

5.5.5.3 System zarządzania kontrolą dostępu do sieci (1 kpl.)

Element	Wymagane minimalne parametry techniczne
Funkcjonalność	Rozwiązanie musi posiadać następujące funkcjonalności: - Aktywne zapobieganie przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów, - Współpraca z rozwiązaniem Microsoft NAP, - Przypisanie na stałe adresu MAC do określonego przełącznika lub portu przełącznika. Jeżeli system końcowy będzie próbował się uwierzytelnić na innym porcie lub przełączniku, zostanie odrzucony lub przypisana mu zostanie polityka w oparciu o akcje określoną podczas przypisywania mu portu MAC, - Funkcja <i>IP-to-ID Mapping</i>, która łączy razem nazwę użytkownika, adres IP, adres MAC oraz port fizyczny każdego punktu końcowego. Ta funkcjonalność jest kluczowa dla potrzeb audytów bezpieczeństwa i analiz dochodzeniowych, - Funkcja portalu rejestracyjnego dla kontroli dostępu, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
Architektura	Rozwiązanie musi posiadać następujące funkcjonalności: - Musi zapewniać rozwiązanie NAC typu <i>inline</i> oraz <i>out-of-band</i>, które może być zarządzane przez jedną centralną aplikację, - Musi być dostarczone jako maszyna wirtualna - Musi mieć możliwość pracy jako redundantne urządzenia wirtualne w trybie wysokiej dostępności.
Raportowanie	Rozwiązanie musi posiadać następujące funkcjonalności: - Informacje o typie urządzeń działających w sieci oraz określonych potrzebach i zagrożeniach, które są z nimi związane, - Powiadamianie poprzez syslog, pocztę elektroniczną lub usługi webowe o zmianach stanu systemów końcowych, rejestracji gości oraz wynikach skanowania stanu zabezpieczeń systemów końcowych.
Narzędzia administracyjne	Rozwiązanie musi posiadać następujące funkcjonalności: - Musi zapewnić rozwiązanie oferujące jednolity, centralny obraz wszystkich niechronionych elementów związanych z użytkownikami i urządzeniami, który pozwoli później zredukować złożoność procesu zarządzania, - Musi posiadać intuicyjny panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych, - Musi posiadać funkcję portalu rejestracyjnego dla kontroli dostępu gości, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
Bezpieczeństwo	Rozwiązanie musi posiadać następujące funkcjonalności: - Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania i autoryzacji podłączanych systemów końcowych, - Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP, - Musi umożliwiać ciągłe mechanizmy analizowania zagrożeń, zapobiegania im i przechowywania ich, - Rozwiązanie musi obsługiwać lokalną autoryzację MAC.

Kontrola	Rozwiązanie musi posiadać następujące funkcjonalności: • Zdolność ciągłego przypisywania polityk określonemu użytkownikowi, adresowi MAC lub OUI (<i>Organizationally Unique Identifier</i>) adresu MAC, tak aby użytkownik, urządzenie lub grupa urządzeń miały przydzielony ten sam zestaw zasobów sieci, niezależnie od swojej lokalizacji lub konfiguracji serwera RADIUS, • Musi obsługiwać mechanizmy w oparciu o role umożliwiające przepuszczanie lub odrzucanie ruchu sieciowego, nadawanie mu priorytetów, ograniczanie jego szybkości, tagowanie, przekierowywanie i kontrolowanie go w oparciu o tożsamość użytkownika, czas i położenie, typ urządzenia i inne zmienne środowiskowe.
Wsparcie dla środowiska wirtualnego	• Możliwość objęcia mechanizmem NAC maszyn wirtualnych oraz VDI.
Automatyzacja	• Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych.
Skalowalność	Rozwiązanie musi posiadać następujące funkcjonalności: • Elastyczna obsługa wielu metod uwierzytelniania wielu użytkowników i urządzeń różnych dostawców, • Kontrola dla minimum 500 sesji autentykacyjnych, • System musi umożliwiać przyszłą rozbudowę dla minimum 1 500 sesji autentykacyjnych.
Gwarancja	• 3 letni bezpłatny dostęp do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.

5.6 Wdrożenie telefonii VoIP

5.6.1 Centrala VoIP

5.6.1.1 Jednostka główna

Wymagania techniczne:

- Obsługa łącz zewnętrznych:
 - sieciowanie IP
 - linie operatorów SIP
 - ISDN BRI
 - ISDN PRI
 - standardowe linie analogowe
- Wewnętrzne porty typu: analogowe, cyfrowe, IP oraz ISDN
- Obsługa do minimum 128 wewnętrznych aparatów
- Wbudowana obsługa Call Center
- Wbudowana uproszczona poczta głosowa
- Wbudowana karta DISA z możliwością importu plików .wav
- Funkcja odtwarzania przygotowanych plików jako źródła muzyki
- Wbudowany klient SNTP, SNMP,
- Dwa porty LAN RJ45
- Wbudowana funkcja automatycznego trasowania najtańszych połączeń
- Wbudowana funkcja równomiernej dystrybucji połączeń
- Wbudowany system łączności bezprzewodowej DECT:
 - Obsługa do minimum 64 słuchawek
- System obsługi połączeń przychodzących wspomagany funkcją CLIP
- Funkcja automatycznej konfiguracji łącza ISDN
- Wbudowana funkcja CLIP dla wszystkich zewnętrznych i wewnętrznych linii analogowych
- Komunikaty w języku polskim na wyświetlaczach aparatów systemowych
- Systemowa książka telefoniczna na 1000 wpisów
- Optyczna sygnalizacja pozostawionej wiadomości
- Możliwość powiadomienia zajętego abonenta o połączeniu
- Blokowanie połączeń wychodzących
- Możliwość pozostawienia wiadomości
- Obsługa konferencji
- Raporty taryfikacji - z połączeń wychodzących, przychodzących
- Obudowa Rack 19"

Należy dostarczyć licencje umożliwiające korzystanie z Centrali VoIP przez wszystkie urządzenia do niej podłączone

5.6.1.2 Karta analogowa portów wewnętrznych

- Umożliwiająca podłączenie 16 wewnętrznych urządzeń analogowych (telefonów, faksów, modemów)
- Funkcja identyfikacji abonenta dzwoniącego w standardzie FSK na wszystkich portach
- Dioda statusu karty
- 16 gniazd RJ45

5.6.1.3 Karta portów miejskich

- Pozwalająca na podłączenie 8 analogowych linii zewnętrznych
- Wbudowana identyfikacja abonenta dzwoniącego na wszystkich portach w standardzie FSK i DTMF
- Dioda statusu karty

5.6.1.4 Karta VOIP

- Obsługująca minimum 8 kanałów VoIP
- Obsługiwane kodeki: G.711 i G.729A
- Pozwalająca na uruchomienie w systemie:
 - linii zewnętrznych IP (H.323 lub SIP)
 - linii wewnętrznych IP (aparaty SIP i systemowe)
 - anten DECT IP
- Możliwość transmisji faksów T.38

5.6.2 Telefon systemowy IP typ1

Wymagania techniczne:

- Współpracujący z zaoferowaną centralą VOIP
- 3-liniowy, 24-znakowy, podświetlany wyświetlacz alfanumeryczny
- Dwa gniazda RJ45
- Zasilanie PoE lub opcjonalny zasilacz
- Przycisk nawigacyjny
- Funkcja głośno mówiąca
- Gniazdo słuchawki nagłownej
- Regulacja głośności w słuchawce
- Współpraca z opcjami:
 - moduł bluetooth
 - słuchawki nagłowne
- Płynna regulacja kąta pochYLENIA wyświetlacza

5.6.3 Telefon systemowy IP typ2

Wymagania techniczne:

- Współpracujący z zaoferowaną centralą VOIP
- 16-znakowy alfanumeryczny wyświetlacz
- Dwa gniazda RJ45
- Zasilanie PoE lub opcjonalny zasilacz
- Przycisk nawigacyjny
- Duża lampka dzwonka i oczekującej wiadomości
- Funkcja głośno mówiąca
- Gniazdo słuchawki nagłownej
- 4-poziomowa regulacja głośności w słuchawce
- 8 przycisków programowalnych
- Praca w dwóch położeniach: wysokim i niskim

6 OGÓLNE WARUNKI WYKONANIA I ODBIORU ROBÓT

6.1 Pozostałe wymagania od Wykonawców

Poza robotami podstawowymi, opisanymi w dokumentacji przetargowej wykonawca jest zobowiązany do skalkulowania wszelkich robót pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania robót dla przyjętej technologii, uwzględniając warunki ich wykonania.

Wykonawca powinien ponadto uwzględnić w cenie – w ramach kosztów dodatkowych – wszelkie pozostałe koszty związane z kompleksową realizacją zamówienia, w tym:

1. koszty opracowania planu bezpieczeństwa i ochrony zdrowia oraz wykonania jego zaleceń – jeśli będzie wymagany
2. koszty zużycia mediów niezbędnych na czas budowy,
3. koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) Użytkownika przed ich zniszczeniem w trakcie wykonywania robót,
4. koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Użytkownika,
5. koszty urządzenia placu budowy,
6. koszty oznakowania robót i zabezpieczenia warunków bhp i ppoż. w trakcie realizacji robót,
7. koszty płatnych prób, badań, odbiorów technicznych, zgodnie z wymogami odpowiednich instytucji,
8. koszty opracowania dokumentacji powykonawczej,

9. koszty uporządkowania oraz przywrócenia obiektu oraz terenu po wykonanych robotach do stanu pierwotnego wraz z naprawą ewentualnych szkód użytkownikowi lub osobom trzecim,
10. wszelkie inne koszty wynikłe z analizy dokumentacji projektowej, przyjętej przez Wykonawcę technologii wykonania inwestycji oraz dokonanej wizytacji terenu budowy

Uwaga!

Zaleca się dokonanie wizji lokalnej dla w/w zakresu robót przed złożeniem oferty, oraz szczegółowe zapoznanie się z dokumentacją przetargową.

6.1.1 Szkolenia dla administratorów sieci

W ramach dostawy wymagane jest przeprowadzenie szkolenia dla wyznaczonych pracowników Zamawiającego w zakresie:

- Konfiguracji i zarządzania radioliniami cyfrowymi
- Podstawowej konfiguracji i zarządzania urządzeniami aktywnymi sieci
- Administracja i zarządzanie systemem radiowym

6.1.2 Dokumenty odbioru końcowego

Wymagane dokumenty do odbioru końcowego:

- Dokumentacja techniczna powykonawcza
- Protokoły odbiorów częściowych
- Protokoły z pomiarów i testów,
- Odpowiednie atesty i certyfikaty
- Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta

7 CZĘŚĆ INFORMACYJNA PROGRAMU

7.1 Warunki prawne i organizacyjne, jakie należy uwzględnić w projektowaniu i technologicznym wykonaniu zamówienia:

7.1.1 Akty prawne i rozporządzenia:

- 1.1 „Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 roku”.
- 1.2 „Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 roku”
- 1.3 „Ustawa o dostępie warunkowym”
- 1.4 „Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym”.
- 1.5 „Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku”.
- 1.6 Prawo Ochrony Środowiska z dnia 27 kwietnia 2001r., w zakresie zasad ochrony środowiska oraz warunków korzystania z jego zasobów
- 1.7 Rozporządzenie Rady Ministrów z dnia 21 sierpnia 2007 (Dz. U. 2007 nr 158 poz. 1105)
- 1.8 Rozporządzenie Rady Ministrów z dnia 9 listopada 2004 r. w sprawie określenia rodzajów przedsięwzięć mogących znacząco oddziaływać na środowisko oraz szczegółowych uwarunkowań związanych z kwalifikowaniem przedsięwzięcia do sporządzenia raportu o oddziaływaniu na środowisko (Dz. U. z dnia 3 grudnia 2004 r.)
- 1.9 Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych,
- 1.10 Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych
- 1.11 Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych
- 1.12 Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce.

7.1.2 Ramy prawne Komisji Europejskiej w sektorze komunikacji elektronicznej

1. Dyrektywa (2002/19/EC) z dnia 7 marca 2002r. w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz ich łączenia (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.);
2. Dyrektywa (2002/20/EC) z dnia 7 marca 2002 r. w sprawie zezwoleń na udostępnianie sieci i usług łączności elektronicznej (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.);

3. Dyrektywa (2002/21/EC) z dnia 7 marca 2002r. w sprawie jednolitej struktury regulacji dla sieci i usług komunikacji elektronicznej (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.);
4. Dyrektywa (2002/22/EC) z dnia 7 marca 2002r. w sprawie usługi powszechnej i praw użytkowników odnoszących się do sieci i usług łączności elektronicznej (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.);
5. Dyrektywa (2002/58/EC) z dnia 12 lipca 2002r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. WE L. 201 z 31 lipca 2002r.);
6. Dyrektywa (2002/77/EC) z dnia 16 września 2002r. w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej (Dz. Urz. WE L. 249 z 17 września 2002r.);
7. Rozporządzenie (EC) 2887/2000 o niezależnym dostępie do pętli lokalnych

7.1.3 Przy projektowaniu i budowie sieci radiowej należy wziąć pod uwagę następujące normy i rekomendacje komitetu ITU:

- PN-ETSI EN 302 326-1
Fixed Radio Systems – Multipoint Equipment and Antennas – Part 1: Overview and Requirements for Digital Multipoint Radio Systems.
- PN-ETSI EN 302 326-2
Fixed Radio Systems – Multipoint Equipment and Antennas – Part 2: Harmonized EN covering essential requirements under article 3.2 of the R & TTE directive for Digital Equipment of Multipoint Radio Systems.
- PN-ETSI EN 302 326-3
Fixed Radio Systems – Multipoint Equipment and Antennas – Part 3: Harmonized EN covering essential requirements under article 3.2 of the R & TTE directive for Antennas of Multipoint Radio Systems.
- ITU-R
Regulations for Radio Communications, Article 5 of the ITU Radio Regulations (Genewa, 2008)
- ECC
EPORT 91 Compatibility of Earth stations on Board Vessels Transmitting within the GAPS in the CEPT Fixed Service channel plan for the lower 6 GHz band