Serwer do obsługi eobiegu dokumentów – 1 szt.

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Tower z możliwością instalacji do 4 dysków twardych 3,5”.
Płyta główna	Z możliwością instalacji jednego fizycznego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Zainstalowany minimum jeden procesor 4-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem osiągający minimum 12 000 pkt CPU Mark w teście PassMark CPU Single CPU http://www.cpubenchmark.net/cpu_list.php.
Pamięć RAM	minimum 16 GB pamięci RAM UDIMM o częstotliwości taktowania minimum 3200MHz
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 4 sloty PCI Express w tym przynajmniej 2 sloty Gen4
Interfejsy sieciowe/FC/SAS	Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express.
Dyski twarde	Możliwość instalacji dysków twardych 3,5” typu: SATA, NearLine SAS, SAS, SSD. Zainstalowane: • 2 dyski SATA o pojemności min. 2TB, 3.5” Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID1.
Wbudowane porty	Minimum 8 portów USB z czego min. 2 w technologii 3.0 Minimum 1x RS-232 Minimum 1x VGA
Video	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Chłodzenie i zasilanie	Wentylator, zasilacz o mocy minimum 300W wraz z kablami zasilającymi.
Diagnostyka i Bezpieczeństwo	• zintegrowany z płytą główną moduł TPM 2.0
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ▪ wsparcie dla: ○ IPv6; ○ WSMAN (Web Service for Management); ○ SNMP; ○ IPMI2.0, ○ SSH, ○ Redfish; ○ dynamic DNS;

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.
Warunki gwarancji	3 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji wykonawcy albo producenta. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta lub wykonawcy podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Możliwość odpłatnego rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – **dokumenty potwierdzające należy załączyć do oferty**, lub równoważnymi (co najmniej w zakresie będących przedmiotem zamówienia). **Wymagane dołączenie do oferty** oświadczenia Producenta lub Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważnymi (co najmniej w zakresie projektowania, produkcji i rozwoju produktów i rozwiązań informatycznych, będących przedmiotem zamówienia). 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 2019, Microsoft Windows Server 2022.

Serwer wraz z oprogramowaniem – 1 szt.

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Tower z możliwością instalacji do 4 dysków twardych 3,5”.
Płyta główna	Z możliwością instalacji jednego fizycznego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Zainstalowany minimum jeden procesor 4-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem osiągający minimum 12 000 pkt CPU Mark w teście PassMark CPU Single CPU http://www.cpubenchmark.net/cpu_list.php.
Pamięć RAM	Minimum 16 GB pamięci RAM UDIMM o częstotliwości taktowania minimum 3200MHz
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 4 sloty PCI Express w tym przynajmniej 2 sloty Gen4
Interfejsy sieciowe/FC/SAS	Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express.
Dyski twarde	Możliwość instalacji dysków twardych 3,5” typu: SATA, NearLine SAS, SAS, SSD. Zainstalowane: • 2 dyski SATA o pojemności min. 2TB, 3.5”, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, cache, możliwe konfiguracje poziomów RAID: 0, 1, 10.
Wbudowane porty	Minimum 8 portów USB z czego min. 1 w technologii 3.0 Minimum 1x RS-232 Minimum 1x VGA
Video	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Chłodzenie i zasilanie	Wentylator, redundantne zasilacze o mocy minimum 600W wraz z kablami zasilającymi.
System operacyjny/dodatkowe oprogramowanie	• Windows Server 2022 Standard lub inny równoważny. Jako równoważny system operacyjny Zamawiający rozumie, system spełniający następujące wymagania funkcjonalne: 1. Wspierający graficzny interfejs użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy.

	2. Zapewniający natywne wsparcie dla środowiska .NET Framework 4.8. 3. Zapewniający możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory. 4. System operacyjny musi wspierać pracę domenową. 5. System operacyjny musi posiadać obsługę zdalnego pulpitu zgodnego z protokołem RDP. 6. System operacyjny musi posiadać możliwość uruchomienia serwera DNS. 7. Licencja na system operacyjny zapewnia uruchomienie systemu operacyjnego w środowisku fizycznym i min. 1 środowiska wirtualnego za pomocą wbudowanego mechanizmy wirtualizacji, bez konieczności zakupu dodatkowych licencji. 8. Umożliwiający obsługę minimum 48 GB pamięci RAM. 9. Posiada wbudowaną zaporę sieciową (firewall) dla połączeń przychodzących i wychodzących z systemu. 10. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 11. Zapewniający pełne wsparcie dla podzespołów zainstalowanych w zamawianym sprzęcie komputerowym (przy ew. wykorzystaniu sterowników od odpowiednich producentów podzespołów). 12. Licencja na system operacyjny musi być bez ograniczeń czasowych.
Diagnostyka i Bezpieczeństwo	• zintegrowany z płytą główną moduł TPM 2.0 • fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ▪ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ▪ wsparcie dla IPv6; ▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ▪ integracja z Active Directory; ▪ wsparcie dla dynamic DNS; ▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ▪ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ▪ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Oprogramowanie do zarządzania	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.

Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważnymi (co najmniej w zakresie projektowania, produkcji i rozwoju produktów i rozwiązań informatycznych, będących przedmiotem zamówienia). 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 2016, 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	3 lata gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.

	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. Możliwość odpłatnego rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające **należy załączyć do oferty**, lub równoważnymi (co najmniej w zakresie, będących przedmiotem zamówienia). Wymagane **dołączenie do oferty** oświadczenia Producenta lub Wykonawcy potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
System operacyjny	Zainstalowany system operacyjny Windows Serwer 2019/2022 w wersji Essential/Standard, lub inny równoważny. Jako równoważny system operacyjny Zamawiający rozumie, system spełniający następujące wymagania funkcjonalne: 1. Wspierający graficzny interfejs użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy. 2. Zapewniający natywne wsparcie dla środowiska .NET Framework 4.8. 3. Zapewniający możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory. 4. System operacyjny musi wspierać pracę domenową. 5. System operacyjny musi posiadać obsługę zdalnego pulpitu zgodnego z protokołem RDP. 6. System operacyjny musi posiadać możliwość uruchomienia serwera DNS. 7. Licencja na system operacyjny zapewnia uruchomienie systemu operacyjnego w środowisku fizycznym i min. 1 środowiska wirtualnego za pomocą wbudowanego mechanizmy wirtualizacji, bez konieczności zakupu dodatkowych licencji. 8. Umożliwiający obsługę minimum 48 GB pamięci RAM. 9. Posiada wbudowaną zaporę sieciową (firewall) dla połączeń przychodzących i wychodzących z systemu. 10. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 11. Zapewniający pełne wsparcie dla podzespołów zainstalowanych w zamawianym sprzęcie komputerowym (przy ew. wykorzystaniu sterowników od odpowiednich producentów podzespołów). 12. Licencja na system operacyjny musi być bez ograniczeń czasowych.

Zasilacz awaryjny UPS do serwera – 1 szt.

Komponent	Minimalne wymagania
Moc pozorna	3000 VA
Moc czynna	2700 W
Topologia	lineinteractive
Typ obudowy	Tower/Rack

Chłodzenie	Wewnętrzne wentylatory
Wejście	
Zakres napięcia	0V -300 V
Zakres częstotliwosci	50Hz / 60Hz ± 5Hz / 40Hz - 70Hz (tryb generatora)
Złącza wejściowe	IEC C20
Konektor do modułu bateryjnego	TAK
Faza	1 - fazowy z uziemieniem
Wyjście	
Napięcie	220V / 230V / 240V
Regulacja napięcia (tryb liniowy)	-10% ~ +6%
Regulacja napięcia (tryb bateryjny)	± 5%
Częstotliwość (zakres synchronizacji)	50Hz / 60Hz ± 5Hz
Częstotliwość (tryb bateryjny)	50Hz / 60Hz ± 0,1Hz
Współczynnik mocy (PF)	0,9
Kształt napięcia (wyjściowego)	Sinusoida
Złącza wyjściowe	IEC C13 (8) i IEC C19 (2)
Sprawność	
Tryb liniowy	Minimum 97%
Czas przełączenia	
Liniowy -bateryjny	2-6 ms (typowy)
Interfejs	
Wyświetlacz	LCD
Porty komunikacyjne	USB / RS232 / SNMP / AS400 / karta przekaźnikowa
Oprogramowanie	Linux, SunSolaris, Windows, IBM Aiz, Compaq True64, SGI IRIX, Free BSD, HP-UX, MAC
Inne	
Poziom hałasu (w obrębie 1m)	<40dB
Temperatura pracy	0°C - 40°C
Wilgotność względna	5% - 95% (bez kondensacji)

Alarmy dźwiękowe	Tak
EPO	Tak
Gwarancja	Minimum 12 m-cy

Stacje robocze z monitorami – 6 szt.

Nazwa komponentu	Wymagane parametry techniczne komputerów
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 18 000 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	Minimum 8GB DDR4 3200MHz. Możliwość rozbudowy do min 128GB. Minimum Trzy sloty DIMM wolne,
Pamięć masowa	Dysk M.2 SSD 256 GB PCIe NVMe Class 35 z certyfikatem FIPS Oraz Dysk 3.5” 1024 GB HDD 7200 RPM.
Wydajność grafiki	Zintegrowana karta graficzna osiągajaca w teście Passmark G3D Mark, w kategorii Average G3D Mark wynik co najmniej 1650 pkt. według wyników opublikowanych na stronie https://www.videocardbenchmark.net/gpu_list.php
Wyposażenie multimedialne	Karta dźwiękowa min. dwukanałowa zintegrowana z płytą główną, zgodna z High Definition, minimum jeden wewnętrzny głośnik w obudowie komputera**.** Port słuchawek i mikrofonu na przednim panelu lub z boku obudowy, dopuszcza się rozwiązanie port combo.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 2 x dysków 2.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Zasilacz o mocy min. 240W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 3,5” oraz 2,5”, bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych, śrub radełkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej raz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi być wyposażona w zamek szybkiego dostępu. Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla

	systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, Możliwość ustawienia z poziomu BIOS hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora (hasła oddzielne). Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Dedykowane w BIOS pole Asset Tag/numeru inwentarzowego umożliwiająca wpisanie oznaczenia sprzętu bezpośrednio z poziomu BIOS bez konieczności wykorzystywania dodatkowego oprogramowania. Pole Asset Tag/numeru inwentarzowego po nadaniu numeru nie może być edytowalne w BIOS i nie może ulegać skasowaniu np. po aktualizacji BIOS. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6,

Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głowej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
System operacyjny	Zainstalowany system operacyjny Windows 10 Professional bądź równoważny , musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego na podstawie dołączonego nośnika bez potrzeby ręcznego wpisywania klucza licencyjnego. Jako równoważny Zamawiający uzna system informatyczny który spełnia następujące wymagania: 1. Wsparcie producenta systemu w postaci aktualizacji systemu w zakresie poprawek bezpieczeństwa, uaktualnień, rozszerzeń udostępnianych do tego systemu przez producenta przez okres min. 5 lat od daty odbioru jakościowego urządzenia. 2. Obsługa aplikacji 32 i 64 bitowych. 3. Graficzny interfejs użytkownika w języku polskim, w tym pomoc do systemu. 4. Obsługa za pomocą myszy i klawiatury. 5. Bezproblemowa współpraca z oferowanym pakietem biurowym. 6. Bezproblemowa współpraca z oferowanym oprogramowaniem antywirusowym. 7. Bezproblemowa współpraca z oferowanymi urządzeniami. 8. Integracja z sieciowym środowiskiem serwerowym MS Windows Server 2013 9. Polska wersja interfejsu użytkownika. 10. W zależności od podłączonej sieci, automatyczna zmiana drukarki domyślnej. 11. Wbudowany FireWall z funkcją zarządzania przez użytkownika. 12. Wbudowany mechanizm wirtualizacji umożliwiający uruchomienie i zarządzanie maszynami wirtualnymi. 13. Obsługa min. 16 GB pamięci RAM. 14. Licencja uprawniająca na bezterminowe użytkowanie systemu i nie uniemożliwiająca w przyszłości upgrade systemu operacyjnego (upgrade nie jest przedmiotem niniejszej umowy). 15. Wersja instalacyjna systemu operacyjnego umożliwiająca przeinstalowanie systemu. 16. Funkcja udostępniania i przejmowania pulpitu zdalnego. 17. Funkcja udostępniania folderów i drukarek lokalnych. Udostępnianie musi być realizowane w sieci lokalnej. 18. Funkcja uruchamiania programów z uprawnieniami innego konta (administratora lokalnego lud administratora). 19. Funkcja szyfrowania partycji dysku z danymi użytkownika i partycji z systemem operacyjnym. Funkcja szyfrowania współpracuje z modułem TPM komputera. W przypadku podłączenia zaszyfrowanego dysku do innego komputera, dostęp do danych zaszyfrowanych partycji jest możliwy dopiero po podaniu odpowiedniego hasła. 20. Obsługa rozszerzonego pulpitu na 2 różne monitory (o różnych rozdzielczościach). 21. Funkcjonalność powiększania obrazu na monitorach o 125%. 22. Korzystania z instalacji oprogramowania na wielu komputerach przy wykorzystaniu jednego standardowego obrazu tzw. „image”. 23. Dostępność do bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego przez okres min. 5 lat od daty odbioru jakościowego komputera. 24. System umożliwiający ustawienie, wskazanej przez użytkownika, sieci WiFi jako tzw. „połączenie taryfowe”, co blokuje automatyczne pobieranie, przez system, aktualizacji systemu operacyjnego oraz pakietu biurowego.
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu - lub równoważny (co najmniej w zakresie projektowania, produkcji i rozwoju produktów i rozwiązań informatycznych, będących przedmiotem zamówienia). Deklaracja zgodności CE (**załączyć do oferty**) Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub równoważną (co najmniej w zakresie projektowania, produkcji i rozwoju produktów i rozwiązań informatycznych, będących przedmiotem zamówienia).

Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 25 dB (załączyć oświadczenie producenta) lub równoważnymi,
Wymagania dodatkowe	Wbudowane porty: • Minimum 2 x DisplayPort 1.4 • Minimum 1 x HDMI 2.0b • Minimum 10 portów USB wyprowadzonych na zewnątrz obudowy, • 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu • Minimum 1 x RJ – 45 Wymagana ilość wszystkich wyżej wymienionych portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika). Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.4, 1 x PCIe x4, 4 x DIMM z obsługą do 128 GB DDR4 RAM, 3 x SATA w tym min. 2 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz jedno złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz laserowa USB z sześcioma klawiszami oraz rolką (scroll) Nagrywarka DVD +/-RW o prędkości min. 8x Dołączony nośnik ze sterownikami
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta lub wykonawcy , umożliwiający Zamawiającemu zgłaszanie awarii. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta lub wykonawcę (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające **należy załączyć do oferty** - lub równoważną (co najmniej w zakresie będących przedmiotem zamówienia). Wymagane **dołączenie do oferty** oświadczenia Producenta lub Wykonawcy potwierdzając,że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego przedłużenia tego okresu do 4 lub 5 lat od daty dostawy. Sposób realizacji usług wsparcia technicznego: • Telefoniczne zgłaszanie usterek w dni robocze w godzinach pracy urzędu tj. 8-17. • Dedykowany bezpłatny portal online producenta lub wykonawcy do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. • Opcjonalna pomoc techniczna za pośrednictwem czat online. Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzien roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.

	Mozliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym. 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.
Monitor	
Proporcje obrazu	16:9
Przekątna ekranu	23.8"
Powierzchnia matrycy	Matowa
Technologia podświetlania	Diody LED
Rozdzielczość	Minimum 1920 x 1080 (FHD 1080)
Jasność	Minimum 250 cd/m²
Kontrast statyczny	1 000:1
Kąt widzenia poziomy	178 °
Kąt widzenia pionowy	178 °
Ilość kolorów	Min.16 mln
Gniazda we/wy	Min. 1 x 15-pin D-Sub Min. 1 x HDMI/DP Min. 2 x USB
Regulacja wysokości	Tak
Technologia eliminująca migotanie obrazu	Tak
Technologia niskiej emisji światła niebieskiego	Tak
Certyfikaty	Energy Star
Standard VESA	Tak

Klasa energetyczna	Min. C
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta lub wykonawcy, umożliwiający Zamawiającemu zgłaszanie awarii. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta lub wykonawcę (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy **załączyć do oferty**, lub równoważnymi (co najmniej w zakresie będących przedmiotem zamówienia). Wymagane **dołączenie do oferty** oświadczenia Producenta lub Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego przedłużenia tego okresu do 4 lub 5 lat od daty dostawy. Sposób realizacji usług wsparcia technicznego: • Telefoniczne zgłaszanie usterek w dni robocze w godzinach pracy urzędu, tj. 8-17. • Dedykowany bezpłatny portal online producenta lub wykonawcy do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. • Opcjonalna pomoc techniczna za pośrednictwem czat online. Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzien roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta lub wykonawcy. Mozliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta lub wykonawcy również dla urządzeń z nieaktywnym wsparciem technicznym. 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. .

Oprogramowanie biurowe – ilość licencji – 6 szt.

W ramach zamówienia Wykonawca dostarczy opgramowanie biurowe Office Home & Business 2021 lub równoważne, z licencją dożywotnią, tzw. Box z kluczem, w ilości 6 sztuk.

Jako równoważne Zamawiający dopuszcza inne oprogramowanie biurowe spełniające następujące wymagania:

- zawierające edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji, program pocztowy.

- poszczególne komponenty oprogramowania muszą zapewniać pełną kompatybilność przy wymianie dokumentów z posiadanym przez Zamawiającego oprogramowaniem MS Office Professional 2007/2010/2013/2016/2019/2021, w tym obsługę makr zagnieżdżonych w dokumentach,

- klient pocztowy będący częścią pakietu ma zapewniać pełną integrację z posiadanym przez Zamawiającego MS Exchange 2013,
- interfejs użytkownika w języku polskim,
- relacyjna baza danych.

Urządzenie do tworzenia kopii zapasowych typu NAS – 1 szt.

Komponent	Minimalne wymagania
Procesor	Procesor 64 bit x86 o taktowaniu nie mniejszym niż 2.0 GHz
Procesor liczba rdzeni	Minimum 4
Typ urządzenia	Urządzenie typu NAS
Pamięć RAM	Minimum 8GB
Pamięć Flash	Minimum 4GB
Liczba zatok na dyski	Minimum 4 x 3,5”
Zainstalowane dyski	Minimum 4 x 6TB 3,5 ``(min. 7200 obr./min)
Obsugiwane dyski	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD
Wbudowane w urządzenie interfejsy na dyski M2	2 x M2 PCIe Gen3x2
Możliwość stosowania dysków twardych o pojemności	Do 20 TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 x RJ-45
Diody LED	Status, LAN, HDD
Porty USB 3.2 Gen2	Minimum 2 szt.
Port HDMI	Tak, minimum 2
Przyciski Typ obudowy	Reset, Zasilanie Tower
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.

Zasilacz	Max. 90 W
Oprogramowanie	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa MPIO Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu Obsługa Windows AD	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,

Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja Konteneryzacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS

	FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata

Dyski rezerwowe do urządzenia do tworzenia kopii zapasowych – 4 szt.

Komponent	Minimalne wymagania
Dysk twardy	4 x 6TB 3,5 ``(min. 7200 obr./min)
Inne	Dyski twarde muszą współpracować z zaoferowanym urządzeniem do tworzenia kopii zapasowych typu NAS

Oprogramowania do tworzenia kopii zapasowych – 1 licencja

Komponent	Minimalne wymagania
Wymagania ogólne	● Oprogramowanie ma być dostarczane w wersji On-premise. ● Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud. ● Interfejs systemu dostępny jest w języku: ○ polskim, ○ angielskim, ● Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych, ● Oprogramowanie może być uruchomione w kontenerze docker, ● Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: ○ Debian: 9+

Zarządzanie	- Ubuntu: 16.04+ - Fedora: 29+ - centOS: 7+ - RHEL: 6+ - openSUSE: 15+ - SUSE Enterprise Linux (SLES): 12 SP2+ - Windows Client: 7, 8.1, 10 (1607+) - Windows Server: 2008 R2+, - System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, - Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),
	- Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli dostępnej z poziomu przeglądarki internetowej, - Zarządzanie całym systemem poprzez dashboardy, - Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego, - System posiada wbudowane predefiniowane zadania backupowe, - System umożliwia tworzenie zadań backupowych w oparciu o kalendarz. - Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, - Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem, - Monitorowanie postępu działania zadania, - Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach: - Zadanie zostało zakończone pomyślnie, - Zadanie zostało zakończone z ostrzeżeniami,

- Zadanie zostało zakończone z błędem,
- Zadanie zostało anulowane,
- Zadanie nie zostało uruchomione.

- System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
- Możliwość zdefiniowania okna backupowego dla każdego z zadań,
- Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
- System pozwala na klonowanie planów kopii zapasowych,
- System umożliwia reset hasła administratora w przypadku jego utraty,
- Oprogramowanie umożliwia definiowanie retencji według schematów:
  - GFS(Grandfather-Father-Son),
  - FIFO(First-In, First-Out).
- Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,
- Konta użytkowników mogą być tworzone poprzez import pliku CSV,
- Oprogramowanie umożliwia tworzenie grup urządzeń,
- Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
- System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:
  - System Administrator,
  - Backup operator,
  - Restore operator,
  - Viewer

Składowanie danych	• Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie z poziomu jednej konsoli,
	• System umożliwia składowanie danych:
	  ○ Lokalnie:
	  ■ Zasób SMB,
	  ■ Zasób NFS,
	  ■ Zasób ISCSI,
	  ■ Zasób S3,
	  ■ Katalog zabezpieczonego urządzenia.
	  ○ W chmurze:
	  ■ Amazon Web Service,
	  ■ Magazyn zgodny z S3,
	  ■ Dostarczanej bezpośrednio przez producenta.
	• System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
	System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle

Odtwarzanie	• Odtwarzanie granularne:
	  ○ Pojedynczych plików z kopii obrazu dysku,
	  ○ Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,
	• Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
	  ○ Windows: 7+,
	  ○ Windows Server: 2008 R2+,
	• Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym

	komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. ● Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a, ● Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V. ● Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK), ● Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL), ● Odtwarzanie zasobów plikowych z prawami dostępu, ● Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows), ● Odtwarzanie danych według harmonogramu, ● Przywracanie danych z określonego urządzenia/użytkownika, ● Przywracanie kopii z wybranego magazynu. ● Przywracanie danych Microsoft 365: ○ do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku: ■ pst, ■ mbox. ○ do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji), ● System posiada możliwość nieodwracalnego kasowania danych, ● Przywracanie repozytoriów GIT: ○ Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket), przywracanie między kontami
Backup	● Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla: ○ Systemów operacyjnych: ■ Alpine 3.10+,

	■ Debian: 9+, ■ Ubuntu: 16.04+, ■ Fedora: 29+, ■ centOS: 7+, ■ RHEL: 6+, ■ openSUSE: 15+, ■ SUSE Enterprise Linux(SLES): 12 SP2+, ■ macOS: 10.13+, ■ Windows: 7, 8.1, 10(1607+), ■ Windows Server: 2008 R2+, ○ Środowisk wirtualnych: ■ Hyper-V, ■ VMware: 6.7+. ■ Dowolne inne w sposób agentowy ○ Repozytoriów GIT: ■ GitHub, ■ Bitbucket. ● Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla: ○ Baz danych: ■ Microsoft SQL, ■ MySQL, ■ PostgreSQL, ■ Firebird, ■ Dowolnych innych przez podpięcie skryptów pre/post. ● Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: ○ 128 bit,

	○ 192 bit, ○ 256 bit. ● Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: ○ ZStandard, ○ LZ4. ● Oprogramowanie umożliwia zarządzanie poziomem kompresji, ● Wykonywanie kopii zapasowej otwartych plików(VSS), ● System umożliwia uruchamianie skryptów przed i po backupie, ● System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, ● System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów, ● Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT, ● Backup plikowy, ● Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, ● Oprogramowanie umożliwia konsolidację wersji kopii zapasowych, ● Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia, ● Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego. ● Oprogramowanie pozwala na backup zaszyfrowanych partycji.
GIT	● Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych), Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).
Licencjonowanie	● Sposób licencjonowania opiera się na: ○ Ilości serwerów/endpointów- dla fizycznych urządzeń, ○ Ilości fizycznych hostów - dla środowisk wirtualnych,

	○ Ilości repozytoriów - dla GIT. ● Licencje w wersji wieczystej powinny pozwalać na : ○ ...fizycznych endpointów, ○ ...fizycznych hostów maszyn wirtualnych, ○ ...fizycznych serwerów. ● Wsparcie techniczne: o Świadczone jest w języku polskim, bezpośrednio przez producenta, o Zapewnia dostęp do aktualizacji oprogramowania, o Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, o Obowiązuje przez okres 12 miesięcy

Urządzenie klasy UTM – 1 szt.

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 4 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.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN 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 Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix 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 oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. 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.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. 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.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. 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.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL 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, oznaczeń Type of Service w nagłówkach IP).
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. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
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 chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. 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. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. 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.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. 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.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i 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 dwu-składnikowego 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.

Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall lub rekomendacja respektowana przez NATO i Unię Europejską NATO Restricted i UE Restricted.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

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

1) 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. Wymagana jest odpowiednia licencja.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres [x] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Wymagany serwis 24x7.

Skaner – 3 szt.

Komponent	Minimalne wymagania
Typ skanera	Płaski
Rozdzielczość optyczna	Min. 2400 x 2400
Moduł skanujący	CIS
Maksymalny format skanowania	A4 /Letter (216 x 297mm)

Prędkość skanowania	Poniżej 15ms na linię (2400 dpi) (kolor) Poniżej 4,5ms na linię (2400 dpi)(czarno biały)
Interfejs	USB2.0 High-Speed Mini-B
Pobór mocy	Poniżej 5W (maks. podczas pracy) poniżej 0,5W (w trybie gotowości)
Obsługiwane systemy operacyjne	Windows 10, Windows 8.1, Windows 7 z dodatkiem SP1 Działanie można zagwarantować tylko w przypadku komputerów z fabrycznie zainstalowanym systemem Windows 7 lub nowszym. OS X 10.11.6, macOS 10.12–10.13
Gwarancja	24 m-ce

Zestaw do przeprowadzania wideokonferencji (kamera+słuchawki) – 3 szt.

Słuchawki

Komponent	Minimalne wymagania
Łączność	Przewodowa
Budowa	Nauszne , Półotwarte
System audio	Stereo 2.0
Redukcja hałasu	Pasywna
Średnica membrany	28mm
Pasmo przenoszenia	20 ~ 20000 Hz 150 ~ 7000 Hz
Czułość	Poniżej 95dB
Regulacja głośności	TAK
Wbudowany mikrofon	TAK , przy słuchawce
Czułość mikrofonu	- 44DB
Złącze	Minijack 3,5 mm - 1 szt. USB - 1 szt.
Kompatybilność	Z systemem Windows
Funcjonalność	Regulacja głośności Przełącznik wyciszania mikrofonu Możliwość wyciszania mikrofonu

	Redukcja szumów otoczenia w mikrofonie Pilot zdalnego sterowania na kablu Odbieranie połączeń Sterowanie muzyką
Waga	Poniżej 200 g
Gwarancja	24 m-ce

Kamera do widekonferencji:

Komponent	Minimalne wymagania
Typ podłączenia	min. USB 2.0
Typ sensora	CMOS
Rozdzielczość	Min. 1920 x 1080
Wbudowany mikrofon	tak
Zasilanie	Przez port USB
Kąt widzenia	Min. 70 stopni
Kompresja wideo	Co najmniej do MJPEG
Długośc kabla	Min. 1,5m