Projekt „Cyfrowa gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020

Załącznik Nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ I Dostawa zestawów komputerowych, sprzętu serwerowego, sieciowego wraz z szkoleniami.

1. Stacje robocze – zestaw komputerowy. Ilość: 18 szt.

Nazwa	Wymagane minimalne parametry techniczne
Typ	Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Wydajność obliczeniowa	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 16500 według wyników ze strony https://www.cpubenchmark.net
Pamięć RAM	Pamięć 8 GB z możliwością rozbudowy do 64 GB
Pamięć masowa	Dysk 256GB M.2
Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę min. dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM,
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane głośniki stereo. Wbudowana w obudowę matrycy cyfrowa kamera 5,0 MPix
Obudowa/monitor	Typu All-in-One zintegrowana z monitorem min. 23" FHD 1920 x 1080. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki).
Bezpieczeństwo	Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Wbudowany system diagnostyczny umożliwiający przetestowanie komponentów komputera w zakresie m.in.: procesor, płyta główna, pamięć RAM, dysk twardy. Taki system musi działać niezależnie od obecności dysku twardego, dostępu do sieci i Internetu oraz bez konieczności stosowania urządzeń zewnętrznych.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.
System Operacyjny	Zainstalowany system operacyjny Windows 11 Pro lub równoważny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: - możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; - Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu

	- Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; - Internetowa aktualizacja zapewniona w języku polskim; - Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; - Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; - Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi) - Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer; - Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. - Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; - Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. - Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. - Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. - Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. - Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. - Wbudowany system pomocy w języku polskim; - Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); - Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; - Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; - Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; - System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; - Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; - Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; - Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem; - Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową; - Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; - Graficzne środowisko instalacji i konfiguracji; - Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na

	dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; - Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. - Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; - Możliwość przywracania plików systemowych; - System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) - Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). - klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
Wymagania dodatkowe	Wbudowane porty: 1x HDMI 1.4 4x USB 3.0 Type-A 1x USB 3.0 Type-C 1 x DisplayPort Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub'ów itp. 1x mikrofon/słuchawki Combo 1x RJ-45 port 10/100/1000 Mbps Karta WiFi ac+ bluetooth Płyta główna wyposażona w min. 2 złącza DIMM z obsługą do 64 GB pamięci RAM, min. 1 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)
Niezawodność / jakość wytwarzania	Potwierdzona certyfikatami: Certyfikat CE ISO 14001 ISO 9001
Warunki gwarancyjne, wsparcie techniczne	Wymagane jest, aby Wykonawca dostarczył sprzęt komputerowy fabrycznie nowy, nieużywany, bez wad i uszkodzeń. Minimum 24 miesiące gwarancji producenta. Miejscem świadczenia usług gwarancyjnych będzie siedziba Zamawiającego. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Dostęp do aktualnych sterowników zainstalowanych w komputerze urządzeń, realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej.

2. Serwer - konfiguracja I. Ilość: 1 szt.

Nazwa	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Do pracy w serwerach jednoprocesorowych
Procesor	Jeden procesor 8-rdzeniowy, umożliwiający osiągnięcie wyniku min. 60 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej.
Pamięć RAM	2x16GB pamięci RAM. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wbudowane porty	min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, min. 1 port RS232
Gniazda PCI	Min. 2 sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Kontroler dysków	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NL SAS Zainstalowane 2 dyski SAS 10k o pojemności min. 1.2TB, 12Gb, Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Napęd optyczny	Nie wymagany
System diagnostyczny	Diody LED informujące o kondycji serwera.
Wentylatory	Minimum 4 wentylatory
Zasilacze	Dwa zasilacze o mocy maks. 600W.
System operacyjny/dodatkowe oprogramowani	Wraz z serwerem należy dostarczyć system operacyjny Windows Server 2022 Standard z możliwością uruchomienia 2 VM. Zamawiający posiada infrastrukturę opartą na maszynach wirtualnych z systemami MS Windows.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie serwera.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca

	dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Oprogramowanie do zarządzania	• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB

	• Przesyłanie alertów „as-is" do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Gwarancja	Min. 24 miesiące gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft, Windows Server 2016, Windows Server 2019.
Instalacja	W raz z serwerem należy dostarczyć szafę Rack 19'' , min 15U max 22U. Serwer musi być zainstalowany w dostarczanej szafie rack.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

3. Serwer - konfiguracja II. Ilość: 1 szt.

Nazwa	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 129 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 64GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Gniazda PCI	Minimum dwa sloty PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD. Zainstalowane 4 dyski SAS o pojemności min. 1.2TB, 12Gb, 2,5“ Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie serwera.
System operacyjny	Wraz z serwerem należy dostarczyć system operacyjny Windows Server 2022 Standard z możliwością uruchomienia 2 VM. Zamawiający posiada infrastrukturę opartą na maszynach wirtualnych z systemami MS Windows.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Oprogramowanie do zarządzania	• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB

	• Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019.
Warunki gwarancji	Minimum 24 miesiące gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

4. System kopii zapasowych - Dysk sieciowy NAS – konfiguracja I. Ilość: 1 szt.

Nazwa	Charakterystyka (wymagania minimalne)
Zastosowanie	Dysk sieciowy NAS zapewniający ciągłość działania kluczowych systemów informatycznych Gminnego Zakładu Komunalnego, wykorzystywany jako system do backupu danych.
Procesor	Dwurdzeniowy procesor
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć	Wbudowana pamięć 2 GB z możliwością rozbudowy do 6 GB
Zgodny typ dysków	Dyski 3,5" lub 2,5" SATA HDD/SSD
Dyski z możliwością wymiany podczas pracy	Tak
Port zewnętrzny	2 porty USB 3.0
LAN	2 x Gigabit (RJ-45)
Zaplanowane włączanie / wyłączanie	Tak
Obudowa	Tower
Protokoły sieciowe	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP).
System plików	• Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Obsługiwane typy macierzy RAID	Basic, JBOD, RAID 0, RAID 1
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania).
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Język interfejsu	Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
Virtual Machine Manager	Wdrażanie i uruchamianie różnych maszyn wirtualnych na NAS, takich jak Windows®, Linux® i Virtual DSM.
iSCSI Manager	Maksymalna liczba iSCSI Target: 128 • Maksymalna liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Zainstalowane dyski twarde	Zainstalowane dyski twarde muszą się znajdować na liście zgodności producenta urządzenia. 2 sztuki Dysk twardy (HDD) SATA 3,5” Pojemność: 2 TB każdy. Interfejs: SATA 6 Gb/s. Szybkość interfejsu: 6.0 Gb/s, 3.0 Gb/s, 1.5 Gb/s. Rozmiar buforu: 256 MiB. Rozmiar sektora: 512e. Obciążenie: 550 TB danych przesyłanych rocznie Średni czas do awarii (MTTF): 2 mln godzin. Maksymalna stała prędkość przesyłu danych: 243 MiB/s. Certyfikaty: CE, EAC, BSMI, RCM, KC, ICES, UKCA, TUV, UL, RoHS.

	W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Stan i gwarancja	Min. 24 miesiące gwarancji. Produkt fabrycznie nowy.

5. System kopii zapasowych - Dysk sieciowy NAS - konfiguracja II. Ilość: 1 szt.

Nazwa	**Charakterystyka (wymagania minimalne)**
Zastosowanie	Dysk sieciowy NAS zapewniający ciągłość działania kluczowych systemów informatycznych Urzędu Gminy Łapanów, wykorzystywany jako system do backupu danych.
Procesor	Czterordzeniowy procesor
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć	Moduł 4 GB (z możliwością rozszerzenia do 32 GB)
Zgodne typy dysków	8 dysków 3,5" lub 2,5" SATA HDD/SSD
Wymiana dysków podczas pracy	Tak
Porty zewnętrzne	• 2 porty USB 3.2 1. generacji • 1 gniazdo rozszerzenia (eSATA)
Obudowa	Typu Rack 2U
Porty LAN	4 porty 1GbE RJ-45
Wentylatory obudowy	Minimum 2
Protokoły sieciowe	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
Systemy plików	Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT
Obsługiwane typy macierzy RAID	Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Wirtualizacja	VMware vSphere® 6,5, Microsoft Hyper-V®, Citrix®, OpenStack®
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Języki interfejsu	Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Virtual Machine Manager	Umożliwia wdrażanie i uruchamianie maszyn wirtualnych na serwerach NAS, w tym z systemami Windows®, Linux® i Virtual DSM.
Usługi katalogowe	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.
iSCSI Manager	Maksymalna liczba iSCSI Target: 128 • Maksymalna liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Zainstalowane dyski twarde	Zainstalowane dyski twarde muszą się znajdować na liście zgodności producenta urządzenia. 4 sztuki Dysk twardy (HDD) SATA 3,5” Pojemność: 4 TB każdy.

	Interfejs: SATA 6 Gb/s. Szybkość interfejsu: 6.0 Gb/s, 3.0 Gb/s, 1.5 Gb/s. Rozmiar buforu: 256 MiB. Rozmiar sektora: 512e. Obciążenie: 550 TB danych przesyłanych rocznie Średni czas do awarii (MTTF): 2 mln godzin. Maksymalna stała prędkość przesyłu danych: 243 MiB/s. Certyfikaty: CE, EAC, BSMI, RCM, KC, ICES, UKCA, TUV, UL, RoHS. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Stan i gwarancja	Min. 24 miesiące gwarancji. Produkt fabrycznie nowy.

6. Projektor multimedialny. Ilość: 1 szt.

Nazwa	**Charakterystyka (wymagania minimalne)**
Zastosowanie	Projektor multimedialny do zdalnej obsługi mieszkańców oraz video-spotkań dla Centrum Kultury Gminy Łapanów.
Rozdzielczość	Full HD (1920 x 1080)
Typ matrycy	DLP
Kontrast	22000 :1
Jasność	4000 ANSI lumen
Format obrazu standardowy / skompresowany	16:9 / 4:3
Zoom optyczny	1,1 :1
Minimalna odległość projekcji od ściany	1,2 m
Wejście HDMI	2
Wejście D-Sub 15pin	1
Wejście kompozytowe	1
Port RS-232	1
Złącze USB	1
Pilot zdalnego sterowania	Tak
Żywotność lampy	5 000 godzin
Stan i gwarancja	Min. 24 miesiące gwarancji. Produkt fabrycznie nowy, urządzenie musi pochodzić z oficjalnej, polskiej dystrybucji i być objęte gwarancją producenta na terenie Polski.

7. Szkolenia dla urzędników w zakresie cyberbezpieczeństwa. Ilość: 1 szt.

Nazwa	**Wymagane minimalne parametry techniczne**
Opis	Szkolenie z zakresu bezpiecznego korzystania z e-usług w urzędzie - 22 osób po 2 godziny Zakres: Korzystanie z aplikacji zapewniających bezpieczeństwo w sieci. Rodzaje licencji, na których mogą być udostępnione treści i oprogramowanie wraz z przykładami/ źródłami.

	Założenie konta w ePUAP i profilu zaufanego oraz wykorzystanie profilu zaufanego. Korzystanie z dowolnych usług e-administracji. Deklaracje podatkowe online Wyszukiwanie informacji na stronach instytucji publicznych.
Realizacja	Wykonawca zapewnia materiały szkoleniowe

8. **Szkolenie on-line dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania – UTM. Ilość: 1 szt.**

Nazwa	**Wymagane minimalne parametry techniczne**
Opis	Szkolenie producenta urządzenia UTM min. 12 godzin obejmujące następujące zagadnienia: 1. Rozpoczęcie pracy z urządzeniem 2. Zbieranie logów i monitorowanie 3. Obiekty 4. Konfiguracja sieci 5. Translacja adresów sieciowych (NAT) 6. Translacja połączeń wychodzących (maskarada) 7. Translacja połączeń przychodzących (przekierowanie) 8. Translacja dwukierunkowa (jeden do jeden) 9. Filtrowanie ruchu sieciowego (Firewall) 10. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection) 11. Ochrona aplikacji 12. Użytkownicy i uwierzytelnianie 13. Wirtualne sieci prywatne (VPN) 14. Szczegółowe omówienie działania modułu IPS 15. SSL Proxy 16. Transparentne uwierzytelnianie użytkowników 17. Wysoka dostępność (HA)
Realizacja	Wykonawca zapewnia materiały szkoleniowe.

9. **16-kanałowe zabezpieczenie przeciwprzepięciowe - Ogranicznik przepięć do ochrony sieci LAN. Ilość: 2 szt.**

Nazwa	**Wymagane minimalne parametry techniczne**
Ilość kanałów LAN	16
Obsługiwane standardy Ethernet	10Base-T, 100Base-T, 1000Base-T, 1000Base-Tx
Zgodność z okablowaniem	Kategoria 5, 5e i 6
Złącze wejściowe (strona niechroniona)	Gniazdo RJ-45, ekranowane, 6 kategorii
Złącze wyjściowe (strona chroniona)	Gniazdo RJ-45, ekranowane, 6 kategorii
Napięcie znamionowe DC (linia-ziemia) UN	90V DC

Napięcie maks. pracy trwałej (linia-ziemia) UC	110V DC
Poziom ochrony 1kV/µs (linia-ziemia) UP	600V
Prąd wyładowczy (8/20µs, linia-ziemia) Iimp	2kA
Napięcie znamionowe DC (linia-linia) UN	3,3V DC
Napięcie maksymalne pracy trwałej (linia-linia) UC	3,5V DC
Poziom ochrony 1kV/µs (linia-linia) UP	<8V
Prąd wyładowczy (8/20µs, linia-linia) Iimp	75A (2kA po zadziałaniu MOSFET)
Chronione Linie	1-2, 3-6, 4-5, 7-8
Pojemność (linia-linia) @1MHz	5pF
Pojemność (linia-ziemia) @1MHz	2-3pF
Element odsprzęgający	Bezpiecznik MOSFET
Rezystancja szeregowa	6Ω / linię
Prąd znamionowy IN	300mA / linię
Napięcie znamionowe DC (linia-linia) UN	57V DC
Napięcie maksymalne pracy trwałej (linia-linia) UC	64V DC
Poziom ochrony UP	75V (po zadziałaniu MOSFET)
Prąd wyładowczy (8/20µs, linia-linia) Iimp	73A (2kA po zadziałaniu MOSFET)
Napięcie znamionowe DC (linia-ziemia) UN	90V DC
Napięcie maks. pracy trwałej (linia-ziemia) UC	110V DC
Poziom ochrony 1kV/µs (linia-ziemia) UP	600V
Prąd wyładowczy (8/20µs, linia-ziemia) Iimp	2kA
Chronione pary	(1+2)-(3+6), (4+5)-(7+8)
Standard pracy PoE	Zgodny ze wszystkimi typami w tym Hi PoE
Zastosowanie	Wewnątrz
Sposób montażu	Montaż w szafie Rack 19"
Sposób uziemienia	Przewód uziemiający
Temperatura pracy	-30ºC~60ºC
Stan i gwarancja	Min. 24 miesiące gwarancji. Produkt fabrycznie nowy.

10. Oprogramowanie umożliwiające prace zdalną pracowników Urzędu Gminy Łapanów. Ilość: 4 szt.

Nazwa	**Wymagane minimalne parametry techniczne**
Zastosowanie	Oprogramowanie umożliwiające zarządzania stacjami końcowymi.
Opis	Oprogramowanie do zdalnego pulpitu z szyfrowaniem TLS / RSA, z licencją posiadającą następujące minimalne cechy: a) Umożliwia zdalne zarządzanie komputerem użytkownika przez innego użytkownika (administratora), podobnie do usługi zdalnego pulpitu (m.in. konfigurowanie usług systemowych, uruchamianie programów, kopiowanie

	plików); b) Połączenie pomiędzy komputerami musi być bezpieczne, z wykorzystaniem szyfrowania TLS oraz RSA, ponadto jest kompresowane; c) Licencja na użytkowanie programu obejmuje okres co najmniej jednego roku; d) Oprogramowanie jest dostępne na platformy Windows, iOS, Linux, Android, MacOS w najnowszych wersjach, dla Windows zarówno w wersji instalacyjnej, jak też portable; e) Licencja umożliwia zarządzanie co najmniej systemami rodziny Windows (w tym Windows Server); f) Oprogramowanie wspiera klawiatury międzynarodowe, w tym polską; g) Oprogramowanie musi posiadać funkcjonalność ograniczającą dostępu do urządzenia tylko do zdefiniowanych klientów; h) Oprogramowanie musi posiadać funkcjonalność Wake-On-LAN; i) Konfiguracja oprogramowania ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

11. Zakup specjalistycznego oprogramowania - Aplikacja do tworzenia i ochrony kopii zapasowych danych i ich odzyskiwania. Ilość: 15 szt.

Nazwa	**Wymagane minimalne parametry techniczne**
Zastosowanie	Oprogramowanie umożliwiające wykonywanie kopii bezpieczeństwa danych i ich odzyskiwanie na zakupionych stanowiskach komputerowych dla Urzędu Gminy Łapanów.
Wsparcie dla systemów operacyjnych	Systemy operacyjne Windows: Windows 7 Service Pack 1 lub nowszy Windows 8/8.1 — wszystkie wersje (x86, x64) z wyjątkiem systemu Windows RT Windows 10 Windows 11
Funkcjonalność	1. Zarządzanie lokalne. 2. Tworzenie kopii zapasowych dysków/partycji. 3. Tworzenie kopii zapasowych plików i folderów. 4. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT. 5. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej 6. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła. 7. Pełne, przyrostowe i różnicowe kopie zapasowe. 8. Szyfrowane kopii zapasowych algorytmem AES. 9. Wysyłanie powiadomień pocztą e-mail. 10. Możliwość utworzenia nośnika startowego. 11. Pomoc techniczna dostępna w języku polskim. 12. Funkcja aktywnej ochrony przed oprogramowaniem ransomware,

	chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem. (Środowisko Windows). 13. Konwertowanie kopii zapasowych na pliki maszyn wirtualnych. 14. Kopia zapasowa „sektor po sektorze". 15. Konfiguracja oprogramowania ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

12. Zakup specjalistycznego oprogramowania - Aplikacja do tworzenia kopii zapasowych danych i ich odzyskiwania. Ilość: 1 szt.

Nazwa	**Wymagane minimalne parametry techniczne**
Zastosowanie	Oprogramowanie umożliwiające wykonywanie kopii bezpieczeństwa danych i ich odzyskiwanie na zakupionym serwerze.
Wsparcie dla środowisk serwerowych	Wsparcie dla środowisk wirtualizacji: Hyper-V, VMware vSphere
Funkcjonalność	1. Produkt i dokumentacja dostępna w polskiej wersji językowej. 2. Licencja dostępna w modelu subskrypcyjnym. 3. Możliwość wdrożenia konsoli zarówno w trybie chmurowym jak i on-premis. 4. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych. 5. Tworzenie kopii zapasowych dysków/partycji. 6. Tworzenie kopii zapasowych plików i folderów. 7. Replikacja kopii zapasowych do wielu lokalizacji docelowych. 8. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT. 9. Kopie zapasowe i granularne przywracanie elementów aplikacji Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint i Microsoft Active Directory. 10. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej. 11. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD 12. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej. 13. Zdalna instalacja i aktualizacja agentów na komputerach klienckich 14. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP. 15. Możliwość generowania planu przywracania kopii zapasowych. 16. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach. 17. Szablony schematów rotacji kopii zapasowych. 18. Polecenia poprzedzające/następujące. 19. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja). 20. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych). 21. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu

	wiersza polecenia. 22. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła. 23. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft. 24. Pełne, przyrostowe i różnicowe kopie zapasowe. 25. Wysyłanie powiadomień pocztą e-mail . 26. Szyfrowane kopii zapasowych algorytmem AES. 27. Tworzenie dynamicznych grup urządzeń na podstawie nazwy urządzenia, ilości pamięci operacyjnej, zakresu adresów IP, typu systemu operacyjnego. 28. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie. 29. Funkcjonalność ciągłej ochrony danych. 30. Wbudowany moduł ochrony antywirusowej: Środowisko Windows. 31. Możliwość integracji z Windows Defender Antyvirus. 32. Filtrowanie adresów URL. 33. Analiza podatności urządzenia (poszukiwanie luk w oprogramowaniu objętym ochroną), środowisko Windows. 34. Funkcjonalność zdalnego pulpitu, możliwa do wywołania z poziomu serwera zarządzania oprogramowaniem backupowym środowisko Windows. 35. Moduł automatycznego łatania wykrytych luk w oprogramowaniu środowisko Windows. 36. Automatyczne tworzenie kopii zapasowej urządzenia, na którym ma zostać wdrożona poprawką. 37. Możliwość wywołania funkcji zdalnego wymazywania danych w oparciu o mechanizm wbudowany w Windowsa 10. 38. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem. (Środowisko Windows). 39. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle. 40. Uruchamianie usług z minimalnymi prawami użytkownika 41. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy. 42. Pomoc techniczna dostępna w języku polskim 43. Administrowanie kontami użytkowników i jednostkami organizacyjnymi. 44. Wykonywanie kopii zapasowych uruchamiane po wystąpieniu określonych zdarzeń i warunków. 45. Migawki wielowoluminowe. 46. Kopia zapasowa „sektor po sektorze". 47. Obsługa dysków dynamicznych. 48. Automatyczne ponawianie prób w przypadku niekrytycznych błędów (prób utworzenia kopii zapasowej). 49. Możliwość utworzenia nośnika startowego. 50. Konfiguracja oprogramowania ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

13. Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania. Ilość: 1 szt.

Nazwa	Wymagane minimalne parametry techniczne
Opis usługi	1. Ustalenie z działem IT Zamawiającego prawidłowej instalacji dostarczonych urządzeń. 2. Montaż dostarczonych urządzeń oraz ich instalacja zgodnie z wytycznymi Zamawiającego. 3. Podstawowa konfiguracja systemów operacyjnych. 4. Na dostarczonym serwerze dla Urzędu Gminy Łapanów Wykonawca skonfiguruje środowisko wirtualne oraz systemy operacyjne zgodnie z wytycznymi Zamawiającego dostarczonymi na etapie realizacji. 5. Zamawiający wymaga przeniesienia środowisk, systemów dziedzinowych firmy KORELACJa oraz firmy Sygnity, plików i danych z istniejących serwerów na dostarczone i uruchomienie jako maszyny wirtualne (dotyczy Urzędu Gminy Łapanów). Środowiskiem wymaganym do przeniesienia w którym pracują systemy dziedzinowe są: SQL EXPRESS, silnik bazy danych Firebird-2.5.7.27050_0 oraz serwer aplikacyjny Jboss. 6. Zamawiający wymaga skonfigurowania na dostarczanym serwerze dla Urzędu Gminy Łapanów tworzenia kopii bezpieczeństwa przy pomocy dostarczonego oprogramowania jako środowisk fizycznych oraz wirtualnych. 7. Zamawiający wymaga uruchomienia na dostarczonym serwerze dla Urzędu Gminy Łapanów oprogramowania PowerChute Network Shutdown (w posiadaniu Zamawiającego) współpracującego z kartą zarządzającą APC UPS Network Management Card (w posiadaniu Zamawiającego) oraz skonfigurowanie sekwencji wyłączania serwerów wirtualnych oraz fizycznych w razie dłuższej utraty zasilania. 8. Zamawiający wymaga instalacji, uruchomienia i skonfigurowania stacji roboczych, w szczególności dołączenia do UTM. 9. Zamawiający wymaga przeniesienia danych i aplikacji z obecnie używanych lokalnych profili użytkownika na nowe stacje robocze. 10. Przenoszenie systemów nie może zakłócać bieżącej pracy użytkowników systemów dziedzinowych. 11. Po przeniesieniu systemów, Zamawiający wymaga przetestowania poprawności działania całego środowiska oraz systemów. 12. Przygotowanie dokumentacji powykonawczej. 13. Dwutygodniowe wsparcie osoby technicznej pomagające w rozwiązaniu ewentualnych problemów z dostarczonymi urządzeniami liczone od momentu ich instalacji. 14. Dla wszystkich wdrażanych systemów, Zamawiający wymaga opracowania pełnej dokumentacji powykonawczej oraz procedur eksploatacyjnych systemu.
Usługa wirtualizacji – serwer dla Urzędu Gminy Łapanów.	1. Przygotowanie serwera - aktualizacja firmware i bios. 2. Konfiguracja RAID i przygotowanie storage. 3. Adresacja i konfiguracja dostępu do portów zarządzania serwerami. 4. Instalacja i konfiguracja silnika wirtualizacji wraz z przygotowaniem wirtualnego przełącznika sieciowego. 5. Adresacja sieciowa hypervisora. 6. Instalacja, konfiguracja i wdrożenie min. 2 maszyn wirtualnych wraz z ich

	adresacją. 7. Optymalizacja zasobów sprzętowych. 8. Test działania sieci na maszynach wirutalnych i storage. 9. Zamawiający wymaga na używanym obecnie serwerze uruchomienia środowiska rezerwowego które w razie awarii środowiska produkcyjnego przejmie jego rolę i nie zakłóci pracy użytkowników systemów dziedzinowych. 10. Przeprowadzenie testu działania maszyn wirtualnych oraz storage na środowisku rezerwowym. 11. Przygotowanie dokumentacji wdrożeniowej.

14. Urządzenie UPS Ilość: 1 szt.

Nazwa	**Wymagane minimalne parametry techniczne**
Moc pozorna	1000VA
Moc	Min. 900W
Napięcie wejściowe	110-290V
Napięcie wyjściowe	200/208/220/230/240V AC
Częstotliwość wejściowa	45-65Hz (wykrywana automatycznie)
Częstotliwość wyjściowa	50Hz lub 60Hz (automatyczne wykrywanie)
Rodzaj akumulatora	2 x 12V/9Ah
Czas reakcji	natychmiastowa reakcja w przypadku zaniku napięcia
Kształt napięcia wyjściowego	Czysta Sinusoida
Zastosowane zabezpieczenia elektroniczne	przeciwprzepięciowe, przed przegrzaniem, przed nadmiernym rozładowaniem, przed przeładowaniem
Gniazda	6x IEC320 C13-10A
Montaż	Rack 19''
Certyfikaty	CE, RoHS
Stan i gwarancja	Min. 24 miesiące gwarancji. Produkt fabrycznie nowy.

CZĘŚĆ II Dostawa zabezpieczeń logicznych (firewall, systemy IDS, IPS)

1. Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS) konfiguracja I. Ilość: 1 szt.

Nazwa	Wymagane minimalne parametry techniczne
Urządzenie	OBSŁUGA SIECI 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. ZAPORA KORPORACYJNA (Firewall) 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma umożliwiać 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 firewall 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, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). INTRUSION PREVENTION SYSTEM (IPS) 12. 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. 13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

	15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 16. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 17. Administrator 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. 18. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 19. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). KSZTAŁTOWANIE PASMA (Traffic Shapping) 20. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 21. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 22. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 23. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. OCHRONA ANTYWIRUSOWA 24. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 25. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 26. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 27. 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 wykrycia infekcji. OCHRONA ANTYSPAM 28. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 29. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 30. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 31. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

	WIRTUALNE SIECI PRYWATNE (VPN) 32. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 33. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 34. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 35. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 36. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 37. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 38. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based. FILTR DOSTĘPU DO STRON WWW 39. Urządzenie ma posiadać wbudowany filtr URL. 40. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 41. Administrator ma mieć możliwość dodawania własnych kategorii URL. 42. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: 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. 43. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 44. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 45. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 46. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 47. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. UWIERZYTELNIANIE 48. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 49. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a. SSL,

	b. Radius, c. Kerberos. 51. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 52. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP) 54. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 56. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 58. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 59. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 60. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. ROUTING (TRASOWANIE) 61. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 62. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 63. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 64. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. ADMINISTRACJA URZĄDZENIEM 65. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 66. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 67. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 68. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 69. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 70. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 71. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny

	poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 72. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 73. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 74. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 75. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 76. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. RAPORTOWANIE 77. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 78. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 79. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 80. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 81. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 82. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 83. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 84. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH). POZOSTAŁE USŁUGI I FUNKCJE 85. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 86. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 87. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 88. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny. 89. Urządzenie ma posiadać usługę DNS Proxy. 90. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

	GWARANCJA I SERWIS 91. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu. 92. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. PARAMETRY SPRZĘTOWE 93. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 94. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów. 95. Liczba portów Ethernet 10/100/1000Mbps – min.8. 96. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 97. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps. 98. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.4Gbps. 99. Przepustowość filtrowania Antywirusowego – minimum 495Mbps. 100. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 600Mbps. 101. Maksymalna liczba tuneli VPN IPSec – minimum 100. 102. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20. 103. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50. 104. Obsługa interfejsów 802.11q (VLAN) – minimum 128 105. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. 106. Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive. 107. Urządzenie nie ma limitu na liczbę użytkowników. 108. Liczba reguł filtrowania – minimum 8 192. 109. Liczba tras statycznego routingu – minimum 512. 110. Liczba tras dynamicznego routingu – minimum 10 000. WDROŻENIE ZDALNE • szczegółowe omówienie polityki bezpieczeństwa stosowanej w przedsiębiorstwie oraz topologii sieci w kontekście możliwości urządzenia UTM • instalacja i konfiguracja oprogramowania zarządzającego/monitorujacego – w zależności od wersji firmware i modelu urządzenia UTM • aktualizacja oprogramowania wewnętrznego (firmware) • konfiguracja ustawień systemowych – czas, nazwa, automatyczne aktualizacje, itp. • konfiguracja interfesów fizycznych i VLAN • tworzenie obiektów zgodnych z topologią sieci klienta jak i wykorzystywanych usług • konfiguracja routingu w tym również w sytuacji gdy klient posiada łącza od kilku dostawców internetowych koniguracja load balancingu • konfiguracja serwera DHCP (w tym rezerwacji hostów) – w przypadku gdy klient będzie korzystał z serwera DHCP w UTM'ie • konfiguracja DNS, DNS PROXY, NTP • konfiguracja reguł zapory sieciowej • konfiguracja translacji NAT (PAT, FORWARDING, BI-MAP (DMZ)) • konfiguracja PROXY SSL, PROXY HTTP, PROXY SMTP, PROXY POP3, PROXY FTP • konfiguracja filtra URL

	• konfiguracja serwera SSL VPN • testowanie wdrożonej konfiguracji • zabezpieczenie konfiguracji: kopia zapasowa konfiguracji, wyrównanie partycji
Realizacja	Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres do lipca 2023 roku.

2. Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS) – konfiguracja II. Ilość: 3 szt.

Nazwa	**Wymagane minimalne parametry techniczne**
Urządzenie	OBSŁUGA SIECI 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. ZAPORA KORPORACYJNA (Firewall) 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma umożliwiać 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 firewall 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, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

	INTRUSION PREVENTION SYSTEM (IPS) 12. 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. 13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 16. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 17. Administrator 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. 18. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 19. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 20. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. 21. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu. 22. Urządzenie musi umożliwiać analizę typu sandbox przeprowadzaną w chmurze producenta. Nie dopuszcza się aby analiza była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza była przeprowadzana przez firmy trzecie. KSZTAŁTOWANIE PASMA (Traffic Shapping) 23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. OCHRONA ANTYWIRUSOWA 27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż

	producent rozwiązania). 28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 29. Urządzenie ma być dostarczone wraz z komercyjnym skanerem Antywirusowym, nie dopuszcza się stosowania skanera rozwijanego w ramach projektów OpenSource. 30. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 31. 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 wykrycia infekcji. OCHRONA ANTYSPAM 32. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 33. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 34. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 35. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. WIRTUALNE SIECI PRYWATNE (VPN) 36. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 37. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 38. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 39. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 40. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 41. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 42. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based. FILTR DOSTĘPU DO STRON WWW 43. Urządzenie ma posiadać wbudowany filtr URL. 44. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 65 kategorii tematycznych stron internetowy. 45. W ramach filtra URL sklasyfikowanych jest co najmniej 100 milionów stron internetowych. 46. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych

	przechowywanej lokalnie w urządzeniu. 47. Administrator ma mieć możliwość dodawania własnych kategorii URL. 48. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: 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. 49. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 50. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 51. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 52. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 53. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. UWIERZYTELNIANIE 54. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 55. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 56. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 57. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 58. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 59. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP) 60. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 61. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 62. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 63. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

	64. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 65. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 66. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. ROUTING (TRASOWANIE) 67. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 68. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 69. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 70. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. ADMINISTRACJA URZĄDZENIEM 71. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 72. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 73. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 74. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 75. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 76. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 77. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 78. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 79. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 80. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 81. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 82. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. RAPORTOWANIE 83. Urządzenie ma posiadać wbudowany w interfejs administracyjny system

	raportowania i przeglądania logów zebranych na urządzeniu. 84. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 85. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 86. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 87. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 88. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 89. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 90. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH). POZOSTAŁE USŁUGI I FUNKCJE 91. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 92. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 93. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 94. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny. 95. Urządzenie ma posiadać usługę DNS Proxy. 96. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. GWARANCJA I SERWIS 97. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu. 98. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. PARAMETRY SPRZĘTOWE 99. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 100. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów. 101. Liczba portów Ethernet 10/100/1000Mbps – min.8. 102. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 103. Przepustowość Firewall (1518 bajtów UDP) – minimum 2Gbps. 104. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1.6Gbps. 105. Przepustowość filtrowania Antywirusowego – minimum 400Mbps.

	106. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 350Mbps. 107. Maksymalna liczba tuneli VPN IPSec – minimum 50. 108. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20. 109. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 20. 110. Obsługa interfejsów 802.11q (VLAN) – minimum 128 111. Liczba równoczesnych sesji – minimum 200 000 i nie mniej niż 15 000 nowych sesji/sekundę. 112. Urządzenie nie ma limitu na liczbę użytkowników. 113. Liczba reguł filtrowania – minimum 4 096. 114. Liczba tras statycznego routingu – minimum 512. 115. Liczba tras dynamicznego routingu – minimum 10 000. WDROŻENIE ZDALNE • szczegółowe omówienie polityki bezpieczeństwa stosowanej w przedsiębiorstwie oraz topologii sieci w kontekście możliwości urządzenia UTM • instalacja i konfiguracja oprogramowania zarządzającego/monitorujacego – w zależności od wersji firmware i modelu urządzenia UTM • aktualizacja oprogramowania wewnętrznego (firmware) • konfiguracja ustawień systemowych – czas, nazwa, automatyczne aktualizacje, itp. • konfiguracja interfesów fizycznych i VLAN • tworzenie obiektów zgodnych z topologią sieci klienta jak i wykorzystywanych usług • konfiguracja routingu w tym również w sytuacji gdy klient posiada łącza od kilku dostawców internetowych koniguracja load balancingu • konfiguracja serwera DHCP (w tym rezerwacji hostów) – w przypadku gdy klient będzie korzystał z serwera DHCP w UTM'ie • konfiguracja DNS, DNS PROXY, NTP • konfiguracja reguł zapory sieciowej • konfiguracja translacji NAT (PAT, FORWARDING, BI-MAP (DMZ)) • konfiguracja PROXY SSL, PROXY HTTP, PROXY SMTP, PROXY POP3, PROXY FTP • konfiguracja filtra URL • konfiguracja serwera SSL VPN • testowanie wdrożonej konfiguracji • zabezpieczenie konfiguracji: kopia zapasowa konfiguracji, wyrównanie partycji
Realizacja	Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres do lipca 2023 roku.