

Gmina Łask
ul. Warszawska 14
98-100 Łask

Nasz znak: OOG.271.4.3.2024

Łask, dnia 12 Listopada 2024 r.



OPIS PRZEDMIOTU ZAMÓWIENIA

**Dostawa sprzętu i oprogramowania informatycznego z wdrożeniem
w ramach konkursu grantowego „Cyberbezpieczny Samorząd”
dla Urzędu Miejskiego w Łasku
(ZADANIE 1 i 2)**

Spis treści

1. Wstęp	3
2. Serwery (2 szt.)	5
3. Serwerowy system operacyjny (SSO)	14
4. Macierz dyskowa (1 sztuka).....	16
5. Oprogramowanie NAC wraz ze wsparciem technicznym na okres 24 miesięcy	18
6. Przełączniki sieciowe 48p (7 sztuk).....	27
7. Przełączniki sieciowe 24p (1 sztuka).....	33
8. Zasilacz awaryjny UPS 60kVA z instalacją (1 sztuka)	40
9. Wdrożenie	42
9.1. Serwery z macierzą.....	42
9.2. Instalacja i konfiguracja systemu dla obsługi oprogramowania zarządzającego kopiami bezpieczeństwa	43
9.3. Segmentacja sieci, podział na VLAN-y	43
9.4. Konfiguracja systemu kontroli dostępu do sieci.	43
9.5. Przełączniki sieciowe	43
9.6. Konfiguracja systemu UTM Firewall.....	44
9.7. Wdrożenie systemu zarządzania siecią	44
9.8. Testy powdrożeniowe	44
10. Wymagania od Wykonawcy	45

1. Wstęp

W ramach zadania Wykonawca dostarczy sprzęty i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia zgodnego z opisem w sekcji „**Wdrożenie**”.

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
- Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą się znajdować na liście „end-of-sale” oraz „end-of-support” producenta.
- Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem);
- Zamawiający wymaga, by dostarczone licencje na oprogramowanie i systemy operacyjne były nowe i nie były nigdy wcześniej aktywowane czy używane na innych urządzeniach;
- Musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczypospolitej Polskiej;
- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów sprzętu.
- Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku bankructwa Wykonawcy niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
- Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V \pm 10%, 50Hz;
- W cenę musi być wliczony koszt dostawy - transportu;
- Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego w dni powszednie w godzinach 8-15;
- Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania;
- Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne.

Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:



- a) połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
- b) łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
- c) zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
- d) wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem.

2. Serwery (2 szt.)

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none">Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5"Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.Obudowa z możliwością wyposażenia w kartę umożliwiającą 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/ WIFI.
Płyta główna	<ul style="list-style-type: none">Płyta główna z możliwością zainstalowania do dwóch procesorów.Obsługa procesorów 56 rdzeniowych.Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci.Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	<ul style="list-style-type: none">Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	<ul style="list-style-type: none">Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.9GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 24500 w teście Average CPU Mark, dostępnym na stronie www.cpubenchmark.net.
RAM	<ul style="list-style-type: none">Minimum 512GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	<ul style="list-style-type: none">Demand Scrubbing,Patrol Scrubbing,Permanent Fault Detection
Gniazda PCI	<ul style="list-style-type: none">minimum trzy sloty PCIe LP
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none">Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)Dwuportowa karta 32GB FC2 wkładki 25GbE SFP28 SR (dual rate – 10/25GbE)
Dyski twarde	<ul style="list-style-type: none">Zainstalowane:<ul style="list-style-type: none">2x dysk SSD SATA o pojemności min. 480GB, Hot-PlugMożliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Kontroler RAID	<ul style="list-style-type: none">Sprzętowy kontroler dyskowy, posiadający<ul style="list-style-type: none">Min. 8GB nieulotnej pamięci cache,

	<ul style="list-style-type: none"> Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Wbudowane porty	<ul style="list-style-type: none"> 4x USB, w tym min. 1 port micro USB na panelu przednim i 1 porty USB 3.0 2x port VGA (jeden na panelu przednim) Możliwość rozbudowy o Serial Port
Video	<ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	<ul style="list-style-type: none"> Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> Windows Server 2025 Datacenter z możliwością Downgrade do poprzednich wersji 120x Windows Server 2025/2022 Device CALs (ilość licencji dotyczy całego proponowanego rozwiązania a nie pojedynczej sztuki serwera) <p>lub rozwiązanie równoważne - Szczegółowy opis pkt. 3. Serwerowy system operacyjny (SSO)</p>
Bezpieczeństwo	<ul style="list-style-type: none"> Zatrask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 V3 Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem 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).
Karta Zarządzania	<ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> 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 autentykację i autoryzację użytkownika; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy, klawiatury;

	<ul style="list-style-type: none"> ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
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 ○ 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

	<ul style="list-style-type: none"> ○ 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.
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. 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

	<ul style="list-style-type: none"> ○ 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 systemu 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 ▪ 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
--	--

	<ul style="list-style-type: none"> ▪ 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 systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ 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 • 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
--	---

	<ul style="list-style-type: none"> ○ 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 deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	<ul style="list-style-type: none"> • Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

	<ul style="list-style-type: none"> 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 min. 3 lat. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) 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. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. 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 oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. 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 zgłoszenia 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.

	<ul style="list-style-type: none"> ○ 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 przekaze dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wystanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. ● Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. ● Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
--	--

3. Serwerowy system operacyjny (SSO)

Dla każdego oferowanego serwera należy dostarczyć serwery system operacyjny (SSO) spełniający poniższe wymagania:

Wymagane minimalne parametry techniczne	
Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i nieograniczonej liczby środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.	
Wymaga się dostarczenia licencji dla klastra 2 serwerów, dwuprocesorowych, każdy procesor posiada 8 rdzeni a nieograniczoną liczbę systemów OSE.	
Jeżeli system operacyjny wymaga licencji dostępowych należy dostarczyć licencję dla 120 urządzeń.	
Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy.	
1	Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym.
2	Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
3	Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
4	Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7	Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8	Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
9	Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ul style="list-style-type: none"> • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, • umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10	Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11	Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12	Posiada możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
13	Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14	Posiada wbudowaną zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15	Graficzny interfejs użytkownika.
16	Zlokalizowane w języku polskim, następujące elementy: <ul style="list-style-type: none"> • menu, • przeglądarka internetowa, • pomoc, • komunikaty systemowe.
17	Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

18	Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
21	<p>Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none">• Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,• Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:<ul style="list-style-type: none">• Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,• Ustawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,• Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.• Zdalna dystrybucja oprogramowania na stacje robocze.• Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej• Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:<ul style="list-style-type: none">• Dystrybucję certyfikatów poprzez http• Konsolidację CA dla wielu lasów domeny,• Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen.• Szyfrowanie plików i folderów.• Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).• Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.• Serwis udostępniania stron WWW.• Wsparcie dla protokołu IP w wersji 6 (IPv6),• Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,• Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla:<ul style="list-style-type: none">• Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,• Obsługi ramek typu jumbo frames dla maszyn wirtualnych,• Obsługi 4-KB sektorów dysków,• Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,• Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) <p>Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p>
22	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
23	Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24	Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25	Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

4. Macierz dyskowa (1 sztuka)

Lp.	Nazwa parametru	Minimalna wartość parametru
1.	Obudowa	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19".
2.	Pojemność:	<p>System musi zostać dostarczony w konfiguracji zawierającej minimum:</p> <p>15 dysków 1.9TB NVME</p> <p>System musi ponadto wspierać dyski:</p> <ul style="list-style-type: none"> - NVME: od 1.9TB do 15TB - SSD, NL-SAS: od 1.9TB do 22TB <p>System musi mieć możliwość rozbudowy do minimum 250TB przestrzeni RAW NVME oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami) jeżeli istnieje model wyższy. Jeżeli nie istnieje model wyższy zamawiający wymaga dostarczenia macierzy z 256GB Cache.</p> <p>Macierz musi mieć możliwość rozbudowy o dyski HDD tj. NL-SAS oraz dyski flash łączone po 12Gb SAS (SSD). Obsługa dysków HDD może się odbywać poprzez dołożenie dodatkowej półki dyskowej, zarządzanie całą przestrzenią dyskową (NVMe oraz NL-SAS lub SAS) musi się odbywać przez te same dwa kontrolery macierzy.</p>
3.	Kontroler	<p>Dwa kontrolery wyposażone w przynajmniej 16GB cache każdy.</p> <p>System musi pozwalać na rozbudowę do 256GB Cache.</p> <p>W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.</p>
4.	Interfejsy	<p>Oferowana macierz musi mieć minimum:</p> <ul style="list-style-type: none"> • 8 portów 32Gb FC • 4 porty SAS 12Gb <p>System musi pozwalać na wymianę lub rozbudowę ww. portów na porty:</p> <ul style="list-style-type: none"> • 100Gb NVMe over InfiniBand lub NVMe over RoCE • 25GbE <p>System musi wspierać rozbudowę o porty SAS dla zewnętrznych półek dyskowych oraz na wymianę portów na 25/100GbE</p>
5.	RAID	<p>Wsparcie dla RAID: 0, 1, 5, 6, 10</p> <p>Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych w tym 15TB SSD.</p> <p>Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w</p>

		sposób sprzętowy przez dedykowany układ w macierzy.
6.	Obsługiwane protokoły	<p>FC, iSCSI, NVMe Over FC, RoCE, Infiniband, S3, CIFS, NFS</p> <p>Zamawiający dopuszcza zrealizowanie protokołu CIFS, NFS i S3 za pomocą zewnętrznego oprogramowania typu Software Defined Storage. Zamawiający wymaga opisanie za pomocą jakiego oprogramowania i w jaki sposób zostaną zapewnione w/w funkcjonalności.</p>
7.	Inne wymagania	<p>Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów:</p> <p>Microsoft® Windows Server®, Red Hat Enterprise Linux®, Novell SUSE Linux Enterprise Server, VMware® ESX®, Oracle® Solaris, HP HP-UX, IBM AIX,</p> <p>Macierz musi posiadać funkcjonalność wykonywania snapshotów minimum 128 per wolumen.</p> <p>Macierz musi posiadać funkcjonalność klonowania danych</p> <p>Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie</p> <p>Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji.</p> <p>Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online wolumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.</p> <p>Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID</p> <p>Z poziomu graficznego interfejsu do zarządzania istnieje możliwość sprawdzenia stanu zużycia dysków flash.</p> <p>Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków</p> <p>Wraz z systemem musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:</p> <ul style="list-style-type: none"> wydajności i opóźnień na wolumenach wydajności I/Ops, MB/s trafności w cache <p>Macierz musi docelowo pozwalać na osiągnięcie 600 000 IOPS przy ruchu random dla bloku 8KB 100% odczytów.</p> <p>Zamawiający wymaga dostarczenia oficjalnego dokumentu od producenta potwierdzającego spełnienie w/w wymogu.</p> <p>Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem uwierzytelniania i dostępu dla użytkowników/administratorów.</p>

		<p>Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z:</p> <ul style="list-style-type: none"> • Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter • VMware VASA • Microsoft <p>Macierz musi zapewniać możliwość szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.</p> <p>Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy.</p>
8.	Gwarancja i serwis	<p>Min. 2 lata serwisu producenta lub partnera serwisowego z 30 min czasem odpowiedzi na awarie krytyczne i dostawę elementów zastępczych na następny dzień roboczy od diagnozy problemu.</p> <p>Zepsute nośniki pozostają własnością zamawiającego</p>
9.	Punktacja	<p>Zamawiający wymaga, aby zaoferowane urządzenia były uznanymi rozwiązaniami na świecie – producent zaoferowanego rozwiązania musi być notowany w raportach Gartnera dla rozwiązań "Primary Storage" nie starszych niż 2 lata przed złożeniem oferty i być wymieniony w grupie liderów (ang. Leaders). Jako równoważny dla raportu Gartnera Zamawiający dopuści również inny raport udostępniany publicznie, powszechnie akceptowany, mający charakter zewnętrznego i obiektywnego raportu standaryzacyjnego, który zapewnia analizę, wgląd w kierunek oraz dojrzałość uczestników rynku w rozwiązaniach typu Primary Storage, aktualizowany co roku od min. 20 lat</p>

5. Oprogramowanie NAC wraz ze wsparciem technicznym na okres 24 miesięcy

Podstawowa funkcjonalność systemu NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.

8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
 - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
 - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
 - serwera RADIUS dla infrastruktury sieciowej,
 - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
 - serwera SYSLOG,
 - serwera TACACS+,
 - serwera Monitoringu,
 - serwera DHCP,
 - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
 - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.

20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.

38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.

59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:

- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
- Czy włączony jest firewall
- Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
- Czy jest włączone szyfrowanie dysku systemowego
- Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
- Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
- Czy w systemie są uruchomione procesy wskazane przez administratora
- Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
- Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
 - Wartości klucza rejestru
 - Typu wartości: Number, String, Version

60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.

61. System musi współpracować z serwerem tokenów.

62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfigurator sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:

- Microsoft Windows
- Mac OS
- iOS
- Android

63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfigurator sieci).

64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
 - MAC,
 - PAP/ASCII,
 - CHAP,
 - SNMP,
 - 802.1X.

3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
 - Tożsamość/Urządzenie końcowe,
 - Grupa tożsamości/urządzeń końcowych,
 - Parametry urządzeń końcowych, min: system operacyjny, wersja,
 - Atrybuty Active Directory,
 - Jednostka organizacyjna tożsamości/urządzeń końcowych,
 - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
 - Grupy urządzeń sieciowych,
 - Porty urządzeń sieciowych,
 - Grupy portów urządzeń sieciowych,
 - Jednostka organizacyjna portów,
 - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
 - Data, czas ważności polityki,
 - Wewnętrzny Captive Portal,
 - Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów NMAP, SNMP, DHCP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.

16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
20. System musi umożliwiać przysyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
 - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
 - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
 - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
 - usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
 - Uruchamianie usługi dla wybranych podsieci,
 - Przypisanie ustalonego adresu IP dla adresu MAC.
 - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
 - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
 - Możliwość określania braku dostępu dla wybranych adresów MAC,
 - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,

- Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
- Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
- Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
- Dokonywanie zmian bez konieczności wyłączenia usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostatnie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadanym adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.

12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
 - Logowania, wylogowania z system w tym błędne logowania
 - Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
 - wiadomości e-mail,
 - Syslog,
 - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
 - Ilości obsługiwanych transakcji RADIUS,
 - Opóźnienie obsługi transakcji RADIUS,
 - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
 - badanie łączności IP za pomocą ping, traceroute,
 - tcpdump protokołów RADIUS, TACACS+,
 - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
 - nazwy użytkownika,
 - adresu MAC,
 - statusu uwierzytelnienia (udana lub nieudana),
 - powodu, jeżeli uwierzytelnienie nieudane,
 - zakresu czasowego, co do dnia, godziny i minuty,
 - wykonanie zdalnego polecenia na urządzeniu sieciowym.

Licencja wsparcia technicznego producenta oprogramowania:

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 24 miesięczną licencję na wsparcie

producenta oprogramowania. Licencja ta powinna obejmować minimum:

- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej.
- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

6. Przełączniki sieciowe 48p (7 sztuk)

Wymagania podstawowe:

1. Przełącznik do sieci LAN w metalowej obudowie;
2. Wysokość urządzenia 1U - montaż w standardowej szafie 19";
3. Głębokość urządzenia nie większa niż 35 cm;
4. Przełącznik musi posiadać wbudowany zasilacz AC 230V;
5. Przełącznik wyposażony w min.:
 - 48 portów 10/100/1000BASE-T;
 - 8 portów SFP+ 1/10G.
6. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex;
7. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet;
8. Przełącznik musi wspierać obsługę diagnostyki wkładek SFP/SFP+;
9. Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów;
10. Przełącznik musi posiadać możliwość łączenia do 8 przełączników w stos;
11. Przepustowość stosu min. 40 Gb/s;
12. Możliwość budowy stosu za pomocą portów 10G SFP+;
13. Stos musi zachowywać się jako jedno urządzenie logiczne, a w szczególności musi mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem;
14. Nieblokująca architektura o wydajności przełączania min. 256 Gb/s;
15. Szybkość przełączania: 190.5 Mp/s;
16. Pamięć operacyjna: min. 1 GB pamięci DRAM;
17. Pamięć flash: min. 1 GB pamięci Flash;
18. Dedykowany port konsoli szeregowej RS-232 (RJ45);
19. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika;
20. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora;

21. Możliwość instalacji min. dwóch wersji oprogramowania – firmware;
22. Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash;
23. Możliwość monitorowania zajętości CPU;
24. Możliwość monitorowania zajętości pamięci;
25. Wsparcie mirroringu ruchu:
 - Lokalny mirroring na przełączniku;
 - Zdalny mirroring;
 - Zdalny mirroring do wskazanego adresu IP poprzez tunel - np. GRE;
 - Możliwość mirroringu ruchu wybranego za pomocą listy kontroli dostępu ACL.
26. Wsparcie diagnostyki okablowania - wykrywanie przerwy, zwarcia oraz odległości do awarii;

Funkcje L2 przełącznika:

27. Tablica MAC adresów min. 32 tys.;
28. Obsługa sieci wirtualnych IEEE 802.1Q - min. 4 tys.;
29. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieciowych;
30. Obsługa Q-in-Q IEEE 802.1ad;
31. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów);
32. Obsługa STP (Spanning Tree Protocol) IEEE 802.1D;
33. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w;
34. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s;
35. Obsługa PVST+ (Per-VLAN Spanning Tree Protocol);
36. Obsługa min. 64 instancji MSTP;
37. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP:
 - obsługa min. 128 grup łączy typu Link Aggregation;
 - obsługa umożliwiająca zgrupowanie min. 8 portów.
38. Obsługa MLAG (Multi Chassis Link Aggregation);
39. Obsługa protokołu EAPS - RFC 3619;
40. Obsługa protokołu ERPS / G.8032;
41. Obsługa Quality of Service:
 - Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p;
 - Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ;
 - 8 kolejek priorytetów na każdym porcie wyjściowym;
 - Obsługa kolejek Strict Priority;
 - Obsługa kolejek Weighted Round Robin;
 - Obsługa WRED (Weighted Random Early Detection);
42. Obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB;
43. Obsługa LLDP Media Endpoint Discovery (LLDP-MED);
44. Obsługa CDPv1 oraz CDPv2;
45. Przełącznik musi posiadać obsługę AVB (Audio Video Bridging);

46. Kontrola sztormów:

- Możliwość ograniczenia liczby pakietów Multicast na porcie;
- Możliwość ograniczenia liczby pakietów Broadcast na porcie;
- Możliwość ograniczenia liczby pakietów Unknown Unicast na porcie.

47. Przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP;

48. Wsparcie DCB (Data Center Bridging):

- DCBX - Data Center Bridging eXchange;
- PFC - Priority-based Flow Control;
- ETS - Enhanced Transmission Selection.

Funkcje L3 przełącznika IPv4:

49. Obsługa min. 1500 interfejsów IP;

50. Wsparcie dla IP multinetting - wiele adresów przypisanych do jednej sieci VLAN;

51. Sprzętowa obsługa routingu IPv4;

52. Pojemność sprzętowej tabeli routingu min. 12 tys. Wpisów;

53. Obsługa routingu statycznego IPv4;

54. Obsługa routingu dynamicznego IPv4:

- RIP v1/v2;
- OSPFv2 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję;
- BGPv4 min. 2 sąsiadów - możliwość rozszerzenia do pełnej funkcjonalności przez licencję;
- ISIS - możliwość rozszerzenia przez licencję.

55. Obsługa redundancji routingu VRRP dla IPv4;

56. Policy Based Routing dla IPv4;

57. Obsługa DHCP Relay;

58. Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów;

59. Obsługa Opcji 82 dla DHCP;

Funkcje L3 przełącznika IPv6:

60. Sprzętowa obsługa routingu IPv6;

61. Pojemność tabeli routingu min. 6 tys. wpisów;

62. Obsługa routingu statycznego IPv6;

63. Obsługa routingu dynamicznego IPv6:

- RIPng,
- OSPFv3 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję;
- BGPv4 min. 2 sąsiadów - możliwość rozszerzenia do pełnej funkcjonalności przez licencję;
- ISIS - możliwość rozszerzenia przez licencję.

64. Obsługa redundancji routingu VRRP dla IPv6;

65. Policy Based Routing dla IPv6;

- 66. Obsługa 6to4 (RFC 3056);
- 67. Opcja IPv6 Router Advertisement dla DNS - RFC 6106.

Obsługa ruchu rozgłoszeniowego:

- 68. Statyczne przyłączanie portu do grupy multicast;
- 69. Filtrowanie IGMP;
- 70. Obsługa IGMP v1 - RFC 1112;
- 71. Obsługa IGMP v2 - RFC 2236;
- 72. Obsługa IGMP v3 - RFC 3376;
- 73. Obsługa IGMP v1/v2/v3 snooping;
- 74. Obsługa PIM-SM;
- 75. Obsługa PIM-DM - możliwość rozszerzenia przez licencję;
- 76. Obsługa PIM-SSM - możliwość rozszerzenia przez licencję;
- 77. Obsługa MLDv1 snooping;
- 78. Obsługa MLDv2 snooping;
- 79. Obsługa MVR (Multicast VLAN Registration).

Funkcje bezpieczeństwa:

- 80. Obsługa logowania do sieci Network Login:
 - IEEE 802.1x based Network Login;
 - MAC address based Network Login;
 - Web based Network Login.
- 81. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants);
- 82. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation;
- 83. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x;
- 84. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication;
- 85. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink;
- 86. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na portach dołączonych do przełączników obsługujących IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging;
- 87. Automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA;
- 88. Automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA;

89. Przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA, np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który "przejmie" rolę uwierzytelniania klientów;
90. Obsługa Guest VLAN dla IEEE 802.1x;
91. Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci;
92. Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu - CoA RFC 5176;
93. Obsługa wymuszania ponownego okresowego uwierzytelnienia (Reauthentication);
94. Obsługa RADIUS Authentication (RFC 2865);
95. Obsługa RADIUS Accounting (RFC 2866);
96. Obsługa RADIUS Per-Command Authentication - uwierzytelnianie każdej komendy wydawanej przez administratora w serwerze RADIUS;
97. Obsługa RADIUS Authentication over TLS (RadSec);
98. Obsługa RADIUS Accounting over TLS (RadSec);
99. Obsługa TACACS+ (RFC 1492):
100. Bezpieczeństwo MAC adresów;
 - ograniczenie liczby MAC adresów na porcie;
 - zatrzaśnięcie MAC adresów na porcie;
 - możliwość wpisania statycznych MAC adresów na port/vlan;
101. Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning);
102. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4:
 - Adres MAC źródłowy i docelowy plus maska;
 - Adres IP źródłowy i docelowy plus maska dla IPv4;
 - Adres IP źródłowy i docelowy plus maska dla IPv6;
 - Protokół - np.. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd..;
 - Numery portów źródłowych i docelowych TCP, UDP;
 - Zakresy portów źródłowych i docelowych TCP, UDP;
 - Identyfikator sieci VLAN - VLAN ID;
 - Quality of Service IEEE 802.1p
 - Quality of Service DiffServ/DSCP
 - Flagi TCP;
 - Obsługa fragmentów.
103. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika;
104. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI
105. Wsparcie 8 tys. wpisów ACL na wejściu (Ingress)
106. Wsparcie 1 tys. wpisów ACL na wyjściu (Egress)
107. Obsługa IP Security:

- Trused DHCP Server,
 - DHCP Snooping and Guard,
 - Gratuitous ARP Protection,
 - DHCP Secured ARP/ARP Validation,
 - IP Source Guard.
108. Ograniczenie przepustowości (rate limiting) na portach wyjściowych;
109. Ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL;
110. Obsługa wykrywania periodycznego zaniku linku (Port-Flap):
- możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu;
 - możliwość automatycznej reakcji polegającej na wyłączeniu portu;
 - możliwość automatycznej reakcji polegającej na wyłączeniu portu na wskazany czas;
 - możliwość raportowania zdarzenia poprzez Syslog;
 - możliwość raportowania zdarzenia poprzez Trap SNMP.
111. Możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE - GCM-AES-128
112. Możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE - GCM-AES-256
113. Wydajność MACSec po rozbudowie przełącznika nie mniejsza niż: 25 Gb/s;

Zarządzanie:

114. Zarządzenia przez SNMP v1/v2/v3;
115. Obsługa SNMP Traps;
116. Obsługa synchronizacji czasu SNTP lub NTP;
117. Obsługa DNS klienta;
118. Zarządzanie przez przeglądarkę www - protokół http i https;
119. Możliwość zarządzania przez protokół XML;
120. Obsługa serwera SSH dla IPv4;
121. Obsługa serwera SSH dla IPv6;
122. Obsługa klienta SSH dla IPv4;
123. Obsługa klienta SSH dla IPv6;
124. Obsługa serwera Telnet dla IPv4;
125. Obsługa serwera Telnet dla IPv6;
126. Obsługa klienta Telnet dla IPv4;
127. Obsługa klienta Telnet dla IPv6;
128. Obsługa transferu plików:
- TFTP,
 - SFTP,
 - SCP,
129. Obsługa SYSLOG;
130. Obsługa Secure SYSLOG (TLS);
131. Obsługa SYSLOG - konfiguracja wielu serwerów SYSLOG z możliwością definicji wysyłanych zdarzeń;

- 132. Obsługa logowania komend CLI do logu systemowego;
- 133. Obsługa logowania komend do serwera SYSLOG;
- 134. Obsługa ping dla IPv4 i IPv6;
- 135. Obsługa traceroute dla IPv4 i IPv6;
- 136. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events;
- 137. Obsługa RMON2.

Inne:

- 138. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników;
- 139. Wbudowany DHCP Server;
- 140. DHCP Server z możliwością definicji opcji (np. opcje 43, 60, 78 itp.);
- 141. Wbudowany DHCP Client;
- 142. Obsługa skryptów CLI;
- 143. Obsługa funkcji TCL/Tk w skryptach CLI;
- 144. Obsługa skryptów Python 3.x;
- 145. Możliwość uruchamiania skryptów:
 - ręcznie z CLI przez administratora,
 - o określonym czasie lub co wskazany czas,
 - na podstawie zdarzeń z logu systemowego,
- 146. Możliwość edycji skryptów bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych;
- 147. Wsparcie standardu IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging;

Zgodność z normami:

- 148. EU RoHS - 2011/65/EU;
- 149. EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage;
- 150. EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation;
- 151. EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational;

Gwarancja:

- 152. Dożywotnia gwarancja na sprzęt - min. 5 lat po zakończeniu produkcji ;
- 153. Dożywotnia aktualizacja oprogramowania na przełączniku;
- 154. Kontrakt serwisowy na okres min. 12 miesięcy umożliwiający:
 - a) wymianę uszkodzonego komponentu z dostawą następnego dnia roboczego od uznania awarii;
 - b) wsparcie techniczne producenta przez linię telefoniczną, e-mail oraz zdalną sesję w cyklu 24x7.

7. Przełączniki sieciowe 24p (1 sztuka)

Wymagania podstawowe

155. Przełącznik do sieci LAN w metalowej obudowie;
156. Wysokość urządzenia 1U - montaż w standardowej szafie 19";
157. Głębokość urządzenia nie większa niż 35 cm;
158. Przełącznik musi posiadać wbudowany zasilacz AC 230V;
159. Przełącznik wyposażony w min.:
 - 24 porty 10/100/1000BASE-T;
 - 8 portów SFP+ 1/10G;
160. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex;
161. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet;
162. Przełącznik musi wspierać obsługę diagnostyki wkładek SFP/SFP+;
163. Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów;
164. Przełącznik musi posiadać możliwość łączenia do 8 przełączników w stos;
165. Przepustowość stosu min. 40 Gb/s;
166. Możliwość budowy stosu za pomocą portów 10G SFP+;
167. Stos musi zachowywać się jako jedno urządzenie logiczne, a w szczególności musi mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem;
168. Nieblokująca architektura o wydajności przełączania min. 208 Gb/s;
169. Szybkość przełączania: 154.8 Mp/s;
170. Pamięć operacyjna: min. 1 GB pamięci DRAM;
171. Pamięć flash: min. 1 GB pamięci Flash;
172. Dedykowany port konsoli szeregowej RS-232 (RJ45);
173. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika;
174. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora;
175. Możliwość instalacji min. dwóch wersji oprogramowania – firmware;
176. Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash
177. Możliwość monitorowania zajętości CPU;
178. Możliwość monitorowania zajętości pamięci;
179. Wsparcie mirroringu ruchu;
 - Lokalny mirroring na przełączniku;
 - Zdalny mirroring;
 - Zdalny mirroring do wskazanego adresu IP poprzez tunel - np. GRE;
 - Możliwość mirroringu ruchu wybranego za pomocą listy kontroli dostępu ACL.
180. Wsparcie diagnostyki okablowania - wykrywanie przerwy, zwarcia oraz odległości do awarii

Funkcje L2 przełącznika:

181. Tablica MAC adresów min. 32 tys.;
182. Obsługa sieci wirtualnych IEEE 802.1Q - min. 4 tys.;

183. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami umożliwieniem łączności do wspólnych zasobów sieciowych;
184. Obsługa Q-in-Q IEEE 802.1ad;
185. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów);
186. Obsługa STP (Spanning Tree Protocol) IEEE 802.1D;
187. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w;
188. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s;
189. Obsługa PVST+ (Per-VLAN Spanning Tree Protocol);
190. Obsługa min. 32 instancji MSTP;
191. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP;
 - obsługa min. 128 grup łączy typu Link Aggregation;
 - obsługa umożliwiająca zgrupowanie min. 8 portów;
192. Obsługa MLAG (Multi Chassis Link Aggregation);
193. Obsługa protokołu EAPS - RFC 3619;
194. Obsługa protokołu ERPS / G.8032;
195. Obsługa Quality of Service:
 - Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p;
 - Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ;
 - 8 kolejek priorytetów na każdym porcie wyjściowym;
 - Obsługa kolejek Strict Priority;
 - Obsługa kolejek Weighted Round Robin;
 - Obsługa WRED (Weighted Random Early Detection);
196. Obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB;
197. Obsługa LLDP Media Endpoint Discovery (LLDP-MED);
198. Obsługa CDPv1 oraz CDPv2;
199. Przełącznik musi posiadać obsługę AVB (Audio Video Bridging);
200. Kontrola szturmów:
 - Możliwość ograniczenia liczby pakietów Multicast na porcie;
 - Możliwość ograniczenia liczby pakietów Broadcast na porcie;
 - Możliwość ograniczenia liczby pakietów Unknown Unicast na porcie.
201. Przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP
202. Wsparcie DCB (Data Center Bridging):
 - DCBX - Data Center Bridging eXchange;
 - PFC - Priority-based Flow Control;
 - ETS - Enhanced Transmission Selection.

Funkcje L3 przełącznika IPv4:

203. Obsługa min. 500 interfejsów IP;
204. Wsparcie dla IP multinetting - wiele adresów przypisanych do jednej sieci VLAN;
205. Sprzętowa obsługa routingu IPv4;

- 206. Pojemność sprzętowej tabeli routingu min. 8 tys. wpisów;
- 207. Obsługa routingu statycznego IPv4;
- 208. Obsługa routingu dynamicznego IPv4:
 - RIP v1/v2;
 - OSPFv2 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję;
 - BGPv4 min. 2 sąsiadów - możliwość rozszerzenia do pełnej funkcjonalności przez licencję;
 - ISIS - możliwość rozszerzenia przez licencję.
- 209. Obsługa redundancji routingu VRRP dla IPv4;
- 210. Policy Based Routing dla IPv4;
- 211. Obsługa DHCP Relay ;
- 212. Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów ;
- 213. Obsługa Opcji 82 dla DHCP.

Funkcje L3 przełącznika IPv6:

- 214. Sprzętowa obsługa routingu IPv6;
- 215. Pojemność tabeli routingu min. 4 tys. wpisów;
- 216. Obsługa routingu statycznego IPv6;
- 217. Obsługa routingu dynamicznego IPv6:
 - RIPng,
 - OSPFv3 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję,
 - BGPv4 min. 2 sąsiadów - możliwość rozszerzenia do pełnej funkcjonalności przez licencję,
 - ISIS - możliwość rozszerzenia przez licencję.
- 218. Obsługa redundancji routingu VRRP dla IPv6;
- 219. Policy Based Routing dla IPv6;
- 220. Obsługa 6to4 (RFC 3056);
- 221. Opcja IPv6 Router Advertisement dla DNS - RFC 6106.

Obsługa ruchu rozgłoszeniowego:

- 222. Statyczne przyłączania portu do grupy multicast;
- 223. Filtrowanie IGMP;
- 224. Obsługa IGMP v1 - RFC 1112;
- 225. Obsługa IGMP v2 - RFC 2236;
- 226. Obsługa IGMP v3 - RFC 3376;
- 227. Obsługa IGMP v1/v2/v3 snooping;
- 228. Obsługa PIM-SM;
- 229. Obsługa PIM-DM - możliwość rozszerzenia przez licencję;
- 230. Obsługa PIM-SSM - możliwość rozszerzenia przez licencję;
- 231. Obsługa MLDv1 snooping;

- 232. Obsługa MLDv2 snooping;
- 233. Obsługa MVR (Multicast VLAN Registration).

Funkcje bezpieczeństwa:

- 234. Obsługa logowania do sieci Network Login:
 - IEEE 802.1x based Network Login;
 - MAC address based Network Login;
 - Web based Network Login.
- 235. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants);
- 236. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation;
- 237. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x;
- 238. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication ;
- 239. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink;
- 240. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na portach dołączonych do przełączników obsługujących IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging;
- 241. Automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA;
- 242. Automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA;
- 243. Przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA, np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który "przejmie" rolę uwierzytelniania klientów;
- 244. Obsługa Guest VLAN dla IEEE 802.1x;
- 245. Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci;
- 246. Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączenia i włączania portu - CoA RFC 5176;
- 247. Obsługa wymuszania ponownego okresowego uwierzytelnienia (Reauthentication);
- 248. Obsługa RADIUS Authentication (RFC 2865);
- 249. Obsługa RADIUS Accounting (RFC 2866);
- 250. Obsługa RADIUS Per-Command Authentication - uwierzytelnianie każdej komendy wydawanej przez administratora w serwerze RADIUS;
- 251. Obsługa RADIUS Authentication over TLS (RadSec);
- 252. Obsługa RADIUS Accounting over TLS (RadSec);
- 253. Obsługa TACACS+ (RFC 1492);

254. Bezpieczeństwo MAC adresów:
- ograniczenie liczby MAC adresów na porcie;
 - zatrzaśnięcie MAC adresów na porcie;
 - możliwość wpisania statycznych MAC adresów na port/vlan.
255. Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning).
256. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4:
- Adres MAC źródłowy i docelowy plus maska;
 - Adres IP źródłowy i docelowy plus maska dla IPv4;
 - Adres IP źródłowy i docelowy plus maska dla IPv6;
 - Protokół - np.. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd..;
 - Numery portów źródłowych i docelowych TCP, UDP;
 - Zakresy portów źródłowych i docelowych TCP, UDP;
 - Identyfikator sieci VLAN - VLAN ID;
 - Quality of Service IEEE 802.1p;
 - Quality of Service DiffServ/DSCP;
 - Flagi TCP;
 - Obsługa fragmentów.
257. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika;
258. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI;
259. Wsparcie 8 tys. wpisów ACL na wejściu (Ingress);
260. Wsparcie 512 wpisów ACL na wyjściu (Egress);
261. Obsługa IP Security:
- Trusted DHCP Server,
 - DHCP Snooping and Guard,
 - Gratuitous ARP Protection,
 - DHCP Secured ARP/ARP Validation,
 - IP Source Guard.
262. Ograniczenie przepustowości (rate limiting) na portach wyjściowych;
263. Ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL;
264. Obsługa wykrywania periodycznego zaniku linku (Port-Flap):
- możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu,
 - możliwość automatycznej reakcji polegającej na wyłączeniu portu,
 - możliwość automatycznej reakcji polegającej na wyłączeniu portu na wskazany czas,
 - możliwość raportowania zdarzenia poprzez Syslog,
 - możliwość raportowania zdarzenia poprzez Trap SNMP.
265. Możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE - GCM-AES-128

- 266. Możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE - GCM-AES-256
- 267. Wydajność MACSec po rozbudowie przełącznika nie mniejsza niż: 25 Gb/s;

Zarządzanie:

- 268. Zarządzenia przez SNMP v1/v2/v3;
- 269. Obsługa SNMP Traps;
- 270. Obsługa synchronizacji czasu SNTP lub NTP;
- 271. Obsługa DNS klienta;
- 272. Zarządzanie przez przeglądarkę www - protokół http i https;
- 273. Możliwość zarządzania przez protokół XML;
- 274. Obsługa serwera SSH dla IPv4;
- 275. Obsługa serwera SSH dla IPv6;
- 276. Obsługa klienta SSH dla IPv4;
- 277. Obsługa klienta SSH dla IPv6;
- 278. Obsługa serwera Telnet dla IPv4;
- 279. Obsługa serwera Telnet dla IPv6;
- 280. Obsługa klienta Telnet dla IPv4;
- 281. Obsługa klienta Telnet dla IPv6;
- 282. Obsługa transferu plików:
 - TFTP,
 - SFTP,
 - SCP.
- 283. Obsługa SYSLOG;
- 284. Obsługa Secure SYSLOG (TLS);
- 285. Obsługa SYSLOG - konfiguracja wielu serwerów SYSLOG z możliwością definicji wysyłanych zdarzeń;
- 286. Obsługa logowania komend CLI do logu systemowego;
- 287. Obsługa logowania komend do serwera SYSLOG;
- 288. Obsługa ping dla IPv4 i IPv6;
- 289. Obsługa traceroute dla IPv4 i IPv6;
- 290. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events;
- 291. Obsługa RMON2.

Inne:

- 292. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników;
- 293. Wbudowany DHCP Server ;
- 294. DHCP Server z możliwością definicji opcji (np. opcje 43, 60, 78 itp.);
- 295. Wbudowany DHCP Client;
- 296. Obsługa skryptów CLI;
- 297. Obsługa funkcji TCL/Tk w skryptach CLI;
- 298. Obsługa skryptów Python 3.x;

299. Możliwość uruchamiania skryptów:
- ręcznie z CLI przez administratora,
 - o określonym czasie lub co wskazany czas,
 - na podstawie zdarzeń z logu systemowego.
300. Możliwość edycji skryptów bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych;
301. Wsparcie standardu IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging

Zgodność z normami:

302. EU RoHS - 2011/65/EU;
303. EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage;
304. EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation;
305. EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational.

Gwarancja

306. Dożywotnia gwarancja na sprzęt - min. 5 lat po zakończeniu produkcji;
307. Dożywotnia aktualizacja oprogramowania na przełączniku;
308. Kontrakt serwisowy na okres min. 12 miesięcy umożliwiający:
- c) wymianę uszkodzonego komponentu z dostawą następnego dnia roboczego od uznania awarii;
 - d) wsparcie techniczne producenta przez linię telefoniczną, e-mail oraz zdalną sesję w cyklu 24x7.

8. Zasilacz awaryjny UPS 60kVA z instalacją (1 sztuka)

Projektuje się zasilacz UPS o mocy 60 kVA / 60 kW z topologią On-Line Double Conversion, zgodnie z klasyfikacją VFI-SS-111, z możliwością pracy równoległej.

Wymagania dot. producenta zasilacza UPS:

- a) Wymaga się, aby producent zasilacza UPS miał swoją główną siedzibę w jednym z krajów należących do NATO.
- b) Producent urządzenia musi mieć wdrożony przynajmniej od 10 lat system zarządzania jakością ISO 9001 w zakresie: projektowania, produkcji, obsługi i wsparcia technicznego dla klientów w zakresie systemów bezprzerwowego zasilania (UPS).

Wymagania ogólne:

- a) Możliwość równoległego połączenia do 4 jednostek w celu zwiększenia wydajności/redundancji;
- b) Pełna kompatybilność z agregatem prądowórczym i siecią dzięki parametrom:
 - niskie zniekształcenia prądu wejściowego do $\leq 3\%$ i współczynnik mocy $\geq 0,99$;

- „Power walk-in” opóźniony rozruch w celu zmniejszenia potrzeby przewymiarowania generatora i zapewnienia kompatybilności.

c) Jednolity nominalny współczynnik mocy wyjściowej (PF=1), z możliwością zasilania obciążeń zniekształconych, skokowych, indukcyjnych i pojemnościowych.

d) Zaawansowane technologicznie rozwiązania projektowe i komponentowe gwarantujące sprawność całkowitą: >96,5% (tryb podwójnej konwersji On-Line) i $\geq 99\%$ dla trybu ECO-MODE, z możliwością z możliwością ustawienia najbardziej odpowiedniego trybu dla danego obciążenia;

e) Oddzielenie linii obejścia awaryjnego od linii zasilającej prostownik (podwójne wejście) „Dual Input”;

f) Komunikacja LAN/SNMP; możliwość integracji z BMS;

g) Menu w języku polskim;

h) Funkcja „Cold Start” – uruchamianie zasilacza UPS z baterii.

Wymagania szczegółowe:

WEJŚCIE	
Napięcie nominalne	380-400-415 Vac 3F + N + PE
Prąd wejściowy (nominalny/maksymalny)	58/86 A
Zakres napięcia (bez przełączania na zasilanie akumulatorowe)	208÷478 Vac przy 100% obciążeniu
Częstotliwość nominalna	50 / 60Hz
Tolerancja częstotliwości wejściowej (bez przełączania na zasilanie akumulatorowe)	45-55 Hz (50 Hz); 54-66 Hz (60 Hz); autodetekcja
Całkowite zniekształcenia harmoniczne (THDi) i współczynnik mocy przy pełnym obciążeniu	THDi $\leq 3\%$, 0,99 FP
Rozruch progresywny prostownika (Power Walk-in czas trwania)	9 sekund
Opóźniony rozruch (opóźnienie rozruchu)	20 sekund
WYJŚCIE	
Moc nominalna (kVA)	60
Moc czynna PF=1 (kW)	60
Napięcie nominalne	380/400/415 Vac 3F + N + PE
Częstotliwość nominalna	50 / 60Hz
Stabilność statyczna / dynamiczna	$\pm 1\%$ / $\leq 5\%$
Współczynnik szczytu	3:1
Zniekształcenia napięcia	$\leq 1\%$ przy obciążeniu liniowym $\leq 3\%$ przy obciążeniu nieliniowym
POZOSTAŁE	
Sprawność AC/AC (On line) (%)	
• Pełne obciążenie	95.5
• 75% obciążenia	95.9
• 50% obciążenia	96.6
• 25% obciążenia	95.9
Sprawność przy zasilaczu UPS w trybie ECO (%)	≥ 99
Hałas słyszalny w odległości 1m (dBA)	50-62 dB(A) w zależności od obciążenia
Temperatura otoczenia w pomieszczeniu UPS	0 ÷ 40° C

Zalecana temperatura pracy dla optymalnego wydajność baterii	20 ÷ 25° C
Wymiary (mm)	
• Szerokość	250
• Głębokość	900
• Wysokość	868
Standardowa ładowarka do akumulatorów	25A

Zasilacz UPS należy wyposażyć w baterię akumulatorów, o minimalnym czasie pracy w trybie autonomii 60 minut przy obciążeniu 20kW. Akumulatory należy umieścić na stojaku akumulatorowym w pomieszczeniu UPS. Obliczono wymaganie 40 szt. akumulatorów 75Ah o napięciu 12V.

Należy zastosować akumulatory bezobsługowe VRLA wykonane w technologii AGM o projektowanej żywotności przynajmniej 10-12 lat dla pracy buforowej.

Dodatkowo zasilacz UPS ma być wyposażony w kartę komunikacji LAN/SNMP.

W celu umożliwienia odstawienia urządzenia, należy zainstalować zewnętrzny ręczny bypass serwisowy. Procedura przełączania musi przewidywać bezprzerwowe przełączenie na zasilanie niegwarantowane.

9. Wdrożenie

9.1. Serwery z macierzą

- a) Przygotowanie planu wdrożenia i migracji środowiska;
 - b) Instalacja dostarczonego sprzętu w szafie rack w siedzibie Zamawiającego;
 - c) Aktualizacja firmware, bios, konfiguracja zarządzania, konfiguracja sprzętowa;
 - d) Podłączenie macierzy dyskowej i serwerów z posiadaną przez Zamawiającego infrastrukturą;
- Konfiguracja:**
- e) Konfiguracja dostarczonych serwerów, macierzy dyskowej i oprogramowania, w celu uruchomienia protokołu FC – wymagana jest pełna konfiguracja hypervisora oraz dostarczonych systemów operacyjnych i sprzętu. Zamawiający wymaga takiej konfiguracji, aby zapewnić wielościeżkowość dla serwera i macierzy dyskowej z wykorzystaniem protokołu FC. System musi działać w klastrze wysokiej dostępności;
 - f) Konfiguracja wirtualizacji;
 - g) Środowisko oparte o 2 serwery fizyczne oraz współdzielony zasób macierzowy.
 - h) Konfiguracja klastra HA dla maszyn virtualnych na 2 maszynach fizycznych;
 - i) Automatyczne przenoszenie i uruchomienie maszyn virtualnych podczas awarii jednego z serwerów fizycznych na host nieuszkodzony;
 - j) Konfiguracja virtualnych switchy (podział na 4 podsieci: BACKUP, DMZ, LAN, MGMT);
 - k) Migracja oprogramowania i systemów operacyjnych znajdujących się na posiadanych przez Zamawiającego środowisku serwerowym;
 - l) Zainstalowanie najnowszej wersji systemu operacyjnego na nowym serwerze, który będzie pełnił rolę kontrolera domeny;
Przeniesienie ról FSMO z obecnego kontrolera na nowo zainstalowany serwer
 - m) Instalacja oprogramowania zarządzania zasilaczem UPS (wraz z konfiguracją i testowaniem działania zasilacza UPS);

- n) Testowanie poprawności działania przeniesionego oprogramowania oraz wykonywania połączeń z zasobami sieciowymi, logowaniem i autoryzacją użytkowników, zasadami użytkowników.

9.2. Instalacja i konfiguracja systemu do obsługi oprogramowania zarządzającego kopiami bezpieczeństwa

- a) Konfiguracja repozytoriów danych
- b) Konfiguracja zadań kopii bezpieczeństwa, retencji i zabezpieczeń.
- c) Wykonanie testów backupów, testy przywracania.

9.3. Segmentacja sieci, podział na VLAN-y

- a) Stworzenie planu podziału sieci na logiczne segmenty (VLANy) w oparciu o funkcje, lokalizację i wymagania bezpieczeństwa;
- b) Przydzielenie numerów VLANów oraz identyfikatorów (ID) dla każdego segmentu;
- c) Określenie ról VLANów, np. VLAN dla użytkowników wewnętrznych, VLAN gościnny, VLAN dla serwerów czy VLAN zarządzający;
- d) Konfiguracja przełączników sieciowych obsługujących VLANy (np. z wykorzystaniem protokołu 802.1Q do tagowania ruchu);
- e) Stworzenie i przypisanie portów trunk i access dla odpowiednich VLANów;
- f) Ustawienie routingów między VLANami na przełączniku warstwy 3 (L3) lub routerze w celu umożliwienia kontrolowanej komunikacji między segmentami;
- g) Testy komunikacji między VLANami oraz sprawdzenie, czy segmentacja działa zgodnie z założeniami.

9.4. Konfiguracja systemu kontroli dostępu do sieci

- a) Analiza istniejącej infrastruktury sieciowej, w tym identyfikacja urządzeń i użytkowników, którzy będą objęci kontrolą NAC;
- b) Określenie polityk dostępu (np. kto i jakie urządzenia mogą mieć dostęp do określonych zasobów);
- c) Przygotowanie listy kontrolnej urządzeń, które będą monitorowane i zarządzane przez system NAC (stacje robocze, laptopy, urządzenia mobilne, IoT);
- d) Przygotowanie mechanizmów redundancji oraz zaplanowanie architektury wysokiej dostępności (HA) systemu NAC;
- e) Instalacja i konfiguracja oprogramowania NAC na serwerach lub urządzeniach fizycznych;
- f) Integracja NAC z infrastrukturą sieciową (przełączniki, zapory ogniowe, routery, punkty dostępowe Wi-Fi) poprzez mechanizmy 802.1X, SNMP, RADIUS, MAC lub inne protokoły;
- g) Połączenie NAC z istniejącymi systemami bezpieczeństwa (np. Active Directory, serwery RADIUS, SIEM) w celu zarządzania autoryzacją i monitorowaniem zdarzeń;
- h) Przeprowadzenie testów autoryzacji w losowych miejscach w organizacji.

9.5. Przełączniki sieciowe

- a) Nadanie adresu IP;
- b) Konfiguracja dostępu SSH;
- c) Skonfigurowanie stosów przełączników zgodnie z zaleceniami działu IT (ustawienia przełącznika master i backup);

- d) Aktualizacja oprogramowania do najnowszej możliwej wersji;
- e) Konfiguracja segmentacji sieci VLAN;
- f) Konfiguracja protokołu MLAG, Orchestration MLAG;
- g) Uruchomienie protokołu zapobiegania pętli MSTP lub równoważny;
- h) Konfiguracja protokołu ELRP lub równoważny;
- i) Konfiguracja funkcjonalności zapobiegającej atakom typu DOS;
- j) Konfiguracja wysyłania logów do serwera logów;
- k) Konfiguracja funkcjonalności wykrywania telefonów IP, protokół LLDP lub równoważny;
- l) Uruchomienie protokołu DHCP Snooping lub równoważny;
- m) IP Przygotowanie do pracy z serwerem z wykorzystaniem protokołu Json RPC lub równoważny;
- n) Konfiguracja VLANów na wszystkich urządzeniach;
- o) Konfiguracja access listy zgodnie z wymaganiami zamawiającego;
- p) Konfiguracja protokołu STP;
- q) Konfiguracja protokołu loop protect.

9.6. Konfiguracja systemu UTM Firewall

- a) Aktualizacja oprogramowania do najnowszej możliwej wersji;
- b) Stworzenie do 500 reguł bezpieczeństwa;
- c) Konfiguracja routingu;
- d) Utworzenie polityk bezpieczeństwa;
- e) Wdrożenie funkcjonalności DPI;
- f) Wdrożenie deszyfracji protokołu SSL;
- g) Konfiguracji VLAN-ów;
- h) Konfiguracja firewall, reguły przychodzące i wychodzące na podstawie obecnie działających usług;
- i) Konfiguracja ochrony przed malware, exploitami oraz stronami zawierającymi złośliwy kod;
- j) Transfer wiedzy do klienta na temat obsługi zaproponowanej konfiguracji.

9.7. Wdrożenie systemu zarządzania siecią

- a) Instalacja maszyny wirtualnej w środowisku serwerowym;
- b) Podłączenie wszystkich przełączników do systemu;
- c) Konfiguracja harmonogramu wykonywania kopii zapasowej konfiguracji przełączników;
- d) Stworzenie mapy sieci;
- e) Wdrożenie systemu Analityki sieci;
- f) Integracja z Kontrolerem Domeny.

9.8. Testy powdrożeniowe

Po dokonaniu całości wdrożenia należy:

- a) przeprowadzić testy poprawności działania całej infrastruktury;
- b) przygotować dokumentację powykonawczą zawierającą listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów;
- c) Ze względu na krytyczne aplikacje które będą dostępne z sieci publicznej, Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

- urządzenia dedykowane (embedded), na przykład routery i przełączniki;
- punkty styku z sieciami obcymi
- zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz
- Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:
 - określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;
 - wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;
 - Badaniu będą podlegały następujące systemy: rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie), Linux; Microsoft SQL; MySQL.

10. Wymagania od Wykonawcy

Ze względu na zaawansowane wdrożenie dotyczące krytycznych aplikacji Zamawiającego, wymaga się aby Wykonawca dysponował odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia tj. do wykazania, że dysponuje co najmniej:

- 2 osobami posiadającymi wiedzę i doświadczenie w zakresie: implementacji środowisk sieciowych i systemowych opartych na platformach Microsoft Server, obejmujące instalowanie i konfigurowanie elementów systemów oraz posiadającymi wiedzę i doświadczenie w zakresie zarządzania tymi środowiskami i rozwiązywania dotyczących ich problemów, obejmujące administrowanie systemami i obsługę ich użytkowników przy spełnieniu wymagań dla Microsoft Certified Solutions Associate (MCSA) lub wymagań równoważnych, tj., określonych na nie niższym poziomie jakości, potwierdzone certyfikatem Microsoft Certified Solutions Associate (MCSA) lub innym równoważnym dokumentem (zaświadczeniem);
- 2 osobami posiadającymi wiedzę i doświadczenie w zakresie definiowania i charakteryzowania najważniejszych technik ataków stosowanych przez hakerów oraz identyfikowania i analizowania podatności na ataki hakerów w organizacji a także w tworzeniu polityki na urządzeniach IDS/IPS dotyczącej wykrywania włamań, spełniającej wymagania dla Certified Ethical Hacker (CEH) lub inne równoważne, tj. określone na nie niższym poziomie jakości niż CEH, potwierdzone certyfikatem ukończenia szkolenia Certified Ethical Hacker (CEH) lub innym tożsamym dokumentem (zaświadczeniem);
- 1 osoba posiadająca wiedzę i doświadczenie z zakresu konfiguracji i rozwiązywania problemów systemu kopii zapasowej i replikacji przy użyciu praktyk spełniających wymagania określone dla oferowanego rozwiązania lub inne równoważne;
- 1 osoba posiadająca wiedzę i doświadczenie z zakresu tworzenia skryptów i programów w języku Python na posiadanym przez Zamawiającego oprogramowaniu lub systemach operacyjnych. Przy użyciu praktyk spełniających wymagania dla PCAP - Certified Associate in Python Programming lub inne równoważne, tj. określone na nie niższym poziomie jakości niż PCAP - Certified Associate in Python Programming, potwierdzone certyfikatem PCAP - Certified Associate in Python Programming lub innym równoważnym dokumentem (zaświadczeniem);
- 1 osoba posiadająca wiedzę i doświadczenie z zakresu konfiguracji i rozwiązywania problemów na zamawianej przez Zamawiającego macierzy dyskowej, przy użyciu praktyk spełniających wymagania certyfikowane szkoleniem producenta.