1. **System ITSM – 1szt. - 50 licencji**
2. **Przełącznik sieciowy 24 portowy zarządzalny – 8szt.**
3. **Przełącznik sieciowy 8 portowy zarządzalny – 3szt.**
4. **Przełącznik sieciowy 8 portowy zarządzalny PoE – 3szt.**
5. **UTM – 5szt.**
6. **UTM – 1szt.**
7. **Serwer – 1szt.**
8. **Licencje CAL 5x user – 2 szt.**

1. System do zarządzania zasobami IT, użytkownikami oraz bezpieczeństwem (ITSM) – 50 licencji

1) Minimalna funkcjonalność systemu

Zarządzanie zasobami

Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne

- Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania
- Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP
- Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
- Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
- Odwzorowanie struktury organizacji w oparciu o Active Directory
- Jednostronna synchronizacja komputerów oraz drukarek z AD oraz AAD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
- Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz AAD) oraz sieci
- Mapowanie atrybutów obiektów AD (oraz AAD) do obiektów
- Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)
- Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
- Utworzenie własnych typów elementów wyposażenia
- Łączenie elementów wyposażenia w zestawy
- Przypisywanie zasobu do wielu zestawów
- Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia
- Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
- Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
- Przypisywanie sprzętu do konkretnych osób
- Przypisywanie sprzętu do wybranej firmy
- Automatyczne wyznaczanie 'Głównego użytkownika' komputera
- Wiązanie wielu rekordów wyposażenia z użytkownikiem
- Przypisywanie sprzętu do dowolnej lokalizacji
- Definiowanie własnych, dowolnych atrybutów sprzętu
- Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu'
- Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia
- Dowolna treść kodu kreskowego
- Określanie loga firmy oraz użycia go na wydrukach
- Grupowa zmiana domeny/grupy roboczej zasobu

Informacje o sprzęcie

- Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu
- Wykrywanie komputerów typu All-In-One
- Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF)
- Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
- Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
- Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany
- Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.)
- Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)
- Odczyt informacji o module TPM

- Odczyt D3Dscore z WinSAT
- Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
- Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu
- Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika)
- Automatyczne tworzenie zestawów: Komputer + Monitor
- Automatyczne utworzenie zestawów: Komputer + drukarka lokalna
- Automatyczne utworzenie zestawów: host + maszyny wirtualne
- Automatyczne wykrywanie czy komputer jest maszyną wirtualną
- Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform
- Określanie informacji o wykorzystywanej wirtualizacji
- Podgląd zestawów, do których należy zasób
- Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami
- Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu
- Definiowanie szczegółowych informacji finansowych
- Obsługa walut w danych finansowych
- Definiowanie bazy dostawców sprzętu i oprogramowania
- Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)
- Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta
- Agent odczytuje identyfikator SID komputera
- Określanie adresu interfejsu webowego urządzenia sieciowego
- Określanie typu gwarancji dla zasobu
- Określenie wpływu biznesowego wybranego zasobu
- Tworzenie własnych typów gwarancji
- Określanie ikony dla typów zasobów
- Integracja z Dell API
- Wyszukiwanie i identyfikacja duplikatów zasobów
- Geolokalizacja komputerów z agentem

Raporty zasobów

- Raport dodanych załączników
- Automatyczne tworzenie historii zmian sprzętu
- Raport zbiorczy historii zmian w sprzęcie
- Ewidencja zdarzeń serwisowych
- Dodawanie notatek\komentarzy dla zdefiniowanych obiektów zasobów
- Informacja na temat pojemności dysków twardych oraz wolnego miejsca
- Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu
- Wydruk\dodawanie jako załącznik protokołu przekazania dla całego zestawu
- Kreator szablonów wydruków WYSIWYG
- Definiowanie dedykowanych profili protokołów
- Zapisywanie protokołów podczas generowania jako załącznik do zasobu
- Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia
- Wydruk lub zapis do pliku raportów ze szczegółami sprzętu
- Porównywarka wyników skanowania sprzętu
- Dzienniki zdarzeń systemu Windows
- Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu
- Geolokalizacja komputerów z agentem

Zarządzanie zasilaniem

- Zdalne włączanie i wyłączenie komputerów
- Obsługa SecureOn przy WakeOnLan
- Tworzenie harmonogramów wyłączania i włączania komputerów
- Wybór 5 trybów zamknięcia systemu: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Wymuszenie wyłączenia, Restart
- Możliwość anulowania /wyświetlenia komunikatu jeśli jest zalogowany użytkownik
- Możliwość przerwania / odłożenia zadania na żądanie użytkownika
- Wymuszenie wylogowania użytkownika przed wyłączeniem komputera
- Raport zadań jednorazowych oraz harmonogramów
- Monitoring obciążenia CPU

Funkcje dodatkowe
- Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych
- Podpisywanie skryptów Powershell certyfikatem
- Wykonywanie skryptów w kontekście sesji użytkownika lub usługi
- Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika
- Wykonywanie zadań dla wszystkich komputerów
- Edytor skryptów z funkcją kolorowania składni
- Wykorzystywanie predefiniowanych skryptów
- Import informacji o wyposażeniu z pliku CSV
- Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL)
- Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu)
- Generowanie kodów paskowych, QR dla każdego elementu wyposażenia
- Obsługa kodów QR
- Archiwum zasobów
- Przeniesienie utylizowanego wyposażenia do archiwum
- Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego
- Zarządzanie sprzętem przez aplikacje mobilną
- Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu
- Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych
- Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej
- Grupowa zmiana atrybutów
- Personalizacja statusów zasobów

Zarządzanie oprogramowaniem

Licencje
- Inwentaryzacja licencji
- Automatyczne tworzenie licencji na podstawie kluczy produktów
- Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego
- Import licencji z pliku tekstowego
- Automatyczne generowanie historii zmian w licencji
- Określanie statusu licencji
- Tworzenie własnych atrybutów licencji
- Tworzenie notatek oraz załączników w dowolnym formacie do licencji
- Tworzenie licencji z poziomu rozliczenia audytu legalności
- Tworzenie licencji z poziomu raportu kluczy licencji
- Tworzenie zestawów licencji
- Relacja licencji z użytkownikiem, firmą, działem, lokalizacją
- Zmiana typu licencji dla wybranej grupy

- Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)
- Przypisywanie licencji do komputera
- Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)
- Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska
- Definiowanie licencji przeznaczonych do przyszłego zakupu
- Definiowanie kluczy seryjnych i przypisywanie do licencji
- Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją
- Określenie wpływu biznesowego wybranej licencji

Skanowanie oprogramowania

- Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera
- Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów
- Śledzenie zmian w stanie zainstalowanego oprogramowania
- Zdalny skan komputerów (bieżący lub okresowy)
- Zmiana priorytetu skanowania oprogramowania
- Skan komputerów niepodłączonych do sieci
- Wysyłanie wyników skanowania offline na serwer FTP (Audyt)
- Przekazywanie konfiguracji wzorcowej dla skanera offline
- Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania
- Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy
- Określanie masek plików dla publikacji elektronicznych (e-book)
- Skan plików skompresowanych
- Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
- Wbudowane profile skanowania (np. profil wzorcowy)
- Definicja własnych ustawień skanowania
- Porównywanie wyników skanowania oprogramowania
- Wykrywanie plików multimedialnych
- Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
- Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
- Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie
- Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
- Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta
- Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)

Audyt oprogramowania

- Rozliczanie pakietów aplikacji
- Rozliczanie systemów operacyjnych
- Rozliczanie licencji typu „Downgrade”, "Upgrade" oraz instalacji innego oprogramowania w ramach licencji
- Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji.
- Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)
- Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
- Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
- Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji

Funkcje

- Mechanizm informujący o nowej bazie wzorców oprogramowania
- Definiowanie własnych wzorców oprogramowania
- Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych
- Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania
- Wykrywanie kluczy/identyfikatorów programów
- W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza
- Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office
- Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania
- Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji
- Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd.
- Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.
- "Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
- Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)
- Zdalna dezinstalacja oprogramowania
- Utworzenie harmonogramu dezinstalacji oprogramowania
- Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania
- Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej
- Raport zainstalowanych aktualizacji systemu Windows

Kontrola wykorzystania sprzętu i oprogramowania

Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne

- Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach
- Odczyt informacji o kontal lokalnych komputera, wraz z odczytem grup do, których konto należy
- Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)
- Określanie firmy do której należy użytkownik
- Określanie przełożonego dla użytkownika
- Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy).
- Prezentacja 'statusu użytkownika' (Zatrudniony, zwolniony, itd.)
- Zarządzanie stanowiskami użytkowników
- Przeniesienie rekordu użytkownika do archiwum
- Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika
- Odczytywanie informacji o użytkownikach z Active Directory oraz AAD
- Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz AAD)
- Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
- Podgląd zdjęcia przypisanego do użytkownika
- Przypisywanie do użytkownika załączników (pliki)
- Przypisywanie notatek do użytkownika
- Ewidencja zdarzeń przypisanych do użytkowników
- Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory

Raporty

- Analiza aktywności użytkowników
- Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko

- Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP)
- Analiza przerw w pracy
- Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)
- Analiza aktywności mikrofonu oraz kamery
- Analiza wykorzystania poszczególnych aplikacji w czasie
- Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie
- Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika
- Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny).
- Statystyki najczęściej wykorzystywanych aplikacji
- Statystyki wykorzystania komputerów przez poszczególnych użytkowników
- Statystyki aktywności użytkownika i grup użytkowników
- Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin
- Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników
- Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)
- Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
- Monitoring wydruków na drukarkach sieciowych
- Monitoring użytkowników stacji terminalowych
- Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)
- Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca
- Raport zbiorczy historii zmian w rekordach użytkowników

Funkcje

- Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.
- Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń
- Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
- Automatycznie budowana baza informacji o napędach zewnętrznych
- Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
- Odczyt i blokada urządzeń PTP/MTP
- Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM
- Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy
- Informacje o ostatnio zalogowanych osobach na stacjach klienckich
- Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje
- Komentowanie przerw pracy
- Kategoryzacja przerwy w pracy na podstawie komentarza

Kontrola wykorzystania Internetu

Funkcje

- Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)
- Blokada pobierania plików wg typu MIM
- Blokada stron internetowych dla protokołu http \ https w najpopularniejszych przeglądarkach WWW
- Kategoryzacja stron internetowych
- Import stron WWW z pliku lub ze schowka
- Slowniki kategorii stron WWW

- Blokada dostępu do witryn zgodnie z harmonogramem
- Blokada dostępu do witryn na podstawie kategorii strony WWW
- Blokada trybu incognito w przeglądarce Google Chrome

Raporty

- Raporty dotyczące aktywności użytkowników w Internecie
- Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)
- Monitoring stron internetowych dla protokołu http \ https (Przeglądarki oparte o silnik Chromium, Edge, Chrome, Vivaldi, Firefox*)
- Analiza liczby wejść na poszczególne strony lub domeny
- Kategoryzacja odwiedzanych domen i stron, opcjonalnie z wykorzystaniem AI
- Raport informujący o plikach pobranych przez przeglądarki WWW
- Raport informujący o danych wysłanych przez przeglądarki (bez Firefox)
- Monitoring plików pobieranych przez przeglądarki internetowe

Zarządzanie użytkownikami

Funkcje

- Raportowanie aktywności pracy
- Przeglądanie ostatnio zgłoszonych incydentów
- Powiązanie użytkownika z licencją
- Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów
- Cykliczne, automatyczne generowanie raportów
- Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze
- Zgłoszenia dotyczące wniosków nieobecności użytkowników
- Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności
- Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika
- Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory
- Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO
- Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych
- Planowanie dni wolnych w widoku kalendarza
- Planowanie zastępstw podczas nieobecności

Funkcjonalności ogólne

- Określanie praw dostępu do grup zasobów lub użytkowników
- Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca")
- Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
- Wersja angielska (en-US) interfejsu użytkownika
- Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL
- Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
- Zdalna instalacja i dezinstalacja agentów na stacjach roboczych
- Odczytywanie struktury organizacji z Active Directory
- Skaner sieci wykorzystywany do wykrywania nowych urządzeń
- Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta
- Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta

- Automatycznie dodane komputery\użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory
- Definiowanie nieograniczonej liczby użytkowników systemu
- Określanie ról dla kont systemu: Administratorzy, Menadżerowie, Zarządcy,Pracownicy
- Indywidualny login i hasło dla poszczególnych użytkowników
- Automatyczne logowanie do systemu
- Zarządzanie uprawnieniami użytkowników - określanie dostępu do poszczególnych obiektów i opcji systemu systemu (konkretny użytkownik, konkretny zasób lub ich grupy) , możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie)
- Dostęp do programu chroniony przy pomocy uwierzytelniania wieloskładnikowego
- Określanie ról użytkowników - zarządzanie grupami
- Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem
- Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)
- Zgodny z pracą w sieciach WLAN
- Podgląd aktualnych zadań serwera
- Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
- Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami
- Wyszukiwanie danych w tabelach raportów
- Dowolne definiowania grup sprzętu i użytkowników
- Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
- Definiowanie i zapamiętywanie własnych widoków
- Eksport danych bezpośrednio do MS Excel
- Budowa zestawień metodą drag'n'drop
- Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów
- Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.
- Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP
- Mechanizm kompresji pakietów danych przesyłanych przez Agenta
- Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery)
- Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy)
- Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server
- Mechanizm zdalnego pobierania bieżących aktualizacji do programu
- Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
- Dostęp do bazy wiedzy systemu
- Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
- Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym
- Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania, sprzętu, sesji zdalnego pulpitu, logów raportów, logów automatyzacji
- Personalizacja pakietu instalacyjnego agenta
- Określanie polityki haseł dla systemu
- Zmiana języka systemu podczas logowania
- Określenie numeru BDO przy definiowaniu rekordu firmy
- Opcja resetu hasła podczas logowania
- Globalne wyszukiwanie obiektów w systemie
- Tworzenie atrybutów jako lista/słownik
- Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników
- Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring
- Wyszukiwarka ustawień w opcjach systemowych

- Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych)
- Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie
- Skanowanie lasu domen
- Budowa personalizowanego pakietu instalacyjnego
- Logowanie do portalu Web za pomocą mechanizmu Single Sign On
- Logowanie operacji kont serwisowych
- Logowanie nieudanych prób uwierzytelnienia
- Eksport danych diagnostycznych oraz dzienników operacji
- Integracja z SMS API
- Definiowanie nazwy hosta, na której serwer nasłuchuje połączeń sieciowych

Dodatkowe wymagania

- Praca w oparciu o MS SQL Server oraz MS SQL Express (2016/2019/2022 32/64 bit) o jeden z darmowych silników baz danych (np. PostgreSQL lub Firebird)
- Obsługa systemów operacyjnych dla agenta: Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10, Windows 11
- Obsługa systemów operacyjnych dla serwera: Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 11
- Dostęp do aktualizacji programu oraz wsparcia technicznego producenta w okresie do dnia 2026-03-28 roku

2) Zakres instalacji i wdrożenia

- Instalacja i konfiguracja programu na maszynie wirtualnej wskazanej przez Zamawiającego,
- Wprowadzenie do systemu informacji o wszystkich urządzeniach sieciowych oraz drukarkach usb i ups-ach na podstawie informacji dostarczonych przez Zamawiającego (bez konieczności inwentaryzacji urządzeń),
- Przygotowanie przykładowych polityk, raportów,
- Przeprowadzenie warsztatów z zakresu eksploatacji systemu w wymiarze 8 godzin – Zamawiający dopuszcza formę online.

2. Przełącznik sieciowy 24 portowy zarządzalny – 8 szt.

Nazwa	Minimalne wymagania dla sprzętu
Porty przełącznika	minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+
Port konsolowy	RJ45 (RS-232)
Szybkość przełączania	minimum 128Gb/s
Przepustowość	minimum 95Mp/s (dla pakietów 64Kb)
Bufor pakietów	minimum 1,5MB
Ramki Jumbo	minimum 10k
Tablica adresów MAC	minimum 16k
Tablica ACL	minimum 512
Tablica VLAN	minimum 4094
Taktowanie procesora	minimum 800MHz
Pamięć RAM	minimum 256MB
Zasilanie	zabudowany zasilacz 230V AC
Certyfikaty bezpieczeństwa	CE, RoHS
VLAN	Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
DHCP	IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
Spanning tree	IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding
Agregacja łączy	IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance
Bezpieczeństwo	Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
Multicast	IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
Lista kontroli dostępu	IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
Diagnostyka	sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP
Zarządzanie	TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking
Oprogramowanie oraz wsparcie techniczne	oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
Dodatkowe wymagania	Dostarczenie wkładek światłowodowych oraz patchkord niezbędnych do połączenia przełączników w stack
Gwarancja	lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

Zakres instalacji i konfiguracji
- aktualizacja oprogramowania firmware do najnowszej wersji,
- konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych.
- instalacja w jednostkach organizacyjnych, wskazanych przez zamawiającego,

Przełącznik sieciowy 8 portowy zarządzalny – 3szt.

Nazwa	Minimalne wymagania dla sprzętu
Porty przełącznika	minimum 8x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+
Port konsolowy	RJ45 (RS-232)
Szybkość przełączania	minimum 96Gb/s
Przepustowość	minimum 71,4Mp/s (dla pakietów 64Kb)
Bufor pakietów	minimum 1,5MB
Ramki Jumbo	minimum 10k
Tablica adresów MAC	minimum 16k
Tablica ACL	minimum 512
Tablica VLAN	minimum 4k
Taktowanie procesora	minimum 800MHz
Pamięć RAM	minimum 256MB
Zasilanie	zabudowany zasilacz 230V AC
Certyfikaty bezpieczeństwa	CE, RoHS
VLAN	Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ DHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
DHCP	IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
Spanning tree	IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding
Agregacja łączy	IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance
Bezpieczeństwo	Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
Multicast	IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
Lista kontroli dostępu	IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
Diagnostyka	sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP
Zarządzanie	TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking
Oprogramowanie oraz wsparcie techniczne	oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
Gwarancja	lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

Zakres instalacji i konfiguracji

- aktualizacja oprogramowania firmware do najnowszej wersji,
- konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych.
- instalacja w jednostkach organizacyjnych, wskazanych przez zamawiającego,

3. Przełącznik sieciowy 8 portowy zarządzalny PoE – 3 szt.

Nazwa	Minimalne wymagania dla sprzętu
Porty przełącznika	minimum 24x 10/100/1000Base-T RJ45 PoE oraz minimum 4x 1/10GBase-X SFP+
Port konsolowy	RJ45 (RS-232)
Szybkość przełączania	minimum 128Gb/s
Przepustowość	minimum 95Mp/s (dla pakietów 64Kb)
Bufor pakietów	minimum 1,5MB
Ramki Jumbo	minimum 10k
Tablica adresów MAC	minimum 16k
Tablica ACL	minimum 512
Tablica VLAN	minimum 4094
Taktowanie procesora	minimum 800MHz
Pamięć RAM	minimum 256MB
Obsługa technologii PoE	IEEE 802.3 af/at
Budżet mocy PoE	minimum 370W
Zasilanie	zabudowany zasilacz 230V AC
Certyfikaty bezpieczeństwa	CE, RoHS
VLAN	Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
DHCP	IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
Spanning tree	IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding
Agregacja łączy	IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance
Bezpieczeństwo	Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
Multicast	IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
Lista kontroli dostępu	IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
Diagnostyka	sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP
Zarządzanie	TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking
Funkcje PoE	Support IEEE 802.3at for all ports, PD failure detection, PoE scheduling
Oprogramowanie oraz wsparcie techniczne	oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
Dodatkowe wymagania	Dostarczenie wkładek światłowodowych oraz patchkord niezbędnych do połączenia przełączników w stack
Gwarancja	lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

Zakres instalacji i konfiguracji

- aktualizacja oprogramowania firmware do najnowszej wersji,
- konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych.
- instalacja w jednostkach organizacyjnych, wskazanych przez zamawiającego,

4. UTM – 5 szt.

Nazwa	Minimalne wymagania dla sprzętu
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 takichjak np. DHCP.
Zapora korporacyjna (firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. 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. 5. 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, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe
Intrusion prevention system (IPS)	1. 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. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. 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. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. 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). 10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

Kształtowanie pasma (traffic shapping)	1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	1. Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. Po rozbudowie 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	1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (VPN)	1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 3. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtr dostępu do stron www	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator ma mieć możliwość dodawania własnych kategorii URL. 4. 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. 5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 7. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

	9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
Uwierzytelnianie	1. 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. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. 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. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneliSSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Administracja łączami do internetu (ISP)	1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
Administracja urządzeniem	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

	4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 17. 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 serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

	2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 5. Urządzenie ma posiadać usługę DNS Proxy. 6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 7. Urządzenie musi mieć zaimplementowane Open API 8. 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. 9. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
Gwarancja i serwis	1. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 3. Urządzenie ma posiadać na czas 24 miesięcy w ramach serwisu aktualizacje do FW+IPS, VPN, filtr URL, AV, AS, Obsługa kart SD.
Parametry sprzętowe	1. Urządzenie ma umożliwiać budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 2. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 3. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. 4. Liczba portów Ethernet 2,5Gbps – min. 8. 5. Liczba portów światłowodowych 1Gbps – min. 1. 6. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 7. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps. 8. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. 9. Przepustowość filtrowania Antywirusowego – minimum 1Gbps. 10. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps. 11. Maksymalna liczba tuneli VPN IPSec – minimum 100. 12. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100. 13. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 100. 14. Obsługa interfejsów 802.11q (VLAN) – minimum 128 15. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę. 16. Urządzenie nie ma limitu na liczbę użytkowników. 17. Liczba reguł filtrowania – minimum 8 192. 18. Liczba tras statycznego routingu – minimum 512. 19. Liczba tras dynamicznego routingu – minimum 10 000. 20. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. 21. Urządzenie musi być wyposażone w moduł TPM.

Zakres instalacji i konfiguracji
• instalacja w jednostkach organizacyjnych, wskazanych przez zamawiającego,
• aktualizacja oprogramowania firmware do najnowszej wersji,
• przeniesienie konfiguracji z dotychczasowego urządzenia brzegowego do dostarczonego urządzenia,
• analiza aktualnej konfiguracji mechanizmów bezpieczeństwa oraz wprowadzenie zmian w konfiguracji urządzenia brzegowego mających na celu zwiększenie poziomu bezpieczeństwa cyfrowego,

- wprowadzenie do konfiguracji urządzenia UTM zmian umożliwiających izolację serwerów od sieci produkcyjnej oraz identyfikacja usług (portów) niezbędnych do zachowania komunikacji ze stacjami roboczymi użytkowników (bez konieczności zmiany adresacji IP),
- analiza ruchu z serwerów aplikacyjnych oraz odseparowanie tych serwerów od sieci Internet; identyfikacja i przepuszczenie połączeń niezbędnych do poprawnej pracy tych serwerów,
- konfiguracja sieci VLAN oraz ograniczeń firewall-a,
- wydzielenie sieci VLAN dedykowanej dla serwera archiwum, przygotowanie reguł fire-wall-a ograniczających ruch z sieci LAN do serwera archiwum,
- przygotowanie opisu konfiguracji oraz przekazanie go Zamawiającemu w wersji elektronicznej (edytowalnej).

Wykonawca zagwarantuje, że zadania określone powyżej wykonywać będzie osoba posiadająca niezbędne umiejętności w tym aktualny certyfikat kompetencji wystawiony przez producenta urządzenia lub autoryzowane centrum szkoleniowe.

5. UTM – 1 szt.

Nazwa	Minimalne wymagania dla sprzętu
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 takichjak np. DHCP.
Zapora korporacyjna (firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. 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. 5. 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, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe
Intrusion prevention system (IPS)	1. 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. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. 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. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. 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).

	10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (traffic shapping)	1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	1. Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. Po rozbudowie 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	1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (VPN)	1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 3. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtr dostępu do stron www	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator ma mieć możliwość dodawania własnych kategorii URL. 4. 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. 5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 7. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

	9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
Uwierzytelnianie	1. 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. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. 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. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneliSSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Administracja łączami do internetu (ISP)	1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
Administracja urządzeniem	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

	4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 85. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 13. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 14. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 15. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 16. 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 serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 17. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 18. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 19. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

	2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 5. Urządzenie ma posiadać usługę DNS Proxy. 6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 7. Urządzenie musi mieć zaimplementowane Open API 8. 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. 9. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 10. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
Gwarancja i serwis	1. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 3. Urządzenie ma posiadać na czas 24 miesięcy w ramach serwisu aktualizacje do FW+IPS, VPN, filtr URL, AV, AS, Obsługa kart SD.
Parametry sprzętowe	1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. 3. Liczba portów Ethernet 2,5Gbps – min. 8. 4. Liczba portów światłowodowych 1Gbps – min. 1. 5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 6. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps. 7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps. 8. Przepustowość filtrowania Antywirusowego – minimum 500Mbps. 9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps. 10. Maksymalna liczba tuneli VPN IPSec – minimum 100. 11. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50. 12. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50. 13. Obsługa interfejsów 802.11q (VLAN) – minimum 128 14. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę. 15. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 16. Urządzenie nie ma limitu na liczbę użytkowników. 17. Liczba reguł filtrowania – minimum 8 192. 18. Liczba tras statycznego routingu – minimum 512. 19. Liczba tras dynamicznego routingu – minimum 10 000. 20. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. 21. Urządzenie musi być wyposażone w moduł TPM

Zakres instalacji i konfiguracji
• instalacja w jednostce organizacyjnej, wskazanej przez zamawiającego,
• aktualizacja oprogramowania firmware do najnowszej wersji,

• przeniesienie konfiguracji z dotychczasowego routera do dostarczonego urządzenia,
• analiza aktualnej konfiguracji mechanizmów bezpieczeństwa oraz wprowadzenie zmian w konfiguracji urządzenia brzegowego mających na celu zwiększenie poziomu bezpieczeństwa cyfrowego,
• konfiguracja sieci VLAN oraz ograniczeń firewall-a,
• analiza ruchu z serwerów aplikacyjnych oraz odseparowanie tych serwerów od sieci Internet; identyfikacja i przepuszczenie połączeń niezbędnych do poprawnej pracy tych serwerów,
• wydzielenie sieci VLAN dedykowanej dla serwera archiwum, przygotowanie reguł firewall-a ograniczających ruch z sieci LAN do serwera archiwum,
• przygotowanie opisu konfiguracji oraz przekazanie go Zamawiającemu w wersji elektronicznej (edytowalnej).

Wykonawca zagwarantuje, że zadania określone powyżej wykonywać będzie osoba posiadająca niezbędne umiejętności w tym aktualny certyfikat kompetencji wystawiony przez producenta urządzenia lub autoryzowane centrum szkoleniowe.

6. Serwer z systemem operacyjnym – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji min. 4 dysków 3,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Obsługa procesorów 8 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta główna powinna obsługiwać do 128GB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
Procesor	• Zainstalowany jeden procesor min. 8-rdzeniowy, min. 2.6GHz, dedykowany do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min 84.4 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla oferowanego modelu serwera wyposażonego w jeden procesor.
RAM	• Minimum 64GB DDR5 UDIMM 5600MT/s • Na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone do instalacji pamięci.
Gniazda PCI	• minimum dwa sloty PCIe generacji 4
Interfejsy sieciowe/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Dyski twarde	• Możliwość instalacji dysków SATA, SAS, SSD • **Zainstalowane 3 dyski HDD SAS o pojemności min. 1.2 TB, 12Gbps, 2,5" Hot-Plug.** • **Zainstalowane 2 dyski M.2 NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1.**

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający:
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących

Wbudowane porty	• 3 x USB z czego nie mniej niż 1x USB 3.2 Gen 1, 1x VGA
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 700W każdy, klasy Titanium • min. 2 kable zasilające typu C13/C14 o długości min. 2 metry
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • 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 dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera

	• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
System operacyjny	• Zakres Przedmiotu Zamówienia obejmuje dostarczenie Serwerowego Systemu Operacyjnego, zwanego dalej SSO w najnowszej dostępnej na rynku wersji. • Licencja musi uprawniać do uruchamiania min. **dwóch** wystąpień SSO, w środowisku fizycznym i wirtualnym lub wyłącznie wirtualnym za pomocą wbudowanych mechanizmów wirtualizacji. • SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: 1. pozwalają na zmianę rozmiaru w czasie pracy systemu, 2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 4. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), r) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, s) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,

	t) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, 3. zdalna dystrybucja oprogramowania na stacje robocze, 4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, 5. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. dystrybucję certyfikatów poprzez http, ii. konsolidację CA dla wielu lasów domeny, iii. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, 6. szyfrowanie plików i folderów, 7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), 8. możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów, 9. serwis udostępniania stron WWW, 10. wsparcie dla protokołu IP w wersji 6 (IPv6), 11. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. obsługi ramek typu jumbo frames dla maszyn wirtualnych, iii. obsługi 4-KB sektorów dysków, iv. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, v. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, vi. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), u) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,

	v) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), w) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, x) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, y) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o wsparcie dla IPv6; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o integracja z Active Directory; o możliwość obsługi przez dwóch administratorów jednocześnie; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • Możliwość rozszerzenia funkcjonalności o: o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze o Automatyczna rejestracja certyfikatów (ACE)
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-14001:2015 oraz ISO-50001:2018 • Serwer musi posiadać deklarację CE • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.**

	• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Minimum 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. • Możliwość odpłatnego przedłużenia gwarancji producenta do 7 lat. • 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 autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, 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 mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera

Zakres instalacji i konfiguracji:

- dostawę kompletnego sprzętu wraz z systemami operacyjnymi serwera, niezbędnym oprogramowaniem oraz niezbędnymi przewodami,
- rozpakowanie i uruchomienie serwera, instalację systemów operacyjnych,
- uruchomienie mechanizmu wirtualizacji zasobów (obsługi maszyn wirtualnych),
- migrację danych z serwerów fizycznych oraz wirtualnych na nową platformę,
- zapewnienie wsparcia technicznego dla Zamawiającego z zakresu eksploatacji środowiska wirtualizacyjnego przez okres zadeklarowany przez Wykonawcę formularzu ofertowym

7. Licencje CAL 5x user – 2 szt.
Licencje dostępowe dla serwerowego systemu operacyjnego

Parametr	Charakterystyka (wymagania minimalne)
Licencja	• do systemu operacyjnego serwer 2022 standard należy dostarczyć 10 sztuk licencji dostępowych na użytkownika. Licencja powinna zapewnić zgodność z wymaganiami dotyczącymi legalnego dostępu do serwerowego systemu operacyjnego, każdemu użytkownikowi korzystającemu lokalnie z jego zasobów.