Zapytanie ofertowe- „Cyfrowa Gmina”

Zbójna, 20.10.2022 r.

ZAPYTANIE OFERTOWE

Wójt Gminy Zbójna zaprasza do składania ofert cenowych na zakup i dostawę sprzętu komputerowego i oprogramowania dla Gminy Zbójna w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

I. ZAMAWIAJĄCY:

Nazwa zamawiającego: Gmina Zbójna

Adres zamawiającego: ul. Łomżyńska 64, 18-416 Zbójna

Telefon/fax: (86) 214 00 29

II. TERMIN REALIZACJI ZAMÓWIENIA:

a) data rozpoczęcia: od dnia podpisania umowy pomiędzy Gminą Zbójna a Wykonawcą

b) data zakończenia: 3 miesiące od dnia wejścia w życie Umowy (ale nie dłużej niż do dnia 31.03.2023 r.)

III. OPIS PRZEDMIOTU ZAMÓWIENIA:

1. Zakup i dostawa serwera z oprogramowaniem – 1 szt.

Serwer powinien spełniać następujące wymagania:

• Pamięć RAM 48GB w kościach DDR4, o taktowaniu minimum 3200MHz, kości pamięci wyposażone w system kodowania korekcyjnego ECC, możliwość rozszerzenia pamięci RAM maksymalnie do 3TB

• Zainstalowany procesor 16 rdzeniowy/32 wątkowy o taktowaniu minimalnym 2.1GHz i TDP typical 100W, procesor powinien osiągać wynik minimum 20 tys. Pkt benchmark w teście cpubenchmark.net

• Zainstalowane dedykowane do danego serwera chłodzenie procesorów umożliwiające poprawną pracę systemu

• Platforma powinna obsługiwać do 8 dysków 2,5 cala w formacie hot-swap, wszystkie dyski powinny być obsługiwane z poziomu jednego kontrolera

• Zainstalowany dedykowany kontroler RAID, posiadający możliwość obsługi co najmniej 8 dysków w tym SATA/SAS/NVME, kontroler musi wpierać minimum RAID 0,1,5,6,10,50,60, kontroler powinien posiadać minimum 4GB cache

• Zainstalowane co najmniej dwa dyski SSD NVME klasy enterprise, o pojemności nie mniejszej niż 960GB

• Zintegrowana karta sieciowa 10GbE posiadająca minimum 2 porty RJ45

• Zainstalowany system operacyjny Windows Server Essential 2022 posiadający licencje na obsługę wszystkich rdzeni zamontowanych procesorów

• Do zestawu dołączony napęd DVD, napęd powinien być zamontowany w obudowie serwera

• System powinien posiadać zasilanie redundantne z dwoma zasilaczami klasy Titanium o mocy minimum 1300W każdy, dedykowane do danego modelu serwera, zasilacze powinny

umożliwiać wyjęcie podczas pracy serwera (hot-swap), do zasilaczy dołączone 2 przewody

zasilające

• Serwer powinien być wyposażony w moduł TPM 2.0

• Serwer powinien posiadać umożliwiać montaż w szafie RACK, wysokość serwera max 1U, do serwera dołączone szyny montażowe w zestawie

• Gwarancja na okres 3 lat, świadczona na miejscu u klienta (on-site) z czasem reakcji 24h (w dni robocze)

• Możliwość rozszerzenia gwarancji do 8 lat w trakcie jej trwania

• W ramach gwarancji klient ma zapewnione pozostawienie uszkodzonego dysku twardego (KYHD) przez cały okres świadczenia usługi serwisowej

• Serwis realizowany przez producenta lub autoryzowanego serwis partnera

• Możliwość weryfikacji na stronie producenta specyfikacji serwera, okresu gwarancji oraz pobrania najnowszych sterowników po podaniu numeru seryjnego sprzętu

• Sprzęt wyprodukowany zgodnie z normami ISO 9001, ISO 14001 oraz CE, produkcja w Europie

• Zintegrowana karta graficzna ze złączem VGA, posiadająca minimum 128MB pamięci

ddr4 ram

• Płyta główna dedykowana do serwera posiadająca obsługę minimum 2 procesorów,

• Serwer powinien mieć możliwość optymalizacji pod kątem wirtualizacji Hyper-V

• Zintegrowana karta zdalnego zarzadzania posiadająca dedykowany port RJ45 i mająca

między innymi funkcjonalność:

a. - Virtual KVM over HTML5

b. - Integrated BMC Web Console

c. - Redfish (Redfish Scalable Platforms Management API)

d. - IPMI 2.0 Node Manager

e. - Out-of-Band BIOS/BMC Update and Configuration

f. - System Inventory

g. - Autonomous Debug-Log

2. Zakup i dostawa stacji roboczej – 7 szt.

Stacje robocze powinny spełniać następujące wymagania:

• Procesor: 4 rdzenie, 8 wątków, taktowanie bazowe 3,6GHz, w trybie turbo 4,3GHz, 6MB cache, TDP – 65W, ze zintegrowaną kartą graficzną, osiągający wynik minimum 8770 punktów w teście PassMark – CPU Benchmarks (na dzień 16.09.2022) opublikowany na stronie https://www.cpubenchmark.net/cpu_list.php

• Pamięć RAM: Minimum 4GB (DDR4, 3200MHz)

• Płyta główna: 2 sloty pamięci, obsługa do 64GB RAM, wbudowana karta sieciowa 1Gbit z obsługą WOL, 1x PCI Express 4.0 x16, 2x PCI Express x1, złącza na tylnym panelu: 2x PS, 1x DVI-D, 1x HDMI, 1x DP, 6x USB z czego min. 2x USB 3.2 Gen1

• BIOS: Zapisana trwale w BIOS informacja dotycząca nazwy producenta, numeru seryjnego i modelu.

• Dysk: SSD, minimum 256GB

• Karta graficzna: Zintegrowana

• Multimedia: Wbudowana karta dźwiękowa 8-kanałowa zgodna z High Definition,

• Łączność: LAN 10/100/1000 Mbps z obsługą WOL

• Obudowa: MiniTower (obsługa kart o pełnym profilu), zaprojektowana i wyprodukowana na zlecenie producenta komputera, suma wymiarów nie większa niż 945mm, 2x USB 3.2 Gen1, Mic-In, Phone-out, możliwość instalacji wewnątrz napędów 2x 3,5” + 1x 2,5”

• Zasilacz: O mocy minimum 350W, spełnia wymagania normy 80 Plus Bronze, Sprawność energetyczna (przy obciążeniu 10%/ 20%/ 50%/ 100%): 82%/ 82%/ 85%/ 82%

Pobór mocy w trybie S3 Mode, Suspend to RAM (funkcja WOL aktywna) - 1.2W. Pobór mocy w trybie Soft off (S5 Mode) – 0,25W

• Właściwości specjalne: Możliwość zabezpieczenia linką, TPM 2.0, Windows AutoPilot ready

• System operacyjny: Windows 10 Pro 64-bit

Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.

• Certyfikaty CE, ISO 9001, ISO 14001

Zgodność: SMBios (DMI), EN62368-1, EN55032, EN55035, EN61000-3-2/3, EN62623, 89/336/ECC

• Gwarancja 24 miesiące. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta.

Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.

Możliwość wydłużenia gwarancji do 5 lat w trakcie trwania okresu gwarancji.

• Wymagania dodatkowe: Sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania, trwale oznaczony logo producenta.

Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego.

Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2022 roku.

Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność

• Monitor: 21,5”, matryca MVA, Full-HD, czas reakcji 5ms, kontrast dynamiczny – 5 000 000:1 (DCR), plamka 0,248mm

Złącza VGA, HDMI

Wbudowane głośniki

Możliwość pochylenia ekranu w zakresie -5 o - 20 o

Funkcja Flicker-Free oraz Anti-Blue-Light

VESA 100x100

Zużycie energii - <0,5W (wyłączony), <0,5W (standby)

Opatrzony logiem producenta komputera

Kabel HDMI i Audio w komplecie.

Gwarancja 24 miesiące – w przypadku usterki zawsze wymiana monitora na nowy na miejscu u klienta.

Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta.

Możliwość sprawdzenia okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.

Możliwość wydłużenia gwarancji do 5 lat w trakcie trwania okresu gwarancji.

3. Zakup i dostawa urządzenia centralnego systemu pamięci masowej 1 szt.

Serwer powinien spełniać następujące wymagania:

• Procesor: Procesor 64 bit x86 o taktowaniu nie mniejszym niż 2.2 GHz

• Procesor liczba rdzeni: Nie mniej niż 4

• Pamięć RAM: Nie mniej niż 8GB

• Pamięć RAM liczba slotów: Minimum 2 sloty

• Pamięć RAM - możliwość rozszerzenia: Nie mniej niż do 64GB

• Pamięć Flash: Nie mniej niż 5 GB

• Liczba zatok na dyski: Minimum 4 zatoki 3,5"

• Obsługiwane dyski: 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD

• Wbudowane w urządzenie interfejsy na dyski M2: Wymagane min. 2 x M2 PCIe Gen3x1

• Możliwość stosowania dysków twardych o pojemności: do 18TB

• Możliwość podłączenia modułu rozszerzającego: Tak, co najmniej 2

• Porty LAN 2,5 GbE: Minimum 2 RJ-45

• Diody LED: Minimum Status, LAN, HDD

• Porty USB 3.2 Gen2: Minimum 3

• Port PCiE: Tak, minimum 2 Gen3x4

• Przyciski: Reset, Zasilanie

• Typ obudowy: Tower

• Dopuszczalna temperatura pracy: od 0 do 40˚C

• Wilgotność względna podczas pracy: 5-95% R.H.

• Zasilanie: Max. 250 W

• Specyfikacja oprogramowania

Obsługa dwóch systemów operacyjnych: Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS

• Wymagania dla systemu operacyjnego opartego o system plików EXT4:

Agregacja łączy: Tak

Obsługiwane systemy plików: Dyski wewnętrzne: EXT4

Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT

Możliwość podłączenia karty WLAN na USB: Tak

Szyfrowanie udziałów: Tak, min AES 256

Szyfrowanie dysków zewnętrznych: Tak

• Zarządzanie dyskami: Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD; Obsługa Hot Spare per grupa RAID oraz global hot spare; Rozszerzanie pojemności Online RAID; Migracja poziomów Online RAID; HDD S.M.A.R.T.; Skanowanie uszkodzonych bloków; Przywracanie macierzy RAID; Obsługa map bitowych; Pula pamięci masowej; Obsługa migawek; Obsługa replikacji migawek

• Wbudowana obsługa iSCSI: Multi-LUNs na Target; Obsługa LUN Mapping & Masking; Obsługa SPC-3 Persistent Reservation; Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN

• Zarządzanie prawami dostępu: Ograniczenie dostępnej pojemności dysku dla użytkownika; Importowanie listy użytkowników; Zarządzanie kontami użytkowników; Zarządzanie grupą użytkowników; Zarządzanie współdzieleniem w sieci; Tworzenie użytkowników za pomocą makr; Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL

• Obsługa Windows AD: Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web

Funkcja serwera LDAP

• Funkcje backup: Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,

• Współpraca z zewnętrznymi dostawcami usług chmury: Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box

• Darmowe aplikacje na urządzenia mobilne: Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer

Dostępne na systemy iOS oraz Android

• Minimum obsługiwane serwery: Serwer plików; Serwer FTP; Serwer WEB; Serwer kopii zapasowych; Serwer multimediów UPnP; Serwer pobierania (Bittorrent / HTTP / FTP); Serwer Monitoringu

• VPN: VPN client / VPN server

Obsługa PPTP, OpenVPN

• Administracja systemu: Połączenia HTTP/HTTPS; Powiadamianie przez e-mail (uwierzytelnianie SMTP); Powiadamianie przez SMS; Ustawienia inteligentnego chłodzenia; DDNS oraz zdalny dostęp w chmurze; SNMP (v2 & v3); Obsługa UPS z zarządzaniem SNMP (USB); Obsługa sieciowej jednostki UPS; Monitor zasobów; Kosz sieciowy dla CIFS/SMB oraz AFP; Monitor zasobów systemu w czasie rzeczywistym; Rejestr zdarzeń; System plików dziennika; Całkowity rejestr systemowy (poziom pliku); Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line; Aktualizacja oprogramowania automatyczna; Możliwość aktualizacji oprogramowania ręcznie; Ustawienia systemu: Kopia, Przywracanie, Resetowanie

•Wirtualizacja: Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.

Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5

Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.

• Konteneryzacja: Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker

• Zabezpieczenia: Filtracja IP; Ochrona dostępu do sieci z automatycznym blokowaniem; Połączenie HTTPS; FTP z SSL/TLS (Explicit); Obsługa SFTP (tylko admin); Szyfrowanie AES 256-bit; Szyfrowana zdalna replikacja (Rsync poprzez SSH); Import certyfikatu SSL; Powiadomienia o zdarzeniach za pośrednictwem Email i SMS

• Możliwość instalacji dodatkowego oprogramowania: Tak, sklep z aplikacjami; możliwość instalacji z paczek

• Gwarancja: 3 lata

• Dyski(4 szt): 4 dyski o pojemności 8TB; Dyski musza być klasy serwerowej (enterprise); Dyski SATA 6 Gbit/s; Obroty minimalnie 7200 / min; Dyski musza posiadać MTTF (MTBF) nie mniejszy niż 2 000 000h; Pojemność pamięci cache minimum 256 MB; Znamionowe roczne obciążenie pracą 550TB (rocznie); Parametr maksymalnej utrzymywanej prędkość przesyłu danych (deklarowana przez producenta dysków):

Dla technologii sektorowej 512e: 248 MiB/s dla pojemności 8TB

Gwarancja 5 lat, gwarancja musi zawierać opcje pozostawienie dysków w razie awarii przez cały okres trwania gwarancji.

Należy dostarczyć z oferta oficjalne dokumenty producenta dysków, spełniających wszystkie powyższe wymagania.

4. Zakup i dostawa komputerów przenośnych - 2 szt.

Komputery przenośne powinny spełniać następujące wymagania:

• Ekran: 15,6" o rozdzielczości FHD (min. 1920x1080 przy 60Hz) z powłoką przeciwodblaskową

• Procesor: 2 rdzenie, 4 wątki, ze zintegrowaną grafiką, taktowanie bazowe 2,1GHz, w trybie turbo 4,1GHz, 4MB cache, osiągający w teście PassMark CPU Mark wynik min. 4000 punktów na dzień 16.09.2022 (należy dołączyć wydruk ze strony https://www.cpubenchmark.net z wynikiem testu dla oferowanego procesora). Pobór mocy TDP nie większy niż 15W.

• Pamięć operacyjna: min. 8GB, 1 slot wolny, możliwość rozbudowy pamięci do 32GB

• Parametry pamięci masowej: Dysk SSD o pojemności min. 256GB

• Karta graficzna: Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią współdzieloną.

• Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki

• Płyta główna: Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora.

• Napęd: Wbudowany napęd DVD±RW

• Komunikacja: Wbudowana karta sieci bezprzewodowej 802.11 a/b/g/n/ac, moduł Bluetooth w wersji min. 5.0, karta sieciowa 10/100/1000 ze złączem RJ-45, możliwość instalacji modemu LTE wewnątrz obudowy (nie dopuszcza się modemu podłączanego do portu USB)

• Klawiatura: Układ klawiszy US, możliwość 4 stopniowej regulacji podświetlenia oraz zmiany koloru podświetlenia, wydzielony blok klawiszy numerycznych

• Bateria i zasilanie: Komputer wyposażony w baterię o pojemności min. 41Wh umożliwiającą pracę przez min. 360 minut (wg. danych producenta) oraz zasilacz. Możliwość wyjęcia i wymiany baterii bez otwierania laptopa.

• Gwarancja: Min. 24 miesiące door-to-door.

Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta. Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu. Możliwość wydłużenia gwarancji do 5 lat w trakcie trwania okresu gwarancji.

• Certyfikaty: Certyfikat CE, ISO14001, ISO9001 lub równoważne

• System operacyjny: Windows 11 Pro 64bit

W pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym Windows 11 Pro PL (wersja 64 – bitowa). Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.

• Wymagania dodatkowe:

Wbudowana kamera internetowa trwale zainstalowana w obudowie matrycy, wejście audio, wbudowany mikrofon, wbudowane głośniki, czytnik kart pamięci, złącza USB – min. 4 szt. w tym 1x USB 3.1 Type-C i 1x USB 3.1 Type-A, wyjście HDMI, wyjście VGA, Touchpad, TPM 2.0, gniazdo Kensington Lock, waga max 2,2 kg, sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania. Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego.

Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2022 roku.

Laptop trwale oznaczony logo producenta.

Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność

5. Zakup i dostawa skanera- 1 szt.

Skaner powinien spełniać następujące wymagania:

• Porty i interfejsy: Standardowe interfejsy; USB 2.0,USB 3.0

• Waga i rozmiary: Wysokość produktu - 163 mm; Szerokość produktu - 300 mm; Głębokość produktu - 170 mm; Waga produktu - 4200 g

• Konstrukcja: Typ skanera - ADF scanner; Kolor produktu- Czarny, Bialy; Typ ekranu- LCD

• Pojemność wejściowa: Pojemność automatycznego podajnika papieru- 80 arkusze

• Wydajność: Typ przetwornika obrazu- CCD; Źródło światła- White LED (2x); Sterowniki skanera- ISIS,TWAIN; Maksymalny dzienny cykl pracy- 4000 strony

• Skanowanie: Czarnobiałe skanowanie; Skala szarości, Monochromatyczne; Podwójne skanowanie; Maksymalny format skanowania- 216 x 355.6 mm; Optyczna rozdzielczość skanowania- 600 x 600 DPI; Głębokość koloru wyjścia- 24 bit; Skanowanie w kolorze; Prędkość skanowania ADF (cz (b, A4))- 60 strony na minutę; Prędkość skanowania ADF (kolor, A4)- 60 strony na minutę; Prędkość skanowania duplex ADF (cz (b, A4))- 120 ipm; Prędkość skanowania duplex ADF (kolor, A4)- 120 ipm

• Moc: Napięcie- 100-240 V; Tryb wyłączenia- 0.35 W; Pobór mocy w trybie czuwania- 1.8 W; Pobór mocy- 38 W; Typ zasilacza- Prąd przemienny

• Warunki pracy: Zakres temperatur (eksploatacja)- 5 - 35 °C; Zakres wilgotności względnej- 20 - 80 %

• Obsługa papieru: Maksymalny rozmiar papieru ISO (seria A)- A4; Gramatura nośników do automatycznego podajnika papieru- 27 - 413 g/m² ;Wykrywanie sklejonych stron; Rozmiary seri A ISO (A0…A9)- A4; Minimalny obszar skanowania (Auto Document Feeder)- 50.8 x 54 mm

• Certyfikaty: Zgodność z RoHS- Tak; Certyfikat EnergyStar- Tak

• Wymagania systemowe:

Obsługiwane systemy operacyjne Windows: Windows 7 Home Basic,Windows 7 Home Basic x64,Windows 7 Home Premium,Windows 7 Home Premium x64,Windows 7 Professional,Windows 7 Professional x64,Windows 7 Starter,Windows 7 Starter x64,Windows 7 Ultimate,Windows 7 Ultimate x64,Windows 8,Windows 8 Enterprise,Windows 8 Enterprise x64,Windows 8 Pro,Windows 8 Pro x64,Windows 8 x64,Windows Vista Business,Windows Vista Business x64,Windows Vista Enterprise,Windows Vista Enterprise x64,Windows Vista Home Basic,Windows Vista Home Basic x64,Windows Vista Home Premium,Windows Vista Home Premium x64,Windows Vista Ultimate,Windows Vista Ultimate x64,Windows XP Home,Windows XP Home x64,Windows XP Professional,Windows XP Professional x64

6. Zakup i dostawa urządzenia (UTM) zabezpieczającego sieć -1 szt.

Urządzenie powinno spełniać następujące wymagania:

• Wymagania Ogólne: Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall; Ochrony w warstwie aplikacji; Protokołów routingu dynamicznego.

• Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

• Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum: 5 portami Gigabit Ethernet RJ-45.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

4. System musi być wyposażony w zasilanie AC.

• Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.

4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.

5. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.

6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.

7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

• Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system Polityki, Firewall

13. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

14. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).
- Microsoft Azure
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.

- Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.

• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

• Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

• Routingu statycznego.

• Policy Based Routingu.

• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

• Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

• Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

• Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

• Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

• Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

• Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

• Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

• Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

• Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

• Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.

• Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

• Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

• Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw.

produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Uwagi: Sprzęt nowy, wolny od wad fizycznych oraz nie będący przedmiotem praw osób trzecich.

7. **Pakiet biurowy: Microsoft Office 2021; Licencja komercyjna, wieczysta**

IV. MIEJSCE I TERMIN ZŁOŻENIA OFERT

Ofertę cenową należy złożyć na formularzu ofertowym /w formie papierowej pocztą tradycyjną/, stanowiącym załącznik do zapytania ofertowego do dnia 31.10.2022r. do godz. 10.00 na adres Zamawiającego:

Urząd Gminy Zbójna ul. Łomżyńska 64, 18-416 Zbójna

Pracownik uprawniony do kontaktu:

Michał Bajno

tel. 86 214 00 23

e-mail: michal.bajno@ug.zbojna.wrotapodlasia.pl

Kryterium oceny ofert: cena 100%.

Przy wyborze oferty Zamawiający będzie kierował się najniższą ceną. Dopuszcza się możliwość negocjacji ceny. Zamawiający zastrzega sobie prawo do prowadzenia negocjacji z wykonawcami, którzy złożyli oferty, jak też do niedokonywania wyboru oferty bez podania przyczyny.