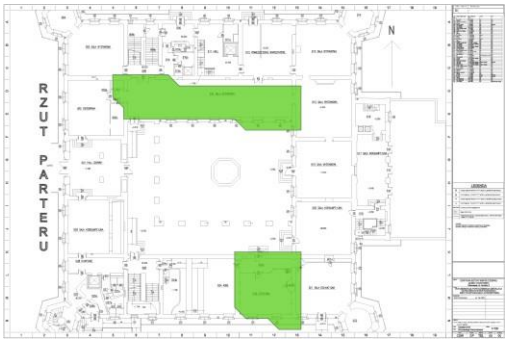
Wyświetla punkt dostępu , z którym jest skojarzone urządzenie klienckie . Obraz pokazuje przewidywane siły sygnału skojarzenia

AP	Punkt dostępowy			
2	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14:	IAP30 5 IAP30

			C0	5
	standardu 802.11 AC standardu 802.11 AC	36 36	C8: B5: AD: F4:14: d0 C8: B5: AD: F4:14: d0	IAP30 5 IAP30 5

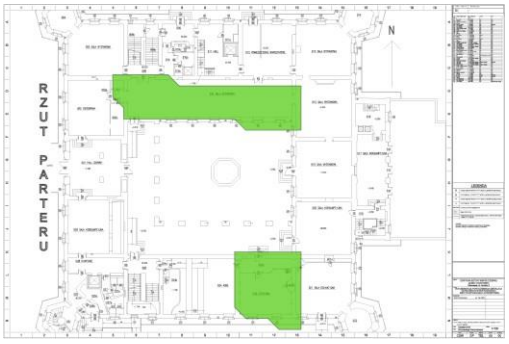
Wykorzystanie widma dla Centrum Sztuki Współczesnej Zamek Ujazdowski 2,4 w paśmie GHz

Wykorzystanie widma pokazuje czas , w którym moc widma mierzona przez Analizator widma jest na tyle wysoka , że kanał można znaczą zajęte.

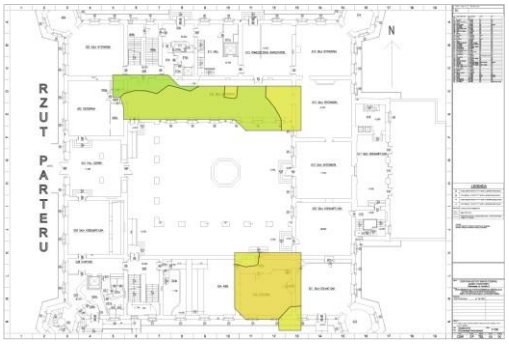


Wykorzystanie widma dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 5 GHz

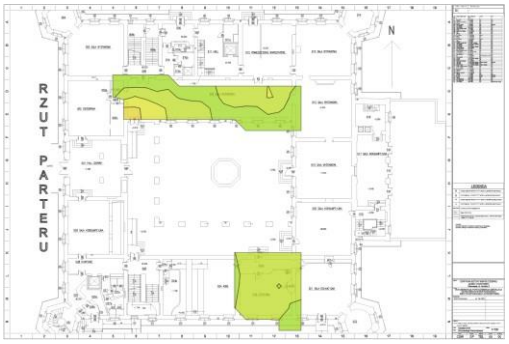
Wykorzystanie widma pokazuje czas , w którym moc widma mierzona przez Analizator widma jest na tyle wysoka , że kanał można znaczą zajęte.



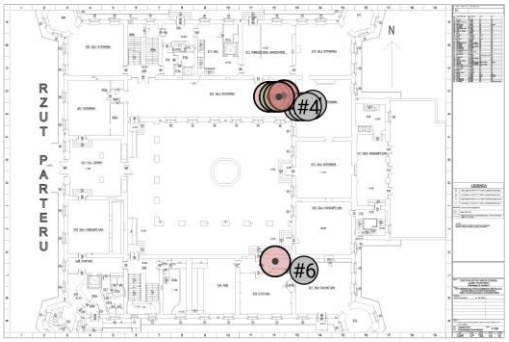
Moc kanału widma dla centrum Sztuki współczesnej zamek ujazdowskiego pasmo 2,4 GHz



Moc kanału widma dla centrum sztuki współczesnej zamek ujazdowskiego pasmo 5 GHz



Punkty dostępowowe na centrum sztuki współczesnej zamek Ujazdowski



Moje punkty dostępu na centrum sztuki współczesnej zamek Ujazdowski

Symulowane punktydostępowowe **na centrum sztuki współczesnej zamek ujazdowskiego**

Brak.

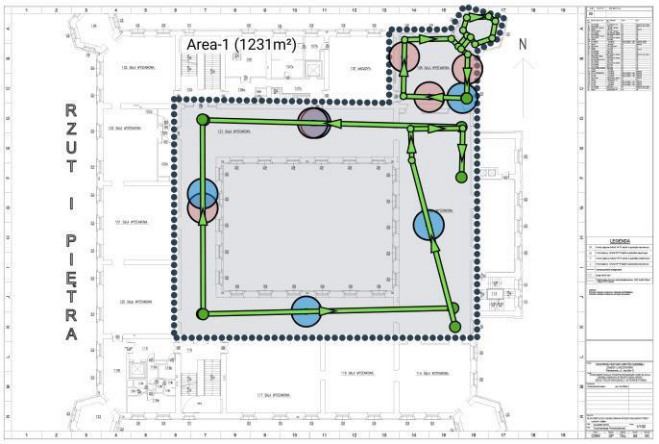
Zmierzone punkty dostępu na centrum sztuki współczesnej zamek ujazdowskiego

AP	Punkt dostępowy			
2	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC standardu 802.11 AC	36 36	C8: B5: AD: F4:14: d0 C8: B5: AD: F4:14: d0	IAP30 5 IAP30 5

2. Pomiar piętro I
a) Sala wystawowa 121
b) Sala wystawowa 110

Centrum Sztuki Współczesnej Zamek Ujazdowski

Trasy pomiarowe i punkty Dostępowowe do centrum sztuki współczesnej Zamek Ujazdowski



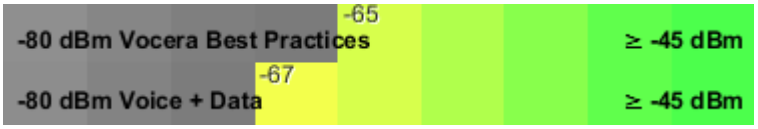
Powierzchnia-1 (1 231 m²)

Zapotrzebowanie na pokrycie	Siła sygnału min	**-65,0 DBM**
	Stosunek sygnałudoszumu min	**25,0 w DB**
	Szybkość transmisji danych min	**11 MB/s**
	Liczba punktów Dostępowych min	**2 at min.-75,0 DBM**

	Nakładanie kanałów maks .	**4 at min.-80,0 DBM**
	Czas błądzenia (RTT) maks .	**200ms**
	Utrata pakietów Max	**2,0%**
Zapotrzebowanie na zdolności produkcyjne	Brak urządzeń pojemności dla tego obszaru	
Notatki		

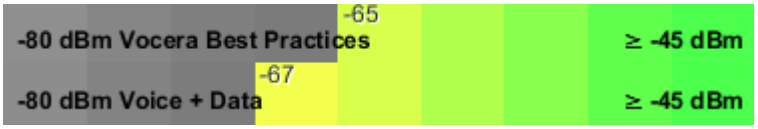
Siła sygnału dla Centrum Sztuki Współczesnej Zamek ujazdowskiego pasmo 2,4 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia niskie dane przepustowość.



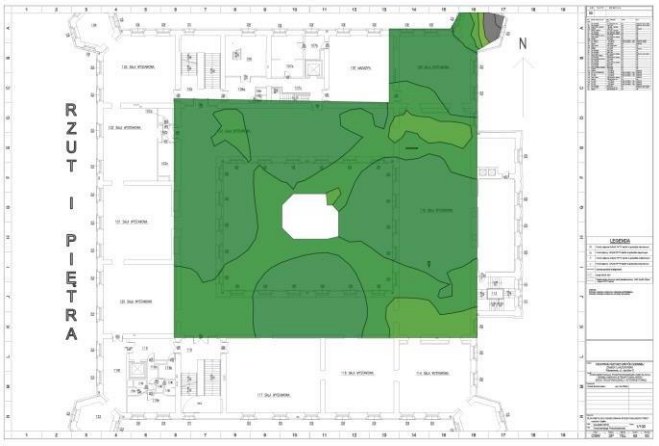
Siła sygnału dla Centrum Sztuki Współczesnej Zamek ujazdowskiego pasmo 5 GHz

Siła sygnału- czasami nazywana zasięg - jest najbardziej podstawowym wymogiem dla sieci bezprzewodowej . Ogólna wytyczna, niska siła sygnału oznacza zawodne połączenia, niskie dane przepływności.



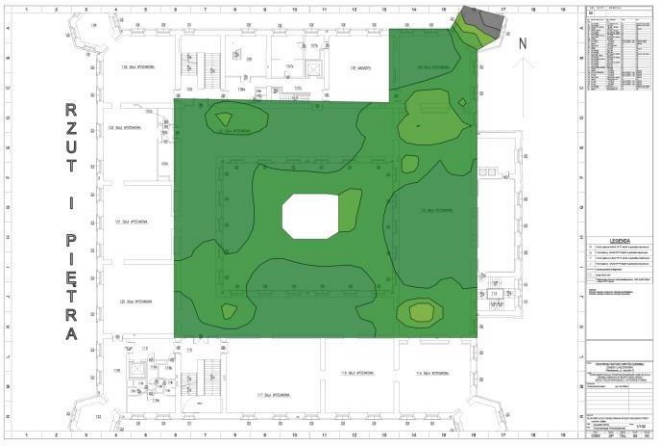
Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek ujazdowskiego pasmo 2,4 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy niż hałas (SNR większy od zera), aby możliwe było przesyłanie danych



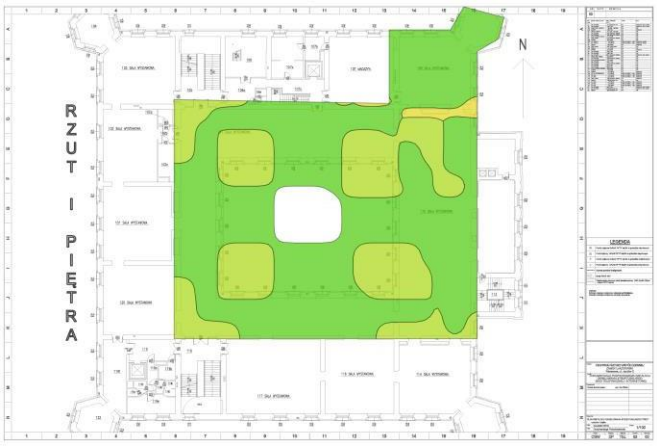
Stosunek sygnału do szumu (SNR) dla Centrum Sztuki Współczesnej Zamek ujazdowskiego pasmo 5 GHz

Stosunek sygnału do szumu wskazuje , ile siła sygnału jest silniejsza niż hałas (interferencja współkanałowa). Sygnał musi być silniejszy od szumu (SNR Greater tHan zero), aby możliwe było przesyłanie danych



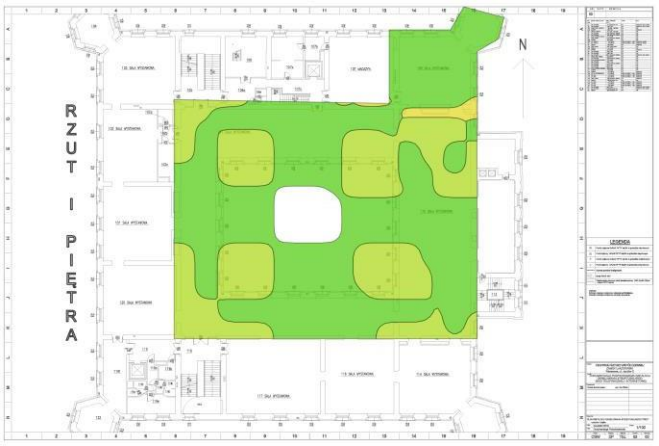
Nakładanie kanałów na centrum sztuki współczesnej zamek ujazdowskiego pasmo 2,4 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



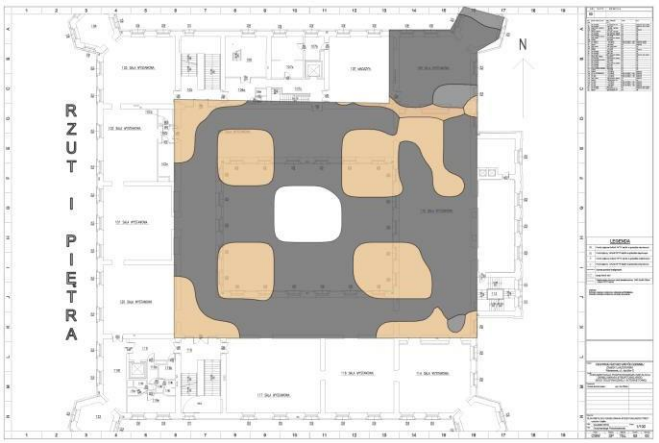
Nakładanie kanałów flub centrum sztuki współczesnej zamek Ujazdowski pasmo 5 GHz

Nakładanie kanałów wskazuje liczbę punktów dostępu słyszalnych każdej lokalizacji w jednym kanale.



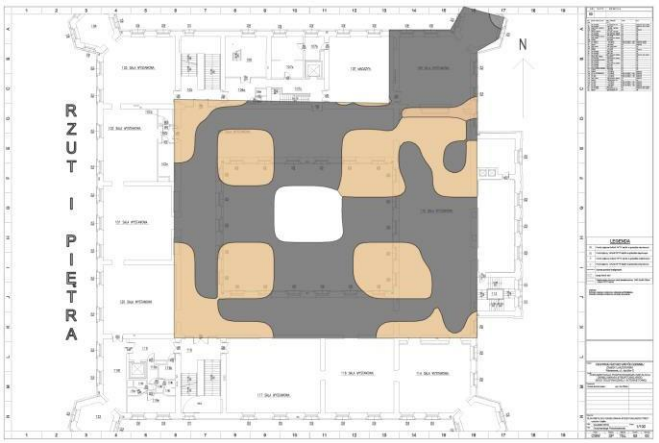
Liczba punktów dostępowy do centrum sztuki współczesnej zamek Ujazdowski pasmo 2,4 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



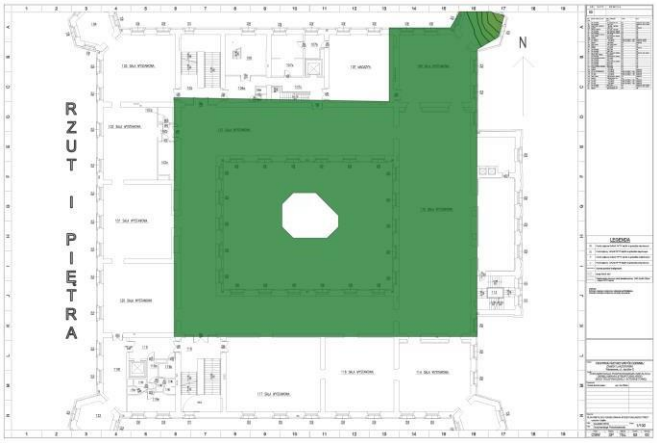
Liczba punktów dostępowy do centrum sztuki współczesnej zamek ujazdowskiego pasmo 5 GHz

Liczba punktów dostępu wskazuje liczbę punktów dostępu słyszalnych w każdej lokalizacji.



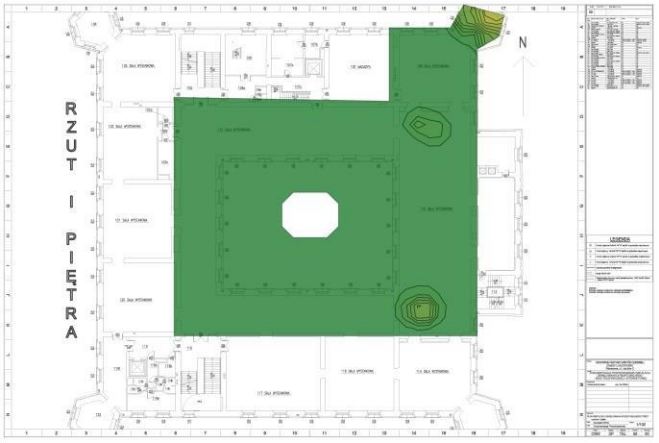
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 2,4 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę) , urządzeńbędziebyćprzekazywaniadanych.Typowotenprawdziwymidanychprzepływnościjestopoło wadanychstawkalubmniej.



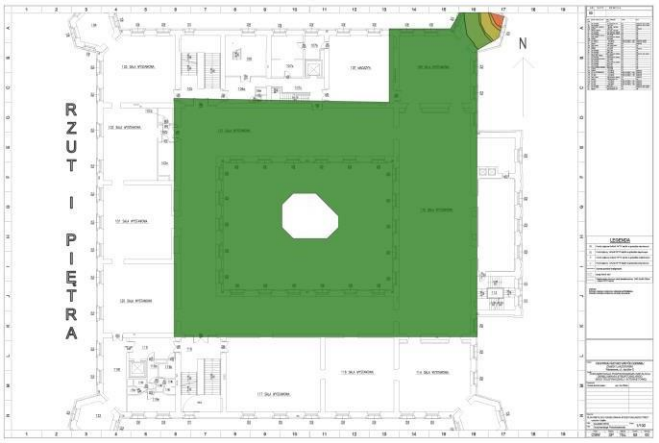
Szybkość transmisji danych dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 5 GHz

Szybkość transmisji danych to najwyższa możliwa prędkość (mierzona w megabitów na sekundę) ,.



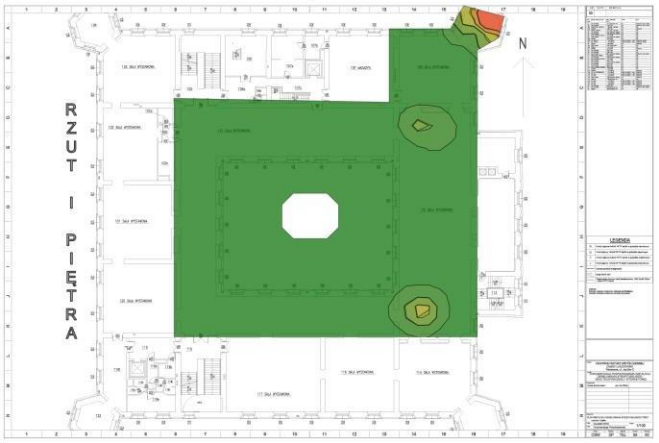
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 2,4 GHz

Wyświetla zmierzoną przepustowość.



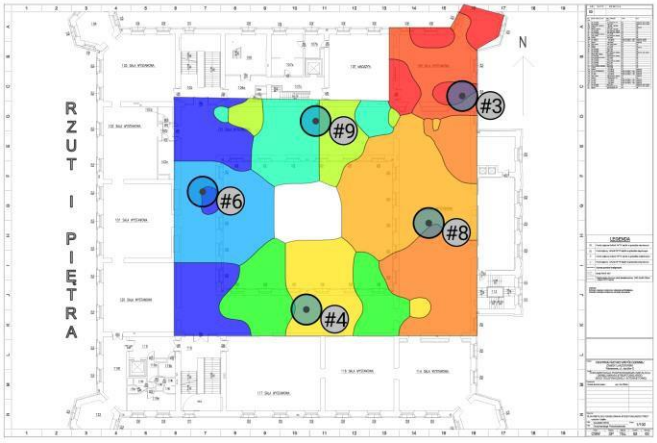
Przepustowość dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 5 GHz

Wyświetla zmierzoną przepustowość.



Powiązany punkt dostępowy Centrum Sztuki Współczesnej Zamek Ujazdowski

Wyświetla punkt dostępu , z którym jest skojarzone urządzenie klienckie . Obraz pokazuje przewidywane siły sygnału skojarzenia



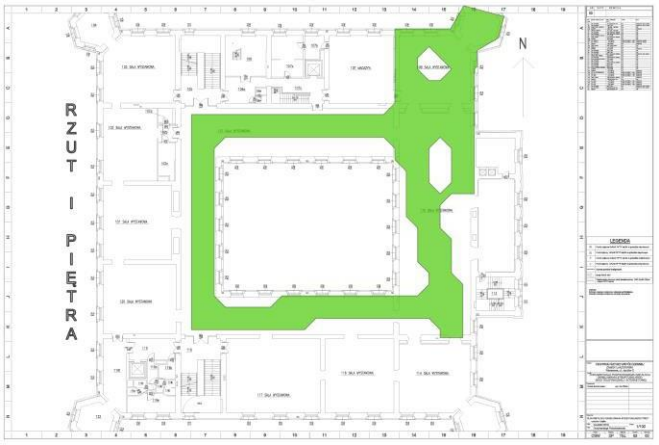
AP	Punkt dostępowy			
3	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14:	IAP30 5 IAP30

			C0	5
	standardu 802.11 AC standardu 802.11 AC	36 36	C8: B5: AD: F4:14: d0 C8: B5: AD: F4:14: d0	IAP30 5 IAP30 5
4	Hp			

	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC standardu 802.11 AC	36 36	C8: B5: AD: F4:14: d0 C8: B5: AD: F4:14: d0	IAP30 5 IAP30 5
6	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC	36	C8: B5: AD: F4:14: d0	IAP305
8	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC	36	C8: B5: AD: F4:14: d0	IAP305
9	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC standardu 802.11 AC	36 36	C8: B5: AD: F4:14: d0 C8: B5: AD: F4:14: d0	IAP30 5 IAP30 5

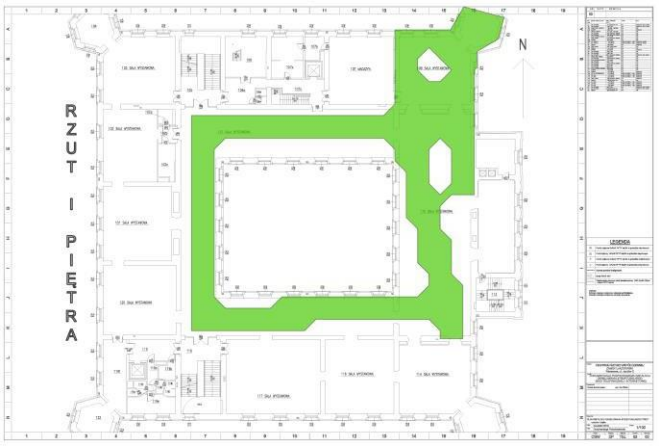
Wykorzystanie widma dla Centrum Sztuki Współczesnej Zamek Ujazdowski 2,4 w paśmie GHz

Wykorzystanie widma pokazuje czas , jaki moc widma mierzona jest przez Analizator widma

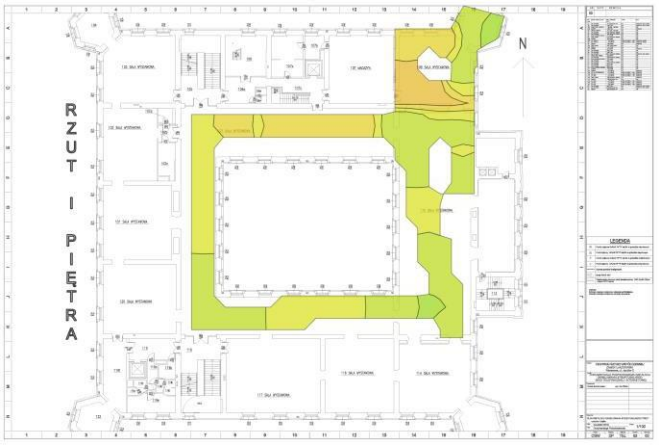


Wykorzystanie widma dla Centrum Sztuki Współczesnej Zamek Ujazdowski pasmo 5 GHz

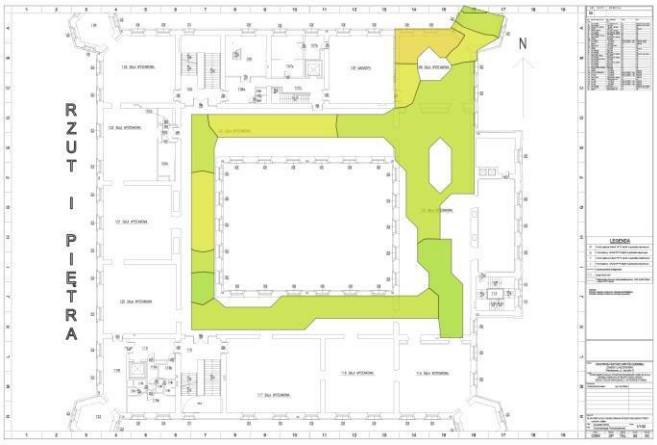
Wykorzystanie widma pokazuje czas , w którym moc widma mierzona przez Analizator widma jest na tyle wysoka , że kanał można znaczą zajęte.



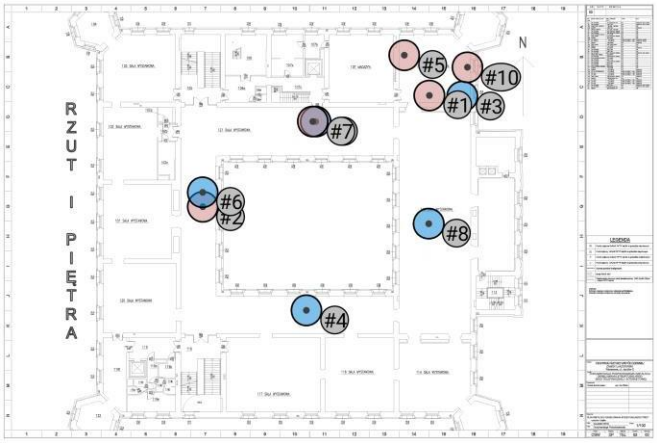
Moc kanału widma dla centrum Sztuki współczesnej zamek ujazdowskiego pasmo 2,4 GHz



Moc kanału widma dla centrum sztuki współczesnej zamek ujazdowskiego pasmo 5 GHz



Punkty dostępowowe na centrum sztuki współczesnej Zamek Ujazdowski



Moje punkty dostępu na centrum sztuki współczesnej Zamek Ujazdowski

Symulowane punkty dostępowe na centrum sztuki współczesnej Zamek Ujazdowski

Brak.

Zmierzone punkty dostępowy na centrum sztuki współczesnej Zamek Ujazdowski

AP	Punkt dostępowy			
3	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC standardu 802.11 AC	36 36	C8: B5: AD: F4:14: d0 C8: B5: AD: F4:14: d0	IAP30 5 IAP30 5
4	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC standardu 802.11 AC	36 36	C8: B5: AD: F4:14: d0 C8: B5: AD: F4:14: d0	IAP30 5 IAP30 5
6	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC	36	C8: B5: AD: F4:14: d0	IAP305
8	Hp			
	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC	36	C8: B5: AD: F4:14: d0	IAP305
9	Hp			

	802.11 n 802.11 n	1 1	C8: B5: AD: F4:14: C0 C8: B5: AD: F4:14: C0	IAP30 5 IAP30 5
	standardu 802.11 AC standardu 802.11 AC	36 36	C8: B5: AD: F4:14: d0 C8: B5: AD: F4:14: d0	IAP30 5 IAP30 5

Załącznik 2 do SIWZ – formularz ofertowy

FORMULARZ OFERTOWY

..……
/miejscowość i data/

……..
/pieczęć Wykonawcy/

Nazwa i siedziba /adres/ Wykonawcy/e-mail:

……

Do: **Centrum Sztuki Współczesnej Zamek Ujazdowski w Warszawie**. Nawiązując do ogłoszenia o przetargu nieograniczonym na: *Dostawę, montaż oraz konfigurację sieciowych urządzeń aktywnych dla Centrum Sztuki Współczesnej - Zamek Ujazdowski*, oświadczamy, iż oferujemy:

1) realizację przedmiotu zamówienia zgodnie z formularzem cenowym za cenę netto …..... zł (słownie: .....) + należny podatek VAT tj. za łączną cenę brutto: ..... zł (słownie: .....);
2) 55/65/75* dniowy termin realizacji przedmiotu umowy licząc od dnia podpisania umowy;

**** Uwaga. Należy wybrać jeden z trzech możliwych, oferowanych wariantów poprzez zakreślenie odpowiadającej mu liczy w numeracji.***

2. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia, nie wnosimy do niej zastrzeżeń oraz uzyskaliśmy konieczne informacje do przygotowania oferty i zobowiązujemy się spełnić wymienione w Specyfikacji wymagania i żądania Zamawiającego.
3. W sytuacji gdy przyjęcie oferty Wykonawcy wiązałoby się z powstaniem po stronie Zamawiającego obowiązku zapłaty podatku VAT, Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
4. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez czas wskazany w Specyfikacji Istotnych Warunków Zamówienia.
5. Oświadczamy, że zawarte w Specyfikacji Istotnych Warunków Zamówienia istotne postanowienia umowy zostały przez nas zaakceptowane i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy na w/w warunkach, w miejscu i terminie wskazanym przez Zamawiającego.
6. Oświadczamy, iż podany powyżej adres e-mailowy zobowiązujemy się utrzymywać w gotowości do przyjęcia transmisji przez okres trwania przedmiotowego postępowania.
7. Oświadczam, wypełniłem ciążące na mnie jako Administratorze danych osobowych w rozumieniu RODO obowiązki informacyjne przewidziane w art. 13 i/lub art. 14 RODO[1)]

wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

8. Załącznikami do niniejszej oferty są:

a. .....

/proszę wymienić wszystkie wymagane w SIWZ dokumenty/

Podpis:

……

Załącznik nr 2a do SIWZ – formularz cenowy

FORMULARZ CENOWY

L.p.	Rodzaj urządzenia	Producent, model / wersja	ilość	j.m.	cena jednostkowa PLN netto	Wartość netto PLN	Wartość brutto PLN
1.	**Przełącznik dostępowy**		**7**	**Szt.**			
2.	**Kontroler sieci WLAN**		**1**	**Szt.**			
3.	**Radiowy punkt dostępowy wewnętrzny**		**43**	**Szt.**			
4.	**Radiowy punkt dostępowy zewnętrzny**		**3**	**Szt.**			
5.	**Zapora sieciowa UTM**		**1**	**Szt.**			
6.	**Przełącznik dystrybucyjny**		**1**	**Szt.**			
					RAZEM		

Uwaga. W przypadku gdy Wykonawca nie wypełni kolumny dotyczącej określenia producenta i modelu oferowanego urządzenia jego oferta zostanie odrzucona.

....., dn. .....

.....
(podpis i pieczęć upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 3 do SIWZ - wzór oświadczenia wykonawcy o niepodleganiu wykluczeniu z postępowania.

ZAMAWIAJĄCY:

Centrum Sztuki Współczesnej Zamek Ujazdowski w Warszawie
ul. Jazdów 2, 00-467 Warszawa

Wykonawca:

……
……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy

składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.

Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. *na dostawę, montaż oraz konfigurację sieciowych urządzeń aktywnych dla Centrum Sztuki Współczesnej - Zamek Ujazdowski* oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust 1 pkt 12-23 ustawy Pzp.

……. *(miejscowość),* dnia ……. r.

……

(podpis)

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. 24 ust. 1 pkt 13-14, 16-20 ustawy Pzp. Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze: …….

……

……..……. *(miejscowość),* dnia ……. r.

……

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.: ……
……*(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)* nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

……..……. *(miejscowość),* dnia ……. r.

……

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

……..……. *(miejscowość),* dnia ……. r.

……

(podpis)

Załącznik nr 4 do SIWZ – wzór oświadczenia wykonawcy o spełnianiu warunków udziału w postępowaniu.

ZAMAWIAJĄCY:

Centrum Sztuki Współczesnej Zamek Ujazdowski w Warszawie
ul. Jazdów 2, 00-467 Warszawa

Wykonawca:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy

składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. *na dostawę, montaż oraz konfigurację sieciowych urządzeń aktywnych dla Centrum Sztuki Współczesnej - Zamek Ujazdowski*, prowadzonego przez Zamawiającego Centrum Sztuki Współczesnej Zamek Ujazdowski, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w pkt 8.1-3 siwz.

……. *(miejscowość),* dnia ……. r.

……

(podpis)

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w 8.1-3 siwz, polegam na zasobach następującego/ych podmiotu/ów...……..……
……., w następującym zakresie: ……

……
(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).

……..……. *(miejscowość),* dnia ……..……. r.

……

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

……..……. *(miejscowość),* dnia ……..……. r.

……

(podpis)

Załącznik nr 5 do SIWZ – wykaz dostaw

WYKAZ WYKONANYCH DOSTAW

L.p.:	Przedmiot zamówienia:	Wartość zamówienia:	Okres realizacji zamówienia:	Podmiot, na rzecz którego realizowana była dostawa
1.				
2.				

W załączeniu wykonawca ma obowiązek przedstawić dowody (referencje, itp.) potwierdzające, że dostawy wskazane w wykazie zostały wykonane w sposób należyty.

....., dn. ....

(podpis i pieczęć upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 6 do SIWZ – wzór umowy

WZÓR UMOWY

zawarta w dniu …… 2019 roku, pomiędzy:
Centrum Sztuki Współczesnej – Zamkiem Ujazdowskim, z siedzibą w Warszawie przy ul. Jazdów 2, wpisanym do Rejestru Instytucji Kultury prowadzonego przez Ministra Kultury Dziedzictwa Narodowego pod numerem RIK 15/92, posiadającym nr NIP: 526-025-12-85, zwanym dalej Zamawiającym, reprezentowanym przez:
1. Urszulę Kropiwiec – Zastępcę Dyrektora,
2. Jolantę Polańską – Główną Księgową.
a
……,
zwanym dalej Wykonawcą

Zgodnie z wynikiem przeprowadzonego na podstawie ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (t.J. Dz. U. z 2018 r. poz. 1986, z późn. zm.) o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, Strony zawierają umowę o następującej treści;

§1 Przedmiot umowy

1. Wykonawca zobowiązuje się zgodnie ze złożoną ofertą do realizacji *dostawy, montażu oraz konfiguracji sieciowych urządzeń aktywnych dla Centrum Sztuki Współczesnej - Zamek Ujazdowski* zaś Zamawiający zobowiązuje się do odbioru przedmiotu dostawy oraz zapłaty umówionej ceny.
2. Szczegółowy opis ww. przedmiotu zamówienia zawiera oferta Wykonawcy oraz załączniki nr 1 i 1a do SIWZ stanowiące integralne części umowy.

§2 Termin

Wykonawca zobowiązuje się zrealizować przedmiot umowy określony w § 1 w terminie …… dni licząc od dnia podpisania umowy z zastrzeżeniem, iż dostawa urządzeń musi zostać zrealizowana w terminie 30 dni licząc od dnia podpisania umowy.

§3 Wynagrodzenie

Za realizację przedmiotu umowy wskazanego w § 1 Wykonawcy przysługuje wynagrodzenie w wysokości netto: ……,00 zł (słownie: …… złote) plus należny podatek VAT, co stanowi łączną cenę brutto: ……,… zł (słownie: …… złotych ……/100).

§ 4 Faktury i płatności

1. Strony ustalają, że rozliczenie za realizację przedmiotu zamówienia nastąpi na podstawie faktury wystawionej przez Wykonawcę.
2. Należność Wykonawcy oparta na wystawionej fakturze będzie realizowana przelewem na konto bankowe podane na fakturze przez Wykonawcę w terminie 21 dni licząc od daty otrzymania przez Zamawiającego faktury od Wykonawcy wraz z bezwarunkowymi protokołami odbioru dostawy: protokołem ilościowym i protokołem jakościowym.

§ 5 Odbiór dostawy

1. Zamawiający dokona odbioru dostawy w siedzibie Zamawiającego sporządzając protokoły odbioru: ilościowy i jakościowy.
2. Strony postanawiają, że z czynności odbioru końcowego będzie spisany protokół zawierający wszelkie ustalenia dokonane w toku odbioru, w szczególności;

a) ustalenia ilościowe – stwierdzające kompletność Przedmiotu Zamówienia i brak zewnętrznych uszkodzeń

b) ustalenia jakościowe – stwierdzające zgodność parametrów dostarczonego Przedmiotu zamówienia z warunkami SIWZ (test przeprowadzony na dostarczonym i uruchomionym przez Wykonawcę Przedmiocie Zamówienia).

3. Wraz ze sprzętem Wykonawca dostarczy Zamawiającemu karty gwarancyjne oraz wszelkie pozostałe dokumenty pozwalające na używanie sprzętu zgodnie z jego przeznaczeniem.
4. Wykonawca zobowiązuje się do przyjęcia zwrotu i wymiany wadliwego przedmiotu umowy i pokrycia kosztów transportu z tym związanych.

§ 6 Gwarancja

Wykonawca udziela gwarancji na dostarczony przedmiot zamówienia w terminach i na warunkach zgodnych z określonymi w załącznikach nr 1 i 1 a do SIWZ.

§7 Przedstawiciele stron

1. Przedstawicielem Zamawiającego upoważnionym w sprawach związanych z niniejszą umową jest Rafał Filipowicz.
2. Przedstawicielem Wykonawcy upoważnionym w sprawach związanych z niniejszą umową jest ..... – .....

§8 Odstąpienie od umowy

1. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach.
2. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.

3. Ponadto, oprócz przypadków wymienionych w Kodeksie Cywilnym, Zamawiającemu przysługuje prawo odstąpienia od umowy w przypadku gdy Wykonawca nie wykona któregokolwiek z obowiązków określonych w umowie, po zażądaniu przez Zamawiającego spełnienia takiego zobowiązania i wyznaczeniu mu dodatkowego co najmniej 7 dniowego terminu.
4. Postanowienie o odstąpieniu od umowy nie umniejszy innych praw Zamawiającego według umowy lub z innego tytułu.
5. Odstąpienie od umowy powinno nastąpić w formie pisemnej pod rygorem nieważności i powinno zawierać uzasadnienie. Prawo odstąpienia Zamawiający może wykonać w terminie 30 dni od daty powzięcia wiadomości o podstawach do jego wykonania.

§9 Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne w wysokości:
   a) 10 % wartości brutto wskazanej w § 3 umowy w sytuacji, gdy Zamawiający albo Wykonawca odstąpi od umowy z powodu okoliczności leżących po stronie Wykonawcy,
   b) 0,2 % wartości brutto wskazanej w § 3 umowy za każdy dzień zwłoki Wykonawcy w wykonywaniu czynności wynikających z umowy,
   c) 0,2 % wartości brutto wskazanej w § 3 umowy za każdy przypadek nienależytego wykonania umowy,
   d) 0,2 % wartości brutto wskazanej w § 3 umowy za każdy przypadek nienależytego wykonania obowiązków gwarancyjnych.
2. W przypadku, gdy szkoda, jaką poniesie Zamawiający w związku z nienależytym wykonywaniem umowy przez Wykonawcę przekroczy wysokość kar umownych wskazanych w ust. 1 Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego na zasadach ogólnych w wysokości przewyższającej karę umowną.
3. Termin zapłaty kary umownej wynosi 14 dni od dnia skutecznego doręczenia Stronie wezwania do zapłaty. W razie opóźnienia z zapłatą kary umownej Zamawiający może żądać odsetek ustawowych za każdy dzień opóźnienia.
4. Zamawiający zastrzega sobie prawo do potrącenia należnych kar umownych z faktury wystawionej przez Wykonawcę.

§10 Warunki zmiany umowy

1. Wszelkie zmiany umowy wymagają zachowania formy pisemnej pod rygorem nieważności.
2. Zmiana umowy może nastąpić w razie zaistnienia okoliczności:

a) zmiana adresu/siedziby Zamawiającego/Wykonawcy,
b) zmiana osób występujących po stronie Zamawiającego/Wykonawcy,
c) zmiana będąca skutkiem poprawy oczywistej omyłki,
d) zmiana stawki podatku od towarów i usług (VAT),
e) zmiana urządzenia w przypadku gdy zaoferowane w ofercie urządzenie zostało wycofane z produkcji lub nie jest dostępne na rynku, co zostanie potwierdzone oświadczeniem producenta lub autoryzowanego dystrybutora. Zaoferowane urządzenie musi posiadać parametry nie gorsze niż określone w treści SIWZ,

f) zmiana terminu realizacji przedmiotu umowy - w przypadku wystąpienia okoliczności niezależnych od Wykonawcy, o zaistnieniu, których Wykonawca niezwłocznie powiadomi pisemnie Zamawiającego podając przyczynę i czas opóźnienia, a Zamawiający wyrazi zgodę na zmianę w tym zakresie.

3. Przyczyny dokonania zmian postanowień umowy oraz uzasadnienie takich zmian należy opisać w stosownych dokumentach (notatka służbowa, pismo Wykonawcy, itp.).
4. Projekt aneksu przygotuje Zamawiający.

§11 RODO

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO" Zamawiający, informuje, że:

1. Administratorem danych osobowych Wykonawcy i osoby wskazanej w §10 ust. 1 pkt 2) jest Centrum Sztuki Współczesnej Zamek Ujazdowski w Warszawie ul. Jazdów 2, 00-467 Warszawa.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się pod adresem email: iod@u-jazdowski.pl;
3. Dane osobowe Wykonawcy będą przetwarzane na podstawie art. 6 ust. 1 lit. b RODO w celu związanym z zawarciem umowy oraz jej realizacją oraz na podstawie art. 6 ust. 1 lit. f RODO. W przypadku przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO za prawnie uzasadniony interes Administratora uznaje się:
   3) ustalenie lub dochodzenie przez Administratora roszczeń cywilnoprawnych wynikających
      z realizacji niniejszej Umowy, a także obrona przed takimi roszczeniami;
   4) weryfikacja danych osobowych w publicznych rejestrach.
4. Odbiorcami danych osobowych Wykonawcy będą osoby lub podmioty upoważnione zgodnie z przepisami prawa powszechnie obowiązującego, oraz podmioty, które na podstawie stosownych umów przetwarzają dane osobowe powierzone do przetwarzania przez Administratora w związku z realizacją usług gwarantujących należyte wykonanie niniejszej Umowy;
5. Dane osobowe Wykonawcy będą przechowywane przez cały czas trwania umowy. W przypadku zawarcia i realizacji umowy obejmuje również okres niezbędny do zabezpieczenia ewentualnych roszczeń wynikających z umowy, chyba, że przepisy szczegółowe stanowią inaczej;
6. W odniesieniu do danych osobowych Wykonawcy decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
7. Wykonawca posiada:
   − na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących Wykonawcy;
   − na podstawie art. 16 RODO prawo do sprostowania danych osobowych Wykonawcy;

- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy Firma uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych, który administrator przetwarza na podstawie art. 6 ust. 1 lit. f RODO w związku z treścią pkt 3 i 5.

§12 Postanowienia końcowe

1. Ewentualne kwestie sporne wynikłe w trakcie realizacji niniejszej umowy strony rozstrzygać będą polubownie. W przypadku nie dojścia do porozumienia spory rozstrzygane będą przez sąd właściwy dla siedziby Zamawiającego.
2. W sprawach nie uregulowanych postanowieniami niniejszej umowy mają odpowiednie zastosowanie przepisy ustawy Prawo zamówień publicznych oraz kodeksu cywilnego.
3. Umowę sporządzono w 2 jednobrzmiących egzemplarzach po 1 dla każdej ze stron.

Zamawiający **Wykonawca**