Część II Zaprojektowanie i wykonanie sieci bezprzewodowej WiFi

Część II obejmuje zaprojektowanie, instalację, konfiguracja oraz wdrożenie systemu „ WiFi" w budynku Ośrodka Dokumentacji Sztuki Tadeusza Kantora Cricoteka przy ul. Nadwiślańskej 2-4 w Krakowie

Na dostarczone produkty i usługi Wykonawca musi udzielić gwarancji na okres nie krótszy niż 36 miesięcy i musi zapewnić serwis gwarancyjny (bezpłatny) i pogwarancyjny.

Dostarczone urządzenia muszą być w całości fabrycznie nowe (nieużywane) i wyprodukowane w 2013 lub 2014 roku, dobrej jakości, w pełni sprawne oraz pochodzić z bieżącej produkcji i z oficjalnego kanału dystrybucji producenta w Polsce, wyposażone w dokumentację użytkową. Oprogramowania (sterowniki oraz wszelkie inne oprogramowanie niezbędne do osiągnięcia funkcjonalności wymaganych przez Zamawiającego, za wyjątkiem systemu operacyjnego, który nie jest objęty niniejszym zamówieniem) muszą być dostarczone jako zapis na nośniku np. płyta CD, DVD i wyposażone w dokumenty licencyjne, dokumentację użytkową (może być w wersji elektronicznej na dostarczonym nośniku).

Sieć bezprzewodowa - wymagania

Zamawiający posiada nowowybudowany budynek wielokondygnacyjny A (muzeum) oraz przylegający budynek zrewitalizowany B (biura). Sieć WiFi będzie obejmować swoim zasięgiem budynek wielokondygnacyjny A o kubaturze 8675,10m3 budynek B o kubaturze 18043.90m3 oraz plac zewnętrzny znajdujący się obok budynku A i B o powierzchni 610m2. Wykonawca przed przystąpienie do złożenia oferty powinien we własnym zakresie dokonać niezbędnych pomiarów.

W ramach przedmiotu zamówienia Wykonawca zobowiązany będzie do:

- przygotowanie projektu i planu wdrożenia,
- wykonania mapy zasięgu,
- dostarczenia, instalacji i konfiguracji urządzeń
- przygotowanie harmonogramu szkoleń w oparciu o wymogi funkcjonalne systemu WiFi,
- przeprowadzenie szkolenia administratorów sieci,
- przygotowanie dokumentacji powdrożeniowej.

1. W ramach przedmiotu zamówienia Wykonawca zobowiązany jest do przygotowanie planu wdrożenia zawierającego:

(1) Czas rozpoczęcia realizacji przedmiotu umowy.
(2) Termin wykonania mapy zasięgu,
(3) Harmonogram szkoleń administratorów sieci,
(4) Imiona i nazwiska osób odpowiedzialnych za realizacje umowy po stronie Wykonawcy,
(5) Termin zakończenia - wykonania przedmiotu umowy.

Plan wdrożeń musi uwzględniać poniższe wymagania:

a) termin dostawy, montażu, instalacji i konfiguracji sprzętu komputerowego: serwera, przełączników, access pointów.

b) wykonanie mapy zasięgu sieci - wymagane do prawidłowego rozmieszczenia urządzeń wewnątrz budynku. Urządzenia powinny zapewnić 100% pokrycie sygnałem na przestrzeni budynku A i B oraz placu zewnętrznego. Zamawiający wskaże przed rozpoczęciem prac dokładne lokalizacje, które należy uwzględnić w projekcie.

c) szkolenie administratorów sieci musi odbywać się w trakcie wdrożenia, przed startem produktywnym oraz podczas użytkowania systemu. Charakter szkolenia musi być ściśle związany z docelową rolą administratora w ramach obsługi systemu WiFi. Szkolenia muszą mieć charakter warsztatowy i odbywać się z wykorzystaniem skonfigurowanego podczas wdrożenia systemu. Założeniem szkoleń dla administratorów jest uzyskanie sprawności w posługiwaniu się systemem WiFi pozwalającej na samodzielną pracę.

d) system WiFi musi być objęty 36 miesięcznym okresem gwarancji liczonym od dnia podpisania protokołu odbioru całości systemu, oraz objęty nieodpłatnym wsparciem technicznym przez cały okres gwarancji.

2. Rozmieszczenie urządzeń wymaga akceptacji przez Zamawiającego przed rozpoczęciem prac wdrożeniowych.

3. Przygotowanie dokumentacji powdrożeniowej, składającej się min. z planu rozmieszczenia urządzeń, wykonanej mapy zasięgu, przydzielonej adresacji IP i tras połączeniowych, opisu konfiguracji urządzeń oraz polityk bezpieczeństwa, procedur serwisowych (dane kontaktowe serwisu, plan postępowania).

Wymagania ogólne

- System zaprojektowany w architekturze klient – serwer
- Umożliwiający wykupienie asysty technicznej u producenta, dla oferowanych urządzeń oraz oprogramowania
- System posiadający konstrukcję modułową ze ściśle zdefiniowanymi powiązaniami i interfejsami międzymodułowymi oraz możliwość rozbudowy systemu
- System powinien być zintegrowany pod względem przepływu informacji - informacja raz wprowadzona do systemu w jakimkolwiek z modułów jest wielokrotnie wykorzystywana we wszystkich pozostałych.
- System ma zapewniać poprawną jednoczesną pracę min. 300 użytkowników
- System powinien być dostarczany w postaci pełnego zestawu instalacyjnego. W skład zestawu powinno wchodzić: wersja instalacyjna oprogramowania oraz szczegółowa instrukcja instalacji. Zestaw instalacyjny musi umożliwić przeszkolonemu administratorowi samodzielną instalację systemu.
- System powinien automatycznie sprawdzać wersje systemu, pozwalać na pobieranie i instalowanie kolejnej aktualizacji.
- System powinien posiadać możliwość pracy użytkowej przez 24 godziny na dobę, 7 dni w tygodniu
- System powinien generować kopie bezpieczeństwa na żądanie operatora oraz umożliwiać odtwarzanie bazy danych z kopii archiwalnej. Możliwość wykonania kopii w trakcie pracy użytkowników systemu, możliwość takiej konfiguracji systemu, aby w przypadku awarii w każdym momencie można odtworzyć dane bez ich utraty
- System powinien umożliwiać dostęp do zarchiwizowanych danych historycznych – logów
- System powinien umożliwiać eksport i import danych z bazy danych
- System powinien posiadać mechanizmy umożliwiające zapis i przeglądanie danych o logowaniu użytkowników do systemu pozwalająca na uzyskanie informacji o czasie i miejscach ich podłączenia
- System powinien umożliwiać administratorowi z poziomu aplikacji definiowanie i zmianę praw dostępu dla poszczególnych użytkowników i grup użytkowników
- W systemie powinny być zaimplementowane mechanizmy walidacji haseł zgodnie z wymaganiami ustawowymi przewidzianymi dla rodzaju danych przetwarzanych przez system
- System powinien umożliwiać eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków
- System może posiadać interfejs przeglądarkowy
- System powinien być zgodny z aktualnymi aktami prawnymi regulującymi działalność sektora podmiotów publicznych, zgodny z Ustawą o ochronie danych osobowych. System, w dniu przekazania w całości do odbioru musi być zgodny z aktami prawnymi obowiązującymi na dzień końcowego odbioru. W szczególności system będzie zgodny z:

Ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 21 lipca 2005 r. oraz aktami wykonawczymi do tej ustawy: określającymi minimalne wymagania dla systemów teleinformatycznych oraz minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie

elektronicznej, określonymi w rozporządzeniu Rady Ministrów z dnia 11 października 2005 r.;
- System powinien umożliwiać podgląd aktualnie zalogowanych do systemu użytkowników
- System powinien umożliwiać administratorowi z poziomu aplikacji definiowanie i zmianę praw dostępu dla poszczególnych użytkowników i grup użytkowników z dokładnością do poszczególnych modułów, funkcjonalności, rodzaju wykonywanej operacji
- Producent powinien zapewnić co najmniej 5 letni okres rozwoju oprogramowania i dostosowania do obowiązujących przepisów prawa. Producent zapewni wsparcie techniczne systemu
- Powinien umożliwić użytkownikom dostęp do aplikacji i jej modułów w oparciu o login i hasło i/lub captitive portal
- System powinien pozwolić na określenie praw dostępu użytkownikom do poszczególnych elementów
- Powinien umożliwić przegląd zalogowanych użytkowników i wysyłanie dowolnej treści komunikatów, wszystkim lub wybranym użytkownikom
- Powinien umożliwić wymuszenie zamknięcia połączenia użytkownikowi z poziomu administratora
- Sieć wifi powinna być jednolita we wszystkich miejscach objętych zasięgiem tzn SSID danej sieci powinien być niezmienny na wszystkich routerach a urządzenia klienckie powinny się przepinać automatycznie do najbliższego punktu AP
- System powinien zapewnić wystawienie jednocześnie minimum 2 sieci o różnych identyfikatorach SSID logicznie ze sobą oddzielonych tak aby użytkownicy sieci nie mogli się między sobą komunikować.
- System powinien być wyposażony w portal autoryzacyjny tzw. "captitive portal" umożliwiający autoryzację użytkowników sieci poprzez podanie odpowiednich danych w tym np adresu e-mail oraz wyświetlenie opracowanego przez zamawiającego regulaminu korzystania z sieci.
- System powinien umożliwiać integrację z serwerem domeny tak aby użytkownicy zarejestrowani w domenie Active Directory systemu Windows Server 2008 mogli autoryzować swój dostęp do sieci wifi korzystając z haseł zapisanych na ich kontach domenowych.
- System powinien być wyposażony w detekcję obcego routera jako urządzenia klienckiego i posiadać możliwość blokady dostępu dla takich urządzeń.
- System powinien być wyposażony w detekcję obcego routera nadającego sygnał o identycznym ssid oraz posiadać możliwość zagłuszania takiego urządzenia.
- System powinien być wyposażony w mechanizm przechowywania logów dostępowych klientów sieci wifi przez okres conajmniej 3 lat oraz konsolę która pozwoli na wprowadzenie filtrów i wyszukanie konkretnego klienta i połączeń jakie nawiązał w zadanym okresie czasu poprzez jego np MAC adres, e-mail, IP adres itp.
- System powinien być wyposażony w mechanizm umożliwiający zrywanie sesji z urządzeniem klienckim zautoryzowanym poprzez "captitive portal" po określonym odstępie czasu, tak aby użytkownik ponownie musiał wykonać autoryzację.
- Rozwiązanie musi zapewniać narzędzie do zarządzania min. dwukrotnością dostarczonych urządzeń takich jak przełącznik sieciowy lub kontroler sieci WLAN
- Rozwiązanie musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci
- Musi pozwalać na centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji
- Musi dostarczać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia
- Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II
- Musi pozwalać na monitorowanie całego systemu i wdrażanie w nim konfiguracji VLAN
- Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware,
- Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania
- Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB (Management Information Base) z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB
- Musi dawać możliwość prezentowania szczegółowych informacji konfiguracyjnych, w tym daty i godziny zapisów konfiguracji, wersji oprogramowania firmware i wielkości pliku konfiguracyjnego

- Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń
- Musi umożliwiać pobieranie oprogramowania firmware do jednego urządzenia lub do wielu urządzeń jednocześnie
- Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby
- Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych w czasie rzeczywistym
- Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci
- Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia
- Musi pozwalać na izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji
- System musi zawierać zintegrowane aplikacje typu plug-in, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania.
- Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami sieci przewodowej.
- Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej
- Musi mieć możliwość instalacji, jako maszyna wirtualna
- Rozwiązanie musi integrować się ze środowiskiem wirtualnym:
Musi posiadać wsparcie dla VMware ESX i ESXi
Musi posiadać wsparcie dla Citrix XEN
Musi posiadać wsparcie dla Microsoft HyperV
- Musi zapewniać obsługę funkcji wysokiej dostępności (High Availability)
- Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń)
- Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu
- Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci
- Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (OID)
- Musi pozwalać na analizę na poziomie portu
- Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń
- Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu firmware urządzenia
- Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych
- Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów
- Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji
- Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC
- Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku
- Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 Trap (Inform)
- Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania
- Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS
- Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https
- Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https. Musi mieć możliwość definiowania polityk:
* ograniczających poziom pasma,
* ograniczających liczbę nowych połączeń sieciowych,

* ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3,
* nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania
- Musi posiadać trzyletnią gwarancję producenta z wymianą na następny dzień roboczy, z dostępem do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.

Dostawca dostarczy sprzęt w ilości niezbędnej do pokrycia zasięgiem WiFi powierzchni wyspecyfikowanej przez zamawiającego oraz wszystkie wymagane do tego dodatkowe elementy oraz licencje.

Minimalne wymagania – punkt dostępowy

1. Porty sieciowe minimum 1x 1gb z funkcją POE
2. Standard sieci A/B/G/N
3. Minimum 2 sieci bezprzewodowe całkowicie odizolowane od siebie technologią VLAN lub równoważną
4. Zabezpieczenia WEP/WPA/WPA2 TKIP/AES
5. Centralne zarządzanie

Minimalne wymagania – serwer dystrybucyjny

1. Procesor 7000 punktów w teście CPU Benchmark ttp://www.cpubenchmark.net
2. Pamięć RAM 16GB
3. Karta sieciowa 2 portowa
4. Pamięć masowa minimum 2x64GB SAS lub SSD pracujące w trybie RAID-1
5. Obudowa Rack 1U głębokość max 800mm
6. Minimum 2 zasilacze pracujące w trybie redundantnym
7 .Dedykowany port do zdalnego zarządzania serwerem poprzez standard IPMI

Dopuszczalne jest także uruchomienie serwera dystrybucyjnego w środowisku wirtualizacyjnym zamawiającego w formie maszyny wirtualnej zamiast dostawy sprzętowego serwera dystrybucyjnego. W takim przypadku wykonawca musi podać wymagania maszyny wirtualnej w celu uruchomienia serwera dystrybucyjnego.

Minimalne wymagania – przełącznik zarządzalny (switch)

1. Ilość portów Min. 10/100/1000Mbit
2. Ilość portów SFP Min 2x1000Mbit
3. Obsługa standardów POE na wszystkich portach RJ45
4. Wydajność (przepustowość wewn) min. 16Gbps
5. Stackowalny, zarządzalny, przystosowany do montażu w obudowie RACK
6. Musi posiadać gwarancję obejmującą aktualizację oprogramowania firmware oraz patce naprawiające błędy oprogramowania (bug fixes), poza tym wsparcie telefoniczne oraz zaawansowaną wymianę sprzętu (z wysyłką następnego dnia roboczego)