**Załącznik nr 1 do SWZ**

**Opis Przedmiotu Zamówienia**

**(po uzupełnieniu danych: Producent / model urządzenia / model procesorów należy podpisać zgodnie z wymogami do oferty i złożyć wraz z ofertą)**

1. **Serwer z oprogramowaniem systemowym – 2szt. (typ I, typ II)**

|  |  |  |
| --- | --- | --- |
| **Serwer – 2 sztuki (typ I, typ II)**  **UWGA! Serwery typ I oraz typ II różnią się od siebie ilością licencji dostępowych do system operacyjnego Producent / model urządzenia / model procesorów (wypełnia Wykonawca) :**  **…………………………………………………………………………………………………………………………………………………………………………………………** | | |
| **Wymagania minimalne:** | | |
| 1 | Obudowa | Obudowa typu „RACK” o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków twardych 2.5”.  Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (dostępnej dla systemów Android/ Apple iOS). |
| 2 | Płyta główna | Płyta główna z możliwością instalacji dwóch fizycznych procesorów,  Płyta główna posiadająca minimum 32 slotów na pamięć RAM, umożliwiająca instalację maksymalnie minimum 8TB pamięci RAM. |
| 3 | Procesor | Zainstalowane dwa procesory min. 8-rdzeniowe, klasy x86, min. 3.5GHz, dedykowane do pracy  z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 206 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| 4 | Pamięć RAM | Zainstalowane minimum 128GB |
| 5 | Kontroler RAID | Zainstalowany sprzętowy kontroler dyskowy, posiadający:  - minimum 8GB nieulotnej pamięci cache,  - możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.  - wsparcie dla dysków samoszyfrujących |
| 6 | Dyski twarde | Zainstalowane minimum 2 dyski SSD SATA typu „hot plug” o pojemności min. 960GB.  Zainstalowane minimum 6 dysków SAS typu „hot plug” o pojemności min. 1.2TB. |
| 7 | Interfejsy sieciowe | Wbudowane min. 4 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (wymagana ilość portów nie może być osiągnięta przez karty rozszerzeń PCIe). |
| 8 | Wbudowane porty | Minimum 3 porty USB z czego min. 2 w technologii 3.1.  Minimum 1 port VGA |
| 9 | Video | Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1920x1200 pikseli |
| 10 | Zasilanie | Redundantne zasilacze „hot-plug” o mocy minimum 800W klasy Titanium |
| 11 | System operacyjny/dodatkowe oprogramowanie | Zamawiający wymaga, aby opisywane serwery z oprogramowaniem systemowym **(2szt.)** zostały dostarczone z następującymi licencjami:  **Serwer z oprogramowaniem systemowym – 1szt. (typ I)**  Licencja na system operacyjny Windows Server 2025 Standard dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 4 maszyn wirtualnych.  Licencja dostępowa do Windows Server 2025 dla 30 użytkowników  Nośniki instalacyjne do Windows Server 2025 Standard  **Serwer z oprogramowaniem systemowym – 1szt. (typ II)**  Licencja na system operacyjny Windows Server 2025 Standard dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 4 maszyn wirtualnych.  Licencja dostępowa do Windows Server 2025 dla 50 użytkowników  Nośniki instalacyjne do Windows Server 2025 Standard. |
| 12 | Bezpieczeństwo | Zatrzask górnej pokrywy oraz blokada na ramce panelu (zamykana na klucz) służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  TPM 2.0.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS musi mieć funkcjonalność przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.  Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| 13 | Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * + zdalny dostęp do graficznego interfejsu Web karty zarządzającej   + 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 SNMP; IPMI2.0, VLAN tagging, SSH   + 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 sześciu administratorów jednocześnie   + Wsparcie dla automatycznej rejestracji DNS   + wsparcie dla LLDP   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej   + możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.   + Monitorowanie zużycia dysków SSD   + Automatyczne zgłaszanie alertów do centrum serwisowego producenta   + Automatyczne update firmware dla wszystkich komponentów serwera   + Możliwość przywrócenia poprzednich wersji firmware   + Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON   + Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych   + Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.   + Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera |
| 14 | Oprogramowanie do zarządzania | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * + 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. |
| 15 | Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą  ISO-9001oraz ISO-14001.  Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2025, Microsoft Windows Server 2022. |
| 16 | Warunki gwarancji | 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta, lub internet.  **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia**, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń **– dokumenty potwierdzające należy załączyć do oferty.**  **Wymagane dołączenie do oferty oświadczenia** Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |

Zamawiający wymaga aby w przypadku serwera z oprogramowaniem systemowym (**typ I**) Wykonawca w ramach dostawy wykonał prace przygotowawcze i wdrożeniowe w następującym zakresie:

* aktualizacja firmware serwera
* stworzenie grup raid, inicjalizacja dysków
* podział dysków na partycje
* instalacja systemu Windows Server 2025 oraz roli Hyper-V
* stworzenie dwóch maszyn wirtualnych
* wypromowanie kontrolera domeny wraz z serwerem DNS
* stworzenie i omówienie przykładowych polityk GPO
* stworzenie trzech przykładowych kont użytkowników i komputerów
* stworzenie i omówienie przykładowych grup i udziałów udostępnionych
* przykładowe dodanie do domeny trzech komputerów
* zapewnienie Zamawiającemu wsparcia przez okres 3 miesięcy w zakresie powyższych czynności

1. **Serwer z oprogramowaniem systemowym – 5szt. (typ III, IV, V, VI, VII)**

|  |  |  |
| --- | --- | --- |
| **Serwer – 5 sztuk**  **UWGA! Serwery typ III – typ VII różnią się od siebie rodzajem licencji na system operacyjny, oraz rodzajem i ilością licencji dostępowych do system operacyjnego Producent / model urządzenia / model procesora (wypełnia Wykonawca) :**  **…………………………………………………………………………………………………………………………………………………………………………………………** | | |
| **Wymagania minimalne:** | | |
| 1 | Obudowa | Obudowa typu tower z możliwością instalacji do 8 dysków twardych 3.5”. |
| 2 | Płyta główna | Płyta główna posiadająca minimum 4 sloty na pamięć RAM, z możliwością zainstalowania do minimum 128GB pamięci RAM. |
| 3 | Procesor | Zainstalowany jeden procesor 8-rdzeniowy klasy x86, o częstotliwości taktowania min. 2.7GHz, 24M Cache, TDP max 65W |
| 4 | Pamięć RAM | Zainstalowane minimum 32GB |
| 5 | Kontroler RAID | Zainstalowany sprzętowy kontroler dyskowy, posiadający:  - minimum 8GB nieulotnej pamięci cache,  - możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.  - wsparcie dla dysków samoszyfrujących |
| 6 | Dyski twarde | Zainstalowane minimum 2 dyski SATA typu „hot plug” o pojemności min. 2TB.  Zainstalowane minimum 2 dyski SSD SATA typu „hot plug” o pojemności min. 480GB.  Możliwość zainstalowania 2 dysków M.2 NVMe o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| 7 | Interfejsy sieciowe | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. |
| 8 | Wbudowane porty | Minimum 6 portów USB z czego min. 3 w technologii 3.0.  Minimum 1 port VGA |
| 9 | Video | Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli |
| 10 | Zasilanie | Redundantne zasilacze „hot-plug” o mocy minimum 700W klasy Titanium |
| 11 | System operacyjny/dodatkowe oprogramowanie | Zamawiający wymaga, aby opisywane serwery z oprogramowaniem systemowym **(5szt.)** zostały dostarczone z następującymi licencjami:  **Serwer z oprogramowaniem systemowym – 1szt. (typ III)**  Licencja na system operacyjny Windows Server 2025 Standard dobrana tak, aby przy oferowanym procesorze umożliwić uruchomienie 2 maszyn wirtualnych.  Licencja dostępowa do Windows Server 2025 dla 20 użytkowników.  Nośniki instalacyjne do Windows Server 2025 Standard.  **Serwer z oprogramowaniem systemowym – 1szt. (typ IV)**  Licencja na system operacyjny Windows Server 2025 Standard **w wersji edukacyjnej** dobrana tak, aby przy oferowanym procesorze umożliwić uruchomienie 2 maszyn wirtualnych.  Licencja dostępowa **w wersji edukacyjnej** do Windows Server 2025 dla 100 użytkowników.  **Serwer z oprogramowaniem systemowym – 1szt. (typ V)**  Licencja na system operacyjny Windows Server 2025 Standard **w wersji edukacyjnej** dobrana tak, aby przy oferowanym procesorze umożliwić uruchomienie 2 maszyn wirtualnych.  Licencja dostępowa **w wersji edukacyjnej** do Windows Server 2025 dla 125 użytkowników.  **Serwer z oprogramowaniem systemowym – 1szt. (typ VI)**  Licencja na system operacyjny Windows Server 2025 Standard **w wersji edukacyjnej** dobrana tak, aby przy oferowanym procesorze umożliwić uruchomienie 2 maszyn wirtualnych.  Licencja dostępowa **w wersji edukacyjnej** do Windows Server 2025 dla 140 użytkowników.  **Serwer z oprogramowaniem systemowym – 1szt. (typ VII)**  Licencja na system operacyjny Windows Server 2025 Standard **w wersji edukacyjnej** dobrana tak, aby przy oferowanym procesorze umożliwić uruchomienie 2 maszyn wirtualnych.  Licencja dostępowa **w wersji edukacyjnej** do Windows Server 2025 dla 260 użytkowników.  Zamawiający przekaże wyłonionemu Wykonawcy wszelkie dane docelowych jednostek edukacyjnych niezbędne do wygenerowania wymaganych licencji. |
| 12 | Bezpieczeństwo | Zintegrowany z płytą główną moduł TPM 2.0.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS musi mieć funkcjonalność przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.  Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| 13 | Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * + zdalny dostęp do graficznego interfejsu Web karty zarządzającej   + 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 SNMP; IPMI2.0, VLAN tagging, SSH   + 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 sześciu administratorów jednocześnie   + Wsparcie dla automatycznej rejestracji DNS   + wsparcie dla LLDP   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej   + możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.   + Monitorowanie zużycia dysków SSD   + Automatyczne zgłaszanie alertów do centrum serwisowego producenta   + Automatyczne update firmware dla wszystkich komponentów serwera   + Możliwość przywrócenia poprzednich wersji firmware   + Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON   + Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych   + Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.   + Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera |
| 14 | Oprogramowanie do zarządzania | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * + 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. |
| 15 | Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą  ISO-9001oraz ISO-14001.  Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2025, Microsoft Windows Server 2022. |
| 16 | Warunki gwarancji | 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta, lub internet  **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia**, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń **– dokumenty potwierdzające należy załączyć do oferty.**  **Wymagane dołączenie do oferty oświadczenia** Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |

Zamawiający wymaga aby w przypadku serwera z oprogramowaniem systemowym (**typ III**) Wykonawca w ramach dostawy wykonał prace przygotowawcze i wdrożeniowe w następującym zakresie:

* aktualizacja firmware serwera
* stworzenie grup raid, inicjalizacja dysków
* podział dysków na partycje
* instalacja systemu Windows Server 2025 oraz roli Hyper-V
* stworzenie dwóch maszyn wirtualnych
* wypromowanie kontrolera domeny wraz z serwerem DNS
* stworzenie i omówienie przykładowych polityk GPO
* stworzenie trzech przykładowych kont użytkowników i komputerów
* stworzenie i omówienie przykładowych grup i udziałów udostępnionych
* przykładowe dodanie do domeny trzech komputerów
* zapewnienie Zamawiającemu wsparcia przez okres 3 miesięcy w zakresie powyższych czynności

Zamawiający wymaga aby w przypadku serwera z oprogramowaniem systemowym (**typ IV**) Wykonawca w ramach dostawy wykonał prace przygotowawcze i wdrożeniowe **w docelowym miejscu instalacji serwera** w następującym zakresie:

* aktualizacja firmware serwera
* stworzenie grup raid, inicjalizacja dysków
* podział dysków na partycje
* instalacja systemu Windows Server 2025 oraz roli Hyper-V
* stworzenie dwóch maszyn wirtualnych
* wypromowanie kontrolera domeny wraz z serwerem DNS
* stworzenie i omówienie przykładowych polityk GPO
* stworzenie trzech przykładowych kont użytkowników i komputerów
* stworzenie i omówienie przykładowych grup i udziałów udostępnionych
* przykładowe dodanie do domeny trzech komputerów
* zapewnienie Zamawiającemu wsparcia przez okres 3 miesięcy w zakresie powyższych czynności

1. **Serwer NAS z oprogramowaniem do kopii zapasowych – 10szt.**

|  |  |  |
| --- | --- | --- |
| **Serwer NAS z oprogramowaniem do kopii zapasowej – 10 sztuk**  **Producent / model urządzenia / model procesora (wypełnia Wykonawca) :**  **…………………………………………………………………………………………………………………………………………………………………………………………** | | |
| **Wymagania minimalne:** | | |
| 1 | Procesor | Procesor wielordzeniowy 64-bitowy o taktowaniu nie niższym niż 2.2GHz uzyskujący wynik co najmniej 4550 punktów w teście PassMark - CPU Mark według wyników dostępnych na stronie <http://www.cpubenchmark.net> – na okres nie wcześniejszy niż 01.09.2025r. |
| 2 | Obudowa | Wolnostojąca, typu “desktop” |
| 3 | Pamięć RAM | Minimum 8GB DDR4 ECC w konfiguracji 2 x 4 GB. Pamięć RAM zgodna z listą kompatybilności producenta oferowanego serwera. Możliwość rozszerzenia RAM do 32GB. |
| 4 | Liczba zatok na dyski twarde | Minimum 4 |
| 5 | Obsługiwane dyski twarde | 3.5" SATA HDD / 2.5" SATA SSD  Zamawiający wymaga dostarczenia minimum 4 dysków 3.5” SATA HDD o pojemności co najmniej 8 TB każdy o parametrach nie gorszych niż:  Prędkość obrotowa: 7200 obr./min.  MTBF: 1 000 000 godzin  Obciążenie roczne: 180 TB  Gwarancja producenta dysku: 3 lata  Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera.  Dyski zgodne z listą kompatybilności producenta oferowanego serwera. |
| 6 | Wbudowane kieszenie dysków M.2 NVMe | Minimum 2 |
| 7 | Możliwość podłączenia modułu rozszerzającego | Tak |
| 8 | Minimalna ilość dysków z opcjonalnymi modułami rozszerzającymi | 9 |
| 9 | Porty LAN | Wbudowane min. 2 x 2.5 GbE RJ-45 |
| 10 | Porty USB 3.2 | Minimum 2 |
| 11 | Gniazdo rozszerzenia | Minimum 1 – typ portu USB C |
| 12 | Zasilanie | Zasilacz o mocy minimalnej 100W |
| 13 | Mechanizm szyfrowania sprzętowego | Tak, min AES-NI |
| 14 | Wewnętrzny system plików | BTRFS, EXT4 |
| 15 | Obsługiwane tryby RAID | JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny |
| 16 | Usługa katalogowa | Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station |
| 17 | Bezpieczeństwo | Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail. |
| 18 | Oprogramowanie do kopii zapasowej | Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów.  Minimalne wymagane funkcje oprogramowania do backupu:  - kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal,  - kopia zapasowa środowisk MacOS  - kopia zapasowa maszyn wirtualnych (VMware, Hyper-V)  - kopia zapasowa serwerów fizycznych (Windows, Linux)  - obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania,  - obsługa wielu wersji i retencji,  - możliwość wyzwalania kopii zapasowej według harmonogramu,  - obsługa klastra przełączania awaryjnego Microsoft Hyper-V,  - automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej, - centralne zarządzanie,  - konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań,  - portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora),  - delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora,  - kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace |
| 19 | Oprogramowanie | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych * Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. * Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. Możliwość utworzenia klastra bez konieczności przywracania systemu do ustawień fabrycznych w serwerze aktywnym. * Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych * Obsługa minimum 256 migawek na folder współdzielony i minimum 2048 migawek na cały system * Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 8jednoczesnych połączeń |
| 20 | Gwarancja producenta | Minimum 3 lata |

1. **Zarządzalny przełącznik sieciowy typ I – 1szt.**

|  |
| --- |
| **Przełącznik sieciowy zarządzalny typ I – 1 sztuka Producent / model urządzenia  (wypełnia Wykonawca):**  **…………………………………………………………………………………………………………………………………………………………………………………………** |
| **Wymagania minimalne:** |

Wymaga się aby urządzenie pochodziło z oficjalnego polskiego kanału dystrybucyjnego.

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany z wysyłką w następnym dniu roboczym po potwierdzeniu przez producenta awarii.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Ilość portów: 48 PoE+ 1GBASE-T, 4 x SFP+
* Tablica MAC min. 16K
* CPU klasy min. Quad-Core Cortex-A57 ARMv8 1.8Ghz
* Min. 2GB RAM
* Bufor 32Mb
* MTBF min. 620000 godzin
* Wydajność min. 130 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB Type-C
* Port zarządzania Out-of-band oraz konsolowy RJ45
* Web GUI
* Interfejs web umożliwiający automatyczne przypisanie konfiguracji do portów właściwej dla protokołów czy też producenta: NVX, AMX, NDI, ZeeVee, Aurora, Kramer, LibAV, Dante Video, SDVoE, AES67, Q-SYS, Audio Dante, AVB, Crestron DigitalMedia AV, NUCLEUS Converged AV, Shure, Sonos, Visionary AV
* Wymaga się aby powyższe szablony konfiguracji były stworzone przez producenta przełącznika a interfejs web w sposób jednoznaczny wskazywał że dany producent AV czy protokół jest obsługiwany przez dany szablon.
* Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH.
* Wymaga się aby w sposób manualny istniała możliwość wyboru trybu wykrywania urządzeń PoE. Jednym z takich trybów powinien być: 4ptdot3af
* HTTPs
* SSH
* Obsługa PTPv2
* STP, MTP, RSTP PV(R)STP
* IPv4/IPv6:
* PIM-SM
* PIM-DM
* SSM
* Obsługa IEEE 802.1AS-2011 gPTP, IEEE 802.1Qav-2009 FQTSS, IEEE 802.1Qat-2010 MSRP, IEEE 802.1ak MMRP, IEEE 802.1ak MVRP
* Kształtowanie ruchu na wejściu oraz wyjściu co 1 Kbps
* Radius
* TACACS+
* IGMPv1,v2 Querier
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* CCC: GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class A)
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014

1. **Zarządzalny przełącznik sieciowy typ II – 2szt.**

|  |
| --- |
| **Przełącznik sieciowy zarządzalny typ II – 2 sztuki Producent / model urządzenia  (wypełnia Wykonawca):**  **…………………………………………………………………………………………………………………………………………………………………………………………** |
| **Wymagania minimalne:** |

Wymaga się aby urządzenie pochodziło z oficjalnego polskiego kanału dystrybucyjnego.

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany z wysyłką w następnym dniu roboczym po potwierdzeniu przez producenta awarii.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Ilość portów: 24 PoE+ 1GBASE-T, 4 x SFP+
* Budzet PoE min.: 640W
* Tablica MAC min. 16K
* CPU klasy min. Quad-Core Cortex-A57 ARMv8 1.8Ghz
* Min. 2GB RAM
* Bufor 16Mb
* MTBF min. 780000 godzin
* Wydajność min. 95 Mp/s
* Przepustowość min. 128 Gb/s
* Port USB Type-C
* Port zarządzania Out-of-band oraz konsolowy RJ45
* Web GUI
* Interfejs web umożliwiający automatyczne przypisanie konfiguracji do portów właściwej dla protokołów czy też producenta: NVX, AMX, NDI, ZeeVee, Aurora, Kramer, LibAV, Dante Video, SDVoE, AES67, Q-SYS, Audio Dante, AVB, Crestron DigitalMedia AV, NUCLEUS Converged AV, Shure, Sonos, Visionary AV
* Wymaga się aby powyższe szablony konfiguracji były stworzone przez producenta przełącznika a interfejs web w sposób jednoznaczny wskazywał że dany producent AV czy protokół jest obsługiwany przez dany szablon.
* Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH.
* Wymaga się aby w sposób manualny istniała możliwość wyboru trybu wykrywania urządzeń PoE. Jednym z takich trybów powinien być: 4ptdot3af
* HTTPs
* SSH
* Obsługa PTPv2
* STP, MTP, RSTP PV(R)STP
* IPv4/IPv6:
* PIM-SM
* PIM-DM
* SSM
* Obsługa IEEE 802.1AS-2011 gPTP, IEEE 802.1Qav-2009 FQTSS, IEEE 802.1Qat-2010 MSRP, IEEE 802.1ak MMRP, IEEE 802.1ak MVRP
* Kształtowanie ruchu na wejściu oraz wyjściu co 1 Kbps
* Radius
* TACACS+
* IGMPv1,v2 Querier
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* CCC: GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class A)
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A

1. **Urządzenie UTM – 2szt.**

|  |
| --- |
| **Urządzenie UTM – 2 sztuki Producent / model urządzenia  (wypełnia Wykonawca):**  **…………………………………………………………………………………………………………………………………………………………………………………………** |
| **Wymagania minimalne:** |

# **Wymagania Ogólne**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę 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 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 5 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 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 protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

# **Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są 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.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# **Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje 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.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

# **Połączenia VPN**

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* 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.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# **Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# **Funkcje SD-WAN**

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

# **Zarządzanie pasmem**

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

# **Ochrona przed malware**

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# **Ochrona przed atakami**

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia 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).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# **Kontrola WWW**

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

# **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia 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.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. 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 mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# **Logowanie**

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# **Testy wydajnościowe oraz funkcjonalne**

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

# **Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

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

# **Gwarancja oraz wsparcie**

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 zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

# **Rozszerzone wsparcie serwisowe**

System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.

System musi być objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

* Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
* Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
* Doradztwo w zakresie konfiguracji.
* Zdalne wsparcie techniczne.
* Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
* Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
* Przygotowanie urządzenia do zdalnej konfiguracji.
* Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
* Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
* Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
* Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Przed podpisaniem umowy Wykonawca zobowiązany będzie dostarczyć:

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne (Help desk) o gotowości świadczenia wymaganego serwisu, zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej.
* Certyfikat ISO 9001 podmiotu serwisującego.

Brak ww. dokumentów traktowany będzie jako uchylanie się od zawarcia umowy.

# **Wsparcie wdrożeniowe**

Zamawiający wymaga aby Wykonawca w ramach dostawy wykonał prace przygotowawcze i wdrożeniowe   
w następującym zakresie:

* inicjalizacja i aktualizacja urządzenia UTM
* stworzenie i omówienie min 3 vlanów
* stworzenie i omówienie przykładowych polityk bezpieczeństwa
* stworzenie i omówienie reagowania na incydenty w sieci

1. **Zasilacz awaryjny typ I – 3szt.**

|  |  |  |
| --- | --- | --- |
| **Zasilacz awaryjny typ I – 3 sztuk**  **Producent / model urządzenia (wypełnia Wykonawca) :**  **…………………………………………………………………………………………………………………………………………………………………………………………** | | |
| **Wymagania minimalne:** | | |
| 1 | Moc pozorna | 3000 VA |
| 2 | Moc rzeczywista | 2700 W |
| 3 | Topologia | Online |
| 4 | Współczynnik mocy | 0,9 |
| 5 | Czas przełączenia na baterię | 0 ms |
| 6 | Liczba, typ gniazd wyjściowych | 6 x IEC C13, 1 x IEC C19 |
| 7 | Typ gniazda wejściowego | IEC C20 16A |
| 8 | Czas podtrzymania dla 100% obciążenia dla pf=0,9 | 3 minuty |
| 9 | Czas podtrzymania przy 50% obciążenia dla pf=0,9 | 10 minut |
| 10 | Kształt napięcia | Sinusoidalny |
| 11 | Ochrona przed przeładowaniem | Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm) |
| 12 | Ochrona przed głębokim rozładowaniem | Tak |
| 13 | Okresowy automatyczny test baterii | Tak |
| 14 | Możliwość uruchomienia bez napięcia w sieci „zimny start” | Tak |
| 15 | Interfejs komunikacyjny | •  USB   • RS232 DB-9 żeński (HID)   • styki przekaźnikowe   • miniport wyłącznik ON/OFF   • SNMP/Ethernet (slot na kartę komunikacyjną) |
| 16 | Panel sterowania z wyświetlaczem LCD | • Panel LCD  • Menu w języku polskim   • Poziomy rząd przycisków sterowania   • Poziomy rząd wskaźników stanu:  zasialanie z sieci (zielony),  trybu bateryjnego (żółty),  usterki (czerwony)   • Sygnalizator akustyczny |
| 17 | Sygnały akustyczne | • Awaria   • Niski stan naładowania baterii   • Przeciążenie   • Serwis |
| 18 | Typ obudowy | Rack 2U |
| 19 | Wyposażenie dołączone do urządzenia | 1 x kabel komunikacyjny USB  2 x kable wyjściowe IEC 10A  2 x szyny do montażu 19' |
| 20 | Masa urządzenia | Masymalnie 35kg |
| 21 | Gwarancja producenta | Minimum 24 miesiące |

1. **Zasilacz awaryjny typ II – 36szt.**

|  |  |  |
| --- | --- | --- |
| **Zasilacz awaryjny typ II – 36 sztuk**  **Producent / model urządzenia (wypełnia Wykonawca) :**  **…………………………………………………………………………………………………………………………………………………………………………………………** | | |
| **Wymagania minimalne:** | | |
| 1 | Moc pozorna | 700 VA |
| 2 | Moc rzeczywista | 420 W |
| 3 | Topologia (klasyfikacja IEC 62040-3) | off-line (standby) |
| 4 | Typ obudowy | tower |
| 5 | Sprawność UPS'a w trybie normalnym | >98% |
| 6 | Sprawność UPS'a w trybie bateryjnym | między 75% a 84% |
| 7 | Przebieg napięcia | Sinusoida aproksymowana |
| 8 | Liczba, typ gniazd wyjściowych z podtrzymaniem zasilania i ochroną przeciwprzepięciową | 3 x FR |
| 9 | Liczba, typ gniazd wyjściowych tylko z ochroną przeciwprzepięciową | 1 x FR |
| 10 | Ochrona przeciwprzepięciowa | Tak, zgodna z normą IEC 61643-1 |
| 11 | Typ gniazda wejściowego | IEC C14 |
| 12 | Zabezpieczenie wejściowe | Resetowalne zabezpieczenie termiczne 10 A |
| 13 | Czas podtrzymania dla obciążenia mocą 280W (70% mocy maksymalnej) | 5 minut |
| 14 | Przeciążalność w trybie normalnym | do 120% mocy znamionowej przez 5 minut, do 150% mocy znamionowej przez 10 sekund |
| 15 | Przeciążalność w trybie bateryjnym | 105-110% 10 sekund, >110% 1 sekunda |
| 16 | Baterie wewnętrzne | 1 x 12 V / 7 Ah |
| 17 | Ochrona przed głębokim rozładowaniem | Tak |
| 18 | Okresowy automatyczny test baterii | Tak |
| 19 | Możliwość samodzielnej wymiany baterii | Tak |
| 20 | Zimny start | Tak |
| 21 | Porty USB do ładowania urządzeń mobilnych | Tak, umieszczone na froncie zasilacza, co najmniej 1xUSB-A oraz 1xUSB-C |
| 22 | Przyciski sterujące i sygnalizacja | sygnalizator akustyczny (awaria, niski stan naładowania baterii, przeciążenie), podświetlany przycisk wł./wył. |
| 23 | Wyposażenie | UPS, instrukcja quick start, instrukcja bezpieczeństwa, przewód USB, przewód zasilający UPS |
| 24 | Dołączone oprogramowanie | Do monitoringu stanu i parametrów UPS i bezpiecznego zamykania systemów operacyjnych Windows przy wyczerpaniu baterii. |
| 25 | Chłodzenie zasilacza | W pełni pasywne, brak wentylatora |
| 26 | Stopień ochrony | IP20 |
| 27 | Temperatura pracy | od 0°C do 40°C |
| 28 | Maksymalna masa UPS | 3,9 kg |
| 29 | Gwarancja producenta | 36 miesięcy na elektronikę oraz 24 miesiące na baterię |

1. **Serwer NAS – 1szt.**

|  |  |  |
| --- | --- | --- |
| **Serwer NAS – 1 sztuka**  **Producent / model urządzenia / model procesora (wypełnia Wykonawca) :**  **…………………………………………………………………………………………………………………………………………………………………………………………** | | |
| **Wymagania minimalne:** | | |
| 1 | Procesor | Procesor wielordzeniowy 64-bitowy o taktowaniu nie niższym niż 2.1GHz uzyskujący wynik co najmniej 9 970 punktów w teście PassMark - CPU Mark według wyników dostępnych na stronie <http://www.cpubenchmark.net> – na okres nie wcześniejszy niż 01.09.2025r. |
| 2 | Obudowa | RACK 19" 2U – wraz z kompletem szyn umożliwiającym zamontowanie w szafie RACK |
| 3 | Pamięć RAM | Minimum 32 GB DDR4 ECC. Pamięć RAM zgodna z listą kompatybilności producenta oferowanego serwera. Możliwość rozszerzenia pamięci RAM do 64 GB. |
| 4 | Liczba zatok na dyski twarde | Minimum 12 |
| 5 | Obsługiwane dyski twarde | 3.5" SATA HDD / 2.5" SATA SSD – Hot Plug  Zamawiający wymaga dostarczenia minimum 8 dysków 3.5” SATA HDD o pojemności co najmniej 8 TB każdy o parametrach nie gorszych niż:  Prędkość obrotowa: 7200 RPM  MTBF: 2 000 000  Obciążenie roczne: 550 TB  Gwarancja producenta dysku: 5 lat  Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera.  Dyski zgodne z listą kompatybilności producenta oferowanego serwera NAS. |
| 6 | Możliwość podłączenia modułu rozszerzającego | Tak |
| 7 | Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi: | Minimum 36 |
| 8 | Porty na karty rozszerzeń | Minimum 2 x Gen3 x8 PCIe (x8 link) |
| 9 | Porty LAN | Wbudowane min. 4 x 1GbE RJ-45, 2 x 10GbE RJ-45 |
| 10 | Porty USB 3.2 | Minimum 2 |
| 11 | Gniazdo rozszerzenia | Minimum 2 |
| 12 | Zasilanie | Redundantny zasilacz o mocy minimalnej 500W |
| 13 | Mechanizm szyfrowania sprzętowego | Tak, min AES-NI |
| 14 | Wewnętrzny system plików | BTRFS, EXT4 |
| 15 | Obsługiwane tryby RAID | JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny |
| 16 | Usługa katalogowa | Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station |
| 17 | Bezpieczeństwo | Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail. |
| 18 | Oprogramowanie do kopii zapasowej | Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów.  Minimalne wymagane funkcje oprogramowania do backupu:  - kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal,  - kopia zapasowa środowisk MacOS  - kopia zapasowa maszyn wirtualnych (VMware, Hyper-V)  - kopia zapasowa serwerów fizycznych (Windows, Linux)  - obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania,  - obsługa wielu wersji i retencji,  - możliwość wyzwalania kopii zapasowej według harmonogramu,  - obsługa klastra przełączania awaryjnego Microsoft Hyper-V,  - automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej, - centralne zarządzanie,  - konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań,  - portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora),  - delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora,  - kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace |
| 19 | Oprogramowanie | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych * Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. * Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. Możliwość utworzenia klastra bez konieczności przywracania systemu do ustawień fabrycznych w serwerze aktywnym. * Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync * Obsługa minimum 512 migawek na folder współdzielony i minimum 16380 migawek na cały system * Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 32jednoczesnych połączeń |
| 20 | Gwarancja producenta | Minimum 5 lat, 1 rok dla szyn montażowych. |

Zamawiający wymaga aby w przypadku oferowanego serwera NAS Wykonawca zapewnił wsparcie telefoniczne lub on-line w obszarze konfiguracji i eksploatacji urządzenia w łącznym wymiarze maksymalnie 2 godzin.   
W uzasadnionej sytuacji Zamawiający zapewni wsparcie Wykonawcy w miejscu instalacji sprzętu po uprzednim obustronnym ustaleniu terminu.

1. **Licencja na oprogramowanie antywirusowe – 2szt. (łącznie 28 stanowisk)**

|  |
| --- |
| **Licencja na oprogramowanie antywirusowe – 2 sztuki (łącznie 28 stanowisk) Producent / nazwa oprogramowania  (wypełnia Wykonawca):**  **…………………………………………………………………………………………………………………………………………………………………………………………** |
| **Wymagania minimalne:** |

Zamawiający wymaga dostarczenie dwóch licencji na oprogramowanie antywirusowe dla dwóch jednostek organizacyjnych (samorządowych) obejmujące następujące ilości stanowisk komputerowych:

I jednostka organizacyjna (samorządowa): **18 stanowisk**

II jednostka organizacyjna (samorządowa): **10 stanowisk**

Zamawiający przekaże wyłonionemu Wykonawcy wszelkie dane docelowych jednostek samorządowych niezbędne do wygenerowania wymaganych licencji.

**Administracja zdalna**

1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:

* Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
* Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
* Buforowanie ruchu HTTPS.

1. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
2. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android: Google Authenticator, Microsoft Authenticator
3. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
4. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:

* adresy sieciowe IP,
* aktywne zagrożenia,
* stan funkcjonowania oraz ochrony,
* wersja systemu operacyjnego,
* podzespoły komputera.

1. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:

* wyrażenie CRON,
* codziennie,
* co miesiąc,
* co rok,
* po wystąpieniu nowego zdarzenia,

1. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim.  
   Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania.
2. Rozwiązanie musi mieć możliwość tagowania obiektów.

**Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków iseciowych, dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń.
12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

* sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego,
* konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników,
* konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy

1. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
2. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
3. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
4. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

* typ urządzenia (pamięci masowe, drukarki USB, urządzenia Bluetooth)
* parametry urządzenia (nr seryjny, producent, model)
* typ dostępu (brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu)

1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
2. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: antywirus, zapora osobista, antispyware, metody heurystyczne.
3. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie   
   i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
4. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
5. Rozwiązanie musi posiadać wbudowany system IDS.
6. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego
7. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
8. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta. Rozwiązanie musi posiadać możliwość filtrowania adresów URL   
   w oparciu o co najmniej 160 kategorii i podkategorii, oraz umożliwiać stworzenie własnego komunikatu na zablokowanych stronach.