ZAŁĄCZNIK NR I

OPIS PRZEDMIOTU ZAMÓWIENIA

I. PRZEDMIOTEM zamówienia „Dostawa i instalacja urządzeń aktywnych oraz projekt i wykonanie sieci światłowodowej dla realizacji projektu „Kompleksowy rozwój infrastruktury społeczeństwa informacyjnego w Gminie Miasto Zgierz" jest:

1. zaprojektowanie i wdrożenie polityki bezpieczeństwa infrastruktury przetwarzania danych w UMZ,
2. dostawa, instalacja i konfiguracja urządzeń aktywnych lokalnej sieci teleinformatycznej,
3. dostawa, instalacja i konfiguracja centrum zarządzania siecią teleinformatyczną,
4. wykonanie projektu sieci optotelekomunikacyjnej łączącej wybrane lokalizacje na terenie miasta Zgierza,
5. wykonanie sieci światłowodowej pomiędzy budynkami UMZ oraz pomiędzy wskazanymi lokalizacjami jednostek organizacyjnych UMZ.

Ia. Wymagania formalne

1. Sieć powstała w wyniku niniejszego zamówienia musi funkcjonować zgodnie z odpowiednimi, obowiązującymi przepisami prawa budowlanego i telekomunikacyjnego.
2. Całość oferowanego sprzętu musi być fabrycznie nowa

Ib. Wymagania związane z promocją unijnego źródła dofinansowania.

1. Sprzęt i oprogramowanie dostarczone w ramach projektu jako zakupione przy współudziale środków z Funduszy Strukturalnych, muszą być oznaczone zgodnie z: Rozporządzeniem Komisji Europejskiej (WE) nr 1159/2000 z dnia 30.05.2000 r. w sprawie wprowadzenia przez Państwa Członkowskie działań informacyjnych i promocyjnych dot. pomocy udzielanej z Funduszy Strukturalnych oraz wytycznych Instytucji Zarządzającej ZPORR. Wszystkie materiały informacyjne i promocyjne, a także dokumenty stosowane podczas realizacji projektu muszą zawierać Logo Unii Europejskiej, Logo ZPORR i informację o EFRR (wraz z tekstem opisującym fundusz).
2. Działania promocyjne zostaną przygotowane, zgodnie z wymogami artykułu 46 Rozporządzenia Rady (WE) nr 1260/1999 z dnia 21.06.1999 r. ustanawiające przepisy ogólne w sprawie funduszy strukturalnych, według wytycznych Planu Promocji ZPORR „Wsparcie Rozwoju Regionalnego w Polsce ze Środków Funduszy Strukturalnych".

Ic. Wymagania, co do harmonogramu realizacji projektu

1. Zamawiający wymaga realizacji przedmiotu zamówienia w dwóch etapach, z czego:

a. etap I - obejmuje realizację zakresu rzeczowego określonego w pkt I ppkt 1, 2, 3 **w terminie do 31.05.2008 r.**

b. etap II - obejmuje realizację zakresu rzeczowego określonego w pkt I ppkt 4, 5 **w terminie do 30.11.2008 r.**

2. Prace realizowane w ramach poszczególnych etapów będą rozliczane na podstawie odbiorów cząstkowych.

3. Ostatecznym terminem zakończenia całego projektu jest 30 listopada 2008 r.

Id. Wymagania ogólne dla dostarczanych rozwiązań

1. całość dostarczanego sprzętu musi być fabrycznie nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana we wcześniejszych projektach – wraz z dostawą należy dostarczyć oświadczenia producentów (lub ich polskich przedstawicielstw) potwierdzające datę produkcji urządzeń,
2. całość dostarczonego sprzętu musi być objęta minimum 3-letnią gwarancją opartą o oświadczenia gwarancyjne producentów - do oferty należy dołączyć odpowiednie oświadczenia Wykonawcy i producentów urządzeń,
3. ze względu na konieczność sprawnego funkcjonowania centrum zarządzania siecią wymagana jest pełna kompatybilność urządzeń oraz oprogramowania dostarczanych w ramach zamówienia. Proponowane rozwiązanie powinno pochodzić od jednego producenta, chyba że wymagania szczegółowe stanowią inaczej; w przypadku oferowania urządzeń różnych producentów, należy dostarczyć oświadczenia ich producentów o pełnej wzajemnej kompatybilności oraz oświadczenia producentów o współpracy ich autoryzowanych placówek serwisowych w zakresie usuwania problemów powstających na styku rozwiązań

II. SZCZEGÓŁOWY ZAKRES ZAMÓWIENIA:

1. Wymagania w zakresie polityki bezpieczeństwa infrastruktury przetwarzania danych

W zakresie zaprojektowania i wdrożenia polityki bezpieczeństwa w sferze dotyczącej bezpieczeństwa teleinformatycznego wymagane jest wykonanie następujących prac:

1. Inwentaryzacja elementów sieci:
   - 1.1. stosowanych adresów sieciowych
   - 1.2. urządzeń aktywnych (routerów, przełączników itp.)
   - 1.3. tras routingu
   - 1.4. VLanów
   - 1.5. aktualnej konfiguracji sieci
2. Stworzenie diagramu sieci
3. Stworzenie polityki bezpieczeństwa informacji w zakresie dostępu do systemów
   - 3.1. Potrzeby biznesowe związane z dostępem do systemu
     - 3.1.1. Polityka kontroli dostępu
   - 3.2. Zarządzanie dostępem użytkowników
     - 3.2.1. Rejestracja użytkowników, procedury nadawania i odbierania dostępu
     - 3.2.2. Zarządzanie przywilejami
     - 3.2.3. Zarządzanie hasłami użytkowników
     - 3.2.4. Przegląd praw dostępu użytkowników
   - 3.3. Zakres odpowiedzialności użytkowników
     - 3.3.1. Procedury dotyczące haseł
     - 3.3.2. Procedury dotyczące kontroli dostępu do stacji roboczych
     - 3.3.3. Procedury dotyczące dostępu do danych

3.3.4. Procedury dotyczące nośników danych

3.3.5. Procedury dotyczące ochrony danych przed utratą

3.4. Kontrola dostępu do sieci

3.4.1. Polityka dotycząca korzystania z usług sieciowych

3.4.2. Wymuszanie dróg połączeń

3.4.3. Uwierzytelnianie użytkowników przy połączeniach zewnętrznych

3.4.4. Uwierzytelnianie węzłów

3.4.5. Ochrona zdalnych portów diagnostycznych

3.4.6. Rozdzielenie sieci

3.4.7. Kontrola połączeń sieciowych

3.4.8. Kontrola routingu w sieciach

3.4.9. Bezpieczeństwo usług sieciowych

3.5. Kontrola dostępu do systemów aplikacyjnych

3.5.1. Automatyczna identyfikacja terminalu

3.5.2. Procedury rejestrowania terminalu w systemie

3.5.3. Identyfikacja i uwierzytelnienie użytkowników

3.5.4. System zarządzania hasłami

3.5.5. Użycie systemowych programów narzędziowych

3.5.6. Automatyczne blokowanie stacji roboczych

3.5.7. Ograniczanie czasu trwania połączenia

3.6. Kontrola dostępu do aplikacji

3.6.1. Ograniczanie dostępu do informacji

3.6.2. Izolowanie systemów wrażliwych

3.7. Monitorowanie dostępu do systemu

3.7.1. Zapisywanie informacji o zdarzeniach

3.7.2. Zapisywanie informacji o autoryzowanych i nieautoryzowanych dostępach

3.7.3. Synchronizacja czasu w logach systemowych

3.8. Komputery przenośne i praca na odległość

3.8.1. Komputery przenośne

3.8.2. Praca na odległość, zasady dostępu z systemów zdalnych

4. Projekt sieci (adresacja , konfiguracja, diagram)

4.1. DNS i przestrzeń nazw

4.1.1. Identyfikacja zewnętrznych wymogów nazewniczych

4.1.2. Identyfikacja wewnętrznych wymogów nazewniczych

4.1.3. Wybór proponowanej nazwy domeny głównej

4.1.4. Dokumentacja proponowanego projektu głównej przestrzeni nazw

4.2. Opracowanie architektury domeny lub lasu AD

4.2.1. Definicja kryteriów tworzenia domen Active Directory

4.2.2. Opracowanie proponowanej architektury domeny/drzewa domen

4.2.3. Dokumentacja proponowanej architektury domeny/drzewa domen

4.3. Active Directory

4.3.1. Propozycja konwencji nazywania serwerów

4.3.2. Propozycja konwencji nazywania komputerów

4.3.3. Dokumentacja proponowanej konwencji nazewniczej

4.4. Projekt DNS-u

4.4.1. Przegląd architektury przestrzeni nazw usług Active Directory

4.4.2. Propozycja projektu struktury DNS

4.4.3. Zgromadzenie wymagań współpracy DNS-u z systemami zależnymi od usługi DNS

4.4.4. Opracowanie zależności do współpracy dla Active Directory i DNS-u

4.4.5. Opracowanie modelu zarządzania DNS-em

4.4.6. Dokumentacja stref DNS i modelu zarządzania

4.5. Opracowanie architektury OU

4.5.1. Definicja kryteriów tworzenia OU Active Direktory

4.5.2. Opracowanie proponowanej architektury OU

4.5.3. Dokumentacja proponowanej architektury OU

4.6. Projekt grup i użytkowników

4.6.1. Opracowanie wytycznych dla grup i użytkowników

4.6.2. Opracowanie konwencji nazewniczych dla użytkowników (pełna nazwa konta użytkownika, nazwy UPN, nazwy dla systemów starszych niż Windows 2003)

4.6.3. Opracowanie konwencji nazewniczych dla grup

4.6.4. Dokumentacja proponowanego projektu użytkowników i grup

5. Projekt integracji Active Directory z systemami zewnętrznymi (składowania kont użytkowników i innych informacji ważnych dla integracji z aplikacjami innych producentów, sprzętem sieciowym i innymi systemami operacyjnymi)
6. Uaktualnienie stacji roboczych do poziomu pozwalającego na używanie Active Direktory. (readresacja zgodnie z projektem sieci oraz instalacja stosownego oprogramowania)
7. Stworzenie projektu implementacji domeny Windows

   7.1. Utworzenie wstępnego harmonogramu implementacji

   7.2. Opracowanie procedur testowania
8. Przeprowadzenie dowodu poprawności koncepcji (stanowisko testowe).

   8.1. Zestawienie laboratorium do testów

   8.2. Ustalenie typowych wymagań pojemności i sprzętu

   8.3. Opracowanie metod zapewnienia jakości

8.4. Dokumentacja proponowanego planu instalacji

9. Uruchomienie pilotowe (produkcyjne) w wybranym obszarze sieci UMZ
10. Wdrożenie domeny.
11. Dokumentacja wdrożenia domeny

2. Wymagania w zakresie funkcjonalności urządzeń aktywnych sieci informatycznej:

2.1 Zabezpieczenie styku z siecią publiczną

Do łączności z Internetem zaplanowane jest wykorzystanie łącza o przepustowości 10 Mb/s. Styk z publiczną siecią Internet powinien realizować kilka funkcji, w tym dostęp lokalnych użytkowników do zasobów Internetu, wymianę korespondencji elektronicznej, publikację informacji urzędowych, ochronę lokalnych zasobów przed nieuprawnionym dostępem z zewnątrz, oraz bezpieczne połączenia z innymi organizacjami. Wszystkie te funkcje mogą być technicznie połączone w jednym urządzeniu. Przy projektowaniu rozwiązania należy uwzględnić aspekt bezpiecznej i niezawodnej publikacji usług sieciowych (witryna WWW, BIP, Portal, Elektroniczna Skrzynka Podawcza).

Minimalne wymagania dla urządzenia zabezpieczenia styku z siecią publiczną:

1. urządzenie modularne pozwalające na uzyskanie funkcji firewall, VPN (sprzętowe wsparcie szyfracji), sondy IPS, kontroli ruchu
2. wyposażone w co najmniej cztery interfejsy Gigabit Ethernet 10/100/1000
3. wyposażone w co najmniej jeden interfejs dla zarządzania pozapasmowego (OOB)
4. wyposażone w moduł sprzętowego wsparcia szyfracji DES i AES
5. minimum dwa porty dedykowane dla zarządzania: port konsoli, port asynchroniczny dla przyłączenia modemu
6. co najmniej jeden port USB (tokeny, certyfikaty etc.)
7. co najmniej 64MB pamięci Flash
8. co najmniej 512MB pamięci DRAM
9. dodatkowy slot pozwalający na wykorzystanie modułów funkcjonalnych zwiększających standardową funkcjonalność urządzenia, a w szczególności
   9.1. moduł umożliwiający osiągniecie pełnej funkcjonalności systemu IPS (Intrusion Prevention System)
   9.2. moduł umożliwiający osiągniecie funkcjonalności ochrony antywirusowej, antyspyware, antyspamowej, filtrowania i blokowania odwołań do niepożądanych adresów URL oraz filtrowania zawartości poczty elektronicznej e-mail
   9.3. moduł zwiększający ilość obsługiwanych interfejsów o co najmniej 4 porty Gigabit Ethernet
10. zasilacz umożliwiający zasilanie prądem przemiennym 230V
11. wydajność
    11.1. co najmniej 450 Mbps ruchu poddawanego inspekcji przez mechanizmy ściany ogniowej
    11.2. co najmniej 225 Mbps ruchu szyfrowanego
    11.3. terminowanie co najmniej 750 jednoczesnych sesji VPN

11.4. możliwość terminowania jednocześnie 750 sesji WebVPN

11.5. obsługa co najmniej 280000 jednoczesnych sesji/połączeń z prędkością 9000 połączeń na sekundę

11.6. obsługa do 20 wirtualnych instancji firewall

12. ściana ogniowa śledząca stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
13. bez ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
14. dostarczone wraz z dedykowanym oprogramowaniem klienta VPN. Oprogramowanie musi mieć możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows, Solaris i Linux, a także komputerach Mac. Oprogramowanie musi umożliwiać zestawienie do urządzenia stanowiącego przedmiot postępowania połączeń VPN z komputerów osobistych PC. Oprogramowanie to powinno pochodzić od tego samego producenta, co oferowane urządzenie i powinno być objęte jego jednolitym wsparciem technicznym.
15. możliwość operowania jako transparentna ściana ogniowa warstwy drugiej ISO OSI
16. możliwość routingu pakietów zgodnie z protokołami RIP, OSPF
17. mechanizmy związane z obsługą ruchu multicast
18. protokół NTP
19. obsługa IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode
20. współpraca z serwerami CA
21. funkcjonalność Network Address Translation (NAT)
22. mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w modelu active/standby oraz active/active
23. funkcjonalność stateful Failover dla ruchu VPN
24. mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:

    24.1. Hypertext Transfer Protocol (HTTP),

    24.2. File Transfer Protocol (FTP),

    24.3. Extended Simple Mail Transfer Protocol (ESMTP),

    24.4. Domain Name System (DNS),

    24.5. Simple Network Management Protocol (SNMP),

    24.6. Internet Control Message Protocol (ICMP),

    24.7. SQL*Net,

    24.8. Network File System (NFS),

    24.9. H.323 (wersje 1-4),

    24.10. Session Initiation Protocol (SIP),

    24.11. Real-Time Streaming Protocol (RTSP),

    24.12. Lightweight Directory Access Protocol (LDAP), Internet Locator Service (ILS),

    24.13. Sun Remote Procedure Call (RPC)

25. inspekcja ruchu głosowego w zakresie protokołów H.323, SIP

26. możliwość blokowania aplikacji tunelowanych z użyciem portu 80 w tym:
    26.1. blokowanie komunikatorów internetowycy w tym AOL Instant Messenger, Microsoft Messenger, Yahoo Messenger
    26.2. blokowanie aplikacji typu peer-to-peer w tym KaZaA i Gnutella
    26.3. zapobieganie stosowaniu aplikacji typu GoToMyPC
27. obsługa protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP w tym:
    27.1. AUTH,
    27.2. DATA,
    27.3. EHLO,
    27.4. ETRN,
    27.5. HELO,
    27.6. HELP,
    27.7. MAIL,
    27.8. NOOP,
    27.9. QUIT,
    27.10. RCPT,
    27.11. RSET,
    27.12. SAML,
    27.13. SEND,
    27.14. SOML,
    27.15. VRFY
28. możliwość inspekcji protokołów HTTP oraz FTP na nie standartowych portach
29. wsparcie stosu protokołów IPv6 w tym:
    29.1. dla list kontroli dostępu dla IPv6
    29.2. inspekcji aplikacyjnej co najmniej dla protokołów
        29.2.1. HTTP,
        29.2.2. FTP,
        29.2.3. SMTP,
        29.2.4. ICMP,
30. mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu
31. współpraca z serwerami autoryzacji (RADIUS, TACACS+ lub równoważny) w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik, o wielkości przekraczającej 4KB
32. zarządzanie i konfiguracja:
    32.1. możliwość eksportu informacji przez syslog
    32.2. możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu RADIUS, TACACS+ lub równoważnego

32.3. konfigurowalne przez CLI oraz interfejs graficzny (oczekiwane są narzędzia dodatkowe w postaci kreatorów połączeń, etc.)

32.4. dostęp do urządzenia przez SSHv1 i SSHv2

32.5. obsługa funkcji SCP

32.6. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją

32.7. urządzenie musi umożliwiać jednoczesne przechowywanie w pamięci nie ulotnej co najmniej 3 niezależnych konfiguracji urządzenia

33. obudowa wykonana z metalu, nie dopuszcza się stosowania urządzeń w obudowie plastikowej

34. możliwość instalacji w rack 19”

35. normy bezpieczeństwa i normy dla oddziaływania elektromagnetycznego:

35.1. EN 60950 IEC 60950

35.2. Znak CE

35.3. EN55022 Class A

35.4. EN61000-3-2,

35.5. EN61000-3-3

36. certyfikacje branżowe

36.1. FIPS 140-2 Level 2

36.2. Common Criteria EAL4+

37. zainstalowany moduł rozszerzający funkcjonalność o kontrolę ruchu:

37.1. funkcjonalność Anti-X zapewniając ochronę aplikacyjną dla organizacji

37.2. ochrona antywirusowa dla hostów ukrytych za urządzeniem poprzez wykrywanie i usuwanie wirusów z ruchu web oraz z treści przesyłek mail

37.3. filtracja oprogramowania typu spyware z treści poczty elektronicznej oraz z ruchu internetowego (www)

37.4. ochrona przed spamem

37.5. ochrona przed ujawnieniem informacji organizacji oraz informacji osobistych użytkownikom osobom niepowołanym poprzez zapewnienie mechanizmów Anti-Phishing

37.6. automatyczne pobierania aktualizacji dotyczących wirusów, spamu oraz oprogramowania szpiegującego (spyware)

37.7. możliwość scentralizowanego zarządzania

37.8. możliwość filtrowania ruchu w oparciu o URL

37.9. filtracja zawartości poczty elektronicznej przechodzącej przez moduł

37.10. ochrona dla co najmniej 250 użytkowników wewnętrznych z możliwością rozbudowy do co najmniej 500 użytkowników wewnętrznych

2.2 Router

Minimalne wymagania dla routera:

1. urządzenie modularne, pełniące funkcję bramy do sieci publicznej transmisji danych
2. możliwość rozbudowy o funkcjonalność bramy głosowej H.323 i SIP
3. urządzenie w stanie nie obsadzonym musi mieć możliwość instalacji modułów:
   - 3.1. moduł poczty głosowej współdziałającej z oferowanym systemem komunikacyjnym (min. 50 skrzynek z możliwością nagrania min. 100 godzin głosu) – min. 1 moduł
   - 3.2. z portami głosowymi FXO - o gęstości co najmniej 4 porty na moduł – min. 4 moduły
   - 3.3. z portami głosowymi FXS/DID - o gęstości co najmniej 4 porty na moduł – min. 4 moduły
   - 3.4. z portami głosowymi E&M- o gęstości co najmniej 2 porty na moduł – min. 4 moduły
   - 3.5. z portami głosowymi ISDN BRI - o gęstości co najmniej 2 porty na moduł – min. 4 moduły
   - 3.6. z portami głosowymi ISDN PRI - o gęstości co najmniej 2 porty na moduł – min. 4 moduły
   - 3.7. moduł Voice over IP z minimum 8 portami FXS – min. 1 moduł
   - 3.8. z przełącznikiem Ethernet - o gęstości co najmniej 16 portów na moduł – min. 2 moduły
   - 3.9. moduł Intrusion Detection System o wydajności co najmniej 45 Mbps – min. 1 moduł
   - 3.10. moduł analizatora sieciowego – min. 2 moduły
   - 3.11. z interfejsem ISDN BRI (styk S/T) - o gęstości co najmniej 8 portów na moduł – min. 2 moduły
   - 3.12. z portami szeregowymi – o gęstości co najmniej 2 porty na moduł – min. 4 moduły
   - 3.13. z interfejsem ISDN BRI (styk S/T) - o gęstości co najmniej 1 port na moduł – min. 4 moduły
4. możliwość instalacji min. 2 modułów funkcyjnych:
   - 4.1. sprzętowego modułu wsparcia szyfrowania
   - 4.2. ATM IMA
   - 4.3. w przypadku gdy moduły funkcyjne zajmują sloty przewidziane na interfejsy sieciowe, konieczne jest zapewnienie dodatkowych 2 wolnych slotów
5. możliwość instalacji min. 4 procesorów DSP:
   - 5.1. gęstość nie mniejsza niż 64 kanały na moduł
   - 5.2. pozwalające na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing) z granulacją do 1 DSP.
   - 5.3. w przypadku gdy moduły DSP zajmują sloty przewidziane na interfejsy sieciowe, konieczne jest zapewnienie dodatkowych 4 wolnych slotów

6. wyposażone w co najmniej dwa interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN. Jeden z interfejsów musi pracować w trybie „dual-physical" z gigabitowym portem światłowodowym definiowanym przez GBIC lub SFP. Dopuszcza się zastosowanie urządzenia z trzema portami Gigabit Ethernet, w tym jednym gigabitowym portem światłowodowym definiowanym przez GBIC lub SFP.
7. wyposażone w min. 2 interfejsy szeregowe, mogące pracować jako V.35, EIA/TIA-449, EIA/TIA-232 i X.21
8. wszystkie interfejsy muszą być „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
9. wyposażone w zintegrowany wewnętrzny moduł sprzętowego wsparcia szyfracji DES, 3DES, AES128, AES192, AES256 o wydajności min. 150 Mbps
10. minimum 2 porty USB, umożliwiające podłączanie zewnętrznej pamięci stałej oraz tokenów uwierzytelniających
11. minimum dwa porty dedykowane dla zarządzania: port konsoli, port asynchroniczny dla przyłączenia modemu
12. co najmniej 64MB pamięci Flash i możliwość jej rozbudowy do minimum 256MB
13. co najmniej 256MB pamięci DRAM i możliwość jej rozbudowy do minimum 1024MB
14. zasilanie:
    - 14.1. zasilanie ze źródeł zmiennoprądowych 230V (zasilacze AC)
    - 14.2. wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V
    - 14.3. urządzenie musi umożliwiać doprowadzenie zasilania do portów Ethernet (tzw. inline-power) - w dostępnych w ofercie producenta modułach sieciowych – bez stosowania dodatkowych zewnętrznych urządzeń (zasilacze, panele etc.)
15. możliwość rozbudowy funkcjonalności o funkcje wirtualnej centralki abonenckiej IP:
    - 15.1. obsługa min. 160 urządzeń końcowych IP (telefony, stacje konferencyjne, oprogramowanie klienckie) min. dla protokołów sygnalizacyjnych SIP, H.323
    - 15.2. obsługa aplikacji XML dla telefonów IP
    - 15.3. funkcjonalności abonenckie:
      - 15.3.1. przekazywanie połączeń (wszystkie / nie odbieram / zajęte)
      - 15.3.2. tryb „nie przeszkadzać"
      - 15.3.3. połączenia oczekujące
      - 15.3.4. hook-flash
      - 15.3.5. mobilny profil użytkownika (możliwość logowania się na aparacie telefonicznym; po zalogowaniu dostęp do własnego numeru, skrótów itp.)
      - 15.3.6. identyfikacja numeru
      - 15.3.7. intercom
    - 15.4. obsługa połączeń konferencyjnych
    - 15.5. obsługa numerów grupowych (hunt groups)

15.6. obsługa Music On Hold

15.7. rejestracja połączeń (call detailed record)

15.8. obsługa bezpiecznych strumieni sRTP

15.9. obsługa kodeków audio G.711, G.729

15.10. polska wersja lokalizacyjna

16. funkcjonalność oprogramowania

16.1. routing pakietów zgodnie z protokołami RIP v1 i v2, OSPF, BGPv4, PIM

16.2. wsparcie Policy Based Routing (PBR)

16.3. funkcje bezpieczeństwa:

16.3.1. szyfrowania połączeń IPSec 3DES oraz AES

16.3.2. firewall z kontrolą stanu sesji (w trybie routed oraz transparent)

16.3.3. Intrusion Prevention System (IPS) – obsługa min. 1000 sygnatur

16.3.4. ochrona samego urządzenia (Control-Plane) przed atakami DDoS i nadużyciami.

16.3.5. możliwość współpracy z dostępnymi systemami kontroli kondycji bezpieczeństwa hostów. Np. Network Access Protection, Network Admission Control etc.

16.3.6. funkcje opisane w tym punkcie muszą działać jednocześnie

16.4. wsparcie dla protokołu IGMPv3

16.5. funkcjonalność Network Address Translation (NAT)

16.6. obsługa tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q

16.7. wydajność routingu proponowanego urządzenia nie może być mniejsza niż 350 kpps,

17. zarządzanie i konfiguracja

17.1. zarządzalne przez SNMPv3, SSHv2

17.2. możliwość eksportu informacji przez NetFlow lub odpowiednik

17.3. konfigurowalne przez CLI oraz interfejs graficzny (oczekiwane są narzędzia dodatkowe w postaci kreatorów połączeń, etc.)

17.4. możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS lub TACACS+

17.5. plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją. Musi istnieć możliwość przechowywania dowolnej ilości plików konfiguracyjnych w pamięci nieulotnej. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

18. obudowa

    18.1. wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej (dopuszczalne są wierzchnie elementy dekoracyjne wykonane z tworzyw sztucznych)

    18.2. możliwość montażu w szafie 19”

2.3 Przełącznik agregujący – 1 kpl.

Minimalne wymagania dla przełącznika agregującego:

1. przełączanie o wydajności co najmniej 6.5 Mpps oraz matrycę przełączającą min. 32Gbps
2. co najmniej 24 porty GE 10/100/1000 BaseT z Auto-MDIX
3. możliwość tworzenia stosu (min. 9 urządzeń) o przepustowości co najmniej 32Gbps w stosie – stos musi być widziany jako jedno urządzenie z poziomu konsoli systemowej; wymagana możliwość utworzenia stosu z przełącznikiem agregującym
4. możliwość zdefiniowania co najmniej 1000 sieci VLAN oraz co najmniej 128 instancji STP
5. możliwość dystrybucji informacji o skonfigurowanych VLANach do przełączników dostępowych z blokowaniem możliwości ich konfiguracji na przełącznikach dostępowych; wymagane uwierzytelnienie przesyłanych informacji (min. hasło)
6. przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv2, OSPF, BGPv4 oraz routing statyczny
7. obsługa tzw. Policy Based Routing
8. obsługa routingu multicast’ów w oparciu o protokoły PIM i DVMRP
9. obsługa IGMP v1 i v2
10. obsługa IPv6 (wymagana obsługa sprzętowa)
11. mechanizmy związane z zapewnieniem ciągłości pracy sieci:

    11.1. 802.1w

    11.2. 802.1s (co najmniej 60 instancji)

    11.3. możliwość grupowania portów (channel, trunk, hunt group) zgodnie z 802.3ad (LACP)

    11.4. protokół HSRP, VRRP lub równoważny

12. mechanizmy związane z zapewnieniem jakości usług w sieci:

    12.1. definiowanie QoS globalnie dla stosu.

    12.2. obsługa co najmniej czterech kolejek sprzętowych dla różnego rodzaju ruchu

    12.3. obsługa mechanizmów Shaped Round Robin (nie jest akceptowalne wsparcie tylko mechanizmów WRR)

    12.4. obsługa co najmniej jednej kolejki ze statusem strict priority

    12.5. możliwość “re-kolorowania” pakietów przez urządzenie – pakiet przychodzący do urządzenia przez przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS.

    12.6. pełne wsparcie dla 64 wartości pola DSCP

    12.7. możliwość ograniczania pasma dostępnego na port (rate limiting) z granulacją do kwantu 8 Kbps lub mniejszego

13. mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    13.1. autoryzacja użytkowników/portów przez 802.1x z możliwością przypisania następujących atrybutów
        13.1.1. podsieć VLAN
        13.1.2. listy dostępowe określające dostępne zasoby
    13.2. dostęp do urządzenia przez SNMPv3 i SSH
    13.3. możliwość definiowania list dostępowych dla portów urządzenia, dla sieci VLAN – wewnętrznych i zewnętrznych (przy routingu pomiędzy sieciami VLAN)
    13.4. możliwość hierarchizacji uprawnień administracyjnych (min. 10 poziomów uprawnień z możliwością definicji zakresu uprawnień z granulacją do poszczególnych komend)
    13.5. możliwość autoryzacji logowania do urządzenia (dostęp administracyjny oraz 802.1x) do serwerów RADIUS lub TACACS+
    13.6. możliwość rejestracji wszystkich poleceń wydawanych przez użytkownika na centralnym serwerze autoryzacyjnym (RADIUS accounting)
    13.7. możliwość ograniczania ruchu broadcast i multicast per port
    13.8. możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu z pozostawieniem możliwości komunikacji z portem nadrzędnym lub funkcjonalność „private VLAN"
    13.9. funkcjonalność DHCP snooping z możliwością korelacji z tablicą ARP (ochrona przed podszywaniem się adresów IP)
    13.10. ochrona przed atakami na ARP (np. poisoning)
    13.11. możliwość ograniczenia ilości stacji dołączanych do pojedynczego portu (z możliwością dynamicznej lub statycznej budowy ich listy)
    13.12. funkcjonalność umożliwiająca kopiowanie ruch z określonych portów lub VLANów na określony port monitorujący; porty źródłowe (monitorowane) mogą znajdować się w obrębie przełącznika lub stosu, jak też poza nim (przenoszenie ruchu monitorowanego przez dedykowany VLAN)
14. plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nie ulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian
15. możliwość tworzenia makr konfiguracyjnych dla portów (lista komend aplikowana pojedynczym poleceniem)
16. możliwość montażu w szafie 19"
17. możliwość zastosowania redundantnego zasilacza (dopuszczalne urządzenia zewnętrzne).

2.4 Przełącznik dostępowy – 4 kpl.

Minimalne wymagania dla przełącznika dostępowego:

1. przełączanie o wydajności co najmniej 38 Mpps oraz matrycę przełączającą min. 32Gbps

2. co najmniej 48 portów GE 10/100/1000 BaseT z Auto-MDIX oraz 4 porty GE definiowanych przez moduły SFP, GBIC lub równoważne (dostępne interfejsy 1000BaseT, 1000BaseSX, 1000BaseLX, 1000BaseZX, CWDM, 100FX); w oferowanej wersji 2 porty obsadzone konwerterami 1000BaseT
3. zasilanie zgodne z 802.3af (PoE) na każdym z portów 10/100/1000; wymagana możliwość jednoczesnego zasilania do 24 urządzeń klasy 0 (15.4W) lub dowolnego rozłożenia takiej mocy pomiędzy większą ilość portów (automatycznie)
4. możliwość zdefiniowania co najmniej 1000 sieci VLAN oraz co najmniej 128 instancji STP
5. możliwość dystrybucji informacji o skonfigurowanych VLANach z przełączników agregujących z blokowaniem możliwości ich konfiguracji na przełącznikach dostępowych; wymagane uwierzytelnienie przesyłanych informacji (min. hasło)
6. przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIP oraz routing statyczny
7. mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   7.1. 802.1w
   7.2. 802.1s (co najmniej 60 instancji)
   7.3. możliwość grupowania portów (channel, trunk, hunt group) zgodnie z 802.3ad (LACP)
   7.4. protokół HSRP, VRRP lub równoważny
8. mechanizmy związane z zapewnieniem jakości usług w sieci:
   8.1. obsługa co najmniej czterech kolejek sprzętowych dla różnego rodzaju ruchu
   8.2. obsługa mechanizmów Shaped Round Robin (nie jest akceptowalne wsparcie tylko mechanizmów WRR)
   8.3. obsługa co najmniej jednej kolejki ze statusem strict priority
   8.4. możliwość "re-kolorowania" pakietów przez urządzenie – pakiet przychodzący do urządzenia przez przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS.
   8.5. pełne wsparcie dla 64 wartości pola DSCP
   8.6. możliwość ograniczania pasma dostępnego na port (rate limiting) z granulacją do kwantu 8 Kbps lub mniejszego
   8.7. możliwość automatycznego wykrycia przez przełącznik podłączenia oferowanego telefonu IP i konfiguracji mechanizmów QoS
9. mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
   9.1. autoryzacja użytkowników/portów przez 802.1x z możliwością przypisania następujących atrybutów
      9.1.1. podsieć VLAN
      9.1.2. listy dostępowe określające dostępne zasoby
   9.2. dostęp do urządzenia przez SNMPv3 i SSHv2
   9.3. możliwość definiowania list dostępowych dla portów urządzenia, dla sieci VLAN – wewnętrznych i zewnętrznych (przy routingu pomiędzy sieciami VLAN)

9.4. możliwość hierarchizacji uprawnień administracyjnych (min. 10 poziomów uprawnień z możliwością definicji zakresu uprawnień z granulacją do poszczególnych komend)

9.5. możliwość autoryzacji logowania do urządzenia (dostęp administracyjny oraz 802.1x) do serwerów RADIUS lub TACACS+

9.6. możliwość rejestracji wszystkich poleceń wydawanych przez użytkownika na centralnym serwerze autoryzacyjnym (RADIUS accounting)

9.7. możliwość ograniczania ruchu broadcast i multicast per port

9.8. możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu z pozostawieniem możliwości komunikacji z portem nadrzędnym lub funkcjonalność „private VLAN"

9.9. funkcjonalność DHCP snooping z możliwością korelacji z tablicą ARP (ochrona przed podszywaniem się adresów IP)

9.10. ochrona przed atakami na ARP (np. poisoning)

9.11. możliwość ograniczenia ilości stacji dołączanych do pojedynczego portu (z możliwością dynamicznej lub statycznej budowy ich listy)

9.12. funkcjonalność umożliwiająca kopiowanie ruch z określonych portów lub VLANów na określony port monitorujący; porty źródłowe (monitorowane) mogą znajdować się w obrębie przełącznika lub stosu, jak też poza nim (przenoszenie ruchu monitorowanego przez dedykowany VLAN)

10. plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nie ulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian

11. możliwość tworzenia makr konfiguracyjnych dla portów (lista komend aplikowana pojedynczym poleceniem)

12. możliwość montażu w szafie 19"

13. możliwość zastosowania redundantnego zasilacza (dopuszczalne urządzenia zewnętrzne)

14. możliwość rozbudowy funkcjonalności o:

14.1. konfigurację tzw. Policy Based Routing

14.2. obsługę routingu multicast'ów w oparciu o protokoły PIM i DVMRP

14.3. obsługę IGMP v1 i v2

14.4. routing OSPF, BGPv4

14.5. obsługę IPv6 (wymagana obsługa sprzętowa)

2.5 System dostępu bezprzewodowego

Minimalne wymagania dla przełącznika dostępowego:

Wymagane jest dostarczenie skalowalnego, inteligentnego systemu dostępu bezprzewodowego, zgodnego ze standardami WiFi Alliance. System musi pracować

w architekturze, gwarantującej centralne zarządzanie i kontrolowanie punktów dostępowych, możliwość rozbudowy i rozszerzenia funkcjonalności systemu.

System musi składać się z urządzenia kontrolującego oraz punktów dostępowych. Całość konfiguracji odbywać się ma na urządzeniu centralnym (kontroler) i następnie ma być automatycznie propagowana na punkty dostępowe. Komunikacja pomiędzy urządzeniami musi odbywać się zgodnie z założeniami określanymi w draftach IETF dotyczącymi opracowywanego standardu CAPWAP (draft-ietf-capwap).

2.5.1. Kontroler sieci bezprzewodowej

Minimalne wymagania dla kontrolera sieci bezprzewodowej

1. urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
   1.1. zarządzanie politykami bezpieczeństwa
   1.2. wykrywanie intruzji
   1.3. zarządzanie pasmem radiowym
   1.4. zarządzanie mobilnością
   1.5. zarządzanie jakością transmisji
2. zarządzanie za pomocą protokołu zgodnego z wytycznymi CAPWAP min. 12-ma punktami dostępowymi (kratowymi lub klasycznymi)
3. min. 2 interfejsy GE (uplink) z możliwością agregacji pasma – styki definiowane przez moduły konwerterów GBIC, SFP lub równoważne
4. zarządzanie pasmem radiowym punktów dostępowych
   4.1. automatyczna adaptacja do zmian w czasie rzeczywistym
   4.2. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
   4.3. dynamiczne przydzielanie kanałów radiowych
   4.4. wykrywanie, eliminacja i unikanie interferencji
   4.5. równoważenie obciążenia punktów dostępowych
5. obsługa mechanizmów bezpieczeństwa
   5.1. 802.11i, WPA2, WPA, WEP
   5.2. 802.1x z EAP (PEAP, EAP-TLS, EAP-FAST, EAP-TTLS)
   5.3. możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID
   5.4. współpraca z mechanizmami zaawansowanej kontroli dostępu do sieci (typu NAC, NAP lub równoważne) – wymuszanie polityki dostępu na poziomie kontrolera
   5.5. możliwość profilowania użytkowników
      5.5.1. przydział sieci VLAN
      5.5.2. przydział list kontroli dostępu (ACL)
   5.6. uwierzytelnianie ramek zarządzania 802.11 (wykrywanie podszywania się punktów dostępowych użytkowników pod adresy infrastruktury)
   5.7. walidacja FIPS 140-2 L2
   5.8. wykrywanie „obcych” punktów dostępowych (współpraca z mechanizmami lokalizacyjnymi oprogramowania do zarządzania)

5.9. obsługa serwerów autoryzacyjnych (RADIUS lub TACACS+),

5.10. współpraca z systemami IDS/IPS

6. obsługa mechanizmów QoS (802.1p, WMM TSpec, kontrola pasma per użytkownik) i VoWLAN (Voice over WLAN)
7. obsługa mobilności (roaming-u) użytkowników
8. współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne
9. obsługa dostępu gościnnego

   9.1. przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony)

   9.2. możliwość kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta

   9.3. możliwość konfiguracji dedykowanego kontrolera do obsługi ruchu gości – całość ruchu z SSID dostępu gościnnego zebranego na pozostałych kontrolerach musi być przesyłana do tego kontrolera (umieszczonego w publicznej części sieci) w sposób zapewniający logiczną separację od ruchu wewnętrznego

10. możliwość redundancji rozwiązania (N+1)
11. zarządzanie przez HTTPS, SNMPv3, SSH, port konsoli szeregowej
12. zgodność ze standardami:

    12.1. SNMP v1, v2c, v3

    12.2. RFC 854 Telnet

    12.3. RFC 1155 Management Information for TCP/IP-Based Internets

    12.4. RFC 1156 MIB

    12.5. RFC 1157 SNMP

    12.6. RFC 1213 SNMP MIB II

    12.7. RFC 1350 TFTP

    12.8. RFC 1643 Ethernet MIB

    12.9. RFC 2030 SNTP

    12.10. RFC 2616 HTTP

    12.11. RFC 2665 Ethernet-Like Interface types MIB

    12.12. RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions

    12.13. RFC 2819 RMON MIB

    12.14. RFC 2863 Interfaces Group MIB

    12.15. RFC 3164 Syslog

    12.16. RFC 3414 User-Based Security Model (USM) for SNMPv3

    12.17. RFC 3418 MIB for SNMP

    12.18. RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs

    12.19. RFC 768 UDP

    12.20. RFC 791 IP

12.21. RFC 792 ICMP
12.22. RFC 793 TCP
12.23. RFC 826 ARP
12.24. RFC 1122 Requirements for Internet Hosts
12.25. RFC 1519 CIDR
12.26. RFC 1542 BOOTP
12.27. RFC 2131 DHCP
12.28. WPA
12.29. IEEE 802.11i (WPA2, RSN)
12.30. RFC 1321 MD5 Message-Digest Algorithm
12.31. RFC 1851 The ESP Triple DES Transform
12.32. RFC 2104 HMAC: Keyed Hashing for Message Authentication
12.33. RFC 2246 TLS Protocol Version 1.0
12.34. RFC 2401 Security Architecture for the Internet Protocol
12.35. RFC 2403 HMAC-MD5-96 within ESP and AH
12.36. RFC 2404 HMAC-SHA-1-96 within ESP and AH
12.37. RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV
12.38. RFC 2406 IPSec
12.39. RFC 2407 Interpretation for ISAKMP
12.40. RFC 2408 ISAKMP
12.41. RFC 2409 IKE
12.42. RFC 2451 ESP CBC-Mode Cipher Algorithms
12.43. RFC 3280 Internet X.509 PKI Certificate and CRL Profile
12.44. RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec
12.45. RFC 3686 Using AES Counter Mode with IPSec ESP
12.46. IEEE 802.1X
12.47. RFC 2716 PPP EAP-TLS
12.48. RFC 2865 RADIUS Authentication
12.49. RFC 2866 RADIUS Accounting
12.50. RFC 2867 RADIUS Tunnel Accounting
12.51. RFC 2869 RADIUS Extensions
12.52. RFC 3576 Dynamic Authorization Extensions to RADIUS
12.53. RFC 3579 RADIUS Support for EAP
12.54. RFC 3580 IEEE 802.1X RADIUS Guidelines
12.55. RFC 3748 Extensible Authentication Protocol

13. możliwość zastosowania redundantnego zasilacza AC
14. możliwość instalacji w szafie rack 19”

15. zgodność z Common Criteria EAL 2 (dopuszczalne rozwiązania będące w trakcie certyfikacji)
16. oznaczenie CE

2.5.2. Punkty dostępowe – 5 kpl.

Minimalne wymagania dla punktu dostępowego:

1. punkty dostępowe umożliwiające utworzenie sieci kratowej (komunikacja między punktami dostępowymi bez medium kablowego, autoryzacja punktów dostępowych w oparciu o certyfikaty X.509, adresy MAC)
2. obsługa 802.11a i 802.11b/g (dual-radio)
   2.1. separacja trybu pracy poszczególnych technologii i/lub kanałów radiowych (np. jedna dedykowana do obsługi klientów, druga do komunikacji między punktami dostępowymi)
   2.2. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo radiowe)
3. interfejs 10/100/1000 zgodny z 802.3u z możliwością zasilania urządzeń zewnętrznych (zgodnie z 802.3af)
4. obsługa 11 kanałów radiowych dla 802.11a i 13 dla 802.11b/g
5. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
6. możliwość programowego ustawiania mocy wyjściowej
7. modularny system antenowy (dołączane anteny zewnętrzne) - w oferowanej wersji anteny zapewniające pokrycie dookólne (min. 5 dBi dla 802.11g, min. 8 dBi dla 802.11a) – obsługa korelacji sygnału anten dla 802.11g (możliwość zastosowania min. 3 równocześnie pracujących anten); w oferowanej wersji wymagana jedna antena 802.11a i 3 anteny 802.11g
8. sprzętowe wsparcie szyfrowania AES
9. filtracja i autoryzacja klientów w oparciu o MAC
10. obsługa połączeń mostowych (bridging)
11. zgodność z 802.11i, WPA i WPA-2, WEP
12. obsługa 802.1x
13. obsługa 802.11e (WiFi Multimedia)
14. obsługa min. 16 rozgłaszanych SSID
15. certyfikat WiFi
16. zróżnicowane możliwości zasilania
    16.1. zasilacz sieciowy 230V AC
    16.2. możliwość zasilania z latarni ulicznej (przejściówka dostarczana przez producenta urządzenia)
    16.3. PoE (zasilanie przez kabel Ethernet)
    16.4. możliwość instalacji wewnętrznej baterii zapewniającej zasilanie awaryjne
    16.5. w oferowanej wersji wymagane dołączenie zasilaczy PoE

17. praca zarządzana przez kontroler WLAN (tzw. „cienki” punkt dostępowy zarządzany przez protokół zgodny z założeniami CAPWAP)
18. obudowa odporna na warunki atmosferyczne, przystosowana do pracy zewnętrznej
    18.1. przystosowany do montażu na ścianach, możliwość instalacji na latarniach/słupach ulicznych (wymagane odpowiednie uchwyty w zestawie)
    18.2. waga nie przekraczająca 7 kg
    18.3. praca przy temperaturach między -40^{o}C a 55^{o}C
    18.4. odporność na wiatr o prędkości min:
        18.4.1. stała prędkość 150 km/h
        18.4.2. porywy 225 km/h
    18.5. zgodność z IP67 i NEMA4X
19. sygnalizacja wizyjna stanu urządzenia (np. diody LED) – z możliwością deaktywacji
20. możliwość przywrócenia ustawień fabrycznych (reset) urządzenia za pomocą wbudowanego przełącznika
21. zgodność z polskimi regulacjami
22. zgodność z dyrektywą UE 1999/5/EC

2.5.3. System zarządzania siecią bezprzewodową

Minimalne wymagania dla systemu zarządzania siecią bezprzewodowej:

1. zarządzanie kontrolerami sieci Wireless LAN oraz punktami dostępu radiowego 802.11a/b/g (wykorzystany protokół Lightweight Access Point Protocol, LWAPP lub równoważny) - minimalna liczba zarządzanych urządzeń: 50 z możliwością rozszerzenia do min. 2500
2. graficzne planowanie i zarządzenie siecią Wireless LAN (hierarchiczne mapy lokalizacji, mapy zasięgu) z wykorzystaniem własnych planów budynków
3. monitorowanie informacji takich jak: poziom szumu, poziom sygnału, interferencje sygnału pochodzących z punktów dostępowych
4. raportowanie i statystyka min: wydajności urządzeń, obciążenia sieci, alarmy pochodzące z urządzeń
5. system musi zawierać gotowe, przykładowe formularze wdrożenia dla polityki bezpieczeństwa, polityki QoS dla wielu punktów dostępu radiowego, a także udostępniać możliwość tworzenia własnych
6. automatyczne wykrywanie nowych punktów dostępowych w sieci radiowej
7. możliwość rozbudowy funkcjonalności o wsparcie usługi lokalizacji urządzeń radiowych (programowe z możliwością rozszerzenia o wsparcie sprzętowe)
8. wykrywanie typowych ataków (typu netstumber, void11, fakeap, spoofing itp.)
9. współpraca z systemami IDS/IPS
10. obsługa sieci kratowych
11. wykrywanie nie autoryzowanych punktów dostępowych i klientów sieci z możliwością ich eliminacji
12. zarządzanie wersjami oprogramowania urządzeń
13. obsługa dostępu bezprzewodowego dla gości

14. zarządzanie urządzeniem przez protokół HTTP oraz HTTPS
15. współpraca z serwerami czasu (NTP), serwerami autoryzacyjnymi
16. praca pod kontrolą systemu operacyjnego Microsoft Windows 2003 lub Linux
17. zgodność z Common Criteria EAL 2 (dopuszczalne rozwiązania będące w trakcie certyfikacji)

2.6 *Warunki gwarancji i serwisu dla urządzeń i oprogramowania sieci teleinformatycznej*

2.6.1 Sprzęt

1. Na dostarczany sprzęt musi być udzielona min. 36-miesięczna gwarancja oparta na gwarancji producenta rozwiązania; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego; usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu następnego dnia roboczego od momentu zdiagnozowania usterki; Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail, WWW (przez 24/dobę).
2. W przypadku Sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki
3. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego
4. Zamawiający uzyska dostęp do części chronionych stron internetowych producentów rozwiązań, umożliwiający:
   4.1. pobieranie nowych wersji oprogramowania
   4.2. dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej
   4.3. dostęp do pomocy technicznej producentów

2.6.2 Oprogramowanie

1. Oprogramowanie powinno być dostarczone z min. rocznym wsparciem producenta – dostarczanie aktualizacji, zdalne (telefon lub e-mail, www) wsparcie techniczne w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem oprogramowania
2. Zamawiający uzyska dostęp do części chronionych stron internetowych producentów rozwiązań, umożliwiający:
   2.1. pobieranie nowych wersji oprogramowania
   2.2. dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej
   2.3. dostęp do pomocy technicznej producentów

3. Wymagania w zakresie funkcjonalności centrum zarządzania siecią

3.1 Oprogramowanie zarządzające urządzeniami sieciowymi

Zaproponowane oprogramowanie powinno:

1. umożliwić zarządzanie min. 300 urządzeniami w sieci lokalnej oraz sieci WAN

2. pracować w trybie dostępu za pośrednictwem przeglądarki pozwalając administratorowi na dostęp z dowolnego miejsca w sieci (po uzyskaniu odpowiednich uprawnień).
3. umożliwiać zbieranie statystyk co najmniej z wykorzystaniem SNMP, RMON
4. posiadać narzędzia automatycznej identyfikacji urządzeń instalowanych w sieci
5. mieć możliwość integracji z oprogramowaniem NMS – HP OV
6. posiadać narzędzia graficznej prezentacji urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu urządzenia (stan portu, etc.)
7. posiadać narzędzia umożliwiające tworzenie list dostępowych poprzez tzw. kreatory
8. posiadać narzędzia pozwalające na identyfikację "wąskich gardeł" sieci, określanie czasów odpowiedzi urządzeń oraz czasu opóźnienia (latency)
9. posiadać narzędzia pozwalające na dokonywanie inwentaryzacji sprzętu i oprogramowania wykorzystywanego w sieci oraz kontrolę zmian dokonywanych w konfiguracji urządzeń
10. posiadać narzędzie umożliwiające zbieranie informacji o nieprawidłowych parametrach pracy zainstalowanego sprzętu:
    - 10.1. Chassis - wykorzystanie matrycy (backplane)
    - 10.2. Wentylatory - nieprawidłowa praca
    - 10.3. Pamięć - wykorzystanie buforów, ilość wolnej pamięci
    - 10.4. Moduły sieciowe:
        - 10.4.1. Aktywacja do matrycy
        - 10.4.2. Wolumen broadcastów
        - 10.4.3. Obciążenie/wykorzystanie modułów
        - 10.4.4. Ilość pakietów usuwanych z kolejek
    - 10.5. Zasilacze – odstępstwa napięcia poza dopuszczalną tolerancję
    - 10.6. Procesory – obciążenie
    - 10.7. Temperatura – odstępstwa poza dopuszczalną tolerancję
11. posiadać narzędzie monitoringu RMON pozwalające na analizę parametrów urządzenia, łącza, portu urządzenia.

3.2. Komputery przenośne – 2 szt.

Minimalne wymagania dla komputerów przenośnych:

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Ekran	13,3" WXGA (1280x800), True Life
2.	Chipset	Min. Intel 965 lub równoważny
3.	Procesor	procesor klasy x86 dedykowany do pracy w komputerach przenośnych zaprojektowany do pracy w układach jednoprocesorowych, taktowany zegarem co najmniej 2,2 GHz, częstotliwość szyny systemowej 800MHz, pamięć L2 4 MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku użycia przez oferenta testów wydajności Zamawiający

		zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
4.	Pamięć RAM	2 GB 667 MHz z możliwością rozbudowy do 4GB
5.	Dysk twardy	Min. 160 GB Serial ATA, 5400 obr/min.
6.	Karta graficzna	Zintegrowana Intel GMA X3100 lub równoważna
7.	Audio	Karta dźwiękowa 5.1, zgodna z HD Audio, wbudowane głośniki stereo.
8.	Karta sieciowa	10/100 LOM – RJ 45
9.	Łączność bezprzewodowa	Wireless LAN 802.11 a/g (dedykowany przełącznik do włączania/wyłączania karty Wi-Fi)
10.	Porty/złącza	2x USB 2.0, złącze słuchawek, złącze mikrofonu, FireWire, RJ-45, HDMI, VGA, czytnik kart 8 w 1 (obsługiwane karty: SD, SDIO, MMC, Memory Stick, Memory Stick PRO, xD, Hi Speed SD, Hi Capacity SD), ExpressCard, Kensington Slot
11.	Klawiatura	Klawiatura (układ US -QWERTY) Touchpad z wydzielonymi strefami przewijania obrazu w pionie i poziomie.
12.	Napęd optyczny	8x DVD+/-RW, wyklucza się obsługę napędu optycznego przy wykorzystaniu elementów wychodzących poza obrys notebooka.
13.	Bateria	Li-Ion, czas pracy na bateriach min. 4 godziny
14.	Zasilacz	Zasilacz min. 65W, waga maksymalna (zasilacz z kablami) 0,26 kg
15.	Kamera	Wbudowana kamera, 2 mega pixele
16.	Bezpieczeństwo	Wbudowany czytnik linii papilarnych
17.	System operacyjny	Microsoft Windows Vista Business PL lub inny równoważny, zainstalowany system operacyjny nie wymagający aktywacji za pomocą telefonu lub Internetu
18.	Certyfikaty i standardy	– Certyfikat ISO9001:2000 dla producenta (należy załączyć do oferty) – Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty)
19.	Waga	Waga max 1.9 kg
20.	Gwarancja	3 lata Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.

3.3 Warunki gwarancyjne dla oprogramowania centrum zarządzania siecią

1. Oprogramowanie powinno być dostarczone z min. rocznym wsparciem producenta – dostarczanie aktualizacji, zdalne (telefon lub e-mail, www) wsparcie techniczne w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem oprogramowania
2. Zamawiający uzyska dostęp do części chronionych stron internetowych producentów rozwiązań, umożliwiający:
   2.1. pobieranie nowych wersji oprogramowania
   2.2. dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej
   2.3. dostęp do pomocy technicznej producentów

4. Projekt sieci światłowodowej

Zakres prac w fazie projektowej obejmuje wszystkie czynności konieczne do opracowania projektów budowlanych oraz wykonawczych na podstawie, których Wykonawca będzie mógł przystąpić do realizacji sieci światłowodowej pomiędzy wskazanymi lokalizacjami Zamawiającego, w tym w szczególności:

- Projektu budowy linii światłowodowej pomiędzy budynkami Zamawiającego,
- Projektu węzła centralnego,
- Projektu wykonawczego sieci optotelekomunikacyjnej na terenie Zgierza
- Projektu elektrycznego - zasilania punktów dostępowych i węzła centralnego sieci

Lista lokalizacji stanowi załącznik nr 1.

Na etapie prac projektowych do obowiązków Wykonawcy należy:

1. pozyskanie map do celów projektowych - obejmuje zakup map jak również założenie i aktualizację map do celów projektowych oraz uzgodnienie przebiegu trasowego w świetle ustawy z dnia 28 lipca 2005 r. o zmianie ustawy - Prawo budowlane oraz o zmianie niektórych innych ustaw (Dz. U. Nr 163 poz. 1369).
2. pozyskanie map do celów opiniodawczych,
3. opracowanie projektów wykonawczych (technicznych),
4. opracowanie projektów budowlanych,
5. pozyskanie zgód właścicieli terenu na dysponowanie nieruchomością na cele budowlane tzw. „prawo drogi”,
6. wykonanie projektów budowlanych i wykonawczych dla lokalizacji węzłów sieci:
7. wykonanie projektów zagospodarowania pomieszczeń, w których zostaną zlokalizowane węzły. Projekty pomieszczeń muszą uwzględniać:
   a. zasilanie energetyczne na odpowiednim do potrzeb poziomie,
   b. odpowiednią do potrzeb powierzchnię użytkową,
   c. odpowiednią liczbę szafy typu rack 19”,
8. opracowanie projektów adaptacji budowlanych,(jeżeli będą wymagane),
9. dla lokalizacji tego wymagających uzyskanie prawomocnej decyzji o pozwoleniu na budowę,
10. każdorazowo uzyskanie u właściciela infrastruktury oświetleniowej pisemnej akceptacji dokumentacji projektowej, poprzez:

a. Uzyskanie opinii w zakresie możliwości umieszczenia instalacji teleinformatycznej na infrastrukturze oświetleniowej z uwagi na jej stan techniczny (ocena w oparciu o przegląd techniczny).

b. Uzyskanie uzgodnienia dokumentacji technicznej sieci teleinformatycznej w zakresie technologii zamocowania

c. Uzgodnienie harmonogramu realizacji robót związanych z montażem sieci teleinformatycznej,

11. przygotowanie wniosku o decyzję środowiskową i wykonanie raportu oddziaływania na środowisko (jeśli będą konieczne)
12. opracowanie projektów specjalistycznych w zakresie skrzyżowań z rzekami, drogami, ciekami wodnymi, torami PKP, gazociągami, kablami energetycznymi itp., wymaganych dla realizacji prac budowlanych w oparciu o projekt.
13. prowadzenia działań formalnych związanych z wykonywanym Projektem, w tym uzyskania, działając w oparciu o otrzymane od Zamawiającego upoważnienie oraz przekazania Zamawiającemu decyzji o ustaleniu lokalizacji inwestycji celu publicznego,
14. opłaty za uzgodnienia branżowe, opinie, ekspertyzy itp.,
15. opłaty za decyzje i pozwolenia administracyjne,
16. dostarczenie dokumentacji (technicznej i formalno – prawnej) w 5 egz. w postaci papierowej oraz w 2 egz. na nośniku optycznym. .
17. wykonanie kosztorysu inwestorskiego w oparciu o program komputerowego wspomagania kosztorysowania ZUZIA lub NORMA.
18. Odczyt i wydruk dostarczonej dokumentacji winien być możliwy z wykorzystaniem oprogramowania: MS-Office, Visio, Auto-CAD, Acrobat Reader, Corel, Zuzia, Norma.

Projekt sieci światłowodowej musi zostać opracowany w taki sposób, żeby umożliwić:

1. układanie kabli światłowodowych z wykorzystaniem miejskiej kanalizacji teletechnicznej, energetycznej i oświetleniowej
2. wykonanie rdzenia sieci w topologii „ringu”
3. wskazanie punktu wymiany danych z operatorami zewnętrznymi (IXP).

Całość prac projektowych należy wykonać zgodnie z zasadami wiedzy technicznej oraz z następującymi normami i instrukcjami:

1.	Instrukcja T-01	Odbiór i utrzymanie kablowych linii telekomunikacyjnych.
2.	ZN-96/TPSA-002	Linie optotelekomunikacyjne. Ogólne wymagania techniczne.
3.	ZN-96/TPSA-004	Zbliżenia i skrzyżowania z innymi urządzeniami uzbrojenia terenowego. Ogólne wymagania techniczne.
4.	ZN-96/TPSA-005	Kable optotelekomunikacyjne jednomodowe dalekosiężne. Wymagania i badania.
5.	ZN-96/TPSA-006	Linie optotelekomunikacyjne. Złącza spajane światłowodów jednomodowych. Wymagania i badania.
6.	ZN-96/TPSA-007	Linie optotelekomunikacyjne. Złączki światłowodowe i kable stacyjne. Wymagania i badania.
7.	ZN-96/TPSA-008	Linie optotelekomunikacyjne. Osłony złączowe. Wymagania i badania.

8.	ZN-96/TPSA-009	Kablowe linie optotelekomunikacyjne. Przełącznice światłowodowe. Wymagania i badania.
9.	ZN-96/TPSA-011	Telekomunikacyjna kanalizacja kablowa. Ogólne wymagania techniczne.
10.	ZN-96/TPSA-012	Kanalizacja kablowa pierwotna. Wymagania i badania.
11.	ZN-96/TPSA-013	Kanalizacja wtórna i rurociąg i kablowe. Wymagania i badania.
12.	ZN-96/TPSA-014	Rury z polichlorku winylu (RPCW). Wymagania i badania.
13.	ZN-96/TPSA-015	Rury polipropylenowe RPP i polietylenowe RPE kanalizacji pierwotnej. Wymagania i badania.
14.	ZN-96/TPSA-016	Rury polietylenowe karbowane dwuwarstwowe (RHDPEk). Wymagania i badania.
15.	ZN-96/TPSA-017	Rury kanalizacji wtórnej i rurociągu kablowego (RHDPE). Wymagania i badania.
16.	ZN-96/TPSA-018	Rury polietylenowe (RHDPEp) przepustowe. Wymagania i badania.
17.	ZN-96/TPSA-019	Rury trudnopalne (RHDPEt). Wymagania i badania.
18.	ZN-96/TPSA-020	Złączki rur kanalizacji kablowej. Wymagania i badania.
19.	ZN-96/TPSA-021	Uszczelki końców rur kanalizacji kablowej. Wymagania i badania.
20.	ZN-96/TPSA-022	Przywieszka identyfikacyjna. Wymagania i badania.
21.	ZN-96/TPSA-023	Studnie kablowe. Wymagania i badania.
22.	ZN-96/TPSA-024	Zasobnik złączowy. Wymagania i badania.

5. Budowa sieci światłowodowej

Zakres prac w fazie wykonawczej budowy sieci światłowodowej obejmuje wszystkie czynności konieczne do wykonania sieci światłowodowej na podstawie wcześniej opracowanych projektów budowlanych oraz wykonawczych pomiędzy wskazanymi lokalizacjami Zamawiającego, w tym w szczególności:

1. budowę sieci optotelekomunikacyjnej na terenie Zgierza pomiędzy budynkami Zamawiającego, wyszczególnionymi w załączniku nr 1,
2. budowę węzła centralnego,
3. wykonania adaptacji zasilania elektrycznego – w zakresie niezbędnym do uruchomienia zasilania punktów dostępowych i węzła centralnego sieci,
4. wykonanie modernizacji miejsca instalacji urządzeń sieciowych w pomieszczeniu serwerowni

5.1 Dodatkowe Informacje:

1. Wykonawca zapewni wykonanie sieci z należytą starannością, przez zespoły projektowe i wykonawcze pod kierownictwem osób dysponujących aktualnymi stosownymi uprawnieniami w dziedzinie telekomunikacji,
2. Dopuszcza się możliwość wykonania niektórych odcinków sieci w oparciu o strukturę transportu światłowodowego stworzoną na zasadzie pozyskiwania pary ciemnych włókien poprzez ich zakup lub wykorzystanie tzw. Nieodwołalnego Prawa Użytkowania (IRU -

Indefeasible Right to Use), od operatorów posiadających własną infrastrukturę kabli światłowodowych.

3. Dopuszcza się możliwość wykonania niektórych odcinków sieci w oparciu o istniejącą kanalizację teletechniczną pozyskaną od operatorów od operatorów posiadających własną infrastrukturę kanalizacji teletechnicznej.

5.2 Gwarancja

Na zaprojektowaną i wykonaną sieć światłowodową musi być udzielona minimum 3-letnia gwarancja. Serwis gwarancyjny świadczony ma być w miejscu instalacji; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego; usunięcie usterki (naprawa lub wymiana wadliwego elementu) ma zostać wykonana w przeciągu następnego dnia roboczego od momentu zdiagnozowania usterki; Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail. Wykonawca udostępni pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań

.....

Podpis

Załącznik 1

Lista lokalizacji objętych projektem

Lp.	PLACÓWKA	ADRES 95-100 Zgierz
1.	Miejski Ośrodek Kultury w Zgierzu	ul. Mielczarskiego 1
2.	Muzeum Miasta Zgierza	ul. Dąbrowskiego 21
3.	Miejsko-Powiatowa Biblioteka Publiczna im. B. Prusa w Zgierzu	ul. Łódzka 5
4.	M-PBP im. B. Prusa - Filia nr 1	ul. Lechonia 2
5.	M-PBP im. B. Prusa - Filia nr 2	ul. Długa 19
6.	M-PBP im. B. Prusa - Filia nr 3	ul. Dubois 23a
7.	M-PBP im. B. Prusa - Filia nr 4	ul. Barlickiego 2
8.	M-PBP im. B. Prusa - Filia nr 6	ul. Staffa26
9.	Miejski Ośrodek Pomocy Społecznej im. bł. o. R. Chylińskiego w Zgierzu	ul. Długa 56
10.	Miejski Ośrodek Sportu i Rekreacji w Zgierzu	ul. Wschodnia 2
11.	Straż Miejska w Zgierzu	ul. Ks. J. Popiełuszki 3a
12.	Redakcja "Ilustrowanego Tygodnika Zgierskiego" w Zgierzu	ul. Długa 18
13.	Miejskie Usługi Komunikacyjne w Zgierzu	pl. Kilińskiego 7
14.	Miejskie Przedszkole Nr 2 w Zgierzu	ul. Boya-Żeleńskiego 6
15.	Miejskie Przedszkole Nr 3 w Zgierzu	ul. Mielczarskiego 26
16.	Miejskie Przedszkole Nr 6 w Zgierzu	ul. Gałczyńskiego 38
17.	Miejskie Przedszkole Nr 7 w Zgierzu	ul. Długa 62
18.	Miejskie Przedszkole Nr 8 w Zgierzu	ul. Łódzka 86
19.	Miejskie Przedszkole Nr 9 "Słoneczny Dom" w Zgierzu	ul. Dubois 10
20.	Miejskie Przedszkole Nr 10 w Zgierzu	ul. Ossowskiego 24
21.	Miejskie Przedszkole Nr 12 w Zgierzu	ul. Gałczyńskiego 30
22.	Miejskie Przedszkole Nr 13 w Zgierzu	ul. Słowackiego 8
23.	Miejskie Przedszkole Nr 14 w Zgierzu	ul. Boya-Żeleńskiego 17
24.	Miejskie Przedszkole Nr 15 w Zgierzu	ul. Boya-Żeleńskiego 10

25.	Miejski Żłobek im. "Koziołka Matołka" w Zgierzu	ul. Tuwima 21
26.	Samorządowe Liceum Ogólnokształcące im. R. Traugutta w Zgierzu	ul. Musierowicza 2
27.	Szkoła Podstawowa Nr 1 w Zgierzu	ul. Piłsudskiego 1
28.	Szkoła Podstawowa Nr 3 im. Dąbrowszczaków w Zgierzu	ul. Szczawińska 2
29.	Szkoła Podstawowa Nr 4 w Zgierzu	ul. Łódzka 2
30.	Szkoła Podstawowa Nr 5 w Zgierzu	ul. 1 Maja 63
31.	Szkoła Podstawowa Nr 8 w Zgierzu	ul. Boya-Żeleńskiego 4
32.	Szkoła Podstawowa Nr 10 w Zgierzu	ul. Ozorkowska 68/70
33.	Szkoła Podstawowa Nr 11 w Zgierzu	ul. Dubois 26
34.	Szkoła Podstawowa Nr 12 im. Armii Krajowej w Zgierzu	ul. Staffa 26
35.	Gimnazjum Nr 1 w Zgierzu	ul. Musierowicza 2
36.	Gimnazjum Nr 2 im. J. Kochanowskiego w Zgierzu	ul. 3 Maja 46a
37.	Gimnazjum Nr 3 im. A. Mickiewicza w Zgierzu	ul. Leśmiana 1
38.	Urząd Stanu Cywilnego	ul. 1-go Maja 5
39.	Centrum Kultury Dziecka	ul. Rembowskiego 17

Publiczne Punkty Dostępu do Internetu (PIAP)

Lp.	PLACÓWKA	ADRES 95-100 Zgierz
1.	PIAP – Urząd Miasta Zgierza	Plac Jana Pawła II 16
2.	PIAP – Urząd Stanu Cywilnego	ul. 1-go Maja 5
3.	PIAP – Miejski Ośrodek Sportu i Rekreacji (MOSiR)	ul. Wschodnia 2
4.	PIAP – MOSiR (Pływalnia)	ul. Leśmiana 1
5.	PIAP – Miejski Ośrodek Kultury	ul. Mielczarskiego 1

.....

Podpis