



Fundusze Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Człuchów, dnia 30.09.2022 roku

Nr 271.19.2022

**Wszyscy Wykonawcy**

### **ZMIANA treści SWZ**

Gmina Człuchów działając zgodnie z art. 286 ust. 1 ustawy z dnia 11 września 2019 roku - Prawo zamówień publicznych, zmienia treść Specyfikacji Warunków Zamówienia:

Załącznik nr 4 do Specyfikacji Warunków Zamówienia - SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA - ulega zmianie i otrzymuje brzmienie:

### **SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

#### **Część 1 Zamówienia – urządzenie wielofunkcyjne – 1 szt.**

Lp.	Typ Parametru	Wymaganie minimalne
1.	Technologia druku	technologia laserowa
2.	Funkcje standardowe	kopiarka, drukarka sieciowa, kolorowy skaner sieciowy, fax
3.	Format oryginału	A4
4.	Format kopii	A4-A6
5.	Prędkość druku	38 stron A4 / min.

6.	Dostępne rozdzielczości drukowania	min. 600x600 dpi
7.	Czas wydruku pierwszej strony	maks. 9 sek.
9.	Kopiowanie wielokrotne	1- 999 kopii
10.	Pamięć RAM	min. 512 MB
11.	Zoom	25-400%
12.	Panel operatora	kolorowy ekran dotykowy z możliwością pochylenia opisy na panelu oraz komunikaty na ekranie w języku polskim
13.	Dupleks	automatyczny, w standardzie
14.	Podajnik dokumentów	automatyczny, dwustronny-jednoprzebiegowy, na min. 50 ark. w standardzie
15.	Podajniki papieru	min. 1 kasetka na min. 250 ark. A5-A4 (80 g/m <sup>2</sup> ) taca uniwersalna na min. 50 ark. A6-A4 (80 g/m <sup>2</sup> )
16.	Funkcja druku sieciowego	w standardzie
17.	Emulacje	PCL 6, PostScript 3
18.	Interfejsy	USB 2.0, Ethernet 10/100/1000Base-T
19.	Funkcja skanowania sieciowego	w standardzie, skanowanie pełno-kolorowe
20.	Funkcje skanowania	skanowanie do e-mail, folderu sieciowego, do pamięci przenośnej USB
21.	Rozdzielczość skanowania	600 dpi
22.	Typy plików	PDF, JPG, TIFF
23.	Możliwość rozbudowy	Dodatkowy podajnik lub podajniki papieru, o pojemności łącznej min. 500 ark. formatu A4 – A5, 80 g/m <sup>2</sup>
24.	Materiały eksploatacyjne jako wyposażenie standardowe	Tonery - właściwa ilość, która zapewni wydrukowanie minimum 3 000 stron A4 przy pokryciu zgodnie z ISO19752. Możliwość zastosowania tonera o minimalnej wydajności 10 tys stron

25.	Wymagania dodatkowe	
		Certyfikat ISO 9001:2015 producenta oferowanego sprzętu – dostarczyć przed podpisaniem umowy
		Certyfikat ISO 14001:2015 producenta oferowanego sprzętu – dostarczyć przed podpisaniem umowy

## **Część 2 Zamówienia – system umożliwiający zarządzanie pracami Rady Gminy**

### **– 1 kpl.**

1. Usługa tworzenia napisów wraz z ich korektą – 80 godzin (160 pakietów) rozliczenie za każde rozpoczęte 30 minut nagrania.
2. Dostawa systemu konferencyjnego - 15 pulpitów.
3. Dostawa tabletów do obsługi systemu – 15 sztuk oraz access pointa sieciowego
4. Przeprowadzenie szkoleń w siedzibie Zamawiającego dla pracowników Biura Rady oraz Radnych.
5. Dostawa i montaż systemu do transmisji z obrad.
6. Utrzymanie wdrożonego systemu w infrastrukturze technicznej wykonawcy.
7. Świadczenie usługi zdalnej asysty technicznej oraz serwisu systemu informatycznego przez okres 24 miesięcy od dnia wdrożenia.

### **System Informatyczny – minimalne wymagane funkcjonalności:**

1. Przygotowywanie i elektroniczna dystrybucja porządku obrad wraz z materiałami dla radnych poprzez konto użytkownika w systemie.
2. Funkcja importu porządku obrad bezpośrednio z pliku .docx, .doc (Word).
3. Możliwość dodawania dokumentów przez administratorów do wbudowanego w systemie repozytorium plików.
4. Możliwość dodawania do porządku obrad załączników w postaci elektronicznej takich jak projekty uchwał, załączniki do uchwał, mapy, prezentacje, itp. załączniki w formatach \*.doc, \*.docx, \*.pdf, \*.xls, \*.xlsx, \*.jpg, \*.jpeg, \*.bmp, \*.ppt, \*.pptx.
5. Możliwość eksportowania dokumentów z edytora aktów prawnych – Legislador do systemu obsługi Rady
6. Możliwość dodawania linków do punktów w utworzonym posiedzeniu.
7. Możliwość dodawania prywatnych notatek do posiedzenia przez operatora oraz radnych.
8. Możliwość edytowania porządku obrad w trakcie posiedzeń.
9. Możliwość wydrukowania materiałów sesyjnych.

10. Zarządzanie bazą kontaktów i wewnętrzną komunikacją między biurem rady, a radnymi z możliwością przesyłania wiadomości poprzez e-mail oraz SMS – możliwość wysyłki min 1000 SMS. Archiwizowanie przesyłanych wiadomości w systemie z możliwością sprawdzenia historii korespondencji.
11. Tworzenie głosowań jawnych (imiennych), zwyczajnych (tajnych), oraz specjalnych (np. do przeprowadzania różnego rodzaju wyborów).
12. Możliwość tworzenia głosowań z własnymi odpowiedziami.
13. Możliwość zabezpieczenia głosowań kodem PIN ustalonym przez administratora oraz jego wyświetlenie na ekranie prezentacyjnym podczas głosowania.
14. Możliwość automatycznego i ręcznego sprawdzenia listy obecności radnych z możliwością ręcznej modyfikacji tej listy, na wypadek spóźnień czy wcześniejszych wyjść.
15. Generowanie raportu obecności z informacją o obecności radnych w poszczególnych punktach porządku obrad.
16. Sprawdzanie obecność w trakcie posiedzenia w formie głosowania.
17. Brak możliwości oddawania głosu przez osoby oznaczone jako nieobecne na posiedzeniu
18. Prezentacja wyników głosowań na urządzeniach wszystkich osób biorących udział w głosowaniach
19. Możliwość zabezpieczenia głosowania na podstawie adresu IP z którego będą przyjmowane głosy – zewnętrzny adres sieci urzędowej, w celu wyeliminowania możliwości oddania głosów przez osoby przebywające poza urzędem.
20. Dostęp do systemu za pomocą urządzeń mobilnych oraz komputerów umożliwiający:
  - sprawdzenie kalendarium posiedzeń nadchodzących oraz archiwalnych,
  - przeglądanie porządków obrad i wyników głosowań,
  - pobieranie i przeglądanie załączników,
  - głosowanie (oddawanie głosów) w czasie rzeczywistym podczas posiedzenia poprzez wybór jednego z 3 przycisków: „za”, „przeciw”, „wstrzymuję się”.
  - zgłaszanie się do dyskusji i przeglądanie listy osób planujących wypowiedź w danej sprawie w czasie rzeczywistym podczas posiedzenia.
  - funkcję wewnętrznego komunikatora dla radnych.
21. Elektroniczna i interaktywna obsługa posiedzeń poprzez:
  - elektroniczną rejestrację radnych zgłaszających się do dyskusji nad projektami uchwał i innymi materiałami będącymi przedmiotem obrad,
  - elektroniczną rejestrację wniosków formalnych,
  - elektroniczną obsługę głosowań podczas sesji (głosowania jawne imienne),
  - prezentację porządku obrad oraz dostęp do załączników w czasie posiedzenia,
  - możliwość dynamicznej modyfikacji porządku obrad oraz materiałów na posiedzenia z automatycznym odświeżaniem zmian na urządzeniach radnych,
  - prezentację przedmiotu głosowania, listy osób uprawnionych do głosowania i wyników głosowania w czasie posiedzenia,
  - dynamiczne zarządzanie listą gości, którym udziela się głosu podczas posiedzenia,
  - możliwość ustawienia czasu wypowiedzi oraz wyświetlanie w czasie posiedzenia licznika czasu wypowiedzi i komunikatu o przekroczeniu czasu wypowiedzi,
  - zatwierdzanie uchwał,

- przygotowanie projektów protokołu z posiedzeń z automatycznym przekazywaniem wyników głosowań,
  - rejestrację dźwięku w systemie informatycznym z możliwością transkrypcji dźwięku na tekst przy wykorzystaniu zewnętrznego oprogramowania,
  - rejestrację dźwięku w systemie informatycznym wraz ze scenariuszem prezentującym punkty porządku obrad oraz wypowiadające się przy tych punktach osoby z możliwością odsłuchania konkretnej wypowiedzi po wybraniu jej ze scenariusza,
  - umożliwienie poprzez sieć Internet dostępu mieszkańcom i podmiotom zainteresowanym do transmisji z posiedzenia (na żywo), przeglądania porządku obrad wraz z załącznikami (bieżących oraz archiwalnych) oraz przeglądanie wyników głosowań.
22. Możliwość tworzenia wewnętrznego rejestru uchwał oraz jego automatyczne publikowanie dla mieszkańców i podmiotów zainteresowanych.
  23. Dostęp interesantów do kalendarza radnego informującego o planowanych dyżurach.
  24. Możliwość integracji z systemami zewnętrznymi Zamawiającego – Wykonawca zobowiązuje się udostępnić API umożliwiające integracje w zakresie przesyłania danych dostępnych w systemie do obsługi Rady
  25. System obsługiwany będzie przez laptopy z systemem Windows lub urządzenia mobilne z systemem android nie starszym niż wersja 4.4

**System transmisji z obrad (dostawa komputera, kamery oraz montaż po stronie Wykonawcy)  
– minimalne wymagane funkcjonalności:**

- System musi współpracować z kamerą szybkoobrotową o minimalnych parametrach dostarczoną przez Wykonawcę:
  - Praca w standardzie TCP/IP,
  - przetwornik 1/2.8",
  - obiektyw w zakresie 2.7-11 mm,
  - zoom optyczny 4x,
  - protokoły sieciowe: IPv4, SSL, RTSP, DHCP, UPnP,
  - zasilanie PoE,
  - ONVIF.
- System ma realizować transmisję z wykorzystaniem komputera o minimalnych parametrach dostarczonego przez Wykonawcę:
  - procesor o wyniku nie niższym niż 11000 punktów AVERAGE CPU ze strony <https://www.cpubenchmark.net/>
  - dedykowana karta graficzna o wyniku nie niższym niż 7800 punktów AVERAGE G3D ze strony <https://www.videocardbenchmark.net/>
  - dysk SSD 240GB
  - 8GB RAM
  - Na komputerze ma być zainstalowany licencjonowany enkoder softwerowy (nie bezpłatny OBS Studio) służący do transmisji i archiwizacji nagrania. Minimalne wymagane parametry:
    - Wejścia: 4, w tym wejścia dla min. 2 kamer
    - Maksymalna rozdzielczość 1920 x 1080px

- Kanały warstw (overlay): 1
  - Nagrywanie, Streaming,
  - 1 wyjście Fullscreen, 1 wyjście zewnętrzne (external)
  - licencja wieczysta
- Transmisje mają być zintegrowane z systemem do obsługi Rady w zakresie:
    - a. Automatycznego wyświetlania w transmisji informacji o:
      - aktualnie przemawiającej osobie
      - aktualnie omawianym punkcie z porządku obrad
      - uruchomionym głosowaniu i temacie tego głosowania
      - wynikach głosowania
      - o trwającej przerwie
      - nazwie instytucji i dacie posiedzenia
  - System ma zapewniać możliwość automatycznego przewinięcia archiwalnego nagrania wideo do wybranego przez oglądającego punktu porządku obrad,
  - Podczas okresu obowiązywania gwarancji wymagana jest transmisja oraz archiwizacja nagrań z sesji o minimalnej jakości 720p poprzez serwery Wykonawcy.

Usługa tworzenia napisów 80 godzin, rozliczenie za każde rozpoczęte 30 minut nagrania (160 pakietów) – minimalne wymagane funkcjonalności:

Napisy powinny zostać przygotowane w odrębnych plikach (SRT / VTT), które umożliwiają dodanie ich do odtwarzacza z nagraniem, co zwiększy ich funkcjonalność oraz dostępność. Napisy muszą zostać wyprodukowane zgodnie ze standardem WCAG 2.1 i ogólnie przyjętymi zasadami:

- Tekst będzie zawierać wszystkie słyszalne dźwięki na nagraniu,
- Tekst będzie dosłowny i może odzwierciedlać błędy (oryginalną wymowę): językowe, składniowe, powtórzenia,
- Słowa niepewne/niezrozumiałe będą zapisane w taki sposób, w jaki zostały usłyszane, oznaczając znakiem [?],
- Elementy niesłyszalne/niezrozumiałe, np. z powodu jakiś zakłóceń czy problemów ze ścieżką audio, będą oznaczone jako: [niesłyszalne], [niezrozumiałe],
- Przerwane wypowiedzi będą zakończone wielokropkiem (np.: W dniu wczorajszym... Proszę mi nie przeszkadzać!),
- Inne elementy głosowe, wpływające na zrozumienie treści, zapisane będą w nawias kwadratowych, np. [śmiech], [jąkanie], [płacz], [krzyk]. Podobnie jak komentarze dotyczące niewerbalnych dźwięków, ważnych dla zrozumienia sytuacji np.: [oklaski], [hymn], [muzyka klasyczna] itd.,
- Edycja będzie wykona zgodnie z zasadami języka polskiego, uwzględniając w to interpunkcję, zasady stosowania dużych liter, zapisywanie skrótów,
- W przypadku nazw własnych skróty stosuje się tylko jeśli nazwa została wypowiedziana z zastosowaniem skrótu,
- Nazwy własne i skróty odmieniane mogą być zapisywane w sposób, w jaki zostały wypowiedziane.

**Jednostki konferencyjne (pulpity dyskusyjne) – 15 szt.**

- Minimalne wymagane funkcjonalności

- Szyjka mikrofonu o długości minimum 480 mm oraz minimum jednym przegubie.
  - Przycisk zabrania głosu z wskaźnikiem LED informującym o aktywnym mikrofonie
  - Wbudowane 3,5 mm stereofoniczne gniazdo słuchawkowe
  - Odporność na zakłócenia z sieci GSM
  - Wskaźnik LED na głowicy mikrofonu informujący o stanie mikrofonu z rozróżnieniem aktywnego mikrofonu i żądaniem udzielenia głosu
  - Pulpity łączone metodą szeregową, każdy z pulpitów musi posiadać gniazdo przelotowe.
  - Wbudowany wysokiej jakości głośnik
  - Możliwość konfiguracji dowolnego pulpitu jako jednostki przewodniczącego lub dostarczenie pulpitu dedykowanego dla przewodniczącego.
- Parametry techniczne
    - Pasmo przenoszenia minimum od 200 Hz do 12,5 kHz
    - Impedancja obciążenia słuchawek  $> 8 \Omega < 1 \text{ k} \Omega$
    - Znamionowy poziom wyjścia głośnika maksymalnie 72 dB SPL
    - Maksymalne wymiary urządzenia bez mikrofonu (wys. X szer. X gł.) 65 x 210 x 150 mm
    - Montaż stołowy
    - Materiał plastik, metal
    - Temperatura pracy od 0 do 35°C

### **Jednostka sterująca systemem konferencyjnym**

- Minimalne wymagane funkcjonalności
  - Kontrola dyskusji odbywa się poprzez wybór jednego z dostępnych trybów dyskusji: Tryb otwarty - uczestnicy mogą mówić, naciskając przycisk na swoim mikrofonie. Gdy maksymalna liczba otwartych mikrofonów zostanie osiągnięta, następny uczestnik, który naciśnie przycisk swojego mikrofonu, zostanie dodany do listy oczekujących. Pierwszy uczestnik z listy oczekujących będzie mógł mówić, gdy zostanie wyłączony któryś z aktywnych mikrofonów; Tryb z wyciszaniem - uczestnicy mogą wyciszać się wzajemnie przez włączanie swojego mikrofonu. Gdy maksymalna liczba otwartych mikrofonów zostanie osiągnięta, następny uczestnik, który naciśnie przycisk na swoim mikrofonie, dezaktywuje mikrofon, który był najdłużej aktywny (mikrofon, który posiada przewodniczący nie jest uwzględniany w liczbie otwartych mikrofonów i dlatego nie może go wyciszyć żaden inny uczestnik); Tryb aktywacji głosowej - uczestnicy mogą aktywować

swoje mikrofony, mówiąc do nich. Mikrofon może być czasowo wyciszony poprzez naciśnięcie i przytrzymanie przycisku mikrofonu.

- Kontrola otwartych mikrofonów pozwalająca wybrać minimum 4 otwarte mikrofony
- Wbudowany rejestrator dźwięku może nagrywać dyskusję w formacie MP3 do pamięci wewnętrznej lub pamięci USB

- Parametry techniczne:

- Z przodu jednostki: 1 x złącze USB
- Z tyłu jednostki: 1x wyjście RCA, 1x wejście RCA,”
- 1x łącze RJ45 do komunikacji
- Napięcie zasilania sieciowego od 100 do 240 VAC  $\pm$  10%
- Maks od 1,6 A (100 VAC) do 0,7 A (240 VAC)
- Minimalne napięcie zasilania do pulpitu dyskusyjnego 24V
- Liczba pulpitów dyskusyjnych na jednostkę sterującą maks. 40 urządzeń (z możliwością rozszerzenia)
- Metoda montażu stołowy lub w szafie typu Rack 19
- Wymiary maksymalne (wys. X szer. X gł.) 45 x 483 x 300

### **Integracja systemu konferencyjnego z dostarczanym systemem do obsługi rady:**

- Zgłoszenie chęci zabrania głosu:
  - Chęć zgłoszenia do głosu przez Radnego musi być możliwa z poziomu tabletu (systemu do obsługi rady) oraz pulpitu konferencyjnego
  - Zgłoszenie z poziomu tabletu spowoduje pojawienie się radnego na liście osób chętnych do zabrania w systemie obsługi rady oraz zaświecenie wskaźnika LED na szyjce mikrofonu przypisanym do radnego w kolorze innym niż kolor aktywnego mikrofonu. Imienia, nazwiska oraz pełnionej funkcji mówcy”
  - Zgłoszenie z poziomu pulpitu konferencyjnego spowoduje zaświecenie wskaźnika LED na szyjce mikrofonu przypisanym do Radnego w kolorze innym niż kolor aktywnego mikrofonu oraz umieszczenie radnego na liście osób chętnych do zabrania głosu w dyskusji”
- Udzielenie radnemu zgody na zabranie głosu:
  - Udzielenie zgody na głos jest możliwe z poziomu aplikacji do obsługi rady dla administratora oraz poprzez aplikację na urządzeniu Przewodniczącego



- Udzielenie głosu spowoduje zmianę koloru wskaźnika LED umieszonego na szyjce mikrofonu na kolor inny niż w przypadku chęci zabrania głosu oraz aktywuje mikrofon”
- Wykonawca dostarczy Zamawiającemu aplikację do integracji wraz z danymi uwierzytelniającymi, którą zamawiający będzie mógł samodzielnie zainstalować na dowolnym urządzeniu z systemem Windows

#### **Tablety do obsługi systemu Rady 15 szt. – minimalne wymagane funkcjonalności:**

- Procesor - 8-rdzeniowy,
- Pamięć RAM - 4 GB DDR4
- Pamięć wbudowana - 64 GB
- Typ ekranu - IPS
- Przekątna ekranu - 10,1"
- Rozdzielczość ekranu - 1280 x 800
- Łączność -Wbudowany modem LTE, Wi-Fi 5 (802.11 b/g/n/ac), Moduł Bluetooth,
- Złącza - USB typ C - 1 szt. Wyjście słuchawkowe - 1 szt. Czytnik kart pamięci - 1 szt. Gniazdo kart nanoSIM - 1 szt.
- Bateria - Litowo-polimerowa 5000 mAh
- System operacyjny - Android 10
- Etui bez klawiatury
- Konfiguracja aplikacji dla Radnych na urządzeniach

#### **Access Point – 1 szt. – minimalne wymagane funkcjonalności**

- Częstotliwość pracy 2.4Ghz 5Ghz
- Tryb PoE 802.3af
- Szyfrowanie: AES,TKIP,WEP,WPA,WPA-Enterprise,WPA-PSK,WPA2
- Poziom wzmacnienia anteny 3dBi
- Przepustowość danych 1733 Mbit/s
- Standardy komunikacyjne: IEEE 802.11a,IEEE 802.11ac,IEEE 802.11b,IEEE 802.11g,IEEE 802.11n,IEEE 802.1Q

#### **Wymagania dodatkowe:**

1. Montaż, konfiguracja oraz parametryzacja wszystkich dostarczonych urządzeń po stronie Wykonawcy.
2. Archiwizacja nagrania transmisji lokalnie na dysku komputera.
3. Publikacja materiałów sesyjnych oraz wyników przeprowadzonych głosowań w Internecie w oparciu o infrastrukturę techniczną Wykonawcy.
4. Przechowywanie danych na serwerach znajdujących się na terytorium Rzeczypospolitej Polskiej.
5. Udostępnienie kopii zapasowej oprogramowania oraz danych wprowadzonych przez

Zamawiającego na żądanie Zamawiającego.

6. Wykonawca winien przed podpisaniem umowy przedstawić karty katalogowe oferowanych urządzeń.

### **Część 3 Zamówienia – system do rejestracji pracy – 1 kpl.**

- Integracja z istniejącymi bazami danych SQL i systemami wraz z ich późniejszymi aktualizacjami przez okres 2 lat
- możliwość obsługi do 4000 Pracowników
- minimum 99 harmonogramów czasowych
- obsługa standardu kart EM 125 kHz oraz 13,56 MHz MIFARE®
- zasięg odczytu kart 15 cm
- możliwość podpięcia większej ilości czytników w standardzie Wiegand 26..66 bit i innych
- tryby identyfikacji: Karta lub PIN, Karta i PIN, tylko Karta, Tylko PIN
- komunikacja oraz zarządzanie LAN WAN - protokół TCP/IP i COM,USB
- minimum 30000 zdarzeń w buforze
- programowane linie wejściowe
- programowalne linie wyjściowe min 1A
- przyciski funkcyjne konfigurowalne z systemu

### **Część 4 Zamówienia – urządzenie UTM – 1 szt.**

#### **OBSŁUGA SIECI**

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.

#### **ZAPORA KORPORACYJNA (Firewall)**

2. Urządzenie ma być wyposażone w Firewall klasy StatefulInspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.

7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u.
8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

### **INTRUSION PREVENTION SYSTEM (IPS)**

10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.
15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
16. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

### **KSZTAŁTOWANIE PASMA (TrafficShapping)**

17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

### **OCHRONA ANTYWIRUSOWA**

21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
24. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

## **OCHRONA ANTYSZPAM**

25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
26. Ochrona antyspam ma działać w oparciu o:
  - a. białe/czarne listy,
  - b. DNS RBL,
  - c. heurystyczny skaner.
27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

## **WIRTUALNE SIECI PRYWANTE (VPN)**

29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
30. Odpowiednio kanały VPN można budować w oparciu o:
  - a. PPTP VPN,
  - b. IPSec VPN,
  - c. SSL VPN
31. SSL VPN musi działać w trybach Tunel i Portal.
32. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię RouteBased.

## **FILTR DOSTĘPU DO STRON WWW**

36. Urządzenie ma posiadać wbudowany filtr URL.
37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
38. Administrator musi mieć możliwość dodawania własnych kategorii URL.
39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
41. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
  - a. blokowanie dostępu do adresu URL,
  - b. zezwolenie na dostęp do adresu URL,
  - c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.

44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
46. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.
47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.

## **UWIERZYTELNIANIE**

48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
  - a. lokalną bazę użytkowników (wewnętrzny LDAP),
  - b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
  - c. usługę katalogową Microsoft Active Directory.
49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.
50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzację w oparciu o protokoły:
  - a. SSL,
  - b. Radius,
  - c. Kerberos.
51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
52. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
53. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

## **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)**

54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. LoadBalancing).
55. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:
  - a. równoważenie względem adresu źródłowego,
  - b. równoważenie względem połączenia.
56. Mechanizm równoważenia łączy musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
57. Urządzenie ma posiadać mechanizm przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego.
58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego.
60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
61. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

## **POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA**

62. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
63. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
64. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
65. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS
66. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
67. Urządzenie musi posiadać usługę DNS Proxy.

#### **ADMINISTRACJA URZĄDZENIEM**

68. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.
69. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
70. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
71. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
72. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
73. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
74. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
75. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
76. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
77. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
78. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

#### **RAPORTOWANIE**

79. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
80. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
81. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
82. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów.
83. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
84. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
85. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy

#### **PARAMETRY SPRZĘTOWE**

86. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash.
87. Liczba portów Ethernet 10/100/1000Mbps – min. 8.
88. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta.
89. Przepustowość Firewalla – min. 3,5Gbps
90. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,4 Gbps.
91. Przepustowość filtrowania Antywirusowego – min. 400Mbps
92. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps.
93. Maksymalna liczba tuneli VPN IPsec nie może być mniejsza niż 100.
94. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20.
95. Obsługa min. VLAN 64
96. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę.
97. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
98. Urządzenie jest nielimitowane na użytkowników.

WÓJT  
*Paweł Gibczyński*  
Paweł Gibczyński