

Załącznik Nr 4c – Szczegółowy Opis Przedmiotu Zamówienia w odniesieniu do Części III zamówienia.

1) Serwer typu Tower – 1 szt.

Komponent	Minimalne wymagania
Obudowa	<ul style="list-style-type: none"> Obudowa typu Tower z możliwością instalacji do 8 dysków twardych 3.5”.
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością instalacji jednego fizycznego procesora, Płyta główna posiadająca minimum 4 sloty na pamięć RAM UDIMM, z możliwością zainstalowania minimum 128GB pamięci RAM. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	<ul style="list-style-type: none"> Zainstalowany jeden procesor 8-rdzeniowy klasy x86, min. 3.0GHz, 24M Cache, TDP max 80W
Pamięć RAM	<ul style="list-style-type: none"> 4x 32GB UDIMM 5600MT
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 2x dysk SAS o pojemności 600GB, Hot-Plug 2x dysk SAS o pojemności 2.4TB, Hot-Plug 4x dysk SSD SAS o pojemności 1.92TB, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 NVMe o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Sloty PCI Express	<ul style="list-style-type: none"> Cztery sloty PCIe
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> Minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT Dwuportowa karta sieciowa 10Gb Ethernet w standardzie BaseT
Wbudowane porty	<ul style="list-style-type: none"> Minimum 8 portów USB z czego min. 4 w technologii 3.0 1x RS-232 1x VGA
Video	<ul style="list-style-type: none"> Zintegrowana karta graficzna, umożliwiającą wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Zasilanie	<ul style="list-style-type: none"> Redundantne zasilacze o mocy 700W klasy Titanium
Diagnostyka i Bezpieczeństwo	<ul style="list-style-type: none"> zintegrowany z płytą główną moduł TPM 2.0 Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

	<ul style="list-style-type: none"> • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń.
System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> • Windows Server 2025 Standard – licencja dobrana tak, aby przy oferowanym procesorze umożliwić uruchomienie 4 maszyn wirtualnych • Nośnik CD/DVD z plikiem instalacyjnym Windows Server 2025 Standard • 10x licencja dostępowa Windows Server 2025/2022 User CALs
Karta Zarządzania	<ul style="list-style-type: none"> • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika ○ możliwość podmontowania zdalnych wirtualnych napędów ○ wirtualną konsolę z dostępem do myszy, klawiatury ○ wsparcie dla IPv6 ○ wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ integracja z Active Directory ○ możliwość obsługi przez ośmiu administratorów jednocześnie ○ Wsparcie dla automatycznej rejestracji DNS ○ wsparcie dla LLDP ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ możliwość podłączenia lokalnego poprzez złącze RS-232. ○ możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. ○ Monitorowanie zużycia dysków SSD ○ możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ Możliwość przywrócenia poprzednich wersji firmware

	<ul style="list-style-type: none"> Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. Możliwość wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI. <p>Możliwość rozszerzenia funkcjonalności karty o:</p> <ul style="list-style-type: none"> możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania Automatyczne odświeżanie certyfikatów SSL możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> 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

	<ul style="list-style-type: none"> ○ 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 przejścia 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. ○ Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:
--	--

	<ul style="list-style-type: none"> ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> • Monitoring: <ul style="list-style-type: none"> ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu

	<ul style="list-style-type: none"> ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware <ul style="list-style-type: none"> ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty <ul style="list-style-type: none"> ○ Możliwość generowania raportów dla serwerów zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym
--	--

	<p>systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej</p> <ul style="list-style-type: none"> ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF <ul style="list-style-type: none"> • Cyberbezpieczeństwo <ul style="list-style-type: none"> ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia <ul style="list-style-type: none"> ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent <ul style="list-style-type: none"> ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności <ul style="list-style-type: none"> ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne <ul style="list-style-type: none"> ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android • Certyfikaty <ul style="list-style-type: none"> ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: <ul style="list-style-type: none"> ▪ ISO 27001 ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization ▪ CSA Cloud Control Matrix
--	--

Certyfikaty	<ul style="list-style-type: none"> Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 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, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja użytkownika	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / 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. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:

	<ul style="list-style-type: none"> ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
--	---

2) Urządzenia bezpieczeństwa sieciowego typu UTM wraz z systemem logowania – 1szt.

Obsługa sieci

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

Zapora korporacyjna (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, 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.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

Intrusion Prevention System (IPS)

13. 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.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. 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.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. 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.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. 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).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

Kształtowanie pasma (traffic shapping)

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

Ochrona antywirusowa

27. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.
28. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
29. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
30. Skaner antywirusowy ma pochodzić od europejskiego producenta.
31. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
32. 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

33. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
34. Ochrona antyspam ma działać w oparciu o:
 - a. białe/czarne listy,
 - b. DNS RBL,
 - c. Skaner heurystyczny.
35. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
36. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

Wirtualne sieci prywatne (VPN)

37. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
38. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
 - a. PPTP VPN,
 - b. IPSec VPN,
 - c. SSL VPN.
39. SSL VPN ma działać w trybie tunelu.
40. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
41. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
42. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
43. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
44. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

Filtr dostępu do stron www

45. Urządzenie ma posiadać wbudowany filtr URL.
46. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
47. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
48. Administrator ma mieć możliwość dodawania własnych kategorii URL.
49. 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.
50. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
51. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
52. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
53. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
54. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
55. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

Uwierzytelnianie

56. 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.
57. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
58. 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.
59. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
60. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
61. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
62. 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).
63. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
64. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
65. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

Administracja łączami do internetu (ISP)

66. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
67. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
- a. równoważenie względem adresu źródłowego,
 - b. równoważenie względem połączenia.
68. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
69. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
70. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
71. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).

72. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

Routing (trasowanie)

- 73. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
- 74. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- 75. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
- 76. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
- 77. Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.

Administracja urządzeniem

- 78. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
- 79. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
- 80. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
- 81. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
- 82. 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.
- 83. Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH)
- 84. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
- 85. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
- 86. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
- 87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
- 88. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
- 89. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
- 90. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
- 91. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
- 92. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

93. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
94. 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
95. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
96. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
97. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

Raportowanie

98. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
99. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
100. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
101. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
102. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
103. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
104. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
105. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
106. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

Pozostałe usługi i funkcje

107. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
108. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
109. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
110. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
111. 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).
112. Urządzenie ma posiadać usługę DNS Proxy.
113. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).

- 114. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
- 115. Urządzenie musi mieć zaimplementowane Open API.
- 116. 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.
- 117. 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

- 118. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
- 119. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
- 120. Urządzenie ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.

Parametry sprzętowe

- 121. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
- 122. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
- 123. Liczba portów Ethernet 2,5Gbps – min. 8.
- 124. Liczba portów światłowodowych 1Gbps – min. 1.
- 125. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
- 126. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
- 127. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
- 128. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
- 129. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
- 130. Liczba tuneli VPN IPSec – minimum 100.
- 131. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
- 132. Obsługa interfejsów 802.11q (VLAN) – minimum 128
- 133. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
- 134. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie ActivePassive.
- 135. Urządzenie nie ma limitu na liczbę użytkowników.
- 136. Liczba reguł filtrowania – minimum 8 192.

- 137. Liczba tras statycznego routingu – minimum 512.
- 138. Liczba tras dynamicznego routingu – minimum 10 000.
- 139. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
- 140. Urządzenie musi być wyposażone w moduł TPM.

System logowania:

Wymagania ogólne:

1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
2. Rozwiązanie musi zostać dostarczone w postaci maszyny wirtualnej instalowanej w środowisku Vmware lub Windows Hyper-V.
3. Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
4. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
5. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
6. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
7. Rozwiązanie musi posiadać predefiniowane panele dla informacji z urządzeń pracujących w sieci OT.

Zarządzanie Logami:

8. Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
9. Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
10. Rozwiązanie musi umożliwiać przysyłanie logów do innego serwera logów (funkcja syslog forwarder).
11. Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.

Rodzaje wyszukiwani

12. Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
13. Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
14. Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
15. Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).
16. Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów).

17. Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.

Raportowanie

- 18. Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
- 19. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
- 20. Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
- 21. Rozwiązanie musi umożliwiać tworzenie własnych raportów.
- 22. Rozwiązanie musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down”.

Zarządzanie incydentami

- 23. Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
- 24. Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.

Wymagania systemowe

- 25. Liczba zdarzeń na sekundę (EPS): min. 10 000
- 26. Zarządzanie logami: min 1 rok
- 27. Liczba obsługiwanych urządzeń min. 500
- 28. Liczba zapisu zdarzeń na dobę: min 13000 MB
- 29. System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV

3) Dysk sieciowy NAS – 1 szt.

Specyfikacja sprzętowa	
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB

Pamięć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 8 zatok 3,5"
Obsługiwane dyski twarde	3.5" SATA oraz 2.5" SATA oraz 2.5" SATA SSD
Możliwość stosowania dysków twardych o pojemnościach	do 22TB
Zainstalowane dyski twarde	8 szt + 2 dodatkowe dyski HotSpare (łącznie 10 szt) , po 8 TB każdy kompatybilne z oferowanym urządzeniem , z których każdy spełnia poniższe minimalne wymagania: Typ dysku HDD Format szerokości 3,5" (LFF) Typ napędu Wewnętrzny Pojemność dysku 8 TB Interfejs dysku SATA Prędkość obrotowa 5640 obr/min Bufor 256 MB TBW 180 TB Poziom hałasu 30 dB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Diody LED	Minimum Status, LAN, HDD,
Porty USB	Minimum 3 x typu A USB 3.2 Gen 2 10 Gb/s Minimum 1 x typu C USB 3.2 Gen 1 5 Gb/s
Port PCIe	Tak, minimum 2xGen 3x4
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 250 W
Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Wymagania dla systemu operacyjnego opartego o system plików EXT4	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak

Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu

VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXI 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

4) Przełącznik sieciowy – 1szt.

Klasa przełącznika	Zarządzalny
Warstwa przełączania	L2
Architektura sieci	GigabitEthernet
Liczba portów 10/100/1000/2500 Mbps	6
Liczba portów 10Gb	4
Liczba portów SFP+	2
Port konsoli	Tak
Przepustowość	110 Gb/s
Rozmiar tablicy adresów MAC	16000
Obsługa ramek Jumbo	Tak
Rozmiar ramki Jumbo	9 KB
Możliwość łączenia w stos	Nie
VLAN	<ul style="list-style-type: none"> • VLAN configuration • IEEE 802.1Q-based VLAN
Obsługiwane protokoły i standardy	<ul style="list-style-type: none"> • IEEE 802.3 Ethernet • IEEE 802.3u 100BASE-T • IEEE 802.3ab 1000BASE-T • IEEE 802.3bz 2.5G/5GBase-T • IEEE 802.3z 1000BASE-SX/LX • IEEE 802.3ae 10G Fiber • IEEE 802.3x Kontrola przepływu w pełnym duplexie • IEEE 802.1Q Oznaczanie VLAN • IEEE 802.1w RSTP • IEEE 802.3ad LACP • IEEE 802.1AB LLDP • IEEE 802.1p Klasa usługi
QoS	<ul style="list-style-type: none"> • Port-based QoS • IEEE 802.1p CoS • IPv4 DSCP-based QoS • IPv4 ToS-based QoS
Bezpieczeństwo	Access Control Lists (ACL): ACL by IP address, ACL by MAC

Zarządzanie, monitorowanie, konfiguracja	<ul style="list-style-type: none"> • Zarządzane przez stronę internetową • Status portu • Statystyki portu • Konfiguracja portu • Obsługa ramek jumbo • Kontrola przepływu IEEE 802.3x • Autonegocjacja prędkości i trybu duplexu • Aktualizacja oprogramowania sprzętowego na żywo (Firmware Live Update) • Ręczna aktualizacja oprogramowania sprzętowego (Firmware Manual Update) • Protokół LLDP (Link Layer Discovery Protocol): urządzenie zdalne LLDP • Interfejs: interfejs WWW (Web UI) • SNMP, DNS, klient DHCP • IEEE 802.1w Rapid Spanning Tree
Funkcje L2	<ul style="list-style-type: none"> • LACP • IGMP snooping v2
Typ obudowy	Rack
Wentylator	Tak
Zasilacz	Wewnętrzny
Pobór mocy	40 W
Wymagania środowiskowe	<ul style="list-style-type: none"> • Temperatura robocza: Od 0C do 40°C (od 32°F do 104°F) • Wilgotność względna: 5-95% bez kondensacji
Certyfikaty	<ul style="list-style-type: none"> • CE • FCC • VCCI • BSMI
Akcesoria w zestawie	<ul style="list-style-type: none"> • Kabel zasilający • Zestaw do montażu w szafie rack • Instrukcja obsługi

5) UPS do serwera – 1szt.

Nazwa elementu, parametru lub cechy	Opis wymagań
Moc pozorna	2200 VA
Moc czynna	2200 W
Architektura UPS-a	line-interactive



Kształt napięcia wyjściowego	Pełna sinusoida
Liczba faz na wejściu	1 (230V)
Czas transferu (maks.)	4 ms
Czas ładowania	3 h
Typ obudowy	Rack/ Tower
Zabezpieczenia / filtry	: Przeciwwprzebieżeniowe, Przeciwwprzepięciowe, Przeciwwzakłócenia
Oprogramowanie	do zarządzania zasilaniem
Porty zasilania we.	IEC-C20
Porty zasilania wy.	: 6 x IEC-C13, 2 x IEC-C19
Gniazda we/wy	: 1 x USB (Type B), 2 x RS-232 (COM), 2 x RJ-11/RJ-45, 1 x EPO
Wymagania środowiskowe	<ul style="list-style-type: none"> • Temperatura robocza: 32 ~ 104 (°F) • Temperatura robocza: 0 ~ 40 (°C) • Względna wilgotność robocza (bez kondensacji): 0 ~ 95 (%) • Wysokość robocza: 0-10 000 stóp (0-3000 metrów) (stopy/metry) • Temperatura przechowywania: 5 ~ 113 (°F) • Temperatura przechowywania: -15 ~ 45 (°C) • Względna wilgotność przechowywania (bez kondensacji): 0 ~ 95 (%) • Wysokość przechowywania (stopy/metry): 0-50 000 stóp (0-15 000 metrów) • Rozproszenie ciepła online: 116 (BTU/hr) • Słyszalny hałas od 1,0 M z powierzchni urządzenia: 38,5~57,5 (dbA)
Akcesoria w zestawie	<ul style="list-style-type: none"> • Szyny rack • Uchwyty rack • Zestaw szyn • Zestaw śrub • Przewód zasilający • Przewód USB • Przewód Serial • Przewód EPO • Instrukcja obsługi • Karta komunikacyjna spełniające następujące wymagania: <ul style="list-style-type: none"> ▪ Port łączności: RJ45, RJ45 (dla czujnika środowiskowego) ▪ Protokół łącza danych: Ethernet 100Base-TX, Ethernet 10Base-T ▪ Obsługa instalacji typu Plug-and-play ▪ Oprogramowanie do zarządzania zasilaniem ▪ Możliwość aktualizacji Firmware przez użytkownika ▪ Zdalne zarządzanie: przeglądarka internetowa, Interfejs wiersza poleceń, NMS ▪ Zarządzanie lokalne: Interfejs sieciowy, Interfejs linii komend

	<ul style="list-style-type: none"> ▪ Powiadomienia o wydarzeniach: E-mail, komunikaty SNMP, Syslog, SMS ▪ Obsługiwane protokoły: IPv4/v6, SNMPv1/v3, HTTP/HTTPS, TCP/IP, UDP, DHCP, NTP, DNS, SMTP, SSH, SSL, TLS, Telnet, FTP i Syslog ▪ Uwierzytelnianie: RADIUS, LDAP, LDAPS, Windows AD ▪ Obsługa czujnika środowiskowego
Gwarancja	2 Lata

6) UPS dla stacji roboczych – 5szt.

Nazwa elementu, parametru lub cechy	Opis wymagań
Moc pozorna	900 VA
Moc rzeczywista	480 W
Technologia	Line-Interactive
Gniazda wyjściowe z podtrzymaniem baterijnym	typu FR, minimum 2szt
Przewód zasilający	Przymocowany na stałe do zasilacza UPS
Port komunikacyjny	USB umieszczony na przednim panelu zasilacza UPS
Wskaźnik stanu UPS	Dioda LED
Parametry wejściowe	
Napięcie znamionowe	220-240 V; 50/60 Hz
Zakres napięcia wejściowego	140-300 V; 45-65 Hz
Parametry wyjściowe	
Znamionowe napięcie wyjściowe	220/230/240 V
Regulacja napięcia w trybie baterijnym	+/-20%
Sprawność w trybie normalnym	>95%
Sprawność w trybie baterijnym	>60%
Regulacja częstotliwości w trybie normalnym	zgodnie z siecią zasilającą
Regulacja częstotliwości w trybie baterijnym	+/-1 Hz
Częstotliwość w trybie normalnym	zgodnie z siecią zasilającą
Częstotliwość w trybie baterijnym	50/60 Hz
Przebieżalność	[110%,120%] 5 min; >120% 1 s
Zdolność zwarciovą w trybie baterijnym	5A
Wytrzymywany czas przepływu prądu zwarciovego	50 ms
Czas przełączania	10 ms dla przejścia z trybu normalnego do trybu baterijnego
Bateria	
Specyfikacja	12 V DC – 1 x 12 V, 7 Ah
Typ	Valve Regulated Lead-Acid (VRLA) szczelne, bezobsługowe, z minimalną żywotnością 3-5 lat w temperaturze 25°C
Monitoring	Zaawansowany monitoring z wczesnym wykrywaniem awarii oraz powiadamianiem.

Zimny start	Tak
Parametry środowiskowe i bezpieczeństwo	
Normy	IEC/EN 62040-1 Safety
	IEC/EN 62040-2 Electromagnetic Compatibility EMC
	IEC/EN 62040-3 Performance
EMC (emisyjność)	CISPR32 Class A
	IEC/EN 61000-3-2 Flickers
	IEC/EN 61000-3-3 Harmonics
EMC (odporność)	IEC 61000-4-2, (ESD): 4 kV Contact Discharge / 8 kV Air Discharge
	IEC 61000-4-3, (Radiated field): 10 V/m
	IEC 61000-4-4, (EFT): 4 kV
	IEC 61000-4-5, (Surges): 1 kV Differentiel Mode / 2 kV Common Mode
	IEC 61000-4-6, (Electromagnetic field): 10 V
	IEC 61000-4-8, (Conducted magnetic field): 30 A/m
Oznaczenia	CE, EAC, Cm, Ukr, UKCA,
Stopień ochrony	IP20
Układ sieci	UPS można podłączyć do układów zasilania TN, TT, IT, ten sam system jest dostarczany do obciążenia.
Klasa ochronności	Klasa I
Temperatura pracy	0°C do 40°C (32°F do 104°F)
Temperatura przechowywania	0°C do 40 °C (32°F do 104 °F) z baterią
	-25°C do 55 °C (-13°F do 131 °F) bez baterii
Wilgotność względna	Przechowywanie: 0-93% bez kondensacji
	Praca: 0-85% bez kondensacji
Wysokość n.p.m. podczas pracy	2000 m
Wysokość n.p.m. podczas transportu	Do 10000 m (32,808 ft) nad poziomem morza
Poziom hałasu	<25 dBA
Gwarancja	24 miesiące